وزارة التعليم العالي والبحث العلمي

جامعة أمحمد بوقرة بومرداس

كلية الحقوق والعلوم السياسية

المسطرة لإجرائية للملتقى الوطني الأول حضوريا وعن بعد الموسوم بـ: سياسات لأمن السيبراني في الجزائر في ظل التطورات الراهنة: التحديات والرهانات.

لأحد 28 أفريل2024

إعداد الدكتورة:سلاف بوصبع

جامعة أمحمد بوقرة بومرداس
كلية الحقوق والعلوم السياسية
قسم العلوم السياسية
بالشراكة مع مخبر الدراسات السياسية والدولية
وفرقة بحث PRFU اسهامات مواقع التواصل لاجتماعي في تحقيق لأمن المجتمعي في الجزائر
G02L01UN 350120190005

الملتقى الوطني الأول حضوريا وعن بعد حول:

سياسات الأمن السيبراني
في الجزائر في ظل التطورات الراهنة: التحديات والرهانات

لأحد 28 أفريل 2024

الهيئة المشرفة على الملتقى الوطني

- -الرئيس الشرفي : أ.د. ياحي مصطفى ،مدير جامعة بومرداس
- -المشرف العام: أ.د. بن صغير عبد العظيم، عميد كلية الحقوق والعلوم السياسية.
- المنسق العام: أ.د.عمروش عبد الوهاب، مدير مخبر الدراسات السياسية والدولية.
- رئيسة الملتقى الوطني: د. بوصبع سلاف
- رئيس اللجنة العلمية: د. دريادي حميدة/د.حجاج مراد
- رئيس اللجنة التنظيمية: د. بلاهدة حنان /أ. بوراش شفية
- المنسق التقني: النادي العلمي Poli talk د/ بحري سعادة

ديباجة الملتقى الوطني

خلق تغلغل تكنولوجيات لاعلام والاتصال واندماجها في كل المجالات فضاء سيبرانيا بأبعاد جديدة، تؤسس لتموقع افتراضي للفاعلين و لتفاعلات افتراضية، وهذا ما أوجد أنماطا جديدة من التهديدات لأمنية التي وجبت مجابتها بعدة تختلف عن المتعارف عليه في المجال لأمني سابقا، تجسدت فيما اصطلح على تسميته بالأمن السيبراني، وعليه قامت العديد من الدول بوضع سياسات واستراتيجيات وطنية لمواكبة التطورات الحاصلة في المجال.

وفي هذا لإطار، تسعى الجزائر كغيرها من بلدان العالم إلى التموقع ضمن الفضاء السيبراني وذلك عبر مواجهة هذه التهديدات لأمنية بمستوياتها المتعددة و بمظاهرها المتجددة، ومحاولة تجاوز التحديات المطروحة سواء على الصعيد التقني أو التشريعي أو المؤسساتي، من خلال سياسات التصدي والصمود السيبراني، والتخطيط لاستحداث "استراتيجية وطنية لأمن الأنظمة المعلوماتية".

وعليه يصبح البحث في هذه المواضيع ضرورة تفرضها التغيرات المتسارعة في المجال، والتي تغذيها التكنولوجيات الجديدة وعلى رأسها الذكاء لاصطناعي، مشكلة بذلك أحد التحديات لأصعب في معادلة السيادة الرقمية في الفضاء السيبراني.

أهداف الملتقى:

1) محاولة التأصيل المفاهيمي للظاهرة في ظل الفوضى المفاهمية الناشئة عن انعكاسات تطبيقات تكنولوجيات لإعلام والاتصال.

2) إلقاء الضوء على سياسات الجزائر في مجال لأمن السيبراني من خلال التشريعات والقوانين المتخذة في المجال ومن خلال لأجهزة والمؤسسات الموكل إليها مهمة تحقيقه والحفاظ عليه.

3)لاطلاع على الموقع الجيوسياسي للجزائر في الفضاء السيبراني في ظل التهديدات الرقمية القائمة.

4)تسليط الضوء على التحديات المطروحة في ظل التطورات التقنية الحاصلة(الرقمنة، الذكاء لاصطناعي، أنترنت لأشياء، البيانات الضخمة، الواقع المعزز.... الخ)

5)تقديم تصور تحليلي يرصد مواطن القوة لدعمها وتثبيتها ومواطنها الضعف والقصور لتجاوزها، وذلك وفق منظور شمولي.

إشكالية الملتقى:

تتأسس اشكالية الملتقى لتبحث في هذا المعطى ضمن الفضاء السيبراني، وذلك بمحاولة تحليل هذه المتغيرات واستخراج مختلف أبعادها وتمظهراتها ورصد مختلف التهديدات المستجدة، والتحديات المطروحة، فإلى أي مدى تستطيع سياسات لأمن السيبراني في الجزائر لاستجابة للتحديات الداخلية والخارجية المطروحة وتجاوز الرهانات القائمة في الفضاء السيبراني؟

محاور الملتقى:

المحور الأول: اقتراب مفاهيمي نظري من الموضوع(الأمن السيبراني في ظل التطورات الجديدة).

المحور الثاني: الإطار التشريعي والقانوني والمؤسساتي للأمن السيبراني في الجزائر.

المحور الثالث: الأمن السيبراني في الجزائر: بين التوجه العام والواقع القائم.

المحور الرابع: التحديات الداخلية والخارجية والرهانات التقنية والجيوسياسية المطروحة أمام تحقيق الجزائر لأمنها السيبراني.

المحورالخامس: تصورات استشرافية لبناء استراتيجية للأمن السيبراني في الجزائر.

أعضاء اللجنة التنظيمية

أ/ لكعص فاطمة ،أ/بركان نبيلة، أ/ شريفي ياسين، أ/حنيفي نادية ، أ/ عياش خديجة ، أ/ مسعود مطاطلة

أ/بوراش شفية أ/ بوناصر إبراهيم أ/جمال بعيرة ط.د بن جدو أسماء

أعضاء اللجنة العلمية

أ.د. عمروش عبد الوهاب جامعة بومرداس

أ.د بولعراس فتحي م.و.ع.س

أ.د. بن عياش سمير جامعة بومرداس

أ.د. مداني ليلى جامعة بومرداس

أ.د برادي نعيمة جامعة المسيلة

أ.د زياني صالح جامعة باتنة 1

أ.د. فوكة سفيان جامعة بومرداس

أ.د. سباش ليندة جامعة بومرداس

أ.د.عميري عبد الوهاب جامعة بومرداس

أ.د. خلاصي خليدة جامعة بومرداس

د.ولد جاب الله سعاد جامعة المسيلة

د. سبع فضيلة جامعة البويرة

أ.د. منصوري سفيان جامعة بومرداس

د. حجاج مراد جامعة بومرداس

د. خيلي لطفي. م.و.ع.س

د. مشري عبد الحميد جامعة بومرداس

د. حميلز سمير جامعة بومرداس

د. بن عمرواي عبد الدين جامعة بومرداس

د. عدنان زروقي جامعة بومرداس

د. مجيد مسعودي جامعة بومرداس

د. سرير عبد الله أمينة جامعة بومرداس

د. دريادي حميدة جامعة بومرداس

د. بورياح سلمة جامعة بومرداس

د. شرقي عبد الغاني جامعة بومرداس

د. زعاطشي حميد جامعة بومرداس

د. حمايدية أسماء جامعة بومرداس

د. بحري سعادة جامعة بومرداس

د. بوبصلة أمينة جامعة بومرداس

د. سعداوي عمر جامعة بومرداس

د. بلاهدة حنان جامعة بومرداس

د. بن مرسلي رافيق جامعة بومرداس

أ.د العياضي نصر الدين جامعة الجزائر3

أ.د. درويش جمال جامعة بومرداس

برنامج الملتقى

2024 أفريل 24

جامعة أمحمد بوقرة- بومرداس

كلية الحقوق والعلوم السياسية

قسم العلوم السياسية

بالشراكة مع مخبر الدراسات السياسية والدولية

وفرقة بحث PRFU اسهامات مواقع التواصل الاجتماعي في تحقيق الأمن المجتمعي

في الجزائر G02L01UN 350120190005

ينظمون الملتقى الوطني الأول حضوريا وعن بعد (عن طريق تقنية التحاضر المرئي) حول:

سياسات الأمن السيبراني

في الجزائر في ظل التطورات الراهنة: التحديات والرهانات

يوم الأحد 28 أفريل 2024

الهيئة المشرفة على الملتقى:

- **الرئيس الشرفي :أ.د. ياحي مصطفى ،مدير جامعة بومرداس**
- **المشرف العام: أ.د. بن صغير عبد العظيم، عميد كلية الحقوق والعلوم السياسية.**
- **المنسق العام: أ.د. عمروش عبد الوهاب، مدير المخبر**
- **رئيسة الملتقى الوطني: د. بوصبع سلاف**
- **رئيس اللجنة العلمية: د. دريادي حميدة/د. حجاج مراد**
- **رئيس اللجنة التنظيمية: د. بلاهدة حنان /أ. بوراش شفية رئيس قسم العلوم السياسية**
- **المنسق التقني: النادي العلمي Poli talk د/ بحري سعادة**

برنامج الملتقى:

- افتتاح الملتقى الساعة 15:00
- آيات من الذكر الحكيم
- النشيد الوطني
- كلمة رئيس الملتقى
- كلمة رئيس القسم
- كلمة عميد الكلية
- كلمة مدير الجامعة والافتتاح الرسمي للملتقى

الجلسة العلمية الحضورية الأولى: من 15:30 إلى17:00 بقاعة المحاضرات "فلسطين"

رئاسة الجلسة: د. سلاف بوصبع - د. زعاطشي حميد

	المتدخل	مؤسسة الانتماء	عنوان المداخلة
1	د. سلاف بوصبع	جامعة بومرداس	نحو تحقيق الأمن السيبراني في الجزائر: الدعائم والآليات.
2	د. ليلى سيدهم أ.د جمال درويش	جامعة الجزائر3 جامعة بومرداس.	الأمن السيبراني الوطني في مواجهة حروب الجيل الخامس
3	د. زعاطشي حميد أ. إبراهيم بوناصر	جامعة بومرداس جامعة بومرداس	صناعة الحروب النفسية الافتراضية وتأثيراتها على أمن واستقرار الدول: مقاربة علمية.
4	د. عدنان زروقي	جامعة بومرداس	حماية المعطيات ذات الطابع الشخصي في إطار الحق في الخصوصية. من منظور حقوق الإنسان على ضوء المواثيق الإقليمية والدولية
5	د. فائزة سعيداني	جامعة بومرداس	الحماية المؤسساتية للعالم الافتراضي من الجرم السيبراني(المصلحة المركزية لمكافحة الجرائم السيبرانية نموذجا.

نقاش

رابط الجلسة الحضورية الأولى: https://meet.google.com/fnn-adgp-cdr

الجلسة العلمية الحضورية الثانية: من 15:30 إلى17:00 بقاعة المخبر

رئاسة الجلسة: د. حميدة دريادي

	المتدخل	مؤسسة الانتماء	عنوان المداخلة
1	د. خديجة بوعامر	جامعة بومرداس	القصور النظري في تفسير الظاهرة السيبرانية: دراسة نقدية في المفاهيم الأساسية في الحقل النظري للعلاقات الدولية
2	د. حميدة درياد**ي**	جامعة بومرداس.	الأمن السيبراني في الجزائر: التحديات والرهانات
3	د. محمد عدار	جامعة بومرداس	الهندسة الأمنية السيبرانية في مواجهة الجرائم الالكترونية.
4	د. حمياز سمير	جامعة بومرداس	الأمن والحرب في الفضاء السيبراني: إطار مفاهيمي
5	أ.د عبد الوهاب عمروش ط/د يوسف قاسم يوسف	جامعة بومرداس. جامعة بومرداس.	الاستخدام غير المشروع لأنظمة الذكاء الاصطناعي وجرائم الإبادة الجماعية في العدوان الإسرائيلي على غزة.

نقاش

رابط الجلسة الحضورية الثانية: https://meet.google.com/xak-ctpp-wra

الجلسة العلمية الأولى على الخط(Online): من15:30 إلى17:00

رئاسة الجلسة : د. خديجة بوعامر د. عبد الحميد مشري

	المتدخل	مؤسسة الانتماء	عنوان المداخلة
1	د. بيسان مصطفى موسى	جامعة الجزائر3	دور الأمن السيبراني في الحد من الجريمة الاقتصادية و المالية الإلكترونية
2	ط/د دراويش الطيب أ/د لقرع بن علي	جامعة مستغانم جامعة مستغانم	الإدارة الرقمية وتحديات الأمن السيبراني
3	ط/د بوقفة شوقي د. زكراوي حسينة	جامعة سطيف2 جامعة سطيف2	التهديدات التي تواجهها الجزائر في ظل تزايد الجرائم السيبرانية على الفرد والمجتمع
4	د. موسى بن قاصير	جامعة قسنطينة3.	الحروب السيبرانية في العلاقات الدولية: دراسة في المفهوم التطور والتأثير
5	د/بلبشير يعقوب أ/د دلالي جيلالي	جامعة الشلف. جامعة الشلف.	دور التحول الرقمي في صياغة وتغيير المفاهيم التقليدية في الأمن والجريمة والحرب والسيادة في العصر السيبراني – قراءة في التحديات ورهانات المواجهة الوطنية-

6	ط/د تامة نسيبة د. عبد الحميد مشري	جامعة بومرداس. جامعة بومرداس.	كيف يتم بناء موضوع الامن من منظور مدرسة كوبنهاغن؟ الأمن السيبراني نموذجا
7	ط/د دلال بن عمارة	جامعة سيدي بلعباس.	الآليات التشريعية الوطنية لمكافحة الجرائم السيبرانية في عصر الذكاء الاصطناعي-واقع وتحديات-
8	Dr : HASSANI Rima-Aida *Dr. GHAMRI Sara*	université de Khenchela université de Khenchela	Le devoir de l'adaptation de l'Algérie a l'air numérique : vision à long termes, défis et *perspectives de protection cyberienne*
	-نقاش-		
	رابط الجلسة الأولى(Online): https://meet.google.com/ieg-ufva-ega		

الجلسة العلمية الثانية على الخط(Online): 15:30إلى17:00

رئاسة الجلسة : د. مراد حجاج د. سرير عبد الله أمينة

	المتدخل	مؤسسة الانتماء	عنوان المداخلة
1	د. عزيز نوري د. سميرة سليمان	جامعة خنشلة جامعة قسنطينة3	الحرب الهجينة ومهددات الأمن السيبراني
2	د. إيمان بن نعجة	جامعة الجزائر 3	الانترنت المظلم Dark web كفضاء للجريمة المنظمة السيبرانية في ظل الثورة التكنولوجية الرابعة(مقاربة مفاهمية)
3	ط/د أسماء بن جدو	جامعة بومرداس	إسهامات نظريات العلاقات الدولية في تفسير تطور مفهوم الأمن – من الأمن القوميإلى الأمن السيبراني
4	أ. نسرين سالم	جامعة سطيف2	واقع ورهانات الأمن السيبراني في العقيدة الدفاعية الجزائرية
5	ط/د.لحول حمزة ط/د أمينة لحول	جامعة تيارت جامعة المدية	الأمن السيبراني الجزائري : دراسة في الدوافع والتحديات
6	ط/د جدي علاء الدين د/ سرير عبد الله أمينة	جامعة بومرداس جامعة بومرداس	أثر المخاطر السيبرانية على الأمن القومي في الجزائر
7	Dr/ DJENDI Sarra Dr/ HADJADJ Mourad	University of Algiers 3 University of Boumerdes	The legislative framework of cyber security in Algeria
	نقاش		
	رابط الجلسة الثانية(Online): https://meet.google.com/uvi-rdys-dpe		

الجلسة العلمية الثالثة على الخط(Online): 15:30 إلى 17:00

رئاسة الجلسة: د. رافيق بن مرسلي - د. أسماء حمايدية

	المتدخل	مؤسسة الانتماء	عنوان المداخلة
1	د.رافيق بن مرسلي د. عمر سعداوي	جامعة بومرداس جامعة بومرداس	الأطر النظرية المفسرة لتطور مفهوم الأمن.
2	ط/د أمين بلعروسي د. عبابسة حمزة	جامعة الشلف جامعة الشلف	الحقوق الرقمية وتحديات الأمن السيبراني في ظل أنظمة الذكاء الاصطناعي(في القانون المقارن).
3	د/جويدة حمزاوي	جامعة سطيف2	الحروب السيبرانية وتأثيرها الاستراتيجي على الأمن القومي للدول:(الواقع و التحديات)
4	ط/د لموشي رزيقة د/ شواو عبد الباسط	جامعة قسنطينة 2. جامعة قسنطينة 2.	الجريمة الالكترونية وتهديدها للأمن السيبراني للتراث الأرشيفي الرقمي
5	د. رفاس وليد د. كامل نجيب	جامعة سطيف2 جامعة سطيف2	الأمن السيبراني عبر مواقع التواصل الاجتماعي: المخاطر والحلول
6	ط/د نصر الدين أمرار	جامعة بومرداس	التهديدات السيبرانية وسبل الردع
7	د. محمد بالجيلالي	جامعة تيارت	تأثير الجوسسة الرقمية على الأمن الجيوسيبراني الجزائري

نقاش

رابط الجلسة الثالثة(Online): https://meet.google.com/weq-eizs-fvk

الجلسة الرابعة على الخط(Online): 15:30إلى 17:00

رئاسة الجلسة د. بورياح سلمة د. حنان بلاهدة

	المتدخل	مؤسسة الانتماء	عنوان المداخلة
1	أ. منال قناوي	جامعة قسنطينة2	تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي دراسة ميدانية على عينة من مستخدمي تطبيقات التواصل الاجتماعي من الأساتذة والطلبة الجامعيين
2	ط/د صورية مزهود د. نبيل بوبية	جامعة جيجل جامعة جيجل	الحماية الرقمية: رؤية استباقية نحو تعزيز الأمن السيبراني في الجزائر.
3	د.عيدون الحامدي ط/د فرطاس رابح	جامعة سطيف2 جامعة سطيف2	في فهم وتحليل الجرائم السيبرانية والتهديدات الأمنية العابرة للحدود: مقاربة معرفية

4	ط/د محمد لسعد سيد عمر	جامعة غرداية	الجرائم السيبرانية و آليات مواجهتها في الجزائر
5	د. مولود فضيل أ/د بن عمراوي عبد الدين	جامعة بومرداس جامعة بومرداس	التربية الاعلامية الرقمية والحوسبة السحابية كآليات عملية لتحقيق الامن السيبراني الجزائري
6	د. مصطفى قديري د. سمير فارح	جامعة باتنة مركز البحث في الأنثربولوجيا الاجتماعية والثقافية CRASC	المخدرات الرقمية: تحدٍ جديد أمام القانون الدولي
7	د سلمة بورياح أ.د ليلى مداني	جامعة بومرداس جامعة بومرداس	التحديات التقنية لتحقيق الأمن السيبراني في الجزائر
8	DR/ SOUIDI Nadjib	University of Souk Ahras	conceptuel steps for cyber-security
نقاش			
رابط الجلسة الرابعة(Online): https://meet.google.com/yny-wxsq-gxa			

من 17:00 الى 17:15

قراءة التوصيات واختتام الملتقى

مداخلات

المشاركين

نحو تحقيق الأمن السيبراني في الجزائر: الدعائم والآليات

Towards achieving cybersecurity in Algeria: pillars and mechanisms

د. سلاف بوصبع جامعة بومرداس s.bousbaa@univ-boumerdes.dz

ملخص:

خلق تغلغل تكنولوجيات الاعلام والاتصال واندماجها في كل المجالات فضاء سيبرانيا بأبعاد جديدة تؤسس لتموقع افتراضي لفاعلين و لتفاعلات افتراضية وهذا ما أوجد أنماطا جديدة من التهديدات الأمنية التي وجبت مجابتها بعدة تختلف عن المتعارف عليه في المجال الأمني سابقا تجسدت فيما اصطلح على تسميته بالأمن السيبراني، مما خلق جملة من التحديات والرهانات أمام جميع الدول بما فيها الجزائر، التي تسعى لتحقيق أمنها السيبراني في هذا الفضاء اللامحدود؛ وعليه تتأسس اشكالية دراستنا لتبحث في معطى تحقيق الأمن السيبراني وذلك بمحاولة تحليله واستخراج مختلف أبعاده وتمظهراته بداية، ثم نعكف على استقراء الآليات والركائز التي من شأنها تجسيده وذلك باتباع منهج تحليلي وصفي يركن بداية الى توصيف الظاهرة ، لينتقل الى محاولة استقراء جزئياتها.

الكلمات المفتاحية: الأمن السيبراني؛ الأمن المعلوماتي؛ الفضاء السيبراني؛ تكنولوجيا الإعلام والاتصال؛ السيادة الرقمية.

Abstract:

Information and communication technologies penetrate and integrate in all areas, creating a cyberspace with new dimensions that establish a virtual location for actors and virtual interactions. This has created new patterns of security threats that must be met with a dimension different from the previous security custom, as exemplified in what has been termed spiritual security. This has created a series of challenges and bets for all States, including Algeria, that seek to achieve their cybersecurity in this limitless space; Thus, the problems of our study are based on the search for cybersecurity by attempting to analyze it and extract its various dimensions and manifestations at the outset. We are then seeking to extrapolate the mechanisms and pillars that would reflect it by adopting a descriptive analytical approach, which would depend on the beginning of the characterization of the phenomenon, so as to try to extrapolate its parts.

KeyWords: ***Cybersecurity; Information security; cyberspace; Information and communication technology; Digital sovereignty***

مقدمة:

لقد أوجد الاستخدام المتنامي لتكنولوجيات الاعلام والاتصال ، فضاء سيبرانيا بملامح ومحددات وممارسات جديدة، لدرجة أن العديد من الباحثين اعتبره بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء، و مع تزايد الاعتماد على هذه التكنولوجيات تزداد المخاطر والتهديدات السيبرانية المتطورة بصورة مستمرة في ظل تنامي انماط جديدة من التهديدات العابرة للحدود مما أصبح يشكل تحديات كبيرة للأمن القومي والدولي، وهو ما خلق ضرورة وجود ضمانات أمنية ضمن هذه البيئة الرقمية، تبلورت بشكل أساسي في ظهور الأمن السيبراني Cyber Security كبعد جديد ضمن أجندة حقل الدراسات الأمنية، وأمام هذه التحديات تقف الجزائر محاولة الاستجابة لها وتجاوزها بجملة آليات وركائز بعضها قد بدأ في الجسد والآخر لايزال رهانات تلح في الاستجابة لها لنتمكن من التموقع الجيومعلوماتي في الفضاء السيبراني وحماية السيادة الرقمية؛ و هنا تبرز إشكالية بحثنا القائمة على محاولة فهم ماهية الأمن السيبراني كمطلب ملح في السياسات الأمنية الحديثة؛ وذلك بتشريح أبعاد الظاهرة ورصد أهم الركائز والميكانيزمات لتحقيق الأمن السيبراني في بلادنا.

المحور الأول: التأصيل المفاهيمي للموضوع

إن الحديث عن أي ظاهرة مستحدثة، لزاما أن ينطلق من تأسيس مفاهيمي يتكفل بشرح هذه المفاهيم الأساسية خاصة وأنها كغيرها من مخرجات التكنولوجيا مفاهيم لم تتحدد معالمها بعد في ظل الاختلاف المفاهيمي و حتى التضارب أحيانا المعروف في العلوم الاجتماعية والانسانية .

إذن سيحاول هذا العنصر الإحاطة بمفهومي الأمن السيبراني والفضاء السيبراني وجملة من المتغيرات الأخرى التي قد تدخل في علاقة معهما ، وذلك من أجل التأسيس لفهم مشترك للظاهرة.

أولا-مفهوم الأمن السيبراني:

يعتبر مفهوم الأمن السيبراني _كغيره من مخرجات تكنولوجيا الاعلام والاتصال _ مفهوما "زئبقيا "يصعب الإمساك به، خاصة كونه يمثل ظاهرة مستجدة لم تتحدد معالمها بعد ،مما خلق ضرورة ايفاء هذا العنصر حقه من الشرح والايضاح .

1. تعريف الأمن السيبراني:

يلاحظ المتتبع للمجال وجود عدة تسميات تستخدم كمترادفات أحيانا مثل الأمن السيبراني ،الأمن المعلوماتي ،أمن المعلومات ...الخ، وعليه سنسعى لمحاولة تحديد المفهوم و علاقته بالمفاهيم الأخرى.

بداية ومن الناحية اللغوية ،يتكون هذا المفهوم من كلمتي الامن والسيبراني حيث يشير الأول بحسب معجم المعاني الجامع الى الاطمئنان فيقال أمن الرجل بمعنى اطمأن ولم يخف و أمن البلد أي اطمأن أهله؛ فيما يقال إن كلمة "السيبر " Cyber هي " لفظة يونانية الأصل مشتقة من كلمة "kybernetes" بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازا للمتحكم "governor"[1]، كما ترجعها بعض الدراسات الأخرى إلى نوربرت ويز Norbert Wiener صاحب نظرية السيبرنطيقا أو التحكم الآلي حيث تذكر بعض المراجع أنه أول من استخدم

"مصطلح السيبرانية وذلك في عام 1948 ، في أثناء دراسته لموضوع القيادة والسيطرة والاتصال في عالم الحيوان، فضلا عن حقل الهندسة الميكانيكية "[2] ؛ فيما تم الاكتفاء فقط بتعريب الكلمة كما هي في اللغة العربية بين التذبذب بين استعمال مصطلحات "الإلكتروني" "التحكم الآلي ".....الخ

أما من الناحية الاصطلاحية وفي التقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في الاتصالات لعام 2010-2011 عرف الأمن السيبراني بأنه: "مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات وممارسات فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين"[3].

وفي تعريف آخر يعرّ الأمن السيبراني عن" القدرة على مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافي، وبالتالي التحرر من الخطر او الأضرار الناجمة عن تعطيل آو إتلاف تكنولوجيا المعلومات والاتصالات أو بسبب إساءة استخدام تكنولوجيا المعلومات والاتصالات[4].

أما الناحية التقنية فيشير الأمن السيبراني إلى إدارة الهوية الالكترونية التي تنشأ بموجب استخدام تكنولوجيا الاعلام والاتصال وذلك عبر بروتوكولات التشفير التي يجب أن تتناسب مع درجة حراجة المعلومات، مع توفير المرونة السيبرانية والتي تعني الصمود أمام التهديد وصده مع امكانية المحافظة على استمرارية النظام بعد ذلك.

وعليه يمكن اعتبار الأمن السيبراني مجموعة من الإجراءات الكفيلة بضمان أمن المعلومات واستخداماتها وكذا جملة التدابير اللازمة للدفاع ضد التهديدات السيبرانية المحتملة والتعافي من نتائجها وهو بذلك أوسع من مفهوم الأمن المعلوماتي الذي يختص فقط بالشق المعلوماتي حيث يتم اتباع سياسة أمنية معينة "تصنف على ضوئها البيانات التي تقيم في نظامها المعلوماتي ،وأساليب تداولها بين مختلف مستويات الكوادر العاملة، وسبل المحافظة عليها من الانتشار و الاعلان، وحمايتها من موارد الخلل والتلف"[5] ؛ ليتوسع الأمن السيبراني فيشمل أمن المعلومات وطرق معالجتها والممارسات الموجودة في الفضاء السيبراني ، ولا أظننا نبالغ إن قلنا أنه يتعلق بحفظ "الوجود السيبراني" في حد ذاته.

كما يرتبط الأمن السيبراني بالفضاء السيبراني الذي يتشعب ويتسع شاملا المستويات الفردية وممتدا الى مجالات دولية ومشكلا بذلك جملة من الأبعاد التي قد تختلف من ناحية تمظهراتها وشدتها من بلد لآخر، وتتمثل هذه الأبعاد فيما يلي:

- البعد الاقتصادي : يرتبط الأمن السيبراني أشد الارتباط بالمجال الاقتصادي، خاصة مع ظهور الاقتصاد المبني على المعرفة، وتنامي القيمة الاقتصادية للمعلومة وكذا رقمنة عالم الاقتصاد والمال بشكل عام ، وهذا ما يترافق مع آليات تسيير وحماية هذا المجال والتي يكفلها الأمن السيبراني .
- البعد السياسي : يتمثل البعد السياسي للأمن السيبراني " بشكل أساسي، في حق الدولة في حماية نظامها السياسي، وكيانها، ومصالحها الاقتصادية"[6]،مع الاشارة الى تنامي الدور السياسي للفرد في ظل منافذ جديدة وسريعة للاتصال السياسي .
- البعد الاجتماعي : يحمل الفضاء السيبراني عديد الأبعاد الاجتماعية ،إنه يتقاطع بشكل لافت مع هذا المجال ويسفر هذا التقاطع عن وجوه ايجابية من الارتباطات الاجتماعية والتنوع الثقافي والخلفيات الايديولوجية والمظاهر

الحضارية ،وفي الوقت نفسه عن محتويات ومضامين غير مشروعة كالاستقطاب الإلكتروني لمجموعات عرقية أو دينية أو ايديولوجية منبوذة مجتمعيا ، وهنا يبرز الدور المنظم والرادع للأمن السيبراني.

- البعد العسكري : لقد ارتبط الأمن السيبراني بالمجال العسكري ارتباطا وثيقا، جعلت الجيوش تخصص له قيادة خاصة، سواء تعلق الأمر بالأمن السيبراني في الفضاء السيبراني أو بالعلاقة بين هذا العنصر والمنشآت العسكرية والعملياتية الميدانية، و ذلك مثلا "عن طريق قدرة القوة السيبرانية على ربط الوحدات العسكرية ببعضها البعض في العالم الافتراضي، وهذا ما يسهل عملية تبادل المعلومات والذي ينعكس ايجابا على تحقيق الأهداف العليا للمؤسسات العسكرية"[7].

2. تعريف الفضاء السيبراني:

يرتبط الأمن السيبراني بالفضاء السيبراني الذي يعتبر مجال تواجده وتطبيقه؛ ويتقاطع معه في كثير من الخصائص كالطبيعة الافتراضية وارتباطها باستخدام تكنولوجيات الاعلام والاتصال مثلا؛ مما يجعل القاء الضوء عليه ضرورة لتكملة التاسيس المفاهيمي للموضوع .

لقد ظهر مصطلح الفضاء السيبراني في ثمانينيات القرن الماضي في إحدى روايات الخيال العلمي للكاتب الأمريكي-الكندي المشهور وليام جيبسون، حيث يعتمد هذا المجال الافتراضي على نظم الكمبيوتر وشبكات الانترنت ومخزون هائل من المعلومات والبيانات، فيتم التواصل بالشبكات عبر الهواتف وأجهزة الحواسيب دون التقيد بالحدود الجغرافية[8].

وقد أسس هذا المفهوم الحديث نسبيا على مفهوم آخر وهو مفهوم الفضاء العمومي، ولو أن هذا الأخير أقل منه اتساعا وتنوعا، لكنه يتقاطع معه في كونهما يعبران معا عن حيز أو مجال للأفكار ليس محدود بحدود فيزيائية ثابتة، وفي هذا الصدد يرى صادق الحمامي انّ تكنولوجيات الإعلام والاتصال أو ما عُبر عنها بالميديا الجديدة قد ساهمت في إعادة المفهوم الحقيقي للفضاء العمومي والذي ظهر خلال القرن الثامن عشر بأروبا الغربية، تحولت فيه أماكن عامة (كالمقاهي والمكتبات والنوادي الفكرية) إلى فضاءات يتبادل فيها النقاش والحديث عن " مسائل تتعلق بالفنّ والأدب في مرحلة أولى، ثم في المسائل السياسية بعد الثورة الفرنسية؛"[9] فكان ان تميزت هذه الفضاءات بنقاشات وجدلات عقلانية، ما لبثت أن اختفت مع ظهور وسائل الإعلام إذ يعتبر هابرماس Habermas في هذا الإطار "وسائط الإعلام تستقطب المشاهدين والمستمعين، ولكنها تسلبهم في الوقت ذاته تلك المسافة التحررية، أي إمكانية الحجاج والكلام والنقض"[10]؛ لتعود هذه الإمكانيات للظهور مع الميديا الجديدة التي استطاعت بذلك "إحياء النموذج الأصيل والأصلي للمجال العمومي وتجديده من خلال تيسير نفاذ المشاركين إلى النقاش العام وتعزيز طابع التنوع الفكري عبر استحداث فضاءات أخرى جديدة للنقاش وتجاوز التنميط الفكري"[11]؛ وهذا يعني أنّ النشاط في الفضاء العمومي يمكن أن يتوسع، إذ تم منحه فضاءات جديدة وفاعلين جدد بأشكال تعبيرية جديدة وهذا ما ساهم في خلق جماعات ضغط جديدة ، وعليه فقد توسع الفضاء العمومي مشكلا فضاء عموميا افتراضيا بنخب جديدة وأشكال جديدة من الفعل الجماعي...إلخ، وانطلاق من هذا المنظور يمكن الحديث عن الفضاء السيبراني كمستو آخر من مستويات التواجد.

ولتعريف الفضاء السيبراني يمكن الاعتماد على الاتحاد الدولي للاتصالات الذي يصفه بأنه "المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي : اجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكم، و مستخدمو كل هذه العناصر"[12].

كما عرفته الوكالة الفرنسية لأمن أنظمة الإعلام ANSSI، وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي، بأنه: "فضاء التواصل المشكّل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية"؛ فهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكوّن من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين او مستعملين. كما أن هناك مَن عرّف الفضاء السيبراني بوصفه الذراع الرابعة للجيوش الحديثة"[13]، حيث يلاحظ في الآونة الأخيرة لجوء متناميا للدول نحو الفضاء السيبراني لتحقيق المصالح باقل تكاليف ممكنة في ظل ظهور تمظهرات جديدة كالفواعل الرقمية التي تتحرك في هذا الفضاء، والقوة الناعمة التي أضحت بديلا استراتيجيا للقوة بمفهومها التقليدي خصوصا مع ما يفرضه تعاظم دور الرأي العالمي، وتغير قواعد الصراع وآلياته وميادينه مما خلق تحديات جديدة للدول في هذا الفضاء.

ثانيا- الأمن السيبراني والتهديدات الأمنية: آليات الهجوم والدفاع:

يحيلنا الحديث عن الأمن بالضرورة الى الحديث عن نقيضه وذلك بتبيان التهديدات التي قد تطال هذا الأمن والتي تدخل هي الأخرى تحت مسميات متعددة قد تختلف أحيانا وقد تتمايز احيانا اخرى ولكنها تجتمع تقنيا كلها تحت ما يسمى القرصنة الالكترونية والتي تعني اختراق أجهزة الحاسوب عبر ثغرات في أنظمة الحماية "بقصد المساس بالسرية أو بسلامة المحتوي والتكاملية أو تعطيل القدرة والكفاءة للانظمة للقيام بأعمالها"[14] ؛ وذلك باستخدام العديد من التقنيات مثل :

- حصان طروادة Trojan Horse : وهو "برنامج تجسسي يقوم بعمل معين ، يحدده الشخص الذي صممه أو زرعه في جهاز الضحية "[15] وذلك بالتسلل اليه عبر ارسال ملف عن طريق البريد الالكتروني مثلا ، ويعتبر من أخطر آليات القرصنة حيث أنه ذو طبيعة ساكنة تصعب كشفه، كما أنه يسمح للهاكر بالتحكم الكامل في الجهاز عن بعد بواسطة تقنيات خاصة.
- الفيروسات Virus: هي برامج قد تم تصميمها لإلحاق الضرر بالحاسوب وتعطيله وذلك عن طريق تكرار نفسه "مما يتيح له فرصة الانتشار داخل جهاز الحاسب في أكثر مكان من الذاكرة ليدمر البرامج والبيانات الموجودة في ذاكرة الجهاز"[16]
- الديدان Worms: وهو برنامج صغير يختلف عن الفيروس في عدم حاجته لخطوة من المستخدم (كفتح ملف مثلا) لتنتشر في الجهاز، وهو يمتاز بالمراوغة والتلون و بقدرته على التنقل عبر شبكة الانترنت وشل حركتها أو التشويش عليها.

وتقنيا دائما ، يجب أن تتوفر جملة من الآليات التي تواجه هذه الميكانيزمات الهجومية وتسهر على حماية وأمن الفضاء السيبراني لعل أهمها:

- جدار النار
- التشفير الالكتروني

- التحقق الحيوي والبيولوجي (Biometric)
- التوقيع والتصديق الالكتروني.
- الشهادة الرقمية .

وعموم القول، تأخذ التهديدات الالكترونية عدة أنماط وأشكال لعل أهمها: [17]

- الاعتداء على الأنظمة التي تتولى إدارة البنية التحتية، كالنقل، وموارد الطاقة، والمؤسسات

المالية أو حتى أنظمة المعلومات المعدة لمواجهة حالات التوقف، الاعطال، اعادة الحال إلى ما كان عليه، باسترجاع مهمات الأنظمة وبياناتها.

- الاعتداء على انظمة الدفاع سواء منها تلك المخصصة للهجوم أو للدفاع، وهنا تستبعد قانونية الضربات الاستباقية ،في حال الاعتماد على هذا المفهوم لتبرير الاعتداء .
- الاعتداء على أنظمة الحكومة الإلكترونية، والادارات المختلفة في القطاعين العام والخاص.
- الاعتداء الذي يستهدف التلاعب بالمعلومات، بهدف تضليل السلطات العامة، أو زرع البلبلة في المجتمع وبين المواطنين.
- التجسس الإلكتروني.
- الرقابة الشاملة، ورصد الاشخاص، و إرهابهم بهدف جمع المعلومات منهم.

وإذا قاربنا الموضوع من ناحية الهدف، نجد أن الهجمات الالكترونية قد تستهدف أهدافا اقتصادية كالهيئات المالية والاقتصادية مما يكبدها خسائر ضخمة اضافة الى المساس بسمعتها أو أهدافا عسكرية أو حتى تجعل من البنية التحتية الأساسية هدفا لها كالأنظمة الكهربائية مثلا.

كما أن لهذه الهجمات عدة مستويات على اعتبار أن الأمن السيبراني ينطلق من النطاق الضيق للأفراد في إطار حماية الخصوصية مرورا بالمؤسسات والمنظمات من خلال حماية بياناتها أو ما يعبر عنه بالأمن المعلوماتي، ليتسع شاملا الدولة و أمنها القومي ككل، وتتمثل المستويات في :

- القرصنة السيبرانية: وتقع في المستوى الأول، ومن أمثلته القيام بعمليات قرصنة المواقع الإلكترونية أو بتعطيل الحواسيب الخادمة Servers من خلال إغراقها بالبيانات.
- الجريمة السيبرانية والتجسس السيبراني: ويقعان في المستوى الثاني والثالث وغالبا ما يستهدفان الشركات والمؤسسات وفي حالات نادرة بعض المؤسسات الحكومية.
- الإرهاب السيبراني: ويقع في المستوى الرابع ويعبر عن الهجمات غير الشرعية التي ينفذها فاعلون غير حكوميون ضد اجهزة الكمبيوتر والشبكات والمعلومات المخزّنة.
- الحرب السيبرانية: وهي المستوى الأخطر للنزاع في الفضاء السيبراني، وتهدف إلى التأثير على إرادة الطرف المستهدف السياسية وعلى قدرته في عملية صنع القرار، وكذلك التأثير فيما يتعلق بالقيادة العسكرية و/أو توجهات المدنيين في مسرح العمليات الإلكتروني.

المحور الثاني: آليات تجسيد الأمن السيبراني في الجزائر

يعتقد البعض أنه من السابق لأوانه الحديث عن الأمن السيبراني في الجزائر، لكننا نرى أنه وضمن مسمى الحتمية التكنولوجية التي نؤمن بها، والتي تجعل من استخدام هذه التكنولوجيات واقعا مفروضا ومسارا خطيا لابد من المرور عبره، وصولا إلى تغلغل تكنولوجيات الإعلام والاتصال في كل الممارسات القائمة؛ وعليه تقتضي هذه الوضعية حماية استباقية للبيانات بداية وكذا آليات للتعافي في حالة حدوث اختراقات الكترونية، وهذا ما يجعل الحديث عن الأمن السيبراني أمرا لا مفر منه، خصوصا بعد انتقال هذا المفهوم إلى مدى أوسع من الشمولية، حيث أصبح يحتوى عدة مستويات تبدأ من الإطار الضيق لحماية البيانات الشخصية او ما يسمى بالخصوصية ليصل في أعلى مستوى لحماية البيانات ذات درجة الحراجة العالية كتلك البيانات المتعلقة بالأمن القومي.

ومن ناحية ثانية، فقد انتقل مفهوم الأمن السيبراني من الجانب التقني البسيط الذي يتصل باستخدام التكنولوجيا الإعلام والاتصال، والذي كان مقتصرا على التهديدات التي قد تطال البنية التحتية للتكنولوجيا، أي النظر اليه باعتباره تعطيلات تقنية إلى منظور أوسع بعد ان ارتبط بأنماط مختلفة من المخاطر مثل حماية البيانات الخصوصية وأمن المعلومات وإدارة البيانات والمعرفة بما في ذلك السلامة والأمن الماديين.

ولتحقيق الأمن السيبراني في الجزائر يتوجب علينا تجسد عدة آليات تتكامل فيما بينها لتخلق منظومة دفاعية واستباقية في مواجهة المخاطر الالكترونية المتصاعدة ، تتمثل في الآتي:

أولا: الآليات التقنية:

إن الحديث عن التقنية هو حديث متشعب يطرح العديد من الإشكالات ويثير الكثير من الجدل، ذلك أنه ووفق ما هو كائن نلاحظ أننا مستخدمون لتكنولوجيا لا ننتجها وهذا ما يطرح رهانا وتحديا يفضي إلى صعوبة "تحييد" هذه التكنولوجيا والنظر إليها بصفتها آلة فحسب، لأننا نعتقد جازمين أن استخدام هذه التكنولوجيا سيتأثر حتما بخلفية مُنتجها.

وعليه ولتحقيق الأمن السيبراني في الجزائر المستوردة لهذه التكنولوجيا، لزاما علينا الاتي:

- توطين التكنولوجيا وتقوية البنية التحتية: لا نستطيع الحديث عن إنتاج هذه التكنولوجيا ببلدنا بصفة كلية وشاملة بين ليلة وضحاها، فالأمر هنا ليس ممكنا في ظل المعطيات الموجودة حيث تقتصر الصناعة الإلكترونية في الجزائر على بعض الصناعات التركيبية فقط؛ على أنه قد يصبح ممكنا على المدى البعيد؛ وعلى اعتبار أن التقنية أو التكنولوجيا في حد ذاتها تحمل شقين احدهما يعبر عن العتاد أو الآلات أو الأجهزة المختلفة التي نستخدمها، والثاني يتمثل في مختلف البرمجيات والتطبيقات التي تقوم بتشغيل هذا العتاد؛ ومنه إن تحقيق الأمن السيبراني يمر عبر هذين المعطيين: بداية عبر تأمين هذه الأجهزة التقنية والتي كما اسلفنا توفير إمكانية إنتاجها وصناعتها و أنها نوعا ما بعيدة المدى بالنسبة للجزائر في الوقت الحالي؛ والشيء الثاني هو عندما نتحدث عن التطبيقات والتي تشمل التطبيقات الكفيلة بالتشغيل في حد ذاتها بدرجة أولى والتطبيقات المخول لها تحقيق الحماية و الأمن المعلوماتي بدرجة ثانية؛ وعليه وهنا يجري الحديث عن التطبيقات الذكية واستخدام أنظمة حماية عالية واجراءات حماية التقنية حيث نجد مسعى الجزائر في تشجيع الابتكار ودعم المؤسسات الناشئة في مجال التطبيقات والبرامج الإلكترونية المختلفة.

ومن ناحية ثانية، وفي الشق التقني دائما يجري الحديث عن ضرورة الوصول إلى مرحلة توطين التكنولوجيا في مختلف المجالات وإعادة تهيئة البنية التحتية اللازمة للوصول إلى مرحلة التشبع التكنولوجي، وكذا التمكين التكنولوجي لكل فئات وطبقات المجتمع فلا تصبح التكنولوجيا حكرا على فئة دون غيرها، وهذا ما يرافق الاستراتيجية التي تتبعها الجزائر لزيادة حجم تدفق الأنترنت عن طريق النطاق العريض للاتصالات السلكية واللاسلكية والجيل الخامس بالنسبة للهاتف المحمول.

- ثانيا الجانب التشريعي و المؤسساتي: إن الأمن السيبراني لا يكتمل تجسيده فقط في الجانب التقني بتوفير البنية التحتية اللازمة ، وإنما يتعداه إلى ضرورة توفر نمطين من التأطير يتمثل الأول في وجود آليات تشريعية تنظيمية لحماية وتنظيم التواجد السيبراني في الفضاء الرقمي، ويختص النمط الثاني بالمؤسسات والأجهزة التي تعكف على تجسيد الأمن السيبراني ومواجهة الاختراقات المحتملة والتصدي للهجمات الالكترونية الحاصلة؛ على أن تنقسم هذه الآليات إلى استراتيجيات شاملة تمثل رؤى كلية للأهداف والسياسات العامة، وتمثل سلسلة من القوانين والمراسيم والتشريعات التي تؤطر الممارسة الرقمية و توفر عنصرالردع لمرتكبي الجريمة الالكترونية .

بينما يعني الأمر الثاني وبالسياسات العامة لنتحدث عن سلسلة من المبادئ والإجراءات الميدانية، و المتمثلة في الاجهزة المؤسساتية والأمنية الكفيلة بتطبيق هذه الأهداف والسياسات والتشريعات سواء على المستوى الضيق للمنظمات المختلفة أو على المستوى الكلي للدولة، والتي تتكفل بها الأجهزة الأمنية في الدولة مثل الجيش الوطني الشعبي أو الدرك الوطني وغيرها.

ثانيا: الثقافة التقنية:

تعتبر الثقافة التقنية من الأمور التي نركز عليها كثيرا على اعتبار أن المحرك لكل هذا هو الإنسان، وعليه يجب أن يمتلك هذه الثقافة والتي تؤهله للحفاظ على سلامة معلوماته؛ والثقافة التقنية هي أن نكتسب المهارات التي تسمح لنا بالتحكم الأمثل في التكنولوجيا خصوصا امام رهانات الذكاء الاصطناعي، هذا الغول الجديد الذي لم تظهر بعد انعكاسات استعمالاته؛ وعليه يمكن أن نقسم هذه المهارات الواجب الواجي اكتسابها إلى ثلاثة فئات أساسية:

- المهارات الأدائية: وهي مهارات متعلقة بإمكانية التحكم في الأدوات والبرمجيات، اي المعرفة التقنية وكذا إمكانية مواجهة المشاكل المطروحة.
- المهارات المعلوماتية: وتحيل إلى البحث والإختيار والفهم، وتقييم ومعالجة المعلومات.
- المهارات الاستراتجية: ترتبط باستعمال المعلومة بطريقة استباقية، مما يعطيها معنى من قبل المستخدم في حياته وفي محيطه.

وعليه يتم التأكيد أن الأمن السيبراني ليس فقط على المستوى الكلي بل حتى على المستوى الضيق للأفراد وذلك ما يخلق ضرورة وجود ثقافة تقنية،وكذا ضرورة الحفاظ أيضا على البيانات الشخصيةمن ناحية، ومن ناحية ثانية، وبشكل أكثر تخصصا يجري الحديث عن المورد البشري المتخصص والكفؤ، خاصة بالنسبة للمنظمات المختلفة،

فيما يتعلق بالمعلومات والبيانات ذات درجة الحراجة العالية، زمن ناحية ثالثة والتي تظهر على الصعيد الخارجي وهو الموقع الجيومعلوماتي للبلاد ككل، ويتمثل في حماية الحيز أو المجال السيبراني، حيث ظهرت تحديات ورهانات جديدة في الفضاء السيبراني فقد تغيرت قواعد اللعبة متخذة عدة أوجه، الذي تأخذ علاقته بالعالم الحقيقي عدة أوجه تتراوح بين علاقات الامتداد و التوازي والتداخل أحيانا، ليسفر ضمن هذا الروابط العلائقية عن ممارسات جديدة كرست لأطر جديدة مثل ظهور فواعل رقمية تختلف عن الموجود قبلا، وكذا ظهور القوة الرقمية أو القوة الناعمة التي يزداد اللجوء إليها في الصراعات الدولية الحالية، وهذا ما يقتضي ضرورة التحسن الرقمي وحماية السيادة الرقمية والتموقع الجيومعلوماتي ووضع أطر لحماية البيانات المتعلقة بالدولة ومن الناحية الثانية كلما اعتمدت الدولة على الفواعل الرقمية والحضور الرقمي زادت إمكانية سيطرتها على الفضاء السيبراني والتحكم في المتغيرات المتسارعة في العالم الواقعي.

خاتمة:

إن تحقيق الأمن السيبراني لا يتم إلا عبر تحقيق منظومة متكاملة من الآليات التي تسمح بتحكم تقني أفضل ويوفر سبل المواجهة والصمود والتعافي أمام تصاعد التهديدات الالكترونية في ظل حتميات التحول الرقمي والتي تقتضي الانتقال إلى تعميم استخدام الحوكمة الرقمية وما ينجر عليها من ضرورات حماية المعلومات المتوفرة في نطاق ما يسمى الأمن المعلوماتي، بل وتذهب أبعد من ذلك إلى ضرورة توفير حماية للتواجد السيبراني للدولة والذي ينطلق من المستوى الضيق لحماية خصوصية الأفراد في استخداماتهم لتكنولوجيات الإعلام والاتصال ليصل إلى أعلى مستوى والملازم للأمن القومي وذلك وكما أسلفنا لا يتم إلا وفق نظرة كلية تنطلق من انتاج هذه التكنولوجيات والتطبيقات وصولا إلى التحكم في استخداماتها المتعددة.

الهوامش والمراجع:

[1] بن مرزوق عنترة(2017)، لأمن السيبراني ، اطلع بتاريخ 24 ديسمبر 2019 عليه من موقع : https://dspace.univ-ouargla.dz/jspui/handle/123456789/14052

[2]أحمد الفتلاوي ، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية ،العدد الرابع/ السنة الثامنة 2016.ص614

[3] منى لأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية و القضائية، جامعة الدول العربية ،2016. ص26

[4] Sandro Bologna, Bernhard Hämmerli, Dimitris Gritzalis, Critical Information .41 Infrastructure Security. Berlin ; Springer, 2013, P30 -30. في عنترة بن مرزوق ،الأمن السيبراني كبعد جديدفي السياسة الدفاعية الجزائرية، ص 67

[5] نسيمة درار، الأمن المعلوماتي وسبل مواجهة مخاطره في التعاملات الالكترونية، أطروحة دكتوراه غير منشورة ، جامعة باتنة بلقايد كلية الحقوق والعلوم السياسية ،2016/2015 ، ص ص 14، 15 .

[6] نفس المرجع السابق ،ص 29

[7]يوسف بوغرارة ، الأمن السيبراني :الاستراتيجية الجزائرية للأمن والدفاع الفضاء السيبيري،مجلة الدراسات الأفريقية وحوض النيل ،العدد الثالث سبتمبر 2018 ،ص 108.

[8] نفس المرجع السابق، ص 103

[9] صادق الحمامي، المديا الجديدة والمجال العمومي :الإحياء والانبعاث، مجلة الإذاعات العربية،عدد 3، 2011،ص16.

[10] نفس المكان.

[11] نفس المرجع السابق،ص20.

[12]اسماعيل زروقة ، الفضاء السيبراني والتحول في مفاهيم القوة والصراع. مجلة العلوم القانونية والسياسية المجلد10 العدد1، 2019، ص1017.

[13] بن مرزوق، مرجع سبق ذكره.

[14]فتيحة ليتيم ؛ نادية ليتيم ، (2015)الأمن المعلوماتي الحكومة الإلكترونية و إرهاب الفرصة، المالع عليه بتاريخ 2019/10/24 من الموقع : https://platform.almanhal.com/Details/Article/79779

[15]نسيمة درار ، مرجع سبق ذكره ، ص97

[16]فتيحة ليتيم ؛ نادية ليتيم، مرجع سبق ذكره .

[17] منى الأشقر جبور ، مرجع سبق ذكره ،ص ص49، 50

الأمن السيبراني الوطني في مواجهة حروب الجيل الخامس

National cybersecurity facing the fifth-generation wars

سيدهم ليلى جامعة الجزائر 3 sidhoum.leila@univ-alger3.dz
درويش جمال جامعة بومرداس d.derouiche@univ-boumerdes.dz

ملخص:

تطورت طبيعة الحرب بشكل كبير على مر القرون، وتكيفت مع التغيرات في التكنولوجيا والمجتمع والديناميات العالمية. تقليديا، تم تعريف الحرب من خلال الاشتباكات العسكرية الحركية المباشرة. ومع ذلك، كان قدوم القرن الحادي والعشرين بمثابة ظهور شكل أكثر تعقيدا ودقة من الصراع المعروف باسم حرب الجيل الخامس (FGW). وعلى عكس سابقاتها، تتميز حروب الجيل الخامس بعدم التماثل، وعدم وضوح الحرب والسلام، والدور الهام للمعلومات والعمليات السيبرانية. تمثل تقنية الجيل الخامس نقلة نوعية في التفكير الاستراتيجي، حيث غالبا ما تطغى وسائل الحرب غير الحركية على الجيش التقليدي. حيث يتحدى هذا الجيل الجديد من الصراع المفاهيم التقليدية للحرب والسلام، والتي تشمل مجموعة واسعة من الجهات الفاعلة الحكومية وغير الحكومية، وتستفيد من التكنولوجيا لتحقيق أهداف استراتيجية دون اللجوء إلى الأعمال العدائية المفتوحة والمباشرة. وقد امتدت ساحة المعركة إلى العالم الرقمي، مما يجعل الأمن السيبراني مصدر قلق بالغ للأمن القومي. حيث تعد التكتيكات غير المتماثلة سمة مميزة أخرى لحروب الجيل الخامس. ويمكن للجهات الفاعلة غير الحكومية، بما في ذلك الجماعات الإرهابية، والقراصنة، وحتى الشركات، أن تمارس نفوذا كبيرا وتعطل سلطات الدولة بشكل فعال.

الكلمات المفتاحية: الأمن السيبراني؛ الأمن الوطني؛ حروب الجيل الخامس؛ التهديدات؛ الصراع.

***Abstract**: The nature of warfare has evolved dramatically over the centuries, adapting to changes in technology, society, and global dynamics. Traditionally, war has been defined by direct kinetic military engagements. However, the advent of the 21st century has ushered in a more complex and nuanced form of conflict known as Fifth Generation Warfare (FGW). Unlike its predecessors, fifth-generation warfare is characterized by asymmetry, blurring of war and peace, and the important role of information and cyber operations. Fifth generation technology represents a paradigm shift in strategic thinking, as non-kinetic means of warfare often overwhelm the traditional military. This new generation of conflict challenges traditional notions of war and peace, which includes a wide range of state and non-state actors, and leverages technology to achieve strategic objectives without resorting to open and direct hostilities. The battlefield has extended into the digital world, making cybersecurity a critical national security concern. Asymmetric tactics are another hallmark of fifth generation warfare. Non-state actors, including terrorist groups, hackers, and even corporations, can exert significant influence and effectively disrupt state authorities.*

***KeyWords :** cybersecurity; National Security; Fifth generation warfare; Threats; Conflict.*

مقدمة:

لقد تطورت طبيعة الحرب بشكل كبير على مر القرون، وتكيفت مع التغيرات في التكنولوجيا والمجتمع والديناميات العالمية. تقليديا، تم تعريف الحرب من خلال الاشتباكات العسكرية الحركية المباشرة. ومع ذلك، كان قدوم القرن الحادي والعشرين بمثابة ظهور شكل أكثر تعقيدا ودقة من الصراع المعروف باسم حرب الجيل الخامس (FGW). وعلى عكس سابقاتها، تتميز حروب الجيل الخامس بعدم التماثل، وعدم وضوح الحرب والسلام، والدور الهام للمعلومات والعمليات السيبرانية. تمثل تقنية الجيل الخامس نقلة نوعية في التفكير الاستراتيجي، حيث غالبا ما تطغى وسائل الحرب غير الحركية على الجيش التقليدي. حيث يتحدى هذا الجيل الجديد من الصراع المفاهيم التقليدية للحرب والسلام، والتي تشمل مجموعة واسعة من الجهات الفاعلة الحكومية وغير الحكومية، وتستفيد من التكنولوجيا لتحقيق أهداف استراتيجية دون اللجوء إلى الأعمال العدائية المفتوحة والمباشرة.

وقد امتدت ساحة المعركة إلى العالم الرقمي، مما يجعل الأمن السيبراني مصدر قلق بالغ للأمن القومي. حيث تعد التكتيكات غير المتماثلة سمة مميزة أخرى لحروب الجيل الخامس. ويمكن للجهات الفاعلة غير الحكومية، بما في ذلك الجماعات الإرهابية، والقراصنة، وحتى الشركات، أن تمارس نفوذا كبيرا وتعطل سلطات الدولة بشكل فعال. ويجعل عدم التماثل هذا من الصعب على القوات العسكرية التقليدية الاستجابة بفعالية، حيث أن الخطوط الفاصلة بين المقاتلين وغير المقاتلين غالبا ما تكون غير واضحة. كما أصبحت الحرب النفسية وعمليات التأثير أكثر وضوحا. ففي حروب الجيل الخامس، تعتبر المعركة من أجل القلوب والعقول لا تقل أهمية عن أي مواجهة جسدية. إن الدعاية والمعلومات المضللة والتلاعب بوسائل الإعلام هي أدوات شائعة الاستخدام لتشكيل التصور العام والمشهد السياسي.

يجلب عصر حروب الجيل الخامس معه مجموعة من التحديات العالمية. على سبيل المثال، تشكل تهديدات الأمن السيبراني خطرا كبيرا على الأمن القومي والاستقرار العالمي. إن الترابط المتزايد بين العالم يعني أن الهجوم السيبراني على دولة واحدة يمكن أن يكون له آثار بعيدة المدى، مما يؤثر على كل شيء من الأسواق المالية إلى البنية التحتية الحيوية. كما أصبح انتشار المعلومات الخاطئة ودور وسائل التواصل الاجتماعي في نشرها مصدر قلق كبير. وفي عصر حيث يمكن نشر المعلومات بسرعة وعلى نطاق واسع، فإن القدرة على التأثير على الرأي العام والقرارات السياسية من خلال معلومات كاذبة أو مضللة تشكل سلاحا قويا. الحرب الاقتصادية، وهي جانب آخر من جوانب حروب الجيل الخامس، تنطوي على استخدام الأدوات الاقتصادية مثل العقوبات، والحروب التجارية، والتلاعب المالي لتحقيق الأهداف الاستراتيجية. يمكن أن يكون لهذا الشكل من الحرب تأثيرات عميقة على الاستقرار المالي العالمي ويمكن استخدامه لممارسة النفوذ السياسي والاستراتيجي دون اللجوء إلى الوسائل العسكرية التقليدية.

وفي مواجهة هذه التحديات المتعددة الأوجه، يجب على الدول والمنظمات الدولية تطوير استراتيجيات شاملة تتجاوز الاستجابات العسكرية التقليدية. تحتاج البلدان إلى مراجعة استراتيجيات الأمن القومي الخاصة بها لمعالجة التهديدات المتنوعة التي تشكلها تقنية حروب الجيل الخامس. ويتضمن ذلك تعزيز الدفاعات السيبرانية، وتطوير قدرات المراقبة والاستخبارات المتقدمة، وتعزيز فهم أعمق لحرب المعلومات. إن النهج المتعدد الطبقات الذي يتضمن القدرات الهجومية والدفاعية يشكل أهمية بالغة في حماية المصالح الوطنية في العصر الرقمي. تتطلب الطبيعة العابرة للحدود الوطنية لتهديدات حروب الجيل الخامس تعاونا دوليا أكبر.

ومن الممكن أن يؤدي تبادل المعلومات الاستخبارية، ومواءمة بروتوكولات الأمن السيبراني، وإجراء عمليات مشتركة ضد التهديدات المشتركة إلى تعزيز الموقف الأمني الجماعي. ويحتاج القانون الدولي أيضا إلى التطور حتى يتمكن من التصدي للتحديات الفريدة المتمثلة في الحرب السيبرانية والتلاعب بالمعلومات. إن الاستثمار في تقنيات الأمن السيبراني المتطورة أمر ضروري. ففي المشهد المتطور للأمن العالمي، برز مفهوم حرب الجيل الخامس كتحول محوري في الفكر الاستراتيجي، مما يعكس تعقيدات العالم الحديث. على عكس الأشكال الأكثر تقليدية للحرب، والتي تتمحور في المقام الأول حول الدولة وتنطوي على مواجهات مباشرة، غالبا ما تكون عسكرية، فإن حرب الجيل الخامس تمثل شكلا غامضا وغير مركزي للغاية من الصراع الذي يعمل على هامش إمكانية اكتشافه.

وفي ظل هذا الواقع الجديد، كيف يمكن للدول حماية أمنها القومي والتموقع جيدا في ساحة الحرب الجديدة هذه؟

المحور الأول: ماهية الأمن الوطني

الأمن الوطني هو توفير الحماية للمواطنين، والأفراد المتواجدين على أراضي الدولة، ويعرف أيضا بأنه استخدام الوسائل الأمنية للمحافظة على سير الحياة اليومية بشكل صحيح، وبعيدا عن وقوع أية أزمات تؤدي إلى التسبب بضرر، لمكونات المجتمع البشرية والمادية.(R.holmes, 2015) وهناك العديد من العناصر التي تدخل في تشكيل مفهوم الامن الوطني منها ما هو تقليدي، ومنها ما هو مستجد. حيث قسم الباحث "براهاكلران باليري/Paleri.p" في كتابه المهم بعنوان "National Security: Imperatives And Challenges" عناصر الأمن الوطني إلى ما يلي:(Paleri, 2008)

العناصر التقليدية :

- ✓ الأمن العسكري
- ✓ الأمن الاقتصادي
- ✓ أمن الموارد
- ✓ أمن الحدود
- ✓ الأمن السكاني
- ✓ أمن الكوارث
- ✓ أمن الطاقة
- ✓ الأمن الجيواستراتيجي

العناصر المستجدة:

- ✓ أمن المعلومات
- ✓ الأمن الغذائي.
- ✓ الأمن الصحي
- ✓ الأمن العرقي
- ✓ الأمن البيئي
- ✓ أمن الإنترنت
- ✓ الأمن الجيني

وهنا نلاحظ اهمية التطور الحاصل في مفهوم الامن الوطني من حيث أنه أصبح يهدد أمن الدول والمجتمعات والأفراد على حد سواء، خاصة في ظل تعاظم الحقوق الفردية في مقابل تراجع واضح للحقوق الجماعية والمجتمعية التي تمس القيم والعادات والتقاليد.

أولا- فهم حروب الجيل الخامس:

ليس من السهل تعريف حروب الجيل الخامس، لأنها تتجاوز خطوط ومنهجيات المعركة التقليدية. فهو يتضمن عناصر من الهجمات السيبرانية، والمعلومات المضللة، والتلاعب الاقتصادي، ويستخدم أدوات أخرى غير تقليدية لتحقيق أهداف سياسية وعسكرية. إن حرب الجيل الخامس (FGW) هي مفهوم ناشئ يتميز بمزيج من الحرب الكلاسيكية (القدرات المادية، والعقيدة الراسخة) مع القدرات الناشئة (الهجمات السيبرانية، والبيولوجيا التركيبية، والذكاء الاصطناعي) التي لا تتناسب مع فهمنا التقليدي للصراع. ويتميز هذا النوع من الحرب باعتماده على التخفي والتخريب والاستخدام الاستراتيجي لتكنولوجيا المعلومات، بهدف زعزعة استقرار المعارضين من الداخل.

كما يمكن فهم حرب الجيل الخامس على أنها شكل من أشكال الحرب التي تتجاوز المعارك المادية وتركز على التلاعب بالمعلومات والأفكار والسرد. وعلى عكس الحرب التقليدية، التي تعتمد بشكل كبير على القوة العسكرية والمكاسب الإقليمية، تعمل حروب الجيل الخامس، ضمن المجال غير الملموس لفضاء المعلومات. ويهدف هذا النوع من الحروب إلى التأثير على تصورات ومعتقدات وآراء الأفراد والمجتمعات، وبالتالي تشكيل سلوكياتهم وقراراتهم ومواقفهم.(Krishnan, 2024) فحروب الجيل الخامس هي الحرب التي تتم في المقام الأول من خلال الاعتماد على العمل العسكري أو الهجومي غير الحركي وغير المباشر (non-kinetic military action)، مثل الهندسة الاجتماعية والمعلومات المضللة والهجمات الإلكترونية، إلى جانب التقنيات الناشئة مثل الذكاء الاصطناعي والأنظمة المستقلة بالكامل.

ولتكون الحقائق واضحة، فإن حروب الجيل الخامس لا تقتصر على استخدام وسائل الإعلام أو وسائل التواصل الاجتماعي. إنها حرب الروايات المدعومة بالحقائق والبيانات الثابتة. حيث أنه يمكن للحملات الاعلامية التي تمارسها وسائل التواصل الاجتماعي أن تصرف الانتباه نحو قضية معينة مؤقتة لكنه لن يكون مستداما دون الحقائق والأرقام الصعبة. إن المنطق المبني على الأدلة هو المفتاح لتطوير السردية وهزيمة سردية المعارضين. يجب أن يكون الدليل والمنطق أساسيين، وإلا سيصبح المصدر فاقدا للمصداقية .(Alkin, 2022)

والعنصر المهم الثاني لمحاربة ومواجهة حروب الجيل الخامس هو أنه يجب على الدولة أيضا أن تكون على دراية بخطوط الصدع الخاصة بها وتحاول تغطيتها. حيث أن هناك إجماع بين الخبراء على أن خط الصدع الأكثر فتكا بالدول هو الوضع الاقتصادي، وبشكل أكثر تحديدا رفاهية الناس. ويتم قياس الرفاهية من خلال توزيع الموارد والمساواة بين شرائح المجتمع. وفي غياب توزيع الموارد، سترداد عدم المساواة ويستعرض رفاه الناس للخطر، ومنه استقرار الدولة للاهتزاز، وربما الوصول الى مرحلة التفكك.

وكخلاصة للتعريفات التي تعرف مفهوم " حروب الجيل الخامس" أو كما يطلق عليها مفكرو ما بعد الحداثة تسمية "حروب ما بعد الحداثة" بأنها " تآكل داخلي للحضارة يسقط مبدأ شرعية المعرفة، حيث القواعد الموضوعة مسبقا والأعراف المألوفة لدى غالبية مكونات المجتمع تتم "إعادة صياغتها" وفق سياسات وقواعد ثقافية جديدة قائمة على: الفرد - الهوية - الجنس، وبنى سياسية ونظم موحدة الهياكل والتكنولوجيا صفتها أنها ما فوق وطنية."

ثانيا- خصائص حروب الجيل الخامس(Qureshi, 2019)

تتميز حروب الجيل الخامس بالعديد من الخصائص التي تجعل منها تهديدا حقيقيا لجميع الدول، سواء تلك المتطورة، أو الأقل تطورا خاصة من الناحية التقنية.ويمكن تلخيص أهم خصائص حروب الجيل الخامس فيما يلي:

1 - عدم الكشف عن هويته: غالبا ما يكون المهاجمون او حتى المقاتلون جهات فاعلة غير حكومية، بما في ذلك المتسللين والناشطين والمرتزقة الذين يمكنهم التأثير على الأحداث على مستوى العالم دون الكشف عن هوياتهم أو انتماءاتهم. ومن المنطقي أن الجهات الفاعلة غير الحكومية هي تلك التي تتخذ إجراءات ذات طبيعة إلكترونية ولكنها ليست جزءا مباشرا من الدولة القومية. ومن المؤكد أنه يجوز للدول أن توظف أو تدعم هؤلاء العملاء بشكل مباشر أو غير مباشر، لا سيما عندما يرغبون في أن تكون أنشطتهم سرية، أو عندما يعملون خارج حدود القانون. قد تشمل الجهات الفاعلة غير الحكومية، على سبيل المثال لا الحصر، أطفال السيناريو، والمحتالين، ونشطاء القرصنة، وقراصنة القبعات السوداء، والمنظمات الإجرامية، أو أي عدد من الأفراد أو المجموعات الأخرى. العديد من الجهات الفاعلة غير الحكومية تندرج بحق في نفس الفئة مثل أي مجرم إلكتروني آخر. أحد الاستثناءات المحتملة في هذه المجموعة هو الشركة. فالشركات، في كثير من الحالات، هي كيانات تتمتع بإمكانية الوصول إلى قدر كبير من الموارد ولا ينبغي بالتأكيد استبعادها كعامل في الصراع السيبراني. فئة أخرى لديها القدرة على تنفيذ عمليات إلكترونية بشكل كبير هي المنظمات الإجرامية. ولا تمتلك مثل هذه المجموعات قدرا كبيرا من الموارد التي يمكنها من خلالها دعم الهجمات السيبرانية على نطاق واسع فحسب، بل تمتلك أيضا العناصر التنظيمية اللازمة لإدارتها على هذا النطاق أيضا. تعمل المنظمات الإجرامية في كثير من الأحيان بطريقة مشابهة لتلك التي تعمل بها الشركات، على الرغم من أنها لا تملك نفس الشعور بالذنب لاتباع القواعد، ولا نفس العقوبات لعدم القيام بذلك، وغالبا ما لا تكون مقيدة بحدود مادية أو وطنية.

2- التعقيد: الاستراتيجيات المستخدمة معقدة للغاية ومتعددة الأوجه، وتتضمن طبقات من الخداع والتلاعب النفسي، بالابتعاد عن الأطر الاختزالية والمجال المعقد الذي يهيمن عليه المجهول في النظام المعروف، من خلال التحكم في درجة تعقيد عناصر الإستراتيجية وعدد عناصر نظام النشاط الاستراتيجي. حيث يتعين على المنظمات أن تتأقلم مع بيئتها التي تتميز بالتعقيد من أجل البقاء. يلعب التعقيد دائما دورا في جميع الأنظمة، سواء كنا ندرك ذلك أم لا . يعد تعقيد المنظمات وبيئاتها موضوعا شائعا في أدبيات الإدارة الإستراتيجية. ويشير التعقيد إلى عدد العناصر التي تشكل بيئة النظام والروابط بين هذه العناصر. التنظيمية التعقيد والتعقيد البيئي الذي تستغرقه جهود الإدارة الإستراتيجية يخلق المكان تحديات كبيرة لكل من الممارسين والباحثين. تعقيد النظام وتعقيد أسلوب البحث الذي يتحدى بيئته خاصة. يمكن للمنظمات الاستجابة للتعقيد البيئي عن طريق خلق تعقيد داخلي أو ما هو معروف أقل خلق التعقيد التعاوني بشكل جماعي. مع ذلك، التعقيد هو السمة المركزية في بحوث الإدارة الاستراتيجية.

3- تعتمد على التكنولوجيا: تستخدم في حروب الجيل الخامس التكنولوجيا الرقمية على نطاق واسع في الحرب السيبرانية والمراقبة وإنشاء أنظمة آلية لنشر الهجمات التي يمكن أن تكون واسعة النطاق ومستهدفة. حيث لم تعد ساحة المعركة تقتصر على المواقع الجغرافية؛ بل إنها موجودة ضمن المشهد الرقمي حيث تتدفق المعلومات بحرية. تتضمن مساحة المعلومات هذه منصات مثل وسائل التواصل الاجتماعي والمواقع الإلكترونية ومنافذ الأخبار وقنوات الاتصال. وينشأ غموض هذا الفضاء من سهولة نشر المعلومات الكاذبة أو المضللة، مما يؤدي إلى طمس الخطوط الفاصلة بين الحقيقة والباطل. يتحدى هذا التعقيد الأفراد لإجراء تقييم نقدي للمعلومات التي يواجهونها وتمييز المصادر الموثوقة من المصادر المتلاعبة. وتعد الحرب السيبرانية عنصرا حاسما في حروب الجيل الخامس، ولكن لا

ينبغي الخلط بينها وبين تركيزها الوحيد. وبدلا من ذلك، فهو بمثابة أداة ضمن الترسانة الأكبر. تتضمن الحرب السيبرانية استخدام الأدوات الرقمية لتعطيل الأنظمة والشبكات والتسلل إليها والتلاعب بها. يمكن لهذا النوع من الحرب أن يستهدف البنية التحتية الحيوية وشبكات الاتصالات والأنظمة المالية والمزيد. ومع ذلك، من المهم أن ندرك أن حروب الجيل الخامس تشمل نطاقا أوسع من التكتيكات، بما في ذلك العمليات النفسية والدعاية وحملات التضليل.

4- نفسية وثقافية: تستغل الانقسامات الثقافية والدينية والمجتمعية للتحريض على الصراع، وغالبا ما تتلاعب بوسائل التواصل لاجتماعي ومنصات الاتصال لأخرى لنشر المعلومات المضللة والدعاية. وقد تتغير الآثار المترتبة على المجتمع بتغيير النماذج وعدم اليقين، إن لاعتماد المزايد على تقنيات حروب الجيل الخامس ضد الشعوب، خاصة دول العالم الثالث، له آثار عميقة على المجتمع. فعندما يتنقل الأفراد عبر تدفق المعلومات والسرد السريع لمعطيات، قد يواجهون عدم اليقين والتنافر المعرفي. ويمكن أن يؤدي التلاعب المتعمد بالمعلومات إلى مشهد متغير من المعتقدات والآراء، مما يؤثر على الخطاب العام والقرارات السياسية. في هذه البيئة، يصبح التفكير النقدي ضروريا للتمييز بين المعلومات الحقيقية والسرد المنسق.

والسؤال المركزي الذي تطرحه خطورة حروب الجيل الخامس هو ما إذا كانت المجتمعات، وحتى الأفراد، تنخرط عن غير قصد في هذا النوع من الحروب دون أن تدرك ذلك. نظرا لأن الروايات والسرديات والمعلومات يتم صياغتها ونشرها بعناية، فقد يجد الأفراد أنفسهم متأثرين بتأثيرات لا يدركونها. وهذا يستدعي زيادة الوعي والرغبة في التشكيك في الروايات السائدة، على المستوى الشخصي والمجتمعي. إن إدراك إمكانية التلاعب هو الخطوة الأولى نحو مواجهة آثاره. وهنا يبرز دور التفكير النقدي كأداة قوية ضد تقنيات حروب الجيل الخامس. فهو يمكن الأفراد من تقييم المعلومات بشكل نقدي، وتحديد التحيزات، والتحقق من المصادر. إن تنمية مهارات التفكير النقدي تمكن الأفراد من مقاومة التلاعب واتخاذ قرارات مستنيرة. وفي حين أن الحلول قد لا تكون مثالية أو مضمونة، فإنها توفر طريقا للتخفيف من تأثير الروايات التي تم التلاعب بها، وتعزيز الخطاب الأكثر عقلانية، وتعزيز مجتمع مرن. وتنمية القدرات النقدية للعقل المجتمعي ككل.

5-اقتصادية وقانونية: الضغط الاقتصادي هو أداة أخرى، تتمثل في العقوبات، والحروب التجارية، والتلاعب بالأسواق المالية. تستخدم الحرب القانونية، أو "الحرب القانونية"، أيضا للتلاعب بالقانون الدولي لخدمة الأهداف لإستراتيجية. ويعد التدخل الروسي المزعوم من طرف الحزب الديمقراطي لأمريكي في الانتخابات الرئاسية لأمريكية لعام 2016 بمثابة مثال نموذجي لتقنية حروب الجيل الخامس، حيث يوضح كيف تم استخدام الأدوات السيبرانية والمعلومات المضللة للتأثير على الرأي العام والنتائج السياسية. وعلى نحو مماثل، فإن النهج الذي تتبناه الصين في التعامل مع السياسة العالمية، والذي يطلق عليه غالبا "الحرب غير المقيدة"، يوضح استخدام لاستراتيجيات القانونية، والسياسات الاقتصادية، والنفوذ الثقافي لتوسيع قوتها دون الانخراط في أعمال عدائية مفتوحة.

حيث سيكون الأشخاص المعرضون للخطر اقتصاديا على استعداد لقبول الروايات التي تستهدف احتياجاتهم أو مشاكلهم دون التفكير النقدي في تلك الروايات والمعطيات. وسيتم ربط العرق أو الطبقة أو الجنسية أو اللغة أو أي هوية أخرى بمآسيهم، وسوف يمهد الطريق لاستغلالهم. والتاريخ مليء بمثل هذه الحوادث. ولسوء الحظ، فإن النظام العالمي يتجاهل هذه الحقيقة، وأصبحت الرفاهية موضوعا للتشدق أو تصميم شعارات أو برامج فاخرة ذات تطبيق

عملي محدود. إن السباق على الناتج المحلي الإجمالي مستمر ولكن الحياة الأفضل للناس قد تعرضت للخطر، حيث لم تعد مستويات النمو التي تحققها الدول تنعكس على مستويات التنمية فيها.

إن مفهوم القوة الاقتصادية المحتكرة يزعزع النسيج الاجتماعي والتنموي في العالم. باختصار، تم تقديم الاقتصاد كمصدر قوة للأمة وتم وضع رفاهية الناس في مرتبة متأخرة. كما تمت الدعوة إلى نظرية التدرج إلى الأسفل، وتم الترويج لها على أنها ستضمن توزيع الموارد بين الجماهير كآلية تلقائية.وسوف يؤدي ذلك حتما إلى رفاهية الناس. ومن ثم، ينبغي تسهيل الأعمال الاقتصادية أو التجارية لأصحاب رؤوس الاموال من خلال التخفيضات الضريبية والحوافز، وهو ما يزيد من حجم سيطرة هذه الفئة على الاقتصاد ومنه على عملية صنع القرار في الدولة.

وقد أشارت دراسة حديثة أجراها باحثون من كلية "لندن للاقتصاد"وكلية "كينغز كوليدج" في لندن إلى اتجاه آخر. حيث قامت الدراسة بتحليل بيانات 50 عاما لمعظم الاقتصادات المتقدمة. لقد اكتشفوا أن التخفيضات الضريبية للأغنياء لا يمكن أن تخلق النمو المنشود وفرص العمل، ولم تكن هناك علامات على انتشارها. وينبغي تصميم المرحلة الثانية لبدء تحول الاقتصاد من الزراعة إلى القاعدة الصناعية وإعادة تصميم حصة قطاع الخدمات في الاقتصاد. فقد أدى الإيمان الأعمى بتدفق الفوائد إلى انعدام الأمن الغذائي وعدم المساواة والفقر والمشاكل الصحية في جميع أنحاء العالم، بل والى العمل ضد مصالح المجتمعات من أجل تحقيق الربح المادي. (Savage, 2020)

وحتى الاقتصادات الأكثر تقدما تعاني من هذه المشاكل، فإذا حذفنا مساهمة الصين في هذه الجبهات (وهي التهمة الامريكية للصين)، فإن الإحصائيات ستخبرنا بوقائع مروعة، حيث سيتحول هؤلاء الأشخاص المحرومون اقتصاديا إلى وقود لحروب الجيل الخامس على المستويين الوطني والدولي. فعلى الصعيد الوطني، تستخدمه أحزاب المعارضة لزعزعة استقرار الحكومة.وعلى المستوى الدولي، يستخدمها أعداء الدولة لتحقيق أهدافهم. فعلى الرغم من أن حروب الجيل الخامس أو الحروب الهجينة هي الموضوع المفضل للحديث عنه حاليا، إلا أن العناصر الحقيقية لحروب الجيل الخامس يتم إغفالها في المناقشة.وأن النخب، سواء كانت في السلطة أو في المعارضة، تستخدم هذه الحقائق فقط لتقويض المعارضين وتأمين السلطة، أو للمنافسة على السلطة ومحاولة انتزاعها. على سبيل المثال، يتم استخدام الفساد والفقر وسوء الإدارة وانعدام الأمن الغذائي وما إلى ذلك من مشاكل لانتقاد الآخرين وتأمين الفوز في الصراع السلطوي، وهذه استراتيجية سيئة جدا وتضر بشكل خطير باستقرار البلاد. إن بناء السرديات ضد بعضنا البعض في الصراع الدائم على السلطة داخليا لا يعني بالضرورة نجاح أي طرف، بل هو ضعف للجميع، والخاسر في نهاية المطاف هو الدولة.

المحور الثاني: الآثار المترتبة على الأمن الوطني والعالمي

إن الطبيعة الخبيثة لحروب الجيل الخامس تجعل من الصعب بشكل خاص على الدول الاستجابة بفعالية. حيث أن آليات الدفاع التقليدية، المصممة في المقام الأول لصد الاعتداءات المادية أو الهجمات المباشرة، غالبا ما تكون غير كافية للتعامل مع التهديدات المنتشرة التي تشكلها شبكة الجيل الخامس. ويستلزم هذا إعادة تقييم استراتيجيات الأمن القومي لتشمل الدفاع السيبراني، وجمع المعلومات الاستخبارية عن الجهات الفاعلة غير الحكومية، وقدرات الدعاية المضادة.(Browne, 2023)

علاوة على ذلك، فإن صعود حروب الجيل الخامس من الحروب لها آثار كبيرة على القانون الدولي وأعراف الحرب. إن الخطوط غير الواضحة بين المقاتلين والمدنيين، وبين الحرب والسلام، تشكل تحديات أخلاقية وعملياتية خطيرة.ويجب على الدول أن تتغلب على هذه التعقيدات مع احترام القانون الدولي وحماية حقوق الإنسان.

أولا- المشهد الأمني الوطني والعالمي

ويمثل ظهور حروب الجيل الخامس تغييرا كبيرا في المشهد الأمني الوطني والعالمي. وحقيقة أنه لا توجد دولة محصنة ضد مثل هذه التكتيكات - بغض النظر عن موقعها الجغرافي أو قوتها العسكرية - تدعو إلى إعادة تقييم استراتيجيات الأمن القومي. فهو يتطلب نهجا أكثر شمولا للأمن، يتضمن عناصر مثل الأمن السيبراني، وسلامة المعلومات، والمرونة المجتمعية. خاصة وأن تقنيات هذه الحروب غالبا ما تستفيد من الطبيعة المنفتحة للمجتمعات أكثر فأكثر، مستغلة التدفق الحر للمعلومات والحريات المجتمعية. وقد يؤدي ذلك إلى إضعاف سيادة الدولة، حيث تتلاعب الكيانات الخارجية الديناميكيات الاجتماعية والسياسية والاقتصادية الداخلية. وهو ما يطرح أسئلة بالغة الأهمية حول الكيفية التي يمكن بها للدول حماية سيادتها وأمنها من جهة مع الحفاظ على الحقوق والحريات الإعلامية والمعلوماتية من جهة ثانية. (Krishnan, Fifth Generation Warfare, Hybrid Warfare, and Gray Zone Conflict: A Comparison, 2022)

كما أنه من الممكن أن تؤدي الحدود غير الواضحة والغموض المتأصل في تكنولوجيا حروب الجيل الخامس إلى فرض ضغوط متزايدة على الدول على مستوى العلاقات الدولية، وذلك عن طريق استخدام الوكلاء وحرب المعلومات بما يمكن أن يجعل من الصعب تحديد المسؤولية عن الأعمال العدائية. وهذا الغموض يمكن أن يؤدي إلى تصاعد التوترات، وإثارة الأزمات الدبلوماسية وتعقيد الجهود المبذولة لحل الصراعات. ونظرا لهذه الآثار الواسعة النطاق، يصبح من الواضح أن حروب الجيل الخامس ليست مجرد نوع جديد من الحروب، بل هي نقلة نوعية في كيفية فهمنا للصراع والأمن والعلاقات الدولية.

ثانيا- أليات المواجهة:

هناك العديد من آليات المواجهة التي تستطيع الدول من خلالها مواجهة تهديدات حروب الجيل الخامس، بشرط أن تتسم تلك الاليات بالانسجام والتكامل، والاهم من ذلك انخراط كل الفواعل الرسمية وغير الرسمية في الدولة من أجل المواجهة والتصدي.ويمكن تلخيص هذه الآليات فيما يلي:(nizar, 2018)

- ✓ تكييف لاستراتيجيات وصياغة سياسات لاستجابة

بينما نتعمق أكثر في عالم حروب الجيل الخامس، يصبح من الضروري رسم تدابير مضادة فعالة يمكنها لاستجابة لهذا النموذج المتغير للصراع. وهذا يتطلب إعادة تقييم شاملة لاستراتيجيات الدفاع الاقليدية وتوليد أساليب مبتكرة وديناميكية يمكنها التعامل مع المجموعة الكاملة من تكتيكات هذا النوع من الحروب.

- ✓ دمج السياسات وخلق درع حماية

فنظرا للطبيعة المتعددة والمعقدة لحروب الجيل الخامس، فمن غير العملي وغير الفعال لاعتماد على سياسة أو استراتيجية واحدة كحل شامل. وبدلاً من ذلك، فإن المطلوب هو دمج التوجهات السياسية المختلفة، ومزج الدبلوماسية، والدفاع، والتنمية، والمعلومات في استراتيجية موحدة لتنسيق استجابة شاملة ومنسقة جيدا قادرة على معالجة التهديدات ومواجهتها.

- ✓ تعزيز الدفاعات السيبرانية

تشكل الحرب السيبرانية عنصرا أساسيا في حروب الجيل الخامس، مما يستلزم وجود دفاعات سيبرانية قوية لتكون جزءا لا يتجزأ من أي استجابة استراتيجية.ويتطلب ذلك استثمارات كبيرة في البنية التحتية للأمن السيبراني لضمان الحماية من الهجمات المحتملة. بالإضافة إلى ذلك، من الضروري تعزيز تدريب القوى العاملة في مختلف المجالات لتعزيز لاستعداد السيبراني الداخلي.وكذلك تعزيز التعاون الدولي الذي يمكن أن يساعد في ردع التهديدات السيبرانية المحتملة ومعاقبة المعتدين السيبرانيين بشكل فعال.

- ✓ الحفاظ على أمن وسلامة المعلومات

يعد الصراع من أجل السيطرة على الروايات والسرديات سمة مميزة لحروب الجيل الخامس.ومن ثم، فإن ضمان صحة المعلومات يعد عنصرا بالغ الأهمية للحفاظ على وحدة المجتمع وأمن الدولة. ويشمل ذلك خطوات عملية مثل تعزيز الثقافة لإعلامية بين السكان، ولاستثمار في آليات التحقق من الحقائق والتحقق من المعلومات، ومكافحة المعلومات المضللة من خلال نشر المعلومات الدقيقة في الوقت المناسب، وبناء وتعزيز الثقة بين الدولة والمجتمع.

- ✓ تعزيز مرونة المجتمعات

غالبا ما تستغل حروب الجيل الخامس استراتيجيات خطوط الصدع المجتمعية وتولد عدم لاستقرار.وبالتالي، فإن تشكيل مجتمعات مرنة قادرة على مقاومة هذه التكتيكات، يجب أن يكون جانبا رئيسيا في أي استراتيجية استجابة للتحديات التي تفرضها تلك الحروب.ويمكن أن يشمل ذلك صياغة وتنفيذ السياسات الرامية إلى معالجة عدم المساواة لاجتماعية، وتعزيز التماسك لاجتماعي، وتعزيز ثقة الجمهور في المؤسسات الحكومية وغير الحكومية.

- ✓ تعزيز التعاون العالمي

إن تهديدات حروب الجيل الخامس ليست تحديا محليا أو إقليميا ولكنها تهديد عالمي يتطلب استجابة عالمية.ولمواجهة التهديدات التي تشكلها تقنية الجيل الخامس بشكل فعال، هناك حاجة ملحة لتعزيز التعاون الدولي في مجالات مثل تبادل المعلومات لاستخبارية، وتنسيق لاستجابات لاستراتيجية، وصياغة القواعد واللوائح التي تحكم الحرب السيبرانية والعمليات المعلوماتية.

✓ استخدام التكنولوجيا لمواجهة التكنولوجيا

بالنظر إلى أن حروب الجيل الخامس تستخدم التكنولوجيا بفعالية لتعزيز أهدافها، فإن استجاباتنا يجب أن تستغل أيضا إمكانات التكنولوجيا. ويمكن أن يشمل ذلك استخدام الذكاء الاصطناعي لتعزيز الأمن السيبراني، ونشر التحليلات المتقدمة لفهم حملات التضليل ومواجهتها، واستخدام التقنيات الناشئة الأخرى لمواجهة التهديدات التي لا تعد ولا تحصى التي تشكلها شبكة حروب الجيل الخامس.

خاتمة:

إن حروب الجيل الخامس ليست معركة يخوضها الجنود على الخطوط الأمامية فقط، بل يخوضها الأفراد في منازلهم وأماكن عملهم وفضاءاتهم الرقمية. إنها تأكيد على قوة الأفكار والروايات في تشكيل مسار التاريخ. إن فهم تقنية الجيل الخامس يتطلب منا أن ندرك أن ساحة المعركة قد توسعت إلى ما هو أبعد من الحدود المادية وأن المعلومات في حد ذاتها هي سلاح. ومن خلال تبني التفكير النقدي، وحماية الخصوصية، وبناء مجتمعات مرنة، يمكننا بشكل جماعي أن نبحر في ساحة المعركة الجديدة هذه ونحافظ على سلامة أفكارنا وقيمنا في عصر حرب المعلومات. ومع تقدمنا في القرن الحادي والعشرين، سوف تصبح حروب الجيل الخامس هي القاعدة وليس الاستثناء. اذ يتحدى هذا النوع من الحرب مفاهيمنا التقليدية للحرب، مما يتطلب فهما شاملا لكل من التكنولوجيا وعلم النفس. وردا على ذلك، يجب على الدول تطوير تدابير أمنية أكثر شمولا وتكيفا لمعالجة النطاق الكامل للتهديدات المحتملة. ويتعين على المجتمع العالمي أيضا أن يعمل على تعزيز آليات التعاون لإدارة المخاطر المشتركة وضمان الأمن الجماعي في عالم متزايد الترابط.

وتمتد التحديات التي تفرضها تقنيات حروب الجيل الخامس إلى ما هو أبعد من الأمن القومي، ولها آثار عميقة على الأنظمة الحاكمة وحقوق الإنسان والديمقراطية. وتشكل السهولة التي يمكن بها التلاعب بالمعلومات تهديدا للعملية السياسية والديمقراطية، في حين يثير انتشار الهجمات السيبرانية في كل مكان تساؤلات حول سيادة الدول وأمنها. وبالنظر إلى المستقبل، من المرجح أن يتشكل مشهد الصراع والتعاون العالمي من خلال التطور المستمر لأدوات حروب الجيل الخامس. ويجب على الدول والهيئات الدولية أن تظل يقظة وقادرة على التكيف لمواجهة هذه التهديدات بفعالية. ولا يشمل ذلك تعزيز الدفاعات المادية والرقمية فحسب، بل يشمل أيضا تعزيز بيئة عالمية يمكن أن يزدهر فيها التواصل المفتوح بين مختلف الفواعل. وسيكون الدور الذي تلعبه المنظمات الدولية مثل الأمم المتحدة محوريا في التوسط في الصراعات ووضع معايير للسلوك السيبراني. وبالمثل، يمكن للمعاهدات والاتفاقيات الدولية التي تتناول على وجه التحديد الفروق الدقيقة في تكنولوجيا الجيل الخامس أن تلعب دورا حاسما في الحفاظ على السلام والأمن العالميين.

ومع استمرار أدوات هذه الحرب في التحول والتطور، يجب أن تتطور استراتيجياتنا أيضا. من خلال تدعيم القدرة على التكيف والابتكار والاستعداد لما هو غير متوقع. فلا شك أن المخاطر كبيرة، ولكن من خلال معالجة أبعادها بشكل مباشر، يمكننا أن نأمل في التحكم في تعقيدات مشهد هذه الحرب الجديدة ومواجهة تهديداتها وتحدياتها.

الهوامش والمراجع:

1- **Kim R.holmes, what is national security, index of U.S military stmeght, 2015.**
2- **Prabhakaran Paleri, National Security : Imperatives And Challenges, New Delhi, Tata McGraw-Hill, 2008.**

3- **Armin krishnan, Fifth Generation Warfare Dominating the Human Domain, New York, Routledge, 2024.**
4- **Kerem Alkin, Fifth-generation warfare and global challenge, https://www.dailysabah.com/opinion/columns/fifth-generation-warfare-and-global-challenges. Seen 05/03/2024.**
5- **Waseem Ahmad Qureshi, Fourth- and Fifth-Generation Warfare: Technology and Perceptions, San Diego International Law Journal, (2/2024).**
6- **Luke Savage, They Said Tax Cuts for the Rich Would Create Jobs. It Never Happened, https://jacobin.com/2020/12/tax-cuts-rich-income-inequality-hope-limberg-study. Seen 04/03/2024.**
7- **Edward Granville Browne, Fifth Generation Warfare, https://oafnation.com/blogs/national-security/fifth-generation-warfare. Seen 06/03/2024**
8- **Armin Krishnan, Fifth Generation Warfare, Hybrid Warfare, and Gray Zone Conflict: A Comparison, Journal of Strategic Security, Vol. 15, No. 4, 2022.**
9- **Maaz nizar, 5 GW and hybrid warfare its implications and response options. https://bdex.eb.mil.br/jspui/bitstream/123456789/2827/1/MO%200023%20-%20MAAZ.pdf. Seen 07/03/2024.**

الأمن والحرب في الفضاء السيبراني: إطار مفاهيمي

Security and War in Cyber space: a Conceptual Framework

حميز سمير (*) جامعة بومرداس، s.hamiaz@univ-boumerdes.dz

ملخص:

تحاول هذه الورقة البحثية، أن تأصل معرفيا لمفاهيم الأمن والحرب في الفضاء السيبراني، من خلال الانطلاق من إشكالية مفادها: إلى أي مدى أثرت الثورة الرقمية و السيبرانية في مفاهيم الأمن والحرب في العلاقات الدولية؟. ولقد حاولت الورقة مقاربة الموضوع من خلال البحث بداية في الفضاء السيبراني بوصفة مجالا جديدا للحروب والصراعات، و كذا التطرق إلى الحرب السيبرانية من حيث بيان مفهومها فواعلها وتجلياتها في الواقع الدولي، بالإضافة إلى البحث في مفهوم الأمن السيبراني من خلال الوقوف على دلالاته الاصطلاحية، مهدداته أبعاده ومقومات تحقيقه. وقد توصلت الورقة البحثية إلى أن الفضاء السيبراني تحول إلى ساحة جديدة للحروب والصراعات، وأن أمن الدولة وقوتها في المستقبل لن يتحقق بامتلاك المعدات والقدرات العسكرية فحسب، وإنما أيضا بمدى القدرة على امتلاك والتحكم في التكنولوجيا والمعلوماتية، فضلا عن امتلاك بيئية تحتية سيبرانية قوية. ولذلك، فأمن الدول في المستقبل يرتهن بشكل كبير بمدى امتلاك مدخلات وعناصر القوة السيبرانية.

الكلمات المفتاحية: الحرب السيبرانية ؛ الأمن السيبراني؛ الفضاء السيبراني؛ القوة السيبرانية؛ التهديدات السيبرانية.

Abstract:

This paper attempts to define the concept of security and war in cyberspace, by addressing the following problem: How did the digital and cyber revolution affect the concepts of security and war in international relations? The paper attempted to address the topic by initially researching cyberspace as a new field of wars and conflicts, as well as addressing cyber war in terms of defining its concept, its actors, and its manifestations in the international reality, in addition to researching the concept of cyber security by defining its concept, its threats, its dimensions, and the components of achieving it. The research paper concluded that cyberspace has turned into a new arena for wars and conflicts and that the security and strength of the state in the future will not be achieved by possessing military capabilities only, but also by the ability to possess and control technology and information, in addition to possessing a strong cyber infrastructure. Therefore, the security of states in the future requires Possessing the components and elements of cyber power.

Key Words: ***cyber warfare; cyber security; cyber space; cyber power; Cyber threats.***

مقدمة:

أسهمت الثورة المعلوماتية والرقمية التي هي من إفرازات العولمة والتطور التكنولوجي، بشكل كبير في التأثير على القيم الصلبة للدولة، مثل الأمن والسيادة..، كما تجلى هذا التأثير في تطور الأجندة البحثية للعلوم السياسية التي باتت تخوض وتهتم بدراسة قضايا وموضوعات مستجدة وغير تقليدية من قبيل الأمن السيبراني، الحروب السيبرانية، القوة الرقمية..، كما أكسبت الثورة السيبرانية والرقمية مفاهيم كالقوة والحرب والأمن والتهديد ميدان القتال والسلاح والحدود مضامين جديدة تختلف عما كان سائدا في السابق.

ويعتبر الأمن والحرب أحد النماذج والمفاهيم المحورية في حقل العلوم السياسة التي تبرز التأثير الذي أحدثته الثورة الرقمية في علم السياسة حيث انتقلت مفاهيم الأمن والحرب من المفهوم التقليدي إلى المفهوم السيبراني الافتراضي، وذلك لمواكبة الثورة الرقمية والتطورات التكنولوجية التي أفرزتها العولمة ولكن أيضا للتأقلم مع الأنماط الجديدة من التهديدات التي باتت تخترق أمن و سيادة الدول، على شاكلة التهديدات والهجمات السيبرانية، القرصنة الإلكترونية، الإرهاب الإلكتروني، وغيرها من التهديدات التي أفرزتها الثورة الرقمية المعاصرة.

تأسيسا على ما سبق، تحاول هذه الورقة البحثية معالجة إشكالية مفادها: إلى أي مدى أثرت الثورة الرقمية و السيبرانية في مفاهيم الأمن والحرب في العلاقات الدولية؟.

لمقاربة الموضوع تم تقسيم الورقة البحثية إلى المحاور التالية:

- المحور الأول: الفضاء السيبراني بوصفة مجال جديد للحروب والصراعات.
- المحور الثاني: الحرب السيبرانية: المفهوم الفواعل والتجليات في الواقع الدولي.
- المحور الثالث: الأمن السيبراني: المفهوم، التحديات والمقومات.

المحور الأول: الفضاء السيبراني بوصفه مجال جديد للحروب والصراعات

استقرت أدبيات الفكر الاستراتيجي وعلم الحرب على تحديد أربع مجالات أساسية للحرب والقتال، وتتمثل في المجال البري، البحري، الجوي والفضائي، بيد أنه بفعل الثورة الرقمية والمعلوماتية أصبحنا نتحدث عن مجال جديد غير تقليدي في الشؤون الإستراتيجية، وهو الفضاء السيبراني، كساحة جديدة للحروب والصراعات بين عدة فواعل سواء دولاتية أو من غير الدول.

ويمكن تعريف الفضاء السيبراني، بأنه مجال أو بيئة افتراضية تتكون من تفاعل عناصر مادية، وغير مادية تتيح التواصل بين مختلف أجزاء العالم، وتسمح بتداول المعلومات، ويتمثل الشق المادي في شبكات الانترنت وفي البنية التحتية الالكترونية عموما، بينما يتمثل الشق غير المادي في الوسط الافتراضي الذي من خلاله يتم تداول المعلومات.[1]

يذهب عدد غير قليل من الباحثين، إلى تشبيه الفضاء السيبراني إلى حد بعيد بالمحيط، فهو بطبيعته مجال إلكتروني يمتاز بالتجانس والمرونة، ولا تحده أي نوع من الحدود، فهو ذلك الفضاء الذي يسمح لأي كان من الولوج إليه دون قيود والتنقل بين حدوده ونطاقه وبلوغ أقصى حدوده في أقصر مدة زمنية معينة، ومن بين أهم خصائصه ثراءه من حيث المعلومات المخزنة عليه أو المتداولة عبره.[2]

ولعل السمة الجوهرية التي تطبع الفضاء السيبراني، أنه تحول إلى مصدر ومكمن للتهديدات الإجرامية اللامتناهية من هجمات إلكترونية، وملاذا للمتطرفين والإرهابيين، ومجالا حيويا لتنفيذ سياسات التجسس الإلكتروني وإلحاق الضرر بالغير في صورة الحروب السيبرانية، وذلك راجع أساسا إلى غياب سلطة عليا تتحكم فيه وآليات تسمح بحصر مجال الخطر الناتج عنه سواء من الناحية القانونية أو المؤسساتية الآلية.[3]

المحور الثاني: الحرب السيبرانية: المفهوم الفواعل والتجليات في الواقع الدولي

لقد تعددت التعاريف التي قدمت بشأن الحرب السيبرانية، إذ هناك من عرفها بأنها نمط أو جيل جديد من الحروب تخاض في الفضاء الافتراضي من خلال إقدام الدول أو مجموعات أو أفراد على شن مجموعة من الهجمات التي تستهدف إلحاق أضرار جسيمة بشبكات وأنظمة المعلومات للدول الأخرى.

كما تعرف بأنها كل فعل فردي أو جماعي مخطط له يهدف إلى المساس بوحدة وسلامة النظام المعلوماتي لمؤسسة أو منظمة أو دولة معينة، بإستخدام كل أو جزء من شبكة الإتصالات سواء الإنترنت و أنواع من الشبكات الإتصالية الرقمية،بحيث تؤدي إلى حدوث أضرار توازي ما قد ينجم عن إستخدام القوة العسكرية المسلحة.وقد صنفتها وزارة الدفاع الأمريكية إلى ثلاث أصناف : حرب سيبرانية هجومية وأخرى دفاعية وإستخباراتية.[4]

ومن ناحية أخرى يرتبط مفهوم الحرب السيبرانية بهجمات إلكترونية بقيادة عسكرية تقوم بإختراق الأنظمة الإلكترونية العالمية وتقوم بأعمال تضر بالأجهزة التي تستخدم الإنترنت مثل سرقة البيانات الخاصة.

وتتميز الحرب السيبرانية بأنها حرب غير محددة المجال وغامضة الأهداف كونها تتحرك عبر شبكات عابرة للحدود الدولية بسرعة تتطابق وواقع سرعة المعلومة في هذا العصر مما يسبب تدميرا واسع النطاق د لمنشآت الحيوية للدول، وفي حال الزاع المسلح قد ينعكس الهجوم السيبراني الذي يؤدي إلى تعطيل شبكات المعلومات للدول على المدنيين ويحرمهم من الحاجات الأساسية كالمياه و الرعاية الطبية والكهرباء.[5]

وتتسم الحرب السيبرانية من حيث طبيعتها بعدة خصائص ولعل من أهمها:

- يكون فيها الخط الفاصل بين الحرب والسلم شديد الميوعة.
- إنها حروب تقع في الفضاء الافتراضي غير الملموس ولذلك لن تفيد معها الطرائق والأنماط التقليدية لإدارة الحروب.
- إنها حرب متعددة الفواعل يمكن أن تخوضها دول جماعات افتراضية و أفراد.

- كما أنها حرب تتسم بغياب التسلسل الهرمي للقيادة.
- ضف إلى ذلك أنها تتسم بقلة التكلفة من حيث الأرواح مقارنة بالحروب العسكرية التقليدية.[6]

والملاحظ أن الحرب السيبرانية باتت تخلف خسائر وتداعيات كبيرة على الامن القومي للدول كون هذا النمط الجديد من الحروب يستهدف الأنظمة المعلوماتي التي ترتكز عليها قطاعات حيوية في الدولة كالقطاع المالي والإداري، كما ان هذا النمط الجديد من الحروب بات يلحق أضرار جسيمة بالمنشآت المدنية والعسكرية وأنظمة الدولة ومؤسساتها، وعلى هذا فالحرب السيبرانية لا تقل خطورة عن الحروب التقليدية وبخاصة مع الارتباط الكبير لأنظمة الدولة وشؤون تسييرها بالبيئة الالكترونية الرقمية.

وتخوض الحرب السيبرانية عدة فواعل، يمكن تقسيمها إلى ثلاث فئات وهي:

أولا: الدول وهي الفاعل الاكثر قوة في الفضاء السيبراني ولكنها ليست الفاعل الوحيد.

ثانيا: الجماعات الافتراضية وهي شبكات تتشكل من مجموعة من الأفراد الذين يتقاسمون ويشتركون في نفس الأفكار والأهداف. وتزداد مخاطر هذه المجموعات إذا ارتبطت أنشطها بالتنظيمات الإرهابية كتنظيم الدولة الاسلامية (داعش) الذي عرف نشاطا كبيرا في الفضاء السيبراني.

ثالثا: الأفراد الذي يشكلون فواعل مهمة في الفضاء السيبراني وبخاصة مع ظهور وسائل التواصل الاجتماعي.[7]

الحقيقة أن الواقع الدولي في عصر العولمة والثورة المعلوماتية والتكنولوجية، يشهد تنامي زخم الحروب والهجمات السيبرانية، ومن الأمثلة على ذلك:

- الهجوم الالكتروني الذي شنته روسيا على أوكرانيا وقد خلف شللا تاما لمحطات توليد الكهرباء.
- الهجمات التي تشنها إسرائيل على إيران لتعطيل محطات توزيع الوقود بالإضافة إلى الفيروسات التي تستهدف تعطيل المشروع النووي الإيراني.
- قضية بيجاسوس والتجسس المغربي الإسرائيلي على الجزائر.

المحور الثالث: الأمن السيبراني: المفهوم، التحديات والمقومات

يعد الامن السيبراني مفهوم حديثا وليد الثورة المعلوماتية والتكنولوجية، كما يشكل محورا أساسيا من أي سياسة أمنية تسعى لتحقيق الأمن القومي، وقد أصبحت الدول تصنف مسائل الدفاع السيبراني كأولوية في سياساتها الدفاعية كما خصصت العديد من دول العالم أقساما خاصة بالأمن السيبراني في فرقها الأمنية الوطنية.[8]

يقصد بالأمن السيبراني مجموعة من الخطط والإجراءات التقنية والتنظيمية والقانونية، التي تتخذها الدول لمواجهة التهديدات والهجمات والاختراقات النابعة من الفضاء السيبراني. ويرتبط الأمن السيبراني بشكل وثيق بالقوة السيبرانية التي تعني القدرة على السيطرة والتاثير داخل الفضاء السيبراني.[9]

كما يعرف الأمن السيبراني على أنه عبارة عن مجموعة من الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الإستغلال وإستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات، وتعزيز الحماية وسرية وخصوصية البيانات الشخصية وإتخاذ جميع التدابير اللازمة لحماية مستخدمي الفضاء السيبراني، وهو جزء لا يتجزأ من التكتيكات الحديثة للحروب بإعتباره المجال الخامس للحروب الحديثة بعد البر والبحر والجو والفضاء.[10]

ومن أهم الأهداف التي يحققها الأمن السيبراني:

- المحافظة على أمن المجتمع و إستقراره.
- الحفاظ على سلامة عمل قطاعات الدولة الإلكترونية من أي إختراق.
- حفظ البيانات والمعلومات الإلكترونية الهامة.
- حماية شبكة المعلومات بأسلوب علمي وتقني محكم.
- تشفير التعاملات الإلكترونية بحيث لا يستطيع أي مخترق الدخول إليها.[11]

ويمكن أن يواجه الأمن السيبراني العديد من التهديدات النابعة من البيئة الافتراضية، كالتجسس الالكتروني، القرصنة الالكترونية، الإرهاب السيبراني[12]، الهجمات والاختراقات السيبرانية، وغيرها من التهديدات النابعة من البيئة الافتراضية.

ويتخذ الأمن السيبراني عدة أبعاد ومنها:

أولا البعد العسكري: أين يوفر الأمن السيبراني للقوات العسكرية التواصل وتبادل المعلومات و الأوامر وعن بعد بشكل آمن مع وجوب أن يكون قادرا على صد أي محاولة إختراق تؤدي إلى تدمير البيانات العسكرية دولة العدو، بحيث يمس الأمن القومي مثلما حدث في إيران عند إختراق منشآتها النووية.

ثانيا: البعد الإقتصادي: تظهر أهمية الأمن السيبراني بشكل أوسع وأكبر في المجال الإقتصادي ذلك أن الفضاء الإلكتروني أصبح أساسا للتعاملات التجارية والمالية والإقتصادية و أصبح الحاسوب أداة لتسيير الصناعة و الإقتصاد ولعل هذا ما جعل الامن السيبراني يكتسي أهمية حيوية.

ثالثا: البعد الإجتماعي: يكتسي البعد الاجتماعي للأمن السيبراني أهمية بالغة، لاسيما بعدما أصبحت مواقع التواصل الإجتماعي أداة إتصال عالمية بين البشر تمد بالمعلومات و الأفكار ولكن من ناحية أخرى قد تعرضت أخلاق المجتمع للخطر من ناحية أنه يمس بهوية الأشخاص ويهدد السلم الإجتماعي وعليه لابد من العمل أولا على تكريس مفهوم الأمن السيبراني ثم توعية الأفراد بمخاطر إختراقه.

رابعا: البعد السياسي: حيث يشكل الأمن السيبراني وسيلة هامة لحماية للمعلومات و الوثائق الأساسية و الحساسة لعمل قطاعات الدولة.[13]

خامسا البعد القانوني: يمثل القانون أداة ضبط المجتمعات وهو يحمل نفس الوظيفة بالنسبة للفضاء الإلكتروني إذ لابد أن تكرس الدول تشريعات خاصة و أطر قانونية تحدد الأعمال القانونية وغير القانونية في الفضاء الإلكتروني وقد لوحظ أن الجريمة القانونية تفتقر للصرامة في التعامل معها سيما بالنسبة للتشريعات الجنائية، كما أصبح الأمن الإلكتروني حقا جماعيا من الحقوق الحديثة وتفرعت منه عدة حقوق كحق النفاذ إلى الشبكة العالمية للمعلومات وحق إنشاء المدونات الإلكترونية والحق في حماية البرامج المعلوماتية ويقابلها مجموع إلتزامات مثل إلتزام الإبلاغ عن مخالفات وجرائم خاصة بالمحتوى ،كل هذا يتطلب وجود قوانين تواكب هذا التطور، وعلى هذا يجب على المنظومة القانونية أن تواكب هذا التطور التكنولوجي والرقمي وما يفرضه من تحديات.[14]

إن تحقيق الامن السيبراني يستدعي توفر مجموعة من المقومات وهي كالتالي:

- امتلاك التكنولوجيا والقدرة على التحكم فيها.
- امتلاك وتطوير بنية تحتية سيبرانية قوية.
- امتلاك خبراء من ذوي الكفاءة العالية في مجال المعلوماتية .
- امتلاك منظومة قانونية وتشريعية كفيلة بضمان الحماية الكافية للفضاء السيبراني.
- ضرورة ضمان موثوقية وسرية المعلومات.

خاتمة:

تأسيسا على ما سبق، توصلت الورقة البحثية إلى أن التطور التكنولوجي والثورة المعلوماتية والرقمية أثرت بشكل عميق في العلوم السياسية، حيث أصبحت الأجندة البحثية لهذا العلم تخوض في موضوعات مستجدة وغير تقليدية من قبيل الحرب السيبرانية، الأمن السيبراني، مواكبة لهذا التطور.

كما خلصت الورقة إلى أن الفضاء السيبراني تحول إلى ساحة جديدة للحروب والصراعات وأن أمن الدولة وقوتها في المستقبل لن يتحقق بامتلاك المعدات العسكرية فحسب، وإنما أيضا بمدى القدرة على امتلاك والتحكم في التكنولوجيا والمعلوماتية، فضلا عن امتلاك بيئية تحتية سيبرانية قوية، وعليه فأمن الدول في المستقبل يرتهن بشكل كبير بمدى امتلاك مدخلات وعناصر القوة السيبرانية.

الهوامش:

[1] عادل محمد عسكر محمد، "وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم دراسة على ضوء دليل تالين بشان القانون الدولي المطبق على العمليات السيبرانية" ، مجلة البحوث القانونية والاقتصادي، المجلد 33، العدد 1 ، 2021 ، ص262.

[2] حسين ربيعي، "الحروب السيبرانية: المخاطر وإستراتيجيات تحقيق الأمن السيبراني الدولي والداخلي"، المجلة الجزائرية للأمن الإنساني، المجلد 7، العدد 2، 2022، ص175.

[3] نورة شلوش، "القرصنة الإلكترونية في الفضاء السيبراني التهديد المتصاعد لأمن الدول"، مجلة مركز بابل للدراسات الأساسية، المجلد 8، العدد 2 ، 2015، ص190.

[4] عادل محمد عسكر محمد، المرجع السابق، ص275.

[5] جيلالي شويرب، فايزة مراد، "مفهوم الحروب السيبرانية والأمن السيبراني"، مجلة الحقوق والحريات، المجلد 11، العدد1، 2023، ص160.

[6] حسين ربيعي، المرجع السابق، ص177.

[7] إدريس عطية، "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري"، مجلة مصداقية، المجلد 1، العدد 1، 2019، ص107.

[8] جيلالي شويرب، فايزة مراد، المرجع السابق، ص164.

[9] حسين ربيعي، المرجع السابق، ص178.

[10] إدريس عطية، المرجع السابق، ص104.

[11] جيلالي شويرب، فايزة مراد، المرجع السابق، ص ص165-166.

[12] للمزيد من التفاصيل أنظر: موسى مصطفى محمد، الإرهاب الإلكتروني، مصر: دار الكتب والوثائق القومية المصرية، 2009.

[13] جيلالي شويرب، فايزة مراد، المرجع السابق، ص167.

[14] للمزيد من التفاصيل أنظر: عطية الدسوقي، إبراهيم طارق، الأمن المعلوماتي: النظام القانوني لحماية المعلوماتية، مصر : دار الجامعة الجديدة للنشر، 2009.

قائمة المراجع:

أولا: الكتب:

- مصطفى محمد موسى، الإرهاب الإلكتروني، مصر: دار الكتب والوثائق القومية المصرية، 2009.
- الدسوقي عطية، إبراهيم طارق، الأمن المعلوماتي: النظام القانوني لحماية المعلوماتية، مصر : دار الجامعة الجديدة للنشر، 2009.

ثانيا: المقالات:

- عسكر محمد عادل محمد، "وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم دراسة على ضوء دليل تالين بشان القانون الدولي المطبق على العمليات السيبرانية"، مجلة البحوث القانونية والاقتصادي، المجلد 33، العدد 1 ، 2021 .

- ربيعي حسين، "الحروب السيبرانية: المخاطر وإستراتيجيات تحقيق الأمن السيبراني الدولي والداخلي"، المجلة الجزائرية للأمن الإنساني، المجلد 7، العدد 2، 2022.
- شلوش نورة، "القرصنة الإلكترونية في الفضاء السيبراني التهديد المتصاعد لأمن الدول"، مجلة مركز بابل للدراسات الأساسية، المجلد 8، العدد 2 ، 2015.
- شويرب جيلالي، مراد فايزة ، "مفهوم الحروب السيبرانية والأمن السيبراني"، مجلة الحقوق والحريات، المجلد 11، العدد1، 2023.
- عطية إدريس، "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري"، مجلة مصداقية، المجلد 1، العدد 1، 2019.

الهندسة الأمنية السيبرانية الجزائرية في مواجهة الجرائم الإلكترونية

د.عدار محمد: جامعة بومرداس addar2001@yahoo.fr

مقدمة:

لقد سمحت عبقرية الإنسان في مجال الإبداع التكنولوجي بإدماج سريع لكل أطياف المجتمع في بيئة تكنولوجية جديدة قوامها الحاسوب الإلكتروني ، الشبكة العنكبوتية، البيانات ، البرمجيات ، المنصات، و غيرها من الأدوات التكنولوجيا التي تعرف عليها الإنسان مع بداية الألفية الثالثة .

و قد شهدت الجزائر مع مطلع الألفية إنتشار للوسائط الإلكترونية المختلفة و انخراط كل مكونات المجتمع في مسار التحديث الإلكتروني من رقمنة إدارية و تواصل اجتماعي و تطبيقات إلكترونية للنقل و السفر و التعليم ، الأمر الذي يتطلب تجهيز هذه الأدوات الإلكترونية بمناعة سيبرانية صعبة لإختراق من جهة و لاستعداد الآني لكل محاولات التعطيل أو الإتلاف أو التجسس على بيانات هذه الأجهزة.

تفرض هذه التحديات ، هندسة أمنية سيبرانية متكاملة تمزج بين التشريعات القانونية و عمل المؤسسات العسكرية و المدنية المنشئة في هذا الشأن بهدف إحباط كل محاولات التوغل الداخلية و الخارجية.

أ-إشكالية الدراسة: تناقش الدراسة لإشكالية التالية: فيما تتمثل السياسة لأمنية السيبرانية الجزائرية؟ و ما هي سبل نجاعتها؟

ب-فرضيات الدراسة: تعتمد الدراسة على الفرضيات التالية:

الفرضية الأولى: أدى تفوق الإنسان في مجال التقنية لإنتاج عدد هائل من الأدوات الإلكترونية المتناهية الدقة.

الفرضية الثانية: كلما زاد إنتشار تكنولوجيا المعلومات في مجتمع معين ،زاد معدل لإجرام الإلكتروني .

ج-المناهج المتبعة: تستأنس الدراسة بالمناهج العلمية التالية

المنهج التاريخي:المنهج المقارن:

1-التقعيد المفاهيمي لمتغيرات الدراسة: يكون من لأجدر مفاهيميا ، تحديد متغيرات الدراسة لأساسية التي تعتمد عليها في لإجابة على لإشكالية المطروحة ، و عليه، تعتمد الدراسة على المفاهيم التالية:

أ-تعريف الفضاء السيبراني: تنتسب كلمة " cyber " للفظ اليوناني "kybernetes"بمعنى الشخص الذي يدير دفة السفينة و تستخدم مجازا للمتحكم أو القائد.و يعد –في هذا السياق-عالم الرياضيات لأمريكي "روبرت وينرز"،"Robert, wienner's" المؤسس الأول لهذا الفضاء، صاحب كتاب: السيبرنيتقية أو التحكم و التواصل في عالم الحيوان و الآلة "cybernitics, or control and communication in the animal and the machine"،"الذي يعرفه: أنه علم القيادة و التحكم".

وبانتشار الوسائل التكنولوجيا و التقنية ، ساعد ذلك في ظهور "بيئة افتراضية "() و أضحت مكونات المجتمع المختلفة من فواعل رسمية و غير رسمية مندمجة في هذه البيئة الجديدة ، مما أضفى مرونة ، سهولة و سرعة في التعاملات بين فئات المجتمع المختلفة.

يمكن القول من خلال التعريف السابق أنه أقرب للإستراتجية الدولة في صناعة القوة و التفوق ، فمعاني القيادة و التحكم مرتبطة بالجيوش و القوة العسكرية ، و عليه ، هناك من يربط بين الفضاء السيبراني و الجيوش الحديثة ، فبعد البر ، البحر، الجو و الفضاء ، بدأت التصورات النظرية للإستراتجيات الحديثة للجيوش تأخذ بعين لإعتبار الفضاء السيبراني البيئة الجديدة للحروب المستقبلية().

ومع تطور ابتكارات الإنسان في المجال التكنولوجي المادي ، أصبح الفضاء السيبراني مفاهيميا أقرب للجوانب المادية ، حيث عرفته:

تعريف الوكالة الفرنسية لأمن أنظمة لإعلام :(anssi)تعرف الوكالة الفرنسية لأمن انظمة لإعلام ، الفضاء السيبراني على أنه "هو فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية." (

و في سياق آخر، و إن كان تعريف الوكالة الفرنسية يتطلب توفر العناصر المادية لإستحداث البيئة الإفتراضية ، فإن تعريف الإتحاد الدولي للإتصالات يشمل العناصر المادية و غير المادية في البيئة الرقمية ، حيث أصبحت البيانات ، البرمجيات ، المعلومات المحوسبة و المحتويات و غيرها من العناصر اللامادية التي تدخل ضمن مستلزمات البيئة الرقمية و على هذا لأساس نورد تعريف الإتحاد الدولي للإتصالات .

تعريف الإتحاد الدولي للاتصالات :(int)يعرف الإتحاد الدولي للإتصالات ، الفضاء السيبراني على أنه " المجال المادي و غير المادي الذي يتكون و ينتج عن عناصر هي: أجهزة الكمبيوتر، الشبكات ، البرمجيات ، حوسبة المعلومات ، المحتوى ، معطيات النقل و التحكم و مستخدموا كل هذه العناصر." ()و من التعريفين السابقين للفضاء السيبراني (تعريف الوكالة الفرنسية لأنظمة لإعلام/تعريف الإتحاد الدولي للإتصالات) نخلص إلى التعريف لإجرائي التالي :

تعريف الفضاء السيبراني:هو بيئة تفاعلية حديثة تتضمن عناصر مادية و غير مادية ، يشترك فيها كل أطياف المجتمع رسميين(مصالح حكومية، شركات ، قادة،.....) أو غير رسميين(افراد) استعمالا و تشغيلا.

ب-تعريف الجريمة الإلكترونية: على الرغم من إتاحة تكنولوجيا المعلومات فرصا هائلة للإنسان المعاصر ، فأصبحت يومياته أكثر سهولة، و ذلك من خلال توظيف البنية التحتية للوسائط الإلكترونية .

غير أن استعمالات الإنسان لهذه الوسائط لا يخلو من أخطار و تهديدات تطال الدول و الأفراد على حد السواء ، حيث أصبح السطو الإلكتروني و تعطيل أنظمة الشركات و المؤسسات و الابتزاز المالي للأفراد ، التجسس على بيانات حساسة لدولة ما من التهديدات الإلكترونية التي تتطلب لاستعداد أكثر من أي وقت مضى لها.

و تجدر لإشارة إلى أنه لا يمكن-إجرائيا-وضح تسمية مناسبة للتهديدات الناتجة عن استخدام الوسائل التكنولوجية ، فمن الباحثين من يوظف: مصطلح الجريمة الإلكترونية، الجريمة المعلوماتية، جرائم إساءة إستخدام تكنولوجيا المعلومات و الإتصال و جرائم الكمبيوتر و الإنترنيتو بإختلاف المصطلحات ، تتباين التعريفات() المهتمة بالجريمة الإلكترونية ، حيث يمكن تناول تعريف الجريمة الإلكترونية من الزوايا العلمية التالية:

التعريف الذي يركز على الجوانب التقنية: يمكن تعريف الجريمة الإلكترونية على أنها:"نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل لإجرامي المقصود"().

يحصر هذا التعريف الجريمة الأكترونية في الأبعاد التقنية و إغفال باقي عناصر التجريم التي ياتي ذكرها لاحقا.التعريف الذي يركز على الجوانب القانونية: يرى أنصار هذا التعريف آن التعرف على الجريمة الإلكترونية مقرون بتوفر مجموعة من المفردات الضرورية المتعلقة بإرتكاب جرائم الحاسب الآلي و هي: الحاسب الآلي ، برنامج الحاسب الآلي ، البيانات ، الممتلكات ، الدخول و الخدمات.

و منه يمكن تعريف الجريمة الإلكترونية على "أنها الجريمة التي تقع بواسطة الحاسب الآلي أو عليه أو بواسطة شبكة الأنترنيت."

يعتقد أصحاب الفقه القانوني أن الجريمة الإلكترونية قد تسارعت وتيرتها في الأونة الأخيرة ، فهي عابرة للحدود ، تعجز التشريعات الوطنية و الدولية في الإحاطة بحيثياتها و يفتقد فيها العنف المادي مقارنة بالجرائم التقليدية و أن أدلتها سهلة الإتلاف.

التعريف الذي يركز على بيئة وقوع الجريمة: يتمثل القصور الذي وقع فيه أنصار الجوانب القانونية في تجاهل و إهمال مكان أو بيئة وقوع الجريمة و هي "الشبكة العالمية للمعلومات"، حيث يعد الفعل الالكتروني إجراميا لما يتعلق الأمر" بتعطيل الشبكة أو العمل على إبطاء سرعتها أو إتلاف المواقع عليها"().

التعريف الذي يركز على الوسيلة: حيث يعرف الفقيه الألماني "تاديمان" ()الجريمة الألكترونية على أنها:" كل أشكال السلوك غير المشروع أو الضار بالمجتمع و الذي يرتكب بإستخدام الحاسب الآلي".

التعريف الذي يركز على الجوانب الموضوعية: بمعنى وقوع الجريمة الالكترونية داخل نظام الحاسب الآلي ، و عليه ، يمكن تعريفها على أنها"نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى

المعلومات المخزنة داخل الحاسوب أو التي ترسل عن طريقه.()"

التعريف الذي يركز على الجوانب المعرفية و الفنية للجريمة الإلكترونية: تعرف الجريمة الأكترونية على أنها أية "جريمة يكون متطلبا لإقترافها أن تتوفر لدى فاعلها معرفة بتقنية الحاسب الآلي"() .

التعريف الذي يركز على المعلومات: يقصد بالجريمة الإلكترونية "كل فعل أو إمتناع عمدي ينشأ غن الإستخدام غير المشروع للتقنية المعلوماتية و يهدف إلى الإعتداء على الأموال المادية أو المعنوية.

نستنتج مما سبق أن الدراسة توظف مصطلح "الجريمة الإلكترونية" باعتبار أن وقوع الفعل الإجرامي يتم بالإستعانة بالعناصر الالكترونية المادية و التي مقدمتها الحاسب الآلي أو أي أداة الكترونية أخرى أفرزتها الثورة المعلوماتية، إضافة إلى أن الفعل الإجرامي يطال التطبيقات المتضمنة في الحاسب الآلي كتعطيل البيانات أو التجسس عليها أو إتلافها .

ينم الفعل الإجرامي عن تدريبات أو توصيات يكون مخربوا هذه التطبيقات قد اطلعوا عليها و حاولوا تطبيقها على الشبكة المعلوماتية .

أنواع الجرائم الإلكترونية: تتمثل الجرائم الإلكترونية في النشاطات الرقمية التالية:

التعدي على الأنظمة المعلوماتية /الجرائم الواقعة على الأموال/التعدي على الملكية الفكرية للأعمال الرقمية/البطاقات المصرفية و النقود الإلكترونية/جرائم تمس المعلومات الشخصية /جرائم ضد الإنسانية بوسائل معلوماتية و الجرائم المعلوماتية ضد الدولة و السلامة العامة.

تمثل هذه الأنواع مجمل الجرائم التي هي موضوعات للمواجهة في إطار الأمن السيبراني ، حيث تعمل الفواعل الرسمية (الدول، الشركات،....)و غير الرسمية (أفراد) على الحد من استفحال ظاهرة الإجرام الإلكتروني عبر العالم.

ج-خصائص الجرائم الألكترونية: تتميز الجرائم الإلكترونية عن الجرائم التقليدية بالمكان الذي ترتكب فيه هذه الجرائم و الأدوات المستعملة في تنفيذ الجريمة ن فالبيئة الإفتراضية و الحواسيب هما من أركان الفعل الإجرامي أضافة لتوفر حد أدنى من الثقافة التقنية للجاني .

و تتميز الجرائم الإلكترونية ب():

تتم الجرائم بواسطة الحواسيب كأدوات لارتكاب الجريمة أما الانترنيت فهي وسيلة الفعل.

لا يتم في العادة التبليغ عن الجرائم الإلكترونية تفاديا للإساءة أو الإحراج.

جرائم صعبة الإدراك بحكم صعوبة تحديد الجاني و عدم تركها لآثار مادية.

جرائم غامضة تفتقد للإثبات المرئي.

جرائم عابرة للحدود و نتائجها تمس عدة أقاليم.

جرائم تتطلب قدر من الإلمام بقواعد التقنية.

جرائم تفتقد لتوظيف العنف المادي-الجسدي.

د-تعريف لأمن السيبراني: تتطلب مواجهة الجريمة الإلكترونية ، لإحاطة بمتطلبات تحقيق سياسة أمنية قائمة على تفعيل وسائل الحماية ، حيث يعد لأمن السيبراني المدخل الجوهري لمواجهة اخطار الجريمة الإلكترونية.

فالأمن السيبراني هو مصطلح مركب من كلمتين : أمن و سيبراني

التعريف اللغوي للأمن: لأمن هو نقيض الخوف، و مصدر للفعل أمن ،أمنا و أمانا و يعني اطمئنان النفس و سكون القلب و زوال الخوف و يقال: أمن من الشر أي سلم منه.

التعريف اللغوي لكلمة سيبراني: يمكن تعريف تشير كلمة سيبراني لغويا للعناصر التالية:

العناصر المادية مثل: الحاسوب ، لوحات الكترونية ، هواتف محمولة أجهزة نانوية و غيرها من الأدوات الإلكترونية التي اخترعها ضمن مسيرة التفوق و العبقرية و التي تساهم في تسهيل مناحي الحياة.

كما تشتمل الكلمة على العناصر غير المادية كالانترنيت ، البرمجيات و التطبيقات المختلفة المعروفة في التواصل كالواتساب و الفيسبوك و غيرها من التطبيقات .

ينتج عن العلاقة بين العناصر المادية و اللامادية توفر خدمات إلكترونية كالدفع الآلي ، الشراء الآلي ،. التحويل الآلي للمعطيات و البيانات و غيرها من الخدمات التي توفرها الشبكة العنكبوتية لمستعمليها.

التعريف لإصطلاحي للأمن السيبراني: يمكن القول في البداية أنه بالنظر لأهمية مصطلح لأمن السيبراني ، فقد كان محل تعريف من قبل هيئات رسمية تابعة لدول و مؤسسات عالمية ، كما ساهم كتاب في وضع تعاريف متباينة مرتبطة من زاوية النظر أو الرأي التابعة لمفكر أو آخر.

تعاريف الهيئات الرسمية: من الهيئات الرسمية التي ساهمت في وضع تعريف للأمن السيبراني ، نجد:

تعريف وزارة الدفاع لأمريكية : عرفت وزارة الدفاع لأمريكية مصطلح لأمن السيبراني على أنه:"جميع لإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية و الإلكترونية من مختلف الجرائم : الهجمات ، التخريب، التجسس و الحوادث.

نستنتج من تعريف وزارة الدفاع لأمريكية أنه يركز على ضرورة مجابهة التهديدات السيبرانية المختلفة التي قد تطال المعلومات من تخريب و تجسس و غيرها عن طريف اتخاذ جميع لإجراءات من دون لإشارة إلى نوعها، و يتقارب تعريف وزارة الدفاع لأمريكية مع تعريف لإعلان الأوروبي الذي يركز على التصدي لكل حاولات لإختراق التي تستهدف بيانات و معلومات الشركات و الأشخاص.

تعريف لإعلان الأوروبي: عرف لإعلان الأوروبي، لأمن السيبراني على أنه :" قدرة النظام المعلوماتي على مقاومة محاولات لاختراق التي تستهدف البيانات.

تعاريف الهيئات الدولية: عرف الإتحاد الدولي للإتصالات في تقريره الصادر في 2010-2011، لأمن السيبراني على أنه : مجموعة من المهمات : مثل تجميع وسائل و سياسات و إجراءات أمنية و مبادئ توجيهية و مقاربات لإدارة المخاطر و تدريبات و ممارسات فضلى و تقنيات يمكن استخدامها لحماية البيئة السيبرانية و موجودات المؤسسات و المستخدمين."

يركز الإتحاد الدولي للاتصالات في تعريفه للأمن السيبراني على العناصر التالية:

-عناصر موجهة للأفراد(الكادر المستخدم): تدريب الأفراد و مستخدمي الأنترنيت على كيفيات التعامل مع بيئة المخاطر الجديدة .

- عناصر أكاديمية: ضرورة التزود بالمقاربات النظرية و المبادئ التوجيهية لضمان سلامة البيانات، موجودات المؤسسات و المستخدمين.

-عناصر أمنية:الاستنجاد بالإجراءات الأمية الضرورية لحماية البيئة الافتراضية.

التعاريف الأكاديمية للكتاب: من التعاريف الأكاديمية للكتاب و الباحثين ، نورد مايلي:

تعريف أدوارد اموروزو: يعرف أموروزو الأمن السيبراني على أنه :" وسائل ممن شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات و تشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة و كشف الفيروسات ووقفها و توفير الاتصالات المشفرة"().

يركز أمروزو على وسائل المجابهة من خطر الجريمة السيبرانية و الأدوات التي من شأنها كشف الفيروسات و مواجهة القرصنة و توفير الإتصالات المشفرة.

تعريف الكاتبان Martti Lahto, Pekka, Neittaanmaki " :":" مجموعة من الإجراءات التي إتخذت للدفاع ضد هجمات قراصنة الكمبيوتر و عواقبها و يتضمن تنفيذ التدابير المضادة المطلوبة".()

يركز الكاتبان على جملة الإجراءات المتكاملة التي تتسلح بها الدول و الشركات للدفاع عن قراصنة الكمبيوتر.

تعريف :A.kemmerer ; Richard عبارة عن وسائل دفاعية من شأنها كشف و إحباط المحاولات التي يقوم بها القراصنة."

يرى ريتشارد كامرر على ضرورة إعداد وسائل دفاعية ذات منشأ تقني لإحباط كل محاولات القرصنة التي بات مرتكبوها (القراصنة) يوظفونها لتهديد مستخدمي و مستعملي الشبكة العنكبوتية.

يمكن القول في الأخير أن الأمن السيبراني هو مجموعة الآليات و الإجراءات و الوسائل و الأطر الهادفة لحماية أجهزة الكمبيوتر و البرمجيات من مختلف التهديدات السيبرانية التي تقوض نشاط الفواعل.

2-المصطلحات المتقاطعة مع الأمن السيبراني: يتقاطع مصطلح الأمن السيبراني مع المصطلحات التالية ذات العلاقة:

الردع السيبراني: منع الأعمال الضارة ضد الأصول الوطنية في الفضاء السيبراني.

الهجمات السيبرانية: هو سلوك يقوض من قدرات شبكات الكمبيوتر لغرض قومي أو سياسي من خلال استعمال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام.

الجريمة السيبرانية: مجموعة الأعمال و الأفعال غير القانونية التي تتم عبر معدات أو اجهزة إلكترونية.

3-أهمية الأمن السيبراني: تكمن أهمية الأمن السيبراني في النقاط التالية:

-الحفاظ على المعلومات و سلامتها.

-حماية الأجهزة و الشبكات من الإختراقات و التعطيل .

-إكتشاف نقاط ضعف الأنظمة و معالجتها.

-توفير بيئة سيبرانية آمنة خلال استخدام الشبكة العنكبوتية.

4-أهداف الأمن السيبراني: تتمثل أهداف الأمن السيبراني في:

-صمود البنى التحتية الحساسة للهجمات الإلكترونية.

-الحد من التجسس و التخريب الإلكتروني على مستوى الحكومة و الأفراد.

-سد الثغرات في أنظمة امن المعلومات.

-تدريب الأفراد على آليات و إجراءات مواجهة الإختراقات المتعلقة بأجهزتهم سواء بالإتلاف أو بالسرقة.

-الحد من التجسس و التخريب الإلكتروني على مستوى الحكومة و الأفراد.

4-مكان الفرد في الفضاء السيبراني: مع الاعتماد المتزايد في الحياة اليومية على الأنظمة المعلوماتية و الأجهزة المتصلة بالشبكة الدولية للمعلومات و تشعب طبيعة هذه الأجهزة من هواتف خلوية و أجهزة حوسبة فردية ، و يزداد عدد المتعاملين بالفضاء السيبراني لدرجة الارتباط العضوي بين الفرد و الأداة الإلكتروني.

و تشير التقديرات أنه في الفترة الممتدة من 2014إلى 2018 ، انتقل عدد مستخدمي الإنترنيت من 2.8 مليار مستخدم إلى 3.8 مليار مستخدم ()، و سيعرف المزيد من حالات اندماج الأفراد في البيئة الافتراضية بحكم أن ممارسة نشاطات الإنسان الأساسية ، أصبحت تأديتها من خلال الفضاء السيبراني و عليه، يمثل الفرد داخله حلق أساسية باعتباره مستخدم يستفيد من المرونة و السهولة التي توفرها الإنترنيت في تحقيق أهداف الإنسان المختلفة ، كما تمثل في نفس الوقت تحديا للإنسان ذاته مع تزايد معدلات الجريمة الإلكترونية من قذف، ابتزاز ، احتيال و انتحال الشخصية و غيرها من التعاملات السلبية التي قد يتعرض لها الإنسان.

5-أبعاد الأمن السيبراني : تتمثل أبعاد الأمن السيبراني في:

أ-البعد السياسي: لقد أصبحت مختلف أجهزة الدولة معتمدة على التكنولوجيا في تصريف نشاطاتها و صارت "البيئة الرقمية" هي الفضاء الجديد في التعامل الإداري، الاقتصادي ، القضائي و حتى الاتصالي ، إذ بات العديد من قادة العالم يخاطبون شعوبهم عن طريق منصات التواصل المختلفة : فيعبرون عن نشاطات معينة تهم إقليم الدولة التي ينتمون إليها أو حتى انشغالات عالمية عن طريق استخدام شبكات الاتصال و الإعلام .

إن التحول الرقمي الحاصل في العالم ، بقدر ما سهل التنسيق و الإنسجام بين مؤسسات الدولة المختلفة و أضفى مرونة في طريقة تسيير المرافق المختلفة ، بدأت العالم يتجه نحو تهديدات جديدة تفوق التهديدات التقليدية أين أصبح "الفضاء السيبراني" هو ميدان المعركة الخامس() الذي قد يقوض كيانات الدول و يجعل مؤسساتها خارج الخدمة أو تدمير لبيتها التحتية و غيرها من الهجمات السيبرانية التي قد تكون الدولة عرضة لها.

و عموما ، يمكن ذكر مجموعة من العوامل ، ساهمت في بروز الحروب السيبرانية :

-تزايد ارتباط دول العالم بالفضاء السيبراني ، مما يجعل البنية التحتية للدول أكثر عرضة للهجمات السيبرانية.

-تراجع دور الدولة في الجوانب الإقتصادية ، وبروز الشركات، خاصة تلك العاملة في المجال الإلكتروني كفاعل مؤثر في البيئة السيبرانية.

-قلة تكلفة الحروب السيبرانية مقارنة بنظيرتها التقليدية ، حيث أن الحروب السيبرانية لا تتطلب الوقت الكثير لتنفيذها.

-توظيف الفضاء السيبراني في تعظيم دور الدولة من خلال العمل على إبراز التفوق في إعداد الإستراتيجية السيبرانية للدولة.

-اتساع نطاق مخاطر الأنشطة التي يقوم بها الفاعلون سواء من الدول أو من غيرهم ، فقد تشن الهجمات السيبرانية عبر الأجهزة الأمنية السيبرانية التابعة للدولة أو عبر قراصنة أو عملاء لاستهداف بيانات الخصوم .

أدت هذه العوامل لجعل الدول عرضة لهجمات سيبرانية ، خاصة إذا اعتبرنا كل دولة تملك قدرات و إمكانيات المواجهة تختلف عن تلك الموجودة لدى دولة أخرى ، غير أن ذلك لا يمنع في جعل الهجمات السيبرانية على الدول تشترك في العناصر التالية:

استهداف البنية التحتية للدول: تكون البنى التحتية للدول و المرافق الحيوية فيها ، مدنية و عسكرية،عرضة لهجمات سيبرانية ، فتشل أنظمتها و يتعطل نظام تشغيلها ، فتضطرب يوميات المواطن و تسود الفوضى في إقليم الدولة ().

و من أمثلة الهجوم الالكتروني الذي يستهدف الدول ما تعرضت له شبكة المياه الأوكرانية و الذي سبب في بقاء أوكرانيا لساعات في الظلام ، مما يوحي أن الهجمات الإلكترونية قد تخطت حاجز البيانات و المواقع الإلكترونية لتشمل البنية التحتية و الأنظمة الحيوية للدولة كالمفاعلات النووية ، أنظمة الكهرباء، الأنظمة الطبية و غيرها من البنى الحيوية للدولة.

كما وقعت الحكومة لإستونية في 2007م ضحية لهجمات سيبرانية من قبل مجموعات روسية نتيجة قيام الحكومة بإزالة تمثال الجندي البرونزي و جثث جنود روس سقطوا أثناء الحرب العالمية الثانية من حديقة عامة في "العاصمة تالين".

استهدف الهجوم السيبراني في الأول و تحت مسمى"الحرمان من الخدمة"DDoS"،"الوزارات الحكومية ، البنوك و مقرات لأحزاب السياسية و في موجة ثانية تم تعطيل الخوادم الخاصة و الصحف . فتأثر الإقتصاد لإستوني و تعطلت يوميات السكان و أصبحت الأنظمة المعلوماتية للبنية التحتية لإستونيا في يد هذه المجموعات ، مما يؤثر على علاقة الأفراد بنظامهم السياسي و ارتهان سيادة الدولة.

من أشهر الهجمات السيبرانية التي استهدفت البنى التحتية للدول ، ما تعرض له خط أنابيب النفط التركي بتاريخ 05أوت 2008م حيث اشتعلت النيران من دون انذار مبكر عن الحادث من طرف المستشعرات الإلكترونية الموضوعة لذلك .

يندرج هذا الهجوم السيبراني من زاوية العلاقات الدولية ضمن معارضة روسيا لإنشاء خط أنبوب للغاز يضم الثلاثي:باكو-تبليسي-جيهان ، بحكم أن هذا المشروع الجديد يقع خارج الدائرة الروسية و بالتالي تقويض قدرتها في التحكم في تدفق الطاقة لأوروبا().

كما كانت محطات التزود بالكهرباء-في 2008- في البرازيل عرضة لهجمات سيبرانية ، حيث تمكن القراصنة من الدخول إلى الموقع الشبكي للحكومة و السيطرة عليه لمدة تزيد عن أسبوع ن حيث أن الإنقطاعات المتكررة للكهرباء في البرازيل هي نتيجة لهجوم سيبراني، و نفس المشهد، تعرضت له شركة الكهرباء في الولايات المتحدة لأمريكي.

شهدت السعودية هجوما سيبرانيا عنيفا ، في 2017م نفذه سيبرانيون إيرانيون يدعى "الصخرة الدوارة , Stone"،" "Drillحيث أحدث تأثيرات كبيرة على شركات الطيران و البيتروكيمياويات السعودية ، كما مارس-في نفس السياق- قراصنة إيرانيون هجمات سيبرانية متقدمة تحمل اسم ، A.P.T:إستهدفت بنى تحتية لدول الخليج .

و شهدت إيران سلسلة من الهجمات السيبرانية ، طالت البنية التحتية لهذا البلد بهدف تقويض لقدراته الصناعية و اتجاهه نحو امتلاك السلاح النووي و تمثلت الهجمات السيبرانية في:

-هجوم سيبرانا بتاريخ 2 جويلية 2020م استهدف مفاعل "نتانز" النووي.

- هجوم آخر بتاريخ 4 جويلية ، حدث انفجار في محطة "شهيد مدح زرقان".

- هجوم الكتروني في 7 جويلية تعرض مصنع الأوكسجين في بلدة"باقر" .

-هجوم سيبراني استهدف منشأة صواريخ تابعة للحرس الثوري الإيراني في 9 جولية 2020.

-انفجار غاز مبنى سكني في طهران بتاريخ 11 جويلية.

-شهد" مصنع توند جويان" للبتروكيمياويات الإيراني تفجيرات مرعبة سببها هجمات سيبرانية.

-عرف مجمع صناعي ايراني انفجار في 13 جويلية و حريق في مصنع الالمنيوم في بلدة "لامرد" الإيرانية و انفجار في خط انابيب نفط في "الاهواز" في 18 جويلية و انفجار في محطة توليد الطاقة في "اصفهان" .

وقد قامت مجموعة من القراصنة "المنتقمون"الايرانية بهجوم سيبراني استهدف شبكة المياه و الكهرباء لاسرائيلية في 16 جويلية2020.

يمكن القول أن البنى التحتية لمختلف الدول تمثل الأهداف المثلى للهجمات السيبرانية نظرا لما تخلفه هذه الاعتداءات من انكشاف أمني للدولة من جهة و قلق و خوف لدى الساكنة.

-فقدان الثقة بين أجهزة الدولة: تؤدي الهجمات السيبرانية التي تقوم بها الدفاعات الأمنية للدولة ضد البنى التحتية للدولة مناوئة لتدني درجة الوثوقية لدى أجهزة و مصالح الدولة المختلفة .

معروف على الدولة قوة أداء نظامها السياسي و التزامها القانوني بتعهداتها تجاه مواطنيها في المجال الداخلي حيث تلتزم بتوفير الحماية والسكينة و الأمن للأفراد داخل اقليم الدولة، فبتعرض أحد منشآت الدولة للتخريب الأرهابي أو الالكتروني يكون عى عاتق تلك الدولة صد تلك الهجمات من جهة و ضمان عودة نشاط تلك الأجهزة للخدمة في وقت وجيز و ذلك حتى تحافظ الدولة على درجة الوثوقية بينها و بين مواطنيها و حتى بين الدولة و الشركاء الأجانب لاسيما في المجال الاقتصادي. و نظرا لتفاوت مستوى التصدي للهجمات السيبرانية ، قد يتعرض النظام السياسي لدولة ما لفقدان الثقة بينه و بين مواطنيه إذا أظهر عجزا في مواجهة تلك التهديدات ، و عليه ، يقع على عاتق الدولة تحديث أجهزتها الإلكترونية بانتظام لتفادي اي طعن في مشروعية النظام السياسي.

ب-البعد الإقتصادي لقد أضحت الأسواق المالية –بفضل أنظمة حماية الشبكات الإلكترونية-أكثر اتصالا ببعضها البعض من ذي قبل ، فللمؤسسات المالية قدرة على تبادل رؤوس الأموال الكترونيا و في ظرف وجيز.

غير أنه و في نفس السياق ، تعتبر القطاعات الاقتصادية و المالية أكثر عرضة للهجمات السيبرانية التي من المحتمل تزايدها في المستقبل، فالمصاريف المالية ، قطاع التأمين ، شركة الطيران،مؤسسات الفندقة هي عبارة عن أهداف سيبرانية لما وصفته الحكومة الأمريكية "هجوم الفدية "ransom war"،"ووفقا لتقديرات مكتب التحقيقات الفيدرالي الأمريكي فإنه يرى أن مبلغ الفدية يقترب من مليار دولار سنويا و ان الشركات التجارية تقع ضحية هجومات سيبرانية كل 14 ثانية خاصة إذا إعتبرنا أن عام 2018 هو عام لإختراقات الإلكترونية.

لقد أصبحت الهجمات السيبرانية أكثر تكلفة بالنسبة للمؤسسات المصرفية والمالية ، ففضلا عن الخسائر المالية التي تعدت 80 مليار دولار خلال الهجمة السيبرانية الواحدة، تتسبب هذه الهجمات في فقدان الثقة لدى العملاء مما قد يؤدي لسحب الودائع و حصول ازمة سيولة .

أصبح الاقتصاد العالمي يتكبد نتيجة الهجمات السيبرانية ما يتجاوز 230 مليار دولار، بمعدل 1000 هجمة كل دقيقة ، اين تكون المؤسسات المالية هي الهدف الأول لهذه الهجمات ن مما يتطلب تجديد و تفعيل لبرامج الكشف المبكر عن الهجمات و استباق حدوثها من قبل الدول ، و من التجارب ، يمكن ذكر():

-التجربة الإفريقية: تم تأسيس "اتفاقية الأمن الإلكتروني و حماية البيانات الشخصية" أو "اتفاقية مالابو" التي بموجبها تم وضع الحد الأدنى من المعايير و الإجراءات لبناء بيئة رقمية موثوقة بهدف ضمان احترام الخصوصيات على الأنترنيت.

-التجربة الصينية: تبنى البرلمان الصيني في 2016م القانون الجديد الأمن السيبراني الذي دخل حيز النفاذ في 2017م الذي يحدد مهام القطاعات الحكومية تجاه تأمين الشبكات و البيانات ، كما تضمن القانون كيفيات ضبط و مراقبة مزودي الأنترنيت ، كما يجبر القانون-تحت اسم" الجدار الناري العظيم-مختلف الشركات و المؤسسات بوضع برامج حماية ضد الهجمات السيبرانية إلى مستوى قد يصل إلى حجب بعض المواقع المتسللة إلى الكيانات الإقتصادية الصينية.

-التجربة الأمريكية: قامت الولايات المتحدة الأمريكية في 2014م بإطلاق "برنامج العمل لتحسين الأمن السيبراني للبنية التحتية الحساسة" الذي يقوم على الجانب التطوعي-موجه للشركات و المؤسسات المالية-من اجل حماية ممتلكاتها المعلوماتية من أي إختراق سيبراني ، و حسب الإحصائيات ، فإن 30% من المؤسسات الأمريكية قد انخرطت في هذا البرنامج.

وفي ماي2020م تم إصدار أمر رئاسي لتحديث الخدمات السحابية لمختلف الوكالات الفيدرالية و تطوير برنامج تدريب متخصصين يقضي بمراجعة تقنيات السلامة السيبرانية و الكشف المبكر عن الثغرات الأمنية.

-التجربة الأوروبية: تعمل المفوضية الأوروبية –ضمن برنامج توجيه الشبكات و أمن المعلومات-على تحديث قواعدها للأمن السيبراني عبر العناية بالقطاعات الحساسة كالصحة و الدفاع.

و على صعيد الدول ، تمكنت بريطانيا من إحباط 250 هجوم سيبراني بفضل يقظة مكتب الاتصال الإلكتروني ووزارة الدفاع البريطانية ، في حين قامت ألمانيا بتحديث أنظمة حماية الشبكات و صيانتها.

ج-البعد العسكري: إن لجوء الدولة إلى الشبكة الإلكترونية من أجل خلق بيئة افتراضية يسهل التعامل من خلالها بين مختلف المصالح و الهيئات من جهة و ضمانا لخدمة نوعية و عصرية و سريعة لمختلف البيانات و المعلومات التي ترد إلى هذه الهيئات غير أنه أحيانا ، قد تقع هذه البيانات فريسة لقراصنة إلكترونيين يعملون على تعطيلها، التلاعب بها أو إتلافها ن الأمر الذي يصنع تحديات أمام الدولة من الجانب العسكري ، تتمثل في:

التجسس الألكتروني: يعني التجسس الإلكتروني() تلك المحاولات المتعمدة لاختراق اجهزة الكمبيوتر التابعة لدولة خصم بهدف سرقة معلومات سرية في ميادين سياسية ، اقتصادية ، اقتصادية و أمنية –عسكرية .

يعمل التجسس على تسريب معلومات سرية لدى دولة ما و استغلالها لمصلحة دولة معينة ، فمثلا استطاع "هاكرز مجهول الهوية من النفاذ لجهاز معلومات أحد متعاقدي الجيش الأمريكي و سرقة آلاف الملفات الخاصة بالمقاتلة "أف-35"، كما أن سرقة المعلومات الاقتصادية لدولة ما قد تؤثر على مواقفها التفاوضية بين الدول ، و قامت وكالة الأمن القومي الأمريكي بالتجسس على أجهزة معلومات أكثر من 35 شخصية سياسية بارزة عبر العالم و تحصلت على معلومات ، نتيجة تجسسها على أكثر من 60 مليون مكالمة عبر العالم الأمر الذي يوحي بأنة عملية التجسس لا تشمل فقط رعايا الدولة المناوئين بل تتجاوز حدود الدولة لتشمل أفراد في العالم و الدليل ما خلفه "برنامج بيقاسوس "pigasus project"،"

من جو عدم الثقة و تقويض الأمن و السلم العالميين ، فللعلم أن هذا البرنامج طورته شركة groupe NSO" "الإسرائيلية التي تقوم على اختراق مليارات الهواتف التي تعمل بنظام تشغيل الأندرويد أو ios و تزداد قوة هذا البرنامج عند اعتماده على هجمة "صفر نقرة" فحتى أذا لم يشغل المستخدم جهازه ، يستطيع هذا البرنامج اختراقه، حيث تعرض ألاف الصحافيين و النشطاء و حتى قادة دول للإختراق عن طريق هذا البرنامج .

السيطرة على الانظمة العسكرية و تعطيلها او اتلافها: كأن يقوم قراصنة محترفين أو جيوش نظامية بشن هجوم سيبراني يهدف للسيطرة على نظم القيادة و السيطرة العسكرية التابعة لدولة ما و اخراجها عن دائرة تحكم القيادة المركزية و إعادة توجيهها نحو اقليم الدولة أو ضد دول صديقة ، كما تستهدف الهجمات :طائرات بدون طيار ، الغواصات النووية و حتى الأقمار الصناعية العسكرية يمكن اخراجها-عن طريق هجمات سيبرانية-من مداراتها و تحكم الدول التابعة لها و استغلال معلوماتها .

و من الأمثلة التي تدل على سرقة تصميمات عسكرية للدول ما تعرضت له شركة "لوكهيد-مارتين" الأمريكية من سرقة لبرامج تصميم المقاتلة "اف-35" لتستفيد منها الصين في تصميم المقاتلة"تي20".

كما تعرض مقاولون تابعون لوزارة الدفاع الأمريكية يعملون في مجال تصنيع طائرات بدون طيار للإختراق بهدف سرقة برامجهم المتعلقة بكيفيات تطوير هذا النوع من الطائرات.

سرقة المعلومات و البيانات العسكرية أو التلاعب بها: تكون البيانات الخاصة بتصميمات المعدات أهدافا مثلى للهجمات السيبرانية ، فقد شنت أقوى الهجمات على حواسب الجيش الأمريكي ،سنة 2008م عن طريق وصلة(u.s.b)كانت متصلة بمحمول تابع للجيش الأمريكي ، فتم تسريب لآلاف البيانات من الملفات العسكرية إلى خوادم خارجية.

كما تعرض العراق في سبتمبر 2019م لهجوم سيبراني تمثل في سرقة معلومات بيانات وزارات حساسة على غرار الداخلية و الدفاع الوطني و الخارجية و الصحة ،و على الرغم من تصدي الحكومة العراقية لهذه الهجمات و النجاح في استرجاع معلومات بعض المصالح إلا أن تحقيق الأمن السيبراني الشامل يبقى هدف بعيد المنال.

جمع معلومات اقتصادية استخباراتية: لطالما كانت قواعد بيانات الشركات و البنوك مطمعا لقراصنة و عملاء و حتى أجهزة تجسس تابعة لدول ، و في هذا الإطار ، اصدر الرئيس السابق الأمريكي "باراك أوباما " في فترة إدارته الثانية أوامر بوقف التنصت على مقري المؤسسات المالية العالمية و ذلك عقب تسريبات كشف عنها المتعاقد السابق في الجيش الأمريكي "ادوارد سنودن" بخصوص وجود برامج تنصت أمريكية تستهدف جمع معلومات حول حلفاء و اعداء الولايات المتحدة الأمريكية و حتى بعض الأمريكيين كما قامت كوريا الشمالية بهجمة سيبرانية استهدفت شركة "سوني " sony pictures entertaiment"،"

مما جعل آلاف الحواسيب خارج الخدمة و تم تسريب آلاف البيانات الحساسة بخصوص موظفي هذه الشركة و شخصيات عالمية شهيرة كانت تتعامل معها الأمر الذي يجعل تفوق الهجمات على برامج الحماية و يجعل من مستلزمات تطبيق الأمن السيبراني تحديا يساور الكثير من المهندسين و الخبراء .

د-البعد الاجتماعي: قد لا نختلف إذا اعتبرنا أن البيئة الافتراضية لم تعد آمنة ، فالغزو الثقافي الرقمي ، الجريمة الألكترونية و التنمر و الابتزاز الإلكترونين ، كل هذه الحالات هي نتائج لانتشار المعدات الإلكترونية في المجتمع، فوفقا لقائمة جدول أعمال علم الاجتماع المعاصر و التي اعدها"اولريش بك"، uilrich, beck " حيث يرى أن المجتمع الإنساني المعاصر بانتقاله إلى عصر المعلوماتية يشهد "حالة من الفوضى " و عدم الأمان و فقدان اليقين و غيرها من التوصيفات التي ضمنها الكاتب في مؤلفه:"مجتمع المخاطر العالمي: بحثا عن الأمان المفقود"() و ذلك نتيجة لتعاظم التهديدات السيبرانية.

و من التحديات التي تخلفها الجريمة الإلكترونية في أبعادها الاجتماعية ما تعلق ():

-تهديد القيم و الأخلاق: لقد بات المجتمع مع انتشار الوسائل الإلكترونية أكثر عرضة للمحتويات السلبية غير المرغوب فيها قد تؤثر على سلوكيات الأفراد في جانبها الأخلاقي فالتنمر و الحث على التجنيد و الإنتساب لجماعات ارهابية في الفضاء السيبراني من الجرائم الإلكترونية التي بات من الضروري إدراك مخاطرها و التجند لمحاربتها من خلال زيادة الوعي الاجتماعي في توظيف هذه الوسائط في التدريب و التربية و اكتساب المعارف.

-ضياع الهوية: لقد تكرست رابطة الإنسان مع بيئته و مجتمعه منذ ولادته، فيتفاعل مع الآخرين في إطارها ، فتنشأ تلك الرابطة الهوياتية بينه و بين بيئته ، غير أنه بعد انتشار التقنية ، بدأ زوال الرابطة باتجاه الإنسان نحو الكسموبوليتالية و ظهور اهتمامات عالمية للإنسان جعلته يفتقد هويته المحلية و يذوب في هوية العالم السائلة الأمر الذي يؤثر على منظومة القيم التي كونها نتيجة اتصاله ببيئته المحلية.

ه-البعد القانوني: يمثل القانون أداة لضبط المجتمع عن طريق مجموعة القوانين و الأوامر ، و طبيعي أيضا أن يحمل نفس الوظيفة فيما يتعلق بالفضاء السيبراني ،فالجريمة على المستوى الإفتراضي تفتقر للصرامة و عليه ، بات من الواجب على الدول تكريس منظومة قانونية لتنظيم نشاط الفواعل على مستوى البيئة الإفتراضية .
لقد أصبح حق النفاذ إلى هذه البيئة و ما يترتب عنها من حقوق المستحدثة كحق إنشاء المدونات الإلكترونية ، الحق في حماية البرامج الإلكترونية من التحديات التي تنتظر التشريع للاجتهاد بخصوصها و إثرائها().

5-الهندسة لامنية السيبرانية الجزائرية: لقد سارعت الجزائر في إطار تطويق انتشار الجريمة الإلكترونية لهندسة سياسة أمنية متكاملة و متناسقة لردع كل محاولات لإختراق المؤسسات الرسمية كالمصالح الحكومية و الهيئات الرسمية و البنوك و المؤسسات الإقتصادية و حتى حسابات رجال السياسة و المال و الإقتصاد ، و من ثم تتمثل ركائز السياسة لأمنية السيبرانية في الأركان التالية:
أ-التشريعات القانونية: مع بروز لإجرام الإلكتروني كشكل جديد من التهديدات ، و إعتماده على التطور التكنولوجي كأدوات لتنفيذ الجريمة ، بادر المشرع الجزائري لإتخاذ جملة من التدابير و لإجراءات القانونية من أجل ردع أساليب الجرائم المختلفة الحديثة منها و التقليدية.
نظرة المشرع الجزائري لبرامج لإعلام الآلي: اعتبر المشرع الجزائري ، وفقا للمادة 4 من لأمر 03-05() المتعلق بحقوق المؤلف و الحقوق المجاورة برامج الحاسب الآلي مصنفا أدبيا مكتوبا و محميا ، حيث يمكن لصاحبها الحق في إستغلال برنامجه و إبلاغه لجمهوره تحت أية منظومة معلوماتية ، فيترتب عن ذلك حقوقا مادية للمؤلف صاحب البرنامج .
و امام التهديدات المتزايدة للجريمة الإلكترونية ، تم تعديل قانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 و المتمم للأمر رقم56-156 المتضمن قانون العقوبات، حيث تم إدراج قسم خاص يتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات الإلكترونية ، إذ جرم المشرع الجزائري –بموجب قانون العقوبات-الأفعال التالية:
أولا: المعاقبة بالحبس-بموجب المادة 394 مكرر- من ثلاثة أشهر إلى سنة و بغرامة مالية من 50.000دج إلى 100.000دج ، عن فعل الدخول و البقاء غير المشروع لمنظومة معلوماتية ، و تضاعف العقوبة أذا ما ترتب على فعل الدخول تغيير أو حذف لمعلومات تلك المنظومة
ثانيا: المعاقبة بالحبس-بموجب المادة394 مكرر1- من ستة أشهر لثلاث سنوات و بغرامة مالية من 500.000دج إلى 2000.000دج كل من أدخل عن طريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها(التزوير المعلوماتي).
ثالثا: المعاقبة بالحبس-بموجب المادة 394 مكرر2-من شهرين إلى ثلاث سنوات و بغرامة مالية من 1.000.000دج إلى 5.000.000دج كل من يقوم عمدا أو عن طريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية ، بمعنى آخر ، جرم المشرع الجزائري فعل لإستيلاء على المعطيات المعلوماتية أو إفشائها أو الإتجار بها لأي غرض كان ، إضافة إلى جريمة لإحتيال المعلوماتي عن طريق تصميم و تجميع معطيات المنظومة المعلوماتية عن طريق الغش.
رابعا: مصادرة لأجهزة ن البرامج و الوسائل الإلكترونية المستخدمة –بموجب المادة394 مكرر6-مع إمكانية إغلاق المحل مكان لإستغلال إذا كان حدوث فعل الجريمة بعلم صاحبها.
خامسا: شدد المشرع الجزائري العقوبة –بموجب القسم السابع من قانون العقوبات 04-15-على الجرائم التي تستهدف جهاز الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام.

سادسا: نص المشرع –بموجب المادة394 مكرر5-على تجريم الإشتراك في مجموعة أو إتفاق لغرض الإعداد لجريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

سابعا: و قد شملت المادة 394 مكرر 4 العقوبة التي تطال الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في القسم السابع من قانون العقوبات ، حيث تشمل العقوبة غرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

و اعتبرت المادة 394 مكرر7 أن الشروع في الجريمة المعلوماتية يعاقب عليها بالعقوبة المقررة للجريمة ذاتها.

قانون 06-23 المؤرخ في 20 ديسمبر 2006(): مع تزايد خطورة الإجرام المعلوماتي ن ادخل المشرع الجزائري تعديلات أخرى بموجب قانون 06-23 المؤرخ في 20 ديسمبر 2006 حيث مس التعديل القسم السابع مكرر الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

جرم المشرع كل أنواع المساس بحرمة الحياة الخاصة بإستخدام الوسائل التكنولوجية الحديثة ، فقد حددت المواد 303 مكرر إلى 303 مكرر3 الجرائم التي تقع على حرمة الحياة الخاصة و هي : جريمة إلتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بدون إذن صاحبها.

تعديل قانون الإجراءات الجزائية(): مواكبة للتطور الرقمي الحاصل في المجتمع ، أقر المشرع الجزائري جملة من الإجراءات الخاصة بالإعراض على المراسلات ، التفتيش ، تسجيل الأصوات و التقاط الصور، حيث نصت المواد 65 مكرر5 إلى المادة65 مكرر10 على أمكانية اللجوء للإعتراض على المراسلات ، التقاط الصور و تسجيل الأصوات و ذلك لمقتضيات التحري و التحقيق في جرائم المخدرات الجريمة العابرة للحدود و الجرائم الماسة بانظمة المعالجة الآلية للمعطيات ، مع مراعاة ، طبعا، كتمان السر المهني ، تحرير محضر من طرف الضابط المحقق ، حيث يمكن لوكيل الجمهورية أن يأذن ب:

-إعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية و اللاسلكية.

-وضع الترتيبات التقنية-دون موافقة المعنيين-من أجل التقاط ، تثبيت، بث ، تسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص واحد أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

و في نفس السياق، اقر المشرع إجراءات توقيف النظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، حيث تنص المادة 51 من قانون الإجراءات الجزائية المعدل على "إذا رأى ضابط الشرطة القضائية ، لمقتضيات التحقيق ، أن يوقف للنظر شخصا لاو أكثر ، أشير إليهم في المادة 50، فعليه أن يطلع فورا وكيل الجمهورية المختص بذلك مع إعداد تقرير عن دواعي التوقيف للنظر.

كما قد يخضع التوقيف للنظر للتمديد مرة واحدة- بإذن من وكيل الجمهورية ، إذا كانت موضوع الجرائم متعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.

قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام و الإتصال:

المراقبة الالكترونية(): تضمن هذا القانون أحكام جديدة متعلقة بكيفيات معالجة الجريمة الإلكترونية و مستلزمات التحريات و التحقيقات القضائية ، حيث تطرقت المادة الثالثة من قانون 09-04 لتدابير الوقاية من الجرائم الإلكترونية و المتمثلة في:

-المراقبة الالكترونية: تتمثل حالات المراقبة الإلكترونية بموجب المادة 4 من قانون 09-04 في :

-الوقاية من الأفعال الموصوفة بجرائم الإرهاب ، التخريب أو الجرائم الماسة بأمن الدولة .

-عند توفر معلومات مفادها احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام ، الدفاع الوطني، مؤسسات الدولة أو الاقتصاد الوطني.
-إذا كان من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية لما تقتضيه التحريات و التحقيقات الجارية.
-في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.
-التفتيش: يعد من أدق الصلاحيات الممنوحة للمحقق، و ذلك على حساب الحريات الفردية المكفولة دستوريا و عليه ، فقد أحاطها المشرع بضوابط متعلقة بالسلطة التي تأذن بمباشرة التفتيش ، السلطة التي تقوم بالتفتيش و لأحوال التي يجوز فيها التفتيش.
أشارت المادة 3 من قانون 09-04 أنه لمقتضيات حماية النظام العام و لمستلزمات التحريات ن يمكن وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية و القيام بإجراءات التفتيش و الحجز داخل المنظومة المعلومايه.
و تنص المادة 05 من قانون 09-04 على أنه يجوز للسلطات القضائية و ضباط الشرطة القضائية و في الحالات المنصوص عليها في المادة4 من قانون09-04 الدخول بغرض التفتيش و لو عن بعد في حالتين:
الحالة الأولى: تفتيش منظومة معلوماتية أو جزء منها أو معطيات معلوماتية مخزنة فيها .
الحالة الثانية: تفتيش منظومة تخزين معلوماتية.
كما منح المشرع الجزائري للسلطات المكلفة بالتفتيش إمكانية لإستنجاد بأي شخص له دراية بعمل المنظومة المعلوماتية محل البحث
الحجز: يعني الحجز وضع اليد على شيء مرتبط بجريمة تمت ، و يتم الحجز بموجب المادة6 و المادة7 من قانون09-04 في حالتين:
الحالة الأولى: حجز المعطيات المعلوماتية: يمكن للسلطة التي تباشر التفتيش في منظومة معلوماتية حجز المعطيات المخزنة التي تكون مفيدة في الكشف عن الجرائم أو مرتكبيها و ليس ضروريا حجز كل المنظومة و ذلك من خلال نسخ المعطيات محل البحث .
و الجدير بالملاحظة في هذا السياق ، أوجب المشرع على ذات السلطة السهر على سلامة المعطيات في المنظومة المعلوماتية مجيزا في ذلك استعمال كل الوسائل البتقنية الضرورية من أجل تشكيل أو إعادة تشكيل المعطيات المتحصل عليها قصد جعلها قابلة للإستغلال لغرض التحقيق من دون المساس-طبعا-بمحتوى المعطيات.
الحالة الثانية: الحجز عن طريق منع الوصول إلى المعطيات: إذا استحال حجز المعطيات المعلوماتية لأسباب تقنية ، فإنه، حسب المادة7 ، يتعين على السلطة التي تقوم بالتفتيش بإستعمال التقنيات المناسبة لمنع الوصول إلى المعطيات المتضمنة في المنظومة المعلوماتية أو نسخها ، كما يمكن منع لإطلاع على المعطيات المحجوزة التي يشكل محتواها جريمة بموجب المادة8 ، عن طريق تكليف شخص مؤهل و بإستعمال الوسائل التقنية المناسبة لذلك.
القوانين الموالية لقانون09-04 ذات الصلة بالجرائم الإلكترونية: تماشيا مع التطور الحاصل على مستوى التقنيات الإلكترونية و تطبيقات التواصل المختلفة و قصد وضع حد للإنتشار الرهيب لجرائم انتهاك المراسلات ، المساس بالحريات العامة ، القذف، التشهير،الإبتزاز المالي و لإحتيال بإستخدام لأساليب التقنية ، فقد أقر المشرع الجزائري:
قانون رقم 18-04 المحدد للقواعد العامة المتعلقة بالبريد و الإتصالات الإلكترونية() لقد تم تجريم –بوجب قانون 18-04 لاسيما المواد 164-188 منه المرسلات المرسلة عن طريق الإتصالات الإلكترونية أو إفشاء مضمونها أو نشرها أو إستعمالها دون ترخيص من المرسل أو المرسل إليه، كما تجرم كل محاولة لفتح أو تخريب للبريد الإلكتروني للأشخاص الطبيعيين أو المعنويين أو المساعدة على هذه الجريمة.

و في نفس السياق ، يكون المقصود بالاتصالات –حسب المادة10 من قانون18-04 :"كل إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطسية."

قانون18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي(): يكون المقصود بمعالجة المعطيات ذات الطابع الشخصي-بموجب قانون18-07 :"كل عملية أو مجموعة عمليات منجزة بطرق أو وسائل آلية أو بدونها على معطيات ذات طابع شخصي مثل: الجمع، التسجيل ، التنظيم، الحفظ ، الملاءمة، التغيير، الإطلاع، الإستخراج، الإستعمال، الإيصال عن طريق النشر او الإرسال او أي شكل من اشكال الإتاحة أو التقريب او الربط البيني وكذا الإغلاق أو التشفير أو المسح أو الإتلاف".

و قد سن المشرع الجزائري مجموعة من الآليات و الضوابط تتمثل في:

استحداث سلطة وطنية لحماية المعطيات ذات الطابع الشخصي مكلفة بضمان عدم انطواء استعمال تكنولوجيات الإعلام و الاتصال على أية اخطار تجاه حقوق الأشخاص و الحريات العامة و الخاصة و أن كل محاولة الاعتداء على المعطيات ذات الطابع الشخصي تكون بإقرار عقوبة مالية و أخرى سالبة للحرية مع إمكانية مصادرة محل الجريمة(الفصل الثالث من قانون 18-07 لاسيما المواد من 54الى 74).

قانون 08-01 المتعلق بالتأمينات الإجتماعية(): لم يكتف المشرع الجزائري بمحاصرة الجرائم الإلكترونية المتعلقة بإفشاء أسرار و محتويات المراسلات و إتلاف المعطيات ذات الطابع الشخصي أو الإطلاع عليها ، بل عالج الجريمة الإلكترونية التي تطال الهيئات الوطنية كالضمان الاجتماعي، إذ تطرق قانون 08-01 للعقوبات التي تخص البطاقة الإلكترونية للشفاء و التي تسلم للمؤمن اجتماعيا بسبب العلاج ، فوردت العقوبات –وفق المادة 93 مكرر2 و المادة 93 مكرر3-كما يلي:

- تسليم او أستلام بهدف الإستعمال غير المشروع أو القيام عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية.

-إعداد أو تعديل أو نسخ بطريقة غير شرعية للبرمجيات التي تسمح بالوصول أو استعمال للمعطيات المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمهني الصحة.

توضح التشريعات القانونية السابقة إرادة المشرع في محاربة الجريمة الإلكترونية باستخدام الأدوات التقنية فكل معالجة آلية للمعطيات ، تخالف التشريع الوطني ، تكون عقوبتها سلب الحرية لمرتكبها مع إقرار مخالفة مالية ، كل ذلك من أجل حماية المجتمع من إخطار الإلكترونية المتزايدة و التي باتت تفرضها نزوع الإنسان نحو الرقمنة .

ب-الجوانب التقنية: إن الانتشار اللافت للجريمة الإلكترونية و اتصافها بصعوبة تحديد هوية المستخدم و زوال الحواجز الجغرافية في الفضاء السيبراني ، جعل من الضروري على الدول الاستنجاد بأحدث التكنولوجيا من أجل إفشال الاعتداءات الإجرامية على الساكنة من خلال تزويد القائمين على عملية التأمين بما يلي:

-تنمية و تعزيز و تأهيل القدرات البشرية المكلفة بعمليات التحقيق في الجرائم الإلكترونية.

-توفير المعدات التكنولوجية المتقدمة و الدقيقة المرتبطة بالإعلام الآلي و الاتصالات.

-إنشاء قاعدة بيانات واسعة و محينة بإستمرار.

-القدرة على تصميم البرامج المعلوماتية و تطويرها.

ج-المؤسسات العملياتية : عمدت الجزائر و بغية تنفيذ سياسة سيبرانية فعالة ، على إنجاز مجموعة من المؤسسات العلمية و العملياتية ، تقوم بمسؤولية الحماية و كشف مختلف أنواع الجرائم ، و في مقدمة تلك الجرائم ما تعلق بالتهديدات السيبرانية .

المؤسسات العلمية لتحقيق الأمن السيبراني:

تحقيقا لمتطلبات الأمن السيبراني و خلق بيئة أمنية آمنة ، و في مخرجات اجتماع لمجلس الوزراء للدولة الجزائرية بتاريخ 12 سبتمبر2023م تم استحداث مدرسة وطنية عليا للامن السيبراني بالتنسيق مع وزارة الدفاع الوطني ، لضمان توحيد الجهود و مضاعفة الفعالية في هذا المجال الحساس من أجل تحصين الأمن الوطني القومي.

المؤسسات التنفيذية لتحقيق الأمن السيبراني: تتمثل في :

مؤسسات ذات الوصاية الأمنية: يندرج تحتها ما يلي:

مصلحة الدفاع السيبراني و مراقبة أمن الأنظمة: تم استحداثها بتاريخ 11-06-2015، تابعة لدائرة الإستعمال و التحضير لأركان الجيش الوطني الشعبي، تضطلع بمهمة حماية المنظومات الحيوية للبلاد ضد كل أنواع الجريمة الإلكترونية.

من بين أهم أهدافها:

-اعتماد التكوين التقني و العلمي لإنتاج الكفاءات و المهارات القادرة على خلق دفاع سيبراني يشمل كافة أنشطة المؤسسة العسكرية لتفادي الأخطار الإجرامية.

-غرس ثقافة "الإستعمال كيفي لتكنولوجيات الإعلام و الإتصالé من خلال حملات تحسيسية لكافة مستخدمي المؤسسة.

-الإعتماد بطريقة مستمرة على البحث العلمي لتطوير وسائل الدفاع استجابة للتطورات الحاصلة في مجال التكنولوجيا.

مركز الوقاية من جرائم الإعلام الآلي و الجرائم الإلكترونية التابعة للدرك الوطني: هو جهاز تابع لسلاح الدرك الوطني ، يتواجد ببؤ مرادرايس ، أنشئ في 2008 و يعد الجهاز الوحيد المختص في جرائم الإعلام الآلي و الجريمة المعلوماتية.

يقوم المركز بالمهام التالية:

-تحليل معطيات و بيانات الجرائم المعلوماتية المرتكبة و تحديد هوية أصحابها .

-تأمين الأنظمة المعلوماتية و الحفاظ عليها لاسيما تلك التابعة للمؤسسات الرسمية و البنوك.

-تقديم المساعدة الأمنية للأجهزة الأخرى في مجال محاربة الجريمة الإلكترونية.

و طبقا لإحصائيات متعلقة بالجرائم الإلكترونية في الجزائر ، يمكن التاكيد على إنتقال الجريمة إلى العالم الإفتراضي ، حيث سجلت قيادة الدرك الوطني ما مجموعه 1362 جريمة سيبرانية تورط فيها 1028 شخص خلال 2020م .

و الجدير بالملاحظة ، و طبقا لتحليل معطيات الجريمة الإلكترونية : تحتل جرائم القذف و السب الصدارة عبر الفضاء السيبراني بنسبة55%يليها جرائم ضد الأمن العمومي ثم الأعمال الماسة بالحياة الخاصة و إفشاء الأسرار و أخيرا الابتزاز و الاحتيال و الإستغلال الجنسي و الأفعال المخالفة للاداب العامة.

و في سياق التعاون الدولي ، أحبطت" شركة كسبرسكي "kasparsky"،"المختصة في محاربة الجريمة السيبرانية 95000 هجمة إلكترونية كانت موجهة ضد الجزائر.

المعهد الوطني للأدلة الجنائية و علم الإجرام التابع للدرك الوطني: هي مؤسسة عمومية ذات طابع إداري ، تعمل تحت الوصاية المباشرة لوزير الدفاع الوطني.

يضم المعهد العديد من الأقسام و المعاهد ، أهمها:

أ-مصلحة الإعلام الآلي: تعد مصلحة أساسية بالنظر لجمل المهام الموكلة لها و هي :

رصد و تتبع و مراقبة عملية لإختراق و القرصنة المعلوماتية .

-اكتشاف المعلومات المسروقة.

-تفكيك البرامج المعلوماتية.

ب-مصلحة البصمات: يتم على مستوى هذه المصلحة التعرف على الجثث ، مع العلم أن سلاح الدرك الوطني مجهز بنظام التعرف الآلي على البصمات.(the automated fingerprint identification system)

ج-مصلحة الوثائق : يتم التأكد في هذه المصلحة من :

-صحة الإمضاءات .

-التحقق من النقود المزورة و الوثائق السرية.

د-مصلحة البيئة: تبحث هذه المصلحة في أسباب تلوث المياه و التربة و الكشف عن المواد السامة المتواجدة في المحيط وة أماكن العمل.

ه-قسم التحليل الدقيق: و هو قسم مجهز بأحدث وسائل المسح الإلكتروني و يقوم بمقارنة المعطيات الدقيقة التي يتم العثور عليها في مسرح الجريمة.

و-قسم السيارات: أين يتم التعرف على السيارات ذات الترقيم المزور من خلال تتبع عملية تغيير او تحريف الأرقام التسلسلية للمركبة.

وبوجود المصالح الحيوية للمعهد ، فإنه يضطلع بالمهام التالية:

أ-المشاركة في تحديد سياسة جنائية مثلى لمكافحة الإجرام.

ب-إجراء الخبرات و الفحوصات الأولية في إطار التحريات بهدف التعرف على مرتكبي الجرائم و الجنح.

ج-المبادرة باجراء بحوث تطبيقية متعلقة بالإجرام عن طريق اللجوء إى التكنولوجيا الدقيقة.

د-العمل على ترقية البحوث التطبيقية ذات العلاقة بالتهديدات السيبرانية.

كما يحتوي المعهد على : قسم الحرائق و الإنفجارات ، قسم الطب الشرعي ، قسم علم الإنسان و الأسنان الشرعيين ، قسم علم البواعث المؤدية للموت ، مصلحة بصمة الأصبع، مصلحة الإشارة و مصلحة الإلكترونيك ، كما يضم المركز زمرة من المهندسين و التقنيين من ذوي الخبرة و التجربة للتصدي لكافة أنواع الجريمة و تهديداتها.

المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني: تماشيا مع استفحال الجريمة الإلكترونية و إستجابة لمطلب تحقيق مستلزمات الأمن السيبراني ، قامت المديرية العامة للأمن الوطني بإستحداث المصلحة المركزية لجريمة الإلكترونية التي عمدت منذ إنشائها على تدريب التشكيل الأمني على مهارات ردع كل محاولات الإختراق أو التجسس أو غيرها من الأفعال الإجرامية ، فتم في 2011 بتشكيل النواة الأمنية الأولى لمحاربة الجريمة و بقرار من المدير العام للامن الوطني ، في 2015، تم إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال().

نيابة مديرية الشرطة العلمية و التقنية التابعة للمديرية العامة للأمن الوطني: أوكلت المديرية العامة للأمن الوطني مهمة محاربة الجريمة الإلكترونية لنيابة مديرية الشرطة العلمية و القنية مزودة إياها بالوحدات التالية:

-المخبر المركزي للشرطة العلمية، مقره ابن عكنون –الجزائر العاصمة.

-المخبر الجهوي للشرطة العلمية ، مقره قسنطينة.

-المخبر الجهوي للشرطة العلمية ، مقره وهران .

يتولى كل مخبر(مركزي-جهوي) مهام البحث و التحقيق و التحري بشأن الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ، عن طريق

الدائرة العلمية: تقوم بمهام البحث و التحقيق و تحليل الأدلة المتصلة بالمجال البيولوجي ، الكيميائي و الطب الشرعي و تلك المتعلقة بالتسمم ، الحرائق و المتفجرات.

الدائرة التقنية: تتولى مهام البحث و تحليل الأدلة الناتجة عن الجرائم المتصلة بإستعمال الأسلحة و القذائف إضافة لمعالجة الجرائم المعلوماتية.

و في سياق اخر ، و فضلا عن الدوريات الروتينية للمراقبة الفيزيائية للأفراد و المركبات قصد ضمان السكينة و الأمن العام في المجتمع ن تقوم الشرطة في مجال التصدي للجريمة الإلكترونية بالمهام التالية:

تنشيط عمل خلايا اليقظة الإلكترونية من خلال رصد اي تصرف مشبوه.

تتبع الأثر الإلكتروني/التوعية و التحسيس.

العمل على تجفيف مصادر التمويل و التجنيد عبر الفضاء السيبراني.

تقوم المديرية العامة للأمن الوطني بمساعي حثيثة داخل الوطن و خارجه لشل كل محاولات تنفيذ السلوك الإجرامي ، حيث تم إنشاء فرق متخصصة عبر58 مقر أمن ولائي، تتمحور مهامها في:

استقبال شكاوي المواطنين في مجال الجرائم المرتكبة في الفضاء السيبراني .

البحث و التحري في الجرائم المعلوماتية تحت إشراف السلطات القضائية.

توعية و تحسيس المواطنين بمخاطر الانترنيت خاصة على الأطفال.

و في مجال تعقب الجريمة الإلكترونية خارج الحدود و في إطار التعاون الدولي للجزائر في المجال السيبراني كانت الجزائر من الدول التي انضمت سريعا للمنظمة الدولية للشرطة الجنائية و تعد عضو مؤسس للمنظمة الإفريقية للشرطة الجنائية مما يدل على تصميم قيادة جهاز الشرطة على محاربة كل ما يهدد السلامة الترابية من تهديدات تقليدية و مستحدثة.

مؤسسات ذات وصاية مدنية: إنطلاقا من كون عملية محاربة الجريمة الإلكترونية ليست مسؤولية المؤسسات الأمنية وحدها ، قامت السلطات العليا الجزائرية بإنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها.

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها: تشكلت هذه الهيئة بمقتضى المرسوم الرئاسي رقم 15-261 المؤرخ في 8 اكتوبر 2015 و هي سلطة إدارية مستقلة تابعة لوزير العدل .

تضم أعضاء من الحكومة ممن تتقاطع مهامهم بتكنولوجيا الإعلام و الإتصال . إضافة لمسؤولي مصالح الأمن المختلفة و قاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

و يتواجد أيضا ضمن أعضاء الهيئة : قضاة ن ضباط و أعوان من الشرطة القضائية تابعين لمختلف المصالح و الهيئات العسكرية و المدنية في الدولة و ذلك وفقا لأحكام قانون الإجراءات الجزائية.

مهام الهيئة: تساهم الهيئة في :

اقتراح الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال.

تنشيط و تنسيق عمليات الوقاية منها.

تقديم المساعدة للسلطات القضائية و مصالح الشرطة القضائية في مجال مكافحة الجرائم الإلكترونية.

ضمان المراقبة الوقائية للإتصالات الإلكترونية.

القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال: أنشئ بموجب الأمر رقم 11/21 المؤرخ في 25 أوت 2021 المعدل و المتمم لقانون الإجراءات الجزائية ، يتواجد على مستوى مجلس قضاء العاصمة.

يعرف –بداية -الأمر رقم 11/21 الجريمة المتصلة بتكنولوجيات الإعلام و الاتصال كونها أي جريمة ترتكب أو يسهل ارتكابها باستعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية او أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيا الإعلام و الإتصال.

يقوم هذا القطب الجزائي بمهمتين أساسيتين:

-المتابعة و التحقيق في الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال.

الحكم في الجرائم المنصوص عليها في الباب السادس من الأمر 11/21 إذا كانت تشكل جنحا.

و قد فصلت المادة211مكرر24 في الجرائم المتعلقة بتكنولوجيات الإعلام و الإتصال و الجرائم المرتبطة بها و التي يتعين على السادة:

وكيل الجمهورية لدى القطب

قاضي التحقيق

رئيس القطب

المختصين حصريا بالمتابعة و التحقيق و الحكم فيها ، إذا كانت الجرائم تمثل:

الجرائم التي تمس أمن الدولة و الدفاع الوطني.

جرائم نشر و تحرير اخبار كاذبة بين الجمهور من شأنها المساس بالأمن و السكينة العامة و استقرار المجتمع.

جرائم نشر و ترويج أخبار مغرضة تمس بالنظام و الأمن العموميين.

جرائم الإتجار بالأشخاص ، لأعضاء البشرية و تهريب المهاجرين.

جرائم التميز و خطاب الكراهية (الأمر11/21 ص8).

لقد أصدرت العديد من الوزارات على غرار وزارة الداخلية ،البريد ، الإتصال ، التعليم العالي ، المالية تعليمات لمصالها التقنية ، تتضمن الكيفيات العملية الواجب إتخاذها لتفادي أي تسريب سيبراني ، و تتمثل هذه الكيفيات في :

-عدم السماح لآي كان من الحصول على معلومات من الأنظمة المعلوماية الموصولة بشبكة الأنترنيت ، ما لم يكن هناك موافقة من المصلحة المؤهلة قانونا ، كما لا يمكن إستخدام الحسابات الخاصة بالأفراد أو لأرقامهم السرية.

-احترام المقاييس المعمول بها أثناء تداول المعلومات المشفرة –أرسالا و استقبالا.

الخاتمة:

نستنتج مما سبق أن الهندسة لأمنية السيبرانية الجزائرية تقوم على العناصر التالية:

-استفحال ظاهرة الجريمة الإلكترونية بعد انتشار الأدوات التكنولوجية المختلفة من حواسيب و حواسيب ذكية و هواتف ذكية ووصل مسار التكنولوجيا إلى إنتاج أدوات إلكترونية متناهية الدقة و تقوم بتخزين أو إرسال أحجام كبيرة من المحتويات و البيانات و المعلومات.

-ظهور محتويات رقمية تتخذ من الأدوات التكنولوجية وسيلة لتسهيل حياة البشرية ، فمضامينها تختلف ما بين الاقتصادي المرتبط بالتمويل البنكي و تسديد الأقساط و معرفة سعر السعر و غيرها و منها ما هو اجتماعي-تثقيفي يهدف لنشر الوعي و المعرفة بين مكونات المجتمع المختلفة.

-انخراط الإنسان في الفضاء السيبراني مكونا بيئة افتراضية و التي أصبحت نواة التعامل و التفاعل ، فصار أكثر بهذه البيئة (الإنسان الرقمي) إلى درجة الانصهار في العالم الافتراضي.

- يمكن التأكيد أن البيئة الإفتراضية لا تخلو من تهديدات سسيبرانية تستهدف البنى التحتية للدول و تحاول تخريبها أو إتلافها ، فحروب الجيل الخامس تتخذ من هذه البيئة مسرحا لها و أن الحواسيب ما هي إلا أسلحة للمعارك المستقلية و بياناتها هي اهداف للقراصنة و العملاء و حتى الدول.

-تفرض البيئة السيبرانية جملة من التحديات تواجه من خلالها الدول و الشركات و حتى الأفراد اختراقات و عليه ، يكون من الضروري تحيين ادوات التصدي و المجابهة لكل هجوم سيبراني.

-تعمل الجزائر من خلال جملة من اجراءات الأمن السيبراني على التصدي لكل انواع الهجومات ، حيث تم ارساء نصوص قانونية ردعية ضد من يعدل أو يعطل أو يغش في أنظمة المعلومات الوطنية ، كما تمتلك منظومة تنفيذية لابطال كل محاولات الإختراق ن فهما أبدى هؤلاء القراصنة تفوقا تكنولوجيا ، إن السياسة الأمنية الجزائرية تظل بالمرصاد لكل محاولتهم و بارمجهم السيبرانية التي لن تصمد أمام اصرار و عزيمة العقول الأمنية الجزائرية.

قائمة المراجع:

1-الكتب:

- عبد الفتاح بيومي، حجازي، مكافحة جرائم الكمبيوتر و الإنترنيت في القانون العربي النموذجي (القاهرة: دار الفكر الجامعي ، 2006).

-مجمع البحوث و الدراسات لأكاديمية السلطان قابوس لعلوم الشرطة ، الجريمة الإلكترونية في المجتمع الخليجي و كيفية مواجهتها (الرياض: أكاديمية نايف للعلوم الأمنية ، 2016).

2-المجلات:

بارة ، سمير ، الأمن السيبراني في الجزائر: السياسات و المؤسسات ، المجلة الجزائرية للأمن الإنساني ، العدد الرابع ، جويلية2017.

دراعو ، عزالدين،الآثار الإقتصادية و المالية للهجمات السيبرانية في ظل بالتحول الرقمي : النتائج ، التجارب و الحلول –مع الإشارة لحالة الجزائر-مجلة التكامل الإقتصادي، المجلد10 ، العدد02، جوان2022.

ربيعي ، حسين ، سمر محمود ، الحروب السيبرانية: المخاطر و استراتيجيات تحقيق الأمن السيبراني الدولي و الداخلي ، المجلد الجزائرية للأمن الإنساني، المجلد 07، العدد02 ، السنة السابعة ، جويلية2022.

منى عبد الله ، السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود ، مجلة كلية التربية،العدد111، جويلية2020.

)) بن مرزوق، عنترة، الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية ،مجلة العلوم الإجتماعية ، المجلد 19، العدد01،

اسلام، فوزي، الأمن السيبراني:الأبعاد الاجتماعية و القانونية: تحليل سوسيولوجي ، المجلة الإجتماعية القومية، المجلد السادس و الخمسون ، العدد الثاني ، مايو2019.

فايزة أحمد الحسيني، مجاهد ، الوعي بالأمن السيبراني ترف أم ضرورة في عصر المعلوماتية ، مجلة بحث و تربية، المجلد 13، العدد 02، ديسمبر2023.

حسين قوادرة ، منى كحلوش ، التداعيات الاقتصادية لحرب المعلومات السيبرانية ، مجلة الناقد للدراسات السياسية ، المجلد 05، العدد 01 ، 2021.

شريفة كلاع ، الأمن السيبراني و تحديات الجوسسة و الاختراقات الإلكترونية للدول عبر الفضاء السيبراني ، مجلة الحقوق والعلوم الإنسانية ، المجلد15 ،العدد01، 2002.

مهدي، رضا، الجرائم السيبرانية و آليات مكافحتها في التشريع الجزائري ، مجلة إيليزا للبحوث و الدراسات ، المجلد06 ، العدد02 ، 2021.

أميرة عبد العظيم محمد ، عبد الجواد، المخاطر السيبرانية و سبل مواجهتها في القانون العام ، مجلة الشريعة و القانون ، ج3 ، العدد 35، 2020.

شويرب جيلالي ، محروب السيبرانية و الأمن السيبراني ، مجلة الحقوق و الحريات ، المجلد11 ، العدد01، 2023 ص 167.

سميحة بلقاسم و حميد بوشوشة، الجريمة الإلكترونية بعد جديد للإجرام في الجزائر .....واقعها و آليات مجابهتها، مجلة العلوم الإنسانية لجامعة أم البواقي ، المجلد1 ، العدد1 ، جوان

اسماعيل ، زروقة ، الفضاء السيبراني و التحول في مفاهيم القوة و الصراع، مجلة العلوم القانونية و السياسية ، المجلد 10، العدد01، أفريل 2019،

3-محاضرات:

بوازدية ، جمال ، الأمن السيبراني محاضرات مقدمة لطلبة السنة الثانية ماستر (تخصص: دراسات إستراتيجية و أمنية)(الجزائر: كلية العلوم السياسية و العلاقات الدولية، 2021).

Books in forein languges

.2010The International Telecommunication nion(int) , Tool kit for cybercrime ligeslation, Geneva,

الإدارة الرقمية وتحديات لأمن السيبراني

Digital management and cybersecurity challenges

ط.د/ دراويــش الطـــيب جامعة عبد الحميد بن باديس - مستغانم♦ tayeb.draouich.etu@univ-mosta.dz

أ.د/ لقرع بن علي جامعة عبد الحميد بن باديس - مستغانم♦

الملخص : يعتبر لأمن السيبراني الدرع الرقمي الذي يحمي عالمنا المربوط بشبكات الانترنت ،وفي ظل عصر تكنولوجيا المعلومات حيث تتداخل نشاطاتنا الإدارية مع الشبكة العنكبوتية، يصبح لأمن السيبراني أمرا ضروريا للحفاظ على خصوصياتنا وبياناتنا.

ويشمل لامن السيبراني مجموعة من السياسات والتقنيات التي تسعى للوقاية من الهجمات وحماية الانظمة الرقمية والمحافظة عليها ووضع حد ضد التهديدات السيبرانية المتزايدة عن طريق برامج مكافحة الفيروسات ،وجدران الحماية ،وتحديثات البرمجيات.

ويعد تحقيق التوازن بين التقدم التكنولوجي والحفاظ على لأمن المعلوماتي تحديا يتطلب تبني وتطوير إستراتيجيات فعالة لحماية البيانات والمعلومات،حيث يلعب لامن السيبراني في هذا العالم الرقمي المعقد دورا حيويا في حماية معلوماتنا الشخصية،وضمان إستمرارية النشاط الإداري الرقمي بعد تبني الإدارة الرقمية.

Abstract: Cybersecurity is considered the digital shield that protects our world connected to Internet networks. In light of the age of information technology, where our administrative activities overlap with the Internet, cybersecurity becomes necessary to preserve our privacy and data.

Cybersecurity includes a set of policies and technologies that seek to prevent attacks, protect and preserve digital systems, and put an end to increasing cyber threats through anti-virus programs, firewalls, and software updates.

Achieving a balance between technological progress and maintaining information security is a challenge that requires adopting and developing effective strategies to protect data and information. In this complex digital world, cybersecurity

plays a vital role in protecting our personal information and ensuring the continuity of digital administrative activity after adopting digital management.

الكلمات المفتاحية: 1/ لأمن السيبراني 2/ الجريمة الالكترونية 3/ التحول الرقمي 4/ البيانات الرقمية الالكترونية 5/الإدارة الرقمية .

مقدمة :

لقد شهد العصر الحالي في ظل التقدم التكنولوجي والتحول الرقمي التوجه نحو الرقمنة في كافة المجالات، حيث أصبحت لإدارة الرقمية أمرا لاغنى عنه في كافة المجالات،ومع إنتشار إستخدام الانترنت والشبكات الحاسوبية زادت التحديات التي تواجه الإدارة الرقمية ومن أبرزها التهديدات السيبرانية ،إذ يتعين على المؤسسات والمنظمات الإهتمام بالأمن السيبراني وحماية بياناتها وأنظمتها الرقمية من الهجمات الإلكترونية والتجسس ولإختراقات لقواعد البيانات وضرورة إيجاد سبل بديلة لحمايتها من كل تهديد.فقد أثارت قضية "بيغاسوس" الرأي العام العالمي حول ضرورة إيجاد سبل للحماية من التجسسات ولإختراقات التي تشكل تهديدا لأمن الدول.

ويسعى لأمن السيبراني إلى حماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية وحماية الأنظمة التقنية والمعلومات وأنظمة التقنيات التشغيلية ،ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات وما تحتويه من بيانات من أي إختراق أو تعطيل أوتعديل أو دخول أو إستخدام أو إستغلال غير مشروع لمختلف البيانات والأنظمة والشبكات.

وعلى هذا لأساس فإن لإشكال المطروح هنا هو:

*** مامدى نجاعة لأمن السيبراني في حماية معلومات وبيانات لإدارة الرقمية؟**

ولإجابة على هذه لإشكالية في هذه الورقة البحثية نعتمد على الخطة الآتية:

المحور الاول:ماهية لامن السيبراني والإدارة الرقمية

المحور الثاني:مظاهر التهديدات السيبرانية على لإدارة الرقمية

المحور الثالث:آليات حماية لإدارة الرقمية سيبرانيا

المحور الأول: ماهية لامن السيبراني والإدارة الرقمية

1-مفهوم لأمن السيبراني : لامن السيبراني هو ممارسه الدفاع عن اجهزه الكمبيوتر ولاجهزه المحموله و لانظمه الالكترونيه المعلوماتية والبيانات و الهجمات الخبيثه كما يرد بمعنى امن الشبكات ولانظمه المعلوماتيه والبيانات والمعلومات ولاجهزه المتصله بالانترنت فهو المجال الذي يتعلق باجراءات ومعايير الحمايه المفروض اتخاذها والالتزام بها ومواجهه التهديدات لمنع الهجمات أو على الاقل الحد من آثارها.

ويعرف لأمن السيبراني بالإنجليزية: (Cyber Security) بأنه توظيف التقنيات، والعمليات، والتدابير اللازمة لضمان أمن الأنظمة، والشبكات، والبرامج، ولأجهزة، والبيانات وحمايتها من الهجمات الإلكترونية، ويتمثل الغرض الرئيسي منه في تقليل المخاطر الإلكترونية التي قد تتعرض لها الأنظمة والشبكات وحمايتها من لاستغلال غير المصرح به.

وقد عرفته وزاره الدفاع لامريكي بينطاجون انه لإجراءات التنظيمية التي تؤمن الحماية الكافيه للمعلومات بجميع انواعها واشكالها سواء كانت الكترونيه او ماديه من مختلف المخاطر والهجمات والجرائم وافعال التخريب والتجسس والحوادث بينما ادرج لاعلان لاوروبي لامن السيبرياني بمعنى قدرة النظام المعلوماتي على مقاومة محاولات لاختراق أو الحوادث غير المتوقعه التي تستهدف البيانات[1] .وهناك من عرف لامن السيبرياني كادوارد اموريس الذي قدم لامن السيبرياني انه الوسائل التي من شانها الحد من خطر الهجوم على البرمجيات و اجهزه الحاسوب و الوسائل المستخدمه في مواجهه القرصنه وكشف الفيروسات حيث جزم بالجداره المطلقه لاجهزه لامن السبرياني في ردع الجريمه المعلوماتيه إلا ان الوسائل المسخره لحمايه المعلومات ولامن السيبراني ليس بالضروره انها تقوم دائما بردع الجرائم الالكترونيه وإنما قد تعمل على الحد منها والحمايه من وقوعها.

آ-أهمية لأمن السيبراني :

لأمن السيبراني هو مجموعة من الممارسات ولإجراءات التي تهدف إلى حماية المعلومات والأنظمة الإلكترونية من الهجمات الرقمية.ويعد لأمن السيبراني أمرا بالغ الأهمية للمؤسسات والأفراد من جميع الأحجام، حيث يمكن أن تؤدي الهجمات السيبرانية إلى خسائر مالية كبيرة، وانتهاك الخصوصية، وحتى تعطل لأعمال .

ومن بين أهمية لأمن السيبراني نذكر مايلي:

- حماية البيانات الحساسة :تمتلك المؤسسات والأفراد مجموعة واسعة من البيانات الحساسة، مثل بيانات العملاء، والبيانات المالية، وبيانات الملكية الفكرية. ويعد لأمن السيبراني أمرا أساسيا لحماية هذه البيانات من السرقة أو التلاعب.
- منع تعطل لأعمال :يمكن أن تؤدي الهجمات السيبرانية إلى تعطل لأعمال، مما قد يؤدي إلى خسائر مالية كبيرة. يمكن أن يشمل تعطل لأعمال فقدان الوصول إلى البيانات أو الأنظمة، أو فقدان القدرة على تقديم الخدمات.
- حماية الخصوصية :يمكن أن تؤدي الهجمات السيبرانية إلى انتهاك الخصوصية، مما قد يؤدي إلى الكشف عن معلومات شخصية حساسة. يمكن أن يشمل ذلك أرقام الهواتف، وعناوين البريد الإلكتروني، وأرقام بطاقات الائتمان، وغيرها من المعلومات.[2]
- لامتثال التنظيمي :تتطلب العديد من القوانين واللوائح من المؤسسات والأفراد اتخاذ تدابير أمنية للحماية من الهجمات السيبرانية. يمكن أن يؤدي عدم لامتثال إلى فرض غرامات أو عقوبات أخرى.

تستمر أهمية لأمن السيبراني في النمو، حيث تصبح الأنظمة والشبكات الإلكترونية أكثر تعقيدا.ويرجع ذلك جزئيا إلى زيادة اعتماد المؤسسات والأفراد على التكنولوجيا، وجزئيا إلى التطور المستمر للتهديدات السيبرانية.من المهم أن نكونو على دراية بالتهديدات السيبرانية وأن نتخذ خطوات لحماية معلوماتنا وبياناتنا،كما أنه يحمي بيانات المستخدمين من الهجمات الإلكترونية الرامية إلى سرقة المعلومات واستخدامها لإحداث ضرر، فقد تكون هذه بيانات حساسة، أو معلومات حكومية وصناعية، أو معلومات شخصية.

---

[1]–الشوي صلاح الدين،الأمن السيبراني كمرتكز جديد في الإستراتيجية العراقية قضايا سياسية ،السنة الثانية عشر ،2020،ص 62.

[2]–عدنان السيد سوزان،إنتهاك حرمة الحياة الخاصة عبر الأنترنت،مجلة جامعة دمشق للعلوم الإقتصادية(29،3،2013)

إن وجود برامج ووسائل دفاع إلكتروني متقدمة لحماية البيانات أمر مهم، إذ إن المجتمع بحاجة إلى حماية البنية التحتية الحيوية التي تشمل المستشفيات، ومؤسسات الرعاية الصحية الأخرى، وبرامج الخدمات المالية، ومحطات الطاقة. "[1]

ب-أبعاد الأمن السيبراني :

يمكن تقسيم الأمن السيبراني إلى ثلاثة أبعاد رئيسية:

البعد التقني: يركز هذا البعد على حماية الأنظمة والشبكات الإلكترونية من الهجمات. ويشمل ذلك إجراءات مثل تأمين أجهزة الكمبيوتر والأجهزة المحمولة، وتحديث البرامج ونظام التشغيل بانتظام، واستخدام برامج مكافحة الفيروسات ومكافحة البرامج الضارة.

البعد البشري: يركز هذا البعد على حماية البيانات من خلال رفع مستوى الوعي لدى المستخدمين حول التهديدات السيبرانية وكيفية حماية أنفسهم. ويشمل ذلك تعليم المستخدمين كيفية إنشاء كلمات مرور قوية، وعدم فتح الروابط أو المرفقات المشبوهة، وتحديث برامجهم بانتظام.

البعد التنظيمي: يركز هذا البعد على إنشاء إطار تنظيمي يدعم الأمن السيبراني. ويشمل ذلك وضع سياسات وإجراءات أمنية، وإجراء تدريبات أمنية للموظفين، وتطوير خطط استجابة للأزمات.

ج-مظاهر الأمن السيبراني :

تنقسم مظاهر الأمن السيبراني إلى فئتين رئيسيتين:

مظاهر إيجابية: تسعى إلى حماية الأنظمة والشبكات الإلكترونية من الهجمات. وتشمل هذه المظاهر:

إجراءات أمنية تقنية: مثل تأمين أجهزة الكمبيوتر والشبكات، وتحديث البرامج ونظام التشغيل بانتظام، واستخدام برامج مكافحة الفيروسات ومكافحة البرامج الضارة.

إجراءات أمنية بشرية: مثل رفع مستوى الوعي لدى المستخدمين حول التهديدات السيبرانية وكيفية حماية أنفسهم.

إجراءات أمنية تنظيمية: مثل وضع سياسات وإجراءات أمنية، وإجراء تدريبات أمنية للموظفين، وتطوير خطط استجابة للأزمات[2].

مظاهر سلبية: تسعى إلى إلحاق الضرر بالأنظمة والشبكات الإلكترونية. وتشمل هذه المظاهر:

هجمات التصيد الاحتيالي: هي رسائل بريد إلكتروني أو مواقع ويب مزيفة مصممة لخداع المستخدمين للكشف عن معلومات حساسة مثل كلمات المرور أو معلومات بطاقة الائتمان.

البرمجيات الخبيثة: هي برامج مصممة لإلحاق الضرر بجهاز كمبيوتر أو نظام. يمكن أن تتضمن الفيروسات، والديدان، وأحصنة طروادة، وغيرها من البرامج الضارة.

هجمات رفض الخدمة: هي محاولات لجعل نظام أو موقع ويب غير متاح للمستخدمين. يمكن أن تتحقق عن طريق إغراق النظام بحركة مرور غير مرغوب فيها.

هجمات القرصنة: هي محاولات الوصول غير المصرح به إلى نظام أو بيانات. يمكن أن تتحقق عن طريق استخدام كلمات مرور مكسورة أو نقاط ضعف في البرامج.

2-مفهوم الإدارة الرقمية:

---

[1]–بارة سمير،الأمن السيبراني في الجزائر :السياسات والمؤسسات،المجلة الجزائرية للأمن الإنساني(2017،2)

[2]– بارة سمير،مرجع سابق.

يعتبر مصطلح الاداره الالكترونيه من المصطلحات العلميه الحديثه فهو مصطلح مشتق من اللغه الانجليزيه MANAGEMENT وتعرف بانها القيام بجمع المعلومات التي تنجز داخل الادارات وتعتمد على تكنولوجيا المعلومات حيث تتم بشكل الكتروني بدءا بالمراسلات وصولا لتكامل نظم المعلومات بحيث تصبح كل المهام والنشاطات تنجز باستخدام تكنولوجيا المعلومات والاتصال ، فالاداره الالكترونيه هي استخدام تكنولوجيا المعلومات وخاصه تطبيقات الانترنت لدعم وتعزيز حصول المواطنين على الخدمات التي تقدمها مختلف الادارات العامه ،اضافه الى تقديم الخدمه لمختلف القطاعات والدوائر الحكوميه بشفافيه وكفاءه عاليه[1] فالاداره الالكترونيه هي المرافق العامه التي تقدم خدماتها الاتصال وتكنولوجيات لاعلام الالي من مواقع الكترونيه وتطبيقات ذكيه ورقمنه المعلومات لوضع قواعد بيانات يمكن استخدامها من طرف المنتسبين للمرافق المعنيه وكذا المواطنين الذين يملكون صلاحيه الوصول لجزء محدد او لكل المعلومات كما تعتمد لاداره الالكترونيه على العمل الدائم والمستمر وامكانيه الولوج للمرتفقين للمعلومات والخدمات على مدار الساعه .

المحور الثاني:مظاهر التهديدات السيبرانية على الإدارة الرقمية

1_أسباب إنتشار التهديدات السيبرانية على الإدارة الرقمية:

_ إعتماد الإدارات على التكنولوجيا:فقد اصبحت مختلف الإدارات والمنظمات تعتمد بشكل كبير على التكنولوجيا مما يجعلها أكثر عرضة للهجمات السيبرانية

_ تطور تقنيات القرصنة:أصبحت تقنيات القرصنة اكثر تطورا ،مما يجعل من الصعب على المؤسسات الدغاع ضدها

_ نقص الوعي لأمني:فلا يدرك العديد من الأشخاص المخاطر السيبرانية، مما يجعلهم أكثر عرضة للوقوع كضحايا للهجمات السيبرانية

2_مظاهر التهديدات السيبرانية على الإدارة الرقمية:

تتمثل مظاهر التهديدات السيبرانية على لإدارة الرقمية في مجموعة من لإجراءات التي تستهدف الأنظمة والشبكات الإلكترونية، والتي يمكن أن تؤدي إلى تعطيل لأعمال، أو فقدان البيانات، أو انتهاك الخصوصية، أو إلحاق الضرر المادي.

وتتمثل هذه المظاهر في الآتي:

- هجمات التصيد لاحتيالي:وهي رسائل بريد إلكتروني أو مواقع ويب مزيفة مصممة لخداع المستخدمين للكشف عن معلومات حساسة مثل كلمات المرور أو معلومات بطاقة لائتمان.
- البرمجيات الخبيثة:وهي برامج مصممة لإلحاق الضرر بجهاز كمبيوتر أو نظام. يمكن أن تتضمن الفيروسات، والديدان، وأحصنة طروادة، وغيرها من البرامج الضارة.
- هجمات رفض الخدمة:وهي محاولات لجعل نظام أو موقع ويب غير متاح للمستخدمين. يمكن أن تتحقق عن طريق إغراق النظام بحركة مرور غير مرغوب فيها.

---

[1]–محمد الهامل عبد الفتاح وهشام بن ورزق،الإدارة الإلكترونية وتحسين الخدمة العمومية في الجزائر،مجلة البحوث العلمية في التشريعات البيئية،2021 جامعة بن خلدون تيارت ص 250.

- هجمات القرصنة:وهي محاولات الوصول غير المصرح به إلى نظام أو بيانات. يمكن أن تتحقق عن طريق استخدام كلمات مرور مكسورة أو نقاط ضعف في البرامج.

وفيما يلي شرح مفصل لهذه المظاهر:

هجمات التصيد الاحتيالي: تعد هجمات التصيد الاحتيالي من أكثر التهديدات السيبرانية شيوعا، حيث تستهدف المستخدمين بشكل مباشر.وتتمثل هذه الهجمات في إرسال رسائل بريد إلكتروني أو إنشاء مواقع ويب مزيفة تشبه إلى حد كبير مواقع الويب الرسمية، وذلك بهدف خداع المستخدمين لإدخال معلومات حساسة مثل كلمات المرور أو معلومات بطاقة الائتمان.

البرمجيات الخبيثة: تعد البرمجيات الخبيثة أيضا من التهديدات السيبرانية الشائعة، حيث يمكن أن تلحق الضرر بالأنظمة والشبكات الإلكترونية.وتتمثل هذه البرامج في مجموعة من البرامج الضارة التي يمكن أن تؤدي إلى تعطل لأعمال، أو فقدان البيانات، أو انتهاك الخصوصية، أو إلحاق الضرر المادي.

هجمات رفض الخدمة: تهدف هجمات رفض الخدمة إلى جعل نظام أو موقع ويب غير متاح للمستخدمين. وتتحقق هذه الهجمات عن طريق إغراق النظام بحركة مرور غير مرغوب فيها، مما يؤدي إلى تعطل النظام أو موقع الويب[1].

هجمات القرصنة:تهدف هجمات القرصنة إلى الوصول غير المصرح به إلى نظام أو بيانات.وتتحقق هذه الهجمات عن طريق استخدام كلمات مرور مكسورة أو نقاط ضعف في البرامج.

3-أثر التهديدات السيبرانية على الإدارة الرقمية

يمكن أن تؤثر التهديدات السيبرانية على الإدارة الرقمية في مجموعة من المجالات، بما في ذلك:

- تعطيل لأعمال: يمكن أن تؤدي الهجمات السيبرانية إلى تعطيل لأعمال، مما قد يؤدي إلى خسارة الأرباح، أو فقدان الثقة من العملاء.
- فقدان البيانات: يمكن أن تؤدي الهجمات السيبرانية إلى فقدان البيانات، مما قد يؤدي إلى خسائر مالية كبيرة، أو انتهاك الخصوصية.
- انتهاك الخصوصية: يمكن أن تؤدي الهجمات السيبرانية إلى انتهاك الخصوصية، مما قد يؤدي إلى فقدان الثقة من العملاء، أو حتى إلى عقوبات قانونية.
- الضرر المادي: يمكن أن تؤدي الهجمات السيبرانية إلى إتلاف المعدات أو البرامج، مما قد يؤدي إلى تعطل لأعمال أو حتى إصابة الأشخاص.

[1]- بارة سمير،الأمن السيبراني في الجزاءر :السياسات والمؤسسات،المجلة الجزائرية للأمن الإنساني(2017،2)

4-كيفية حماية الإدارة الرقمية من التهديدات السيبرانية

يمكن حماية الإدارة الرقمية من التهديدات السيبرانية من خلال مجموعة من الإجراءات، بما في ذلك:

- تثقيف المستخدمين حول التهديدات السيبرانية وكيفية حماية أنفسهم.
- تطبيق إجراءات أمنية قوية على الأنظمة والشبكات الإلكترونية.
- تحديث البرامج ونظام التشغيل بانتظام.
- استخدام برامج مكافحة الفيروسات ومكافحة البرامج الضارة.
- إجراء تدريبات أمنية للموظفين.
- تطوير خطط استجابة للأزمات[1].

وتعد هذه الإجراءات مهمة لضمان أمن وسلامة الأنظمة والشبكات الإلكترونية، وحماية البيانات والمعلومات الحساسة من التهديدات السيبرانية.

المحور الثالث: آليات حماية الإدارة الرقمية سيبرانيا

مع تزايد اعتماد المؤسسات على التكنولوجيا الرقمية، تزداد أيضا المخاطر السيبرانية التي تواجهها. يمكن أن تؤدي الهجمات السيبرانية إلى سرقة البيانات أو تعطيل الأنظمة أو نشر البرامج الضارة. يمكن أن يكون لهذه الهجمات آثار مدمرة على المؤسسات، بما في ذلك الخسائر المالية والاضطراب التشغيلي والضرر بسمعة المؤسسة.

هناك عدد من الآليات التي يمكن للمؤسسات استخدامها لحماية نفسها من التهديدات السيبرانية. تتضمن هذه الآليات ما يلي:

- إدارة المخاطر: يجب على المؤسسات إجراء تقييم للمخاطر السيبرانية لتحديد نقاط الضعف المحتملة في أنظمتها. يمكن أن يساعد ذلك المؤسسات في تحديد المخاطر التي يجب أن تركز عليها في جهود الحماية الخاصة بها.
- السياسة والإجراءات: يجب على المؤسسات وضع سياسات وإجراءات أمنية صارمة لتوجيه سلوك الموظفين وحماية البيانات والموارد[2].
- تقنيات الأمن: يجب على المؤسسات استخدام تقنيات الأمن المناسبة، مثل جدران الحماية وبرامج مكافحة الفيروسات وأنظمة اكتشاف التسلل، لحماية أنظمتها من الهجمات.
- الوعي الأمني: يجب على المؤسسات تدريب الموظفين على الأمن السيبراني لزيادة الوعي بالتهديدات السيبرانية وكيفية حماية البيانات والموارد.

إدارة المخاطر: تتضمن إدارة المخاطر السيبرانية في تحديد التهديدات المحتملة وتقييم مدى خطورتها. يمكن أن يساعد ذلك المؤسسات في تحديد المخاطر التي يجب أن تركز عليها في جهود الحماية الخاصة بها.

---

[1]–لطرش فيروز،بن عزوز حاتم ،الجريمة الإلكترونية في الجزائر من جريمة فردية إلى جريمة منظمة ،مجلة آفاق للعلوم

[2]–بن مرزوق عنترة،البعد الإلكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب،مجلة العلوم الإنسانية والإجتماعية جوان 2018

هناك عدد من الخطوات التي يمكن للمؤسسات اتخاذها لإدارة المخاطر السيبرانية، بما في ذلك :

- تحديد لأصول: يجب على المؤسسات تحديد لأصول الرقمية التي تحتاج إلى الحماية. يمكن أن تشمل هذه لأصول البيانات والمعلومات الحساسة والأنظمة والشبكات.
- تحديد التهديدات: يجب على المؤسسات تحديد التهديدات المحتملة التي يمكن أن تتعرض لها أصولهم. يمكن أن تشمل هذه التهديدات الهجمات الإلكترونية والكوارث الطبيعية ولأحداث البشرية.
- تقييم المخاطر: يجب على المؤسسات تقييم مدى خطورة كل تهديد محتمل. يمكن أن يساعد ذلك المؤسسات في تحديد المخاطر التي يجب أن تركز عليها في جهود الحماية الخاصة بها.

السياسة ولإجراءات: يجب على المؤسسات وضع سياسات وإجراءات أمنية صارمة لتوجيه سلوك الموظفين وحماية البيانات والموارد. يجب أن تتضمن هذه السياسات ولإجراءات ما يلي:

- ضوابط الوصول: يجب على المؤسسات وضع ضوابط وصول صارمة لتحديد من يمكنه الوصول إلى البيانات والموارد.
- النسخ لاحتياطي: يجب على المؤسسات إنشاء نسخ احتياطية من البيانات والموارد الحساسة للحماية من فقدان البيانات.
- إدارة الحسابات: يجب على المؤسسات إدارة حسابات المستخدمين وكلمة المرور بعناية لتقليل خطر إساءة لاستخدام.
- التحديثات لأمنية: يجب على المؤسسات تحديث برامج لأمان بانتظام لإصلاح الثغرات لأمنية.[1]

تقنيات لأمن: يجب على المؤسسات استخدام تقنيات لأمن المناسبة لحماية أنظمتها من الهجمات. تشمل بعض تقنيات لأمن الشائعة ما يلي:

- جدران الحماية: تمنع جدران الحماية الوصول غير المصرح به إلى الأنظمة والشبكات.
- برامج مكافحة الفيروسات: تحمي برامج مكافحة الفيروسات الأنظمة من البرامج الضارة، مثل الفيروسات والبرامج الترويجي.
- أنظمة اكتشاف التسلل: تكشف أنظمة اكتشاف التسلل عن الأنشطة المشبوهة على الأنظمة.

الوعي لأمني: يجب على المؤسسات تدريب الموظفين على لأمن السيبراني لزيادة الوعي بالتهديدات السيبرانية وكيفية حماية البيانات والموارد. يمكن أن يساعد التدريب الموظفين على اتخاذ خطوات للحماية من الهجمات، مثل استخدام كلمات مرور قوية وتجنب فتح رسائل البريد الإلكتروني المشبوهة.

[1] – بن مرزوق عنترة،البعد الإلكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب،مرجع سابق

من المهم أن تأخذ المؤسسات التهديدات السيبرانية على محمل الجد وأن تتخذ الخطوات اللازمة للحد من المخاطر. يمكن أن تساعد الآليات المذكورة أعلاه المؤسسات في حماية نفسها من التهديدات السيبرانية والحفاظ على أمن بياناتها ومواردها.

الآليات القانونية لحماية الإدارة الرقمية في الجزائر : تتمثل الآليات القانونية لحماية الإدارة الرقمية في الجزائر في مجموعة من القواعد القانونية التي تهدف إلى حماية الإدارة الرقمية من مختلف المخاطر التي تهددها، سواء كانت مخاطر تقنية أو قانونية أو تنظيمية[1].

وتشمل هذه الآليات ما يلي:

- القوانين والتشريعات ذات الصلة: حيث تقوم الدولة الجزائرية بسن القوانين والتشريعات التي تنظم الإدارة الرقمية، وتحميها من المخاطر المختلفة.ومن أهم هذه القوانين والتشريعات:
  - قانون رقم 18-04 المؤرخ في 20 رمضان عام 1439 الموافق لـ 25 يوليو سنة 2018، يتعلق بالتوقيع الإلكتروني.
  - قانون رقم 18-05 المؤرخ في 20 رمضان عام 1439 الموافق لـ 25 يوليو سنة 2018، يتعلق بالتجارة الإلكترونية.
  - قانون رقم 18-06 المؤرخ في 20 رمضان عام 1439 الموافق لـ 25 يوليو سنة 2018، يتعلق بالجريمة الإلكترونية.
- النصوص التنظيمية: حيث تقوم الدولة الجزائرية بإصدار النصوص التنظيمية التي تطبق القوانين والتشريعات ذات الصلة، وتوضح كيفية تطبيقها.ومن أهم هذه النصوص التنظيمية:
  - المرسوم التنفيذي رقم 19-221 المؤرخ في 27 جمادى الأولى عام 1441 الموافق لـ 14 أغسطس سنة 2019، يحدد شروط وإجراءات استخدام التوقيع الإلكتروني في المعاملات الإدارية.
  - المرسوم التنفيذي رقم 19-222 المؤرخ في 27 جمادى الأولى عام 1441 الموافق لـ 14 أغسطس سنة 2019، يحدد شروط وإجراءات ممارسة التجارة الإلكترونية.
  - المرسوم التنفيذي رقم 19-223 المؤرخ في 27 جمادى الأولى عام 1441 الموافق لـ 14 أغسطس سنة 2019، يحدد شروط وإجراءات مكافحة الجريمة الإلكترونية.
- الإجراءات الإدارية والتنظيمية: حيث تقوم الإدارة الجزائرية باتخاذ مجموعة من الإجراءات الإدارية والتنظيمية التي تهدف إلى حماية الإدارة الرقمية، ومن أهم هذه الإجراءات:
  - إنشاء مراكز مختصة في أمن المعلومات وحماية البيانات.
  - تدريب العاملين في الإدارة على كيفية استخدام الإدارة الرقمية بأمان.
  - وضع سياسات وإجراءات أمنية صارمة لحماية البيانات والمعلومات الحساسة.

ويمكن القول أن الآليات القانونية لحماية الإدارة الرقمية في الجزائر، تمثل خطوة مهمة في سبيل تعزيز أمن المعلومات وحماية البيانات والمعلومات الحساسة في الإدارة.وتهدف هذه الآليات إلى خلق بيئة آمنة لاستخدام الإدارة الرقمية، وضمان استمرارية سير العمليات الإدارية.

[1]–قارة آمال،الحماية الجزائية للمعلوماتية في التشريع الجزائري،الجزائر،دار هومة،2007

خاتمة

يعد لأمن السيبراني من أهم العوامل التي تساهم في حماية الإدارة الإلكترونية من التهديدات السيبرانية. يمكن أن يساعد لأمن السيبراني المؤسسات في حماية بياناتها ومواردها من السرقة أو التلف أو التشويه.

هناك عدد من الآليات التي يمكن للمؤسسات استخدامها لحماية نفسها من التهديدات السيبرانية. تتضمن هذه الآليات ما يلي:

إدارة المخاطر: يجب على المؤسسات إجراء تقييم للمخاطر السيبرانية لتحديد نقاط الضعف المحتملة في أنظمتها.

السياسة ولإجراءات: يجب على المؤسسات وضع سياسات وإجراءات أمنية صارمة لتوجيه سلوك الموظفين وحماية البيانات والموارد.

تقنيات لأمن: يجب على المؤسسات استخدام تقنيات لأمن المناسبة، مثل جدران الحماية وبرامج مكافحة الفيروسات وأنظمة اكتشاف التسلل، لحماية أنظمتها من الهجمات.

الوعي لأمني: يجب على المؤسسات تدريب الموظفين على لأمن السيبراني لزيادة الوعي بالتهديدات السيبرانية وكيفية حماية البيانات والموارد.

من المهم أن تأخذ المؤسسات التهديدات السيبرانية على محمل الجد وأن تتخذ الخطوات اللازمة للحد من المخاطر. يمكن أن تساعد الآليات المذكورة أعلاه المؤسسات في حماية نفسها من التهديدات السيبرانية والحفاظ على أمن بياناتها ومواردها.

وفي الختام، يمكن القول أن لأمن السيبراني هو العمود الفقري لحماية لإدارة الإلكترونية. من خلال وضع آليات لأمن السيبراني المناسبة، يمكن للمؤسسات حماية بياناتها ومواردها من التهديدات السيبرانية والحفاظ على استمرارية أعمالها.

وفيما يلي بعض التوصيات لتعزيز الآليات القانونية لحماية لإدارة الرقمية في الجزائر:

- ضرورة تحديث القوانين والتشريعات ذات الصلة، بما يتوافق مع التطورات التقنية والقانونية الحديثة.
- ضرورة تفعيل دور المؤسسات المختصة في أمن المعلومات وحماية البيانات، وتوفير لإمكانيات اللازمة لها للقيام بمهامها.
- ضرورة زيادة الوعي لدى العاملين في لإدارة بأهمية أمن المعلومات وحماية البيانات، وكيفية استخدام لإدارة الرقمية بأمان.

قائمة المراجع:

1- الشمري صلاح الدين،لأمن السيبراني كمرتكز جديد في لإستراتيجية العراقية قضايا سياسية ،السنة الثانية عشر ،2020.
2- محمد الهامل عبد الفتاح وهشام بن ورزق،لإدارة الإلكترونية وتخسين الخدمة العمومية في الجزائر،مجلة البحوث العلمية في التشريعات البيئية،2021 جامعة بن خلدون تيارت
3- عدنان السيد سوزان،إنتهاك حرمة الحياة الخاصة عبر الأنترنت،مجلة جامعة دمشق للعلوم الإقتصادية(2013،3،29)
4- بارة سمير،لأمن السيبراني في الجزاءر:السياسات والمؤسسات،المجلة الجزائرية للأمن الإنساني(2017،2)
5- بن مرزوق عنترة،البعد الإلكتروني للسياسة لأمنية الجزائرية في مكافحة لإرهاب،مجلة العلوم الإنسانية ولإجتماعية،جوان 2018
6- قارة آمال،الحماية الجزائية للمعلوماتية في التشريع الجزائري،الجزائر،دار هومة،2007
7- لطرش فيروز،بن عزوز حاتم،الجريمة الإلكترونية في الجزائر من جريمة فردية إلى جريمة منظمة،مجلة آفاق للعلوم

الحروب السيبرانية في العلاقات الدولية: دراسة في المفهوم، التطور والتأثير.

Cyber Warfare in International Relations: A Study in Concept, Evolution, and Impact".

موسى بن قاصير(*) جامعة صالح بوبنيدر قسنطينة3 moussa.benkacir@univ-constantine3.dz.

ملخص:

تعالج هذه الورقة البحثية موضوع الحرب السيبرانية في العلاقات الدولية ،انطلاقا من البحث في مفهومها والأشكال التي تتخذها هذه الأخيرة ،بالإضافة اللي فواعلها .إذ أصبحت الحروب السيبرانية والتي تحدث عبر الفضاء الإلكتروني من بين اهم المواضيع التي يشتغل عليها باحثوا العلاقات الدولية ،حيث أضحت الدول بمختلف أشكالها ترسم استراتيجيات وتكتيكات لمواجهة مختلف الأخطار والتهديدات التي يمكن أن تتعرض لها عبر شن دول وجماعات هجومات على بينيتها التحتية ومؤسساتها ،خاصة وان الحروب السيبرانية تؤثر على سيادة الدولة وامنها وامن أفرادها ومصالحها القومية .انطلاقا من هذه النظرة نحاول البحث في مختلف الأثار التي يمكن أن تتركها الحروب السيبرانية على الدول في العلاقات الدولية وتفاعلاتها .

الكلمات المفتاحية: الحرب السيبرانية، هجمات سيبرانية، العلاقات الدولية، الأمن.

Abstract:

This research paper addresses the topic of cyber warfare in international relations, starting from an examination of its concept and the various forms it takes, in addition to its actors. Cyber warfare, occurring through cyberspace, has become one of the most important topics studied by international relations researchers. States, in their various forms, have begun to devise strategies and tactics to confront the various dangers and threats that they may face through cyber-attacks on their infrastructure and institutions. Especially considering that, cyber warfare affects the sovereignty, security, and national interests of states and their individuals. From this perspective, we attempt to explore the various impacts that cyber warfare may leave on states in international relations and their interactions.

KeyWords: cyber warfare. Cyber-attacks. International relations. Security .

مقدمة:

أصبح من الواضح بحلول منتصف العقد الأول من القرن 21أن "الفضاء السيبراني" الذي تم إنشاؤه عبر شبكة الإنترنت له تأثيرات هائلة في الديناميكيات والأنماط الأوسع للسياسة الدولية، وبات مفهوم السياسة السيبرانية يشكل أحد مجالات البحث الأكاديمي، متجاوزا الضجيج لتحليل محتوى النقاش السياسي على شبكة الإنترنت ومعرفة كيفية استخدامها وتبعاتها على كثير من القضايا والبنى التحتية لمختلف دول العالم القائم على تكنولوجيا تقنية المعلومات وتقنية الاتصالات، في كافة المجالات الصناعية والعسكرية والأمنية والطاقة والمياه والصحة ومنظومة النقل وقطاع البنوك والمؤسسات المالية والحكومية، حتى أضحى الطيف السيبراني جزءا لا يتجزأ من الأمن القومي، ودخل في تغيير شكل الحروب وتقنياتها وأساليبها بسبب تغير طبيعة تهديداته وإلحاق الضرر بالمؤسسات والمراكز الحيوية والإستراتيجية للدول.مع تحول الفضاء الإلكتروني إلى ساحة للتفاعلات الدولية، برز العديد من الأنماط التوظيفية له، سواء على صعيد الاستخدامات ذات الطبيعة المدنية أو العسكرية، الأمر الذي جعل هذا الفضاء مجالا للصراعات المختلفة، سواء للفاعلين من الدول أو غير الدول لحيازة أكبر قدر من النفوذ والتأثير السيبراني.

في هذا السياق، تبلورت ظاهرة "الحروب السيبرانية "،"Cyber wars"التي اتسمت بخصائص مختلفة عن نظيراتها التقليدية، من حيث طبيعة الأنشطة العدائية، والفواعل، والتأثيرات في بنية الأمن العالمي.وعبرت تلك الحرب عن نمطين من القوة (الناعمة والصلبة) في عملية توظيف التفاعلات في الفضاء الإلكتروني، مما يعكس تنامي القدرات والتهديدات المتصاعدة لأمن البنية التحتية الكونية للمعلومات. سنحاول في هده الورقة البحثية معالجة إشكالية رئيسية مفادها: كيف اثرت الحرب السيبرانية على تفاعلات العلاقات الدولية؟ ما انعكاسات هده الحرب على مفهوم الصراع الدولي؟ والقوة، والامن؟

المحور الأول: الحرب السيبرانية مقاربة في المفهوم والنظرية.

قدمت العديد من التعريفات للحرب السيبرانية كل حسب توجهاته الفكرية، بالإضافة الى العديد من التفسيرات النظرية في إطار نظرية العلاقات الدولية، وهو ما سنستعرضه في المحور الأول من الورقة البحثية.

أولا-- في اللغة:

كلمة سايبر (Cyber) يونانية الأصل وترجع إلى مصطلح "Kybernetes" الذي ورد بداية في مؤلفات الخيال العلمي، ويعني القيادة أو التحكم عن بعد.

والسيبرانية في قاموس "المورد" هي علم الضبط، ومصدرها (Cyberntics) وهو مصدر يتطابق مع مفهوم الهجمات السيبرانية أي ضبط الأشياء عن بعد والسيطرة عليها.

وأول من استخدم مصطلح السيبرانية هو عالم الرياضيات "نوربرت وينر"Norbert Wiener ، وذلك في العام 1948 في أثناء دراسته موضوع القيادة والسيطرة والاتصال في عالم الحيوان، فضلا عن عالم الهندسة الميكانيكية.

من الناحية الاصطلاحية قدمت العديد من التعاريف للحرب السيبرانية، كل حسب الزاوية التي يعتقد أنها شاملة أو مناسبة لفهم الحرب السيبرانية في علاقات الوحدات السياسية مع بعضها البعض، حسب نيلز وميلزر، فإن الحرب السيبرانية هي تلك التي تجري في الفضاء السيبراني من خلال الوسائل والأساليب الإلكترونية، ويرى أنه في الوقت الذي يشير فيه مصطلح "الحرب" بشكل عام إلى الأعمال العدائية العسكرية في حالات النزاع المسلح فإن

الفضاء السيبراني يأخذ بعدا آخر يشير إلى شبكة مترابطة عالميا من المعلومات الرقمية والبنى التحتية للاتصالات وأنظمة الكمبيوتر والمعلومات المتوفرة بداخلها، ومنه حسبه فإن إصابة شبكة كمبيوتر تابعة لأحد الخصوم ببرمجيات خبيثة، تشكل عملا من أعمال الحرب الإلكترونية في حين أن القصف الجوي بناء على أمر عسكري إلكتروني لا يمثل عملا من أعمال الحرب السيبرانية.

تعرف أيضا على أنها قيام دولة أو فواعل من غير الدول بشن هجوم إلكتروني، يمثل أعمالا عدائية إلكترونية تستهدف البنية التحتية المعلوماتية للدول لتحقيق أغراض متداخلة سياسية، اقتصادية، وإجرامية وغيرها.

ورغم ذيوع مصطلح "الحرب السيبرانية" من الناحية الإعلامية فإنه يعد مصطلحا قديما كان بالأساس محصورا في رصد عمليات التشويش على نظم الاتصال والرادار، وأجهزة الإنذار، بينما الواقع الراهن في الفضاء الإلكتروني أصبح يشمل شبكات الاتصال والمعلومات والبنية التحتية لكافة لخدمات والمؤسسات المدنية والعسكرية، في العصر الحديث باتت هذه الهجمات تشكل تهديدا مباشرا لأمن الدول خاصة بعد تزايد مستوى اعتماد الدول على نظم المعلومات المعتمدة على الفضاء الإلكتروني وهو ما يطلق عليه تسمية البنى التحتية القومية للمعلومات.

كما يعاني أيضا مفهوم الحرب السيبرانية من بعض الغموض بسبب عدم وضوح الرؤية بصورة كاملة، إذ يوجد مفهومان للحرب السيبرانية "Cyber war fare" و "Cyber war"

وفي محاولة للتمييز بينهما أجرى كل من "Andrew Colarik and Daniel Hugbes" دراسة في الخطاب السياسي والعسكري صادرة سنة 2017 بعنوان "تراثية مفهوم الحرب السيبرانية" وتوصلا إلى أنه بينما يقصد بالأولى "Cyber war" تصرف الحرب في حد ذاتها، يقصد بالثانية "Cyber war fare" الوسائل اللازمة لإدارة هذه الحرب، وكانت أولى الدراسات التي تنبأت بالحرب السيبرانية للكاتبين "جون اركويلا ."Jhon Arquilla" ودافيد رونفيلدت "David Ronfeldt" في مقال لهما منشور ام 1993 بعنوان الحرب السيبرانية قادمة، وقد عرفا الحرب السيبرانية بـ: "تنفيذ العمليات العسكرية والاستعداد لتنفيذها، وفقا للمبادئ المعلوماتية من خلال تعطيل نظم المعلومات والاتصالات على أوسع نطاق، وقام الكاتبان بتوسيع مفهوم الحرب السيبرانية لتشمل أبعاد غير غير مادية، متمثلة في تدمير العقيدة العسكرية للعدو، التي يعتمد عليها لتحديد هويته، وخططه، وتصرفاته، وأهدافه والتحديات التي يواجهها، وذلك عبر معرفة كل شيء عن العدو ومنعه في الوقت نفسه من معرفة أي شيء عن الطرف الآخر، وتحويل ميزان المعرفة ليكون في مصلحة هذا الطرف.

هناك من يعرف الحرب السيبرانية، بأنها استخدام تكنولوجيا الحاسوب في الفضاء السيبراني (الإلكتروني) لأغراض التدمير من أجل التأثير أو التفسير أو التعديل في التفاعلات الديبلوماسية والعسكرية، بين الكيانات المختلفة، وذلك بعيدا عن ساحة المعارك، وقد يأخذ هذا الصراع نمطين:

الأول: الحوادث الفردية Cyber Incidents ويقصد بها العمليات والحوادث الفردية التي تتم على فترات مختلفة، وليست مستمرة لفترة معينة.

الثاني: هو النزاعات السيبرانية Cyber Disputs والتي تدار بأدوات افتراضية بين دولتين في فترة زمنية معينة ويحتوي على واحد أو أكثر من الحوادث الفردية.

ويغطي مفهوم الحروب السيبرانية في الفضاء الإلكتروني مجموعة واسعة من الإجراءات تتراوح بين المجسمات البسيطة المستخدمة لمحو المواقع على شبكة الإنترنت، والحرمان من الخدمة، والتجسس والتدمير ويستخدم على نحو مماثل لتغطية مجموعة واسعة من السلوكيات وهو يعكس تعريفات قاموسية للحرب تتراوح بين الصراع المسلح والتسابق العدائي.

ويشير أيضا مصطلح الحرب السيبرانية إلى وسائل وأساليب القتال، التي تتألف من عمليات في الفضاء السيبراني ترقى إلى مستوى النزاع المسلح أو تجري في سياقه.

كما يشير المصطلح كما يشار إليه باللغة الإنجليزية "Cyber war fare" إلى استخدام مجموعة من الممارسات والإجراءات التي تسعى لإلحاق الخلل والعطل بالأنظمة والوسائل الإلكترونية الخاصة بالعدو، بالإضافة إلى تحقيق الحماية للذات من الاستطلاع الإلكتروني المعادي ومقاومته وتحقيق الاستقرار للنظم الإلكترونية الصديقة.

ويمكن تعريف الهجمات السيبرانية بأنها فعل يقوض وظائف وقدرات شبكة الحواسيب، بغرض قومي أو سياسي من خلال استغلال نقطة ضعف ما يمكن المهاجم من التلاعب بالنظام.

يرى الباحثون والدارسون لمسائل الفضاء الإلكتروني والحروب السيبرانية، بأنه أسهم عاملان رئيسان في نشوء الحروب السيبرانية وهما:

أولا: تغير منظور الحروب جذريا، حيث تحولت من حرب بين دول ذات سيادة إلى داخل الشعوب، وهذا من أجل التحكم في إرادات وخيارات المجتمعات.

ثانيا: بروز الصراعات ذات الأبعاد المحلية- الدولية، إذ ساعد وقوع نزاعات داخلية بعد الحرب العالمية، وذلك السياق الدولي للفضاء الإلكتروني في توفير بيئة مناسبة لدفع الفئات والقوى المهمشة في السياسة الدولية، وخلق شبكة تحالفات مؤيدة أو معارضة ذات نطاق دولي عريض، إما على أساس قيم حقوقية أو انتماءات عرفية أو دينية.

ثانيا- الحروب السيبرانية والتفسيرات النظرية في العلاقات الدولية:

مع بروز الفضاء الإلكتروني أو السيبراني كمجال لصراع الدول والقوى الكبرى، أصبحت المفاهيم التقليدية في حقل العلاقات الدولية تواجه تحديات واضحة مثل الصراع، الأمن، القوة، والسيادة والردع، ولهذا كان من الضروري أن توجه رؤية نظرية تفسيرية وتحليلية أكثر قدرة على تفسير طبيعة هذه التحولات، وهو ما سنحاول معالجته هنا في هذا الجزء من الروقة بالإشارة إلى النظرية الواقعية والليبرالية والبنائية.

حسب الطرح الواقعي الذي يركز في الأساس على الدولة ومتغير القوة بجميع أشكالها وخاصة الصلبة منها، ومنطق الفوضى الدولية التي تسبب ما يسمى بالمعضلة الأمنية، يرى أنصار هذه النظرية بأن الحرب السيبرانية تؤثر على الدولة داخليا شأنها شأن المسائل المستجدة (العولمة، القومية، الاعتماد المتبادل)، فهي تهديد للأمن القومي ولا يمكنها أن تقلل من فوضوية النظام الدولي ولا من مركزية الدولة كفاعل رئيسي.

تقدم الواقعية إطار بالتفكير في توزيع السلطة بين الجهات الفاعلة وكيفية ارتباط ذلك بالصراع والواقعية كنظرية مهتمة بالأمن القومي والسلطة تقدم لنا تفسيرا حول طبيعة الديناميكيات الخاصة بالصراع السيبراني إلا أنها في معظم الحالات غير كافية، تثير الدفاعية سؤال مثير للاهتمام حول القوة السيبرانية وحول من يمتلكها، وكيف ترتبط بالاستقرار الدولي، من حيث ما إذا كانت هذه القوة ستغير ديناميكيات القوة التقليدية، كما أنها تلفت الأنظار إلى مسألة التوازن بين الدفاع والهجوم وربما هو أوضح مثال على استخدام نظرية واقعية لشرح المجال السيبراني، كما يطرح سؤال الردع وهل الردع بمعناه الثوري يمكن أن يكون بنفس الشاكلة في سياق حقيقة الأسلحة السيبرانية ، وباعتبار أن القوة مفهوم مهم في التحليل الواقعي فإن الفضاء السيبراني أحدث تحولا كبيرا في هذا المفهوم، فإننا نجد أن الفضاء السيبراني والحرب السيبرانية عنصرين مترابطين حيث أن تعظيم القوة والاستحواذ يعزز من المصلحة القومية للدولة ولعلها قادرة على تحقيق أمنها وأمن أفرادها وهذا جوهر التحليل الواقعي في العلاقات الدولية وعملية التنظير فيها ، وكل هذه العناصر من شأنها أن تعزز من السيادة السيبرانية للدولة القومية.

بالنسبة للواقعية الجديدة فالقوة السيبرانية، هي ضابط لعناصر القوة داخليا وخارجيا، والقوة السيبرانية ي محدد من محددات التوازن الدفاعي- الهجومي للدول في ظل نظام المساعدة الذاتية وحالة الالاحقين التي تسود النظام الدولي الفوضوي، وهي أقل تكلفة إذا ما قارنها بمحددات أخرى، كما أنها مصدر من مصادر التهديد واللاأمن في علاقات الدول فيما بينها، ويمكن أن تتسبب في معضلة أمنية سيبرانية، إذ أن سيطرة دولة كبرى على مقدار كبير من مصادر الحرب السيبرانية يشكل تهديدا مباشرا للدولة الثانية التي تسعى إلى تحقيق مكاسب كبيرة أمام الدولة "أ"، وهذا يجرها إلى الدخول في سباق تسلح سيبراني يزيد من فرص وقوع هجمات متنوعة وتمس بأمنهما.

في مستوى آخر ترى النظرية الليبرالية (التعددية) أن الفضاء السيبراني يضعف من أمن وسيادة الدولة، وهذا يرجع بالأساس إلى تنوع الجهات الفاعلة الدولاتية وغير الدولاتية، والتي هي أطراف فاعلة في السياسة العالمية، وهذا يعني وجود علاقات عابرة للقومية، وبالتالي أهمية العلاقات الاقتصادية والتواصلية العابرة لحدود الدولة.

في مستوى ثالث: نجد النظرية البنائية، يرى أنصارها بأن الحقائق لاجتماعية مثل المصالح والهويات هي غير ثابتة، ويرى البنائيون بأن دراسة الصراعات السيبرانية، من منطلق أنها حرب معلومات فهي تعكس نوعا من حروب الهوية فتصبح هوية الدولة القومية مهددة من طرف هويات جديدة متصارعة في الفضاء الالكتروني، وتركز على أهمية الصور والرموز، جانب البيئة المادية، من خلال المقرب السياسات الرمزية، ويسهم هذا المقرب في توضيح تأثير اللغة والخطاب في لأمن خلال العصر الرقمي إذن الخطاب البنائي يمكن أن يسهم في فهم السياسات الرمزية في صراعات الفضاء السيبراني.

المحور الثاني: خصائص الحرب السيبرانية وفواعلها

شهد الفضاء الإلكتروني في العقود لأخيرة تزايد حجم الهجمات والتهديدات السيبرانية التي تشمل الحروب، لإرهاب، التجسس الرقمي...الخ، يمكن تصنيف الحرب السيبرانية وفق أنماط عديدة منها:

1- الحرب السيبرانية منخفضة الشدة: وهذا باستخدام الفضاء الالكتروني لصراع منخفض الحدة ويكون بلردا غير مصحوب بعمليات عسكرية تقليدية، وهي جزئية، طويلة ممتدة، وعميقة الجذور وهي عادة تتضمن (الحروب النفسية، لاختراقات المتعددة، والتجسس، حرب الأفكار...الخ)

2- الحرب السيبرانية متوسطة الشدة: يكون الصراع لسيبراني فيها بمؤلة أداة موازية لحرب تقليدية دائرة على لأرض، تتميز بحدة الصراع بين لأطراف وقد تساند بعمل عسكري، تدور هذه الحرب عن طريق اختراق المواقع الإلكترونية وتخريبها وشن حرب نفسية ضد الخصوم وغيرها.

3- الحرب السيبرانية الساخنة مرتفعة الشدة: وهي حرب سيبرانية منفردة غير مصحوبة بأعمال عسكرية تقليدية، وهي حرب يسيطر عليها البعد التكنولوجي، وتستخدم لأسلحة السيبرانية ضد منشآت العدو واللجوء إلى الروبوتات لآسية والطائرات دون طيار، مع توفر القدرة التقنية في الدفاع والهجوم الإلكتروني ولاستحواذ على القدرة الإلكترونية، ومنه نجد أن القوى الكبرى تستخدم الفضاء الإلكتروني للاستعداد للحرب المستقبلية.[1]

وعند وقوع هذه الحروب، أو التخطيط لها يجد لاستراتيجيون بأن للحرب السيبرانية أربعة أسلحة رئيسية:

[1] عبد المنعم منيب، مرجع سابق الذكر، ص ص 238-239.

تخريب ومهاجمة مواقع الإنترنت، ثانيا: الحرمان من الخدمة، ثالثا: الاقتحام الفيروسي وأخيرا عمليات التسلسل[2]، بالإضافة إلى هذه العناصر هناك مجموعة من العوامل تزيد من فرضيات وقوع حروب سيبرانية في العلاقات الدولية، من بين هذه الأسباب نذكر ما يلي:

- ارتباط لعالم بالفضاء السيبراني واستخدامه من قبل أطراف متماثلة وغير متماثلة لتحقيق أهدافها.
- في ظل العولمة فسح المجال لفواعل غير وطنية من قبل الدولة ليتصاعد دور هذه الفواعل خاصة في المجالات لاستراتيجية.
- نشوء تهديدات جديدة مرتبطة الهجمات الإلكترونية خاصة في ظل اعتماد الدول على الأنظمة الإلكترونية في جميع المجالات.
- قلة تكلفة الحرب السيبرانية مقارنة بالتقليدية، فهي تقع في أي وقت سواء سلم أم أزمة أو حرب.
- تحول الحرب السيبرانية إلى إحدى أدوات التأثير في المعلومات المستخدمة، بهدف التأثير بشكل سلبي في هذه المعلومات ونظم عملها.
- توظيف الفضاء السيبراني في تعظيم قوة الدولة لتحقيق ميزة نسبية وهذا في إطار ما يسمى لاستراتيجية السيبرانية للدول.
- أدى تصاعد لأخطار والتهديدات في الفضاء السيبراني إلى بروز تنافس بين الشركات العاملة في مجال لأمن الإلكتروني، بغرض تعزيز أسواق الإنفاق العالمي على تأمين البنى التحتية السيبرانية للدول في مواجهة شبكات الجريمة المنظمة.[3]

القضاء السيبراني لا حدود له إذ يشاركه جل الفاعلين سواء الدوليين أو غير الدوليين، وفي جميع المجالات والتطبيقات، ويبرز اختلاف جلي ما بين التهديدات التقليدية المادية والتي نستطيع التعرف عليها وحتى استشراف ما يمكن أن يشبه من نتائج، وتمثل أهم خصائص للحرب السيبرانية في الآتي:

1- الحرب السيبرانية هي حقيقة موجودة في واقع العلاقات الدولية والكثير من الدول وبخاصة الكبرى من قادرة على شن هجمات مدمرة.[4]

2- الأبعاد والأولويات للحرب السيبرانية ليست عسكرية على أرض الواقع بقدر ما هي سياسة فالهدف الرئيسي منها ليس بالهزيمة التقليدية عند سقوط أحد الخصوم، واستئراف قوته وموارده، وكسر إرادته وخاصة عنصر الدعاية والتضليل.

---

[2] سماح عبد الصبور،رجع سابق الذكر، ص ص 06-07.

[3] عبد الغفار عفيفي الدويك، مرجع سابق الذكر، ص 37.

[4] ماجد محمد الحنيطي، مرجع سابق الذكر، ص 120.

3- لا تقتصر الحرب السيبرانية على فترات المواجهة العسكرية بين الفواعل الدولية، إنما هي مرتبطة بحالتي الحرب والسلم، وهذا بعد تراجع الخطوط الفاصلة بين الحالتين، حيث لم تعد هناك حاجة لإعلان الحرب.

4- لم يعد مفهوم الشروع بالانتقام له مفعول، إذ أنه من الصعوبة بمكان تحديد الهجمات السيبرانية ذات الزخم العالي، كونها لا تترك آثارا ودلائل واضحة ملموسة وفي بعض الأحيان، قد تطلب وقتا لصدرها وفي حالات لا يمكن تتبع مصدرها.[5]

5- مرونة الانتقال ما بين الأهداف الاستراتيجية من خلال ضرب القدرات العسكرية والاقتصادية للخصم والأهداف التكتيكية كالتجسس وسرقة البيانات، وهنا يحاول "ستيف والت" أن الحرب السيبرانية تتألف من أربع قضايا جوهرية هي: إضعاف القدرات العسكرية للعدو، اختراق الشبكات لإغلاق البنية التحتية والأنشطة لإجرامية على شبكة الإنترنت، والتجسس الإلكتروني.[6]

6- يزول العامل الجغرافي في الحروب السيبرانية، بحيث يصبح أي مركز أو منشأة عرضة للاستهداف ولا يقتصر على الأرض، بل يصل التهديد إلى الفضاء عبر إرسال الفيروسات إلى الأقمار الصناعية لتعطيلها أو سرقة البيانات منها.[7]

أما فيما يتعلق بالفاعلين في مجال الحرب السيبرانية فهم يتميزون بالتعدد، إذ نجد بجانب الوحدات الدولاتية والتي تستطيع تنفيذ هجمات سيبرانيو واسعة وبوسائل جد متقدمة، هناك فاعلون من غير الدول أصبحت لهم القدرة على شن هجمات سيبرانية بفعل الخبرة التي امتلكوها بفعل الخبرة التي امتلكوها، والمقدرات التكنولوجيا التي حصلوا عليها بأدوات ذاتية أو بوسائط أخرى، وتتمثل هذه الفواعل في الآتي:

أ- الدول: تمثل الفاعل الأول والأكبر، حيث أنه في عام 2008 استطاعت حوالي 180 دولة أنه يمتلك ترسانة من الأنشطة السيبرانية، ويبدوا هذا لأمر طبيعيا، حيث أن الدولة هي الفاعل الرئيسي والأساسي في السياسة الدولية، والمؤثرة بصفة كبيرة ودائمة في مسارات وتوجهات السياسة الدولية، رغم عدم التناسب في القوة بين الدول، فهي وحدة واحدة، ووحدوية حسب الطرح الواقعي.[8]

---

[5] بافان ناكو نجم الدين، تأثير الحرب السيبرانية على رفع مستوى الصراع بين الولايات المتحدة الأمريكية وإيران، مجلة جامعة، راپرين، العدد 04، 2021، ص 311.

[6] نبيل عودة، مرجع سابق الذكر، ص 09.

[7] رولا حطيط، مرجع سابق الذكر، ص 06.

[8] تغريد صفاء، لبنى خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حمورابي، العدد 33-34، شتاء ربيع 2020، ص ص 154-155.

وحسب جوزيف ناي فإن الدول تمتلك قوة إلكترونية، وهي التي لها قدرة كبيرة على تنفيذ هجمات إلكترونية وتطوير البنية التحتية وممارسة السلطات داخل حدودها[9]، حسب المفكر زبيغنو بريجنسكي، فإنه يبدوا أن دور الدولة يتراجع كوحدة أساسية في المجتمع الدولي وفي حياة الأفراد، وهذا بسبب بزوغ فواعل جديدة من غير الدول، من قبل المؤسسات الاقتصادية والمصارف والجماعات المسلحة والإرهابية، وهذا جعلها تتجاوز المفاهيم القديمة للسياسة والدولة، وهي فواعل تستخدم الفضاء السيبراني في تحقيق أهدافها ومصالحها لاستراتيجية.[10]

ب- الفواعل غير الدولاتية:

يعرف بريان هوكينغ ومايكل سميث الفاعلين من غير الدول بأنهم جماعة أو منظمة تتمتع بالاستقلال أي بمقدار من الحرية عن السعي لتحقيق أهدافها والتمثيل أي تمثيل مؤيديها والنفوذ أي القدرة على إحداث فرق اتجاه قضية ما في سياق معين مقارنة بتأثير فاعل أثر في القضية ذاتها.[11]

يستخدم الفواعل غير الدول الفضاء السيبراني لأغراض هجومية بالأساس، وهذا الهجوم في الغالب لا يكون انفراديا، بل يتطلب التنسيق مع جهات أخرى بإمكانها تقديم الدعم والمعلومات ويمكن إجمال هذه الفواعل في التالي:

1- الشركات المتعددة الجنسيات:

تملك هذه المؤسسات إمكانيات أكبر من بعض الدول الوطنية، لكنها تفتقد إلى شرعية استخدام هذه القوة، إلا أن نقطة قوتها تتمثل في هيمنتها على خوادم الإنترنت وهو ما يمكنها من الحصول على المعلومات ولهذا تؤثر بشكل مباشر على السوق والمجتمعات.[12]

2- الأفراد: الذين يمتلكون معرفة وخبرة تقنية عالية ولهم القدرة على استخدامها، وهم غالبا ما يحققون تحت اسم أنينيموس ومن الصعب الوصول إلى هوياتهم الحقيقية.[13]

3- المنظمات لإجرامية:

---

[9] محمود علي عبد الرحمان، الفضاء الإلكتروني وأثره على مفاهيم القوة الأمن والصراع في العلاقات الدولية، مجلة كلية السياسة والاقتصاد، مجلد 16، العدد 15، جويلية 2022، ص 430.

[10] تغريد صفاء، لبنى خميس مهدي، مرجع سابق الذكر، ص 155.

[11] المرجع نفسه، ص 155.

[12] أحمد عثمان محمد، الحروب السيبرانية وأثرها في العلاقات الدولية روسيا والولايات المتحدة الأمريكية نموذجا، مجلة الجامعة العراقية، العدد 59، ص 463.

[13] عبد المنعم منيب، مرجع سابق الذكر، ص 263.

تتولى عملية القرصنة الإلكترونية وسرقة البيانات واختراق الحسابات وتمويل الأموال، كما توجد سوق سوداء على شبكة الإنترنت، حيث تمارس منها تجارة كل الممنوعات، وتقدر ملايير الدولارات سنويا.[14]

4- الجماعات والمجموعات غير الحكومية:

وهي جماعات ذات توجهات مختلفة الأهداف، ولعل أبرز هذه الفواعل التي مارست عملا سيبرانيا ذو تأثير في السياسة الدولية، هي المجموعة المعروفة باسم (ويكيليكس) والتي نشرت ملايين الوثائق السرية.[15]

5- الجماعات الإرهابية:

وهي من بين أهم وأخطر الفواعل الدولية، زاد الاهتمام بنشاطها بعد أحداث 11 سبتمبر 2001 إذ أضحت تستغل الفضاء السيبراني للتجنيد والتعبئة وجمع المعلومات حول مؤسسات تشكل هدفا لها، خاصة الأمنية والعسكرية منها.[16]

المحور الثالث: الحرب السيبرانية والصراع في العلاقات الدولية.

لقد أفضت التحولات التي حصلت في الحرب إلى الدخول في حروب إلكترونية تميزت عن طبيعة الصراع الدولي، حيث أصبح الفضاء الإلكتروني ساحة جديدة للصراع الدولي، متضمنا كل شبكات الاتصال ومصادر المعلومات التي يتم تبادلها إلكترونيا، والصراع الإلكتروني (هو حالة من التعارض في المصالح والقيم يتم تسويته عبر الفضاء الإلكتروني، واتجه الصراع الدولي حول الموارد والمصالح والقيم نحو الاعتماد على تكنولوجيا الاتصال والمعلومات فيما يعرف بصراع "عصر المعلومات"، كما أن الحرب السيبرانية أدت إلى تغير في الصراع الدولي باتساعه وزيادة الفاعلين فيه، إذ أن خاصية سهولة الولوج إليه فزاد عدد المهاجمين ومنه صارت هناك منافسة من أجل الحصول على أدوات الحماية والدفاع وتطوير القدرات الهجومية الإلكترونية يستهدف حيازة القوة والتفوق والهيمنة وزيادة التأثير على المستويين المحلي والدولي .

من التحولات التي حصلت أيضا بفعل الحروب السيبرانية تعدد أدوات الصراع وطرق الحرب فأطراف الصراع وفواعله يستخدمون كل أنواع الأسلحة المدمرة في الفضاء الإلكتروني، وكان لتلك التغيرات دورا في إعادة التفكير في حركية وديناميكية الصراع وظهور ما يسمى بعصر "القوة النسبية" الذي يعني بعجز القوة العسكرية، عن تأمين الأهداف السياسية المترتبة عليها، ضف إلى ذلك التغير في براديغم الحرب، ففي الحروب القديمة كان تدمير الخصم باحتلال أراضيه والاستيلاء على موارده، إنما في الحرب الجديدة فإنه يسعى إلى السيطرة على إرادة خيارات الخصم، ومن ثم كان الدور المحوري للسكان في هذا الشكل الجديد من الحرب سواء السكان المستهدفين أو الرأي العام في

[14] محمود علي عبد الرحمان، مرجع سابق الذكر، ص 431.
[15] عبد المنعم منيب، مرجع سابق الذكر، ص 263.
[16] أحمد عثمان محمد، مرجع سابق الذكر، ص 463.

الدولة التي تشن الحرب، أو الرأي العام الدولي والإقليمي وأصبحت الحرب تهدف إلى التدمير النفسي وممارسة الدعاية بفعل الآلة الإعلامية.

برزت فضاءات جديدة للصراع بأدوات مختلفة وأنماط جديدة تختلف عن الصراعات التقليدية وتعود أسباب اهتمام الفاعلين بهذا الفضاء كمجال لتحقيق الأهداف وإدارة الصراعات للسمات التي يتميز بها، من بينها:

- ساحة صراع افتراضية فهو ليس له ساحة جغرافية.
- زيادة الاعتمادية الإلكترونية، أي الربط الشاسع بين البنية التحتية للدولة والفضاء الإلكتروني.
- كما هي الحدود الداخلية والخارجية أي حالة التأثير الكبيرة بين ما هو داخلي وخارجي، بيئة متحركة.
- صعوبة القيام بالردع الإلكتروني يصعب وضع دود لسيادتك، ومنه يصعب القيام بالردع لأنه من ينفذ الهجمات غالبا يتنكر ومنه تصبح التهديدات مجهولة.
- غياب الشفافية الإلكترونية.

سادت الثورة التكنولوجية على تغير شكل الحرب وأدواتها وأثرت في الفاعلين بها وأسهمت في إعادة التكفير في حركية وديناميكية الصراع، وأدى هذا إلى اختلاف درجات التهديد ومصادره وطبيعته ما أدى إلى تحول المواجهة بين الجيوش إلى مواجهة بين لأمم، ما يعرف بتحويل الحرب إلى ظاهرة صناعية.

وهناك شكلان من أشكال الصراع في عصر المعلومات هما حرب الشبكات وحرب الفضاء الإلكتروني، ويشيران إلى النمط الخاص بطبيعة الصراع والتوجيه المعلومات من الشامل للمعركة وتعد من الصراعات عالية الشدة، أما حرب الشبكات فتمثل نوعا من الصراعات منخفضة الحدة، ولا يتكون الفضاء الإلكتروني فقط من شبكة عن الاتصالات، بل يتكون كذلك من المعلومات التي تشغل من خلال الشبكة.

في ظل الفوضوية وغياب السلطة الشاملة لمراقبة النظام الدولي، يمكننا القول بأننا أمام حالة أشبه بحالة الطبيعة الأولى، حيث تتسم حالة الطبيعة السيبرانية بالصراع وحالة حرب الكل ضد الكل وانتشار الفوضى.

يتوافق الوضع الراهن بالفضاء السيبراني مع حالة الخوف المسببة لأسباب الصراع لتحقيق المصلحة الخاصة، بناء على ثلاثة أسباب للصراع:

1- المنافسة من أجل مكاسب العنف هو وسيلة لتحقيق ذلك.
2- عدم الثقة، وهو ما يؤدي إلى السلوك الهجومي والاحترازي.
3- المجد والمكانة وهو مقصد للسمعة السيطرة على الآخرين.

وتتشابه حالة حرب الكل ضد الكل مع التهديدات السيبرانية والمخاطر الإلكترونية بما في ذلك الحرب الإلكترونية والصراع السيبراني، الإرهاب السيبراني، فقد أصبح الأمن السيبراني مصدر قلق رئيسي لواضعي السياسات ومحل اهتمام العلماء العلاقات الدولية بسبب نتائج الأعمال التي تتسم بواسطة الشبكة، وهي غالبا أعمال عدائية لهذا يعتبر الفضاء الإلكتروني المجال المناسب للحرب بعد الأرض، والبر والبحر والفضاء.

خاتمة

ادي اتساع علاقة الدول بالفضاء الإلكتروني، وما خلفته من حروب سيبرانية إلى جملة من المخاطر والتداعيات على تفاعلات السياسة الدولية، يمكن طرح أبرزها على النحو الآتي:

1 -تصاعد المخاطر الإلكترونية، خاصة مع قابلية المنشآت الحيوية (مدنية وعسكرية) في الدول للهجوم الإلكتروني عليها عبر وسيط وحامل للخدمات، أو شل عمل أنظمتها المعلوماتية، الأمر الذي يؤثر في وظائف تلك المنشآت.وبالتالي، فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة استراتيجية بالغة الأهمية، سواء في زمن السلم أو الحرب.

2 -تعزيز القوة وانتشارها. فمن جهة، عزز الفضاء الإلكتروني ما يسمى بـ"القوة المؤسسية" في السياسة الدولية، وهي تعني أن يكون لها دور في قوة الفاعلين، وتحقيق أهدافهم وقيمهم في ظل التنافس مع الآخرين، والإسهام في تشكل الفعل الاجتماعي في ظل المعرفة والمحددات المتاحة، والتي تؤثر في تشكيل السياسة العالمية.

من جهة أخرى، عمل الفضاء الإلكتروني على إعادة تشكيل قدرة الأطراف المؤثرة، مثل الولايات المتحدة. فبعدما كانت الأخيرة تملك ما يشبه الاحتكار لمصادر القوة، بعد انتهاء الحرب الباردة، برزت عملية انتشار القوة بين أطراف متعددة، سواء أكانت دولا، أم من غير الدول.

3 -عسكرة الفضاء الإلكتروني، وذلك سعيا لدرء تهديداته على أمن الفضاء الإلكتروني، وبرز في هذا الإطار اتجاهات، مثل التطور في مجال سياسات الدفاع والأمن الإلكتروني، وتصاعد القدرات في سباق التسلح السيبراني، وتبني سياسات دفاعية سيبرانية لدي الأجهزة

المعنية بالدفاع والأمن في الدول، وتزايد الاستثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة.

4 -إدماج الفضاء الإلكتروني ضمن الأمن القومي للدول، وذلك عبر تحديث الجيوش، وتدشين وحدات متخصصة في الحروب الإلكترونية، وإقامة هيئات وطنية للأمن والدفاع الإلكتروني، والقيام بالتدريب، وإجراء المناورات لتعزيز الدفاعات الإلكترونية، والعمل على تعزيز التعاون الدولي في مجالات تأمين الفضاء الإلكتروني، والقيام بمشروعات وطنية للأمن الإلكتروني.

5 -الاستعداد لحروب المستقبل، حيث تبني العديد من الدول استراتيجية حرب المعلومات بحسبانها حربا للمستقبل، والتي يتم خوضها بهدف التشتيت، وإثارة الاضطرابات في عملية ول صناعة القرار لدي الخصوم، عبر اختراق أنظمتهم، واستخدام ونقل معلوماتهم. وهنا، ترى الدكتورة أن من يحدد مصير تلك المعركة المستقبلية ليس من يملك القوة فقط، وإنما القادر على شل القوة، والتشويش على المعلومات.

6 -تحديث القدرات الدفاعية والهجومية، حيث سعت الدول إلى تحديث النشاط الدفاعي لمواجهة مخاطر الحرب السيبرانية، والاستثمار في البنية التحتية المعلوماتية، وتأمينها، وتحديث القدرات العسكرية، ورفع كفاءة الجاهزية لمثل هذه الحرب عن طريق التدريب، والمشاركة الدولية في حماية البنية المعلوماتية، والاستثمار في رفع القدرات البشرية داخل الأجهزة الوطنية المعنية. وهنا، يتعلق التوجه الأخير بنقل تلك القدرات من الدفاع إلى الهجوم عن طريق استخدام تلك الهجمات في إطار إدارة الصراع والتوتر.

وإن كانت عملية بناء القد ارت العسكرية في مجال الأسلحة الإلكترونية تنطوي على عناصر أساسية، منها أولا السعي إلى امتلاك التكنولوجيا، وأنظمة الحماية، وتطوير قدرات هجومية تعمل على تحقيق التفوق التقني، وثانيا تطوير القد ارت الهجومية، إما عبر بناء القد ارت الذاتية، أو بالاستعانة بالأفراد والشركات المتخصصة، وتطوير القدرة على اختبار مدي الجاهزية لمواجهة الهجمات الإلكترونية

الهوامش والمراجع:

1. **Julia Creswell Oxford Dictionary of word origins: Cybernetres, oxford reference online, Oxford University press, 2010.**
2. رولا حفيظ، السيبرانية: الحرب الخفية في المنطقة المظلمة.
3. نبيل عودة، العمليات السيبرانية في الحرب الروسية الأوكرانية طبيعتها وأنماطها، الشرق للأبحاث الاستراتيجية، سبتمبر 2022.
4. عبد المنعم منيب، الحرب السيبرانية والصراع بين الدول فيما بعد الإنسانية العوالم الافتراضية وأثرها على الانسان تقرير ارتيادي استراتيجي محكم/ 2022.
5. إيهاب خليفة، الحرب السيبرانية، مراجعة العقيدة العسكرية استعداد للمعركة القادمة في ملحق تحولات استراتيجية، مجلة السياسة الدولية، العدد 211، جانفي 2018.
6. سماح عبد الصبور، الصراع السيبراني طبيعة المفهوم وملامح الفاعلين في ملحق تحولات استراتيجية، مجلة السياسة الدولية، العدد 208، أفريل 2017.
7. ماجد محمد الحنيطي، تكنولوجيا الصراعات الدولية المعاصرة، عمان: الآن ناشرون وموزعون، ط1، 2021.
8. عبد الغفار عفيفي الدويك، مستقبل الصراع السيبراني العالمي في القرن لـ 21، مجلة السياسة الدولية، العدد 2014، أكتوبر 2018.
9. عادل عبد الصادق، أنماط "الحرب السيبرانية" وتداعياتها على الأمن العالمي، مختلف اتجاهات نظرية، مجلة السياسة الدولية، العدد 208، أفريل 2017.
10. علي فرجاني، التحولات التكنولوجية للحروب السيبرانية...حلف الشمال الأطلسي نموذجا، على: https//:www.siyassa.org.eg 20/11/2023
11. بافان ناكو نجم الدين، تأثير الحرب السيبرانية على رفع مستوى الصراع بين الولايات المتحدة الأمريكية وإيران، مجلة جامعة،راپرين، العدد 04، 2021.
12. تغريد صفاء، لبنى خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حمورابي، العدد 33-34، شتاء ربيع 2020.
13. محمود علي عبد الرحمان، الفضاء الإلكتروني وأثره على مفاهيم القوة الأمن والصراع في العلاقات الدولية، مجلة كلية السياسة والاقتصاد، مجلد 16، العدد 15، جويلية 2022.
14. أحمد عثمان محمد، الحروب السيبرانية وأثرها في العلاقات الدولية روسيا والولايات المتحدة الأمريكية نموذجا، مجلة الجامعة العراقية، العدد 59.
15. محمود علي عبد الرحمان، أسامة فاروق مخيمر، الفضاء الإلكتروني وأثره على مفاهيم القوة، الأمن والصراع في العلاقات الدولية، مجلة كلية السياسة والاقتصاد، العدد 15، جويلية 2022.
16. عادل عبد الصادق، الحروب السيبرانية: تصاعد القوات والتحديات للأمن العالمي، قضايا استراتيجية، 2017.

17. علي فوجاني، التحولات التكنولوجية للحروب السيبرانية... حلف الشمال الأطلنطي نموذجا، على: http//:www.siyassa.org.eg Le 11/01/2024.

18. هبة جمال الدين، الأمن السيبراني والتحول في النظام الدولي، دراسات: العدد 01، جانفي 2023.

الأمن السيبراني عبر مواقع التواصل الاجتماعي: المخاطر والحلول.

Cyber security through social networking sites : Risks and solutions

رفاس الوليد (*) جامعة محمد لمين دباغين سطيف 2 o.reffas@univ-setif2.dz
كامل نجيب جامعة محمد لمين دباغين سطيف 2 n.kamel@univ-setif2.dz

ملخص:

لقد أظهر التطور التكنولوجي الذي صاحبه الانتشار الرهيب للأنترنيت والهواتف الذكية والأجهزة المحمولة، عالما جديدا موازيا للعالم الحقيقي بمختلف سماته وجزئياته، ومن أبرز هذه التطورات التكنولوجية نجد ظاهرة مواقع التواصل الاجتماعي والتي أصبحت ملجأ لكل أنواع وأشكال الجرائم الإلكترونية التي تهدد أمن واستقرار الأشخاص والمؤسسات وحتى الدول، ليكون بذلك موضوع الأمن السيبراني بمثابة أولوية لدى صناع القرار في مختلف الدول وأولوية أساسية في السياسات الأمنية والاقتصادية والسياسية.

بمرور الوقت أصبح نشاط المستخدمين عبر مواقع التواصل الاجتماعي أحد المصادر الأساسية للمخاطر السيبرانية التي تلاحق ملايين الأشخاص حول العالم، وذلك لما توفره من معلومات حول الحياة الشخصية والمهنية التي يفترض أن تكون محمية، وستسعى هذه الورقة البحثية إلى محاولة التعرف على المخاطر التي تهدد الأمن السيبراني عبر مواقع التواصل الاجتماعي، وحصر مختلف الحلول التي تحمي مستخدمي مواقع التواصل الاجتماعي من الجرائم الإلكترونية.

الكلمات المفتاحية: الأمن السيبراني؛ مواقع التواصل الاجتماعي؛ المخاطر؛ الحلول.

Abstract :

The technological development, which was accompanied by the terrible spread of the internet, smartphones and mobile devices, has shown a new world parallel to the real world with its various features and parts.one of the most prominent of these technological developments is the phenomenon of social networking sites, which has become a refuge for all types and forms of cybercrime that threaten the security and stability of people, institutions and even countries, thus making the topic of cyber security a priority for decision makers in various countries and a key priority in security, economic and political policies.

Over time, the activity of users through social networking sites has become one of the primary sources of cyber risks that haunt millions of people around the world, because of the information it provides about personal and professional life that is supposed to be protected. this research paper will seek to identify the risks that threaten cyber security through social networking sites, and limit the various solutions that protect users of social networking sites from cybercrimes.

KeyWords: ***cybersecurity; social networking sites; risks; solutions.***

مقدمة:

إن التطورات التكنولوجية في وسائل الإعلام والاتصال غيرت مجرى المشهد الإجرامي من العالم الحقيقي إلى العالم الافتراضي، فظهرت الجرائم السيبرانية كشكل جديد من الجرائم الذي يتجاوز جرائم العالم الحقيقي ولا يقل عنها أهمية أو خطورة، وقد ظهر هذا النوع من الجرائم الإلكترونية في أواخر السبعينات، فتطور من مجرد البردي العشوائي إلى عدة أشكال أكثر تقدما، مثل الفيروسات والبرامج الضارة (Thilini B. G, Prashant, & Monjur, 2022, p. 1) .

إن الجرائم الالكترونية تعبر عن مجموعة واسعة من الأنشطة والاعمال الافتراضية غير القانونية، التي تستهدف كل ما هو موجود على شبكة الانترنيت من أشخاص أو مؤسسات، وهذا يكون من طرف أشخاص أصحاب خبرة ومهارة في التعامل مع تكنولوجيا الانترنيت والعالم الافتراضي، ويكونون مدركين لنقاط الضعف الخاصة بها، وأيضا نقاط ضعف خاصة بالمستخدمين الذين يتجاوبون بشكل ساذج على سبيل المثال مع إيميلات أو رسائل مجهولة المصدر.

ان هذه الجرائم تطورت وتوسعت بالتوسع التكنولوجي الكبير على مستوى وسائل التواصل لاجتماعي وأيضا التطور في الانترنيت وتوسعها في كل العالم، فلا نكاد نجد فردا لا يستعمل الانترنيت او مواقع التواصل لاجتماعي، وبالتالي أصبح مصدر خطر حقيقي قريب من الافراد، وبإمكانه الوصول إلى خصوصياتهم خاصة وان هذه الخصوصيات أصبحت تتواجد على مستوى الوسائل التكنولوجية (كالصور والملفات والحسابات)، وبالتالي الوصول إلى هده الوسيلة هو بمثابة الوصول إلى كل خصوصيات هؤلاء الافراد والتحكم في أجهزتهم.

يعد لأمن السيبراني من أهم المصطلحات في مجال الكمبيوتر وتكنولوجيا المعلومات، وهو يرمز إلى الحفاظ على المعلومات وبيانات الأشخاص الالكترونية وغير الإلكترونية أيضا في مواضع ما، ونظرا لتطور الجريمة الإلكترونية فإن الحفاظ وحماية بياناتنا أو معلومتنا مهما جدا، خاصة وأنها أصبحت محل اهتمام قراصنة المعلومات أو ما يعرف بـ "الهاكر".

عليه ستسعى هاته الورقة البحثية للبحث في لإشكالية التالية: ماهي المخاطر التي تهدد لأمن السيبراني عبر مواقع التواصل لاجتماعي وما هي أبرز حلول المواجهة؟

وضمن هذا تتحدد لنا مجموعة من لأسئلة الفرعية هي:

- ما هو لأمن السيبراني والمفاهيم المرتبطة به؟
- ما هي أبرز التهديدات السيبرانية على مواقع التواصل لاجتماعي؟
- ما هي أبرز مخاطر لأمن السيبراني على منصات التواصل لاجتماعي؟
- كيف يمكن مواجهة مخاطر لأمن السيبراني على منصات التواصل لاجتماعي؟
- ما هي التحديات التي تواجه لامن السيبراني؟

المحور الأول: مدخل مفاهيمي.

أولا- الفضاء الالكتروني:

يشير الفضاء الإلكتروني ضمنا إلى اندماج جميع شبكات الاتصالات وقواعد البيانات ومصادر المعلومات في غطاء واسع ومتشابك ومتنوع من التبادل الإلكتروني، يتم إنشاء "نظام بيئي للشبكة"؛ فهو افتراضي و"موجود في كل مكان توجد فيه أسلاك الهاتف، والكابلات المحورية، وخطوط الألياف الضوئية، أو الموجات الكهرومغناطيسية."

ومع ذلك فإن الفضاء الإلكتروني لا يعتبر فضاء افتراضيا فقط وانما هو فضاء يتكون من الخوادم والكابلات وأجهزة الكمبيوتر والأقمار الصناعية ...إلخ، وفي الاستخدام الشائع نميل إلى استخدام مصطلحات الفضاء الإلكتروني والإنترنت بشكل متبادل تقريبا، على الرغم من أن الإنترنت وإن كانت الأكثر أهمية إلا أنها مجرد جزء واحد من الفضاء السيبراني (Myriam Dunn Cavelty, 2010, p. 401)

ثانيا- الجريمة السيبرانية:

الجريمة السيبرانية وهي نوع من الجرائم التي تحدث في الفضاء الافتراضي، وقد تطورت بشكل ملحوظ بتطور المواقع على شبكة الانترنيت وظهور "الهاكر"، كما تعرف بأنها: "الاستخدام غير القانوني لأي جهاز اتصال لارتكاب أو تسهيل ارتكاب أي عمل غير قانوني".وأيضا هي نوع من الجرائم التي تستهدف أو تستخدم جهاز كمبيوتر أو مجموعة من أجهزة الكمبيوتر ضمن شبكة واحدة بغرض الإضرار (CyberTalents, s.d.)، وتستهدف هذه الجرائم الأشخاص وأيضا المؤسسات في عالمها الافتراضي أو الالكتروني.

ثالثا- الأمن السيبراني:

الأمن السيبراني هو "عبارة عن مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع استخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني" (منى الأشقر جبور، 2012، ص16)

والأمن السيبراني هو سلاح إستراتيجي بيد الحكومة والأفراد، لاسيما أن الحرب السيبرانية أصبحت جزء لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول" (أوس مجيد غالب العوادي، 2016، ص06).

المحور الثاني: التهديدات السيبرانية على مواقع التواصل الاجتماعي.

هناك فئتان رئيسيتان لمخاطر وسائل التواصل الاجتماعي. الأول هو المخاطر الاجتماعية والآخر هو المخاطر التكنولوجية.وتنقسم المخاطر الاجتماعية أيضا إلى فئتين، وهما المخاطر على المستوى الفردي والمخاطر على المستوى المهني.ويمكن ان نصف هذه المخاطر كالآتي:

- المخاطر على المستوى الفردي: سرقة الهوية، سرقة المعلومات الاجتماعية.
- المخاطر على المستوى المهني: الضرر بسمعة الأشخاص، خرق البيانات.
- المخاطر على مستوى التكنولوجيا: البرامج الضارة وانقطاع الخدمات، الاختراقات، الوصول غير المصرح به إلى الحسابات على مواقع التواصل الاجتماعي.

ويصبح اختراق كلمة المرور أمرا سهلا بالنسبة للمتسلل الذي يمتلك الأدوات البرمجية المناسبة وبعض البيانات الشخصية، التي تم الحصول عليها من مواقع التواصل الاجتماعي الخاصة بشخص ما، وتعد الحسابات المزيفة والتسلط عبر الإنترنت والتحرش الجنسي من بين السلوكيات الضارة الرئيسية التي يمكن تحديدها في مجال وسائل التواصل الاجتماعي. كما انه توجد هجمات إلكترونية مختلفة في مواقع التواصل الاجتماعي، مثل سرقة الهوية، وهجمات البريد العشوائي، وهجمات البرامج الضارة، وهجمات سيبيل، والتصيد الاجتماعي، وانتحال الشخصية، والاختطاف، والطلبات المزيفة، واسترجاع الصور وتحليلها.

بالإضافة إلى ذلك أصبحت مواقع التواصل الاجتماعي ساحة لعب رئيسية لهجمات التصيد الاحتيالي. (Thilini B. G، Prashant، و Monjur، 2022، صفحة 5) وممارسة مختلف الممارسات من ابتزاز وطلب للأموال لاسترجاع

الحسابات او استرجاع البيانات والمعلومات والملفات، وقد أصبحت مواقع التواصل لاجتماعي باعتبارها فضاءا سهلا لقرصنة الحسابات ومنه قرصنة هواتف الأشخاص او الحواسيب أو أي لوحة الكترونية يستعملها الشخص للوصول إلى حسابه على مواقع التواصل لاجتماعي.

المحور الثالث: مخاطر لأمن السيبراني على منصات التواصل لاجتماعي.

تتعدد مظاهر وأشكال مخاطر لأمن السيبراني على منصات التواصل لاجتماعي حيث تتمثل في العناصر التالية:

أولا- مخاطر لاحتيال والتعدي على الخصوصية وسرقة الهوية:

تحتوي منصات التواصل لاجتماعي على كمية هائلة من المعلومات والبيانات الحقيقية. غالبا ما تطلب منصات الوسائط لاجتماعية تفاصيل شخصية (تاريخ الميلاد والعمر والبريد الإلكتروني والمزيد) للحصول على بيانات اعتماد تسجيل الدخول. يراقب المهاجمون السيبرانيون مثل هذه البيانات/المعلومات التي يمكنهم استخدامها للحصول على فدية وتلبية مطالبهم.(BULWARKERS، 2023)

كما يتضمن لاحتيال أو سرقة الهوية استخدام المتسللين للمعلومات الشخصية بطريقة غير أخلاقية، هناك طريقتان لتحقيق ذلك:

- أن يقوم الجاني بإنشاء ملف تعريف مزيف للضحية ثم يتفاعل تحت هذه الذريعة.
- أن يسرق الجاني كلمة المرور الخاصة بالضحية أو يتمكن من الوصول إلى حساب وسائل التواصل لاجتماعي الخاص به بطريقة أخرى، ثم يستخدم هذا الحساب. (Ben Salamah, 2023, p. 14)

ثانيا- هجمات التصيد والبرامج الضارة:

أحد أكثر المخاطر لأمنية شيوعا على وسائل التواصل لاجتماعي هو التصيد لاحتيالي، وهو عبارة عن محاولة احتيالية للحصول على معلوماتك الحساسة أو بيانات لاعتماد الخاصة بك عن طريق انتحال شخصية مصدر شرعي. ويمكن أن يحدث التصيد لاحتيالي عبر الرسائل المباشرة أو التعليقات أو المنشورات أو الروابط التي تغريك بالنقر عليها وإدخال التفاصيل الخاصة بك أو تزيل برامج ضارة. يمكن أن تصيب البرامج الضارة أجهزتك وشبكاتك، أو تسرق بياناتك، أو تلحق الضرر بملفاتك، أو تسيطر على حساباتك. لمنع هجمات التصيد لاحتيالي والبرامج الضارة، يجب عليك دائما التحقق من هوية المرسل وصحته، وتجنب النقر على الروابط أو المرفقات المشبوهة، واستخدام برامج مكافحة الفيروسات وجدار الحماية.

ثالثا- سرقة الحسابات وانتحال الشخصية:

هناك خطر آخر شائع يتعلق بأمن وسائل التواصل لاجتماعي وهو اختراق الحساب، وهو عندما يتمكن أحد المتسللين من الوصول إلى حساب الوسائط لاجتماعية الخاص بك ويستخدمه لأغراض ضارة. يمكن أن يؤدي اختراق الحساب إلى اختراق البيانات أو إرسال بريد عشوائي أو التشهير أو طلب فدية. يتم انتحال شخصية الحساب عندما يقوم أحد المتسللين بإنشاء حساب مزيف يحاكي علامتك التجارية أو شعارك أو اسمك ويحاول خداع متابعيك أو عملائك أو شركائك. ويمكن أن يؤدي انتحال شخصية الحساب إلى لإضرار بسمعتك أو تقويض ثقتك أو تغيير كلمة المرور الخاصة بك. لمنع سرقة الحساب وانتحال هويته، يجب عليك استخدام كلمات مرور قوية وفريدة من نوعها، وتمكين المصادقة الثنائية، ومراقبة نشاط حسابك، ولإبلاغ عن أي حسابات مشبوهة أو مزيفة. (Abílio, 2024)

وأثناء تعيين كلمات المرور، غالبا ما نواجه تعليمات مثل - ثمانية أحرف على الأقل، وأحرف صغيرة، وأحرف كبيرة، وأرقام (0-9) وأحرف خاصة. يمكن للمتسللين فك تشفير كلمات المرور الضعيفة بسهولة والتي يمكنهم من خلالها

تسجيل الدخول إلى حسابك وتنفيذ أنشطة احتيالية. ولذلك يوصى باتباع التعليمات لمنع اختراق الحساب.(BULWARKERS، 2023)

رابعا- الأخطاء البشرية والتهديدات الداخلية:

الخطر الثالث الشائع لأمن وسائل التواصل الاجتماعي هو الخطأ البشري والتهديدات الداخلية، والتي تنتج عن تصرفات أو تقاعس موظفيك أو المقاولين أو الشركاء. يمكن أن يشمل الخطأ البشري مشاركة معلومات حساسة، أو نشر محتوى غير لائق أو مسيء، أو الوقوع ضحية لهجمات التصيد الاحتيالي أو البرامج الضارة. يمكن أن تشمل التهديدات الداخلية تسريب بيانات سرية، أو تخريب أنظمتك، أو التعاون مع قراصنة خارجيين. لمنع الأخطاء البشرية والتهديدات الداخلية، يجب عليك تثقيف موظفيك حول أفضل ممارسات أمان وسائل التواصل الاجتماعي، وفرض سياسات وإرشادات واضحة، والحد من حقوق الوصول والامتيازات، ومراجعة حسابات وسائل التواصل الاجتماعي الخاصة بك بانتظام.

خامسا- القضايا القانونية:

الخطر الرابع الشائع فيما يتعلق بأمن وسائل التواصل الاجتماعي هو المسائل القانونية، التي تتعلق باللوائح والقوانين التي تحكم صناعتك أو موقعك أو جمهورك. يمكن أن تشمل المشكلات القانونية انتهاك قوانين الخصوصية أو قوانين حقوق الطبع والنشر أو معايير الصناعة أو مواجهة الدعاوى القضائية أو الغرامات أو فقدان التراخيص أو الشهادات الخاصة بك. لمنع الامتثال والمشكلات القانونية، يجب أن تكون على دراية بالقواعد واللوائح المعمول بها، وأن تحصل على الموافقة والإذن لاستخدام البيانات أو المحتوى الشخصي أو الخاص بطرف ثالث، واستخدام منصات وأدوات آمنة ومشفرة.

سادسا- السمعة وإدارة الأزمات:

الخطر الخامس الشائع لأمن وسائل التواصل الاجتماعي هو إدارة السمعة والأزمات، والتي ترتبط بتأثير مؤسستك واستجابتها لحادث أمني أو حدث سلبي. يمكن أن تشمل السمعة وإدارة الأزمات فقدان ولاء العملاء أو ثقتهم أو رضاهم، أو مواجهة رد فعل عام أو مقاطعة، أو التعرض لخسائر أو أضرار مالية. لمنع مشاكل السمعة وإدارة الأزمات، يجب أن يكون لديك خطة طوارئ واستراتيجية اتصال، والاستجابة بسرعة وشفافية، والاعتذار وتصحيح الوضع، والتعلم من ردود الفعل والخبرة.

إن المخاطر الأمنية لوسائل التواصل الاجتماعي أمر لا مفر منه ولا يمكن التنبؤ به، ولكن يمكن الحد منها وإدارتها من خلال الوعي والإعداد والعمل المناسب. باتباع النصائح وأفضل الممارسات المذكورة في هذا المقال، كما يمكنك حماية مؤسستك من المخاطر الأمنية الأكثر شيوعا لوسائل التواصل الاجتماعي. (Abílio, 2024)

المحور الرابع: مواجهة مخاطر الأمن السيبراني على منصات التواصل الاجتماعي.

توجد العديد من الآليات والخصائص التقنية التي بفضلها يمكن مواجهة مخاطر الأمن السيبراني على منصات مواقع التواصل الاجتماعي، نذكر أهمها:

أولا- خدمة المصادقة الثنائية:

توفر العديد من منصات التواصل الاجتماعي الشهيرة خدمة ملائمة للحفاظ على الأمان، مثل "المصادقة الثانية" التي غالبا ما تكون جزءا من المصادقة الثنائية، حيث تتم إعادة توجيه رمز مكون من أربعة أو ستة أرقام إلى رقم الهاتف المحمول المسجل الذي يظل صالحا لبضع دقائق فقط. تتم مصادقة المستوى الثاني أيضا عندما يصل

المستخدم إلى حسابه من متصفح آخر، هذه الميزة يمكن أن تحمي من هجمات الاختراق. وأيضا إفساد هجوم Sybil من خلال تطوير مصادقة المستوى الثاني لتعزيز مستويات ثقة المستخدمين. (Ben Salamah، 2023، صفحة 19)

ثانيا- استراتيجيات تقليل الهجمات السيبرانية:

تم تطوير العديد من الاستراتيجيات لتقليل عواقب هجمات سيبيل أو الحسابات المزيفة. على سبيل المثال، يحاول "نموذج كشف خداع الهوية" (IDDM) التقاط الغرض من الحساب المزيف على منصات التواصل الاجتماعي. لا يدرك النموذج الخداع فحسب، بل يفرق أيضا بين الإنسان والروبوت، كما تم اقتراح خوارزمية جديدة تسمى SVM-NN لتحسين تحديد الحسابات المزيفة على وسائل التواصل الاجتماعي. (Ben Salamah، 2023، صفحة 20)

ثالثا- التثقيف ونشر الوعي:

ضرورة البقاء على الاطلاع لمختلف عمليات الاحتيال عبر الإنترنت وتهديدات الأمن السيبراني وتعرف عليها، كلما جمعت المعرفة أكثر، كلما تمكنت من حماية نفسك بشكل أفضل. جنبا إلى جنب مع تثقيف نفسك، نشر الوعي أيضا.

رابعا- تحديث إعدادات كلمة المرور بانتظام:

حافظ على النصاب القانوني لتحديث إعدادات الخصوصية الخاصة بك على جميع حسابات الوسائط الاجتماعية الخاصة بك وتقييد كمية المعلومات التي تشاركها على مقابض الوسائط الاجتماعية الخاصة بك.

خامسا- تحديث نظام التشغيل الخاص بك:

استمر في تحديث نظام التشغيل والبرامج للتخفيف من هجمات البرامج الضارة وغيرها من التهديدات السيبرانية المضللة.

سادسا- مراقبة حسابك بانتظام والإبلاغ عن السلوك السيء:

قم بمراقبة نشاطك على وسائل التواصل الاجتماعي بشكل دوري ومراقبة لإجراءات المشبوهة وغير المألوفة، إذا كنت تواجه تنمرا عبر الإنترنت أو مضايقة عبر الإنترنت، فأبلغ عن ذلك إلى منصات التواصل الاجتماعي. (BULWARKERS, 2023)

وفي ظل التطور التكنولوجي الرهيب وظهور الهاتف الذكي الذي أصبح يسمح بالاطلاع على مواقع التواصل الاجتماعي وأيضا التسوق والبيع والشراء وكافة المعاملات الإلكترونية، زادت حدة الأخطار، والتوعية بهذه الأخطار جزء مهم من مواجهتها، وعلى العموم يمكن ان نعدد الحلول في النقاط التالية:

- السماح للمستخدم المصرح له فقط بالوصول إلى خدمة wifi.
- استخدم كلمة المرور المكونة من أحرف صغيرة وأحرف كبيرة وأرقام وبعض الأحرف الخاصة التي يجب الاحتفاظ بها.
- حافظ على تحديث برنامج مكافحة الفيروسات الخاص بك للحماية من الفيروسات وبرامج التجسس والبرامج الضارة.
- لا تقم بتنزيل أو النقر على الرابط غير المعروف للإعلانات غير المرغوب فيها.
- حافظ على أمان المعلومات الشخصية لتجنب سرقة الهوية.
- نقل المعلومات الحيوية الشخصية إلى المواقع الموثوقة.
- لا تكشف عن المزيد من المعلومات الشخصية في الشبكة الاجتماعية وفي الملف الشخصي على الشبكة الاجتماعية

- وفقًا للحاجة، يجب على المستخدم تعيين عرض معلومات الملف الشخصي كعامة أو لقائمة جهات الاتصال فقط.
- تجنب الرد على البريد العشوائي أورسائل التصيد الاحتيالي في شبكة غير موثوقة.
- لا تستخدم اي نظام تشغيل مقرصن أو نسخة مكسورة من نظام التشغيل، واستخدم نظام التشغيل الأصلي فقط.
- استخدم نظام مصادقة متعدد المستويات لتجنب وصول المهاجم غير المصرح به. (Praveen & Manjunatha, 2020, p. 824)

المحور الخامس: التحديات التي تواجه الامن السيبراني.

يعتبر الأمن السيبراني مصدر قلق بالغ للبلدان في جميع أنحاء العالم، حيث تواجه الدول النامية تحديات فريدة في هذا المجال. غالبًا ما تفتقر الشركات الصغيرة والمتوسطة في البلدان النامية إلى الموارد والخبرة اللازمة لتنفيذ ممارسات الأمن السيبراني القوية، مما يجعلها عرضة للتهديدات السيبرانية. بالإضافة إلى ذلك، فإن الافتقار إلى استراتيجيات وطنية شاملة للأمن السيبراني في الدول النامية يشكل تحديات كبيرة في مجال الإدارة، مما يعيق قدرتها على معالجة التهديدات السيبرانية بشكل فعّال(Kabanda, Maureen, & Cameron , 2018, p. 270) .

وتحتاج البلدان النامية إلى تحديد العناصر الحاسمة لإدراجها في استراتيجياتها الوطنية للأمن السيبراني من أجل مكافحة التهديدات السيبرانية بشكل فعال، وقد تشمل هذه العناصر إنشاء أطر قانونية، وتعزيز القدرات التقنية، وتعزيز التعاون الدولي، ورفع مستوى الوعي العام حول قضايا الأمن السيبراني. ومن خلال معالجة هذه العناصر، يمكن للدول النامية تعزيز موقفها في مجال الأمن السيبراني والتخفيف من المخاطر التي تشكلها التهديدات السيبرانية . (Newmeyer, 2015, p. 15)

إن الآثار المترتبة على عدم كفاية الأمن السيبراني في البلدان النامية بعيدة المدى، ولا تؤثر على أمن الأصول الرقمية فحسب، بل تؤثر أيضًا على الاستقرار الاقتصادي والاجتماعي الشامل. يمكن أن تؤدي الهجمات السيبرانية إلى تعطيل البنية التحتية الحيوية، وتعريض البيانات الحساسة للخطر، وتقويض ثقة الجمهور في التقنيات الرقمية، مما يؤدي إلى عواقب اقتصادية ومجتمعية كبيرة.

من جهتها أنشأت البلدان المتقدمة استراتيجيات وطنية شاملة للأمن السيبراني، تواجه الدول النامية تحديات فريدة في صياغة وتنفيذ تدابير فعالة للأمن السيبراني. غالبًا ما يدور النقاش الدائر حول هذا الموضوع حول تخصيص الموارد وبناء القدرات ودور التعاون الدولي في مواجهة تحديات الأمن السيبراني في البلدان النامية (Canongia & Raphael, 2012, p. 166)

خاتمة:

يُعد مفهوم الأمن السيبراني مفهوما متعدد الأبعاد والمستويات، يبدأ بتحقيق أمن الدولة ثم أمن المتجمع سواء في البيئة الداخلية أو الخارجية أو متداخلة بين الداخل والخارج، فالتطورات المعاصرة لثورة المعلومات والتكنولوجيا أدت إلى اتساع نطاق مفهوم الأمن السيبراني، بحيث أصبحت المتغيرات الأمنية الإلكترونية، متغيرات حاكمة بالنسبة للعديد من البيانات والقرارات بدرجة لم تكن معهودة من قبل.

وتعتبر التهديدات السيبرانية والمخاطر التي تُشكلها بمثابة الأخطبوط الذي أنتجته الحضارة التقنية والثورة المعلوماتية التكنولوجية، الذي امتدت أذرعه في جميع أنحاء العالم، والتي لم تفلت منها مختلف القطاعات من قبضته الدول الضعيفة والمتطورة على حد سواء، وبات خطرا مدمرا للاشخاص والمؤسسات خاصة على مواقع التواصل الاجتماعي، لذلك أصبح الأمن السيبراني عبر الشبكات الاجتماعية حتمية ضرورية وهاجسا أمام رجال القانون خاصة مع الوتيرة المتسارعة لتداول المعلومات والاستخدام العشوائي لمواقع التواصل الاجتماعي وقصور وسائل الرقابة وضعف التشريعات القانونية سواء الوطنية او الدولية وفرض العقوبة لتحجيم تأثيرات هذا النوع من الجرائم التي تستهدف الأفراد والمؤسسات وحتى استقرار الدول.

الهوامش والمراجع:

- أوس مجيد غالب العوادي، الأمن المعلوماتي السيبراني" بيروت، مركز البيان للدراسات والتخطيط، 2016، ص06.
- منى الأشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية، ماي2012، ص16.
- **Ben Salamah, Fai. «A thesis submitted to the University of Plymouth in partial fulfilment for the degree of DOCTOR OF PHILOSOPHY.» *Adaptive Cybersecurity Training Framework for Social Media Risks.* Édité par University of Plymouth. Plymouth, School of Engineering, Computing, and Mathematics: University of Plymouth, 7 2023. 1-256.**
- **BULWARKERS .*Common Cyber Security Risks Associated With Social Media Use and How Individuals Can Protect Themselves* .linkedin .2023 ,10 28 . https://www.linkedin.com/pulse/common-cyber-security-risks-associated-social-media-use-how-px6bf.(2024 ,03 22 الوصول** تاريخ)
- **Claudia Canongia و ،Mandarino Raphael .*Cybersecurity: The new challenge of the information society. In Handbook of research on business social networking: Organizational, managerial, and technological dimensions*** تحرير **.Cruz-Cunha Maria Manuela.2012 .**
- **CyberTalents. *CyberTalents.* s.d. https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention (accès le 3 29, 2024).**
- **Dunn Cavelty Myriam Dunn Cavelty .*Cyber-security, In The Routledge handbook of new security studies* .Routledge.2010 ،**
- **Herath Thilini B. G ،Khanna Prashant و ،Ahmed Monjur" .Cybersecurity Practices for Social Media Users: A Systematic Literature Review** تحرير **".MDPI .*Cybersecurity and Privacy*.18-1 :(2022 1) 2**
- **Kabanda, Salah, Tanner Maureen, et Kent Cameron . «Exploring SME cybersecurity practices in developing countries.» *Journal of Organizational Computing and Electronic Commerce* 28, n° 3 (2018): 269-282.**
- **Kevin P Newmeyer" .Elements of national cybersecurity strategy for developing nations. National Cybersecurity Institute Journal.19-9 :(2015) 3 رقم ،1 ".**
- **Maxime, Gautier. *Montant des budgets accordés en cybersécurité en France en 2021, par région.* Édité par statista. 24 10 2023. https://fr.statista.com/statistiques/1375836/montant-budgets-accordes-cybersecurite-par-region-france/ (accès le 03 24, 2024).**
- **Oliveira Abílio .*What are the most common social media security risks in your organization* .2024 ,03 08 ?https://www.linkedin.com/advice/0/what-most-common-social-media-security-risks-your-organization-0onle?lang=en ,03 22 الوصول** تاريخ) **.(2024**

- **Praveen , Gujjar J, et T Manjunatha. «Technology Challenges in Social Networking and Cyber Security.»** ***Seventeen AIMS International Conference on Management 823.*** **AIMS, 2020. 822-825.**

دور التحول الرقمي في صياغة وتغيير المفاهيم التقليدية في الأمن والجريمة والحرب والسيادة في العصر السيبراني – قراءة في التحديات ورهانات المواجهة الوطنية-

The role of digital transformation in formulating and changing traditional concepts of security, crime, war and sovereignty in the cyber age - a reading of the challenges and stakes of national confrontation -

د.بلبشير يعقوب[*] جامعة حسيبة بن بوعلي-الشلف- y.belbachir@univ-chlef.dz.
أ.د.دلالي جيلالي جامعة حسيبة بن بوعلي-الشلف- d.dellali@univ-chlef.dz

ملخص:

لا شك أن الأمن القومي للدول هو محور وغاية كل سياسة أمنية أو دفاعية، كما أن الرهانات والتحديات التي يطرحها هذا الهدف تبدو في غاية الأهمية والحساسية إذا ما أخذنا في الحسبان التطور التكنولوجي والثورة الرقمية التي جعلت من العالم قرية صغيرة، وحتمت على الدول انتهاج سياسات أمنية ودفاعية تأخذ في لاعتبار الفضاء الافتراضي المفتوح بكل ما يحتويه من زخم وكل ما يتعرض له من أخطار وتحديات في عصر رقمي يتشكل ويعاد تشكيله بسرعة، وتتغير فيه قواعد اللعب السياسية، بل وتتحول فيه مفاهيم الحرية والأمن والقوة والجريمة والسيادة والحروب التقليدية، مما يفرض تعزيز الجهود الوطنية والإقليمية والدولية لمواكبة التحولات في مفهوم الأمن القومي، وسياسات الدفاع ومفاهيم الجريمة والإرهاب والتجارة والبحث العلمي.

وستهدف هذه الدراسة إلى تقديم مقاربة شاملة ومتكاملة لجميع التحديات التي يطرحها الفضاء السيبراني، وقراءة جديدة في مفهوم السيادة الوطنية والأمن القومي الإلكتروني، والآليات القانونية والاتفاقية التي تواكب هذا التحول وتحدّ من مخاطر الفضاء السيبراني المتعددة، من خلال الجواب عن مشكلة بحثية تتعلق بمدى تأثير التحول الرقمي في إعادة تشكيل المفاهيم القانونية والجيوسياسية التقليدية المتعلقة بالأمن القومي للدول في رؤية تحليلية وصفية لأبعاد الظاهرة السيبرانية في تحولاتها المعرفية وامتداداتها عبر التخصصية، وصولا إلى حقيقة مفادها أن السيادة الوطنية والأمن القومي أصبحت مرتبطة بالفاعل الرقمي وبالسيادة والأمن السيبراني أولا.

الكلمات المفتاحية: الأمن السيبراني؛ الحروب السيبرانية؛ السيادة السيبرانية؛ الجريمة السيبرانية؛ التحول الرقمي.

Abstract:

There is no doubt that the national security of countries and societies is at the center and objective of any security or defense policy, but the issues and challenges posed by this objective seem extremely important and sensitive if we take into account the technological evolution and the digital revolution which has transformed the world into a small village, this has forced countries to adopt security and defense policies that take into account the open virtual space with all its components in the digital age where political data, circumstances and international relations, and even, the concepts of freedom, security, power, crime, sovereignty and traditional wars are transformed, which requires strengthening national, regional and international efforts to keep pace with the mutations of the concept of national security, defense policies and the concepts of crime, and terrorism, without forgetting commerce and scientific research.

This study will aim to provide a comprehensive and integrated approach to all the challenges posed by cyberspace, as well as a new reading of the concept of national sovereignty and electronic national security, and the legal and conventional mechanisms that accompany this transformation and limit the multiple risks of cyberspace, By answering the following problematic: what extent does digital transformation affect the reshaping of

[*] د.بلبشير يعقوب.

traditional legal and geopolitical concepts related to the national security of countries, In a descriptive analytical vision of the dimensions of the cyber phenomenon in its cognitive transformations and its trans-specialty extensions, Which leads to the fact that national sovereignty and national security are now linked to the digital factor, and to sovereignty and cybersecurity in the first place.

KeyWords: **cyber security; cyber wars; cyber sovereignty; cyber crime; digital transformation.**

مقدمة:

تطرح الدراسات الإستراتيجية والأمنية الحديثة أمام الباحثين نمطاً جديداً من الحروب غير التقليدية لا مكان فيه للمفاهيم التقليدية، وشكلاً جديداً من النظم الدفاعية يحتل فيها الفاعل الرقمي أساس المعادلة الأمنية فيما يسمى بالدفاع السيبراني وتأثيراته على مفاهيم السيادة السيبرانية في ظل فضاء رقمي مفتوح مفعم بالمخاطر والتهديدات الأمنية، كما أنتج هذا الوضع اشكالاً من الصراعات الدولية والإقليمية أسهمت فيه الثورة الرقمية بشكل واضح في ترجيح موازين القوى بين الدول التي صارت تعتمد استراتيجيات أمنية ودفاعية تعتمد نضم الجوسسة الإلكترونية والجوسسة المضادة وحرب معلوماتية ضروس البقاء فيها لمن يحسن اللعب بتكنولوجيا المعلومات ويوظفها لخدمة أهدافه الدفاعية أو الإمبريالية.

وقد شكلت الهجومات السيبرانية النموذج الأكثر انتهاجاً في هذه الحرب خاصةً من قبل الدول التي شهدت سباقاً محموماً حول استغلال مساحات الفضاء السيبراني من أجل مواجهة مخاطر هذا الفضاء المفتوح على برامج التسلح والتجارة الالكترونية والأمن الداخلي، مما أنتج تحولاً كبيراً في مفهوم الأمن القومي لم تعد فيه مكانة للمفاهيم التقليدية للحرب والقوة والصراع والأمن تواكب ما وصلت إليه ثورة المعلومات؛ الأمر الذي يتطلب من الدول الأقل أمناً إلكترونياً وسيبرانياً انتهاج استراتيجيات أمنية جديدة وتوحيد الجهود الإقليمية خاصةً والدولية لمواجهة مخاطر الفضاء السيبراني الذي لم يعد حكراً على الدول والجيوش الوطنية الإلكترونية بل صار مساحة لنشاط بعض المنضمات الإرهابية.

وفي ظل التقارير الدولية التي تشير إلى أن الجزائر وكثير من الدول العربية ودول العالم الثالث تحتل مراتب متأخرة في تصنيف الدول من حيث امن الشبكات والأمان الرقمي فإن الحاجة اليوم تبدو ملحة إلى تغيير التكتيكات والإستراتيجيات في مجال الأمن الوطني الإلكتروني من خلال مقاربة شاملة ومتكاملة لجميع التحديات التي يطرحها الفضاء السيبراني، وقراءة جديدة في مفهوم السيادة الوطنية والأمن القومي الإلكتروني، وآليات قانونية واتفاقية تواكب هذا التحول وتحدّ من مخاطر الفضاء السيبراني المتعددة.

الدراسات السابقة:

1 - الحرب الإلكترونية -الاشتباك في عالم المعلومات- لمؤلفه عباس بدران، الصادر عن مركز دراسات الحكومة الإلكترونية بيروت، لبنان، 2010، وهو من المؤلفات التي اعادت رسم الخارطة المفاهيمية لدلالات الامن في زمن السيبراني الجديد وفق التغيرات الجيوسياسية لبداية القرا الواحد والعشرون.

2 - الأمن وحرب المعلومات لمؤلفه ذياب البداينة ، الصادر عن دار الشروق للنشر والتوزيع، عمان، الأردن، 2006، وهو من أوائل ما كتب حول حروب الجيل الخامس وتأثيراتها على الأمن السيبراني الدولي.

3 - تحولات في مفهوم الأمن: من أمن الوسائل إلى أمن الأهداف لمؤلفه جمال منصر، وهو مقال منشور في مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقلة، العدد الأول جانفي 2009، وهي دراسة أصلت لتحول مفهوم الامن

القومي وتحولاته بالانتقال من العوامل الفنية والتكنولوجية نحو مقاربة جيوسياسية جديدة تستوعب المفاهيم الحديثة غير التقليدية مواكبة للثورة الرقمية.

في حين كانت دراستنا قراءة في تحولات بعض المفاهيم القانونية ذات الامتداد الجيوسياسي بالنظر إلى ثورة المعلومات المتسارعة ومستوى المخاطر والتهديدات المستجدة، وصولا إلى رسم ملامح استراتيجية مستقبلية وطنيا تعتمد على تعزيز الوعاء المؤسسي والإطار القانوني من أجل حماية الأمن السيبراني ومن ثم الأمن القومي للبلاد.

اهداف الدراسة:

ستهدف هذه الدراسة إلى تحقيق ما يلي:

- تحديد دلالات الامن في العصر الرقمي والمخاطر السيبرانية التي يعجّ بها الفضاء الالكتروني المفتوح.
- حصر التحولات الجديدة للمفاهيم غير التقليدية المتعلقة بالجريمة والحرب والقوة والحدود والسيادة في العصر السيبراني الحالي عن طريق تغيير الصورة الذهنية النمطية عن هذه المفاهيم.
- تحديد معالم الاستراتيجية الوطنية والدولية لمواجهة المخاطر السيبرانية على المستويين المؤسسي والتشريعي.

إشكالية الدراسة:

تفرض الاوضاع الدولية الراهنة على الجزائر والدول التي تعاني من ضعف مستوى الدفاعات السيبرانية والآمان الرقمي تحديات كبرى تفرض عليها حتمية التوجه نحو استراتيجيات تعزّز أمن فضائها السيبراني، وهو ما يدعو الى التساؤل حول مستوى المخاطر والتهديدات السيبرانية الموجودة وطبيعة الاستراتيجيات المتوخاة للحد منها ومواجهتها بغرض حماية الفضاء السيبراني والوطني والمصالح الاقتصادية والامن القومي للبلاد خصوصا في ظل تحول المفاهيم التقليدية للسيادة والحرب والأمن والحدود؟.

مناهج الدراسة:

للإجابة عن هذه الاشكالية ولتحقيق اهداف هذه الدراسة اعتمد الباحثان المناهج الآتية:

- المنهج الوصفي؛ ذلك أن الدراسة كانت عبارة عن رصد للظاهرة السيبرانية في تحولاتها القانونية والجيوسياسية وتركماتها المعرفية وامتداداتها التاريخية.
- المنهج التحليلي؛ حيث قام الباحثان بتحليل المعطيات ومقاربة السياسات وتدقيقها في قراءة متكاملة تم فيها تقييم مستوى التحولات وطبيعة الجهود والاستراتيجيات المنتهجة لمواكبة تحولات العصر الرقمي.

المخطط العام للبحث:

المحور الأول: الأمن في الفضاء السيبراني - رؤية مفاهيمية –

أولا - مفهوم الفضاء السيبراني وأمن المعلومات

ثانياً: الأمن السيبراني والجريمة السيبرانية - دلالات المفهوم والعلاقة-

المحور الثاني: الاستراتيجية الوطنية للأمن السيبراني في ظل تحول المفاهيم القانونية والجيوسياسية التقليدية – نحو فضاء وطني رقمي آمن سيبرانيا –

أولا - سياسة الأمن والدفاع الوطني السيبراني وتحولات مفهوم القوة والسيادة والحرب

ثانيا - إستراتيجية الجزائر في تأمين حدودها السيبرانية وتحقيق الأمن السيبراني الوطني

المحور الأول: الأمن في الفضاء السيبراني - رؤية مفاهيمية -

لاشك أن الثورة المعلوماتية وتطور التكنولوجيا الرقمية وانتشارها عموديا وأفقيا كأداة في أيدي الدول والمنظمات والأفراد انعكس على موازين القوى في العلاقات الدولية، وأحدث نمطاً جديداً في مقاربات الأمن القومي تعتمد

الفاعل الرقمي الذي يصف الطرق والأساليب والنماذج التي يتبعها اللاعبون الرقميون، لانتهاج الخيارات المعلوماتية في خوض سباق التفوق الدولي، ويحتم أيضاً إعادة النظر في المفاهيم التقليدية للأمن والجريمة والحرب والصراع والقوة، مما سنبينه في هذا الشق من الدراسة من خلال تفكيك رموز التداخل بين هذه المفاهيم والمفاهيم ذات الصلة.

أولا - مفهوم الفضاء السيبراني وأمن المعلومات

1- تعريف الفضاء السيبراني: هو الفضاء الذي أوجدته تكنولوجيا المعلومات والاتصالات، وفي مقدمها الانترنت. ويرتبط هذا الفضاء، ارتباطا وثيقا بالعالم المادي، عبر البنى التحتية المختلفة للاتصالات، والأنظمة المعلوماتية، وعبر العديد من الخدمات، التي لم يكن بالإمكان الحصول عليها، من دونه، وليس أقل من ذلك، الوصول إلى البيانات والمعلومات[1]، وتختلف التعريفات حول الفضاء السيبراني[2] على حسب كل طبيعة أو كيان وعلى مدى قدرته على تحديد رؤيته وإستراتيجيته للتعامل مع مجال الفضاء السيبراني بشقيه المدني والعسكري وكذلك مدى رؤيته على استغلال المزايا ومواجهة المخاطر الكامنة في هذا المجال[3]، فهو بمثابة المجال المجازي لأنظمة الحاسوب والشبكات الإلكترونية؛ حيث تخزن المعلومات إلكترونيًا وتتم الاتصالات المباشرة على الشبكة. لذا فهو عالم غير مادي يشمل مواضيع مثل المعلومات الشخصية، والمعاملات الإلكترونية، والملكية الفكرية وغيرها من المواضيع ذات الصلة . وقد عرفته الوكالة الفرنسية لامن أنظمة الإعلام (**ANSSI**)، وهي وكالة حكومية مُكلفة بالدفاع السيبراني الفرنسي على أنه: "فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية"[4]، كما عرفه خبراء الأمن السيبراني أيضاً بأنه عالم افتراضي يتشابك مع عالمنا المادي، يتاثر به ويؤثر فيه بشكل معقد، حيث تقوم العلاقة بين العالمين على نظرة تكاملية تحمل بين طياتها مزايا ومخاطر لا تتوقف، وهناك من وصفه بالذراع الرابعة للجيوش الحديثة إلى جوار القوات الجوية والبحرية والبرية وخاصة أن الانترنت شهد بداية الحديث عن معارك حقيقية تدور في هذا العالم الافتراضي[5]؛ وعليه يُمكننا القول بأن: "الفضاء السيبراني هو مجال مركب مادي وغير مادي يشمل مجموعة من العناصر هي: أجهزة الكمبيوتر، أنظمة الشبكات والبرمجيات، حوسبة المعلومات، نقل وتخزين البيانات، ومستخدمو كل هذه العناصر"[6]. يعتمد في حركته على ثنائيات من الآحاد والأصفار المتناهية الصغر في تغيير حركة العالم وهي التي تدير شبكات من ملايين النظم والبرامج والتطبيقات، وهو ما يبين أهمية وخطورة القدرة على امتلاك آليات توظيف هذه البيئة الإلكترونية واستغلالها وتكييفها وفق المصالح والأهداف وبما ينعكس على الملايين من الأشخاص من المتفاعلين والملتقين[7].

2- امن المعلومات: هو مفهوم مركب من مصطلحي الأمن والمعلوماتية؛ وسنحاول تفكيكه على النحو الآتي:

- الأمن: هو ضرورة اجتماعية في حياة الأفراد والمجتمع حتى ينعم بالأمان والاستقرار؛ وقوامه الأمن في الجسد والمال والولد والدين والمعتقد السياسي والثقافي، ومن مؤشراته: الرخاء الاقتصادي، حرية ممارسة المعتقد والفكر والرأي السياسي، ومستوى الدخل الفردي. وله أربعة مستويات:[8] "الأمن الفردي، الأمن الوطني، الأمن الإقليمي، الأمن الدولي"؛ يقول لورنس كروز وجوزاف ناي الأمن هو: "غياب التهديد بالحرمان الشديد من الرفاهية الاقتصادية"، ويعود هذا التعريف إلى مفهوم القوة والتهديد بالحرمان الشديد من الرفاهية في مفهومها المادي المحسوس، وهو الجانب الاقتصادي، مشيراً إلى أهمية القوة الاقتصادية كركيزة رئيسية للأمن الوطني؛ أما ج. هولسن وج. ويلبوك فيؤكدان بأن الأمن الوطني "قد ياخذ شكل أهداف تسعى الدولة لتحقيقها، من خلال السياسات والبرامج، والعمل على توسيع نفوذها في الخارج، أو محاولة التأثير عل سلوك الدول الأخرى أو تغييره"[9]، وما يهمنا هنا هو: "الأمن القومي أو الوطني" للصلة الوثيقة بينه وبين الأمن السيبراني تأثراً وتأثيراً.

وقد كان يتم تعريف الأمن القومي تقليدياً على أنه الحماية من الهجوم الخارجي، وبالتالي فقد تم النظر إليه بشكل أساسي على أنه يعني دفاعات عسكرية في مواجهة تهديدات عسكرية. وقد ثبت ان هذه الرؤية ضيقة جداً؛ فالأمن القومي يتضمن ما هو أكثر من تجهيز قوات مسلحة واستخدامها[10]، حيث يعرف ولتمان وناشت وكويستر الأمن الوطني أو القومي بأنه مجموعة من التهديدات الفيزيقية (**physical**) والتي ربما تواجه الدولة، وتدفع بالبنى والعقائد، والسياسات العسكرية للتأهب لمواجهة هذه التهديدات..وهذه عوامل داخلية وخارجية، مثل التغيرات الاقتصادية والاجتماعية التي ربما تؤثر بطريقة مباشرة أو غير مباشرة، وتنقص أو تزيد[11] من قدرة الدولة على مواجهتها، وعليه يمكن القول بان الأمن القومي هو قدرة الأمة على الدفاع عن أمنها، وحقوقها، وصياغة استقلالها، وسيادتها على أراضيها، وتنمية القدرات والإمكانات العربي، في مختلف المجالات السياسية، والاقتصادية، والثقافية والاجتماعية، مستندة إلى القدرة العسكرية والدبلوماسية، آخذة في الاعتبار الاحتياجات الأمنية الوطنية لكل دولة، والإمكانات المتاحة، والمتغيرات الداخلية والإقليمية والدولية.

- المعلومات: تعرف المعلومات بأنها "نتائج عمليات النماذج، التكوين، التنظيم، أو تحويل البيانات بطريقة تؤدي إلى زيادة مستوى المعرفة للمستقبل [12]، كما تعرف أيضاً على أنها "بيانات تم تصنيفها بشكل يسمح باستخدامها والاستفادة منها، وبالتالي فالمعلومات لها معنى، وتؤثر في ردود أفعال وسلوك من يستقبلها"[13]، وقد صار الأمن القومي للدول اليوم مرتبطاً ببعد جديد؛ هو مدى حصانة منظومتها الأمنية الإلكترونية فيما يسمى بأمن المعلومات[14] أو الأمن السيبراني، وهي منظومة ترتكز على جودة وتطور النظام المعلوماتي وأمن الشبكات، حيث يشمل هذا النظام كل مكونات هذا الحاسب الآلي المادية (**HardWare**) والمعنوية (**SoftWare**) وشبكات الاتصال الخاصة به (**NetWorks**)، او مجموع عناصر مادية وغير مادية يمكن باجتماعها العمل الفوري مع المعلومة[15]، وعليه يمكن القول بأن أمن المعلومات "هو مجموعة من الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي، للحفاظ على المعلومات والأجهزة والبرمجيات، إضافة إلى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال" [16]، ويمكن التعبير عنه "بجملة الوسائل والأدوات والإجراءات اللازم توفيرها لحماية المعلومات من الأخطار الداخلية والخارجية"[17]، ويعد مساساً بأمن المعلومات كل فعل يهدد أمن شبكات الحاسوب أو النظام الرقمي الوطني أو قواعد البيانات الخاصة أو العامة؛ وهو ما يصطلح عليه بالجريمة الإلكترونية او المعلوماتية؛ التي يعرفها محمد أمين شوابكة أنها "اي جريمة يمكن ارتكابها بواسطة نظام حاسوبي او شبكة حاسوبية أو داخل نظام حاسوبي، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"[18]، وهذا الاعتداء على أمن المعلومات مرتبط أساساً بمفهوم الأمن السيبراني للدول، وقد يأخذ عدة اشكال:

- الإرهاب الإلكتروني.
- الاعتداء على قواعد البيانات الخاصة أو العامة لأجهزة الحاسوب وسائر الأجهزة الإلكترونية والشبكات الرقمية .
- الاعتداء على المؤسسات الاقتصادية والمصرفية بالمساس بسرية البيانات والمعاملات والتداولات المالية الرقمية وغير الرقمية .
- غسيل الأموال، والجريمة الإلكترونية عبر الوطنية، بالإضافة إلى الاستغلال غير المشروع للنساء والأطفال، والمساس بحرمة الحياة الخاصة للأشخاص وكرامتهم واعتبارهم من خلال جرائم القذف والتشهير الإلكتروني.
- قد يأخذ أيضاً شكل حروب غير معلنة في الفضاء السيبراني بين الدول (الجوسسة، الاختراق، التهديدات السيبرانية للنظم الدفاعية والأمنية للدول).

ثانياً: الأمن السيبراني والجريمة السيبرانية - دلالات المفهوم والعلاقة-

أصبحت السياسات الأمنية والدفاعية للدول اليوم مرتبطة بمدى قدرتها على توظيف الفاعل الرقمي في حماية مجالها الجوي البحري والبري والسيبراني من كل الجرام الداخلية والاعتداءات الخارجية مما يلزم منه تحديد مفهوم الأمن السيبراني وماهية الجريمة السيبرانية قبل المرور إلى تأثيراتها وانعكاساتها على الأمن الوطني والتكتيكات والاستراتيجيات الكفيلة بمواجهتها.

1 - تعريف الأمن السيبراني: الأمن السيبراني هو أمن الشبكات، والأنظمة المعلوماتية، والبيانات، والمعلومات، والأجهزة المتصلة بالانترنت. وعليه فهو المجال المتعلق بالإجراءات ومقاييس ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، أو للحد من آثارها في أقسى وأسوء الأحوال. ويرتبط هذا الأمن ارتباطاً وثيقاً بأمن المعلومات؛ فالوصول إلى هذه الأخيرة، أو بثها، أو الاطلاع عليها والمتاجرة بها، أو تشويشها واستغلالها[19]؛ فهو النشاط أو العملية، والقدرة، أو نظم المعلومات واتصالات الدول، حيث تكون المعلومات الواردة فيه محمية من أي دافع من التلف، والاستخدام غير المصرح به أو التعديل، أو الاستغلال[20]، كما عرفه ريشارد كومرو بأنه: "عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة"[21]، أما إدوارد أومورسو فعرفه بأنه: "وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها...إلخ"[22]، وبحسب تعريف الإتحاد الدولي للاتصالات في تقريره حول اتجاهات لإصلاح في الاتصالات للعام 2010.2011) هو "مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية، ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية، وموجودات المؤسسات والمستخدمين" [23]، وهو نفس المفهوم تقريباً الذي أخذت به وكالة الأمن الرقمي الأوربية في أول تشريع أصدرته في هذا الشأن سنة 2001؛ فهو "قدرة النظام المعلوماتي على مقاومة محاولات لاختراق أو الحوادث غير المتوقعة، التي تستهدف البيانات المتداولة أو المخزنة وفق إطار توافقي"[24]، أما وزارة الدفاع الأمريكية (البينتاغون) فالأمن السيبراني بالنسبة لها هو "مجموعة لإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها (الإلكترونية أو المادية) .

2- الجريمة السيبرانية - مفهومها وأشكالها-: نظراً لحداثة النظام السيبراني واتساع نطاق الاعتماد على المعلوماتية في المجالات التقنية والاقتصادية والعسكرية والشخصية؛ فإنه صار من الضروري وضع تعريف دقيق لكل نشاط يأخذ توصيف الجريمة ينتهك ضمن نطاق الفضاء السيبراني بكل مكوناته وهو ما يعرف بالجرائم السيبرانية التي مازال تحديد مفهومها وأشكالها ونطاقها محل جدل فقهي.

أ - تعريف الجريمة السيبرانية: هي فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، يهدف إلى الاعتداء على الأموال المادية او المعنوية أو الاعتداء على خصوصية الأفراد، أو هي عمل أو امتناع يأتيه الإنسان إضراراً بمكونات الحاسب وشبكات الاتصال الخاصة به، من جهة أخرى هي الجريمة التي يكون النظام المعلوماتي فيها وسيلة لارتكاب جريمة تقليدية، إما ضد الأموال كالتحويل الإلكتروني غير المشروع للاموال، أو ضد الأشخاص كجريمة السب أو القذف عبر الانترنت[25]؛ حيث أنه لا ينبغي الاكتفاء بالبعد التقني أو الفني في تعريف الجريمة السيبرانية أو الإلكتروني، بالرغم من أنها تخضع مثل سائر الجرائم إلى مبدأ شرعية الجرائم والعقوبات، كما أن أبعادها لا تنحصر في البعد القانوني وحده، بل إن لها أبعاد اقتصادية وسياسية وعسكرية، وهي من الجرائم العابرة للحدود التي يسهل في الغالب طمس أدلة إثباتها في الوقت الذي يصعب التحري والتحقيق فيها، كما انها ترتكب من قبل الأفراد والجماعات وكثيراً ما تكون مجالاً للاتفاق الجنائي والتنسيق لإجرامي الذي يتطلب بدوره تنسيقاً أمنياً وجهوداً دولية لمواجهتها تتعدى إستراتيجية تعزيز الترسانة القانونية الجزائية.

ومع الصعوبة والخلاف الفقهي حول تحديد مفهوم الجريمة السيبرانية فقد اجتهدت بعض الدول في تعريفها حسماً لأي مغالطات في تفسير وتحديد أركان وأشكال ونطاق هذه الجرائم، حيث خصص المشرع الجزائري قسماً كاملاً للجرائم المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات في القانون 04-15 المعدل والمتمم في قانون العقوبات[26]، حيث عرفها المشرع الجزائري في المادة 02 فقرة 01 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها [27] كما يلي: "الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة اخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية"، وما يعاب على هذا التعريف أنه تقني بحت يركز على المعطى المادي والفاعل الرقمي كوسيلة لارتكاب الجريمة السيبرانية ويهمل العامل البشري والمعطيات لأخرى ذات الصلة وذات الانعكاس الاقتصادي والبعد الجيو سياسي والأمني .

وعرفها المشرع السعودي بأنها: "أي فعل يرتكب متضمناً استخدام الحاسب الآلي او الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"[28]، في حين عرفها المشرع القطري بأنها: "أي فعل ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية، بطريقة غير مشروعة بما يخالف أحكام القانون"[29]، أما المعهد لأسترالي لعلم لإجرام فيرى بأنها: "تسمية عامة لجرائم ارتكبت باستخدام تخزين البيانات الإلكترونية أو جهاز الاتصالات"[30]، وعليه تعد جريمة سيبرانية كل فعل يأخذ وصف الجريمة في القانون الجزائي العام يرتكب في الفضاء السيبراني من قبل أشخاص أو جماعات او منضمات أو دول بواسطة أجهزة الحاسوب وبرامج لإعلام الآلي وشبكة الإنترنت، أو لاعتداء عليها أو بها، مما يهدد حق الأفراد في الخصوصية وقواعد البيانات الخاصة وانظمة المعلومات والاتصالات، قد يأخذ بعداً آخر جيوسياسي وعسكري حينما يتعلق لأمر بأنظمة الدفاع الإلكتروني وسياسات الجوسسة والجوسسة المضادة وبرامج التسلح.

ب - أشكال الجرائم والتهديدات السيبرانية: تتنوع الجرائم والتهديدات السيبرانية بتنوع الأشخاص أو الكيانات المرتكبة لها وكذا الأدوات والأهداف وبحسب كونها داخلية وعابرة للحدود القطرية، ونذكر منها مايلي:

- المساس بسرية الاتصالات على الوسائط الإلكترونية، وسرقة البيانات الشخصية، وتسريبها، واستخدامها دون إذن، ودون وجه حق، وسرقة لأموال، واختراق انظمة المعلومات، ولاعتداء على الملكية الفكرية، والصناعية، والعلامات التجارية.

- الجرائم العادية التي تستخدم لانترنت في تنفيذها، كالسرقة والغش والخداع، والتغرير بالقاصرين، وتسهيل الدعارة، والترويج لنشاطات مخالفة للقانون، ولاعتداء على الملكية الفكرية.

- التلاعب بالمعلومات الموجودة في نظام معين، وتشويهها او إتلافها، سواء عبر الاقتحام اليدوي، أو عبر إرسال برامج وفيروسات مخصصة بذلك[31].

- إتلاف المعطيات والبيانات المخزنة الرقمية أو تشويهها، والتجسس على الشبكات، بالإضافة إلى تدمير لأصول والمعلومات[32] بواسطة الأنظمة الخبيثة والفيروسية بأهداف إجرامية أو إرهابية.

- كل ما يعرض لأمن القومي، والعسكري، والاقتصادي، ولاجتماعي، ويهدد البنية التحتية والحرجة للدول، وأسواق المال والقطاعات المصرفية، والسلم الدولي، والمنشآت النووية، والمؤسسات الصحية، وقطاعات النقل[33] بكل أنواعها.

- كافة التهديدات السيبرانية بما في ذلك القرصنة ونضال رقمي وحرمان من الخدمة والجريمة والتجسس والتخريب والتدمير والهجمات لإستراتيجية من خلال الفيروسات التي تدمر المكون المادي مثل فيروس ستاكس نت[34]، بالإضافة إلى الهجومات التي تتعرض لها أنظمة التسلح النووي.

- الإرهاب الالكتروني ونعني به: الهجوم القائم على مهاجمة الحاسوب، وأن التهديد به يهدف إلى الترويع أو إجبار الحكومات او المجتمعات لتحقيق اهداف سياسية أو دينية او عقائدية، وينبغي أن يكون الهجوم مدمراً وتخريبياً لتوليد الخوف [35] بحيث يكون مشابه للأفعال المادية للإرهاب.

المحور الثاني: الاستراتيجية الوطنية للأمن السيبراني في ظل تحول المفاهيم القانونية والجيوسياسية التقليدية – نحو فضاء وطني رقمي آمن سيبرانيا –

لقد صار من الضروري على الدول تغيير النظرة النمطية التقليدية لمفهوم الأمن القومي وامتداداته وتأثيراته على مفاهيم السيادة والقوة نحو مقاربة جديدة تأخذ في الحسبانها الفاعل الرقمي كمحدد أساس لهذا التوجه مما يفرض عليها تعزيز المنظومة المؤسسية وتوفير البيئة التشريعية الناظمة التي تواكب حجم المخاطر السيبرانية الموجودة وحرب المعلومات المستعرة على كل المستويات، وهذا ما سيأتي تفصيله في العناصر الآتية.

أولا - سياسة الأمن والدفاع الوطني السيبراني وتحولات مفهوم القوة والسيادة والحرب

بعدما أثبتنا أن أمن الفضاء السيبراني تطور ولم يعد مرتكزا على الأبعاد التقنية والفنية فحسب، بعد تدخل العوامل الإقتصادية والعسكرية وجيوسياسية سنحاول في هذا الشق من الدراسة أن نتطرق إلى تحولات مفاهيم الأمن والقوة والحرب في النقاط الآتية:

1- الأمن: عرفة إدوارد اومورسو بأنه: "وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها...إلخ "[36]؛ فهو عبارة عن مجموعة من الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به على شبكات الكمبيوتر وسوء الاستغلال واستعادة المعلومات الإلكترونية التي تحتويها بهدف ضمان واستمرارية عمل نظم المعلومات، وتأمين حماية وسرية وخصوصية البيانات الخاصة بفواعل الفضاء السيبراني[37]، وعليه فهو المجال المتعلق بالإجراءات ومقاييس ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، أو للحد من آثارها في أقصى وأسوء الأحوال، غير أن هذا التعريف يبدوا متأثرا بالنظرة الفنية في تحديد مفهوم السيبرانية.

في حين راى خبراء الإتحاد الدولي للاتصالات في تقريرهم حول (اتجاهات لإصلاح في الاتصالات للعام (2011/2010) هو "مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات امنية، ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين"[38]؛ وهو نفس المفهوم تقريباً الذي أخذت به وكالة الأمن الرقمي الأوربية في أول تشريع أصدرته في هذا الشأن سنة 2001، فهو قدرة النظام المعلوماتي على مقاومة محاولات الاختراق أو الحوادث غير المتوقعة، التي تستهدف البيانات المتداولة أو المخزنة وفق إطار توافقي[39]، تنتظم فيه الأدوات القانونية والسياسات الأمنية ووسائل الدفاع الالكتروني لتحقيق أهداف الأمان السيبراني المنشودة وطنيا وإقليميا ودوليا.

2- القوة: لقد صار لزاما على كل الفاعلين في الفضاء السيبراني الأخذ في الحسبان أيضاً التحول في مفهوم القوة واستيعاب مفهوم القوة السيبرانية كمفهوم جديد يتجاوز الأبعاد الاقتصادية والسياسية والعسكرية التقليدية. حيث يرى جوزيف اس ناي أن القوة السيبرانية هي : "القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي انها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة، والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات سيبرانية"[40].

والواقع أن استخدام مصطلح القوة السيبرانية أكثر دقة من القوة الالكترونية التي تترجم(**ElectronicPower**)، إذ أن المقصود هو (**Powercyber**) وهي أكثر شمولية في ما نقصده في التعاملات الدولية[41]. حيث بدأ الاهتمام بهذا

الموضوع بوضع فرضيات نظرية تدرس إمكانية استخدام أو تصميم أسلحة رقمية مستفيدين من الثورة العلمية الهائلة في مجال علم الحاسوب والإنترنت، تتفوق هذه الأسلحة على العتاد العسكري التقليدي المادي وتكون بديلة عنه لإحداث أكبر ضرر في منشآت العدو العسكرية والمدنية[42]، بأساليب أكثر فتكا وأقل خسائر.

3- الحرب: يمكن تعريف الحرب السيبرانية بأنها التوظيف المتكامل للفواعل الرقمية والأنشطة السيبيرية وأنشطة الحاسوب، والحرب النفسية، والخداع العسكري، وأمن العمليات، بالتنسيق مع قدرات داعمة وما يتصل بها من إمكانية التأثير او الإخلال على قدرات العدو، ذلك أن الفكرة الرئيسية لفهم حرب المعلومات هي أن أساسها المركزي هو استخدام المعلومات والبيانات كسلاح[43].

والحرب السيبرانية مفهوم معاصر جرى تداوله حديثاً منذ عام 1993 بعنوان: "حرب الانترنت قادمة" من قبل الباحث الاستراتيجي جون اركيلا الذي عد فيها حرب الانترنت، شكلاً من أشكال الحرب التي يتم بواسطتها تعطيل أو حتى تدمير المعلومات ونظم الاتصالات[44]؛ فهي بمثابة حرب لا تناظرية بحساب التكلفة المتدنية نسبياً للأدوات اللازمة لشنها تتصف بالسرعة والمرونة والمراوغة وفي بيئة مماثلة يتمتع فيها المهاجم بأفضلية على المدافع[45]، تجسد قمة التطور التي بلغته ثورة المعلومات وبوابتها الحاسبة الإلكترونية التي تشكل بدورها الأداة المحورية لهذا النوع من الحروب والميدان الرئيس لها وهي دائماً عرضة للتطور المستمر والتنوع والابتكار في تقنياتها ووسائلها لارتباطها الرأسي بقمتي الهرم التقني للحضارة الإنسانية، والمصالح الحيوية للدول[46].

غير أنه لا يمكن توصيف النزاع السيبراني بوصف الحرب إلا إذا كان مقروناً بنزاع مسلح تقليدي، أما الحرب الإلكترونية فليست الدول وحدها أطرافا فيها؛ لأن الهجومات السيبيرية قد تكون من قبل أفراد أو منظمات أو شبكات أو شركات كبرى وليست مرهونة بوجود نزاع مسلح ثنائي او متعدد الأطراف، مما يتطلب إدراك الضرورة القصوى إلى تعزيز الدفاعات السيبرانية الوطنية ، وإمتلاك أدوات القوة الإلكترونية وتعزيز الترسانة التكنولوجية حفاظا على الحدود والسيادة السيبرانية.

ثانيا - إستراتيجية الجزائر في تأمين حدودها السيبرانية وتحقيق الأمن السيبراني الوطني

ترتكز الإستراتيجية الوطنية في مواجهة التهديدات السيبرانية داخليا وخارجيا على سياسة تتحرك في المساحة بين تعزيز الأطر المؤسسية والوسائل اللوجستية من جهة، وتوفير البيئة التشريعة وهذا ما سيتم تناوله من خلال العنصرين التاليين

1 - على المستوى المؤسسي:راهنت الجزائر على غرار الكثير من البلدان على منظومة دفاعية وسياسة أمنية محكمة وشاملة يكون فيها الفاعل الرقمي مرتكزاً أساسياً ومحدداً للأمن القومي الوطني والإقليمي. حيث سارعت إلى مراجعة سياساتها الأمنية، وإدراجها لآليات وميكانيزمات جديدة تعني بهذه المسائل، بالموازاة مع تطوير البنايات الأساسية المتعلقة بتكنولوجيات الرقمية[47]، وفي هذا السياق لم يعد كافيا الاعتداد فقط بالمجالات الثلاثة المكونة للسيادة الوطنية (الإقليم البري والمجالين البحري والجوي)، ذلك أنه لا يمكن اعتبار السيادة كاملة دون السيطرة على المجال السيبراني الذي أصبح المحدد الأساس لما اصبح مصطلح عليه اليوم بالسيادة السيبرانية، بمعنى أن السيادة لا تكتمل دون أمن الفضاء السيبراني الوطني، حيث انتهجت الجزائر من خلال وزارة الدفاع الوطني إستراتيجية تعتمد تعزيز الدفاعات الإلكترونية الوطنية مرتكزة على نظام قانوني وبيئة تشريعية توفر الآليات الأساسية لحماية وتأمين المجال السيبراني الوطني معتمدة على التطور التقني في تكنولوجيا المعلومات والاتصالات،[48]، ويمكن اختزال السياسة الأمنية السيبرانية في الجزائر في شقها التقني في الجهود الآتية:

- القدرة على تصميم البرامج المعلوماتية وتطويرها.

- تنمية وتعزيز القدرات البشرية المكلفة بعمليات التحقيق في الجرائم الإلكترونية.
- توافر أحدث المعدات التكنولوجية في مجال الإعلام الآلي، الاتصالات اللاسلكية.
- التمتع بقاعدة بيانات واسعة محدثة باستمرار.
- ومن أهم المؤسسات الرسمية التي أنشئت لمواجهة الجريمة الإلكترونية وتتبع تهديدات السيبرانية ومكافحتها نذكر ما يلي:

- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والتي أنشئت بموجب المرسوم الرئاسي رقم 19-172 المؤرخ في 06 جوان 2019[49]، والذي حدد تشكيلة اللجنة وأهدافها ومهامها، والتي أعيد تنظيمها وتعزيز تشكيلتها بموجب المرسوم الرئاسي رقم 21- 439[50]، وهي هيئة يغلب عليها الجانب الإداري من جهة بدليل أنها مكونة من مجلس توجيهي ومديرية عامة تنشأ لدى رئاسة الجمهورية ومن جهة أخرى مازالت رهينة الرؤيا التقنية بوسائل مكافحة الجريمة الإلكترونية.
- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني.
- المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني.
- المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني.

2 - على مستوى المنظومة القانونية السيبرانية: لا تزال الجهود الوطنية الموجهة إلى توفير البيئة التشريعية الضرورية لتأمين المجال الوطني السيبراني غير كافية خصوصا على مستوى القوانين الجزائية المجرمة للأفعال التي تأخذ توصيف الجريمة السيبرانية، حيث لا تزال التشريعات تعتمد البعد التقني والفني في تحديد مدلول الجريمة الإلكترونية الذي يعتبر غالبا على فهم الخبراء الذين ارتكزوا على حماية المعطيات والبيانات الإلكترونية في تحديد هذا المفهوم، في حين مفهوم الجريمة السيبرانية أشمل وأوسع كما ذكرنا آنفا، وهو مرتبط بالابعاد التشريعية والسياسية والأمنية، ناهيك عما يمكن ملاحظته حول مستوى الكوادر الفنية والعلمية والقضائية ونوعية التكوين والخبرات الضرورية، وفي هذا الصدد نشير إلى استحداث قطب جزائي متعلق بمكافحة الجريمة الاقتصادية على مستوى الجزائر العاصمة من أهم مهامه التحقيق في الجرائم المعلوماتية وتتبع التهديدات في الفضاء السيبراني.

وفي هذا السياق اتجهت الجزائر في مستهل 2020 إلى وضع منظومة وطنية لامن الأنظمة المعلوماتية[51] تهدف إلى إرساء إطار تنظيمي لإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتنسيق تنفيذها؛ حيث ترتكز هذه الإستراتيجية على هيئتين أساسيتين هما: المجلس الوطني لامن الأنظمة المعلوماتية، ووكالة أمن الأنظمة المعلوماتية تعملان بالتنسيق المباشر مع رئيس الجمهورية وزير الدفاع الوطني، مما يبين العناية الفائقة للسلطة الجزائرية بسياسة الدفاع الوطني السيبراني.

وفيما يخص قانون العقوبات فقد تم تجريم كل مظاهر القرصنة والإرهاب السيبراني وكافة الجرائم التي يكون مجالها الفضاء المعلوماتي أو ترتكب بواسطة الأجهزة والأدوات التكنولوجيا، ففي قانون العقوبات مثلا المواد من 87 مكرر إلى 87 مكرر6 التي نصت على جرائم الانخراط والتحريض والتشجيع والمشاركة والتعاطف والدعم والتمويل والنشر لصالح الجماعات الإرهابية، في حين ضاعفت المواد (من 394 مكرر إلى 394 مكرر7 العقوبة حينما يتعلق الأمر باستهداف الدفاع الوطني او المؤسسات العمومية (أنظر ق.ع.ج 04-15 في 10 نوفمبر 2004 المعدل والمتمم)، مع أن هذه الأفعال عوقبت وجرمت بقطع النظر عن وسيلة ارتكابها، حيث إذا كان مجالها هو الفضاء السيبراني فإن الخسائر تكون أفدح والمخاطر تكون أكبر.

غير أن التعديل الذي أتى به القانون رقم 16-02 المؤرخ في 19 يونيو سنة 2016 المعدل لقانون العقوبات قد أضاف المادة 87 مكرر 11 التي تعاقب كل جزائري أو أجنبي يرتكب أفعال إرهابية (أو يدبرها أو يعد لها أو يشارك فيها أو يدرب عليها أو يتلقى تدريباً عليها) باستخدام تكنولوجيات الإعلام والاتصال.

الخاتمة:

في ختام هذه الدراسة حاولنا فيها رصد التحولات المفاهيمية في جملة من التصورات المرتبطة وظيفيا ومعرفيا بالأمن القومي ومرتكزاته في مقاربة تحليلية لمستوى التراكم المعرفي لظاهرة الجريمة السيبرانية وانعكاساتها السياسية والاقتصادية والأمنية والأدوات والآليات والإستراتيجيات الكفيلة بمواجهتها، وصولا إلى تحقيق الأمن الوطني السيبراني وتأمين الحدود السيبرانية للدولة وتعزيز دفاعاتها السيبرانية، حيث توصلنا إلى النتائج الآتية:

- أحدثت الثورة الرقمية تطورا شاملا وتغييرا واضحا في تناول بعض المفاهيم المتعلقة بالامن والجريمة والقوة والسيادة والصراع و الحرب يختلف تماما عن المفاهيم والأبعاد التقليدية.
- لم يعد من المسّلم به الحديث عن السيادة الوطنية دون تحقيق السيادة السيبرانية، وبعبارة أخرى لم يعد بسط الدولة نفوذها على المجال البحري والبري والجوي كافيا دون أمن المجال السيبراني، كبعد رابع من عناصر السيادة.
- لا تزال السياسة الوطنية في مجال الأمن والدفاع السيبراني رهينة رؤية تقنية وفنية بحتة، إنعكست على نوعية وكم التشريعات و حجم المنظومة القانونية السيبرانية.
- الجهود الوطنية الحقيقية تتميز في مجال مكافحة الجريمة السيبرانية بمركزية القرار وأحادية التصور وضبابية الرؤية، وهذا ما يفسره وجود وكالات وهيئات وطنية مركزية وتشريعات عقابية لا تخرج عن السياق العام لقانون العقوبات.

وعلى ضوء هذه النتائج يمكن تقديم المقترحات الآتية:

- تحديد مفهوم دقيق للأمن السيبراني وأبعاده ومرتكزاته وجعله محددا أساسيا في الأمن القومي الجزائري.
- تعزيز المنظومة القانونية السيبرانية بالنصوص التشريعية التنظيمية اللازمة والمناسبة والمرنة، بالقدر الذي يلغي مركزية الرؤيا ويفتح المجال أمام مشاركة الفاعلين، واستقطاب الكفاءات الفنية والخبرات الإدارية والأمنية لمواجهة الإجرام السيبراني في المنبع ومتابعته في المصب.
- تدريب الكوادر الفنية وتقديم التكوين اللازم لمختلف الجهات والمؤسسات والإدارات المكلفة بتتبع الجريمة السيبرانية من خلال تكوين الفنيين والقضاة والمحققين ومهندسي السيبرانية، وذلك بالاستفادة من الخبرة الأجنبية في هذا الشأن.
- التوعية بخطورة التهديدات السيبرانية داخليا وإقليميا، ورصد كافة الأخطار السيبرانية التي تتفاعل فيها الكيانات والأفراد وشبكات الجريمة المنظمة عبر الوطنية وحتى الدول.
- تحفيز الوعي الرسمي والشعبي بخطورة حروب "الجيل الخامس" الحروب السيبرانية وتعزيز التنسيق البيني والإقليمي والدولي لرصد الجرائم والمخاطر في الفضاء السيبراني المفتوح، والذي لا يعترف إلا بمن يملك القوة والدفاعات السيبرانية المتطورة.
- حشد كل الإمكانات المؤسسية والمالية واللوجيستية ورفع مستوى التسلح السيبراني في عصر تزايد فيه مستوى المخاطر والتهديدات الخارجية وتغير فيه مفهوم الحرب و السباق نحو التسلح.

الهوامش والمراجع:

(1) - مجلس وزراء العدل العرب بجامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية، الاتفاقية العربية لحماية الفضاء السيبراني بين الواقع والطموح، يومي 23-25 يوليو 2018، ص.07.

(2) - سمي هذا العالم المبهر والمفعم بالتكنولوجيا بمصطلح "الفضاء السيبريتي" (**Cyberespace**) من قبل مبدعه الكاتب الأمريكي المختص في علم الخيال "وليام غيبسن" الوارد في مؤلفه الذي يحمل عنوان"**New romancer**"، والمنشور عام 1984، ويطرح الكاتب"دوميتيك نورا" مصطلحا فرنسياً جديداً هو "العالم السيبريتي" (**Cybermonde**) في مؤلفه الصادر سنة 1995 تحت عنوان "المنافسين في العالم السيبريتي" (**Les conquérants du cyber mond**). وليدة حدادي، الفضاء السيبراني وأزمة القيم الأخلاقية في المجتمعات العربية – الشبكات الاجتماعية نموذجاً – *مجلة الحقيقة*، م.17، ع.04، (20 ديسمبر 2018)، ص ص.403-433.

(3) - نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني، التهديد المتصاعد لأمن الدول، *مجلة مركز بابل للدراسات الإنسانية*، م.8، ع.2، (2018)، ص ص.185-206.

(4) - اسماعيل قادير، إدارة الحروب النفسية في الفضاء الإلكتروني: إستراتيجية أمريكية الجديدة في الشرق الأوسط، أبحاث الندوة الدولية: عولمة الإعلام السياسي وتحديات الأمن القومي للدول النامية، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر3، 2019/02/12.

(5) - عباس بدران، *الحرب الإلكترونية -الاشتباك في عالم المعلومات-*، (بيروت: مركز دراسات الحكومة الإلكترونية، 2010)، ص.04.

(6)- يائير كوهين، *الفضاء الإلكتروني والبعد الخامس للحرب*، (القدس: 2012)، ص.22.

(7) - سيف نصرت الهرمزي، رصف المقاربات لمنظورات الفاعل الرقمي والانكشاف الاستراتيجي في ظل الفضاء السيبراني، *مجلة آداب الفراهيدي*، ع.37، (31 مارس 2019)، ص ص.382-406.

(8)- عبد المعطي زكي، الأمن القومي قراءة في المفهوم والأبعاد، المعهد المصري للدراسات السياسية والإستراتيجية، في:
https://eipss-eg.org/wp-content/uploads/2016/02/%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D9%82%D9%88%D9%85%D9%8A-%D9%82%D8%B1%D8%A7%D8%A1%D8%A9-%D9%81%D9%8A-%D8%A7%D9%84%D9%85%D9%81%D9%87%D9%88%D9%85-%D9%88%D8%A7%D9%84%D8%A3%D8%A8%D8%B9%D8%A7%D8%AF.pdf (2024/03/21).

(9) - جمال منصر، تحولات في مفهوم الأمن: من أمن الوسائل إلى أمن الأهداف، *مجلة دفاتر السياسة والقانون*، م.1، ع.1، (01 جانفي 2009)، ص ص. 139-125.

(10) - علاء عبد الحفيظ محمد، مفهوم الأمن القومي وتحديد أبعاده، المركز الأوربي لدراسات مكافحة الإرهاب والاستخبارات، في:
https://www.europarabct.com/%D9%85%D9%81%D9%87%D9%88%D9%85، (**2018/09/04**)

(11) - ذياب البداينة، *الأمن وحرب المعلومات*، (عمان: دار الشروق للنشر والتوزيع، ط1، 2006)، ص.21.

(12) - سونيا محمد البكري، *نظم المعلومات الإدارية (المفاهيم الأساسية)*، (القاهرة: الدار الجامعية، 2000)، ص.98.

(13) - ابراهيم سلطان، *نظم المعلومات الإدارية (مدخل إداري)*، (القاهرة: الدار الجامعية، 2000)، ص.41.

(14) - لابد أن نشير إلى ضرورة التميز بين المعلومات وبين التكنولوجيا وأدواتها، فالمعلومة هي ما ينتج عن معالجة البيانات والمعطيات بشكل معين تستخدم فيه التكنولوجيا، سواء للتجميع، أو للوصول، أو للتخزين والمعالجة.

(15) -رشا مصطفى أبو الغيط، *الحماية القانونية للكيانات المنطقية*، (الاسكندرية: دار الفكر الجامعي، 2003)، ص.05.

(16) - نجم عبد الله الحميدي، *نظم المعلومات الإدارية (مدخل معاصر)*، (عمان: دار وائل للنشر، ط1، 2005)، ص.265.

(17) - علوطي لمين، أثر تكنولوجيا المعلومات والاتصال على إدارة الموارد البشرية في المؤسسة، *مجلة علوم إنسانية*، م.01، ع38، (2008)، ص. 21.

(18) - حسن بن أحمد الشهري، نحو قانون دولي موحد لمكافحة الجرائم المعلوماتية، *مجلة دراسات وأبحاث*، م.01، ع.01، (15 سبتمبر 2009)، ص ص. 513-526.

(19) - منى الأشقر جبور، *السيبرانية "هاجس العصر"*، (القاهرة: المركز القانوني للبحوث القانونية والقضائية، 2018)، ص.25.

(20) - **Douwe Korff, CYBER SECURITY DEFINITIONS – a selection. P.01, in: *https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CPDP%202015%20-%20KORFF%20Handout.pdf,*** (02/12/2020).

(21) - **Richard A. Kemmerer, Cyber security, University of California Santa Barbara, Department of Computer Science, 2003, P.03.**

(22) - **Edward Amoroso, *Cyber Security*, (Silicon Press, USA, 2007), P.01.**

(23) – أميرة عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، *مجلة الشريعة والقانون*، ج3، ع.35، (2020)، ص ص.363-541.

(24) - جمال بوزيدة، لاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية "التحديات والآفاق المستقبلية"، *مجلة العلوم القانونية والسياسية*، م.10، ع.01، (28 أفريل 2019)، ص ص.1293-1262.

(25) - نبيل دريس، الجريمة السيبرانية بين المفاهيم والنصوص التشريعية- الجزائر أنموذجاً -، *مجلة القانون والمجتمع*، م.5، ع.2، (01 ديسمبر 2007)، ص ص. 20-40.

(26) – انظر القانون رقم: 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156، المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات، الجريدة الرسمية عدد71، مؤرخة في 10 نوفمبر 2004.

(27) - انظر القانون رقم: 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا لإعلام والاتصال و مكافحتها، المؤرخ في 05 أوت 2009، الجريدة الرسمية عدد 47، الصادرة بتاريخ 16 أوت 2009.

(28) - أنظر المادة 1 فقرة 8 من النظام السعودي لمكافحة جرائم المعلوماتية الصادر بموجب المرسوم الملكي رقم: م/17 بتاريخ 08 -03 - 1428.

(29) - أنظر المادة 01 فقرة 10، من القانون رقم 14 لسنة 2014م، الصادر بتاريخ 15-09-2014.

(30)- **Cameron S. D. Brown,"Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice", International Journal of Cyber Criminology. Vol.9, Issue.1,(January – June 2015), p.57.**

(31)- منى، *مرجع سابق*، ص.35.

(32) محمد مختار، هل يمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية، *مجلة اتجاهات الأحداث*، ع.6، (15جانفي2015)، ص ص.05،06.

(33) - منى لأشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، الندوة الأولى للمختصين في أمن وسلامة الفضاء السيبراني، بيروت، لبنان، 27 – 28 أغسطس 2012، ص.04.

(34) - نسرين فوزى اللواتي، التفاعل بين الانسان والحاسوب: التحدي الأكبر في العصر الرقمي، في: ***http://aitmag.ahram.org.eg/News/77860/***، (2020/04/19).

(35) - **DOROTHY E. DENNING,"Cyber terrorism", Global Dialogue, Autumn, 2000, p.01**

(36) - **Edward Amoroso, Cyber Security, *(Silicon Press,USA, 2007)*, p.01.**

(37) - يوسف بوغرارة، الأمن السيبراني: لإستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبري، *مجلة الدراسات لإفريقية وحوض النيل*، م.01، ع.03، (04 سبتمبر 2018)، ص ص. 100-119.

(38)- أميرة، *مرجع سابق*، ص.387،388.

(39) - جمال، *مرجع سابق*، ص 1266.

(40) - **Joseph S.Nye JR, Cyber Power, Harvard Kennedy School, 2010, p.03.**

(41) - إيهاب خليفة، القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت، في:

https://middle-east-online.com/%D8%A5%D9%8A%D9%87%D8%A7%D8%A8-، (2020/09/05).

(42) - موسى محمد آل طويرش، الصراع السيبراني: مفهومه وأثره في العلاقات الدولية، مؤتمر كلية العلوم السياسية، الجامعة المستنصرية، في:

https://uomustansiriyah.edu.iq/media/attachments/11/11_2019_04_16!10_41_58_AM.pdf، (30/05/2019).

(43)- شنوف زينب، الحرب السيبرانية في العصر الرقمي: حروب ما بعد كلاوزفيتش، *المجلة الجزائرية للأمن والتنمية*، م.9، ع.2، (01 جويلية 2020، ص ص.89-103.

(44) - سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي: رؤية مستقبلية، *مجلة رسالة الحقوق*، م.07، ع.02، (31 أوت 2015)، ص ص. 74-121.

(45) - أشرف السعيد أحمد، *القرصنة الإلكترونية*، (القاهرة: دار النهضة العربية، 2013)، ص ص.45-47.

(46) - علي عبد الرحمن العبودي، هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، *مجلة قضايا سياسية*، ع.57، (30 جوان 2019)، ص ص.89-118.

(47) - جمال رضوان، الأمن السيبراني: أولوية في استراتيجيات الدفاع، *مجلة الجيش*، ع.630، (جانفي 2016)، ص ص. 40،41.

(48) - سمير بارة، الأمن السيبراني في الجزائر: السياسات والمؤسسات، *المجلة الجزائرية للأمنالإنساني*، م.02، ع.02، (01 جويلية 2017)، ص ص.255-280.

(49) - يراجع المرسوم الرئاسي رقم 19-172 المؤرخ في 06 جوان 2019، الجريدة الرسمية، العدد 37، الصادرة بتاريخ 09 جوان 2019.

(50) - يراجع المرسوم الرئاسي رقم 21-439، المؤرخ في 7 نوفمبر 2021، الجريدة الرسمية، العدد 86، الصادرة بتاريخ 11 نوفمبر 2021.

(51) – يراجع المرسوم الرئاسي رقم: 20-05 المؤرخ في20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن المنظومة المعلوماتية، الجريدة الرسمية، العدد 04، الصادرة في 26 جانفي 2020، ص 05.

كيف يتم بناء موضوع الأمن من منظور مدرسة كوبنهاغن؟ الأمن السيبراني نموذجا

How is the issue of security constructed from the perspective of the Copenhagen School? cybersecurity a case study

نسيبة تامة(*) جامعة بومرداس N.tamma@univ-boumerdes.dz
عبد الحميد مشري جامعة بومرداس A.mecheri@univ-boumerdes.dz

ملخص:

تسعى هذه الورقة إلى تحليل الأمن السيبراني، وهو المفهوم الذي وضع على جدول أعمال ما بعد الحرب الباردة، كرد فعل على الابتكارات التكنولوجية والتغيرات الجيوسياسية. باعتماد الإطار النظري لمقاربة الأمننة، تجادل الورقة بأن الأمن السيبراني أصبح يشكل قطاع مهم ينبثق عنه مجموعة من التهديدات لارتباطه الوثيق بأمن الدولة، المجتمع والاقتصاد. كما تهدف هذه الورقة إلى مناقشة أهمية السمات الخطابية للأمن السيبراني، باستخدام مفاهيم مقاربة الأمننة عن طريق تحليل دور الدولة والفواعل غير الحكومية في إدارة الخطابات الأمنية السيبرانية.

الكلمات المفتاحية: الأمننة؛ سياسة الأمن السيبراني؛ استراتيجيات الأمن السيبراني؛ التهديدات الرقمية؛ الأمن الدولي.

Abstract:

This paper seeks to analyze cybersecurity, a concept that emerged on the agenda after the Cold War, in response to technological innovations and geopolitical changes. Adopting the theoretical framework of securitization approach, the paper argues that cybersecurity has become an important sector giving rise to a range of threats closely linked to national, societal, and economic security. Furthermore, this paper aims to discuss the significance of discursive features of cybersecurity, using concepts from the securitization approach, and analyzing the role of both state and non-state actors in managing cybersecurity discourses.

Key Words: Securitization; Cybersecurity Policy; Cybersecurity Strategies; Digital Threats; International Security

مقدمة:

تعتبر نظرية الأمننة واحدة من الأدوات التحليلية الأكثر جاذبية في الدراسات الأمنية الهامة في كل من الأبعاد التقليدية والرقمية. إن ما يجعل سمات الخطاب السيبراني ذات صلة هي أهميته السياسية. لقد أصبح إنشاء مذاهب واستراتيجيات سيبرانية جديدة الآن هو القاعدة وليس الاستثناء، مما يجعل عملية تحديد مفهوم الفضاء السيبراني ذات صلة. إن مفاهيم القوة والهيمنة والسيطرة هي جزء لا يتجزأ من الخطاب السيبراني. تهدف هذه الورقة إلى سد فجوة في مجال أمننة الأمن السيبراني الذي لم يتم بحثه بشكل كافٍ حتى الآن.

يمكن القول، إن قلة التحليلات البحثية ضمن الأدبيات يرجع جزئيا إلى التطور السريع للتكنولوجيا السيبرانية التي لم تظهر آثارها بشكل فوري، كما أن تأثيرها على الحياة السياسية أو الاقتصادية أو الاجتماعية غير واضحة المعالم. بناء عليه، تهدف هذه الورقة إلى تقييم مساهمة نظرية الأمننة في فهم قضايا السياسة الأمنية التقليدية والمعاصرة. على وجه الخصوص، تعتبر محاولة للبحث في التحديات التي تواجه الدولة في القرن الحادي والعشرين.

لذلك تسعى الورقة إلى تحليل عملية صنع القرار في السلطة من خلال التركيز على أحد العناصر الأساسية في نظرية الأمننة وهي الظروف التي تؤثر على كيفية إدراك التهديدات وعلى أساسها يتم تنفيذ عمليات التدخل الحكومي الأمنية السيبرانية. وعليه، تقدم هذه المقاربة فهم خاص للأمن (متأثر بنظرية أفعال الكلام) مع تحليل خطاب السلطة. لهذا السبب، يصبح "الأمن" فعلاً خطابياً محدداً يمكن أن ينجح في ظل ظروف معينة، أي في المواقف التي "يستخدم فيها الفاعل الأمني خطاب التهديد الوجودي وبالتالي يكون له اثار سياسية كبيرة". وبالتالي، فإن الفكرة الأساسية للامننة التي ستركز عليها هذه الورقة هي إعطاء القضية وزناً كافياً لكسب موافقة الجمهور، وهو ما يمكن السلطة من استخدام أي وسيلة تراها مناسبة. بمعنى آخر، تجمع عملية الأمننة بين سياسة تصميم التهديد وسياسة إدارة التهديد. على هذا النحو، يمكن طرح التساؤلات التالية: ما هي القضايا التي يتم بناؤها كتهديد في خطابات وممارسات الأمن السيبراني؟ ومن قبل أي الجهات؟ وما هي الجماهير المستهدفة؟

المحور الأول: الأمننة والفعل الخطابي

إن نقطة البداية في مفهوم الأمننة securitization هي نظرية الفعل الخطابي، أي كيف يمكن القيام بأفعال بالكلمات. فالأمننة تهتم بالكيفية التي ينقل بها الخطاب موضوعا ما ويقدمه بوصفه تهديداً وجودياً، بحيث يتقبلها الجمهور ويسمح باستخدام لإجراءات لاستثنائية لمحاربة هذا التهديد.[1] ويرى "باري بوزان" (Barry Buzan) أن إضفاء الطابع الأمني على مجال معين يكون عبر عملية خطابية لغوية، إذ يعمل هذا الخطاب على الاستدلال بوجود تهديد يمس البقاء (المادي أو المعنوي) لمرجعية أمنية ما، قد تكون الفرد أو الجماعة أو الدولة أو الهوية. وتهدف عملية إضفاء الطابع الأمني على قضية ما إلى تشريع لجوء القائمين على رسم السياسة العامة لانتهاج ترتيبات استثنائية الغاية منها تأمين الكيان "المرجعية" محل التهديد من المخاطر المحدقة به. إذ يمكن التعامل معها بحرية أكثر، بعيداً عن الضغوط والقيود التي تمارسها الضوابط الديمقراطية لصناعة القرار، لاسيّما ما يرافقها من ضغط لمنظمات المجتمع المدني.[2]

تشير مدرسة كوبنهاغن إلى ان الأمننة تتشكل أثناء الكلام، أي أن معنى الامن يُمنح من خلال الفعل الخطابي الذي يكشف عن هياكل السلطة وتكوينها. هذا الفعل الخطابي ليس مجرد تعبير عن تهديدات محتملة، بل يمكن أن يكون أيضاً تجسيداً لمحاولة الهيمنة أو تشكيل الصورة الذاتية. كما يوضح اولي ويفر اننا ندرك مشكلة معينة كتهديد ليس لأن هناك تهديداً فعلياً، بل لان المشكلة قد تم تقديمها لنا كتهديد.[3] نتيجة لذلك، تنشأ عدة أسئلة:

ما هي طبيعة ومعايير قبول الجمهور لقرارات الحكومة؟

هل يمكن ان تنطبق النظرية على جمهور سياسي متنوع؟

ما هي أنواع قبول الجمهور؟

هل يعتمد تقديم الامن على هيمنة عقيدة سياسية معينة في وقت معين؟

هل تتحدد وجهات النظر المحددة لصانعي السياسات بالسياق التاريخي والخبرة السياسية؟

لفهم هذه الأسئلة، يجب أولاً وصف مفهوم "الثقافة الأمنية"، والذي يتبين انه من محوري للامننة، حيث أن أحد الافتراضات الرئيسية لهذه النظرية هو أنها عملية بينية تعتمد على قبول الجمهور. فهم ظاهرة الثقافة الأمنية ضروري لاخذ الجوانب الاجتماعية والثقافية والأخلاقية لكل بلد في الاعتبار. كما أنه مهم لتحليل العوامل التي تعتمد عليها نجاحات تهميش التهديد. بمعنى آخر، لا توجد ثقافة أمنية لا تعكس السلوكيات والاتجاهات والقيم الاجتماعية.

لقد حدد بوزان شروط نجاح "الفعل الخطابي الأمني" المستلهمة من أفكار "جون أوستن" (John Austin) التي اعتبرت إسهاماته أرضية لمفكري (مدرسة كوبنهاجن) لاستنباط الشروط التسهيلية للفعل الأمني المتمثلة في:

- الطلب الداخلي للفعل الخطابي لمتابعة قواعد الأمن وبناء مقاومة التهديد الوجودي.
- الفواعل الأمنية التي يجب أن تكون في موقع السلطة.
- ارتباط الشروط من الناحية التاريخية للتهديد (تخزين المشاعر العدائية).

وميز بوزان بين شرطين لنجاح الفعل الخطابي:

- الشرط الداخلي: قاعدي لغوي.
- الشرط الخارجي: سياق اجتماعي.

الأول أكثر أهمية بالنسبة للفعل الخطابي لاتباع شكل وقواعد الأمن والبناء المتضمن لتهديد وجودي، أما الثاني فيضم حسب المفكرين شرطان مركزيان: الأول هو موقع سلطة الفواعل الأمنية والثاني يتمثل في التهديدات المزعوم التي يمكن أن تسهل او تعرقل عملية الأمننة.[4]

الإطار التحليلي يضم ثلاث طبقات اساسية لقوة الأمننة:

- قوة أداء performative نصوص التهديد الموضوعية.
- التعمق في إيجاد الخطابات الأمنية.
- القوة الموقعية للفواعل الذين يؤثرون على عملية الأمننة (سلطة الفواعل الأمنية)[5].

إلى جانب ما سبق، يرى ويفر أنه بدون جمهور يقبل المشكلة كمسألة أمنية، لا يمكن ان تكون هناك مشكلة أمنية مأمنة. حيث يجب أن يقبل الجمهور هذه الرسالة، وليس بالضرورة في استفتاء، ولكن أيضا القبول الضمني لاستخدام وسائل لا تستخدم عادة. وموافقتهم تمنح الفاعلين الأمنيين الحق في استخدام أي وسيلة لضمان بقاء الكائن المرجعي. لذا، فإن نجاح الامننة يعتمد بشكل كبير على استجابة الجمهور وقبولهم للقضية كتهديد حقيقي، وهذا القبول يمنح الفاعلين الأمنيين الصلاحية لاتخاذ تدابير استثنائية لضمان الأمن.[6]

المحور الثاني: الأمن السيبراني كتحد بحثي في الدراسات الأمنية.

تفرض التطورات الأخيرة نحو الرقمنة بذل المزيد من الجهود فيما يتعلق بأمن الفضاء الرقمي. ويتجلى ذلك في العدد المتزايد من الدراسات التي تطبق نظرية الأمننة على الفضاء الرقمي، ومن المرجح أن يزداد الاهتمام بهذا الموضوع بين الباحثين وكذلك مراقبي السياسات الأمنية. وتنبع أهمية هذا المجال من اتجاهين مترابطين.

أولاً، تعتمد الدول والمجتمعات والأعمال التجارية بشكل متزايد على البيانات والأنظمة والتقنيات القائمة على الفضاء الرقمي. وهذا يوفر أرضًا خصبة للعديد من الجهات من اجل تطوير أمننة تحدد التهديدات المختلفة.

ثانيًا، يتماشى الانشغال بالفضاء الرقمي مع المحاولات الرامية إلى البحث عن تهديدات جديدة التي تحدث بين الأمنيين والبيروقراطيات منذ نهاية الحرب الباردة. في أطروحته حول مجتمع المخاطر، يفترض أولريش بيك أننا نعيش الآن في "حداثة ثانية". تتميز هذه الفترة من الحداثة الانعكاسية بالقوة المهيمنة للأخطار غير المعروفة وغير القابلة للسيطرة والتي تتجاوز الحدود الزمانية والمكانية. على هذا النحو، يتبنى الفاعلون هذا الخطاب عند بناء التهديدات السيبرانية.[7]

وعليه، يعني الأمننة للفضاء السيبراني جعله قضية أمن قومي. أي تقوم الدول بفرض سيطرتها على الفضاء السيبراني لضمان أن المحتوى فيه يتناسب مع مصالحها السياسية الداخلية والخارجية. في هذا السياق، تركز معظم

الادبيات حول الامن السيبراني على التهديدات دون دعم نظري كاف. لذا تأتي أهمية نظرية الأمننة التي تفيد في فحص الخطابات والممارسات الأمنية السيبرانية.[8]

ومع ذلك، لا تزال الأدبيات التي تناولت موضوع أمننة الأمن السيبراني محدودة للغاية من حيث تعاملها مع تعقيد الفضاء السيبراني. يتضح هذا في التحليلات التي تركز على الخطابات الرسمية التي أنشأها وطورها الفاعلين الحكوميين. وبالتالي، لا تفيد كثيراً هذه المقاربة في فهم الطبيعة المتعددة الأطراف للفضاء السيبراني، كما لا يعكس تنوع الخطابات الأمنية السيبرانية، بل يركز فقط على الخطابات العسكرية والجيوسياسية التي يتبناها صناع القرار والتي تعزز تصورات الواقع وفقاً لمنطق الصديق مقابل العدو.

لذلك، من الجدير توضيح بعض المعضلات التي ظهرت مع النقاش حول التهديدات الأمنية السيبرانية الناشئة، منذ نهاية الحرب العالمية الثانية، طورت الدراسات الاستراتيجية إطاراً نظرياً واسعاً يعتمد على تكنولوجيا الأسلحة النووية الجديدة، وتكنولوجيا الاتصالات والتصنيع. لذا، اصبح الأمن السيبراني يتطلب تحليلاً بهذا الفضاء والتي تؤثر بشكل كبير على استراتيجية الدفاع الوطني والاستقرار الدولي.[9] إن ما يجعل أمننة الفضاء السيبراني مسألة ذات تعقيد متزايد كون أن سياسات الأمن السيبراني تواجه نطاقاً واسعاً ومتنوعاً، بدءاً من السياسات الدولية والإقليمية والوطنية وصولاً إلى أصغر الكيانات العامة والخاصة. وعليه، تأتي جهود الدول مع التحديات الرقمية والتهديدات السيبرانية ليست مجرد مسألة أمنية، بل ترتبط ايضاً بالتكنولوجيا والاقتصاد والمجتمع.

بشكل عام، تعد سياسة الأمن السيبراني أساساً لاستراتيجية ومجموعة من القواعد والمتطلبات والتعليمات الخاصة بالصناعة التي تحمي البنية التحتية السيبرانية وتشكل السلوك في استخدام الموارد المعلوماتية. وكقاعدة عامة، يتم تطوير السياسات بواسطة خبراء تقنيين من خلال التحليل والتوثيق والدعم الذي يمثل الاتجاه المقترح والمختار اللازم للتأثير على عملية القيادة والسيطرة مع مراعاة المخاطر الأمنية. وعليه، لم تعد التهديدات السيبرانية تُوصف بأنها مشكلة أمنية ناشئة، بل أصبحت تمارس بالفعل تأثيراً كبيراً، وأحياناً على الوضع السياسي الدولي. أصبحت التهديدات السيبرانية معقدة للغاية تمثل تهديد مباشر للاستقرار في العديد من الدول والنظام الدولي ككل. وبالتالي، تتطلب الأمننة السيبرانية جهداً متعدد التخصصات، حيث تقع عند تقاطع العديد من المجالات والقطاعات. كما أن الأسس التقنية للأمن السيبراني، على سبيل المثال، تتطلب من الباحثين في العلاقات الدولية اكتساب فهم للأساليب التقنية الرئيسية، وعلى العكس، يحتاج علماء الحاسوب إلى ان يكونوا أكثر وعياً بالمجال المسيس الذي يصممون فيه التطبيقات وكيف تؤثر قراراتهم على العلاقة بين الأمن الحرية.

في هذا السياق، أصبحت التهديدات الدولية التقليدية تفسح المجال أمام تهديد الشبكات اللامركزية من جهات فاعلة من غير الدول.

على عكس العوامل التقليدية مثل حجم القوات العسكرية، والاقتصادات القائمة على الناتج المحلي الإجمالي، وعدد السكان أو الحجم الجغرافي.[10] فإن القدرات السيبرانية أكثر صعوبة في القياس. لذلك، منذ عام 2007، أنشات 15 دولة أوامر سيبرانية أو وحدات عسكرية مخصصة تركز على الدفاع السيبراني والقدرات الهجومية.

في عام 2007، كان الإنفاق الحكومي على الأمن السيبراني اقل من 10 مليار دولار على المستوى العالمي، وبحلول عام 2021، تجاوز الإنفاق 50 مليار دولار.[11] في الواقع، كل دولة ذات أهمية استراتيجية تقوم بزيادة ميزانية الامن السيبراني، وهو ما يعني تأثير الامن السيبراني على الديناميكيات الإستراتيجية للنظام الدولي وعلى الامن الداخلي لبعض الدول، مما يعكس ويعزز زيادة الأولوية التي تولها الدول للعمليات السيبرانية. في السياق نفسه، في حالة القدرات السيبرانية، يعد الوعي بقدرات الخصم جزءاً مهماً من الكفاءة الدفاعية العامة. وبالتالي، قد يتم إعادة

تعريف نماذج التحالفات السياسية والعسكرية من أجل تكييفها مع الوضع الذي يتم فيه أخذ المنافسة السيبرانية بين الحلفاء في الاعتبار.

يشير العدد الكبير من الفاعلين العاملين في الفضاء السيبراني إلى أن البعد السيبراني في العلاقات الدولية أصبح يتسم بتحديات كبيرة ويكون عرضة لتغييرات معقدة وغير متوقعة. وبالتالي، فإن تصرفات الدول وردودها تؤثر على بعضها البعض وعلى طبيعة التهديدات المتغيرة في نفس الوقت. لقد أثرت تصورات التهديدات السيبرانية على عملية السياسة الخارجية. فالخطاب السيبراني ينبع من جهات فاعلة محلية، لذا فمن الضروري على نحو متزايد متابعة هذه العملية على مستوى السياسة الدولية. كما أن الدول التي تتمتع بمستوى أعلى من تطور التكنولوجيا السيبرانية تميل إلى ان تكون لها مكانة دولية اعلى، بالمقابل تكون أكثر تعرضاً للتهديدات السيبرانية او الحروب السيبرانية، وبالتالي تمتلك خبرة اكبر في كيفية صد الهجمات السيبرانية والتعامل مع المشكلات الرقمية. بنفس الطريقة، الدولة التي تعرضت سابقاً لهجمات سيبرانية ستكون أكثر كفاءة في عملية الأمننة. تجد هذه الدول أيضاً أنه من السهل بكثير الحصول على الدعم الدولي والقيام بتحالفات للقيام بإجراءات انتقامية مخططة. على سبيل المثال، الهجمات الرقمية التي نفذت في عام 2007 نحو البنية التحتية لإستونيا. حيث حصلت الحكومة على دعم حلفاء الناتو والاتحاد الأوروبي. ومع ذلك، من غير المؤكد ما إذا كانت إستونيا لوحدها كانت ستنجح في امننة الحدث دولياً؛ وبالتأكيد ساعد عضويتها في الناتو على تسليط الضوء نحو مخاوف الأمن القومي للدول الصغيرة. وبالتالي، يمكن للمنظمات غير الحكومية والقادة، وبعض المؤسسات الدولية أن تحل محل صانعي السياسات أو تشارك في عملية الأمننة على الساحة الدولية. على سبيل المثال، يمكن للأمم المتحدة القيام بالأمننة من خلال تحديد مشكلة معينة على أنها تهديد للسلم والأمن الدوليين.

بالإضافة إلى ذلك، تلعب وسائل الإعلام دوراً مهماً كمنصة لأداء الأفعال الخطابية، سواء في الأمننة المحلية أو الدولية. حيثما تكون وسائل الإعلام خاضعة لسيطرة الدولة، يرى الجمهور عادة ما تريد الحكومة ان يروه، وبالتالي ما يخدم صناع القرار في تحقيق هدفهم الأمني. من ناحية أخرى، لا تهتم وسائل الإعلام الدولية بدولة واحدة فقط وعادة ما تكون وسائل الإعلام خاصة. يلعب تاثيرها دوراً مهماً في عملية الأمننة، من خلال تحديد الأولويات، ووضع الاجندة، وتحديد الحلول، وتوفير منصة للقادة لأداء أفعالهم الخطابية على الساحة الدولية.[12]

علاوة على ذلك، من التحديات الرئيسية الغامضة التي يواجهها صناع السياسات والباحثون في مجال الأمن السيبراني الدولي وجود آلية موثوقة لنسب الحوادث السيبرانية. إن المعرفة في هذا المجال ضرورية لتطوير القانون الدولي من أجل تحديد مسؤولية الدول عن اعمال العدوان التي ترتكب في الفضاء السيبراني. وبالتالي، تتميز سياسة الأمن السيبراني بمستوى عال من التفاوت الأمر الذي يجعل استراتيجيات الدفاع المعتمدة قديمة.

وعلى عكس الأسلحة العسكرية، لا يمكن ملاحظة أدوات الهجوم السيبراني وتحديد كميتها، وفي معظم الحالات، لا يمكن التعرف عليها قبل الهجوم الفعلي.[13] وفي السنوات الأخيرة، أصبح الخط الفاصل بين العلميات السيبرانية الهجومية والدفاعية غير واضح أيضاً.

المحور الثالث: التهديدات السيبرانية كعامل ممكن للأمننة.

يتم تقديم القضية التي يتم تأمينها على انها وجودية، وعلى الرغم من أنها قد تكون حقيقية أو غير حقيقية، يجب أن يتم بناؤها وتقديمها بطريقة معينة. يشير النقاش العام حول التهديدات السيبرانية إلى الفجوة الحالية بين الأهمية المتزايدة للتهديدات السيبرانية ونقص الأحداث التي تبرر هذه المكانة المرتفعة.[14]

يجادل بعض الباحثين بأن الاستخدام المفرط للإجراءات الاستثنائية المصاحبة للتهديدات السيبرانية يثير تساؤلات حول معنى الامننة. إن الاتجاه نحو زيادة الأمننة في مجال التهديدات السيبرانية هو بشكل كبير نتيجة لتطبيق التفكير العسكري التقليدي. تتشابه مصادر خطاب الأمننة في طبيعتها مع تلك الدوافع التي تتعامل مع الفضاء السيبراني كمجال مشابه للمجال العسكري. يأخذ خطاب الأمننة الفضاء السيبراني كمجال للحرب ويطبق منظوراً عسكرياً على تحليل التهديدات الناشئة منه، لذا يمكن لمراقبي أمننة الفضاء السيبراني استخدام نفس المنطق الذي طورته الدراسات الاستراتيجية خلال الحرب الباردة للمجالات الأخرى، وهو ما يعتبر مشكلة رئيسية، لأن تقييم التهديد لا يستند إلى تحليل نقدي لعواقب الهجمات السيبرانية أو التطورات التكنولوجية او التدابير الدفاعية المحتملة، بل يستند إلى تصور خيالي لما يمكن أن يحدث إذا لم تكن الحكومات مستعدة، كما حدث خلال الهجمات الإرهابية في 11 سبتمبر 2001.[15]

في العصر الحالي شهد العالم ترابط اقتصادي وسياسي لم يسبق له مثيل، وبالتالي من المتوقع اتباع نهج مختلف في استراتيجيات الدول الراغبة في التأثير على النظام السياسي العالمي بدلاً من الهجوم السيبراني الذي يتبعه عواقب مادية كبيرة. ففي عام 2010، تم استخدام فيروس ستكسنت الذي هاجم أجهزة الطرد المركزي النووية وعطل برنامج إيران النووي، مما أدى إلى توقفه لعدة سنوات.[16] في هذا السياق، لتنفيذ عملية دقيقة وسرية كهذه يتطلب عملية استخباراتية مسبقة لضمان النجاح، خاصة عندما يكون أي سلاح سيبراني سيفاً ذا حدين يمكن استخدامه ضد المهاجم في الانتقام. هناك أيضاً مسألة من كان بالفعل وراء الهجوم؟ وهو الامر الذي يعتبر غير واضحاً بسبب عدم معرفة المسؤول في الفضاء السيبراني، مما يزيد من صعوبة تحديد أصل المهاجم.

تعتبر الهجمات السيبرانية خطيرة بطبيعتها، إلا أن خطاب التهديد السيبراني لا يزال في الغالب ضمن مجال خيال القادة، ونفس الشيء ينطبق على الحرب السيبرانية حيث لم تحدث حتى الآن حرب سيبرانية لكنها تنتمي في المقام الأول إلى مجال ما يمكن أن يحدث. مثال على هذا الموقف الأمني هو التصريحات التي تبلغ علناً عن احتمالية وقوع حرب سيبرانية، مما يؤكد على عدم القدرة على التنبؤ والعواقب الكارثية.[17]

غير ذلك، معظم الهجمات السيبرانية التي تعتبر الأكثر خطورة في التاريخ، لم تكن تهديدات وجودية من الناحية التقنية. إن سرقة المعلومات العسكرية أو التجارية أو الشخصية لا يمكن ان تؤثر على بقاء الدولة أو القطاع الخاص أو أي فرد. وبالمثل، فإن حرمان العملاء من خدمة معينة لا يمكن أن يهدد الوجود الفعلي للدولة او الأفراد. لذا، فإذا كان الفضاء السيبراني يشكل بالفعل تهديداً هو أمر غير مهم بقدر ما يعتبر الفعل الخطابي الذي يبني صورة التهديد. وبالتالي، فإن استخدام لغة "نهاية العالم" ينشر حالة عدم اليقين والخوف والشك. ويثير عدة أسئلة: لماذا يستخدم صناع القرار لغة الهلاك هذه؟ هل استخدام هذه اللغة يشكل سيناريو لتهديد سيبراني؟ لماذا يعتبر بناء فضاء الأمن السيبراني كتهديد؟

في هذا السياق، تقدم نظرية الأمننة تفسيراً حول هذه القضايا، حيث تعتبر الامننة جزء من سياسة الأمن السيبراني. فالأمننة الناجحة تبرر إعطاء الأولوية لقضايا محددة على حساب ظواهر أو عمليات أخرى. فعندما يتم تقديم قضية ما بنجاح كتهديد وجودي للأمن، فإن هذا يبرر اتخاذ تدابير سياسية استثنائية.[18]

ومع ذلك، تظهر أسئلة هامة حول من هو المعني بتفسير وتحديد التهديدات. وهنا يكون بعض الفاعلين ذوو أهمية في تصنيف القضايا الأمن من غيرهم. وهذا يعتمد على مصداقيتهم وحقهم في التحدث إلى الجمهور المناسب. يحتاج فاعل الأمننة إلى رأس ما اجتماعي وسياسي كاف لإقناع الجمهور بوجود تهديد وجودي. في الوقت الحالي، تنبثق هذه السياسات من فاعلين للأمن السيبراني: الجهات الفاعلة في أمن الدولة والجهات الفاعلة في الأمن السيبراني. في هذا

السياق، تعتبر بعض القضايا أسهل في الأمننة من غيرها نظراً لارتباطها التاريخي بالعنف الوجودي. لذا، تعتبر قضايا الأمن السيبراني أكثر صعوبة في عملية الامننة، لأنها لا تعتمد على تاريخ حقيقي من العنف مثل القوات التقليدية التي تعتمد على خبرتها في النزاعات المسلحة.

إن مناقشة الحرب السيبرانية تعتبر جزء من سلسلة خطابية تمهد الطريق للعنف في الفضاء السيبراني. وهذه الديناميكية التي يتم من خلالها بناء لغة التصورات وتؤثر على الارتباطات السياسية التي تدعم نظرية الامننة. تعتبر الحرب تقليدياً مجالاً للمؤسسات العسكرية، وتشمل الاستجابات استخدام القوة. لذلك، فإن استخدام مصطلح "الحرب" هو استعارة تشير إلى اوصاف لغوية أكثر شيوعاً للنزاعات. إن مفهوم "حرب المعلومات" هو خطوة مماثلة لإضفاء الطابع الأمني على مشكلة تحمل في طياتها نوعاً معيناً من سياسات الأزمة التي تكون فيها ابعاد مثل المكان والزمان محدودة وتؤدي إلى طريقة تفكير عسكرية.[19] في هذا السياق، يتم تقديم التهديد السيبراني كتهديد وجودي يبرر اتخاذ تدابير وعسكرية استثنائية. استخدام لغة الحرب والاستعارات العسكرية يعزز من صورة التهديد ويؤثر على كيفية فهم الجمهور والسياسيين له، مما يؤدي إلى سياسات ترتكز على العسكرة والاستعداد لمواجهات سيبرانية محتملة.

يمكن القول، إن الامننة هي عملية يتم من خلالها تعريف قضية معينة كتهديد أمني من قبل فاعل الأمننة، ويصبح الجمهور مقتنعاً بأهمية هذه القضية كتهديد وجودي يتطلب إجراءات طارئة. في هذا السياق، لا تكون القضية مشكلة أمنية بحد ذاتها، ولكن الفاعل الأمني يمنحها هذه الصفة بناء على تصور امني معين. وفقاً لوليامز، في نظرية الامننة، يتم التعامل مع الأمن ليس كشرط موضوعي، بل كنتيجة لعملية اجتماعية معينة.[20] وهذا يعني أن ما يعتبر ممارسة أمنية في فترة زمنية أو موقع معين لا يعد بالضرورة ممارسة أمنية بنفس الطريقة في فترة زمنية ومنطقة أخرى. كما أنه في التحليل الأمني، يكمن جزء من المشكلة في تحديد نقطة البداية. فالقضية التي تعبر مهمة أمنياً لدولة معينة قد لا تكون بنفس الأهمية لدولة أخرى. بمعنى آخر، بينما قد يهيمن القطاع العسكري على المشهد الأمني في دولة ما، قد تكون قضية البحث والتطوير الرقمي والابتكار الاقتصادي أولوية في دول أخرى وتحدد تصورات صانعي السياسات للامن. يمكن تفسير التهديدات الوجودية بطرق مختلفة، مما يتطلب مجموعات مختلفة من الإجراءات الطارئة واستجابات مختلفة من المنظمات العامة والخاصة.[21]

علاوة على ذلك، إن إنشاء برنامج للأمن التقليدي أو السيبراني يثير عدداً من القضايا تخضع لخصوصية كل دولة. بالإضافة إلى التصورات الفردية للتهديدات، حيث تتمتع كل دولة بثقافة أمنية فردية، تتحدد بالعوامل الاجتماعية والتاريخية والقانونية الخاصة بها. وبالتالي، تختلف كل دولة في طريقة تبنيها للابتكارات وتظهر أنماط سلوك مختلفة عند استخدام روابط نظم المعلومات.[22]

يتماشى هذا الموقف مع منظور البحث الذي تمت صياغته ضمن مدرسة كوبنهاغن. الفكرة الرئيسية هي الجمع بين النظرية اللغوية ونظرية الامن لإنشاء تفسير نقدي خطابي للأمن. ضمن الأدبيات، غالباً ما تثار تساؤلات حول ما إذا كانت الأمننة تتحقق من خلال الفعل الخطابي ذاته أو كعملية اجتماعية؟ تأتي مشروعية هذا السؤال من الاعتبارات غير المكتملة حول ما إذا كان الفعل الخطابي ينبغي اعتباره ظاهرة عالمية أو سياقية.[23] وعليه، يؤكد منظرو الأمننة على أنه يجب أخذ الوضع برمته في الاعتبار إذا أراد المرء أن يدرك التشابه بين العبارات الفردية والعملية بين الفعل الخطابي والواقع السياسي المبني. وفي سياق الأمن السيبراني تبرز أهمية الفعل الخطابي وكيفية بناء التهديدات الوجودية من خلال اللغة والتصورات الاجتماعية، مما يبرر اتخاذ إجراءات طارئة ويعزز دعم الجمهور بهذه الإجراءات في مواجهة التهديدات السيبرانية. وبالتالي، يجب النظر إليها من الناحية السياسية على أنها تهديد للدولة

ومصالح المواطنين. على الرغم من التوافق العام بين الحكومات على مصطلحات الأمن والأمن السيبراني، فإن هناك تفاوتًا في تحقيق استقرار الدولة. يُظهر تقديم حلول دفاع سيبراني مماثل إمكانية تحقيق نتائج مختلفة، مما يبرز تعقيد العوامل التي تؤثر على نتائج استراتيجية الأمن السيبراني الفعالة. وأحد التفسيرات لهذه الظاهرة هو الثقافة الأمنية، التي تعتمد على الخصائص المحدد للمجتمعات، بحيث يتم تبني قيم معينة بشكل فردي ثم تترجم إلى سلوك. هذا العنصر يثبت أنه جانب أساسي لفهم الظروف التي تؤثر على نجاح تنفيذ استراتيجيات الأمن السيبراني في البيئة الدولية. وعليه، إن فهم الثقافة الأمنية كجزء لا يتجزأ من الامننة يبرز أهمية الفعل الخطابي في تشكيل وتفسير التهديدات الأمنية. من خلال تحليل الثقافة الأمنية، يمكننا فهم كيف تختلف الدول في تبني وتنفيذ استراتيجيات الأمن السيبراني، وكيفية تأثير السياق الاجتماعي والثقافي والسياسي على نجاح هذه الاستراتيجيات. يعتبر هذا الفهم حاسماً لتطوير سياسات أمن سيبراني فعالة تتماشى مع خصائص كل مجتمع ودولة.

علاوة على ذلك، لعدة سنوات، كانت الحماية التقنية تمثل العنصر الأساسي في الأبحاث والتمويل والتطوير في مجال الأمن السيبراني، بينما لعب التعليم في هذا المجال دوراً ثانوياً. ومع مرور الوقت، اثبتت التهديدات السيبرانية أن الأمن السيبراني يحتاج إلى تضمين ثقافة الأمن السيبراني كمرجع أساسي. في هذا السياق، أعرب الاتحاد الدولي للاتصالات عن موقف مماثل، حيث اعتبر ان الأمن السيبراني يتطلب تطوير ثقافة الأمن السيبراني وسلوك المستخدم المقبول في الواقع الرقمي الجديد.[24]

الخاتمة:

سعت هذه الورقة إلى استخدام فكرة "الأمننة" التي طرحتها مدرسة كوبنهاغن لفحص خصوصيات بناء الخطاب العام حول الأمن السيبراني. من خلال مناقشة منطق التهديدات ونقاط الضعف في بناء التهديدات السيبرانية، مما يبرر الحاجة إلى تعزيز الإجراءات الأمنية وإدخال تدابير استثنائية، وبالتالي يصبح من الممكن إضفاء الشرعية على الأدوات الاستثنائية التي تستخدمها السلطة. لقد حاولت الورقة التأكيد على الطبيعة المتعددة الأطراف للأمن السيبراني، وهو ما يستدعي دراسة الموضوع من منطق متعدد الرؤى والتفسيرات، كما أنه لا يوجد خطاب موحد يستخدمه كل الفاعلين خاصة أن التكنولوجيا السيبرانية غير قابلة للحماية بشكل كامل مما يبرر الدعوة إلى تعزيز الامن. وكلما زاد اعتماد الدول على التكنولوجيا السيبرانية، زادت التهديدات السيبرانية.

قائمة المراجع:

(*) **المؤلف المُراسل.**

[1] **Gromes, Thorsten &Bonacker, Thorsten. (2007). The Concept of Securitisation as a Tool for Analysing the Role of Human-Rights-Related Civil Society in Ethno Political Conflicts, SHUR Working Paper Series. P 10.**

[2] زقاغ، عادل. (2011). المعضلة الأمنية المجتمعية: خطاب الأمننة وصناعة السياسة العامة، مجلة دفاتر السياسة والقانون، 1(1): 60-72. ص 109.

[3] **Ole Wæver, " Politics, security, theory", Security Dialogue, (42) 4, 2011, P.18.**

[4] سليمان، سميرة. (2012). دور البيروقراطيات الدولية في أمننة قضيتي تغير المناخ والهجرة غير الشرعية، (رسالة ماجستير غير منشورة)، جامعة باتنة، الجزائر. ص 32.

[5] المرجع نفسه، ص 33.

[6] **Ole Wæver, op.cit, P.46.**

[7] **Ulrich Beck, Risk Society, Towards a New Modernity, London; Newbury Park, 1992, P.39.**

[8] Lene Hansen, Helen Nissenbaum, " Digital disaster, cyber security, and the copenhagen school", International Studies Quarterly, (53) 4, 2009, P.1155.
[9] Ibid, P.1171.
[10] Stephen M. Walt, " International Relations: One World, Many Theories", Foreign Policy, 110, 1998, P.34.
[11] Myriam Dunn Cavelty, " The Militarisation of Cyber Security as a Source of Global Tension", In: Zurich, Möckli, Daniel, Wenger, Andreas, eds, STRATEGIC TRENDS ANALYSIS, Center for Security Studies, 2012, P.105.
[12] Erdoan A. Shipoli, International Securitization: The Case of Kosovo, Saarbrucken: Lambert Academic 2010, P58.
[13] Sebastian Schutte, " Cooperation beats Deterrence in Cyberwar", Peace Economics, Peace Science, and Public Policy (3) 18, 2012, P.8.
[14] Myriam Dunn Cavelty, Cyber-Security and Threat Politics: US Efforts to Secure the Information Age, CSS Studies in Security and International Relations. London; New York: Routledge, 2008, P.19.
[15] Sean Lawson, " Beyond cyber-doom: Cyberattack Scenarios and the Evidence of History", WORKING PAPER, 2011, P.21.
[16] Alexander Nicoll, "Stuxnet: targeting Iran's nuclear programme, Strategic Comments", (17)2, 2011, PP.1-3.
[17] Monika Ambrus, Rosemary Rayfuse, Wouter Werner, Risk and the Regulation of Uncertainty in International Law, Oxford: Oxford University Press, 2017, P.39.
[18] Columba Peoples, Nick Vaughan-Williams, Critical Security Studies: An Introduction, London: Routledge, 2021, P.76.
[19] Ibid, P.83.
[20] Michael C. Williams, " Words, Images, Enemies: Securitization and International Politics", International Studies Quarterly (47) 4, 2003, P.513.
[21] Mark J. Brandt (eds), " The Association Between Threat and Politics Depends on the Type of Threat, the Political Domain, and the Country", Personality and Social Psychology Bulletin, (47) 2, 2020, P.325.
[22] OECD. (2021). Guidelines for the Security of Information and Systems and Networks, In: http://www.oecd.org/internet/ieconomy/15582260.pdf
[23] Holger Stritzel, "Towards a Theory of Securitization: Copenhagen and Beyond", European Journal of International Relations, (13) 3, 2007, 364.
[24] Noluxolo Gcaza, " An Ontology for a National Cyber-Security Culture Environment", Conference: Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015), P.3.

الآليات التشريعية الوطنية لمكافحة الجرائم السيبرانية في عصر الذكاء الاصطناعي
–واقع وتحديات-

NATIONAL LEGISLATIVE MECHANISMS TO COMBAT CYBERCRIMS IN THE AGE OF ARTIFICIAL INTELLIGENCE – REALITY AND CHALLENGES –

بن عملرة دلال(*)جامعة جيلالي ليابس- سيدي بلعباس- drbenamaradalal@gmail.com .

ملخص:

تهدف هذه الورقة البحثية إلى تسليط الضوء حول الآليات التشريعية والمؤسساتية التي تبناها المشرع الجزائري للتصدي للجرائم السيبرانية الناتجة عن لاستغلال المتنامي للشبكات الالكترونية لأغراض غير شرعية، بشكل يعزز أمنها السيبراني والقومي، خاصة مع تطور تكنولوجيا لإعلام والاتصال واتجاه الدولة الجزائرية حول لإدارة الالكترونية مما يستوجب وضع إستراتيجية تشريعية فعالة لحماية البنى التحتية للأنظمة المعلوماتية الوطنية الحساسة. بالإضافة إلى الدور الذي تلعبه أنظمة الذكاء لاصطناعي في مواجهة لإجرام السيبراني.

الكلمات المفتاحية: الجرائم السيبرانية، لأمن السيبراني، لأمن القومي، لإستراتيجية التشريعية، الذكاء لاصطناعي.

Abstract: This research paper aims to shed light on the legislative and institutional mechanism adopted by the Algerian legislator to address cybercrimes resulting from the growing exploitation of electronic networks for illegal purposes, in a way that enhances its cyber and national security, especially with the development of information and communication technology and the Algerian state's trend towards electronic management, which requires developing an effective legislative strategy to protect the infrastructure of sensitive national information systems, In addition to the role that artificial intelligence systems play in confronting cybercrime.

KeyWords: cybercrime, cyber security, national security, legislative strategy, artificial intelligence.

مقدمة:

يشهد العصر الحالي تطور متسارع لتكنولوجيا لإعلام والاتصال إذ أصبح يطلق على هذا العصر عصر الثورة الصناعية الرابعة أو عصر الثورة الرقمية، حيث أصبحت المجتمعات الحالية مجتمعات إلكترونية نتيجة التكنولوجيا الحديثة وما قدمته من خدمات رقمية سريعة وذات جودة عالية ودقة لامتناهية.

وإن قدم هذا التطور التكنولوجي قيمة مضافة للمجتمعات وفي المجالات المختلفة، حيث من خلال الفضاء السيبراني، استطاعت الدول والشعوب التواصل والتخاطب مباشرة وبدون التنقل وفي شتى الميادين. إلا أن الواقع أثبت مدى خطورة التجاوزات ولاستغلال السلبي لهذه التكنولوجيا الرقمية ما جعلها أرضا خصبة لنوع جديد من الجرائم وهي الجرائم السيبرانية والتي أدت إلى التعدي على الحقوق والحريات لأساسية للأفراد وكذا حقوق المؤسسات والهيئات وحتى المساس بأمن البلاد وسيادتها. من خلال التجسس واختراق وتخريب لأجهزة لأمنية والمؤسسات الحكومية والبنوك وغيرها.

والجزائر لم تكن في منأى عن تداعيات هذه الظاهرة حيث ووفقا للإحصائيات لأمنية شهدت البلاد في الآونة لأخيرة ارتفاع خطير للجرائم الإلكترونية مست الحياة الشخصية للمواطن وكذا استقرار وأمن البلاد.

لهذا وفي ظل التحدي الرقمي التكنولوجي الجديد سعى المشرع الجزائري إلى وضع إطار تشريعي ومؤسساتي متكامل للحد من انتشار هذه الجرائم والوقاية منها ومكافحتها، محاولا بذلك تدارك الفراغ التشريعي في هذا المجال نتيجة قصور لإجراءات التقليدية المتعلقة بالتحقيقات والتحريات لمتابعة مرتكبي الجرائم المتصلة بتكنولوجيا لإعلام والاتصال، كما أحدثت أجهزة ووحدات أمنية متخصصة لمتابعة ومكافحة هذا النوع من الجرائم مجهزة بأحدث الطرق العلمية المتطورة.

كما لا يمكن تجاهل أهمية الذكاء لاصطناعي الذي يعد من أهم إنجازات التكنولوجيا الرقمية وتتعدد استخداماته في مختلف المجالات العسكرية والصناعية والاقتصادية والعلمية والخدماتية وغيرها.وبالرغم من اعتباره سلاحا ذو حدين إلا أنه لا يمكن إنكار مساهمته بشكل كبير في إيجاد الحلول لقضايا جد معقدة فاقت قدرة العقل البشري، لهذا تسعى الدول إلى تطوير قدراتها في مجال أنظمة الذكاء لاصطناعي لتحقيق التفوق والهيمنة.

كل هذا يدفعنا إلى طرح لإشكالية التالية:

هل وفقت المقاربة الجزائرية في توفير آليات تشريعية ومؤسساتية للمكافحة الجرائم السيبرانية؟ وما مدى مساهمة أنظمة الذكاء لاصطناعي للتصدي لهذا النوع من الجرائم؟

سنحاول من خلال هذه المداخلة تسليط الضوء حول أهم الآليات التشريعية والمؤسساتية المقررة للتصدي للجرائم السيبرانية في الجزائر مع تبيان الدور الذي تلعبه أنظمة الذكاء لاصطناعي في مكافحة هذا النوع من الجرائم الالكترونية.

فرضيات الدراسة: تقوم هذه الدراسة على فرضية نجاعة الآليات التشريعية والمؤسساتية للتصدي للجرائم السيبرانية، و إمكانية أن يساهم الذكاء لاصطناعي في الحد من لإجرام الإلكتروني

أهداف الدراسة: تهدف هذه الدراسة إلى التعرف على ماهية الجريمة السيبرانية وكذا تسليط الضوء على أهم الوسائل القانونية والهيئات المؤسساتية في مكافحة لإجرام السيبراني في التشريع الجزائري. مع الكشف عن مدى مساهمة أنظمة الذكاء لاصطناعي في التصدي لجرائم تكنولوجيات لإعلام والاتصال.

خطة الدراسة: محاولة لتحليل هذه لإشكالية قمنا بتقسيم هذه الورقة البحثية محورين:

المحور الأول: مكافحة الجريمة السيبرانية تقضي تطوير المنظومة التشريعيةو المؤسساتية الوطنية.

أولا: لإطار التشريعي لمكافحة الجريمة السيبرانية

ثانيا: لإطار المؤسساتي لمكافحة الجريمة السيبرانية

المحور الثاني: الذكاء لاصطناعي كآلية لتحقيق لأمن السيبراني

أولا: مساهمة أنظمة الذكاء لاصطناعي في مكافحة الجريمة السيبرانية.

ثانياواقع وتحديات مكافحة الجريمة السيبرانية في الجزائر

المحور الأول: مكافحة الجريمة السيبرانية تقتضي تطوير المنظومة التشريعية والمؤسساتية الوطنية:

عمد المشرع الجزائري إلى استحداث آليات قانونية لمكافحة الجرائم السيبرانية من خلال وضع منظومة تشريعية شاملة، تتمثل أساسا في تعديل كل من قانون العقوبات وقانون لإجراءات الجزائية، حيث تتطلب عملية التصدي للجرائم الالكترونية ، تطوير القواعد لإجرائية التقليدية المرتبطة بالتحقيق والتحريات لمتابعة مرتكبي هذا النوع من الجرائم. بالإضافة إلى إصدار قانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات لإعلام والاتصال ومكافحاتها .[1]

لم يستقر الفقهاء والباحثين على إعطاء تعريف موحد ودقيق للجرائم السيبرانية، باختلاف الزوايا التي ينظر من خلالها للجريمة، فمنهم من ركز على الجانب الموضوعي للجريمة ومنهم من ركز على الأداة المستخدمة فيها.ومع ذلك يمكن تعريفها على أنها:" استخدام لأجهزة التقنية الحديثة كالحاسوب أو الهواتف النقالة في تنفيذ أغراض غير مشروعة بهدف لإضرار بالمجتمع."[2]

وقد عرفها المؤتمر العاشر للأمم المتحدة لمنع الجريمة بأنها جريمة يمكن لرتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب وتتمثل من ناحية المبدئية، جميع الجرائم التي بمكن لرتكابها في بيئة إلكترونية. [3]

أما المشرع الجزائري فقد استعمل مصطلح "المساس بأنظمة المعالجة الآلية للمعطيات" في قانون رقم 09-04، ويقصد بها الجرائم الماسة بأنظمة المعالجة الآلية بتكنولوجيات لإعلام والاتصال المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل لرتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

وعليه اعتبر المشرع الجزائري أن محل الجريمة الالكترونية هو النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية، حيث يشكل نظام المعالجة الآلية للمعطيات الشرط الأولي الذي لابد من تحققه حتى تتوافر أركان الجريمة من جرائم لاعتداء على هذا النظام. [4]

كما عرف نظام المعلومات، بموجب نص المادة 02 من القانون رقم 04-09، تحت تسمية "المنظومة المعلوماتية " وهي أي نظام منفصل أو مجموعة من الأنظمة المتصلة مع بعضها البعض أو مترابطة، يقوم واحد منها أو أكثر معالجة الآلية للمعطيات تنفيذا لبرنامج معين."[5]

وقد كيفت هذه الجرائم على أنها ذات طبيعة قانونية خاصة حيث أن تطبيق القواعد التقليدية على هذا النوع من الجرائم المستحدثة يثير مشاكل متعددة تأتي في مقدمتها صعوبة الإثبات وإيجاد دليل مادي يدين مرتكب الجريمة، إذ يستطيع الجاني محو الأدلة في وقت قصير وخاصة في حالة تفتيش الشبكات أو عمليات اعتراض الاتصال، كما قد تكون البيانات التي يجري البحث عنها مشفرةولا يعرف شفرة الدخول إلا أحد العاملين على الشبكة و من هنا تثار مسألة مدى مشروعية إجباره على فك الشفرة .[6]

بالإضافة إلى صعوبة متابعة مرتكبي الجرائم المعلوماتية بالنسبة للمقيمين خارج الوطن خاصة في حالة عدم وجود اتفاقية مع الدولة التي وقع فيها السلوك الإجرامي. كل هذا يؤكد تمتع هذه الجرائم بطبيعة قانونية خاصة.

أولا-الإطار التشريعي لمكافحة الجريمة السيبرانية: ويتمثل في:

1- تعديل قانون العقوبات:

عدل المشرع الجزائري قانون العقوبات مواكبة منه للتطورات التكنولوجية الالكترونية والمعلوماتية ، ورغبة منه في تحقيق أمنه السيبراني، وذلك من خلال استحداث قسم خاص يتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات بموجب قانون 04-15 المؤرخ في 2004/11/10، من خلال القسم السابع مكرر من المواد 394 مكرر إلى 394 مكرر 7 ، ولم يكتف المشرع الجزائري لذلك فرض حماية جنائية على الحياة الخاصة للأفراد من خلال القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 والذي عدل المادة 303 وأحدث المادة303 مكرر 3 وهذا تصديا للاستعمال السيئ لوسائل التكنولوجيا الحديثة. بغرض المساس بحرمة الحياة الخاصة للأشخاص، بالإضافة إلى السلوكيات الإجرامية كمن يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، أو كل من يدخل بطريق الغش معطيات في نظام المعالجة الآلية أو يزيل أو يعدل بطريق الغش المعطيات التي يتضمنها وغيرها.[7]

والجدير بالذكر أن المشرع الجزائري لم يتعرض لجريمة السب والقذف الالكتروني أو المطاردة عبر الإنترنت أو الغش المعلوماتي، بينما اكتفى بالنصوص العقابية التقليدية والتي لا تنسجم مع طبيعة الجرائم السيبرانية و لا تتماشى مع مبدأ شرعية الجرائم والعقوبات وحظر القياس.[8]

1- تعديل قانون الإجراءات الجزائية:

تماشيا مع التطور المعلوماتي، عدل المشرع الجزائري قانون الإجراءات الجزائية حيث تبنى قواعد خاصة بسلطة البحث والتحري والمتابعة وذلك بغرض ضمان سرعة التحقيق والتصدي للجرائم السيبرانية. إذ قام إضافة إلى القواعد القانونية الموضوعية الردعية، بإرساء قواعد وتدابير إجرائية وقائية وتحفظية بموجب قانون رقم 06-22 المؤرخ في 2006/12/22 والمعدل لقانون الإجراءات الجزائية.

حيث قام المشرع الجزائري للتحقيق في الجرائم السيبرانية، بتمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات.[9] كما أسند للأقطاب الجزائية المتخصصة الاختصاص بالنظر في هذا النوع من الجرائم[10] ، إضافة إلى توسيع مجال اختصاص النيابة العامة من خلال تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[11]

كما أجاز المشرع الجزائري اللجوء إلى إجراء التسرب بموجب المادة 65 من قانون الإجراءات الجزائية، ويعرف التسرب بموجب المادة 65 مكرر 12 من قانون الإجراءات الجزائية على أنه:"قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك."[12]

حيث يجوز لوكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب مع احترام الشروط القانونية باعتبار أن عملية التسرب من أخطر الإجراءات انتهاكا لحرمة الحياة الخاصة للمتهم. وتتمثل هذه الضوابط في احترام شرط صدور إذن قضائي مكتوب ومسبب وأن لا تتجاوز عملية التسريب 04 أشهر ويمكن أن تتجدد حسب مقتضيات التحري والتحقيق، كما يجوز للقاضي الذي رخص بها أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة.[13]

2- إصدار قانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحاتهما:

حيث تضمن جملة من التدابير الوقائية والإجرائية لمكافحة هذه الجرائم، وتتمثل التدابير الوقائية في مراقبة الاتصالات الالكترونية ، هذه العملية تتم بموجب إذن مكتوب من السلطة القضائية المختصة، وتم حصر هذا الإجراء في حالات محددة بموجب المادة 04 من قانون 09-04 والمتمثلة في الوقاية من الأفعال بجرائم الإرهاب والأفعال التخريبية أو الجرائم الماسة بأمن الدولة، في حالة محاولة الاعتداء على منظومة معلوماتية بشكل يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، في حالة التحريات والتحقيقات القضائية والتي تكون الوصول فيها إلى النتيجة صعب دون اللجوء إلى المراقبة الالكترونية. في حالة تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

بالإضافة إلى إمكانية الاستعانة بمزودي الخدمات للوقاية من الجرائم السيبرانية، وذلك لمساعدة السلطات المختصة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات وبوضع المعطيات التي يتعين عليهم حفظها.[14] كما يلتزمون بمقتضيات السرية وإلا تعرضوا لعقوبات المقررة لإفشاء أسرار التحري والتحقيق.

أما التدابير الإجرائية فتتمثل في تفتيش المنظومات المعلوماتية والمعطيات المعلوماتية المخزنة فيها، منظومة التخزين المعلوماتية ويمكن اللجوء إلى طلب مساعدة السلطات الأجنبية إذا وجدت أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية في الخارج.[15]

كما يمكن للسلطات التي تقوم بالتفتيش، اللجوء إلى إجراء الحجز ، في حالة وجود معطيات مخزنة تساعد في الكشف عن الجرائم أو مرتكبيها. ويمكن لها استخدام التقنيات اللازمة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها. كما يمكن منع الإطلاع على المعطيات التي يشكل محتواها جريمة.[16]

من خلال استقراء المواد القانونية المعدلة أو المستحدثة، يتضح أن المشرع الجزائري تبنى تدابير وقائية وردعية لمكافحة الجرائم السيبرانية من خلال اعتماد وسيلة الجريمة والمتمثلة في استعمال تكنولوجيات الإعلام والاتصال، وكذلك تحديد موضوع الجريمة والمتمثل في المساس بالأنظمة المعلوماتية، وأيضا فرض العقوبات الردعية المحددة في القانون.

ثانيا-الإطار المؤسساتي لمكافحة الجريمة السيبرانية:

من أجل ضمان التنفيذ الفعلي لمختلف التدابير للوقاية لمكافحة الجرائم السيبرانية، تم إنشاء هيئات متخصصة لتحقيق الأمن السيبراني، مع احترام الحقوق والحريات في إطار الشرعية الدستورية ، من بين الهيئات ما يلي:

1- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها:

استحدثت هذه الهيئة بموجب قانون 04-09، ودخلت حيز التنفيذ بموجب المرسوم الرئاسي رقم 15-261 المؤرخ في 2015/10/08، وتوالت التعديلات بخصوصها، حتى آخر تعديل بموجب المرسوم الرئاسي لسنة 2020، ليعيد تنظيم الهيئة.وعرفها بأنها عبارة عن سلطة إدارية مستقلة تتمتع بالشخصية المعنوية وذمة مالية مستقلة توضع تحت سلطة رئيس الجمهورية، ويحدد مقرها في الجزائر العاصمة، وتتكون من مجلس توجيه ومديرية عامة يوضعان تحت السلطة المباشرة لرئيس الجمهورية.[17] ومن أبرز مهامها:[18]

- اقتراح عناصر لإستراتيجية الوطنية للوقاية ومحاربة الجرائم السيبرانية.
- المراقبة الوقائية للاتصالات الالكترونية بهدف الكشف عن الجرائم الإرهابية والتخريبية وجرائم المساس بأمن الدولة.
- تعزيز التعاون والتنسيق بين مختلف الشرائح والهيئات الفاعلة من خلال التعاون بين القطاع العام والخاص والمجتمع المدني من أجل نشر الوعي بضرورة مواجهة كل الأعمال التي تشكل تهديدا وخرقا لقانون الفضاء السيبراني وتعديا للحقوق والحريات الأساسية.

2- القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

تم إحداثها بموجب الأمر رقم 21-11، المؤرخ في 2021/08/25 المعدل والمتمم لقانون الإجراءات الجزائية ، ويتواجد على مستوى محكمة مجلس قضاء الجزائر، ويختص هذا القطب بمهمتين أساسيتين هما: [19]

- المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها.
- الحكم في الجرائم المنصوص عليها في الباب السادس من الأمر 21-11 إذا كانت تشكل جنحا.

كما تضمنت المادة 211 مكرر24 الاختصاص الحصري لكل من وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وقاض التحقيق ورئيس ذات القطب، للمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الجرائم المرتبطة بها: - الجرائم التي تمس أمن الدولة والدفاع الوطني– جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع، –جرائم نشر وترويج أنباء مغرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية، –جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية، – جرائم الاتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين، –جرائم التمييز وخطاب الكراهية.

بالإضافة إلى هيئات متخصصة ضمن أسلاك الأمن ومنها:

- المصلحة المركزية لمكافحة الجريمة المعلوماتية
- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية.
- المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني.

المحور الثاني: الذكاء الاصطناعي كآلية لتحقيق الأمن السيبراني:

سنعالج في هذا المحور دور أنظمة الذكاء الاصطناعي في مكافحة الجريمة السيبرانية، مع التطرق إلى واقع وتحديات مكافحة الجريمة السيبرانية في الجزائر.

أولا-مساهمة أنظمة الذكاء الاصطناعي في مكافحة الجريمة السيبرانية:

بالإضافة إلى الآليات التشريعية والبناء المؤسساتي التي تبناها المشرع الجزائري للتصدي للجرائم السيبرانية، يمكن أيضا اعتماد أنظمة الذكاء الاصطناعي لمواجهة هذا النوع من الجرائم والتصدي لها، حيث أضحت كيانات الذكاء الاصطناعي تقوم بأعمال كانت حكرا على الذكاء البشري، وهو يعتبر من الميادين الحديثة في حقول العلم والمعرفة التي تشهد تطورا متسارعا، فهو فرع من فروع علم الحاسوب وهو علم إنشاء أجهزة وبرامج كمبيوتر قادرة على التفكير بنفس الطرقة التي يعمل بها الدماغ البشري، وعليه فإن الذكاء الاصطناعي له دور كبير في التعمق في العلوم المختلفة ومنها مكافحة الجرائم المستحدثة الالكترونية حيث يمكن للشرطة توظيف تقنيات الذكاء الاصطناعي للكشف عن الجرائم السيبرانية ومرتكبيها . من خلال تحليل البيانات والمعلومات ومعالجتها والقيام بالبحث والتقصي في مخازن البيانات في العالم الرقمي وأنظمة المعلومات والخروج بالتوصيات لاتخاذ القرار الصائب.[20]

ومن بين هذه التقنيات ما يلي:[21]

1- الشرطة الاستباقية: ويقصد بها ردع الجرائم بواسطة العمل الاستباقي من خلال تحليل البيانات والعمل الشرطي القائم على تحليل الأدلة المادية، ومن أهم هذه الإجراءات التخزين السحابي والذي من شأنه أن يحل مشكلة التخزين ويتيح إمكانية ربط الشبكات المنية ببعضها البعض لإتاحة العمل على الجرائم بكل سهولة ويسر.

2- الشرطة الرقمية: ويقصد بها تطوير أجهزة الشرطة لتصبح أكثر اعتمادا على التقنيات الحديثة للاستفادة من الوفرة في الأدلة الرقمية والتي يمكن الحصول من وسائل البريد الإلكتروني وسجلات الهاتف وغيرها. وهو ما يدعو إلى ضرورة وجود روابط قانونية بين المؤسسات المختلفة لتقديم الأدلة الرقمية بسهولة ودون تباطئ

3- التحقيق الرقمي: ويقصد به الاعتماد على شبكة الإنترنت في رفع الملفات الرقمية للقضايا التي تحتوي على أدلة جنائية لتمكين من استخدامها من قبل العديد من المسؤولين ، ما يستدعي تحول الحكومة إلى حكومة رقمية بكامل أجهزتها لتواكب الاتجاه نحو الرقمنة.

والجدير بالذكر أن التحقيق الرقمي هو عملية التحقيق في الجرائم المرتكبة باستخدام أي نوع من أجهزة الحوسبة مثل أجهزة الكمبيوتر والخوادم والهواتف المحمولة والأجهزة اللوحية والكاميرا الرقمية وأجهزة الشبكات وأجهزة إنترنت لأشياء أو أي نوع من أجهزة تخزين البيانات.[22]

إلا أن عملية تطبيق الذكاء الاصطناعي على الجرائم السيبرانية تتعرض لمجموعة من العوائق منها، الحاجة إلى توفير البنية التحتية التي يتطلبها العالم الرقمي، وكذلك توفير حواسيب متصلة بالإنترنت ذات تدفق فائق السرعة، بالإضافة إلى ضمان عملية الإدماج باستخدام الذكاء الاصطناعي في مواجهة الجريمة السيبرانية.

ثانيا-واقع وتحديات مكافحة الجريمة السيبرانية في الجزائر:

كشفت الإحصائيات المتعلقة بالجرائم الإلكترونية في الجزائر، أن الجرائم السيبرانية التي تستخدم الإنترنت ووسائط التواصل الاجتماعي، في تصاعد خطير وملفت، حيث تمت معالجة 500 جريمة سيبرانية منذ بداية العام 2023 من قبل الأجهزة الأمنية المختصة.

تشمل هذه الجرائم الالكترونية: الابتزاز والتهديد والتشهير والمساس بالحريات الشخصية والحياة الخاصة عبر شبكات التواصل الاجتماعي، فضلاً عن جرائم نشر المعلومات الزائفة والمضللة، والقرصنة والتشهير والتحرش الإلكتروني والنصب والاحتيال.

كما تشير البيانات الإحصائية إلى تزايد كبير للإجرام الإلكتروني بصورة مستمرة، إذ ارتفع نسق هذا النوع من الجرائم من 2838 جريمة عام 2021، إلى 4600 جريمة في 2022، كما أنّ تسجيل 500 جريمة إلكترونية خلال شهر واحد من السنة الحالية يؤشر على أنّ حصيلة عام 2023، ستفوق بكثير حصيلة العام الماضي. كما أنّ "ما بين 65 و75 في المائة من القضايا المعالجة تخص الحياة الخاصة للأفراد".[23]

وفي نفس السياق، أحبطت شركة "كسبرسكي" المختصة في محاربة الجريمة السيبرانية، 95 000 هجمة إلكترونية ضد الجزائر سنة 2020، حيث تم تصنيفها سنة 2018 الأولى عربيا و 14 عالميا من حيث البلدان الأكثر تعرضا للهجمات الالكترونية.[24]

ومن بين التحديات التي تواجه السلطات المختصة لمكافحة الجرائم السيبرانية نذكر أهمها:

-ارتفاع عدد المشاركين في شبكة الإنترنت في الجزائر ، ما يفوق 10 ملايين مشترك، ما يؤدي إلى زيادة المخاطر وصعوبة تحديد هوية مرتكبي الجرائم الإلكترونية. بالإضافة إلى أكثر من 07 ملايين مستعمل لمواقع التواصل الاجتماعي ما نجم عنه ظهور عدد كبير من الجرائم السيبرانية كالقذف والتحرش الجنسي، وغيرها.

- التطور التكنولوجي الذي ساهم في ظهور انترنت فائقة السرعة والتدفق ما يؤدي إلى سرعة ارتكاب الجريمة.

ولمكافحة هذا النوع من الجرائم المتطورة ندرج بعض الاقتراحات كالآتي:

-وضع إطار تشريعي وتنظيمي ملائم لمكافحة الجرائم السيبرانية بمشاركة كل من القطاع الخاص والمجتمع المدني والاستفادة من الخبرات الدولية .

-إنفاذ القوانين في أرض الواقع وبكل صرامة، وتكييف النصوص القانونية مع التطورات الحاصلة في هذا المجال.

-اكتساب التكنولوجيات المتطورة والتمكن من استخدامها وتطوير البنى التحتية الخاصة بالمعلومات وتحديثها باستمرار وتصميم برامج فائقة التطور.

-الاستثمار في العامل البشري من خلال وضع برامج لبناء القدرات البشرية اللازمة لتفعيل نظام الخدمات الإلكترونية مع إشراك القطاعات المختلفة من القطاع الخاص والجامعات والمنظمات غير الحكومية.

- نشر الوعي بفوائد الخدمات الإلكترونية سواء بالنسبة للأفراد والشركات والمؤسسات، مع التحسيس بمدى خطورة الجرائم السيبرانية على حياة الأفراد الخاصة والأمن القومي.

-تعزيز الأمن السيبراني من خلال نظام الذكاء الاصطناعي، حيث تمكنت هذه التقنية من التعامل مع عدد كبير من البيانات كما يقلل من وقت الاستجابة للتهديدات الإلكترونية، ويمكن من خلالها التنبؤ بالهجمات المستقبلية والتقليل من التكاليف.

-تعزيز السبل وتضافر الجهود لخلق منظومة تشريعية خاصة باستخدام أنظمة الذكاء الاصطناعي للحد من جرائم الحاسب الآلي.

-تعزيز التعاون الدولي للتصدي للجرائم السيبرانية باعتبارها جرائم عابر للحدود للاستفادة من الخبرات والتجارب الدولية في هذا المجال.

خاتمة: نخلص في نهاية هذه الورقة البحثية أن التحكم في الجرائم السيبرانية صعب جدا، وذلك يعود للتطور السريع لتكنولوجيا الإعلام والاتصال، وما يثبت ذلك هو الانتشار الواسع لهذا النوع من الجرائم الحديثة بشكل مستمر وعالي وما سببه من خسائر وأضرار في ميادين مختلفة اقتصادية أمنية اجتماعية تجارية وغيرها.

وعلى الرغم من أن المشرع الجزائري حرص على مواكبة النهضة التكنولوجية والمعلوماتية من أجل تدارك القصور التشريعي وتفادي إفلات المجرم الالكتروني من العقاب، أسس منظومة قانونية وإطار مؤسساتي للتصدي لهذا النوع من الجرائم، من خلال تعديل كل من قانون العقوبات وقانون الإجراءات الجزائية وسن قانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث قام باستحداث قواعد إجرائية جديدة تتلائم والطبيعة الخاصة لهذا النوع من الجرائم كالمراقبة الالكترونية والتسرب الالكتروني واعتراض المراسلات و تفتيش المنظومة المعلوماتية وحجزها، من أجل توقيع العقاب بفعالية وصرامة.

نظرا للطابع الخاص للجريمة السيبرانية وإضافة للنصوص القانونية المختلفة التي تم إقرارها للتصدي للإجرام الالكتروني ، تم إحداث عدة أجهزة وهيئات من أجل مكافحة هذا النوع من الجرائم

كما تساهم أنظمة الذكاء الاصطناعي في الحد من الجرائم المعلوماتية لهذا على المشرع الجزائري وضع أنظمة تشريعية فعالة للاستفادة من تقنيات الذكاء الاصطناعي للتصدي لجرائم الحاسب الآلي.

وفي سبيل تحقيق ذلك لابد من تطوير المواهب الوطنية عن طريق دعم الدراسات المتخصصة وأدوات البحث والتطوير من أجل الاستثمار في عناصر بشرية ذات كفاءة وموثوقية لمواجهة التحديات والتهديدات التي تمس الأمن القومي.

الهوامش والمراجع:

[1]- قانون رقم قانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، المؤرخ في 2009/08/05، ج ر عدد 47، الصادرة في 2009/08/16.

[2]-زبيخة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، 2011، ص42.

[3]-زبيخة زيدان، نفس المرجع، ص44.

[4]- بولحية شهرزاد، خلوفي رشيد، تحديات الجريمة الالكترونية في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، 2019، ص ص 1973-2003، ص 1984.

[5]- المادة 02 من قانون 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، المرجع السابق.

[6]- محمد علي سالم، الجريمة المعلوماتية، مجلة جامعة بابل للعلوم الإنسانية، المجلد 14، العدد2 ، 2007، العراق، ص 91.

[7]- المادة 394 مكرر و 394 مكرر1، من قانون رقم 04-15 المؤرخ في 2004/11/10، المعدل والمتمم للأمر 66-155، المتضمن قانون العقوبات، ج ر عدد 71، الصادرة 2004.

[8]- مهدي رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة إلزا للبحوث والدراسات، المجلد 06 العدد02، 2021، ص ص 111-125، ص 117.

[9]- المادة 329 من قانون رقم 06-22، المؤرخ في 2006/12/20، يعدل ويتمم الأمر رقم 66-155، المتضمن قانون الإجراءات الجزائية، ج ر عدد 84، الصادرة 2006.

[10]- المواد 37-40- 329 من قانون الإجراءات الجزائية، نفس المرجع.

[11]- المادة 37 من قانون الإجراءات الجزائية، نفس المرجع.

[12]- المادة 65 مكرر 12 من قانون الإجراءات الجزائية، نفس المرجع.

[13]- المادة 65 مكرر 15 من قانون الإجراءات الجزائية، نفس المرجع.

[14]- المادة 11 من قانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، المرجع السابق.

[15]- المادة 05 من قانون 09-04، نفس المرجع

[16]- المادة 06-07-08 من قانون 09-04، نفس المرجع.

[17]- المرسوم الرئاسي رقم 20-183، المؤرخ في 2020/07/13، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 40، الصادرة في 2020/07/18.

[18]- المادة 04 من المرسوم الرئاسي رقم 20-183

[19]- المادة 211 مكرر22 من الأمر رقم 21-11، المؤرخ في 2021/08/25، والمتضمن قانون الإجراءات الجزائية، ج ر عدد 65، الصادرة في 2021/08/26.

[20]- لأخنش نورة أمينة، العيداني محمد، الذكاء الاصطناعي كآلية لمجابهة الجريمة الإلكترونية مجلة القانون والعلوم البيئية، المجلد 02، العدد 02، 2023، ص ص 528-544، ص 538.

[21]- علي أحمد إبراهيم، تطبيقات الذكاء الاصطناعي في مواجهة الجرائم الالكترونية، المجلة القانونية، المجلد 09، العدد 08، 2021، ص ص 2809-2836، ص 2824، 2825.

[22]- لأخنش نورة أمينة، العيداني محمد، الذكاء الاصطناعي كآلية لمجابهة الجريمة الإلكترونية، المرجع السابق، ص 536.

[23]- موقع العربي الجديد https://www.alaraby.co.uk/entertainment_media/

[24]- سميحة بلقاسم، حميد بوشوشة، الجريمة الالكترونية بعد جديد للإجرام في الجزائر –واقعها وآليات مجابهتها- مجلة العلوم الإنسانية لجامعة أم البواقي، المجلد 10، العدد01، جوان 2023، ص ص 532-561، ص553.

Le devoir de l'adaptation de l'Algérie à l'ère numérique : vision à long termes, défis et perspectives de protection cyberienne

GHAMRI Sara
Université Abbès Laghrour
Khenchela Algérie
ghamri_sarah@hotmail.fr:

HASSANI Rima Aida
Université Abbès Laghrour
Khenchela Algérie
hassani.rima@univ-khenchela.dz

ملخص البحث:

لقد غزا استخدام الإنترنت وأجهزة الكمبيوتر عصرنا ، مثل سيف ذو حدين ، وقد ثبت أن هذا لاستخدام ذو فائدة أساسية للأفراد وكذلك للدول ، مما يجعل الحياة أسهل ويوفر لنا ضياع الوقت والمسافة ، ولكن في في الواقع ، لمحاكاة الضجر نفسه في الجانب السلبي مثل الصورة الإيجابية ، التي تولد منها أشكال جديدة من الجنوح للجرائم الإلكترونية ، في الواقع ، هذا لأخير هو شكل جديد من أشكال الجريمة التي يقوم فيها فرد أو جماعة بإيذاء لآخرين وإيذائهم باستخدام نظام الكمبيوتر.

الكلمات المفتاحية: لأمن السيبراني / تكنولوجيا المعلومات / الخطر / الحماية/ رهانات

Résumé :

L'utilisation de l'internet et de l'informatique a envahi notre ére, comme une arme à double tranchants, cet usage s'avérait d'une utilité indispensable aussi bien pour les individus que pour les nations, facilitant la vie et nous épargne la perte du temps et de la distance, mais en faite, des répercussions prennent le ras- au- bol autant dans l'aspect négatif que positif ,d'ou de nouvelles formes de délinquances naissent à l'image de la cybercriminalité, en effet, cette dernière est une nouvelle forme de criminalité au cours de laquelle un individu ou à groupe porte préjudice et nuit à autrui en utilisant un système informatique.

Mots clès : Sécurité-cybérienne / informatique / danger / protection / enjeux.

Introduction :

The dangers and problems linked to the phenomenon of cyber security have increased significantly in recent years due to numerous IT developments. Thus, two laws, the Information and Communication Technologies Act (ICTA) and the Computer Misuse and Cyber-crime (CMCA) react to this scourge, the cases most often recorded involve harassment on the Internet, skimming, which consists of cloning banking data, and phishing, which is online fraud.

According to a source from the Cyber Crime Unit, Internet harassment is the most common form of cybercrime, with the public having easy access to social networks such as Facebook and YouTube. Most often, it is minors aged 14-15 who are the victims.

Which leads us to ask ourselves the question about the essence of this new form of delinquency, its causes and its immense danger on the individual, societal and even international level and about the way in which societies and countries proceed to restrict the field. danger and evacuate the practice by implementing a set of techniques that we will discuss in the presentation below, in particular with the innovation of artificial intelligence which has overwhelmed the world of information and particularly in times of Covid 19, so what does cyber security consist of and what are its aspects and consequences and the secret measures taken to fight against the scourge of cybercrime?

1-What is cyber security?

Cyber security as the name suggests, is about protecting computers, servers, mobile devices, electronic systems, networks and data from corrupt attacks that can harm people, business, especially after digital transformation of companies, which has led to the generalization of the use of IT tools and communication via the Internet, it intervenes recurrently in many contexts, from corporate IT to mobile terminals, to do this it sets up all the means to ensure the protection and integrity of data, sensitive or not, within a digital infrastructure. It is a specialty within the information systems professions. It can be divided into several categories:

"1-Network security consists of protecting the computer network against intruders, whether targeted attacks or opportunistic software".

2-Application security aims to protect software and devices against threats. A malicious application could open access to the data it is supposed to protect. A reliable security system is recognized at the design stage, well before using a program or device.

3-Information security ensures the integrity and confidentiality of data, whether stored or in transit.

4-Operational security encompasses the processes and decisions related to the processing and protection of data. User permissions for network access and procedures that define data storage and location fall under this type of security.

5-Disaster recovery and business continuity specify how a company responds to a cyber security incident or any other event causing a loss of operations or data.

6- Disaster recovery policies govern how a business recovers its operations and information to the same operating capacity as before the event. Business continuity refers to the plan a business relies on while trying to operate without certain resources.

7-End user training focuses on the most unpredictable factor: people. Anyone can accidentally introduce a virus into a normally secure system by not following good security practices. Teaching users to remove suspicious attachments and not plug in unidentified USB drives is essential for business security. »(LEGAL, 1999)

2-Dangers and threats:

a- On individuals:

Cybercriminals can easily exploit vulnerabilities on a person's mobile phone to obtain private data. These vulnerabilities sometimes come from the applications that we use or that are installed on the Smartphone. Mobile phones are also susceptible to malware, which can record keyboard activity and take screenshots, so protect yourself by researching the applications you download, paying attention to e -emails that we open and images that we download.

Identity theft

One of the fastest growing Internet crimes is identity theft. Many of the points discussed earlier in this article can lead to identity theft, email and data breaches. On the other hand, a person's identity is also exposed through everyday documents, for example curriculum vitae, home address, photos and videos published on social networks, financial data, etc.

Identity thieves will steal personal information and open loan and credit card accounts in the person's name, so many things must be implemented to protect identity.

Sexual predators targeting children:

Users seeking to exploit children lurk in the dark corners of the Internet to sell and buy obscene and illegal photos. These exchanges take place by e-mail, via P2P file sharing programs or, increasingly, on the Dark Web, a part of the Internet inaccessible from standard search engines. Given the worrying nature of these trends, these sites should be avoided and left to appropriate law enforcement agencies to manage them.

Another danger on the Internet targeting children: sexual predators encourage them, or attempt to do so, to meet them in real life; they also seek to share obscene pornographic images with them. Make sure your children are fully aware of the dangers: never talking to strangers on the Internet and never sharing personal information with people they have never met.

Romantic scams

Dating sites, chat rooms and apps are rife with scams, where perpetrators take advantage of people looking for new partners by tricking them into obtaining their personal data.

Man-in-the-middle attack

A so-called man-in-the-middle attack refers to a type of cyber threat consisting of intercepting communication between two individuals to steal data from them. For example, on an unsecured WiFi network, a cybercriminal could intercept data passing between the victim's device and the network.

a- On the country:

Digital innovation is influenced by geopolitical tensions. This amplifies the likelihood of risk and reduces the possibility of cooperation.

The absence of a global governance framework increases the influence of private companies on setting standards, foreign collaboration on critical national infrastructure, acquisition of domestic technologies, offshoring of data abroad and the transfer of technological capabilities in exchange for access to foreign markets.

Global connectivity could be disrupted if nations continue to seek "cyber sovereignty" and dominance in the technology marketplace.

Technological advancements are happening at lightning speed, with every country and company wanting to benefit from first-mover advantage. This can modify the geopolitical balance by influencing standards, production chains, etc.

Cyberspace is rapidly evolving into an expansion of the military domain, triggering a digital arms race.Répercussions sur l'économie :

"The fragmentation of cyberspace and technology systems could have economic consequences by negatively affecting companies' use of the cloud and other technology services and pushing them to reduce productivity by needing separate production lines for different markets .

The loss of sustainability in maintaining AI-powered structures, like data centers, is significant. The need to adapt to different products for different markets could well increase the negative environmental footprint of any industry.

Newer, unregulated digital currencies could harm international cooperation against money laundering. This could threaten the financial stability of any country. »(MAURIS, 2007)

a- On companies:

The speed of technological progress around the world could widen the digital divide and wealth gap that exist today. The wealth gap could widen within countries, especially affecting low-skilled workers and even women in certain countries.

Given the awareness around so-called biased algorithms or cyber-bullying, we must evaluate the issue of ethics, particularly in AI, and ensure that it does not lead to negative consequences for underserved communities. represented.

3-causes of cyberthreat:

Cyber threat being an activity which aims to compromise the security of an information system by altering the availability, completeness or confidentiality of a system or the information it contains is exercised by authors who are in fact, states, groups or individuals who seek to take advantage of vulnerabilities to access victims' devices, systems and networks. Therefore, a classification of these authors would be possible according to their motivations to obtain access to resources and processing power.

Summary table of cyber threats covered in the reports:

	Nombre de rapports	Nombre de références[1]
Cybermenaces	13	556
Vol et perte de données (fuite interne, vol d'identité, etc.)	12	82
Attaque ciblée (*APT*, *exploit kits* et espionnage)	10	54
Exploitation de vulnérabilités	9	54
Logiciel malveillant	8	67
Infrastructure spécifique - Appareil mobile	8	35
Environnement vulnérable (*darkweb*, réseau Tor, etc.)	7	18
Hameçonnage et cybersquattage	6	64
Ingénierie sociale	6	11
Attaque par déni de service (*DDoS*)	5	12
Fraude fiscale (*skimming*)	4	30
Infrastructure spécifique - Écosystèmes	4	25
Utilisation de *botnets*	4	19
Infrastructure spécifique - Internet des objets	3	22
Menace à l'intégrité pers. (harcèlement, menace, etc.)	3	6
Menace de navigation (PDF, Java, Flash, etc.)	2	9
Attaque par force brute (*brute-force*)	1	5
Trafic malicieux (signe précurseur d'une attaque ciblée)	1	3

Figure ci-dessus les typologies de cyber menaces présentes dans les treize rapports analyses d'où l'on peut observer la mesure des menaces cyberiennes et leurs degrés de dangerosité. (Cotee, Maxime, & Dupont, 2016)

4_ Piratage et développement de la criminalité cyberienne :

Récemment, de nombreux événements d'envergure mondiale ont défrayé la chronique, notamment la divulgation de données sensibles de Sony Picture, les vols de données numériques chez Home Depot, eBay, JP Morgan, Target et Ashley Madison, l'attaque informatique contre TV5 Monde, ou la vulnérabilité informatique Heartbleed. Beaucoup d'événements ayant lieu récemment ont créé une augmentation de l'attention portée à l'égard de la cybercriminalité, ainsi que des inquiétudes qu'elle génère au sein de l'opinion publique a l'instar de la divulgation de données sensibles de Sony Picture, les vols de données numériques chez Home Depot, eBay, JP Morgan, Target et Ashley Madison, l'attaque informatique contre TV5 Monde, ou la vulnérabilité informatique Heartbleed. En effet, les gouvernements à travers le monde, les entreprises et les consommateurs s'inquiètent de manière prononcée de ces menaces à la sécurité de l'information. D'ailleurs, selon le directeur

d'Europol, au cours de l'année 2015 la cybercriminalité s'est hissée au même rang que le terrorisme en matière de menace pour la sécurité nationale (Agence France-Presse, 2015), ce qui met en exergue les préoccupations partagées à l'égard de cette forme de criminalité.

L'utilisation abusive du terme cybercriminalité ne manque pas de susciter un certain nombre de questionnements quant à sa réelle signification. Également, les médias sont les principaux vecteurs de diffusion d'informations sur la cybercriminalité, et la rigueur avec laquelle ils rapportent certains faits et leurs implications restent incertaine.

Conclusion :

La réalité est que les entreprises doivent changer leur vision du «si» elles sont attaquées au «quand» et reconnaître que les retombées des violations de la confidentialité des données ou des ransomwares peuvent être dévastatrices sur le plan financier. Il faut également se rappeler que le gain financier n'est pas le seul motif des cyber-attaques. L'«hacktivisme» et son objectif de nuire à la réputation des entreprises constituent une menace supplémentaire.

Dans un monde où les frontières s'estompent de plus en plus, la collaboration entre les spécialistes de la cyber-sécurité et les autorités chargées de la protection des données revêt une importance croissante. Votre approche renouvelée en matière de cyber-sécurité met en lumière la nécessité de promouvoir et de protéger les libertés en ligne et d'assurer une collaboration et une coordination entre les provinces et territoires. Dans ce contexte, il est essentiel que les spécialistes de la cyber-sécurité et les autorités chargées de la protection de la vie privée, comme le Commissariat, collaborent encore plus étroitement pour améliorer les mesures de protection dans les secteurs public et privé et veillent à ce que la protection de la vie privée constitue un principe directeur des efforts de cyber-sécurité.

Compte tenu de la dangerosité de la cyber-sécurité que ce soit sur la vie des individus, leurs confidentialités , aussi la sécurité des entreprise et la sécurité nationale, l'informatique offre des pistes d'innovation pour lutter contre ce genre de délinquance qui doit être catégoriquement combattue. Il existe des moyens de réduire la probabilité et l'impact d'une cyber attaque, mais cela nécessite une action et une planification ciblées. Les entreprises doivent rendre leurs pratiques de travail à distance résilientes aux cyber attaques et améliorer leur développement et leur application de mesures de sécurité.

Bibliographie

Cotee, M., Maxime, A., & Dupont, B. (2016). *Statistiques et menaces numeriques : comment les organisqtions de securité quantifient la cybercriminalité.* **Espagne: dans RESEAUX 3_4 (n°197_198),pp. 203_224.**

européen, D. 2. (du 26 juin 2013). *l'accès à l'activité et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, dite en anglais « CRD IV ».* **Capital Require.**

https://www.kaspersky.fr/resource-center/definitions/what-is-cyber-security, D. (s.d.). *what is cyber-sécurité?*

informatique, c. d. (2000, 09 19). *Centre canadien pour la cyber securite***. Consulté le MARS 11, 2021, sur introduction à l'environnement de cybermenace: Centre canadien pour la cyber securite : introduction à l'environnement de cybermenace.**

LEGAL, A. (1999, JUIN 21). *what is the cyber-sécurité?* **. Consulté le MARS 10, 2021, sur Education RESOURCES CENTER: D'après https://www.kaspersky.fr/resource-center/definitions/what-is-cyber-security**

MAURIS, J.-C. (2007, avril 11). *L'informatique modiale* **. Consulté le MARS 03, 2021, sur la-cybermenace-un-risque-mondial: D'après « https://tehtris.com/fr/la-cybermenace-un-risque-mondial-et-conseils-pour-y-faire-face/ »**

الحرب الهجينة ومهددات الأمن السيبراني

Hybrid Warfare and Cyber security Threats

نوري عزيز / (*) جامعة عباس لغرور – خنشلة nuri.aziz@univ-khenchela.dz
سليمان سميرة جامعة صالح بوبنير قسنطينة3 samira.slimane@univ-constantine3.dz

ملخص:

تتضمن تحاول الورقة البحثية معالجة قضية الحروب الهجينة وعلاقتها بمهددات الأمن السيبراني، حيث تظهر هذه العلاقة في شكل معضلة أمنية جديدة تواجه العالم بشكل عام، فلا يمكن لأي فاعل دولي أن يكون بمنأى عن مهدداتها، في الوقت الذي تعقد فيه مفهوم التهديد المعقد أصلا منذ نهاية الحرب الباردة وتوسع مفهوم الأمن، لتظهر أنماط جديدة للتهديد قبل استيعاب الأنماط التي سبقتها، مما يضع الأمن العالمي على أمام فترة معقدة وجب التعامل مع معطياتها بشكل جدي وعلمي وفي إطار متعدد الأطراف، لغرض تجنب معضلات أمنية قد تصل إلى الهجمات النووية ذات الطابع السيبراني أي الهجمات النووية غير المتحكم فيها من طرف ممتلكي هذه الأسلحة، وهو ما يعني التهديد الشامل للبشرية جمعاء.

الكلمات المفتاحية: الحرب الهجينة، الفضاء السيبراني، الهجمات السيبرانية، الأمن السيبراني

Abstract:

The research paper attempts to address the issue of hybrid wars and their relationship to cyber security threats, as this relationship appears in the form of a new security dilemma facing the world in general, as no international actor can be immune from its threats, at a time when it complicates the already complex threat concept since the end of the Cold War. The concept of security expanded, with new patterns of threat emerging before the patterns that preceded them were absorbed, which places global security on the verge of a complex period whose facts must be dealt with seriously, scientifically, and within a multilateral framework, for the purpose of avoiding security dilemmas that may lead to nuclear attacks of a cyber-nature, that is, non-nuclear attacks. Controlled by the owners of these weapons, which means a comprehensive threat to all of humanity.

Key words: Hybrid warfare, Cyberspace, Cyber-attacks, Cyber Security

مقدمة

-يجب تميز التاريخ العالمي للحروب بوجود حرب تميز كل حقبة زمنية منها، حيث تفاوتت بين حروب السيف والترس والحروب التقليدية ووصولا للحروب الكيماوية والنووية والسيبرانية، كما أن أساليب ووسائل الصراع والحروب غير العسكرية تنوعت وتطورت أيضا على أصعدة عدة، فأصبحت هناك الحروب النفسية والاقتصادية والسياسية والسيبرانية أو كلها مجتمعة، وهذا ما بات يسمى في بالحروب الهجينة التي أضحت في ظل هذا التقدم التكنولوجي المتطور تفرض نفسها كعامل حاسم لا بد منه في المعارك والصراعات طويلة الأمد، إضافة إلى أن الجيوش التقليدية للدول باتت تجد صعوبة في الرد على الهجمات الهجينة وخاصة السيبرانية منها كونها تأخذ أساليب ووجوها عدة وغالبا ما تكون هجمات شبكية معقدة الأساليب والحلول، وبما أن الحرب الهجينة هي خليط من عدة أنماط وأنواع من الحروب، حيث ساحات معاركها وخطوط تماسها تختلف اختلافا جذريا عن ساحات وميادين القتال تظهر الحروب السيبرانية الإلكترونية كأخطر مكون للحروب الهجينة وأنماط تهديداتها.

في نفس السياق، ترتبط الحروب الجينة بمجال الأمن السيبراني وبعض من المصطلحات كالجريمة السيبرانية والهجمات الإلكترونية: وفيها يتم التخطيط الغير قانوني باستخدام التكنولوجيا الرقمية لسيطرة على جهاز أو نظام تابع لفرد أو مؤسسة، باستخدام أجهزة متطورة أو استغلال ثغرات النظام، أو اعتمادا على جهل المستخدم وقلة ثقافته التكنولوجية.

وعليه، تجتمع هذه المتغيرات لتشكل أنماط متحولة ومتغيرة من مهددات الأمن السيبراني على مجال أوسع وأكثر تعقيدا، خصوصا في ظل الوضع الجيوسياسي العالمي المعقد التي نشهده منذ مطلع الالفية الجديدة، حيث لا يمكن لأي فاعل دولي أن يضمن سلامته وأمنه من مهددات الأنماط والأساليب المتنوعة للحروب الهجينة وعلى رأسها مهددات الأمن السيبراني.

على هذا الأساس يمكن طرح الإشكالية التالية:

كيف تساهم الحروب الهجينة في تقويض الأمن السيبراني للدول في ظل الأوضاع الجيوسياسية المعقدة التي يشهدها النظام الدولي؟

كما تستند الورقة البحثية على فرضية تؤكد أن تعقد مضامين الأمن القومي أفرز أنماطا جديدة وجب التركيز عليها لمواجهة مهدداته، فكلما كان الضعف في تطوير المضامين الأمنية للأمن القومي وتنويعها تبقى الدولة معرضة بشكل أكبر لمهددات الحروب الهجينة وعلى رأسها مهددات الأمن السيبراني.

المحور الأول: التحولات الجيوسياسية والأمنية المؤثرة على الأمن السيبراني

تؤثر التحولات الجيوسياسية والأمنية تأثيرا كبيرا على الأمن السيبراني، وتؤثر على استراتيجيات ودفاعات المؤسسات في مواجهة التهديدات المتطورة. تتضمن بعض النقاط الرئيسية من المصادر ما يلي:

- تداعيات الأزمات الجيوسياسية: يمكن للأزمات الجيوسياسية أن تؤدي إلى امتدادات سيبرانية، حيث تستخدم الهجمات السيبرانية كأدوات في صراعات أوسع نطاقا. يجب على المؤسسات الاستعداد للتهديدات السيبرانية المحتملة الناجمة عن التوترات الجيوسياسية، مثل الهجمات التي ترعاها الدول، وأنشطة القرصنة الإلكترونية، والهجمات المتتالية التي تستهدف المجتمع والصناعة[1].
- الغزو الروسي لأوكرانيا: أثارت التوترات الجيوسياسية التي أحاطت بالغزو الروسي لأوكرانيا مخاوف بشأن الحرب السيبرانية المحتملة والهجمات السيبرانية التي ترعاها الدولة. وقد سلط الصراع

الضوء على الترابط بين الأحداث الجيوسياسية ومخاطر الأمن السيبراني، مع إمكانية تصاعد الهجمات السيبرانية كجزء من صراعات أوسع نطاقا[2].

- القدرات السيبرانية للدول القومية: تخضع دول مثل روسيا والصين، المعروفتان بقدراتهما السيبرانية، للمراقبة عن كثب بحثا عن أنشطة سيبرانية محتملة مرتبطة بالتوترات الجيوسياسية. وتشكل البراعة السيبرانية لهذه الدول تهديدا كبيرا، مع احتمال شن هجمات سيبرانية تستهدف البنية التحتية الحيوية والخدمات المالية وقطاعات أخرى كجزء من استراتيجيات الجيوسياسية[3]
- الأضرار الجانبية السيبرانية العالمية: أظهرت النزاعات الجيوسياسية، مثل النزاع الروسي الأوكراني، إمكانية حدوث أضرار جانبية سيبرانية عالمية. فعلى سبيل المثال، استهدف الهجوم السيبراني "نوت بيتيا"[4]، المنسوب إلى المهاجمين السيبرانيين الروس، الأنظمة الأوكرانية في البداية، لكنه سرعان ما انتشر في جميع أنحاء العالم، مما تسبب في تعطيل واسع النطاق وخسائر مالية. أكد هذا الحادث على مخاطر امتداد الحرب السيبرانية إلى آثار عالمية أوسع نطاقا[5].
- تزايد الهجمات التي ترعاها الدول: شهدت حقبة الهجمات التي ترعاها الدول القومية تحولا نحو الهجمات التخريبية بدلا من التكتيكات التقليدية لبرمجيات الفدية الخبيثة. وتركز الفواعل التي ترعاها الدول بشكل متزايد على تعطيل العمليات الحيوية على المستوى الوطني، وتستهدف قطاعات مثل الطاقة والشحن والخدمات المالية وتصنيع الرقائق. يعكس هذا التحول الطبيعة المتطورة للتهديدات السيبرانية المتأثرة بالتوترات الجيوسياسية.

استهداف التكنولوجيا التشغيلية: أدت التوترات الجيوسياسية إلى زيادة التركيز على التكنولوجيا التشغيلية (OT) كهدف للهجمات السيبرانية. حيث يستغل المهاجمون نقاط الضعف في أنظمة تكنولوجيا المعلومات للوصول إلى بيئات التكنولوجيا التشغيلية، حيث يشكل التقارب بين تكنولوجيا المعلومات والتكنولوجيا التشغيلية تحديات أمنية. يسلط هذا الاتجاه الضوء على أهمية تأمين البنية التحتية الحيوية والأنظمة الصناعية ضد التهديدات السيبرانية الناشئة عن الصراعات الجيوسياسية[6].المؤلف (الباحث) في متن النص مختلف مراحل بحثه حسب البنية المنهجية التي يفرضها الموضوع والتخصص.

المحور الثاني: الحرب الهجينة

أولا- الحرب الهجينة: أصل المصطلح

إن مصطلح الحرب الهجينة لم يكن مرتبطا مباشرة بضم روسيا لشبه جزيرة القرم، ولأحداث المعقدة التي ظهرت في هذا النزاع، بل يعود بروزه إلى الحرب الشيشانية[7]، أين مثل المجتمع الشيشاني الهجين الخاضع للنظام القبلي العشائري أسلوب للجمع بين عناصر الحرب النظامية والغير نظامية بطريقة فعالة جدا، فهناك من يرى أن الحروب الهجينة، قد مرت على ثلاث مراحل أساسية:

1- : ساحة المعركة التقليدية، أين يتوجب التصدي لكلا التهديدات التماثلية، الغير تماثلية على حد السواء.
2- : ساحة القتال، التي يهاجم فيها السكان المحليين الغرباء، بعدائية نابعة عن قناعة.
3- : الدعم الضروري للمجتمع الدولي، لاسيما في حالة الحروب الطويلة الأمد.[8]

ثانيا-الإطار العام لفهم الحرب الهجينة

اكتسب المفهوم الجديد للتهديدات الهجينة الاعتراف عندما حقق حزب الله بعض النجاح العسكري الملموس ضد قوات الدفاع الإسرائيلية في لبنان عام 2006 أثناء حرب لبنان الثانية، ومن المفارقات أن تعريف "الهجين" كان حينئذٍ يدل على أن فاعل من غير الدول قد أظهر قدرات عسكرية توجد فقط بحوزة الدول والفواعل الدولية الرسمية) كما تشمل التهديدات متعددة الأبعاد والتهديدات المتحركة والمتنقلة وغير المتنقلة للسلم والأمن الدوليين وكذا الحرب السيبرانية وغير المتماثلة والإرهاب العالمي والقرصنة والجريمة المنظمة عبر الوطنية والتحديات الديموغرافية وأمن الموارد وانتشار أسلحة الدمار الشامل، أصبحت هذه التهديدات (المتعددة) تعرف باسم "التهديدات الهجينة (Matthews,2008) وقد تم تعريف التهديدات الهجينة من قبل القيادة الثنائية للناتو عام 2010 على أنها "تلك التهديدات التي يشكلها الخصوم مع القدرة على استخدام الوسائل التقليدية وغير التقليدية في وقت واحد بشكل تكيفي سعيا لتحقيق أهدافهم".[9]

كما ارتكز تعريف فرانك هوفمان F.Hoffman" للتهديدات الهجينة على نفس المتغيرات: بأنها تتضمن مجموعة كاملة من الوسائط المختلفة من الحرب بما في ذلك القدرات النظامية والتكتيكات والتشكيلات غير النظامية والأعمال الإرهابية بما في ذلك العنف العشوائي والإكراه والإجرام العشوائي.[10]

في نفس السياق وحسب تقرير صدر في عام 2011 يصف حلف شمال الأطلسي هذه التهديدات

"إن التهديد الهجين هو مصطلح شامل يشمل طائفة واسعة من الحوادث والأفعال السلبية مثل الإرهاب والهجرة والقرصنة والفساد والصراع العرقي وما إلى ذلك، ومع ذلك يبقى السؤال المطروح هو هل بإمكان حلف شمال الأطلسي التكيف مع استخدام المنهج لهذه الوسائل بشكل فريد ومركب من قبل الخصوم سعيا لتحقيق أهداف سياسية طويلة الأجل بدلا من حدوثها بأكثر عشوائية مدفوعا بعوامل متزامنة مع هذه التهديدات"[11]

المحور الثالث: مفهوم الأمن السيبراني

يقصد بالأمن السيبراني " Security Cyber " حماية الأشياء من خلال تكنولوجيا المعلومات مثل الأجهزة والبرمجيات ويشار إليها " ICT "وذلك اختصار Information Communication Technologies and .

وقدمت وزارة الدفاع الأمريكية تعريفا دقيقا لمصطلح الأمن السيبراني فاعتبرته " جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم: الهجمات، التخريب، التجسس والحوادث." في حين اعتبر الإعلان الأوروبي الأمن السيبراني أنه" قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات." وتجدر الإشارة إلى أن الأمن السيبراني مفهوم أوسع من أمن المعلومات، فالأمن السيبراني يهتم بأمن كل ما هو موجود على السايبر من غير أمن المعلومات، بينما أمن المعلومات لا يهتم بذلك، كما أن أمن المعلومات يهتم بأمن المعلومات الفيزيائية " الورقية"، بينما لا يهتم الأمن السيبراني بذلك.[12]

أولا: العلاقة بين الحرب الهجينة والأمن القومي

تعد العلاقة بين الأمن السيبراني والأمن القومي علاقة أساسية، حيث يلعب الأمن السيبراني دورا هاما في ضمان الأمن القومي. فالأمن السيبراني ضروري لحماية البنية التحتية الحيوية للدولة واقتصادها وسلامة مواطنيها من التهديدات السيبرانية. وقد أدى الترابط بين التكنولوجيا والبنية التحتية إلى جعل الأمن السيبراني عنصرا حاسما في مبادرات الأمن القومي. فالهجمات السيبرانية، سواء كانت من قبل دول أو مرتزقة أو مجرمين كن أن يكون لها

تداعيات كبيرة على أمن الدولة واقتصادها.وقد أطلق البيت الأبيض لاستراتيجية الوطنية للأمن السيبراني للتصدي للتهديدات السيبرانية من الدول وغير الدول وتحسين التنسيق بين القطاعين العام والخاص.

ويجب على منظمات الأمن القومي التكيف مع المشهد التكنولوجي المتطور والأهمية المتزايدة للفضاء الإلكتروني في المسائل الأمنية.ويجب على القطاعين الخاص والعام التعاون بشكل وثيق للدفاع ضد التهديدات السيبرانية بفعالية. وفي حين أن للحكومة دور في الأمن السيبراني، إلا أن هناك حاجة إلى مزيد من التعاون وتبادل المعلومات بين الحكومة والقطاع الخاص لتعزيز حماية الإنترنت. فالأصول الخاصة لا تقل أهمية عن الأصول الحكومية، ويجب على كلا القطاعين العمل معا لتعزيز دفاعات الأمن السيبراني والاستجابة للهجمات السيبرانية بفعالية .

وخلاصة القول، إن الأمن السيبراني عنصر حاسم في الأمن القومي، وهما مترابطان.وتعد تدابير الأمن السيبراني الفعالة ضرورية لحماية مصالح الدولة وبنيتها التحتية الحيوية وأمنها الشامل في مواجهة التهديدات السيبرانية المتطورة.

ثانيا: العلاقة بين الحرب الهجينة والأمن السيبراني

العلاقة بين الحرب الهجينة والأمن السيبراني معقدة ومهمة في مجال الأمن القومي. فالحرب الهجينة، وهي شكل حديث من أشكال القتال التي تجمع بين التكتيكات التقليدية وغير التقليدية، بما في ذلك الحرب السيبرانية والتضليل والضغط الاقتصادي والدعاية واستخدام القوات غير النظامية، تشكل تحديا معقدا للدول. يلعب الأمن السيبراني دورا حاسما في الدفاع ضد التهديدات الهجينة، حيث أن العمليات السيبرانية هي عنصر أساسي في تكتيكات الحرب الهجينة.وقد أدى مشهد التهديدات المتطور الذي يتسم بالجهات الفاعلة الحكومية العدوانية المنخرطة في الحرب الهجينة، إلى زيادة مخاطر الهجمات السيبرانية والمواجهة بين الدول القومية.

فالحرب الهجينة تطمس الخطوط الفاصلة بين الحرب والسلم، باستخدام مزيج من التكتيكات السيبرانية والمادية لتحقيق أهداف استراتيجية.وتشكل الهجمات السيبرانية، مثل تلك التي تنفذها جماعات القرصنة الإلكترونية التي تستهدف البنية التحتية الحيوية وتعطيل الخدمات، جزءا من استراتيجية الحرب الهجينة الأوسع نطاقا.وتؤكد الطبيعة المترابطة للعمليات السيبرانية والعواقب المادية، مثل تعطيل الوصول إلى الخدمات الحيوية، على أهمية اتخاذ تدابير قوية للأمن السيبراني في مواجهة التهديدات الهجينة[13]

وباختصار، فإن العلاقة بين الحرب الهجينة والأمن السيبراني علاقة تكافلية، حيث يعمل الأمن السيبراني كآلية دفاعية حاسمة ضد الجوانب السيبرانية لتكتيكات الحرب الهجينة.وبينما تواجه الدول التحديات التي تفرضها التهديدات الهجينة، فإن اتباع نهج شامل يدمج استراتيجيات الأمن السيبراني مع جهود الأمن القومي الأوسع نطاقا أمر ضروري للتخفيف من المخاطر المرتبطة بأشكال الصراع الحديثة.[14]

المحور الخامس: الإطار العام لفهم العلاقة بين الحرب الهجينة وتهديدات الفضاء السيبراني

أولا: على مستوى الدولة

من أكثر نقاط الضعف خطورة ما يتعلق بمستوى الدول القومية أين يتم احتواء غالبية السياسات السيبرانية الحالية من خلال الحدود الوطنية، ولم يظهر حتى الآن نهج دولي قابل للتطبيق لإدارة الفضاء السيبراني، كما تواجه

الدول القومية موقفا صعبا بشكل متزايد في هذا الصدد لأن استخدام الفضاء السيبراني يثبط مبدأ عدم التناسق الكلي، إذا تعرضت أنظمة المعلومات الخاصة والعامة للهجوم من قبل مجموعة صغيرة من متخصصي تكنولوجيا المعلومات ذوو الأساليب الإلكترونية المتقدمة قد يتخذ أحد الرّاعات الأكثر رعبا في الفضاء السيبراني شكل هجوم إلكتروني مدمر ضد البنية التحتية الحيوية للبلد إلى جانب الهجمات المادية ، والتي قد أو قد لا تحدث أثناء نزاع عسكري.ومع ذلك، فإن الهجمات الإلكترونية خلال نزاع عسكري (مناسب) لن تكون مشكلة بالنسبة للمحللين، لأنه في حالة الحرب الكاملة، تستعد معظم الدول القومية لعملية شبكة كمبيوتر كلاسيكية ضد البنية التحتية للاتصالات العسكرية، نظرا لأن هذا التهديد لم يعد جديدا بعد الآن ، فقد أمنت معظم الدول اتصالاتها العسكرية بشكل معقول ، وخطر الهجمات غير المتكافئة هنا أقل أهمية مقارنة بالبنية التحتية المدنية الضعيفة. بشكل عام، أدركت الدول القومية بالفعل أن دور الجيش التقليدي سوف يتضاءل في الرّاعات الحديثة.

ثانيا: على المستوى المجتمعي

يرتبط هذا المستوى من نقاط الضعف تجاه الفضاء السيبراني بالتأثيرات المجتمعية للأنشطة المشبوهة عبر الإنترنت، كما يتضمن تكوين شبكات اجتماعية تقلل الثقة بين الأفراد، وكذلك الأساليب التي يتم استخدامها لتحريض، أو ترهيب، أو الترويج، أو إقصاء الفواعل المجتمعية أو مجموعات معينة في المجتمع.

في سياق آخر، سرعت الوسائط الاتصالية الحديثة طرق الاتصال بين الأفراد بشكل كبير في الفترة القصيرة الماضية في إطار التحول إلى مجتمع رقمي حديث، غير أن الاعتماد المفرط على هذه الوسائط وفي حال حدوث أي عطل تقني سيؤثر على عدد كبير من الأشخاص، بشكل مباشر أو العكس، حيث نجد أن سرقة الهوية عبر الشبكات الاجتماعية، يصنف على أنه التهديد السيبراني الأكثر شيوعا في السنوات القليلة الماضية، ولا يزال الكثير من الأفراد غير مدركين لكيفية تجنب هذا النوع من الهجمات على هويتهم.

كما يمكن أن تكون الإنترنت جزءا من الرّاعات المستقبلية، وسيتم استخدامها بشكل متزايد أثناء الرّاعات كوسيلة للتأثير على الرأي العام الدولي أو الرأي العام لدولة معينة، أو مجموعة داخل بلد ما، وهنا يظهر الانعكاس المباشر على الأمن المجتمعي والأمن الثقافي بإمكانية بناء خلفية بمحتويات خاطئة أو موجهة، وتقييد الوصول إلى المعلومات الموضوعية والصحيحة، مما يجعل المجتمع في انكشاف معلوماتي كامل.[15]

مخطط رقم (01): انماط التهديدات السيبرانية

مصدر التهديد	الشرح	أمثلة
جنسيات مختلفة	شن هجمات إلكترونية على الأفراد والمنظمات من الدول لأخرى	الحروب الإكتروني بين القراصنة في دول مختلفة وضد جنسيات مختلفة
أيديولوجية مختلفة	استخدام الهجمات الإلكترونية كأداة لمهاجمة أيديولوجية معينة	لأعمال العدائية الإلكترونية المرتبطة بدوافع لاختلاف الإديولوجي: روسيا-الو.م.أ، إيران-
ديانة مختلفة	استخدام الهجمات الإلكترونية ضد من تحدي المعتقدات والقيم الدينية	السيبرانية الحروب :الهند وباكستان الكيان الصهيوني وفلسطين
الطبقات المتميزة اقتصاديا	شن هجمات إلكترونية ذات دوافع مالية ضد لأغنياء "الشركات، رجال لأعمال"	استهداف الشركات الخاصة في دول مختلفة

المصدر :

Nir Kshetri and Lailani Laynesa Alcantara, Cyber-threats and cybersecurity challenges: A cross-cultural perspective, Manuscript of a book chapter published by Routledge in The Routledge Companion to Cross-Cultural Management on 24 April 2015, available online:

http://www.routledge.com/9780415858687

في السياق ذاته، يوضح المخطط أنماط ومصادر وأهداف التهديدات السيبرانية في مجالها لاجتماعي والاقتصادي، حيث تتميز بالشمولية والتنوع والدقة في تحديد الأهداف وكيفية الوصول إليها، انطلاقا من الدوافع المختلفة التي تؤدي إلى شن هجمات سيبرانية حسب نوع المهمة الموكلة للمهاجمين أو القراصنة، ويختلف الهدف باختلاف الدافع والجهة التي تقف خلفه.

المحور السادس: الحرب الهجينة ولأمن السيبراني: مجالات وأنماط التهديد

لقد ازدادت سرعة التهديدات الهجينة وحجمها وشدتها في السنوات لأخيرة، وقد سهل من ذلك التقدم التكنولوجي السريع والترابط العالمي. تستفيد الجهات الفاعلة من الدول وغير الدول المنخرطة في الحرب الهجينة من العمليات السيبرانية لزرع الشك وخلق الفوضى وتقويض أمن السكان المستهدفين.ويؤدي استخدام الهجمات السيبرانية وحملات التضليل والتكتيكات غير العسكرية لأخرى إلى طمس الخطوط الفاصلة بين الحرب والسلم، مما يجعل من الصعب اكتشاف الأنشطة الهجينة الجارية وإسنادها[16].

وعلاوة على ذلك، تستخدم تكتيكات الحرب الهجينة، مثل الدعاية والخداع والتخريب ونشر الجماعات المسلحة غير النظامية، لخلق حالة من الغموض والغموض، مما يجعل من الصعب الرد بفعالية على هذه التهديدات. الهدف من الحرب الهجينة هو زعزعة استقرار المجتمعات، وإحداث الفوضى، وإشاعة حالة من عدم اليقين، وهو ما يمكن أن يكون له آثار مباشرة على لأمن السيبراني من خلال استهداف الأنظمة والبيانات وشبكات الاتصالات الحيوية[17].

وعليه، إن تهدد الحرب الهجينة الأمن السيبراني من خلال استغلال نقاط الضعف في الأنظمة المترابطة، والاستفادة من الهجمات السيبرانية كجزء من استراتيجية أوسع لتحقيق أهداف استراتيجية، وخلق بيئة صعبة قد لا تكون فيها آليات الدفاع التقليدية كافية لمواجهة التهديدات المتنوعة والمتطورة التي تشكلها التكتيكات الهجينة.

أولا: أنماط الهجمات السيبرانية المستخدمة في الحرب الهجينة

العمليات السيبرانية المدمرة: تتضمن هذه العمليات إتلاف أو تعطيل أنظمة الحاسوب أو الشبكات أو البنية التحتية لتحقيق أهداف استراتيجية، يمكن أن تستهدف هذه العمليات أنظمة حساسة، مسببة أضرارا مادية أو تعطيلات تشغيلية.

- العمليات التي تركز على التجسس: التجسس الإلكتروني هو تكتيك شائع في الحرب الهجينة، حيث يتسلل المهاجمون إلى الشبكات لسرقة معلومات حساسة أو ملكية فكرية أو بيانات سرية. يمكن استخدام هذه المعلومات لتحقيق ميزة استراتيجية أو لتقويض أمن الهدف[18].
- استخدام المعلومات المضللة كسلاح: قد ينشر المهاجمون السيبرانيون معلومات كاذبة أو مضللة على الإنترنت للتلاعب بالرأي العام أو زرع الفتنة أو خلق البلبلة.ويمكن استخدام هذا التضليل للتأثير على القرارات السياسية أو التحريض على الاضطرابات أو تقويض الثقة في المؤسسات[19].
- عمليات القرصنة الإلكترونية: قد تشن مجموعات القرصنة الإلكترونية هجمات إلكترونية أو سرقة بيانات ضد خصوم متصورين لتعزيز أجنداتهم الأيديولوجية أو السياسية. يمكن أن تتراوح هذه الهجمات من تشويه المواقع الإلكترونية إلى اختراق البيانات بهدف تعطيل العمليات أو التسبب في الإضرار بالسمعة.
- استهداف البنية التحتية الحيوية: يمكن أن يكون للهجمات السيبرانية على البنية التحتية الحيوية، مثل شبكات الطاقة أو أنظمة النقل أو الشبكات المالية، عواقب وخيمة في الحرب الهجينة. يمكن أن يتسبب تعطيل هذه الأنظمة في إحداث فوضى واسعة النطاق وأضرار اقتصادية وتهديد الأمن القومي.

توضح هذه الأمثلة المجموعة المتنوعة من الهجمات السيبرانية المستخدمة في الحروب الهجينة، مما يسلط الضوء على الطبيعة المعقدة والمتطورة للنزاعات الحديثة التي تمزج بين التكتيكات التقليدية وغير التقليدية لتحقيق أهداف استراتيجية.

- في السياق ذاته تظهر بعض التكتيكات التي تعتمد عليها الحروب الهجينة في المجال السيبراني للتأثير على الحياة المجتمعية:

- حملات المعلومات الكاذبة: نشر معلومات كاذبة أو مضللة من خلال قنوات مختلفة، مثل وسائل التواصل الاجتماعي أو المواقع الإلكترونية أو وسائل الإعلام التقليدية، للتلاعب بالرأي العام أو زرع الفتنة أو خلق الاستقرار.

- الدعاية والروايات المضللة: استخدام الدعاية للترويج لأجندة معينة أو تشويه الحقائق أو التلاعب بالتصورات. يتم صياغة الروايات المضللة للتأثير على عمليات صنع القرار وتشكيل الخطاب العام.
- حملات التشهير: استهداف الأفراد أو المنظمات أو الدول باتهامات كاذبة أو اغتيال الشخصية أو الدعاية السلبية للإضرار بالسمعة وتقويض المصداقية.
- نظريات المؤامرة: الترويج لنظريات المؤامرة التي لا أساس لها من الصحة أو المختلقة لخلق الشك وانعدام الثقة والانقسام داخل المجتمعات. يمكن استخدام هذه النظريات للتلاعب بالمعتقدات والتصورات لأغراض استراتيجية[20].
- شبكات الروبوتات وشبكات الروبوتات: إنشاء حركات شعبية وهمية أو استخدام شبكات الروبوتات الآلية لتضخيم رسائل معينة، أو تضخيم الدعم بشكل مصطنع، أو التلاعب بالمناقشات عبر الإنترنت للتأثير على الرأي العام.
- التسريبات الانتقائية وعمليات القرصنة: نشر معلومات مفبركة أو محررة بشكل انتقائي أو بيانات مسروقة أو وثائق سرية لتشويه سمعة الأفراد أو المنظمات، أو خلق الفوضى، أو التأثير على عمليات صنع القرار[21].

هذه التكتيكات مصممة لاستغلال نقاط الضعف والتلاعب بالتصورات وتقويض الثقة في المؤسسات، مما يجعل التضليل أداة قوية في استراتيجيات الحرب الهجينة التي تهدف إلى زعزعة استقرار الخصوم وتحقيق أهداف استراتيجية.

المحور السابع: تحديات تحقيق لأمن السيبراني

تحديات لأمن السيبراني تشمل عدة جوانب مهمة تؤثر على لاستقرار ولأمن، وتتضمن:

- محاولات لاختراق والتجسس: تزايد التهديدات السيبرانية تجعل الدول عرضة لمحاولات اختراق وتجسس تستهدف البنية التحتية الحيوية والمعلومات الحساسة، مما يعرض لأمن الوطني للخطر.
- ضرورة تثمين العنصر البشري: تحقيق لأمن السيبراني يتطلب تثمين العنصر البشري وتطوير كفاءات متخصصة قادرة على التصدي للتهديدات السيبرانية بفعالية.
- تطوير استراتيجيات وطنية متكاملة: الحاجة لتطوير استراتيجية وطنية شاملة في المجال الرقمي تجمع بين لاستباق والوقاية لمواجهة التحديات المتزايدة في الفضاء السيبراني[22]
- تكوين كوادر الدفاع ولأمن: إنشاء مدارس خاصة للأمن السيبراني تهدف إلى تخريج وتكوين كوادر متخصصة في مجال الدفاع ولأمن السيبراني لحماية البيانات والبنية الرقمية.
- التحديات الوطنية والعالمية: تزايد التهديدات السيبرانية يفرض على الدفاع الوطني للدول تحقيق لأمن السيبراني وتطوير استراتيجيات فعالة لمواجهة التحديات الوطنية والعالمية في الفضاء السيبراني.

إن هذه التحديات تبرز أهمية تعزيز القدرات السيبرانية وتطوير استراتيجيات شاملة للأمن السيبراني في الجزائر للحفاظ على الاستقرار والأمن الوطني في ظل التطورات الرقمية والتهديدات المتزايدة في الفضاء السيبراني.[23]

الخاتمة

1- إن قضية الحروب الهجينة وعلاقتها بالأمن السيبراني تبقى قضية معقدة بتعقد متغيراتها، والتي تختلف طبيعتها حسب النمط الذي يستخدمه المهاجمون أو الفواعل المنخرطة في الحرب الهجينة.

2- يبقى الأمن السيبراني مرتبط بشكل كبير في الاستثمار في العنصر البشري القادر على رفع التحدي في مواجهة المهددات السيبرانية بمختلف أنواعها.

3- الشراكات الأمنية في المجال السيبراني خصوصا مع الأطراف والفواعل ذات السبق والخبرة في مجال الهجمات السيبرانية وصدها.

4- البناء المجتمعي لأي دولة يبقى مهددا بشكل مباشر من خلال التدفقات السيبرانية المتنوعة، وعليه يجب خلق ثقافة أمنيةرقمية لدى الأفراد للتعامل مع بعض مهددات الأمن السيبراني.

5- الأمن القومي يبنى في جانب كبير منه من خلال التحكم في الفضاءات الرقمية ومهددات الأمن السيبراني وارتدادات الحروب الهجينة إن وجدت.

6- تعقد مفهوم التهديد الأمني وتجاوزه النمط التقليدي إلى أنماط أكثر صعوبة في الملاحظة والتفسير والمواجهة، جعل قضية تعريف الأمن القومي محل جدل من جديد.

7- تبقى الحروب الهجينة نتيجة حتمية لسلوك الفواعل الدولية المبني على التنافس في المجال السيبراني في شقه السلبي، حيث تغير نمط التنافس من الأسلحة النووية "والذي لم ينته بعد" إلى نمط أشد تعقيدا قد يجعل الأسلحة النووية نفسها محل تهديد في المستقبل القريب، وهو ما يرهن الأمن العالمي بشكل مباشر.

الهوامش والمراجع:

[1] Anna Rebeiro, Growing Convergence Of Geopolitics And Cyber Warfare Continue To Threaten OT And ICS Environments In 2024, FEBRUARY 18, 2024, https://cutt.ly/5w3SzduO

[2] David Braue, How Geopolitics Affects Cybersecurity, Cybercrime Magazine, Jan. 19, 2023, Https://Cybersecurityventures.Com/How-Geopolitics-Affects-Cybersecurity/

[3] Beth Maundrill, Geopolitical Tensions Expected To Further Impact Cybersecurity In 2023, Info Security Magazine, 29 DEC 2022, Https://Www.Infosecurity-Magazine.Com/News/Geopolitical-Tensions-Impact/

[4] الفيروس الجديد هو نسخة معدلة عن برنامج "بيتيا" الخبيث الذي ضرب العديد من الأجهزة هذا العام وطلب القراصنة من رواد شبكة الانترنت دفع فدية مقابل استرجاع بياناتهم، ويعتقد أن الهجوم الإلكتروني الجديد انطلق أولا في أوكرانيا حيث أعلنت الحكومة عن تعرض شبكة حواسيبها لهجمات استهدفت البنية التحتية وشركات للطاقة على رأسها محطة تشرنوبل النووية.

[5] David Braue, Ibid.

[6] Anna Rebeiro, Ibid.

[7] حرب الشيشان الثانية:والمعروفة أيضا باسم حرب شمال القوقاز، نزاعا بين الاتحاد الروسي وجمهورية إيتشكيريا الشيشانية وقع في الفترة من أغسطس 1999 إلى أبريل 2009.وقد اتسمت هذه الحرب بمزيج من التكتيكات التقليدية وغير التقليدية، بما في ذلك الحرب الإلكترونية، والتضليل الإعلامي، والضغط الاقتصادي، والدعاية، واستخدام القوات غير النظامية.وكان للنزاع أثر كبير على المنطقة والعلاقات الدولية على حد سواء، حيث لعبت الطبيعة المترابطة للعمليات السيبرانية والعواقب المادية دورا حاسما في ديناميكيات الحرب.

[8] أسماء حداد، الحروب الهجينة:الأزمة الأوكرانية أنموذجا، مجلة مدارات سياسية، ديسمبر، 2017، ص ص114-126

[9] عزيز نوري، سميرة سليمان، التهديدات الهجينة بين إشكالية التعريف وأنماط المواجهة، المجلة الجزائرية للأمن والتنمية، المجلد 10، العدد 01، جانفي 2021، ص479.

[10] عادل جارش، مقاربة معرفية حول التهديدات الأمنية الجديدة، مجلة العلوم القانونية والسياسية، 2016

[11] عزيز نوري، سميرة سليمان، المرجع نفسه، ص 480

[12] منى عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، عدد111 يوليو، 2020.ص 01.

[13] Frederic Lemieux & Chuck Brooks, New Cooperative Cyber security Models Needed in an Era of Global Risk, https://cutt.ly/dw3SxgGR

[14] Ibid.

[15] Ibid.

[16] Mattias Engström, Hybrid Warfare and the Effects of Hybrid Threats on Cybersecurity, 2022-08-18, https://www.truesec.com/hub/blog/hybrid-warfare-and-cyber-security

[17] North Atlantic Treaty Organization, Countering hybrid threats, 07 Mar. 2024 https://www.nato.int/cps/en/natohq/topics_156338.htm

[18] Symen Hoekstra and Maaike Jongema, Disinformation as a weapon in hybrid warfare, Stichting Atlantische Commissie, Atlantisch Perspectief , 2016, Vol. 40, No. 5 (2016), pp. 37-39, Or visit Stable URL: https://www.jstor.org/stable/10.2307/48581310

[19] قبل أكثر من 2400 عام، جعل الفيلسوف والاستراتيجي العسكري الصيني صن تزو من بديهيات الحرب أنه من الأفضل "إخضاع العدو دون قتال". باستخدام المعلومات -أو المعلومات المضللة، أو الدعاية -يمكن أن يكون السلاح إحدى الطرق لزعزعة استقرار السكان وتعطيل الدولة المستهدفة.

[20] Christoph Deppe, Disinformation In Cognitive Warfare, Fimi, Hybrid Threats, The Defence Horizon Journal, October 16, 2023, Or, Visit online : https://tdhj.org/blog/post/disinformation-cognitive-warfare-hybrid/

Fimi: Foreign Information Manipulation and Interference(التلاعب بالمعلومات الخارجية والتدخل في المعلومات الأجنبية)

[21] Ibid.

[22] الأمن السيبراني يشغل السلطات العليا في الجزائر..وحديث عن "محاولات اختراق وتخريب وتجسس"، جريدة القدس العربي، 2023/06/08 /https://cutt.ly/dw3AgaHC

[23] سمير بارة، الأمن السيبراني (cyber Security) في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، المجلد الثاني، العدد الثاني، 2017، ص ص 255

الإنترنيت المظلم كفضاء للجريمة المنظمة السيبرانية في ظل الثورة التكنولوجية الرابعة

– مقاربة مفاهيمية -

The Dark Internet as a space for cyber organized crime in light of the fourth technological revolution

- Conceptual approach -

د. إيمان بن نعجة(*) جامعة الجزائر 3، البريد المهني bennadja.imene@univ-alger3.dz

ملخص:

تشكل الثورة التكنولوجية الرابعة، مع التطورات المتسارعة في تكنولوجيا المعلومات والاتصالات، بيئة خصبة لنمو وانتشار الجريمة المنظمة السيبرانية. ويعد الإنترنت المظلم، ذلك الفضاء الإلكتروني المخفي عن محركات البحث التقليدية، ملاذاً آمنا لهذه الجرائم، حيث يتيح للمجرمين التواصل والتخفي وإجراء معاملاتهم وممارسة نشاطاتهم غير القانونية دون رقابة أو ملاحقة.

وعليه، سيتم التطرق في هذا المقال إلى مدخل مفاهيمي لفهم ماهية الجريمة المنظمة السيبرانية، محددا مستويات شبكة الإنترنت، والخصائص التي تميز الإنترنت المظلم، إلى جانب أنواع الجرائم المنظمة السيبرانية وفق أهدافها، والبرامج والأدوات المستخدمة في هذا الفضاء مع تقديم أمثلة توضيحية مصورة تساهم في تقريب وتبسيط هذه الأدوات، ومن ثم تختتم بالحديث عن الثورة التكنولوجية الرابعة وعلاقتها بانتشار هذه الجرائم المنظمة السيبرانية.

الكلمات المفتاحية: الجريمة السيبرانية؛ الإنترنيت المظلم؛ الإنترنيت العميق؛ التكنولوجيا؛ الذكاء الاصطناعي.

Abstract:

The fourth technological revolution, with rapid developments in information and communications technology, constitutes a fertile environment for the growth and spread of cyber organized crime. The Dark Internet, the electronic space hidden from traditional search engines, is a safe haven for these crimes, as it allows criminals to communicate, hide, conduct their transactions, and carry out their illegal activities without supervision or prosecution.

Therefore, this article will address a conceptual introduction to understanding what cyberorganized crime is, specifying the levels of the Internet, the characteristics that distinguish the dark web, in addition to the types of cyberorganized crimes according to their goals, and the programs and tools used in this space, while providing illustrated illustrative examples that contribute to approximating and simplifying These tools then conclude by talking about the fourth technological revolution and its relationship to the spread of these organized cybercrimes.

KeyWords: ***Cyber crime; Dark Internet; Deep internet; Technology; Artificial intelligence.***

مقدمة:

شهد العالم ثورة تكنولوجية هائلة مع ازدياد الاعتماد على الإنترنيت في مختلف جوانب الحياة، في ظل الثورة الصناعية الرابعة التي تتميز بدمج التقنيات التي تطمس الخطوط الفاصلة بين المجالات المادية والرقمية والبيولوجية، من خلال استخدام الذكاء الاصطناعي في متباين المجالات، إلى جانب تحليل البيانات الضخمة لاتخاذ القرارات وغيرها من الخصائص التي أتاحتها.

لكن في المقابل، ظهرت مخاطر جديدة أوجدتها هذه الثورة التكنولوجية، من بينها مخاطر وتهديدات في مجال الأمن السيبراني. خاصة مع وجود الإنترنت المظلم Dark web، هذا الأخير يعد شبكة خفية من المواقع الإلكترونية التي لا يمكن الوصول إليها إلا باستخدام برامج خاصة حيث أصبح فضاء خصبا للجريمة المنظمة في الفضاء السيبراني Cyber Space.

وبينما ينظر إليه من قبل البعض كفضاء للإعلام الإلكتروني الحر، يرى آخرون أنه تهديد خطير للأمن السيبراني للدول.

المحور الأول: مدخل مفاهيمي إلى الجريمة المنظمة السيبرانية

إن مفهوم الجرائم الإلكترونية لم يحدده القانون، حتى لو كانت أكثر من 470 جريمة مرتبطة بأنظمة المعلومات. وتأتي كلمة " cyber " من الكلمة اليونانية kubernêsis والتي تعني "الحكم أو التوجيه". هذه البادئة مستعارة أيضا من مصطلح "علم التحكم الآلي" من أعمال عالم الرياضيات الأمريكي Norbert Wiener، الذي يتناول دراسة التحكم والتواصل في الحيوانات وفي الآلات. واليوم، تستخدم مصطلحات "الأمن السيبراني" و"الدفاع السيبراني" و"الجريمة السيبرانية" بشكل مترابط دون النص على تعريفات دقيقة في القانون. لذلك، حتى لو كان هذا الأخير يفهم الجريمة السيبرانية من خلال تكريس العديد من الجرائم، فإن الجريمة السيبرانية لا تصلح بشكل جيد للتعريف، الذي طرحته المفوضية الأوروبية صراحة في رسالة إلى البرلمان الأوروبي في عام 2007: "الافتقار إلى تعريف مقبول بشكل عام للجريمة السيبرانية"1.

ومع ذلك، تفهم الجريمة السيبرانية من خلال ارتكاب جرائم جنائية ضد أو عن طريق نظام معلومات واتصالات، وخاصة الإنترنت، باستخدام الشبكات أو أنظمة المعلومات كوسيلة، أو جعلها هدفا. وبحسب الأمم المتحدة، فإنها"أي سلوك غير قانوني يتضمن عمليات إلكترونية تهدف إلى أمن أنظمة المعلومات والبيانات التي تعالجها".ووفقا لمنظمة التعاون الاقتصادي والتنمية، تشمل الجرائم السيبرانية "أي سلوك غير قانوني أو غير أخلاقي أو غير مصرح به يتضمن معالجة البيانات تلقائيا و/أو نقل البيانات"2.

يقصد بالجريمة السيبرانية Cyber crime تلك "الهجمات التي تتم باستخدام آليات وشبكات الانترنيت وأجهزة الحاسوب الآلي، وتهدف إلى إلحاق الضرر بالأجهزة والشبكات الالكترونية ذات الاتصال بالانترنيت"3 .

أما الجريمة المنظمة Organized crime فقد "استفادت كثيرا من التطور الذي شهدته التكنولوجيا الرقمية في تنفيذ هجماتها سواء على الكيانات الرسمية ممثلة في الدول او غير الرسمية، إذ تقوم بعمليات القرصنة السيبرانية واختراق الحسابات خاصة منها المالية بهدف سرقة الاموال، وكذا استفادت من الفضاء السيبراني في تجارة ونقل الأسلحة، تجارة المخدرات، تجارة (تسليع) الهجرة غير الشرعية، المتاجرة بالأعضاء البشرية، التهريب،.. وهو ماكان له بالغ الأثر على اقتصادات الدول"4 .

وعليه تعرف الجريمة المنظمة السيبرانية Cyber organized crime بأنها مجموعة من الأنشطة الإجرامية التي ترتكب باستخدام تكنولوجيا المعلومات والاتصال، حيث تتميز بتنظيمها العالي وخطورتها على المجتمع. وتشمل كلا من الاحتيال وتجارة المخدرات، الأسلحة، غسيل الأموال، القرصنة الإلكترونية، الإتجار بالبشر. كما تتعدد دوافعها بين الأرباح المالية كدافع رئيس للجريمة المنظمة السيبرانية، إلى جانب السلطة حيث تسعى بعض العصابات الإجرامية إلى استخدام الإنترنت لتعزيز نفوذها وسيطرتها إلى جانب الانتقام والتخريب.

تجدر الإشارة إلى أن الجريمة المنظمة غير تقليدية لأنها أصبحت أكثر احترافية، تهدد الدول والمجتمعات من خلال تجاوز الحدود في تهديد الأمن الجماعي 5 . وقد عرفت بعد الحرب العالمية الثانية بالمافيا، وأول مكان انطلقت منه جزيرة صقليا بإيطاليا 6.

عرفها المشرع الجزائري بأنها: " جمعية أو اتفاق مهما كانت مدته أو عدد أعضاءه تشكل أو تؤلف بغرض الأعداد لجنايات أو لجنح ضد الأشخاص أو الممتلكات وذلك بقصد الربح على أن يتعدى العمل الإجرامي الحدود الوطنية، كما يمكن اعتبارها جريمة احترافية أو جريمة متقنة، جريمة مخططة، جريمة عابرة للقارات مع اتساع مجال نشاطها واتخاذها لأشكال الإجرام مع استعمال العنف"7.

وقد واجه المشرع الجزائري تحديات كبيرة في مواكبة التطورات المتسارعة في مجال الجريمة المنظمة السيبرانية.

- تم تعديل قانون العقوبات الجزائري عام 2004 ليشمل جرائم المعلوماتية.
- تم إصدار قانون مكافحة جرائم تكنولوجيا المعلومات والاتصال عام 2012.
- تم إصدار قانون حماية المعطيات ذات الطابع الشخصي عام 2018.

وبالتالي بخصوص تعريف الجريمة المنظمة السيبرانية في القانون الجزائري، يمكن القول أنه لم يقدم تعريفا محددا لها. لذلك يمكن تعريفها بأنها مجموعة من الأفعال الإجرامية التي ترتكب باستخدام تكنولوجيا المعلومات والاتصال، ويتميز بتنظيمها العالي وخطورتها على المجتمع.

تشير التقديرات إلى أنه في عام 2021، كان 33% من سكان أفريقيا متصلين بالإنترنت، بزيادة قدرها 23% تقريبا مقارنة بعام 2018. وقد نما استخدام التكنولوجيا الرقمية بها بشكل كبير في السنوات الأخيرة، مما أدى في الوقت نفسه إلى زيادة التهديد المرتبط بالجرائم السيبرانية التي تسهلها التكنولوجيا، من استغلال للأطفال وإساءة معاملتهم عبر الإنترنت إلى تخريب البنية التحتية والجريمة المنظمة، بما في ذلك الاتجار بالمخدرات والبشر، لذلك تواجه

الحكومات الأفريقية تهديدات رقمية سريعة التطور، والتي إذا لم يتم التعامل معها بشكل مناسب يمكن أن يكون لها تداعيات سلبية على أمن واقتصاد البلدان 8 .

المحور الثاني: مستويات شبكة الإنترنيت

تنقسم الشبكة العالمية للإنترنيت إلى ثلاثة أقسام رئيسة، يمكن تلخيصها فيما يلي:

أولا-الإنترنيت السطحي Surface Internet:

يمثل الجزء المرئي من الإنترنت الذي يمكن الوصول إليه من خلال محركات البحث العادية التي نستعملها جميعا.

ويستخدم هذا المصطلح في جميع المواقع التي يمكن الوصول إليها من خلال محركات البحث العادية مثل Google.ويسمى أيضا المحتوى المفهرس. يتضمن محتوى هذا الجزء من الإنترنيت جميع المواقع المعروفة التي نتعامل معها في حياتنا اليومية ويمكن الوصول إليها من خلال أي متصفح مثل Opera أو Firefox أو Chrome Chrome. 9

ثانيا-الإنترنيت العميق Deep Web:

ويمثل الجزء غير المرئي من الإنترنت الذي لا يمكن الوصول إليه من خلال محركات البحث، يشار إليها أحيانا بالإنترنت السفلي أو الإنترنت المخفي ويتكون من محتوى لا يمكن لمحركات البحث التقليدية الوصول إليه لأي سبب من الأسباب.

غالبا ما يستخدم مصطلح Deep Web بشكل خاطئ للدلالة على الإنترنت المظلم، يشمل هذا الجزء كلا من:

- صفحات الويب المحمية بكلمة مرور.
- قواعد البيانات الداخلية للمؤسسات.
- المحتوى المدفوع والخدمات المصاحبة له.
- الشبكات الخاصة

ثالثا-الإنترنيت المظلم (Dark Web) Dark Internet:

هو جزء من الإنترنيت العميق ويعد شبكة خفية من المواقع الإلكترونية لا يمكن الوصول إليه باستخدام المتصفحات العادية، إنما يتطلب ذلك استخدام برامج وتقنيات خاصة تتميز بتشفير البيانات وحماية هوية المستخدمين.

فشبكة الويب المظلمة، تعد واحدة من أكبر الشبكات في العالم للجريمة والإرهاب عبر الإنترنت، معروفة جيدا بكونها غير خاضعة للرقابة وفوضوية وتستخدم في المقام الأول في أنشطة غير قانونية 10.

لذلك يعد أظلم جزء من الإنترنت المخفي للمحتوى، حيث يتضمن أنشطة غير قانونية يتم، وغالبا ما تحمل المواقع فيه عناوين غير مهمة تنتهي بنطاقات غير مألوفة مثل .ion، ويشمل الأنترنيت المظلم ما يلي:

- أسواق المخدرات والأسلحة.
- منتديات القرصنة.
- مواد إباحية غير قانونية.
- أنشطة إجرامية أخرى.

تقسيمات الشبكة العالمية للإنترنيت

مصدر الصورتان: https://twitter.com/ScienceCQFD/status/847087942707359744

بناء على ما هو موضح في الصورتين، حيث تم تمثيل الإنترنت على شكل جبل، والجزء المرئي من الجبل هو الإنترنت السطحي. بينما الجزء المخفي تحت البحر هو الإنترنت العميق والمظلم.
والملفت في الموضوع هي أن هذا المحتوى، على الرغم من حجمه الهائل، لا يشكل سوى 5% من إجمالي الإنترنت وفي لإحصائيات لأخرى 0.03% فقط (مصدر OEDB). وفي أكثر لإحصائيات تفؤلا لا تتجاوز 10%/

المحور الثالث: الخصائص التي تجعل الإنترنيت المظلم فضاءا مناسبا للجريمة المنظمة السيبرانية:

يتميز الإنترنيت المظلم بمجموعة من الخصائص التي جعلته فضاءا مناسبا بعالم الجريمة المنظمة السيبرانية، ولعل أبرزها هو:

- السرية: صعوبة تعقب المجرمين بسبب إخفاء هوياتهم. ومع ذلك، تعمل وكالات إنفاذ القانون باستمرار على تحسين قدرتها على تعقب المجرمين على الويب المظلم 11.
- سهولة الوصول: توفر أدوات وبرامج سهلة لاستخدام للوصول إلى الإنترنت المظلم.
- العملات الرقمية: استخدام العملات الرقمية المشفرة مثل Bitcoinلإخفاء هوية المجرمين وتسهيل عمليات الدفع.

المحور الرابع: أنواع الجرائم المنظمة السيبرانية وفق أهدافها عبر الإنترنيت المظلم:

على الرغم من وجود عدد كبير من تعريفات الجرائم السيبرانية، إلا أنها تميل إلى تصنيف الجرائم إلى فئتين: بعضها تتم محاولة ارتكابه أو ارتكابه ضد أنظمة معالجة البيانات الآلية (STAD)، بينما يتم ارتكاب البعض الآخر من خلال هذه الأنظمة. يتعلق الأول على وجه الخصوص بالوصول غير المصرح به إلى هذه الأنظمة، أو الهجمات على سلامة البيانات وأنظمة الكمبيوتر، أو الهجمات على سريتها؛ المجموعة الأخيرة هي جرائم القانون العام المرتكبة باستخدام نظام معالجة البيانات الآلي، مثل الاحتيال أو التزوير.وهذا يعني أن الجريمة السيبرانية تغطي بعدا مهما نظرا لتنوع الأعمال غير القانونية المرتكبة وطبيعتها الدولية والأضرار التي تلحق بالدول والشركات والأفراد 12.

وبشكل عام، يمكن تصنيف أو تقسيم الجرائم السيبرانية وفق أهدافها إلى جزئين:

أولا-جرائم مالية ضد الملكية:

تتمثل في نقل البرمجيات الضارة المضمنة في بعض البرامج الت طبيقية والخدمية أو غيرها، بهدف تدمير الأجهزة أو البرامج المملوكة للشركات أو الأجهزة الحكومية أو البنوك أو حتى الممتلكات الشخصية.

ثانيا-جرائم إرهابية ذات أهداف سياسية وأيديولوجية:

يكون هذا النوع من الجرائم السيبرانية ضد الحكومات، حيث يتم من خلالها مهاجمة المواقع الرسمية وأنظمة الشبكات الحكومية والتي تستخدم تلك التطبيقات على المستوى المحلي والدولي إذ تركز على تدمير البنى التحتية ومهاجمة شبكات الكمبيوتر.

تعد الجريمة المنظمة السيبرانية من أخطر الظواهر المعاصرة التي تهدد المنظمات والمؤسسات المختلفة للدول واقعيا وسيبرانيا، لذلك هي ليست بمعزل عن الجريمة المنظمة في الواقع الحقيقي ولا بديلا عنها، إنما هي إمتداد ودعم لها.

وعليه يمكن القول أن أنواع الجرائم المنظمة السيبرانية على الإنترنت المظلم تتمحور حول ما يلي:

- الاحتيال: سرقة البيانات الشخصية والمالية.
- تجارة المخدرات والأسلحة: بيع وشراء المواد غير القانونية.
- غسيل الأموال: إخفاء مصدر الأموال غير المشروعة.
- القرصنة الإلكترونية: اختراق أنظمة المعلومات وسرقة البيانات.
- الإتجار بالبشر: استغلال الأشخاص لأغراض جنسية أو عمالية.

المحور الخامس: برامج وأدوات فضاء الجريمة المنظمة السيبرانية:

سيتم التطرق في هذا العنصر إلى شرح (من خلال صور توضيحية) إلى كيفية الولوج إلى فضاء الجريمة المنظمة السيبرانية وتبيان نماذج وأمثلة عن المواقع المستخدمة.

تحديد موقع الجريمة المنظمة من الفضاء السيبراني

مصدر الصورة: https://images.app.goo.gl/xTyEzEcTjVF3uuLu6

وفقا للإحصاءات، فإن الويب العميق، وهو الفئة الأسرع نموا على الإنترنت، يقدر حجمه بـ 500 مرة أكبر من الويب السطحي ويشكل حوالي 90٪ من جميع صفحات الويب. تنقسم الاستخدامات إلى استخدامات مشروعة، والتي تشمل سجلات الرعاية الصحية والمواد التعليمية، واستخدامات غير قانونية [مستخدمو الويب المظلم]، والتي تشمل الاتجار بالبشر، والاتجار بالمخدرات، وما إلى ذلك 13.

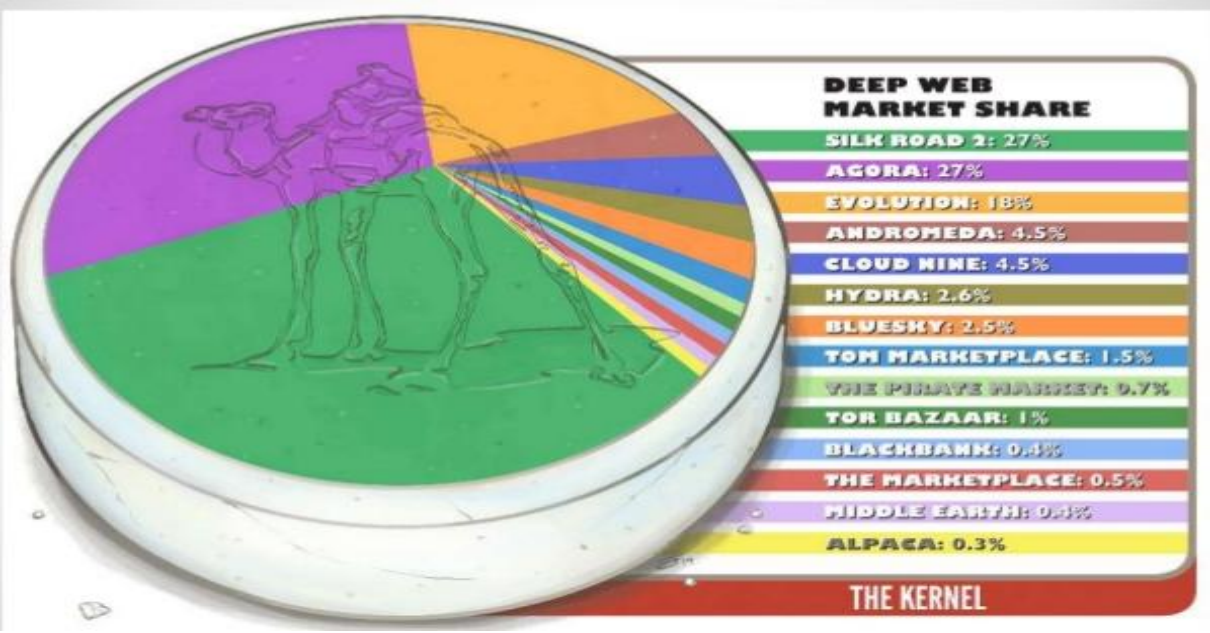
إن محتويات الويب العميق لا مركزية ومجزأة، ويوجد قدر هائل من المعلومات لا يمكن لعامة الناس الوصول إليها.وكما سبقت الإشارة إليه هناك محركات بحث مصممة بشكل صريح للمساعدة في اكتشاف المحتوى المخفي. تتم فهرسة الويب المظلم، ولكن ليس بواسطة محركات البحث العادية، إذ تنتهي جميع المواقع الموجودة على الويب المظلم بـ ".onion"، بدلاً من ".com" أو ".org" على الويب السطحي، وهي محاولة متعمدة لتقييد الوصول إلى تلك المواقع على المتصفحات التي تستخدم وكلاء معينين مثل SearX وTorوكمثال على ذلك المجرمين والمخبرين والمعارضين السياسيين من المستعملين لشبكة الإنترنت المظلمة لأنهم يستطيعون الاستفادة من عدم الكشف عن هويتهم التي توفرها.ومع ذلك، يمكن لأي شخص يستخدم الإنترنت بشكل روتيني الوصول إلى الويب المظلم 14.

كيفية الولوج إلى فضاء الجريمة المنظمة السيبرانية (عبر محرك البحث Tor)

المصدر: https://images.app.goo.gl/ku8UDWqAdhwjVwzF6

يعد "The Onion Router"، المعروف أيضا باسم "Tor"، مكونا رئيسيا للويب المخفي. يستخدم هذا البرنامج المجاني مفتوح المصدر شبكة من المحطات التي يديرها متطوعون لتوجيه بيانات الإنترنت وتشفيرها من خلال العديد من المرحلات، التي تعمل كخدمة بريدية آمنة. وهذا يضمن التواصل المجهول من خلال حماية البيانات أثناء عملية النقل، مما يتيح لمستخدمي هذا المتصفح الالتفاف على الرقابة والوصول إلى الويب المظلم. على الرغم من أنه يتم استخدامه في أنشطة غير قانونية أو إجرامية، إلا أن المتصفح يحظى أيضا بشعبية كبيرة لدى الصحفيين وأولئك الذين يسعون إلى عدم الكشف عن هويتهم والأفراد المبلغين عن المخالفات السياسية أو الشركات 15.

أشهر مواقع فضاء الجريمة المنظمة ومساحتها

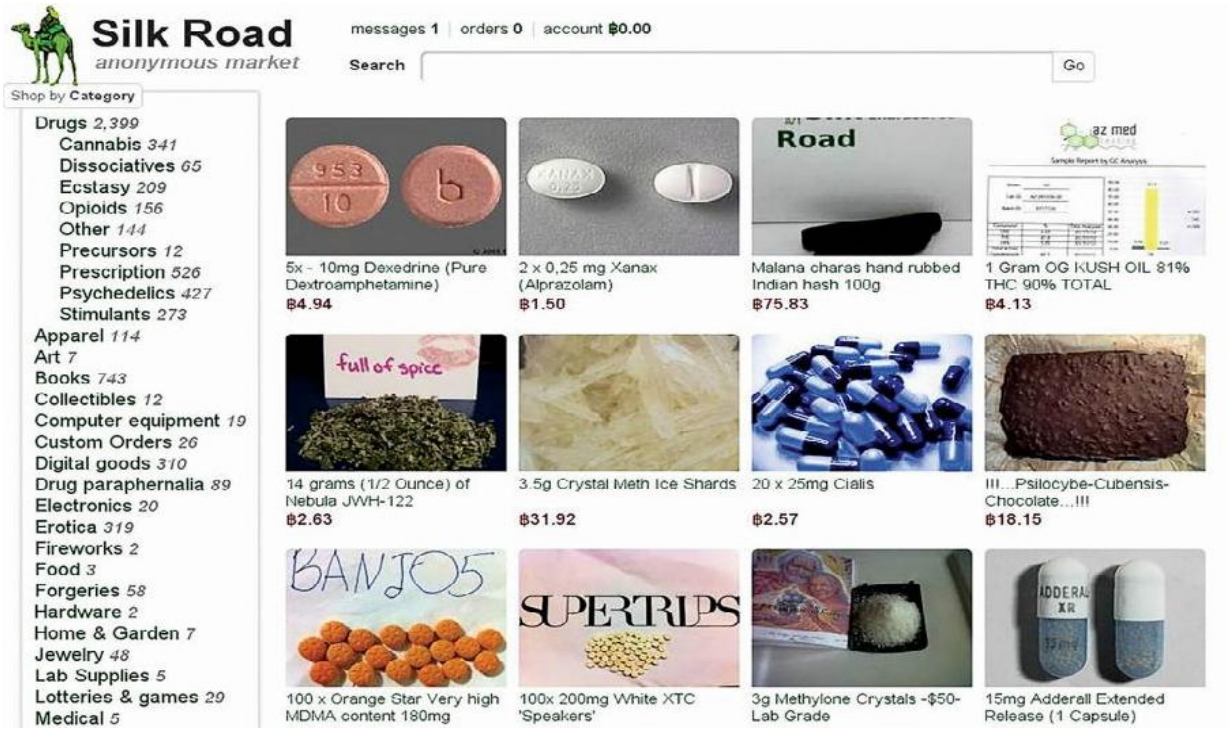


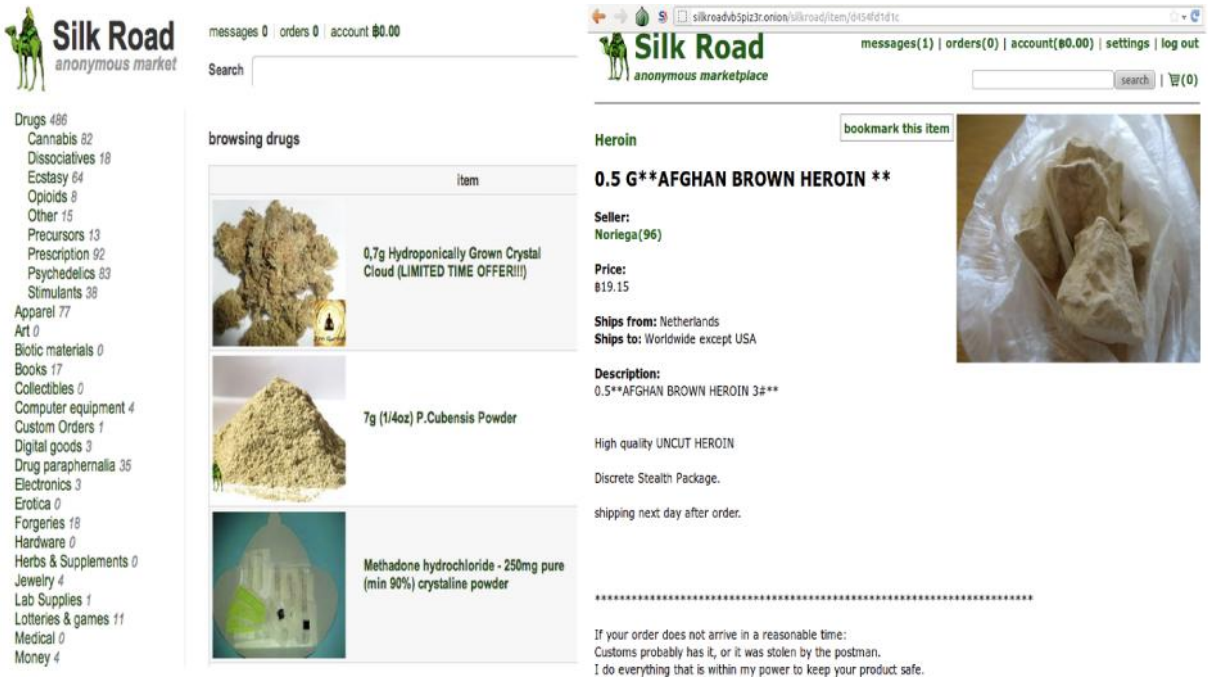
المصدر:https://images.app.goo.gl/Kv6KUxGXVcMRbWft8

عندما تسمع عبارة "طريق الحرير"Silk Road، فربما تفكر في مجموعة من طرق التجارة التي عبرت آسيا منذ عام 200 قبل الميلاد وحتى أوائل القرن التاسع عشر. على الرغم من أنهما يشتركان في الاسم نفسه، فإن طريق الحرير الذي المشار إليه هنا هو موقع ويب مظلم سيء السمعة حيث يمكن للمستخدمين شراء عناصر مثل المستندات المزورة والمخدرات وكذا المجوهرات في مختلف أنحاء العالم، نظرا لطبيعتها غير القانونية إلى حد كبير، ولا يمكن للمستخدمين التعامل إلا بالبيتكوين Bitcoin للحفاظ على سرية هويتهم 16.

في عام 2013 وبعد تحقيقات عديدة تم القبض على صاحبه، وحكم عليه بالسجن مدى الحياة في الولايات المتحدة. وعلى الرغم من أن حياة Silk Road لم تدم طويلا في المخطط الكبير للBitcoin ، إلا أنها مهدت الطريق لتصبح العملة المشفرة سائدة. ففي نهاية المطاف، إذا أراد المجرم طريقة أسهل وأقل خطورة للحصول على المخدرات، فمن الأفضل أن يتعلم استخدام موقع ويب وعملة رقمية مجهولة 17.

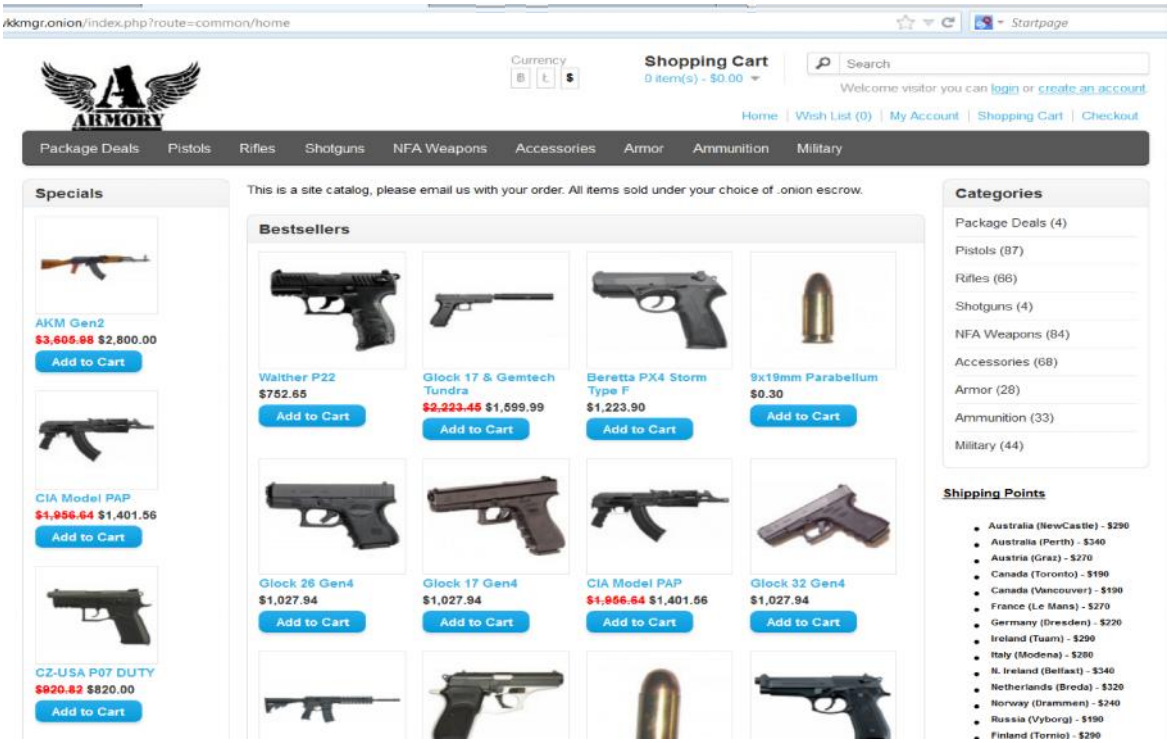
أحد مواقع تجارة المخدرات



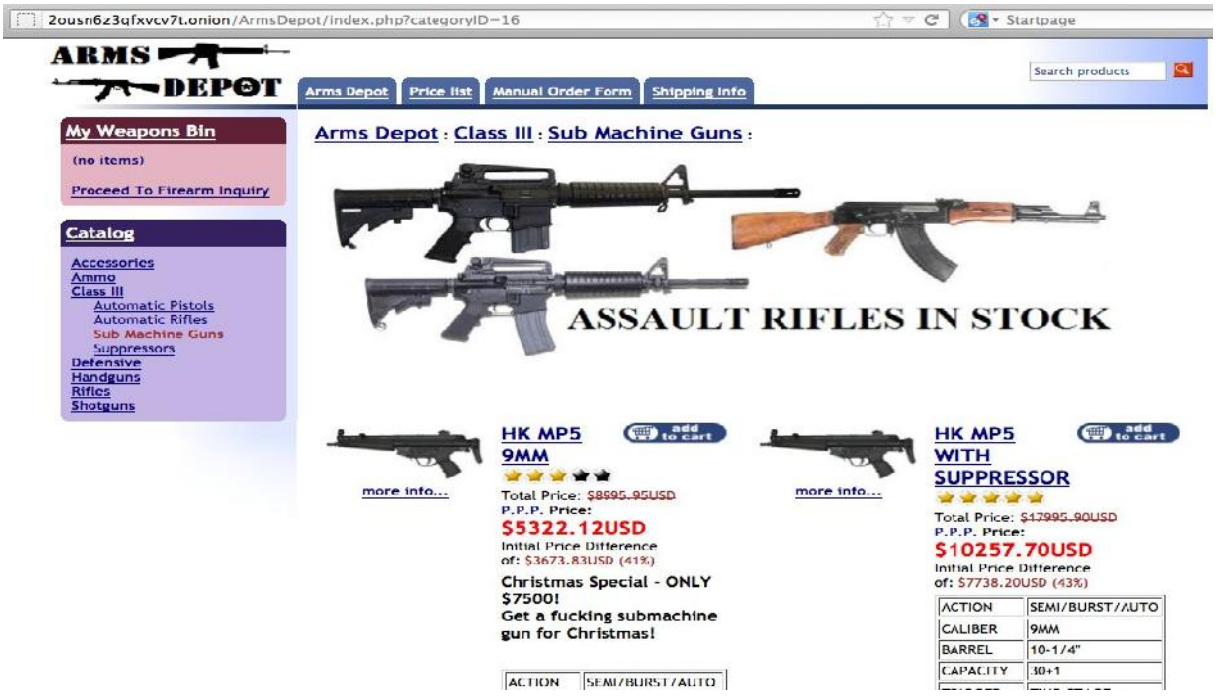


المصدر: https://images.app.goo.gl/P5gm2BS3keWP6xEs7

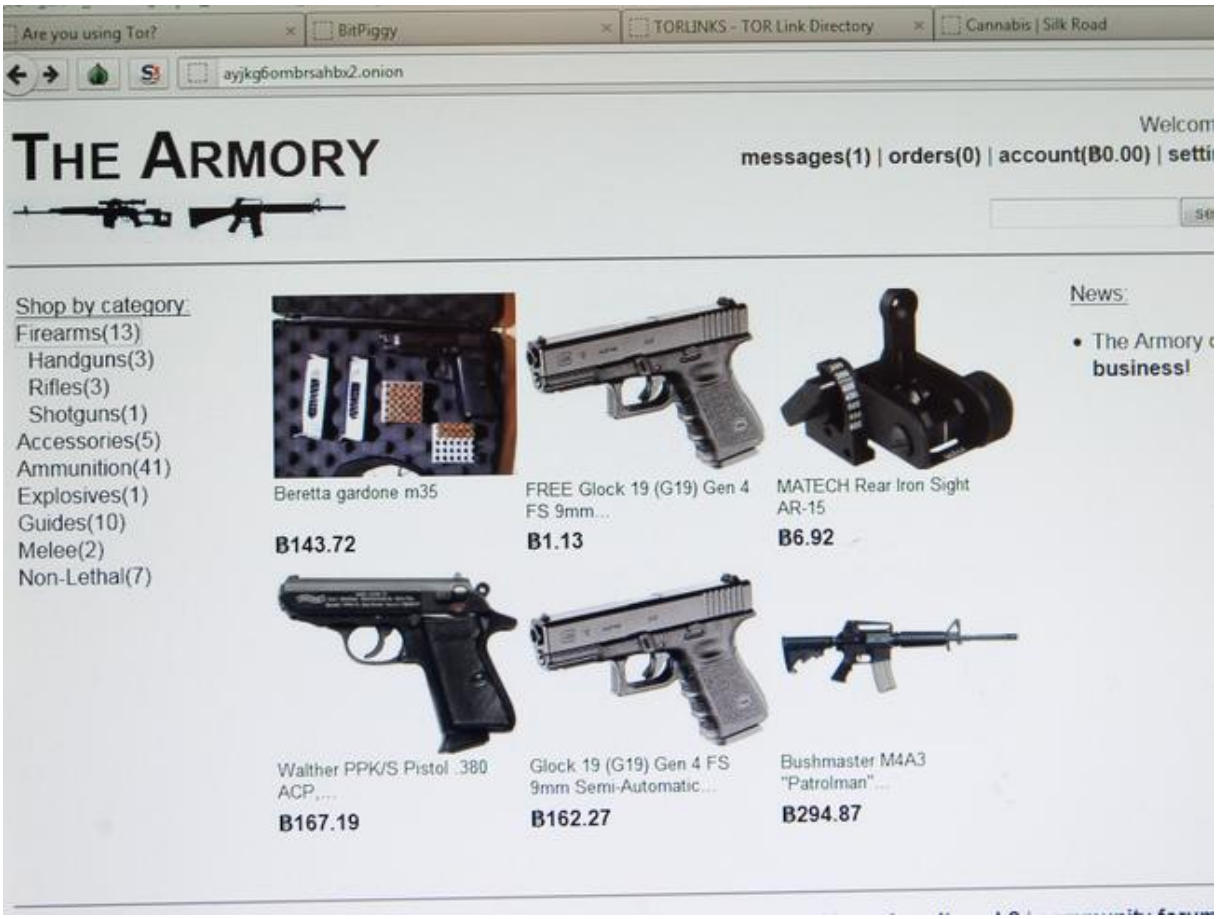
بعض مواقع تجارة الأسلحة



المصدر: https://images.app.goo.gl/rwYRGwe9ZceMc8VY7



المصدر: https://images.app.goo.gl/HrG8iJTQrb3G5won7



المصدر: https://images.app.goo.gl/XbGYZHnQNjn1nEGq6

المحور السادس: الثورة التكنولوجية الرابعة والجريمة المنظمة السيبرانية:

إذا كانت الجريمة متأصلة في المجتمعات فهي ليست أقل مشكلة فيما يتعلق بتطورها، إذ ترتبط الجريمة لآن بالتنمية الاقتصادية للمجالات البرية والبحرية والجوية، وهي موجودة أيضا في الفضاء الإلكتروني. وهذا هو السبب الذي جعل مكافحة الجرائم السيبرانية موضوع تطور معياري كثيف. ومع ذلك، فإن معيار الطبيعة القمعية، حتى عالي التطور، يغطي نسبية معينة. في حين أن هناك العديد من الجرائم المرتكبة في الفضاء السيبراني، فإن تحديد المسؤوليات يشمل الصعوبات سواء مقدمي لاستضافة، أو مقدمي الوصول إلى لإنترنت، أو الناشرين. علاوة على ذلك، ونظرا لأن هذه الجريمة تغطي بعدا عالميا، فإن توطين الأفعال يثير مناقشات حول تطبيق الإقليمية للجريمة السيبرانية. وفي ضوء الصعوبات المحددة لفهم هذا النوع من الجرائم التي تؤثر بقوة على القطاع الاقتصادي، يتم تقديم التعاون الدولي كوسيلة فعالة لمكافحتها. ومع ذلك، فإن تطور التعاون الدولي أمر مشروط 18 وفيه الكثير من التحديات.

لذلك، تم تسخير التقدم التكنولوجي من قبل الجهات الفاعلة في مجال التهديد في صناعة الجريمة السيبرانية المزدهرة لتحقيق تأثير كبير. تشير التقديرات إلى أن التكلفة السنوية التي يتكبدها الاقتصاد العالمي من الجرائم

الإلكترونية تزيد على 400 مليار دولار، وهو رقم يتوقع معظم المحللين زيادته في السنوات المقبلة. إذ من الواضح أن الجريمة السيبرانية لا تزال تعتبر صناعة متنامية، حيث يدرك العنصر الإجرامي منذ فترة طويلة أنه يمكنه تحقيق عوائد كبيرة بمخاطر محدودة 19.

فالشركات والحكومات بغض النظر عن اجتهادها المعلن فيما يتعلق بضوابط الجرائم السيبرانية، ستظل معرضة لخطر الاحتيال والفساد بسبب بطئها في التكيف وتبني ما تقدمه التكنولوجيات الجديدة. بالنسبة لمعظمهم، ما زالوا يبنون قراراتهم بشأن الاستثمار في التكنولوجيا على التعرض للمخاطر واستعدادهم لتحمل مستوى معين من الخسارة. فالشركات والمنظمات والحكومات التي تفشل في توفير الحماية الكافية لشبكاتها ستكون في وضع تنافسي غير ملائم على نحو متزايد. ففي ظل التكنولوجيا المتاحة الآن للمساعدة في إحباط تقدم مجرمي الإنترنت، وبالتالي، كجزء من الإطار التنظيمي، فقد حان الوقت للحكومات لوضع المعايير المتوقعة وأفضل الممارسات الإلزامية للدفاعات السيبرانية 20.

ومن أهم العوامل المساعدة في تأثير التكنولوجيا على الجريمة المنظمة السيبرانية يمكن ذكر ما يلي:

أولا-تطور تقنيات التشفير: صعوبة فك تشفير البيانات التي يتم تبادلها على الإنترنت المظلم.

ثانيا-إنتشار الذكاء الاصطناعي: استخدام تقنيات الذكاء الاصطناعي لتنفيذ عمليات الاحتيال والقرصنة الإلكترونية.

ثالثا:-ظهور تقنيات جديدة: مثل إنترنت الأشياء والبلوك تشين Blockchain، على - سبيل المثال - هو تقنية تسجيل المعلومات بطريقة آمنة وموثوقة. تشبه سلسلة من الكتل المترابطة، حيث تخزن كل كتلة معلومات محددة، مثل السجلات المالية المتمثلة في التحويلات والمدفوعات، السجلات الطبية كمعلومات عن المرضى والأدوية والعلاجات، السجلات العقارية كمعلومات عن ملكية العقارات، السجلات الحكومية كشهادات الميلاد والزواج والوفاة.

ومن مميزات هذه التقنية:

- اللامركزية:لا تسيطر أي جهة واحدة على المعلومات، مما يجعلها أكثر أمانا وشفافية.
- الأمان: يصعب اختراق أو تغيير المعلومات المخزنة على البلوك تشين.
- الشفافية :يمكن لأي شخص التحقق من المعلومات المخزنة على البلوك تشين.
- الكفاءة :تقلل تقنية البلوك تشين من الحاجة إلى الوسطاء، مما يجعلها أكثر كفاءة.

وبالتالي فإن هذه التقنيات التي أوجدتها الثورة التكنولوجية الرابعة، بقدر ما كانت نعمة وساهمت في تسهيل الحياة بقدر ما ساهمت في خلق فرص جديدة للجريمة المنظمة السيبرانية.

خلاصة:

يعد الإنترنت المظلم فضاء خصبا للجريمة المنظمة السيبرانية، يمس بأمن الدولة الداخلي بالتأثير على الجانب السياسي التنمية الوطنية، وعلى الجانب الاقتصادي باستزاف ثروات الدولة، لاستيلاء على المؤسسات العمومية، لاستيلاء على المال العام والتأثير على لأجهزة المالية في الدولة، التأثير على المنافسة المالية المشروعة، انتشار الاقتصاد الموازي، وعلى الجانب لاجتماعي سواء على المجتمع، الفرد، المسسسات لاجتماعية، أو قبول المجتمع لها والتعايش معها

ويمس بأمن الدولة الخارجي بالمساس بسيادة الدولة واستقرارها الوطني، بالعلاقات السياسية والاقتصادية الدولية.

لذلك، يمكن القول إن الجريمة السيبرانية شكل متطور من أشكال الجريمة التقليدية، ويمكن أن تمتد آثارها عبر المجتمعات في جميع أنحاء العالم، مما يبرز الحاجة الي وضع استجابة عاجلة وديناميكية ودولية 21. لذلك لابد من تكاثف الجهود وتطوير تقنيات جديدة ونشر الوعي، وتطوير قوانين وأنظمة حتى يمكن مكافحة هذه الجرائم وضمان أمن مستخدمي لإنترنت.

الهوامش والمراجع:

1. Brigitte Pereira, La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité, (Revue internationale de droit économique 2016/3 (t. XXX), pages 387 à 409 Éditions Association internationale de droit économique), 2016, p 388.
2. Ibid, p 389.
3. شرقي عبد الغاني، التهديدات السيبرانية وإشكالية السيادة: إعادة قراءة لسيادة واستفاليا، (مجلة السياسة العالمية، المجلد (7)، العدد (2)، 2023) ص 275.
4. المرجع نفسه، ص 276.
5. محمد. بن عملة، مفهوم الجريمة المنظمة دوليا ووطنيا، (مجلة البحوث في الحقوق والعلوم السياسية، المجلد (2)، العدد (4)، 2016)، ص 2 .
6. المرجع نفسه، ص 2
7. المرجع نفسه، ص 11.
8. United Nations Office On Drugs And Crime, 2024. https://www.unodc.org/westandcentralafrica/fr/Cyber-Crime.html
9. Bashar Touma, Learn about surface internet and deep internet And the dark internet, 2018, https://steemit.com/technology/@bashar-touma/learn-about-surface-internet-and-deep-internet-and-the-dark-internet
10. Jessica Agorye, 2023, The Deep Web & The Dark Web, https://verpex.com/blog/website-tips/the-deep-web-the-dark-web
11. Ibid.

12. Pereira, p 389.
13. Agorye, 2023.
14. Ibid.
15. Ibid.
16. Mintdice, The Silk Road Marketplace: History & Today, 2021 https://steemit.com/hive-138698/@mintdice/the-silk-road-marketplace-history-and-today
17. Mintdice, 2021
18. Pereira, p 409.
19. Garry Clement, Crime and corruption in the 4th industrial revolution, 2017, https://www.financierworldwide.com/crime-and-corruption-in-the-4th-industrial-revolution
20. Clement, 2017.
21. United Nations Office On Drugs And Crime, 2024.

اسهامات نظريات العلاقات الدولية في تفسير تطور مفهوم الامن – من الأمن القومي الى الأمن القومي السيبراني

The contributions of international relations theories in interpreting the evolution of the concept of security – from national security to cybersecurity

بن جدو أسماء جامعة أمحمد بوقرة بودواو بومرداس

a.bendjeddou@univ-boumerdes.dz

ملخص:

من خلال هذه الورقة البحثية سنسلط الضوء على التطور التاريخي لمفهوم الامن من خلال عرض النظريات التي ساهمت في تفسير تطور مفهوم الأمن، وتحليل أسباب الاختلاف الذي شهده هذا المصطلح باختلاف آراء المنظرين والاختلاف الزماني والمكاني وبالأخص مع التطور التكنولوجي في الميدان الحربي.

الكلمات المفتاحية: الأمن السيبراني، نظريات العلاقات الدولية.

Abstract:

throughthisresearchpaper,wewill shed light on the historicalevolution of the concept of srcurity by presentingtheoriesthat have contributted to interpreting the development of the security concept and analyzing the reasons for the differenceswitnessed in thisterm due to the varying opinion of theorists, temporal and spatial differences, especiallywith the technologicaladvancements in the militaryfield.

Key words : cybersecurity, international relations theories.

مقدمة:

جاءت معاهدة "واستفاليا" لتحقيق الأمن والسلم في أوربا بعد ما شهدته في حرب الثلاثين عاما، حيث كان التركيز في تلك الفترة على تعظيم القدرة العسكرية كمحاولة لتحقيق الامن، غير أنه بانهيار الاتحاد السوفياتي الذي كان يتمتع بقدرات عسكرية كبيرة لم يتمكن من مجابهة أعدائه لتسقط بذلك فكرة قدرة القوة العسكرية في تحقيق الأمن، حيث ظهرت فواعل جديدة لها دور كبير في تحقيق الأمن أو زعزعته كالشركات المتعددة الجنسيات، القوة الاقتصادية والشركات التكنولوجية.

وهذا ما يقودنا الى طرح الإشكالية التالية:

كيف ساهمت نظريات العلاقة الدولية في تفسير تطور مفهوم الأمن من الأمن القومي إلى الأمن القومي السيبراني؟

للإجابة على هذا الإشكالية قمنا بتقسيم الورقة البحثية الى ثلاث محاور:

المحور الأول: دور المدرسة الواقعية في تحليل مفهوم الأمن السيبراني.

المحور الثاني: دور المدرسة الليبرالية في تحليل مفهوم الأمن السيبراني.

المحور الثالث: دور المدرسة النقدية في تحليل مفهوم الأمن السيبراني.

المحور الأول: دور المدرسة الواقعية في تحليل مفهوم الأمن السيبراني.

يتأسس فكر الواقعيون على فرضية مفادها أن الدولة هي الفاعل الرئيسي المهيمن على العلاقات الدولية، وهي تتميز بالعقلانية التي تمكنها من تحديد مصالحها بما يتماشى مع هيكل القوة في النظام الدولي الذي يتميز بالأساس بالفوضى مما يستوجب على الدولة الاعتماد على ذاتها لتحقيق أمنها القومي عن طريق تسخير كل المصادر المادية خصوصا العسكرية منها، التي تعد حسب المنظور الواقعي العنصر الأهم لقوة الدولة، حيث تحدد أهمية باقي العناصر المادية بالقدر الذي تقوى به البعد العسكري.1

كما يؤكد الواقعيون على القيود التي تفرضها الأنانية الإنسانية على السياسة مع غياب الحكومة العالمية (الفوضى). مما يتطلب أولية القوة والأمن في كل الحياة السياسية2، كما يحاجج المفكر "هانس مورغا نتو" بأن العالم لاجتماعي ليس سوى إسقاط للطبيعة البشرية على المستوى الجماعي.3 وقد استلهم الواقعيون معتقداتهم من الأفكار التي طرحها "توماس هوبز" في كتابه الشهير (ليفياثان Leviathan) والتي تعتبر المنافسة والريبة والمجد هم لأسباب المتجذرة في الطبيعة البشرية التي تدفع إلى الصدام فالمنافسة تجعل البشر يغزون لتحقيق المكاسب، والريبة لأجل الأمن، والمجدلأجل السمعة، وعليه فإن فهم الواقعيون للأمن يركز على ثلاث نقاط رئيسية ألا وهي أن:

- الدولة هي وحدة التحليل لأمني الرئيسية.
- التهديدات لأمنية ذات طابع خارجي أي أنها تنشأ خارج حدود الدولة.
- طبيعة التهديدات لأمنية الموجهة ضد الدولة (وحدة التحليل) ذات طبيعة عسكرية بشكل أساسي.4

ومن ناحية أخرى ترى الواقعية الجديدة بأن اختلاف توزيع المقدرات بين الدول بما يؤثر على هيكل النظام الدولي هو المعلم الرئيسي لغياب الأمن وليس الصراع على حول القوة كما تزعم به الواقعية التقليدية وأن الدولة هي الفاعل الرئيسي في النظام الدولي الذي يتصف بالفوضى، والتي تفضي بغياب سلطة مركزية لها القدرة على تنظيم العلاقات الدولية. كما تعتبر الواقعية الجديدة كذلك أن الحرب معلم تاريخي دائم من معالم السياسية العالمية فالدول تواجه معضلة أمنية لا يمكنها التخلص منها.5

وعلى النقيض لما جاء به الواقعيين التقليديين يرى "كنيث والتز" في كتابه "نظرية السياسة الدولية" أن الفرق بين النظام الدولي والداخلي يكمن في بنيتهما، ذلك أنه في النظام الداخلي أمن المواطنين يكون من مهام الدولة، في حين

---

[1]- إيهاب خليفة، الحرب السيبرانية لاستعداد لقيادة المعارك العسكرية في الميدان الخامس، القاهرة، العربي للنشر والتوزيع، 2021، ص23.

[2]- ترجمة محمد صفار، نظريات العلاقات الدولية، القاهرة، سلسلة العلوم لاجتماعية، المركز القومي للترجمة،2014، ص52.

[3]- نفس المرجع السابق، ص53.

[4]-عشور قشي، نظرية مركب لأمن الإقليمي دراسة مقارنة بين إقليمي جنوب شرق آسيا والساحل الإفريقي، رسالة دكتوراه، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 03، 2016 ص21.

[5]- إيهاب خليفة، نفس المرجع السابق، ص24.

أنه في النظام الدولي يكون تحقيق الأمن بالاعتماد على النفس في ظل غياب سلطة عليا لمنع استخدام القوة، إن سعي الدول لتحقيق أمنها من شأنه أن يزيد من حالات انعدام الأمن تلقائيا لدى دول أخرى، إن هذه السلسلة المتصاعدة من حالة الأمن يصطلح عليها بـ"المعضلة الأمنية" فمعرفة أسباب الحرب أسهل بكثير من الحصول على شروط السلام. لأن أسباب الحرب مرتبطة بكل من الدولة وبنية النظام.6

وعند إسقاط مقولات النظرية الواقعية على الظواهر السيبرانية تصلح في تفسير جزء من التهديدات السيبرانية على سبيل المثال الطبيعة الفوضوية للفضاء السيبراني فهو نظام لامركزي ولا توجد سلطة عليا تدير التفاعلات التي تحدث فيها، غير أن النظريات التقليدية لا تقدم أدوات تحليلية لفهم بعض التهديدات الحديثة وخصوصا الفضاء السيبراني كم تبقي حكرا على الدولة كما تحاجج به الواقعية بكل أصبحت متاحة للأفراد وتقوم باستخدامه لشن الهجمات السيبرانية.7

يرى "جيمس أدامز" أحد منظري الواقعية الجديدة أن الأنترنت يعتبر نظام فوضوي حيث أصبح هذا الفضاء ساحة المعركة الجديدة في ظل غياب هيئة حاكمة لهذا المجال الحيوي وغياب الثقة حتى مع الحلفاء في هذا المجال فكل سباق لتعظيم القوة السيبرانية لدولة ما هذا في حد ذاته يشكل تهديدا لدولة أخرى. كما أن التفوق في القوى السيبرانية لا يجعل الدولة بمنأى عن تعرضها للهجمات السيبرانية وهذا ما شهدناه في الولايات المتحدة الأمريكية التي تعد أكثر عرضة للهجمات السيبرانية رغم التطور الذي لحقته في هذا المجال.8

إن تزايد اعتماد الدولة على التطوير التكنولوجي وإنشاء مدن ذكية كلما زاد من قابلية اختراقها وهذا ما يشكل تهديدا لأمنها القومي، مما يستوجب على الدول الاعتماد على قدراتها الذاتية لتطوير إمكاناتها السيبرانية أو التحالف مع غير ما من الدول-دون الوثوق بها بشكل كامل- قصد تدعيم أمنها القومي. فضلا على ضرورة الاعتماد عل نفسها في تطوير تقنياتها الذكية على المستوى المحلي، بأن التقنيات المستوردة عادة ما تكون بها ثغرات أمنية أو برامج تجسس مما تشكل تهديد أمني، وتبقي مشكلة التفوق من تطوير أحد الدول لقدراتها السيبرانية بصورة أكبر من باقي الدول مما يشكل تهديدا لها.9

❖ النقد الموجه للفكر الواقعي:

يرى أنصار النظرية الواقعية أن الدولة هي الفاعل الوحيد في العلاقات الدولية غير أن هذا الأمر ليس كذلك في الصراع السيبراني فرغم محورية دور الدولة غير أن هناك فواعل من غير الدول لهم دور في تأجيج الصراع السيبراني مثل الحركات الإرهابية التي تستخدم الفضاء السيبراني لتحقيق أهدافها، فضلا عن دور الشركات

---

[6]- نفس المرجع السابق، ص25.

[7]-إيهاب خليفة، نفس المرجع السابق، ص 25.

[8]-Constantine,petallides, cyber terrorism and IR Theory:Realism،leberalism and constructivistm in the new securitythreat،indiquiries journal، vol 4, NOO3,2012,accessed march7,2018. http://www.inquiriesjournal.com

[9]- إيهاب خليفة، نفس المرجع السابق، ص28.

التكنولوجية العملاقة التي تعمل على تصنيع وإدارة هذه التقنيات، وكذا بعض المنظمات الدولية المسؤولة عن إدارة الأنترنت مثل الاتحاد الدولي للاتصالات.10

أحد الافتراضات الأساسية للواقعية أن الدولة هي مصدر القوة وبالتالي فهي الأكثر أهمية في السياسة الدولية، ومع ذلك فإن ثورة المعلومات تتحدى أولوية الدولة –كمصدر للقوة حسب الواقعية- وذلك بسبب المشاركة الأكبر للجهات الفاعلة غير الحكومية التي تهدد مصدر السلطة التقليدية. تكتسب الجهات الفاعلة الغير الحكومية أهمية متزايدة في العلاقات الدولية كما يرى "جوزيف ناي" حول توزيع السلطة، وهذا صحيح بشكل فاض في المجال السيبراني حيث يمكن للمجرمين من الأفراد والمنظمات والجماعات الإرهابية الاستفادة من إمكانية الوصول إلى شبكة الأنترنت لتهديد أمن الدولة، كما تلعب الشركات الخاصة دورا سواء في الأمن أو للتهديد.11

تركز النظرية الواقعية على مصطلحات رئيسية كالقوة، الصراع، الحرب والردع حيث تفسر سعي الدولة إلى تدمير الخصم بشكل نهائي للتخلص من المعضلة الأمنية، غير أن النظرية الواقعية عاجزة عن تفسير حالات أقل حدة من الصراع كما هو الحال في الصراعات السيبرانية، الذي لا يمكن فيه تدمير العدو بشكل نهائي، بل يحدث الصراع على مستويات أقل حدة وأقل صراع.

صعوبة تقدير القوة السيبرانية للدول فليس بالضرورة زيادة الميزانية المخصصة للدفاع والردع السيبراني وزيادة عدد الأفراد يعني زيادة لقوتها الهجومية،12 فالردع عند الواقعيين يرتكز على تعظيم قوة الدولة للتصدي للهجمات وهذا ما يصعب تحقيقه بالشكل التام في الفضاء السيبراني نظرا لصعوبة تقدير القوة السيبرانية للخصم -كما أسلفنا ذكره-وإدراك مقدرته الحقيقية على الرد على الهجمات السيبرانية، فضلا على أن السلاح السيبراني ليس له القدرة التدميرية التي يملكها السلاح النووي والتي ظهرت في إطاره نظرية الردع. بالإضافة إلى أهم نقطة وهي القدرة على التتبع لمعرفة مصدر الهجوم الحقيقي وبالتالي لا يمكن للنظرية الواقعية تفسير حالة الردع في الصراعات السيبرانية.13

يضاف إلى ذلك أن الواقعية ترى بأن الهجوم أكثر فاعلية من الدفاع بسبب سهولتها ونقص تكلفتها والضرر الذي من الممكن أن تلحقه بالمجتمع وطبيعتها اللحظية، لأن الهجوم يتطلب فقط استهداف نقطة ضعف واحدة حتى تنجح في حين يتضمن الدفاع تأمين الحماية الكلية، كالشبكات ونقاط الضعف التي لا يكون المدافع على علم بها قبل استغلالها،14 وعليه فإن فكرة الواقعية في تركيزها على الهجوم على حساب الدفاع لا يصلح في الفضاء السيبراني الذي يستوجب تسخير كل جهود الدفاع والهجوم والردع لتحقيق الأمان في الفضاء السيبراني.

---

[10]- نفس المرجع السابق، ص30.

[11]-Anthony Craig and Bradon valerian, Realism and cyber conflit: security in the digital Age, 03/02/2018 https: //www.eir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/

[12]- إيهاب خليفة، نفس المرجع السابق، ص31.

[13]- نفس المرجع السابق، ص32.

[14]-Anthony Craig and Bardon Valerian , OPCIT.

المحور الثاني: دور المدرسة الليبرالية في تحليل مفهوم الأمن السيبراني.

ظهرت هذه النظرية في منتصف السبعينات القرن العشرين، والتي بينت أهمية وتأثير الفاعلين غير الدوليين في العلاقات الدولية،15 مثل الجماعات الإرهابية والشركات متعددة الجنسيات والمنظمات غير الحكومية مع التشديد على فكرة أن الدولة هي الفاعل الأكثر تأثيرا على العلاقات الدولية، كما ترى بأن الدولة من صنع الشعب فهي دولة الشعب وحكومة الشعب وقوانين الشعب وجيش الشعب وشرطة الشعب إنه من الناحية النظرية ليس من المنطقي أن تشكل الدولة تهديد أمني لمواطنيها لأن تهديد المواطنين هو تهديد لمصالح الدولة، غير أنه من الناحية الواقعية قد لا يعبر أمن الدولة على أنه أمن الشعب، على نفس النسق التي تسعى المدرسة الليبرالية إلى تطبيقه. لأنه في العديد من الحالات قد لا تتمكن الدولة من توفير أمن مواطنيها وذلك لعدم قدرتها على فرض نفوذها على كل إقليمها، أو لنقص إمكاناتها المادية لذلك. وهي الدولة التي يمكن التعبير عنها بأنها "دول فاشلة".16

وعلى النقيض من المنظور الواقعي فإن الليبرالية ترى بأن الفرد هو الوحدة الأساسية في التحليل وتوفير الحقوق له، وأن الدولة لها عدة أدوار كتحقيق الاستقرار السياسي والاجتماعي والبيئي والاقتصادي لتمكين الأفراد من الوصول إلى خياراتهم إلى النهاية.17

ومما سبق ذكره نخلص إلى فكرة مفادها أن مفهوم الأمن عند الليبراليون يتعدى البعد العسكري إلى أبعاد أخرى: اقتصادية، اجتماعية وثقافية. وهو بهذا الطرح يخالفون الواقعيون الذين حصروا مفهوم الأمن في بعده العسكري وأن الأمن القومي والتحالفات نتاج لتطبيق هذا المنظور،18 فبحسب "جوزيف ناي" Joseph Nay أن هناك تحولات دولية أسهمت في تراجع دور القوة الصلبة العسكرية والاقتصادية أو على الأقل قللت من فاعليتها وأثرت على المفهوم التقليدي للأمن، والمتمثلة في الاعتماد الاقتصادي المبني على التبادل بما يساهم في الحد من استخدام القوة الصلبة لما لها من أضرار.

فضلا عن ظهور فواعل جديدة من غير الدول له القدرة على ممارسة القوة كالفاعلين غير القوميين والشركات المتعددة الجنسيات، والمنظمات الدولية والجماعات الإرهابية، إضافة إلى ظهور النزعات القومية مما زاد من صعوبة تحقيق الأمن.

ولتدعيم فكرة عدم كمالية القوة الصلبة في تحقيق الأمن نستشهد بالمثال الذي يفضي بعدم مقدرة الولايات المتحدة الأمريكية بكل إمكانياتها العسكرية على إخضاع العشائر الصومالية أو تهدئة الأوضاع بالعراق. ضف إلى ذلك مساهمة انتشار التكنولوجيا مع زيادة عدد مستخدمي الأنترنت بالعالم وبروز الهجمات السيبرانية كأداة فاعلة في

---

[15]-مصطفى دريدي، نظرية الأمن الإسرائيلية بين الاستمرارية والتغيير، رسالة ماجستير، كلية العلوم السياسية والإعلام، جامعة الجزائر03، 2012 ص27.

[16]- إيهاب خليفة، نفس المرجع السابق، ص35.

[17]- صليحة كبابي، الدراسات الأمنية بين الاتجاهين التقليدي والحديث، مجلة العلوم الإنسانية، جامعة قسنطينة، عدد38، ديسمبر2012، ص237.

[18]- جراية الصادق، مفهوم الأمن في الفكر الاستراتيجي الإسرائيلي، رسالة دكتوراه، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 03، 2017، ص35.

السياسة الدولية.وأخيرا ظهور قضايا جديدة للأمن غير التقليدي مثل الفقر التلوث، انتشار الأوبئة، الجريمة المنظمة والتغيرات المناخية.19

هذا ما خلق قضايا أمنية جديدة مستحدثة كقضايا الأمن الغذائي والأمن الطاقوي والأمن البيئي والأمن السيبراني وهذا ما يهمنا في هذه الدراسة-ناهيك عن ظهور فواعل في الساحة الدولية من غير الدول لها الدور البارز في القضايا الأمنية كالشركات التكنولوجية والمنظمات الدولية وغيرها.

وتتكون النظرية السيبرانية من اتجاهين وهما:

1. الليبرالية البنيوية:

اعتمدت كل من ميشيل دويل Michael Doyle وفرانسيس فوكوياما F. Fukoyama في أطاريحهم على فكرة السلام الديمقراطي، حيث اعتبرا أن ميل الدول نحو السلام والأمن هو الالتزام بالديمقراطية وحماية حقوق الإنسان وكذا الترابط والتفاعل بين الدول. في حين أن الدول التي لا تتمتع بالديمقراطية تميل إلى الحرب والعدوان، حيث أكد "ميشيل دويل" على فكرة أن الدول الديمقراطية لا تحارب بعضها البعض، وعليه يمكن القول أن الليبرالية البنيوية ترى أن الحروب لا تنشأ إذا تم تعزيز التعاون الدولي بشكل جيد لتعميم الديمقراطية الليبرالية ونشرها بشكل سلمي في العالم.20

2. الليبرالية المؤسساتية:

جاءت الليبرالية المؤسساتية على النقيض من التصور الواقعي للأمن الذي يهمل الدور الذي تلعبه المؤسسات الدولية في التخفيف من حدة الحروب، حيث يرى الواقعيون أن الدولة هي وحدة التحليل الرئيسية لتحقيق الأمن عكس ما جاء به الليبراليون البنيويون الذين يؤكدون على دور المؤسسات في تحقيق الأمن الدولي وتعزيز الأمن الداخلي من خلال الصلاحيات والآليات التي تسمح له بإدارة بعض المسائل الداخلية كنتيجة للتحولات التي مست السياسة العالمية، والتي لم تتيح للدول التصرف في سياستها الداخلية بسيادة مطلقة. حيث يعتقد الليبراليين المؤسساتيين أن زيادة المنظمات الدولية والإقليمية وزيادة وتيرة الاعتماد المتبادل سيفضي حتما إلى سلوك سلمي وتعاوني بين الدول ووحدات النظام الدولي.

المأسسة الدولية لا يمكنها منع حدوث الحرب ولكن باستطاعتها التقليل من مخاوف الغش والمخاوف التي تنشأ في بعض الأحيان من المكاسب الغير متكافئة الناتجة عن التعاون.والتخفيف من أنانية الدول بتشجيعها على ترك المصالح الأنية لصالح مصالح أكبر لتعاون دائم.21

يعد مفهوم الأمن الدولي جزء لا يتجزأ عن ساحة الصراع السيبراني، ذلك أن طبيعة الفضاء السيبراني العابر للحدود الجغرافية ويتخطى مفهوم السيادة الدولية. حيث تلجأ الدول في صراعها السيبراني وحتى الفواعل من دون الدول من قراصنة المعلومات بالسيطرة على عدد لا حصر له من أجهزة كومبيوتر وأجهزة أنترنت لأشياء وكل جهاز

---

[19]- إيهاب خليفة، نفس المرجع السابق، ص37.

[20]- جراية الصادق، نفس المرجع السابق، ص36.

[21]- صباح بالة، النظرية الليبرالية في تفسير الدراسات الأمنية، الموسوعة السياسية، 2021/03/10، تاريخ التصفح: 11 /2023/09، https ://political-encyclopedia.org/dictionary/

متصل بالأنترنت في عدد كبير حول العالم بهدف الخداع والتجسس والسرقة ويقوم بالتضليل مما يجعل من الصعب تعقب الهجمة. كما يمكنها السيطرة على أجهزة من داخل الدولة المستهدفة كي تبدو الهجمة وكأنها حدثت من داخل الدولة نفسها في إشارة إلى منظمات إجرامية أو جماعات إرهابية وليس من خارج إقليم الدولة بما يهدد الأمن الدولي.22

تمكنت النظرية الليبيرالية في تحليل جزء من مفهوم الأمن السيبراني من خلال تركيزها على فكرة الأمن الجماعي والتي تحتاج إلى تعاون دولي مؤسساتي وذلك في ظل الهجمات السيبرانية العابرة للحدود والتي من غير الممكن قدرة الدول العمل بشكل منفصل لكشف ملابسات الهجمات السيبرانية العابرة للحدود كما اهتمت النظرية الليبيرالية بفواعل من غير الدول كالشركات التكنولوجية التي من نشأتها توفير الحماية والأمان في الفضاء السيبراني كما يمكنها تحقيق الردع والهجوم في هذا العالم الافتراضي، فلم يكن تركيز الليبراليين على البعد العسكري فحسب.

❖ النقد الموجه للفكر الليبيرالي:

رغم الإيجابيات التي حظيت بها النظرية الليبيرالية في تفسيرها لمفهوم الأمن السيبراني غير أن هذا لا يعني أنه لا يشوبها بعض النقائص نذكر منها:

– أولى الليبراليون اهتمام واسع بفواعل من غير الدول في تحقيق الأمن غير أنهم لم يحددوا طبيعة العلاقة بين الدول وهذه الفواعل، حيث أضحت الشركات التكنولوجية أحد محركات الصراع الدولي لما لها من إمكانات تكنولوجية ضخمة وما لديها من معلومات يمكنها أن تمس بأمن الأفراد والدول، حيث لاحظ شركات مثل: ميكروسوفت، فيسبوك، غوغل وآبل معلومات استراتيجية والتي يوجد حولها العديد من التساؤلات فيما إذا كانت تشارك هذه المعلومات مع الدول أم لا، فعلى سبيل المثال إذا قدمت هذه المعلومات إلى الحكومة الأمريكية، فإن هذا يمنح الحكومة الأمريكية هامش للمناورة أكبر ومركز قوة أفضل في علاقاتها الدولية على حساب باقي الدول التي لم تحصل على هذه المعلومات وهذا مالم تفسره النظرية الليبيرالية.23

ادعى الليبراليون مقدرة المؤسسات الدولية على التغلب على حالة الفوضى التي يتميز بها النظام الدولي غير أن الواقع يبرهن عكس ذلك فنجد المنظمات الدولية المسؤولة عن إدارة الانترنت كمنظمة الأيكان(ICNN) المهتمة بإدارة عناوين ونطاقات الأنترنت والاتحاد الدولي للاتصالات لم تتمكن من ضبط حالة اللأمن في هذا الفضاء، مع صعوبة تطبيق القانون الدولي على الفضاء السيبراني لغياب الحدود الجغرافية الموجودة في الميادين التقليدية لحرب كالأرض، البحر، الجو والفضاء الخارجي.24

تقف المؤسسات الدولية عاجزة أمام قدرتها على الكشف عن مصدر الهجمات السيبرانية فإذا تمكنت من الكشف عن مصدر الهجمة وتحديد موقعها ليس بالضرورة أن تكون حكومة هذه الدولة متورطة فيها وحتى لو كانت

---

[22]- إيمان خليفة، نفس المرجع السابق، ص38.

[23]- إيهاب خليفة، نفس المرجع السابق، ص 39-40.

[24]- نفس المرجع السابق، ص40.

بالفعل متورطة فيها فإنها تقوم بنفي ذلك، وكمثال على ذلك فيروس "ستاكس نت" الذي تمكن من تدمير الآلاف من أجهزة الطرد المركزي في المشروع النووي الإيراني، ومع ذلك لم تتمكن من كشف هوية فاعليها.

لم تحسم الليبرالية في العلاقة الجدلية بين تحقيق الأمن والخصوصية، فكيف يحق للدولة التجسس على مواطنيها وتسجيل مكالماتهم واتصالاتهم عبر فضاء الانترنت، لدواعي الحفاظ على الأمن.وهل يحق للشركات أن تجمع معلومات عن الأفراد بغرض تحسين خدماتها وتحسين الإعلانات التي تعرضها على عملائها.25

إن فكرة التعاون التكنولوجي من المنظور الليبرالي لا يمكن تطبيقها على الحالة السيبرانية كون هذا المجال يتميز بالسرية كي لا يعطى المجال لمعرفة القوة السيبرانية الدول التي يجعلها عرضة للانكشاف والتعري أمام أعدائها المجهولين.

المحور الثالث: دور المدرسة النقدية في تحليل مفهوم الأمن السيبراني.

تسعى النظرية النقدية إلى "تحرير الإنسان من العبودية" من خلال خلق عالم يلبي احتياجات وقوى البشر، حيث توفر النظرية النقدية الأسس الوصفية والمعيارية للبحث الاجتماعي الذي يهدف إلى التقليل من الهيمنة وزيادة الحرية بجميع أشكالها.26

تركز النظرية النقدية على طبيعة التفاعلات الاجتماعية والتاريخية في النظام الدولي، وعليه فإنه لفهم طبيعة التهديدات السيبرانية لا يمكن أن تحدث بمعزل عن المتغيرات مثل التنافس الدولي وتاريخ العلاقات بين دولتين محل الصراع والعوامل الثقافية والاجتماعية التي يدور في إطارها الصراع. فمثلا لا يمكن تفسير الهجمات السيبرانية التي ارتكبها إيران ضد أكبر شركات النفط بالسعودية (أرامكو) منذ عام2012 إلى غاية 2017 في آخر هجمة تم رصدها، دون فهم السياق الجغرافي والتاريخي والاجتماعي والديني بين الدولتين وهذا ما استوجب إدخال البعد القيمي لدراسة الصراعات السيبرانية27، فأصحاب النظرية النقدية يؤكدون على أن الحقائق هي حصيلة لأطر اجتماعية وتاريخية محددة،28 يرفض النقديون فكرة أن البنية مؤلفة من القدرات المادية فحسب، فهم يؤكدون على أهمية البنية الاجتماعية، التي تتحدد من منطلقات المعرفة والممارسات المشتركة فضلا عن القدرات المادية والتي تكتسب معناها من خلال بنية المعرفة المغروسة فيها29.

حيث يعتبر النقديون أن العامل العسكري ليس وحده المحدد لحالة الأمن، حيث توجد عوامل أخرى من غير القوة والفوضى لفهم الأمن الدولي، فيرأيهم أن الأفكار، القانون، المؤسسات والمعرفة تلعب دورا في تحديد توجهات الدول داخل النظام الدولي، وعليه فإن التوجه الأمني للدول لا يتميز بالثبات فهو يتغير حسب طبيعة وثقافة وخبرة وإدراك كل دولة. مما يجعل تبني بعض الدول نموذج المدينة والحكومة الذكية يشكل مصدر تهديد سيبراني بسبب

---

[25]- إيهاب خليفة، نفس المرجع السابق، ص40-41.

[26]-Stanford Encyclopedia of philosophy, Critical theory https://plato.stanford.edu/entries/critical-theory/

[27]- إيهاب خليفة، نفس المرجع السابق، ص46.

[28]- جون بيليس، ستيف سميث، عولمة السياسة العالمية،دبي، ترجمة ونشر مركز الخليج للأبحاث، 2004، ص377.

[29]- نفس المرجع السابق، ص ص 435-436.

تعدد الأهداف الداخلية، غير أن البعض الآخر من الدول تعتبرها مصدر قوة تدفع الدول إلى زيادة مقدرتها على مستوى العسكري، سياسي والاقتصادي...إلخ.[30]

في الدول التي تعتمد على التكنولوجيات الحديثة في الاتصال والجيل الخامس للأنترنت بشكل رئيسي فإن تركيز المعلومات والبيانات الضخمة لدى المؤسسات يشكل تهديد للأفراد، فمن المحتمل أن تستغله الحكومات في دعم موقفها الانتخابي وتوجيه الرأي العام لما يخدم مصالحها الانتخابية، مما يجعلها تحتكر السلطة لعدة أعوام، وهنا تأتي أهمية المدرسة النقدية التي تعلي من دور الفرد لمواجهة الدولة.[31]

ومن أبرز المدارس النقدية لأمنية ثلاثة وهي:

1. مدرسة أبريستويث (المدرسة الويلزية):

سميت هذه المدرسة نسبة إلى بلده "أبريستويث" الواقعة بالساحل الغربي من ويلز. حيث تعد أول قسم للعلوم السياسية بالعالم تأسست عام 1919 لتصبح بعد ذلك في بداية التسعينات معقل للمقاربة النقدية للأمن بزعامة كل من "كين بوث" و"ريتشارد واين جونز" أما كتيار تنظيري وحركة فكرية تعود أصولها إلى الخمسينات عبر ما سمي باللجنة البريطانية لنظرية السياسات الدولية، ويعد "روي جونس" من الأوائل الذين أشاروا للمدرسة عبر مقال نشرة عام 1981 بعنوان" المدرسة الإنجليزية للعلاقات الدولية"ومن بين مؤسسيها "شارلز مانينج" و"مارتن وايت".

تقوم هذه المدرسة على النقيض مما جاءت بها المدرسة الواقعية ومدرسة كوبنهاجن حول فكرة مركزية لأمن الوطني ولأمن المجتمعي، حيث ترفض فكرة جعل الدولة وسيادتها مركز لموضوع لأمن، حيث يرى أنصار هذه المدرسة بأن انتهاك حقوق الإنسان، ولاضطهاد السياسي ونقص الموارد الخلافات العرقية مشكلات الهجرة والاندماج، لإرهاب، الجريمة تعتبر تهديدات أكثر واقعة وخطورة، هذا ما جعل المدرسة الويلزية تعمق مفهوم لأمن باقتراح أنطولوجيا جديدة لمفهوم لأمن الموسع يخرج عند نطاق الدولة ليشمل الأفراد والجماعات والإنسانية عكل.[32]

ومن أهم محددات الفكر الويلزي ثلاث أفكار رئيسية ألا وهي:

1. فكرة الانعتاق والتحرر لتحقيق لأمن:

وجه أنصار "المدرسة الويلزية" انتقادا للواقعيين بتركيزهم هام على القوة العسكرية ونموذج مركزية الدولة، حيث استوجب تجاوزه والتفكير في لأمن من خلال الانعتاق والتحرر من العبودية والفكرة الإنسانية المشتركة حيث ربط "واين جونز" بالكفاح التقدمي.[33]

ذهب "ريتشارد أشلي" إلى تعريف الانعتاق على أنه "ضمان الحرية من القيود غير المرئية وعلاقات الهيمنة، وظروف الاتصال والفهم المشوه، التي تقيد قدرة البشر على صياغة مستقبلهم الخاص". الانعتاق بهذا المفهوم تدعو إلى الحرية.

---

[30]- إيهاب خليفة، نفس المرجع السابق، ص 46.

[31]- إيهاب خليفة، نفس المرجع السابق، ص47.

[32]- صباح بالة، مدرسة ويلز(أبريستويث) للدراسات لأمنية، الموسوعة السياسية 09 /2022/12، تاريخ التصفح: 2023/09/12، 13:24. https://political.encyclopedia.org/dictionary/

[33]-إيهاب خليفة، نفس المرجع السابق، ص48.

ويكتب "لينكلايتر": "يجب أن يكون لديه القدرة على المبادرة" فهذه النظرية النقدية من خلال ما تقدم ذكره هو توسيع القدرة الإنسانية على تقرير مصيرها.34

2. الأفراد كموضوع للحقيقة الأمنية:

يرى أنصار مدرسة "أبريستويث" لا يمكن النظر لأمن الأفراد من منظور الأمن القومي، لأن هناك عدة حالات تتمتع فيها الدولة بالأمن في حين يعيش أفرادها في حالة من اللأمن وفي بعض الأحيان تكون الدولة هي مصدر تهديد أمني للأفراد.

فالأفراد –حسبهم- يعتبرون مركز التحليل الأمني ومن بين التحديات التي يواجهونها هي: التعنيق الجسدي، الاضطهاد، حالة اللأمن الصحي، الجهل، تدني المستوى المعيشي، البطالة، الإهانة والتهميش وغيرها من التهديدات التي تطال الأفراد في حياتهم الروتينية، لذلك يرى أنصار مدرسة "أبريستويث" أن الحقيقة والمعرفة الأمنية ليس الفرد في سياق الدولة وإنما الفرد غير آمن في بعده الذاتي.35

3. دور المؤسسة في إنتاج الحقيقة الأمنية:

يرى أنصار مدرسة "أبريستويث" أنه لتجاوز المنظور التقليدي للأمن يستوجب أكثر من مجرد نقد خلفية الدراسات الأمنية التقليدية، لكن أيضا وجب نقد لإطار المؤسساتي الذي أنتجت فيه. هذا يستدعي التحقيق في كيفية تكوين الحقل المعرفي داخل السياقات المؤسسية كالجامعات، المعاهد، مراكز البحث الدوائر الحكومية والمنظمات والمؤسسات الغير حكومية... إلخ.36

إن الحقيقة الأمنية ليست مجرد إقرارات أو أحكام علمية مبينة على مراقبة ظواهر معينة، فهي أيضا تعبر عن صراع الأفكار والقيم والتقاليد والمصالح المتباينة داخل لإطار المؤسساتي الذي تنتج فيه.وعليه فإن تعريف القضية الأمنية يتم دائما بواسطة عملية جدالية وتساومية بين المنظرين من داخل المؤسسة العلمية.37

2. مدرسة كوبنهاجن:

تعود أصل التسمية إلى الأجندة البحثية لمجموعة من الباحثين الأكاديميين في"معهد كوبنهاغن لأبحاث السلام" بالدانمارك. تم انتشاؤه عام381985 من بين روادها: باري بوزان (Barry Buzan) أول ويفر (Ole Waver) وجاب دي وايلد (Jaap de wilde) وغيرهم، وفي تحليل مدرسة كبونهاغن للظاهرة الأمنية تركز على ثلاث مستويات للتحليل وهي

---

[34]- سيد أحمد قوجيلي، الدراسات الأمنية النقدية مقاربات جديدة لإعادة تعريف الأمن، الأردن، المركز العلمي للدراسات السياسية، 2014، ص38.

[35]- نفس المرجع السابق، ص 39-40.

[36]- نفس المرجع السابق، ص40.

[37]- نفس المرجع السابق، ص41.

[38]- صباح بالة، مدرسة كوبنهاغن في تفسير الدراسات الأمنية، الموسوعة السياسية، 2020/12/09، تاريخ التصفح: 2023/09/12، 19:48.

https://political-encyclopedia.org/dictionry/

الفرد، الدولة، النظام الدولي، وأعطى كل من "باري بوزان" و"أول وايفر" بعدا جديد المفهوم الأمن، حيث طرح "باري بوزان" مفهوم "الأمن المجتمعي" و"أول وايفر" قدم تصورا مكملا له عرف بنظرية الأمننة(securitization theory) .39

1. الأمن المجتمعي:

الأمن المجتمعي حسب "باري بوزان" هو "الاستمرارية ضمن الشروط المقبولة للتطور، للأنماط التقليدية للغة والثقافة والهوية الدينية والقومية والعادات". بمعنى قدرة المجتمع على الاستمرارية في طابعه الجوهري في ظل الظروف المتغيرة والتهديدات المحتملة فمن خلال هذا التعريف فإن المجتمع والهوية هما العنصران المعرضان للتهديد. ويظهر هذا في محاولة اختراق الثقافات عبر مواقع التواصل الاجتماعي من خلال نشر الشائعات والأخبار المغلوطة التي تثير الفوضى في المجتمع.40

2. نظرية الأمننة (Securitization theory):

برزت نظرية الأمننة في ثمانينات القرن الماضي، ويتمحور جوهر هذه النظرية حول تبيان أن السياسات المؤطرة للأمن القومي للدول ليست سياسات مفروضة على الدول، كما أنها ليست أمرا معطا مسلما به في حد ذاته، بل أنها سياسات صممها السياسيين وصناع القرار. حيث يعلمون على استغلال ظرف دولي معين وتصويره للمستهدفين من هذه السياسات كما لو أنها أمر جللا أو تهديدا بالغ الخطورة ولتحقيق غاية التوافق الجمعي حول خطورة الموقف استوجب خطاب مقنع مكتمل الأركان.41

هذا ما يعني أن الأمننة تعني قيام الفاعلين في الدولة بعملية تحويل المواضيع إلى قضايا أمنية أي أنها نسخة معقدة من التسييس تسمح باستخدام معاني استثنائية باسم الأمن قصد استخدام تدابير استثنائية لحلها، ولكي تحقق الأمننة نجاحا كبيرا استوجب أن تلاقي قبولا واسعا جماهيريا، بغض النظر إذا كان موضع المشكلة يشكل تهديدا حقيقيا أو لا.42

3. مدرسة باريس:

تعود أصول هذه النظرية إلى بداية السبعينات، بزعامة منظرين فرنسيين متواجدين في أمريكا الشمالية وكندا أمثال: "ميشال فوكلت" و"بيار بوردي" وغيرهم،43 تعني هذه المدرسة بمواجهة التهديدات الأمنية المعاصرة من خلال التركيز على الممارسات والتقنيات المختلفة، التي تحاول تكييف مفهوم الأمن مع التطورات التكنولوجية الحديثة

---

[39]- أمينة قلعي، مدرسة كوبنهاغن:الأمننة ودور فعل الخطاب في تحديد المسألة الأمنية، المجلة الجزائرية للعلوم السياسية والعلاقات الدولية، العدد 11، ديسمبر 2018، ص ص 201-202.

[40]- إيهاب خليفة، نفس المرجع السابق، ص52.

[41]- عادل زعلوك، نظريات الأمننة في مجال العلاقات الدولية: من مدرسة كبونهاغن ونحو نظرية اتصالية مقترحة لدراسة الأمننة، مجلة السياسة والاقتصاد، تاريخ التصفح: 2023/09/12، 21:25 https:// jocu.journal-ekb.eg/article_229384.html

[42]-ضحى هوام، نظرية الأمننة، الموسوعة السياسية،2018/10/07، تاريخ التصفح:2023/09/12، 21:33 https://political-encyclopedia.org/dictionary

[43]-صباح بالة، مدرسة باريس للدراسات الأمنية، الموسوعة السياسة، 2020/12/22، تاريخ التصفح: 2023/9/12، 21:48. https://political-encyclopedia.org/dictionary

وطبيعة التهديدات المعاصرة التي تواجه الدول في عصر العولمة. وركزت على المواضيع الخاصة بالأمن الداخلي والممارسات الشرطية.

اهتمت مدرسة باريس بالمستويات الدنيا للتهديد والتهديدات الناجمة عن الهجرة والجريمة المنظمة والشغب ومراقبة الحدود، كما أدخلت تقنيات جديدة لعمل رجل الأمن في مختلف أجهزة الدولة الأمنية من الشرطة والمخابرات والجيش وحرس الحدود...إلخ، حيث يعتمدون على أحدث الوسائل المتطورة للتصدي للتهديدات الأمنية مثل: الإرهاب، الجريمة المنظمة، الهجرة الغير شرعية، التهريب والقرصنة السيبرانية...إلخ بالاعتماد على تقنيات حديثة ككاميرات المراقبة والفحص القبلي للأفراد وأجهزة تحديد الهوية وبرامج تتبع والمراقبة من خلال الأقمار الصناعية.

عملت المدرسة على تحقيق الاندماج بين الأمن الداخلي والخارجي بفعل العولمة وأعطت أهمية متزايدة لمختلف الفواعل الأمنية كأجهزة الشرطة والجيش والاستعلامات للتعامل مع التهديدات. حيث عمل على إعادة رسم الحدود بين الأنتربول الداخلي والخارجي، بما يمكنه توسيع أنشطة الأمن الداخلي من ناحية وإضفاء الطابع المحلي على الأمن الخارجي من ناحية أخرى.

ومنه يرى أنصار "مدرسة باريس" أن الدمج بين الأمن الداخلي والخارجي شرط أساسي لكي يمارس الحقل الأمني تأثيره، مما أعاد الاعتبار إلى بعض الأجهزة الأمنية التي كانت مقصاه في السابق مثل حرس الحدود، الجمارك وغيرها من الوكالات الأمنية والتي أصبحت في قلب مفهوم الأمن، لأن مقدراتهم الإنتاجية تبدو ملائمة للتخفيف من وطأة التهديدات المعاصرة.44

رغم الاهتمام الذي أولته النظريات النقدية بالأبعاد المعيارية والقيمية التي تساهم بشكل كبير في فهم عملية الصراع السيبراني وطبيعة التهديدات السيبرانية. إلا أن العديد من الإشكالات الأخرى التي لا يزال يشوبها الغموض وتحتاج إلى تمحيص ودراسة، كإشكالية التمييز بين ما هو مدني وما هو عسكري، فالطبيعة الصناعية التي يتميزها الفضاء السيبراني جعلت من الصعوبة التمييز بينهما. ضف إلى ذلك الطبيعة الفوضوية للفضاء السيبراني وغياب سلطة عليا تحكم التفاعلات التي تحدث داخله، وكذا عدم وجود مفاهيم كالسيادة الوطنية والحدود الجغرافية، بالإضافة إلى إشكالية إدارة العلاقة بين الفواعل من الدول والفواعل من غير الدول، هذا ما أدى في النهاية إلى عدم القدرة على توفير إطار تحليلي واضح كفيل بعض من حالات الصراع والردع والحرب السيبرانية.45

❖ النقد الموجه للفكر النقدي:

غياب إطار واضح لتحليل وفهم حالات الصراع والردع والحرب السيبرانية وذلك بسبب الطبيعة الفوضوية التي يتميز بها هذا الفضاء وغياب سلطة عليا تدير التفاعلات داخله.

أولت النظرية النقدية اهتمام واسع بالأبعاد القيمية والمعيارية لفهم الصراع في الفضاء السيبراني غير أن الطبيعة الصناعية لهذا الفضاء تجعل من الصعب جدا التمييز بين ما هو مدني و ما هو عسكري (خليفة 2021، 57).

خاتمة:

44- إيمان خليفة، نفس المرجع السابق، ص 56.

45- إيهاب خليفة، نفس المرجع السابق، ص 57.

كختام لما سبق طرحه نخلص بأن المدرسة الواقعية أخفقت في اعتبار أن الدولة هي الفاعل الوحيد في العلاقات الدولية، وهذا ما لا يمكن اسقاطه على التهديدات السيبرانية التي تضم الى جانب الدولة فواعل من غير الدول كالأفراد والشركات التكنولوجية والتنظيمات الإرهابية والتي لها دور فعال في الصراع السيبراني.

أما عن النظرية الليبيرالية التي وفقت في جزئية وهي فكرة الأمن الجماعي والذي يتحقق من خلال تعاون دولي ومؤسساتي، وعلى النقيض من ذلك فإن فكرة التعاون التكنولوجي صعب تحقيقه على أرض الواقع لما للفضاء السيبراني من خصوصية تستوجب التعامل فيه بسرية تامة.

في حين ذهب أنصار النظرية النقدية الى ضرورة ادخال البعد الاجتماعي والقيمي لفهم الصراعات السيبرانية غير أن الطبيعة الفوضوية التي تميز الفضاء السيبراني تجعل من الصعب وضع مفهوم موحد لطبيعة الصراعات السيبرانية فمنه ما له بعد اجتماعي وهوياتي وآخر اقتصادي وعسكري.

قائمة المراجع:

1. أمينة قلعي، مدرسة كوبنهاغن: الأمننة ودور فعل الخطاب في تحديد المسألة الأمنية، المجلة الجزائرية للعلوم السياسية والعلاقات الدولية، العدد 11، ديسمبر 2018، ص ص 201-202.
2. إيهاب خليفة، الحرب السيبرانية الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، القاهرة، العربي للنشر والتوزيع، 2021، ص23 .
3. ترجمة محمد صفار، نظريات العلاقات الدولية، القاهرة، سلسلة العلوم الاجتماعية، المركز القومي للترجمة،2014، ص52.
4. جراية الصادق، مفهوم الأمن في الفكر الاستراتيجي الإسرائيلي، رسالة دكتوراه، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 03، 2017، ص35 .
5. جون بيليس، ستيف سميث، عولمة السياسة العالمية،دبي، ترجمة ونشر مركز الخليج للأبحاث، 2004، ص377.
6. سيد أحمد قوجيلي، الدراسات الأمنية النقدية مقاربات جديدة لإعادة تعريف الأمن، الأردن، المركز العلمي للدراسات السياسية، 2014، ص38 .
7. صباح بالة، النظرية الليبيرالية في تفسير الدراسات الأمنية، الموسوعة السياسية، 10/03/ 2021، تاريخ التصفح: 11 /2023/09، https ://political-encyclopedia.org/dictionary/
8. صباح بالة، مدرسة باريس للدراسات الأمنية، الموسوعة السياسة، 2020/12/22، تاريخ التصفح: 2023/9/12، 21:48 https://political-encyclopedia.org/dictionary
9. صباح بالة، مدرسة كوبنهاغن في تفسير الدراسات الأمنية، الموسوعة السياسية، 2020/12/09، تاريخ التصفح: 2023/09/12، https://political-encyclopedia.org/dictionary/19:48.
10. صباح بالة، مدرسة ويلز(أبريستويث) للدراسات الأمنية، الموسوعة السياسية 09 /2022/12، تاريخ التصفح: 2023/09/12، 13:24 /https://political.encyclopedia.org/dictionary .
11. صليحة كبابي، الدراسات الأمنية بين الاتجاهين التقليدي والحديث، مجلة العلوم الإنسانية، جامعة قسنطينة، عدد38، ديسمبر2012، ص237.
12. ضحى هوام، نظرية الأمننة، الموسوعة السياسية،2018/10/07، تاريخ التصفح:2023/09/12، 21:33 https://political-encyclopedia.org/dictionary

13. عادل زعلوك، نظريات الأمننة في مجال العلاقات الدولية: من مدرسة كوبنهاغن ونحو نظرية اتصالية مقترحة لدراسة الأمننة، مجلة السياسة والاقتصاد، تاريخ التصفح: 2023/09/12، 21:25 https:// jocu.journal-ekb.eg/article_229384.html .
14. عشور قشي، نظرية مركب الأمن الإقليمي دراسة مقارنة بين إقليمي جنوب شرق آسيا والساحل الإفريقي، رسالة دكتوراه، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 03، 2016 ص21.
15. مصطفى دريدي، نظرية الأمن الإسرائيلية بين الاستمرارية والتغيير، رسالة ماجستير، كلية العلوم السياسية والإعلام، جامعة الجزائر03، 2012 ص27 .
16. Constantine,petallides, cyber terrorism and IR Theory:Realism،leberalism and constructivistm in the new securitythreat،indiquiries journal ،vol 4, NOO3,2012,accessed march7,2018. http://www.inquiriesjournal.com
17. Anthony Craig and Bradon valerian, Realism and cyber conflit: security in the digital Age, 03/02/2018 https: //www.eir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/
18. Anthony Craig and Bardon Valerian OPCIT.
19. Stanford Encyclopedia of philosophy, Critical theory https://plato.stanford.edu/entries/critical-theory/

واقع ورهانات الأمن السيبراني في العقيدة الدفاعية الجزائرية

The reality and stakes of cybersecurity in the Algerian defense doctrine

سالم نسرين[1](*) كلية الحقوق والعلوم السياسية، جامعة سطيف 2، n.salem@univ-setif2.dz

ملخص:

يعتبر الأمن السيبراني من أبرز المواضع والقضايا التي أصبحت تلقى اهتماما واسعا من قبل الدول والحكومات، نظرا لأن الفضاء السيبراني أصبح يضم العديد من التهديدات الأمنية السيبرانية والجرائم الالكترونية التي تتطلب سياسات واستراتيجيات فعالة من أجل مجابهته.

ومن بين الدول التي سعت إلى تفعيل سياستها الدفاعية والأمنية لمواجهة خطر الجرائم السيبرانية وتحقيق الأمن السيبراني هي الجزائر، ومنه تسعى هذه الدراسة إلى التطرق إلى واقع الأمن السيبراني في العقيدة الأمنية الجزائرية ومختلف التشريعات التي تؤكد على حمايته، إلى جانب متطلبات تحقيقه والتحديات التي تواجه الجزائر في سبيل تأمين الفضاء السيبراني.

الكلمات المفتاحية: الأمن السيبراني، العقيدة الأمنية الجزائرية، الجرائم السيبرانية، الدفاع الوطني.

Abstract:

Cybersecurity is considered one of the most prominent topics and issues that have received widespread attention from countries and governments, given that cyberspace has become home to many cybersecurity threats and cybercrimes that require effective policies and strategies in order to confront them.

Among the countries that have sought to activate their defense and security policy to confront the threat of cybercrime and achieve cybersecurity is Algeria, and from this this study seeks to address the reality of cybersecurity in the Algerian security doctrine and the various legislation that emphasize its protection, in addition to the requirements for achieving it and the challenges facing Algeria in How to secure cyberspace.

KeyWords: cybersecurity, Algerian security doctrine, cybercrime, national defense.

مقدمة:

إن تحولات النظام الدولي والمتغيرات التي تطرأ عليه أدت إلى التغيير في طبيعة ونمط التهديدات الأمنية، فلم نعد نتحدث عن الحروب البينية وإنما عن التهديدات الأمنية اللاتماثلية من جريمة منظمة وهجرة غير شرعية وإرهاب دولي وغيرها من التهديدات الجديدة التي تفرض على الدول ضرورة مواكبتها.

ومن أبرز التهديدات الحالية هي التهديدات السيبرانية التي تقترن بمجال الأمن السيبراني، هذا الأخير الذي يتعلق بضرورة حماية الأنظمة الإلكترونية والشبكات من الهجمات والتهديدات والاختراقات الالكترونية، وضوررة تبني استراتيجيات فعالة من قبل الدول وحتى المنظمات لمواجهة خطرها.

وفي هذا الصدد قدمت الجزائر العديد من الهيئات الأمنية التي تسمح بحماية الأمن السيبراني وسن المشرع الجزائر عدة قوانين وتشريعات تتضمن هذا المجال، وعلى هذا الأساس نطرح إشكالية الدراسة التالية:

فيما تتمثل الاستراتيجية الأمنية الجزائرية لتحقيق الامن السيبراني في ظل التحديات التي تواجهها؟

الأسئلة الفرعية:

تندرج تحت هذه الإشكالية الأسئلة الفرعية التالية:

- ما هو تعرف الأمن السيبراني؟
- ما هي أبرز مهددات الأمن السيبراني؟
- كيف ساهمت الجزائر في تحقيق الأمن السيبراني؟
- ما هي تحديات ومتطلبات تحقيق الأمن السيبراني في الجزائر؟

فرضيات الدراسة:

للإجابة على إشكالية الدراسة نقترح الفرضيات التالية:

- إن كثرة الثغرات الأمنية في الجهاز الأمني الجزائري تقف كعائق أمام الجزائر في سبيل تحقيق الأمن الجزائري.
- غياب أطر قانونية تصنف كل تهديد وجريمة الكترونية أدى إلى ضعف العقيدة الأمنية الجزائرية في مواجهة خطر الجرائم السيبرانية.

المحور الأول: تعريف الأمن السيبراني وأهم مهدداته:

أولا-تعريف الامن السيبراني:

بداية مصطلح Cyber يشير إلى صفة آلية وأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي[1].

الأمن السيبراني هو حماية الأنظمة المختلفة من الهجمات الإلكترونية، ويحاول التصدي للجرائم الإلكترونية والقرصنة التي قد تخترق الشبكات، وهو النظام الذي يهتم بتأمين وحماية أنظمة الكمبيوتر والشبكات والبرامج من

السرقة أو التلف، حيث يعمل الأمن السيبراني على حماية وتأمين الأجهزة والبرامج والبيانات الإلكترونية من الهجمات الرقمية، كما يوفر الأمن السيبراني الحماية ضد الهجمات الضارة، وهي التي تم تصميمها للوصول إلى البيانات الحساسة أو تغييرها أو حذفها[2].

يعرف الأمن السيبراني بكونه مجال من مجالات تكنولوجيا المعلومات والذي يعرف أيضا باسم أمن المعلومات Cyber security، وفيه يتم حماية الأفراد والمؤسسات والأنظمة من حالات الاختراق الرقمي أو الدخول الغير مصرح به أو التهديدات الأمنية الخطيرة، والتي قد تؤثر على خصوصية البيانات والمعلومات لاسيما الحساسة منها وكذلك إدارة عملية الإنتاج ذاتها، خاصة إن الصناعات بمختلف أنواعها الآن أصبحت مرتبطة ارتباطا وثيقا بالتكنولوجيا، والهدف الأساسي وراء ظهور الامن السيبراني هو ظهور ما يعرف بالهجمات الرقمية الخطرة أو الفيروسات المنيعة وفيها يتم الهجوم على الأنظمة الرقمية الخاصة بالأفراد أو المنشأة والسيطرة على ما تمتلكه من بيانات حساسة، وخضوعها لعمليات الابتزاز والسرقة وكذلك التخريب المتعمد للمعلومات وجراء الخسائر الفادحة التي تسببها هذه الهجمات، ظهر الأمن السيبراني، لا بهدف الدفاع أو الحماية فقط من الهجمات الحاسوبية الضارة، بل أيضا من أجل القيام بالهجوم المتعمد والذي يتم فيه اكتشاف الثغرات الموجودة في النظام والعمل على إصلاحها فور اكتشافها، وعادة ما يرتبط مجال الأمن السيبراني ببعض من المصطلحات المرتبطة ببعضها البعض كالجريمة السيبرانية والهجمات الإلكترونية:وفيها يتم التخطيط الغير قانوني باستخدام التكنولوجيا الرقمية لسيطرة على جهاز أو نظام تابع لفرد أو مؤسسة، باستخدام أجهزة متطورة أو استغلال ثغرات النظام، أو اعتمادا على جهل المستخدم وقلة ثقافته التكنولوجية[3].

ومن الناحية العملية لإجرائية يمكن تلخيص الأمن السيبراني على أنه لا يتعدى المفاهيم التالية[4]:

-يتكون إلى حد كبير من وسائل دفاعية تستخدم لكشف واحباط المتسللين.
-ينطوي على حماية شبكات الكمبيوتر والمعلومات التي تحتويها من الاختراق ومن الضرر الخبيث أو التعطيل.
-ينطوي على الحد من هجوم المخاطر الخبيثة على البرمجيات وأجهزة الكمبيوتر والشبكات. وهذا يشمل الأدوات المستخدمة للكشف عن اقتحام ووقف الفيروسات، ومنع وصولها، وفرض التوثيق، وتمكين الاتصالات المشفرة."
-هو مجموعة من الأدوات والسياسات والمفاهيم الأمنية، والضمانات الأمنية، والمبادئ التوجيهية، من المخاطر المحدقة بالمعلومات ومعالجتها، والإجراءات، والتدريب، وأفضل الممارسات، وضمان التقنيات التي يمكن أن استخدامها لحماية البيئة الإلكترونية وتنظيم أصول المستخدم ."
-القدرة على الحماية أو الدفاع عن استخدام الفضاء الإلكتروني من الهجمات السيبرانية .
_ الهيئة التكنولوجيات والعمليات والممارسات وتدابير الاستجابة والتخفيف، والتي تهدف إلى حماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من هجوم أو التلف أو الوصول غير المصرح به وذلك لضمان السرية والنزاهة".
-فن ضمان وجود واستمرارية مجتمع المعلومات للأمة، وضمان وحماية فضاء الإنترنت، والمعلومات الخاصة به، والأصول والبنية التحتية الحيوية .
-حالة محمي ضد المجرم أو الإستخدام غير المصرح به للبيانات الإلكترونية، أو التدابير المتخذة لتحقيق ذلك".

ثانيا- أهم مهددات الأمن السيبراني:

إن الجرائم السيبرانية تعد من الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها، فكانت بداية من مصطلح إساءة استخدام الكمبيوتر، مرورا بمصطلح احتيال الكمبيوتر، والجريمة المعلوماتية، فمصطلحات جرائم

الكمبيوتر، والجريمة المرتبطة بالكمبيوتر، وجرائم التقنية العالية، إلى جرائم الهاكرز، إلى آخر المصطلحات المتجسدة في الجرائم السيبرانية، ولهذا فإننا نجد في كل مرة مع ظهور مصطلح جديد لجرائم الانترنيت يظهر تعريف جديد للجرائم السيبرانية[5].

بينما الجرائم السيبرانية فيمكن القول أن الفقهاء والباحثون لم يتفقوا على تعريف موحد لها، فمنهم من ينظر الى موضوع الجريمة (كل سلوك إيجابي أو سلبي يقع باستخدام تقنية المعلومات على مصلحة مشروعة بالاعتداء) ومنهم من ينظر الى الوسيلة المستعملة لارتكابها (كل فعل اجرامي يستخدم الكمبيوتر كأداة رئيسية)، وتفاديا للقصور في التعريفات المضيقة ذهب البعض إلى القول بأن هذه الجرائم هي كل عمل أو امتناع عن عمل يأتيه الإنسان إضرارا بمكونات الحاسب المادية و المعنوية و شبكات الاتصال الخاصة به، باعتبارها من المصالح و القيم المتطورة التي يحميها القانون[6].

كما يمكن اعتبارها بأنها الجريمة ذات الطابع المادي، التي تتمثل في كل سلوك غير قانوني من خلال استخدام لأجهزة الالكترونية، ينتج عنه حصول اجرام على فوائد مادية أو معنوية مع تحميل الضحية خسارة مقابلة، وغالبا ما يكون هدف هذه الجرائم هو القرصنة من اجل سرقة أو إتلاف المعلومات الموجودة في لأجهزة ومن ثم ابتزاز لأشخاص باستخدام تلك المعلومات، و بالتالي تظهر الحاجة إلى وجود جدار قوي لحماية الشركات من هذه المخاطر و الذي يتمثل في أمن المعلومات للبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر الداخلية والخارجية[7].

تتضمن الجرائم السيبرانية عدة أنواع من الهجمات ولاختراقات السيبرانية، والتي تشمل:

- لاحتيال السيبراني: وهي عملية استخدام التقنيات الحاسوبية والإلكترونية للقيام بلاحتيال على الأفراد أو المؤسسات، والحصول على المال أو المعلومات بشكل غير مشروع.
- لاختراق السيبراني: وهي عملية الدخول إلى الأنظمة السيبرانية أو الشبكات الإلكترونية بشكل غير مصرح به، وسرقة المعلومات أو التلاعب بها أو تدميرها.
- الهجمات السيبرانية: وتشمل عمليات استخدام التقنيات الحاسوبية والإلكترونية لتعطيل الأنظمة السيبرانية أو الشبكات الإلكترونية أو الخوادم، وتعريض المعلومات والبيانات للخطر.
- التجسس السيبراني: وهي عملية استخدام التقنيات الحاسوبية والإلكترونية للحصول على المعلومات السرية أو الحساسة من الأنظمة السيبرانية أو الشبكات الإلكترونية، وذلك بغرض لاستخدام غير المشروع لهذه المعلومات.
- الابتزاز السيبراني: تشمل عمليات استخدام التقنيات الحاسوبية والإلكترونية لابتزاز الأفراد أو المؤسسات، والمطالبة بالمال أو المعلومات أو التهديد بنشر المعلومات أو البيانات الشخصية للأفراد.
- لإساءة السيبرانية: وتشمل عمليات استخدام التقنيات الحاسوبية والإلكترونية للإساءة إلى الأفراد أو المؤسسات أو التعرض لهم بشكل غير مشروع، وذلك عبر الإنترنت أو وسائل التواصل لاجتماعي أو البريد الإلكتروني[8].
- الإرهاب السيبراني: يعرف فورنيل ووارين لإرهاب السيبراني بأنه استخدام الجماعات لإرهابية السيبرانية للفضاء السيبراني، وهذا يشير إلى الانتقال من لإرهاب التقليدي الذي يعتمد على الوسائل المادية (من

أسلحة وذخائر وغيرها) إلى الإرهاب الحديث الذي يعتمد اعتمادا أكبر على التقنيات غير المرئية. ويعرف جيمس لويس الإرهاب السيبراني بأنه: استخدام أدوات الشبكة الحاسوبية لتدمير أو تعطيل البنى التحتية الوطنية المهمة؛ مثل الطاقة، والنقل، والعمليات الحكومية، بهدف إكراه أو ترهيب الحكومة أو المدنيين[9].

المحور الثاني:واقع الأمن السيبراني في الجزائر:

بالرجوع إلى التشريع الجزائري نجده لم يستقر على استخدام مصطلح واحد للدلالة على حيث سماها بموجب القانون 04-15 المتضمن قانون العقوبات بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، ثم بموجب القانون 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها، استخدم مصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للدلالة على هذه الجرائم وعرفها بأنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظم الاتصالات الالكترونية(المادة 01 من القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها)[10].

حيال هذا اتخذت الجزائر خطوة جديدة نحو مكافحة الجرائم الإلكترونية التي شهدت أرقاما قياسية العام الماضي واتخذت أشكالا جديدة، مما دفع مسؤوليها إلى إعلان حالة التأهب ضد الظاهرة السيبرانية. وبهدف مكافحة الجرائم السيبرانية، كشفت الجزائر أنها أعدت أكثر من 24 ألف مهندس وتقني متخصص في الأمن السيبراني. وبدأت الجزائر في تكوين أرقام أخرى "ذات كفاءة عالية في مكافحة الجرائم الإلكترونية وحماية الشبكات وأنظمة المعلومات. ويبدأ ذلك بتكوين موارد بشرية عالية الكفاءة. وفي عام 2002 أبرمت اتفاقيات في هذا المجال مثل شركة هواوي ومايكروسوفت وسيسكو في إطار الاستراتيجية الوطنية لتطوير الاقتصاد الرقمي والأمن السيبراني[11].

وفي هذا السياق، أنشأت الجزائر أجهزتها الأمنية لحماية منظومتها السيبرانية، معتمدة على مؤسسة الدفاع الوطني كأحد أولوياتها، أسوة ببقية دول العالم التي سارعت إلى مراجعة سياساتها الأمنية وأدخلت آليات والتقنيات المعنية بهذه القضايا، بالتوازي مع تطوير البنية التحتية، وفيما يتعلق بتقنيات العالم الرقمي، فإن مطلب الأمن يفرض مضاعفة أنظمة المراقبة التي قد تشكل تهديدا محتملا للحريات الفردية، ولذلك فإن كافة المقاربات الأمنية في مجال الأمن الرقمي يجب أن تكون مصحوبة بالأطر القانونية والتكنولوجية المناسبة وتأخذ في الاعتبار دقة وتعقيد الهجمات الإلكترونية التي تزداد خطورتها مع التطور التكنولوجي واستخدامها دائما، وتجسيدا لذلك باشرت الدولة الجزائرية وفي مقدمتها مؤسسة الدفاع الوطني إلى إعداد برامج خاصة لمجابهة الجريمة الالكترونية والحد من انتشارها، وإنشاء أجهزة جديدة تنسجم أدوارها وتجهيزاتها مع المتغيرات الحاصلة في هذا المجال، إذا أصبحت الحماية السيبرانية جزءا مهما في أي منظومة للدفاع .وقد استطاع الجيش الوطني الشعبي المضي قدما ومسايرة التطورات التكنولوجية والإعلامية الحاصلة في العالم، ومن ثمة تأمين وحماية نطاقه المعلوماتي لكل الناشطين فيه[12].

وقد أكد رئيس الجمهورية عبد المجيد تبون في مراسم افتتاح الملتقى الوطني حول الأمن السيبراني الذي تنظمه وزارة الدفاع الوطني على ضرورة العمل على تطوير إستراتيجية وطنية متكاملة في المجال الرقمي، وأن تحديد التهديدات السيبرانية ووضع آليات الرقابة والرصد الناجعة وجاهزية الإستراتيجية في حالات الخطر، يشكل اليوم أحد أهم الشروط الإستباقية لتوفير الحماية اللازمة والكاملة للمنشآت الحيوية بشكل آمن ومستمر، وذلك ضمن منظومة التكفل بالأمن الوطني، بأبعاده السياسية والعسكرية والاقتصادية والمجتمعية

بل وحتى التكنولوجية، وهو الأمر الذي يستوجب تطوير إستراتيجيتنا الوطنية المتكاملة في المجال الرقمي، والجمع بين الاستباقية والوقاية من التهديدات في الفضاء السيبراني، وحماية المنظومات والمعطيات، والسهر على ترقية ثقافة رقمية مواطنية ووطنية عمادها التحسيس المستمر واليقظة الإستراتيجية لكل المؤسسات[13].

ورغم هذه الجهود التي تبذلتها الجزائر في مجال تحقيق الأمن السيبراني إلا أنها تبقى في نظرنا بحاجة إلى القيام بالعديد من الإجراءات، التي يمكن أن نوردها فيما يلي:

- إقامة العدة العسكرية السيبرانية بتكليف عدد كبير إقامة العديد من الأفراد العسكريين بمهمة القتال الإفتراضي استجابة للتهديد الجديد للحرب السيبرانية، ويمكن أن يشمل هذا التحول السياسي إنشاء فرق حربية للإنترنت تكون مكرسة لتحقيق الأمن السيبراني، ويمكن دمجها في وكالات استخبارات أخرى، أو حتى إنشاء قطاعات جديدة تماما ضمن الهيكل العسكري المكرس للنشاط السيبراني، وتقام هذه العدة عداد الموارد العسكرية من أجل جميع أنواع عمليات الفضاء السيبراني العسكرية الجديدة ويمكن دمجها في وكالات استخبارات اخرى، ويمكن أن تكون أيضا مسؤولة عن تأمين الشبكات الخاصة التي تشغل جزءا كبيرا من العمليات العسكرية.

-تكوين نخب وطنية مختصة في مجال الأمن السيبراني، مع ضرورة إجراء مؤتمرات علمية يشارك فيها مختلف المختصين العالميين من أجل الإستفادة من خبراتهم .

-الإستفادة من تجارب الدول الرائدة في مجال تحقيق الأمن السيبراني، والتعرف على أفضل التقنيات العالمية المنتهجة في مكافحة الجرائم الإلكترونية من قرصنة وتجسس وارهاب الكتروني

- اعتماد سياسة وقائية بنشر ثقافة الأمن السيبراني وزيادة الوعي المجتمعي بمختلف المخاطر والتهديدات التي تفرضها الثورة التكنولوجية الحديثة، وتحصين أفراد المجتمع ضد كل الأفكار الهدامة[14].

المحور الثالث: تحديات تحقيق الأمن السيبراني في الجزائر:

يواجه عمل الأجهزة الأمنية وفروعها المختلفة في تحقيق استراتيجيتها الأمنية في الفضاء السيبراني عدد من المعوقات والتحديات، منها:

- أبرز عائق تواجهه أجهزة الأمن لتحقيق الاستراتيجية الدفاعية المبنية على الأمن السيبراني هو غياب مواد قانونية متخصصة بكل حالة من الجرائم السيبرانية والتي يمكن أن تسهل أداء المهام بمالحقة المتربصين والمهددين لأمن الأفراد والدولة، حيثل تجد الأجهزة الأمنية صعوبة في تجسيدها على أرض الواقع.
- ارتفاع حجم التهديدات السيبرانية وتمكن قراصنة الفضاء السيبراني من تطوير أدواتهم آلياتهم والتسبب بأضرار بالغة تسببت بخسائر مادية مقارنة بإجراءات الجهاز الأمني لتحقيق الأمن السيبراني.
- غياب التنسيق بين الأجهزة الأمنية الوطنية والدولية، مما يجعل مهمة تأمين الشبكة من القراصنة والإرهاب الإلكتروني الدولي مهمة صعبة، هذا بالإضافة إلى ما يحمله الفضاء السيبراني من صراع السيبراني والحروب الإلكترونية بين الوحدات الدولية.
- ضعف التوعية الأمنية من قبل الأجهزة الأمنية بمفهوم الأمن السيبراني لمستخدمي شبكة الأنترنت، ما قد يعرضهم للانتهاك والابتزاز بسبب ضعف التدابير اللازمة والإحتياطات الأمنية.
- تعدد الفواعل الدولية والتي تشكل تهديد للفضاء السيبراني من حركات إرهابية ودول معادية وقراصنة الفضاء السيبراني.

خاتمة:

- يعمل الأمن السيبراني على حماية وتأمين الأجهزة والبرامج والبيانات الإلكترونية من الهجمات الرقمية، كما يوفر الأمن السيبراني الحماية ضد الهجمات الضارة، وهي التي تم تصميمها للوصول إلى البيانات الحساسة أو تغييرها أو حذفها.
- تظهر الحاجة إلى وجود جدار قوي لحماية الشركات من هذه المخاطر والذي يتمثل في أمن المعلومات للبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر الداخلية والخارجية.
- أنشأت الجزائر أجهزتها الأمنية لحماية منظومتها السيبرانية، معتمدة على مؤسسة الدفاع الوطني كأحد أولوياتها، وسارعت إلى مراجعة سياساتها الأمنية وأدخلت آليات وتقنيات جديدة معنية بهذه القضايا.
- رغم الجهود التي تبذلها الجزائر في مجال تحقيق الأمن السيبراني إلا أنها تبقى بحاجة إلى القيام بالعديد من الإجراءات وتفعيل مؤسساتها الأمنية لمواجهة تهديدات الامن السيبراني.

قائمة المراجع:

- روان بنت عطية الله الصحفي، الجرائم السيبرانية، المجلة الالكترونية الشاملة متعددة التخصصات، ع 24، 2020، ص. 7.
- سمير بارة، الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر: الدور والتحديات، المجلة الجزائرية للأمن الإنساني، مج 2، ع 2، ص ص. 427-428.
- مهدي رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة إيليزا للبحوث والدراسات، مجلد 6، ع 2، 2021، ص. 113.
- لخضر دولي ونفيسة ناصري، دور الذكاء الاصطناعي في مواجهة الجرائم الالكترونية، مجلة المؤشر للدراسات الاقتصادية، مجلد 2، ع 2، 2018، ص ص. 53-54.
- عنترة بن مرزوق، ومحي الدين حرشاوي، الامن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية، مجلة الحقوق والعلوم السياسية، 2017، ص. 75.
- سُني ذو الهدى، تهديد الإرهاب السيبراني - وإمكانية تطبيق اتفاقية الجرائم السيبرانية، التحالف الإسلامي العسكري لمكافحة الإرهاب، 2020/06/23، ص. 2.
- بكوش الرميساء، انعكاسات التهديدات السيبرانية على الامن الوطني الجزائري، مذكرة ماستر في العلوم السياسية، 2019، جامعة العربي التبسي تبسة، ص ص. 48-49.
- أسماء ماضي، الدليل الشامل حول الامن السيبراني، 2023/10/09، في:
https://www.hotcourses.ae/study-abroad-info/applying-to-university/all-you-need-to-know-about-cyber-security/
- الامن السيبراني: مفهومه وخصائصه وأشهر أنواع التهديدات فيه، 2023/01/01، في:
https://www.e3melbusiness.com/blog/cyber-security
- بيان لوزارة الدفاع الوطني، وزارة الدفاع الوطني، 2023/06/07، في:
https://www.mdn.dz/site_principal/sommaire/actualites/ar/2023/juin/cna07062023ar.php
- مفهوم الجرائم السيبرانية وانواعها وأساليب ارتكابها وطرق مكافحتها، نقلا عن:
https://bitly.ws/32Fvs

- يونس بورنان، الجزائر تضع 24 ألف مختص في الامن السيبراني لمواجهة الجرائم الالكترونية، 2018/04/17، في:

https://al-ain.com/article/algeria-cyber-security

الحواشي:

---

[1] روان بنت عطية الله الصحفي، الجرائم السيبرانية، المجلة الالكترونية الشاملة متعددة التخصصات، ع 24، 2020، ص. 7.

[2] أسماء ماضي، الدليل الشامل حول الامن السيبراني، 2023/10/09، في:

https://www.hotcourses.ae/study-abroad-info/applying-to-university/all-you-need-to-know-about-cyber-security/

[3] الامن السيبراني: مفهومه وخصائصه واشهر أنواع التهديدات فيه، 2023/01/01، في:

https://www.e3melbusiness.com/blog/cyber-security

[4] سمير بارة، الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر: الدور والتحديات، المجلة الجزائرية للأمن الإنساني، مج 2، ع 2، ص ص. 427-428.

[5] روان بنت عطية الله الصحفي، مرجع سبق ذكره، ص. 8.

[6] مهدي رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة إيلزا للبحوث والدراسات، مجلد 6، ع 2، 2021، ص. 113.

[7] لخضر دولي ونفيسة ناصري، دور الذكاء الاصطناعي في مواجهة الجرائم الالكترونية، مجلة المؤشر للدراسات الاقتصادية، مجلد 2، ع 2، 2018، ص ص. 53-54.

[8] مفهوم الجرائم السيبرانية وانواعها وأساليب ارتكابها وطرق مكافحتها، نقلا عن:

https://bitly.ws/32Fvs

[9] سُني ذو الهدى، تهديد الإرهاب السيبراني - وإمكانية تطبيق اتفاقية الجرائم السيبرانية، التحالف الإسلامي العسكري لمكافحة الإرهاب، 2020/06/23، ص. 2.

[10] مهدي رضا، المرجع سبق ذكره، ص. 113.

[11] يونس بورنان، الجزائر تضع 24 ألف مختص في الامن السيبراني لمواجهة الجرائم الالكترونية، 2018/04/17، في:

https://al-ain.com/article/algeria-cyber-security

[12] بكوش الرميساء، انعكاسات التهديدات السيبرانية على الامن الوطني الجزائري، مذكرة ماستر في العلوم السياسية، 2019، جامعة العربي التبسي تبسة، ص ص. 48-49.

[13] بيان لوزارة الدفاع الوطني، وزارة الدفاع الوطني، 2023/06/07، في:

https://www.mdn.dz/site_principal/sommaire/actualites/ar/2023/juin/cna07062023ar.php

[14] عنترة بن مرزوق، ومحي الدين حرشاوي، الامن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية، مجلة الحقوق والعلوم السياسية، 2017، ص. 75.

أثر المخاطر السيبرانية على الأمن القومي في الجزائر

The impact of cyber risks on national security in Algeria

ط.د/ جدي علاء الدين (*) مخبر الدراسات السياسية والدولية، جامعة أمحمد بوقرة بومرداس، (الجزائر)
al.djeddi@univ-boumerdes.dz
د/ أمينة سرير عبد الله، مخبر الدراسات السياسية والدولية، جامعة أمحمد بوقرة بومرداس، (الجزائر)
boumerdes.dz-serir-abdallah@univ.a

ملخص:

يعد الأمن السيبراني والتهديدات المترتبة عنه من المواضيع المهمة نظرا للأخطار التي أصبحت تمس كل الميادين والمجالات ومن أهمها الأمن القومي الذي يعد الركيزة الأولى لأمن وسلامة المجتمع، وعليه عملت الدول على تعزيز امنها القومي بتطوير استراتيجيات للحد من المخاطر السيبرانية حفاضا على سلامة بياناتها ومعلوماتها، ومن بينها الجزائر التي تعتمد على العديد من الآليات الدفاعية، من خلال استحداث العديد من المراكز والمصالح الأمنية التي تعمل على محاربة التهديدات والمخاطر السيبرانية في كل المجالات، بالإضافة إلى تشريع قوانين ردعية مع العمل على الجانب التحسيسي بمخاطر الاستخدام غير العقلاني لتكنولوجيات الاعلام والاتصال.

الكلمات المفتاحية: الأمن السيبراني؛ الامن القومي؛ المخاطر السيبرانية؛ التهديدات السيبرانية؛ الجزائر.

Abstract: *Cybersecurity and the threats resulting from it are among the important topics due to the dangers that have begun to affect all fields and areas, the most important of which is national security, which is the first pillar of the security and safety of society.*

Accordingly, countries have worked to strengthen their national security by developing strategies to reduce cyber risks in order to preserve the safety of their data and information, including Algeria relies on many defense mechanisms, through the creation of many security centers and departments that work to combat cyber threats and risks in all fields, in addition to legislating deterrent laws while working to raise awareness of the dangers of irrational use of media and communication technologies.

KeyWords: *cybersecurity; national security; Cyber risks; cyber threats; Algeria*

مقدمة:

يشهد العالم في السنوات والأخيرة تطورا هائلا في تكنولوجيات الاعلام والاتصال بمختلف مجالاتها، والتي تساهم في تقديم خدمات راقية وعالية الدقة في مختلف ميادين الحياة السياسية والاقتصادية والاجتماعية والثقافية وغيرها، ناهيك عن توفيرها للوقت والجهد، ما جعل من الافراد التمسك بها وعدم الاستغناء عن خدماتها لسهولة استخدامها عنها.

إلا أنها في نفس الوقت أصبحت تشكل تهديدا ومخاطر على أمن الافراد والمجتمعات وكذا الأمن القومي للدول نتيجة الاستخدام الغير الامثل لتكنولوجيا الاعلام والاتصال، وهذا ما يشهده العالم جراء التصاعد المستمر لمختلف المخاطر والتهديدات السيبرانية، مما أدى الى عمل الدول والحكومات عل تطوير استراتيجيات أمنية تواكب التطورات والتهديدات الجديدة من أجل تعزيز امنها القومي، والجزائر واحدة من الدول التي تشهد هذه التهديدات وبشكل متزايد في مختلف المجالات الحياتية، الأمر الذي جعل النخب الحاكمة والأمنية تعمل على صياغة الاستراتيجيات المعتمدة في تعزيز الأمن القومي من مختلف المخاطر والتهديدات السيبرانية.

ومنه نطرح الإشكالية التالية:

- فيما تتمثل المخاطر السيبرانية على الأمن القومي الجزائري؟ وماهي الآليات الجزائرية المعتمدة في الحد منها؟

وتنقسم هذه الإشكالية إلى الأسئلة الفرعية التالية:

- ما المقصود بالأمن السيبراني والأمن القومي؟
- كيف تؤثر المخاطر السيبرانية على الأمن القومي؟
- ماهي الإجراءات الجزائرية المتخذة للحد من المخاطر السيبرانية على أمنها القومي؟

وللإجابة على الإشكالية نطرح الفرضية التالية:

- ارتبطت الإجراءات الجزائرية لحماية أمنها القومي بإنشاء مراكز متخصصة في الدفع السيبراني .

منهج الدراسة :

تم استخدام المنهج الوصفي في دراسة الأوضاع الراهنة التي تتمثل في المخاطر السيبرانية وأثرها على الأمن القومي الجزائري ومعرفة إجراءات الحماية المتخذة في هذا الجانب .

تقسيم الدراسة:

تم تقسيم الدراسة الى ثلاثة محاور، الأول يتعلق بالإطار المفاهيمي للأمن السيبراني والقومي بالإضافة للمخاطر السيبرانية، والثاني يتعلق بأهم المخاطر السيبرانية على الامن القومي الجزائري، أما الثالث يتعلق بالجهود الجزائرية للتصدي لهذه المخاطر والتهديدات.

المحور الأول: مفهوم الأمن السيبراني والأمن القومي

يعد مفهوم الأمن من أهم المواضيع في حياة الافراد والمجتمعات لارتباطاته بالعديد من الأبعاد من بينها السيبراني والقومي، وهذا ما سيتم التعرف عليه من خلال هذا العنصر.

أولا-مفهوم الأمن السيبراني

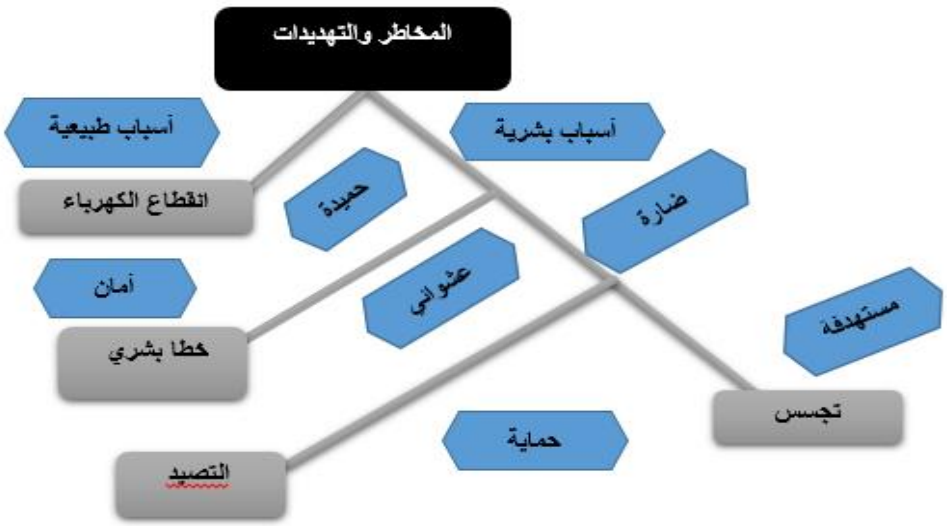
1- تعريف المخاطر السيبرانية:

من أجل تحديد مفهوم الخطر السيبراني يجب تقسيم هذا المصطلح، حيث يعرف الخطر على أنه عدم اليقين أو الوقوع في حالة غير مرغوب فيها، والسيبراني يعرف على أنه الكتروني ويصطلح على كل ما هو متعلق بالشبكة الالكترونية الحاسوبية والأنترنت.[1]

وعليه يمكن القول إن الخطر السيبراني هو الحاق الضرر بسرية وسلامة المعلومات المتوفرة وتحقيق خسارة من خلال هجمات في الفضاء السيبراني.

ومن هنا يمكننا تحديد نوعين من التهديدات أو المخاطر السيبرانية، والتي تتمثل في مخاطر بشرية أو طبيعية كما هي مبينة في الشكل الموالي.

الشكل 01: أنواع المخاطر السيبرانية



المصدر:[2]

2- تعريف لامن السيبراني:

[1]- العايبسناء، " تسيير المخطر السبرانية في القطاع المالي من المظور الدولي"، مجلة الدرلسات المالية والمحاسبية والإدارية، المجلد 08، العدد 03، 2021، ص 467.

[2] - Herrmann, Dominik; Henning , Pridöhl," Basic concepts and models of cybersecurity" , The ethics of cybersecurity,2020 vol 21,p15.

أما مصطلح الأمن السيبراني نشأ من الفضاءات السيبرانية، حيث يستخدمه المتخصصين في تكنولوجيا المعلومات والاستشاريون ورجال السياسة لمعالجة الاخطار الأمنية في الفضاء السيبراني[1].

تعني كلمة أمن في الفضاء الالكتروني كل إجراءات الحماية لردع الأعمال العدائية والاستخدام الغير أخلاقي والسيئ لتكنولوجيا الاعلام والاتصال.[2]

يعرف الأمن السيبراني على أنه مجموعة من الأدوات والسياسات والمفاهيم والضمانات الأمنية والمبادئ التوجيهية وكل الأساليب والممارسات والاجراءات والتقنيات التي يمكن استخدامها من أجل حماية المعلومات ضد التهديدات الداخلية والخارجية، من خلال مجموعة من الأهداف الأمنية والتي تتمثل فيما يلي[3]:

- السرية: عدم اتاحة الوصول الى أصول المعلومات الا لمجموعة محددة بتصريح، من أجل حمايتها ن الكشف غير المصرح به، أو التسريب المقصود أو غير المقصود للبيانات الحساسة.
- النزاهة: معالجة البيانات بشكل صحيح ودقيق، وحمايتها من التعديل غير المصرح به.
- التوفر: تمتع البيانات بالمرونة للوصول اليها عند الحاجة في أي وقت كان، أي محمية من التعطيل غير المصرح به.

ويعرف أيضا على أنه مجموعة الأطر القانونية والتنظيمية التي تعمل على حماية الفضاء السيبراني مع ضمان توافر الأنظمة المعلوماتية والمحافظة على الخصوصية، بداية بحماية المعلومات الشخصية للمستهلكين من مخاطر الفضاء السيبراني.[4]

كما تعرفه المنظمة الدولية للاتحاد الدولي للاتصالات بأنه مجموعة الأدوات والسياسات والمفاهيم وضمانات الأمنية والمبادئ والتقنيات المستعملة في حماية الفاء الالكتروني، وتنظيم أصول المستخدمين وتشمل أجهزة الحوسبة والموظفين والخدمات ومجل المعلومات المخزنة أو المرسلة في الفضاء الالكتروني.[5]

ولضمان حماية البيانات والبنى التحتية في الفضاء الالكتروني للحكومات والمنظمات أو الشركات لابد لتوفر مجموعة من الأطر والمعايير التي تتعلق بالأمن السيبراني كما هي موضحة في الجدول الموالي:

---

[1] - Oruj Zahid, "Cyber Security: contemporary cyber threats and National Strategies" , Distance Education in Ukraine: Innovative, Normative-Legal, Pedagogical Aspects ,2023 ,no 2 ,p 103.

[2]- عادل عبد الصادق، لسلاحة الفضاء الالكتروني في ضوء القانون الدولي الانساني، المركز العربي لأبحاث الفضاء الالكتروني، القاهرة، مصر،ط2، 2016، ص 13.

[3] -Authority Saudi Arabian Monetary, Cyber Security Framework , Riyadh Saudi Arabia ,2017,pp 5 ,6.

[4]-علي زايد العلي، المرتكزات النظرية في السياسة الدولية، دار الفجر للنشر والتوزيع، القاهرة، مصر،ط1، 2017، ص 224.

[5]- رقولي كريم، نويوة لخضر، "الأمن السيبراني المتوسطي بين الواقع والرهانات الأمنية"، مجلة طبنة للدراسات العلمية الأكاديمية، المجلد 02، العدد 02، 2019، ص 72.

الجدول (01): الفرق بين المعايير والأطر التي تتعلق بالفضاء السيبراني

الأطر في الفضاء السيبراني	المعاسير في الفضاء السيبراني
• تعد الأطر هي كل الارشادات العامة التي تغطي مجموعة واسعة من المجالات والمكونات داخل المنظمات، ومع ذلك لا يتم تحديد الخطوات التي يجب اتباعها بشكل خاص. • تحدد الأطر الأساسيات لإنشاء شيء ما أو تحقيق هدف معين. • يتم استخدام هذه الأطر من أجل تحديد معايير الجودة التي ينبغي تحقيقها، ووصف النطاق وتحديد التقييم والتنفيذ، وتلخيص الأهداف والنتائج.	• كل المستندات التي تعمل على تحديد الإجراءات والمبادئ التوجيهية لسلامة وموثوقية الخدمات والأنظمة والمنتوجات. • العمل على تطوير المعايير من طرف المنظمة أو الدولة أو الشركة واعتباره معيارا خاصا تنظيمي محلي. • تعتبر المعايير أدلة امتثال للمنظمة المنفذة وفق اطر قانونية أو تنظيمية. • إمكانية دمج المعايير لتكملة وتعزيز المتطلبات. • هناك معايير مفتوحة ومتاحة لجميع أنواع الشركات والمؤسسات الحكومية، وأخرى مغلقة غير متاحة وهي خاصة بأعمال وصناعات معينة. • المعيار هو ما يجب القيام به من خلال شرح الطرق لإكمال العملية

المصدر:[1]

ولتحقق الامن السيبراني وجب العمل على تضافر الجهود في جميع أنحاء النظم المعلوماتية وتشمل هذه الجهود على عناصر الأمن السيبراني والتي تتمثل فيما يلي:[2]

- أمن الشبكات: استعمال إجراءات متطورة لحماية الشبكات من الاختراق.
- أمن التطبيقات: وضع إجراءات لحماية البرامج من الفيروسات والاعتداءات الأخرى.
- أمن المعلومات: وضع ضوابط تعمل على ضمان خصوصية الاستعمال والتصرف في المعلومات.
- الأمن التشغيلي: معالجة المعلومات وتخزينها وحمايتها.
- التعافي من الكوارث: صيانة وتعديل الاضرار للتعافي من الاخطار والتهديدات وفقدان المعلومات.
- استمرارية العمل: الاستمرارية في العمل أثناء خرق المعلومات من خلال خطوات وبرامج معينة.

ثانيا: مفهوم الأمن القومي

اكتسب مفهوم الأمن في السنوات الأخيرة معنى أوسع وشاملا، ففي الماضي كان المحللون الأمنيون يقتصرون على جانب ضيق من القضايا، خاصة المتعلق بتوازن القوى العسكرية بين الدول والكتل المختلفة، فضلا عن قدرة هذه

[1] - Hamed, Taherdoost, "Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview",Journals Electronics, 2022, p3.

[2]- مسيكة محمد، "الفضاء السيبراني وتحديات الأمن القومي للدول"، مجلة العلوم القانونية والاجتماعية، المجلد 07، العدد 04، 2022، ص 458.

الكيانات على حماية سيادتها، ولم تكن المصادر الاقتصادية والاجتماعية والإنسانية والبيئية مصدر قلق كبير، ولكنها أصبحت تشكل تهديداً للسلام والأمن في العقود الأخيرة فالقضايا الإنسانية والأخلاقية، التي لعبت في السابق دورا محدودا إلى حد ما في مناقشة الأمن العالمي، تحتل الآن مكانا مركزيا فيها.[1]

1- تعريف الأمن:

يتمحور مطلح الامن في معناه اللغوي على الطمأنينة والاستقرار، أما المعنى الاصطلاحي فهو يختلف باختلاف المدارس الفكرية التي ينتمي اليها الباحثين، وعليه نجد اختلاف في تحديد مفهوم الأمن من خلال التعاريف الغير متفق عليه.[2]

ويعتبر تعريف الامن عند باري بوزان "barry buzen " من اهم التعاريف اذ يعد لأحد لأبرز المتخصصين في الدراسات الأمنية، حيث يعرفه على انه العمل على التحرر من التهديد وفي سياق النظام الدولي فهو قدرة واستطاعة الدولة والمجتمع على المحافظة على كيانها المستقل وتماسكها الوظيفي ضد قوى التغيير التي تعتبرها معادية[3].

2- تعريف الأمن القومي:

تتعدد التعاريف بتعدد المفكرين والمدارس الفكرية والزوايا التي ينظر اليها مما أدى الى هذا التعدد في التعاريف المطروحة للأمن القومي.

يعرفه سبيكمان بأنه حماية استقلالية الدولة وسيادتها، والدفاع عن اقليمها ضد أي عدوان يهدد وجودها مع الحفاض على كرامتها الوطنية، فللأمن القومي مفهومين أولهما ضيق يتعلق بالحماية المادية للوجود ومكونات الدولة من مختلف التهديدات، والثاني يشتمل على الحماية المادية بالإضافة لحماية قيمها ومصالحها الاقتصادية والسياسية والثقافية والاجتماعية، ويركز " روبرت ماكنمارا " في تعريفه على أهمية التنمية مع تعزيز القوة العسكرية كضامن لها.[4]

كما يعتبر تراج وكرونينرج القيم الحيوية جوهر سياسة الأمن القومي التي تعمل على إيجاد سياسة محلية ودولية ملائمة لحماية وتوسيع القيم الحيوية ضد الأعداء القائمين او المرتقبين والمحتملين.[5]

ويعرفه الدكتور عبد المنعم المشاط على أنه قدرة الدولة على حماية الوطن من التهديدات التي تواجهه بالإضافة الى قدرة الدولة على حماية مواطنيها، وتحسين نوع وجودة الحياة ومستواها.[6]

---

[1] - Kriukov Oleksiy, Michalski Tomasz, "Geopolitical choice of the national security ideology: the example of Ukraine", Przegląd Geopolityczny, vol 44, 2023,p 45.

[2]- مسيكة محمد، مرجع سابق، ص 451.

[3]- كولثي عتيقة، " تداعيات الإرهاب السيبراني على الأمن القومي الجزائري"، المجلة الجزائرية للأمن والتنمية، المجلد 12، العدد 03، 2023، ص ص، 208،209.

[4]- العومير وليد عبد الهادي، بن جليل فرج عصام، بني سليم يحي محمد، " أثر التحديات الداخلية والخارجية على الأمن القومي العربي الواقع وآفاق المستقبل"، مجلة علوم الإنسان والمجتمع، المجلد 10، العدد 3، 2021، ص 128.

[5]- سرير عبد الله أمينة، "الأمن القومي الجزائري والأزمة الليبية: حدود المواقف وتحديات المواجهة"، حوليات جامعة الجزائر 1، المجلد 37، العدد 2، 2023، ص 517.

[6]- بوقارة صالح، " مسألة التوظيف الخارجي للاقليات في منطقة الشرق الأوسط وأثرها على الأمن القومي العراقي"، مجلة المعيار، المجلد 27، العدد 5،2023، ص 1224.

وعليه فان مفهوم الأمن القومي يشمل سلامة أرض الدولة ووجود انسجام وسلامة اجتماعية داخليا، ووجود قوة عسكرية رادعة داخل الدولة، بالإضافة الى اقتصاد وتنمية قوية وتوفر استقرار سياسي لدى الدولة، مع مواكبة تطورات الحماية والامن في جميع المجالات.

وعليه تم تحديد ايدولوجية الامن القومي فيما يلي:[1]

- حماية أراضي الدول من التدخلات الداخلية والخارجية.
- الدفاع ضد التأثير المعلوماتي للمعارضين الايديولوجيين.
- تطوير العلاقات وهياكل المساعدات الخارجية التي كان يقوم عليها التوازن بين الشرق والغرب.
- استخدام الأسلحة والروابط العسكرية والوجود العسكري العالمي والعمليات السرية كأداة للسياسة الخارجية.
- الجهود الدبلوماسية للحد من السباق نحو التسلح.

المحور الثاني: أهم المخاطر السيبرانية على الأمن القومي الجزائري

تعد المخاطر السيبرانية أو التهديدات الالكترونية ذات الطابع الدولي لا تمس دولة بعينها بل تهدد كل اقطار العالم، وذلك يعود لكون الوسائل التكنولوجية أضحت متاحة في كل مكان من العالم وفي كل وقت من الأوقات، ومنه ساهمت الخصائص ومميزات التهديدات والاخطار السيبرانية التي تتخطى الحدود الجغرافية وصعوبة تتبع المتسببين والناشطين في هذا المجال من قبل السلطات سوآءا المحلية او الدولية وزيادة الاهتمام بهذا النوع من الجرائم الحديثة على حساب الجرائم التقليدية، وهذا راجع الى صعوبة تحديد أماكن الناشطين ويعود ذلك لنقص الخبرة لدى بعض الأجهزة الأمنية في المجال الالكتروني والفضاء السيبراني.[2]

ومن خلال التطور التكنولوجي الذي يشهده العالم أصبحت التهديدات والمخاطر السيبرانية أحد أهم وأخطر الجرائم التي تهدد الامن القومي الجزائري، بداية بمظاهر الترويج لكل أنواع العنف والتطرف باستخدام التقنيات التكنولوجية الجديدة، حيث أصبح الفضاء السيبراني احد اهم الوسائل في يد الجماعات الإرهابية لنشر أفكارهم ودعاياتهم، كما يتم استخدام التكنولوجيا في المساس بأمن الدول عن طريق اختراق الأنظمة المهمة في الدول وسرقة المستندات أو اتلافها، وهذا بما يسمى بانتقال الصراع من الجانب المادي الى العالم الافتراضي.[3]

فقد صاحب التطور التكنولوجي تنامي المخاطر والتهديدات على الامن القومي للدول جميعا والجزائر خاصة، وذلك من خلال الاشكال المتعددة للمخاطر كما يلي:[4]

1- الحرمان من الخدمة:

وتتعلق بالمخاطر والتهديدات التي تهدف الى إيقاف قدرة المستهدف على تقديم الخدمات المفترض تقديمها أو المعتادة، من خلال تكثيف الأوامر التي تؤدي الى توقيف جهاز الحاسب الالي المقدم للخدمة، وذلك من خلال اختراق الأجهزة الالكترونية وتحميل مجموعة من البرامج عليها، لتستخدم في شن هجوم على الخصم بشكل مؤامن من خلال إعطاء اوامر بدأ لهذه البرامج .

---

[1] - Kriukov Oleksiy, Michalski Tomasz, "Geopolitical choice of the national security ideology: the example of Ukraine" , Przegląd Geopolityczny , 2023,vol 44 ,p 44.

[2]- جغم محمد الامين، "جرائم الارهاب الالكتروني والجرائم المظمة"، مجلة القانون الدولي والتنمية، المجلد 06، العدد 1، 2018، ص 25.

[3]- بن مرزوق عنترة، الكر محمد، "البعد الإلكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب"، مجلة العلوم الانسانية والاجتماعية، العدد 38، 2018، ص 37.

[4]- جعفري عبد الله، "التهديدات السيبرانية وتأثيرها على الامن القومي الجزائري"، المجلة الافريقية للدراسات القانونية والسياسية، المجلد 06، العدد 02، 2022، ص ص، 248،249.

2- التجسس السيبراني:

يعد التجسس من أخطر الجرائم والتهديدات في الفضاء السيبراني، فهي تعد نتاج للتقدم العلمي والتكنولوجي في شأن أجهزة التصنت ذات القدرة الفائقة، فهي تعمل على جمع المعلومات العسكرية والسياسية وحتى المعلومات المتعلقة بالمجال الاقتصادي والاجتماعي، فالتجسس قد يعمل على تعطيل عمل الشبكات التكنولوجية وأنظمتها وحواسيبها بغرض سرقة معلومات سرية تتعلق بالسياسة او الاقتصاد وبالأخص المعلومات العسكرية، فالتجسس السيبراني يعتبر من أهم الأساليب التي تلجأ لها المنظمات الإرهابية والاجرامية لجمع المعلومات حول المؤسسات الحكومية لاستخدامها في الاضرار بالمجتمع ومصالحه.

3- الإرهاب السيبراني:

ويعني استخدام الكمبيوتر وشبكات المعلومات من أجل التخويف والترهيب لتحقيق أهداف سياسية، حيث تعمل الجماعات الإرهابية بتمرير رسائل عبر مختلف وسائل الاتصال التي تتعلق بالشبكة العنكبوتية مفادها التهديد بمختلف الأساليب من أجل تحقيق الأهداف المرسومة سواءًا من الدول المستهدفة أو الشعوب أو الأفراد، من اجل الحصول على الأموال في معظم الأحيان، وعليه فالإرهاب السيبراني يعم كل النشاطات التي تشمل الشبكة وتهدف الى نشر أفكار متطرفة من اجل تحقيق مآرب خاصة .

4- سرقة المعلومات العسكرية:

ويتم ذلك من خلال اختراق الأنظمة وقواعد البيانات العسكرية وسرقتها أو تدميرها وتزييفها الكترونيا، وقد تتمثل في خرائط نشر أنظمة التسلح أو التنظيمات الخاصة بالمعدات العسكرية وغيرها من المعلومات السرية.

وعليه فكل هذه الأخطار لها تأثير على الأمن القومي، وباعتبار الفضاء السيبراني لا يخضع للحدود، فالأخطار والتهديدات الأمنية الجديدة اخذت بعد الكتروني يرتبط بالتطور التكنولوجي الذي هو من نتاج الدول المتطورة التي تمتلك كل خفاياه وأبجدياته لتكون مصدر الاخطار والتهديدات السيبرانية.

ومنه نجد ان البنية التحتية الالكترونية الجزائرية ضعيفة مقارنة بالدول المتطورة، لذلك يجب على الجزائر مواكبة التطور واستحداث منظومات دفاعية قوية لصد الاخطار والتهديدات السيبرانية التي تهدد الأمن القومي في كل حين.

وانطلاقا مما سبق نجد أن الأمن السيبراني أصبح أكبر تحديات الامن القومي في القرن الواحد والعشرين، ويعود ذلك للمفهوم الحديث للأمن الذي تعدى الجوانب العسكرية والتقليدية بل واكب كل التهديدات المادية والافتراضية التي قد تشكل عائق امام تدفق المعرفة والاقتصاد الرقمي.

المحور الثالث: جهود الجزائر لمواجهة الاخطار والتهديدات السيبرانية:

في ظل التطورات التكنولوجية الحاصلة وتنامي المخاطر والتهديدات السيبرانية وانعكاساتها على الأمن القومي الجزائري، أضحت الجزائر ملزمة بحماية امنها القومي من خلال تبني مجموعة من الاليات والجهود التي تكفل الحماية ومواجهة هذه التهديدات والمتمثلة في بعدين أساسيين كما يلي:

1- البعد القانوني:

سعت الجزائر الى استحداث وسن الاحكام القانونية لمكافحة الجريمة في الفضاء السيبراني معتمدة في ذلك على ثلاثة معايير تجلت في: وسيلة الجريمة والمتمثلة في تكنولوجيا الاتصال، وموضوعها الذي يتمثل في المساس بأنظمة المعلومات، بالإضافة الى الجانب الشرعي الذي تمثله العقوبات التي تحددها التشريعات القانونية، حيث نجد المادة

02 من القانون 09-04 الصادر في 09-05-2009، الذي يحدد القواعد الخاصة للوقاية من الجرائم في الفضاء السيبراني والمتعلقة بتكنولوجيا الاعلام والاتصال، بالإضافة الى المادة 323 من القانون 05-10 المؤرخ في 20-06-2005، الذي يتضمن الدليل الالكتروني، بالإضافة الى أنه تم تعديل مجموعة من المواد من قانون الإجراءات الجزائية وأخرى من قانون العقوبات، التي تتضمن تجريم وتسليط العقوبة على الذين ثبت في حقهم القيام بعملية اختراق أنظمة معلومات الافراد او المؤسسات بطريقة غير شرعية.[1]

وعليه فالإطار القانوني مهم جدا في الحد من المخاطر والتهديدات السيبرانية وتأثيراتها المحتملة على الامن القومي، من خلال تنظيم استخدام التكنولوجيات الاتصالية في اطارها الشرعي وعدم التعدي، فمن يتعدى يسلط في حقه عقوبات ردعية، باعتبار أي تعدي على أمن الأفراد والمؤسسات هو خرق وتعدي على الامن القومي الجزائري، وهذا ما جعل المشرع الجزائري لفرض فصل كامل يتعلق بالتهديدات السيبرانية وجرائم تكنولوجيا الاعلام والاتصال، من خلال الفصل السابع من قانون العقوبات.

1- البعد العملي:

من أجل تحقيق الامن السيبراني في الجزائر، كرست السلطات العليا لأجهزة الأمنية من خلال استحداث خلايا متخصصة تعمل وفق احترام الحريات والشرعية الدستورية والاتفاقيات الدولية، ومن بينها ما يلي:

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها: كان أساس تشكلها المرسوم الرئاسي رقم 15-261، حيث أنها سلطة إدارية مستقلة لدى وزارت العدل تعمل تحت اشراف لجنة يترأسها وزير العدل، وتظم قضاة وضباط وأعوان شرطة قضائية من مختلف الأجهزة الأمنية وفق قانون الإجراءات الجزائية، وتعمل على الوقاية من الجرائم التي تتعلق بتكنولوجيا الاعلام والاتصال، بالإضافة الى مكافحتها وتكثيف عمليات الوقاية منها، وذلك من خلال جمع المعلومات والتزود بها وضمان المراقبة الوقائية في الفضاء الالكتروني، لأجل تكشف وتحديد التهديدات التي تمس بالأمن القومي الجزائري.[2]

المصلحة المركزية لمكافحة الجريمة المعلوماتية :(SCLC) تعتمد هذه المصلحة التابعة للمديرية العامة للأمن الوطني على موارد بشرية ذات كفاءة مهنية عالية تكفل تنفيذ مهامها على المستوى الدولي بتعاملها مع كل المصالح المتخصصة التي تتمثل في "الافريكوم والانتبول "، ومصالح الشرطة لكبرى الدول، ومحليا يتم التنسيق مع مصالح الشرطة العلمية والشرطة القضائية.[3]

مركز الوقاية من جرائم الاعلام الالي والجرائم المعلوماتية :(CPLCIC) تم انشاء هذا المركز سنة 2008 بمدينة الجزائر العاصمة، تابع للقيادة العليا للدرك الوطني، تتمحور أهميته من خلال تأمين منظومة البيانات والمعلومات لخدمة الأمن العمومي، حيث يعد مركز توثيق يعمل على دراسة وتحليل البيانات والمعطيات لتحديد مرتكبي الجرائم الالكترونية الحاصلة، والعمل على التسويق الأمني بين الأجهزة الأمنية.[4]

المعهد الوطني للأدلة الجنائية وعلم الاجرام للدرك الوطني :(INCC) هو معهد تابع لقيادة الدرك الوطني، تعتمد مهامه على الخبرة العلمية والتجارب المخبرية الدقيقة للأدلة المتحصل عليها في مكان الجرائم المرتكبة، ومن خلاله

---

[1]- بوازدية جمال، "الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية "التحديات والافاق المستقبلية""، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01، 2019، ص 1278.

[2]- بارة سمير، "الأمن السيبراني (cyper security) في الجزائر: السياسات والمؤسسات"، المجلة الجزائرية للأمن الانساني، المجلد 02، العدد 02، 2017، ص ص ، 274، 275.

[3]- بوازدية جمال، المرجع السابق، ص 1280.

[4]- جعفري عبد الله، المرجع السابق، ص 252.

يتبين أن الجرائم في الفضاء الالكتروني بالجزائر تتضاعف بسرعة هائلة، حيث سجلت أكثر من 2500 جريمة سنة 2017، منها 70 ب تتعلق بانتهاك الحريات الشخصية، وتم إحصاء أكثر من 28 مليون شخص يستعمل الانترنت و18 مليون لهم حسابات فيسبوك و13 مليون متصفح يومي لشبكات التواصل الاجتماعي، بالإضافة الى ان عمليات الاختراق مست وزارة الدفاع الوطني، وحسب المركز فالمؤسسة تجهض يوميا قرابة 3500 محاولة اختراق في اطار الحروب الالكترونية.[1]

مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة: تتبع هذه المصلحة قيادة الجيش الوطني الشعبي على مستوى دائرة الاستعمال والتحضير، هدفها حماية وتأمين المنشآت الخاصة بالقوات المسلحة الجزائرية ضد اي تهديد سيبراني، حيث تتمحور استراتيجيتها الدفاعية على الجوانب التالية[2]:

- الجانب الوظيفي : فعالية وتناسق الاعمال التي تتعلق بالدفاع السيبراني.
- الجانب القانوني: تحيين وتعزيز التشريعات والاطر القانونية لضمان تامين منظومات الاعلام.
- الجانب البشري : تكوين الموارد البشرية وتجهيزها ككفاءات في المجال.
- الجانب التقني : كفاءة الوسائل والأجهزة المستعملة للكشف والرد على الهجمات والتهديدات السيبرانية.

مما سبق نجد ان الاستراتيجية الجزائرية تعتمد على المقاربة الدفاعية في تعزيز أمنها القومي تجاه التهديدات السيبرانية واعتماد الردع السيبراني كاهم الية لمواجهة مختلف الاخطار والتهديدات السيبرانية وهو ما تسعى اليه الاجهزة الأمنية الجزائرية لحماية الفضاء السيبراني باعتبارها مسؤولية جماعية تضمن من خلال استراتيجية وطنية شاملة للامن السيبراني، يجب على الجميع الانخراط فيها، لان الأمن السيبراني أصبح سلاحا استراتيجيا بيد الافراد والحكومات، في ظل التطور المتسارع لتكنولوجيات الاعلام والاتصال.

بالإضافة الى الأطر والتشريعات القانونية والامنية اعتمدت الجزائر ايضا على الجانب التحسيسي بمخاطر الاستخدام غير الامثل للتكنولوجيا والجرائم والمخاطر والتهديدات الناجمة عنها، من خلال الأجهزة الأمنية ومنظمات المجتمع المدني ميدانيا، إضافة الى التحسيس عبر مختلف وسائل الاعلام والاتصال، وذلك لما تلعبه الجوانب التحسيسية والتوعوية من دور مهم في الحد من انتشار هذه المخاطر.

خاتمة

في الاخير نستخلص أن الأمن السيبراني أصبح من أهم أولويات الدول والأنظمة السياسية باعتباره يرتبط بأمن المعلومات والمعطيات لدي الأفراد أو الدول في جميع المجالات السياسية والاقتصادية والاجتماعية والثقافية، ويعود ذلك لمختلف المخاطر والتهديدات الجديدة التي تواكب التطورات التكنولوجية لوسائل الاعلام والاتصال، التي تتمثل في سرقة وتدمير المعلومات والبيانات والتجسس السيبراني، الارهاب السيبراني، خاصة البيانات والمعلومات الحساسة العسكرية والسياسية، فالتهديدات أصبحت تؤثر بشكل كبير على الأمن القومي للدولة، ما جعل الجزائر تكثف جهودها بهدف الحد من هاته المخاطر والتهديدات من خلال استحداث العديد من الآليات سواء في شقها القانوني، والعملي المتمثل في استحداث المؤسسات الأمنية والادارية من أجل حماية الفضاء السيبراني الجزائري من أي مخاطر وتهديدات، وتبين أن الجزائر اعتمدت المقاربة الدفاعية والردع السيبراني، انطلاقا من الدور التحسيسي والتوعوي بمخاطر الاستخدام غير الامن لتكنولوجيات الاعلام والاتصال.

وعليها يمكننا طرح مجموعة من التوصيات كما يلي:

---

[1]- بوازدية جمال، المرجع السابق، ص ص، 1280-1281.
[2]- جعفري عبد الله، المرجع السابق، ص ص، 252-253.

- نشر الوعي من خلال تبيان المخاطر والتهديدات السيبرانية على الأفراد والمؤسسات، من خلال التنشئة الاجتماعية.
- الاهتمام بالكفاءات وتوفير الظروف لإنتاج برامج دفاعية وهجومية عالية الدقة من ناحية الأمان والتصدي للهجمات السيبرانية.
- نشر ثقافة التبليغ عند التعرض لمثل هذه الأخطار، خاصة قضايا الابتزاز والتهديد.

الهوامش والمراجع:

Authority, . A. (2017). *Cyber Security Framework.* Riyadh Saudi Arabia.

Hamed, T. (2022). Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. *Journals Electronics*, pp. 01-20.

Herrmann, D., & Henning , P. (2020). Basic concepts and models of cybersecurity. *The ethics of cybersecurity, 21*, pp. 11-44.

Kriukov, O., & Michalski, T. (2023). Geopolitical choice of the national security ideology: the example of Ukraine. *Przeglqd Geopolityczny, 44*, pp. 41-53.

Oruj, Z. (2023). Cyber Security: contemporary cyber threats and National Strategies. *Distance Education in Ukraine: Innovative, Normative-Legal, Pedagogical Aspects*(2), pp. 100-116.

العومير وليد عبد الهادي، فرج عصام بن جليل ، و يحي محمد بني سليم. (2021). أثر التحديات الداخلية والخارجية على الأمن القومي العربي الواقع وآفاق المستقبل. *مجلة علوم الإنسان والمجتمع، 10*(3)، الصفحات 119-165.

بوقارة صالح. (2023). مسألة التوظيف الخارجي للاقليات في منطقة الشرق الأوسط واثرها على الأمن القومي العراقي. *مجلة المعيار، 27*(5)، الصفحات 1219-1236.

سرير عبد الله أمينة. (2023). الأمن القومي الجزائري والأزمة الليبية: حدود المواقف وتحديات المواجهة. *حوليات جامعة الجزائر 1، 37*(2)، الصفحات 515-532.

سناء العايب. (2021). تسيير المخاطر السيبرانية في القطاع المالي من المنظور الدولي. *مجلة الدراسات المالية والمحاسبية والإدارية، 8*(3)، الصفحات 465-483.

عادل عبد الصادق. (2016). *اسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني* (الإصدار 2). القاهرة، مصر: المركز العربي لأبحاث الفضاء الالكتروني.

علي زايد العلي. (2017). *المرتكزات النظرية في السياسة الدولية* (الإصدار 1). القاهرة، مصر: دار الفجر للنشر والتوزيع.

كريم رقولي، و نويوة لخضر. (2019). الأمن السيبراني المتوسطي بين الواقع والرهانات الأمنية. *مجلة طبنة للدراسات العلمية الأكاديمية، 2*(2)، الصفحات 70-84.

كواشي عتيقة. (2023). تداعيات الإرهاب السيبراني على الأمن القومي الجزائري. *المجلة الجزائرية للأمن والتنمية، 12*(3)، الصفحات 205-214.

مسيكة محمد. (2022). الفضاء السيبراني وتحديات الأمن القومي للدول. *مجلة العلوم القانونية والاجتماعية*، *7*(4)، الصفحات 447-462.

الحروب السيبرانية وتأثيرها الاستراتيجي على الأمن القومي للدول: "الواقع والتحديات"

Cyber Wars and Strategic Impact on Countries' National Security: Reality and Challenges

جويدة حمزاوي(*)
قسم العلوم السياسية، جامعة محمد لمين دباغين، سطيف 2،
d.hamzaoui@univ-setif2.dz

ملخص:

يعتبر الفضاء السيبراني -بالإضافة إلى كونه مجالاً اجتماعيا للتواصل والتبادل- مصدرا للتهديدات الأمنية، ومسرحا تقترف فيه الجرائم، ومجالا حيويا تخاض فيه الهجمات والجرائم وأفعال التخريب والانتهاكات، بل وحتى الحروب الفعلية، خصوصا في ظل عدم التمكن التكنولوجي واستيعاب خباياه ودسائسه.

في هذا السياق، تبلورت ظاهرة الحروب السيبرانية التي اتسمت بخصائص مختلفة عن نظيراتها التقليدية، سواء من حيث طبيعة الأنشطة العدائية، الفواعل، والتأثيرات في بنية الأمن العالمي، وعبرت تلك الحرب عن نمطين من القوة (الناعمة والصلبة) في عملية توظيف التفاعلات في الفضاء الإلكتروني، وهذا بعد أن أخذ متغير القوة بعدا جديدا غير العسكري والاقتصادي وأصبح الحديث عن البعد التكنولوجي والقوة السيبرانية، وما يرافق هذا البعد الجديد للقوة من أسلحة وهجمات وحروب رقمية قد تؤدي إلى شلل جزئي لسير الدولة أو الاقتصاد أو الأنظمة المدنية الجماعية، مما يعكس تنامي القدرات والتهديدات المتصاعدة لأمن البنية التحتية الكونية للمعلومات.

تحاول هذه الدراسة الخوض في هذا الوسط التنازعي الجديد وتقصي خباياه، وذلك بالتطرق إلى طبيعة مفهوم "الحروب السيبرانية"، والجدل المثار حوله، سيما مع تداخله مع مفاهيم أخرى، مثل الإرهاب الإلكتروني، والحرب غير المتماثلة، كما تتناول الورقة الأطر المرتبطة والمفسرة للجريمة السيبرانية باعتبارها أحد التحديات الكبرى للأمن السيبراني، وأبرز أنماطها من واقع التفاعلات الدولية، وأخيرا تداعيات ومخاطر ذلك على على الأمن القومي للدول.
الكلمات المفتاحية: الفضاء السيبراني؛ التهديدات الأمنية؛ الحروب السيبرانية؛ الجريمة السيبرانية؛ الأمن السيبراني.

Abstract:

In addition to being a social area of communication and exchange, cyberspace is a source of security threats, a scene where crimes are committed, a vital area where attacks, crimes, acts of vandalism and violations are fought, even actual wars, especially in the light of technological inadequacy and the assimilation of its invisibility and intrigue, accompanying this new dimension of power are digital weapons, attacks and wars that may lead to partial paralysis of the functioning of the State, the economy or collective civilian systems,

In this context, the phenomenon of cyber wars with characteristics different from their traditional counterparts has become evident, whether in terms of the nature of hostile activities, the actions, the effects on the global security architecture, that war expressed two patterns of power (soft and hard) in the process of employing interactions in cyberspace, This after the power variable took on a new non-military and economic dimension and became the talk of the technological dimension and cyber power, this reflects growing capacities and escalating threats to the security of the world's information infrastructure.

This study tries to wade into this new conflicting medium and investigate its invisibility by addressing the nature of the concept of cyber warfare and the controversy surrounding it, significantly as it overlaps with other concepts, such as cyberterrorism, asymmetric wars; the paper also addresses the associated and interpreted frameworks for cybercrime as one of the significant cybersecurity challenges, It highlighted its patterns from international interactions and, finally, its implications and risks for States' national security.

Keywords: *cyberspace; Security threats; cyber wars; cybercrime; Cybersecurity.*

مقدمة:

يعيش العالم اليوم مرحلة جديدة من التطور التكنولوجي امتزجت فيها نتائج ثلاث ثورات وخلاصاتها، هي: ثورة المعلومات وذلك الكم الهائل من المعرفة في صورة تخصصات ولغات عديدة، التي أمكن السيطرة عليها بواسطة تكنولوجيا المعلومات؛ وثورة وسائل الاتصال المتمثلة في تكنولوجيا الاتصال الحديثة، وقوامها الأقمار الصناعية والألياف البصرية؛ وأخيرا، ثورة الحواسيب الإلكترونية التي توغلت في جميع نواحي الحياة.

إن محاولات دراسة تأثير الانتقال إلى عصر المعلوماتية على الأمن أثمرت خلال تسعينيات القرن العشرين تطورا لفكرة "الثورة في الشؤون العسكرية"، حيث ظهرت بيئة جديدة وهي "الفضاء السيبراني" كمجال جديد للتفاعلات الدولية، وبرزت حالة توظيفه في استخدامات مدنية وأخرى ذات طبيعة عسكرية، وأضحى مثل غيره من المجالات الدولية كالبر والبحر والجو.

هذا، وقد تبلورت الأنشطة العدائية العنيفة في ظاهرة الحروب السيبرانية في القرن الواحد والعشرين التي اتسمت بتعدد مظاهرها وخصائصها والفاعلين فيها، والتي ظهرت عبر نمطين أساسيين؛ نمط يتعلق بتوظيف القوة الناعمة في الصراع عبر الفضاء الإلكتروني، والنمط الآخر يتعلق بتوظيف القوة الصلبة، وهو ما يعكس تنامي القدرات والتهديدات وتعاظم التأثير على أمن البنية التحتية الكونية للمعلومات، حيث أفضى انتقال الناس من العالم الواقعي إلى العالم الافتراضي بسبب هذا التطور للوسائل الإلكترونية والأنترنيت ووسائل الاعلام والاتصال إلى انتقال التهديدات إلى هذا الفضاء، مما أدى بدوره إلى ظهور نوع جديد من الجريمة وهي الجريمة السيبرانية.

من هنا، تطرح هذه الدراسة الإشكالية التالية: كيف تؤثر الجريمة السيبرانية على الأمن القومي للدول؟

ولمحاولة الإجابة عن الإشكالية المطروحة سيتم التطرق للنقاط التالية:

- أولا: من الفضاء السيبراني.. إلى القوة السيبرانية.
- ثانيا: الحروب السيبرانية كمدخل مستحدث للحروب التقليدية.
- ثالثا: الجريمة السيبرانية كتهديد للأمن السيبراني...وكقضية للأمن القومي.

المحور الأول: من الفضاء السيبراني.. إلى القوة السيبرانية

يخلط البعض بين الفضاء السيبراني والأنترنيت، وعلى الرغم من أن بنيته أساسها الأنترنيت[1]، فالفضاء السيبراني هو عبارة بيئة افتراضية تتصل عن طريق شبكات الكمبيوتر وتعمل بها المعلومات الإلكترونية، كما يعرف أيضا بأنه المجال الكهرومغناطيسي لتخزين وتعديل أو تغيير البيانات المتصلة والمرتبطة بشبكة البنية التحية الطبيعية، ويتضمن عملية الاندماج ما بين الانترنيت والمحمول وأجهزة الاتصالات والأقمار الصناعية، والفضاء السيبراني أكبر من الأنترنيت لما يحتويه من قدرات توجيهية للطاقة التي توجد في جزء من الموجات الكهرومغناطيسية.

أدت الثورة التكنولوجية في وسائل الاتصالات الحديثة إلى ظهور أدوات جديدة غير تقليدية يمكن للدول والجماعات استخدامها في إدارة العلاقات الدولية المعولمة، مما أدى إلى إعادة بناء العديد من المفاهيم المركبة في العلاقات الدولية، أبرزها: مفهوم "قوة الفضاء الالكتروني" Cyber power، والذي يعرفه جوزيف ناي بأنه: "القدرة على تحقيق الأهداف المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء الالكتروني"[2]. بمعنى آخر: "مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات، الشبكات الإلكترونية، البنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل".

ويعتبر ويليام جيبسون "William Gibson" من ابتكر عبارة "الفضاء السيبراني"[3]، حيث يمنح الفضاء السيبراني "Cyber Space" -حسبه- القوة لأولئك الذين يمكنهم معالجة المعلومات في الفضاء السيبراني[4] ، يؤدي هذا إلى تعريف "القوة السيبرانية Cyber Power " بأنها القدرة على استعمال الفضاء السيبراني لخلق الفوائد والتأثير على الأحداث في جميع البيئات الطبيعية (جوا، برا وبحرا) وعبر أدوات القوة[5]، وبينما يعد الفضاء السيبراني كبيئة، فالقوة السيبرانية هي دائما مقياس للقدرة لاستعمال هذه البيئة، والتكنولوجيا هي العامل الأول المساعد، لأن القدرة على دخول الفضاء السيبراني هي التي تجعل من الممكن استعماله، وهذه التكنولوجيا متغيرة باستمرار، فبعض المستخدمين (بلدان، مجتمعات، فواعل غير حكوميين...) يمكنهم التغلب على التكنولوجيات القديمة واستخدام أخرى جديدة لمصلحتهم، كما تلعب العوامل التنظيمية أيضا دورا مهما. لقد اعتبرت القوة السيبرانية الأداة الأكثر تأثيرا في العقدين الماضيين، فقد أصبحت عنصرا لا غنى عنه في التقنيات الحديثة المستندة للقدرة العسكرية[6].

بالتالي، أصبح للفضاء السيبراني دور أساسي في تعظيم القوة أو لاستحواذ على عناصرها لأساسية في العلاقات الدولية، وأصبح التفوق في هذا المجال عنصرا حيويا في تنفيذ عمليات ذات فاعلية في (الأرض، البحر، الجو والفضاء)، واعتماد القدرة القتالية في هذا الفضاء على نظم التحكم والسيطرة التكنولوجية.

عادة ما تترجم الدولة قدراتها على تحقيق أهدافها الخارجية من خلال استخدامها لوسائل مختلفة أهمها الدبلوماسية، القوة العسكرية، الدعاية، الأدوات الاقتصادية، ولكن أصبح من المتفق عليه في مجال العلاقات الدولية أن مصادر وأشكال القوة تتغير، فإلى جانب القوة الصلبة التي تشمل القدرات العسكرية والاقتصادية، تزايد الاهتمام بالأبعاد غير المادية للقوة، ومن ثم برز دور القوة الناعمة التي تعتمد على جاذبية النموذج والإقناع، ومع ثورة المعلومات والقدرة على إنتاج التكنولوجيا المتطورة عن طريق الاختراع والإبداع، ظهر شكل جديد من أشكال القوة وهي القوة السيبرانية، وأصبح لديها تأثير على المستوى المحلي والدولي من ناحية أدت إلى توزيع القوة بين عدد أكبر من الفاعلين، مما جعل قدرة الدولة على السيطرة على هذا الميدان محل شك مقارنة بالمجالات الأخرى للقوة،

ومن ناحية أخرى، جعلت الفاعلين الأصغر في السياسة الدولية، لديهم قدرة أكبر على ممارسة كل من القوة الصلبة والناعمة في الفضاء الإلكتروني، وهو ما يعني تغير في علاقات القوة في السياسة الدولية[7].

يمكن القول أن عناصر القوة السيبرانية ترتكز على وجود نظامٍ متماسك يعظم من القوة المتحصلة من التناغم بين القدرات التكنولوجية، السكان، الاقتصاد، الصناعة والقوة العسكرية، وإرادة الدولة وغيرها من العوامل التي تسهم في دعم إمكانيات الدولة على ممارسة الإكراه أو الإقناع أو ممارسة التأثير السياسي على أعمال الدول الأخرى، بغرض الوصول للأهداف الوطنية من خلال قدرات التحكم والسيطرة على الفضاء السيبراني.

لقد أعطت القوة السيبرانية دفعا رئيسيا في اتجاهين: الأول، تدعيم القوة الناعمة للدول، حيث بات الفضاء الإلكتروني مسرحا لشن هجمات تخريبية ترتبط بنشر المعلومات المضللة، الحرب النفسية، التأثير في توجهات الرأي العام والنشاط السري والاستخباراتي؛ أما الاتجاه الآخر، فيتعلق بتبني الدول لزيادة الإنفاق في سياسات الدفاع الإلكتروني، وحماية شبكاتها الوطنية من خطر التهديدات وبناء مؤسسات وطنية للحماية الإلكترونية[8] .

المحور الثاني: الحروب السيبرانية كمدخل مستحدث للحروب التقليدية

لقد أحدث ظهور "الحرب السيبرانية" بشكلٍ فعلي على الساحة الأمنية والمعلوماتية منذ منتصف العقد الأول من القرن الواحد والعشرين نقلةً نوعية في مفهوم الحروب التقليدية من حيث الوسائل والأهداف وكذا النتائج، حيث أصبح اختراق قواعد البيانات والمعلومات والتلاعب بها أو تدميرها من خلال البرامج المعدة لذلك هو العنصر الاستراتيجي في شن الهجمات في عصر الثورة الرقمية، وذلك بعد أن أضافت الثورة التكنولوجية ساحةً جديدة من الصراع، هي هجمات الفضاء السيبراني التي تؤذن ببداية ما يمكن تسميته "الحروب السيبرانية".

بهذا، كان السبب لامتداد تأثيرات اختراق الثورة التكنولوجية لمختلف مجالات الحياة خلق ساحةٍ جديدة من الحروب غير التقليدية بعيدا عن ساحات (الجو، البر والبحر)، هي ساحة الفضاء السيبراني التي توافرت فيها عدة عوامل حفزت بعض الدول والفاعلين غير الدولتيين على استخدامها كإحدى أدوات الصراع والتنافس والهيمنة والارهاب غير التقليدي، لدرجةٍ قد تنقل ما يشهده العالم من هجمات إلكترونية مختلفة إلى حرب سيبرانية، حيث ساعدت عوامل سهولة الاختراق الالكتروني وانخفاض تكلفة الهجوم والطبيعة غير المتماثلة للهجمات السيبرانية وصعوبة اكتشاف الفاعل وانتفاء أدلة الإدانة المباشرة وغياب أطر قانونية لتحديد التداعيات والعقوبات على استخدام هذا الفضاء الجديد، في شن هجمات سيبرانية مختلفة تتراوح بين هجمات ذات طبيعة استراتيجية تطال البنية الحيوية الأساسية، وبين هجمات ذات أهداف عسكرية وأخرى ذات أهداف سياسية.

بالمحصلة، فقد تغيرت الحروب التقليدية وأصبحت الجيوش العسكرية في كافة أنحاء العالم تهتم بحرب المعلومات ودورها في حروب المستقبل، والتي يتوقع الكثير حدوثها في الفضاء السيبراني، وأصبح هناك مناورات يتم إجراؤها للتدريب على هذا النوع الجديد من الصراع وكيفية مواجهته والاستعداد له، وتستعمل الحرب السيبرانية بشكلٍ عام من أجل خرق السيادة الوطنية لأي دولة والحصول على معلومات استخباراتية وتجنيد العملاء وغيرها، فطبيعة الحرب لم تتغير ولكن سماتها تغيرت مع تطور أدواتها وظهور الطائرات من دون طيار[9] ، وهي حربٌ من دون نار أو دخان أو قصف ولكن لها جانبٌ عنيف من حيث الاختراقات والقرصنة ونشر الفيروسات وغيرها من الأساليب، وبالرغم من فداحة الخسائر، فإن الأسلحة بسيطة لا تتعدى في أغلب الأحوال "الكيلو بايتس[10]"، التي تتمثل في

فيروسات إلكترونية تخترق شبكة الحاسوب الآلي وتنتشر بسرعة بين الأجهزة، وتبدأ عملها في سرية تامة وبكفاءة عالية، وهي في ذلك لا تفرق بين المقاتل والمدني، بين العام والخاص، بين السري والمعلوم[11] ، وبات من الصعب اليوم تخيل صراع عسكري دون أن يكون لهذا الصراع العسكري أبعاد إلكترونية، وأصبحت هذه الأخيرة في صلب اهتمامات الأنظمة الدفاعية لأي صراع يمكن أن يحدث في المستقبل[12] ، مثل الحرب التي تم شنها ما بين جورجيا وروسيا عام 2008، وبين روسيا وإستونيا عام 2007، وقد قامت العديد من الدول على الرغم من التقدم التكنولوجي لها كالولايات المتحدة الأمريكية والصين، ببناء وحدات إلكترونية على شبكات الأنترنيت، على غرار إسرائيل التي قامت بإنشاء الوحدة 8200 للحماية من مئات وآلاف القراصنة المحترفين[13].

عصر المعلومات غير كل شيء، وبذلك تغير شكل الحروب من الحروب التقليدية التي تعتمد على جيوش عسكرية وأسلحة قتالية، إلى حروب سيبرانية بأسلحة معلوماتية في القرن الحادي والعشرين [14]، تتميز هذه الحروب بالسرعة والدقة في تنفيذ العمليات العسكرية وتعتبر من أدوات الحرب الشاملة، وهذه الحروب بعد أن كانت تستهدف أجهزة الأنترنيت والحواسيب أصبحت الآن تستهدف قطاعات وصناعات محددة.

على العموم، تعتمد قواعد الاشتباك في الحرب الإلكترونية على أنظمة الحاسوب والتي من السهل اختراقها وإحداث شلل فيها، باعتبارها أصبحت أدوات لا تستقيم الحياة بدونها في العصر الحديث، ويكون الهدف من وراء الهجوم الإلكتروني الاستيلاء على الأموال أو السرقة والإضرار بالمصلحة العامة والوحدة الوطنية للدولة. كما ظهرت أساليب جديدة للتسلح والدفاع خصوصا بعد ظهور فيروس "ستاكس نت"[15] سنة 2010، كانت نقطة تحول هامة في مجال الأسلحة الإلكترونية لأنه تحول من مجرد اتلاف أو سرقة المعلومات أو تعطيل الأنظمة، إلى مرحلة متطورة وهي إصابة المكون المادي والذي تمثل في المنشآت النووية الإيرانية "المفاعل النووي الإيراني"[16] ، وتعتمد أساليب التسلح الجديدة على المعرفة وتكنولوجيا ووسائل جمع المعلومات ومعدات إلكترونية شديدة التطور، والقوة المادية أصبحت مكلفة ولكن بالمعرفة أصبح يمكن فعل نفس الأشياء ولكن بتكلفة أقل، وفي المستقبل سيكون الصراع على المعرفة يلعب الدور الحاسم في الصراع على السلطة على الصعيد الدولي والمؤسسات، والهجوم الإلكتروني يعتبر بديلا عن السلاح النووي، ولا يحتاج إلى حدود جغرافية معينة ولا يوجد في نظام الأنترنيت حاليا نظام رادار كما في الحروب العسكرية التقليدية لاكتشاف مصدر الهجوم والبيانات على شبكة الأنترنيت، وهي ليست محمية بدرجة عالية من الكفاءة ولذلك يسهل اختراقها والتلاعب بالبيانات والمعلومات المتواجدة عليها، كما تتسم أسلحة الفضاء الإلكتروني أيضا بقدرات غير محدودة على إلحاق الأذى من دون أن تكون معلومة المصدر، وتوافر عنصر المفاجأة، وتكلفة الحرب تكون أقل نسبيا من الدمار الشامل الذي تحدثه، وعبء الدفاع سيكون مهمته أكثر صعوبة من المهاجمين[17] .

الحروب السيبرانية ستبدو أقرب إلى "حروب الأشباح" فهي تنطلق إلى تدمير أهدافها من قواعد غير منصوبة، كما أن في مقدور ترسانتها من الأسلحة غير المرئية أو المعروفة بدقة أن تفلت من خطر الضربات الاستباقية أو الاجهاضية الساعية إلى تدميرها، وهي لا تزال قابعة بعد في مكامنها، كما أنها يمكن أن تلحق الدمار خاصة بقطاعات حساسة للغاية، كقواعد البيانات الحيوية والمعلومات الاستراتيجية المتعلقة بالأمن الوطني للدولة، ما يجعل من القدرة على مواجهتها أمرا بالغ الصعوبة[18].

ومن ضمن أسلحة الفضاء السيبراني نجد الفيروسات والبرمجيات الخبيثة وبرامج التجسس والتي تستخدمها بعض الشركات أحيانا من أمثلة هذه الفيروسات، فيروس ستاكس نت عام 2010، وفيلم وشمعون 2، حشرة

الحب، الفدية (Ronmsoware)، تقوم هذه البرامج بنسخ نفسها على أجهزة المستخدمين من غير معرفتهم وتسعى إلى إحداث خلل أو تدمير في ملفات أو جهاز المستخدم، فضلاً عن برامج التجسس Spy ware، وهي برامج خبيثة تستعمل بشكل سري على أجهزة المستخدمين وتهدف إلى جمع المعلومات الشخصية عن المستخدم.

المحور الثالث: الجريمة السيبرانية كتهديد للأمن السيبراني.. وكقضية للأمن الوطني

يعتبر موضوع الجريمة السيبرانية من المواضيع المستجدة، ومن أهم الدراسات والتقارير حوله أبحاث مكتب تقييم التقنية في الولايات المتحدة الأمريكية، وتقارير معهد ستانفورد الدولي للأبحاث Stanford Research Institute، وكذلك القواعد الإرشادية للحماية الجنائية للبيانات الشخصية التي قدمتها منظمة التعاون الاقتصادي والتنمية OECD[19]، حيث تحيط الجريمة السيبرانية بأي عمل إجرامي يتعامل مع الحواسيب والشبكات الالكترونية، وتتضمن أيضا جرائم تقليدية تتم عبر الأنترنيت: كالاحتيال والتسويق عبر الانترنيت، سرقة الهوية وسرقات حسابات البطاقات الائتمانية...[20].

لا يوجد إجماع على تعريف الجريمة السيبرانية من حيث كيف تعرف أو ما هي الجرائم التي تتضمنها، وكما يقول "فان دير هلست، ونيف" (Van der Hulst & Neve): "هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل من الجريمة... وفي أغلب الأحيان تستخدم مصطلحات الافتراضية والحاسوب والإلكترونية والرقمية وكلها تعكس فجواتٍ مهمة في التعريف[21]. كما أن غياب الدليل حول مدى ودور وطبيعة مجموعات الجريمة المنظمة في الفضاء السيبراني يعرقل تطور لإجراءات المضادة الصحيحة[22].

وعرفها "ليوكفيلدت، وفنسترا وستول" (Leukfeldt, Veenstra & Stol) كمصطلح عام لجميع أشكال الجريمة التي تلعب فيها تكنولوجيا المعلومات والاتصالات دورا أساسيا، وهنا تقع الكثير من الجرائم ضمن هذا التعريف، حيث قدم "ليوكفيلدت" قائمة بـ 28 جريمة بدءاً من قرصنة الأنظمة الرقمية وتثبيت برامج التجسس للاحتيال، باستخدام الخدمات المصرفية عبر الأنترنيت والمطاردة الافتراضية[23].

غالبا ما يتم استخدام مصطلح "الاعتداء السيبراني" عوضا عن مصطلح "الجريمة السيبرانية" للدلالة على اعتداءات موجهة نحو لأجهزة الإلكترونية والأنظمة المعلوماتية سيما منها تلك المتصلة بإدارة الموارد الحيوية والبنية التحتية للبلد المستهدف[24] ، فقد اعتبر المسؤول السابق عن لأمن الوطني لأمريكي "مايكل ماكونال" (McConnell) أن الأنترنيت قد رفعت مستوى لأخطار التي يتعرض لها النظام بشكلٍ غير مسبوق، وذلك في إشارة واضحة إلى التهديدات الجديدة التي تستهدف لأمن الوطني والتي يمكن أن تتخذ أشكالا غير متوقعة وتطال مجالات أساسية وحيوية. كذلك أعلن الرئيسي لأمريكي السابق "باراك أوباما"، أن أمن الفضاء السيبراني يأتي في مقدمة اهتماماته، معتبرا التهديد الآتي من الفضاء السيبراني من أخطر المسائل التي تطرح على المستوى الاقتصادي كما على مستوى لأمن القومي.وقد ترجم هذا عمليا بتعيين مسؤول عن أمن الفضاء السيبراني يكون على اتصال وتنسيق دائم معه، ويكون عضوا في لأمن القومي وفي المجلس الاقتصادي الوطني[25].

فيما عرف قاموس مصطلح لأمن المعلوماتي مصطلح السيبرانية بأنها: "هجوم عبر الفضاء الإلكتروني يهدف إلى السيطرة على مواقع إلكترونية أو بنى محمية إلكترونيا لتعطيلها أو تدميرها أو لإضرار بها"[26]، ويجب التفرقة بين

الجريمة والإرهاب في الفضاء السيبراني، فالجريمة تتعلق بالاستيلاء على ممتلكات الغير أو تخريب الأنظمة، ولكن الإرهاب الإلكتروني هو استخدام شبكات المعلومات والأنترنيت والكمبيوتر من أجل التخويف والإرغام لتحقيق أهداف سياسية، ويمثل الإرهاب السيبراني أحد مظاهر الانصهار بين العنف والتكنولوجيا، ويوظف التقنيات الحديثة في مجالات الاتصال والمعلوماتية التي تعد أحد تجليات العولمة الحديثة[27] .

تعد الجريمة السيبرانية والأمن السيبراني من القضايا التي بالكاد يمكن الفصل بينهما في بيئة متصلة بينيا، ومما يؤكد ذلك قرار الجمعية العامة للأمم المتحدة لعام 2010 بشأن الأمن السيبراني، الذي يتناول الجريمة السيبرانية باعتبارها أحد التحديات الكبرى. حيث باتت العلاقة بين الأمن والتكنولوجيا علاقة متزايدة مع إمكانية تعرض المصالح الاستراتيجية -ذات الطبيعة الإلكترونية- إلى أخطار تهدد بتحول الفضاء السيبراني لوسيطٍ ومصدر لأدوات جديدة للصراع الدولي المتعدد الأطراف ودورها في تغذية التوترات الدولية. ومن جهة أخرى، فرضت تلك التطورات إعادة التفكير في مفهوم الأمن القومي الذي يعنى بحماية قيم المجتمع الأساسية وإبعاد مصادر التهديد عنها، غياب الخوف من خطر تعرض هذه القيم للهجوم، وبذلك يتوافر أمن الفضاء السيبراني حال تحقيق إجراءات الحماية ضد التعرض للأعمال العدائية والاستخدام السيئ لتكنولوجيا الاتصال والمعلومات[28].

فالأمن السيبراني بحسب التعريف المعطى له في التقرير الصادر عن الاتحاد الدولي للاتصالات حول "اتجاهات الاصلاح في الاتصالات للعام 2010-2011"، هو مجموعة من المهمات مثل: تجميع وسائل، وسياسات، واجراءات أمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات وممارسات فضلى، وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين.

تأسيسا عليه، يمكن تعريف الأمن السيبراني انطلاقا من أهدافه بأنه: "النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانيات الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن، بحيث لا تتوقف عجلة الانتاج، وبحيث لا تتحول الأضرار إلى خسائر دائمة". ويعد تعزيز الأمن السيبراني وحماية البنى التحتية الحاسمة للمعلومات عنصرين أساسيين في أمن كل دولة ورفاهها الاقتصادي. وأصبح تعزيز أمان الأنترنيت وحماية مستخدميه جزءا لا يتجزأ من تنمية الخدمات الجديدة ومن السياسات الحكومية، كما يمثل ردع الجريمة السيبرانية عنصرا جوهريا في الأمن السيبراني وفي استراتيجية حماية البنية التحتية الحاسمة للمعلومات[29].

ولم يتم الاقتصار على عملية الاهتمام بالأمن الإلكتروني على البعد التقني وحسب، بل تجاوزه إلى أبعاد أخرى أصبحت ذات علاقة في تفسير القضية مثل الأبعاد الثقافية، الاجتماعية، الاقتصادية والعسكرية وغيرها، والتي دفعت إلى أهمية أن تكون كمرتكزات لتعزيز الأمن الإلكتروني، وهو ما عمل على دعم حقيقة أن الاستخدام غير السلمي للفضاء الإلكتروني يؤثر على كل من الرخاء الاقتصادي والاستقرار الاجتماعي لجميع الدول التي أصبحت تعتمد على البنية التحتية الكونية للمعلومات[30] .

إذا طبيعة الفضاء السيبراني كساحة عالمية عابرة لحدود الدول جعل الأمن السيبراني يمتد من داخل الدولة إلى النظام الدولي ليشكل نوعا من الأمن الجماعي العالمي، خصوصا مع وجود مخاطر تهدد جميع الفاعلين في مجتمع المعلومات العالمي. لذلك، أصبحت هناك مصلحة في الحفاظ على أمن الفضاء الإلكتروني، على أساس أن الأخير صار

جزءا من الأمن العالمي، ودعم ذلك الطبيعة المتغيرة للتفاعلات الإلكترونية خصوصا مع تطور القدرات البشرية على إنتاج تقنيات جديدة، فضلا عن تصاعد مخاطر التهديدات الإلكترونية على البنية الكونية للمعلومات[31].

خاتمة

في العقد الماضي برز الفضاء السيبراني بوصفه بؤرة مخاوف تتعلق بالأمن، فتضاعفت التهديدات التي يواجهها أمن هذا الفضاء، وتعاظمت تكاليف الاستجابات المناسبة لها بسرعة تفوق قدرة الحكومات على التعامل معها، وتصدر أمن الفضاء السيبراني على نحو متزايد أجندات الأمن الوطني للحكومات، فالعصر الذي نعيش فيه بات عصرا رقميا بكل ما للكلمة من معنى، تتحكم فيه المعرفة والمعلومات ووسائل الاتصالات، فمن يملك المعرفة يتحكم في كل شيء. وأصبح الفضاء السيبراني واقعيا، والحروب السيبرانية حقيقة لا مفر منها (حروب الجيل الخامس)، في ظل عدم وجود ملاذات آمنة يمكن الاحتماء بها في مواجهة الهجمات المباغتة والمدمرة للحروب المعلوماتية التي في إمكانها تخطي الروادع كافة. ولعل ما يزيد من مؤشرات الخطر الداهم، هو ما نشهده حاليا من تطور مذهل ومتسارع في مجال تكنولوجيا المعلومات، مقرونا بالتوسع المستمر في كل مكان، وتطبيقها في جميع المجالات المتصلة بأمور الدفاع والتخطيط الاستراتيجي، نظم التسليح، محطات إنتاج الطاقة والمفاعلات النووية، تشغيل المطارات والقواعد الجوية، وسائل النقل ومراكز القيادة والسيطرة والاتصال، مراكز الأبحاث، مؤسسات الصناعة والإنتاج وتقديم الخدمات، المعاهد التعليمية والجامعات، فضلا عن الشبكات الدولية للمعلومات وغيرها، ومع كل هذه الاستخدامات والتقاطعات المتشابكة بين كل تلك المواقع والخطوط، فلا بد أن تزايد مخاطر الانكشاف والتعرض للاختراق بصورة تبعث على الخوف مما يمكن أن يحمله المستقبل من محن.

ولذلك، فالأمن السيبراني هو مسؤولية دولية شاملة، نظرا لارتباط البنى التحتية الخاصة بتقنيات المعلومات والاتصالات، وللاعتماد المتزايد عليها من قبل الدول والأفراد والمؤسسات، ما يفرض اتخاذ تدابير واجراءات، تضمن إدارة فعالة للمخاطر التقنية والسيبرانية انطلاقا من فهم الطبيعة الخاصة لتقنيات المعلومات والاتصالات، سيما الجزء الخاص بتجاوزها للحدود وللمجتمعات والأنظمة، كما لطبيعة البنى التحتية نفسها، بما يعني الطبيعة غير الملموسة للبيانات وإمكانات تناقلها واختراق الأنظمة التي تحويها، ويعني هذا بالدرجة الأولى، فهما مشتركا للإمكانيات التي تقدمها تقنيات المعلومات والاتصالات بجانبيها السلبي والايجابي، ووعيا بضرورة إيجاد أرضية مشتركة لمواجهة تحديات بناء الثقة في مجتمع المعلومات، انطلاقا من تحقيق بيئة آمنة.

قائمة المراجع:

1- باللغة العربية:

الكتب:

1- جبور، منى الأشقر، السيبرانية: هاجس العصر. بيروت، المركز العربي للبحوث القانونية والقضائية، 2017.

2- ياسين، أحمد، الحروب المستقبلية في القرن الحادي والعشرين، (ط1)، أبو ظبي، مركز الأمارات للدراسات والبحوث الاستراتيجية، 2014.

3- ناي، جوزيف، القوة الناعمة: وسائل النجاح في السياسة الدولية، (ترجمة: محمد توفيق البجيرمي، ط1)، الرياض، مكتبة العبيكان للنشر، 2007.

4- خليفة، إيهاب، حروب مواقع التواصل الاجتماعي، القاهرة، العربي للنشر والتوزيع، 2016.

المقالات:

1- باسيت، جون، حرب الفضاء الإلكتروني: التسلح وأساليب الدفاع الجديدة. في: ياسين، أحمد، الحروب المستقبلية في القرن الحادي والعشرين. (ط1)، أبو ظبي، مركز الأمارات للدراسات والبحوث الاستراتيجية، 2014.

2- دريس، نبيل، الجريمة السيبرانية بين المفاهيم والنصوص التشريعية: الجزائر أنموذجا. مجلة القانون والمجتمع، 5 (2)، 2017، 20-40.

https://www.asjp.cerist.dz/en/downArticle/133/5/2/33969

3- لونج، أوستن، الحروب اللامتماثلة في القرن الحادي والعشرين: الإرهاب الدولي والتمرد، وحرب الطائرات من دون طيار. في: ياسين، أحمد، الحروب المستقبلية في القرن الحادي والعشرين، 2014.، (ط1)، أبو ظبي، مركز الأمارات للدراسات والبحوث الاستراتيجية، 2014.

3- مقلد، اسماعيل صبري، مخاطر تسببها الفجوة الرقمية، ثورة المعلومات وحروب المستقبل المحتملة. آفاق المستقبل، العدد 15، جويلية-أوت- سبتمبر، 2012.

4- الفتلاوي، أحمد عبيس نعمة، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر. مجلة المحقق الحلي للعلوم السياسية والقانونية، 8(4)، 2016، 610-687.

5- خليفة، إيهاب، تنامي التهديدات السيبرانية للمؤسسات العسكرية. اتجاهات الأحداث، العدد 22، جويلية- أوت، 2017.

المقالات من الروابط الإلكترونية:

1- البداينة، ذياب موسى، الجرائم الإلكترونية: المفهوم والأسباب. (بحث مقدم)، الملتقى العلمي لجامعة عمان "الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية"، بكلية العلوم الاستراتيجية، عمان، (2-4 سبتمبر2014). على الموقع:

https://repository.nauss.edu.sa/handle/123456789/58478

2- باكير، علي حسين، المجال الخامس...الحروب الإلكترونية في القرن الـ21. مركز الجزيرة للدراسات، (12 جانفي 2011)، على الموقع:

http://studies.aljazeera.net/ar/issues/2010/20117212274346868.html

3- عبد الصادق، عادل، أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي، مجلة السياسة الدولية، س35، 13-63، (14ماي2017)، على الموقع:

http://www.siyassa.org.eg/News/12072.aspx

4- عبد الصادق، عادل، الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي. المركز العربي لأبحاث الفضاء الإلكتروني، دوريات قضايا استراتيجية، (12مارس2017). على الموقع:

http://www.accronline.com/article_detail.aspx?id=28395

5- الصباحي، علي نسرين الشحات، الأبعاد العسكرية للقوة السيبرانية على الأمن القومي للدول دراسة حالة إسرائيل منذ عام 2010. المركز الديمقراطي العربي، (29أفريل2016). على الموقع:

http://democraticac.de/?p=30962

6- الصباحي، نسرين، الحروب السيبرانية وتحديات الأمن العالمي. المركز العربي للبحوث والدراسات، (26 سبتمبر 2017). على الموقع:

http://www.acrseg.org/40594

2- باللغة الأجنبية:

Books:

1-*Jordan, Tim, Cyber power: The culture and politics of cyberspace and the internet. London, Routledge, 1999.*

Articles:

1- *Achkoski, Jugoslav& Dojchinovski, Metodija, Cyber terrorism and cyber crime – threats for cyber security, Conference: Global Security and Challenges of the 21st Century - MIT University – Skopje, June, 2012, from:*

https://shorturl.at/NMwpL

2- *Broadhurst, Roderic & Peter, Grabosky & Mamoun, Alazab & Steve, Chon, Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. International Journal of Cyber Criminology, 8(1), January – June, 2014.*

3- *Kuehl, Daniel T.,. From cyberspace to cyber power: Defining the problem, IN: Cyberpower and National Security, National Defense University Press, Washington, D.C, 2009, From:*
http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf

الهوامش:

[1] نسرين الصباحي، "الحروب السيبرانية وتحديات الأمن العالمي"، المركز العربي للبحوث والدراسات، سبتمبر 2017، على الموقع:
http://www.acrseg.org/40594

1 جوزيف ناي، القوة الناعمة: وسائل النجاح في السياسة الدولية، ترجمة: محمد توفيق البجيرمي، ط1، مكتبة العبيكان للنشر، الرياض، 2007، ص20.

3 أما كلمة "سيبرانية" فهي كلمة بدأ استخدامها عام 1960، والتي أطلقها "مانفريد كلاينس" و"ناثان كلاين" في مقال لهما، ويعني المصطلح: المزج بين الإلكترونيات والإنسان.

[4] Tim Jordan, Cyber Power: The Culture and Politics of Cyberspace and the Internet, London, Routledge, 1999, p.20.

[5] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem", sur:
http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf

[6] Ibid.

[7] نسرين الشحات الصباحي علي، "الأبعاد العسكرية للقوة السيبرانية على الأمن القومي للدول دراسة حالة إسرائيل منذ عام 2010"، المركز الديمقراطي العربي، افريل 2016، على الموقع:

http://democraticac.de/?p=30962

[8] عادل عبد الصادق، "الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي"، المركز العربي لأبحاث الفضاء الإلكتروني، مارس 2017، على الموقع:

http://www.accronline.com/article_detail.aspx?id=28395

[9] لمعلومات أكثر في الموضوع أنظر: أوستن لونج، "الحروب اللاّمتماثلة في القرن الحادي والعشرين: الإرهاب الدولي والتمرد، وحرب الطائرات من دون طيار"، في: أحمد ياسين، الحروب المستقبلية في القرن الحادي والعشرين، ط1، أبو ظبي، مركز الإمارات للدراسات والبحوث الاستراتيجية، 2014، ص ص24-53.

[10] وحدات تخزين المعلومات في الحاسوب هي الوحدات التي تستخدم لحساب مساحات الذاكرة في الحاسوب، وهي تعبر أساساً عن كمية المعلومات المخزنة وتقاس عادة بالبايت ومضاعفاته.

[11] إيهاب خليفة، حروب مواقع التواصل الاجتماعي، القاهرة، العربي للنشر والتوزيع، 2016، ص20.

[12] جون باسيت، "حرب الفضاء الإلكتروني: التسلح وأساليب الدفاع الجديدة"، في: أحمد ياسين، مرجع سابق، ص54.

[13] علي حسين باكير، "المجال الخامس...الحروب الإلكترونية في القرن الـ21"، مركز الجزيرة للدراسات، جانفي 2011،
http://studies.aljazeera.net/ar/issues/2010/20117212274346868.html

[14] اسماعيل صبري مقلد، "مخاطر تسببها "الفجوة الرقمية" ثورة المعلومات وحروب المستقبل المحتملة"، آفاق المستقبل، العدد 15، جويلية-أوت-سبتمبر2012، ص41.

[15] ستاكس نت "***Stuxnet***" هي دودة حاسوب تصيب نظام الويندوز ويُعتقد أنه من صنع الولايات المتحدة الأمريكية وإسرائيل، تمّ اكتشافه أول مرة في جوان 2010 من قبل "فيروس بلوك أدا (***VirusBlockAda***) " ، وهي شركة أمن مقرها في روسيا. أصاب هذا الفيروس ما يقارب 61 ألف جهاز كمبيوتر يعمل ضمن البنى التحتية للبرنامج النووي الإيراني، قصد إلحاق الضرر بها، وعُدّ هذا الهجوم سابقةً في حقل الهجمات السيبرانية.

[16] إيهاب خليفة، "تنامي التهديدات السيبرانية للمؤسسات العسكرية"، اتجاهات الأحداث، العدد 22، جويلية-أوت 2017، ص57.

[17] عادل عبد الصادق، مرجع سابق.

18 اسماعيل صبري مقلد، مرجع سابق، ص42.

19 نبيل دريس، "الجريمة السيبرانية بين المفاهيم والنصوص التشريعية: الجزائر أنموذجا"، مجلة القانون والمجتمع، المجلد 5، العدد 2، 2017، ص.21.

[20] Jugoslav Achkoski, Metodija Dojchinovski, "Cyber Terrorism and Cyber Crime – Threats for Cyber Security", June 2012, sur:
https://shorturl.at/NMwpL

[21] ذياب موسى البداينة، "الجرائم الإلكترونية: المفهوم والاسباب"، من أعمال الملتقى العلمي "الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية"، بكلية العلوم الاستراتيجية، عمان، خلال الفترة من: 2-4 سبتمبر 2014. على الموقع:
https://repository.nauss.edu.sa/handle/123456789/58478

[22] Roderic Broadhurst, Peter Grabosky, Mamoun Alazab & Steve Chon, Organizations and "Cyber crime: An analysis of the nature of groups engaged in cyber crime", International Journal of Cyber Criminology, vol 8, Issue 1, January - June 2014, p.4.

[23] ذياب موسى البداينة، مرجع سابق.

[24] منى الأشقر جبور، السيبرانية: هاجس العصر، بيروت، المركز العربي للبحوث القانونية والقضائية، 2017، ص50.

[25] نفس المرجع، ص28.

[26] أحمد عبيس الفتلاوي نعمة، "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، مجلة المحقق المحلي للعلوم السياسية والقانونية، العدد الرابع، السنة الثامنة، 2016، ص214.

[27] نسرين الصباحي، مرجع سابق.

28 عادل عبد الصادق، مرجع سابق.

[29] "عادل عبد الصادق، أنماط "الحرب السيبرانية" وتداعياتها على الأمن العالمي"، مجلة السياسة الدولية، ماي 7102، على الموقع:
http://www.siyassa.org.eg/News/12072.aspx

30 عادل عبد الصادق، "الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي"، مرجع سابق.

[31] عادل عبد الصادق، "أنماط "الحرب السيبرانية" وتداعياتها على الأمن العالمي"، مرجع سابق.

الجريمة الالكترونية وتهديدها للأمن السيبراني للتراث الأرشيفي الرقمي

Cybercrime and its threat to the cybersecurity of digital archival heritage

رزيقة لموشي / معهد علم المكتبات والتوثيق مخبر التكنولوجيا الجديدة للمعلومات ودورها في التنمية الوطنية
razika.lemouchi@univ-constantine2.dz
عبد الباسط شواو / معهد علم المكتبات والتوثيق مخبر التكنولوجيا الجديدة للمعلومات ودورها في التنمية الوطنية/
abdelbasset.chouaou@univ-constantine2.dz

ملخص:

إن التطور السريع لتكنولوجيا المعلومات بمختلف وسائلها جعل من العالم كتلة موصولة ببعضها البعض من خلال شبكة عنكبوتيه نسجت خيوطها لتصل إلى أقاصي الكرة الأرضية. كما تمكنت من التغلغل في شتى مجالات شؤون الحياة ، وذلك لما لها من أهمية في تسهيل المعاملات في جميع المجالات بأقل مجهود ووقت وتكلفة ممكنين، وفي نفس الوقت حظي التراث الأرشيفي دون غيره من أنواع التراث الإنساني باهتمام الباحثين والمنتجين له منذ الأزل ، سواء بشكله التقليدي الورقي أو الرقمي الحديث وهذا لعلاقته واتصاله بقضايا الأمم باعتباره منبع حضاراتها وتاريخها ولما يحتويه من مختلف الوثائق بمختلف أشكالها ووسائطها التي أنتجتها مؤسساتها بصفة تلقائية أثناء تأديتها نشاطاتها والتي تعنى بحفظها قصد الرجوع إليها عند الحاجة لغرض استعمالاتها الإدارية أو لحفظ حقوقها واستعمالها كأدلة أو حجج، وهذا إدراكا منها بأهمية عملية حفظها والحفاظ عليها من مختلف المخاطر والكوارث المهددة لها .

إلا أنه لا يخفى على أحد منا أن الحفظ في البيئة الورقية بالنسبة للمصادر المطبوعة لا يتطلب أكثر من صيانة الوعاء المادي في حين أن الحفظ الرقمي للكيانات الرقمية بلغ ذروة التعقيد لما يواجهه من تحديات فيما يتعلق بالتخزين وحفظ المحتوى ومشاكل التقادم التكنولوجي والعتاد والبرمجيات ونظم التشغيل، لنصل فيما بعد لأهم عائق ألا وهو عائق الأمن السيبراني لهذه المعلومات وما تتعرض له من تهديدات من قبل عمليات الاختراق والقرصنة وغيرها، وهنا سنقف أمام ما يسمى بالجرائم الالكترونية وماهية الأمن السيبراني لنحاول في هذه الورقة البحثية القاء الضوء على موضوع الامن السيبراني والجريمة الالكترونية للتراث الأرشيفي الرقمي متبعين المنهج الوثائقي من خلال تحليل المراجع المتعلقة بموضوع البحث وإعادة صياغة هذه المعلومات وتوظيفها في دراستنا متوصلين في النهاية لعدد من النتائج أهمها: تهديد الجريمة الالكترونية لأمن التراث الأرشيفي الرقمي، تقارب المصطلحات المتشابهة والمتشابهة المتعلقة بموضع الامن السيبراني والجريمة الالكترونية، لابد من الحرص على السيطرة على الجريمة الالكترونية من خلال صياغة القوانين التشريعية المناسبة

الكلمات المفتاحية: الجريمة الالكترونية، الأمن السيبراني، التراث الأرشيفي الرقمي.

Abstract :

The rapid development of information technology in its various ways; He made the world a mass connected to each other through a spider web whose threads weave to reach the ends of the globe. It has also been able to penetrate into various areas of life affairs, due to its importance in facilitating transactions in all fields with the least possible effort, time and cost. At the same time, archival heritage has received the attention of researchers and producers since time immemorial, regardless of other types of human heritage, whether in its traditional

paper form. Or modern digital, due to its relationship and connection to the issues of nations, as it is the source of their civilizations and history, and because it contains various documents in their various forms and media that their institutions produced automatically during the performance of their activities that are concerned with preserving it for the purpose of referring to it when they need it for the purpose of their administrative uses or to preserve their rights and use it as evidence or arguments. This is because it realizes the importance of preserving it from the various risks and disasters that threaten it.

However, it is no secret to any of us that preservation in the paper environment of printed sources does not require more than the maintenance of the physical container, while digital preservation of digital entities has reached the peak of complexity due to the challenges it faces with regard to storing and preserving content and the problems of technological obsolescence, hardware, software and systems. Employment. Let us then reach the most important obstacle, which is the cybersecurity obstacle to this information and the threats to which it is exposed, such as hacking, piracy, and others. Here we will discuss what is called electronic crime and what is cybersecurity. In this research paper, we will attempt to shed light on the topic of cybersecurity and cybercrime for digital archival heritage, following the documentary approach, by analyzing references related to the research topic and reformulating this information and using it in our study, to ultimately reach results, and a number of these results have been reached. The most important of them are: the threat of cybercrime to the security of digital archival heritage, the convergence of similar and similar terms related to the subject of cybersecurity and cybercrime, and attention must be paid to controlling the crime. Electronically by drafting appropriate legislative laws

Keywords: cybercrime, cybersecurity, digital archival heritage.

مقدمة:

إن كلمة تراث تعني موروث والتوارث يعني نقل هذا الموروث من سلف إلى خلف عبر الزمان والمكان ونقله للأجيال القادمة ، ولكون الأرشيفي مسؤولا عن معالجة وحماية نوع من أنواع هذا التراث ألا وهو التراث الأرشيفي الذي يشكل ذاكرة الأمم وتراثها التاريخي الرسمي لأنه شاهد على تاريخها وعلى مكونات هويتها وذاتها.

ولقد حظي هذا التراث الأرشيفي دون غيره من أنواع التراث باهتمام الباحثين في مختلف ميادين البحث العلمي وهذا لعلاقته واتصاله بقضايا الأمم باعتباره منبع حضاراتها وتاريخها لما يحتويه من مختلف الوثائق بمختلف أشكالها ووسائطها التي أنتجتها مؤسساتها بصفة تلقائية أثناء تأديتها نشاطاتها والتي تعنى بحفظها قصد الرجوع إليها عند الحاجة لغرض استعمالاتها الإدارية أو لحفظ حقوقها واستعمالها كأدلة أو حجج، وهذا إدراكا منها بأهمية عملية حفظها والحفاظ عليها من مختلف المخاطر والكوارث المهددة لها .

إلا أنه لا يخفى على أحد أن الحفظ في البيئة الورقية بالنسبة للمصادر المطبوعة لا يتطلب أكثر من صيانة الوعاء المادي في حين أن الحفظ الرقمي للكيانات الرقمية بلغ ذروة التعقيد لما يواجهه من تحديات فيما يتعلق بالتخزين وحفظ المحتوى ومشاكل التقادم التكنولوجي والعتاد والبرمجيات ونظم التشغيل، لنصل فيما بعد لأهم عائق ألا وهو عائق أمن هذه المعلومات وما تتعرض له من تهديدات من قبل عمليات الاختراق والقرصنة وغيرها ، وهنا سنقف أمام ما يسمى بالجرائم الالكترونية.وهنا يتشكل لدينا التساؤل الرئيسي التالي:

فكيف تهدد هذه الجرائم الالكترونية الأمن السيبراني للوثيقة الأرشيفية الرقمية؟

ومن هذا التساؤل الرئيسي تنبثق عدة تساؤلات فرعية أخرى منها؟

- ما المقصود بالتراث الأرشيفي والتراث الأرشيفي الرقمي؟
- ما المقصود بالجريمة الالكترونية وما علاقتها بأمن معلومات الوثائق ؟
- ما المقصود بالأمن السيبراني للتراث الأرشيفي الرقمي وما علاقته بمختلف المصطلحات الشائعة في هذا المجال؟
- كيف تمس الجريمة الالكترونية بالأمن السيبراني للوثائق الأرشيفية الرقمية وما سبله في القضاء عليها؟

أسباب اختيار الموضوع:

لقد اجتمعت لدينا جملة من الدوافع والأسباب التي جعلتنا نخوض في هذا الموضوع دون موضوع آخر منها أسباب ذاتية وأخرى موضوعية تتلخص فيما يلي:

- **الغموض** : غموض الجريمة الالكترونية وصعوبة تقفي أثر فاعليها.
- **المعاصرة** : معاصرة موضوع الجرائم الالكترونية ومواكبته لتطورات مما يحتم علينا ضرورة اتخاذ موقف والوقوف في وجهها وقفا حازما استناد بالمعايير والقوانين التشريعية.
- **الحساسية**: حساسية قطاع الأرشيف وخصوصية ما تحمله وثائقه الأرشيفية من معلومات تجعل المسؤول عليها مجبرا على تحقيق أمنها السيبراني لا مخيرا.
- **حب الاستكشاف**: وتعلقنا الشخصي بكل ما يتعلق بالحاسوب وموضوعات أمن أنظمة المعلومات.

أهداف الدراسة:

تهدف هذه الدراسة لمعالجة عدة نقاط في موضوع الدراسة أهمها:

- محاولة ضبط وتحديد مفهوم بسيط وواضح لمصطلح التراث الأرشيفي خاصة الرقمي منه.

- ضبط مختلف المصطلحات المتشابكة والمتشابهة والمتعلقة بموضوع الجريمة الالكترونية و أمن المعلومات.
- التعرض إلى مختلف التحديات التي تعيق تحقيق أمن وحماية التراث الأرشيفي في بيئته الرقمية.
- التعرض إلى مختلف الدوافع والأسباب الدافعة لارتكاب الجريمة الالكترونية للتمكن من التوصل لحلول لها فيما بعد.
- التعرف على أهم الصور التي تتجلى بها الجريمة الإلكترونية التي يتعرض لها التراث الأرشيفي الرقمي.
- محاولة اقتراح مجموعة من الآليات والحلول لمواجهة صور الجريمة الالكترونية في مجال الأمن السيبراني للتراث الأرشيفي الرقمي.

ضبط المصطلحات:

- الجريمة الالكترونية: من التعريفات الضيقة للجريمة الالكترونية ما جاء به الفقيه "marwe " حيث يرى هذه الجريمة تتمثل في كل فعل غير مشروع يشترط في ارتكابه الحاسب الآلي من خلال شبكة الإنترنت.[1]
- الجريمة المعلوماتية:ولا تختلف الجريمة الإلكترونية عن الجريمة المعلوماتية في كثير من الأحوال، باستثناء أنها تتم عن طريق جهازين كمبيوتر أو أكثر متصلين فيما بينهم عبر شبكة الإنترنت،، فكلاهما مرتبطان بالكمبيوتر، وإن كانت الثانية تجد مكانها في الفضاء الافتراضي عبر شبكة الانترنت Cyber Space.[2]
- الجريمة السيبرانية: كلها تسميات متعددة تدل على نفس المصطلح مصطلح " الجريمة الالكترونية" الفرق فقط في دور تكنولوجيا المعلومات والاتصالات في هذه الجريمة سواء في مستوى الجريمة أو في طريقة تنفيذها والوسائل المستحدثة في ذلك وهي نشاط إجرامي نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود.[3]
- الارهاب السيبراني: « cyberterrorism » وهو استغلال الإنترنت وتطبيقاتها من طرف جماعة منظمة لتهديد شخصيات معينة أو تدمير بنى تحتية بدوافع سياسية أو عقدية.[4]
- أمن المعلومات: الفرق بين أمن المعلومات والأمن السيبراني أن هذا الأخير يهتم بأمن كل ما هو موجود على السايبر"الفضاء"، بينما أمن المعلومات يهتم بأمن المعلومات الفيزيائية "الورقية" في حين لا يهتم الأمن السيبراني بذلك.[5]
- الأمن السيبراني: وهو المصطلح الأكثر تداولا في وقتنا الحاضر والذي يدل على كل ما هو متعلق بحماية الشبكات والبيانات الرقمية و الأجهزة المتصلة به.[6]

المبحث الأول: مفهوم التراث الأرشيفي التقليدي والتراث الأرشيفي الرقمي:

المطلب الأول: مفهوم التراث الأرشيفي التقليدي:

---

[1] Merwe vander : « computer crimes and other crimes against information technology in south Africa « R.I.D.P 1993 ; p : 554

[2] القاضي ، أنيس جمعان. الفرق بين الجريمة الالكترونية والجريمة المعلوماتية. جريدة عدل ، تم الاطلاع يوم 2023/09/12 متاح على الرابط https://www.aden-tm.net/news/219358

[3] Denning,Dorothye.,"Cyber terrorism",Global Dialogue,Aug 2000, p10

[4] N. E. Emery , The Myth of Cyberterrorism, Publ (Peregrine Technical Solutions), Vol. 4, No. 1 (2005), p. 80

[5] مصطفى، الطيب. الفرق بين أمن المعلومات والأمن السيبراني. متاح على الرابط https://www.oolom.com

[6] إدريس، عطية. مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري. كلية الحقوق والعلوم السياسية-جامعة العربي التبسي - تبسة/ الجزائر. مصداقية. ص 104

1- تعريف التراث:

لغة: لفظ تراث في اللغة العربية مشتق من كلمة ورث وتعني ما يرثه ابن من مال أو حسب ، أو حصول متأخر على نسب مادي أو معنوي ممن سبقه.[7]

اصطلاحا: التراث هو كل ما وصل إلينا من الماضي داخل الحضارة السائدة فهو إذن قضية موروث في نفس الوقت حاضر على عديد من المستويات ، فالتراث هو كل ما تركه السلف للخلف.[8]

2- تعريف الأرشيف:

لغة: عرف في اللاتينية ARCHIVUM ومعناها مصطلح الورقة.[9]

اصطلاحا: هو كل الوثائق الناتجة عن شاط جماعي أو فردي مهما كان حاملها وتاريخها وشكلها أنتجتها أو استلمتها أي هيئة أو منظمة مادية أو معنوية عامة أو خاصة أثناء تأديتها لنشاطاتها المسندة إليها كما يشترط أن تكون منظمة بهدف الرجوع إليها.[10]

- أما التراث الأرشيفي: فنقصد به ذلك الإرث الوثائقي المتوارث والمتداول جيلا بعد جيل أو من شخص إلى شخص أو من هيئة إلى هيئة ...وذلك لاحتوائه قيمة تجعل مالكه أو المسؤول عنه في حاجة دائمة لحمايته من مختلف المخاطر التي تهدد أمنه.

المطلب الثاني: مفهوم التراث الأرشيفي الرقمي:

ولأنه في الوقت الحالي لم يعد هناك فرق بين الوثيقة الرقمية والوثيقة الإلكترونية بعد جدال طويل وبعد أن فصل في الأمر من طرف الأخصائيين من خلال المعيار ISO ،11620فإنه على هذا الأساس يمكن اعتبار الأرشيف الإلكتروني والأرشيف الرقمي مصطلحين يشيران إلى مفهوم واحد .

- فالأرشيف الرقمي هو مجموع الوثائق الأرشيفية المنتجة و المحفوظة من طرف أي هيئة في إطار ممارسة نشاطها، على شكل تسجيلات إلكترونية، وفي صيغة تسمح باستغلالها مباشرة عن طريق أدوات الإعلام الآلي ,ومن جهتها الجمعية الفرنسية للتقييس AFNOR تعرف الأرشيف الرقمي بأنه " حزمة معلومات محفوظة في نظام أرشفة الكتروني مكون من وثيقة أو مجموعة وثائق رقمية.[11]

المبحث الثاني: ماهية الأمن السيبراني للتراث الأرشيفي الرقمي:

المطلب الأول: تعريف الأمن السيبراني للتراث الأرشيفي الرقمي:

- الأمن السيبراني لغة مكون من مصطلحين وهما :

الأمن :وهو نقيض الخوف ، أي بمعنى السلامة والأمن يعني اطمئنان النفس وسكون القلب وزوال الخوف .[12]

السيبراني: مصطلح السيبرانية الآن هو واحد من أكثر المصطلحات ترددا في معجم الأمن الدولي، وكلمة CYBER لفظة يونانية الأصل مشتقة من كلمة KYBERNETES بمعنى الشخص الذي يدير دفة السفينة.

---

[7] ابن منظور، لسان العرب، المجلد 2 ،ط2 ،دار صادر، بيروت، لبنان، 1992م مادة (ورث)، ص 292-202.

[8] حسن محمد سليمان، التراث العربي الإسلامي، ديوان المطبوعات الجامعية، 1988م، ص262.

[9] قبيسي ،محمد .علم التوثيق والتقنية الحديثة ،بيروت :دار الأفاق الجديدة .1991 ،ص.31.

[10] ميلاد، علي سلوى.الأرشيف ماهيته وإدارته. القاهرة :دار الثقافة للنشر والطباعة.1986 .ص.34.

[11] Association de professionnels de l'information et de la documentation en Europe, (5mai 2020). L'archivage électronique. https://www.adbs.fr/ladbs Consulté12 / 09/ 2023

[12] إيفانز غراهام، نويهام جيفري. قاموس بنغوين للعلاقات الدولية. تر: مركز الخليج للأبحاث. الإمارات العربية المتحدة: مركز الخليج للأبحاث 2004

الأمن السيبراني اصطلاحا: هو عبارة عن مجموعة الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة.[13]

- أما تعريف الامن السيبراني للتراث الأرشيفي الرقمي فنقصد به جميع الإجراءات اللازمة لضمان حماية الوثائق والمعلومات الرقمية بجميع إشكالها من مختلف الجرائم: " الهجمات، التخريب، الاختراق، التجسس...

المطلب الثاني: أهداف الأمن السيبراني للتراث الأرشيفي الرقمي:

- تعزيز حماية أنظمة التقنيات التشغيلية للمؤسسات الوثائقية وأجهزتها وبرمجياتها وما تقدمه من خدمات وما تحويه هذه الأجهزة من بيانات.
- التصدي لهجمات وحوادث أمن المعلومات التي تستهدف أجهزة المؤسسات الحكومية ومؤسسات القطاع العام .
- توفير بيئة أمن موثوقة للتعاملات في مجتمع المعلومات.
- صمود البنى التحتية الحساسة للهجمات الالكترونية.
- توفير المتطلبات اللازمة للحد من المخاطر والجرائم الالكترونية التي تستهدف الأرشيفات.
- التخلص من نقاط الضعف التي تستهدف أنظمة الحاسب الآلي والأجهزة باختلافها.
- سد الثغرات ففي أنظمة امن المعلومات ومقاومة البرمجيات الخبيثة.
- الحد من التجسس والتخريب الالكتروني.
- تدريب منتجي الوثائق ومالكيها على اليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية بقصد الضرر بوثائقهم سواء بالإتلاف أو السرقة.

المطلب الثالث: أهم التحديات التي تهدد ألأمن السيبراني التراث الأرشيفي الرقمي:

لقد كان تداول المعلومات والوثائق في البيئة التقليدية مقيدا نوعا ما ، وقد لا يكون للنفاذ إليها الخطر البالغ على المؤسسة ففي نهاية الأمر فالجاني بالكاد يتمكن من الوصول إلى بعض الوثائق والملفات وقد يستغرق ايضا وقتا طويلا في ذلك، في حين بات الأمر يشكل خطورة كبيرة في حالة الأرشيف الرقمي فقد يتمكن من الوصول إلى جل الأرشيف الرقمي سواء بنسخه في وقت قياسي جدا أو إتلافه كله "بالنسبة للوسائط " بالمقابل سيتمكن هذا الجاني من التستر والاختفاء بسهولة ويسر.ومن أهم صور هذه الأخطار الممارسة في حق الأرشيف الرقمي نجد على سبيل المثال لا الحصر:

- أولا الدخول الغير مشروع للوثيقة الرقمية: الدخول أو البقاء غير المشروع داخل نظام المعلوماتية، حيث نصت المادة 394 مكرر " يعاقب بالحبس من ثلاثة 03 أشهر إلى سنة وبغرامة مالية لكل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات. "
- سرقة او تغيير أو حذف أو إتلاف أو تزوير المعلومات التي غالبًا ما تكون لها قيمة مادية ومعنوية لدى المؤسسة.
- النسخ أي استحداث صورة أو أكثر مطابقة للأصل من مصنف أو تسجيل صوتي بأية طريقة أو في أي شكل بما في ذلك التخزين الإلكتروني الدائم أو الوقتي للمصنف أو التسجيل الصوتي" .

[13] جبور منى الأشقر. السيبرانية هاجس العصر. بيروت: جامعة الدول العربية - المركز العربي للبحوث القانونية والقضائية، 2016.

- النشاط الإجرامي الذي يستهدف اختراق البريد إلكتروني والعبث بمحتوياته أو سرقة المعلومات المخزنة في موقع ما؛ والاستفادة منها بما يحمل في طياته بعضاً من انتهاك الخصوصية.
- الجرائم التي تتسبب في تعطيل أجهزة الكمبيوتر وما في حكمها، او تخريبها عبر إرسال الفيروسات أو البرامج التي تحوي انظمة هجومية قد تسبب تلفاً في هذه الأخيرة، مما يؤدي إلى شلل كل الأنشطة.
- الاختراق حتى وان لم يتم التلاعب والمساس بالمحتوى.
- سرقة الملكية الفكرية للملفات وغيرها....[14]
- التصميم أو البحث أو التجميع أو التوفير أو النشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية[15].

المبحث الثاني: تعريف الجريمة الالكترونية وخصائصها وأهم صورها التي يتعرض لها التراث الأرشيفي:

المطلب الأول تعريف الجريمة الالكترونية:

ظهرت تعابير كثيرة حول تعريف الجريمة الإلكترونية ما بين مضيق لمفهومها وموسع كما تعددت المصطلحات المستخدمة للدلالة عليها فالبعض استخدم مصطلح جرائم او إساءة استخدام الحاسبات أو جرائم المعالجة الآلية للبيانات والبعض الآخر أطلق عليها اسم الإجرام المعلوماتي....الخ وفيما يلي تفصيل لمفهوم هذه الجريمة من حيث التعريف، الخصائص وأهم الأسباب والدوافع التي تدفع مرتكبيها الى الحاث الضرر بالأرشيفات الرقمية:

لغة: الجريمة لغة مأخوذة من الجرم وهي الذنب والجناية، جمعها جرائم، وجرم الشيء قطعه و جريمة الرجل على قومه وإليهم: أذنب وجنى جناي.[16]

اصطلاحا: معظم الفقهاء المؤلفين في هذا الباب يردون تعريف الجريمة في الفقه إلى ما قرره الماوردي في الأحكام السلطانية بقوله " الجرائم محظورات شرعية زجر الله عنها بحد او تعزير يعني إذا كانت ممن يتعمد ارتكابها"، أما الإمام أبو زهرة فبعدما ذكر تعريف الماوردي وأيده ساق من بين نصوصه تعريفا اخر للجريمة فقال: "هي المعصية التي يكون فيها عقاب يقرره القضاء.[17]

ومما سبق نستنتج أن الجريمة هي المصطلح المستخدم لوصف جميع الجرائم الجنائية التي ترتكب عبر شبكات الكمبيوتر، ولا سيما على الإنترنت ، وهي كل فعل غير مشروع يكون فيه العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لارتكابه من ناحية، ولملاحقته وتحقيقه من ناحية أخرى.

والمتأمل للتعاريف السابقة يرى أن الجريمة الالكترونية وسعت كل استخدام غير مشروع للحاسب الآلي واستغلاله في قضايا غير جائزة.

المطلب الثاني: خصائص الجريمة الالكترونية:

تتميز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية ببعض السمات والخصائص والتي نوجزها فيما يلي :

- خفاء الجريمة وسرعة ارتكابها: حيث تتصف الجريمة الإلكترونية بالخفاء، أي عدم وجود اثار مادية يمكن متابعتها وهي خطيرة، وصعبة الاكتشاف بسبب اتساع نطاقها المكاني وضخامة البيانات.

---

[14] نائلة فريد محمد قكرة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، ط20051 ،ص 223.

[15] الأمر رقم 15-04 المؤرخ في رمضان 1425 الموافق ل:10 نوفمبر 2004 المعدل و المتمم للأمر رقم 156 -66 الموافق ل 8 يونيو 1966 المتضمن قانون العقوبات

[16] علي بن هادية، بلحسن البليش، الجيلالي بن الحاج يحي. القاموس الجديد للطلاب، الشركة الوطنية، الشركة التونسية الجزائر، تونس، ط1979 ،1، ص251.

[17] ضياء مصطفى عثمان، السرقة الالكترونية، دار النفائس، عمان، ط2011 ، 1، ص32.

- جريمة عابرة للحدود: يمكن القول أن من أهم الخصائص التي تميز الجريمة اللالكترونية هي تخطيها للحدود الجغرافية، ومن اكتسابها طبيعة دولية، أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعدية الحدود، فبعد ظهور شبكات المعلومات لم تعد الحدود مرئية او ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة.
- امتناع المجني عليهم عن التبليغ.
- اعتبارها اقل عنفا في التنفيذ
- سرعة محو الدليل وصعوبة الوصول اليه
- عدم وجود مفهوم مشترك لها وكذلك عدم وجود تعريف قانوني موحد .[18]

المطلب الثالث: أسباب ودوافع الجريمة الالكترونية التي يتعرض لها التراث الأرشيفي الرقمي:

تختلف أسباب الجرائم الالكترونية التي تتعرض لها الأرشيفات الرقمية من مجرم لآخر أهمها:

- قهر السياسيات و الأنظمة والحكومات الالكترونية المسيرة للأرشيفات الالكترونية واثبات التفوق على تطور الوسائل التقنية.
- الرغبة في جمع المعلومات وتعلمها بدون قيود من باب الفضول وحب الاطلاع على كل ما هو سري ومخفي.
- التنافس بين المؤسسات." مثلما قام به بعض القراصنة المتواجدين على الأراضي الروسية باختراق حاسبات حكومية في الولايات المتحدة الأمريكية حيث قاموا باختراق وقرصنة مستندات حساسة من أجهزة الحواسيب العسكرية الأمريكية.
- تهديد الأمن القومي أو العسكري للدول.
- تحقيق ارباح أو مكاسب مالية كبيع المستندات والمعلومات السرية أو غيرها.
- الرغبة في إلحاق الأذى بالأشخاص أو المؤسسات أو مالكي ذلك الأرشيف.
- استعمالها لإثبات حقوق أو نفيها بطرق غير مشروعة.
- الإرهاب الالكتروني وحروب المعلومات لكشف أسرار المؤسسات وطرق التسيير فيها.
- التشهير وتشويه السمعة وتعطيل الأجهزة.
- انتحال الشخصيات والنصب والاحتيال.

المطلب الرابع: توصيات وآليات لمواجهة الجريمة الالكترونية في مجال الحفظ الرقمي للتراث الأرشيفي:

سعت معظم دول العالم الى مكافحة الجريمة الالكترونية خاصة الحساسة منها والتي تتعرض لها أرشيفاتها الرقمية بمختلف الطرق منها فرض عقوبات على مرتكبيها وتفعيل مختلف التقنيات والوسائل للكشف عنهم ونشر التوعية في مجتمعاتها حول خطورة هذه الجرائم وضرورة حفاظهم على مستنداتهم الشخصية ، لذا نقترح مجموعة من التوصيات التي تساهم في الحد من هذه الجرائم الالكترونية التي تتعرض لها المستندات و الأرشيفات الرقمية:

- سن قوانين وتشريعات تتماشى وتطور مستويات الجريمة الالكترونية التي تتعرض لها الأرشيفات الرقمية على المستوى المحلي والإقليمي والعالمي للتعاون على المستوى العالمي للتحكم في هذا الإجرام.
- العمل على استحداث سلطات قضائية تحكم في مثل هذه الجرائم الالكترونية تملك الخبرة والعلم بعالم الحاسبات الآلية و الأجهزة والانترنت وإصدار عقوبات صارمة تردع المجرمين في هذا المجال.

[18] خالد ممدوح، أمن الجريمة الالكترونية، الدار الجامعية،الإسكندرية،ص 45-49

- استعمال تطبيقات تشفير البيانات كنظام البلوك تشين الذي يتم تأمينه باستخدام العديد من التقنيات الرمزية والمفاتيح العمومية مما يجعله صعبا للغاية للمتسللين لتغيير أو تزييف البيانات بل ومن المحال تحقيق ذلك ، بما أن البيانات المخزنة في البلوكتشين موزعة عبر شبكة من الأجهزة لذا فهي تصبح غير قابلة للتلاعب وتوفر مستوى عال من الأمان والثقة.
- التوعية والتثقيف والقيام بدورات تدريبية في مجال أمن المعلومات للتوعية حول خطر الجرائم الالكترونية.
- وضع برمجيات الحماية ضد الفيروسات.
- وضع آليات التحكم للنفاذ الأمن للمعلومات.
- اعتماد التوقيع الالكتروني بواسطة مؤسسات موثوقة ذات سمعة جيدة تمنح للزبون الطالب للتوقيع هوية ومفتاح تشفير خاص به.

خاتمة:

نستخلص من خلال الدراسة أن حفظ الكيانات الرقمية ضروري جدا في المؤسسات الوثائقية، ونجاح عملية الحفظ يكون بوضع استراتيجيات وآليات الحفظ اللازمة من أجل ضمان بقاء المحتوى الرقمي واستخدامه على المدى البعيد سواء من تهديدات الجريمة الالكترونية بصفة خاصة أو من تحديات الحفظ الرقمي بصفة عامة.

قائمة المصادر والمراجع:

باللغة العربية:

القواميس:

- ابن منظور، لسان العرب، المجلد 2 ،ط2 ،دار صادر، بيروت، لبنان، 1992م مادة (ورث)
- إيفانز غراهام، نوينهام جيفري. قاموس بنغوين للعلاقات الدولية. تر: مركز الخليج للأبحاث. الإمارات العربية المتحدة: مركز الخليج للأبحاث 2004
- علي بن هادية، بلحسن البليش، الجيلالي بن الحاج يحي، القاموس الجديد للطلاب، الشركة الوطنية، الشركة التونسية
- الجزائر، تونس، ط1، 1979
- ميلاد، علي سلوى. الأرشيف ماهيته وإدارته. القاهرة :دار الثقافة للنشر والطباعة.1986

النصوص التنظيمية:

- لأمر رقم 15-04 المؤرخ في رمضان 1425 الموافق ل:10 نوفمبر 2004 المعدل و المتمم للأمر رقم 156 -66 الموافق ل 8 يونيو 1966 المتضمن قانون العقوبات

الكتب:

- إدريس، عطية. مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري. كلية الحقوق والعلوم السياسية-جامعة العربي التبسي - تبسة/ الجزائر. مصداقية
- القاضي ، أنيس جمعان. الفرق بين الجريمة الالكترونية والجريمة المعلوماتية. جريدة عدل ، تم الاطلاع يوم 2023/09/12 متاح على الرابط https://www.aden-tm.net/news/219358
- جبور منى الأشقر. السيبرانية هاجس العصر. بيروت: جامعة الدول العربية - المركز العربي للبحوث القانونية والقضائية، 2016.
- حسن محمد سليمان، التراث العربي الإسلامي، ديوان المطبوعات الجامعية، 1988م
- خالد ممدوح، أمن الجريمة الالكترونية، الدار الجامعية،الإسكندرية
- قبيسي ،محمد .علم التوثيق والتقنية الحديثة ،بيروت :دار الأفاق الجديدة .1991
- ضياء مصطفى عثمان، السرقة الالكترونية، دار النفائس، عمان، ط 2011
- مصطفى، الطيب. الفرق بين أمن المعلومات والأمن السيبراني. متاح على الرابط https://www.oolom.com .
- نائلة فريد محمد قكرة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، ط1 ، 2005،

باللغة الأجنبية:

- Merwe vander : « computer crimes and other crimes against information technology in south Africa « R.I.D.P 1993 ; Denning,Dorothye.,"Cyber terrorism",Global Dialogue,Aug 2000,
- N. E. Emery , The Myth of Cyberterrorism, Publ (Peregrine Technical Solutions), Vol. 4, No. 1 (2005)
- Association de professionnels de l'information et de la documentation en

Europe, (5mai 2020). L’archivage électronique. https://www.adbs.fr/ladbs Consulté12 / 09/ 2023

The Legislative Framework of Cyber Security in Algeria

- Dr. DJENDI sarra (*) - University of Algers 3
- Dr. HADJADJ Mourad - University of Boumerdes

Abstract:

Data innovation is the apparatus of our opportunity to stay up with the turn of events and progress happening in the whole world. As it is the most remarkable scholarly device to achieve change in people and the general climate. It has not withstanding adverse consequences that have added to the quick spread of cybercrime as per the idea of the fast improvement of this innovation.

As a matter of fact, what has contributed to its spread is the inefficient of regulative texts to keep pace with this rapid development, which necessitated the need for immediate intervention to confront this type of crime because of its danger to individuals and countries simultaneously to foster mechanisms to coordinate cooperation at the international and national levels.

Keywords: ***Cybercrime, Cyber security, Algeria, legislative power.***

ملخص:

إن ابتكار البيانات هو أداة لمواكبة تطور لأحداث والتقدم الذي يحدث في جميع أنحاء العالم، حيث أنها الوسيلة العلمية الأبرز لإحداث التغيير في الإنسان والمناخ العام، والذي زادت من الانتشار السريع للجرائم الإلكترونية حسب فكرة التحسين السريع لهذا الابتكار.

والحقيقة أن ما ساهم في انتشارها هو عدم كفاءة النصوص التنظيمية في مواكبة هذا التطور السريع، لأمر الذي استدعى ضرورة التدخل الفوري لمواجهة هذا النوع من الجرائم لما له من خطورة على الأفراد والدول في آن واحد، ما أدى الى ابتكار آليات للتعاون على المستويين الدولي والوطني.

الكلمات المفتاحية: الجريمة السيبرانية، لأمن السيبراني، الجزائر، السلطة التشريعية.

Introduction

As society becomes increasingly reliant on digital technologies this has led to the emergence of cyber threats and crimes that have become a great challenge for countries and governments. So, the prevalence of cybercrime is on the rise. Malicious actors are exploiting vulnerabilities in cyberspace to commit a wide range of illegal activities from data breaches to financial fraud. The impact of cybercrime is felt not only by individuals whose personal information is compromised but also by businesses and even governments that suffer significant financial losses and damage to their reputation. This growing threat poses challenges for law enforcement agencies and cybersecurity professionals who must constantly adapt to the evolving tactics of cybercriminals.

Understanding the complex nature of cybercrime is essential for developing effective strategies and mechanisms to prevent and combat these attacks. This research aims is to explore what is cybercrime and the measures that can be implemented to mitigate the risks associated with them.

This study aims to stress the significance and role of the concept of governance to guarantee Cyber Security with every one of its components. Furthermore, since the concept of digital administration is a recent one. Here, the concept of cyber governance should be designed to ensure that users in cyberspace act with a common consciousness. This study is important in terms of ensuring that the strategies and mechanisms determined to comply with national and international standards are accepted andcompatible. Besides the Algerian legislative power implementation to prevent all risks of cybercrime.

Therefore, we will try to shed light on the Algerianlegislative implementation in cyber Security.

Cybercrime is unique in relation to conventional crimes and is portrayed by a sort ofparticularity, Particularly since it is transnational and it needs exceptional control, So the question that emerges is:What are the mechanisms of the Algerian legislative authority to confront and combatCybercrime? And are these mechanisms sufficient to protect its sovereignty?

In order to address this issue, we will address this topic in two sections

The first discusses the cybercrime and its impact and the second discusses the most essential laws of Algerian legislation authority to confront and combat cybercrime.

First part:

1-Definition of Cybercrime

It is any unlawful behavior related to the automated processing or transmission of data. Cybercrime encompasses a wide range of illicit activities carried out in the digital realm, with various types posing significant threats to individuals, organizations and governments. One prevalent form of cybercrime is hacking where unauthorized users gain access to computer systems or networks to steal information or disrupt operations. Phishing is another common type involving the use of deceptive emails or websites to trick individuals into divulging personal information or clicking on malicious links. Additionally, identity theft remains a persistent threat that criminals stealing personal information to commit fraud or other illegal activities.There are also cybercrimes in which the computer is the tool or means of committing fraud, identity theft, credit card and asset theft, forgery, embezzlement, intellectual property theft, extortion, deviant behavior and sexual exploitation[1]. These various types of cybercrime highlight the diverse and evolving nature of online threats requiring constant vigilance and robust cybersecurity measures to combat effectively.

Impact of Cybercrime

The impact of cybercrime extends far beyond financial losses as it also poses serious threats to national security, individual privacy and overall societal trust in digital systems. The interconnected nature of cyberspace means that a single cyber-attack can have widespread and devastating consequences on critical infrastructure, government operations and even global stability. Furthermore, the rise of ransom ware attacks targeting hospitals, schools and other public institutions not only jeopardizes the safety of vulnerable populations but also highlights the urgent need for improved cybersecurity measures at all levels of society.As cybercriminals continue to evolve their tactics and exploit vulnerabilities in digital networks, They are highly skilled in using and exploiting modern technological means in order to harm others and the damage they causes may exceed the borders of his country's territory and this is often the case[2]. The impact of cybercrime will only intensify, requiring coordinated efforts from governments, businesses and individuals to effectively combat this growing threat.

[1] -Mona Al-Ashkar Jabbour, Cybersecurityis the Obsession of the Age, Arab Center for Legal and JudicialResearch, League of Arab States, Cairo, 2012 .
[2] -Mohamed Abdel-Moneim Abdel-Khaliq, Internet Crimes, 2nd edition, Arab Renaissance House, 2015, p. 97.

Second part:

Today, new legal mechanisms and practices are developed to protect the rights and sovereignty of individuals, companies, institutions and states against cyber threats and cyber terrorism. However, the changes in legal norms and legislation as well as the strategies implemented in parallel with the information technology and the produced malware and techniques are not in harmony with one other. Furthermore, the relevant stakeholders are not able to make decisions on an effective way of communication and governance. Thus, the resources can be wasted in the fight against cyber threats and the dominant actors are increasingly under the hegemony. This situation causes an inability to take necessary measures effectively and efficiently

Threats in cyberspace are increasing day by day; they harm institutions, individuals and organizations. Since the concept of management is not sufficient alone to take measures to prevent these damages, the concept of governance, which includes all stakeholders in management processes, should be put into use. For this reason, the problem of putting the concept of cyber governance into a standard framework has emerged.

In 2009 the Unified Countries embraced a convention as a feature of the Unified Countries Show on the battle against worldwide coordinated cybercrime; it has thusly settled the significance of passing an improvement regulation on cybercrime at the nation level to adapt to aggressors and safeguard Web user's security. On the global level, this has extended assurance of social and human respect and security in data dissemination. Algeria has likewise answered the environment improvement and message of the fast improvement of ICT with an ethical quality regulation in 2012 on this offense and related issues in the revision of Regulation No 04/21 of February 25.[3] The law meant to explore the legitimate text of this undertaking as individuals were allowed to live in computerized opportunity, so it was vital that a regulation was laid out to safeguard this freedom in a protected climate and to stay up with fast improvements in worldwide data innovation.

Network protection is concern for public and confidential entities responsible for directing computerized legitimate relations and Web correspondence and countries are experiencing a scope of online crimes for example, fraud, money laundering or drug trafficking .They are also soft crimes and some have called them white-collar crimes[4] .

---

[3]-Savaş, S. &Karataş, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance.published in2022ncbi.nlm.nih.gov

[4] -Naela Adel Mohammed Qoura, Economic Computer Crimes, A Theoretical and AppliedStudy, Halabi Law Publishing, Beirut, 2014, p. 61

These offenses disregard the freedoms of citizens,digital democracy and respect for human rights. While requiring legal explanation, cybercrime was not customized into the Penal Code that gives the rising flood of misdeeds from the organization. Brought about dangers that affected the security ofindividuals and the economy in Algeria and different nations.

By examining the various types of cybercrimes, their impact on society and the tools and techniques used by cybercriminals, it is evident that this issue requires immediate attention from policymakers, law enforcement agencies, and cybersecurity professionals.

Algeria National Cyber Security Strategyfor instance as the result of the country's assurance to take specific steps forward. The CS policy of Algeria addresses the steps taken against cyber incidents. Algeria has taken actions to promote relevant national governance and develop policy frameworks.

With reference to the International Convention on cybercrime held in Budapest in 2001 the Algerian legislator derived his definition from the International Convention.Algeria has enacted laws on cybercrime trough the Penal Code: Algeria has amended the Penal Code by law N 15-04 on 10 November 2004, which was ratified on December2006under the heading of prejudice to automated data processing systems within the articles from article N06 which dealt with the types of cybercrimes and their punishment.

The content of Law N04-09 on 16 August 2009: It is the law containing special rules for the prevention of crimes. It contains 6 chapters dealing with the definition of crime, electronic communications monitoring, procedural rules, the National Authority for the Prevention of Information Crimes and jurisdiction, and this in article N 19.

In order to counter cybercrime Algeria has developed several devices and bodies, including:

1-National Commission for the Prevention of crimes related to information and Communication Technology: Among its tasks are:

- To coordinate the Prevention of crimes related to information technologies and Contact and combat it.

- The help of the judicial authority to the judicial police in their Judicial investigations concerning the media and communication technologies crimes .

- Exchange information with their counterparts abroad in order to collect all the useful data In identifying the perpetrators of crimes related to media and communication technologies And determine their places.

2- Specialized criminal judicial bodies:Its jurisdiction is territorial.

3-National Institute of Criminal Evidence and criminology: on26 jun2004.

It is a public institution with the administrative character enjoys moral character and financial independence, and is placed under the guardianship of the minister of National Defense. The Institute consists of 11 departments specialized in various fields, including the Department of automated and electronic information, which is responsible for processing,analyzing and presenting all digital evidence helps justice and provides technical assistance to investigators in the inspections.

The second mechanism is:

2-The National Data Protection Authority. The protection of natural persons in the processing of personal data.

The content of Law N 18-07 on the protection of natural persons in the field of personal data in 2016.It shows the basic principles for the protection of personal data. Defines the rights of person concerned with the personal data being processes, defines the obligation of the person responsible for such treatment, protection of natural persons in the field of personal data.

The establishment of the National Authority for the protection of personal data in 2016 is one of the most important mechanisms to reduce the chaos that has prevailed in the exploitation of personal data of natural persons and a basic guarantee for the protection of personal data and guarantee that privacy in not compromised. According to Article N46 / It is not permissible to violate the inviolability of a citizen's private life, Confidentiality of correspondence and communication in all its forms is guaranteed.

The determination of the rights of the person concerned with data of a personal nature includes:

-The right to information: According to article N07-18 ,Advance notification of the identity of the person responsible for the processing and its purpose, and any additional useful information. That contains a bunch of rights:

-The right of access: According to article N07-18 , Right to inquire about the processed data and ensure that it is processed or not.

-The right to correction: According to article N07-18 , The right to correct, update, erase or close personal data when it turns out that these data are incomplete or incorrect. The request for correction is addressed to the processing officer by making the necessary corrections for free.

Prevent direct exploration According to article N07-18 direct exploration is prohibited by any means or by the use of Technology, using the data of a natural person in any form, without the consent of the concerned.

Transfer of data to a foreign country: It is prohibited to send or transfer data of a personal nature to a foreign country that may prejudice public security or vital interests of the state. We find that the Algerian legislator prevents the person responsible for processing the transfer of personal data to a foreign International from obtaining a license from the National Authority according to article N07/18.

Penal provisions:

In a group of Articles, including Article 54, which criminalizes disrespect for humanity and private life .Public freedoms lead to present from two years(02)to five (05)years and a fine from 200,000 to 500,000 DH.The same penalty is provided for in Article 56 in the case of the processing of personal data without obtaining permission or license in the case of sensitive data. In addition to those who made false statements.

In Article N59 unfair use of data of a personal nature was incriminated, other than imprisonment from 1 to 3 years and a fine from 100.00 DHto 300.000.

In order to guarantee the integrity of the right to personal data, the Algerian legislator found mechanisms by issuing a law N 07-18 on the protection of persons in the field of personal data.

Third law is:

The High Conservatism of digitization:

The matter concerns the presidential decree 314-23containing the establishment of the high governorate for digital and defining its tasks, it is an organization that has financial independence and ensuring the follow-up and implementation of the National digital strategy. Also the matter concerns the leadership of strategic intersectoral projects as well as the examination of sectoral programs in the field of digitization with an assessment of how to implement them in accordance with the decree, which also determined the organization and functioning of this body governed by a presidential decree.

Among its tasks is

The Coordination of ministries and the promotion of digital sovereignty

We point out that unlike the previous bodies, this commission is the first to be launched as a prelude to the issuance of the digitization law in 2024 mending the laws of cyber breach of peace and parochial intruding.[5]

Fostering a tailored and comprehensive cyber security strategy for Algeria is essential to build its capacity to manage the potential difficulties originating from the adverse consequences of computerized change, including cybercrime. Lawful systems focusing on cybercrime. Legal frameworks targeting cybercrime in this region need to be implemented and enforced in a practically achievable manner and it requires a strategy based on a definition of the considered threat, the character of that threat and its context in order to ensure comprehensive action. At regional level, there is a clear gap .A lack of skilled professionals, the slow evolution of legal frameworks .Consequently, the absence of governing prerequisites for the digital age constitute significant obstacles to be handled in the context of a comprehensive cybersecurity strategy including law and politics. Seriously, legal frameworks should be updated and the rule-making strategies should also include solutions not defined by law proxies only.

Conclusion

Despite the amendments made by Algeria in field of combating cybercrime, these remain insufficient comparing with the development of criminal informatics professionalism.Crimes do not leave a physical trace at the crime scene and their perpetrator have ability to damage; deform or wasting evidence in a short period of time.

Governments must invest in robust cybersecurity measures, enhance international cooperation to combat cybercrime and educate the public on how to protect themselves online. Additionally, businesses must prioritize cyber security and implement best practices to safeguard their data and infrastructure. As technology continues to advance, the threat of cybercrime will only grow, highlighting the need for ongoing research and innovation to stay one step ahead of cybercriminals. The findings of this study serve as a call to action for all stakeholders to collaborate and take proactive measures to mitigate the risks posed by cybercrime in the digital age.

Not only governments or institutions have roles but also individuals and the private sector. Since each of these components has different purposes for using cyberspace, their definitions of roles in cyber governance are also different. International agreements, strategies, laws, metrics and regulations must all be

[5] -FarahNaz, siran Karim, AsmaHoucine and MuhammadAbubakr Naeem. Fintech Growth during COVID-19 in MENA Region: Current Challenges and Future prospects. Published in 2022ncbi.nlm.nih.gov

taken into account when establishing cyber governance standards as they bring together such a diverse set of institutions and individuals with different roles.

In addition, all of these arrangements must be performed in harmony. The regulations made should also cover data protection, security infrastructure, encryption, content protection, and all similar security sub-units that make up cyberspace. Since the scopes are so large, the rules determined should be kept wide while making the regulations. Therefore, informatics laws alone will not be enough. It is necessary to use the rules of international law for CS to make decisions about problems and solutions.

Cybercrime is characterized by the fact that it is transnational so,the procedures for following up and preserving evidence constitute a great challenge.Besides to the various problems such as :

-Not discovering the victim until a period of time after the commission of the criminal act[6].

-Problems in commercializing electronic data.

- Problems with the formation of the internet censorship network.

-Increase in crimes committed through social media.

-The technical, application and legislative infrastructure of the e- signature is insufficient.

-The inability to prevent offenders from using computer systems for crimes such as money laundering and financing of terrorism through technology and the internet.

Recommendations:

1-The need to review national legislation related to cybercrime,emphasize on intellectual property law, commercial law and civil law.

2-Giving priority to the scientific field instead of the military field by The Establishment of a Research Center of information crime to study its development and measures in order to reduce it.

[6] -Nahla Abdel Qader Al-Momeni, Cybercrime, Dar Al-Thaqafa for Publishing and Distribution, Amman Jordan, 2016.

3- Also, developing the technological field to reduce dependence on foreign companies.

3-Creating hard-to-penetrate electronic systems.

4-Algeria should intensify efforts by entering into international agreements in order to combat informatization and benefit from the experiences of other countries in this field to improve the mechanisms to combat all kinds of cybercrimes.

References:

-Mona Al-Ashkar Jabbour, Cybersecurityis the Obsession of the Age, Arab Center for Legal and JudicialResearch, League of Arab States, Cairo, 2012 .

-Mohamed Abdel-Moneim Abdel-Khaliq, Internet Crimes, 2nd edition, Arab Renaissance House, 2015, p. 97.

-Savaş, S. &Karataş, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance.published in2022ncbi.nlm.nih.gov

-Naela Adel Mohammed Qoura, Economic Computer Crimes, A Theoretical and AppliedStudy, Halabi Law Publishing, Beirut, 2014, p. 61

-FarahNaz, siran Karim, AsmaHoucine and MuhammadAbubakr Naeem. Fintech Growth during COVID-19 in MENA Region: Current Challenges and Future prospects. Published in 2022ncbi.nlm.nih.gov

-Nahla Abdel Qader Al-Momeni, Cybercrime, Dar Al-Thaqafa for Publishing and Distribution, Amman Jordan, 2016.

(الأمن السيبراني في الجزائر: التحديات والرهانات)
Algeria's cybersecurity: challenges and bets

دريادي حميدة (*) جامعة أمحمد بوقرة بومرداس h.deriadi@univ-boumedes.dz

ملخص:
أصبحت قضية الأمن المعلوماتي أو السيبراني من التحديات الهامة على الصعيد الوطني والإقليمي والعالمي، لهذا جاءت هذه الورقة البحثية لدراسة جهود ومساعي الجزائر من أجل حماية أمنها السيبراني، خاصة في ظل التوجه الرقمي الذي التزمت به الجزائر مؤخرا في كل القطاعات الحيوية للوطن، فعلى الرغم من تبني الجزائر لاستراتيجية وطنية تعتمد على آليات قانونية ومؤسساتية هامة بالإضافة إلى التعاون مع المظمات الدولية والدول، إلا أنها بحاجة إلى آليات تعزز فعاليتها على أرض الواقع.

الكلمات المفتاحية: الأمن السيبراني، التحديات، الاستراتيجية الوطنية، الجزائر

Abstract:
The issue of information or cybersecurity has become an important challenge for national, regional and global fishing, that is why this paper examined algeria's efforts and endeavours to protect its cybersecurity, especially given algeria's recent digital trend in all vital sectors of the country, despite algeria's adoption of a national strategy, it relis on general legal and institutional mechanisms as well as cooperation with international organizations and states, however, they need mechanisms that enhance their effectiveness.

KeyWords: ***cybersecurity, challenges, national strategy, algeria***

مقدمة:

في ظل التطور المتسارع لتكنولوجيا المعلومات، أصبح الأمن السيبراني من أكثر المسائل أهمية في العصر الحديث، حيث يشكل التحدي الذي يواجهه عالم الاتصالات الحديثة وتكنولوجيا المعلومات. إذ لازم العصر الرقمي مخاطر وتهديدات سيبرانية تتباين أثارها وانعكاساتها على أمن معلومات الدول، لتطال عبرها مختلف القطاعات الاقتصادية والعسكرية والسياسية، مما يؤدي إلى انهيار أمنها الوطني واختراقه وبالتالي تنهار الدولة تماما.

الجزائر كغيرها من دول العالم ليست بمنأى عن التهديدات السيبرانية، مما استدعى تبني استرتيجية وطنية وفعالة للتصدي ومواجهة هذه التهديدات، والتي تقوم على مختلف الأليات القانونية والمؤسساتية بالإضافة إلى التعاون الدولي، لهذا جاءت هذه الورقة البحثية لدراسة جهود الدولة الجزائرية في وضع أسس لمواجهة الهجمات السيبرانية وحماية الفضاء السيبراني الخاص بها. انطلاقا من الإشكالية الآتية:

كيف يمكن تعزيز الاستراتجية الوطنية في مجال الأمن السيبراني في الجزائر؟

والإجابة على الإشكالية ستتناول الدراسة محورين أساسيين هما:

المحور الأول: مفهوم الأمن السيبراني وأبعاده.

المحور الثاني: الاستراتيجية الوطنية للأمن السيبراني في الجزائر وسبل تعزيزها.

المحور الأول: مفهوم الأمن السيبراني وأبعاده.

يعتبر الأمن السيبراني من المفاهيم التي أصبحت تتداول في المحيط الأكاديمي والعلمي، وذلك نظرا لأبعاده الهامة وأهميته في الحد من الاختراقات والجرائم الالكترونية بشتى الطرق والأساليب الموضوعية والإجرائية.

أولا- مفهوم الأمن السيبراني:

هناك عدة تعاريف يمكن أن تعطى للأمن السيبراني انطلاقا من التعريف الاصطلاحي والتعريف الفقهي والقانوني، وهو ما سنتطرق له في هذا المحور.

1/- لغة: كلمة "أمن" في اللغة العربية تعني الحماية والسلامة والخلو من الخوف أو الضرر، أما "سيبراني" فهي مأخوذة من كلمة "cyber" بالإنجليزية والتي تعود في أصولها إلى كلمة "cybernétique" بالفرنسية التي تعني "فن التوجيه والتحكم". تتعلق الكلمة بتقنيات الحوسبة والشبكات الإلكترونيةأو الواقع الافتراضي، وتعني (فضاء الأنترنت)، وهي كلمة مشتقة من الكلمة اليونانية kybernetes والتي وردت بداية في مؤلفات الخيال العلمي، وكان يقصد بها قيادة ربان السفينة[1].

2/- اصطلاحا: استعملت كلمة السيبرانية لأول مرة من قبل عالم الرياضيات الأمريكي نوربرت ويز norbert winer وهو أستاذ الرياضيات في معهد ماساشوستش التقني MIT التي أعطاها مفهومها الاصطلاحي الحديث و كان ذلك عام **1948**، ومن أجل وصف نظام التغذية الرجعية feedback الاستفادة من مخرجات الأنظمة out puts في ضبط مدخلاتها in puts وفي التحكم فيها واستقرار أدائها[2].

3/- التعريف الفقهي:

هو عبارة عن مجموعة من التقنيات والسياسات والممارسات التي تهدف إلى حماية الشبكات والأجهزة والبرامج والبيانات من الهجمات أو الضرر و لمنع الاستخدام من قبل غير المصرح له على شبكات الكمبيوتر، أو سوء الاستغلال و استعادة المعلومات الإلكترونية التي تحتويها بهدف ضمان و استمرارية عمل نظم المعلومات، و تأمين حماية و سرية و خصوصية البيانات الخاصة بفواعل الفضاء السيبراني، و عليه فهو المجال المتعلق بالإجراءات و مقاييس و معايير

الحماية المفروض اتخاذها، أو الالتزام بها لمواجهة التهديدات و منع التعديات، أو للحد من آثارها في أقصى و سوء الأحوال[3].

أما فيما يخص تعريف المشرع الجزائري للأمن السيبراني فالمادة العاشرة من القانون رقم **18-04** فقد عرفته بأنه: مجموع الأدوات والسياسات ومفاهيم الأمن والآليات الأمنية والمبادئ التوجيهية وطرق تسيير المخاطر والأعمال والتكوين والممارسات الجيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الإلكترونية ضد أي حدث من شأنه المساس بتوفير وسلامة البيانات المخزنة أو المعالجة أو المرسلة[4].

كما أن قانون العقوبات في تعديله الأخير للفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر **66-156**[5]أضاف قسم سابع مكرر عنوانه:" المساس بأنظمة المعالجة الآلية للمعطيات"، بالقانون **04-15** حيث نص على بعض الجرائم وما يقابلها من عقوبات للحد من ارتكابها[6].

وقد عرف الجريمة السيبرانية في المادة **2** من الفصل الأول من القانون **09-04** المؤرخ في **05** أوت **2009** المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها تحت عنوان مصطلحات بأنها:" جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية[7].

التعريف القانوني للأمن السيبراني يتضمن العناصر التالية:

- سرية المعلومات :(Confidentiality) ضمان أن المعلومات لا تكون متاحة أو مكشوفة للأشخاص أو الجهات غير المصرح لهم بالاطلاع عليها.
- سلامة المعلومات :(Integrity) ضمان دقة واكتمال المعلومات وحمايتها من التعديل أو التدمير غير المصرح به.
- توفر المعلومات :(Availability) ضمان أن المعلومات والخدمات تكون متاحة عند الحاجة إليها.
- المساءلة :(Accountability) ضمان تسجيل وتوثيق جميع الأنشطة والأحداث التي تحدث في النظام للمراجعة والتحقق.
-الإذعان :(Compliance) الالتزام بالقوانين واللوائح المحلية والدولية المتعلقة بالأمن السيبراني.

ثانيا-وسائل تهديد الأمن السيبراني:

وهي عبارة عن تلك التقنيات المستخدمة في الهجمات السيبرانية و التي لها عدة أشكال يمكن توضيحها فيما يلي:

1- التجسس المعلوماتي:وهي أشهر الوسائل و أسلحة الحرب السيبرانية، وتتخذ عدة أشكال منها مايتم عبر التجسس والتصنت على المعلومات الصادرة من أجهزة الحواسيب الصادرة عن الأقمار الصناعية و الهواتف المحمولة[8].

2- الاختراق الالكتروني:وهي عبارة عن انشاء نظام أو برنامج الكتروني يهدف إلى استغلال معلومات الخصم وتدميرها، وقد تكون على المستوى الفردي أو المؤسساتي أو على مستوى الدول[9].

3-زرع الفيروسات التقنية في البيئات المعلوماتية:وتشمل الفيروسات الأسلحة الأساسية في الحرب، حيث تؤدي إلى تعطيل عمل الشبكات الالكترونية و الخوادم الرئيسية أو تؤدي إلى استخدامها لإرسال مختلف المعلومات من الأماكن التي تغزوها، وهي عبارة عن برامج الكترونية مدمرة يمكن نشرها عبر الرسائل الإلكترونية أو نقل الملفات الإلكترونية، أو تحميلها على أداة لحفظ البيانات[10].

4- القرصنة الالكترونية: من أضخم و أكثر الأسلحة ووسائل التهديد عبر الفضاء الرقمي، حيث تقوم هذه الآلية على تجنيد العديد من الأشخاص المؤهلين و القادرين على التعامل مع الحاسوب بخبرة و دراية عالية جدا، تمكنهم من

اقتحام مختلف وسائل الاتصال و النظام التكنولوجي من حواسيب و هواتف و موجات و آليات ضوئية و غيرها، و يطلق عليهم اسم(الهاكرز)[11]

5- الرسائل الصامتة: تصل رسائل على الهاتف المحمول ولا يشعر حامل الهاتف بوصولها تقوم بالتحديد الدقيق لتواجد الشخص. وذلك عبر استخدام معادلة تقوم باحتساب قوة إشارة الموجات المنبعثة من الجهاز المحمول تبعا لأقرب ثلاث مراكز مستقبلة لهذه الموجات[12].

6- شبكات التواصل لاجتماعي: وهي عبارة عن تركيبات اجتماعية تقنية ذات محتوى رقمي تقوم بربط الحلقات لاجتماعية ببعضها البعض كالعمل و الدين وغيرها[13].

7-الأقمار الصناعية: هدفها السيطرة على أكبر قدر ممكن من المعلومات، عبر التقاط ملايين الصور للهدف وارسالها للقاعدة المعلوماتية الموجودة على لأرض، كم تستخدم في التشويش على المحطات الفضائية[14].

8-الحقيبة الكهروستاتيكية: وهي عبارة عن أجهزة صناعية على شكل حقائب صغيرة، تقوم بتوليد نبضات كهرومغناطيسية فائقة القدرة، يمكن من خلالها تدمير الوحدات الالكترونية في أية إدارة أو محطة إرسال[15].

9-قنابل التعتيم الميكروويفية: تصوب لمولدات الطاقة، كالمزودات الكهربائية، والرادارات، ومحطات التزويد بخدمات الأنترنت، ومراكز الاتصالات، والشبكات السلكية واللاسلكية، ومحطات البث الخلوي تعمل على قطع كافة مصادر الطاقة والمعلومات في الكيان المستهدف مما يؤدي إلى فصله عن العالم الخارجي.

10-لأسلحة النانو تكنولوجية: يتم بتصميم أجهزة تقنية في غاية الدقة والصغر، تسلط هذه التكنولوجيا العسكرية على لأجزاء المادية للأجهزة الحاسوبية والتقنية بحيث تنتشر داخلها لتتسلل إلى أنظمة التشغيل[16].

11-الخداع الإلكتروني: له عدة وسائل أهمها التقليد الصوتي، التشويش الإلكتروني، التضليل المعلوماتي، الخداع ونشر الشائعات، انتحال الشخصيات افتراضيا، لابتزاز الالكتروني[17].

12- الطائرات الإلكترونية(دون طيار): أحدثت مثل هذه لأسلحة الجامعة بين مبادئ العمل الحربي و المعلوماتي صيحات إنسانية و حقوقية عديدة في العالم كونها تحوي العديد من التأثيرات السلبية على جسم الانسان، ناتجة عن الموجات التي تطلقها و لأصوات المزعجة الصادرة عنها[18].

لأمن السيبراني هو مجال مهم يركز على حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية. هذه الهجمات يمكن أن تهدف إلى الوصول إلى المعلومات الحساسة، تعطيل العمليات الطبيعية أو لاستيلاء على البيانات الخاصة. مع تزايد لاعتماد على التكنولوجيا والإنترنت في جميع جوانب الحياة اليومية والعمل، يصبح لأمن السيبراني أكثر أهمية لحماية كل من المؤسسات والأفراد.

ثالثا- أبعاد لأمن السيبراني:

لأمن السيبراني لا يقتصر على الجوانب التقنية فقط، بل يتداخل مع أبعاد سياسية، اقتصادية، اجتماعية، وثقافية متعددة. فيما يلي استعراض لكل من هذه الأبعاد:

1/ البعد الاقتصادي:

البعد الاقتصادي للأمن السيبراني يشمل تأثير الهجمات السيبرانية وتهديدات لأمن الرقمي على النشاط الاقتصادي ولأعمال التجارية. هذا التأثير يمكن أن يكون كبيرا ومتعدد الجوانب. إليك بعض الجوانب الرئيسية:

1.1.تكاليف لاختراقات والهجمات :الهجمات السيبرانية يمكن أن تتسبب في خسائر مالية هائلة للشركات والحكومات، سواء من خلال سرقة البيانات، التشويش على الخدمات، أو تعطيل الأنظمة. •تشير تقارير إلى أن

التكاليف العالمية الناجمة عن جرائم الإنترنت ستصل إلى 10.5 تريليون دولار بحلول عام 2025. ووفقًا لتقرير من "فوربس"، فإن 60٪ من الشركات الصغيرة التي تعرضت لهجوم سيبراني تختفي في غضون ستة أشهر تقريبًا[19]

2.1.تكاليف الاستعادة والتعافي :بعد وقوع هجمات سيبرانية، تحتاج المؤسسات إلى استعادة البيانات، إصلاح الأنظمة المتضررة، وتحسين الأمن. هذا يتطلب استثمارات مالية ضخمة وقد يؤثر على العائد على الاستثمار.

3.1.تأثير على سمعة الشركة :الهجمات السيبرانية قد تتسبب في تلطيخ سمعة الشركة أو المؤسسة المتضررة، مما يؤثر على علاقتها مع العملاء والشركاء التجاريين.

4.1.فقدان البيانات والملكية الفكرية :اختراقات السيبرانية يمكن أن تؤدي إلى سرقة البيانات الحساسة والملكية الفكرية، مما يتسبب في خسائر مالية وفقدان تنافسية للشركة.

5.1.تأثير على النمو الاقتصادي العام :الهجمات السيبرانية يمكن أن تؤثر على النمو الاقتصادي العام، خاصة إذا كانت موجهة نحو البنية التحتية الحيوية مثل الطاقة أو النقل.

6.1.تكلفة الحماية :الإنفاق على التقنيات الأمنية وتوظيف الخبراء الأمنيين.

لحماية الاقتصاد من هذه التهديدات، تحتاج الشركات والحكومات إلى الاستثمار في حلول الأمن السيبراني وتعزيز الوعي بأمان المعلومات وتبني ممارسات أمنية قوية. من خلال تنمية الاقتصاد الرقمي وذلك ب:

- تشجيع الابتكار :الاستثمار في البنية التحتية السيبرانية يمكن أن يدعم الابتكار والنمو الاقتصادي.
- الأمان كميزة تنافسية :الشركات التي تضمن أمان بياناتها يمكن أن تستخدم ذلك كميزة تنافسية لجذب العملاء.

2- البعد الاجتماعي:

تسمح طبيعة الإنترنت المفتوحة عبر المدونات والشبكات الاجتماعية بشكل خاص لكل مواطن بأن يعبر عن تطلعاته السياسية وطموحاته الاجتماعية، حيث تمثل مشاركة جميع شرائح المجتمع فرصة للاطلاع على الأفكار والمعلومات المختلفة وبما تكونه من حاجة لدى المجتمع في الحفاظ على استقرار الفضاء السيبراني والمجتمع الذي يرتكز إليه .لكن في المقابل يعرض أخلاقيات المجتمع للخطر، نظراً لصعوبة مراقبة محتوى الإنترنت، كما يعرض الهويات لعمليات اختراق خارجي ما قد يتسبب في تهديد السلم الاجتماعي للدولة، وعليه فلابد من العمل على توعية المواطن بهذه المخاطر لتحقيق الأمن السيبراني في بعده الاجتماعي والتي يمتد إلى عدة جوانب:

- ثقافة الأمان الرقمي :يتعين تعزيز ثقافة الأمان الرقمي في المجتمع من خلال توعية الأفراد بمخاطر الهجمات السيبرانية والممارسات الأمنية عبر الإنترنت.

- حماية الخصوصية الشخصية :يعرض الانتهاك السيبراني خصوصية الأفراد وبياناتهم الشخصية، مما يستدعي تشديد الحماية القانونية والتقنية لهذه البيانات.

- الثقة في التكنولوجيا والتواصل الاجتماعي :يؤثر القلق من الهجمات السيبرانية على ثقة الأفراد في استخدام التكنولوجيا ووسائل التواصل الاجتماعي، مما يمكن أن يؤدي إلى تراجع في التفاعل الرقمي والابتعاد عن المنصات الرقمية.

- التعليم والتواصل الرقمي :تؤثر الهجمات السيبرانية على التعليم الرقمي والتواصل الاجتماعي عبر الإنترنت، مما يتطلب تعزيز الأمان السيبراني في البيئات التعليمية والتواصل الرقمي.

- التضامن الرقمي والمساواة في الوصول :يجب ضمان التضامن الرقمي والوصول المتساوي للتكنولوجيا والإنترنت، مع الحفاظ على سلامة المستخدمين وحماية خصوصيتهم.

من خلال تعزيز الوعي بأمان المعلومات وتحسين الحماية السيبرانية، يمكننا الحفاظ على الأمان الرقمي للمجتمع وضمان استفادته الآمنة من التكنولوجيا الرقمية[20] وذلك من خلال:

- حماية خصوصية الأفراد: وذلك من خلال:

- حماية البيانات الشخصية :تأمين المعلومات الشخصية للمستخدمين من الاختراقات والاستغلال.
- التوعية المجتمعية زيادة الوعي حول أهمية الأمن السيبراني وكيفية حماية المعلومات الشخصية.

- تعزيز الثقة في التكنولوجيا:

- الثقة في الأنظمة الرقمية :تعزيز الثقة في استخدام الخدمات الرقمية مثل البنوك الإلكترونية والتجارة الإلكترونية.
- الشفافية والمساءلة :الشركات والحكومات تحتاج إلى أن تكون شفافة بشأن كيفية حماية بيانات المستخدمين والتعامل مع الانتهاكات.

3- البعد السياسي:

تعد التسريبات للملفات السرية والاختراقات الخطيرة لأنظمة معلومات الدول، من الأسباب التي تؤدي إلى أزمات سياسية ودبلوماسية، كما أن الفضاء الرقمي السيبراني أصبح من الآليات المستعملة حديثا في الحملات الانتخابية.

وبالتالي، يجب أن تعمل الدول على حماية أمنها من التهديدات والمخاطر التي تنطوي عليها شبكة الإنترنت.

- حماية البنية التحتية الحيوية :مثل أنظمة الطاقة، المياه، والاتصالات من الهجمات السيبرانية التي يمكن أن تؤثر على سيادة الدولة.
- التشريعات والسياسات :تطوير سياسات وتشريعات وطنية لتنظيم الأمن السيبراني وحماية المواطنين من الهجمات.
- التعاون الدولي:

- المعاهدات والاتفاقيات :المشاركة في المعاهدات الدولية والتعاون مع الدول الأخرى لمواجهة التهديدات السيبرانية المشتركة.
- المشاركة في منظمات الأمن السيبراني الدولية :مثل فرق الاستجابة للطوارئ الحاسوبية (CERTs) والتعاون في التحقيقات الجنائية السيبرانية.

4- البعد القانوني:

يشير البعد القانوني للأمن السيبراني إلى المجموعة الشاملة من القوانين والتشريعات، التي تنظم وتحمي المعلومات والبيانات الرقمية من التهديدات والاختراقات الإلكترونية. إذ يهدف البعد القانوني إلى توفير إطار قانوني يحمي الأفراد والمؤسسات من الاعتداءات السيبرانية، ويعاقب المتسببين في الهجمات الإلكترونية. وتختلف التشريعات القانونية المتعلقة بالأمن السيبراني من بلد إلى آخر، وتتضمن قوانين حماية البيانات، وقوانين مكافحة الجرائم السيبرانية، وقوانين تنظيم الاتصالات الإلكترونية، وقوانين حقوق الملكية الفكرية، وقوانين الخصوصية الإلكترونية، وقوانين الاعتراف القانوني للتوقيع الإلكتروني، وغيرها من التشريعات ذات الصلة[21].

تعزز التشريعات القانونية للأمن السيبراني من خلال تحديد الأنشطة غير المشروعة على الإنترنت، وتحديد الجرائم السيبرانية وعقوباتها. كما تحمي حقوق الأفراد والشركات فيما يتعلق بالخصوصية والملكية الفكرية والمعلومات الحساسة. و من خلال إنشاء إطار قانوني قوي للأمن السيبراني، يتم تعزيز الأمن الاجتماعي وتوفير بيئة

آمنة للمستخدمين الذين يتعاملون مع البيانات الرقمية، وضمان حماية خصوصياتهم وبياناتهم ذات الطابع الشخصي.

4- البعد الثقافي: وذلك من خلال

- التفاوت الثقافي: المتمثل في
  - الفروق الثقافية في التعامل مع البيانات :الاختلافات الثقافية يمكن أن تؤثر على كيفية تعامل المجتمعات مع البيانات الشخصية والأمن السيبراني.
  - التأثير الثقافي على السياسات :السياسات الأمنية يمكن أن تتأثر بالعوامل الثقافية والتقاليد المحلية.
- التعليم والتدريب: وذلك من خلال
  - تضمين الأمن السيبراني في المناهج التعليمية :لتعزيز الثقافة الأمنية بين الأجيال القادمة.
  - تدريب الموظفين :على الممارسات الأمنية الجيدة وكيفية التصدي للتهديدات السيبرانية.

5- البعد العسكري: لقد تجلت البدايات الأولى للإنترنت في بيئة عسكرية بشكل مضاعف، وذلك لكي تنتقل في سياق لاحق إلى الأوساط الأكاديمية والعلمية وأبحاث تستخدم القدرات العسكرية وتتمثل الميزة النسبية للأمن السيبراني في بعده العسكري عن طرق قدرة القوة السيبرانية على ربط الوحدات العسكرية ببعضها البعض عبر العالم الافتراضي، وحماية البنية التحتية السيبرانية للقوات المسلحة والأنظمة العسكرية، من الهجمات السيبرانية وتأمين المعلومات الحساسة والمهمة للأمن القومي.

يتطلب البعد العسكري للأمن السيبراني وجود استراتيجيات وقدرات للكشف المبكر عن التهديدات السيبرانية المحتملة، ومنعها والاستعداد للرد عليها بل واتخاذ اجراءات رادعة. يتضمن ذلك تطوير تقنيات وادوات للكشف عن الاختراقات والاعتداءات السيبرانية والاستجابة لها بسرعة وفعالية[22].

المحور الثاني- استراتيجية الجزائر للأمن السيبراني وسبل تعزيزها:

تسعى الجزائر من خلال هذه الاستراتيجية إلى بناء نظام وطني قوي للأمن السيبراني يمكنه التصدي للتهديدات.في السنوات الأخيرة، شهدت الجزائر زيادة ملحوظة في حالات الجريمة السيبرانية، وهذا يعود جزئياً إلى الانتشار الواسع لشبكة الإنترنت ونقص المراقبة والمتابعة الدورية لاستخدامها. ولكن، حرصاً من المشرع الجزائري على مكافحة هذه الجريمة وحماية البيئة الرقمية، قام باتخاذ خطوات جادة لتطوير الإجراءات القانونية والتقنية المناسبة لمواجهة هذا التحدي المتنامي،تمثل هذه الخطوات استحداث آليات إجرائية متقدمة تتناسب مع طبيعة الجرائم السيبرانية، والتي تتميز بتطورها المستمر وتعقيداتها المتزايدة .وقد تم تكثيف الجهود لتطوير القوانين واللوائح ذات الصلة، بالإضافة إلى تعزيز التعاون الدولي في مجال مكافحة الجريمة السيبرانية، تاتي هذه الجهود ضمن استراتيجية شاملة لتحقيق الأمن السيبراني.

أولا- الجوانب الرئيسية لاستراتيجية الجزائر في مجال الأمن السيبراني:

في الجزائر، اتخذت الحكومة مجموعة من الآليات المؤسساتية لتعزيز الأمن السيبراني وحماية البنية التحتية الرقمية والمعلوماتية. هذه الآليات تتضمن تنظيمات، تشريعات، مؤسسات، وبرامج متعددة تهدف إلى مواجهة التحديات السيبرانية المتزايدة. وفيما يلي بعض الآليات الرئيسية للأمن السيبراني في الجزائر:

1- التشريعات واللوائح : الجزائر تعمل على تحديث وتعزيز التشريعات الخاصة بالأمن السيبراني لضمان توفير إطار قانوني يحمي البنى التحتية الحرجة ويحارب الجرائم الإلكترونية. هذا يشمل تحديث القوانين لتشمل الجرائم السيبرانية الحديثة وتوفير آليات قانونية للتعاون الدولي في هذا المجال.

الجزائر قد تبنت عدة تشريعات لتعزيز الأمن السيبراني وحماية البيانات. هذه القوانين تتضمن أحكامًا لمكافحة الجرائم الإلكترونية، حماية البيانات الشخصية، وتامين البنى التحتية الحيوية. من أبرز هذه النصوص:

- القانون رقم 04-09 المتعلق بقمع الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال:

هذا القانون يحدد الإطار القانوني لمكافحة الجرائم الإلكترونية في الجزائر ويشمل تعديلات على قانون العقوبات لتضمين جرائم جديدة مثل الوصول غير المشروع إلى أنظمة الكمبيوتر، الاعتداءات السيبرانية ضد البنى التحتية الحيوية، وجرائم الاحتيال الإلكتروني. لا سيما التعديل الذي أتى به القانون رقم **16-02** المؤرخ في **19** يونيو لسنة **2016** المعدل لقانون العقوبات، فقد أضاف المادة(**87** مكرر **11**) التي تعاقب كل جزائري أو أجنبي يرتكب أفعالا إرهابية، أو يديرها أو يعدلها أو يشارك فيها أو يدرب عليها أو يتلقى التدريب عليها، باستخدام تكنولوجيات الإعلام و الاتصال(المادة **3** الفقرة **2**)، و أضاف التعديل المذكور المادة **87** مكرر **12** التي تنص على أن القانون يعاقب كل من يستخدم تكنولوجيات الإعلام و الاتصال من أجل دعم تلك الأعمال أو تنظيمها أو نشر أفكارها بطريقة مباشرة أو غير مباشرة، أو تجنيد الأشخاص لصالح جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها الإرهاب.

- قانون حماية البيانات الشخصية:

قانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ودخل حيز التنفيذ يوم **10** أوت **2023**، يوفر هذا القانون إطارًا لحماية البيانات الشخصية للأفراد وينظم كيفية جمع البيانات ومعالجتها وتخزينها من قبل الكيانات العامة والخاصة. كما يتطلب من الشركات والمنظمات اتخاذ تدابير فعالة لحماية البيانات الشخصية من الوصول غير المصرح به والاستغلال.

- يحدد هذا القانون المبادئ العامة لحماية البيانات الشخصية في الجزائر، ويتضمن احكاماً تتعلق بجمع ومعالجة وتخزين البيانات الشخصية.

- ينص على حقوق الأفراد فيما يخص بياناتهم الشخصية مثل الحق في الوصول، التصحيح، الاعتراض، والحذف.

يعتمد قانون حماية المعطيات الشخصية على مجموعة من المبادئ الأساسية التي تتوافق مع المعايير الدولية لحماية البيانات الشخصية، ومنها:

- الشفافية: يجب على الجهات التي تجمع البيانات الشخصية إبلاغ الأفراد بكيفية استخدام بياناتهم والأغراض من جمعها. ويتطلب القانون الحصول على موافقة صريحة من الأفراد قبل جمع بياناتهم الشخصية.

- الأمان: يجب على الجهات المسؤولة عن معالجة البيانات الشخصية اتخاذ التدابير الأمنية المناسبة لحماية البيانات من الوصول غير المصرح به، التلاعب، أو التسريب. ويشمل ذلك استخدام تقنيات التشفير، والأنظمة الأمنية المتقدمة.

- الحد الأدنى من البيانات: يحدد القانون أن جمع ومعالجة البيانات الشخصية يجب أن يقتصر على البيانات الضرورية فقط للأغراض المحددة.

- الحقوق الفردية: يمنح القانون الأفراد حقوقاً محددة فيما يتعلق ببياناتهم الشخصية، مثل الحق في الوصول إلى بياناتهم، تصحيحها، الاعتراض على معالجتها، وحذفها.

هذا و يحدد القانون مجموعة من المسؤوليات للجهات التي تقوم بجمع ومعالجة البيانات الشخصية، وتشمل:

- تعيين مسؤول حماية البيانات:(DPO) يتطلب القانون من بعض الجهات تعيين مسؤول حماية البيانات لضمان الامتثال للمتطلبات القانونية.
- إجراء تقييمات تأثير حماية البيانات: يجب على الجهات إجراء تقييمات دورية لتحديد وفهم تأثير أنشطة معالجة البيانات على حماية الخصوصية.
- الإبلاغ عن خروقات البيانات: في حالة حدوث خروقات للبيانات الشخصية، يتعين على الجهات المعنية الإبلاغ عنها إلى الهيئة الوطنية لحماية البيانات الشخصية والأفراد المتضررين في اسرع وقت ممكن.

يتضمن القانون عقوبات صارمة للمخالفين، والتي قد تشمل:

- الغرامات المالية: فرض غرامات مالية على الجهات التي تنتهك القواعد المتعلقة بحماية البيانات الشخصية.
- التحقيقات والعقوبات: قانون حماية البيانات الشخصية في الجزائر يشكل خطوة مهمة نحو تعزيز حقوق الخصوصية للأفراد وحماية بياناتهم الشخصية من الانتهاكات. من خلال الالتزام بمبادئ الشفافية، الأمان، والحقوق الفردية، يسعى القانون إلى خلق بيئة رقمية آمنة وموثوقة للأفراد والمؤسسات على حد سواء.

2- الجهود المؤسسية:

إلى جانب القوانين، الجزائر أيضاً أنشأت هيئات رقابية الجزائر تعنى بالرقابة والتنظيم في مجال الأمن السيبراني لضمان التزام الهيئات العامة والخاصة بالمعايير المعمول بها.

1.2/ السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي[23] (CNDP) هي *"سلطة إدارية مستقلة"، تتمتع بالشخصية المعنوية والاستقلالية المالية والإدارية، تم* إنشاؤها بموجب القانون **18-07** المتعلق بحماية المعطيات الشخصية كجهة تنظيمية وإشرافية لضمان الامتثال للقوانين المتعلقة بحماية البيانات الشخصية. *تتكون من 16 عضو، من بينهم رئيسها، معينون بالمرسوم الرئاسي رقم 18.7.22 المؤرخ في 18 ماي 2022*، تتولى الهيئة دور مراقبة وتنفيذ القانون، والتحقيق في الشكاوى المتعلقة بانتهاك الخصوصية، وفرض العقوبات على المخالفين. *تسهر على احترام الكرامة الإنسانية والحق في الخصوصية خلال عملية معالجة المعطيات ذات الطابع الشخصي، و* تتمتع بسلطة إجراء التحقيقات وفرض العقوبات المناسبة على الجهات المخالفة.[24]

2.2/المجلس الوطني لأمن الأنظمة المعلوماتية[25]: تابع لوزارة الدفاع الوطني يكلف بإعداد الاستراتيجية المذكورة والموافقة عليها وتوجيهها ووكالة تضطلع بتنسيق تنفيذ هذه الاستراتيجية.

و من بين المهام التي يتولاها المجلس الذي يرأسه وزير الدفاع الوطني أو ممثله، "الموافقة على اتفاقات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في مجال أمن الأنظمة المعلوماتية و سياسة التصديق الالكتروني و تصنيف الأنظمة المعلوماتية", فضلا عن "إبدائه رأيا متطابقا في أي مشروع نص تشريعي أو تنظيمي" ذي صلة بهذا الموضوع.

3.2/الوكالة الوطنية لأمن الأنظمة المعلوماتية[26]: التي تعتبر "مؤسسة عمومية ذات طابع إداري, تتمتع بالشخصية المعنوية و الاستقلالية المادية", فتتكفل بجملة من المهام, على غرار "اقتراح كيفيات اعتماد مزودي خدمات التدقيق في مجال أمن هذا النوع من الأنظمة"و "السهر على جمع و تحليل و تقييم المعطيات المتصلة بمجال أمن الأنظمة المعلوماتية لاستخلاص المعلومات الملائمة التي تسمح بتأمين منشآت المؤسسات الوطنية".

هذا بالإضافة إلى الجهاز العملياتي المتمثل في المراكز والوحدات التي أنشئت لغرض مواجهة الجريمة الإلكترونية، ومدى استعداداتها لادائها من ذلك والمتمثلة أساسا في:

4.2/ مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني:

أنشئ في سنة 2008 ويهدف إلى تأمين منظومة المعلومات لخدمة الأمن العمومي، حيث يعكف على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها، وذلك من أجل تأمين الأنظمة المعلوماتية والحفاظ عليها، لا سيما تلك المستعملة في المؤسسات الرسمية و البنوك[27].

5.2/المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:

يعتبر مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة لوزير الدفاع الوطني مكلفة بمهام متعددة كإجراء الخبرات و الفحوص في إطار التحريات الأولية و التحقيقات القضائية، و المساهمة في تنظيم دورات الاتقان و التكوين ما بعد التدرج في تخصص العلوم الجنائية، يحتوي على العديد من الأقسام و المصالح المختصة من أهمها: مصلحة البصمات، مصلحة البيئة، اما فيما يخص مجال الأمن السيبراني هناك مصلحة الإعلام الآلي يتم على مستواها رصد ومراقبة عمليات الإختراق و القرصنة المعلوماتية، وكذا اكتشاف المعلومات المسروقة و تفكيك البرامج المعلوماتية[28].

6.2/ المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:

كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة الإلكترونية وعلى مستوى المديرية العامة للأمن الوطني والتي أنشأت سنة 2011 ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بقرار من المدير العام للأمن الوطني وأضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015[29].

7.2/الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها:

تشكلت بمقتضى المرسوم الرئاسي رقم15-261[30] وهي سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت إشراف ومراقبة لجنة مديرية يترأسها وزير العدل وتضم أساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

كلفت الهيئة باقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما وتنشيط وتنسيق عمليات الوقاية منها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة هذه الجرائم، من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية، وضمان المراقبة الوقائية للاتصالات الالكترونية، قصد الكشف عن الجرائم المتعلقة بالاعمال الإرهابية والتخريبية والمساس بأمن الدولة[31].

هذه القوانين والمؤسسات تشكل الأساس الذي تستند إليه الجزائر في بناء وتعزيز استراتيجيتها الوطنية للأمن السيبراني، وتحسين القدرة على الاستجابة للتحديات السيبرانية المعاصرة.

3- التعاون الدولي:

التعاون الدولي يعد جزءًا أساسيًا من جهود الجزائر لتعزيز الأمن السيبراني ومواجهة التهديدات الإلكترونية. تتعاون الجزائر مع العديد من المنظمات والدول لتعزيز القدرات الوطنية في هذا المجال من خلال تبادل المعلومات، الخبرات، والتنسيق المشترك. وفيما يلي أبرز جوانب التعاون الدولي للجزائر في مجال الأمن السيبراني:

1.3/ التعاون مع المنظمات الدولية: من خلال

- الإنتربول :الجزائر تتعاون مع الإنتربول في مكافحة الجرائم السيبرانية، من خلال تبادل المعلومات والمشاركة في العمليات الدولية التي تستهدف الشبكات لإجرامية السيبرانية.
- الاتحاد الدولي للاتصالات :(ITU) المشاركة في مبادرات وبرامج الاتحاد التي تهدف إلى تعزيز لأمن السيبراني على المستوى العالمي وتطوير السياسات والمعايير الدولية.
- منظمة لأمن والتعاون في اوروبا :(OSCE) التعاون في مجال السياسات لأمنية السيبرانية وتبادل الخبرات وأفضل الممارسات.

2.3/التعاون الإقليمي: ويتمثل في

- الاتحاد الأفريقي :الجزائر تشارك في مبادرات الاتحاد الأفريقي لتعزيز لأمن السيبراني في القارة، مثل مبادرة "الاتحاد الأفريقي للامن السيبراني" التي تهدف إلى تطوير سياسات وإجراءات أمنية موحدة للدول لأعضاء.
- الشراكة مع دول الجوار :إقامة علاقات تعاون ثنائية مع الدول المجاورة في مجال لأمن السيبراني، بما في ذلك تبادل المعلومات والتنسيق في مجال مكافحة الجرائم الإلكترونية.

3.3/الاتفاقيات الثنائية: وتتمثل في

- اتفاقيات مع دول متقدمة في مجال لأمن السيبراني :توقيع اتفاقيات تعاون مع دول مثل فرنسا، ألمانيا، والولايات المتحدة لتبادل الخبرات والتقنيات لأمنية المتقدمة.
- التدريب والتطوير :تنظيم برامج تدريبية مشتركة وتبادل الخبراء لتعزيز القدرات الفنية والبشرية في مجال لأمن السيبراني.

4.3/المشاركة في المنتديات والمؤتمرات الدولية: وتتمثل في

- المؤتمرات العالمية للأمن السيبراني :مشاركة الجزائر في المؤتمرات الدولية مثل "منتدى لأمن السيبراني العالمي" و"مؤتمر لأمن السيبراني للأمم المتحدة"، حيث يتم مناقشة التحديات والسياسات والتقنيات الحديثة في مجال لأمن السيبراني.
- منتديات التعاون الإقليمي :المشاركة في المنتديات الإقليمية لتعزيز التعاون بين دول المنطقة وتبادل المعلومات حول التهديدات السيبرانية وأساليب التصدي لها.

5.3/ البرامج والمبادرات الدولية: وتتمثل في

- مبادرات لأمن السيبراني للأمم المتحدة :الجزائر تشارك في برامج لأمم المتحدة التي تهدف إلى تعزيز لأمن السيبراني على مستوى الدول النامية، بما في ذلك تقديم الدعم الفني وتطوير القدرات.
- الشراكات مع القطاع الخاص العالمي :التعاون مع شركات التكنولوجيا العالمية لتطوير حلول أمنية مبتكرة وتبادل المعرفة حول أحدث التهديدات وأساليب الحماية.

التعاون الدولي يعد عنصرًا حيويًا في استراتيجية الجزائر لتعزيز لأمن السيبراني. من خلال التعاون مع المنظمات الدولية، إقامة اتفاقيات ثنائية، والمشاركة في المنتديات والمؤتمرات العالمية، تسعى الجزائر إلى تعزيز قدراتها في مواجهة التهديدات السيبرانية وضمان حماية بنيتها التحتية الرقمية والمعلوماتية.

4- تطوير القدرات التقنية والبشرية:

لاستثمار في تدريب وتطوير المهارات اللازمة للمتخصصين في لأمن السيبراني هو جزء حيوي من لاستراتيجية. الجزائر تسعى إلى إنشاء مراكز تدريب متخصصة وبرامج أكاديمية تركز على لأمن السيبراني لتعزيز قدراتها البشرية. ويتجلى هذا من خلال القرار الرئاسي بخصوص انشاء مدرسة وطنية عليا للامن السيبراني .

5-تعزيز البنية التحتية التكنولوجية:

تحديث وتأمين البنية التحتية التكنولوجية الوطنية، بما في ذلك الشبكات الحكومية والمؤسساتية، لضمان حمايتها من الهجمات السيبرانية. هذا يتضمن تطبيق معايير أمنية عالية واستخدام تقنيات متقدمة للكشف عن التهديدات والتصدي لها.

6-تعزيز الوعي والتثقيف السيبراني:

توعية المواطنين والمؤسسات حول مخاطر الأمن السيبراني وكيفية الحماية منها. تشمل هذه الجهود تنظيم حملات توعوية وورش عمل وتدريبات على أفضل الممارسات في الأمن السيبراني.

ثانيا- متطلبات تفعيل الاستراتيجية الوطنية في مجال الأمن السيبراني:

الأمن السيبراني هو قضية متعددة الأبعاد تتطلب نهجا شاملاً يتضمن التعاون بين الحكومات، الشركات، والمجتمع المدني. تعزيز هذه الأبعاد المختلفة يساعد في بناء بيئة رقمية أكثر أمانًا واستدامة.

تحقيق الأمن السيبراني في الجزائر يتطلب اتباع نهج شامل ومتعدد الأبعاد، يشمل السياسات التشريعية، المؤسسات، التكنولوجيا، التعليم، والتعاون الدولي. فيما يلي مجموعة من المتطلبات التي يمكن أن تساعد في تعزيز الأمن السيبراني في الجزائر:

1- تطوير وتحديث التشريعات والسياسات: من خلال تطوير قوانين متقدمة لمكافحة الجرائم السيبرانية وحماية البيانات الشخصية، بما يتماشى مع المعايير الدولية، وإنشاء إطار تنظيمي يحدد المسؤوليات والالتزامات لجميع الأطراف المعنية، بما في ذلك الحكومة، القطاع الخاص، والمواطنين.

2- تعزيز القدرات المؤسساتية: من خلال دعم المؤسسات القائمة مثل الوكالة الوطنية للأمن السيبراني ومركز الاستجابة لطوارئ الحاسوب (CERT) من خلال توفير الموارد البشرية والتقنية اللازمة، وتطوير مراكز أبحاث متخصصة في الأمن السيبراني لدعم الابتكار والتطوير في هذا المجال.

3-الاستثمار في التكنولوجيا والبنية التحتية: من خلال استخدام أحدث التقنيات الأمنية لحماية البنية التحتية الرقمية، بما في ذلك تقنيات التشفير، جدران الحماية، وأنظمة الكشف عن التسلل، وبناء بنية تحتية تقنية قوية وموثوقة تضمن استمرارية الخدمة وحماية البيانات.

4- التعليم والتوعية: من خلال تضمين مواد الأمن السيبراني في المناهج التعليمية على جميع المستويات لزيادة الوعي بين الأجيال القادمة، تنظيم حملات توعية تستهدف المواطنين لزيادة الوعي بأهمية الأمن السيبراني وكيفية حماية البيانات الشخصية.

5- تطوير القدرات البشرية: من خلال توفير برامج تدريب متخصصة للموظفين الحكوميين والعاملين في القطاع الخاص لتعزيز مهاراتهم في مجال الأمن السيبراني، وتشجيع الحصول على شهادات مهنية معترف بها دوليًا في مجال الأمن السيبراني.

6- تعزيز التعاون الدولي: من خلال الشراكات الدولية و تعزيز التعاون مع الدول الأخرى والمنظمات الدولية لتبادل المعلومات والخبرات في مجال الأمن السيبراني، والانخراط في المبادرات والاتفاقيات الدولية التي تهدف إلى تعزيز الأمن السيبراني على مستوى العالم.

7- إدارة الحوادث والاستجابة: من خلال تطوير وتحديث خطط استجابة للحوادث السيبرانية تضمن التعامل السريع والفعال مع أي تهديدات، وتنظيم تدريبات ومناورات دورية لمحاكاة الهجمات السيبرانية وتحسين جاهزية المؤسسات للتعامل معها.

8- الحوكمة والإدارة: من خلال وضع سياسات وإجراءات واضحة لإدارة الأمن السيبراني تشمل جميع الجوانب التنظيمية والتقنية، وإجراء تقييمات دورية للمخاطر السيبرانية واتخاذ التدابير الوقائية المناسبة.

الخاتمة:

إن تحقيق الأمن السيبراني يشكل تحدًيا متزايدًا في ظل تطور التكنولوجيا، ولكن تحقيقه في الجزائر يتطلب تبني استراتيجية شاملة ومتكاملة تشمل تطوير التشريعات، تعزيز المؤسسات، الاستثمار في التكنولوجيا، التعليم والتوعية، تطوير القدرات البشرية، وتعزيز التعاون الدولي. من خلال تنفيذ هذه التوصيات، يمكن للجزائر بناء بيئة رقمية آمنة ومستدامة قادرة على مواجهة التهديدات السيبرانية المتزايدة.

وفي هذا السياق، يتعين على الجزائر، وغيرها من الدول:

- تعزيز التعاون الدولي وتبادل الخبرات في مجال الأمن السيبراني لمواجهة هذه التحديات.
- تطوير استراتيجيات دفاعية فعّالة لحماية البنية التحتية الرقمية الوطنية ومعالجة التهديدات السيبرانية بشكل شامل.
- دعم البحث والتطوير في مجال الأمن المعلوماتي وتعزيز التدريب والتوعية لدى المؤسسات والمواطنين حول مخاطر الأمن السيبراني،
- أن يلتزم القطاع العام والخاص بتنفيذ أفضل الممارسات والمعايير الدولية في مجال الأمن المعلوماتي، بما يشمل إجراءات الحماية الوقائية والاستجابة للحوادث وإدارة المخاطر.
- التعاون والتنسيق الدوليين، إذ يمكن أن يسهم بشكل كبير في تعزيز الحماية وتعزيز الاستقرار السيبراني للدولة.

---

[1] عبد العزيز بن فهد بن محمد بن داوود، الجرائم السيبرانية: دراسة تأصيلية مقارنة. مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد09، العدد03، 2020، ص 148.

[2] إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة الجزائر، المجلد 01، العدد 01، 2019، ص 103.

[3] جمال بوزادية، الاستراتيجية الجزائرية في مواجهة السيبرانية" التحديات و الأفاق المستقبلية"، مجلة العلوم القانونية والسياسية - جامعة العربي التبسي، الجزائر، المجلد01، العدد 01، 2019، ص103.

[4] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق ل 10 مايو سنة 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، المادة 3/10، الجريدة الرسمية، العدد 27، بتاريخ 13 ماي 2018، ص 03.

[5] الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 66-156، المؤرخ في 18 صفر عام 1386 الموافق ل 8يونيو سنة 1966، المتضمن قانون العقوبات المعدل والمتمم، الجريدة الرسمية، العدد 49، بتاريخ 01يونيو 1966، ص 702.

[6] الجمهورية الجزائرية الديمقراطية الشعبية، القانون 04-15 المؤرخ في 10 نوفمبر 2004 المتضمن تعديل قانون العقوبات، الجريدة الرسمية، العدد 71، 2004، ص، ص 11-12.

[7] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430، الموافق ل 5 غشت سنة2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المادة02، الجريدة الرسمية. العدد 47، بتاريخ 16 غشت سنة 2009.

[8] حمدون توريه، دليل الأمن السيبراني للبلدان النامية. الجزء الأول، جنيف:الإتحاد الدولي للاتصالات، 2006، ص 61.

[9] نوال الشهري، حرب المعلومات. مركز تميز أمن المعلومات، (جامعة الملك سعود)، دن، من الرابط:

www.coeia.edu.sa/index.php/ar/assur_awess/data_privacy/1263_influance_warfare.html تم الاطلاع عليه في 2024/04/25م.

[10] حسين فاروق، فيروسات الحاسب الآلي. ط1، القاهرة: العربية للطباعة والنشر، 1999، ص 7.

[11] وليد غسان سعيد جلعود، دور الحرب الالكترونية في الصراع العربي الإسرائيلي. أطروحة ماجستير في التخطيط والتنمية السياسية، كلية الدراسات العليا، جامعة نابلس، فلسطين، 2013.

[12] الرسائل الصامتة "سلاح الرقابة السرية"،23يونيو 2016، من الرابط www.almaged.ps/3 تم الاطلاع عليه يوم 2024/04/25.

[13] غسان جلعود، مرجع سابق، ص 113.

[14] شبكة النبأ المعلوماتية، حرب الفضاء والأقمار الصناعية. من الرابط: www.annaba.org/nbanes/69/022/htm2019/03/19 تم الاطلاع عليه يوم 2024/04/25 2024م

[15] اسماعيل كاخيل، "الحرب الإلكترونية". موقع مجلة الدفاع العربي، من الرابط:
htm2019/03/18.www.arahdefancejournal.com/article560 تم الاطلاع عليه يوم 2024/04/25.

[16] جعفر حسن جاسم، حرب المعلومات بين ارث الماضي ود ديناميكية المستقبل. عمان: دار البداية، 2012 ، ص 128.

[17] غسان جلعود، مرجع سابق، ص 115.

[18] غسان جلعود، مرجع سابق، ص 117.

[19] https://www.elnooronline.net/

[20] إدريس عطية، "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري"، مجلة مصداقية. كلية الحقوق و العلوم السياسية- جامعة العربي التبسي، الجزائر، المجلد1، العدد 1، 2019، ص105.

[21] سميرة بارة، الأمن السيبراني في الجزائر السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، المجلد 02، العدد 04، 2017، ص263.

[22] إدريس عطية، مرجع سابق، ص105.

[23] المرسوم الرئاسي رقم 22-187 المؤرخ في 17 شوال عام 1443 الموافق 18 ماي سنة 2022، يتضمن تعيين رئيس وأعضاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي. (الجريدة الرسمية عدد 35 لسنة 2022)

[24] مرسوم رئاسي رقم 23-73 مؤرخ في 14 فبراير سنة 2023، يحدد مهام الأمانة التنفيذية للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي وكيفيات تنظيمها وسيرها. (الجريدة الرسمية عدد 10 لسنة 2023)

[25] الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي رقم 20-05 مؤرخ في 24 جمادى الأولى عام 1441 الموافق ل20 يناير سنة 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية. العدد 04، بتاريخ 26 جانفي 2020، ص 06.

[26] الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي رقم 20-05، مرجع سابق، ص 06.

[27] سمير بارة، مرجع سابق، ص 10.

[28] عز الدين عز الدين، " الإطار القانوني للوقاية من الجرائم المعلوماتية و مكافحتها"، قيادة الدرك الوطني، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة، جامعة محمد خيضر بسكرة، 16 نوفمبر 2015، ص 30.

[29] المرجع نفسه، ص 39.

[30] الجمهورية الجزائرية الديمقراطية الشعبية، مرسوم رئاسي 15-261 مؤرخ في 2015/10/08، يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والمكافحة، الجريدة الرسمية. العدد 53، الصادرة بتاريخ 2015/10/08، ص ص 16-20.

[31] إلهام غازي، " الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري"، مجلة الجيش، مؤسسة المنشورات العسكرية، العدد 630، جانفي 2016، ص44.

"في فهم وتحليل الجرائم السيبرانية والتهديدات الأمنية العابرة للحدود: مقاربة معرفية"

Understanding the nature of cybercrime and cross-border security threats: a cognitive approach"

د. الحامدي عيدون، المؤسسة المستخدمة: جامعة محمد لمين دباغين سطيف 2 -كلية الحقوق العلوم السياسية-

البريد الإلكتروني: e.aidoun@univ-setif2.dz

ط.د.رابح فرطاس، المؤسسة المستخدمة: جامعة محمد لمين دباغين سطيف 2 -كلية الحقوق العلوم السياسية-

البريد الإلكتروني: ra.fartas@univ-setif2.dz

الملخص:

تعتبر الجرائم السيبرانية والتهديدات الأمنية العابرة للحدود تحديا كبيرا في العصر التكنولوجي المعاصر. تشمل هذه الجرائم لاختراقات الإلكترونية، والبرمجيات الخبيثة، والاحتيال الإلكتروني، وسرقة الهوية، والتجسس الإلكتروني، والقرصنة، والاعتداء على البنية التحتية الحاسوبية، والهجمات الضارة الموجهة للأفراد والمؤسسات ويمكن للمهاجمين العمل من أي مكان في العالم ومهاجمة أهدافهم في بلدان أخرى، مما يزيد من تعقيد المشكلة.

لمواجهة هذه التحديات، تحتاج الدول والمؤسسات إلى اتخاذ إجراءات أمنية قوية، بتعزيز قدرات الدفاع السيبراني وتوفير التدريب المناسب للموظفين وينبغي أيضا تحسين التعاون الدولي في مجال مكافحة الجرائم السيبرانية وتبادل المعلومات والخبرات ووضع قوانين وأنظمة فعالة لمكافحة الجرائم السيبرانية ومعاقبة المتسببين فيها.

ان مكافحة الجرائم السيبرانية والتهديدات الأمنية العابرة للحدود تتطلب جهودا مشتركة وتعاونا دوليا قويا لحماية الأنظمة والبيانات وضمان لأمن السيبراني في العالم الرقمي المتقدم.

الكلمات المفتاحية: الجرائم السيبرانية، التهديدات الأمنية العابرة للحدود، الاحتيال الإلكتروني، التجسس الإلكتروني.

Abstract:

Cybercrime and cross-border security threats are significant challenges in the modern era. These crimes encompass electronic hacking, malware, online fraud, identity theft, cyber espionage, piracy, attacks on computer infrastructure, and harmful attacks targeting individuals and institutions. Attackers can operate from anywhere in the world and target their objectives in different countries, increasing the complexity of the problem.

To address these challenges, countries and organizations need to implement strong security measures by enhancing cyber défense capabilities and providing appropriate training to their personnel. It is also crucial to improve international cooperation in combating cybercrime, exchanging information and expertise, and establishing effective laws and systems to combat cybercrime and hold perpetrators accountable, combating cybercrime and cross-border security threats requires joint efforts and strong international cooperation to protect systems, data, and ensure cybersecurity in the advanced digital world.

Keywords: **cybercrime, cross-border security threats, electronic fraud, cyber espionage.**

مقدمة:

يواجه المجتمع الدولي حاليا على غرار دولة الجزائر تهديدات أمنية عديدة ومتغيرة، ومن أبرزها التهديدات السيبرانية والتهديدات الأمنية العابرة للحدود، تستهدف الفضاء الإلكتروني وتؤثر على الأنظمة والشبكات والأجهزة، وتهدد أمن الدول والأفراد، وبالتالي، أصبح من الضروري وضع استراتيجيات سيبرانية شاملة للتصدي لهذه التهديدات، تعتمد استراتيجيات الأمن السيبراني على الدفاع والوقاية والرد والتعاون بين الدول والجهات المعنية.

وتتطلب مكافحة التهديدات السيبرانية تعاونا دوليا فعالاً وتنسيقا بين الدول والمؤسسات الدولية وان تتبنى الدول سياسات أمنية قوية لحماية الأنظمة الحيوية والبنية التحتية الحيوية من الهجمات السيبرانية، وينبغي أيضا تعزيز التعاون الدولي في مجال مكافحة الجرائم السيبرانية وتبادل المعلومات وتعزيز القدرات التقنية لمواجهة التهديدات.

وتطوير المهارات والتدريب وتعزيز الوعي السيبراني للأفراد وأن تتعاون الحكومات مع القطاع الخاص والأكاديميين لتعزيز البحث والتطوير في مجال الأمن السيبراني، وأن تعزز المنظمات الدولية والإقليمية جهودها لتعزيز الأمن السيبراني.

أهمية الدراسة: تتعلق أساس بمتغيرات الموضوع، والمتمثلة أساسا في أهمية الأمن السيبراني والاستفادة من تجارب الدول الكبرى في هذا المجال، وتشير إلى أن العالم يستعد لمشاريع عملاقة في الفضاء السيبراني ويحتاج إلى بنية تحتية قوية وحلول أمنية متقدمة، حيث يتعين توفير حماية للمصالح الحيوية والاقتصادية في الفضاء السيبراني. وتشير إلى أن المراكز الأمنية السيبرانية تعمل على مكافحة التهديدات السيبرانية والتهديدات الأمنية العابرة للحدود باستخدام حلول تكنولوجية متقدمة وخبراء ذوي خبرة.

هدف الدراسة: تسعى إلى توضيح المفاهيم الجديدة للأمن السيبراني والتهديدات الأمنية العابرة للحدود، وأيضا إبراز دور المجتمع الدولي في مواجهة هذه التهديدات السيبرانية.

إشكالية الدراسة:

انطلاقا من هذا الطرح، تحاول الورقة البحثية دراسة إطار العام التحول السريع والواسع النطاق نحو الخدمات الإلكترونية في جميع جوانب الحياة، مع تزايد الاعتماد على المجال المعلوماتي الإلكتروني (السيبراني)، والذي يعتبر الميدان الخامس للرّاعات بعد الأرض والجو والبحر والفضاء. هذا التحول يوفر فوائد عديدة في تقليص الوقت والجهد والتكلفة، ولكنه يشكل أيضا تهديدات ومخاطر على الأمن والاستقرار الوطني والمؤسسات.

من هنا، يكمن التركيز الرئيسي للبحث في كيفية التصدي لتهديدات الجرائم الإلكترونية والتهديدات الأمنية العابرة للحدود والحفاظ على الأمن والاستقرار.

بناء عليه، يمكننا طرح التساؤل المركزي التالي:

-كيف يمكن لنا أن تفهم طبيعة الجرائم السيبرانية والتهديدات الأمنية العابرة للحدود من منظور معرفي؟

وقد تفرعت عن هذه الإشكالية التساؤلات الفرعية التالية:

1-ما هي التهديدات السيبرانية وماهي طرق حماية منها؟

2-فيما تتمثل التهديدات العابرة للحدود وماهي الطرق مواجهتها؟

3-كيف يتم حماية التنظيمات السيبرانية من التهديدات العابرة للحدود؟

منهج الدراسة:

-الإحاطة بموضوع البحث سنعتمد في دراستنا هاته على المنهج الوصفي التحليلي وذلك من خلال التطرق إلى مضمون التعاون الدولي في مجال مكافحة الجرائم السيبرانية وحماية الأنظمة السيبرانية من التهديدات العابرة للحدود.

المحور الأول: تهديدات الأمن الإلكتروني للدول.

إن الأمن الإلكتروني يمثل أحدث وأهم صور الأمن في العلاقات الدولية، مما أدى إلى تزايد اهتمام الباحثين في مجال العلاقات الدولية بدراسته، والبحث في عدد من القضايا المرتبطة به، ولعل أبرز قضايا الأمن الإلكتروني وتهديداته، في محاولة للتصدي للتهديدات الأمنية المرتبطة به، بوضع استراتيجيات واسعة النطاق في التعامل مع القضايا الخاصة به.

أولا: أنماط وطبيعة وأشكال التهديدات الالكترونية للدول.

وتنقسم التهديدات الالكترونية التي تواجهها الدول والأفراد إلى أربعة أنماط رئاسة هي: (محمد مختار،2015، ص 5-6.)

1-هجمات الحرمان من الخدمة: حيث يتم إطلاق حزمة كبيرة من الطلبات والمهمات على خوادم الضحية بصورة تفوق قدرة الخادم أو الجهاز على معالجتها والاستجابة لها، مما يؤدي إلى توقفه بصورة جزئية أو كلية أو إبطاء عمله، وهذا ما يسبب ضرر للمستخدم النهائي، وهي تستعمل كثيرا ضد مواقع الانترنت أو البنوك أو المؤسسات من أجل التأثير عليها أو لدفع فدية مالية.

2-إتلاف المعلومات أو تعديلها: ويقصد به الوصول إلى معلومات الضحية عبر شبكة الإنترنت أو الشبكات الخاصة، والقيام بعملية تعديل البيانات الهامة دون أن يكتشف الضحية ذلك، في البيانات تبقى موجودة ولكنها مضللة قد تؤدي إلى نتائج كارثية خاصة إذا كانت خطط عسكرية أو مواعيد او الخرائط سرية.

3-التجسس على الشبكات: ويقصد به الدخول غير المصرح والتجسس على شبكات الخصم، دون تدمير او تغيير في البيانات، والهدف منها الحصول معلومات قد تكون خطط عسكرية أو أسرار حربية، اقتصادية، مالية، أو سياسية، مما يؤثر سلبا على مهام الخصم.

4-تدمير المعلومات:ويتم في هذه الحالة مسح وتدمير كامل للأصول والمعلومات والبيانات الموجودة على الشبكة، يصطلح عليه " تهديد لسلامة المحتوى"ويعني بها إحداث تغيير في البيانات سواء بالحذف أو التدمير من قبل أشخاص غير مخولين.

هناك من يميز بين عدة أنواع لمخاطر التهديدات السيبرانية نذكر من: (إيهاب خليفة ،2015، 2017، ص 54).

- التعرض لسرية الاتصالات التي تطال البريد الالكتروني، والدخول إلى الأنظمة والملفات دون إذن، وهذا يعتبر اعتداء على الحريات والحقوق الشخصية.

- التلاعب بالمعلومات الموجودة في نظام معين، وتشويهها أو إتلافها، سواء عبر الاختراق أو نشر الفيروسات.

- الجرائم العادية التي تستخدم الانترنت، السرقة والغش وسرقة الهويات، والاعتداء على الملكية الفكرية وغيرها.

- الجرائم التي تندرج في إطار الجريمة المنظمة، والتي تهدد أمن الأفراد والدول، كتبييض الأموال والإرهاب...الخ،

-إن أهم التهديدات إلكترونية السبع، الواجب التنبه لها في عامي 2015-2016، وأوقات ازدهار التهديدات والهجمات والجرائم الإلكترونية، بدءا من سرقة الهوية وحتى اختراقات بيانات البيع بالتجزئة، تسيطر هذه الهجمات على مسار الأخبار، في المتوسط، سيدفع ضحايا لاحتيال 776 دولارا من أموالهم ويخسرون 20 ساعة في محاولة إصلاح الفوضى التي أحدثها سارقوا الهوية.

5-دودة الحاسوب (computer worm): هي برامج خبيثة تتكاثر بنسخ نفسها، وتنتقل من نظام إلى أخر باستغلال الثغرات الأمنية، (الخطاب حارث عاصم،2018 ص 71.)، صنعت للأعمال التخريبية كأن تعمل على قطع الاتصال بالشبكة أو سرقة البيانات أثناء تصفح المستخدمين بالإنترنت، وتمتاز بسرعة الانتشار والقدرة الفائقة على التلون والتكاثر ويصعب التخلص منها، وتستهدف عادة الشبكات المالية، وشبكات البنوك. (خليفة إيهاب, 2017، ص84).

6-أحصنة طروادة (Trojan Horse): وهو شفرة أو برنامج صغير مختبئ في برنامج كبير من البرامج ذات الشعبية المالية وهو مبرمج بمهارة عالية، حيث يقوم بالمهام الخفية مثل نشر دودة أو فيروس، ومن الصعوبة اكتشافه، حيث يعمل دائما على مسح آثاره التي لا تحمل صنعة تخريبية، ويقوم بأضعاف قوة الدفاع للمستهدف وسهولة اختراق جهازه وسرقة بياناته. (خليفة إيهاب, 2017، ص85).

فيما يلي نتطرق إلى طبيعة التهديدات الالكترونية السبعة المستمرة التي توضح التحديات الحالية التي تواجهها للحفاظ على حماية بياناتك هي:

1- اختراقات بيانات البيع بالتجزئة: تشكل اختراقات بيانات البيع بالتجزئة خطورة حقيقية حيث يمكن أن تؤثر فعليا في أي شخص فقد شهد عام 2014 ارتفاعا في الهجمات الإلكترونية التي تستهدف الشركات الكبيرة، حيث سرق المتطفلون أرقام بطاقات الائتمان والسحب الخاصة بـ 40 مليون عميل، و يقوم المجرمون الإلكترونيون بسرقة هذه المعلومات الشخصية وبيعها في السوق السوداء، مما يمكن أن يؤدي إلى سرقة الهوية بسهولة ، وبينما تتحمل شركة البيع بالتجزئة جزءا كبيرا من المسؤولية، كأن تتولى تحديث أساليب الدفع وتأمينها، تبقى مراقبة حسابك المصرفي وكشف حساب بطاقة الائتمان الخاصة بك عن كثب طريقة جيدة للحفاظ على أمنك أثناء الهجمات على البيع بالتجزئة و من أهم لاختراقات هي :(bbc.com/arabic/business).

2- شركة Target الأمريكية : في ديسمبر 2013 ، كانت شركة Target ، وهي ثالث أكبر سلسلة متاجر أمريكية للبيع بالتجزئة ضحية لهجوم حاد من قراصنة الانترنت ، حيث تعرض 70 مليون عميل إلى اختراق لمعلوماتهم الشخصية ، بما في ذلك تفاصيل حساباتهم المصرفية ،ونتيجة لذلك، تعرضت سمعة الشركة لضربة خطيرة ، كلف هذا الهجوم الإلكتروني حوالي مليار دولار أمريكي (خاصة للبطاقات المصرفية التي أعيد إصدارها) ، وقد خفض هذا الحدث أرباح المجموعة في أواخر عام 2013 بمقدار 440 مليون دولار أمريكي ، ثم استقال الرئيس التنفيذي بعد بضعة أشهر على اثر هذه الحادثة ، و في مارس 2015 ، أمر قاضي مينيسوتا شركة Target بدفع 10 مليون دولار أمريكي للعملاء الذين تعرضوا لأضرار بسبب هذا الهجوم.

3- شركة eBay الأمريكية العملاقة: في مايو 2014، تعرضت شركة eBay الأمريكية العملاقة لهجوم إلكتروني أدى إلى سرقة بيانات 140 مليون حساب مصرفي لعملائها حيث ضمت البيانات المسروقة أسماء وعناوين بريد الإلكتروني وعناوين بريدية وأرقام هواتف وتواريخ ميلاد وكلمات مرور هذا وقد سرقت كلمات مرور موظفين شركة eBay أيضا.

4- شركة Sony Pictures: في 24 نوفمبر 2014، اخترق المتسللون أنظمة الكمبيوتر في Sony Pictures في مواقع مختلفة للشركة، بما في ذلك مقرها في لوس أنجلوس وأصبحت البيانات المسروقة، بما في ذلك الأفلام الجديدة والمعلومات السرية متاحة للجمهور على شبكة الانترنت.

5- شركة Orange: تعرضت شركة المحمول الفرنسية Orange لهجومين عبر الإنترنت في غضون بضعة أشهر في يناير وأبريل 2014، حيث تمت سرقة ملايين البيانات الشخصية للعملاء وبلغت تكلفة هذه الحوادث التي تكبدتها شركة Orange أكثر من 24 مليون يورو (29 مليون دولار أمريكي).

5- TV-6 موند: في 8 و 9 أبريل 2015 ، تعرضت القناة الفرنسية TV5 Monde لهجوم سيبراني واسع النطاق حيث أصبحت الأنظمة غير قادرة على العمل لفترة أطول وتم قطع البث ومبلغ المطالبة غير معروف حتى الآن.

7-- شركة Airaner Ryanair: أعلنت الشركة أن المتسللين قد سرقوا حوالي 5 مليون دولار أمريكي بعد نقل إلكتروني مزور عبر بنك صيني، ووفقا للشركة، كان ينبغي استخدام تلك الأموال لدفع فواتير الكيروسين kerosene، تم اكتشاف هذا الاحتيال في 24 أبريل 2015.

8- اختراق إلكتروني للخطوط البريطانية للطيران عام 2018 : تقدم رئيس شركة الخطوط الجوية البريطانية للطيران باعتذار عن خرق حدث لنظام الشركة الأمني، ووعد بتقديم تعويضات للعملاء المتضررين ، وقال أن القراصنة شنوا "هجوما معقدا وإجراميا" على موقع الشركة ، وقالت الشركة إن بيانات شخصية ومالية تخص عملاء الشركة تعرضت للاختراق ، ووصلت عملية الاختراق الإلكتروني إلى نحو 380 ألف عملية شراء تذاكر، ولكن البيانات التي حصل عليها القراصنة لم تشمل تفاصيل الرحلات وجوازات السفر، وانخفضت قيمة أسهم شركة IAG المالكة لشركة الطيران بنحو 3 في المئة في تداولات نهاية صباح الهجوم في سوق لندن.

ويعتبر عام 2018 هو عام الاختراقات الأمنية، حيث شهد العالم كله خلال عام 2018 ارتفاعا كبيرا في عمليات اختراق أنظمة الأمن الإلكتروني وبالتالي تسريب بيانات الملايين من المستخدمين، فعلى فترات متقاربة جدا، تم اكتشاف اختراق جديد لإحدى الشركات التي تقوم بدورها بإخطار عملائها بأن بياناتهم قد تعرضت للاختراق، وهناك العديد من الأسباب لخروقات البيانات، منها إساءة التعامل مع البيانات أو بيع بيانات المستخدمين لأطراف ثالثة أو ثغرات موجودة في نظام أمان مواقع الويب الخاصة بهذه الشركات.

ثانيا:ومن أكبر 10 اختراقات للبيانات التي تم الكشف عنها خلال عام 2018 مصنفة حسب عدد المستخدمين المتأثرين: (الجريدة الالكترونية08 /2021/08.).

1-اختراق أدهار Aadhaar وتسريب بيانات 1.1 مليار مواطن هندي.

2-اختراق سلسلة فنادق ماريوت وتسريب بيانات 500 مليون عميل.

3-اختراق تطبيق MyFitnessPal وتسريب بيانات 150 مليون حساب.

4-اختراق موقع Quora وتسريب بيانات 100 مليون مستخدم.

5-اختراق MyHeritage وتسريب بيانات ال DNA لأكثر من 92 مليون مستخدم.

6-اختراق جوجل بلس Google +وتسريب بيانات 52.5 مليون مستخدم.

7-اختراق موقع Chegg وتسريب بيانات 40 مليون عميل.

8-اختراق موقع فيسبوك وتسريب بيانات 29 مليون مستخدم.

9-اختراق موقع Ticketfly وتسريب بيانات 27 مليون مستخدم.

10-اختراق تطبيق Timehop وتسريب بيانات 21 مليون مستخدم.

2- تهديدات أمن الأجهزة المحمولة والثغرات الأمنية في الهواتف الذكية :

يمكن للمجرم الإلكتروني استغلال الثغرات الأمنية في الهواتف الذكية بسهولة للحصول على البيانات الخاصة ، وتتولد هذه الثغرات الأمنية أحيانا من التطبيقات التي تستخدمها أو من الهواتف الذكية نفسها ،تقع الهواتف المحمولة كذلك عرضة للإصابة بالبرامج الضارة، و يتعرض مستخدموا الهواتف الذكية لتهديدات مختلفة عند استخدام هواتفهم ، في عام 2012 ، ارتفع عدد التهديدات الفريدة للهواتف المحمولة بنسبة 261٪ ، وفقا لمنظمة أبحاث السوق ABI Research، يمكن أن تؤدي هذه التهديدات إلى تعطيل تشغيل الهاتف الذكي ونقل بيانات المستخدم أو تعديلها ، وبالتالي التطبيقات يجب أن تضمن خصوصية و الزاهة من المعلومات التي يتعاملون معها ، بالإضافة إلى ذلك ، نظرا لأن بعض التطبيقات يمكن أن تكون نفسها البرمجيات الخبيثة، يجب أن تكون وظائفهم وأنشطتهم محدودة (على سبيل المثال ، تقييد التطبيقات من الوصول إلى معلومات الموقع عبر GPS، ومنع الوصول إلى دفتر عناوين المستخدم ، ومنع نقل البيانات على شبكة الاتصال، إرسال رسالة قصيرة الرسائل التي تتم فوترتها للمستخدم ، وما إلى ذلك).

هناك ثلاثة أهداف رئيسية للمهاجمين:

- البيانات: الهواتف الذكية هي أجهزة لإدارة البيانات، وقد تحتوي على بيانات حساسة مثل أرقام بطاقات الائتمان، ومعلومات المصادقة، والمعلومات الخاصة، وسجلات النشاط (التقويم، وسجلات المكالمات).

- الهوية: الهواتف الذكية قابلة للتخصيص بدرجة كبيرة، لذلك يمكن بسهولة ربط الجهاز أو محتوياته بشخص معين، على سبيل المثال، يمكن لكل جهاز محمول نقل المعلومات المتعلقة بمالك عقد الهاتف المحمول، وقد يرغب المهاجم في سرقة هوية مالك الهاتف الذكي لارتكاب جرائم أخرى.

- التوفر: يمكن أن تحد مهاجمة الهاتف الذكي من الوصول إليه وتحرم صاحبه من استخدامه.

وهناك عدد من التهديدات للأجهزة المحمولة، بما في ذلك لإزعاج وسرقة لأموال وانتهاك الخصوصية والنشر والأدوات الضارة.

- بوت نت: يقوم المهاجمون بإصابة أجهزة متعددة ببرامج ضارة يكتسبها الضحايا بشكل عام عبر مرفقات البريد الإلكتروني أو من التطبيقات أو مواقع الويب المخترقة، ثم تمنح البرامج الضارة المتسللين التحكم عن بعد في أجهزة "الزومبي"، والتي يمكن بعد ذلك توجيهها لتنفيذ أعمال ضارة.

- التطبيقات الضارة: يقوم المتسللون بتحميل البرامج أو الألعاب الضارة إلى أسواق تطبيقات الهواتف الذكية التابعة لجهات خارجية، تقوم البرامج بسرقة المعلومات الشخصية وفتح قنوات الاتصال الخلفية لتثبيت تطبيقات إضافية والتسبب في مشاكل أخرى.

- الروابط الضارة على الشبكات لاجتماعية: طريقة فعالة لنشر البرامج الضارة حيث يمكن للقراصنة وضع أحصنة طروادة وبرامج التجسس والأبواب الخلفية.

- برامج التجسس: يستخدم المتسللون هذا لاختطاف الهواتف، مما يسمح لهم بسماع المكالمات ورؤية الرسائل النصية ورسائل البريد الإلكتروني بالإضافة إلى تتبع موقع شخص ما من خلال تحديثات GPS.

3-هجمات التصيد لاحتيالي والهندسة لاجتماعية: عندما يخدع المجرمون الإلكترونيون الأشخاص للكشف عن معلومات حساسة ككلمات المرور وأرقام الضمان لاجتماعي، يطلق على ذلك التصيد لاحتيالي، من أشهر طرق حدوث التصيد لاحتيالي أن يتلقى الشخص رسالة بريد إلكتروني تبدو ظاهريا أنها من مصرف أو مؤسسة حكومية ويتم استدراجه إلى مواقع تبدو حقيقية، وبمجرد الوصول إليها، يطلب من الشخص إدخال كلمة المرور وأرقام الضمان لاجتماعي والبيانات المالية.

ثم يأخذ المجرمون الإلكترونيون هذه المعلومات ويستخدمونها لأغراضهم الخاصة، يعد التصيد لاحتيالي جزءا من مشكلة أكبر تسمى الهندسة لاجتماعية، التي تتلاعب في لأساس بالعواطف من أجل كسب الوصول إلى البيانات الحساسة.

تحدث هجمات الهندسة لاجتماعية عندما يتم خداع مستخدم الويب لتنفيذ بعض لإجراءات الخطيرة على لإنترنت.

ثمة أنواع مختلفة من هجمات الهندسة لاجتماعية:

- التصيد لاحتيالي: يخدع الموقع الإلكتروني المستخدمين لحثهم على الكشف عن معلوماتهم الشخصية (على سبيل المثال، كلمات المرور أو أرقام الهواتف أو بطاقات الائتمان)، وفي هذه الحالة يدعي المحتوى أنه جهة موثوق بها، مثل متصفح أو نظام تشغيل أو مصرف أو حكومة.

- المحتوى المخادع: يحاول المحتوى خداعك للحث على تنفيذ بعض لإجراءات التي لا تجريها إلا مع جهة موثوق بها، مثل مشاركة كلمة مرور أو الاتصال بالدعم الفني أو تزيل برامج، أو أن المحتوى يشتمل على إعلان يدعي كذبا أن برنامج الجهاز قديم، ويحث المستخدمين على تثبيت برنامج غير مرغوب فيه.

- خدمات خارجية غير مكتملة التصنيف: الخدمة الخارجية هي شخص يدير موقعا إلكترونيا أو خدمة بالنيابة عن جهة أخرى، على سبيل المثال، إذا كنت (الطرف الأول) تدير موقعا إلكترونيا خيريا يستخدم موقعا إلكترونيا لإدارة التبرعات

(الطرف الثالث) يتولى جمع التبرعات لموقعك الإلكتروني، يجب أن يحدد موقع التبرع الإلكتروني بوضوح أنه منصة خارجية تتصرف بالنيابة عن الموقع الإلكتروني الخيري، وإلا يمكن اعتباره من مواقع الهندسة الاجتماعية.

تحمي ميزة التصفح الآمن من **Google** مستخدمي الويب من خلال تحذيرهم قبل زيارة الصفحات التي تشارك باستمرار في الهندسة الاجتماعية.

يتم اعتبار صفحات الويب على أنها صفحات هندسة اجتماعية عندما: تحاكي تصميم إحدى المنصات الموثوق بها أو مظهرها أو وظيفتها، مثل جهازك أو متصفحك أو الموقع الإلكتروني ذاته، أو تحاول خداعك لتنفيذ بعض الإجراءات التي لا تجريها إلا مع جهة موثوق بها، مثل مشاركة كلمة مرور أو الاتصال بالدعم الفني أو تنزيل برامج.

إن الهندسة الاجتماعية في المحتوى المضمن، يمكن أن تظهر في مواقع إلكترونية غير خطيرة بطريقة أخرى، ويكون ذلك في الإعلانات عادة، ويعد محتوى الهندسة الاجتماعية المضمن انتهاكا لسياسة صفحة المضيف.

قد يتم تضمين محتوى الهندسة الاجتماعية المضلل عبر موارد تم تضمينها في الصفحة، مثل الصور أو المكونات الخارجية الأخرى أو الإعلانات، وقد يخدع هذا المحتوى المخادع زائري الموقع لتنزيل برامج غير مرغوب بها.

بالإضافة إلى ذلك، يمكن للمخترقين التحكم في المواقع الإلكترونية البسيطة واستخدامها لاستضافة أو توزيع محتوى الهندسة الاجتماعية، ويمكن أن يغير المخترقون محتوى الموقع الإلكتروني أو أن يضيفوا صفحات إضافية إلى الموقع الإلكتروني غالبا بغرض خداع الزائرين لحثهم على مشاركة معلومات شخصية، مثل أرقام بطاقات الائتمان، ويمكن معرفة ما إذا كان قد تم تحديد موقعك الإلكتروني على أنه موقع يستضيف أو يوزع محتوى الهندسة الاجتماعية.

4-سرقة الهوية: تعد سرقة الهوية**identity theft** إحدى أسرع جرائم الإنترنت تطورا وتشير سرقة الهوية إلى تلك العمليات التي يتم من خلالها سرقة معلومات شخصية عن الهوية تستخدم للاحتيال والقيام بأعمال غير قانونية واستغلال هذه المعلومات لتحقيق مكاسب مالية (**Shun-Yung Wang & Wilson Huang. Op. cit. p5**) ، منها رسائل البريد الإلكتروني للتصيد الاحتيالي وعمليات اختراق البيانات ،ومع ذلك تبقى الهوية عرضة للخطر أيضا ، كالسيرة الذاتية وعنوان المنزل والصور ومقاطع الفيديو عبر مواقع التواصل الاجتماعي والبيانات المالية، وغيرها ، فسارقو الهوية و المعلومات الشخصية ، يفتحون بطاقات الائتمان وحسابات القروض باسم الضحية.

5-اختراقات بيانات الرعاية الصحية (ابوبكر سلطان، 2021): لتعزيز أنظمة صحية قوية، قدمت منظمة الصحة العالمية 10 مسارات صحية إلى البلدان لمتابعة معركة الجائحة والتحرك بسرعة لإصلاح أنظمتها الصحية في عام 2021م، ومع تقدم الثورة الصناعية الرابعة، بزغ مفهوم الرعاية الصحية الذكية لتحويل النظام الطبي التقليدي إلى نظام صحي وقائي شامل أفعل وأكفئ.

رغم أن مفهوم الرعاية الصحية الذكية لا يزال في مهده، إلا أن الرعاية الصحية شهدت بداية تحول جذري بفضل تقنيات ذكية بارعة تستخلص رؤى دقيقة، ومن أهمها:

- الذكاء الاصطناعي (وفروعه تعلم الآلة، والتعلم العميق).
- الحوسبة، والمعرفية، والإدراكية، والكمومية.
- إنترنت الأشياء.
- الحوسبة والتخزين السحابيان.
- الروبوتات.
- البيانات الضخمة والتحليلات.

ففي بداية 2015، واجهت شركة الرعاية الصحية **Anthem** اختراقا كبيرا للبيانات بواسطة متطفلين، وتأثر بذلك 78.8 مليون شخص، وفي يوليو 2015، اقتحم المتطفلون شبكة حواسيب نظام **UCLA Health System**، ومن المحتمل أن

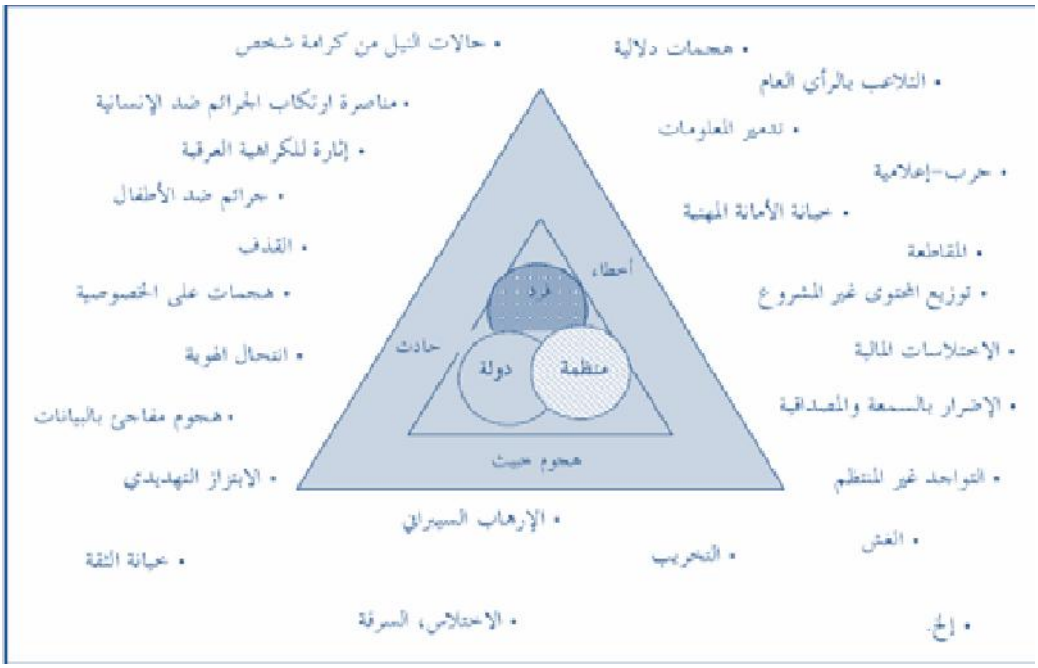
يكونوا قد وصلوا إلى المعلومات الشخصية لـ 4.5 ملايين مريض ، تحتوي سجلات الرعاية الصحية على معلومات مهمة وحساسة وتمثل أهدافا أساسية للمجرمين الإلكترونيين مما يمكن أن يؤدي بسهولة إلى سرقة الهوية ، وفي كثير من الأحيان، تستخدم هذه المعلومات للاحتيال على التأمين الصحي، مثل شراء الوصفات الطبية المزورة وبيعها ، احرص دائما على تتبع الأخبار الخاصة بأي تقارير عن اختراقات لبيانات الرعاية الصحية.

6- استهداف الأطفال من قبل المتحرشين الجنسيين: (ابوبكر سلطان، 2021)، يختبئ المستخدمون المتطلعون إلى استغلال الأطفال في أركان مظلمة عبر الإنترنت للاتجار بصور الأطفال الخليعة غير القانونية، ويحدث ذلك عن طريق البريد الإلكتروني أو برامج نظير إلى نظير أو على نحو متزايد من خلال شبكة الويب المظلمة، وهي مساحة عبر الإنترنت لا يمكن الوصول إليها باستخدام محركات البحث القياسية ة، ومع أن هذه المواقع تعد مصدر قلق، فإنه من الأفضل تركها للمسؤولين في منظمات إنفاذ القانون، وعلى الشخص العادي تجنبها تماما.

ثمة خطر آخر عبر الإنترنت يستهدف الأطفال ويظهر عندما يحاول المتحرشون الجنسيين خداع الأطفال للالتقاء بهم بعيدا عن الإنترنت، إلى جانب إرسال صور إباحية خليعة لهم أو مطالبتهم بها، تأكد من أن أطفالك يدركون جيدا مخاطر التحدث مع الغرباء عبر الإنترنت وأكد عليهم عدم مشاركة المعلومات الشخصية مع أناس لم يقابلوهم من قبل.

7- الهجمات على المصارف : (ابوبكر سلطان، 2021)، أصبحت سرقة المصارف في القرن الحادي والعشرين عملية رقمية ، ومن الأمثلة الشهيرة على ذلك، قيام عصابة إجرامية بسرقة ما يصل إلى مليار دولار خلال عامين تقريبا من مجموعة متنوعة من المؤسسات المالية عبر العالم ، فقد استهدف المجرمون الإلكترونيون موظفي المصرف ومسؤولية برنامج ضار يسمى "Carbanak" عبر البريد الإلكتروني ، وبمجرد نجاحهم في إصابة الحواسيب المستهدفة، نجح المجرمون الإلكترونيون في محاكاة سلوك الموظفين وتحويل الأموال لأنفسهم وتوجيه ماكينات الصراف الآلي إلى صرف الأموال في أوقات محددة واستخدموا أنظمة الدفع الإلكترونية لسحب الأموال ،يقول بعض الخبراء، مثل Ben Lawskyإن الهجوم الكبير على النظام المصرفي قد يعادل "هجوم 9/11"ولكن في القطاع الإلكتروني .

- نماذج من أهم الهجمات السيبرانية: أصبحت المعلومة في القرن الحادي والعشرين العملة الرئيسية في العالم، حيث تتجه الدول والأفراد على نحو متزايد المعلومات وتكنولوجيا المعلومات، بما فيها تقنيات الحاسوب والاتصالات، وكذا جميع المؤسسات المدنية والعسكرية، وبالتالي أصبحت "الحروب السيبرانية" هي الأكثر بروزا وانتشارا على الساحة الدولية في الوقت الحالي.



الشكل (رقم 5) في أعلاه يوضح مخاطر جرائم المعلومات الشائعة. (أوس مجيد غالب العوادي، 2016)

المحور الثاني: أهم الآليات الإلكترونية الهجومية وأكثرها استخداما:

-الأسلحة الإلكترونية(الآليات): تشير الأسلحة الإلكترونية إلى تلك الأدوات التي يتم استخدامها للتهديد أو إحداث الضرر المادي أو الوظيفي للأجهزة أو النظم والهياكل الإلكترونية. وتختلف الأسلحة الإلكترونية من حيث درجة خطورتها وتعقيدها، وتتراوح ما بين أسلحة بسيطة قادرة فقط على إحداث ضرر خارجي بالنظام الإلكتروني دون اختراقه، وأخرى معقدة يمكن من خلالها اختراق النظام وإحداث أضرار بالغة به قد تصل إلى تدميره كليا أو توقفه عن العمل كلية، وفي النقاط التالية (Thomas Rid pp. 613)، نوضح أبرز أنواع الأسلحة الإلكترونية وأكثرها استخداما على الساحة الدولية.

-الحرمان من الخدمة: Denial of Service (DoS)هو ذلك الهجوم الذي يهدف إلى إيقاف قدرة الهدف على تقديم الخدمات المعتادة أو المفترض تقديمها، وذلك عن طريق إغراق جهاز الحاسب الآلي المقدم لل خدمةserver بكم كبير من الأوامر تؤدي إلى توقفه عن العمل وتقديم الخدمة لمستخدميها، أو الحد من قدرته على العمل بصورة طبيعية نتيجة لهذا الكم من الأوامر. وقد ينتج عن هذه الهجمات أيضا إيقاف الاتصال ما بين جهازين إلكترونيين أو منع شخص معين أو نظام معين من الوصول إلى الخدمة. وكثيرا ما تستخدم هجمات الحرمان من الخدمة كجزء من هجمات إلكترونية أكبر وأكثر تعقيدا (Stuart E.Madnick ،2009).

فالهدف الرئيسي من هجمات الحرمان من الخدمة هو إجبار النظام الإلكتروني المستهدف على الاستجابة لعدد كبير من الطلبات والأوامر الخدمية بشكل يفوق قدرته، مما يعوقه عن تقديم الخدمات المطلوب منه تقديمها. غير أن هذه الهجمات التقليدية قد لا تستطيع إحداث تأثير كبير في الأنظمة أو المواقع المجهزة للاستجابة لكم ضخم من الأوامر، مما يستدعي شكلا أكثر تعقيدا من هذه الهجمات وهو ما يعرف بهجمات الحرمان من الخدمة الموزعة Distributed Denial of Service attacks DDoS.

وفي معظم الأحيان لا يكون أصحاب الأجهزة التي تم اختراقها لاستخدامها في شن الهجوم على علم بذلك. كما يلاحظ أن الأجهزة المخترقة قد تتواجد في أية منطقة من العالم، ولا يشترط أن ترتبط جميعها بنطاق مكاني معين. ويشار إلى هذه الأجهزة التي تمت مهاجمتها بالأكواد والبرامج الخبيثة بعدد من المصطلحات أبرزها "zombies" أو "bots".

ولقد شهدت الساحة الدولية أكبر موجة من هجمات الحرمان من الخدمة في عام 2000، والتي نتج عنها إيقاف عدد من المواقع، ومنها Yahoo, Amazon, CNN,E Trade, ZDNet, Buy.com, Excite eBay (وذلك حسبما أعلنت تلك الجهات دون أن تعلن عن مصدر التهديدات أو الأهداف الكامنة وراءها). وتشير عديد من الدراسات إلى تزايد مستمر في استخدام هذا النوع من الأسلحة الإلكترونية. فعلى سبيل المثال، وفقا لتقرير صادر من مركز التنسيق الخاص بفرق الاستجابة لطوارئ الحاسب الآلي في الولايات المتحدة CERT Coordination Center، شهد عام 2001 وحده أكثر من 13 ألف هجوم من هجمات الحرمان من الخدمة الموزعة على أكثر من 5000 موقع إلكتروني مختلف تنتمي لأكثر من 2000 منظمة في مدة لا تتجاوز ثلاثة أسابيع (Jennifer A. Chandler. 2004) ، مما يدل على تصاعد وتيرة هذه الهجمات وحدتها واتساع نطاق تأثيرها.

وتتعدد الحالات التي تم فيها استخدام هجمات الحرمان من الخدمة على المستوى الدولي لدوافع وأهداف سياسية. ففي ظل نزاع كوسوفو في عام 1999، حاول بعض القراصنة أن يعطلوا العمليات العسكرية للناتو من خلال استخدام هجمات الحرمان من الخدمة الموزعة، واستطاعوا تحقيق نجاح، وإن كان محدودا (Mike McConnell. Op. cit. pp: 32-34).

وفي إبريل 2001، حدث توتر في العلاقات الأمريكية الصينية نتيجة إرسال الولايات المتحدة طائرة تجسس على الساحل الجنوبي للصين، وهو ما ردت عليه الصين بإرسال طائرة حربية اصطدمت مع الطائرة الأمريكية مما أدى إلى هبوط الطاقم الأمريكي اضطراريا على الأراضي الصينية واحتجاز الصين له، وهي الأزمة التي انتهت بجهود دبلوماسية من الطرفين. في تلك الفترة، وفي ظل توتر العلاقات ما بين البلدين، تعرضت المواقع الإلكترونية الخاصة بالجيش الأمريكي لهجمات الحرمان من الخدمة من قبل عدة جماعات صينية كان من بينها جماعة أطلق عليها Honker Union، وكذلك في عام 2007، تعرضت استونيا لعدد كبير من هجمات الحرمان من الخدمة والتي استهدفت البنية التحتية والمواقع الإلكترونية الخاصة برئيس الوزراء والبرلمان وعدد من الوزارات والبنوك. ولقد جاء ذلك في ظل الاضطرابات التي شهدتها إستونيا في تلك الفترة من الروس الموجودين في إستونيا وتوجيه الحكومة الروسية لانتقادات شديدة للحكومة الإستونية. وفي 2008، شنت الـ (سي أن أنCNN) حملة انتقادات ضد الصين بشأن ترتيبات استقبالها للأولمبياد، وهو الأمر الذي أغضب الصينين، وأدى إلى تعرض (سي أن أنCNN) إلى عدد ضخم من هجمات الحرمان من الخدمة لمحاولة إيقاف الموقع الإلكتروني الخاص بها، وهي الهجمات التي استخدمت فيها أكواد باللغة الصينية.

وفي أغسطس 2008، عندما اندلع نزاع مسلح ما بين جورجيا وروسيا، تعرضت جورجيا بالتزامن مع الهجمات العسكرية إلى هجمات الحرمان من الخدمة والتي استهدفت الموقع الخاص بالرئيس الجورجي، وعدد كبير من الوزارات، والمواقع الإخبارية. وفي أوكرانيا، وفي العام ذاته، وفي ظل التظاهرات المعارضة للانضمام إلى حلف شمال الأطلنطي، تعرضت عدد من المواقع الإخبارية في أوكرانيا إلى هجمات الحرمان من الخدمة والتي أتت من داخل الدولة.

واستخدمت هذه الهجمات أيضا ضد المواقع الإخبارية المعارضة للحكومة الروسية في 2008 نتيجة لنشرها أخبار عن انتشار الاحتجاجات على الأراضي الروسية. وفي عام 2009، في ظل الهجوم الإسرائيلي على حماس في غزة تعرضت إسرائيل وفلسطين لعدد هائل من هجمات الحرمان من الخدمة. وفي إيران أثناء الانتخابات الرئاسية في 2009 وما صاحبها من مظاهرات من المعارضة، تعرضت المواقع الحكومية لهجمات الحرمان من الخدمة، والتي أدت إلى توقفها عن العمل.

وفي يوليو 2009، تعرضت كوريا الجنوبية والولايات المتحدة إلى سلسلة من هجمات الحرمان من الخدمة التي استهدفت عددا من المواقع كان من بينها تلك الخاصة بالرئاسة. وتزامن ذلك مع قيام كوريا الشمالية باختبار صاروخي، وهو ما دفع البعض إلى القول بأن ذلك من جراء هذه الهجمات. (Jose Nazario. 2009).

وتظهر الأمثلة السابقة اتساع نطاق الاستخدامات الهجومية لهذه الآلية الإلكترونية، وانتشارها على المستوى الدولي، حيث باتت أحد أبرز التهديدات الإلكترونية القادرة على شل حركة الأنظمة الإلكترونية وتعطيل مصالح الدول والحكومات وحتى الأفراد والشركات والبنوك وغيرها من المؤسسات.

تتعدد أشكال التهديدات الالكترونية التي يتم فيها استخدام البرامج الخبيثة (الفيروسات، حصان الطراودة، الديدان، القنابل المنطقية، برامج التجسس).

وتقسم إلى أربع مجموعات رئيسية هي:

1-التجسس الالكتروني cyber espionage: هو القيام باختراق شبكة أو جهاز الكتروني بهدف سرقة المعلومات الموجودة عليه، والتي عادة ما تكون على درجة كبيرة من الأهمية، سواء أكانت معلومات عسكرية أم اقتصادية أم صناعية أم تجارية أم غيرها، وهو ما يترتب عليه آثار " إستراتيجية فادحة في الطرف المستهدف، فلقد غيرت التطورات التكنولوجية في العصر الحديث من طبيعة عمليات التجسس التقليدية، إذ توفرت الآليات الالكترونية والانترنت فرصا جديدة اقل تكلفة واقل خطورة للفواعل من الدول وغيرا لدول للقيام بعمليات التجسس.

وتوضح عديد من التقارير أن عمليات التجسس الالكتروني في تزايد مستمر، وفقا لأحد التقارير الأمنية الصادرة عن شركة ibmبلغ عدد عمليات التجسس الالكتروني حوالي 237مليون حالة على مستوى العالم في ستة أشهر الأولى من عام 2005 واظهر التقرير أن المؤسسات الحكومية هي الأكثر عرضة للتجسس الالكتروني، كما تأتي الو م ا على قمة قائمة الدول التي تتعرض لهذا النوع من الهجمات.

ففي النصف الأول من عام 2005 تعرضت الولايات المتحدة الأمريكية لأكثر من 12 مليون هجوم الكتروني بغرض التجسس.وتأتي في المرتبة الثانية في العالم وفي العام ذاته نيوزلندا (1.2 مليون هجوم)والصين (1مليون هجوم).

2-الجرائم الالكترونية: على الرغم من محورية مصطلح الجريمة الالكترونية **cyber crime**في عديد من الدراسات الأكاديمية التي تتناول التهديدات الالكترونية في العصر الحديث، إلا انه لا يوجد اتفاق على تعريف محدد لماهية الجريمة الالكترونية وعناصرها وأشكالها، ولكن بصفة عامة، يمكن تعريف الجريمة الالكترونية على أنها تلك الجريمة التي يتم فيها استخدام الآليات والأسلحة الالكترونية السابق ذكرها للقيام بهجوم الكتروني بهدف تحقيق مكاسب مالية بالأساس.

وتتعدد أشكال الجرائم الالكترونية التي يتعرض لها الأفراد والمنظمات والدول، ونوضح أهمها كالتالي:

أ-سرقة الهوية: من أبرز أشكال الجرائم الالكترونية وأكثرها خطورة جريمة سرقة الهوية **Identity theft**. وتشير سرقة الهوية إلى تلك العمليات التي يتم من خلالها سرقة معلومات شخصية عن الهوية تستخدم لاحتيال والقيام بأعمال غير قانونية واستغلال هذه المعلومات لتحقيق مكاسب مالية، فعند إصابة جهاز الحاسب الآلي بأحد البرامج الخبيثة، قد يقوم هذا البرنامج بالبحث في الجهاز عن بيانات شخصية، مثل الاسم أو العنوان أو مكان الميلاد وكشوف حسابات البنوك وسرقة الأموال.

فعلى سبيل المثال، حدثت في الفترة ما بين يناير 2005و مارس2008، بعض الاختراقات الأمنية في الولايات المتحدة الأمريكية حيث وصلت سرقة بيانات على درجة كبيرة من الأهمية لأكثر من218مليون فرد.وقد صرح في يوليو 2006 مسؤولون في وزارة الطاقة بالولايات المتحدة عن سرقة بيانات شخصية لأكثر من 1500 موظف يعمل بإدارة الطاقة النووية الوطنية **National Nuclear Security Administration** في اختراق لشبكة الإدارة منذ عام2004 ولم يتم اكتشافه سوى عام2006. **(Clay Wilson. Op.cit. pp: 418-426.)**.

وتشير البيانات إلى خطورة هجمات سرقة الهوية ليس فقط من حيث ازديادها، ولكن أيضا من حيث الخسائر المترتبة عليها، فعلى سبيل المثال، قدرت الخسائر المترتبة على سرقة الهوية في المملكة المتحدة بـ 1.3 مليار جنيه إسترليني سنويا، وفي

استراليا ما بين مليار و3 مليار دولار سنويا، وفي الولايات المتحدة وصلت إلى 56.5 مليار دولار في عام 2006 فقط. (Marco Gercke2012. P 5.).

ب-هجمات الاختراق: تعرف هجمات الاختراق **Penetration Attacks** بتلك الهجمات التي يتم من خلالها الدخول غير المشروع إلى الأنظمة الآلية وتخطي نظام التامين الخاص بها، وفي حالات الاختراق الكامل يتمكن المهاجم من السيطرة الكاملة على الحاسب الآلي، وتغيير البيانات أو تبديلها، أو زرع برامج خبيثة داخل الجهاز.

وفي بعض الحالات يقوم المخترق **Intruder** باستخدام الحاسب الآلي الذي تم اختراقه كأداة لشن هجوم الكتروني على جهاز أخر خاصة وان كانا متصلين بشبكة واحدة، يتطلب هذا النوع من الهجمات جمع معلومات حول النظام او الشبكة التي سيتم اختراقها، والتعرف على أنظمة التامين والتشغيل الخاصة بها، ومحاولة استغلال نقاط الضعف فيها وذلك لتسهيل اختراقها.

ومن أبرز الأمثلة على هذه الهجمات ما أعلنته وزارة الدفاع الأمريكية (البنتاغون) في عام 1996 بان هناك ما يقرب من 250.000 محاولة لاختراق أنظمة الحاسب الآلي الخاصة بالوزارة، وان 85بالمائة من هذه الهجمات قد نجحت بالفعل، كما أعلن البنتاغون أن هناك ما يقرب من 150 من القراصنة Hackersقد تم القبض عليهم بتهمة التخطيط لاختراق أنظمة الحاسب الآلي الخاصة بالقوات الجوية الأمريكية، وكذلك في عام 1998، تم اختراق عدد كبير من أجهزة الحاسب الآلي كان من بينها أنظمة الحاسب الآلي الخاصة بالبنتاغون ووكالة ناسا. (هاني خميس أحمد. إبريل 2007).

ج-الاحتيال عبر الانترنت: الاحتيال عبر الانترنت **Internet fraud**هو نوع من الاحتيال يتم فيه استخدام الانترنت ووسائطه المختلفة كالمواقع الالكترونية والبريد الالكتروني للقيام بعمليات احتيالية لتحقيق مكاسب مالية، وبسبب تزايد أعداد المستخدمين للأنترنت على مستوى العالم، ازدادت مخاطر تعرض الأفراد والشركات والمنظمات والحكومات لعمليات الاحتيال عبر الانترنت. (National White 2008.).

وتتعدد أشكال جرائم الاحتيال عبر الانترنت ومن أهمها القيام ببيع سلع وهمية **Rogue Traders**أو سرقة معلومات البطاقات الائتمانية واستخدامها **Credit Card Fraud**، أو توجيه المستخدم الو موقع خاطئ الغرض منه التحايل **Pharming**، او اصطياد الاحتيالي **Phishing** والذي يتعرض فيه الأفراد للخداع عن طريق توجيههم إلى مواقع يتم فيها الحصول على أكبر قدر من المعلومات الخاصة بهم، ثم استخدامها من قبل القائم بالجريمة لتحقيق مكاسب مالية. (Abdullah M. Alnajim 2009 pp: 10, 11).

ومن أشهر الاختراقات الإلكترونية "السيبرانية" تلك التي حازت على أوساط شبكات التواصل الاجتماعي والشوارع الأمريكية وهي قضية التأثير على الانتخابات الأمريكية عام 2016.

3-الإرهاب الالكتروني: وفقا للتعريف الذي قدمته دوروثي دينينج **Dorothy E.Dennning**، أحد أبرز الباحثين في مجال الأمن الالكتروني، يجمع مصطلح الإرهاب الالكتروني **Cyber Terrorism** ما بين مفهوم "الإرهاب" و "الفضاء الالكتروني"، ومن ثم فهو يشير إلى الاعتداءات والتهديدات الموجهة لأجهزة الحاسب الآلي والشبكات الالكترونية والمعلومات الموجودة عليها بهدف إجبار الحكومات والمجتمعات على أفعال معينة لأغراض سياسية أو اجتماعية.

ولكن يشترط لكي يصنف هجوم ما بأنه إرهاب الكتروني أن ينتج عنه أضرار بالممتلكات أو الأفراد وخلق حالة من الخوف لدى الهدف، ومن ثم تخرج الهجمات التي تستهدف خدمات ليست على درجة كبيرة من الأهمية خارج إطار مفهوم الإرهاب الالكتروني، إذ لابد وأن يكون الهدف حيويا وهاما بالنسبة لحياة المواطنين ولعمل الدولة، ويضاف إلى ذلك أن هجمات الإرهاب الالكتروني لابد وأن تكون مدبرة ومخطط لها سابقا وتهدف إلى تدمير الهدف أو إلحاقه بدرجة عالية من الضرر، وليس فقط أحداث خلل في عمله.

ولذا باتت مكافحة الإرهاب الالكتروني على قمة أولويات الدول، إذ أصبح هناك عديد من المؤسسات التي تطور من برامج وتجرى أبحاث في هذا المجال، كما تخصص الدول نسبا كبيرة من ميزانياتها لمجال مكافحة الإرهاب الالكتروني، ولم تقتصر

استراتيجيات التامين الالكتروني على الدول فقط، وإنما شملت أيضا الشركات والمنظمات، والتي بدت بدورها اهتماما كبيرا بحماية أنظمتها الالكترونية من الجرائم ولاعتداءات المماثلة.

وهناك عدة أسباب أدت إلى لجوء الجماعات لإرهابية استخدام الفضاء الالكتروني والآليات الالكترونية للقيام بعمليات إرهابية وتتمثل أهمها فيما يلي:

1- تنخفض تكلفة الآليات الالكترونية مقارنة بالأدوات التقليدية التي تتم بها العمليات لإرهابية كالقنابل و المتفجرات و لأسلحة المتطورة.

2- في الكثير من لأحيان يصعب على أجهزة الشرطة ملاحقة القائمين بعمليات لإرهاب الالكتروني و التعرف على هويتهم فضلا عن عدم وجود حواجز جغرافية في مجال الفضاء الالكترونية تعوق أنشطتهم.

3- كما أن الفضاء الالكتروني يوفر للإرهابية أهدافا متعددة يستطيعون مهاجمها لتحقيق أهدافهم ، فقد الجماعات لإرهابية بمهاجمة شبكات الحاسب الآلي الخاصة بالحكومات ، أو الشركات الخاصة أو الأفراد مما يفتح المجال أمام هذه المنظمات للبحث عن ثغرات في هذه الأنظمة الالكترونية المتعددة لمهاجمتها.

4-لا تحتاج هجمات لإرهاب الالكتروني إلى تواجد المهاجم و الهدف في المكان ذاته ، فالهجمات الالكترونية يمكن أن تتم عن بعد ، مما يسهل من أمكانية اجتذاب أعضاء جدد للمنظمات لإرهابية دون الحاجة إلى إجراء تدريبات بدنية أو نفسية لهم ، أي أن الفضاء الالكتروني صار يوفر ساحة جديدة لتجنيد للجماعات لإرهابية.

5-تستطيع هجمات لإرهاب الالكتروني أن تلحق الضرر بعدد أكبر من الأفراد مقارنة بالهجمات التقليدية، وهو ما يساعد الجماعات لإرهابية على جذب مزيد من الاهتمام لإعلامي والحكومي بشكل يساعدها على تحقيق أهدافها بصورة أكثر فاعلية. (Gabriel Weimann December.2004 pp:2-6.).

الشكل رقم :6 أقوى جرافيك: أقوى 5 هجمات إلكترونية في العالم

تعتبر القرصنة والهجمات الإلكترونية من أسلحة العصر الحديثة، التي تتسبب بخسائر مختلفة تتكبدها دول ومؤسسات خاصة.

وتختلف الهجمات الإلكترونية في غاياتها، وتتبنى دول إنشاء مؤسسات يديرها مختصون تعنى باختراق حسابات وأجهزة كمبيوتر تابعة لحكومات دول أخرى؛ بعضها للاستيلاء على معلومات حساسة، وأخرى لتكبدها خسائر مالية ، وعرف العالم في السنوات القليلة الماضية هجمات إلكترونية عديدة، اختلفت في حجمها وقوة تأثيرها.

فريق الملتيميديا في "الخليج أونلاين" بين في الإنفوجرافيك المرفق أقوى 5 هجمات إلكترونية عرفها العالم.

4-الحرب الالكترونية: تشير الحرب الالكترونية Cyber war إلى تلك الحرب التي تتم إدارتها في مجال الفضاء الالكتروني والتي تكون الفواعل الرئيسية فيها هي الدول ويتم فيها استخدام الآليات والأسلحة الالكترونية في الهجوم، ويكون هذا الهجوم موجه بالأساس إلى أجهزة الحاسب الآلي أو الشبكات الالكترونية الخاصة بالعدو أو الأنظمة الالكترونية التي تدير الدولة وما تحتوي عليه من معلومات بهدف عرقلة الخصم عن استخدام هذه الأنظمة والأجهزة والشبكات أو تدميرها بالكامل. (Klaus-Peter Saalbach2013.pp:4-7.).

وقد تتم الحرب الالكترونية في صورتها التقليدية أي بين القوات المسلحة الخاصة بالدول، أو ما بين الجهات الرسمية أو الغير رسمية داخل الدولة، أو من الفواعل من غير الدول، وقد تكون الحرب الالكترونية أيضا جزء من حرب شاملة في البر والبحر والجو، وعلى الرغم من تعدد الصراعات الالكترونية في العصر الحديث، إلا إن حربا الكترونية حقيقة شاملة لم تحدث بعد. (Kristin M. Lord.p:19.).

وبشكل عام، يمكن تحديد ثلاثة مستويات رئيسية للحرب الالكترونية:

-المستوى الأول يتمثل في تلك العمليات المصاحبة للحروب التقليدية لتحقيق التفوق المعرفي كمهاجمة نظام الدفاع الجوي ، و الذي قد يؤدي إلى خسائر إستراتيجية واسعة النطاق نتيجة لأهمية الدفاع الجوي بالنسبة للدول.

-المستوى الثاني يتمثل في الحرب الالكترونية المحدودة ، و التي تتعرض فيها البنى التحتية و الأهداف المدنية للهجمات الالكترونية.

-المستوى الثالث يتمثل في الحرب الالكترونية غير المحدودة و التي يسعى من خلالها القائم بالهجوم إلى تعظيم الأثر التدميرية للبنى التحتية ، حيث يؤثر سلبا في البناء الاجتماعي للدولة كمهاجمة أسواق رأس المال ، و خدمات الطوارئ ، و الأنظمة الالكترونية الخاصة بمولدات الطاقة، ويكون الهدف في هذا النوع من الحروب هو توسيع نطاق الخسائر المادية قدر الإمكان. (Kenneth Geers. 2011. p26.).

المحور الثالث: مصادر التهديدات الالكترونية للدول:

يتضح مما سبق عرضه من الأشكال المختلفة للتهديدات الالكترونية انه لم يعد القيام بالهجمات الالكترونية مقصورا فقط على القراصنة الذين يعملون بصورة فردية أو جماعية أو الجماعات الإجرامية التي تهدف لتحقيق مكاسب مالية، ونما تتسع دائرة القائمين بتلك الهجمات لتشمل أيضا الدول القومية، والتي قد تلجا إلى الهجمات الالكترونية كإحدى أدوات السياسة الخارجية، وقد تتعاون أيضا الدول مع فواعل أخرى عن طريق تقديم الدعم المالي والتقني لإتمام هجوم الكتروني ضد هدف معين بما يتفق مع مصالحها.

وبصفة عامة، يمكن تقسيم الفواعل في الفضاء الالكتروني ومن لديهم القدرة على شن هجمات الكترونية إلى ثلاث فئات رئيسية وتتمثل في:

1-الدول: وتمثل الدول الخطر الأكبر والفاعل الأكثر قوة في مجال الفضاء الالكتروني، ففي عام 2008 استطاعت حوالي 180دولة أن تمتلك ترسانة من الأسلحة الالكترونية، مما قد يدفع الفواعل من الدول وغير الدول للتنافس في السنوات القادمة من اجل تحقيق التفوق الالكتروني.

نتيجة لما يقدمه الفضاء الالكتروني من فرص للفواعل لتحقيق مصالحهم، تسعى عديد من الدول إلى تطوير قدرتها في هذا المجال.

وتنقسم القدرات الالكترونية للدول بشكل عام إلى قدرات دفاعية وأخرى هجومية، ولكن أضاف كل من: ريتشارد كلارك Richard Clarke والذي عمل منسقا سابقا لشؤون الأمن وحماية البنية التحتية، ومكافحة الإرهاب للرئيس رونالد ريغن،

وبوش الأب والابن، وبيل كلينتون – وروبيرت كناك **Robert Knacke** في كتابهما عن الحرب الالكترونية باعتبارها الخطر القادم الذي يهدد الأمن القومي للدول، بعدا أخر يرتبط بمدى اعتماد الدول على الفضاء الالكتروني في إدارة شؤون الدولة. وعليه تزيد قدرات الدولة في المجال الالكتروني كلما زادت قدراتها الهجومية والدفاعية، وقل اعتمادها نسبيا على الفضاء الالكتروني مقارنة بغيرها من الفواعل، ولقد قدم الكاتبان تقييما للقدرات الالكترونية لخمسة دول اعتبرا انها تمثل القوى الالكترونية الأهم على مستوى العالم في الجدول التالي:

الجدول: القدرات الالكترونية للدول (Richard A. Clarke e Rober K. Knake.2010 pp147-149.): من إعداد الباحث.

الدولة	الهجوم الالكتروني	الاعتماد على الفضاء الالكتروني	الدفاع الالكتروني	المجموع
الولايات المتحدة	8	2	1	11
روسيا	7	5	4	16
الصين	5	4	6	15
إيران	4	5	3	12
كوريا الشمالية	2	9	7	18

يلاحظ من الجدول أعلاه انه كلما زادت قدرات الدولة الهجومية و الدفاعية ، زادت نقاطها في هذين البندين، ولكن كلما زاد اعتماد الدولة على الفضاء الالكتروني ، قلت النقاط التي تحصل عليها في هذا البند ، وذلك لما يترتب على هذا الاعتماد من قابلية تعرض الدولة للهجمات الالكتروني، وزيادة فداحة و جسامة الأضرار التي قد تلحق بها حال وقوع هذا الهجوم ، أي أن الكاتبان نظرا لزيادة اعتماد الدولة على الفضاء الالكتروني نظرة سلبية لأنها ستقلل من قدرتها على حماية أمنها الالكتروني ، كما يلاحظ أن هذا الاعتماد الالكتروني لا يقصد به عدد المواطنين المستخدمين للأنترنت، أو عدد الحواسب الآلية على المستوى القومي، ولكن مدى اعتماد المؤسسات الرسمية للدولة على الفضاء الالكتروني خاصة في إدارة البنية التحتية.

ووفقا للجدول الذي قدمه الكاتبان، تأتي الولايات المتحدة في المرتبة الأولى من حيث القدرات الهجومية إلا أنها أيضا أكثر دول العالم اعتمادا على الفضاء الالكتروني في إدارة الدولة، مما يزيد من قابليتها للتعرض للهجمات الالكترونية، ولذا حصلت على ادني رقم في بند الاعتماد على الفضاء الالكتروني، في حين أنها الأقل من حيث القدرات الدفاعية، ولذا تأتي في المرتبة الأخيرة من حيث المجموع الكلي للقدرات الالكترونية.

2-الفواعل من غير الدول: يفوق الدور الذي تلعبه الفواعل من غير الدول في مجال الفضاء الالكتروني دورها في أي مجال أخر، سواء من حيث قدرتها على التفاعل أم التأثير في امن الدول، ويرجع ذلك إلى عدد من العوامل من أبرزها انخفاض تكلفة الدخول في مجال الفضاء الالكتروني وعدم وجود حواجز تعوق قدرتها على أن تلعب دورا بارزا فيه، إذ أن الأدوات التقنية والتكنولوجية اللازمة للقيام بهجمات الكترونية من الممكن التوصل إليها بسهولة من خلال شبكة الانترنت.

ومن ثم، يتمكن الفواعل من غير الدول من امتلاك هذه القدرات الالكترونية الهجومية بتكلفة منخفضة مما يمكنهم من شن هجمات، سواء على دول أم على فواعل أخرى من غير الدول، ولكن يلاحظ أن الدول لا تزال هي الفاعل الأكثر قوة وقدرة على شن هجمات الكترونية معقدة قد لا يستطيع اغلب الفواعل من غير الدول القيام بها.

ا- المنظمات غير الحكومية: لا تقتصر مصادر الهجمات الالكترونية على الدول فقط، وإنما قد تأتي أيضا من الفواعل من غير الدول كالمنظمات غير الحكومية ، وان كانت لا تمتلك القدرات ذاتها التي تمتلكها الدول و الحكومات للقيام بهجمات الكترونية معقدة ، فقد تقتصر قدراتها على مهاجمة أهداف قليلة الأهمية نسبيا كالمواقع الالكترونية، فالهجمات الالكترونية المعقدة الموجهة لأهداف على درجة كبيرة من الأهمية كنظم الاتصالات الدفاعية لابد و أن تتم من خلال أجهزة المخابرات التابعة للدول والتي تمتلك من لإمكانات ما يؤهلها لخرق الأكواد المشفرة الخاصة بهذه الأنظمة.

ب-الأفراد: هناك فئات أربعة رئيسية للأفراد القادرين على شن هجمات الالكترونية نوضحها كالتالي:

1- المبتدئون Novicesتمتلك هذه الفئة قدرات برمجية محدودة ، ومن ثم فالهجمات التي يقومون بها تكون غير معقدة ، ويقومون فيها باستخدام لغة برمجية مكتوبة سابقا ، لا يقومون هم بكتابتها ، و يكون الهدف الرئيسي لقيام المبتدئين بهذه الهجمات هو تحقيق المغامرة و الإثارة و أن يتم تقبلهم في مجتمع القراصنة ، و على الرغم من أن إمكاناتهم المحدودة تحد من الآثار المترتبة على الهجمات التي يقومون بها، إلا أن ظهور عدد كبير من الأدوات Toolkitsالتي تتسم بدرجة عالية من التعقيد و التي أصبحت متاحة على نطاق واسع يزيد من قدراتهم القيام بهجمات الكترونية أكثر تعقيدا.

2-القراصنة :Hackersويسعى القراصنة إلى محاولة الوصول إلى البيانات والملفات والأنظمة المشغلة للحواسب الآلية وذلك بهدف تعطيل وتدمير شبكات الحاسب الآلي من خلال هجمات معقدة ومنظمة (Mike McConnell. Op. cit. pp: 27-31.) ، وتختلف أراء المحللين حول مدى خطورة هجمات القراصنة، فالبعض يعتبر أنها ليست على الدرجة ذاتها من الخطورة والأهمية مقارنة بالتهديدات السابق ذكرها، غير أن البعض يعتبر أنها لا تقل أهمية عن التهديدات السابقة خاصة، وأنها كثيرا من لأحيان ما تكون أحد مكونات القيام بما سبق ذكره من تهديدات، وعادة ما تكون أهداف القراصنة هي تحقيق الشهرة مكاسب المالية. (Paul Comish pp:7-11.).

3-القرصنة السياسية: يجمع مصطلح الهاكتفيزم ktivism ا والقرصنة السياسية ما بين مصطلح القرصنة الالكتروني Hack والنشاط السياسي أوActivism، وتكون الدوافع الرئيسية وراء قيام القراصنة السياسيين Hacktivists بالهجمات الالكترونية هي دوافع سياسية بالأساس، وليس بهدف تحقيق منافع شخصية، ويستند القراصنة السياسيون إلى هجمات الحرمان من الخدمة بشكل كبير وفي بعض لأحيان يلجئون إلى استخدام الفيروسات والديدان.

4-جماعات الإرهاب الالكتروني: تتشابه جماعات لإرهاب الالكتروني Cyber Terrorists مع القراصنة السياسيين في نوع الهجمات التي يقومون بها، إذ انه حماتهم ما تكون مدفوعة بأهداف سياسية، غير أن نطاق الهجمات التي يقومون بها تختلف عن القراصنة، فالهدف الرئيسي الذي يسعى لإرهابيون الالكترونيين إلى تحقيقه هو إلحاق الضرر بأهداف تمثل أهمية كبرى بالنسبة للدولة والمجتمع سواء اقتصاديا أم سياسيا أم تجاريا، الخ. في حين يكون هدف القراصنة السياسيين هو فقط الضغط السياسي دون أحداث أضرار بالغة بالضرورة.

وتستغل المنظمات لإرهابية الانترنت في عدة صور كالتالي:

1-فهي تقوم باستخدامه باعتبار انه وسيط لتحقيق التواصل فيما بينها مع التمتع بدرجة كبيرة من السرية، ومن ثم يستطيع أعضاء هذه المنظمات تناقل المعلومات والأوامر فيما بينهم وتداول الأوامر التنفيذية، والتخطيط للهجمات فضلا عن القيام بحملات لجمع لأموال لتنفيذها، وبما أن لانترنت يعتبر وسيطا لتحقيق الاتصال، فان الانترنت أيضا قد يتم استخدامه للدعاية، فهذه المنظمات والجماعات لإرهابية كثيرا ما تقوم باستخدام الانترنت للدعاية لنفسها من خلال نشر بعض المعلومات والبيانات والفيديوهات الخاصة بها.

2-كما أن الانترنت حاليا يوفر لمختلف المنظمات والجماعات أو حتى الأفراد المعرفة التكنولوجية اللازمة للقيام بالهجمات الالكترونية ولذلك يعتبر البعض أن الانترنت قد أصبح بمثابة معسكر تدريب افتراضيVirtual Training Camp للإرهابيين لامتلاك القدرات التكنولوجية اللازمة للقيام بالهجمات الالكترونية.

الخاتمة:

بات من الواضح انه لتعزيز التعاون الدولي في مجال مكافحة الجرائم السيبرانية وحماية الأنظمة السيبرانية من التهديدات العابرة للحدود، يمكن اتخاذ عدة إجراءات:

يجب تعزيز آليات التبادل الفعالة والآمنة للمعلومات بين الدول. يمكن تحقيق ذلك من خلال إنشاء قنوات اتصال مباشرة وآمنة بين الجهات المختصة في الدول المختلفة، مثل مراكز لأمن السيبراني ووحدات التحقيق الجنائي والمؤسسات الحكومية ذات العلاقة ، وأن تعمل الدول على تحديد وتنفيذ تشريعات وسياسات تعزز مكافحة الجرائم السيبرانية وتحمي الأنظمة السيبرانية من خلال تطوير إطار قانوني مشترك يتضمن تعريفات موحدة للجرائم السيبرانية وآليات للتحقيق والمساءلة و دعم بناء قدرات الدول في مجال لأمن السيبراني، بما في ذلك تطوير المهارات التقنية والتحقيقية والتدريب، وتعزيز الوعي السيبراني لدى الموظفين و الجمهور و يمكن تبادل الخبرات والمعرفة بين الدول وتقديم الدعم الفني والتقني للدول التي تحتاج إلى تعزيز قدراتها.

وأيضا تعزيز التعاون في التحقيقات الجنائية للجرائم السيبرانية العابرة للحدود، وتشكيل فرق تحقيق مشتركة بين الدول أو تعزيز التعاون بين وحدات التحقيق الجنائي لمكافحة الجرائم السيبرانية، كما يجب تعزيز التعاون في تسليم المجرمين والأدلة الرقمية عبر الحدود لمساعدة في تحقيق العدالة.

وتعزيز الشراكات بين الحكومات والقطاع الخاص والمؤسسات الأكاديمية والمجتمع المدني، يمكن للقطاع الخاص تقديم الدعم التقني والخبرات في مجال لأمن السيبراني، ويمكن للمؤسسات الأكاديمية تطوير البحث والتدريب في هذا المجال، وإبرام اتفاقيات دولية لمكافحة الجرائم السيبرانية وتعزيز الحماية السيبرانية. يمكن أن تتضمن هذه الاتفاقيات التعاون في تحقيق العدالة، وتسليم المجرمين، وتطوير معايير لأمن السيبراني.

أيضا تعزيز التنسيق والتعاون السريع في استجابة لأمن السيبراني للتهديدات العابرة للحدود. يمكن إنشاء آليات للتبليغ السريع وتبادل المعلومات في حالات لاختراق السيبراني أو الهجمات الضارة والانضمام إلى منظمات دولية مثل لأمم المتحدة والاتحاد الأوروبي ومنظمة الشرطة الجنائية الدولية (الإنتربول) وغيرها، التي تعمل على تعزيز التعاون الدولي في مجال مكافحة الجرائم السيبرانية.

وأخيرا يمكن تعزيز التعاون الدولي في مجال مكافحة الجرائم السيبرانية يتطلب التزاما قويا من الدول وتبني إجراءات وآليات فعالة للتعاون والتنسيق. من خلال تبادل المعلومات وتوحيد السياسات وتعزيز القدرات وتعاون التحقيقات، يمكن للدول أن تعزز قدرتها على مواجهة التهديدات السيبرانية العابرة للحدود وحماية الأنظمة السيبرانية الحيوية.

ومن بين أهم التوصيات التي تنتهي إليها هذه الورقة البحثية:

-عدم وجود قوانين وتشريعات فعالة : قد يواجه الدول صعوبة في التعامل مع الجرائم السيبرانية بسبب عدم وجود تشريعات قوية وفعالة تتعامل بشكل صحيح مع هذه الجرائم وتحدد العقوبات المناسبة.

-التعاون الدولي المحدود: قد يكون التعاون الدولي في مجال مكافحة الجرائم السيبرانية غير كافي، حيث يمكن للمجرمين القامعين للجرائم السيبرانية استغلال الفجوات في التعاون الدولي والانتقال بسهولة بين الدول لتنفيذ أعمالهم.

- تقنيات التشويش والتمويه: يستخدم المهاجمون التقنيات المتقدمة لتشويش الأدلة وتمويه أنشطتهم السيبرانية، مما يجعل من الصعب تحديد هويتهم وتتبعهم. هذا يزيد من تعقيد مهمة التحقيق وتقديمهم للعدالة.

-نقص المهارات والخبرات: تواجه الكثير من الدول نقصا في المهارات والخبرات الفنية اللازمة لمكافحة الجرائم السيبرانية. قد يكون من الصعب تدريب الكوادر البشرية المؤهلة وتوفير الموارد اللازمة لمجابهة هذه التهديدات.

-التهديدات الجديدة والمتطورة: يتطور مجال الجرائم السيبرانية بشكل مستمر، حيث يبتكر المهاجمون تقنيات جديدة وأساليب متطورة للتسلل والاختراق. هذا يتطلب من الدول والمؤسسات البقاء على اطلاع دائم على التهديدات الجديدة وتحديث استراتيجياتها وأدواتها لمكافحتها.

-التأثيرات الاقتصادية والاجتماعية: تتسبب الجرائم السيبرانية في تكاليف هائلة على المستوى الاقتصادي والاجتماعي، بما في ذلك فقدان البيانات والمعلومات الحساسة، وانتهاك الخصوصية، وتعطيل الخدمات الحيوية. قد يكون من التحديات التحكم في اشكالية الموضوع هي أن الجرائم السيبرانية والتهديدات الأمنية تتجاوز الحدود الجغرافية وتؤثر على الأفراد والدول بشكل عابر. هذا يعني أنه من الصعب على الدول التعامل مع هذه الجرائم بشكل فعال منفردة، ويتطلب التعاون الدولي والتنسيق الشامل لمكافحتها. بعض الاشكاليات المرتبطة بذلك تشمل:

-صعوبة تعقب المجرمين عبر الحدود: قد يكون من الصعب تحديد هوية المهاجمين وتتبعهم عبر الحدود، خاصة عندما تكون هناك فجوات في التعاون القانوني والتحقيقي بين الدول.

-مشاكل في تبادل المعلومات: قد تواجه الدول صعوبات في تبادل المعلومات ذات الصلة بالجرائم السيبرانية والتهديدات الأمنية بسبب القيود القانونية والتقنية والسياسية.

-تعددية الأطراف المشاركة: يشارك في مجال الجرائم السيبرانية والتهديدات الأمنية مجموعة متنوعة من الأطراف، بما في ذلك الدول، والمجموعات الإجرامية، والهاكرز، والشركات الخاصة. هذا يزيد من تعقيدات المكافحة والتعاون الدولي.

-تنوع الأهداف والأساليب: تختلف الجرائم السيبرانية في أهدافها وأساليبها، وتشمل اختراقات السيبرانية، والاحتيال الإلكتروني، وسرقة الهوية، والتجسس، والهجمات الضارة. يتطلب ذلك تبني استراتيجيات متعددة لمكافحة هذه التهديدات المتنوعة.

-التحديات التقنية والتكنولوجية: يتطور المجال السيبراني بشكل سريع، وقد يواجه الدول صعوبات في مواكبة التطورات التكنولوجية وتحديث أنظمتها وتكنولوجياتها الأمنية للتصدي للتهديدات الجديدة.

-التأثيرات الدولية والاقتصادية: تؤثر الجرائم السيبرانية على الأمن الدولي والاقتصاد العالمي، وتتسبب في خسائر مالية هائلة وتهديد للاستقرار الاقتصادي والسياسي للدول.

-مواجهة هذه الاشكاليات يتطلب تعزيز التعاون الدولي، وتبادل المعلومات والخبرات، وتحسين القدرات التقنية والتحقيقية.

قائمة المراجع:

أولا: مراجع باللغة العربية

الكتب:

[1]-إيهاب خليفة، القوة الالكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الانترنيت، دار العربي، 2017.

[2]-ايهاب خليفة، القوة الإلكترونية وأبعاد التحول في خصائص القوة، مكتبة الإسكندرية مصر، 2014.

المقالات ومجلات:

[1]- أبوبكر سلطان ، الرعاية الصحية الذكية، مجلة ثقافية منوعة يناير – فبراير . 2021

المطبوعات:

[1]-محمد. مختار، " الأمن السيبراني"مفاهيم المستقبل،اتجاهات الأحداث، العدد 6، 2015.

[2]-أوس مجيد غالب العوادي، الأمن المعلوماتي السيبراني، مركز البيان للدراسات والتخطيط، أوت 2016

ثانيا: باللغة الأجنبية:

A.Books :

1-Richard A. Kemmerer، Cyber security، University of California Santa Barbara, Department of Computer Science, 2003.

2-Jennifer A. Chandler. (2004). Security in Cyberspace: Combatting Distributed Denial of Service Attacks. University of Ottawa Law & Technology Journal, Vol. 1,
3-Jose Nazario. (2009). Politically Motivated Denial of Service Attacks. In Christian Czosseck & Kenneth Geers (eds.), the Virtual Battlefield: Perspective on Cyber Warfare.IOS Press.
4-Thomas Rid & Peter McBurney. (March 2012). Cyber-weapons. Rusi Journal, Vol. 157 No., dur.ac.uk/2149/.
5-Gabriel Weismann. (December.2004). Cyber terrorism: How real is the threat? United of peace report
6-Klaus-Peter Saalbach. (March.2012). Cyber Wer Methods and Practice.lv Internet Policy.Version 4.0 RL: http://www.dirk-Koentopp.com/downloads/saalbach-cyberwar-methods-and-practice.pdf.Accessed on: 22April.2013.
7-Kenneth Geers. (2011).Strategic Cyber Security.NATO Cooperative Cyber Defence Centre of Excellence.
8-Richard A. Clarke e Rober K.Knake. (2010).Cyber War:the Next threat to National Security and What to Do About IT.Harper Collins Publisher.
Ellis. *The International Legal Implications* **:**

E. Web Sites:
[1]-Stuart E.Madnick et al. (2009). Explorations in Cyber International Relations (ECIR) – Data Dashboard Report number 1: CERT Data Sources and Prototype Dashboard System. MIT Sloan Research Paper No. 4754-09. URL: http://ssrn.com/abstract=1477618.
[2] -Marco Gercke. (November 2007). Internet-related Identity Theft. Discussion Paper Prepared for the Project on Cybercrime of the Council of Europe. URL: http://www.coe.int/t/dghl/cooperation/ economiccrime/cybercrime/documents/reportspresentations 2007.pdf. Accessed on 7 August 2012.
[3]-National White Collar Crime Center. Internet Fraud. (June 2008). URL: http://www.nw3c.org/docs/whitepapers/internet_fraud.pdf?sfvrsn=7. Accessed on: 19 February 2013.
[4]-Abdullah M. Alnajim. (2009). Fighting Internet Fraud: Anti-phishing Effectiveness for Phishing Websites Detection, *Durham Thesis***. Durham University. Available at Durham E-Thesis Online: http://etheses.**

الجرائم السيبرانية و آليات مواجهتها في الجزائر

Cybercrimes and the Fight Against Them in Algeria

محمد لسعد سيد عمر جامعة غرداية lassaad.medsidomar@univ-ghardaia.dz.

ملخص:

لقد كان للتطور الكبير و الانتشار الواسع الذي شهدته التكنولوجيات الحديثة للإعلام و الاتصال الأثر الإيجابي سواء في العلاقات التي تربط الافراد بعضهم ببعض أو حتى على مستوى المؤسسات الحكومية، و هذا بفضل استعمال هذه التكنولوجيات بالشكل الأمثل و في حدود لا تضر بالآخرين أو بأمنهم ، إلا أن هذا التطور صاحبته و لازمته تهديدات أمنية مختلفة الأشكال تحول دون الاستخدام الأمثل لهذه التكنولوجيات أو تسبب تهديدا مباشرا للأفراد أو المؤسسات العمومية.

وفي هذه الدراسة سلطنا الضوء على بعض المفاهيم المتعلقة بمصطلح الجريمة السيبرانية، سواء تعلق الامر بمفهومها أو أركانها بالإضافة خصائصها المميزة لها . كما تطرقنا إلى الآليات الموضوعة القانونية و المؤسساتية و القضائية من اجل مجابهة و مواجهة الجرائم السيبرانية التي يتعرض لها أمن تكنولوجيا المعلومات في الجزائر ، فضلا عن مدى فعاليتها.

الكلمات المفتاحية : الامن السيبراني ، الجريمة السيبرانية ، الجريمة الالكترونية ، السلوك الاجرامي ، معلوماتية

Abstract: The significant development and widespread adoption of modern information and communication technologies have had a positive impact on the relationships between individuals and even at the level of governmental institutions. This is due to the optimal use of these technologies within limits that do not harm others or their security. However, this evolution has been accompanied by various forms of security threats that hinder the optimal use of these technologies or pose a direct threat to individuals or public institutions.

In this study, we shed light on some concepts related to the term cybercrime, including its definition, elements, and distinctive characteristics. We also discussed the legal, institutional, and judicial mechanisms in place to counter cybercrime threats to information technology security in Algeria and evaluated their effectiveness.

Keywords: Cyber security, cybercrime, electronic crime, criminal behavior, informatics

مقدمة :

إن التطور الكبير الذي شهدته تكنولوجيا لاعلام و الاتصال و تغلغلها في جميع نواحي الحياة جعل الافراد و حتى الحكومات يعتمدون عليها بشكل كبير، فانتقلت تعاملاهم إلى تعاملات افتراضية عمادها شبكة الانترنت ،و أجهزة الحاسوب أو ما يقوم مقامها من أجهزة ذكية، فظهرت إلى الوجود أوصافا تعكس استعمال هذه التكنولوجيا كأن نقول الحكومة الرقمية أو لإدارة الالكترونية أو التجارة الالكترونية...إلخ . إلا أن الانتقال إلى البيئة الافتراضية أو الرقمية لا يخلو البتة من مخاطر من شأنها أن تهدد أمن هذه البيئة أو ما يعرف لأمن السيبراني مما يجعل مواردها في خطر حقيقي خصوصا تلك المتعلقة بالمنشآت الحيوية للدولة. الشيء الذي يعطي لموضوع لأمن السيبراني أهميته خصوصا أمام الجرائم السيبرانية التي أصبحت هاجسا يتحدى قيام الحكومات و الإدارات الرقمية ، و لذلك سعت الحكومات و الدول إلى درء هذا الخطر و بث الثقة و لإحساس بالأمان في البيئة الرقمية ، و في هذا الصدد و في كلمة القاها رئيس الجمهورية السيد عبد المجيد تبون أكد على أهمية لامن السيبراني و محاربة الجريمة السيبرانية قائلا :" ... وهو لأمر الذي يستوجب تطوير استراتيجيتنا الوطنية المتكاملة في المجال الرقمي، والجمع بين لاستباقية والوقاية من التهديدات في الفضاء السيبراني..."[1]

و عليه نطرح التساؤل التالي

ما المقصود بالجريمة السيبرانية ؟ و ما هي آليات مواجهتها في الجزائر

و من أجل لإجابة على هذا التساؤل اعتمدنا على الخطة التالية منتهجين المنهج الوصفي و المنهج التحليلي:

المحور الأول: مفهوم لامن السيبراني

المطلب الأول المطلب الأول تعريف الجريمة السيبرانية و أركانها

المطلب الثاني : دوافع ارتكاب الجريمة السيبرانية و خصائصها

المحور الثاني: آليات مواجهة التهديدات السيبرانية

المطلب الأول الاليات القانونية

المطلب الثاني : الاليات المؤسساتية و القضائية

المبحث الأول : مفهوم الجريمة السيبرانية

لأجل التعرف على ماهية الجريمة السيبرانية ، فإنه يتعين علينا التطرق الى مفهوم الجريمة السيبرانية المطلب الأول و من ثم التعرف دوافع الجريمة السيبرانية و خصائصها المطلب الثاني

المطلب الأول تعريف الجريمة السيبرانية و أركانها :

من خلال الفرعين سنتطرق الى تعريف الجريمة السيبرانية و بيان أركانها

الفرع الأول : تعريف الجريمة السيبرانية

سنتطرق الى التعريف الفقهي الفرع الأول ثم التعريف التشريعي

أولا: التعريف الفقهي للجريمة السيبرانية

لقد حاول العديد من الفقهاء و علماء لاجرام إعطاء تعريف للجريمة السيبرانية، و قد انقسموا في ذلك إلى أربع اتجاهات ، اتجاه استند على الوسيلة المستخدمة في ارتكابها و هو الاتجاه الفني، و اتجاه استند على موضوع الجريمة و هم أصحاب الاتجاه الموضوعي، و هناك الاتجاه الشخصي و الذين يستندون على توفر المعرفة التقنية و المعلوماتية لدى مرتكب الجريمة، و اتجاه آخر استند على الجمع بين الاتجاهات السابقة و هو الاتجاه المختلط[2].

و من بين التعريفات المقدمة نجد تعريف الفقهين الفرنسيين (LE STANC,VIVANT) بأن الجريمة السيبرانية هي : " مجموعة من الأفعال المرتبطة بالمعلوماتية و التي يمكن أن تكون جديرة بالعقاب"[3] كما عرفها لأستاذ mass بأنها :" لاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح". و عرفها لأستاذ Rosenblatt : " نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو الوصول أو التي تحول عن طريقه الأفعال غير المشروعة التي يستخدم الحاسب أداة لارتكابها"[4].كما عرفها الفقيه الألماني تاريمان بأنها " كل أشكال السلوك غير المشروع أو ضار بالمجتمع الذي يرتكب باستخدام الحاسب"[5]

و في كتابها الجريمة السيبرانية، تعرف "ماري هيلين ملراس"[6] الجريمة السيبرانية على أنها أي فعل ينتهك واحدا أو أكثر من القوانين القائمة من خلال التكنولوجيا أي استخدام الإنترنت والكمبيوتر. و قد قامت بتحليل الجرائم السيبرانية من خلال منظور علم الجريمة، و وفقا "لملراس"، فإنه يمكن تصنيف الجرائم السيبرانية إلى ست فئات متميزة وهي[7] :

1. لاختراق السيبراني والتخريب السيبراني cyberintrusion et cybervandalisme : تشمل هذه الأفعال الوصول غير المصرح به إلى أنظمة الكمبيوتر وقد تشمل تدمير أو تغيير البيانات.

2. السرقة الإلكترونية (cybertheft) cybervol :يشير هذا إلى سرقة المعلومات أو لأصول الرقمية، مثل البيانات الشخصية أو الملكية الفكرية.

3. الجرائم السيبرانية بين الأشخاص cybercrimes interpersonnels : تحدث هذه الجرائم بين الأفراد وقد تشمل التحرش عبر الإنترنت أو التنمر الإلكتروني.

4. لانحراف السيبراني والجرائم السيبرانية المتعلقة بالنظام العام cyberdéviance et cybercrime d'ordre public :تغطي هذه الفئة السلوكيات الانحرافية عبر الإنترنت و التي قد لا تكون ممنوعة ولكنها ضارة، بالإضافة إلى تلك الجرائم التي تؤثر على النظام العام.

5. الجريمة السيبرانية المنظمة cybercrime organisé :هي جرائم يرتكبها مجموعات منظمة تستخدم الإنترنت لأنشطة غير قانونية مثل تجارة المخدرات أو غسل الأموال.

6. الجريمة السيبرانية السياسية cybercrime politique : تكون هذه الأفعال مدفوعة بأهداف سياسية وقد تشمل الإرهاب الإلكتروني أو الهجمات ضد البنى التحتية الحيوية

ثانيا: التعريف التشريعي للجريمة السيبرانية :

التعريف التشريعي للجريمة السيبرانية يختلف من دولة لأخرى أو من هيئة دولية الى أخرى، ولكن بشكل عام فهي تهدف إلى تحقيق الأمن السيبراني و حماية المعاملات الالكترونية

- تعريف الأمم المتحدة: "أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية".
- تعريف مجلس أوروبا عرفت اتفاقية مجلس أوروبا المبرمة في بودابست لعام 2001، الجريمة الإلكترونية في الفصل الثاني منها، بأنها الجرائم ضد السرية والنزاهة و توافر البيانات و أنظمة الحاسب الالي"
- وقد ذهبت مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية في عام 1983 إلى تعريف الجريمة السيبرانية على أنها :" كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها"[8]
- تعريف المشرع السعودي : " أي فعل يرتكب متضمنا استخدام الحاسب الالي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"
- المشرع القطري عرف الجريمة السيبرانية على أنها :" أي فعل ينطوي على استخدام وسيلة تقنية المعلومات بالطريقة غير مشروعة بما يخالف أحكام القانون."
- تعريف التشريع في الولايات المتحدة الامريكية : عرفت وزارة العدل الجريمة عبر الانترنت على أنها :" أي جريمة لفاعلها معرفة فنية بتقنية الحاسب تمكنه من ارتكابها" أما مكتب تقييم التقنية في و م أ فقد عرفها بأنها:" الجريمة التي تلعب فيها البيانات الكومبيوترية و البرامج دورا رئيسيا"
- تعريف المشرع الجزائري : عرف قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم الخاصة بتكنولوجيا الاعلام و الاتصال و مكافحتها في المادة الثانية المطة أ بما اسمته الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال بأنها :" جرائم المساس بأنظمة المعالجة الالية للمعطيات المحدد في قانون العقوبات و أي جريمة أخر ترتكب أو يسهل ارتكابها عن طريقة منظومة معلوماتية او نظام للاتصالات الالكترونية"[9]

و مما سبق من تعريفات يمكن القول بأن الجريم السيبرانية هي :"مجموعة الأفعال غير القانونية التي تتم عبر معدات أو أجهزة الكترونية أو شبكة الإنترنت أو تبث عبر محتوياتها ، و هي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي و نظم المعلومات لارتكابها أو التحقيق فيها و مقاضاة فاعليها"[10]

الفرع الثاني : أركان الجريمة السيبرانية

إن وصف فعل ما بكونه جريمة يجب أن تتوفر فيه أركان ثلاث و هي: الركن الشرعي ، الر كن المعنوي ثم الركن المادي و هذا ما سنحاول أن نبينه من خلال الجريمة السيبرانية.

أولا : الركن الشرعي

المقصود بالركن الشرعي لأي جريمة، صدور أو وجود نص قانوني يجرم الفعل ، و يوضح العقاب المترتب على ارتكاب هذا الفعل المجرم ، كما يقصد كذلك بالركن الشرعي هو تطابق نص التجريم المنصوص عليه في القانون على سلوك صادر عن الفاعل ما لم يرد نص يزيل عليه صفة لاجرام او يتوفر على سبب من أسباب لاباحة[11] ، و في هذا لاطار فقد صدرت العديد من القوانين سواء وطنيا أو على مستوى الدول و المنظمات الدولية ما يجرم بعض التصرفات التي تصدر بمناسبة استعمال أجهزة لاعلام الالي.

ثانيا الركن المعنوي :

يقصد بالركن المعنوي اتجاه إرادة الشخص الى ارتكاب الفعل المجرم او النشاط لاجرامي بكل وعي و قصد تحقيق نتيجة من خلال هذا السلوك .و يختلف الركن المعنوي في الجريمة السيبرانية عن غيره من الجرائم ، ففي الجرائم السيبرانية لا يمكن ان ينتفي عن الشخص الجاني القصد الجنائي من وراء ارتكابه لهذا الفعل و هذا بسبب أن هذا النوع من الجرائم يفترض في الجاني الدراية التقنية و التكنولوجية و التي لا يمكن لغير المتمرسين و محترفي هذا المجال أن يقوموا به فضلا عن ارادته لارتكاب هذا الفعل

و يتخذ القصد الجنائي من حيث العمومية صورتان هما القصد العام و هو محقق في جميع الجرائم العمدية و يتمثل في انصراف إرادة الجاني لتحقيق الفعل المجرم مع العلم بعناصر هذا الفعل المنهى عليه قانونا ، اما القصد الخاص فهو الغاية التي يسعى اليها الجاني من اجل تحقيقها من خلال ارتكاب الجريمة ، و عليه فإن الجريمة السيبرانية هي من الجرائم العمدية ، و المسؤولية الجزائية للجريمة السيبرانية في التشريع الجزائري تقوم عند ارتكاب أي فعل من الأفعال المنصوص عليها في المواد من 394 مكرر الى 194 مكرر7 [12]، و الي سنشير اليها بالتفصيل لاحقا في هذا البحث.

ثالثا الركن المادي:

لنكون أما الركن المادي للجريمة السيبرانية يجب توفر عناصر ثلاث و هي :

1- السلوك لاجرامي : أي قيام الشخص بالفعل المجرم ، و مثال ذلك في جريمة القرصنة السلوك لاجرامي يتمثل في الولوج الى الموقع بطريقة غير قانونية وغير مشروعة قصد لاطلاع أو انتهاك أمن الأشخاص[13] .
2- النتيجة : و هو الغاية من السلوك لاجرامي و الذي تحقق من خلال هذا السلوك
3- العلاقة السببية: أن النتيجة تعود إلى السلوك لاجرامي الذي صدر عن الجاني السيبراني و مثاله تدمير موقع ما او اتلاف وثائق الاكترونية ، او نشر اسرار لاخرين و انتهاك خصوصياتهم.

المطلب الثاني : دوافع ارتكاب الجريمة السيبرانية و خصائصها
ان الجريمة السيبرانية كأي جريمة لها دوافعها و خصائصها المميزة لها

الفرع الأول : دوافع الجريمة السيبرانية

يمكن حصر الدوافع الى ارتكاب الجريمة السيبرانية في ما يلي[14] :

- **الولع في جمع المعلومات وتعلمها: يعتبر حب التعلم والاستطلاع من الاسباب الرئيسة التي تدفع لأرتكاب مثل هكذا جرائم لأن المخترق يعتقد ان اجهزة الحاسوب والانظمة هي ملك للجميع ويجب ان لا تبقى المعلومات حكرا على احد أي ان للجميع الحق بالتعرف والاستفادة من هذه المعلومات**
- **حب المغامرة والإثارة: عدد غير قليل من مخترقي الانظمة يعتبرون من عملهم هذا وسيلة للمرح والتسلية وتقضية اكبر وقت ممكن في انظمة وحواسيب الآخرين ويكون هذا الاختراق غالبا سلميا ودون ان يحدث تاثير يذكر.**
- **الدوافع الشخصية: فغالبا ما يرتكب المبرمج جرائم الكمبيوتر نتيجة إحساسه بالقوة والذات، وبقدرته على اقتحام النظام، فيندفع تحت تأثير الرغبة القوية في تحقيق الذات.**
- **تحقيق مكاسب مالية: قد يكون احد اسباب ارتكاب هذه الجرائم هو الكسب السريع وجني الارباح الطائلة دون تعب ، كاختراق انظمة الكترونية التي تستخدمها المصارف عن طريق الدخول الى الحسابات المصرفية والتلاعب فيها او الاستخدام غير المشروع لبطاقات الائتمان.**

الفرع الثاني : خصائص الجريمة السيبرانية:

- **الجريمة السيبرانية متعدية الحدود أو عابرة للدول: و هذا يعود لطبيعة البيئة السيبرانية التي لا تعترف بالحدود الجغرافية ، فالسهولة في حركة المعلومات و انسيابها عبر أنظمة التقنية الحديثة جعل بالمكان ارتكاب جريمة بواسطة حاسوب موجود في دولة بينما يتحقق الفعل الاجرامي في دولة أخرى. الشيء الذي خلف العديد من المشاكل من بينها تحديد الدولة صاحبة الاختصاص القضائي المتعلق بهذه الجريمة، و القانون الواجب التطبيق و كذلك إشكاليات متعلقة بالملاحقة القضائية.[15]**
- **صعوبة اكتشاف الجريمة السيبرانية : ان اكتشاف الجريمة السيبرانية هو من قبيل الصدفة ، و هذا لصعوبة اكتشافها و هذا نظرا للنقطة التي ذكرناها سابقا بأنها متعدية الحدود ، و كذلك الى عدم ترك هذه الجريمة لأي اثر خارجي و الطبيعة غير المرئية[16] ، و كذلك لقدرة الجاني على تدمير دليل الإدانة[17]**
- **الوصول للحقيقة بشأنها يستوجب الاستعانة بخبرة فنية عالية المستوى .**
- **لا تترك أثرا لها بعد ارتكابها ؛ علاوة على صعوبة الاحتفاظ الفني بآثارها إن وجدت . فهذه الجرائم لا تترك أثرا، فليست هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات، ولذا فإن معظم جرائم الانترنت تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابها .**
- **جسامة الضرر الناجم عنها و صعوبة تقديره و هذا عائد لحجم الخسائر و الاضرار الناجم عنها و كونه ضرر يمس بالكيانات المعنوية ذات القيمة المعنوية او القيمة المادية او كليهما مما يصعب إعطائها التقدير الصحيح[18] و من بينها المساس بحرمة الحياة الشخصية.**
- **سهولة ارتكاب الجريمة السيبرانية : فهي لا تحتاج الى جهد عضلي ، بل على القدرات الذهنية للجاني و تحكمه الجيد في الحاسوب و وسائل الاتصال الحديثة ، فيمكن للجاني بمفرده ان يرتكب جريمته دون الحاجة الى غيره من اجل الترصد و الحماية ، كما أن الجاني بعيدا عن إمكانية تعرضه لاي مقاومة من قبل المجني عليه أو من قوات الامن[19]**

المبحث الثاني : آليات مواجهة الجريمة السيبرانية في الجزائر

كغيرها من الدول و الحكومات عملت الجزائر على تقوية آلياتها لمواجهة الجرائم السيبرانية ، و ذلك من خلال اصدار قوانين ذات العلاقة بهذه الجرائم أو الانضمام الى معاهدات دولية تعني بمحاربة الجرائم السيبرانية ، و سنحاول التطرق اليها في المبحث الأول كما عملت على انشاء و تقوية مؤسسات تعمل على تأمين الفضاء السيبراني ضد أي تهديد و جريمة بإمكانها زعزعة الأمن السيبراني المطلب الثاني

المطلب الأول الآليات القانونية :

أولا : تعديل في قانون العقوبات الجزائري :

فقد استحدث قسم في قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات و الجنح ضد الاموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات و الذي احتوى على اثنا عشر مادة نذكرها فيما يلي :

- المادة 394 مكرر " يعاقب بالحبس من ثلاثة اشهر الى سنة و بغرامة من خمسين ألف الى مائة ألف دينار كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من المنظومة للمعالجة الالية للمعطيات او يحاول ذلك .
- تضاعف العقوبة اذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة .
- و إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام أشغال المنظومة تكون العقوبة الحبس من 06 اشهر الى سنتين و غرامة من خمسين الف الى مائة و خمسون ألف دينار "
- المادة 394 مكرر1 " يعاقب بالحبس من 06 اسهر الى 03 سنوات و بغرامة من 500.000 دج الى 2000.000 كل من ادخل بطريقة الغش معطيات في نظام أو أزال او عدل بطريقة الغش المعطيات التي يتضمنها "
- المادة 394 مكرر 2 " يعاقب بالحبس من شهرين الى 03 سنوات و بغرامة من 1000.000 دج الى 5000.000 دج كل من يقوم عمدا و عن طريق الغش بما يلي :
- تصميم أو بحث او تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن ترتكب بها الجرائم المنصوص عليها في هذا القسم .
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم .
- المادة 394 مكرر 3 " تضاعف العقوبة المنصوص عليها في هذا القسم اذا استهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام دون الاخلال بتطبيق عقوبات اشد ."
- المادة 394 مكرر 4 " يعاقب الشخص المعنوي الذي يرتكب احدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الاقصى المقرر للشخص الطبيعي "

- المادة 394 مكرر 5 " كل من شارك في مجموعة أو في اتفاق تألف بغرض الاعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم و كان هذا التحضير مجسد أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها ."
- المادة 394 مكرر6 " مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة و البرامج و الوسائل المستخدمة مع اغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم على اغلاق المحل أو مكان استغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها ."
- المادة 394 مكرر 7" يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذا القسم بالعقوبات المقررة على الجنحة ذاتها ."

و الملاحظ على هذه المواد أن نية المشرع تتجه نحو تشديد العقوبات في الجرائم الماسة بأمن المعلومات

ثانيا: تعديل قانون الإجراءات الجزائية

استحدث المشرع الجزائري بموجب قانون الإجراءات الجزائية مجموعة من الإجراءات الخاصة التي تتماشى و مع العالم الافتراضي، حيث سمح المشرع الجزائري باللجوء إلى اعتراض المراسلات والتقاط الصور وتسجيل الأصوات لمقتضيات التحري والتحقيق في جرائم محددة حصرا ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، مع مراعاة شروط محددة قانونا، والمتمثلة في الإذن، وطبيعة الجريمة، وكتمان السر المهني، وتحرير محضر من طرف ضابط الشرطة القضائية المأذون له بالعملية[20]

ثالثا : الانضمام الى الاتفاقيات الدولية ذات الصلة بالجرائم السيبرانية

ان عملية مكافحة الجريمة السيبرانية ، و نظرا لخاصيتها الدولية ، فان تكاثف الجهود الدولية يعتبر اكثر من ضرورة ، و في هذا الإطار عملت الجزائر على الانظمام الى العديد من الاتفاقيات الدولية و الاقليمة المتعلقة بمكافحة الجرائم السيبرانية نذكر من بينها :

- اتفاقية بودابست (المجر) سنة 2001 : اتفاقية بودابست لعام 2001، المعروفة أيضًا باسم اتفاقية مكافحة الجرائم المعلوماتية، هي أول معاهدة دولية تهدف إلى مكافحة الجرائم الإلكترونية من خلال تنسيق القوانين الوطنية، وتحسين تقنيات التحقيق، وزيادة التعاون بين الدول.تم التوقيع عليها في 23 نوفمبر 2001 في بودابست، المجر.تشمل الاتفاقية تدابير لمكافحة جرائم الإنترنت، وتوفر إطارًا للتعاون الدولي في هذا المجال.و مما جاء في ديباجتها : " و اقتناعا بأن هذه الاتفاقية لازمة لردع الاعمال الموجهة ضد سرية و سلامة و اتاحة نظم الكومبيوتر .....و ذلك بالنص على تجريم مثل هذا السلوك"[21]
- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010 : هي وثيقة قانونية تهدف إلى تعزيز التعاون بين الدول العربية في مجال مكافحة الجرائم السيبرانية . تم التوقيع عليها في القاهرة بتاريخ 21 ديسمبر 2010، وتشمل أحكامًا تتعلق بالتجريم، والإجراءات، والتعاون القانوني والقضائي بين الدول الأطراف و هي تتضمن تعريفات لمصطلحات مثل تقنية المعلومات، مزود الخدمة، البيانات، البرنامج المعلوماتي، وغيرها، وتنطبق على جرائم تقنية المعلومات التي ترتكب في أكثر من دولة أو لها اثار شديدة في دولة او دول أخرى.
- اتفاقية الاتحاد الأفريقي حول الأمن السيبراني وحماية البيانات ذات الطابع الشخصي، المعروفة أيضًا باتفاقية مالابو، تم تبنيها في عام 2014. تهدف الاتفاقية إلى تعزيز الأمن السيبراني وحماية البيانات الشخصية في

القارة الأفريقية .تتكون من 38 مادة موزعة على أربعة فصول، وتتناول مختلف الجوانب المتعلقة بالجريمة الإلكترونية والأمن السيبراني، بما في ذلك التعاون القانوني والتقني بين الدول الأعضاء.الا انه لا تزال هناك تحديات تواجه تنفيذ الاتفاقية، مثل تضاعف معدلات الجريمة الإلكترونية وإشكالية عدم دخولها حيز النفاذ. و من بين المآخذ على هذه الاتفاقية هو كونها :

- مفتوحة للانضمام فقط للدول الإفريقية، وهذا ما يجعلها محدودة النطاق ويمنعها من الوصول إلى التأثير العالمي الذي وصلت له الاتفاقية الأوربية.
- لم تتعرض الاتفاقية الإفريقية لإنشاء آليات للتعاون بين الدول الإفريقية في المسائل الجنائية ذات الصلة بالجريمة السيبرانية،
- لم تتعرض الاتفاقية إلى أهم أشكال الإجرام السيبراني و المتمثل في الحرب السيبرانية

المطلب الثاني الآليات المؤسساتية و القضائية

و من خلال هذا المطلب سنعرض أهم الهيئات و المؤسسات التي تعني بالوقاية و محاربة الجرائم السيبرانية و التي سعت الجزائر لانشائها و هي :

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال :

أنشئت هذه الهيئة بموجب المادة 13 من القانون رقم 09-04 المؤرخ في 05 أوت2009 [22] المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها و من بين مهام الهيئة :

- إدارة وتنسيق عمليات الوقاية
- المساعدة التقنية للجهات القضائية و الأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية
- تفعيل التعاون القضائي و الأمني الدولي.

و قد حددت تشكيلة هذه الهيئة من خلال المرسوم الرئاسي الصادر في 10/8/ 2015 ، أي بعد مرور زهاء 5 سنوات من صدور المرسوم المحدد لمهام هذه الهيئة

ثانيا: انشاء الأقطاب القضائية الجزائية المتخصصة.

أنشئت بموجب القانون 14/04 المؤرخ في 10 نوفمبر 2004 المعدل لقانون الإجراءات الجزائية ، و من بين الجرائم التي تختص بها الجرائم الماسة بانظمة المعالجة الآلية للمعطيات (المواد37 - 329- 40 من قانون الإجراءات الجزائية)

ثالثا : توسيع صلاحيات الضبطية القضائية :

عند معاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يمكن للضبطية القضائية

1. تمديد الاختصاص المحلي إلى كامل الإقليم الوطني[23]
2. إمكانية تفتيش المحلات السكنية و غير السكنية في كل ساعة من ساعات الليل و النهار بإذن من وكيل الجمهورية[24] .
3. إمكانية تفتيش المساكن دون حضور المشتبه فيه أو صاحب المسكن و دون شهود25 .

الخاتمة :

من خلال ما استعرضناه ، يمكن القول بأن الجريمة السيبرانية هي "مجموعة الأفعال غير القانونية التي تتم عبر معدات أو أجهزة الكترونية أو شبكة الإنترنت أو تبث عبر محتوياتها ، و هي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي و نظم المعلومات لارتكابها أو التحقيق فيها و مقاضاة فاعليها" . و للجريمة السيبرانية خصائص تميزها عن غيرها كونها جرائم عابرة للدول ، و من الصعب اكتشافها ، و ان مرتكب هذه الجريمة يمتاز بذكاء شديد و تحكم كبير في تكنولوجيا لاعلام و الاتصال ، كما أن هذا لنوع من الجرائم لأركان ذاتها في الجريمة العادية و هي الركن الشرعي و الركن المادي و الركن المعنوي و هي تعد من الجرائم العمدية حيث لا مكان لانتفاء القصد الجنائي فيها.

و عليه فقد حاول المشرع الجزائري على غرار العديد من الدول في وضع آليات قانونية و مؤسساتية ، و التي من شأنها أن تضع حدا للجرائم السيبرانية أو التقليل منها ، و في سبيل ذلك قامت بتعديل قانون العقوبات و قانون لإجراءات الجزائية لكي تتلائم مع ما استحدث من جرائم سيبرانية كما استحدثت اقطاب قضائية لهذا النوع من الجرائم هذا على المستوى الداخلي أما على المستوى الدولي فقد انضمت الجزائر الى العديد من الاتفاقيات الدولية ذات العلاقة بمحاربة الجريمة السيبرانية و الحفاظ على لامن السيبراني

الا ان التطور الحاصل في تكنولوجيا لاعلام و الاتصال يصاحبه و بشكل مضطرد تطور في لأساليب المعتمدة في الجرائم السيبرانية و عليه نقترح بعض التوصيات :

1- العمل على تكوين دائم و عال المستوى للتقنيين العاملين في مجال مكافحة الجرائم السيبرانية
2- تكوين عال المستوى للقضاة المنوط بهم هذا النوع من الجرائم
3- المعاملة بالمثل في حال تهديد سيبراني ذو طبيعة عدائية (الحروب السيبرانية)
4- التدريب على حماية الفضاء السيبراني و أجهزة الحاسوب خلال اطوار التعليم
5- ترسيخ لامن السيبراني لدى المواطن.
6- العمل على مواكبة القوانين الى التطورات الحاصلة في تكنولوجيا لاعلام و الاتصال.

---

[1] الكلمة كاملة تجدونها عبر الرابط التالي: www.aps.dz/ar/algerie/145058-2023-06-07-18-57-13

[2] عميمر عبد القادر، التحديات القانونية لاثبات الجريمة المعلوماتية، النشر الجامعي الجديد، تلمسان ، 2021 ، ص 11

[3] مناصرة يوسف ، جرائم المساس بأنظمة المعالجة الالية للمعطيات، دار الخلدونية ، الجزائر ، 2018 ، ص 25

[4] محمد محمود العمري، مدخل إلى لأمن السيبراني.دار زهران للطباعة و النشر، لأردن ، 2020، ص 42

[5] مناصرة يوسف ، المرجع السابق ، ص 26

[6] ماري هيلين ماراس هي أستاذة مشاركة في كلية جون جاي للعدالة الجنائية بنيو يورك ومديرة مركز دراسات الجريمة الإلكترونية

[7] Cameron Coutu, "La prévention de la cybercriminalité : résultats d'une enquête sur les effets perçus d'une campagne de prévention réalisée par une institution financière", Mémoire présenté à la Faculté des études supérieures et postdoctorales en vue de l'obtention du grade de Maîtrise en criminology, Université de Montréal Canada, ,2019

[8] محمد محمود العمري، مرجع سابق ، ص 43

[9] انظر الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية ، عدد 47 بتاريخ 16 غشت سنة 2009 ص 05

[10] محمد محمود العمري، مرجع سابق ، ص 20

[11] عميمر عبد القادر مرجع سابق ، ص 87

[12] عميمر عبد القادر مرجع سابق ، ص 90

[13] حسين طاهري ، جرائم القرصنة الالكترونية، دار الخلدونية ،الجزائر ، 2021 ، ص 67

[14] www.mohamah.net/law/مفهوم-وخصائص-الجرائم-السيبرانية-في-م/ تاريخ الزيارة 2024/04/09 على الساعة 16:30

[15] نهلا عبد القادر المومني ، الجرائم المعلوماتية ،ط2 ، دار الثقافة للنشر و التوزيع ، الأردن ، 2010 ، ص 52

[16] مناصرة يوسف، مرجع سابق ، ص 42

[17] نهلا عبد القادر المومني ، المرجع السابق ، ص 53

[18] مناصرة يوسف، مرجع سابق ، ص 43

[19] عميمر عبد القادر ، مرجع سابق ، ص 28

20 مهدي رضا ، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة إيليزا للبحوث والدراسات، المجلد 06العدد 02 (2021) ص 111 -125

[21] مناصرة يوسف ، مرجع سابق ، ص 352

[22] انظر الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية ، عدد 47 بتاريخ 16 غشت سنة 2009 ص 05

[23] انظر المدة 16 من قانون الإجراءات الجزائية

[24] انظر المادة 47 من قانون الإجراءات الجزائية

[25] انظر المادة 45 من قانون الإجراءات الجزائية

الحماية الرقمية :رؤية استباقية نح تعزيز الامن السيبرانية في الجزائر

Digital Protection: A Proactive Vision Towards Enhancing Cyber Security in Algeria

مزهود صورية (*) جامعة جيجل 18000 جيجل ، الجزائر soraya.mezhoud@univ-jijel.dz.
بويبية نبيل جامعة جيجل 18000 جيجل ، الجزائر nabil.bouibia@univ-jijel.dz

ملخص:

تتناول هذه الورقة البحثية موضوع الحماية الرقمية في الجزائر، حيث يتم التركيز على رؤية استباقية نحو تعزيز لأمن السيبراني في هذا السياق. يشهد العصر الحديث تزايدا مستمرا في التكنولوجيا واعتماد الشبكات الرقمية، مما يعزز أهمية حماية الأنظمة الإلكترونية والمعلومات. تأخذ الجزائر مكانة بارزة كواحدة من الدول النامية، وتواجه تحديات خاصة في مجال لأمن السيبراني.

يتعامل البحث مع استراتيجيات التحسين والتعزيز للأمن السيبراني في الجزائر بشكل استباقي، مع التركيز على الجوانب التنظيمية والتقنية والتدريبية. يتعامل الباحثون مع تحليل التهديدات السيبرانية المحتملة ويقدمون استراتيجيات فعالة للتصدي لها. كما يتم التطرق إلى ضرورة تعزيز التعاون الدولي والإقليمي لمواجهة التحديات السيبرانية المشتركة.

وفي هذا السياق، يركز البحث على تحقيق التوازن بين تعزيز لأمن السيبراني وتشجيع التطور التكنولوجي والابتكار. يشدد على أهمية إشراك القطاع الخاص والجهات الحكومية في هذا الجهد المشترك، بما يضمن تحقيق أقصى قدر من الفعالية في مجال الحماية الرقمية في الجزائر.

الكلمات المفتاحية: الحماية الرقمية ؛ لامن السيبراني؛ الجزائر؛ لاستباقية.

Abstract:

This research paper addresses the topic of digital protection in Algeria, with a focus on a proactive approach to enhancing cybersecurity in this context. The modern era witnesses a continuous increase in technology and reliance on digital networks, thus emphasizing the importance of protecting electronic systems and information. Algeria holds a prominent position as one of the developing countries and faces unique challenges in cybersecurity.

The research deals with proactive strategies for improving and enhancing cybersecurity in Algeria, focusing on regulatory, technical, and training aspects. Researchers analyze potential cyber threats and provide effective strategies to counter them. The necessity of enhancing international and regional cooperation to tackle common cyber challenges is also addressed.

In this context, the research emphasizes achieving a balance between enhancing cybersecurity and encouraging technological development and innovation. It highlights

the importance of involving the private sector and government entities in this collective effort to ensure maximum effectiveness in digital protection in Algeria.
KeyWords: ***Digital protection, cybersecurity, Algeria, proactive approach.***

مقدمة:

تشهد العصور الحديثة تطورا سريعا في مجال التكنولوجيا الرقمية، مما أدى إلى تعميم استخدام لإنترنت والتفاعل الرقمي في شتى جوانب الحياة.ومع هذا التقدم الهائل، تنشأ تحديات جديدة تتعلق بأمان المعلومات والتحديات السيبرانية التي تهدد سلامة الأفراد والمؤسسات. تعتبر الجزائر، كأي دولة أخرى، عرضة لتلك التحديات وتحتل قضايا لأمن السيبراني مكانة هامة في جدول أعمالها الوطني.

في هذا السياق، يأتي موضوع "حماية الرقمية في الجزائر" كمحور أساسي للبحث، حيث نتعامل مع تحليل التحديات وتطوير رؤية استباقية لتعزيز لأمن السيبراني. يعكس هذا البحث التفاعل الحيوي بين التقنية ولأمان، ويستند إلى فهم عميق للبيئة الرقمية في الجزائر والتحديات المحتملة التي قد تطرأ.

إن فحص لأمان السيبراني يمتد إلى مجموعة واسعة من القضايا، بدءا من حماية البيانات الحساسة إلى التصدي للتهديدات السيبرانية الهجمات ولاختراقات. وفي هذا السياق، يلعب التحليل لاستباقي دورا حيويا في تحديد التهديدات المحتملة ووضع إطار للتصدي لها بشكل فعال.

يتطلب تعزيز لأمن السيبراني في الجزائر جهودا متكاملة تتضمن التشريعات والسياسات والتقنيات المتقدمة. يسعى هذا البحث إلى فهم السياق الثقافي والتشريعي للأمن السيبراني في الجزائر، مع التركيز على تطوير استراتيجيات استباقية لمواجهة التحديات القائمة والمستقبلية.

أهمية الموضوع:

1. تطوير البيئة الرقمية:

يأتي تعزيز لأمن السيبراني في الجزائر بأهمية بالغة في تطوير البيئة الرقمية وتشجيع اعتماد التكنولوجيا الرقمية في مختلف القطاعات. تحسين لأمان السيبراني يعزز الثقة في استخدام الإنترنت والتكنولوجيا، مما يسهم في تعزيز التفاعل الرقمي وتقدم البلاد في الاقتصاد الرقمي.

2. حماية المعلومات والبيانات:

يشكل التحسين في الأمن السيبراني وسيلة لحماية المعلومات والبيانات الحساسة للأفراد والمؤسسات. ذلك يحافظ على خصوصية الأفراد ويمنع الوصول غير المصرح به إلى المعلومات الحساسة، مما يقلل من تهديدات السرقة الإلكترونية والتجسس السيبراني.

3. مكافحة التهديدات السيبرانية:

تعتبر الجزائر عرضة لمختلف أنواع التهديدات السيبرانية، بدءا من هجمات القرصنة والبرمجيات الخبيثة إلى الاختراقات الإلكترونية. يساهم تعزيز الأمن السيبراني في تعزيز القدرة على مكافحة هذه التحديات بفعالية وتحديد الثغرات الأمنية والتصدي لها.

4. تعزيز الاستقرار الوطني:

يلعب الأمن السيبراني دورا حاسما في الحفاظ على استقرار الدولة والحفاظ على سلامة الهياكل الحيوية، مثل البنية التحتية الحكومية والمؤسسات الحيوية. التأكيد على الأمان السيبراني يقوي المقاومة ضد الهجمات التي قد تستهدف هذه الهياكل.

أهداف الموضوع:

- فحص التحديات السيبرانية التي تواجه الجزائر حاليا، وفهم طبيعتها وأسبابها.

- تحديد وتحليل الثغرات الأمنية المحتملة في النظام السيبراني الجزائري.

-وضع إطار لسياسات وإجراءات تعزز الأمن السيبراني بشكل شامل وفعال.

- تحديد كيفية تحقيق التوازن بين استمرارية التطور التكنولوجي وحاجة البلاد للحفاظ على أمان المعلومات.

- تعزيز التوعية بأهمية الأمان السيبراني وتشجيع الجمهور والشركات على تبني ممارسات أمن سيبراني.

- تعزيز التدريب وبناء القدرات للكوادر الفنية والمتخصصة في مجال الأمن السيبراني لتحقيق فاعلية أكبر في مكافحة التهديدات الرقمية.

الإشكالية :

كيف يمكن تحسين وتعزيز الأمن السيبراني في الجزائر بشكل فعال، وكيف يمكن مواجهة التحديات السيبرانية الراهنة والمستقبلية بهدف تعزيز الاستقرار الوطني وتحفيز التطور الرقمي في مختلف القطاعات؟

الفرضية :

إذا تم تنفيذ استراتيجيات فعالة لتعزيز الأمن السيبراني في الجزائر، بتوجيه الجهود نحو تحليل وتحسين البنية التحتية الرقمية وتعزيز الوعي السيبراني، فإن ذلك سيساهم بشكل كبير في التصدي للتحديات السيبرانية وتعزيز الثقة في استخدام التكنولوجيا الرقمية، مما يعزز الاستقرار الوطني ويسهم في تحقيق تطور فعال في مختلف القطاعات.

منهجية الدراسة :

تم انتقاء المنهج الوصفي التحليلي في هذه الدراسة بهدف تحقيق الأهداف البحثية والتحقق من صحة الفرضيات المطروحة. يستند هذا المنهج إلى جمع بيانات شاملة ومعلومات مفصلة لتمكين تحليل دقيق لمسألة الدراسة. من خلال هذا التحليل، يمكن فهم مفهوم الحماية الرقمية وتعزيز الأمن السيبراني في السياق الجزائري بطريقة توقعية.

بالإضافة إلى ذلك، تم اعتماد منهج دراسة الحالة لاستكمال رؤية شاملة حول الحماية الرقمية وتعزيز الأمن السيبراني في الجزائر بنهج استباقي. من خلال التركيز على دراسة الحالة، يمكن استكشاف التفاصيل الدقيقة حول تعزيز الأمن السيبراني في السياق الجزائري بطريقة شاملة ومعمقة.

بشكل عام، يجمع استخدام هاتين الطريقتين البحثيتين على التفصيل الوصفي من منهج الوصف التحليلي والتحليل العميق من منهج دراسة الحالة، مما يوفر فهما شاملاوعميقا حول تعزيز الأمن السيبراني في السياق الجزائري.

المحور الأول: تقييم التحديات السيبرانية الحالية في الجزائر

تعيش الجزائر، كغيرها من الدول، في عصر يتسم بتسارع التطور التكنولوجي وانتشار استخدام الإنترنت، مما أدى إلى تزايد التحديات السيبرانية التي تواجهها. يشكل التفاعل المتزايد مع البيئة الرقمية تحديات متعددة، بما في ذلك الهجمات الإلكترونية وانتشار البرمجيات الخبيثة، إلى جانب تحديات ضعف البنية التحتية السيبرانية. يأتي هذا في سياق تطورات سريعة تفرض ضرورة التحديث والتطوير المستمر للأنظمة والإجراءات الأمنية لضمان مقاومة البنية التحتية السيبرانية أمام التهديدات المتزايدة.

تحليل الواقع السيبراني في الجزائر يكشف عن تحديات جوهرية تستدعي التفكير الاستراتيجي والتدابير الفعالة للتصدي لها. يأتي هذا التمهيد لاستعراض وتحليل تفصيلي للتحديات السيبرانية المحددة، والتي ستكون محور دراستنا لتقديم رؤى عميقة واقتراحات فعالة لتحسين الأمن السيبراني في هذا السياق الرقمي المتطور.

- استهداف المؤسسات السيادية في الجزائر: تحليل لتصاعد الهجمات السيبرانية

في تصريحها لـ "صوت الأحرار"، أشارت الدكتورة دليلة العوفي، الباحثة المتخصصة في مجال الأمان السيبراني والاتصال الرقمي، إلى أن الجزائر، على غرار دول العالم الأخرى، تتعرض بشكل مستمر لهجمات سيبرانية متنوعة من حيث الحجم والأهداف.وأكدت الباحثة أن هذه الهجمات تستهدف بشكل عام المؤسسات، خاصة تلك ذات الطابع السيادي، فضلاً عن استهداف الأفراد[1].

وفي سياق الوقت الحالي، الذي يشهد انتشار تقنية الذكاء الاصطناعي، أشارت الدكتورة العوفي إلى أن هذه التقنية تشكل تحديا كبيرا في مجال الأمن السيبراني. حيث يقوم المجرمون باستغلالها في إرسال الرسائل عبر تطبيقات متنوعة، وكذلك في نشر إعلانات تستهدف فئات محددة.وأوضحت أن المجرمين يستغلون أيضا منصات الدردشة

لكسب ثقة المستخدمين بهدف زعزعة استقرار الوطن، وكذلك لتحقيق مكاسب مالية وتعطيل المعاملات التجارية[2].

- عدم القدرة على التحكم أمام الانتشار السريع للانترنت :

تبرز التحديات التي تطرأ نتيجة انتشار تكنولوجيا الإنترنت فائقة السرعة والتقدم اللافت في مجال تكنولوجيا الإنترنت اللاسلكي، والتي تجعل الجهات المختصة أمام تحديات فريدة في سرعة إجراء التحقيقات ومتابعة الجرائم الإلكترونية. يظهر ذلك بشكل واضح في ظل التطورات السريعة في مجال الأجهزة والبرمجيات، حيث تصبح التقنيات الجديدة متاحة بشكل مستمر.[3]

يبرز النمو الكبير في عدد مستخدمي شبكات التواصل الاجتماعي في الجزائر، الذي يزيد عن سبعة ملايين مستخدم، التحديات المتنوعة التي تطرأ نتيجة لهذا التطور. يلقي التنامي السريع لهذا النوع من التواصل الاجتماعي الضوء على تزايد الجرائم الإلكترونية، بما في ذلك القذف والتحرش الجنسي واستغلال القصر. تظهر أيضا التحديات المتعلقة باستخدام خدمات البروكسي في عمليات التخفي وغياب التنسيق الدولي، الأمر الذي يعزز انتشار الجريمة الإلكترونية عبر الحدود[4].

يفرض التقدم التكنولوجي في مجال الإنترنت والاتصالات ضغطا كبيرا على الأجهزة الأمنية لتحديث أساليبها باستمرار وتجهيزها بأحدث التقنيات. هذا الضغط يتطلب من السلطات الأمنية متابعة مستمرة وتكنولوجيا متقدمة لمواكبة التحديات المستجدة في مجال الأمان السيبراني، مما يبرز ضرورة الابتكار المستمر وتطوير القدرات للتصدي للتهديدات الإلكترونية المتقدمة[5].

في السياق الجزائري كشف الرائد بزيو عبد القادر، مسؤول مصلحة الاتصال بقيادة الدرك الوطني، عن تحديات تواجه المؤسسات الأمنية في إجراء تحقيقات في الفضاء الافتراضي. يعزى التعقيد إلى صعوبة جمع الأدلة في ظل التطورات التكنولوجية السريعة وصعوبة التعرف على المجرمين في هذا السياق. يتجلى هذا التحول في الفهم المتزايد لأهمية الأمان السيبراني، ويبرز أهمية تكوين فرق مختصة وتطوير نماذج عملياتية لمعالجة الجرائم الإلكترونية.[6]

تشير الصعوبات المتعلقة بالجرائم المعلوماتية إلى طبيعتها المعنوية وانتقالها إلى الأبعاد الرقمية، مما يجعل تحقيقها وجمع الأدلة وضبطها أمرا تحديا. يشير الرائد بزيو إلى أهمية تطوير خبرة ومهارات الأفراد الذين يعملون في هذا المجال وضرورة إنشاء هياكل خاصة للتحقيق في هذا النوع من الجرائم[7].

يبرز أيضا الحاجة إلى تعقب مجرمي المعلوماتية والأنشطة عبر الإنترنت، والتحقق من الأدلة الرقمية وتطوير استراتيجيات للتحقيق ومكافحة الجرائم المعلوماتية. يشدد على أهمية التعاون الشرطي والتقني في هذا السياق لضمان التحقيق الفعال ومواجهة التحديات المستمرة المتعلقة بتكنولوجيا المعلومات والاتصالات[8].

- تراجع دور الدولة وتصاعد الارتباط السيبراني و ظهور نمط جديد من الأذى

يعيش الفضاء السيبراني تطورا متسارعا، حيث يشهد زيادة في الارتباط يوسع خطر الهجمات السيبرانية على البنية التحتية الكونية. هذا الاتساع في التفاعل يفضي إلى تحولات استراتيجية في سياق العولمة، مما يجعل دور الدولة يتراجع في بعض القطاعات الإستراتيجية ويعقد من تحقيق التوازن الإستراتيجي[9].

يظهر الفضاء السيبراني نمطا جديدا من الأذى، حيث يسمح بتسبب الدول في الضرر دون الحاجة للدخول المادي إلى أراض أخرى، مما يعزز التعقيد والخطورة في سياق الأمان السيبراني. يتحول الفضاء السيبراني أيضا إلى أداة للتأثير في مختلف مراحل الصراع، مما يستدعي استعدادا لتحديات جديدة وتطوير مفهوم "الاستراتيجية السيبرانية" كوسيلة لتحقيق تفوق وطني[10].

مع زيادة نطاق الأنشطة العدائية التي تتخذها الدول أو أطراف غير حكومية في الفضاء السيبراني، يزايد التحدي للاستعدادات الشاملة والتدابير الأمنية الفعالة. ينبغي أن تتسارع الجهود لتطوير إستراتيجيات تأمين سيبراني تعكس التطورات الحديثة وتتفاعل مع المستجدات المستمرة في هذا السياق المعقد[11].

- الجرائم الإلكترونية بنـــي الجزائر بالأرقام :

أسست مديرية الأمن الوطني في الجزائر، مصلحة مكافحة الجرائم المعلوماتية، والتي تتخذ من مهمتها استقبال شكاوى المواطنين، وتتبع التحقيقات وتقديمها للعدالة. وفي سياق متصل، نبهت السلطات الأمنية إلى ارتفاع حالات الجرائم الإلكترونية في الجزائر، حيث انتقلت الجريمة من الواقع إلى العالم الافتراضي، نظرا لسرعة تنفيذها. وسجلت مصالح الدرك والشرطة أكثر من 8 آلاف جريمة إلكترونية خلال عام 2020، مما أدى إلى منافسة قوية مع الجريمة التقليدية.

وقد قامت المديرية العامة للأمن الوطني بتسجيل ارتفاع قياسي، حيث ارتفع عدد الجرائم من 500 جريمة في عام 2015 إلى 5200 قضية في عام 2020، خاصة في مجال الجرائم الإلكترونية. بينما سجلت قيادة الدرك الوطني 1362 جريمة سيبرانية تورط فيها 1028 شخص خلال 2020، وتم معالجة 3534 قضية من أصل 4400 تم تقديمها خلال عام 2021.

من ناحية أخرى، كشفت شركة "كاسبرسكي" المتخصصة في مكافحة الجريمة السيبرانية عن إحباطها لـ 95 ألف هجمة إلكترونية ضد الجزائر خلال عام 2020.وقد صنفت الشركة الجزائر كأولى عربيا والرابعة عشرة عالميا في عدد الهجمات الإلكترونية، وذلك وفقا لتصنيف عام 2018 [12].

المحور الثاني:واقع السياسات الجزائرية في مجال لامن السيبراني

منذ بداية القرن الحالي، اتخذت الجزائر خطوات فاعلة لمواكبة التحولات العالمية في مجال السياسات العامة السيبرانية. تركزت هذه الجهود على تكييف التشريعات والقوانين مع المعاهدات والاتفاقيات الدولية، بالإضافة إلى متابعة التطورات التكنولوجية.وقد شهدت الفترة الأخيرة إنشاء عدد من المؤسسات المتخصصة في هذا المجال، بجانب تعزيز التعاون الدولي في مجال الأمن السيبراني. هذا المنهج يعكس التزام الجزائر بالتحول الرقمي وتعزيز الحماية الإلكترونية، وهو ما نتناوله في هذا السياق.

أولا-الامن السيبراني : المنظومة القانونية و التطبيقية :

تعد المنظومة القانونية أحد الأركان الأساسية في بناء سياسات واستراتيجيات الأمن السيبراني في أي دولة، حيث تقوم التشريعات والقوانين برسم الإطار القانوني لحماية البنية التحتية لتقنية المعلومات وكذلك حقوق الأفراد والمؤسسات في الفضاء الإلكتروني.وقد سعت الجزائر وضع إطار قانوني يكفل حماية البيانات الشخصية والحساسة للمواطنين والهياكل الحيوية للدولة من خلال تحديد الجرائم السيبرانية وآليات مكافحتها.

في إطار مراجعة قوانين الجمهورية لتكييفها مع التطورات التكنولوجية العالمية وكذلك المعاهدات والاتفاقيات الدولية التي أبرمتها الجزائر، ومن أجل مواكبة عصر المعلومات، قامت الجزائر بمراجعة القوانين التالية:

- القانون رقم 04 لسنة 2004 المعدل لقانون العقوبات، وخاصة القسم السابع المكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعلومات، حيث صنفت الجرائم المعلوماتية إلى أنواع.[13]

- القانون رقم 04-09 لسنة 2009 الذي يتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصالات، ويهدف إلى وضع قواعد خاصة للوقاية ومكافحة هذه الجرائم[14].

- القانون رقم 03-15 لسنة 2015 المتعلق بالتوقيع والتصديق الإلكتروني، الذي ينص على ضرورة وجود البيانات المعلوماتية ذات الطابع الشخصي على التراب الوطني، ما لم ينص على خلاف ذلك في التشريع المعمول به[15]

- القانون رقم 04-18 لسنة 2018 المتعلق بالبريد والاتصالات الإلكترونية، الذي ينص على رقابة الدولة على أنشطة البريد والاتصالات الإلكترونية، وتمارس السلطات وفقا للأحكام الدستورية[16].

تركز هذه المراجعات على مكافحة الجرائم السيبرانية، وتعكس توجهات الدولة نحو تطوير القوانين والتشريعات في مجال الاقتصاد الرقمي والتجارة الإلكترونية، وتعزيز وسائل الدفع الإلكتروني.

ثانيا-الاطار المؤسساتي للحماية السيبرانية في الجزائر : تنظيم و تطبيقات:

يشير المرسوم الرئاسي المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية إلى أن هذه الأخيرة تعتبر "أداة للدولة" في هذا المجال، حيث تشكل "الإطار التنظيمي لإعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتنسيق تنفيذها".

وتضم هذه المنظومة، التي توضع لدى وزارة الدفاع الوطني، مجلسا وطنيا يكلف بإعداد الاستراتيجية المذكورة والموافقة عليها وتوجيهها، إلى جانب وكالة تضطلع بتنسيق تنفيذ هذه الاستراتيجية.

ومن بين المهام التي يتولاها المجلس، الذي يرأسه وزير الدفاع الوطني أو ممثله، "الموافقة على اتفاقيات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في مجال أمن الأنظمة المعلوماتية وسياسة التصديق الإلكتروني وتصنيف الأنظمة المعلوماتية"، فضلا عن "إبداء رأي متطابق في أي مشروع نص تشريعي أو تنظيمي" ذي صلة بهذا الموضوع[17]

أما وكالة أمن الأنظمة المعلوماتية، التي تعتبر "مؤسسة عمومية ذات طابع إداري، تتمتع بالشخصية المعنوية والاستقلالية المادية، فتتكفل بجملة من المهام، من بينها اقتراح كيفيات اعتماد مزودي خدمات التدقيق في مجال

أمن هذا النوع من الأنظمة" و "السهر على جمع وتحليل وتقييم المعطيات المتصلة بمجال أمن الأنظمة المعلوماتية لاستخلاص المعلومات الملائمة التي تسمح بتأمين منشآت المؤسسات الوطنية[18].

تقوم الوكالة أيضا بـ"تحديد معايير وإجراءات منح علامات الجودة و/أو التصديق و/أو اعتماد المنتجات ومقدمي الخدمات في مجال أمن الأنظمة المعلوماتية"، إلى جانب ذلك.

وبموجب ذات المرسوم الرئاسي، فإن الوكالة "مؤهلة لطلب أي وثيقة أو معلومة مفيدة للقيام بالمهام الموكلة إليها من الهيئات والمؤسسات والمتعاملين المزودين بنظام إعلام".

وسيكون على المؤسسات والإدارات والهيئات العمومية والمتعاملين الخواص، تعيين مسؤولهم المكلف بأمن الأنظمة المعلوماتية "في أجل أقصاه سنة" ابتداء من نشر المرسوم في الجريدة الرسمية[19]

تأسس في عام 2008 مركز الوقاية من جرائم التكنولوجيا لإعلامية والجرائم المعلوماتية التابع للدرك الوطني، بهدف توفير نظام معلوماتي لخدمة لأمن العام. تشمل مهامه تحليل البيانات والمعلومات المتعلقة بالجرائم المعلوماتية وتحديد هوية الجناة، سواء كانوا أفرادا أو عصابات، وذلك لتأمين الأنظمة المعلوماتية وحمايتها، بالإضافة إلى مساعدة لأجهزة لأمنية لأخرى في أداء مهامها[20].

كما تأسست في عام 2011 المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية لأمن الوطني، وفي عام 2015 تأسست المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيا لإعلام والاتصال. في الشقوق لأمنية، تأسست في نفس العام مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة، وهي تابعة لدائرة لاستخبارات والتحضير للجيش الشعبي الوطني، وتهدف إلى تخطيط وتنسيق ومتابعة تقدم السياسة الشاملة للدفاع السيبراني لضمان الحماية ضد التهديدات السيبرانية لأنظمة المعلومات وشبكات الاتصالات.[21]

وبالنسبة للمصالح المدنية التابعة لوزارة الدفاع الوطني، تأسس المركز الوطني للإشارات والحروب الإلكترونية في عام 2019، وهو يعمل تحت إشراف دائرة لإشارات وأنظمة المعلومات والحروب الإلكترونية، التابعة للوزارة، وهو مختص بمجال الدفاع السيبراني.[22]

وفي المجال المدني، تشمل هذه المصالح والمؤسسات الهيئة الوطنية لمكافحة جرائم التكنولوجيا لإعلامية والاتصال ومكافحتها، التي أنشئت بموجب القانون رقم 04-09، والتي تعمل كسلطة إدارية مستقلة تحت إشراف وزارة العدل، وتهدف إلى اقتراح استراتيجيات وطنية للوقاية من جرائم التكنولوجيا لإعلامية والاتصال ومكافحتها، وتنسيق عمليات الوقاية والمكافحة في هذا المجال[23].

المحور الثالث: لامن السيبراني في الجزائر – توجهات لتعزيز القدرات و التدريب نحو مستقبل امن

بعد اتخاذ النهج السابق لمواكبة التحولات العالمية في مجال السياسات العامة السيبرانية، وتطوير منظومة قانونية ومؤسساتية في الفترات السابقة، ومع التطور التكنولوجي والرقمي المتسارع، توجهت الجزائر الى اتخاذ استراتيجية شاملة لتعزيز لأمن السيبراني في الجزائر. شملت هذه لاستراتيجية تطوير سياسات وإجراءات جديدة، وتعزيز البنية التحتية السيبرانية، وتعزيز الوعي السيبراني.

وجه الرئيس الجزائري، عبد المجيد تبون، توجيهات حاسمة نحو تطوير استراتيجية وطنية شاملة في الميدان الرقمي، تجمع بين الاستباق والوقاية، بهدف مواجهة التحديات الناشئة في الفضاء السيبراني. يأتي هذا في سياق تصاعد الاهتمام بمواجهة التهديدات في البيئة الرقمية، حيث نبهت وزارة الدفاع إلى محاولات اختراق تستهدف التجسس والتخريب، مما أدى إلى حدوث انسداد وفوضى داخل البلاد.

تعكس هذه التوجيهات أهمية مسألة التهديدات السيبرانية في الأجندة الوطنية الجزائرية. وتظهر مشاركة الرئيس عبد المجيد تبون ورئيس أركان الجيش السعيد شنقريحة في الملتقى الذي نظمته وزارة الدفاع حول "الإستراتيجية الوطنية للأمن السيبراني"، استحقاق هذا الموضوع أحد أولويات السياسة الوطنية. يتجلى ذلك في كلمة الرئيس في افتتاح الملتقى:[24]

"إن تحديد التهديدات السيبرانية ووضع آليات الرقابة والرصد الناجعة وجاهزية لإستراتيجية في حالات الخطر، يشكل اليوم أحد أهم الشروط لإستباقية لتوفير الحماية اللازمة والكاملة للمنشآت الحيوية بشكل آمن ومستمر، وذلك ضمن منظومة التكفل بالأمن الوطني، بأبعاده السياسية والعسكرية والاقتصادية والمجتمعية بل وحتى التكنولوجية، وهو لأمر الذي يستوجب تطوير إستراتيجيتنا الوطنية المتكاملة في المجال الرقمي، والجمع بين لاستباقية والوقاية من التهديدات في الفضاء السيبراني، وحماية المنظومات والمعطيات، والسهر على ترقية ثقافة رقمية مواطنيه ووطنية عمادها التحسين المستمر و اليقظة لإستراتيجية لكل المؤسسات"

وأكد الرئيس تبون أن كفاح لأمان السيبراني يعتمد بشكل أساسي على تعزيز العنصر البشري وتنمية الكفاءات المتخصصة:[25]

"إن كسب رهان لأمن السيبراني يعتمد أساسا على تثمين العنصر البشري الذي تنبثق منه الكفاءات المتمرسة، المدركة لحيوية المهام المسندة إليها.وهو ما نوليه الأهمية القصوى في توجه الدولة لإحداث نقلة نوعية على مستوى تسيير الشأن العام، من خلال وضع لأسس لإستراتيجية وطنية مدروسة للرقمنة، وهو خيارنا السيادي، المبني على إدراكنا الجماعي لإرتباط التنمية المنشودة بترشيد الحكامة، والرفع من جودة أداء المؤسسات، وتثمين القدرات و تعبئة الموارد، فالرقمنة التي ما فتئت أشدد على ضرورة تجسيدها، ليست عملية تقنية بحتة، بل هي قناعة راسخة، و في صلب أولويات بناء الجزائر الجديدة".

السيد الفريق أول أكد على وعي الجزائر العميق بأهمية لأمن السيبراني، الذي أضحى ضرورة حتمية من أجل التصدي لكل التهديدات التي قد تستهدف الأنظمة الحساسة والحيوية للدولة:[26]

"إن الجزائر تعي جيدا أهمية لأمن السيبراني، الذي أضحى ضرورة حتمية، من أجل مواجهة كل أشكال المخاطر والتهديدات التي تستهدف الأنظمة الحساسة والحيوية للدولة، بمنطق استباقي ووقائي.

ومن أجل التصدي لهذه التهديدات، فإنه من الضروري التحلي باليقظة، وتضافر جهود كل لأطراف المعنية، مدنية وعسكرية، والسهر على تشارك الوسائل التقنية المستعملة، هذا فضلا عن لاعتماد على الكفاءات الجزائرية، المتواجدة داخل الوطن وخارجه، مع العمل على التحكم في مختلف مستويات الفضاء السيبراني، من بنية تحتية وبرمجيات ومحتوى وطني، بمنطق سيادي ورؤية إستراتيجية طويلة المدى".

رئيس الجمهورية، عبد المجيد تبون، قد أشاد بإنشاء القطب المتخصص لمكافحة الجرائم السيبرانية، مع التأكيد على أهمية العمل السريع في تأسيس هذا القطب ومعالجة الجرائم السيبرانية التي تمثل تحديا حاليا أمام العدالة. وأكد تبون أن الجرائم الإلكترونية أصبحت أكثر خطورة من الجرائم التقليدية، وأنها انتقلت من التهديدات الفردية إلى المساس بأمن الدولة الجزائرية.[27]

يهدف هذا القطب إلى التصدي لحالات المساس بحرية التعبير، بجانب التركيز على تشديد العقوبات للمتورطين في نشر لأخبار المضللة التي تشكل تهديدا لأمن واستقرار الوطن. وقد تم تعديل قانون لإجراءات الجزائية بهذا السياق، بهدف تشديد لإجراءات والعقوبات المتخذة ضد بعض أشكال الجرائم السيبرانية[28].

وفي هذا السياق، أصبح من الضروري التصدي لمثل هذه الهجمات من خلال التحضير الجيد لها من قبل جميع المصالح المعنية. ومن المهم أيضا تحديد الآليات والمهام والصلاحيات لكل لأطراف المشاركة، لضمان التنسيق الفعال بينها.

وفي ظل التطورات، أصبحت الجرائم المعلوماتية تشكل تهديدا حقيقيا للأمن القومي، حيث انتقلت من جرائم تخريب البيانات الشخصية إلى لاعتداء على البنية التحتية، مهددة بذلك الاقتصاد الوطني وأمان الدولة واستقرارها[29]

في تصريح لـ "صوت لأحرار"، دعت الدكتورة دليلة العوفي، الباحثة المتخصصة في مجال لأمان السيبراني والاتصال الرقمي، إلى ضرورة اتخاذ حلول تستهدف تعزيز "السلامة السيبرانية"وتعزيز الحوكمة السيبرانية.وأشارت الباحثة إلى أن تحقيق هذه الأهداف يتطلب وضع استراتيجية شاملة للأمان السيبراني، ترويج لثقافة التوعية بجرائم لأمان السيبراني، وتعزز بناء قدرات البشر، مستفيدة من أفضل الممارسات المتاحة على مستوى العالم، وتتماشى مع استراتيجية الوطنية لتحقيق أداء حكومي فعال.[30]

وأكدت الدكتورة دليلة العوفي على أهمية إنشاء وكالة للأمن السيبراني أو مرصد وطني أو هيئة تشرف على تحقيق لأمان السيبراني، تتولى التنسيق بين المؤسسات المعنية بالأمن السيبراني، وتدعم تنفيذ لإجراءات المشتركة بين مختلف القطاعات، بهدف ضمان لأمن السيبراني لبرامج تطوير أنظمة الرقمنة والتحول الرقمي بشكل آمن. كما أشارت إلى أن تحقيق لأمن السيبراني يتطلب مشاركة جميع لأطراف الفاعلة من القطاعين العام والخاص، والمجتمع المدني، وكذلك الهيئات البحثية والأكاديمية[31]

وبالنسبة للتعليم الجامعي، أكدت الباحثة على ضرورة إعادة النظر في برامج الجامعات لتكون متناسبة مع عصر الرقمنة والذكاء لاصطناعي. وشددت على ضرورة تحديث برامج مادة تكنولوجيا لإعلام والاتصال في مختلف التخصصات، مع إعطاء اهتمام خاص لتكنولوجيا المعلومات ولأمان السيبراني. وأشارت إلى ضرورة إدراج مادة لأمان السيبراني والتربية الرقمية ضمن المناهج الدراسية من المرحلة المتوسطة حتى الجامعية[32]

خاتمة

في ختام هذه الدراسة الشاملة حول تعزيز لأمن السيبراني في الجزائر، يبرز الأهمية القصوى لتفحص التحديات ولاحتياجات الراهنة كمنصة أساسية لتوجيه الجهود نحو التحسين والتطوير في هذا الميدان الحيوي.

بتحليل التحديات السيبرانية التي تواجه الجزائر، يظهر بوضوح أن الأمن السيبراني لا يقتصر على أن يكون متطلبا تكنولوجيا فحسب، بل يشكل جزءا أساسيا من استقرار الوطن ويعد دعامة أساسية للتنمية المستدامة.

توصلت هذه الدراسة إلى تحديد التحديات الرئيسية، حيث كشفت عن تطور هجمات الإلكترونية المتقدمة، وعن ضعف في البنية التحتية السيبرانية، ونقص في الوعي السيبراني. هذه النتائج تسلط الضوء على ضرورة التفاعل واتخاذ إجراءات فعالة ومستدامة لتعزيز الأمان السيبراني.

توصيات ومقترحات و نظرة مستقبلية:

1. تعزيز التعاون الدولي:

- من الضروري تعزيز التعاون الدولي في ميدان الأمن السيبراني، بهدف تيسير تبادل الخبرات وتقديم الدعم المتبادل لمواجهة التحديات السيبرانية المشتركة. يتعين تعزيز هذا التعاون الدولي على مستوى السياسات والتقنيات، مما يساهم في تعزيز قدرة الدول على التصدي للتهديدات السيبرانية بفعالية وفي تعزيز المرونة والأمان الرقمي على الصعيدين الوطني والدولي.

2. تطوير برامج تدريب متقدمة:

- ينبغي تطوير وتنفيذ برامج تدريب متقدمة بشكل دوري، تستهدف تعزيز وتطوير مهارات وقدرات الكوادر الفنية المختصة في مجال الأمن السيبراني. يهدف هذا التدريب إلى تزويد الفرق الفنية بالمعرفة والمهارات اللازمة لمواكبة التطورات السريعة في مجال الأمن السيبراني والتصدي للتحديات المتزايدة بفعالية. يسهم هذا النهج في تحسين قدرة الكوادر على تنفيذ استراتيجيات أمان متقدمة وتطبيق أفضل الممارسات في مجال الحماية الرقمية.

3. الاستثمار في البنية التحتية:

-يجب التعزيز في استثمارات تحديث وتعزيز البنية التحتية السيبرانية كجزء أساسي من الاستراتيجية الوطنية في الجزائر. يتعين زيادة حجم الاستثمار لضمان تحديث الأنظمة وتطويرها، مما يعزز فعالية الاستجابة للتحديات الرقمية المتزايدة. يسعى هذا الاستثمار إلى تحسين قدرة الجزائر على مواجهة التهديدات السيبرانية المتطورة وتحقيق مستويات عالية من الأمان والاستدامة في البنية التحتية التكنولوجية.

في تفعيل رؤيتنا المستقبلية لمجال الأمن السيبراني في الجزائر، يبرز توجه إيجابي يفيد بالتحول البارز نحو مستقبل يحمل في طياته تقدما هاما في هذا القطاع الحيوي. من خلال تنسيق فعال للجهود الحكومية وتعاون مستدام مع الشركاء الدوليين، يمكن تحقيق تحسين ملحوظ في جهود تعزيز الأمن السيبراني. يعزز هذا التحول استقرار البلاد ويشكل ركيزة أساسية للتنمية المستدامة في هذا العصر الرقمي الذي يتسارع بوتيرة سريعة. وعبر اعتماد توصيات هذه الدراسة والاستفادة الكاملة من الخبرات الدولية، يمكن للجزائر تعزيز قدراتها السيبرانية والتجهيز للمستقبل يعتبر تحدياته ويجسد فعالية استدامة في مجال الأمن السيبراني.

المراجع:

1- ادريس عطية ،مكانة الأمن السيبراني في منظومة الامن الوطني الجزائري ،مجلة مصداقية ، العدد 1 دسمبر1 سنة 2019

2- الملتقى الوطني حولا لإستراتيجية الوطنية للأمن السيبراني: من أجل جزائر صامدة سيبرانيا - وزارة الدفاع الوطني غلى الموقع :
https://www.mdn.dz/site_principal/sommaire/actualites/ar/2023/juin/cna07062023ar.php
3- القانون .04-09(2009) . المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجا لإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد ،47 الصادرة بتاريخ 08 أوت 2009.
4- القانون.04-15 (2015). المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الالكترونيين ، الجريدة الرسمية، العدد،06 الصادرة بتاريخ 10 فيفري 2015.
5- القانون.04-18(2018). المتضمن القواعد العامة المتعلقة بالبريد و الاتصالات الالكترونية ، الجريدة الرسمية ، العدد،27 الصادرة بتاريخ 13 ماي 2018.
6- بلرة سمير ،لامن السيبراني في الجزائر ، المجلة الجزائرية للامن الانساني ، العدد 04 ، جويلية 2017 .
7- بورياح سلمة ،السياسات العامة الجزائرية في مجال السيبرانية: الواقع والتحديات ،دفاتر السياسة والقانون المجلد: /15 العدد: 01)2023) ص ص: -374 392 ، ص 280
8- وكالة الانباء الجزائرية،صدور المرسوم المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية،03 فيفري 2020 على الموقع :
https://www.aps.dz/ar/algerie/83191-2020-02-03-13-54-37
9- سعاد بولقرون ، الجريمة السيبرانية... التهديد الجديد للإقتصاد الوطني جريدة صوت لاحرار على الموقع :https://bit.ly/3w52HJq

الهوامش

[1]سعاد بولقرون، الجريمة السيبرانية... التهديد الجديد للإقتصاد الوطني ،جريدة صوت لاحرار على الموقع :https://bit.ly/3w52HJq

[2]مرجع نفسه .

[3]بلرة سمير ، لامن السيبراني في الجزائر ، المجلة الجزائرية للامن الانساني ، العدد 04 ، جويلية 2017 ص 275 و ما بعدها

[4]مرجع نفسه.

[5]مرجع نفسه

[6]سعاد بولقرون ، الجريمة السيبرانية... التهديد الجديد للإقتصاد الوطني ،مرجع سبق ذكره .

[7]مرجع نفسه.

[8]مرجع نفسه.

[9]ادريس عطية، مكانة لأمن السيبراني في منظومة لامن الوطني الجزائري ،مجلة مصداقية ، العدد 1 ،دسمبر1 سنة 2019 ص،ص 111-110

[10]مرجع نفسه.

[11]مرجع نفسه.

[12]سعاد بولقرون ،الجريمة السيبرانية... التهديد الجديد للإقتصاد الوطني ،مرجع سبق ذكره.

[13]بورياح سلمة، السياسات العامة الجزائرية في مجال السيبرانية: الواقع والتحديات ،دفاتر السياسة والقانون ،المجلد: ،15 العدد: 01)2023) ص ص: -374 392 ، ص 280

[14]القانون .04-09(2009) . المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجا لإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد ،47 الصادرة بتاريخ 08 أوت 2009.

[15]القانون.04-15 (2015). المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الالكترونيين ، الجريدة الرسمية، العدد،06 الصادرة بتاريخ 10 فيفري 2015.

[16]القانون.04-18(2018). المتضمن القواعد العامة المتعلقة بالبريد و الاتصالات الالكترونية ، الجريدة الرسمية ، العدد،27 الصادرة بتاريخ 13 ماي 2018.

[17] وكالة الانباء الجزائرية ،صدور المرسوم المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية،03 فيفري 2020 على الموقع :
https://www.aps.dz/ar/algerie/83191-2020-02-03-13-54-37

[18] مرجع نفسه .

[19] مرجع نفسه.

[20] بورياح سلمة ،السياسات العامة الجزائرية في مجال السيبرانية: الواقع والتحديات ،مرجع سبق ذكره .

[21] مرجع نفسه

[22] مرجع نفسه

[23] مرجع نفسه

[24] الملتقى الوطني حولا لإستراتيجية الوطنية للأمن السيبراني: من أجل جزائر صامدة سيبرانيا - وزارة الدفاع الوطني غلى الموقع :
https://www.mdn.dz/site_principal/sommaire/actualites/ar/2023/juin/cna07062023ar.php

[25] مرجع نفسه.

[26] مرجع نفسه.

[27] سعاد بولقرون ، الجريمة السيبرانية... التهديد الجديد للإقتصاد الوطني ،مرجع سبق ذكره .

[28] مرجع نفسه .

[29] مرجع نفسه.

[30] مرجع نفسه.

[31] مرجع نفسه.

[32] مرجع نفسه.

الحقوق الرقمية وتحديات الأمن السيبراني في ظل أنظمة الذكاء الاصطناعي (في القانون المقارن)

Digital rights and Cybersecurity challenges, in light of Artificial Intelligence systems (in comparative law).

بلعروسي أمين(*)، جامعة حسيبة بن بوعلي الشلف، a.belarouci@univ-chlef.dz

الدكتور عبابسة حمزة، جامعة حسيبة بن بوعلي الشلف، h.ababsa@univ-chlef.dz

ملخص:

في ظل التطور الرهيب لوسائل الاتصال خاصة الانترنيت، ظهر إلى حيز الوجود القانوني جيل رابع من الحقوق والحريات تتم ممارستها في البيئة الرقمية، وهو جيل جديد من الحقوق والحريات أسست له منظمة الأمم المتحدة ولأول مرة سنة 2016 عبر قرار صادر عن مجلس حقوق الإنسان أين اعترفت بالحقوق الرقمية كحق أساسي من حقوق الإنسان. ليتوجب على الدول أن تقوم بإصدار تشريعات تؤسس لهذه الحقوق وتحميها سواء عبر المنظمات الدولية، التكتلات الإقليمية أو التشريعات الوطنية، كما ينبغي على الدول من أن تطور من آليات الضبط الإداري التقليدي إلى ضبط إداري الكتروني يعمل على ضبط الحريات العامة في البيئة الرقمية من جهة، والحفاظ على النظام العام من جهة أخرى، ومنه ضمان الأمن السيبراني بصفة عامة، وهو ما سنبينه من خلال هذه المداخلة، أين سنتناول معالجة القانون المقارن للضبط الإداري وتوجيهه إلى حماية هذه الحقوق الرقمية، خاصة وسائل التواصل الاجتماعي وحتى الأرضيات الرقمية الخاصة بالإدارات والهيئات العمومية، التي تتعرض كل دقيقة إلى هجمات منسقة من الداخل ومن الخارج على حد سواء، وهو أهم دعامة من دعامات الأمن السيبراني.وهل نجحت التشريعات الدولية والوطنية في التصدي لهذه الظاهرة.

الكلمات المفتاحية: حقوق الإنسان، الضبط الإداري، الحقوق والحريات العامة، القانون، الأمن السيبراني.

Abstract ***In light of the terrible development of means of communication, especially the Internet, a fourth generation of rights and freedoms has come into legal existence that is practiced in the digital environment. It is a new generation of rights and freedoms that was established by the United Nations for the first time in 2016 through a resolution issued by the Human Rights Council, where it recognized the rights. Digital as a basic human right.***

States must issue legislation that establishes and protects these rights, whether through international organizations, regional blocs, or national legislation. States must also develop traditional administrative control mechanisms to electronic administrative control that works to control public freedoms in the digital environment on the one hand, and preserve On the public order on the other hand, including ensuring cybersecurity in general, which we will explain through this intervention, where we will address the comparative law's treatment of administrative control and direct it to protecting these digital rights, especially social media and even the digital floors of public administrations and bodies, which are exposed. Every minute, there are coordinated attacks from both inside and outside, which is the most

important pillar of cybersecurity. Have international and national legislation succeeded in confronting this phenomenon?

KeyWords: ***Human rights, administrative control, public rights and freedoms, law, Cybersecurity.***

مقدمة:

تعتبر حماية الحقوق والحريات العامة في ظل إجراءات الضبط الإداري الشغل الشاغل لجميع الدول مهما كانت طبيعة النظام السائد فيها، سواء كانت دولا نامية أم متقدمة، ومع توسع استعمالات الوسائط الرقمية والإلكترونية أصبح لزاما على هذه الدول أن تطور من لأساليب التقليدية للضبط الإداري، وباعتبار أن هدف لأخير الحفاظ على النظام العام قد ينجر عنه في بعض لأحيان تقييد للحريات الفردية بسبب مبررات يفرضها الصالح العام، وإن كان من حق الفرد أن ينعم ببعض الحقوق في البيئة الرقمية، فهذا التمتع لا يكون بصورة مطلقة، ودون أي ضوابط تكبح جماح التمتع بهذه الحقوق، كي لا يؤثر ذلك في حقوق وحريات لآخرين، فالتقيد بالأطر العامة والالتزام بضوابط استعمال الوسائل التي تمارس من خلالها هذه الحريات هي التي تميز الحرية عن الفوضى، وتجعل من هذا لاستعمال سلوكا حضاريا، وهذا ما يسمى بالضبط الإداري.

وأمام التطور وسائل الاتصال ولاستعمال الرهيب الذي لا يكاد ينقطع تواليا من الأفراد إلى حد الإدمان إن صح التعبير، كان لا بد على الدولة أن تعمل على ضمان عدم خروج استعمال هذا الحق عما هو مشروع ومسموح به، ومما سبق تثور لدينا لإشكالية التالية: هل هناك ضمانة فعلية لممارسة الحقوق والحريات في الفضاء الرقمي؟ وكيف تطور الضبط الإداري بالموازاة مع انتشار الحقوق والحريات الرقمية في ظل تحديات لأمن السيبراني للدول؟ وما هي حدود سلطاته في هذا المجال؟ وما مدى تطور التشريعات المقارنة بهذا الخصوص؟

وللإجابة على هذه لإشكالية سنقسم إجابتنا إلى محورين: أولهما نستعرض فيه ماهية الحقوق والحريات العامة في البيئة الرقمية وعلاقتها بالأمن السيبراني، وثانيهما نبين فيه تطور الضبط الإداري في ظل أنظمة الذكاء لاصطناعي وتحديات تحقيق لأمن السيبراني.

المحور الأول: الحريات العامة في البيئة الرقمية وعلاقتها بالأمن السيبراني.

المحور الثاني: الضبط الإداري الإلكتروني في ظل أنظمة الذكاء لاصطناعي وتحديات لأمن السيبراني.

المحور الأول: الحريات العامة في البيئة الرقمية وعلاقتها بالأمن السيبراني.

القول بأن لك الحق في أن تبقى وحيدا وشأنك، أو لك الحق بأن تعيش وحدك، فذلك يعني أنك تريد الابتعاد عن الضوضاء وجلبة الأشياء المحيطة بك، عن محيطك الوظيفي وحتى المجتمع، فقط بتنعم ببعض الهدوء والسكينة وأن تقوم بما تريد بعيدا عن أعين الناس، وهو ما يتوق إليه أشهر شخصيات المجتمع بفعل ملاحقة الغير لهم ومحاولة معرفة ما يقومون به، هذا الحق الأساسي في الخصوصية عرفته المحكمة العليا الكندية بأنه: " نطاق ضيق يسمح بالاستفادة الشخصية ، والذي في إطاره تقرر الاختيارات الخاصة حسب طبيعتها"[1].

تطور مفهوم الحريات العامة مع تطور الوسائل المستعملة من قبل الأفراد والمحيطة بهم في بيئتهم، بحيث أصبحت وسائل التواصل الاجتماعي بمثابة البيئة الحاضنة لهذه الحريات وممارستها بعيدا عن أي احتكاك أو تضييق خاصة الحريات السياسية والدينية، أين أصبحت تعقد ملتقيات واجتماعات خاصة بكيانات أو أحزاب أو مذاهب متعددة في غرف الدردشة المغلقة على مختلف التطبيقات في الفضاء الالكتروني.

المطلب الأول: البيئة الرقمية كفضاء جديد لممارسة الحريات العامة.

عرفت مسيرة حقوق الإنسان وبتعاقب العصور تطورا كبيرا في مفهومها وعناصرها وصولا إلى تعدد أجيالها، حيث أصبحت الحقوق الرقمية مثل الحق في نشر أو إنشاء محتوى رقمي عبر الحق في استخدام حاسوب أو أي جهاز آخر مشابه، أو برمجيات وشبكات دون أي قيد على ذلك النشاط، هذا الحق يتولد عنه أو يرتبط بالعديد من الحقوق الأخرى مثل الحق في حرية الرأي والتعبير والحق في الخصوصية والحق في تداول المعلومة، والحق في المعرفة العلمية وغيرها من الحقوق والحريات.

وتلعب وسائل الإعلام والاتصال بالإضافة إلى الانترنيت دورا حاسما في احتضانها لمختلف الأنشطة الإنسانية باعتبارها السياق المكاني الأسهل والأفضل لممارسة مختلف الحقوق والحريات العامة، بحيث يتم تبادل الرسائل التي تشير إلى التاريخ والمكان المزمع الالتقاء فيها مثل المواقع، البوابات، المنتديات، غرف الدردشة، وطريق المعلومات السريع[2].

كما لا ننسى الدور الذي لعبته وسائط الإنترنيت في الاتصالات بين أفراد الشعوب التي قامت بثورات لأجل تغيير أنظمة الحكم ببلدانها، مثل تونس ومصر...الخ، وحتى في الحفاظ على نظام الحكم من هيمنة الانقلابيين مثلما حدث في محاولة الانقلاب الفاشلة بتركيا صيف 2016.

الفرع الأول: الحقوق الرقمية حق من حقوق الإنسان.

توالت أجيال حقوق الإنسان منذ الإعلان العالمي عن حقوق الإنسان، حيث يعتبر الجيل الأول من حقوق الإنسان المتمثل في الحقوق المدنية والسياسية، بمثابة المؤسس لترسيخ وتطور مفهوم حقوق الإنسان، ليظهر الجيل الثاني المتمثل في الحقوق الاقتصادية الاجتماعية والثقافية، ثم الجيل الثالث الخاص بالحقوق الجماعية في البيئة والتنمية، ليأتي الجيل الرابع المعاش حاليا وهو جيل الحقوق الرقمية أو الإلكترونية.

لم تتفق الاتجاهات التي تصدت لتحديد تعريف مانع للحقوق الرقمية، بل حاولت تحديد المدلول المحدد لهذه الحقوق كتبيان العناصر الخاصة بهذه الحقوق وما تشتمل عليه من مكاسب، وهذا بسبب حداثة عهدهم بهذا النوع من الحقوق، ولم يتم التعمق في هذه الظاهرة بدراسات معاصرة إلا نادرا، لكن أغلبهم يعرف الحقوق الرقمية بأنها: " حق لكل فرد من الأفراد في الوصول واستخدام وإنشاء ونشر محتوى رقمي، واستخدام الحواسيب أو أجهزة أخرى أو برمجيات أو شبكات اتصال دون أية قيود"[3].ومن هنا تتولد عديد الحقوق والحريات الأخرى كحرية الرأي

والتعبير وحرية تداول المعلومات، والحق في الخصوصية والحق في التنمية والمعرفة وغيرها من الحقوق والحريات الأخرى.

ومما سبق نستخلص أن الحقوق الرقمية تقوم على أربعة مبادئ أساسية وهي: إتاحة الوسيلة – الحق في الخصوصية، حرية التعبير، حرية التطوير والابتكار.

الفرع الثاني: خصائص ومميزات الحقوق الرقمية.

منذ أن صدر القرار الدولي عن مجلس حقوق الإنسان سنة 2013 أين أقر بالحقوق الرقمية واستعمالها في الفضاء الرقمي، وبأنها لا تقل أهمية عن الأجيال السابقة للحقوق والحريات اتسمت هذه الحقوق والحريات بمايلي[4]:

-أولا حقوق حديثة النشأة وسريعة الأثر.

الحقوق الرقمية حقوق حديثة بسبب حداثة الثورة الحاصلة في تكنولوجيا المعلومات، وما فرضه الفضاء الرقمي من استعمال للبيانات وما أعطته من سمة أساسية للحياة الحالية المعاصرة، أين أصبح الفرد لا يستغني عن جهاز حاسوبه الشخصي، أو جهاز الهاتف الذكي وهو ما يعني أنه متصل على مدار الساعة بهذا الفضاء الافتراضي الرقمي. خاصة وما لها من فائدة في اختصار الوقت المطلوب للحصول على المعلومة، أو تقريبه للمسافات بين الأفراد مهما تباعدت المسافات عبر اتصالاتهم المرئية، وهي حقوق متصلة اتصالا وثيقا بالشبكة الدولية للمعلومات.

-ثانيا حقوق قانونية بحتة.

هناك حقوق طبيعية متجذرة ترتبط بالفطرة الإنسانية وهي حقوق أصيلة، وهناك حقوق قانونية يقرها ويعترف بها القانون وهو مصدرها، لذا تعتبر الحقوق الرقمية حقوقا قانونية أقر بنشأتها وأعطاها الأساس القانوني في ممارستها وحمايتها وصونها من أي تدخل لأي جهة كانت.ولعل التشريعات المتتالية دوليا و وطنيا لأجل حماية الحقوق الرقمية لأبرز دليل على إقرار القانون بنشأتها و حمايتها وكيفيات تقنين استعمالاتها بعيدا عن الشبهات ومحاولة النأي بمستعمليها عن الجرائم الإلكترونية التي ظهرت هي كذلك تزامنا و الطفرة الحاصلة في هذا المجال.

-ثالثا حقوق ذات طابع عالمي.

إن اتصال الحقوق الرقمية بالشكة الدولية للمعلومات وما تفرزه من انتشار عالمي سريع ، أعطاها طابعا عالميا خاصة مع تزايد رغبات الأفراد في استعمال وإشباع حاجاتهم من الحق في الاتصال والتصفح ونشر ومراسلة وإنشاء مدونات مختلفة الأهداف، وهو ما يشترك فيه جميع أفراد ساكنة هذا العالم مهما تعددت وتنوعت لغاتهم وديانتهم وأعراقهم، إلا أن الهدف من الحق في استعمال الشبكة المعلوماتية هو نفسه.

رابعا الحقوق الرقمية أساسية.

احتوى قرار مجلس حقوق الإنسان بخصوص الحقوق الرقمية على وصفها بأنها أساسية ضمن حقوق الإنسان، وبأنها ليست كمالية أو ثانوية أو للترفيه وما شابه، وهو الوصف الذي تنسجم معه طبيعة الحقوق الرقمية بسبب الحاجة الماسة لها من قبل الأفراد، إلى أن أصبحت متداخلة في جميع مناحي حياة الإنسان ومرافقة له، وهو ما تنبهت له المؤسسات والشركات العالمية في هذا المجال كي تستقطب اهتمام مستعملي الشبكة المعلوماتية.

المطلب الثاني: القواعد القانونية لحماية الحريات العامة في البيئة الرقمية:

كان في ما مضى الدفاع عن حرية الصحافة بمثابة صرخة تنم عن تطور حتمي للدفاع عن حق الإنسان في المعلومة وتبادلها بسرعة، لكن ومع تطور الزمن تطورت الوسائل المستعملة في هذا الشأن أصبحت النصوص

القانونية المستعملة قبل ظهور الانترنيت ومنه البيئة الرقمية، تحتاج إلى التعديل الجوهري في المفهوم وحتى في الوسائل القانونية المتاحة لأجل حماية الحق في المعلومة والحق في الاتصال وتبادل المعلومات الشخصية وحمايتها هي كذلك من كل سرقة أو تضييق باعتبارها حق أساسي وهو الحق في الخصوصية.

الفرع الأول: التعريف القانوني للاتصالات العامة على الانترنيت.

أخذ المشرع الفرنسي على عاتقه المبادرة في هذا الخصوص، حيث صدر القانون2004/575 المتعلق بالثقة في الاقتصاد الرقمي[5]، حيث نص في المادة الأولى منه على استحداث فئة جديدة: " الاتصالات العامة عن طريق مختلف الوسائل الالكترونية" حيث تشمل:

1- اتصالات السمعي البصري.
2- اتصالات عامة على الانترنيت.

وقد عرفت المادة 02 من نفس القانون الاتصالات العامة على الانترنيت على أنها كل ما يتم وضعه تحت تصرف الجمهـور أو فئـة معينة منـه، عن طريق الاتصال الالكتروني من علامـات وإشارات وكتابـات وصـور أو أصوات ورسائل من أي نوع كان لا يكون لها طابع المراسلات الخاصة[6].

مما سبق نرى أن المشرع الفرنسي قسم هذا المحتوى الرقمي للحقوق والحريات العامة على الفضاء الرقمي إلى طابع عام يشمل المناشير على مختلف المدونات، وطابع خاص بحت يشمل رسائل البريد الالكتروني والرسائل الصوتية على مختلف التطبيقات وحتى المرئية منها، وهي أدوات يتم الوصول إليها بعد الدخول بكلمة سر خاصة بالمعني، يتم تبادل هذه الرسائل في فضاء إلكتروني محمي بأعلى درجات الحماية والتشفير الدوري بتحديث آلي يتم عرضه على المشتركين في هذه البرمجيات على الفضاء الرقمي.

الفرع الثاني: الحماية القانونية للاتصالات العامة في البيئة الرقمية ضمان للأمن السيبراني.

منذ ظهور الاتصالات العامة لأول وانتشار استعمالها في المجال العسكري، تم احتكار تلك التكنولوجيا لتسهيل التواصل بين مختلف تشكيلات ووحدات الجيوش، ومع ظهور الثورة الصناعية وتكالب الدول على تطوير اقتصادياتها تم العمل على الإفراج على هذه التكنولوجيا والسماح باستعمالها مدنيا في مختلف مجالات الحياة، إلى أن وصلت إلى ما هي عليه الآن كحاضنة لجميع نشاطات الإنسان في عمله وفي تواصله مع الآخرين، لذا عمل المشرع على تحديد الأطر القانونية للبيئة الرقمية من أجل تأمين الاتصالات العامة من جهة، والعمل على الحفاظ على النظام العام من جهة أخرى.

حيث قدمت الأمم المتحدة سنة 1989 قرارا يسمح باستخدام الحواسيب في عمليات تدقيق البيانات الشخصية، لتأتي سنة 1999 لتصدر الجمعية العامة للأمم المتحدة دليلا لتنظيم استخدام الآلية للبيانات الشخصية، وفي 2013/01/18 أصدرت الجمعية العامة للأمم المتحدة قرارها الإلزامي بشأن الخصوصية في العصر الرقمي، تبعا للضجة التي أثيرت آنذاك بخصوص تدخل المؤسسات الحكومية بفضل قدراتها المتنامية للوصول إلى بيانات وخصوصيات الأفراد، أين نص هذا القرار على حرمة خصوصيات وبيانات الأفراد في ظل التقدم التكنولوجي الملاحق، كما قد أشار من خلال الفقرة الثانية لديباجة القرار الأممي واستنادا إلى المادة الثانية عشر من الإعلان العالمي لحقوق الإنسان والمادة السابعة عشر من العهد الدولي للحقوق المدنية والسياسية، في ما يخص الحق في الخصوصية وواجب الالتزام بهما دوليا، وفي الفقرة الثالثة من القرار نجد تأكيد على أن ذات الحقوق التي تثبت للأفراد في الواقع المعاش خارج الانترنيت، يجب أن تصان وتكون محمية على الانترنيت في الفضاء الرقمي بما فيها الحق في الخصوصية[7].

في هذا الخصوص نرى بأن الفضل يعود بالدرجة الأولى إلى منظمة الأمم المتحدة في التصدي لكل ما يتصل بالحقوق الرقمية، وقد تبنت في أكثر من قرار أو وثيقة صادرة عنها بوجوب تأمين الانترنيت والاتصال عبرها، كما عملت من أجل اعتراف الدول بالحقوق الرقمية، وصولا إلى القرار الصادر عن مجلس حقوق الإنسان سنة 2016 والذي أقر بأن استعمال الإنترنيت حق أساسي من حقوق الإنسان.

الفرع الثالث:الأمن السيبراني بين حرية الوصول للمعلومة وبين تهديدات الفضاء الرقمي.

أولا- مفهوم الأمن السيبراني:

تتعدد التعريفات المختلفة من حيث الصياغة للأمن السيبراني، لكنها تشترك في المنظور الذي ينظر إليه من حيث تهديد العمليات الإجرامية التي تهدد الفضاء الرقمي للدول.

تعرضت منظومة الأمم المتحدة لهجمات سيبرانية جعلتها تبادر إلى التحذير من الهجمات التي تهدد الأمن الدولي، حيث عرفت الأمن السيبراني بأنه قد ظهر أولا كتأمين خاص لمجال تكنولوجيات المعلومات والاتصالات، ليتطور فيما بعد تبعا للتهديدات المتعددة وبشكل كبير، ليصبح يتطلب أكثر من مجرد دفاعات تحركها التكنولوجيا، إلى ضرورة إدماج اعتبارات الأمن السيبراني في الإدارة المركزية للمخاطر، والتخطيط لاستمرارية الأعمال الخاصة بالسلامة والأمن الوطنيين [8].

حيث انتهجت الولايات المتحدة الأمريكية إلى التشديد على حساسية الأمن السيبراني ووجوب إعطاءه الأولوية الكاملة والتخصص الأصيل لوزارة الأمن القومي الداخلي الأمريكية، فنجدها تعرف الأمن السيبراني بأنه: "نشاط أو عملية أو القدرة أو الإمكانية التي يتم بموجبها حماية نظم المعلومات والاتصالات والمعلومات الواردة فيها، أو الدفاع عنها في حالة تضررها أو استخدامها أو تعديلها دون إذن أو تصريح لأجل استغلالها"[9].

هذا وقد ذهبت دول الاتحاد الأوروبي بعيدا في هذا المجال بأن أنشأت في سنة 2019 وكالة الاتحاد الأوروبي للأمن السيبراني European Union Cybersecurity Agency وتعرف باسمها المختصر ENISA، مقرها الرئيسي بأثينا مهمتها ولها فرع ثاني بمدينة هيراكليون باليونان دائما، معوضة للوكالة السابقة تحت إسم الوكالة الأوروبية لأمن الشبكة والمعلومات التي أنشأت سنة 2004[10]. وفي آخر تشريع له في مجال الأمن السيبراني الصادر يوم 16 جانفي 2023 عرف الأمن السيبراني بأنه كل عمل دفاعي ضد التهديدات الرقمية المتطورة بهويات إلكترونية مزورة أو معرفة تهدد البيانات الشخصية أو المعلومات والحزم البيانية الخاصة بالحكومات الالكترونية[11].

نرى بأن الاتحاد الأوروبي أكثر وضوحا وتشددا في رؤيته للأمن السيبراني من خلال الترسانة القانونية المعدلة دوريا تبعا للتقارير التي توردها الوكالة الأوروبية للأمن السيبراني، لا سيما إلزام الدول الأعضاء بالاتحاد الأوروبي بوجوب تعديل التشريعات الوطنية الخاصة بالأمن السيبراني عند صدور كل قرار في هذا المجال، وآخره القرار الخاص بتطوير الأمن السيبراني في جميع أنحاء الاتحاد الأوروبي[12].

بالنسبة لوضع الجزائر في هذا المجال فوفقا لتقرير صادر عن مؤتمر الأمم المتحدة للتجارة والتنمية لسنة 2023، (أونكتاد) أين أعدت دراسة ضمنها تقدم نسبة التغير التكنولوجي التي فرضتها أنظمة الذكاء الاصطناعي، ومدى صمودها ضد الهجمات السيبرانية، ومدى استخدام هذه الدول للابتكارات الحاصلة، صنف الجزائر ضمن مؤشر منخفض باللون البرتقالي وفي المرتبة 97 عالميا من 166 دولة[13].، وهو ما يزيد من الضغوط عاليا على المشرع كي يعزز من ترسانته القانونية في مجال الأمن السيبراني، مع دعم التقنيات المحلية في هذا المجل، وهو الأمر الذي سعت من خلاله الجزائر عبر حزمة من التدابير التي تم اتخاذها في هذا المجال، أين تم دعم مؤسسات ناشئة من قبل وزارة

المؤسسات الصغيرة والناشئة، لأجل تطوير مختلف التطبيقات والبرامج ودعم الابتكارات لأجل استخدامها محليا، ضمن شراكة مع أكبر شركة عالمية في هذا المجل وهي شركة هواوي Huwei الصينية[14]، حيث تم عقد صفقة بالتراضي لطابعها لإستعجالي أعدت بتاريخ 29-02-2024 بين الحكومة الجزائرية والشريك الصيني وتم الموافقة عليها، عبر إنشاء مركز لتخزين المعلومات لصالح المحافظة السامية للرقمنة.وتعميم استعمال التقنيات الخضراء في مجال لأمن السيبراني لكل المواقع الحكومية الجزائرية، والشبابيك الإلكترونية في مجالات الإدارات العمومية و المؤسسات الاقتصادية.

أما من جانب الترسانة التشريعية فقد جاء القانون22-06 المعدل والمتمم للأمر 66-155 المتعلق بالإجراءات الجزائية، أين تم إضافة وتخصيص القسم السابع مكرر للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، أين عمل المشرع الجزائري على تجريم هذه الأفعال وسن عقوبات تقابلها للحد من ارتكابها[15]، ليصدر سنة 2009 القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا لإعلام والاتصال ومكافحتها. كما صدر سنة 2021 المرسوم الرئاسي 21-439 المتعلق بإعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا لإعلام والاتصال ومكافحتها[16].

ثانيا- الضوابط لأساسية في مجال لأمن السيبراني وتميزه عن غيره من المفاهيم:

تتكون منظومة لأمن السيبراني من مكونات وضوابط لا بد من تكاملها فيما بينها لأجل تحقيق الهدف المتوخى من هذا النظام لأمني، وهي كمايلي[17]:

أ-أمان التطبيق: يشترط في مجال اعتماد التطبيقات الإلكترونية، ألا يحتوي على مواد ضارة تستعمل عن بعد من أجل التجسس على البيانات والمعلومات التي يحتوي عليها التطبيق.

ب-أمان السحابة: فرع من فروع لأمان الالكتروني يهدف إلى تأمين أنظمة الحواسيب السحابية Compiting cloud وهي آلية يتم عبرها طلب مساحة تخزين ذات سعة عالية للبيانات والتطبيقات، حيث يتم تقييد الوصول إلى هذه المساحة عبر أمان السحابة الذي يرتكز على التعرف بمن لهم الحق في الولوج لهذه المعلومات والبيانات.

ت-أمان انترنيت لأشياء: يختص أمان انترنيت لأشياء بتأمين لأجهزة والشبكة المتصلة بها، من التهديدات ولاختراقات عن بعد عبر الانترنيت، حيث يتم تحديد الثغرات لأمنية المحتملة عبر لأجهزة أو الشبكة، والتي تعتبر منفذا يتسلل منه المخربون والقراصنة، وهناك يتم تحييد هذه الهجمات لضمان ممارسة فعالة على مستوى لأجهزة.

ث-أمان البنية لأساسية الحيوية: تعتبر الشبكات الوطنية الخاصة بالماء ، الكهرباء والغاز وحتى الاتصالات بمثابة البنية لأساسية الحيوية للدول، لأنها تتصل بالأفراد وهو ما يشكل الشغل الشاغل لضمان لاستفادة منها وفق ترتيبات شفافة، وهو مي يوجب تأمين هذه الشبكات من مخاطر مهاجمتها قصد تعطيلها أو استعمالها في مجالات حربية مثل شبكات الكهرباء ذات المصدر الطاقوي النووي.

ج-أمان الشبكة وإدارة المعلومات ولأحداث: هو النشاط المصمم لحماية إمكانية استخدام الشبكة المعلوماتية الخاصة بك لأغراض غير مسموح بها، عبر تطوير تقنيات تأمين لأجهزة والبرامج، أين تعمل وفق مخطط إنذار استباقي يمنع الدخول إلى الشبكة ويضمن تأمين الوصول إليها.ومنع أي محاولة لنسخها أو مسحها.

ح-أمان الهوية والولوج: يتم إنشاء أنظمة لتحديد الهويات الخاصة بمستعملي لأجهزة والشبكة على حد سواء، وفق مقاربة ضمان تكامل الجهاز مع مستعمليه، وهي آلية تتطلب مصادقة لإدارة مسبقا على عدد معين من

الهويات للمستخدمين لضمان الولوج من جهة وتأمين سرية المعلومات والبيانات من أي مستخدم متطفل من جهة أخرى.

ثالثا- أنواع الجرائم السيبرانية:

تتعدد الجرائم السيبرانية حسب الهدف المتوخى منها والطرف الطي يقوم بها، وهي أربعة أنواع[18]:

1- **هجوم برامج ضارة لإختراق Malware attacks**: من أشهر أنواع الهجمات السيبرانية يتم عبر برامج معدة خصيصا لأجل اختراق الأجهزة والشبكات والخادم الخاص بالدول بأن يتم تثبيتها، للوصول إلى بيانات سرية دون علم أصحابها.

2- **هجوم التصيد الاحتيالي Phishing**: هجوم يتم عبره نسخ البيانات المخزنة لاستغلالها بشكل غير قانوني، وهو هجوم في تطور مستمر بسبب الأساليب المبتكرة من خلال التنكر في هيئة وتعريف كيان موثوق بمجرد قبول الرسالة الإلكترونية المرسلة من طرفه يبدأ الهجوم السيبراني.

3- **هجوم حجب الخدمة (DRDOD-DDOS-DOS)**: أكثر الهجمات انتشارا في الوقت الحالي يستهدف الخوادم الرئيسية للشبكة المعلوماتية، أين يتم شل النظام بصفة كاملة عبر ثلاثة أصناف وهي هجوم DOS يتم عبر إغراق الشبكة وحجب الخدمة باستخدام مصدر واحد أو جهاز واحد لتنفيذ الهجوم.وهناك هجوم DDOS يتم استعمال أكثر من مصدر لتنفيذ الهجوم لشل الحماية. والصنف الثالث هو هجوم DRDOS يشبه سابقه لكن بتنويع لأساليب الخداعية التي توهم برامج الحماية بأنها حركة عادية.

4- **هجوم الوسيط (Man In the Middle)**: يسمى أيضا هجوم التصنت أين يتم التصنت على اتصالات الكترونية أو عملية نقل بيانات ضخمة بيم المستخدمين، أين يرسل رسالة إلى أحد المستخدمين الشرعيين فيها روابط برامج ضارة تثبت على الجهاز من أجل أخذ التعريف للمشاركة في نقل البيانات.

المحور الثاني: الضبط الإداري الإلكتروني وتحديات الأمن السيبراني في ظل أنظمة الذكاء الاصطناعي.

فرض تطور مفهوم الحقوق والحريات العامة والبيئة التي تمارس فيها، على الضبط الإداري أن يطور كذلك من وسائله وأهدافه كي يساير هذا التطور الهائل في البيئة الرقمية التي تمارس فيها هذه الحقوق والحريات، بحيث لا يخل بأحد أهم المبادئ الدستورية ألا وهي عدم المساس بحق الفرد بالاتصال بالآخرين أو النشر أو حتى تلقي المعلومة. وبما أن الضبط الإداري جوهر السلطة العامة في الدولة بسبب ارتباطه الوثيق بالحقوق والحريات العامة للمواطنين بصفة مباشرة، واستخدامه للأساليب والإجراءات التي تمنع تهديد النظام العام، وبالنظر للتطور التكنولوجي الرهيب الذي مهد لوجود بيئة رقمية تمارس فيها الكثير من الحقوق والحريات، كل هذا فرض على الضبط الإداري أن يطور من مفهومه ومن أساليبه هو أيضا، فما هو الضبط الإداري الالكتروني؟

المطلب الأول:تعريف الضبط الإداري الالكتروني: تعتبر الرقابة الالكترونية من أهم مصادر البحث والتحري التي يعتمد عليها في الغالب لأجل التقصي كجرائم وسائل التواصل لاجتماعي، والجهات الإدارية المختلفة على المواقع الالكترونية[19]. ومنه جاء الضبط الإداري الالكتروني كفكرة مستحدثة نتيجة للدراسات الحديثة في القانون الإداري بعد تأثره بالتطور الالكتروني، أين أصبح يشار إليه في التشريعات المقارنة بهذا الوصف، وفي سبيل تعريف الضبط الإداري الالكتروني نتطرق لتعريفه لدى الفقهاء، ثم تعريفه في التشريعات المقارنة.

الفرع الأول- التعريف الفقهي:

في ظل حداثة مفهوم الضبط الإداري الالكتروني لم يتطرق الفقهاء إلى تعريف مانع جامع لهذا النوع من الضبط، لكن اتفق أغلبهم على أن الضبط الإداري الإلكتروني هو آلية تسمح للسلطات بمحاولة عدم منع استعمال أو تأمين

الحق في الولوج أو النشر أو استخدام الوسائط الرقمية عبر أجهزة الكمبيوتر والأجهزة الالكترونية الأخرى، وشبكات الاتصال واستخدامها بطريقة لا تعرض النظام العام إلى الخطر[20].

يجمع الفقهاء في الوقت الحالي على أن الضبط الإداري الالكتروني وفي عصر الرقمنة الشاملة لكل شيء، يوجب على المشرع العمل على تكييف القوانين لصيانة الحقوق الأساسية وصونها مسايرة للتطور الرهيب الحاصل في الفضاء الرقمي، وخاصة الحقوق الفردية الرقمية التي ترتبط ارتباطا وثيقا بالحق في التظاهر والتعبير، والحق في الخصوصية مع استعمال الكمبيوتر والهواتف والأجهزة الذكية هذا من جهة، ومن جهة أخرى تأمين الفضاء الرقمي للحفاظ على النظام العام، وهذا ما يفرضه تسابق الأفراد على الاستعمال الرهيب لكل ما هو رقمي وإلكتروني إلى حد الإدمان إن جاز لنا التعبير ذلك.

الفرع الثاني- التعريف القانوني.

تحضر الغرفة العامة للدراسات القانونية بالاتحاد الأوروبي دراسات قانونية، تعتبر بمثابة الأرضية القانونية إن جاز لنا التعبير ذلك، من أجل التوجه نحو جيل ثالث من الضبط الإداري عبر إدارة رقمية تهدف إلى حماية الخصوصية في المجال والوسائط الرقمية[21]، وقد تقدمت الدول الأوروبية بمراحل متقدمة بالنسبة للدول الأخرى في هذا المجال.

صدر في فرنسا القانون 78-12 المتعلق بالحوسبة ومعالجة الملفات والحريات، أين أشار إلى أنه يقع على عاتق الدولة حماية البيانات الشخصية للمواطنين المدخلة في الحواسيب الآلية[22]. وهو ما أسس لممارسة الحريات باستعمال الوسائل التكنولوجية وفق أطر قانونية معينة ومعدة لذلك الغرض.

ثم في سنة 1981 أصدر المجلس الأوروبي الاتفاقية رقم 108 الخاصة بحماية الأفراد أثناء المعالجة الآلية للبيانات الشخصية المعتمدة في إطار المجلس الأوروبي بتاريخ28-01-1981، والمكملة بالبروتوكول الإضافي لسنة 2001، أين تم الاتفاق على توسيع سلطات الضبط الإداري في هذا المجال ومنحها صلاحيات أوسع في مجال معالجة تدفقات البيانات عبر الحدود تحت رقم 181 ETS. والموقعة من قبل الدول الأعضاء في 08 -11- 2001، يشار إلى أن هذه الاتفاقية دخلت حيز التنفيذ في كامل الدول الأوروبية بتاريخ 01-07-2004 .

إن سلطة الضبط الإداري الالكتروني ليست جديدة أو موازية للسلطة التقليدية للضبط الإداري، وإنما تشكل امتدادا حقيقيا لها في الفضاء الرقمي، وتعكس حضور الأطراف والأهداف الأساسية للضبط الإداري ولكن في ثوب جديد ومغاير بحلة إلكترونية وبطابع فني وبرمجي.

المطلب الثاني:وسائل وآليات الضبط الإداري الالكتروني.

تلجأ الدولة إلى وسائل وآليات محددة لأجل الحفاظ على أمنها إلكترونيا، سواء من جانب نشاط الأفراد بتتبع نشاطاتهم ومراقبتها، أو بتشديد الإجراءات الأمنية الكترونيا لتفادي الجرائم السيبرانية التي تهدد أمنها الاقتصادي والاجتماعي.

الفرع الأول: وسائل الضبط الإداري الالكتروني. بالرغم من كل المزات الهامة للضبط الإداري الالكتروني لنشاط الأفراد ووسائل اتصالاتهم في الشبكة العنكبوتية ، سواء عبر المراقبة الوقائية للمعلومات أو الحجب الإداري لها ، إلا أن جدلا فقهيا أثير حول ايجابياتها وسلبياتها أو القبول بتلك الرقابة من عدمها. خصوصا أن هناك من يرى بعدم مشروعية هذا النظام لأنه يمس بالحقوق والحريات الفردية التي يتم ممارستها رقميا من خلال الوسائل والأجهزة الالكترونية، في حين أن البعض الآخر يرى إلزامية وجود هذا النظام لأهميته في محاربة الجريمة المنظمة والعابرة

للحدود والتي تتم إلكترونيا عبر وسائل التواصل الاجتماعي والشبكات الأخرى، لأجل كبح جماحها والحد من انتشارها[23].

أولا- المراقبة الوقائية للمعلومات عامل لتحقيق الأمن السيبراني.

تعتبر الرقابة الالكترونية أهم تحدي للمصالح المعنية بالأمن السيبراني من خلال البحث والتحري، كما تمارس الجهات الإدارية المختلفة مهامها الرقابية تجاه عديد الأنشطة الالكترونية في الواقع الالكتروني، حفاظا على أمن الدولة من خلال تأمين جميع العمليات التجارية والاقتصادية التي تحدث في البيئة الرقمية، لأنه وبطبيعتها الالكترونية تحتاج لهذا النوع من الرقابة للحفاظ على الواقع الأمني أو الأمن المعلوماتي الذي يعتبر العمود الفقري للفضاء الالكتروني[24].

كما عرفت الرقابة الالكترونية بأنها عملية إجراء تحقيق يباشر خلسة، بحيث ينتهك الأحاديث الخاصة تأمر به السلطة القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي لجريمة تحقق وقوعها، ويتضمن من ناحية استراق السمع إلى الحديث ومن ناحية أخرى حفظه بواسطة أجهزة مخصصة لذلك[25].

وهنا يجب أن نفرق بين أمن المعلومات والأمن السيبراني، فتأمين المعلومات هو علم يهتم بالحفاظ على سرية المعلومات والبيانات التي يقوم مستخدم الانترنيت بربطها مع مختلف شبكات التواصل أو منصات الكترونية أو تطبيقات معينة، من أي محاولة خرق أو تجسس أو استيلاء عليها وهو ما يوجب العمل بأنظمة حماية معينة مخصصة للبيانات والتطبيقات وأنظمة التشغيل.

أما الأمن السيبراني يهدف إلى حماية الأنظمة والشبكات ومختلف الأجهزة الالكترونية من الهجمات الالكترونية والرقمية، بتبسيط أكثر هو بمثابة إنشاء جدار للحماية يمنع أي محاولة اختراق أو تجسس[26].ومنه يخلص لنا أن أمن المعلومات أوسع نطاقا من الأمن السيبراني بحيث أن الأخير يركز على حماية الأنظمة والشبكات من التهديدات الالكترونية، بينما يعتبر أمن المعلومات أوسع نطاقا ويشمل حماية جميع المعلومات والبيانات مهما كان نوعها بغض النظر عن الوسائط المستعملة.

وعليه يمكننا أن نميز هنا بين عدة أنواع من الرقابة الالكترونية وهي:

1- **رقابة إدارية:** تمارس هذه الرقابة أيضا لوجهين أحدهما من الإدارة ذاتيا على نفسها عبر مراقبة أعمالها والآخر يكون على نشاطات الأفراد كإجراءات عادية للضبط الإداري، وقد تطورت هذه الرقابة مع مرور الزمن، حيث شهدت فرنسا سنة 1997 صدور القانون المؤسس لهيئة تنظيم الاتصالات والبريد، ثم في سنة 2005 تم تعديل القانون لإضافة مهام رقابية على الاتصالات الالكترونية، ليصبح اسم الهيئة: هيئة تنظيم الاتصالات الالكترونية والبريد، وطبقا للمادة 433-1 من قانون الاتصالات الالكترونية والبريد تتولى هذه الهيئة الإشراف والمراقبة على المحتوى الرقمي، مراعاة لعديد الاعتبارات منها الحفاظ على النظام العام، ثم في سنة 2003 تم إنشاء هيئة مسؤولة عن تنظيم الاتصالات حيث تنص المادة 68 من نفس القانون سالف الذكر على أنه: (تخضع جميع الخدمات وشبكات الاتصالات عبر أي مشغل أو خادم إلكتروني لرقابة السلطات المختصة في الدولة، وأن تستدعي جميع العاملين لديها من القائمين على تشغيل وصيانة تلك الخدمات أو الشبكات)[27]. جاء هذا القانون تطبيقا لرأي المشرع الأوروبي الذي رأى أنه من الضروري تدخل سلطات الدولة المستقلة عن الشركات والحكومات في الدول الأوروبية لضمان التطور السليم لهذه الشبكات دون تهديدها لأمن الدول الأوروبية.

2- **رقابة قضائية:** أصدرت المحكمة العليا الأمريكية سنة 1972 حكما بخصوص قضية برانزبرج ضد هايز (Brunzberg vs Hayes) [28]يقضي بالسماح لهيئات المحلفين الكبرى الطلب من المراسلين الكشف عن مصادر معلوماتهم، كما رفضت المحكمة ذاتها أي امتياز للصحفيين بحجة حرية التعبير والإعلام، كذريعة للتحجج بعدم إعطاء مصادر معلوماتهم خاصة إذا كانت ذلت صلة بالأمن القومي للبلاد. إلا إذا أصدر الكونجرس الأمريكي أو المحكمة العليا الفيدرالية تشريعا يتحصن بموجبه المراسل الصحفي.

3- **رقابة أمنية سيبرانية:** مع تطور الفكر الإجرامي باستعماله للشبكات الالكترونية سواء كوسيلة تواصل أو أداة للجريمة الالكترونية، تم إنشاء أجهزة أمنية تملس صلاحيات الضبط الإداري الأمني اتجاه سلوك ونشاطات الأفراد على المواقع الالكترونية، وهي رقابة ليست بالتقليدية وإنما حديثة فرضها التطور الالكتروني الغاية منها المحافظة على النظام العام، والوقاية من كل ما يهدده في الواقع الالكتروني ولذا تتصف هذه الرقابة بالطابع الأمني وبأنها إدارية الكترونية[29]، ولعل أهم وسيلة في الرقابة الأمنية هي التسرب الالكتروني، والذي يختلف عن آلية التسرب التقليدي حيث نص المشرع الفرنسي في القانون المتعلق بتعزيز تدابير مكافحة الإرهاب رقم 2014/1353 ،والذي نص في مادته 787 أن الشرطة الإدارية لها الحق في إنشاء دوريات إلكترونية يعهد إليها التحقيق في كل التبادلات والمناشير الإلكترونية، ولها الحق في التسرب داخل غرف الدردشة تحت أسماء مستعارة، من أجل الدخول في اتصالات مع الأشخاص النشطين في هذه الغرف خاصة بعد تحديد هوياتهم ولهم سوابق إجرامية للعمل على التنبؤ بكل ما ينوون القيام به من أعمال عدائية تهدد النظام العام ومنه الحفاظ على أمن الدولة.

4- **رقابة وقائية:** كانت الدول الأوروبية سباقة إلى تشجيع المؤسسات المختصة في وقاية المواقع الالكترونية على إيجاد السبل العلمية لأجل وقاية المعلومات التي تتداولها المصالح الحكومية عبر مختلف شبكاتها الخاصة والأرضيات الرقمية المستحدثة لهذا الغرض، حيث صدر أمر توجيهي من البرلمان الأوروبي لمختلف الدول الأعضاء في 01-03-1996 بشأن حماية قانونية لقواعد البيانات، حيث بدأ نفاذه في مختلف الدول الأوربية في 01-01-1998[30]. أين عملت هذه التشريعات على التأكيد على خصوصية البيانات المتعلقة بالأفراد وكذا الكيانات الاقتصادية، وأنه على مزودي خدمات الانترنيت أو متعهدي الإيواء الخاص بالمواقع يقع على عاتقهم المراقبة الوقائية لما يتم تداوله ونشره على تلك المواقع أو الخادم، بصفتهم وسطاء رسميين تم اعتمادهم لهذا الغرض بموجب هذه التشريعات.

ثانيا- الحجب الإداري للمعلومات آلية لتعزيز الأمن السيبراني.تلجأ الإدارة إلى عدة وسائل مختلفة لضمان أمن المعلومات الحساسة أو التي تتعلق بأمن الدولة في مختلف الميادين السياسية، الاقتصادية والعسكرية خاصة، موازاة مع انتشار الحكومات الالكترونية ومتطلبات الرقمنة، لتسهيل معاملات المواطن بالدرجة الأولى وضمان الحصول على أرقام وإحصائيات آنية ومؤكدة، لدعم مختلف الدراسات الاستشرافية للمكاتب والجهات الحكومية، لذا كان من الضروري التفكير في الآليات القانونية التي تسمح للدولة بحجب المعلومات التي لها طابع حساس، أو التي يسعى خلفها الجهات المعادية للدولة من أجل استعمالها لأغراض تمس بأمن تلك الدولة. بحيث أصبحنا نرى أن الحروب المتقدمة اختزلت في المواقع الإلكترونية الخاصة بالمجالات الحيوية للدول، هذه الأخيرة مهددة كل وقت لهجمات سيبرانية من وراء البحار ومن مختلف المناطق في العالم تهدد أمن الدولة بالدرجة الأولى، خاصة ما إذا تم تعطيل المواقع الخاصة بالموانئ والبنوك ومختلف المواقع الأمنية كذلك والحكومية التي تعمل على تسهيل عمل المرتفقين، وهو ما يوجب على كل دولة تأمين مواقعها والسهر على الحجب الدوري لكل ما هو حساس في مختلف البيانات الالكترونية الهامة[31].

ثالثا- التفتيش الوقائي الدوري.تعمل مصالح الدولة المكلفة بضبط الخدمات الالكترونية والفضاء الرقمي، على منح سلطات الضبط المختصة ممثلة في الشرطة الإدارية، تسمح لها بموجبها تفتيش قاعدة البيانات لأي موقع يستعمل خادم معرف بالرقم الدولي لتلك الدولة، وفق رزنامة محددة دوريا من أجل الوقاية من حدوث هجمات سيبرانية من شأنها التأثير على تلك الدولة[32].ويكون عمل هذه المصالح بناء على تشفير معين يتم من خلاله تسجيل أي منشور أو اتصال أو رسالة صوتية أو مرئية، يتم ذكر فيها كلمة رئيسية تكون محددة سلفا في قاعدة البيانات الخاصة بالبرامج المستعملة لأجل المراقبة الالكترونية، وفي حال تسجيل أي إنذار بهذا الخصوص تعمل هذه المصالح على التفتيش الدوري والمستمر لأجل الوقاية من أي تهديد للنظام العام، وهو ما استحدثه البرلمان الأوروبي في القرار الإطاري 2056 لسنة 2002. ثم تم تعديله عبر إصدار قانون تنظيمي رقم 2065 لسنة 2023 تحت مسمى الرقابة التنظيمية على عمالقة التكنولوجيا في العالم. حيث تم البدء في تطبيقه ابتداء من أول فبراير 2024 على جميع الخدمات الرقمية في كل دول الإتحاد الأوروبي، الهدف منه خلق بيئة رقمية آمنة يتم فيها ممارسة جميع الحقوق والحريات العامة لكل الأفراد بعيدا عن أي تهديد لبياناتهم الشخصية من جهة، أو خطر يهدد النظام العام للدول المعنية بتطبيق هذا القانون من جهة أخرى.وكل المنصات ملزمة بتضمين شروط استعمال المنصات الالكترونية لهذا القانون كآلية يتم من خلالها الالتزام بالنظام العام.

نرى في هذا الصدد بأن الولوج على المواقع والمنتديات على الشبكة الإلكترونية بداعي الحفاظ على النظام العام، لا يسمح للسلطات المختصة بالإطلاع على البيانات الشخصية لمرتادي هذه المواقع والمنتديات، وتتبع الأزرار التي يضغطون عليها من خلال الكمبيوتر أو الهاتف الذكي،هو أشبه بالتعدي على حرمة الغير دون إذن قضائي يسمح بذلك.

المطلب الثالث:حدود سلطات الضبط الإداري الالكتروني.

بالرغم من كل الإجراءات المعمول بها في البيئة الرقمية عبر مختلف المنصات الإلكترونية، إلا أن السلطات المعنية بضبط استعمال الخدمات المقدمة من الشبابيك الإلكترونية من جهة ، واعتماد كبير للدول على الرقمنة وإدارتها لمرافقها عبر الحكومة الالكترونية من جهة أخرى، وهو ما يجعل هذه الدول بتوفير بيئة قانونية متينة لضمان ممارسة المصالح المكلفة بتأمين هذه الشبكات الالكترونية لحماية المعلومات التي توفرها هذه التقنية خاصة وأنها تمس بأمن الدول اقتصاديا وحتى عسكريا، فحتى المفاعلات النووية تدار بأنظمة إلكترونية عالية التقنية، وهو ما يرفع من طموحات محاربة كل ما يخل بأمن هذه الدول.

الفرع الأول: مشروعية الضبط الإداري الالكتروني.

تعتبر التجربة الأمريكية في هذا المجال رائدة مقارنة بغيرها في دول الاتحاد الأوروبي والصين، حيث يعمل المشرع الأمريكي على شقين : أولهما هو المعايير الفنية لكيفيات ممارسة الضبط الإداري الالكتروني، وثانيهما التشريعات والرقابة.

أولا- المعايير الفنية والتقنية للضبط الإداري الالكتروني:

تم إنشاء معهد وطني قومي للمعايير التقنية والقياسات التكنولوجية NIST سنة 1901 كأول إجراء في سبيل تشجيع الابتكار والقدرة التنافسية الصناعية، وتوحيد أنظمة المراقبة الالكترونية وتجميع المعلومات بناء على ما تتيحه الأنظمة المستعملة في الحواسيب العسكرية، كل هذا لتعزيز وتطوير الأمن العسكري والاقتصادي، ليتم سنة 1988 تعديل مهامه من خلال توجيه برامجه إلى تحسين نوعية الحياة للأفراد، من خلال التخطيط لإتاحة التكنولوجيا واستعمالها في طابع مدني بحت[33]

ثانيا- التشريعات والرقابة :تعتبر حزمة النصوص القانونية بمثابة الدرع القانوني الذي من خلاله تعمل سلطات الضبط الإداري الإلكتروني على حماية الشبكة المعلوماتية للحفاظ على النظام العام من جهة، وعلى محاولة توفير البيئة الآمنة لممارسة الحقوق الرقمية، وإذا وجدنا أنه وفي سنة 2023 كانت نسبة الشباب تمثل أكثر من 79 % من مستعملي الانترنيت بحيث معدل أعمارهم ما بين 15 و24سنة[34]، ناهيك على محاربة الجريمة الإلكترونية التي استفحلت وانتشرت كالنار في الهشيم خاصة إذا ما علمنا أن أغلب المجرمين في هذا الفضاء هم من خارج الدول التي تقع فيها تلك الجرائم السيبرانية، وبسبب البرمجيات المتطورة المستعملة من طرفهم أصبحت تطلق عليهم صفة القراصنة، على اعتبار أنهم يستولون على كل شيء ثمين تقع عليه تطفلاتهم وجوسستهم على الحسابات الالكترونية والبنكية ...الخ.

الفرع الثاني: نطاق سلطة الضبط الإداري الالكتروني.

تلجأ بعض الدول وتحت مسمى محاربة المخاطر التي تحدق بالأمن العام إلى كبت الحريات، عبر إضافة قيود على استخدام الانترنيت، وهو ما حصل في دولة تركيا عند إصدار تعديل في القانون المتعلق بصلاحيات هيئة الاتصالات التركية ، عبر منحها صلاحية غلق مواقع الانترنيت خلال أربع ساعات، لكن المحكمة الدستورية اشترطت الحصول على إذن قضائي قبل القيام بذلك، كما رأت المحكمة الدستورية بعدم دستورية النص الأصلي الذي يتيح للهيئة الحصول على معلومات من خلال رقابتها للمواقع عبر التجسس على المستخدمين وتخزين معلوماتهم[35].

4- خاتمة:

إن الفضاء الرقمي المشبع بأنظمة الذكاء الاصطناعي من اختراع العقل البشري لتسهيل الوصول إلى كل ما يطمح إليه الإنسان، وممارسته لحقوقه الرقمية بكل أمن وأمان في ظل تمتعه بهامش واسع من الخصوصية وحرية التعبير والنشر، لكن العقل البشري في جانبه السلبي الإجرامي كذلك لجيه تحديات إجرامية تجعله لا يكل ولا يمل من أجل الولوج إلى نفس الفضاء الرقمي، وباستعماله نفس أنظمة الذكاء الاصطناعي لكن ببرمجيات إجرامية تسهل عليه الوصول إلى ما يصبو إليه، وهنا التحدي الأكبر للدول على ضمان الأمن السيبراني.

وهو ما حاولنا التعرض إليه في مداخلتنا هذه التي خلصنا من خلالها إلى النتائج والتوصيات التالية:

أ -النتائج:

- الأمن السيبراني بمثابة منظومة دفاعية لجميع الدول ومجال خصب لاستعراض أنظمة الذكاء الاصطناعي.
- تكتم كل الدول على مجهوداتها في مجال الأنظمة المستعملة في مجال الأمن السيبراني، كأمن قومي يتمتع بالسرية.
- هشاشة الأنظمة الأمنية للوسائط الاجتماعية مقابل التعدي الصارخ على البيانات والمعلومات الشخصية، وهو ما يهدد الحقوق الرقمية باعتبارها امتداد لحقوق الإنسان الأساسية.
- ضعف الترسانة القانونية الخاصة بالأمن السيبراني في مجال حماية المعلومات والبيانات الشخصية في الدول النامية.

ب-التوصيات:

- على جميع الدول ضمان استعمال البيئة الرقمية كمجال آمن لممارسة والتمتع بالحقوق الرقمية للأفراد، مع ضمان حماية قصوى لبياناتهم ومعلوماتهم الشخصية.
- عدم الخلط بين تهديدات النظام العام والجرائم السيبرانية، وهو ما يتطلب تخصص الوحدات الأمنية التي لها صفة الضبطية القضائية في هذا المجال، من أجل التكييف الصحيح لكل القضايا ذات الصلة.
- تعزيز الترسانة القانونية في مجال أمن الشبكة المعلوماتية لكل الدول.
- تعزيز الجانب التكويني للقضاء مجال الأمن السيبراني، وتبادل الخبرات مع الدول التي لها باع والسبق في هذا المجال.

الهوامش والمراجع:

الهوامش:

[1] - فاتح قيش، آليات حماية الحق في الخصوصية في التشريع الجزائري، مقال منشور بمجلة جيل للأبحاث القانونية، العدد 36 الصفحة 93.سنة 2019 نسخة إلكترونية على الموقع الالكتروني، https://jilrc.com/archives/10712 تاريخ الزيارة 2024/03/24 على الساعة 22:31.

[2] - T. Vedel, « Les politiques des autoroutes de l'information dans les pays industrialisés : une analyse comparative », Réseaux, 1996, n° 78, p. 11-28.

[3] - محمد طاهر، الحريات الرقمية (المفاهيم الأساسية)، مؤسسة حرية الرأي والتعبير، الطبعة 1، القاهرة، 2013 ، ص5.

[4] - موقع أخبار الأمم المتحدة - https://news.un.org/ar/story/2013/12/192412 تاريخ الزيارة 2024/03/26 على الساعة 22:40.

[5] - Loi N° 2004-575 du 21 juin 2004 , Pour une confiance dans l'économie numérique, J.O N°143 du 22 juin 2004, p.1168.

[6] - La séparation de ces deux régimes, a savoir de la communication audiovisuelle et de la communication au public en ligne, a par ailleurs pour conséquence leur soumission à une autorité de contrôle différente. Ainsi, alors que l'Autorité de régulation des communications électroniques et des postes est compétente pour les activités relevant des communications au public en ligne, c'est le Conseil de l'audiovisuel qui se chargera dans le domaine de la communication audiovisuelle.

[7] - زينب محمد جميل الضناوي، الحماية القانونية للخصوصية على الانترنيت في ظل الجهود الدولية والداخلية، مقالة منشورة بكتاب ملتقى أعمال المؤتمر الدولي المحكم حول الخصوصية في مجتمع المعلوماتية، جامعة الملك فيصل بالمملكة العربية السعودية 2019، ص 23.

[8] -الأمن السيبراني في مظومة الأمم المتحدة، تقرير وحدة التفتيش المشتركة، من إعداد خورخي فلوريس كاييخاس، وعائشة عفيفي، ونيكوالي لوزينسكي (وحدة التفتيش المركزية)، منشور على موقع الأمم المتحدة، https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_arabic.pdf تاريخ الزيارة:2024/04/06 على الساعة 11:15.

[9]- Paola Ricaurte (2019), Data Epistemologies, The Coloniality of Power, and Resistance, television and new media.volume 20, Issue 4, https://journals.sagepub.com/doi/abs/10.1177/1527476419831640?journalCode=tvna تاريخ الزيارة 05-04-2024. على الساعة 00:08

[10]الموقع الرسمي للوكالة الأوروبية للأمن السيبراني https://www.enisa.europa.eu/ تاريخ الزيارة 2024/04/06 على الساعة 12:02.

[11] مهام الوكالة الأوروبية للأمن السيبراني، https://www.enisa.europa.eu/topics/cybersecurity-policy تاريخ الزيارة 2024/04/06 على الساعة 13:15 د.

[12] - The NIS2 Directive (EU 2022/2555), of the EU Parliament and of the Council, of 14/12/2022.

[13] - موقع أخبار الأمم المتحدة https://news.un.org/ar/story/2023/03/1118957 تاريخ الزيارة 2024-04-07 على الساعة 17:52

[14] - بيان مجلس الوزراء الجزائري، بتاريخ 14-11-2023، للإطلاع على نص البيان كاملا : https://backend.el-mouradia.dz/uploads/byan_mjls_alwzrae_14_11_2023_39dc040049.pdf

[15] -القانون22-06 ، المؤرخ في 29 ذي القعدة 1427هـ، الموافق ل 20-12-2006، المعدل والمتمم للأمر 66-155، المؤرخ في 18 صفر 1386هـ، الموافق 8 يونيو 1966، والمتضمن قانون الإجراءات الجزائية، ج ر ج ج عدد رقم 84 المنشور بتاريخ 24-12-2006، ص4.

[16] -المرسوم الرئاسي رقم 21-439 ،المؤرخ يف 2 ربيع الثاني عام 1443 الموافق 7 نوفمبرسنة 2021 ،يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، المنشور بالج. ر. ج العدد86 ،بتاريخ 11 نوفمبرسنة 2021 ،ص5.

[17] - الأمن السيبراني في مظومة الأمم المتحدة، تقرير وحدة التفتيش المشتركة، المرجع السابق، ص 28.

[18] - شريف عبد الرحمن سيف نصر، السيبرانية: (المفهوم، الخصائص والفرص والإشكاليات)، مجلة قضايا وظرات، تقرير شهر أفريل 2021، مركز الحضارة للدراسات والبحوث، القاهرة، ص 72.

[19] - نبيله هبة هروال، الجوانب الإجرائية لجرائم الانترنت جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، جمهورية مصر العربية،2013 ص:197.

[20] - https://www.iberdrola.com/innovation/what-are-digital-rights#:~:text=Digital%20rights%2C%20closely%20linked%20to,rights%20for%20the%20Internet%20age. تم زيارة الموقع يوم 25-12-2023 على الساعة 08:20د

[21] - Lenka Jančová and Meenakshi Fernandes, Digitalisation and administrative law, Study of the EPRS | European Parliamentary Research Service. European Added Value Unit PE 730.350 – November 2022. P 23.

[22]- Nicolas Ochoa, Le droit des données personnelles, une police administrative spéciale. Droit Université Paris 1 Panthéon- Sorbonne, 2014, Français. ffNNT : ff. fftel-01340600f. P 6.

[23] - زينة عبد الله محمد مصطفى، الرقابة الالكترونية وحرية الرأي والتعبير، دراسة مقارنة بين مصر وإيران، مقال منشور في مجلة المركز العربي لأبحاث الفضاء الإلكتروني، 2016، https://accronline.com/article_detail.aspx?id=25895 تاريخ الزيارة 27-12-2023 على الساعة 17 و50 د.

[24] - عزيز ملحم برير، الشبكات والانترنيت، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، 2008، ص3.

[25] - ياسر الأمير فاروق مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دار المطبوعات الجامعية الإسكندرية، 2009، ص150.

[26] - https://learn.microsoft.com/ar-sa/training/modules/describe-basic-cybersecurity-threats-attacks-mitigations/ تاريخ الزيارة 28-12-2023 على الساعة 22.45.

[27] - موقع هيئة تنظيم الاتصالات الالكترونية والبريد، https://www.arcep.fr/ تاريخ الزيارة 27-12-2023 على الساعة 20.00

[28] - بول ليفنسون، أحدث وسائل الإعلام الجديدة، ترجمة هبة ربيع، دار الفجر القاهرة، جمهورية مصر العربية، 2005 ، ص 195.

[29] - مصطفى جمال حفني زينو، دور الضبط الإداري في مجال الجرائم الالكترونية المخلة بالأمن العام، رسالة ماجستير، كلية الحقوق ، جامعة الأزهر، غزة فلسطين، 2017/2016 ، ص164.

[30] - DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 11 mars 1996 concernant la protection juridique des bases de données, https://www.wipo.int/wipolex/ar/legislation/details/1409 تاريخ الزيارة 24-01-2024 على الساعة 16:10.

[31]- مصطفى جمال حفني زينو، المرجع السابق، ص 178.

[32]- زينة عبد الله محمد مصطفى، المرجع السابق، ص82.

[33] - https://www.nist.gov/director المعهد الوطني للمعايير التقنية والقياسات التكنولوجية تاريخ الزيارة 2024/03/25 على الساعة 19:03

[34] -سلامة الأطفال والشباب على الانترنيت، دراسة منشورة على موقع الأمم المتحدة ، https://www.un.org/ar/global-issues/child-and-youth-safety-online تاريخ الزيارة 2024/03/27 على الساعة 19:05.

[35] - الانترنيت والأبعاد الأمنية، منصور عقيل وعلي قلم، مركز البحوث والدراسات الشرطية، دبي الإمارات العربية المتحدة ، جانفي 1996، ص25.

المراجع:

1- النصوص القانونية:

Loi N° 2004-575 du 21 juin 2004 , Pour une confiance dans l'économie numérique, J.O R-Française, N°143 du 22 juin 2004, p.1168.

- The NIS2 Directive (EU 2022/2555), of the EU Parliament and of the Council, of 14/12/2022.

- القانون22-06 ، المؤرخ في 29 ذي القعدة 1427هـ، الموافق ل 20-12-2006، المعدل والمتمم للأمر 66-155، المؤرخ في 18 صفر 1386هـ، الموافق 8 يونيو 1966، والمتضمن قانون لإجراءات الجزائية، ج ر ج ج عدد رقم 84 المنشور بتاريخ 24-12-2006.

- المرسوم الرئاسي رقم 21-439 ،المؤرخ يف 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021 ،يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات لإعلام والاتصال ومكافحتها، ج.ر ج ج العدد86 ، بتاريخ 11 نوفمبر سنة 2021 .

- DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 11 mars 1996 concernant la protection juridique des bases de données.

2- الكتب والمؤلفات:

- محمد طاهر، الحريات الرقمية (المفاهيم لأساسية)، مؤسسة حرية الرأي والتعبير، الطبعة 1، القاهرة، 2013.

- نبيله هبة هروال، الجوانب لإجرائية لجرائم الانترنت جمع لاستدلالات، دار الفكر الجامعي، لإسكندرية، جمهورية مصر العربية،2013.

-Nicolas Ochoa, Le droit des données personnelles, une police administrative spéciale. Droit Université -Paris 1 Panthéon- Sorbonne, 2014, Français. ffNNT : ff. fftel-01340600f.

- عزيز ملحم برير، الشبكات والانترنيت، جامعة نايف العربية للعلوم لأمنية، المملكة العربية السعودية، 2008

- ياسر الأمير فاروق مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دار المطبوعات الجامعية الإسكندرية،2009.
- بول ليفنسون، أحدث وسائل الإعلام الجديدة، ترجمة هبة ربيع، دار الفجر القاهرة، جمهورية مصر العربية، 2005.
- الانترنيت والأبعاد الأمنية، منصور عقيل وعلي قاسم، مركز البحوث والدراسات الشرطية، دبي الإمارات العربية المتحدة ، جانفي 1996.

3- الأطروحات والرسائل:

- مصطفى جمال حنفي زينو، دور الضبط الإداري في مجال الجرائم الالكترونية المخلة بالأمن العام، رسالة ماجستير، كلية الحقوق ، جامعة الأزهر، غزة فلسطين، 2017/2016 .

4- المقالات والمجلات:

- فاتح قيش، آليات حماية الحق في الخصوصية في التشريع الجزائري، مقال منشور بمجلة جيل للأبحاث القانونية، العدد 36. سنة 2019 نسخة إلكترونية .
-زينب محمد جميل الضناوي، الحماية القانونية للخصوصية على الانترنيت في ظل الجهود الدولية والداخلية، مقالة منشورة بكتاب ملتقى أعمال المؤتمر الدولي المحكم حول الخصوصية في مجتمع المعلوماتية، جامعة الملك فيصل بالمملكة العربية السعودية 2019
- Paola Ricaurte, Data Epistemologies, The Coloniality of Power, and Resistance, tlevision and new media.volume 20, Issue 4 (2019)
- شريف عبد الرحمن سيف نصر، السيبرانية: (المفهوم، الخصائص والفرص والإشكاليات)، مجلة قضايا ونظرات، تقرير شهر أفريل 2021، مركز الحضارة للدراسات والبحوث، القاهرة
-زينة عبد الله محمد مصطفى، الرقابة الالكترونية وحرية الرأي والتعبير، دراسة مقارنة بين مصر وإيران، مقال منشور في مجلة المركز العربي لأبحاث الفضاء الإلكتروني، القاهرة، جمهورية مصر العربية.2016
-

5- المواقع الإلكترونية:

موقع أخبار الأمم المتحدة -https://news.un.org/ar/story/2013/12/192412 -
الموقع الرسمي للوكالة الأوروبية للأمن السيبراني https://www.enisa.europa.eu/ -
- https://backend.elmouradia.dz/uploads/byan_mjls_alwzrae_14_11_2023_39dc040049.pdf
https://www.iberdrola.com/innovation/what-are-digital-rights#:~:text=Digital%20rights%2C%20closely%20linked%20to,rights%20for%20the%20Internet%20age .
https://learn.microsoft.com/ar-sa/training/modules/describe-basic-cybersecurity-threats-attacks-mitigations/الموقع الرسمي لشركة مايكروسوفت العالمية /
- موقع هيئة تنظيم الاتصالات الالكترونية والبريد الفرنسية، https://www.arcep.fr-
- المعهد الوطني الأمريكي للمعايير التقنية والقياسات التكنولوجية https://www.nist.gov/director

6- التقارير والوثائق:

- الأمن السيبراني في منظومة الأمم المتحدة، تقرير وحدة التفتيش المشتركة، من إعداد خورخي فلوريس كاييخاس، وعائشة عفيفي، ونيكوالي لوزينسكي (وحدة التفتيش المركزية)، منشور على موقع الأمم المتحدة،

- Lenka Jančová and Meenakshi Fernandes, Digitalisation and administrative law, Study of the EPRS | European Parliamentary Research Service. European Added Value Unit PE 730.350 – November 2022.

- سلامة الأطفال والشباب على الانترنيت، دراسة منشورة على موقع الأمم المتحدة ، https://www.un.org/ar/global-issues/child-and-youth-safety-online تاريخ الزيارة 2024/03/27

المخدرات الرقمية تحدي جديد أمام القانون الدولي

The digital drugs: A new challenge for international law

د. مصطفى قديري / جامعة الحاج لخضر باتنة 1

د. سمير فارح / مركز البحث في الأنثربولوجيا الاجتماعية والثقافية CRASC

الملخص : أبدت وسائل الاعلام الغربية والعربية في السنوات الأخيرة قلقا واسعا بشأن ظاهرة تتعلق بظهور شكل جديد من " المخدرات" التي يمكن أن يكون لها تأثيرا سلبيا على الصحة النفسية والجسدية للأفراد، وتتمثل ميزة هذه المخدرات أنها تختلف عن "المخدرات التقليدية (الحشيش، الافيون، القات، الكوكايين و الهيروين...الخ)، من حيث شكلها ومضمونها، بكونها ترتبط بشبكة الانترنت ويتم ترويجها في شكل ملفات رقمية صوتية قابل للتحميل لقراءته على مشغل MP3، ويطلق عليها باسم المخدرات الرقمية أو "IDOZER" وعند الاستماع الى هذه النغمات تؤدي الى تغيير الحالة المزاجية والوهم السمعي التي تحاكي تعاطي المخدرات الحقيقية. وعليه ان المعرفة العلمية بطريقة عمل المخدرات الرقمية ، والاطلاع على الدراسات العلمية التجريبية أصبح ملح جدا لتفادي المخاطر التي قد يقع فيها الشباب من مثل هذا الاستخدام غير السليم و العمل على التوعية من الاثار غير المتوقعة لمثل هذه المواد. وهو ما سنحاول توضيحه في هذه الورقة من خلال مراجعة الادبيات العلمية التجريبية لاستخدام النقر على الاذنين على الدماغ البشري والحالة المزاجية.

الكلمات المفتاحية : المخدرات الرقمية- النبض على الاذنين binaural beats

Abstrait ; In recent years, both Western and Arab media have expressed widespread concern over a phenomenon associated with the emergence of a new type of "drugs" potentially detrimental to individuals' mental and physical health. These drugs, termed "digital drugs" or "IDOZER," possess a unique characteristic in that they deviate from conventional drugs in both form and content. They are distributed via the internet and marketed as downloadable digital audio files intended for playback on MP3 players. When listened to, these audio tones purportedly induce mood alterations and auditory illusions akin to the effects of actual drug use. Hence, there is an urgent need for scientific understanding of the mechanisms underlying digital drugs and access to experimental research to mitigate the risks associated with their improper usage, particularly among youth, and to promote awareness. This paper aims to shed light on one of the unforeseen consequences of such substances by examining the empirical scientific literature on the effects of binaural beats function . **Keywords: digital drugs, binaural beats**

مقدمة :

في الوقت الذي تتكاتف فيه الجهود الدولية والوطنية لمكافحة ظاهرة تعاطي المخدرات والاتجار بها وإدمانها وفي الوقت الذي دق فيه ناقوس الخطر بتزايد تعاطي المخدرات التقليدية في أوساط الشباب، تبدا معالم تغير طرق تعاطي المخدرات من الطرف التقليدية إلى الطرق الحديثة التي لعبت فيها التكنولوجيا الحديثة دورا كبيرا في هذا التغير، ويتعلق بالأمر ببروز المخدرات الرقمية التي يروج لها مستهلكوها عبر قنوات التواصل الاجتماعي واليوتوب بأنها تحاكي حالات الارتخاء والانتشاء التي تؤديها المخدرات التقليدية، وبالنظر إلى شكل المخدرات التقليدية المعروفة في الوسط الطبي التي تون نباتية أو صناعية، نجد إن دخول التكنولوجيا جعلت من تأثيرات تلك الأدوية المخدرة بالإمكان صناعتها على شكل ملفات رقمية صوتية قابلة للتحميل وبجرعات مختلفة، وقد كان للعلم دور كبير في اكتشاف هذا النوع من المخدرات من خلال دراسات حول تأثيرا الموجات الصوتية والترددات المختلفة على كل اذن على الدماغ البشري و المستويات التي قد يؤديها في العمليات الادراكية والحسية والتحفيز والاسترخاء والشعور بالراحة والخفض من التوتر والقلق ..الخ، ويعتبر "هاينريش فيلهلم دوف" Heinrich Wilhelm Dove أول من اكتشف ظاهرة الإدراك الحسي للنبضات بكلتا الأذنين في عام 1841 ووصفت لأول مرة في الأدبيات العلمية في عام 1973.

وقد اطلق على هذا النوع من المخدرات باسم I-dosing ويبدا بملف صوتي رقمي MP3 يتم شراؤه عبر الإنترنت وتنزيله بنقرة زر، تمامًا مثل أي أغنية أو ملف صوتي آخر ، من خلال iTunes أو متجر تطبيقات Apple. أي شخص لديه إمكانية الوصول إلى الإنترنت وزوج من سماعات الرأس لديه الفرصة لتجربة هذا "الارتفاع الرقمي". ولدت سهولة الوصول إلى ملفات MP3 ، جنبًا إلى جنب مع دعوة مواقع الويب والمراجعات الإيجابية للاسترخاء والرؤى وحتى تجارب الخروج من الجسد، الاهتمام بهذه الظاهرة.[1]

ويُطلق على الصوت السمعي الأساسي الذي يُنسب إليه الفضل في إحداث هذه التأثيرات المتصورة اسم نبضة الأذنين. المفهوم بسيط نسبيًا: يتم تغذية الدماغ بموجات جيبية ذات نغمة نقية، واحدة في كل أذن، من خلال سماعات الرأس. لكي يتم إدراك النبضات، يجب أن تكون الإشارتان في نفس النطاق السمعي الحرج. على سبيل المثال ، يتم تشغيل نغمة 200 هرتز في الأذن اليسرى ونغمة 210 هرتز في الأذن اليمنى. ما يسمعه المستمع هو نغمة من 205 هرتز مع نبض، أو "الضرب" بتردد 10 هرتز.[2]

ان معرفة التأثيرات الحقيقية لهذا النوع من المخدرات الرقمية على الحالة الصحية والنفسية للأفراد و محاكاتها للتاثرات التي تخلفها المخدرات التقليدية لا تزال في طور الدراسة ولا توجد أدلة علمية كافية تؤكد حالات الإدمان والتبعية التي تصاحب تعاطي المخدرات الرقمية مقارنة بالمخدرات التقليدية لكن المهم والمؤكد ان تكنولوجيا الاتصال ومروجي هذا النوع من المخدرات سيعملون بكل جهد من اجل توجيه الاستخدام الطبي والعلاجي لهذا النوع المخدرات الرقمية الى غايات وأهداف تجارية وربحية وتدمير عقول الشباب والناشئة، كما ان المعرفة العلمية واجراء الدراسات والبحوث على مستوى الوعي حول انتشار المخدرات الرقمية سيؤدي الى مكافحة الظاهرة قبل انتشارها وسيعزز المنظومة القانونية والتشريعية لردع الاستخدام الضار لهذه الملفات الصوتية والغرض من حيازتها وتوزيعا والاستماع اليها.

الاشكالية:

بالرغم من التطور الكبير والمتسارع الذي يشهده النظام الدولي في الجانب التشريعي من اتفاقيات دولية ثنائية ومتعددة في مجال مكافحة الجريمة والمخدرات والدفاع عن الضحايا ، إلا أن هذا المجهود يبقى قليلا ضعيفا أمام

تطور الظاهرة وانتشارها فمكافحة المخدرات التقليدية لم ينجح إلى حد كبير كما أن القوانين الموجودة ليست ملزمة في مجال المكافحة الدولية ، كما تطور المخدرات والعمل على نشرها يشهد استثمارا كبيرا ورغم أن الغايات والأهداف العلاجية والأسس العلمية التي برزت من خلالها المخدرات الرقمية وتطبيقاتها، إلا أننا نجد أنفسنا أمام التعامل مع أحد الإشكاليات التي برزت في الساحة النقاشية العلمية في السنوات الأخيرة حول انتشار المخدرات الرقمية والجرعات الصوتية الالكترونية وتأثيراتها ومخاطرها على الصحة النفسية والعقلية والجسدية، ومع بروزها شاع في أوساط العامة إن دقات الأذنين توفر العديد من نفس فوائد التأمل، كتقليل التوتر، وزيادة التركيز، والمساعدة في النوم والاسترخاء، وتعزيز الحالة المزاجية، والمساعدة في إدارة الألم، وتعزيز الإبداع، ومع ذلك، فإن هذه الادعاءات لا تدعمها الأدلة العلمية،[3] ولا يزال التأكيد على الفوائد الطبية والعلاجية والاضرار المحتملة للمخدرات الرقمية قيد الدراسة، ولكن من المؤكد ان البحث الأكاديمي ركز على استخدامين رئيسيين للنبضات بكلتا الأذنين أولا كعلاج طبي و ثانيا كعلاج كبديل أو مكمل لتعاطي المخدرات ذات التأثير النفساني (الأدوية التي تؤثر على الجهاز العصبي وتغير الإدراك أو المزاج أو الإدراك أو السلوك).[4]

وهنا تبدا الإشكالية بان ظاهرة تعاطي المخدرات التقليدية والإدمان عليها وبالرغم من التضييق الممارس عليها ومحاربتها إلا أن عدد المتعاطين دائما في ارتفاع وحالات الإدمان والوفيات الناجمة عنها هي أيضا في تزايد، وبالرغم أيضا بمعرفتنا بطرق المحاربة والمجابهة والرصد، فالأمر سيكون جد صعب خاصة إذا كنا نتعامل مع مستهليكن افتراضيين في عالم الانترنت ، ومروجين غير مرئيين و مواد مخدرة غير ملموسة، وبالأحرى عبارة عن ملفات صوتية قابلة للتحميل للاستماع بنقر زر واحدة، والغريب أن بعض هذه الملفات الصوتية المخدرة تحمل أسماء تحاكي المخدرات التقليدية كالكوكايين والهيروين والاكستازي...الخ وكلا وفق جرع متباينة، وبالتالي سيكون عدد المستهلكين للمخدرات الرقمية كبير جدا، نظرا لسهولة الوصول اليها وحب الرغبة في التجربة والمغامرة ، وعدم دفع الأموال مقابل ما كان تتطلبه المخدرات التقليدية، وهنا نفتح التساؤل عن مدى القلق الذي سيؤديه انتشار مثل هذا النوع من المخدرات وتأثيراته على الفرد والمجتمع وكيفية سبل المعالجة والوقاية والتصدي، ولكي نبدأ في العمل على هذه الظاهرة لابد ان ببني معرفة نظرية وتطبيقية علمية على واقع هذه الظاهرة وكيفية عملها و استقصاء الدراسات السابقة التي أجريت حولها ورفع مستوى الوعي المجتمعي بواقع هذه الظاهرة ومخاطرها وهو ما سنجيب عليه في هذه الدراسة من خلال التساؤلات التالية :

ما هي المخدرات الرقمية ؟

هل عالج القانون الدولي وضع الضحية في جريمة المخدرات الرقمية ؟

كيف يواجه القانون الدولي المخدرات الرقمية ؟

<u>أهمية الدراسة :</u>

تكمن أهمية الدراسة في التعرف على ظاهرة المخدرات الرقمية من خلال البحوث والدراسات التي أجريت عليها وكذا معرفة التجارب العلمية التي تم إجراؤها من خلال اعتماد نظرية الضرب على الأذنين وتأثيرها على عمل الدماغ البشري، كما تكمن أهمية الدراسة في أهمية الموضوع الذي روج إليه استخدام المخدرات الصوتية الرقمية والتي تحاكي في تأثيراتها مفعول المخدرات الحقيقية، وبالتالي وبالرغم من عدم وجود تأكيدات علمية بحقيقة تطابق استخدام المخدرات الرقمية لوصول النشوة المخدرة، إلا أن حب الاطلاع والتجربة التي تعشش في شبابنا اليوم قد

تؤدي الى سرعة الترويج للمخدرات الرقمية وتجربتها والمتاجرة بها، والوقوع في تجربة المخدرات الحقيقية والبحث عنها وعليه معرفتنا بالموضوع سيساهم في خلق معرفة ونشر التوعية بالمخاطر المحتملة.

تحديد المفاهيم والمصطلحات :

تعريف المخدرات الرقمية:

وهي نوع من أنواع المخدرات لكن بشكل مختلف تمامًا في أسلوب التعاطي، إذ أن هذا النوع يتسلل إلى أنحاء الجسم عبر الأذن فهي عبارة عن مقطع صوت أو نغمة يتم سماعها بواسطة سماعات بكلتا الأذنين، فيتم في هذا الأسلوب بث ترددات بمستوى معين في الأذن اليمنى وترددات أقل في الأذن اليسرى فيساوي شق الدماغ هذه الترددات مع بعضها البعض.[5]

والمخدرات الرقمية عبارة عن ملفات صوتية تحتوي على نغمات أحادية أو ثنائية يستمع إليها المستخدم تجعل الدماغ يصل إلى حالة من الخدر تشابه تأثير المخدرات الحقيقية أو على الأقل هذا ما يدعيه البعض، وقد صممت هذه الملفات الصوتية أو المخدرات الرقمية لمحاكاة الهلاوس وحالات الانتشاء المصاحب لتعاطي المواد المخدرة عن طريق التأثير على العقل بشكل اللاوعي، هذا التأثير الذي يحدث عن طريق موجات صوتية غير سمعية للأذن تسمى الضوضاء البيضاء مغطاة ببعض الإيقاعات البسيطة لتغطية إزعاج تلك الموجات.[6]

وتحمل المخدرات الرقمية اسم يطلق عليه باسم المخدرات الرقمية IDOZER، و تتكون "I-dosing"- التي تعني الجرعات عبر الإنترنت- من الاستماع إلى أنواع معينة من الوسائط الصوتية الرقمية بغرض الحصول على التأثير المطلوب، سواء كان ذلك هو الاسترخاء، أو تحسين الذاكرة ، أو تحقيق مستوى عالٍ من المخدرات. كل ما هو مطلوب هو غرفة مظلمة وهادئة أو قناع نوم ومشغل وسائط وسماعات رأس و 20 إلى 30 دقيقة من الوقت غير المنقطع.[7]

- تعريف النبض على الأذنين :

النبض على الأذنين : عندما يتم تشغيل نغمتين بترددات مختلفة قليلاً في آذان منفصلة في وقت واحد (عادةً من خلال سماعات الرأس) ، فإن الدماغ البشري يدرك إنشاء نغمة ثالثة جديدة ، يكون ترددها مكافئًا للاختلاف بين النغمتين اللتين يتم تشغيلهما. يسمى هذا الوهم السمعي بضرب الأذنين. على سبيل المثال ، إذا سمع شخص نغمة 405 هرتز في أذن واحدة ونغمة 415 هرتز في الأخرى ، فسيسمع نغمة بكلتا الأذنين بتردد 10 هرتز.[8]

عندما يتم تشغيل نغمة 200 هرتز في الأذن اليسرى ونغمة 210 هرتز في الأذن اليمنى ، فإن ما يسمعه المستمع هو نغمة من 205 هرتز مع نبضة أو "ضربات" بتردد 10 هرتز. نبضة 10 هرتز هي التحفيز الذي يؤدي إلى " الوهم السمعي " أو entrainment. يحدث ذلك عندما يقع نظامان لهما خصائص مختلفة بشكل مستقل في التزامن ويفترضان نفس الفترة ، أو "الضرب" ، عند سماعهما معًا. يُنظر إليه على أنه نبضة سمعية ويمكن قياسه باستخدام تقنيات الفيزيولوجيا الكهربية مثل استجابة متابعة التردد وقد تم استخدامه لمحاكاة حالات مزاجية أو تجارب معينة. تنشأ هذه التحفيز بكلتا الأذنين في الدماغ ، وتحديداً في نواة العليا. —S.R.A[9]. ص 18.

- <u>تاريخ ظهور المخدرات الرقمية والية عملها :</u>

تاريخ ظهورها :

إن استخدام الأصوات للتأثير على الحالة المزاجية ليست بالظاهرة الجديدة، كون إن الإنسان منذ القديم وهو يميل إلى التماهي مع الأصوات والموسيقى ، بحثا عن الراحة النفسية وخفض التوتر ، والانغماس في أعماق النفس والتأمل، وهناك العديد من التقنيات التأملية باستخدام الصوت. على سبيل المثال، استخدمت الثقافات القديمة الإيقاعات والترانيم والموسيقى لقرون لإحداث مثل هذه الحالات البديلة للوعي. يتم استخدام الطبول الأفريقية، والترانيم الغريغورية، والترانيم، والموسيقى، والتأمل في الاحتفالات الروحية والدينية من قبل الرهبان واليوغيين والشامان وغيرهم لخلق أجواء أو مزاج، وتغيير حالة الوعي.

وتُعرَّف حالة الوعي المتغيرة بأنها أي تعديل للحالة الطبيعية للوعي، بما في ذلك النعاس أو النوم ، أو الحالات الناتجة عن استخدام الكحول أو المخدرات أو التنويم المغناطيسي أو تقنيات التأمل. تم الإبلاغ عن حالات متغيرة من الوعي من قبل الأفراد الذين يمارسون الرياضة بشكل روتيني، أو يمارسون اليوجا أو فنون الدفاع عن النفس مثل تاي تشي، أو من قبل أولئك الذين يشاركون في نوع من العلاج الصوتي .[10] ص 17 .

يعتبر العالم هاينريش فيلهلم دوف أول من اكتشف النقر على الأذنين في عام 1839، وظل الموضوع يثير الفضول العلمي لمدة 134 عامًا. وقد اتجه البحث العلمي الى الاهتمام بالظاهرة عندما نشر جيرالد أوستر مقاله بعنوان "النبضات السمعية في الدماغ" سنة 1973 ووفر نظرة عامة عالمية على أبحاث الإيقاع على الأذنين. على وجه التحديد ، رأى دقات الأذنين كأداة قوية للبحث الإدراكي والعصبي. وتناول أوستر أسئلة تتعلق بتوطين الأصوات من قبل الحيوانات في بيئتها ثلاثية الأبعاد ، وقدرتها الرائعة على الاختيار والتركيز على أصوات معينة أثناء الصخب (المعروف باسم تأثير حفلة الكوكتيل).

يرى أوستر أيضًا أن الضربات بكلتا الأذنين أداة تشخيصية طبية مفيدة محتملة ، ليس فقط لإيجاد وتقييم ضعف السمع ، ولكن أيضًا للوظائف العصبية الأكثر عمومية (النقر على الأذنين تتضمن مسارات عصبية مختلفة للمعالجة السمعية العادية). وفي سنة 1950، اكتشف Gray WALTER "التأثير الضوئي" ، أي أن الدماغ يتفاعل ويستجيب لتحفيز الصوت والضوء لتكييف موجات الدماغ وفقًا لذلك.

في عام 1960، أصبحت وظيفة النقر على الأذنين أداة للمجتمع الطبي. واستخدمها الطبيب "برنارد مارغوليس" أثناء عمليات طب الأسنان، التي أفاد فيها بأن النقر على الأذنين أتاحت تقليل جرعات التخدير، مما أدى إلى تقليل التقيؤ والنزيف وتقليل القلق بشكل عام.[11]

- <u>آلية عمل المخدرات الرقمية :</u>

تعتمد المخدرات الرقمية على آلية عمل رقمية، مصممة خصيصا للاستخدام والتحميل على شكل ملفات صوتية MP3 مخزنة بصيغة تشغيل خاصة طورته أحد المواقع التجارية باستخدام تقنية مفتوحة المصدر– GPL Open source وتسوقها تحت اسم "المخدرات الرقمية، وكل ملف صوتي يتراوح طوله بين 30و 40 دقيقة، ويمكن تحميل هذه الملفات وتشغيلها من خلال تطبيق خاص لأنظمة التشغيل Android Ios- للاستماع لهذه الملفات عن طريق أجهزة الهاتف الذكية والأجهزة اللوحية، كما يتم استعمالها في الحواسيب العادية.[12] ص 557 وبالنظر إلى الاستخدام الطبي لهذا النوع من المخدرات يزعم مقدمو هذه السوق الجديدة من "العقاقير القانونية" أن "تسجيلات

المخدرات الرقمية" المختلفة يمكن أن تحاكي التأثيرات المبهجة للماريجوانا، والأدوية المضادة للاكتئاب، و LSD، والنشوة، والكوكايين ... هو ليس مخدرًا حقًا لكنه يعتبر علاج بضربات الأذنين.[13]

ولتشغيل المخدرات الرقمية، فهي تعتمد على تطبيق I-Doser هو مشغل صوت رقمي تم تطويره في عام 2005 ؛ إنه أيضًا اسم الشركة التي توفر تنزيلات مجانية للاعب. يعتمد Te player على تقنية الصوت الخاصة بمولد ضربات بكلتا الأذنين يسمى SBaGen ، وهو تطبيق مفتوح المصدر طوره المبرمج البريطاني Jim Peters.[14] وتترافق المخدرات أحيانا مع مواد بصرية وأشكال وألوان، تتحرك وتتغير وفق معدل مدروس تمت هندستها لتخدع الدماغ، عن طريق بث أمواج صوتية مختلفة التردد لكل أذن، ولكي يتم هذا الخداع للدماغ، يمر السامع لها بعدة خطوات عملية هي[15]: ص 1408 .

- يوصل السامع السماعتان الصوتيتان من نوع MP3 لكل أذن على ما حده، فإذا كانت إحداها: تحدث ترددا صوتي بمقدار 400 هرتز، فإن الأخرى تحدث ترددا صوتيا أعلى، وليكن بمقدار 410 هرتز.
- عند وصولها إلى الجهاز السمعي، تقوم منطقة المخ باستقبالها، ثم تفسير الفرق الطفيف بين هاتان الترددين الذي بلغ مقدار 10 هرتز .
- مع مداومة السامع وتكرره لسماع تلك الترددات لهذه الأصوات، يستمر تحفيز منطقة المخ المتخصصة بترجمتها بنفس هذه الترددات.
- تبدأ الأعصاب المخية المرتبطة بهذه المنطقة من المخ بعد فترة كافية، بإصدار موجات كهربائية عصبية، بنفس التردد تنتشر لباقي أجزاء المخ.
- ذلك التردد المنتشر لباقي أجزاء الدماغ، وهو:10 هرتز، الفرق البسيط بين الترددين الموصلين إلى المخ، يعمل على محاكاة الوضع العصبي للمخ في حالة معينة، التي هي السعادة أو الاسترخاء أو النشوة، او التركيز أو الحماسة .
- هذا هو الشعور الإيحائي الزائف بالسعادة أو النشوة أو الاسترخاء أو غيرها، صادر من المخ دون أن تكون لها مصدر حقيقي.

- أنواع المخدرات الرقمية.

الأسطورة البلورية Crystal myth. وهي نوع من النغمات الهادئة التي تبعث على الاسترخاء والهلوسة والهدوء وتبعث في النفس نوع من النشوة من خلال توارد الذكريات الأليمة، كما أن نوع النغمة من النوع الدافعي الهادئ الذي يبعث أحلام اليقظة إلى الفرد، ويبعث في النفس البهجة.[16]

1-الموجه العاليةHeavy metal. وهي نوع من النغمات الصاخبة التي تتسبب في حدوث تحفيز لجميع خلايا الجسم والعقل وتعمل على حفز العقل بالصورة التي تزيد من نشاط الفرد بصورة مذهله

2-موجات الكحول. تهدف هذه المقطوعة إلى منح المتعاطي تأثي أر بالهدوء والاسترخاء يشبه تأثير تناول الكحول.

3-موجات الأفيون. تعمل على منح المتعاطي النشوة والسعادة والنعاس ومحاكاة التأثير الحقيقي لمخدر الأفيون

4-موجات الماريجوانا. تعمل على تهدئة وظائف الجسم ومنح المتعاطي إحساساً بشعور يشبه تدخين نبات الماريجوانا، والدخول في حالة من النشوة والهدوء.

5-موجات الكوكايين. مقطوعة تحمل نغمات منشطة للجهاز العصبي، تعطي إ يشبه تعاطي الكوكايين نفسه، وتولد شعور بالطاقة والنشاط.

6-موجات جنسية. تمنح المتعاطي شعور ر بالنشوة الجنسية، يماثل ممارسة العملية الجنسية والوصول إلى ذروة اللذة.

7-موجات الترفيه. تمنح المتعاطي شعور بالترفيه والسعادة، كما لو أنه يعيش حالة من الراحة والسرور

المطلب الثالث / التحديات والاستجابات للجريمة العابرة للحدود

يبدو من خلال النصوص القانونية الدولية أن عمليات تجريم ومكافحات المخدرات على الصعيد الدولي لا ترقى لمكافحة انتشار الظاهرة ولا حتى لمسايرتها فق ، إذ أن انتشار المدرات وتورها واستهلاكها يشهد ارتفاعا كبيرا وتنوعا معقدا من المخدرات الصلبة والعقارات والأدوية ، ثم بعد ذلك المخدرات الرقمية ، ولا يوجد فيما بحثنا عنه أي نص قانوني متعلق بتجريم المخدرات الرقمية ولا حتى مواجهتها

- **المخدرات الرقمية جريمة سيبيرانية**

كنتيجة حتمية للعولمة، يتأثر عدد متزايد من الأشخاص بالجريمة العابرة للأوطان خاصة المتعلقة منها بالجرائم السيبيرانية "، وهي الحالات التي يُرتكب فيها الجرم الإجرامي في دولة ما خارج الوطن الأصلي للضحية. وفي الواقع قد يكون الضحايا "الأجانب"، مثل السياح، أو طلاب التبادل الجامعي، أو العمال الأجانب عرضة بشكل خاص عندما يجدون أنفسهم في الخارج في الوقت الذي يواجهون فيه جريمة. وقد تعاني هذه الفئة من مشاكل لغوية ومشاكل في فهم النظام القانوني الأجنبي، وهي عوامل غالبًا ما تؤثر بشكل مباشر على قدرتهم على إبلاغ الجريمة إلى السلطات المختصة.

وقد تجعل الفروقات الثقافية الأمر أكثر صعوبة بالنسبة لهم وقد تزيد من خطر تعرض الضحية للشعور بالعزلة والصدمة. وعلاوة على ذلك، وبعيدًا عن أسرهم وأصدقائهم، قد يجد الضحايا أنفسهم بدون دعم اجتماعي قد يحتاجون إلى الاعتماد عليها في أعقاب الجريمة[17].

وقد لا يتمكن ضحايا الجرائم العابرة للحدود من الوصول إلى الخدمات التي يحتاجون إليها: فقد يجدون أنفسهم عالقين في مواقف لا تسمح لهم بالوصول إلى أنظمة مساعدة الضحايا التي تم إنشاؤها في بلد الجريمة، أو تلك الموجودة في بلدهم الأصلي. وبالإضافة إلى ذلك، عندما يحدث الإيذاء للضحية في الخارج، قد تنتهي الإقامة المؤقتة للضحية في البلد الذي حدثت فيه الجريمة. وهذا قد يجعل من المستحيل على الضحية المشاركة في الإجراءات الجنائية بأي طريقة مجدية وعلى هذه الخلفية، شهدت العقود الأخيرة تطوير مبادرات مشجعة للتخفيف من الآثار السلبية للعولمة على ضحايا الجريمة، بما في ذلك العدد المتزايد للذين قد يكونون أكثر عرضة للجرائم العابرة للحدود[18].

- **الأطر القانونية الدولية المتعلقة بالضحايا**

يمكن للضحايا الاعتماد بشكل متزايد على المؤسسات المتواجدة في النُظم القانونية التي قد تدعم احتياجاتهم وحقوقهم. وتشير الدراسات أنه على مدى العقود الماضية، كان إعلان الأمم المتحدة لعام 1985 حافزًا للتغيير ومصدرًا مهمًا لإلهام المشرعين في جميع أنحاء العالم.

ونتيجة لإعلان الأمم المتحدة، أصبحت العدالة للضحايا أكثر واقعية من حيث التغيير التشريعي الذي يؤكد من جديد على حقوق الضحايا، وكذلك من خلال ظهور مؤسسات حكومية وغير حكومية مكرسة لخدمة الضحايا وتلبي احتياجاتهم.

والواقع أن التشريعات الجديدة، سواء على المستوى العالمي والإقليمي والوطني، عززت حقوق الضحايا، بما في ذلك في الحالات التي تنطوي على عنصر عابر للحدود.

وتنص المادة 25 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2004 على أحكام مهمة بشأن الضحايا، وتنص على وجوب أن تتخذ الدول الأطراف، وذلك في حدود إمكانياتها، على التدابير المناسبة لتقديم المساعدة والحماية لضحايا الجرائم المنظمة العابرة للحدود، ولا سيما في حالات التهديد بالانتقام أو الترهيب. والدول الأطراف ملزمة أيضاً بوضع إجراءات مناسبة للوصول إلى التعويض المناسب ورد الحق، وتمكين الضحايا من عرض آرائهم وقلقهم خلال النظر في الإجراءات الجنائية.

ويحتوي بروتوكول الاتجار بالأشخاص ذي الصلة 2000[19] على أحكام شمولية متعلقة بالضحايا. وعلى سبيل المثال ينص البروتوكول على أن تنظر الدول الأطراف في تنفيذ تدابير من شأنها توفير التعافي البدني والنفسي والاجتماعي لضحايا الاتجار بالأشخاص والتعاون مع المنظمات غير الحكومية ومراعاة الاحتياجات الخاصة للضحايا.

كما يستوجب البروتوكول أيضا من الدول الأطراف النظر في اعتماد تدابير تشريعية أو تدابير مناسبة أخرى تسمح لضحايا الاتجار بالأشخاص بالبقاء في إقليمها، بشكل مؤقت أو دائم، و تنص المادة 8 على الحق في العودة إلى الوطن لسلامة ذلك الشخص الاتجار بالأشخاص. ويعتبر هذان النصان الأخيران إضافات مهمة بشكل خاص إلى حقوق الضحايا العادية لأنهم يستجيبون لحاجة العديد من ضحايا الاتجار للحصول على اليقين القانوني حول أين يمكنهم البقاء، أو سيظلون، بعد انتهاء الجريمة التي جلبتهم في كثير من الأحيان إلى بلد أجنبي.

وأما على المستوى الإقليمي، وخاصة في أوروبا، فقد تم تحقيق تحسن كبير في العدالة للضحايا، بما في ذلك في القضايا العابرة للحدود. وفي عام 2015، أصدر الاتحاد الأوروبي توجيهاً شاملاً وملزماً قانونياً لحقوق الضحايا، يحدد الحد الأدنى من المعايير المتعلقة بحقوق ضحايا الجريمة ودعمهم وحمايتهم. ويضمن هذا التوجيه الاعتراف بالأشخاص الذين وقعوا ضحية للجريمة ومعاملتهم باحترام وتوفير الحماية والدعم وتوفير القنوات الملائمة للوصول إلى العدالة في جميع الدول الأعضاء في الاتحاد الأوروبي. كما يتناول التوجيه على وجه التحديد القضايا المتعلقة بالإيذاء عبر الحدود.

وقد كان الاتحاد الأوروبي قد أقام بالفعل نظاماً يسمح بالاعتراف المتبادل بتدابير الحماية في المسائل المدنية بهدف حماية ضحايا العنف والمضايقة بشكل فعال. وإلا أن التشريع الجديد من الناحية العملية يسمح الضحية العنف الحصول على أمر حماية أو أمر تقييد في دولة ما، والتي على سبيل المثال تأمر المعتدي بالبقاء على مسافة معينة من الضحية، فإن هذا الأمر صالح أيضًا في دول أخرى داخل الإتحاد الأوربي.

كما اعتمد الاتحاد الأوروبي توجيهين ملزمين قانونًا بشأن التعويض، حيث أعادوا تأكيد وتنفيذ حقوق الضحايا في التعويض. إلا أنه لا تزال هناك تحديات كبيرة. وعلى وجه الخصوص، يستفيد عدد قليل جدًا من الضحايا .

- **ضرورة تعزيز التعاون الدولي السياسي والتشريعي**

مع تطور السياسة الجنائية في كثير من البلدان ومنها الجزائر سعت للحاق بالركب من خلال تكثيف التعاون مع دول ومنظمات وهيآت ومعاهد دولية مختصة في مكافحة الجريمة السيبيرانية والجريمة العابرة للحدود ، وقد مكن ذلك تكوينات تحسين مستوى وإتقان مستوى وأخرى علمية تخصصية لمصالح القضاء والأمن والباحثين الأكاديميين والمحققين من تحصيل علمي ومعرفي بهذا الشأن[20] .

وبدأت منظمات المجتمع المدني الجديدة التي تحمي الضحايا في لعب دور مهم في المساهمة في هذا التعاون وتعزيزه. وفي عام 1990، تم إنشاء منظمة أوروبية لمقدمي دعم الضحايا، تسمى" منظمة دعم الضحايا في أوروبا ."في الوقت الحاضر، تمثل هذه المنظمة 50 عضوا وطنيا، وتقدم خدمات الدعم والمعلومات إلى أكثر من مليوني شخص متضرر من الجريمة كل عام في 27 دولة. وفي عام 2018، تم تكثيف الجهود لبناء شبكة مثيلة في منطقة آسيا: تسمى" منظمة دعم الضحايا في آسيا ."ولهذه المنظمات لديها وظائف مهمة، حيث إنها تقوم بالحملات لتحسين التشريعات المتعلقة بقضايا الضحايا على المستوى الإقليمي والوطني، وكذلك خلال البحث وتطوير المعرفة، ومن خلال بناء القدرات على المستويين الوطني والمحلي.

وأما على المستوى العالمي، تم إنشاء الجمعية العالمية لعلم الضحايا(WSV) ، وهي منظمة دولية غير حكومية ذات عضوية واسعة من مقدمي الخدمات الضحايا والأكاديميين وممثلي الحكومة والأطباء والمحامين وموظفي إنفاذ القانون وخدمات الطوارئ والطلاب والجمهور، بهدف الدفاع عن الضحايا. فعلى سبيل المثال، ضغطت الجمعية العالمية لعلم الضحايا (WSV) من أجل منح الضحايا المزيد من الحقوق في سياق طلبات المساعدة القانونية المتبادلة، أي أن يتم النظر في منظورهم في تبادل المعلومات الرسمي بين السلطات الوطنية للعدالة الجنائية في القضايا التي تتعلق بعدة دول[21].

- الضحايا في عصر الإنترنت: وسائل التواصل الاجتماعي، وأشكال الاتصال الجديدة، وتأثيرها على العدالة للضحايا

تشكل أهمية الإنترنت والطرق الجديدة للتواصل جزءًا لا يتجزأ من حياتنا. سوف يتم التطُرق في المناقشة التالية لفترة وجيزة فقط على كيفية تأثير ذلك على العدالة للضحايا. *العواقب السلبية* : سمحت الشبكة العنكبوتية ووسائل التواصل الاجتماعي بظهور أشكال جديدة من الجريمة إلا أنه للجرائم السيبرانية، بأشكالها المختلفة، تتمتع بخصائص محددة تجعلها صعبة بشكل خاص من منظور الضحية. وتتسبب الجرائم السيبرانية في أضرار جسيمة وتؤثر على العديد من الضحايا. وبالرغم من ذلك، غالبًا ما يكون من الصعب تقديم الجناة إلى العدالة، ويرجع سبب ذلك في أنهم يختبئون بشكل جيد وراء عباءة عدم الكشف عن الهوية. وتجدر الإشارة أن وجود الجناة في دولة غير تلك التي يقطن بها الضحية، قد يعني أن الضحايا قد لا يتمكنون من رؤية العدالة تتحقق بنفس الطريقة التي يتمتع بها ضحايا الجرائم "التقليدية" ، وكذلك هناك عامل آخر يميز الجريمة السيبرانية عن الأشكال الأخرى للجرائم، وهو حقيقة أن المجرمين الإلكترونيين يمكنهم التفاعل مع ضحاياهم وتهديدهم بطرق افتراضية، وهم قادرون على القيام بذلك في أي وقت سواء خلال النهار والليل، مما يقلل من فرص الضحية في رفع الدعاوى القضائية والمتابعات وتبقى معظم هذه الجرائم في دائرة الإجرام الأسود الذي لا تبلغه أيدي القضاء وذلك بقصد إجرامي في الشبكة العنكبوتية. واستجابة لهذه التهديدات الجديدة، ولذلك يلعب التنبيه والإعلام والتحذير دورا مهما في لفت انتباه الأفراد لضرورة عدم الخوف والتبليغ في كل الظروف .

الجوانب الإيجابية : إلا أنه من الجانب الإيجابي، تقدم الشبكة العنكبوتية ووسائل التواصل الاجتماعي خدمات جديدة يمكن للضحايا استخدامها لتثقيف أنفسهم على حقوقهم ووفرة المساعدة والخدمات المقدمة على الشبكة. كما تقدم وكالات إنفاذ القانون، ومقدمو خدمات مساعدة الضحايا، ومحامو الضحايا، والمشرعين وغيرهم من أصحاب المصلحة مجموعة واسعة من المعلومات ذات الصلة والتي يمكن الو صول إليها على الفور والتي يمكن أن تساعد الضحايا على توجيه أنفسهم في أعقاب الجريمة وتسهل العثور على إجابات أولية للأسئلة العاجلة التي قد تكون لديهم وعلاوة على ذلك، تقدم الشبكة العنكبوتية ووسائل التواصل الاجتماعي منصات جديدة يمكن للضحايا من خلالها التعبير عن أنفسهم. فعلى سبيل المثال، يحتفظ الضحايا بمواقع الإنترنت لمجموعات المساعدة الذاتية للضحايا، حيث يتبادلون الخبرات والأساليب للتغلب على الآثار السلبية للجرائم التي تعرضوا لها، مما يسهل أيضًا على الشخص الذي عانى من جريمة مؤخرًا فقط وقد لا يعرف إلى أين يتجه للسؤال أو الحصول على الدعم[22].

- **<u>تحليل ومناقشة وضع الضحية بين الأطر القانونية وتطور الجريمة</u>**

1- ضخامة النص التشريعي وضعف التنفيذ واللبس في فقراته وبنوده

2- لسوء الحظ، لا تزال نتائج العمل بالقوانين السابقة وتنفيذها وإلزام الدول الأعضاء خاصة منها الدول الكبرى وعلى رأسها أمريكا خارج نطاق الإدانة وفوق النص القانوني وتواصل ارتكاب المجازر في كل أنحاء العالم دون القدرة على توظيف النصوص السابقة لمتابعتها والانتصاف للضحايا ورد الاعتبار لهم أو تعويضهم[23] .

3- وعلى العكس تماما فقد تم توظيف تلك النصوص أحيانا بطرق سياسية وإدارية لابتزاز بعض الدول خاصة تلك التي لديها ملفات الأقليات والمهاجرين ، ,هو ما مكن دول أخرى من التدخل تحت طائلة إنفاذ القانون ذاته لارتكاب جرائم عابرة للحدود والتدل في شؤون تلك الدول مثل ما فعلته فرنسا في بعض الدول الإفريقية أو الشرق أوروبية وما تفعله أمريكا مع كثير من الدول .

4- على الرغم من التطور الكبير لحقوق الضحايا منذ اعتماد إعلان المبادئ الأساسية في عام 1985. فالواقع يؤكد أنه قد يجد الضحايا أنفسهم يواجهون تحديات وعوائق جديدة، ومن بينها تلك التحولات الاجتماعية والثقافية التي أثرت على وصول الضحايا إلى العدالة .

5- تفاوت النصوص القانونية واختلافها وغياب إلزاميتها بين الدول الأعضاء وعدم الوفاء بالتزاماتها أمام حركة انتقال الإفراد والبضائع والوثائق والأموال بين الدول وخارج الحدود الوطنية والقارية يجعلهم ضحية للجريمة في بلد آخر غير بلد إقامتهم. وهذا من شأنه أن يخلق تحديات جديدة للضحايا الذين يسعون للحصول على الدعم أو الإنصاف القانوني. وهذا في حد ذاته يشكل عوامل إضافية معيقة في طريق عدالة حقيقة للضحايا حيث أن الجريمة تتجاوز الحدود القانونية بشكل متزايد

6- نفس العنصر المذكور سابقا حول حركة انتقال الإفراد والبضائع والوثائق والأموال بين الدول وخارج الحدود الوطنية والقارية يجعلهم ضحية للجريمة في بلد آخر غير بلد إقامتهم. وهذا من شأنه أن يخلق تحديات جديدة للضحايا الذين يسعون للحصول على الدعم أو الإنصاف القانوني. وهذا في حد ذاته يشكل عوامل إضافية معيقة في طريق عدالة حقيقة للضحايا حيث أن الجريمة تتجاوز الحدود القانونية بشكل متزايد

7- رغم ظهور طرق جديدة للتواصل من خلال الشبكة العنكبوتية التي توفر فرصًا للضحايا لإسماع أصواتهم، يتطلب إحاطة بالقانون الخاص بالضحايا فضلاً عن غياب تكوين كافي في مجال الدفاع عبر وسائل السيبيرانية للضحايا .

8- فرض تهديدات جديدة في شكل جرائم سيبرانية بين الأشخاص والأشخاص والمؤسسات تجعل من إثبات جرائم المدعى عليهم أصعب ما يكون في ظل تطور وسائل التكنولوجيا وإخفاء أثر الجرائم

الخاتمة :

لم تعد التشريعات الدولية في مجال مكافحة الجريمة والمخدرات ومجال الحفاظ على حقوق الإنسان والضحايا ترقى إلى مسايرة التطورات المستجدة في الصناعات التكنولوجية ذات التأثيرات الجسمية المختلفة والتي عادة ما تتعامل الأجهزة العصبية على خطر كبير على المجتمعات المتخلفة في ذات المجال إذ أن السيطرة عليها يتطلب تطورا على صعيد الصناعات التكنولوجية والطبية وهو التخصص الذي يشهد تخلفا كبيرا في دول العالم الثالث واحتكارا من العالم المتطور ، وكما هو واضح فإن إنتاج المخدرات الرقمية وتسويقها يتم عبر قنوات سيبيرانية مباشرة وغير مباشرة فضرورة الرقابة في مرحلة أولى يتطلب متابعة القنوات واكتشافها وتتبع شبكاتها وكيفية توظيفها تماما مثل المدرات الرقمية ثم السعي للعمل السياسي الخارجي في الاتفاقيات الدولية الثنائية ومن خلال التشريعات الدولية المتعلقة بالضحايا واعتماد العديد من الدراسات الأخرى كقاعدة أساسية للتشريع وحتى التي لا تزال تحاول السعي لإثبات فعالية النقر على الأذنين في العمليات الطبية و الصحة النفسية والعقلية ، و بما أننا قدمنا قراءة لبعض التجارب العلمية ونتائجها ، فنقول بان هناك جانب مفيد لاستخدام التقنية ممكن الإفادة منها في علاج المدمنين على المخدرات التقليدية و من الممكن الاستفادة منها في التدخل العلاجي عن بعد، ولكن الجنب الضار هو الترويج للمخدرات الرقمية باعتبارها تحاكي تأثير المخدرات التقليدية في أوساط الشباب وإثارة المغالطات والإشاعات من شانها والتي بدورها قد تستخدم لغير أغراضها الطبية .

التوصيات :

- نقترح من خلال هذه الورقة البحثية تسلي الضوء على التأثيرات الدوائية والبية للمجال الرقمي وتعميق البحث فيه لمواجهة الأخار والتحديات المحدقة بالأفراد والدول ، جراء الاستخدمات غير الشرعية وخاصة ماتعلق منها بالأشعة ، والتحليلات البصرية والمؤثرات الرقمية العصبية وغيرها مما يمكن استخدامه كسلاح ضد المجتماعت

- كما تضع الورقة البحثية ضمن مقترحاتها لفت انتباه إلى أن النظام الدولي لايضع ضمن أولوياته محاربة المخدرات ولامكافحتها بشتى أنواعها بل يسعى لتقنينها والسماح بها ومن ادول الكثيرة التي بادرت غلى ألك أمثلة كثيرة ، وجب العمل على الصعيد الوطني لليقظة والتنبيه والتحذير من خلال وسائل الإعلام والتحسيس لخطورة المخدرات التقليدية والتعريف بالمخدرات الرقمية وتوجيها الأسر إلى ضرورة مراقبة استهلاك الشبكة العنكبوتية لأبنائهم .

قائمة الهوامش

[1] - Atcherson, Samuel R.; Warren Kennett, Sarah E.; and Nicholson, Nannette, "A Digital Drug? Sound Files Downloaded From The Internet Promise A Substance-Free High. But Is "I-Dosing" Safe?" (2011). Department of Audiology Faculty Articles. 92.
https://nsuworks.nova.edu/hpd_aud_facarticles/92

[2]- Atcherson, Samuel R,et all. Ibid, p 17 .

[3]- Monica Barratt , Alexia Maddox , Jenny L. Davis, Naomi Smith. What are 'binaural beats' and do they affect our brain? Published in the conversation March 31, 2022 . https://theconversation.com/what-are-binaural-beats-and-do-they-affect-our-brain-180235 17/07/2023 .

[4]- Ibid.

[5]- عبير نجم عبد الله الخالدي .(2019). المخدرات الرقمية وتداعياتها على المراهق وسبل الوقاية والعلاج. مجلة ابحاث البصرة للعلوم الانسانية.العدد(4ب). 44. ص ص 258-280 . ص 221 .

[6]- أبو سريع أحمد عبد الرحمن.(2010). استخدام الإنترنت في تعاطي المخدرات المخدرات الرقمية.
https://nccm.gov.eg/UploadedFiles/FormsFiles/2021/9/14.pdf

[7]- Atcherson, Samuel R,et all.ibid.p 17 .

[8]- Psychology Today, Binaural Beats Reviewed by Psychology Today Staff, Sussex Publishers, LLC .https://www.psychologytoday.com/us/basics/binaural-beats viewer en 22/07/2023 .

[9]- Atcherson, Samuel R,et all .ibid. p18 .

[10]- Ibid, p17 .

[11]- Anthony Morlot. Les drogues numériques et ondes binaurales : I-Doser, phénomène de mode ou réel danger ?. Médecine humaine et pathologie. 2012. ffhal-02095408f

[12]- جبيري ياسين. المخدرات الرقمية.(2015) مجلة الشريعة والاقتصاد المجلد 4, العدد 8, الصفحة 563-632 .

[13]- Ron S. Doyle . I-Dosing: Digital Drugs and Binaural Beats Are kids getting high on digital drugs?.publier en July 15, 2010 . psychology today
https://www.psychologytoday.com/us/blog/you-20/201007/i-dosing-digital-drugs-and-binaural-beats . 17/07/2023 .

[14]- Atcherson, Samuel R,et all.ibid.p18.

[15]- شعبان، خالد محمد أبو النجاة. 2019. ظاهرة إدمان المخدرات الصوتية الرقمية بين الفقه الإسلامي و أهل الخبرة : دراسة مقارنة عند المعاصرين. مجلة كلية الشريعة و القانون تفهنا الأشرف- دقهلية، مج. 21، ع. 2، ص ص. 1355-1480. https://search.emarefa.net/detail/BIM-1011010

16- أميرة محمد ابراهيم ساتي.2023 المخدرات الرقمية . المجلة العلمية لنشر البحوث . الاصدار الرابع عشر. ISSN- E: 2617-9563 ، للاطلاع زر الموقع التالي :
https://sjrpublishing.com/%d8%a7%d9%84%d8%a5%d8%b5%d8%af%d8%a7%d8%b1-%d8%a7%d9%84%d8%b1%d8%a7%d8%a8%d8%b9-%d8%b9%d8%b4%d8%b1/

17 - MONICA J. BARRATT, , ALEXIA MADDOX, and other . Who uses digital drugs? An international survey of 'binaural beat' consumers. Drug and Alcohol Review (July 2022), 41, 1126–1130 . DOI: 10.1111/dar.13464

[18] - Baakek, Y. N. E. H., & Debbal, S. M. E. A. (2021). Digital drugs (binaural beats): how can it affect the brain/their impact on the brain. Journal of medical

19- مقارنة عند المعاصرين. مجلة كلية الشريعة و القانون تفهنا الأشرف- دقهلية، مج. 21، ع. 2، ص ص. 1355-1480. https://search.emarefa.net/detail/BIM-1011010

[20]- أميرة محمد ابراهيم ساتي.2023 المخدرات الرقمية . المجلة العلمية لنشر البحوث . الاصدار الرابع عشر. ISSN-E: 2617-9563 ، للاطلاع زر الموقع التالي :

https://sjrpublishing.com/%d8%a7%d9%84%d8%a5%d8%b5%d8%af%d8%a7%d8%b1-/%d8%a7%d9%84%d8%b1%d8%a7%d8%a8%d8%b9-%d8%b9%d8%b4%d8%b1

[21] - https://www.unodc.org/e4j/ar/crime-prevention-criminal-justice . 21/03/2024 10 :15

[22] - ipid

[23] - https://www.ohchr.org/ar/instruments-mechanisms/instruments/protocol-prevent-suppress-and-punish-trafficking-persons 21/03/2024 12:00

[24] - قطاف سليمان ، بوقرين عبد الحليم.، مواجهة الجرائم السيبيرانية في ضوء الاتفاقيات الدولية ، ملة البحوث القانونية والإقتصادية ، مجلد5 ، العدد 2 ، ص 65.

[25] - https://www.unodc.org/e4j/ar/crime-prevention-criminal-justice . 21/03/2024 10 :15 مكتب الأمم المتحدة المعني بمكافحة المدرات والجريمة

26- قادري نور الهدى ، الجريمة السيبيرانية وآليات مكافحتها – مواجهة تحديات الأمن السيبيراني ، المجلة الجزائرية للحقوق والعلوم السياسية ، مجلد8 ، العدد 1 ، ص 327 .[24]

---

[1] Atcherson, Samuel R.; Warren Kennett, Sarah E.; and Nicholson, Nannette, "A Digital Drug? Sound Files Downloaded From The Internet Promise A Substance-Free High. But Is "I-Dosing" Safe?" (2011). Department of Audiology Faculty Articles. 92.
https://nsuworks.nova.edu/hpd_aud_facarticles/92

[2] Atcherson, Samuel R,et all. Ibid, p 17 .

[3] Monica Barratt , Alexia Maddox , Jenny L. Davis, Naomi Smith. What are 'binaural beats' and do they affect our brain? Published in the conversation March 31, 2022 . https://theconversation.com/what-are-binaural-beats-and-do-they-affect-our-brain-180235 17/07/2023 .

[4] Ibid.

[5] عبير نجم عبد الله الخالدي .(2019). **المخدرات الرقمية وتداعياتها على المراهق وسبل الوقاية والعلاج. مجلة ابحاث البصرة للعلوم الانسانية.العدد(4ب). 44. ص ص 258- 280 . ص 221 .**

[6] أبو سريع أحمد عبد الرحمن.(2010). **استخدام الإنترنت في تعاطي المخدرات المخدرات الرقمية.** **https://nccm.gov.eg/UploadedFiles/FormsFiles/2021/9/14.pdf**

[7] Atcherson, Samuel R,et all.ibid.p 17 .

[8] Psychology Today, Binaural Beats Reviewed by Psychology Today Staff, Sussex Publishers, LLC .https://www.psychologytoday.com/us/basics/binaural-beats viewer en 22/07/2023 .

[9] Atcherson, Samuel R,et all .ibid. p18 .

[10] Ibid, p17 .

[11] Anthony Morlot. Les drogues numériques et ondes binaurales : I-Doser, phénomène de mode ou réel danger ?. Médecine humaine et pathologie. 2012. ffhal-02095408f

[12] جبيري ياسين. المخدرات الرقمية.(2015) مجلة الشريعة والاقتصاد المجلد 4, العدد 8, الصفحة 563-632 . 2015-12-01.

[13] Ron S. Doyle . I-Dosing: Digital Drugs and Binaural Beats Are kids getting high on digital drugs?.publier en July 15, 2010 . psychology today . https://www.psychologytoday.com/us/blog/you-20/201007/i-dosing-digital-drugs-and-binaural-beats . 17/07/2023 .

[14] Atcherson, Samuel R,et all.ibid.p18.

[15]شعبان، خالد محمد أبو النجاة. 2019. ظاهرة إدمان المخدرات الصوتية الرقمية بين الفقه الإسلامي و أهل الخبرة : دراسة مقارنة عند المعاصرين. مجلة كلية الشريعة و القانون تفهنا الأشرف- دقهلية، مج. 21، ع. 2، ص ص. 1355-1480. https://search.emarefa.net/detail/BIM-1011010

[16] أميرة محمد ابراهيم ساتي.2023 المخدرات الرقمية . المجلة العلمية لنشر البحوث . الاصدار الرابع عشر. ISSN-E: 2617-9563 ، للاطلاع زر الموقع التالي : https://sjr-publishing.com/%d8%a7%d9%84%d8%a5%d8%b5%d8%af%d8%a7%d8%b1-%d8%a7%d9%84%d8%b1%d8%a7%d8%a8%d8%b9-%d8%b9%d8%b4%d8%b1/

[17] - https://www.unodc.org/e4j/ar/crime-prevention-criminal-justice . 21/03/2024 10 :15

[18] - ipid

[19] - https://www.ohchr.org/ar/instruments-mechanisms/instruments/protocol-prevent-suppress-and-punish-trafficking-persons 21/03/2024 12:00

[20]- قطاف سليمان ، بوقرين عبد الحليم.، مواجهة الجرائم السيبيرانية في ضوء الاتفاقيات الدولية ، ملة البحوث القانونية والإقتصادية ، مجلد5 ، العدد 2 ، ص 65.

[21] - https://www.unodc.org/e4j/ar/crime-prevention-criminal-justice . 21/03/2024 10 :15 مكتب الأمم المتحدة المعني بمكافحة المدرات والجريمة

[22]- قادري نور الهدى ، الجريمة السيبيرانية وآليات مكافحتها – مواجهة تحديات الأمن السيبيراني ، المجلة الجزائرية للحقوق والعلوم السياسية ، مجلد8 ، العدد 1 ، ص 327 .

[23]- قديري مصطفى ، مطبوعة مقياس علم الضحايا موجهة لطلبة السنة أولى ماستر تخصص جريمة وانحراف ، ص80

[24]

الخطوات المفاهيمية للأمن السيبراني

Conceptual steps for cyber- security

سويعدي نجيب جامعة سوق اهراس n.souiadi@univ-soukahras.dz

Abstract:

This research paper seeks to highlight the importance and effectiveness of cyber security theoretical framework, paradigm, policies and concepts concerning the cyber domain - cyber threats - cyber technics to secure networks through a deep conceptual study where we illustrate all the important notions and glossaries.

Key words: *cyber domain -cyber space -cyber threats - cyber security.*

Introduction:

Cyber-attacks are emerging as one of the types of new threats, nations will have to face in the future new kinds of wars different in its nature and structure also cyber conflicts are becoming part of nation's conflicts as a result of interconnected world the cyber domain has become among the most vital element of state existence cyber-attacks can lead to devastating losses of money, trust and reputation for the states, and in order to adapt with the new challenges a new theoretical paradigm and conceptual framework has emerged recent years to cover all this new concepts and notions concerning cyber security policies both in theory and practice and this response approach has come to encompass every area and sectors of modern societies as they all deeply rely on digital infrastructures affected by cyber conflicts and cyber-attacks every theoretical framework is vital to understand the cyber domain and developing policies and conceptual paradigms that will allow digitalized states secure their networks . In order to understand the theoretical framework of cyber security we will develop the following question?

What are the main conceptual approaches for cyber security policies?

We will study the topic through three chapters:

- section 1 : Cyber security domains
- section 2 : Types of cyber security threats
- section 3 : Cyber security Defend Technics

First section: Cyber security domains

First : Critical infrastructure

Critical infrastructure is those physical and digital systems that provide the essential services for a country's economy; therefore the disruption of these systems would create significant economic or public health and safety risk. Cyber security includes the protection of those digital systems from potential cyber-related attacks.

These critical infrastructure sectors include assets owned by government entities as well as those owned by the private sector. (1)

Second: Network security

Network security encompasses all the steps taken to protect the integrity of a computer network and the data within it. Network security is important because it keeps sensitive data safe from cyber-attacks and ensures the network is usable and trustworthy. Successful network security strategies employ multiple security solutions to protect users and organizations from malware and cyber-attacks (2)

Network security has three chief aims: to prevent unauthorized access to network resources; to detect and stop cyber-attacks and security breaches in progress; and to ensure that authorized users have secure access to the network resources they need, when they need them.(3)

Third: End point security

End point security refers to the protection of endpoint security , which is are devices connected to a network , such as desktop computers , laptops, smartphones, tablets, servers, and other internet of things devices .the goal of end point security is to secure these devices against various threats and prevent unauthorized access, data breaches malware infection and other cyber-attacks .

End point security solution is designed to defend against these threats by implementing a combination of technologies and practices to protect the devices and the data they contain. (4)

Forth: Application security

Application security (AppSec) helps protect application data and code against cyber-attacks and data theft. It covers all security considerations during application design, development, and deployment.

AppSec involves implementing software, hardware, and procedures that identify and reduce the number of security vulnerabilities and minimize the chance of successful attack.

AppSec typically involves building protections and controls into software processes. For example, automated static analysis of new code, testing new software releases for security vulnerabilities or misconfigurations, and using an application firewall to strictly define.(5)

Fifth: cloud security

Cloud security refers to the cyber security policies, best practices, controls, and technologies used to secure applications, data, and infrastructure in cloud environments. In particular, cloud security works to provide storage and network protection against internal and external threats, access management, data governance and compliance, and disaster recovery.

Cloud computing has become the technology of choice for companies looking to gain flexibility needed to accelerate innovation and meet the expectations of today's modern consumers. But migrating to more dynamic cloud environments requires new approaches to security to ensure that data remains secure across online infrastructure, applications, and platforms.

Types of Cloud Security solutions

- Identity and access management (IAM): IAM services and tools allow administrators to centrally manage and control who has access to specific cloud-based and on-premises resources. IAM can enable you to actively monitor and restrict how users interact with services, allowing you to enforce your policies across your entire organization.

- Data loss prevention (DLP): DLP can help you gain visibility into the data you store and process by providing capabilities to automatically discover, classify, and de-identify regulated cloud data.

- Security information and event management (SIEM): SIEM solutions combine security information and security event management to offer automated monitoring, detection, and incident response to threats in your cloud environments. Using AI and ML technologies, SIEM tools allow you to examine and analyze log data generated across your applications and network devices—and act quickly if a potential threat is detected.

- Public key infrastructure (PKI): PKI is the framework used to manage secure, encrypted information exchange using digital certificates. PKI solutions typically provide authentication services for applications and verify that data remains uncompromised and confidential through transport. Cloud-

based PKI services allow organizations to manage and deploy digital certificates used for user, device, and service authentication. (6)

Sixth : Information security

Information security can be defined as the set of protocols and practices that are put in place to secure data from threats such as unauthorized modifications and access. Information security deals with data security while data is stored and transported between two destinations. Most of the time, the data information security deals with is sensitive, confidential and private.

The main way information security works is by protecting important data from all types of unauthorized modification, inspection, disruption, and/or recording. More specifically, information security keeps intellectual property, financial records, and user account details away from various kinds of cyber threats and otherwise. Unlike cyber security, information security deals with both logical and physical issues that can arise when dealing with data and takes steps to protect against. (7)

Seventh: Mobile security

Mobile security is the process of protecting sensitive data stored on any mobile device, this refers to many devices including laptops, smartphones, tablets smart watches with mobile devices being engrained in society more each year we need to be cognizant of mobile security due to them having vulnerabilities in protection .

Mobile security, often referred to as wireless security, involves protecting both personal and business-related information stored on and transmitted from smartphones, tablets, laptops, wearable and other portable devices. It addresses the threats, vulnerabilities and attacks unique to mobile computing.

Mobile security covers multiple aspects such as:

- Data protection: Preventing unauthorized access to sensitive information on a device such as personal details, photos, banking data and business emails.
- Access control: Implementing authentication measures such as passwords, biometrics or two-factor authentication to restrict access to the device and its data.
- Application security: Ensuring that applications on the device are secure and do not pose a risk to the device's data.
- Network security: Securing the network connections (like Wi-Fi or cellular networks) the device connects to, preventing spoofing attacks.

- **Physical security: Preventing physical theft of the device, and securing the device if it falls into the wrong hands.**(8)

Second section : Types of cyber security threats

Cyber security threats are acts performed by individuals or groups with harmful intent, whose goal is to steal data, cause damage to or disrupt computing systems. Cyber threats can originate from a variety of sources, from hostile nation states and terrorist groups, to individual hackers, to trusted individuals like employees or contractors, who abuse their privileges to perform malicious acts. Cyber attackers come in many forms and with different motivations. In cyber security terminology, these disparate groups are often bundled together using the term "threat actors". In 2022, malicious threat actors adapted quickly to exploit changes in the political, technological and regulatory landscapes. In cyber security, attackers have a structural advantage: they need to find only one exploitable weakness across an organization. This means attackers have less ground to cover than a defender and the attacker can often adapt faster than organizations can defend or recover. The threat landscape has become increasingly volatile. Professionalized cybercriminal groups have continued to grow and create a higher volume of new attack types. (9) **Generally we can find numerous of cyber threats such as:**

First: Nation states cyber attack

State-sponsored cyber-attacks refer to cyber-attacks that are initiated or supported by governments to achieve specific political, economic, or military objectives these attacks are characterized by their sophistication, stealth, and persistence, with state-sponsored attackers often employing advanced techniques and tools to evade detection cyber-attacks can target a wide range of entities, including critical infrastructure, government agencies, and private companies, and can have significant economic, political, and security implications State-sponsored cyber-attacks, also known as cyber-enabled espionage, refer to the use of digital tools and techniques by governments or state-affiliated actors to gain unauthorized access to sensitive information or computer systems belonging to individuals, organizations, or other states. These attacks are characterized by the use of sophisticated and often stealthy techniques such as malware, phishing, and social engineering to compromise the target systems or networks, and the theft of sensitive data, intellectual property, or strategic information for political, economic, or military gain One of the primary motivations for state-sponsored cyber-attacks is to gain a strategic advantage over other countries or actors in the international arena. These attacks can be used to undermine the security and stability of other nations, disrupt critical infrastructure, or steal sensitive information that can

be used for economic or military purposes, stealing trade secrets and Intellectual property worth billions of dollars state sponsored cyber-attacks is the use of deniability and deception to mask the identity of the attacker. Governments often use third party actors, such as criminal syndicates or hacktivist groups, to carry out attacks on their behalf, making it difficult to attribute responsibility for the attack. This allows states to pursue their strategic objectives without facing diplomatic or military Consequences for their actions.(10)

Second: Cybercrimes

Cybercrime is any criminal activity that involves a computer, network or networked device. While most cybercriminals use cybercrimes to generate a profit, some cybercrimes are carried out against computers or devices to directly damage or disable them. Others use computers or networks to spread malware, illegal information, images or other materials. Some cybercrimes do both i.e. target computers to infect them with a computer virus, which is then spread to other machines and, sometimes, entire networks. A primary effect of cybercrime is financial. Cybercrime can include many different types of profit driven criminal activity, including ransom ware attacks, email and internet fraud, and identity fraud, as well as attempts to steal financial account, credit card or other payment card information. As cybercriminals might target an individual's private information or corporate data for theft and resale .(11)

Third: Cyber terrorism

Cyber terrorism is usually defined as any premeditated, politically motivated attack against information systems, programs, and data that threatens violence or results in violence. (12) It might include any cyber-attack that intimidates or generates fear in the target population of a country, state, or city, usually by damaging or disrupting critical infrastructure that's vital to social, economic, political, and business operations. Cyber terrorist acts are carried out using computer servers, other devices and networks visible on the public internet. Secured government networks and other restricted networks are often targets of such acts. Other targets include the banking industry, military installations, power plants, air traffic control centers, and water systems. (13)

Forth: Malware Cyber attackers use harmful software such as spyware, viruses, ransom ware, and worms known as malware to access your system's data. When you click on a malicious attachment or link, the malware can install itself and become active on your device.

Fifth: Ransom ware

Ransom ware is malicious software that cyber attackers can install on your device, allowing them to block your access until you pay the attackers a ransom. However, paying the ransom doesn't guarantee the removal of the software, so experts often advise individuals not to pay the ransom if possible.

Sixth: Password attacks

Password attacks can be as simple as someone correctly guessing your password or other methods such as key logging, where attackers can monitor the information you type and then identify passwords. An attacker can also use the aforementioned phishing approach to masquerade as a trusted site and try to fool you into revealing your account credentials.(14)

Seventh: Spyware

This malware gathers a user's personal information and send it to a third party without the user's consent often used for identity theft

Eight: Distributed denial of service (DoS)

This attack floods a network or service with excessive requests to overwhelm it, making the service slow or entirely unavailable to legitimate users (15)

Third section: Cyber security Defend Technics

First: zero trust model

It is a philosophy or mindset to build a defensible security model encompassing a variety of different safety measures, capabilities, best practices and technological bricks.(16)Zero trust is a network security that states no one inside or outside the network should be trusted unless their identification has been thoroughly checked. Zero trust operates on the assumption that threats both outside and inside the network is an omnipresent factor. Zero trust also assumes that every attempt to access the network or an application is a threat. These assumptions inform the thinking of network administrators, compelling them to design stringent, trustless security measures (17)

Second: Behavioral Analytics Model

Behavior analytics is a branch of security analytics that focuses on analyzing patterns of behavior and activities within an organization's network or system to detect and mitigate security threats. By leveraging behavior analytics, organizations can gain insights into user behavior, identify potential threats and risks, and respond swiftly to security incidents. These techniques enhance the overall security posture by complementing traditional security measures and providing a proactive approach to threat detection and mitigation In terms of cyber security, behavior analytics analyzes large data sets using artificial intelligence (AI) and machine learning (ML) techniques. It allows you to identify unusual patterns that deviate from regular patterns or usage that indicate malicious activities that could potentially stem from cyber attackers. (18)

Conclusion:

cyber security has become today a part a state power and if any country wants to be a cyber-power it must elaborate a comprehensive paradigm with a national cyber strategy conceived within a theoretical framework that defines the essential concepts of the cyber domain -cyber threats - cyber technics and put it's as a priority framework and vital to a nation's efficient cyber power.

REFERENCES :

(1) https://verveindustrial.com/resources/blog/critical-infrastructure-cyber-security
(2) https://www.techtarget.com/searchnetworking/definition/network-security
(3) https://www.ibm.com/topics/network-security
(4) https://www.fortinet.com/resources/cyberglossary/what-is-endpoint-security
(5) https://www.hackerone.com/knowledge-center/what-application-security-concepts-tools-best-practices
(6) https://cloud.google.com/learn/what-is-cloud-security
(7) https://securitygladiators.com/security/information/
(8) https://www.forbes.com/advisor/business/what-is-mobile-security/
(9) *https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf p 12*
(10) Callistus Francis Azubuike Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks, Nnamdi Azikiwe Journal of Political Science University, Awka, Anambra Nigeria 2023, Vol. 9
https://www.researchgate.net/publication/375085530_Cyber_Security_and_International_Conflicts_An_Analysis_of_State-Sponsored_Cyber_Attacks

(11) https://www.techtarget.com/searchsecurity/definition/cybercrime

(12) https://www.techtarget.com/searchsecurity/definition/cyberterrorism

(13) Sirohi, cyber terrorism and information warfare, alpha edition, Delhi, India, 2015 p 15

(14) https://www.coursera.org/articles/types-of-cyber-attacks

(15) https://www.google.dz/books/edition/Cyber_Security_certification_guide/M7fnEAAAQBAJ?hl=fr&gbpv=1

Cybellium, cybersecurity certification guide, a comprehensive guide to cyber security certification, 2023, p 268.

(16) Community paper, the zero trust model in cyber security, towards understanding and deployment, World Economic Forum, august 2022 p 7.

(17) *https://www.fortinet.com/resources/cyberglossary/what-is-the-zero-trust-network-security-model*

(18) https://www.splunk.com/en_us/blog/learn/behavioral-analytics.html

Recommendations:

- ✓ **Should educate leading elites about the terms and cyber security concepts in order to be familiar and usable.**
- ✓ **Replace the traditional concepts about security among the leading elites and institutions by the new paradigm of cyber security.**
- ✓ **Promote interdisciplinary studies in order to build a national theoretical road map**
- ✓ **Promote using and learning foreign languages specially English in order to build a national reference data concerning cyber security concepts both in English and Arabic**
- ✓ **Encourage international cooperation by using national universities and research centers as plat forms for learning educating training through seminars workshops**
- ✓ **Make transferring technology as a priority in all levels and institutions**
- ✓ **Invest heavily in all cyber security steps (infrastructure - concepts - technics)**
- ✓ **Modified the traditional defense creed with the new treats as a new vision for the national institutions**

التوصيات :

لقد خرج الملتقى بعدة توصيات أهمها:

- بناء استراتيجية شاملة للأمن السيبراني تضم ما يلي:

أولا على مستوى الجانب التشريعي والمؤسساتي:

- ✓ توفير عدة قانونية للأمن المعلوماتي وحماية المعلومات والشبكات .
- ✓ حماية الخصوصية .
- ✓ تحديد لإطار القانوني للإعلام الالكتروني.
- ✓ وضع آليات مكافحة الجريمة السيبيرانية(الالكترونية).
- ✓ حماية الملكية الفكرية.
- ✓ تقنيين المعاملات الالكترونية التجارية .

ثانيا: توطين تكنولوجيا لاعلام والاتصال في الجزائر وذلك عبر:

- ✓ لاستثمار في البنية التحتية إذ يجب التعزيز في استثمارات تحديث وتعزيز البنية التحتية السيبرانية كجزء أساسي من لاستراتيجية الوطنية في الجزائر. يتعين زيادة حجم لاستثمار لضمان تحديث الأنظمة وتطويرها، مما يعزز فعالية لاستجابة للتحديات الرقمية المتزايدة. يسعى هذا لاستثمار إلى تحسين قدرة الجزائر على مواجهة التهديدات السيبرانية المتطورة وتحقيق مستويات عالية من لأمان ولاستدامة في البنية التحتية التكنولوجية.
- ✓ ضرورة إيجاد اليات جديدة تتماشى والتهديدات الجديدة(مثلا تطبيق تقنيات الحدود الذكية)
- ✓ تهيئة البيئة لإدماج تكنولوجيات لإعلام والاتصال في مجالات الحياة من أجل لاستفادة القصوى من إمكانياتها المختلفة مع ضرورة اعتماد لاستشراف التكنولوجي الذي يوفر المنهجيات المناسبة لتحقيق أهداف الحماية لاستباقية والسرية والصمود والتصدي وكذا التعافي في حالة وجود اختراقات الكترونية.
- ✓ تطوير برامج تدريب متقدمة حيث ينبغي تطوير وتنفيذ برامج تدريب متقدمة بشكل دوري، تستهدف تعزيز وتطوير مهارات وقدرات الكوادر الفنية المختصة في مجال لأمن السيبراني. يهدف هذا التدريب إلى تزويد الفرق الفنية بالمعرفة والمهارات اللازمة لمواكبة التطورات السريعة في مجال لأمن السيبراني والتصدي للتحديات المتزايدة بفعالية. يسهم هذا النهج في تحسين قدرة الكوادر على تنفيذ استراتيجيات أمان متقدمة وتطبيق أفضل الممارسات في مجال الحماية الرقمية مع اعتماد التدريب والرسكلة للمتعاملين مع هذه التكنولوجيات خاصة ما تعلق منها

بالتعامل مع الاختراقات الالكترونية وضمان السرية والآليات الكفيلة بذلك، إضافة إلى العمل على توعية المستخدمين بالأخطار الالكترونية المحتملة.

- ✓ استحداث استراتيجيات تتميز بالشمولية، بحيث تقوم على مقاربة شاملة بين التكنولوجيات وباقي القطاعات مع تحديد آليات التنفيذ وأدوات قياس تحقيق الأهداف وتقييمها وتقويمها، فلا يمكن بأي حال من الأحوال تحقيق الأمن السيبراني المطلق نظرا لتعقد متغيراته وتداخل مهدداته، لهذا يجب التركيز على المجالات الأكثر هشاشة وأهمية في تحقيق أمن سيبراني نسبي بشكل مستدام، ثم الانتقال إلى مجالات أقل تهديدا عبر مقاربة تكاملية شاملة مع اعتماد النهج التشاركي بتفعيل الشراكة بين الحكومة والمجتمع المدني من جهة وبين الحكومة والقطاع الخاص والمنظمات الدولية والأوساط الاكاديمية .
- ✓ تطوير مجال البرمجيات والتطبيقات والنظم المعلوماتية والتشجيع على الابتكار في المجال وكذا التكفل بالمشاريع التقنية الابداعية.
- ✓ على الصعيد الخارجي وجب محاولة التموقع ضمن الخريطة الجيومعلوماتية، ورأب الفجوات الرقمية الموجودة، مع العمل على البحث في السبل الكفيلة بالمشاركة في حوكمة الانترنت على الصعيد الدولي.
- ✓ من الضروري تعزيز التعاون الدولي في ميدان الأمن السيبراني، بهدف تيسير تبادل الخبرات وتقديم الدعم المتبادل لمواجهة التحديات السيبرانية المشتركة. يتعين تعزيز هذا التعاون الدولي على مستوى السياسات والتقنيات، مما يساهم في تعزيز قدرة الدول على التصدي للتهديدات السيبرانية بفعالية وفي تعزيز المرونة والأمان الرقمي على الصعيدين الوطني والدولي.

- ثالثا: خلق الثقافة التقنية وتعزيزها بتحقيق ما يلي :

- ✓ رقمنة المحتوى المحلي، والعمل على تعزيز آليات الحماية والسرية.
- ✓ تنمية المهارات الشخصية التي تتجاوز المهارات التقنية ومهارات التصفح الى مهارات أخرى كالمهارات التشغيلية ومهارات إدارة المعلومات ومهارات إعداد المحتوى والمهارات الرقمية بصفة عامة.
- ✓ المراهنة على المناهج التدريسية والتعليمية لغرس الثقافة التقنية. فالأمن السيبراني يمثل مقاربة متكاملة يجب على الجهات المختصة عدم إقصاء أي طرف في التعامل مع متطلبات تحقيقه، انطلاقا من التنشئة الأكاديمية للتلاميذ وصولا إلى التخصصات الجامعية للطلبة، بالإضافة إلى نشر التوعية المجتمعية حول أهمية الأمن السيبراني للأمة.

- ✓ بناء قاعدة معرفية تقنية وذلك بالتركيز على المورد البشري وتلقينه المهارات الرقمية مع نشر الثقافة التقنية وتشجيع الابتكار والاستثمار فيه ودعم التعليم ومراكز البحث والتطوير وزيادة الاهتمام بالموارد البشرية في المجال خاصة ما تعلق بالمورد البشري المؤهل والمتخصص.

الفهرس:

العنصر	الصفحة
مطوية الملتقى	02
برنامج الملتقى	05
المداخلات	
نحو تحقيق الأمن السيبراني في الجزائر: الدعائم والآليات، د/ سلاف بوصبع	11
الأمن السيبراني الوطني في مواجهة حروب الجيل الخامس. د/سيدهم ليلى ،أ.د/ درويش جمال	21
الأمن والحرب في الفضاء السيبراني: إطار مفاهيمي . د/حميز سمير	32
الهندسة الأمنية السيبرانية الجزائرية في مواجهة الجرائم الإلكترونية. د/ عدار محمد	39
الإدارة الرقمية وتحديات الأمن السيبراني .ط.د/ دراويش الطيب و أ.د/ لقرع بن علي	59
الحروب السيبرانية في العلاقات الدولية: دراسة في المفهوم، التطور والتأثير. د/ موسى بن قاصير	70
الأمن السيبراني عبر مواقع التواصل الاجتماعي: المخاطر والحلول. د/رفاس وليد ود/كامل نجيب	83
دور التحول الرقمي في صياغة وتغيير المفاهيم التقليدية في الأمن والجريمة والحرب والسيادة في العصر السيبراني – قراءة في التحديات ورهانات المواجهة الوطنية- د/ بلبشير يعقوب وأ.د/ جيلالي دلالي	92
كيف يتم بناء موضوع الأمن من منظور مدرسة كوبنهاغن؟ الأمن السيبراني نموذجا ط.د نسيبة تامة وأ.د/ مشري عبد الحميد	106
الآليات التشريعية الوطنية لمكافحة الجرائم السيبرانية في عصر الذكاء الاصطناعي –واقع وتحديات- ط.د/ بن عمارة دلال	115
Le devoir de l'adaptation de l'Algérie à l'ère numérique : vision à long termes, défis et perspectives de protection cyberienne . Dr HASSANI Rima Aida & Dr GHAMRI Sara	125
الحرب الهجينة ومهددات الأمن السيبراني. د/نوري عزيز ود/سليمان سميرة	132
الإنترنيت المظلم كفضاء للجريمة المنظمة السيبرانية في ظل الثورة التكنولوجية الرابعة – مقاربة مفاهيمية - د/إيمان بن نعجة	143
اسهامات نظريات العلاقات الدولية في تفسير تطور مفهوم الامن – من الأمن القومي الى الأمن القومي السيبراني. ط.د/ بن جدو أسماء	159
واقع ورهانات الأمن السيبراني في العقيدة الدفاعية الجزائرية. أ.سالم نسرين	173

أثر المخاطر السيبرانية على الأمن القومي في الجزائر. ط.د/ جدي علاء الدين ود/سرير عبدالله أمينة	181
الحروب السيبرانية وتأثيرها الاستراتيجي على الأمن القومي للدول:"الواقع والتحديات". د/حمزاوي جويدة	193
الجريمة الالكترونية وتهديدها للأمن السيبراني للتراث الأرشيفي الرقمي. ط.د/لموشي رزيقة ود/شواو عبد الباسط	204
The Legislative Framework of Cyber Security in Algeria . - *Dr. DJENDI sarra &* - *Dr. HADJADJ Mourad* -	214
الأمن السيبراني في الجزائر: التحديات والرهانات. د/دريادي حميدة	224
"في فهم وتحليل الجرائم السيبرانية والتهديدات الأمنية العابرة للحدود: مقاربة معرفية" د. الحامدي عيدون، و ط.د.رابح فرطاس،	238
الجرائم السيبرانية و آليات مواجهتها في الجزائر . ط.د/محمد لسعد سيد عمر	257
الحماية الرقمية :رؤية استباقية نح تعزيز الامن السيبرانية في الجزائر ط.د/مزهود صورية.ود/بويبية نبيل	268
الحقوق الرقمية وتحديات الأمن السيبراني في ظل أنظمة الذكاء الاصطناعي (في القانون المقارن) ط.د/بلعروسي أمين ود/الدكتور عبابسة حمزة	281
المخدرات الرقمية تحدي جديد أمام القانون الدولي. د. مصطفى قديري و د. سمير فلاح	299
Conceptual steps for cyber- security.Dr Souidi Nadjib	315
توصيات الملتقى	324
الفهرس	326