

الآليات المسخرة لمواجهة تحديات الأمن السيبراني في الجزائر

د. عادل بوعرعار،¹

1. جامعة المدية ، الجزائر bouarar.adel@univ-medea.dz

تاريخ الاستلام: 2025/05/15 تاريخ القبول: 2025/06/10 تاريخ النشر: 2025/06/30

الملخص:

إن الواقع الرقمي الذي فرض وجوده في العالم، أصبح بيئة خصبة لجرائم كلاسيكية وجد مرتكبوها وسائل جديدة لارتكابها، وكذا جرائم مستحدثة لم تكن لتظهر لولا هذه البيئة الرقمية، وتسعى دول العالم والجزائر من بينها إلى مواكبة هذه التهديدات السيبرانية التي تستهدف الأفراد والمؤسسات، عبر انتهاج مخططات أمنية قصد حماية منظومتها المعلوماتية من جهة والأشخاص سواءا طبيعيين أو معنويين من جهة أخرى. من خلال هذه المداخلة سنحاول التطرق للآليات الأمنية المنتهجة من طرف الدولة، وكذا الترسانة المؤسساتية المعتمدة لمواجهة تهديدات الجرائم الإلكترونية المختلفة وتدعيم الأمن السيبراني. الكلمات المفتاحية: الجريمة الالكترونية، الامن السيبراني. التهديدات السيبرانية .

Abstract:

The cyber reality that swept the world has become a fertile environment for classic crimes whose perpetrators found new means to commit them, as well as new crimes that would not have appeared without this digital environment. Countries around the world, including Algeria, are striving to keep pace with these cyber threats that target individuals and institutions, by adopting security strategies in order to protect their information system and people, both ordinary and legal.

In this intervention, we will try to address the security mechanisms adopted by the state, as well as the institutional arsenal dedicated to confronting various cybercrime threats and strengthening cybersecurity.

.Keywords::Cybercrime, cybersecurity. Cyber threats

مقدمة:

لقد عرف العالم خلال العقد الأخير طفرة تكنولوجية في مجال الإعلام و الاتصال، هذه الأخيرة شملت ظهور فضاءات سيبرانية تتفاعل فيها مختلف الكيانات من أفراد و مؤسسات و شركات و إدارات و حكومات.. الخ ، حيث وصل عدد مستخدمي الأنترنت في العالم سنة 2021 إلى 4.9 مليار شخص بنسبة 63% من سكان العالم ، و هو الأمر الذي ساعد في إرتفاعه حالات الحبر الصحي المرافقة لجائحة كورونا خلال السنتين الماضيتين، إن تفاعل هذا العدد الهائل من المستخدمين ينجر عنه ارتفاع عدد الجرائم السيبرانية التي تعددت أشكالها فمنها الجرائم التقليدية التي وجد مرتكبوها فضاءات افتراضية جديدة لارتكابها، و منها جرائم مستحدثة و اكبت التطور التقني و الرقمي .. و تماشيا مع هاته المستجدات كان على الدول و المؤسسات استحداث أنظمة أمن سيبراني لحماية بياناتها وقواعدها الرقمية.

والجزائر كذلك ككل دول العالم تحاول مجارات التطورات الرقمية عبر تحديث أنظمتها الأمنية، قصد حماية الأفراد و المؤسسات وكذا الإدارات وقواعد البيانات والنظم الرقمية الوطنية، وذلك عبر تحيين التشريعات القانونية لتتماشى مع الجرائم المستحدثة من جهة، وكذا إستحداث مؤسسات متخصصة ذات كفاءة في مجابهة تحديات الأمن السيبراني.

1. الجريمة السيبرانية :

1.1 ماهية الجريمة السيبرانية :

لقد تطورت أنماط الجريمة بشكل واضح خلال العشرية الأخيرة، حيث تعدت أهدافها استهداف الضحايا في الأنفس و الأموال فقط بل طالت البيانات و المعلومات، حيث عرف هذا النوع من الجرائم في بعض الأوساط بإجرام ذوي "الباقات البيضاء" حيث يستطيع المجرم العصري ارتكاب جريمته ليس فقط دون عنف مباشر أو إراقة الدماء، و لكن دون أن يتحرك من مكانه أو ينهض من كرسيه، و هو ما جعل البعض يصفها بالجرائم الناعمة، فببضع ضغطات على لوحة المفاتيح من قبل المجرم السيبراني يمكن أن تتبعها آثار كارثية على الأفراد أو المؤسسات و حتى الاقتصادات، و ما زاد هذا النوع من الجرائم تأثيرا أنه غير مرتبط بإطار مكاني محدود فهي جريمة عابرة للدول و القارات، لذلك في تعتبر مشكلة عالمية تمس كل الدول على حد سواء. (سميرة 2010، 276)

2.1 تعريف الجريمة السيبرانية :

للجريمة السيبرانية عدة تسميات، فهناك من يسميها بجرائم الحاسوب أو جرائم الأنترنت، أو الجريمة التقنية، وتعدد المسميات تتعدد التعاريف فمنهم من يربطها بالشق التقني، فيما يربطها آخرون بالشق القانوني، فتعرف على أنها فعل ضار يستخدم فيه الفاعل "الذي يفترض أن تكون لديه خلفية معرفية بتقنيات الحاسوب" نظاما حاسوبيا أو شبكة بيانات حاسوبية للوصول إلى البيانات أو البرامج بقصد (نسخها، تغييرها، حذفها، تزويرها، تخريبها، تجميدها، الاستيلاء عليها، توزيعها أو نشرها بشكل غير مشروع. (كامل 2000).

كما تعرف أيضا بأنها "الجرائم التي ترتكب ضد أفراد أو مجموعات مع وجود دافع إجرامي لإلحاق الضرر عمدا بسمعة الضحية، أو التسبب بالأذى الجسدي أو النفسي للضحية بشكل مباشر أو غير مباشر، باستخدام شبكات الاتصال الحديثة مثل الإنترنت (مواقع التواصل الاجتماعي، غرف الدردشة، البريد الإلكتروني...)، والهواتف النقالة (الرسائل النصية القصيرة ورسائل الوسائط المتعددة)، وتشمل الجرائم الإلكترونية أي فعل إجرامي يتم من خلال الحواسيب أو الشبكات كعمليات الاختراق والقرصنة، كما تضم أيضا أشكال الجرائم التقليدية التي يتم تنفيذها عبر الإنترنت، ولقد عرفها الدكتور عبد الفتاح مراد على أنها: "الأفعال المخالفة للقانون والشرعية والتي ترتكب بواسطة الحاسب الآلي من خلال شبكة الانترنت وهي تتطلب إلمام خاص بتقنيات الحاسب الآلي و نظم المعلومات سواء لارتكابها أو للتحقيق فيها ويقصد بها أيضا أي نشاط غير مشروع ناشئ في مكون أو أكثر من مكونات الانترنت مثل مواقع الانترنت وغرف المحادثة أو البريد الإلكتروني كما تسمى كذلك في هذا الإطار بالجرائم السيبرانية لتعلقها بالعالم الافتراضي"، وهناك من يسميها أيضا بجرائم التقنية العالية أو جرائم أصحاب الياقات. (إسرائيل جبريل 2016)

كما يشار إلى إساءة استخدام تكنولوجيا المعلومات والاتصالات من قبل المجرمين بالتبادل على أنها جرائم الإنترنت، أو إساءة استخدام الكمبيوتر، والجريمة المرتبطة بالحاسب الآلي، جريمة التكنولوجيا العالية، والجريمة الإلكترونية، والجريمة الإلكترونية كما عرفت رابطة كبار ضباط الشرطة (ACPO) تنطوي على "استخدام الكمبيوتر أو الإنترنت شبكات تكنولوجيا لارتكاب أو تسهيل ارتكاب الجريمة". بينما من جانب آخر فيعتبر المعهد الاسترالي لعلم الإجرام (AIC) بأنها "تسمية عامة لجرائم ارتكبت باستخدام تخزين البيانات الإلكترونية أو جهاز الاتصالات (Brown) (2015, 57).

أما في الجانب القانوني فقد اصطلح المشرع الجزائري على تسمية الجرائم الإلكترونية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وعرفها بموجب المادة 02 من القانون 09-04 المؤرخ في 05 أوت 2009، على أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات الآلية المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية. (القانون رقم 09-04 المؤرخ في 05 أوت 2009، (5

وبشكل أوسع يمكن تعريف الجريمة الإلكترونية بأنها كل أشكال السلوك غير المشروع، والمتعمد الذي يرتكب باستخدام الحاسب الآلي المرتبط بالإنترنت، والتي تمس به أو بمحتوياته أو بالعمليات التي تتم بواسطته، بغرض إلحاق الضرر بالضحية أو الكسب المادي أو غير ذلك من الأغراض، من طرف أفراد على دراية كاملة بتقنيات التكنولوجيا المعلوماتية وأسرارها.

3.1 مجالات تصنيف الجريمة السيبرانية :

لم يستقر الفقهاء على معيار واحد لتصنيف الجرائم الإلكترونية وذلك راجع إلى تشعب هذه الجرائم، وسرعة تطورها، فمنهم من يصنفها بالرجوع إلى وسيلة ارتكاب الجريمة، أو دافع المجرم، أو على أساس محل الجريمة، وعلى هذا الأساس يمكن تصنيفها إلى ما يلي: (صغير 2013، 43-58)

1.3.1 الجرائم الواقعة على الأموال: في ظل التحول من المعاملات التجارية التقليدية إلى المعاملات التجارية الإلكترونية، وما انجر عنه من تطور في وسائل الدفع والاستلام، وفي خضم التداول المالي عبر الإنترنت، أصبحت هذه المعاملات عرضة لشتى أنواع الجرائم.

2.3.1 الجرائم الواقعة على الأشخاص: مع تطور شبكة الإنترنت أصبحت المعلومات المتعلقة بالأفراد متداولة بكثرة عبرها، مما جعلها عرضة للانتهاك من طرف هؤلاء المجرمين وجعلت سمعة الأفراد مستباحة.

3.3.1 الجرائم الواقعة على أمن الدولة: من أهم الجرائم الإلكترونية التي تهدد أمن الدول وهي ما يلي:

- **الجماعات الإرهابية :** استغلت الكثير من الجماعات المتطرفة الطبيعة الاتصالية للأنترنت من أجل بث معتقداتها وأفكارها، بل تعداه الأمر إلى ممارسات تهدد أمن الدولة المعتدى عليها.

- **الجريمة المنظمة :** استغلت عصابات الجريمة المنظمة الإمكانيات المتاحة في وسائل الاتصال والآنترنت في تخطيط وتوجيه المخططات الإجرامية وتنفيذ العمليات الإجرامية بيسر وسهولة.

- **الجرائم الماسة بالأمن الفكري :** يبقى الأمن الفكري من بين أخطر الجرائم المرتكبة عبر الإنترنت، حيث تعطي الآنترنت فرصا للتأثير على معتقدات وتقاليد مجتمعات بأكملها مما يجعلها عرضة للهزيمة الفكرية وهو ما يسهل خلق الفوضى.

- **جريمة التجسس الإلكتروني :** سهلت شبكة الإنترنت الأعمال التجسسية بشكل كبير حيث يقوم المجرمون بالتجسس على الأشخاص أو الدول أو المؤسسات الدولية أو الوطنية، وتستهدف عملية التجسس في عصر المعلوماتية ثلاث أهداف رئيسية وهي : التجسس العسكري، والتجسس السياسي، والتجسس الاقتصادي. وفي تصنيف آخر موسع يمكن تعداد مظاهر الجريمة السيبرانية فيما يلي:

1. تخريب المعلومات وإساءة استخدامها ويشمل ذلك قواعد المعلومات المكتبات تخريب الكتب تخريف المعلومات وتخريف السجلات الرسمية.

2. سرقة المعلومات ويشمل بيع المعلومات كالبحوث أو الدراسات الهامة أو ذات العلاقة بالتطوير التقني أو الصناعي أو العسكري أو تخريبها أو تدميرها. الخ.
3. تزوير المعلومات ويشمل الدخول للقواعد في النظام التعليمي وتغيير المعلومات وتحويلها، مثل تغيير علامات الطلاب.
4. تزيف المعلومات وتشمل تغيير في المعلومات على وضع غير حقيقي مثل وضع سجلات شهادات لم تصدر عن النظام التعليمي وإصدارها.
5. انتهاك الخصوصية ويشمل نشر معلومات ذات طبيعة خاصة عن الأفراد، أو الدخول لحسابات الأفراد الإلكترونية ونشر معلومات عنهم أو وضع معلومات تخص تاريخ الأفراد ونشرها.
6. التصنت وتشمل الدخول لقواعد المعلومات وسرقة المحادثات عبر الهاتف.
7. التجسس ويشمل اعتراض المعلومات ومحاولة معرفة ما يقوم به الأفراد.
8. التشهير ويشمل استخدام المعلومات الخاصة أو ذات الصلة بالانحراف أو الجريمة ونشرها بشكل يقصد منه اغتيال شخصية الأفراد أو الإساءة.
9. السرقة العلمية الكتب والبحوث العلمية الأكاديمية وخاصة ذات الطبيعة التجريبية والتطبيقية.
10. سرقة الاختراعات وخاصة في المجالات العلمية لاستخدامها أو بيعها.
11. الدخول غير القانوني للشبكات بقصد إساءة الاستخدام أو الحصول على منافع من خلال تخريب المعلومات أو التجسس أو سرقة المعلومات.
12. قرصنة البرمجيات ويشمل النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى.
13. قرصنة البيانات والمعلومات ويشمل اعتراض البيانات وخطفها بقصد الاستفادة منها وبخاصة أرقام البطاقة الائتمانية وأرقام الحسابات وكلمات الدخول وكلمات السر.
14. خلاعة الأطفال وتشمل نشر صور خاصة للأطفال "الجنس السياحي" للأطفال وللإناث خاصة على الشبكات بشكل عام ونشر الجنس التخليفي.
15. سرقة الأرقام والمتاجرة بها وخاصة أرقام الهواتف السرية واستخدامها في الاتصالات الدولية أو أرقام بطاقات الائتمان.
16. التحرش الجنسي ويقصد به المضايقة من الذكور للإناث أو العكس من خلال المراسلة أو المهاتفة، أو المحادثة.
17. القنابل البريدية وتشمل إرسال فيروسات لتدمير البيانات من خلال رسالة الكترونية.
18. إفشاء الأسرار وتشمل الحصول على معلومات خاصة جدا ونشرها على الشبكة.

19. الاحتيال المالي بالبطاقات وهذا ناتج عن استخدام غير شرعي لبطاقات التسوق أو البطاقات المالية أو البطاقات الهاتفية.

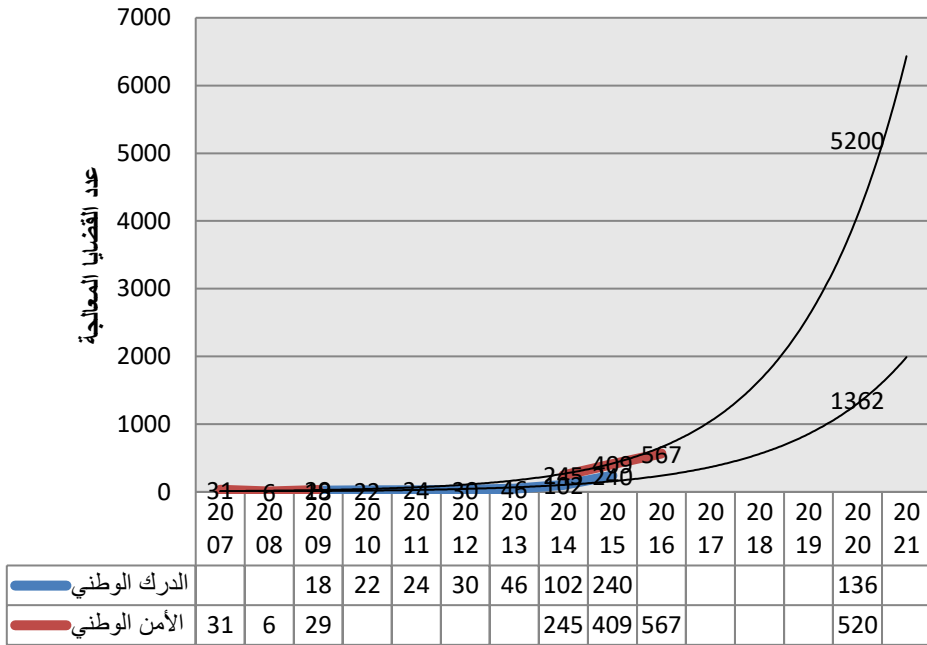
20. المطاردة والملاحقة والابتزاز وتشمل ملاحقة الذكور للإناث أو العكس والتتبع بقصد فرض إقامة علاقة ما وذلك من خلال استخدام البريد الإلكتروني وإرسال الرسائل.

21. الإرهاب الإلكتروني، يشمل جميع المكونات السالفة الذكر في بيئة تقنية متغيرة والتي تؤثر على فرص الإرهاب بمصادر هذه التغيرات تؤثر على تكتيكات الإرهاب وأسلحته وأهدافه ومن التكتيكات الإرهابية ما يعرف بالإرهاب الإلكتروني. (إسرائيل جبريل 2016) .

4.1 واقع الجريمة السيبرانية في الجزائر :

عرفت الجزائر بداية الجريمة السيبرانية قبل سنة 2008 بصورة محدودة نسبيا، حيث لم تتعد عمليات نسخ الأقراص بشكل غير قانوني وما إلى ذلك، فلم تكن تتطلب التدخل الأمني، لكن بعد اقتحام الجزائر عالم الأنترنت الفائق السرعة عبر خطوط ADSL والزيادة الطردية لعدد المشتركين سنة بعد سنة حتى وصل سنة 2021 إلى 26.35 مليون مشترك في مواقع التواصل حسب آخر تقرير لموقع "داتاريورتال - DATAREPORTAL"، حيث أدى هذا التحول الرقمي الهائل إلى حتمية مواجهة السلبيات المرافقة له، فمن خلال المخطط البياني التالي سنحاول استعراض تطور نسب الجرائم السيبرانية المسجلة بدلالة التسلسل الزمني:

شكل رقم 01: قضايا الجرائم السيبرانية المعالجة من قبل المصالح الأمنية خلال 15 سنة الماضية



المصادر: (حملاوي و المقدم عز الدين 2015)(باشوش 2021)

2. الأمن السيبراني :

1.2 تعريف الأمن السيبراني:

يعرف كل من MarttiLehto, PekkaNeittaanmäki الأمن السيبراني "على أنه مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها ويتضمن تنفيذ التدابير المضادة المطلوبة"، أما، وقد أيدته في الطرح واحد من أهم المختصين في الميدان: الأستاذ إدوارد أموروزو Edward Amoroso، الذي عرفه " بأنه تلك الوسائل التي من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة، إلخ."

أما التعريف الذي جاء به الاتحاد الدولي للاتصالات الصادر في تقريره حول " اتجاهات الإصلاح في الاتصالات للعام 2010-2011"، والذي يعتبر بمثابة أرضية إجماع لمختلف التوجهات الفكرية والمهنية "هو مجموعة من المهمات، مثل تجميع وسائل، وسياسات، واجراءات امنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلي، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين". من هذا المنطلق، يمكننا إعطاء تعريف شامل بالقول " أن الأمن السيبراني أو الالكتروني هو مجمل القوانين، الأدوات،

النصوص، المفاهيم والميكانيزمات الأمنية وطرق تسيير الأخطار والممارسات التقنية المتعلقة بتكنولوجيات المعلومات والاتصالات المستخدمة لحماية مصالح الدول والأشخاص ليبقى الهدف الأخير، هو قدرة هذه الأدوات على مقاومة التهديدات المتعمدة من طرف قراصنة المعلومات أو غير المعتمدة من طرف المستخدمين (الخطأ البشري) للتعافي، وبالتالي التحرر من الأضرار الناجمة عن تعطيل أو سوء استخدام تكنولوجيا المعلومات والاتصالات. (جمال 2019، 1265)

2.2 الأمن السيبراني في الجزائر :

لقد قدمت الجزائر الأمن السيبراني كأحد أولوياتها على غرار باقي دول العالم التي سارعت تحديث سياساتها الأمنية، واعتمادها آليات وميكانيزمات جديدة تعني بهذه المسائل، بالموازاة مع تطوير البنيات الأساسية المتعلقة بتكنولوجيات العالم الرقمي، ويفرض مطالب الأمن مضاعفة أنظمة الرقابة التي قد تشكل تهديدا ممكنا للحريات الفردية. لقد أصبح الأمن السيبراني ركن أساسي ضمن العقيدة الأمنية الجزائرية المعاصرة، والتي يجب على الدفاع الوطني من خلال أجهزتها المختلفة، ولا ننسى كذلك الجانب القانوني والمشرع الجزائري وكيف قام بمواجهة هذه الجرائم والاعتداءات الأمنية وتشير الإحصائيات المسجلة في الجزائر أن الجريمة الإلكترونية أخذت منحاً تصاعدياً في الآونة الأخيرة، ولهذا فإن السلطات الجزائرية ملزمة باتخاذ الاحتياطات الأمنية اللازمة لتفادي أي نوع من الجرائم السيبرانية. (إدريس 2019، 112).

3.2 تحديات الأمن السيبراني في الجزائر :

تواجه مصالح الدرك الوطني ومصالح الأمن الوطني العديد من العوائق والتحديات التي تعيقها في تحقيق الأمن الإلكتروني، يمكن أن نذكر أهمها فيما يلي:

- **زيادة عدد المشتركين في شبكة الإنترنت (أكثر من 10 ملايين مشترك بالجزائر):** ومع زيادة عدد مستخدمي الشبكة تزداد المخاطر، لتتحول عملية اكتشاف هوية مرتكبي الجرائم الإلكترونية إلى تحدي بسبب صعوبة البحث والتحري ضمن هذا العدد الهائل والمتجه نحو الارتفاع باستمرار.

- **التطور التكنولوجي وظهور الإنترنت اللاسلكي WIFI/3G/4G:** عبر هذه التقنيات لم يعد المجرم يحتاج للجلوس وراء الحواسيب الموصولة سلكياً بشبكة الإنترنت، للقيام بجريمته، مما يستدعي من الجهات الأمنية رفع التحدي، والاستعداد بأحدث التقنيات لمواجهة والتصدي لهذه التطورات.

- **الاستعمال الواسع لشبكات التواصل الاجتماعي:** إذ وصل عدد مستعملي هذه المواقع في الجزائر إلى أكثر من 7 ملايين مستعمل، وهو ما ساهم بشكل كبير في ارتفاع أنواع متعددة من الجرائم الإلكترونية، مثل: القذف، التحرش الجنسي، استغلال القصر، وغيرها وهذا ما يستوجب وضع استراتيجيات جد محكمة لضمان الأمن السيبراني عند استخدام مواقع التواصل الاجتماعي.

- انتشار تكنولوجيا الإنترنت فائقة السرعة والتدفق ADSL/ VSAT/SDSL: تسهم التكنولوجيا المتطورة في سرعة إنجاز الجريمة، وهذا يضع الجهات الأمنية المختصة أمام تحدي سرعة مباشرة التحقيقات ومتابعة الجناة، والتسلح بالأجهزة المتطورة والبرامج الحديثة السريعة الخدمة.

- عمليات التخفي أثناء استعمال خدمات شبكة الانترنت (Proxy): وهي من أكبر الإشكاليات التي تواجهها الجهات المختصة بالتحقيق، ويتطلب تعاون جهات متعددة، والتسلح بالوسائل المتطورة التي يمكن لها رصد الجزئيات وفك الشفرات، وتطوير البنى التحتية الخاصة بالمعلومات وتحديثها باستمرار، وتصميم برامج عالية التطور.

- غياب التنسيق بين الدول والحكومات: إذ من المعلوم أن الجريمة الإلكترونية عابرة للحدود والقارات، وهو ما يعني أن مرتكبيها يمكنهم النفاذ إلى أنظمة الحاسوب في أحد الدول، ليتم التلاعب واختراق البيانات في بلد آخر، تسجل النتائج في بلد عن أنه من الممكن تخزين أدلة الجريمة الإلكترونية في حاسوب موجود في بلد آخر، غير الذي ارتكبت فيه الجريمة، وكل هذا يساعد المجرم الإلكتروني في إخفاء هويته ونقل المواد من خلال قنوات موجودة في بلدان مختلفة، وبالتالي ونتيجة القدرة على التنقل إلكترونيا من شبكة إلى أخرى والنفاذ إلى قواعد البيانات في قارات مختلفة، تصبح عدة دول ومحاكم وقوانين وقواعد معنية بذلك، ما يشكل تحديا حقيقيا، ولذلك فإن الحاربة الفعالة للجريمة الإلكترونية تستدعي تعاوننا دوليا متزايدا، سريعا، وفعالا، وعلى أعلى درجات التنسيق.

- التطور التكنولوجي في مجال الانترنت والاتصالات: وهو ما يفرض على الأجهزة الأمنية المختصة بأن تساير هذا التطور، سواء من حيث اكتساب التكنولوجيا والتقنية أو من حيث التمكن من استخدامها واستثمارها بالشكل اللازم، وهذا قد يرهق ميزانيتها المحدودة، ولذلك يتوجب توفير جميع الامكانيات المادية، المالية والبشرية اللازمة للتحقيق الأمن السيبراني.

- نشر التوعية بمفهوم الأمن السيبراني لمستخدمي شبكة الإنترنت: وهو ما يستوجب القيام بحملات توعوية بين مستخدمي شبكة الانترنت لاتخاذ التدابير اللازمة لضمان الحد الأدنى من الأمان، وتعليمهم آليات التشفير، والاحتياطات الواجب توفيرها عند استخدام مواقع التواصل الاجتماعي، كما يجب توعيتهم بضرورة التحلي بثقافة التبليغ في الوقت اللازم لتتمكن الجهات المعنية من القيام بدورها في الوقت المناسب، والتوصل إلى مرتكبي الجرائم.

- تفعيل القوانين على أرض الواقع وتطبيقها بصرامة: إذ من بين أكبر الإشكالات التي تسهم في انتشار الجريمة الإلكترونية، هو الإفلات من العقاب، والتأخر في تفعيل القوانين، وهو يمنح المجرم فرصا لتكرار جرائمه، ولذلك من الضروري تأكيد على تطبيق القوانين، كما يجب أن تتكيف النصوص القانونية مع التغيرات الحاصلة في هذا المجال، كما يتوجب إنشاء محاكم متخصصة بالجرائم الإلكترونية، نظرا للانتشار الواسع لهذه الجرائم. (سمير 2017، 275)

3. المؤسسات الأمنية المسخرة للتصدي للجرائم السيبرانية :

إن المحيط الكمي لإجرام المعلوماتي في الجزائر غير واضح لعدم وجود دراسات وبحوث من شأنها كشف اللثام عن أرقام ومؤشرات للخسائر في بلادنا جراء هذا النمط الاجرامي. وإن كانت الجزائر ليست بمنادى عن خطورة الجرائم المعلوماتية طالما أنها تحتل جزءا من الفضاء الإلكتروني خاصة فيما يتعلق بالحاسوب المالية وبعض الهيئات الحكومية التي يعتبر اختراق مواقعها ضمن حجم الأضرار الناتجة عن الجريمة المعلوماتية.

1.3 مركز الوقاية من جرائم الإعلام الآلي للدرك الوطني: CPLCIC

تم إنشاؤه سنة 2008 ويعد الجهاز الوحيد المختص بهذا الصدد في الجزائر، ويهدف إلى تأمين المنظومة المعلوماتية للأمن العمومي، واعتبر بمثابة مركز توثيق ومقره يوجد ببئر مراد راييس، وهذا المركز يعكف على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها سواء كانوا أشخاص فرادي أو عصابات، وهذا كله من أجل تأمين الأنظمة المعلوماتية والحفاظ عليها، لاسيما تلك المستعملة في المؤسسات الرسمية والبنوك. (خيرة 2010، 78)

ويقوم هذا المركز بمساعدة الأجهزة الأمنية الأخرى بالتعاون من أجل مكافحة الجرائم المعلوماتية، حيث يعنى المركز بتطوير أساليب التعامل مع هذه الجرائم ووضع قوانين لتنظيم مجال استغلال المعلومة من خلال تنسيق مع وزارة العدل وكذا من خلال معهد خاص بعلم الإجرام لتطوير مستوى التعامل مع الجريمة بصفة عامة والجريمة المعلوماتية بصفة خاصة، فالجزائر تعمل جاهدة للاستفادة من خبرات البلدان الأخرى في تأمين المنظومة المعلوماتية وحمايتها من الجرائم ضمن مجموعة من العناصر أهمها: (هند 2008، 41)

الوقاية: وتشمل حملة تحسيسية وتوعية بالتنسيق مع وزارة التضامن الوطني والأسرة، والعمل على ملتقيات ومحاضرات وأياما دراسية ومنتديات دولية، ومشاركة في منتديات صحفية وحصص تلفزيونية وإذاعية وغيرها من وسائل النشر والإشهار.

المكافحة: توعية الجزائريين من خلال استعمالهم لشبكات التواصل واستخدام الأنترنت وذلك من خلال تعليقاتهم المدافعة عن الجزائر ومعرفة الأخطار بسلوكيات مشبوهة أو اعتداءات عبر نشر فيديوهات توصل إلى الجناة، مما يسهل التحقيق لدى مصالح الدرك وإلقاء القبض على المشبوهين ومرتكبي الجرائم في الوقت المناسب.

2.3 المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني: INCC

مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة لوزير الدفاع الوطني مكلفة بمهام متعددة كإجراء الخبرات والفحوص في إطار التحريات الأولية والتحقيقات القضائية، ضمان المساعدة العلمية أثناء القيام بالتحريات المعقدة. يعتبر المعهد أحد المشاريع المنجزة في إطار تطوير سلك الدرك الوطني «ببوشاوي»، حيث تم إنشاءه بموجب مرسوم رئاسي 04/133 المؤرخ في 26 جوان 2004، ودخل حيز الخدمة ابتداء من الفاتح جانفي 2009، أما الفترة الممتدة بين 2004 و2009 كرسست لتكوين المورد البشري واقتناء المعدات العلمية والتقنية الضرورية، ويقوم المعهد

بالعديد من المهام التي من شأنها تلبية الطلبات الواردة من السلطة القضائية، ضباط الشرطة القضائية والسلطات المؤهلة، قانونيا خاصة اثناء معالجة القضايا المعقدة، وكذا تنظيم دورات الإتقان والتكوين ما بعد التدرج في تخصص العلوم الجنائية، ولتأدية مهامه على أكمل وجه فإن المعهد الوطني للأدلة الجنائية وعلم الإجرام يحتوي على العديد من الأقسام والمصالح المختصة من أهمها: مصلحة البصمات؛ مصلحة البيئة؛ أما فيما يخص مجال الأمن السيبراني هناك مصلحة الإعلام الآلي؛ على مستوى هذه المصلحة يتم رصد ومراقبة وتتبع عمليات الاختراق والقرصنة المعلوماتية وكذا اكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية. (عادل، 2014، 64)

3.3 المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني: SCLC

استجابة لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الإلكترونية قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الإلكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية، والتي كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة الإلكترونية وعلى مستوى المديرية العامة للأمن الوطني والتي انشئت 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. (إدريس، 2019، 114).

4.3 الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:

تشكلت هذه الهيئة بمقتضى المرسوم الرئاسي رقم 15-261 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. وكلفت الهيئة باقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها 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 الإلكترونية، قصد الكشف عن جرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة.

وقد نص سابقا على إنشاء هذه الهيئة المادة 13 من القانون 04/09 المؤرخ في أوت المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها من خلال النص: «تنشأ هيئة وطنية وتنظيمها وكيفيات سيرها عن طريق التنظيم» أما مهامها فقد أوردت المادة 14 من نفس القانون وتتمثل في: (أسماء، ياسين و عصام، 2013، 4).

1.4.3 الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: إن إجراءات الوقاية تكون بتوعية مستعملي

تكنولوجيات الإعلام والاتصال بخطورة الجرائم التي يمكن ان يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه

التكنولوجيات، ومن أهم هذه الجرائم: التجسس على الاتصالات والرسائل الإلكترونية، التلاعب بحسابات العملاء، اختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية.. الخ

2.4.3 مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال: بحسب نص المادة 14 من القانون 04/09 هناك نوعان من المكافحة تقوم بهما هذه الهيئة :

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيا الاعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية المادة 14 فقرة (ب) من القانون 04/09.

- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، يقترح المشروع في هذا الفصل إنشاء هيئة وطنية مختصة تتولى مهام أهمها : تنسيق وتنسيق عملية الوقاية من الجرائم المعلوماتية ومساعدة السلطات القضائية ومصالح الشرطة القضائية من التحريات التي تجريها بشأن هذه الجرائم، وما تقوم به أيضا من تجميع المعلومات من نظيرتها في الخارج قصد محاربة هذا النوع الخطير من الإجرام.

5.3 مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة :

بالنظر لحساسية قطاع الدفاع الوطني: أستحدث بتاريخ 06 نوفمبر 2015، على مستوى دائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي " مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة"، وأوكلت لها مهمة، حماية المنظومات والمنشآت الحيوية للبلاد ضد كل أنواع الجريمة السيبرانية، ومن بين المحاور التي تناولتها الارضية العملياتية لهذه المصلحة، تذكر ما يلي:(جمال 2019، 1289).

- توجيه، تنفيذ وتأطير الاعمال في هذا المجال لا يجب أن يتعدى الإطار الوظيفي أو التنظيمي.

- تطوير وتعزيز المنظومة القانونية لتفادي التجاوزات أثناء استخدام التكنولوجيا وضمان حماية منظومات الاعلام.

- اعتماد التكوين التقني والعلمي لإنتاج الكفاءات والمهارات القادرة على خلق نظام الدفاع السيبراني في كافة أنشطة المؤسسة العسكرية وبالتالي تفادي الاخطار الاجرامية.

- غرس ثقافة الاستعمال الكيفي لهذا العنصر الحيوي " تكنولوجيا الاعلام والاتصال "من خلال حملات تحسيسية لكافة مستخدمي المؤسسة بغض النظر عن الرتبة أو الوظيفة.

- الاعتماد وبطريقة مستمرة على البحث العلمي لتطوير وسائل الدفاع استجابة للتطورات الحاصلة في مجال التكنولوجيا.

-فتح مجال التعاون الدولي مع المؤسسات العسكرية الاجنبية، خاصة تلك التي لها رصيد في المجال لتبادل الخبرات والاستفادة من تجاربهم في هذا المجال.

كما أصدرت العديد من الوزارات على غرار وزارة البريد والاتصال، المالية، التعليم العالي، الداخلية، تعليمات وتوجيهات إلى مصالحها التنفيذية تتضمن الآليات والكيفيات الواجب تطبيقها من الناحية العملية لتفادي الوقوع في الاخطاء، نلخصها فيما يلي :

-عدم السماح لأي كان من الحصول على معلومات من الأنظمة المعلوماتية الموصولة بشبكة الأنترنت، ما لم يكن هناك إذن أو موافقة من المصلحة المؤهلة قانونا، كما لا يمكن استخدام الحسابات الخاصة للأفراد أو تداول أرقامهم السرية.

-احترام المقاييس المعمول بها في تداول المعلومات المشفرة "إرسالا واستقبالا"، سواء تعلق الامر بالأنظمة المعلوماتية الداخلية للشبكات الوطنية أو الدولية.

-احترام القواعد العلمية والمهنية المعمول بها عالميا في توظيف تكنولوجيا الاعلام سواء لأغراض شخصية أو مهنية حتى لا تعرض الأنظمة للقرصنة، لأن الاستخدام المفرط بقدر ما يخلق ثغرات، فإنه يساهم كذلك في حرمان الآخرين من الاستفادة من خدمات التكنولوجيا.

ما يلاحظ في هذا الباب، أن المجهودات التي تبذلها الجزائر للإلمام بأهم العناصر الكفيلة بتحقيق الأمن السيبراني، ما زالت بعيدة، لأن الاجراءات الادارية المتخذة لحد الآن من طرف الهيئات المذكورة أعلاه للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها تبقى غير كافية وتتطلب المزيد والاستمرارية في الموقف والنهج.

6.3.القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

المادة 211 مكرر 22 ينشأ على مستوى محكمة مقر مجلس قضاء الجزائر، قطب جزائي وطني متخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها كما يختص بالحكم في الجرائم المنصوص عليها في هذا الباب إذا كانت تشكل جنحا.

يقصد بمفهوم هذا القانون، بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، أي جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أي وسيلة أخرى أو آليه ذات صلة بتكنولوجيات الإعلام والاتصال.

"المادة 211 مكرر 23 يمارس وكيل الجمهورية لدى القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكذا قاضي التحقيق ورئيس القطب صلاحياتهم في كامل الإقليم الوطني."

"المادة 211 مكرر 24 مع مراعاة أحكام الفقرة 2 من المادة 211 مكرر 22 أعلاه، يختص وكيل الجمهورية لدى القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و قاضي التحقيق ورئيس ذات

الآليات المسخرة لمواجهة تحديات الأمن السيبراني في الجزائر

القطب حصريا بالمتابعة والتدقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المذكورة أدناه وكذا الجرائم المرتبطة بها:

- الجرائم التي تمس بأس الدولة أو بالدفاع الوطني.
- جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع.
- جرائم نشر وترويج أنباء مغرضه تمس النظام 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 " (الجريدة الرسمية للجمهورية الجزائرية 2021، 8-9)

خاتمة:

تبذل الجزائر جهود هامة في إطار تعزيز منظومة الأمن السيبراني، وذلك من خلال مواكبة التطورات الرقمية المتسارعة، حيث تساهم عبر الاتفاقيات الدولية والإقليمية في ربط وتنسيق الإستراتيجيات الدولية وكذا الوطنية، بقصد إحتواء المد السيبراني في إطار دولي وكذا محلي، حيث تعمل الجزائر على تحديث واستحداث فروع ومؤسسات خاصة بالأمن السيبراني تحت سلطة مصالح الأمن ووزارة الدفاع وكذا المؤسسة القضائية.

رغم كل هاته الجهود إلا أن الجرائم السيبرانية تتميز بكونها عابرة للحدود وسرعة تطورها وتشعبها في مختلف المعاملات والفضاءات الرقمية، الأمر الذي يجعل من الدول في وضع دفاعي ويرفع من تحديات الأمن السيبراني.

قائمة المراجع:

1. معاشي سميرة. (أفريل، 2010). ماهية الجريمة الإلكترونية. مجلة المنتدى القانوني، 07، الصفحات 275-285.
2. السالك فريد كامل. (2000). الجريمة الإلكترونية. ندوة التنمية و مجتمع المعلوماتية (الصفحات 1-9). سوريا: مؤتمر الجمعية السورية للمعلوماتية في حلب.
3. رشاد مرعي إسرائيل جبريل. (9 أوت، 2016). الجرائم الإلكترونية ” الأهداف - الأسباب - طرق الجريمة ومعالجتها”. تم الاسترداد من المركز الديمقراطي العربي <https://democraticac.de/?p=35426> :
4. Brown, C. (2015, January-June 1). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. International Journal of Cyber Criminology, 9(1),p 55-119. doi:10.5281

5. القانون رقم 04-09. (المؤرخ في 05 أوت 2009). والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجزائر: الجريدة الرسمية رقم 47.
6. يوسف صغير. (2013). الجريمة المرتكبة عبر الانترنت، رسالة ماجستير في القانون. تيزي وزو: كلية الحقوق و العلوم السياسية، جامعة مولود معمري.