

البعد الاستراتيجي لتحقيق الجزائر لأمنها السيبراني The strategic dimension of Algeria's cybersecurity

بحاش وفاء أستاذ محاضر أ

جامعة محمد بوضياف المسيلة -الجزائر

Wafa.bahache@univ-msila.dz

تاريخ النشر: 2026/06/10	تاريخ القبول: 2026/02/08	تاريخ الارسال: 2025/08/31
-------------------------	--------------------------	---------------------------

ملخص :

في ظل التطور التكنولوجي والرقمي الذي شهده العالم برز مفهوم الامن السيبراني والذي اضحى أمرا ضروريا للأفراد والمؤسسات والشركات لحماية وتأمين أنظمتها المعلوماتية وبياناتها من أي اختراق.

باعتباره مجموعة من الممارسات والتقنيات التي تهدف إلى حماية الأنظمة والشبكات والبيانات من الهجمات الرقمية، هذه الهجمات والتي تعد بمثابة جرائم عابرة للحدود تستهدف الوصول للمعلومات والبيانات الحساسة بغية التلاعب بها وتغييرها او اتلافها والحاق الضرر بأصحابها .

وفي هذا الاطار توجهت الجزائر لانتهاج استراتيجية أمنية وطنية للدفاع عن منظومتها المعلوماتية من أي اختراق أو أي خطر قد يطل امن بياناتها الحساسة، تجسدت في منظومتها التشريعية والمؤسسية التي أخذت على عاتقها توفير الوقاية ومكافحة الجرائم السيبرانية .
الكلمات المفتاحية : الامن السيبراني ، الجرائم الالكترونية ، تكنولوجيا المعلومات، البعد الاستراتيجي.

(*) بحاش وفاء

Abstract :

In light of the technological and digital development witnessed by the world, the concept of cybersecurity has emerged, becoming essential for individuals, institutions, and companies to protect and secure their information systems and data from any breach.

It is considered a set of practices and techniques aimed at protecting systems, networks, and data from digital attacks. These attacks, which constitute cross-border crimes, target access to sensitive information and

data with the aim of manipulating, changing, or destroying it, harming its owners.

In this context, Algeria has adopted a national security strategy to defend its information systems from any breach or any threat that may affect the security of its sensitive data. This strategy is embodied in its legislative and institutional system, which has taken it upon itself to provide prevention and combat cybercrime.

Keywords: cybersecurity, electronic crimes, information technology, strategic dimension.

مقدمة:

شهدت دول العالم مؤخرا تطورا متسارعا في مجال تكنولوجيا الاعلام والاتصال ، مما جعلها تواجه تهديدات تتعلق بالحفاظ على امنها السيبراني من مختلف الهجمات وحماية منظومتها المعلوماتية من أي اختراق أو تلاعب أو اتلاف قد يطل معطياتها وبياناتها.

والجزائر ليست بمعزل عن هذه الدول التي تسعى للحفاظ على امنها السيبراني خاصة في ظل الانتشار الواسع لتكنولوجيا الانترنت فائقة السرعة والتدفق وارتفاع عدد مستخدمي شبكة الانترنت ، مما يصعب عملية الكشف عن مرتكبي الجرائم الالكترونية وملاحقتهم .

لذا نجد ان الجزائر قد سطرت استراتيجية للدفاع عن امنها السيبراني وحماية مؤسساتها وشركاتها من أي هجمات الكترونية قد تطل منظومتها المعلوماتية في الفضاء السيبراني .

اذ وضعت حماية وتأمين البنى التحتية للمعلومات الوطنية الحساسة ولاسيما المعلومات الشخصية في أولوية برنامجها من خلال مجموعة من الآليات والضوابط تمثلت في ترسانة من القوانين سنها المشرع الجزائري ترمي لمعاقبة الجناة ، هذا من الناحية التشريعية ، أما من الناحية العملية (المؤسسية) فقد طورت الجزائر هيئات مختصة تأخذ على عاتقها الوقاية ومكافحة الجريمة السيبرانية بإجراء الخبراء والفحوص العلمية في اطار التحري والتحقيق وجمع المعلومات وتبادلها مع المصالح المختصة بقصد التعرف على المجرمين.

وبناء على ماتقدم نطرح الإشكالية التالية :

هل تمكنت الجزائر من تحقيق امنها السيبراني في ظل التحديات التي تفرضها تكنولوجيا الاعلام والاتصال؟

ويتفرع عن هذا التساؤل المحوري مجموعة من التساؤلات الفرعية :

- هل تملك الجزائر استراتيجية لتحقيق أمنها السيبراني؟
 - هل ساهمت التدابير الوقائية والاجرائية التي اقترتها السلطات الجزائرية من خلال التعديلات القانونية المتلاحقة من التصدي للجرائم السيبرانية؟
- وستتم الإجابة عن هذه التساؤلات من خلال الفرضيات التالية:
- تبنت الجزائر مجموعة من التدابير الوقائية والاجرائية في مواجهتها التحديات التي فرضتها عليها تكنولوجيات الاعلام والاتصال في سبيل تحقي أمنها السيبراني.
 - لقد ساهمت التعديلات القانونية المتلاحقة التي اقترتها السلطات الجزائرية في التصدي للجرائم السيبرانية بنسبة كبيرة.

وسيتم معالجة الموضوع بالتطرق للنقاط التالية :

المحور الأول: الاطار المفاهيمي للأمن السيبراني

أولاً: مفهوم الامن السيبراني

ثانياً: عناصر وأهداف الأمن السيبراني

ثالثاً: أنواع الامن السيبراني

رابعاً: أنواع الهجمات السيبرانية

المحور الثاني: استراتيجية الجزائر للدفاع عن أمنها في مواجهة الجرائم السيبرانية

أولاً: الجريمة السيبرانية

ثانياً: آليات مواجهة الجرائم السيبرانية

ثالثاً: محاور الاستراتيجية الجزائرية لتحقيق أمنها السيبراني

رابعاً: معوقات تحقيق الامن السيبراني في الجزائر

وقد تم الاعتماد على المنهج الوصفي التحليلي والذي يهدف لوصف الظاهرة المدروسة ألا وهي الأمن السيبراني ، بالتطرق لمفهومه وبيان عناصره وأهدافه وأنواعه ، كما تم التطرق لمفهوم الجريمة السيبرانية ، اما الجزء المتعلق بالتحليل فيمكن في تحليل الاستراتيجية الأمنية التي اعتمتها الجزائر في سبيل الدفاع عن أمنها السيبراني، ويظهر ذلك جليا في الجانب التشريعي ، بتحليل القوانين والتعديلات المختلفة التي طالت قانون العقوبات والإجراءات الجزائية في مواجهة الجرائم الالكترونية المستحدثة .

المحور الأول: الإطار المفاهيمي للأمن السيبراني

سنحاول من خلال هذا المحور التطرق لكل مايتعلق بالأمن السيبراني من مفهوم وأهداف وأنواع.

أولا : مفهوم الامن السيبراني

وردت العديد من المفاهيم التي تناولت الأمن السيبراني ، وسنحاول فيما يلي التطرق لبعضها من أجل الالمام بمفهومه بشكل واضح ، وقبل ذلك يجب التطرق لمفهوم الفضاء السيبراني باعتبار المجال الذي يتيح استخدام نظم وتكنولوجيات الاعلام والاتصال.

✓ تعريف الفضاء السيبراني:

يعتبر الفضاء السيبراني مجال افتراضي تتواجد فيه أجهزة الكمبيوتر ، الشبكات ، ومختلف البرمجيات وكم هائل من المعلومات والبيانات والمعطيات ، وهو من صنع الانسان.

كما يمكن تعريفه على أنه : " بيئة تفاعلية وفضاء للتواصل البيئي يشتمل على عناصر مادية وغير مادية ، تتكون من الأجهزة الرقمية (الحواسيب) ، أنظمة الشبكات والبرمجيات ، مستخدموا كل هذه العناصر " ¹.

وبناء على ذلك فإن الفضاء السيبراني يتشكل من أربع جوانب أساسية تتمثل في:

- مساحة تشغيلية: **Anoperational space** : فالفضاء الالكتروني هو مساحة يستخدمها الأفراد والمنظمات على حد سواء للعمل وإحداث التأثيرات.

- مجال طبيعي **A natural domain** : فالفضاء الالكتروني وفق ذلك يتكون من نشاط كهرومغناطيسي يتم إدخاله باستخدام التكنولوجيا الالكترونية.

- يستند للمعلومات **Information based**: حيث يعتبر مجالا لإنشاء المعلومات وتخزينها واستغلالها وتبادلها.

- مجموعة شبكات مترابطة **inter connected net work** : إذ يتركز على وجود اتصالات تسمح للنشاط الكهرومغناطيسي بنقل المعلومات ².

✓ تعريف الأمن السيبراني:

يعتبر الأمن السيبراني : " النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن بذلك الحد من الخسائر والاضرار في حال تحقق المخاطر والتهديدات ، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن. بحيث لا تتوقف عجلة الإنتاج وبالتالي لا تتحول الأضرار إلى خسائر دائمة"³

كما يعرف بأنه : " ينطوي على حماية شبكات الكمبيوتر والمعلومات التي تحتويها من الاختراق ومن الضرر الخبيث أو التعطيل".

فهو يهدف للحد من الهجمات الالكترونية الخبيثة على برمجيات وأجهزة الكمبيوتر والشبكات، وهذا من خلال مجموعة من الأدوات والوسائل والتقنيات التي تساعد على الكشف على المتسللين ووقف الفيروسات ومنع وصولها وفرض نظم التوثيق وتمكين الاتصالات المشفرة."⁴

كما نجد ريتشارد كمور Richard kemmere (أستاذ الاتصالات في جامعة كاليفورنيا) عرفه : "بأنه مجموعة وسائل دفاعية من شأنها كشف و إحباط المحاولات التي يقوم بها القرصنة".

أما Edward Amoroso أموروز فعرفه 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...الخ"⁵.

ويعرفه التقرير الصادر عن الاتحاد الدولي للاتصالات بأنه : " مجموعة من الأدوات والسياسات ومفاهيم وضوابط الأمن والمبادئ التوجيهية لإدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وآليات الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة المعلوماتية وأصول المؤسسات والمستعملين."⁶

وتأسيسا على ما تقدم يمكن الاجماع على تعريف شامل للأمن السيبراني كونه يعمل على توفير الحماية السيبرانية بغرض ضمان استمرارية نظم المعلومات باتخاذ التدابير اللازمة والمناسبة لتوفير الحماية للأفراد والدول من المخاطر والهجمات الموجهة التي تتم عبر الفضاء السيبراني بواسطة البرمجيات الخبيثة (Malwar) والتي تشمل الفيروسات وأحصنة طروادة وبرامج التجسس وتعطيل الأنظمة أو سرقة البيانات.

ثانيا: عناصر وأهداف الامن السيبراني

مع تزايد التهديدات والمخاطر السيبرانية المتصاعدة والتي فرضها التحول الرقمي في ظل تسارع وتيرة التطور الحاصل في تكنولوجيا المعلومات ، بات من الضروري على الدول والافراد ومختلف المنظمات التعامل مع هذه التهديدات بدمج تدابير الامن السيبراني ضمن منظومتها الأمنية .

✓ ومن بين العناصر الأساسية للأمن السيبراني:

التوافر: ونقصد به الحفاظ على المعلومات وضمان بقائها وكذا توفر إمكانية الوصول اليها واستخدامها في أي وقت.⁷

الصحة والسلامة : ويتمثل في توفير الحماية للمعلومات والحفاظ على سلامتها من أي تخريب وإتلاف أو تغيير أو تلاعب أثناء تخزينها ونقلها ، ويتم توفير السلامة للمعلومات بعدة آليات : المراقبة الصارمة على النفاذ ، حمايتها من الفيروسات وتشفير البيانات وأي برامج خبيثة .

السرية : والمقصود به المحافظة على سرية المعلومات وتدفقها وكتمان الخدمات والإجراءات التي تتم في الفضاء السيبراني.⁸

✓ أهداف الامن السيبراني:

1- يهدف الأمن السيبراني إلى حماية البيانات الرقمية للمواطنين وتأمين البنية التحتية لأمن المعلومات من أي هجمات خبيثة يمكن أن تتعرض لها.

2- حماية الشبكات وأجهزة الكمبيوتر من الاختراق أو التعطيل أو الاستخدام غير المصرح به والدفاع عنها باستخدام الآليات والتقنيات التكنولوجية المخصصة لذلك.

3- ضمان استمرارية الأعمال لأن الهجمات الالكترونية تشكل خطرا كبيرا على الأنظمة الالكترونية التي تعتمد عليها المؤسسات والشركات في إدارة عملياتها ، حيث قد تؤدي لتعطيل الخدمات وفقدان البيانات وإتلافها مما يكبدها خسائر مالية كبيرة.

4- كما أن الهجمات الالكترونية قد تلحق الضرر بسمعة الأفراد والشركات ويساهم الأمن السيبراني على حماية السمعة من خلال بناء الثقة مع العملاء والشركات بممارساته.

5- الامتثال للقوانين المختلفة واللوائح التي تلزم العديد من الشركات على حماية بيانات عملائها، ويساعد الامن السيبراني على ضمان امتثال هذه الشركات للوائح والقوانين تجنباً للعقوبات المالية والمسائلة القانونية التي قد تلحق بها في حال تعرض بيانات عملائها لأي إتلاف أو اختراق.⁹

6- يمكن أن تساعد إجراءات الامن السيبراني الاستباقية في تمكين المؤسسات من الكشف المبكر عن التهديدات والاستجابة والتعامل معها بكفاءة وفعالية ، وتفادي الاضرار والتعطيلات المحتملة وبالتالي الحفاظ على منظومتها المعلوماتية من أي اختراق أو تغيير أو اتلاف.¹⁰

ثالثاً: أنواع الأمن السيبراني

1- أمن الشبكة: وهو من أهم عناصر الأمن السيبراني وأبرزها لأن أغلب الهجمات تحدث عبر الشبكات ، وهو عبارة عن عملية تتضمن مجموعة من تقنيات البرامج والأجهزة من اجل حماية البيانات الرقمية من التهديدات المحتملة.

ومن أنواعه: برامج مكافحة الفيروسات – البرامج الضارة- أمن التطبيقات – أمن البريد الالكتروني- منع فقدان البيانات – جدار الحماية.

2- أمن المعلومات: وهو عبارة عن عملية تتضمن تصميم ونشر أدوات لحماية المعلومات الهامة من الاختراق والتدمير والاتلاف والتعطيل.

ومن أنواعها: الأمن السحابي- أمن البنية التحتية- التشفير – الاستجابة للحوادث- إدارة الضعف- النسخ الاحتياطي للبيانات والتحكم والوصول إليها.

3- أمن المستخدم النهائي : ويتمثل أمن المستخدم النهائي في تأمين الأجهزة الفردية (أجهزة الكمبيوتر، الهواتف الذكية، أجهزة الكمبيوتر المحمولة) بالاعتماد على برامج مكافحة الفيروسات وأنظمة التسلل (IPS) وتشفير الجهاز وتحديثات البرامج بشكل منتظم.

4- أمن البنية التحتية: هو إجراء أمني يتخذ لحماية البيئة التحتية الحيوية مثل اتصالات الشبكة – مركز البيانات أو الخادم (مركز تكنولوجيا المعلومات) ضد أي تخريب، باستخدام العديد من التقنيات كالتحكم في الوصول المادي أنظمة الكشف عن المتسللين – أنظمة الإنذار المبكر.

5- أمن السحابة: وهذه الاستراتيجية تتضمن حلول الأمن السيبراني والضوابط والسياسات والخدمات التي تساعد على حماية نشر السحابة بالكامل للمؤسسة ضد الهجمات الإلكترونية.

6- امن الهاتف المحمول: ويتضمن تأمين مختلف البيانات التنظيمية والشخصية المخزنة على الأجهزة المحمولة والأجهزة اللوحية ضد التهديدات المحتملة والتي تتجسد في فقدان الأجهزة أو سرقتها. الوصول غير المصرح به للمعلومات والبيانات ومختلف البرامج الضارة من خلال برامج مكافحة الفيروسات وتطبيقات الأمان وكلمات المرور القوية .

7- أمن انترنت الأشياء Lots: وتتجسد مهمته الأساسية في حماية مختلف الأجهزة المتصلة بالانترنت والمعرضة للتهديدات الإلكترونية باكتشاف وتضييق الأجهزة المتصلة والتجزئة التلقائية للتحكم في أنشطة الشبكة - التحديثات الأمنية - التحكم في الوصول أو الايقاف- التشفير.

8- أمن التطبيقات: حيث يركز على حماية التطبيقات من الثغرات الأمنية والهجمات الإلكترونية باستخدام العديد من التقنيات، كمنع هجمات الروبوت ومنع أي تفاعل ضار معها ، من خلال ممارسات الترميز أو التشفير الأمانة وتحديثات برنامجية منتمة وتحليل الثغرات الأمنية.¹¹

بالإضافة الى هذه الأنواع هناك أنواع أخرى يمكن الإشارة إليها:¹²

الأمن الإلكتروني: ويتركز على حماية الأنظمة والشبكات من الهجمات الإلكترونية التي تشنها الدول أو الجماعات الممولة من الدول.

الأمن القانوني: ويتركز على ضمان امتثال المنظمات للقوانين واللوائح المتعلقة بالأمن السيبراني.

الأمن المادي: ويرتكز على حماية الأجهزة والبرامج والبنى التحتية المادية من التهديدات المادية والتي تعرض المنظمة لخسائر مالية جمة مما يتسبب في فقدان سمعتها وثقة عملائها بها وفقدان حصتها السوقية أو انخفاضها .

رابعاً: أنواع الهجمات السيبرانية

تتنوع الهجمات السيبرانية بتنوع واختلاف التقنيات الحديثة وقدرات المخترقين الذين يحاولون دائماً إيجاد طرق وأساليب جديدة ومبتكرة لتحقيق أهدافهم والمتمثلة في سرقة البيانات، تلفيق المعلومات، تعطيل الأنظمة الرقمية للأفراد والمنظمات.

ومن أبرز التقنيات المستخدمة في الهجمات السيبرانية:

1- هجمات التصيد الاحتيالي (Phishing Attacks): وهذا النوع أصبح منتشرًا مؤخراً بشكل ملحوظ وهو نوع من هجمات الهندسة الاجتماعية يستخدمه غالباً المجرم الإلكتروني بسرقة بيانات المستخدم (بيانات الائتمان) وهذا بعد تنكره في هيئة بيانات موثوق به فيصل للضحية بريد الكتروني أو رسالة نصية تحفزه على النقر عليها وفي هذه الحالة يتم تثبيت برامج ضارة على جهاز الضحية كجزء من هجوم برامج الفدية أو الكشف عن معلومات سرية أو حساسة خاصة بالمستلم.

ويشمل هذا الهجوم على سرقة أموال أو هوية الضحية بالنسبة للأفراد أو الوصول لبيانات المنظمة الحساسة والمحمية بالنسبة للمنظمات من خلال الحصول على موطن قدم في شبكات المنظمة أو الشبكات الحكومية كجزء هام من أجل تجاوز الحدود الأمنية الخاصة بالمنظمة باختراق الموظفين وتوزيع برامج ضارة، وهذا النوع من الهجمات يكبد المنظمات خسائر كبيرة.¹³

2- هجمات التصيد الاحتيالي بالرمح Spear phishing

وتتمثل في عملية احتيال عبر البريد الإلكتروني أو الاتصالات الإلكترونية والتي قد تبدو للضحية (منظمة أو فرداً) أنها مصدر موثوق تعود لموقع ويب مزيف ملئ بالبرامج الضارة.

3- هجمات تصيد الحيتان whale phishing

هدفه الوصول لمعلومات حساسة وسرية لشخصيات نافذة وبارزة في المجتمع ومن هنا يتم جاء وصفه بتصيد الحيتان، حيث يعتمد على انتحال شخصية عنصر معين في شركة أو مؤسسة من قبل مجرمي الأنترنت بغية سرقة معلومات سرية أو اقناع الضحية بإرسال أموال أو هدايا للمنتحل.

4- هجمات drive -By : يتسبب فيه برنامج نصي ضار يقوم بتنزيل وتثبيت نفسه على جهاز الضحية دون إذن مسبق منه والهدف منه سرقة المعلومات أو اتلاف البيانات.¹⁴

5- برامج الفدية ransom ware وهي من أكثر الهجمات السيبرانية خطورة وخبثا لكونها تستخدم بغرض الابتزاز والحصول على الأموال من خلال تقييد الوصول لأنظمة الحاسوب وبياناته، وفي حال فشل الضحية في دفع الفدية فإن المتسلل سيحذف جميع المعلومات الهامة على حاسوب الضحية أو يقوم بنشر ملفاته السرية التي تشكل خطورة عليه¹⁵.

6- الهجوم بكلمة المرور: حيث يحاول المهاجمة من خلال اختراق حسابات مختلفة للضحايا والوصول لملفاتهم الشخصية باختراق كلمات المرور الخاصة بهم.

7- هجمات التنصت EAVE SDROPPING

وهو معروف باسم هجوم sniffing أو التطفل snooping وهو نوع من سرقة المعلومات عبر شبكة عن طريق هاتف ذكي أو جهاز كومبيوتر أو أي جهاز آخر متصل. ويمكن تجنب ومنع هذا النوع من الهجمات من خلال: استخدام جدار حماية شخصي- تحديث برامج مكافحة الفيروسات – استخدام شبكة افتراضية خاصة (VPN) – تجنب شبكة WIFI العامة- استخدام كلمات مرور قوية.

8- هجمات البرامج الضارة mal ware attaks

ويتم هذا النوع من الهجمات بتصميم برامج ضارة موجهة لإحداث ضرر أو تلف للجهاز أو الخادم أو العميل أو الشبكة دون معرفة المستخدم النهائي بسرقة المعلومات الشخصية أو المالية أو التجارية.

9- حصان طروادة trojan hores

وهذا النوع من البرامج الضارة عادة ما يتم إخفاؤه كمرفق في رسالة بريد الكتروني أو ملف مجاني للتنزيل ثم ينتقل مباشرة لجهاز المستخدم بمجرد التنزيل، حيث يستنفذ الكود الضار المهمة التي صمم من أجلها كالتجسس على نشاط المستخدمين أو سرقة البيانات والمعلومات الهامة والحساسة...إلخ

10- هجمات الرجل في الوسط Man in the miodle attacks

وإن نوع من الهجمات التي تحدث أثناء تبادل البيانات والمعلومات الحساسة بين طرفين كالبيانات المالية من قبل طرف آخر وهو نوع من هجمات التنصت.

11- التلاعب URL Manipulation

حيث يمكن للمتسلل التلاعب بأجزاء معينة من عنوان URL والتحول لصفحات الويب التي لا يفترض إمكانية الوصول إليها. ويعد هذا الهجوم من أسهل أنواع الهجمات، فعناوين URL هي عبارة عن طلبات من المتصفح إلى الخادم وهي شكل من أشكال البرمجة منخفضة المستوى وليست مجرد عناوين ، فعندما يطلب المتصفح X من الخادم يستجيب الخادم ب Y.

12 - القوة الغاشمة Brute-force

حيث يعمل المهاجمون على تخمين المفتاح الذي يتم إنشاؤه من كلمة المرور باستخدام وظيفة اشتقاق المفتاح KEY derivation function بغية العثور على كلمة المرور الصحيحة واختراق جهاز الضحية.

13- هجمات البرمجة النصية عبر المواقع cross sit scripting

هذا النوع من الهجمات عبر المواقع (xss) هي عبارة عن حقن برامج نصية خبيثة في مواقع الويب الموثوقة.

14- التهديدات من الداخل: فأغلب الهجمات السيبرانية يقوم بها شخص من الداخل يساعد المهاجم في حصوله على المعلومات اللازمة للولوج للمنظمات بغية سرقتها أو الوصول للملفات السرية ومن هذه الهجمات (الهجمات على البنوك و المؤسسات المالية).

15- هجمات الذكاء الاصطناعي: يستخدم في هذا النوع من الهجمات الذكاء الاصطناعي لاختراق الأنظمة الرقمية والحصول على المعلومات الحساسة كالبيانات المالية.¹⁶

المحور الثاني : استراتيجيات الجرائم للدفاع عن أمنها في مواجهة الجرائم السيبرانية

سنحاول من خلال هذا المحور التطرق لمفهوم الجريمة السيبرانية ورؤية المشرع الجزائري لها والعقوبات التي اقراها لهذا النوع من الجرائم ، بالإضافة الى التطرق للمحاور الرئيسية التي ركزت عليها الجزائر في استراتيجيتها الأمنية للدفاع عن أمنها السيبراني.

أولاً: الجريمة السيبرانية

يشار الى إساءة استخدام تكنولوجيات المعلومات والاتصالات من قبل المجرمين بالتبادل على انها جرائم الانترنت ، أو جريمة التكنولوجيا العالية ، أو الجريمة الالكترونية.

فقد عرفها المعهد الأسترالي لعلم الاجرام بأنها: "تسمية عامة لجرائم ارتكبت باستخدام تخزين البيانات الالكترونية او جهاز الاتصالات".¹⁷

يمكن تعريف الجريمة السيبرانية بكونها: "كل نشاط اجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة او هدف لتنفيذ الفعل الاجرامي المقصود".¹⁸

الجرائم الالكترونية هي كل فعل او نشاط غير قانوني او غير مشروع يستخدم فيه الحاسوب كموضوع او كوسيلة للجريمة او أي تقنية متعلقة بتكنولوجيات المعلومات قد ينجم عن هذا الفعل انتهاك الملكية المادية او المعنوية".¹⁹

كما يعرفها البعض الآخر بأنها: "تشمل كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب".²⁰

كما تتمثل الجريمة الالكترونية في استخدام الأجهزة التقنية الحديثة كالحاسوب والهواتف النقالة في تنفيذ أغراض غير مشروعة بهدف الإضرار بالمجتمع.²¹

أما المشرع الجزائري فقد استخدم مصطلح "المساس بالأنظمة الآلية للمعطيات" بدلا من مصطلح الجريمة الالكترونية وأشار اليها في المواد من 394 مكرر الى 394 مكرر 7 من قانون العقوبات وعرفها في القانون رقم 04-09²² المتضمن للقواعد الخاصة بالوقاية المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها في المادة 2 منه ، بأنها : " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات .

كما نجد أن المشرع الجزائري وفقا للمادة 12 من القانون 04-09 خص مقدمي الانترنت بجملة من الالتزامات تمثلت في السحب الفوري للمحتويات المخالفة للقانون وتخزينها وحظر الدخول اليها.²³

ومن هنا يمكن القول بأن المشرع الجزائري يعتبر الجريمة الالكترونية كل ما يدخل في الحاسب الآلي من النظام المعلوماتي وعليه فإن نطاق الجريمة الالكترونية بناء على ذلك جاء واسعا ليشتمل على كل ما تفرزه التطورات التكنولوجية من جديد.

ومما سبق يمكن القول بأن الجرائم السيبرانية تشتمل على كل نشاط او فعل غير قانوني باستخدام الحاسب الآلي ، أو احد التقنيات الحديثة لتكنولوجيا الاعلام والاتصال.

ومن هذا المنطلق يمكن أن نستشف بعضا من خصائص الجرائم السيبرانية كالآتي:

- الجرائم السيبرانية جرائم تتم باستخدام تكنولوجيات الاعلام والاتصال أداة ووسيلة.²⁴
- تتمثل في أفعال غير قانونية وغير مشروعة .
- هي جرائم عابرة للحدود.
- في الجرائم السيبرانية يغيب الدليل المادي مما يجعل من الصعب اكتشافها كونها تتعلق ببيانات ومعطيات عبارة عن رموز لا يمكن قرائتها.
- جرائم لا تتسم بالعنف ولكنها تتوقف على مدى المام مرتكبها بالتقنيات الحديثة والخبرة في مجال الحاسب الآلي.

ثانيا : آليات مواجهة الجرائم السيبرانية

من اجل مواجهة المخاطر والتهديدات السيبرانية لابد من استخدام تقنيات الوقاية من الهجمات السيبرانية وأهمها :

- برامج مكافحة الفيروسات Antivirus Programs ، أدوات التخزين الاحتياطي للبيانات والمعلومات كالأقراص المضغوطة .
- استعمال برامج التصفية Filters للتأكد من سلامة الرسائل الالكترونية والصور ...الخ
- استخدام برامج الوقاية كجدران الحماية (جدار النار) Fire wall ومزودات بروكسي Proxy servers ، البرامج النشطة Activex ضمن المستعرض Internet explore وبروتوكولات SST.SSL .
- التعامل بتقنية التشفير Cipharing بين المستخدمين .
- حوكمة الانترنت : من خلال وضع قواعد المراقبة والملاحقة والتنفيذ من اجل حماية امن الانترنت وبالتالي تحقيق حماية الفضاء السيبراني بالجوء للنظام واشراك أكبر عدد من الأطراف المعنية بسبب اتساع نطاق مهمة تشغيل الانترنت وتأمين الموارد الأساسية لها من قدرات وامكانيات مادية وبشرية مؤهلة.²⁵
- تعقب ومتابعة الجرائم السيبرانية : وهذا من خلال تحديث المنومة التشريعية وجعلها تستجيب لمتطلبات التطور التكنولوجي الحاصل وإقرار العقوبات الرادعة لمرتكبي هذه الجرائم ، بالإضافة لضرورة تطوير أساليب ووسائل الكشف عن هذه الجرائم ، والتعاون مع الخبراء والمتخصصين في المعلوماتية للكشف عن الجناة .

- تعزيز التعاون الدولي في مجال الملاحقة وتسليم المطلوبين ، نظرا لطبيعة هذه الجرائم كونها عابرة للحدود كما يجب في هذا الصدد تأهيل القضاة بإخضاعهم لدورات تدريبية عالية المستوى لتمكينهم من التعامل مع هذا لنوع من الجرائم وإقرار الأدلة وإدانة مرتكبيها.²⁶
- إقرار نظام عالمي للمكافحة: تعد التهديدات السيبرانية عالمية لذا فإن حلولاها يجب ان تكون عالمية لذا من الضروري أن تتوصل جميع الدول الى إقرار نظام عالمي للأمن السيبراني يقضي بمكافحة الجرائم الالكترونية من خلال الاتفاق على مجموعة من الآليات والمعايير والقواعد القانونية التي تضمن سلامة الممتلكات والأشخاص، بتوفير الحماية من النفاذ غير المشروع والتلاعب في المعلومات والبيانات واختراقها واتلافها ، مما يفرض الى ضرورة تعزيز التنسيق والتعاون الدولي في حماية الفضاء السيبراني . وفي هذا الصدد تشير الى دور الأمم المتحدة في انشائها لمجموعات عمل لمكافحة الجريمة السيبراني ، حيث أصدرت قرار رقم 63-55 في 04 ديسمبر 2000 وقرار 56/12 في 19 ديسمبر 2001 بشأن مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات والقرار رقم 57/239 في 20 ديسمبر 2002 بشأن ثقافة عالمية للأمن السيبراني بالإضافة لدور الاتحاد الدولي للاتصالات من خلال وضع مبادئ مشتركة بين الدول والحكومات التي تعتمد على تكنولوجيات المعلومات ووضعه لمخطط يعزز الامن السيبراني العالمي.²⁷

ثالثا: محاور الاستراتيجية الجزائرية لتحقيق أمنها السيبراني

لقد سطرت الجزائر استراتيجية للدفاع عن أمنها حيث وضعت الأمن السيبراني كأولوية في برنامجها لمواجهة الجريمة الإلكترونية. وقد ركزت في سبيل تحقيقها لذلك على مجموعة من المحاور.

✓ الجانب القانوني (التشريعي):

واكب المشرع الجزائري التطورات التكنولوجية الحاصلة بإدخال تعديلات هامة على قانون العقوبات بإدراجه لقسم خاص يتعلق بأنظمة المعالجة الآلية للمعطيات بموجب القانون 04-15 المؤرخ في 10 نوفمبر 2004 كما توالى التعديلات بإدراجه لبعض السلوكيات الإجرامية ، بموجب القانون 06-23 المؤرخ في 20 ديسمبر 2006 ، حيث تقوم بمعاقبة كل من يدخل ويلقي عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات (المادة 394 مكرر1) ، أو

الادخال عن طريق الغش معطيات في نظام المعالجة الآلية أو الإزالة أو التعديل بطريق الغش لبعض المعطيات (المادة 394 مكرر2)، أو في حالة تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلّة عن طريق منظومة معلوماتية أو حيازة أو افشاء أو نشر أو استعمال المعطيات بطريق الغش، كما شددت العقوبة في حالة حذف أو تغيير المعطيات أو تخريب نظام اشتغال المنظومة (المادة 394 مكرر3)²⁸.

كما ضمّ تعديل قانون العقوبات 04-15 المادة 04 من الأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة أن برامج الحاسب الآلي تعتبر كمصنف أدبي مكتوب ومحمي، وبناء على هذا فإنه يمكن لصاحب الحق استغلال برنامجه بأي طريقة شاء دون غيره ويترتب على ذلك حقوق مادية للمؤلف (صاحب البرنامج) بالاستغلال التجاري له ولورثته.²⁹

كما تم تعديل قانون الإجراءات الجزائية بتجريم وتسليط العقاب على كل من يثبت في حقه اختراق أنظمة معلومات المؤسسات أو الأفراد بطريقة غير شرعية، حيث جاءت المادة 87 من نفس القانون صريحة في تجريم وتسليط العقاب على من يثبت تورطه في أعمال الإشادة والتجنيد لصالح الجماعات الإرهابية.³⁰

كما سمح المشرع في ذات السياق باللجوء لمجموعة من الإجراءات الخاصة والتي تتماشى مع العالم الافتراضي تتمثل في اعتراض المراسلات والتقاط الصور وتسجيل الأصوات لمقتضيات البحث والتحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.³¹

كما سن المشرع الجزائري مجموعة من الضوابط والآليات المتعلقة بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي (القانون 07-18)³² والتي يقصد بها كل عملية منجزة بطرق آلية أو بدونها على معطيات ذات طابع شخصي مثل: الجمع، التسجيل، التنظيم: الحفظ، ... عن طريق الإرسال أو النشر أو أي شكل من أشكال الإتاحة أو التشفير والإغلاق أو المسح والاتلاف. في سياق حماية الحريات العامة واحترام كرامة الإنسان وعدم المساس بحقوقه وسمعته، ومن بين تلك الآليات استحداث سلطة وطنية لحماية المعطيات ذات الطابع الشخصي، مكلفة بالسير على مطابقة معالجة المعطيات ذات الطابع الشخصي لأشخاص القانون.

بالإضافة للقانون 08-01 المتعلق بالتأمينات الاجتماعية: فقد جرم المشرع الجزائري في الجانب المتعلق بالتأمينات الاجتماعية كل ما يتعلق بتسليم أو تسليم أو القيام بتعديل أو حذف كلي أو جزئي للمعطيات والمعلومات الواردة في البطاقة الالكترونية التي تسلم للمؤمن له

اجتماعيا بغرض العلاج، وهو ما جاء في المادة 93 مكرر2 والمادة 93 مكرر3 من القانون (08-01).³³

مما سبق يمكن القول أن المشرع الجزائري تصدى للجرائم السيبرانية بترسانة من القوانين والتعديلات القانونية للتعامل مع هذا النوع من الجرائم.

كما تدعمت المنظومة القانونية الجزائرية بالقانون 04-09 والمتعلق بالوقاية من تكنولوجيايات الإعلام والاتصال ومكافحتها وقد ضم مجموعة من التدابير الوقائية والإجراءات للوقاية من الجرائم السيبرانية ومكافحتها وأهما:

■ التدابير الوقائية:

المراقبة الالكترونية : وفقا للمادة 04 من القانون 04-09 حيث يمكن الاستعانة بالمراقبة الالكترونية في تقديم المساعدة القضائية الدولية المتبادلة في حال توفر معلومات عن احتمال تعرض المنظومة المعلوماتية لهجمات أو اعتداء يشكل خطرا على النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

الاستعانة بمزودي الخدمات للوقاية من الجرائم السيبرانية: من أجل جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات والتي تشمل وفقا للمادة 11 من القانون 04-09

(معطيات تسمح بالتعرف على مستعملي الخدمة ، المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال، عناوين المواقع المطلع عليها ، تاريخ ووقت ومدة كل اتصال ، المرسل اليه).

■ التدابير الإجرائية : ويمكن حصرها فيمايلي:

تفتيش وحجز المنظومة المعلوماتية: وفقا للمادة 3 من القانون 04-09 تم وضع مجموعة من الترتيبات التقنية لمراقبة الاتصالات وتجميع تسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية.³⁴

تمديد الاختصاص بالنظر في هذه الجرائم: حيث يؤول الاختصاص للنظر في الجرائم المتصلة بتكنولوجيا الاعلام والاتصال للمحاكم الجزائرية في حال الجرائم المرتكبة خارج الإقليم الوطني في حال استهدافها لإحدى مؤسسات الدولة أو المصالح الاستراتيجية للاقتصاد الوطني أو الدفاع الوطني .

تبادل المساعدة القضائية الدولية: فيما يتعلق بجمع الأدلة وتبادل المعلومات واتخاذ الإجراءات التحفظية في حال ارتكاب الجريمة الالكترونية وفقا للاتفاقيات الدولية.

وبالرغم من المجهودات المبذولة من قبل السلطات الجزائرية لتحديث وتطوير منظومتها القانونية بحيث تواكب تطور الجرائم الالكترونية الا أن المختصين في هذا الشأن يرون بأن البنية التنظيمية والتشريعية لازالت في طور التشكيل إذ أن هناك العديد من الجوانب التي لم يتم تطويرها بما يتوافق والبيئة الوطنية كالمواصفات التقنية للمعلومات، البرامج، الأجهزة...الخ³⁵

وفي هذا الصدد عملت الحكومة الجزائرية على تدارك هذه النقائص مواكبة التحولات الطارئة بالتحسين والتطوير المستمر لآليات المواجهة وتعزيز الجانب التشريعي وتطويره من خلال الهيئات المختصة.

حيث تم استحداث القانون 04-18 المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية³⁶، حيث تعكف آليات وسلطة الضبط على السهر على احترام متعاملي البريد والاتصالات الالكترونية للأحكام القانونية والتنظيمية المتعلقة بالأمن السيبراني في المادة 13 من ذات القانون 04-18.

حيث تم بموجبه تجريم انتهاك سرية المراسلات أو افشاء مضمونها أو استخدامها دون ترخيص من المرسل أو المرسل اليه.

إضافة لتجريم كل محاولة فتح أو تخريب أو تحويل البريد أو المساعدة في ارتكاب هذه الجريمة.

✓ الجانب العملي (الجهاز العملي):

وتمثل في مجموعة من الهيئات والمصالح التي أخذت على عاتقها مكافحة الجرائم الالكترونية بمختلف أنواعها.

- المصلحة المركزية لمكافحة الجريمة المعلوماتية: وهي عبارة عن وحدة متخصصة تابعة لمديرية الامن الوطني تتولى التحقيق في الجرائم المرتكبة عبر الانترنت (الاختراق والاحتيال والتصدي الالكتروني...)، حيث تهدف لتطوير قدرات الشرطة في مجال مكافحة الجرائم المعلوماتية بتوفيرها للموارد البشرية المتخصصة والمؤهلة وكذا التقنيات الحديثة.

- مركز الوقاية من جرائم الاعلام الآلي والجرائم المعلوماتية للدرك الوطني: أنشئ سنة 2008 بغرض تأمين منظومة المعلومات لخدمة الامن العام حيث اعتبر بمثابة مركز توثيق يعمل هذا المركز على تحليل المعلومات والبيانات المتعلقة بالجرائم المعلوماتية المرتكبة وتحديد هوية أصحابها³⁷، من خلال :
 - المراقبة الدائمة والمستمرة على شبكة الانترنت ومراقبة الاتصالات الالكترونية والمشاركة في عمليات التحري لفائدة وحدات الدرك الوطني والجهات القضائية.
- المعهد الوطني للأدلة الجنائية وعلم الاجرام للدرك الوطني: تم اشأؤه بموجب المرسوم الرئاسي رقم 04-183 المؤرخ في 26 يونيو 2004 وتتمثل مهامه فيما يلي:
 - المساعدة في التحريات المعقدة بالاعتماد على مناهج الشرطة العلمية والتقنية في جمع الأدلة وتحليلها المأخوذة من مسرح الجريمة.
 - اجراء الخبرات والفحوص العلمية في إطار التحريات الأولية والتحقيقات القضائية بغرض التعرف على الجناة.
 - تصميم وإنجاز بنوك المعطيات بما في ذلك تلك المتعلقة بالبصمات الجينية ووضعها في متناول المحققين والقضاة بغرض الكشف عن المجرمين.
 - المشاركة في الملتقيات والمحاضرات والندوات الوطنية بهدف تطوير مستخدمي المعهد.³⁸
- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها:

أنشئت هذه الهيئة بموجب المادة 13 من القانون 09-04 المتضمن للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال وتتولى هذه الهيئة المهام التالية:

 - مكافحة الجرائم المتعلقة بتكنولوجيات الاعلام والاتصال بتنشيط وتنسيق عمليات الوقاية بمساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات وجمع المعلومات وتبادلها مع نظيراتها بقصد التعرف على المجرمين ومكان تواجدهم.³⁹
 - تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الاعلام والاتصال.
 - كما تساهم في تكوين المحققين المتخصصين في مجال التحريات التقنية.

- **القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال:** تم إنشاؤه بموجب الامر رقم 21-11 المؤرخ في غشت 2021 المعدل والمتمم لقانون الإجراءات الجزائية، ويتولى هذا القطب مهمة المتابعة والتحقيق في جرائم تكنولوجيا الاعلام والاتصال وكذا الحكم في الجرائم المنصوص عليها في الباب 6 من الامر رقم 21-11 إذا كانت تشكل أو الدفاع الوطني وكذا جرائم نشر وترويج اخبار كاذبة بين الجمهور تدعو الى المساس بالأمن والنظام العام واستقرار المجتمع.
- **نيابة مديرية الشرطة العلمية والتقنية التابعة للمديرية العامة للأمن الوطني:** وتتولى اعمال البحث والتحري و جمع الأدلة الجنائية بمختلف أنواعها في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال من خلال المخبر المركزي للشرطة العلمية (بالجزائر العاصمة) و المخبر الجهوي للشرطة العلمية (قسنطينة وهران) ، وتقوم الشرطة الجزائرية بدور بالغ الأهمية في مكافحة الجرائم السيبرانية من خلال تتبعها للأثر الالكتروني و قطع مصادر التمويل والتجنيد عبر الفضاء السيبراني، بالإضافة لنشر حملات التوعية والتحسيس وتحقيق التعاون الدولي في مجال تبادل المعلومات والخبرات.⁴⁰

رابعاً: معوقات تحقيق الامن السيبراني في الجزائر

- تواجه الجزائر وبالتحديد مصالح الدرك الوطني ومصالح الامن العديد من التحديات التي تقف حائلاً أمام تحقيق أمنها السيبراني ومن بين هذه المعوقات ماييلي:
- صعوبة اكتشاف هوية المجرمين مرتكبي الجرائم الالكترونية وهذا راجع لزيادة عدد مستخدمي شبكة الانترنت مما يصعب عمليات البحث والتحري.
 - سرعة القيام بالجرائم الالكترونية مما يفرض تحدياً امام الجهات الأمنية المختصة في الكشف عن الجناة وملاحقتهم وهذا راجع لانتشار تكنولوجيا الانترنت فائقة السرعة والتدفق مثل: ... ADSL; VSAT
 - الاستخدام الواسع لشبكات التواصل الاجتماعي في الجزائر وهو ماساهم في انتشار وارتفاع وتنوع الجرائم الالكترونية المرتكبة .
 - تعدد عمليات الخفي Proxy أثناء استعمال خدمات الانترنت من اكبر المعوقات التي تواجه السلطات المختصة في التحقيق مما يستوجب امتلاك الوسائل المتطورة لرصد هذه الجرائم وملاحقة الجناة.

- عدم وجود تنسيق بين الدول اذ يمكن لمرتكبي الجرائم الالكترونية النفاذ لأنظمة الحاسوب واختراق البيانات في دولة أ بلد آخر دون شرط التواجد في ذات البلد فهي جريمة عابرة للحدود مع إمكانية تخزين دليل الجريمة في حاسوب موجود في بلد آخر (ثالث)، وهذا ما يمكن المجرم من الإفلات بجريمته بإخفاء هويته ويصعب من عملية الكشف عليه ومحاسبته، وهذا ما يستدعي تعاوننا دوليا سريعا لمحاربة هذه الجرائم .
 - عدم توفر وامتلاك الإمكانيات المادية والبشرية اللازمة للحد من الجرائم السيبرانية.
 - عدم الوعي بمفهوم الامن السيبراني وآلياته لدى مستخدمي شبكة الانترنت وهو ما يمكنهم من الوقوع فريسة سهلة لدى المجرمين وخاصة مستخدمي مواقع التواصل الاجتماعي.⁴¹
 - عدم فعالية القوانين المعتمدة وعدم الكفاءة والتأخر في تطبيقها على أرض الواقع وهذا ما يمنح مرتكبي الجرائم الالكترونية مجالا واسعا للإفلات بجرائمهم.
- الخاتمة:**

من خلال هذه الورقة البحثية نخلص للقول بأنه ورغم التحديات التي واجهتها الجزائر في سبيل تحقيقها لأمنها السيبراني إلا أنها عملت ولازالت تعمل على التصدي ومكافحة الجرائم السيبرانية التي تستهدف أمن منظومتها المعلوماتية، من خلال ما يلي:

- تعديل منظومتها القانونية وجعلها تتماشى وتواكب التحدي الرقمي المفروض عليها، حيث عدلت القانون رقم 04-15 المتضمن لقانون العقوبات، وكذا عدلت قانون (الإجراءات الجزائية)، كما قام المشرع الجزائري بسن القانون رقم 09-04 والمتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.
- تضمنت التدابير الوقائية: كالمراقبة الالكترونية والاستعانة بمزودي الخدمات من اجل جمع وتسجيل المعطيات المتعلقة بالاتصالات للوقاية من الجرائم السيبرانية والتدخل من خلال السحب الفوري للمحتويات المخالفة للقانون.
- الاحتكام لمجموعة من التدابير الإجرائية، تجسدت في تفتيش وحجز المنظومة المعلوماتية وتمديد الاختصاص بالنظر في هذه الجرائم وتبادل المساعدة القضائية الدولية للكشف عن الجناة وملاحقتهم.

- وفي الختام نقترح مجموعة من التوصيات التي تفعل من دور السلطات الجزائرية في مجال مكافحة الجريمة السيبرانية :
- نشر ثقافة الامن السيبراني في أوساط مختلف شرائح المجتمع، وتوعيتهم بمدى خطورة الجرائم السيبرانية ، وضرورة اتخاذ نظم للحماية من أجل تأمين معلومات وبيانات مستخدمي شبكة الانترنت.
 - تعزيز التعاون الدولي في مجال تبادل المعلومات والأدلة للكشف عن مرتكبي الجرائم الالكترونية وملاحقتهم .
 - الانضمام للاتفاقيات الدولية في مجال حماية الأنظمة المعلوماتية والمشاركة في الدورات لتكوينية واللقاءات العلمية للاستفادة من الخبرات في مجال توظيف واستغلال تكنولوجيا الاعلام الاتصال.
 - العمل على تطوير المنظومة التشريعية بما يتوافق والتطور الرقمي الحاصل ن خاصة في ظل تنوع الجرائم الالكترونية المرتكبة .

الهوامش:

- ¹ زروقة إسماعيل ، " الفضاء السيبراني والتحول في مفاهيم القوة والصراع" ، مجلة العلوم القانونية والسياسية ، المجلد 10 ، العدد 1 ، افريل 2019 ، ص 1017.
- ² بركان اكرام ، .رلمي فهمي ، " واقع واشكالات الأمن السيبراني في الجزائر" ، ورقة بحثية مقدمة للمؤتمر العلمي الوطني الأول حول " الاستراتيجية الجزائرية الكبرى لتحقيق أهداف الأمن الشامل والتنمية المستدامة" ، كلية العلوم السياسية ، جامعة صالح بوبنيدر قسنطينة 3 ، فيفري 2024.
- ³ بارة سمير ، " الأمن السيبراني في الجزائر: السياسات والمؤسسات ، المجلة الجزائرية الأمن الإنساني" ، العدد 04 جويلية 2017 ، ص 257.
- ⁴ نفس المرجع ، نفس الصفحة.
- ⁵ بوزادية جمال ، " الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية: التحديات والآفاق المستقبلية" ، مجلة العلوم الاقتصادية والسياسية ، المجلد 10 ، العدد 1 ، أفريل 2019 ، ص 1266.
- ⁶ بوعبسة محمد ، بن ناصر بلقاسم ، " المخاطر السيبرانية وأمن الشبكات الالكترونية " ، تم الاطلاع عليها بتاريخ: 2025/08/15 على الساعة 13:00 على الموقع التالي: <http://despace.univ-eloued.dz>
- ⁷ العتيبي عمر بن محمد ، " الامن المعلوماتي في المواقع الالكترونية ومدى توافقه مع المعايير المحلية والدولية " ، أطروحة دكتوراه ، في العلوم الأمنية ، كلية الدراسات العليا ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، 2010 ، ص 17.
- ⁸ بوعبسة محمد ، بن ناصر بلقاسم ، مرجع سابق .
- ⁹ نوفل سيو ، " أهمية الامن السيبراني : حماية بياناتك وأمان مستقبلك الرقمي" ، تم الاطلاع بتاريخ: 2025/08/18 ، على الساعة 15:00 على الموقع التالي: <https://nofalseo.com/>

- ¹⁰ (ب.ذ.صاحب المقال) ، " الامن السيبراني : أهميته وفوائده" ، تم الاطلاع بتاريخ: 2025/08/20 ، على الساعة: 14:00 على الموقع التالي: <https://holistiquetraining.com/public/ar/news/importance-of-cyber-security>

- ¹¹ (ب.ذ.صاحب المقال)، "أنواع الأمن السيبراني ومجالاته وعناصر تكوينه"، تم الاطلاع بتاريخ: 2025/08/15 على الساعة 15:00 ، على الموقع التالي: <http://bakkah.com/ar/knowledgege.center>
- ¹² نوفل سيو ، مرجع سابق.
- ¹³ نفس المرجع
- ¹⁴ حمود رؤى ، "أبرز أنواع الهجمات السيبرانية حتى عام 2021"، تم الاطلاع بتاريخ: 2025/08/15 ، على الساعة 13:00 ، على الموقع التالي: <http://www.rnig-sa.com>.
- ¹⁵ (ب.ذ.صاحب المقال)، "الأمن السيبراني ، مفهومه وتاريخه"، تم الاطلاع بتاريخ: 2025/08/10، على الساعة 9:00، على الموقع التالي: <https://www.aljazeera.net/encyclopedia/2024/9/19>
- ¹⁶ حمود رؤى ، مرجع سابق.
- ¹⁷ Cameron S.D.Brown , « Investigating and Prosecuting Cyber crime : Forensic Dependencies and Justice », International Journal of Cyber criminology .vol 9, Issue 1 , January-june 2015, p57.
- ¹⁸ القرعان محمود احمد ، الجرائم الالكترونية ، عمان : دار وائل للنشر والتوزيع ، 2017، ص19.
- ¹⁹ سي عبد القادر حنان ، "الأمن السيبراني وأثره على دول العالم"، مجلة البصائر للدراسات القانونية والاقتصادية ، المجلد 4، العدد 7 ، 2024 ، ص25.
- ²⁰ الاكلي نادية ، "الجريمة السيبرانية في الجزائر والعقوبات المقررة لها"، مجلة الاجتهاد القضائي ، المجلد 15، العدد 1، مارس 2023، جامعة محمد خيضر بسكرة ، ص259.
- ²¹ زبيخة زيدان ، الجريمة المعلوماتية في التشريع الجزائري والدولي، الجزائر : دار الهدي، 2011، ص42.
- ²² المؤرخ في 5 غشت 2009، ح.ر، الصادرة في 16 غشت 2009، العدد 47.
- ²³ مهدي رضا ، "الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري"، مجلة إيليزا للبحوث والدراسات ، مجلد 6 ، العدد 2 ، 2021، ص118.
- ²⁴ هروال نبيلة ، "جرائم الانترنت: دراسة مقارنة"، كلية الحقوق والعلوم السياسية ، جامعة تلمسان ، 2013-2014، ص37.
- ²⁵ بوعيسى محمد ، بن ناصر بلقاسم ، مرجع سابق .
- ²⁶ صغير يوسف ، "الجريمة المرتكبة عبر الانترنت"، رسالة ماجستير في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية ، جامعة مولود معمري تيزي وزو ، 2013، ص19-20.
- ²⁷ الاتحاد الدولي للاتصالات ، "بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات"، محلة اخبار الاتحاد ، العدد 10 ديسمبر 2010، ص46.
- ²⁸ مهدي رضا ، مرجع سابق ، ص116-117.
- ²⁹ بلقاسم سميحة ، بوشوشة حميد ، "الجريمة الالكترونية بعد جديد للإجرام في الجزائر وأقبعها وآليات مجاهمتها"، مجلة العلوم الإنسانية لجامعة ام البواقي ، المجلد 10، العدد 1 ، جوان 2023 ، ص539.
- ³⁰ مهدي رضا ، مرجع سابق ، ص117.
- ³¹ بوازدية جمال ، مرجع سابق ، ص1278.
- ³² قانون رقم 1807 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ، ج.ر رقم 34 الصادرة بتاريخ 10 يونيو 2018، ص12.
- ³³ قانون 01-08 ، الصادر في 23 يناير 2008 والمتمم للقانون رقم 83-11 المؤرخ في 2 يوليو 1983 والمتعلق بالتأمينات الاجتماعية ، ج.ر رقم 04 الصادرة بتاريخ 07 يناير 2008.
- ³⁴ مهدي رضا ، مرجع سابق ، ص119.

³⁵ جمال بوزادية ، مرجع سابق ، ص1279.

³⁶ القانون 04-18 المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية المؤرخ في 10 مايو 2018 ، ج.ر ، عدد 27 الصادر بتاريخ 13 مايو 2018.

³⁷ ادريس عطية ، "مكانة الامن السيبراني في منظومة الامن الوطني" ، مجلة مصداقية ، المجلد 1، العدد 1، 2019، ص112.

³⁸ المرسوم الرئاسي رقم 183-04 ، 2004، ص19.

³⁹ القانون رقم 04-09، 2009، ص8.

⁴⁰ بلقاسم سميحة ، بوشوشة حميد ، مرجع سابق ، ص549-550.

⁴¹ بارة سمير ، مرجع سابق ، ص276-277.