المجلة الجزائرية للسياسة والأمن
ISSN: 2800-1095

المجلد: 2 – العدد: 2 سنة: ديسمبر 2023
ص.ص73-92/

الأمن السيبراني في العقيدة الدفاعية الجزائرية :الفرص والقيود

Cyber Security in the Algerian defensive doctrine: opportunities and restriction

د. شريط نجمة *
[1] جامعة وهران 2 ، (الجزائر)،إيميل : cheriet.Nedjema@univ-oran2.dz

تاريخ الاستلام: 2024-02-02 - تاريخ القبول: 2024-02-22 - تاريخ النشر: 2024-03-10

الملخص :

تهدف هذه الدراسة إلى إبراز أهمية تحقيق الأمن السيبراني في العقيدة الدفاعية الجزائرية التي استدعت من هذه الأخيرة التصدي لخطر السلاح الاستراتيجي الذي يهدد أمنها الداخلي باعتمادها لاستراتيجيات وقائية دفاعية تزامنا مع ما آل إليه التطور التكنولوجي الذي يمثل الحجر الأساس لأي سياسية أمنية أو اقتصادية كانت في ظل تفشي ظاهرة الاستخدام غير الشرعي للفضاء الرقمي " القرصنة الالكترونية "وأشكال جديدة من الحروب الالكترونية" التي باتت تشكل إحدى أهم المخاطر الأمنية التي تهدد الاستقرار في شتى مجالاته الامنية والسياسية والاقتصادية.

الكلمات المفتاحية: الأمن، الأمن السيبراني، العقيدة الدفاعية، السلاح الاستراتيجي، القرصنة.

Abstract:

This study aims to clarify the importance of emphasizing on cyber security in the Algerian defense doctrine that has been calling lately to confront the danger of strategic weapon that threatens its intern security, by using preventive-defensive strategies that

*شريط نجمة ،دكتوراه في العلوم السياسية والعلاقات الدولية ،جامعة وهران 2.

concides With technologic revolution which is the basic for any economic or security policies .on the light of the illegal uses of digital space ,electronic piracy and new kinds of electronic wars which has became one of the most dangerous threats to security and stability in its different domains (politic, economy, security)

Keywords: security, cyber security, defense doctrine, strategic weapon, piracy.

مقدمة:

يعاني المجتمع الدولي منذ نهاية الحرب الباردة من سلسلة تهديدات و تحديات أمنية لا تماثلية زادت من تعقيد المعضلات والمشكلات الأمنية التي عرفها ومن عملية البحث عن الحلول و الآليات لمكافحتها، فقد شكلت تحديا لإستراتيجيات الدّفاعية التقليدية، حيث أدى الاعتماد على التطور التكنولوجي و الثورة التقنية إلى ظهور تهديدات تمس الفضاء السيبراني،و تشل حركة أغلب الميادين الحيوية للوحدة الدولية كما تُعرض أمنها للخطر مما استدعى من الدول أن تولي اهتمام و تجند كل إمكانياتها لتحقيق الأمن السيبراني،باعتباره أحد تحديات الأمن القومي في القرن الواحد والعشرين ،و الجزائر إحدى هذه الدول و التي سعت في السنوات الأخيرة إلى بذل المزيد من الجهود وتفعيل استراتيجيات دفاعية بغية تحقيق الأمن السيبراني.و إعادة صياغة استراتيجيات تتماشى و العهد الجديد المحفوف بالمخاطر و الحروب السيبرانية. وبناء على ذلك نطرح السؤال التالي :

- **إلى أي مدى تؤثر التهديدات السيبرانية على إستراتيجية العقيدة الدفاعية الجزائرية؟**

وتتفرع عن هذه الإشكالية الأسئلة التالية :

- ما هو مفهوم الأمن السيبراني؟ ما هو واقع الأمن السيبراني الجزائري من التهديدات السيبرانية؟ وما هي الجهود المبذولة لتحقيقه؟

تنطلق الدراسة من فرضية مفادها أن غياب الأطر القانونية في المجال السيبراني، وكثرة الثغرات الأمنية، أديا إلى زيادة الهجمات والمخاطر السيبرانية على العقيدة الدفاعية الجزائرية.

وقد اعتمدت الدراسة على المنهج الوصفي التحليلي، الذي يهتم بوصف طبيعة التهديدات اللاتماثلية التي أضحت تشكل خطر أمني على السياسات الأمنية، ومنها الدفاعية .

ومن أجل معالجة هذه الإشكالية ستحاول هذه الورقة البحثية تناول المحاور التالية :

- **ماهية الأمن السيبراني و التهديدات السيبرانية.**
- **و اقع الأمن السيبراني الجزائري .**
- **تحديات تحقيق الأمن السيبراني في الجزائر.**

المبحث الأول: ماهية الأمن السيبراني والتهديدات السيبرانية

اهتمت العديد من مراكز البحث والدراسات المختصة في العلاقات الدولية والدراسات الأمنية بالتهديدات والجرائم السيبرانية ضمن مجال الدراسة،حيث شكلت ولا تزال تحدي للأمن القومي والدولي.فقد اعتبر الباحثين وخبراء الأمن الدولي مجال "الفضاء السيبراني " فضاء جديد للتفاعلات الدولية وتهديداته قد ينجر عنها حروب سيبرانية وهو ما جعل منه المجال الخامس للحروب بعد كل من الحروب التقليدية (البرية ،البحرية الجوية، الفضائية) والذراع الرابعة للجيوش الحديثة، وبهذا انضم الأمن السيبراني Cyber Security إلى حقل الدراسات الأمنية والإستراتيجية ،ودعت الحاجة إلى ضرورة تحديد المفاهيم و المصطلحات المتعلقة بالفضاء السيبراني في إطار العلاقات الدولية.

المطلب الأول: الفضاء السيبراني

اعتبره البعض عبارة عن " البيئة الافتراضية التي تعمل بها المعلومات الإلكترونية و التي تتصل عن طريق شبكات الكمبيوتر" بينا رآه الآخرون على أنه"المجال الذي يتميز باستخدام الإلكترونيات والمجال الكهرومغناطيسي لتخزين و تعديل أو تغيير البيانات،عن طرق النظم المتصلة والمرتبطة بالبنية التحتية الطبيعية "[1] و عرفته الوكالة الفرنسية لأمن أنظمة الإعلام على أنه" فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية "[2]. إلا أن وزارة الدّفاع الأمريكية أوكلت مهمة تعريف الفضاء السيبراني إلى فريقا من المختصين ،و قد استغرقوا أكثر من عام للاتفاق حول مفهومه وإعداد مسودة لـ" الإستراتيجية القومية لحماية الفضاء السيبراني "The National Strategy to Secure Cyberspace الموقعة في 2003[3]،و جاء تعريف الفضاء السيبراني كالآتي" المجال العالمي الذي فيه بيئة من المعلومات تتألف من ترابط شبكة البنى التحتية للمعلومات،التي تتضمن الاتصالات السلكية و اللاسلكية وأنظمة حواسيب ما ضم معالجات و أجهزة تحكم "[4] ، وبذلك يمكن القول بأن الفضاء السيبراني عبارة مجال افتراضي تفاعلي ،يعتمد على عناصر مادية وغير مادية أساسها الأنظمة المعلوماتية المتصلة على مستوى دولي عبر شبكات الإنترنت والتي يتعامل بها المجتمع الدولي بكثافة في شكل تطبيقات.

لم يسلم هذا العالم الافتراضي هو الآخر من تهديدات واختراقات مما استدعى تأمينه، فالتفاعل بين الفضاء السيبراني والتهديدات السيبرانية أنتجا مفهوم جديد في حقل الدّراسات الأمنية " الأمن السيبراني " كبعد جديد ضمن الأجندة الأمنية الدولية .

---

[1] - صباح عبد الصبور عبد الحي ، **استخدام القوة الإلكترونية في التفاعلات الدولية** ،المعهد المصري للدراسات29أكتوبر 2016 ،الرابط :https://eipss-eg.org

[2] -Olivier Kemph ,**inttroduction à la cyberstratégie**,paris ,Economica,2012,p9.

[3] - فرد كابلان ، **المنطقة المعتمة :التاريخ السري للحرب السيبرانية**،ت: لؤي عبد المجيد ،المجلس الوطني للثقافة و الفنون ، الكويت ،مارس 2019،ص 174.

[4] -Peter Warren Singer, Allan A.Friedman ,**Cybersecurity and Cyberwar-what evryone neeeds to Know**, A Thesis Submitted in Fulfillment of the Requirements for M.A in Translation ,Oxford university,2014,pp17-18.

فقد أصبح الفضاء الالكتروني أداة فعالة في التأثير بالنظام الدولي ،و مسألة أمن الفضاء الالكتروني مسألة مهمة و مطروحة بقوة خوفا من تعرض المصالح الإستراتيجية ذات الطبيعة الالكترونية إلى ساحة الصراع الدولي [1].

المطلب الثاني: الأمن السيبراني

يعنى الأمن في الفضاء السيبراني بالإجراءات الحماية ضد التعرض للأعمال العدائية و الاستخدام السيئ لتكنولوجيا الاتصال و المعلومات[2] ،وقد عرفته وكالة الأمن القومي في الولايات المتحدة الأمريكية بأنه جملة المعايير و الإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين بها عبر الاتصالات و لضمان أصالة و صحة هذه الاتصالات"[3]. أما التعريف المعطى له من خلال التقرير الصادر عن الاتحاد الدولي للاتصالات حول "اتجاهات الإصلاح في الاتصالات للعام 2010-2011"،هو مجموعة من المهمات،مثل تجميع وسائل،و سياسات،إجراءات أمنية و مبادئ توجيهية ،مقاربات لإدارة المخاطر وتدريبات و ممارسات فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانية،وموجودات المؤسسات و المستخدمين "[4] وبهذا يشمل الأمن السيبراني التحكم في الوصول الفعلي من قبل الأجهزة إلى الشبكة العنكبوتية و البيانات المتاحة فيها، فضلا عن حمايتها ضد الضرر الذي قد يحدث جراء ذلك النفاد و الوصول [5].

مما سبق يتضح أن الأمن السيبراني هو مجموع الآليات والأطر القانونية والهياكل التنظيمية وجهود خلايا الدفاعية والأمنية الوطنية والدولية التي من شأنها العمل على حماية مصالح الفواعل الدولية وغير الدولية من المخاطر والتهديدات

---

[1] - صباح عبد الصبور عبد الحي ، **المرجع السابق**.

[2] -Martin C.Libicki,**Conquest in Cyberspace :National Security and Information Warface** ,New york,Combridje university press,2007,p1.

[3] - عادل عبد الصادق ،"أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني" ، **المركز العربي للأبحاث الفضاء الالكتروني** ،7جوان 2018، ص 15.

[4] - منى الأشقر جبور ،**السيبرانية هاجس العصر**،المركز العربي للبحوث القانونية و القضائية ،جامعة الدول العربية ،ص 26.

[5] - حسين باسم عبد الأسير ، "تحديات الأمن السيبراني "،**مركز الدراسات الإستراتيجية** ،2018.

والجرائم السيبرانية التي تفتك بالفضاء السيبراني و الحد منها، والتي تشكل خطرا ليس على أنظمة المعلومات فحسب بل على الأمن القومي و الدولي .

أ- أبعادالأمن السيبراني: تعددت أبعاد الأمن السيبراني بتعدد الميادين التي أضحت تعتمد بقوة على الفضاء السيبراني

- فالبعد العسكري : يعد من أكثر الأبعاد التي تسعى الدول لتأمينه من خطر التهديدات السيبرانية.حيث بات الجناح العسكري يعتمد بشكل كبير على تقنيات الثورة التكنولوجية ،من خلال التواصل عبر الشبكات العسكرية و تبادل المعلومات و البيانات والأوامر،وإصابة الأهداف عن بعد[1]و إعداد الخطط الإستراتيجية و الدفاعية ،فمهمة تحقيق الأمن السيبراني في الجانب العسكري باتت ضرورة نظرا للحجم الخطر الذي يمكن أن يحدثه الاختراق من تدمير لقواعد البيانات العسكرية أو قطع الاتصال بين القيادة والوحدات العسكرية فضلا عن إمكانية التحكم في بعض الأسلحة وخروجها عن السيطرة (طائرات بدون طيار،صواريخ موجهة...)[2]، ويشكل بهذا خطرا على الأمن القومي.

- البعد الاقتصادي: يعد المجال الاقتصادي من أكثر المجالات تعرضا للهجمات والتهديدات السيبرانية نظرا لحجم التبادلات الاقتصادية الدولية خاصة في التعاملات المالية و التجارية و اعتمادها بشكل كبير على شبكة الإنترنت في تسييرها .

- البعد السياسي: لم يسلم المجال السياسي هو الآخر من التهديدات والهجمات السيبرانية و التي وصلت إلى حد الحروب السيبرانية وسباق التسلح السيبراني، وتبادل القرصنة في الملفات والقضايا الحساسة فقد أحدث الاعتماد على الفضاء السيبراني ثورة على مفاهيم علم السياسة (القوة السيبرانية والردع السيبراني و غيرها) كما أثر في آليات التجسس بين الدول والتي باتت تعتمد أكثر على القرصنة،إذ تعتبر القرصنة أهم أداة تستخدمها الدول للتجسس، وعموما تصل هذه الدول إلى المعلومات من خلال الثغرات الرقمية التي ترغب الحكومات والشركات في حمايتها ،وبالإضافة إلى عملية القرصنة

[1] - إسماعيل زروقة ،"الفضاء السيبراني و التحول في مفاهيم القوة و الصراع "،**مجلة العلوم القانونية والسياسية** ،المجلد 10، العدد 01،أفريل 2019، ص 1022.

[2] - **المرجع نفسه** ،ص 1022.

تحاول جهات فاعلة التأثير على رأي العالم من خلال نشر أخبار كاذبة [1]،و في بعض الحالات،تحدث الاختراقات الحكومية بالتزامن مع حملات الترويج[2].

- البعد الاجتماعي : فتح التواصل الالكتروني الباب عاليا وجعل من القيم الاجتماعية و الثقافية و التقاليد و العادات عرضة للاختراق والتهديد مقابل غزو ثقافات أخرى منتهكة لمعتقدات و القيم المميزة لمجتمع معين والأمر الأكثر خطورة هو حجم التأثير المسلط على بعض الهويات المشكلة للمجتمع والذي ينجر عنه تهديد للسلم الاجتماعي[3] وفي نفس السياق يأتي التشديد من قبل المنظمات والهيئات الدولية على نشر ثقافة الأمن في الفضاء السيبراني وضرورة تعاون المجتمع بكل مكوناته على تحقيقه وضمانه سواء ما يتعلق بالخدمات أو التأثير السلبي على أخلاقيات المجتمع .

- البعد القانوني : دعت الحاجة لتشريع قانوني يحمي الأفراد والمجتمع من الاختراق السيبراني و كذلك يواكب التطور الحاصل في المجتمع الإنساني بحماية بياناته الشخصية و حقه في إنشاء مدونة إلكترونية ،وصيانة حقوقه الملكية الفكرية على شبكة الانترنت ،و كذلك ضرورة تفعيل تعاون دولي من أجل بناء أطر وهياكل قانونية تهتم بفض النزاعات الدولية على مستوى الفضاء السيبراني و رصد ومعاقبة منتهكيه.

ب- الأمن السيبراني والأمن القومي:

باتت مسألة تحقيق الأمن في مجال الفضاء السيبراني ،مسألة بالغة الأهمية وتطرح بقوة على أجندة الأمن والدفاع،نظرا لخطورة التهديدات السيبرانية (الحروب السيبرانية ، الجوسسة ، الإرهاب السيبراني ....) والتي أضحت تؤرق الدول بشكل خاص وتضعف من قدراتهم الدفاعية والإستراتيجية،ومن هذا المنطلق أصبح الباحثون في العلاقات الدولية والحقول المعرفية المختصة " الدراسات الأمنية والإستراتيجية يركزون

---

[1] - هاكان تانريفيردي ،"هكذا تخلق الهجمات الإلكترونية المشاكل السياسية،زود دويتشه تسايتونغ"، **نون بوست** ،2018/10/1 ،الرابط :https://www.noonpost.com/content/24990

[2] - **المرجع نفسه**.

[3] - سمير بارة ، "الأمن السيبراني Cyper Security في الجزائر : السياسات و المؤسسات" ، **المجلة الجزائرية للأمن الإنساني** ، العدد الرابع ، جويلية 2017،ص 262.

بشكل متزايد حول أثر التكنولوجيا على الأمن القومي و الدولي.وقد تنبهت الدول الكبرى والمنظمات الدولية باكرا من حجم مخاطر الهجمات الالكترونية وخاصة منذ تعرض استونيا عام 2007 لهجمات الكترونية شاملة عصفت بالمرافق الحيوية في البلاد، الأمر الذي حدا بحلف شمال الأطلسي " الناتو" إلى تطوير سياسة للردع الالكتروني[1] في إطار إستراتيجية الأمن السيبراني،ومنذ ذاك الحين ،سعت الدول إلى تجنيد خبراء في جميع الهياكل وخاصة بميدان الدفاع والجيش لرصد التهديدات السيبرانية و ردعها.

المطلب الثالث: التهديدات السيبرانية

تلك الهجمات التي تتم باستخدام آليات و شبكات الكترونية كالانترنت وأجهزة الحواسيب الآلية- وتهدف إلى إلحاق الضرر بأجهزة أو شبكات الكترونية أو سرقة المعلومات الموجودة عليها[2] ،أما الهجمات السيبرانية فهي كل فعل يقوض من قدرات وظائف شبكة الكمبيوتر ،فهدف أنظمة المعلومات هو إتاحة المعلومات وضمانة سلامتها[3].

وقد ينجر عن تلك التهديدات السيبرانية صراع بين الفواعل الدولية وغير الدولية(منظمات إرهابية وغيرها) في الفضاء السيبراني تصل إلى حد الحروب السيبرانية ، والتي تختلف كثيرا عن نمط الحروب التقليدية و أدواتها، فالحرب السيبرانية هي التغلغل في شبكات الحواسيب في دولة عبر شبكة الانترنت وحواسيب التابعة لدولة أخرى أو منظمة ما و توصف هذه الأنشطة الجارية في هذا الخصوص بالهجوم الالكتروني،وتجري الهجمات السيبرانية بين الدول لثلاث أغراض رئيسية :التجسس والتخريب والتلاعب

---

[1] - أشرف محمد كشك، "الأمن السيبراني والأمن الوطني :رؤية إستراتيجية "،**مركز البحرين للدراسات الإستراتيجية و الدولية و الطاقة** ،جريدة أخبار الخليج ،2019/9، الرابط :-http://www.akhbar alkhaleej.com/news/article/1182104

[2] - نوران تسفيق، "أشكال التهديدات الإلكترونية ومصادرها ،دراسات مكافحة الإرهاب" ، **المركز الأوروبي** ،29يناير2020، الرابط : https://www.europarabct.com.

[3] - رغدة البهي ، "الردع السيبراني : المفهوم و الإشكاليات و المتطلبات" ،**المركز العربي للأبحاث الفضاء الإلكتروني** ،مفاهيم إستراتيجية، 17أغسطس 2017.

[1]،ومن هذا المنطق سعت كل الدول إلى تجنيد قدراتها الدفاعية لحماية مصالحها في الفضاء السيبراني وتفعيل آلية الأمن السيبراني في عقيدتها الدفاعية لردع التهديدات والمخاطر السيبرانية ، ومن بينها الجزائر .

أ- الجريمة السيبرانية:

لم يتم الإجماع على تعريف موحد للجرائم السيبرانية فمنهم من ينظر إلى موضوع الجريمة ومنهم من ينظر إلى الوسيلة المستعملة لارتكابها[2]، إلا انه يقصد بها مجموعة من الأفعال غير القانونية المرتكبة عبر أجهزة إلكترونية وشبكات الانترنيت والتي تهدف إلى الإضرار بالأفراد أو المؤسسات من خلال الولوج إلى النظم المعلوماتية الخاصة بهم[3] .

ب- العقيدة الأمنية:

والتي تمثل تصورا أمنيا يحدد المنهجية التي تقارب بها الدولة أمنها، كما يحدد كذلك أفضل السبل لتحقيقه، وعليه عادة ما تكون مرجعية هذه العقيدة عبارة عن أطروحات نظرية تتبناها الدول وصناع القرار فيها، كما يمكن أن تأخذ صبغة أيديولوجية إذا وصلت حد النظام الفكري المتجانس والمتناغم الذي يوفر تفسيرات معينة للواقع ويترتب على ذلك تبني القوى النافذة في المجال الأمني لهذه التفسيرات والرؤى[4].

المبحث الثاني: واقع الأمن السيبراني في الجزائر

أضحى الاختراق السيبراني هاجس يؤرق كل الدول و خاصة بعد أحداث الحادي عشر من سبتمبر عام 2001، و تمكن الحركات الإرهابية من إيجاد أرضية جديدة تهدد

---

[1] - الحرب السيبرانية ،"تهديدات حقيقية من العالم الافتراضي "،**تقارير** ،أنقرة ،2019/03/15.

[2] - مهدي رضا، "الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري"،**مجلة إليزا للبحوث والدراسات** ، المجلد 06، العدد 02، 2021/12/15، ص113.

[3] - نادية لاكلي، "الجريمة السيبرانية في الجزائر والعقوبات المقررة لها"،**مجلة الإجتهاد القضائي**، المجلد15، العدد01، 30 مارس 2023، ص259.

[4] - عبد النور بن عنتر. **البعد المتوسطي للأمن الجزائري، الجزائر، أوروبا والحلف الأطلسي**، المكتبة العصرية للطباعة،الجزائر، 2005 ، ص41.

بها الأمن القومي و الدولي ، فسارعت كل الدول ومنها الجزائر لبذل جهود في هذا الفضاء وتبني الأمن السيبراني في إستراتيجيتها الدفاعية و الأمنية .

المطلب الأول: ميكانيزمات الإستراتيجية الدفاعية الجزائرية

حاولت قيادة الدفاع والجيش الوطني مراجعة إستراتيجيتها وإدراج آليات وميكانيزمات تماشيا مع التهديدات والمخاطر الجديدة ،من خلال تخصيص آليات قانونية ومؤسساتية لرصد التهديدات والجرائم الالكترونية ومكافحتها ،والحد من انتشارها ،وقد أكد اللواء شريف **زراد** بوزارة الدفاع الوطني "أنه في ظل تطور تحديات الأمن السيبراني نتيجة التطور العلمي الكبير الذي بات يشبه السباق نحو تكنولوجيا أسرع وأدق وأحدث، تأتي حماية الأنظمة والبنية القاعدية لتكنولوجيا الإعلام و الاتصال على رأس أولويات القيادة العليا للجيش الوطني الشعبي ،التي تواصل بذل المزيد من الجهود الرامية إلى تعزيز أمنها السيبراني فضلا عن التعاون مع الهيئات الوطنية و الدولية لضمان تأمين أفضل لفضائها السيبراني "[1]. وقد اعتمدت القيادة العليا لوزارة الدفاع الوطني في بلورة إستراتيجيتها الدفاعية القائمة على تحقيق الأمن السيبراني بالتركيز على الآليات والميكانيزمات التالية :

أ- الجانب القانوني : سارع المشرع الجزائري إلى بناء أطر قانونية لحماية و تأمين البنى التحتية للفضاء السيبراني،ومواجهة التحديات والجرائم الالكترونية وتأثيرها على أمن الأشخاص والممتلكات و الأمن الوطني.من خلال مواد كفلها دستور عام 1996 والذي تم تعديله ليتماشى مع التهديدات الجديدة ،حيث تضمنت مواده " المادة 38-44" حماية الحريات و الحقوق الأساسية للمواطن [2]. وكذلك تعديل واستحداث قواعد في "قانون العقوبات" لمحاربة الجريمة الالكترونية ، فتناول القانون رقم 04-15 المعدل في فقرته السابعة مواد قانونية تتضمن المساس بالأنظمة المعالجة الآلية للمعطيات، ومعاقبة كل

[1] - وزارة الدفاع الوطني ،"تطور التهديدات السيبرانية و طرق الأمن السيبراني والدفاع السيبراني" ،"ملتقى الثاني -الأمن و الدفاع السيبراني" ،**النادي الوطني للجيش** ،الجزائر ،25-26مارس 2019.

[2] - القانون رقم 16_ 01 المؤرخ في 6-3-2016، **الجريدة الرسمية**، 2014.

من يخل عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات[1] ،أمّا القانون رقم 09-04 لسنة 2009 فتضمن قواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها و كذلك مراقبة الاتصالات الإلكترونية للوقاية من أفعال الاعتداء و التخريب .

ب- الجانب المؤسساتي : استدعت الإجراءات القانونية ضرورة إنشاء أجهزة وهياكل مؤسساتية تسهر على مواجهة التهديدات الالكترونية و مكافحتها ،و تمثلت بـ:

- **مركز الوقاية من الجرائم الإعلام الآلي و الجرائم المعلوماتية للدرك الوطني:** أنشئ هذا المركز في 2008، لهدف تأمين منظومة المعلومات لخدمة الأمن العمومي ،هو بمثابة مركز توثيق، وتحليل معطيات والبيانات للجرائم المعلوماتية المرتكبة ، و محاولة تحديد أصحابها، مقره ببئر مراد رايس [2].
- **المصلحة المركزية لمكافحة الجريمة المعلوماتية (SCLC):**

أنشأت مصالح الأمن المصلحة المركزية لمكافحة الجريمة المعلوماتية سنة 2011، استجابة لمطلب الأمن المعلوماتي،و تعتمد هذه المصلحة على موارد بشرية لها الكفاءة المهنية و 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 العملية والمكاتب اللامركزية المختصة في الإجرام (الشرطة القضائية)[3] .

---

[1] - بارة سمير ، **المرجع السابق** ،ص 264.

[2] - بوغرارة يوسف،"الأمن السيبراني: الإستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني"،**مجلة الدراسات الإفريقية و حوض النيل**،المجلد الأول – العدد الثالث ،سبتمبر 2018، ص 111.

[3] - جمال بوازدية ،"الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية " التحديات والآفاق المستقبلية "،**مجلة العلوم القانونية و السياسية** ، المجلد 10، العدد01، أفريل 2019،ص 1280.

- **المعهد الوطني للأدلة الجنائية و علم الإجرام للدرك الوطني (INCC) :** وهو تابع للقيادة العامة للدرك الوطني، يتكون من إحدى عشر دائرة متخصصة في عدة مجالات متباينة .يعتمد في أداءها لمهامها على الخبرة العلمية والتجارب المخبرية الدقيقة لكل الأدلة المتحصل عليها من مكان ارتكاب الجريمة عامة ،من أجل تنوير العدالة و توجيه الجهات الأمنية كلما تعلق الأمر باستكمال التحقيق .[1]

المطلب الثاني: الجهود الأمنية لمكافحة التهديدات السيبرانية

منذ أحداث الحادي عشر من سبتمبر عام 2001، أولت الجزائر في إستراتجيتها الأمنية و الدفاعية اهتماما بالغا بالإرهاب السيبراني ،خاصة أنها عانت طويلا من الحركات الإرهابية وتهديدها لأمنها القومي ، فبات تأمين الفضاء السيبراني من خطر تطرف هذه الحركات إحدى المهمات التي أوكلت لجهاز الدفاع ، وهذا ما أكده اللواء مناد نوبة القائد العام للدرك الوطني في كلمته بمناسبة افتتاح الندوة الدولية حول " الأمن السيبراني" ،قائلا:" **إن الإرهاب الإلكتروني بات من أخطر الجرائم التي تستهدف الجزائر،من خلال تنامي مظاهر الترويج لكل أشكال العنف والإرهاب والتطرف باستعمال أحدث التقنيات التكنولوجية خاصة شبكات التواصل الاجتماعي والمنتديات الالكترونية ..."**[2]، وقد تحدث "جاك دريدا" عن الحرب الجديدة ،و دور الحركات الإرهابية فيها بالقول لقد تحول الإرهاب إلى خطر مجهول ويهدد الجميع لقدرته الفائقة على التدمير ،فلم يعد عن طريق القنابل والتفجيرات وإنما أصبح يتم على الصعيد الرقمي بالهجوم الالكتروني واختراق أنظمة المعلومات والتشويش[3]. وفي هذا السياق ،طالبت الجزائر بصياغة ميثاق دولي يضبط ويقنن النشر في وسائل التواصل الاجتماعي حتى لا يستخدمها الإرهابيون كمنبر لنشر

---

[1] - جمال بوازدية ،**المرجع السابق** ،ص 1280.

[2] - بن مرزوق عنترة ،ا"لأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية"، ص 68.

[3] - ريهام عبد الرحمن رشاد العباسي، "أثر الإرهاب الالكتروني على تغير مفهوم القوة في العلاقات الدولية ،دراسة حالة " تنظيم الدولة الإسلامية "،**المركز الديمقراطي العربي** ،24جويلية 2016، الرابط:https://democraticac.de/?p=34528 .

أفكارهم ، بسبب سهولة سيطرة تلك الحركات المتطرفة و الإرهابية على الفضاء السيبراني ، كما سعت إلى تطوير قدرات جهاز الشرطة في مجال مراقبة التكنولوجيا الرقمية و الانترنت،بتدريب فرق متخصصة لملاحقة المتطرفين على الشبكة و مراقبة كل ما ينشر من بيانات ومعلومات يمكن أن توجه الرأي العام من الشباب[1] .

واعتمدت مصالح الأمن الوطني في دفاعها السيبراني على إستراتيجية متكاملة بين الوحدات العسكرية والأمنية : فتوجهت الإستراتيجية العسكرية الجزائرية لتحقيق الأمن السيبراني بتكثيفها لأجهزة مراقبة الأنظمة لتحمي الدولة من كافة التهديدات ،ومتابعة حالة تقدم نشاطات لتجسيد السياسة الشاملة للدفاع السيبراني الرامية لضمان فعالية الحماية ضد التهديدات السيبرانية التي تستهدف أنظمة المعلومات ومنظومات الاتصال وكذا منظومة أسلحة الجيش[2]،كما استحدثت "مصلحة الدّفاع السيبراني ومراقبة أمن الأنظمة "على مستوى الاستعمال والتحضير لأركان الجيش الوطني الشعبي، بهدف تأمين وحماية المنشآت الجوية للقوات المسلحة الجزائرية ضد أي تهديد سيبراني [3].

تبنت الإستراتيجية الدفاعية الجزائرية تنشيط الدفاع الوقائي الالكتروني من خلال:

- الكشف المبكر عن الهجمات في وقتها الحقيقي والهجوم الالكتروني الاستباقي ، وكذلك إستراتيجية التضليل والإخفاء والخداع [4].هذا بالإضافة إلى مبادرة الجزائر للمشاركة في فعاليات المؤتمرات والاجتماعات والملتقيات الدولية القائمة على تجنيب

---

[1] - فتحي بولعراس ،"مداخل متعددة : الدرس الجزائري في تفكيك التطرف ومحاربة الإرهاب" ،**المستقبل للأبحاث والدراسات المتقدمة** ،2 نوفمبر 2017،الرابط : https://futureuae.com/ar/Mainpage/Item/3401.

[2] - نوارة باشوش ، "الجيش يدخل في حرب الفضاء الإلكتروني ومكافحة الجوسسة" ، **الشروق** ،يوم 2-8-2018، الرابط :https://www.echoroukonline.com

[3] - بوغرارة يوسف ،**المرجع السابق** ،ص 114.

[4] - إيهاب خليفة ،" تنامي التهديدات السيبرانية للمؤسسات العسكرية" ،**المستقبل للأبحاث والدراسات** ،أبو ظبي ،2017ص 53.

ومنع استعمال الفضاء الالكتروني ووسائله للإرهاب و الدّعاية له بغية تبادل الخبرات والتقنيات الدولية . فبالرغم من محاولة تطوير الآليات الدفاعية لمواجهة الإرهاب السيبراني إلا أنه ليس التهديد الوحيد الذي تعاني منه المنظومة الأمنية الدفاعية الجزائرية ،ففي دراسة لشركة "McAfee" الخاصة بأمن المعلومات لعام 2018،احتلت الجزائر صدارة الدول العربية،فجاءت في المركز 14 عالميا،وقد أحبطت " KASPERSKY" فيها 95 ألف هجمة الكترونية، وقد سبق و صنفتها الشركة أكثر بلد مهدد سيبرانيا حول العالم بنسبة هجمات طالت44 بالمئة من المستخدمين [1] ،فعام2018 كان حافلا بالجرائم الالكترونية ،بسبب ازدياد اعتماد الحكومة الجزائرية على الفضاء السيبراني في تسيير معاملاتها الدولية وميادينها الحيوية ،وتربص قراصنة المعلوماتية بها باستخدام أدوات أكثر فتكا، والتي قد تهدف للتلاعب بالرأي العام و إثارة الكراهية العرقية و الدينية وكذلك لسرقة معلومات و بيانات مهمة و توقيف المرافق الحيوية للبلد.

المبحث الثالث : تحديات تحقيق الأمن السيبراني وسبل تحقيقه في الجزائر

سعت الهياكل الأمنية في مختلف الميادين، العمل على تحقيق الأمن السيبراني بالرغم من حجم التحديات المتزايدة، والتي فرضتها التكنولوجيا المتطورة، بحيث سمحت للكثير من الفواعل المهددة ومنها المنظمات الإرهابية، للترويج لأفكارها المتطرفة وتحقيق إستراتيجيتها وخططها المهددة لاستقرار وأمن الوطن ووحدته، لذا فقد بات من الضروري تسخير جميع الأجهزة الأمنية، للبحث عن السبل الكفيلة لتحقيق الأمن السيبراني.

المطلب الأول: عوائق تحقيق الأمن السيبراني

يعترض عمل أجهزة الأمن وفروعها المختلفة في سبيل تحقيق إستراتجيتها الأمنية في الفضاء السيبراني جملة من العوائق و التحديات، نذكر منها :

[1] - "الجزائر الأولى عربيا ،أكثر الدول تعرضا للهجمات الالكترونية في العالم" ،ساسه **Post**، 13جوان 2018، على الرابط :

- أبرز عائق تواجهه أجهزة الأمن لتحقيق الإستراتيجية الدفاعية المبنية على الأمن السيبراني هو غياب مواد قانونية متخصصة بكل حالة من الجرائم السيبرانية والتي يمكن أن تسهل أداء المهام بملاحقة المتربصين و المهددين لأمن الأفراد و الدولة ، حيث تجد الأجهزة الأمنية صعوبة في تجسيدها على الأرض.

- ارتفاع حجم التهديدات السيبرانية وتمكن قراصنة الفضاء السيبراني من تطوير أدواتهم آلياتهم و التسبب بأضرار بالغة تسببت بخسائر مادية مقارنة بإجراءات الجهاز الأمني لتحقيق الأمن السيبراني .

- غياب التنسيق بين أجهزة الأمنية الوطنية و الدولية ،مما يجعل مهمة تأمين الشبكة من القراصنة و الإرهاب الإلكتروني الدولي مهمة صعبة ،هذا بالإضافة إلى ما يحمله الفضاء السيبراني من صراع السيبراني والحروب الالكترونية بين الوحدات الدولية .

- ضعف التوعية الأمنية من قبل الأجهزة الأمنية بمفهوم الأمن السيبراني لمستخدمي شبكة الانترنت ، ما قد يعرضهم للانتهاك والابتزاز بسبب ضعف التدابير اللازمة و الاحتياطات الأمنية .

- تعدد الفواعل الدولية والتي تشكل تهديد للفضاء السيبراني من حركات إرهابية ودول معادية و قراصنة الفضاء .

المطلب الثاني :سبل تحقيق الأمن السيبراني الجزائري

تعد مسألة حماية وتحقيق الأمن السيبراني من المسائل المهمة والمعقدة والتي باتت تشغل كل أجهزة الدولة الأمنية والسياسية والاقتصادية، وغيرها من الميادين الحساسة والمؤثرة في قوة الدولة، حيث بات الخطر السيبراني يشكل أكبر تهديد لأمن الدولة، ويعود ذلك لقدرة الفواعل الخارجية المهددة من التسلل، وتمكنها من التكنولوجيا لتحقيق أهدافها بكل سلاسة، لذا فمن الضروري العمل لإيجاد آليات وسبل لتحقيق الأمن السيبراني والتي تتمثل في:

1- تكوين نخب وطنية مختصة بمجال الأمن السيبراني ،وتكثيف الملتقيات الوطنية و الدولية والتي من شأنها الاستفادة من تجارب الدولية وخبراتهم في مكافحة التهديدات السيبرانية .

2- بناء قواعد قانونية تتناسب مع كل حالة من التهديدات السيبرانية ،وتفعيلها على أرض الواقع وتطبيقها بصرامة حتى لا يفلت المنتهك من العقاب .

3- بناء منظومة الكترونية دقيقة ومتطورة لمنع الهجمات الالكترونية التي تستهدف مفاصل الدولة المختلفة لاسيما المتعلقة بالأمن الوطني العسكرية منها والمدنية كالنشاط المصرفي و المالي و المؤسسات الأخرى [1].

4- مسايرة التطور التكنولوجي بتجديد التقنيات وامتلاك كل الأسلحة الالكترونية والتي من شأنها رصد التهديدات السيبرانية قبل وقوعها ومراقبة المنتهكين والمهددين لأمن الأفراد و المؤسسات و الأمن القومي.

الخاتمة:

لم يعد الأمن يتعلق بحماية الحدود الإقليمية للوحدة الدولية وبقدراتها العسكرية فقط ،فنهاية الحرب الباردة وموجة التهديدات اللاتماثلية ،أظهرت متغيرات جديدة غيرت من مفهوم الأمن والقوة في العلاقات الدولية ، وأصبح مفهوم الأمن واسع ليشمل ميادين لم تكن تشكل خطرا على أمن الدولة ، وبات تأمين الفضاء السيبراني للدولة أحد أهم الأهداف التي تسعى لتحقيقها .وبلوغ الأمن السيبراني أحد أهم أهداف الإستراتيجية الأمنية و الدفاعية نظرا لقوة تأثيره على الأبعاد الأخرى للأمن .

ومن هنا فإن الجهود المبذولة من قبل الجهاز الأمني والدفاعي الجزائري بغية تحقيق الأمن السيبراني تبقى ضئيلة بالنظر لحجم التهديدات السيبرانية التي تحيط بالجزائر من جهة وتعدد فاعليها ومن جهة أخرى التطورات التكنولوجية المتسارعة

[1] - موسى محمد آل طويرش ،الصراع السيبراني – مفهومه و أثره في العلاقات الدولية ،**المؤتمر الفصلي لكلية العلوم السياسية بجامعة المستنصرية** ، 2019/2/27، العراق ،ص 4.

والثغرات السيبرانية التي تسهل الأمر على قراصنة الفضاء ليحكموا السيطرة و التهديد ، مما يزيد مهمة تحقيق الأمن تعقيدا و صعوبة ،من تم فإنه يقع على عاتق الجهاز الأمني والدفاعي مهمة بذل المزيد من الجهود واستحداث سياسات أمنية تتماشى مع التطور التكنولوجي وحجم التهديدات السيبرانية و كذلك تبني مقاربات إستباقية و تفاعلية.

قائمة المراجع:

1-الكتب:

1-عادل عبد الصادق ،**أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني** ، المركز العربي للأبحاث الفضاء الالكتروني، القاهرة ،7جوان 2018.

2-عادل عبد الصادق ، **الفضاء الإلكتروني والعلاقات الدولية :دراسة في النظريةوالتطبيق**، المركز العربي لأبحاث الفضاء الإلكتروني، ط3، القاهرة، 3جوان 2016.

3- عبد النور بن عنتر. **البعد المتوسطي للأمن الجزائري، الجزائر، أوروبا والحلف الأطلسي**، المكتبة العصرية للطباعة،الجزائر، 2005.

4-منى الأشقر جبور ،**السيبرانية هاجس العصر**،**المركز العربي للبحوث القانونية والقضائية**،جامعة الدول العربية ،2016 .

5-فرد كابلان ،**المنطقة المعتمة :التاريخ السري للحرب السيبرانية** ، ت: لؤي عبد المجيد ، المجلس الوطني للثقافة و الفنون و الآداب ، الكويت ، مارس 2019.

2- المقالات :

1-إسماعيل زروقة ،الفضاء السيبراني والتحول في مفاهيم القوة والصراع ،**مجلة العلوم القانونية و السياسية** ،المجلد 10، العدد 01،أفريل 2019.

2-القانون رقم 16_ 01 المؤرخ في 6-3-2016، الجريدة الرسمية 2014.

3-إيهاب خليفة ، تنامي التهديدات السيبرانية للمؤسسات العسكرية ،**المستقبل للأبحاث و الدراسات** ،أبو ظبي ،2017.

4- بارة سمير ،الأمن السيبراني Cyper Security في الجزائر : السياسات و المؤسسات ، **المجلة الجزائرية للأمن الانساني** ، العدد الرابع ، جويلية 2017.

5-بن مرزوق عنترة،حرشاوي محي الدين ،الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية،**مجلة الحقوق والعلوم السياسية**،2017.

6-بوغرارة يوسف،الأمن السيبراني: الإستراتيجية الجزائرية للأمن و الدفاع في الفضاء السيبراني،**مجلة الدراسات الإفريقية و حوض النيل**، المجلد الأول – العدد الثالث ،سبتمبر 2018.

7-جمال بوازدية ،الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية " التحديات والآفاق المستقبلية "،**مجلة العلوم القانونية والسياسية** ، الجزائر ،المجلد 10، العدد01، أفريل 2019.

8-حسين باسم عبد الأسير ، تحديات الأمن السيبراني ،**مركز الدراسات الإستراتيجية** ،ماي 2018 ،الرابط : https://rb.gy/hios4x.

9-رغدة البهي ، الردع السيبراني : المفهوم والإشكاليات والمتطلبات ،مجلة العلوم السياسية والقانون،**المركز العربي للأبحاث الفضاء الإلكتروني** ،العدد1، 17أغسطس 2017.

10- مهدي رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري،**مجلة إليزا للبحوث والدراسات** ، المجلد 06، العدد 02، 2021/12/15.

11- نادية لاكلي، الجريمة السيبرانية في الجزائر والعقوبات المقررة لها،**مجلة الاجتهاد القضائي**، المجلد15، العدد01، 30 مارس 2023.

3- المو اقع الالكترونية الأكاديمية:

1- أشرف محمد كشك، الأمن السيبراني والأمن الوطني :رؤية إستراتيجية ،مركز البحرين للدراسات الإستراتيجية و الدولية و الطاقة ،جريدة أخبار الخليج ،2019/9، الرابط: http://www.akhbar-alkhaleej.com/news/article/1182104

2- الجزائر الأولى عربيا ،أكثر الدول تعرضا للهجمات الالكترونية في العالم ،ساسه Post، 13جوان 2018، على الرابط :https://rb.gy/93vi18 .

3- الحرب السيبرانية ،تهديدات حقيقية من العالم الإفتراضي ،تقارير ،أنقرة ،2019/03/15،الرابط :https://rb.gy/bt07ks .

4- عادل عبد الصادق ، أنماط الحرب السيبرانية و تداعياتها على الأمن العالمي ،بوابة الأوان،22جوان 2017،الرابط :https://rb.gy/9l2c6q .

5- نوارة باشوش ، الجيش يدخل في حرب الفضاء الإلكتروني ومكافحة الجوسسة ، الشروق ،يوم 2-8-2018، الرابط :https://rb.gy/72cmi6 .

6- هاكان تانريفيردي ،هكذا تخلق الهجمات الإلكترونية المشاكل السياسية،زود دويتشه تسايتونغ،ت :نون بوست ،نون بوست ،2018/10/1 ،الرابط: https://rb.gy/98or01.

7- ريهام عبد الرحمن رشاد العباسي، أثر الإرهاب الالكتروني على تغير مفهوم القوة في العلاقات الدولية ،دراسة حالة " تنظيم الدولة الإسلامية "،المركز الديمقراطي العربي ،24جويلية 2016،الرابط:https://rb.gy/q7gx17 .

8- فتحي بولعراس ،مداخل متعددة : الدرس الجزائري في تفكيك التطرف ومحاربة الإرهاب، المستقبل للأبحاث و الدراسات المتقدمة ،2 نوفمبر 2017، الرابط: https://rb.gy/gdwiu4 .

9- صباح عبد الصبور عبد الحي ، استخدام القوة الإلكترونية في التفاعلات الدولية ،المعهد المصري للدراسات، 29 أكتوبر 2016الرابط : https://rb.gy/zqflx9 .

10- نوران شفيق، أشكال التهديدات الإلكترونية ومصادرها ، المركز الأوروبي، 29يناير 2020، الرابط :https://rb.gy/ywagha .

4-الملتقيات:

1- موسى محمد آل طويرش ،الصراع السيبراني – مفهومه و أثره في العلاقات الدولية ،المؤتمر الفصلي لكلية العلوم السياسية بجامعة المستنصرية ، 2019/2/27، العراق.

2- وزارة الدفاع الوطني ،تطور التهديدات السيبرانية و طرق الأمن السيبراني والدفاع السيبراني ،"ملتقى الثاني -الأمن و الدفاع السيبراني" ،النادي الوطني للجيش ،الجزائر ،25- 26مارس2019، الرابط:https://www.aps.dz/ar/algerie/68706-2 .

2-المراجع باللغات الأجنبية :

أ- الفرنسية :

-Olivier Kemph ,inttroduction **à la cyberstratégie**,paris ,Economica,2012.

ب- الأنجليزية :

1- Peter Warren Singer ,Allan A.Friedman ,**Cybersecurity and Cyberwar-what evryone neeeds to Know**, A Thesis Submitted in Fulfillment of the Requirements for M.A in Translation ,Oxford university,2014.

2-Martin C.Libicki,**Conquest in Cyberspace :National Security and Information Warface** ,New york,Combridje university press,2007.