تعزيز الأمن السيبراني في الجزائر

–الجهود القانونية، العلمية والعملية–

الأستاذة/ قيطة فاطمة الزهراء جامعة الشهيد حمه لخضر الواد، الجزائر

الأستاذة/ صالحي دليلة جامعة الشهيد حمه لخضر الواد، الجزائر fadel927@gmail.com

ملخص

إنّ كل المؤشرات تنبأ بخطر داهم في مجال الجريمة الإلكترونية، فالاختراقات الإلكترونية والهجمات السيبرانية بمختلف أشكالها ستكون في المستقبل أخطر على الجانب المعلوماتي والجانب المادي، ولها تأثير مدمّر على البُنى التحتية يفوق الأضرار الناجمة عن الكوارث الطبيعية، خاصةً مع التزايد السريع للأجهزة المتصلة بالشبكة العنكبوتية، ونمو المعاملات الإلكترونية والتطبيقات المتعلقة بها في مختلف المجالات.

وتأسيسا على ذلك، بات من الأهمية بمكان تبنّي الدول والحكومات، خاصة العربية، إستراتيجيات تعززّ بها أمنها السيبراني، وإنشاء وحدات أو هيئات مختصة بحماية البنى التحتية من المخاطر الإلكترونية، وعلى رأس ذلك الاستثمار في البحث العلمي، وزيادة الوعي بهذا المجال بما يعزّز مستوى الأمن ومواكبة التكنولوجيا والتقنيات الحديثة التي من شأنها أن تجعل الأنظمة الإلكترونية أكثر أمنا، دون إغفال جانب التشريعات القانونية التي من شأنها مواجهة تحديات الأمن السيبراني بشكل أكثر صرامة وفاعلية.

والجزائر كغيرها من الدول تسعى إلى تعزيز أمنها السيبراني، في مواجهة مخاطر الرقمنة التي أضحت تهدد الأمن الوطني، خاصة في ظل التوجه نحو الحكومة الإلكترونية. وهنا تسعى هذه الورقة البحثية إلى معرفة خطوات وبرامج الاستراتيجية الجزائرية في مجال تدعيم الأمن السيبراني.

الكلمات المفتاحية: الجريمة السيبرانية_ الأمن السيبراني_ التنظيم القانوني_ الاستراتيجية

Summary

Cybercrime will not disappear soon, as cyber-intrusions and cyber-attacks of all kinds will be worse and more costly in the future, and have a more devastating impact on infrastructure than damage caused by natural disasters, especially with the rapid increase in devices connected to the Internet, and the growth of electronic transactions and applications related to them in various fields.

Based on this, it has become of great importance for countries and governments, especially Arab countries, to adopt strategies to enhance their cyber security, and to establish units or bodies specialized in protecting infrastructure from electronic risks, on top of that investing in scientific research and raising awareness in this field in order to enhance the level of security and keep pace with Technology and modern technologies that would make electronic systems more secure without neglecting the aspect of legal legislation that would confront cyber – security challenges in a more stringent and effective manner.

Algeria, like other countries, seeks to enhance its cyber security in the face of the risks of digitization that have become a threat to national security, especially in light of the trend towards e-government. Here, this research paper seeks to know the steps and programs of the Algerian strategy in the field of strengthening cyber – security.

Keywords:

cyber crime, cyber security, legal regulation, strategy

مقدمة:

إنّ كل المؤشرات تنبأ بخطر داهم في مجال الجريمة الإلكترونية، فالاختراقات الإلكترونية والهجمات السيبرانية بمختلف أشكالها ستكون في المستقبل أخطر على الجانب المعلوماتي والجانب المادي، ولها تأثير مدمّر على البُنى التحتية يفوق الأضرار الناجمة عن الكوارث الطبيعية، خاصةً مع التزايد السريع للأجهزة المتصلة بالشبكة العنكبوتية، ونمو المعاملات الإلكترونية والتطبيقات المتعلقة بها في مختلف المجالات.

وتأسيسا على ذلك، بات من الأهمية بمكان تبنّي الدول والحكومات، خاصة العربية، إستراتيجيات تعززّ بها أمنها السيبراني، وإنشاء وحدات أو هيئات مختصة بحماية البنى التحتية من المخاطر الإلكترونية، وعلى رأس ذلك الاستثمار في البحث العلمي، وزيادة الوعي بهذا المجال بما يعزّز مستوى الأمن ومواكبة التكنولوجيا والتقنيات الحديثة التي من شأنها أن تجعل الأنظمة الإلكترونية أكثر أمنا، دون إغفال جانب التشريعات القانونية التي من شأنها مواجهة تحديات الأمن السيبراني بشكل أكثر صرامة وفاعلية.

والجزائر كغيرها من الدول تسعى إلى تعزيز أمنها السيبراني، في مواجهة مخاطر الرقمنة التي أضحت تهدد الأمن الوطني، إذ تشير الاحصائيات المسجلة أن الجريمة الإلكترونية أخذت منحا تصاعدي في الأونة الأخيرة وهو ما ينبأ بخطورة الوضع، خاصة في ظل التوجه نحو تبني مقاربة الحكومة الإلكترونية، ومن هذا المنطلق فإن السلطات الجزائرية بكل هيئاتها ملزمة باتخاذ الاحتياطات اللازمة لتفادي أي جرائم سيبرانية.

وتأسيسا لما سبق تسعى هذه الورقة البحثية إلى معرفة خطوات وبرامج الاستراتيجية الجزائرية في مجال تدعيم الأمن السيبراني، من خلا الإجابة على الإشكالية التالية: **ماهي الاستراتيجية التي تبنتها الجزائر لتعزيز أمنها السيبراني؟**

وسنجيب على هذه الاشكالية من خلال الاجابة على التساؤلات الفرعية التالية:

1- ما مفهوم الجريمة السيبرانية وما أشكالها؟

2- ما لمقصود بالأمن السيبراني وماهي أبعاده؟

3- هل هناك جانب قانوني واضح لمواجهة الجريمة الإلكترونية في الجزائر؟

4- ماهي أهم البرامج والخطط التي اتبعتها الجزائر لموجهة الجريمة السيبرانية؟

5- ماهي النظرة المستقبيلة للجزائر في مجال الأمن السيبراني؟

اتبعنا في هذه الدراسة المنهج الوصفي التحليلي من خلال وصف الجريمة السيبرانية والأمن السيبراني وتحليل مختلف الجهود التي بذلتها الجزائر لمواجهة الجريمة السيبرانية على اختلاف اشكالها .

أولا: الجريمة السيبرانية:

- **المفهوم:** تعددت التعريفات واختلفت حول مفهوم الجريمة الإلكترونية كما يطلق عليها أو السيبرانية، فمنهم من يحصرها في مفهوم ضيق يرتبط بسوء تداول المعلومة فقط، ومنهم من يحصرها في مجال المال، وغيرهم يربطها بكل فعل غير لائق عبر وسيط إلكتروني، وهذا التعريف الأشمل الذي سنتبناه في تعريفاتنا:

- حيث هناك من عرفها أنها: هو كل فعل وكل سلوك غير مشروع أو غير أخلاقي أو غير مسموح به صادر عن إرادة جنائية يقوم به شخص ما لديه دراية ومعرفة بتكنولوجيا المعلومات المختلفة(تكنولوجيا التخزين الاسترجاع وتكنولوجيا الاتصالات الحديثة) ويوجه ضد المصلحة العامة و الخاصة عبر وسط الكتروني. (المؤمن 2022، ص61)
- وطرف أخر يعرفها : هي كل عمل ضار يحدث في الفضاء السيبراني كالإحتيال ونشر محتويات غير قانونية والهجمات التي تستهدف منظومات الإعلام للمؤسسات أو للأفراد بغرض التجسس أو التخريب أو الإبتزاز أو التأثير السلبي على الرأي العام. (بوقرص 2022، ص65)

وعليه نصل إلى **تعريف إجرائي** مفاده أن **الجريمة السيبرانية** : هي كل نشاط غير قانوني بواسطة تداول المعلومات عبر وسيط إلكتروني، قد يشكل تهديدا لأمن الأشخاص أو الدول على المستوى الداخلي أو الخارجي.

- **أشكال الجريمة السيبرانية:**

للجريمة السيبرانية عدة أشكال يمكن إيجازها فيما يلي:

1- اعتراض البيانات والتلاعب بها أو اتلافها من خلال الفيروسات أو يدويا، وهنا تدخل حقوق الملكية الفكرية و سلامة المواقع الخاصة أو العامة. (جبور 2013، ص35)

2- إتلاف وتخريب البيانات والبرامج، والتلاعب بالمعلومات المخزنة. (روان 2020، ص18)

3- سرقة الهويات الرقمية.

4- تعطيل المصالح والخدمات. (بارة 2017، ص260)

5- التجسس: وهي عمليات الاختراق الإلكتروني التي تتم عن طريق استعمال التقنيات العالية من طرف أجهزة الاستخبارات الجنبية للوصول إلى المعلومات السرية المخزنة في المواقع الحيوية والاستراتيجية للدولة على شاكلة تسريبات ويكي ليكس، (بوازدية 2019، ص1267)

6- الإبتزاز: كنشر معلومات أو صور أو بيانات صحيحة أو غير صحيحة عن شخص بغرض الحصول على المال أو علاقة غير شرعية. (روان 2020، ص19)

7- التحايل والتصيُّد وهو عندما يخدع المجرمون الإلكترونيون الأشخاص للكشف عن معلومات حساسة ككلمات المرور وأرقام الضمان الاجتماعي، يُطلق على ذلك التصيّد الاحتيالي. من أشهر طرق حدوث التصيّد الاحتيالي أن يتلقى الشخص رسالة بريد إلكتروني تبدو ظاهريًا أنها من مصرف أو مؤسسة حكومية ويتم استدراجه إلى مواقع تبدو حقيقية. وبمجرد الوصول إليها، يُطلب من الشخص إدخال كلمة المرور وأرقام الضمان الاجتماعي والبيانات المالية. ثم يأخذ المجرمون الإلكترونيون هذه المعلومات ويستخدمونها لأغراضهم الخاصة. يُعد التصيّد الاحتيالي جزءًا من مشكلة أكبر تُسمى الهندسة الاجتماعية، (صحيفة البيان 2022)

8- التأثير السلبي على الرأي العام، من خلال التلاعب بحقيقة البيانات أو التحريض أو نشر الاشاعات وغيرها .

ثانيا: الأمن السيبراني:

❖ **المفهوم:** تعرف وزارة الدفاع الامريكية الأمن السيبراني على أنه" مجموعة الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها – الإلكترونية والمادية– من مختلف الجرائم، الهجمات، التخريب، التجسس والحوادث". (قرة 2019)

- ويمكن أن ندرج تعريف آخر: وعليه فإن الأمن السيبراني هو مزيج من العمليات والتقنيات الممارسة، والهدف منه حماية البرامج والتطبيقات والشبكات وأجهزة الكمبيوتر والبيانات من الهجوم، ويشمل الأمن السيبراني الأمن المادي للبرامج والتطبيقات والشبكات وأجهزة الكمبيوتر، وأمن غير مادي أو معنوي يتعلق بالبيانات والمعلومات من أي هجوم وأضرار متعمدة وسرقة المعلومات والتحكم في الوصول الصحيح للأجهزة والتطبيقات والشبكات لحمايتها من الضرر الذي قد يحدث عبر الشبكات. (الشمري 2021، ص157)

تتعدد التعريفات وتختلف باختلاف الجهة المعنية به، غير أنه يمكننا وضع **تعريف إجرائي** انطلاقا من الاطلاع على هذه التعاريف وفهمها: يعتبر **الأمن السيبراني** كل السبل التي تنتهجها الدول أو الأطراف الخاصة لحماية معلوماتها وأفرادها مما قد يلحق بهم من ضرر من مستعملي الفضاء الإلكتروني سواء بشكل مادي أو معنوي.

❖ **أبعاد الأمن السيبراني:**

الأبعاد العسكرية: وتتمثل الميزة النسبية للأمن السيبراني في بعده العسكري عن طرق قدرة القوة السيبرانية على ربط الوحدات العسكرية ببعضها البعض عبر العالم الافتراضي، وهذا ما يسهل عملية تبادل المعلومات الذي ينعكس إيجاباً على تحقيق الأهداف العسكرية. (قرة 2019)

الأبعاد الاجتماعية: تسمح طبيعة الإنترنت المفتوحة بالاطلاع 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. (جبور 2013، ص29)

الأبعاد السياسية: هناك أمثلة كثيرة تدفع نحو الاهتمام بالبعد السياسي للأمن السيبراني، كالتسريبات المختلفة للوثائق الحساسة التي تؤدي إلى مشكلات كبرى على المستوى الخارجي والدولي، كما أنه لا أحد يُنكر الدور المتعاظم لشبكات التواصل الاجتماعي على المستوى السياسي (حملات انتخابية، تظاهرات افتراضية،...)، كما يتم استغلال هذه المواقع من طرف العديد من الحكومات لتمريرها. (بارة 2017، ص261)

الأبعاد الاقتصادية: يرتبط الأمن السيبراني ارتباطاً وثيقاً بالاقتصاد، فالتلازم واضح بين اقتصاد المعرفة وتوسع استخدام تقنيات المعلومات والاتصالات والتي تتيح تعزيز التنمية الاقتصادية لبلدان كثيرة عبر إفادتها من فرص الاستخدام التي تقدمها الشركات الدولية والشركات الكبرى التي تبحث عن إدارة كلفة إنتاجها بأفضل الشروط، إلا أن هذا الواقع المشرق يطرح مسائل مختلفة سواء ما تعلق بحماية مقدم الخدمة والعمل أو بحماية المستهلك عبر الإنترنت. ضف إلى ذلك دخول العالم عصر المال الإلكتروني ضمن بيئة تقنية متحركة بعد إطلاق خدمات المحفظة الإلكترونية، إذ تتزايد استثمارات المصارف والمؤسسات المالية في مجال المال الرقمي. (جبور 2013، ص30)

الأبعاد القانونية: إن التطورات التكنولوجية المتسارعة، تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية في الفضاء السيبراني، فالملاحظ أن الجريمة السيبرانية تفتقد في معظم البلدان إلى الأطر القانونية الصارمة للتعامل معها، إضافة إلى ضرورة تفعيل التعاون الدولي المشترك لمكافحتها، وهو ما سنطرحه في الجانب التشريعي لاستراتيجية الجزائر في تعزيز الامن السيبراني. (السمحان 2020، ص15،16)

ثالثا: الاستراتيجية الجزائرية في مواجهة الجريمة السيبرانية:

انتهجت الجزائر جملة من السياسات الدفاعية في سبيل محاربة الجريمة الإلكترونية على اختلاف اشكالها، بدءا بالنصوص التشريعية واستحداث هيئات تتبع ومكافحة الجريمة، وصولا إلى التعاون الدولي تمثلا في جملة من الاتفاقيات والشراكات مع المؤسسات العربية والإفريقية والدولية، في حين أنها لم تنسى أهمية الجانب العلمي من خلال عديد الندوات والملتقيات العلمية، وفيما يلي تفاصيل حول كل خطوة من هذه الخطوات:

الجانب التشريعي:

أ-قانون العقوبات:

على غرار الدستور الجزائري أعلى قانون في الدولة والذي جرم مختلف أشكال الجريمة بما فيها الجريمة الإلكترونية والمعلوماتية ، قام المشرع الجزائري بتعديل قانون العقوبات بموجب القانون رقم 04 / 15 من أجل تجريم الأفعال الماسة بأنظمة الحاسب الآلي، وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام، حيث جاء التعديل في المواد 394 مكرر إلي المادة 394 مكرر 7، تحت عنوان "المساس بأنظمة المعالجة الآلية. (بوهرين 2021، ص56)

كما أضاف المشرع الجزائري في سنة 2006 تعديلات جديدة مست القسم السابع مكرر منه، وجاء هذا التعديل لتشديد العقوبة المقررة لهذه الجرائم دون المساس بنص المواد في هذا القسم، إلى جانب زيادة الوعي بخطورة مثل هذه الجرائم المستحدثة.

وتتجسد الجرائم التي نصت عليها التعديلات فيما يلي:

- جريمتا الدخول والبقاء غير مصرح بهما: المادة 394 مكرر.
- جريمة الاعتداء على المعطيات: المادة – 394 مكرر1.
- جريمة التعامل في المعلومات غير مشروعة : المادة – 394 مكرر2. (قانون العقوبات، 2004)

ب- القوانين والمراسيم الخاصة بالجرائم الإلكترونية:

- **القانون رقم - 09 / 04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها** :وهو القانون الذي عرف الجريمة الإلكترونية وإدراجها ضمن الأعمال المعاقب عليها قانونا في المادة -02- ، كما نص على مراقبة الاتصالات الإلكترونية وذلك بتحديد الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتيه. (الجمهورية الجزائرية الشعبية الديمقراطية 2009)
- • **القانون رقم 15 / 04 المتعلق بالتوقيع والتصديق الإلكترونيين:** وتعلق بتجريم بعض الأفعال المربطة بالمعلومات ذات الطابع الشخصي وقد حدد جملة من هذه الجرائم من خلال النص على جملة من العقوبات الردعية :
  - جريمة إفشاء البيانات الشخصية أو اساءة استعمالها : حسب نص المادة - 68 .
  - جريمة الإخلال بسرية البيانات: وفقا لنص المادة -42.
  - جريمة جمع البيانات الشخصية للمعني دون موافقة: وفقا لنص المادة - 43 . (الجمهورية الجزائرية الشعبية الديمقراطية 2015)
- **القانون رقم 18 / 04 المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية:** الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات التكنولوجيا والذي الغى بموجبه قانون رقم 2000 / 03 ، والذي أكد فيه على وجوب عدم مساس استعمال شبكات وخدمات الاتصال الإلكترونية بحفظ الحياة الخاصة للأفراد، (المؤمن 2022، ص66) وقد حدد عقوبات كل من الجرائم التالية:
  - إنتهاك سرية المراسلات الالكترونية: حسب نص المادة - 164.
  - تحويل المراسلات الصادرة عن طريق البريد: حسب نص المادة -165. (الجمهورية الجزائرية الشعبية والديمقراطية 2018)
- **القانون رقم 18 / 07 المتعل ق بتحديد قواعد حماية الشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي:** 2018 والذي هدف من خلاله إلى تحديد قواعد حماية الأشخاص الطبيعيين في مجال معالجة

المعطيات ذات الطابع الشخص ي وذلك في إطار احترام الحياة الخاصة للأفراد. (الجمهورية الجزائرية الشعبية الديمقراطية 2018)

دون أن نسى القانون 05 – 10 الصادر في 2005.06.20 المتضمن الدليل الالكتروني، بالإضافة إلى تدعيم الاجراءات القانونية بآلية تقنية جديدة تتمثل في صدور القانون 16.03 المؤرخ في 2016.06.19 المتضمن البصمات الجنائية في الاجراءات الجزائية لتحديد هوية الاشخاص، كل هذا إلى جانب النصوص القانونية عامة لها علاقة بالجريمة بشكل عام و الإلكترونية بشكل ضمني، مثل قانون الإجراءات المدنية وقوانين الملكية الفكرية و والثقافية، قانون تبيض الأموال وقانون التأمينات، قانون البريد والاتصالات اللاسلكية (بوضياف 2018، ص365–367)، وغيرها من القوانين التي تدعم مجال مكافحة الجريمة الإلكترونية في الجزائر.

الجانب العملي:

لعل الاستراتيجية الجزائرية في تعزيز الأمن السيبراني ركزت على الجانب العسكري وهو ما يسمى بالدفاع الإلكتروني في الاستراتيجيات العسكرية، والذي عرف في الاستراتيجية الجزائرية على أنه: "مراقبة الأنظمة التي تحمي الدولة من كافة التهديدات ، و متابعة حالة تقدم نشاطات تجسيد السياسة الشاملة للدفاع السيبراني الرامية لضمان فعالية الحماية ضد التهديدات السيبرانية، التي تستهدف أنظمة المعلومات ومنظومات الاتصال وكذا منظومة الأسلحة للجيش. (بوغرارة 2018، ص113)

1– المصلحة المركزية لمكافحة الجريمة المعلوماتية(SCLC) :

وهي مصلحة تابعة لمديرية الأمن الوطني، و التي أنشأت سنة 2011 وتعتمد هذه المصلحة على موارد بشرية لها من الكفاءة المهنية ما يؤهلها لتنفيذ مهامها على المستوى الدولي من خلال التعامل مع المصالح المختصة – أنتربول، أفريكوم – أو مصالح الشرطة لكبرى الدول، وعلى المستوى الوطني تتواصل هذه الهيئة مع الشرطة العلمية والمكاتب اللامركزية المختصة في الاجرام (الشرطة القضائية). (بوازدية 2019، ص1280)

2–مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية .(: (CPLCIC)

التابعة للقيادة العامة للدرك الوطني، لا تختلف كثيرا في مهام التحقيق والتحريات في هذا المجال عن نظيرتها التابعة للأمن الوطني سواء محليا أو وطنيا، بل بالعكس يتم التنسيق بينهما تحت المسؤولية المباشرة للنائب العام على مستوى دائرة الاختصاص. (عطية 2019، ص112)

3- المعهد الوطني للأدلة الجنائية وعلم الجرام للدرك الوطني(: (INCC)

التابع للقيادة العامة للدرك الوطني، يعتمد المعهد في أداء مهامه على الخبرة العلمية و التجارب المخبرية الدقيقة لكل الأدلة المتحصل عليها من مكان ارتكاب الجريمة عامة، وهو هيئة تتمتع بالشخصية المعنوية والاستقلال المالي، تتكون من دوائر متخصصة في مجالات مختلفة مثل دائرة الإعلام الألي والإلكتروني. (بوهرين 2021، ص57)

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 حيّز الخدمة ابتداءً من الفاتح جانفي 2009 أما الفترة الممتدة بين 2004 و 2009 كرست لتكوين المورد البشري واقتناء المعدات العلمية والتقنية الضرورية. (عطية 2019، ص113)

4- الهيئة – الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات العلام والاتصال ومكافحته

التي أنشئت سنة 2009 ، بموجب المادة 13 من قانون 09-04، ووضعت تحت السلطة المباشرة لوزير العدل حافظ الاختام، (الجمهورية الجزائرية الشعبية الديمقراطية 2009)، ولم تدخل حيز التنفيذ إلا بعد صدور المرسوم الرئاسي رقم 15-261 المؤرّخ في 2015.10.08 ، من أبرز المهام المنوطة بها:

– استغلال المعطيات المتوفرة بطريقة تسمح بمتابعة كل ما يجري في الفضاء السيبراني من نشاطات غير شرعية وبالتالي توجيه القدرات البشرية والمالية للحد من الثغرات، مع العلم ان هذا المجال أصبح مفتوحا على كل الاحتمالات في ظل التطور السريع لتكنولوجيا الاعلام والاتصال.

– تعزيز التنسيق بين مختلف الفاعلين في الميدان والتشديد على ضرورة التعاون بين القطاعين العام. (حوالف 2021، ص151)

– العمل من أجل خلق إطار مركزي للمعلوماتية على شاكلة وحدة بحث، يتم من خلالها جمع المعطيات والاحصائيات في هذا المجال من أجل التحليل المستمر للتهديدات واقتراح الحلول المناسبة.

– التنسيق والتعاون بين مختلف الأجهزة المنية، المالية والإدارية التي لها علاقة مباشرة بأنشطة تكنولوجيا الاعلام.

– اقتراح الأرضية اللازمة لتجسيد الاستراتيجية الوطنية للوقاية ومحاربة الجرائم الالكترونية والخاص والمجتمع المدني. (دقيش 2022، ص10،11)

5- **مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة :**

والتي أستحدثت بتاريخ 2015.06.11 ، على مستوى دائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي، وأوكلت لها مهمة، حماية المنظومات والمنشآت الحيوية للبلاد ضد كل أنواع الجريمة السيبرانية. (بوغرارة 2018، ص114)

الجانب العلمي:

لا يقل الجانب العلمي من ملتقيات ودراسات وابحاث وندوات أكاديمية، أهمية عن باقي الجوانب التي انتهجتها الجزائر في سبيل مكافحة الجريمة السيبرانية، إذ سعت دائما إلى التذكير بأهميته، مجال البحث العلمي في دعم مجهودات الدولة في اطار الاستفادة من أراء الخبراء والنخبة المثقفة الجزائرية حول الأمن السيبراني ،لذا تسعى جاهدة لعقد مؤتمرات تشخص الواقع وتضع الحلول والتوصيات، كما سعت دائما إلى اتاحة الفرص أمام الهيئات العلمية لتناول هذا الموضوع على اعتبار أن البحث العلمي هو الأخر أحد أهم الخطوط الدفاعية في مجال الامن السيبراني، وفيما يلي جرد لأهم اهذه الفعليات :

- في إطار تجسيد مخطط الاتصال للجيش الوطني الشعبي لسنة 2015-2016، وتحت إشراف السيد الفريق نائب وزير الدفاع الوطني، رئيس أركان الجيش الوطني الشعبي، نظمت مديرية الإيصال والإعلام والتوجيه لأركان الجيش الوطني الشعبي، يوم 21 ديسمبر 2015، بالنادي الوطني للجيش ببني مسوس، ملتقى بعنوان " الجيش الوطني الشعبي ورهانات تداول المعلومة عبر شبكات التواصل الاجتماعي ". (جريدة النهار أونلاين 2015)
- الطبعة الثالثة لملتقى حول الأمن السيبراني والدفاع السيبراني المعنون: " رهانات وتحديات على ضوء التحولات الجديدة المتعددة الأبعاد"، بالنادي الوطني للجيش بني مسوس، بتاريخ 22 ماي 2021. (وزارة الدفاع الجزائري 2021)
- ملتقى حول "الدفاع السيبراني، مكون أساسي للأمن والدفاع الوطني"، بتاريخ 15 ماي 2017. من اجل خلق فضاء نقاش بين مختلف الفاعلين في الفضاء السيبراني على المستوى الوطني لفهم أفضل لرهان الامن السيبراني والدفاع السيبراني وتحسين واثراء المعارف في مجال الوقاية ومكافحة التهديدات السيبرانية وكذا تحديد أثرها على الامن الوطني. (وكالة الأنباء الجزائرية 2022)

* كما نظمت الجزائر الطبعة الثالثة للقمة الإفريقية للأمن السيبراني بالجزائر يومي 16 و17 نوفمبر 2022، حيث أن المشاركين في هذه الطبعة يمثلون خبراء ومختصين في الأمن السيبراني وتكنولوجيات المعلومات والاتصالات، وكذا صناعيين وناشرين وباحثين، إلى جانب أرباب العمل.

- رهانات الأمن السيبراني في الجزائر محور ندوة نظمت بتاريخ 27 مارس 2022 بالجزائر العاصمة بحضور الوزير المنتدب لدى الوزير الأول المكلف باقتصاد المعرفة والمؤسسات الناشئة. (وكالة الأنباء الجزائرية 2022)
- تنظيم ملتقى وطني حول الأمن السيبراني، الموسوم بـ "الإستراتيجية الوطنية للأمن السيبراني: من أجل جزائر صامدة سيبرانيا"، بتاريخ الأربعاء 07 جوان 2023 من طرف وزارة الدفاع الوطني بالنادي الوطني للجيش ببني مسوس/الجزائر العاصمة، حسب ما ورد في موقع وزارة الدفاع الوطني بذات التاريخ.
- والعديد من الملتقيات الوطنية بالجامعات الجزائرية والتي هدفت كلها إلى إيجاد مخارج وسبل حديثة لتعزيز الأمن السيبراني في البلاد، وكمثال نجد : الملتقى الوطني حول –واقع الجريمة الإلكترونية بين مبادئ الحرية وظوابط المسؤولية، الملتقى الدولي الذي نظمته كلية الحقوق، جامعة برج بوعريريج بتاريخ 2017.04.12 تحت عنوان " الاجرام السيبراني، المفاهيم والتحديات. وكذا الملتقى الدولي المزمع عقد 17-18-19 /2022/11 حول التحكيم الإلكتروني وتحديات الأمن السيبراني، بالشراكة بين المركز الاستشاري الافريقي للتحكيم والوساطة بالجزائر والمركز المغاربي –شرق أدنى للدراسات الاستراتيجية ببريطانيا وكلية القانون جامعة الزيتونة ليبيا، والعديد من النشاطات العلمية حلو هذا الموضوع.
- وكذا نشر العشرات من المقالات العلمية والدراسات في المجلات الوطنية والدولية المحكمة، التي تشرح الواقع السيبراني في الجزائر وتحدد الواقع القانوني لها وهو ما نجده في المنصة الوطنية للمجلات العلمية في العديد من المجلات المحكمة وغيرها من المجلات، ونذكر على سبيل المثال لا الحصر (إلهام غازي: "الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري"، مجلة الجيش. العدد: 630)، أيضا كمثال (ساعد بوقرص : الأمن السيبراني مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة)، وغيرها بحيث لا يمكننا حصرها هنا نظرا للحد المطلوب من صفحات الورقة البحثية، ولكثرتها ايضا.
- كما يعد هذا الملتقى الذي نحن بصدد المشاركة فيه إحدى المحاولات الجادة والفاعلة في الجانب العملي، لتدعيم استراتيجية تعزيز الامن السيبراني علميا، من خلال تبادل الأراء والاقتراحات.

جانب التعاون الدولي:

أولت الجزائر جانب التعاون الدولي والاتفاقيات الدولية في مجال الأمن السيبراني أهمية قصوى، كما كانت دائما ملتزمة بنصوص هذه الاتفاقيات سواء في مجال التطبيق العملي أو في مجال نصوصها القانونية، وفيما يلي بعض الأمثلة:

على المستوى العربي نضرب مثال بتوقيع العديد من الاتفاقيات الثنائية والمتعددة الاطراف مع الدول العربية في إطار الاتفاقية العربية لمكافحة الارهاب لسنة 1998. (جامعة الدول العربية 1998)، والاتفاقية العالمية لمكافحة الجريمة المنظمة العابرة للحدود لسنة 2000 و الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، (وزارة العدل 2022) هدفها ضمان أمن المجتمعات العربية في عصر الرقمنة، من خلال التعاون الكلي والجاد في هذا المجال.

في حين شمل التعاون الدولي عدة أمور نذكر منها على سبيل المثال:

1- الندوة الدولية حول الأمن السيبراني المنظمة بالنادي الوطني للجيش، تحت رعاية نائب وزير الدفاع الوطني، رئيس أركان الجيش الوطني الشعبي الفريق قايد صالح، التي تم فيها التأكيد على، أن "مكافحة الجرائم الالكترونية أضحت من بين أولويات الدولة الجزائرية، بتاريخ2022/03/27. (وكالة الأنباء الجزائرية 2018)

2- العمليات التكوينية التي برمجت بالجزائر لفائدة القضاة من 14 إلى 18 فيفري 2021:

- في إطار التعاون مع البرنامج الأوروبي لمكافحة الجريمة السيبيرانيةCyberSud ، يشارك 06 قضاة في ورشة عمل وطنية عبر الانترنت حول "تحضير التقرير السنوي حول وضعية الجريمة المعلوماتية و الدليل الالكتروني"، يوم 17 فيفري 2021.
- في إطار التعاون مع البرنامج الأوروبي لمكافحة الجريمة السيبيرانيةCyberSud ، يشارك 04 قضاة ممارسين رفقة قاض ومهندس في الإعلام الآلي من المديرية العامة لعصرنة العدالة، في ملتقى تقني عبر الانترنت حول" تطبيقات التشفير في مجال الجريمة المعلوماتية و/أو التجريم الرقمي"، من تنظيم المنظمة الدولية للشرطة الجنائية و برنامج العمل الشامل حول الجريمة المعلوماتية الموسعة + GLACY من 15 إلى 25 فيفري 2021، إلى جانب ممثلين عن الشرطة و مكونين من الهيئات المسؤولة على التكوين في المجال. (وزارة العدل الجزائرية 2021)

3- تم التوقيع على مذكرة تفاهم بين المكتب الاممي المكلف بالمخدرات والجريمة والاتحاد الدولي للاتصالات للاستفادة من خبرة هذا الاخير لمساعدة الدول لاتباع الاجراءات الملائمة للحد من المخاطر التي تشكلها الجريمة السيبرانية. (بوازدية 2019، ص1287)

4- تنظيم ورشة عمل حول تطوير قوانين الأمن السيبراني في المجال النووي، من 7 إلى 11 جانفي 2024، في إطار التعاون بين محافظة الطاقة الذرية والإدارة الوطنية للأمن النووي/وزارة الطاقة للولايات المتحدة الأمريكية، حسب ما ورد في موقع محافظة الطاقة الذرية بذات التاريخ.

والعديد من الاتفاقيات والشراكات التي تصب جميعها في مجال جهود الجزائر الجادة في تعزيز الامن السيبراني، كما يتجسد ذلك في الشراكة الجزائرية الاوروبية في مجال محاربة الإرهاب السيبراني

رابعا: النظرة المستقبيلة للجزائر في مجال الأمن السيبراني:

رغم كل المجهودات التي بذلتها الجزائر في سبيل مواجهة الجريمة الإلكترونية على اختلاف أشكالها، من خلال الترسانة القانونية والهيئات الوقائية والرقابية، وكذا جانب التوعية والإرشاد من طرف مختلف الهيئات والمصالح، والتصديق على عديد الاتفاقيات الدولية، إلا أنها لازالت تصنف في مراتب متأخر تطمح للوصول إلى مراتب متقدمة ضمن مؤشر الدول الأكثر مجابهة للجريمة الإلكترونية، إذ تقع في المرتبة 104 عالميا وال11 في منطقة الشرق الأوسط، ، وهذا راجع لعديد المعوقات التي تحول دون محاربة الجريمة الإلكترونية والتي شق منها يتعلق بالجريمة في حد ذاتها وطبيعة الافتراضية التي تسهل من عملية اخفائها، وشق يتعلق بوجود المختصين القادرين على تتبعها والتحكم بها مقارنة بعدد التقنيات الضخم وحجم المعلومات المتزايد، ولنصدق القول أن هذه المعوقات لا تواجه الجزائر وحدها وإنما مختلف بلدان العالم بما فيها هيئة الأمم المتحدة.

وهنا كان على الجزائر وضع رؤية مستقبلية لموضوع الأمن السيبراني بشكل أكثر استعداد وأكثر تقدما وتحديثا خاصة في ظل ظهور أجيال متقدمة من خدمات النت، والتطور المتسارع لملحقاتها الأمر الذي صعب سبل التحكم بها، وعليه يرى الباحثون أن الجزائر بحاجة إلى تطوير البنية التحتية المتعلقة بتكنولوجيا المعلومات والاتصالات، وتطوير المنظومة القضائية والأمنية، وجعلها تتماشى مع التطورات الدولية، إلى جانب أن محاربة الجريمة المعلوماتية في الجزائر مرهونة ببناء القدرات البشرية، وهذا لن يتأتى إلا بوضع برنامج وطني لتطوير مهارات المتخصصين في أمن المعلومات الذين يدعمون المؤسسات العمومية والخاصة، من أجل حماية أنظمتها الحساسة من التهديدات من جهة، وزيادة الوعي والتدريب

في مجال أمن المعلومات لدى مستعملي الإنترنت من جهة ثانية، بالإضافة إلى ضرورة إيجاد آليات تعاون بين مختلف الأطراف المعنية من حكومة ومجتمع مدني وقطاع خاص وأكاديميين ومؤسسات بحثية، مع وضع هذا الاهتمام من الأولويات الاستراتيجية للبلاد.

وفي هذا السياق أكد وزير العدل الجزائري، عبد الرشيد طبي، ن السلطات العليا للبلاد بادرت بإنشاء قطب وطني متخصص في مكافحة الجريمة المعلوماتية لمواجهة المخاطر العديدة لها، خصوصاً على الأنظمة المعلوماتية والحياة الخاصة للأشخاص (ياحي 2022).

كما أن التوجهات العالمية الجديدة تفرض تحقيق خطة التنمية لعام 2030 وأهداف القمّة العالمية لمجتمع المعلومات للفترة ما بعد عام 2015 –wsis+10 – على الدول العربية ، والتي تعد الجزائر من بينها، عدة إلتزامات، منها تنفيذ الخطط العالمية التنموية، (عطية 2019، ص116) ومجابهة التحديات التي تحول دون تنفيذها. وذلك من خلال إبداء الإلتزام، السياسي اللازم وتحديث الإستراتيجيات، لاسيما تكنولوجيا المعلومات والإتصالات، بما يتلاءم مع الأهداف التنموية الجديدة ووفقا الأولويات الدول العربية بما فيهم الجزائر. (العنزي 2017، ص96)

في حين يشكل القطاع الخاص دورا هاما في النظرة المستقبلية لتعزيز الامن السيبراني في الجزائر، وهو ما نلمسه في محاولة السيدة فلة قوار، رئيسة شركة " INTELLIGENT NETWOR" في وضع مشروع أول مركز وطني للتكوين في قضايا الأمن السيبيراني في الجزائر، المعتمد من طرف المنظمات الدولية، والذي يهدف حسبها إلى تعزيز تقنيات الدفاع والحماية ضد مختلف أنواع الهجمات السبيرانية التي تتعرض لها مختلف المؤسسات والبنى التحتية وحتى الأشخاص في الجزائر. (الدور 2022)

خاتمة:

وتبقى الجريمة السيبرانية أكثر أنواع الجرائم تعقيدا وخطرا، إلى جانب صعوبة ضبطها بفعل التحديث الهائل في تقنياتها وأساليبها وأشكالها المتفردة والمتعددة، إلا أن ذلك لم يمنع من محاولات ناجحة دولية ووطنية لمجابهتها والحد من مخاطرها ولو بشكل جزئي، فهي كانت ولازالت تسعى دائما لإجاد الحلول المناسبة من خلال التحري والبحث وتوفير الإمكانيات اللازمة وسن التشريعات المطلوبة. فالجزائر ورغم كونها لاتزال في مراتبة متأخرة دوليا في مواجهة الجريمة الإلكترونية كما أسلفنا الذكر، تبقى تجربتها في تعزيز الأمن السيبراني يُشهد لها، إذ بذلت جهود كبيرة لتوفير أنجع السبل وأحدث الوسائل عسكرية كانت أو مدنية، علمية أو عملية. وما إحباطها لعشرات الهجمات السيبرانية على مؤسساتها الأمنية أو غيرها من المؤسسات، وسعيها لحماية أمن مواطنيها الجسدي والمعلوماتي إلا دليل على ملامح استراتيجية تستحق التثمين كما تستحق إعادة النظر في بعض المواضع التي تبقى مستعصية حتى على كبريات الدول تقنيا.

قائمة المراجع والمصادر:

القوانين والمراسيم:

1- الجمهورية الجزائرية الشعبية الديمقراطية.(فيفري2015).القانون رقم 15 / 04 المتعلق بالتوقيع والتصديق الإلكترونيين." الجريدة الرسمية، (6).

2- الجمهورية الجزائرية الشعبية الديمقراطية.(ماي 2018). القانون رقم 18 / 07 المتعلق بتحديد قواعد حماية الشخاص الطبيعيين في مجال معالجة المعطيات ذات." الجريدة الرسمية، (34).

3- الجمهورية الجزائرية الشعبية الديمقراطية.(2009).قانون 09/04 الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجريدة الرسمية، (47).

4- الجمهورية الجزائرية الشعبية الديموقراطية.(نوفمبر 2018). "قانون العقوبات المعدل." الجريدة الرسمية، (74).

5- الجمهورية الجزائرية الشعبية والديمقراطية.(ماي2018). " القانون رقم 18 / 04 المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية." الجريدة الرسمية، (27).

6- جامعة الدول العربية.(1998).الاتفاقية العربية لمكافحة الارهاب، القاهرة.

الكتب:

1- جبور منى الأشقر.(2013)، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية .

المقالات العلمية:

1- عطية ادريس.(2019)، "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري." المصداقية، 1(1)، الجزائر.

2- العنزي فواز.(أكتوبر، 2017)، أمن المعلومات والقرصنة الإلكترونية." مجلة التقدم العلمي، (99).

3- بارة سمير.(جويلية،2017)،الأمن السيبراني في الجزائر- السياسات والمؤسسات." المجلة الجزائرية للأمن السيبراني، (4).

4- بوازدية جمال.(أفريل،2019)، "الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية " التحديات والافاق المستقبلية"، مجلة العلوم السياسية والقانونية، 10(01).

5- بوضياف اسمهان.(سبتمبر،2018) "الجريمة الإلكترونية والاجراءات التشريعية لمواجهتها في الجزائر." مجلة الأستاذ الباحث للدراسات القانونية والسياسية، (11).

6- بوغرارة يوسف.(2018)، "الأمن السيبراني: الإستراتيجية الجزائرية للأمن و الدفاع في الفضاء السيبيري." مجلة الدراسات الإفريقية وحوض النيل – المركز الديمقراطي العربي،1(3).

7- بوهرين، فتيحة.(2021)، "الجريمة المعلوماتية في التشريع الجزائري." مجلة الحقوق والعلوم الانسانية، 14 (04).

8- حوالف، حليمة، مهاجي فاطمة الزهراء.(2021)،"معالم الجريمة المعلوماتية في القانون الجزائري." مجلة البحوث القانونية والسياسية، 3(16).

9- دقيش، جمال.(2022)، "واقع الجريمة الإلكترونية في الجزائر–دراسة تحليلية للفترة2013–2017." (بحث مقدم)،ملتقى وطني حول واقع الجريمة الإلكترونية بين مبادئ الحرية وظوابط المسؤولية، غليزان، الجزائر .

10- الصحفي، روان بنت عطيه الله.(ماي،2020)، "الجرائم السيبرانية." المجلة الإلكترونية الشاملة متعددة التخصصات، (24).

11- بوقرص، ساعد(جوان،2022)."الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة،" مجلة الأبحاث في الحماية الاجتماعية، 3،(1).

12- سي، محمد عبد المؤمن،قيرة، سعاد.(جوان،2022). "الجريمة الإلكترونية وآليات التصدي لها في القانون الجزائري." مجلة البيان للدراسات القانونية والسياسية، 7(1).

13- الشمري، مصطفى إبراهيم سلمان(2021)." الأمن السيبراني وأثره في الأمن الوطني العراقي." مجلة العلوم القانونية والسياسية، 10(1).

المواقع الإلكترونية:

1- العمليات التكوينية المبرمجة بالجزائر لفائدة القضاة من 14 إلى 18 فيفري 2021. وزارة العدل الجزائرية. (14 فيفري، 2021). *https://www.mjustice.dz*. استرجعت بتاريخ 31 اكتوبر، 2022.

2- وزارة الدفاع الجزائري، (24 ماي، 2021)، *https://www.mdn.dz*، استرجعت بتاريخ31 أكتوبر، 2022.

3- الجيش الوطني ينظم ملتقى حول الجيش ورهانات تداول المعلومة عبر مواقع التواصل الإجتماعي .(21ديسمبر2022). النهار أونلاين .https://www.ennaharonline.com ، استرجعت بتاريخ 31 اكتوبر، 2022.

4- شايب دور، أمال. (28مارس، 2022). الأمن السيبيراني ..خط الدفاع الاول عن خصوصية و معلومات الجزائر .https://elmaghrebelawsat.dz (تاريخ الوصول 6 نوفمبر، 2022).

5- قرة، فارس.(28 08, 2019). الأمن السيبراني .https://political-encyclopedia.org. (تاريخ الوصول 30 10، 2022).

6- ياحي،علي.(مارس،2022). تطوير المنظومة القضائية والأمنية في الجزائر لمواجهة الجرائم المعلوماتية اندبندنت عربية. "https://www.independentarabia.com. (تاريخ الوصول 05 نوفمبر، 2022).

7- وزارة العدل.(2022 (.https://www.mjustice.dz. (تاريخ الوصول 05 نوفمبر، 2022).

10-تنظيم الطبعة الثالثة للقمة الإفريقية للأمن السيبراني بالجزائر يومي 16 و17 نوفمبر القادم..(12 جوان، 2022) .وكالة الأنباء الجزائرية.https://www.aps.d.z . (تاريخ الوصول 3 أكتوبر، 2022).

10- التصيد الإلكتروني (Phishing).(13جانفي2014).البيان.https://www.albayan.ae .(تاريخ الوصول2022/11/11).

11- الندوة الدولية حول الأمن السيبراني: مكافحة الجرائم الالكترونية من أولويات الدولة الجزائرية.(2022/03/27). وكالة الأنباء الجزائرية.https://www.aps.dz .(تاريخ الوصول2022/11/11).