Journal of Police and Legal Sciences

Volume 14 | Issue 1 Article 3

1-17-2023

The security and cyber defence realities and difficulties in Algeria

Kada aicha

واقع ورهانات الأمن والدفاع السيبراني في الجزائر

د. عائشة قادة بن عبد الله
المؤسسة: جامعة أبي بكر بلقايد –تلمسان

الملخص:

ستحاول هذه الورقة البحثية؛ تسليط الضوء على التحدي الرقمي الذي تخوضه الجزائر وذلك بدخولها إلى عالم مجتمع المعرفة؛ الذي سيؤهلها إلى تحقيق الأمن والدفاع السيبراني ضد مختلف أشكال وأنواع التهديدات الأمنية وفي مقدمتها تهديدات الفضاء السيبراني.

ولمعالجة هذا الموضوع استعانت الباحثة **بالمنهج التحليلي** للوقوف على الظاهرة محل الدراسة وتتبع أسبابها، بالإضافة إلى **منهج دراسة الحالة** – لدراسة كافة جوانب الظاهرة المدروسة والتعرف على خصائص الحالة المدروسة – هنا تم اختيار الجزائر كوحدة تحليل-.

وقد خلصت الدراسة إلى مجموعة من النتائج أهمها:

- أن عجز المؤسسات الأمنية وأنظمة المراقبة فيها جعلها عرضة للتهديدات السيبرانية.
- كلما زاد حجم التهديدات السيبرانية كلما شكل ذلك تحدياً أمنياً للمنظومة الدفاعية الجزائرية.
- أن التهديدات الأمنية الجديدة والمرتبطة أساساً بالتكنولوجيا تفرض على المؤسسات الأمنية بناء خطة استراتيجية لمجابهتها.
- أن من يمتلك القوة المعلوماتية يعرف جيداً كيف يتحكم في الآخرين ويؤثر فيهم.
- برهن التصدي للهجمات الإلكترونية على مدى قدرة الأجهزة الأمنية الجزائرية وتأهبها.

ومن بين **التوصيات** التي خلصت إليها الدراسة نذكر:

- زيادة تأهيل العنصر البشري للتحكم في التكنولوجيات الرقميّة عن طريق فتح التكوينات الجامعية ذات الارتباط، والمشاركة في صياغة البرامج التعليمية الأكاديمية في تخصص الأمن والدفاع السيبراني.
- تنمية وتوعيّة الحس الوطني بمدى شدة وخطورة التهديدات السيبرانية عن طريق المنشورات، الحصص الإذاعية والتلفزيونية مع استضافة الخبراء.

الكلمات المفتاحية:الهجمات السيبرانية، الرقمنة، الأمن السيبراني، الدفاع السيبراني، الأجهزة الأمنية الجزائرية.

The security and cyber defence realities and difficulties in Algeria

Dr. Kada Benabdallah Aicha
The institution: University of Telemcen- Abou Bekr Belkaid

Abstract:

This research paper aims to shed light on the digital challenge faced by Algeria as it enters the world of the knowledge society, which qualifies it to achieve cybersecurity and cyber defense against various forms and types of security threats, including cyber threats. The researcher used an analytical approach to understand the phenomenon under study and trace its causes, in addition to a case study method to study all aspects of the studied phenomenon and identify the characteristics of the case study - Algeria was chosen as the analysis unit. The study concluded several important results, including:

The deficiency of security institutions and surveillance systems in Algeria has made it vulnerable to cyber threats.The increasing volume of cyber threats poses a security challenge to the Algerian defense system.New security threats mainly related to technology require security institutions to develop a strategic plan to counter them.Those who possess information power know well how to control and influence others.The ability of Algerian security agencies to respond to cyber attacks depends on their capabilities and readiness.

Among the recommendations drawn from the study, the following are mentioned:

Increasing the qualification of human resources to control digital technologies through opening university programs related to cybersecurity and cyber defense, and participating in the formulation of academic educational programs in the field of cybersecurity and cyber defense.Developing national awareness of the severity and danger of cyber threats through publications, radio and television programs with the participation of experts.

Keywords: Cyber attacks, Digitization, Cybersecurity, Cyber defense, Algerian security agencies.

مقدمة

أفضت التطورات التكنولوجية الرقمية التي شهدها العالم إلى حالة من التعقد الشديد؛ وقد حقق التقدم التكنولوجي تغييرات جوهرية في حياة الإنسان والمجتمع، ويشمل ذلك التحولات في ميدان الدبلوماسية، الاستراتيجية، الاقتصاد، الثقافة والطب، وألغت الابتكارات عامل المسافة بين الدول، كم أتاحت التقنيات الحديثة توسعاً في الدائرة المعرفية لأن هذه التقنيات تشجع النشاطات ذات المميزات الرئيسية الأربع باعتبارها عالمية ودائمة وفورية وغير مادية في آن معاً(توفيق، 2017: 289).

وعلى الرغم من المزايا والإيجابيات التي طرأت على سير العالم وتطوره إلا أنها حملت مظاهر سلبية شكلت تهديداً لأمن الدول؛ المؤسسات والأفراد؛ وذلك بفعل تزايد عمليات القرصنة، التجسس والهجمات الإلكترونية؛ ما جعل الدول عرضة لنوع جديد من الحروب الحديثة تختلف عن تلك التقليدية في وسائلها واستراتيجياتها.

تعتبر هذه الحروب نوعًا من الاستراتيجيات الجديدة في العلاقات الدولية؛ لاعتمادها بشكل كلي على الوسائل المتطورة، التقنيات الحديثة؛ وما ساعدها في ذلك هو السرعة الهائلة للتطور الهائل في نظم الاتصالات الحديثة، الرقمنة والفضاءات الرقميّة. لذا أصبح لزاماً على الدول اليوم خوض غمار هذا التحوّل التكنولوجي لخلق منظومة دفاعيّة غير تقليدية لمجابهة التهديدات الأمنية التي تغيّرت طبيعتها وحتى مصادرها؛ فتحديات اليوم تفرض على الدول الاستعداد لهذا النمط من التحولات الجديدة؛ بالنظر إلى طبيعة التهديد في حد ذاته وخاصة وأن المهدد هو طرف مجهول فائق القدرة على التخفي واستعمال التكنولوجيا الرقميّة.

وقلبت الثورة التكنولوجية كل المعطيات الاستراتيجية العسكرية، فانتقل العالم إلى عصر الصواريخ العابرة للقارات وطائرات التجسس بدون طيار والأقمار الصناعية القادرة على تصوير هدف سري(colard, 1977: 76)، ومن أجل تغطية الفجوة بين هذه الدول أصبح من الضروري أن تقوم الدول الصناعية بمساعدة الدول النامية في نقل التكنولوجيا، وفي الحالة المعاكسة فإن سيطرة تكنولوجيا الأغنياء ستؤدي بشكل دائم إلى اعتماد الفقراء عليهم(seicherman, 1975: 139)

أدرك صانع القرار الجزائري المعضلة وحجم التحديات التي تواجه أجهزته الأمنية باعتبارها خط الدفاع الأول للأمن الوطني؛ فعمد بذلك إلى تبني تصورات حول الدفاع السيبراني ومراقبة أنظمة الأمن لحماية المنشآت الحيوية والمؤسساتية ضد التهديدات الداخلية والخارجية (الأفراد والمؤسسات) وبخاصة التصدي لعمليات التجسس والاختراق كخطوة نحو تعزيز أمنه السيبراني والمعلوماتي.

مشكلة الدراسة:

بات اليوم من الصعب السيطرة على الفضاء الرقمي في ظل التقنيات الحديثة وسرعة تدفق الإنترنيت والمعلومات؛ وهذا ما يضع الدول في تحدٍ مستمر لتحصين نظم أمنها السيبراني؛ والجزائر كغيرها من الدول تسعى إلى بلورة الاستراتيجيات الفعالة لمجابهة التهديدات الأمنية السيبرانية. لذا تم طرح الإشكالية التالية:

ما هي طبيعة التهديدات الأمنية التي تواجه المنظومة الدفاعيّة السيبرانية الجزائرية؟ وما هي الاستراتيجيات التي تبناها صانع القرار لحماية وتأمين نظم أمنه المعلوماتي ضد مختلف التهديدات السيبرانية؟

وانبثقت عنها مجموعة التساؤلات الفرعية التالية:

- ما مدى خطورة التهديدات السيبرانية للمنظومة الأمنية الجزائرية؟
- ما هي الإجراءات والآليات التي اعتمدتها الجزائر لمواجهة التهديدات السيبرانية؟

وللإجابة على هذه التساؤلات تم صياغة الفرضيات التالية:

- تشكل التهديدات السيبرانية تحديًا أمنيًا للمنظومة الدفاعية السيبرانية الجزائرية.
- يرتهن تأمين وحماية الأمن السيبراني الجزائري بمدى الاستراتيجيات القانونية والمؤسساتية الردعيّة لمجابهة التهديد.

أهمية الدراسة

ينطوي البحث على أهمية نظرية باعتباره يبحث في موضوع القوة من جهة ومن جهة أخرى مفاهيم الفضاء السيبراني، الهجوم السيبراني وأيضاً مفهوم الأمن الذي انتقل في مفهومه من أمن صلب إلى أمن ليّن ذلك لتنوع مصادر التهديد؛ أما من ناحية أخرى فيتوجب على الباحثين الخوض في غمار هذا الموضوع الذي يعتبر ذو أهمية سواء من الناحية الأكاديمية أو العملية؛ فمن الناحية الأكاديمية نقص الكتابات في الموضوع بالنظر إلى حداثته خاصة في أوساط الدول العربية؛ والذي تزايد الاهتمام به عقب الجرائم المعلوماتية والإلكترونية؛ في حين أن الأهمية العملية للموضوع ترتبط بالمؤسسات الأمنية نفسها التي أصبح لزاماً عليها التطوُّر واكتساب الخبرة والمعرفة لمجابهة هذا النوع الجديد من التهديدات الأمنية.

أهداف الدراسة

- التعرف على خصوصية الأمن السيبراني في الجزائر.
- معرفة وتحليل طبيعة التهديدات السيبرانية التي تواجه الأجهزة الأمنية الجزائرية.
- إدراك مدى قدرة وتأهب الأجهزة الأمنية الجزائرية للدفاع السيبراني ضد مختلف أشكال التهديدات الأمنية.

التعريفات الإجرائية:

التهديدات السيبرانية: هي إلحاق الضرر والأذى سواء بالأشخاص، الممتلكات وحتى المؤسسات؛ وينجم عن الضرر أخطار جسيمة.

الأمن السيبراني: هو مختلف الإجراءات التي تتخذها الدول لحماية نظم معلوماتها، من التخريب، التجسس وحتى الحروب الإلكترونية.

الدراسات السابقة:

تأتي دراستنا هذه ضمن سلسلة مجموعة من المقالات التي تناولت موضوع التهديدات السيبرانية بشكل عام، والأخطار المنوطة بها؛ في حين أن دراستنا تسلط الضوء على الأمن الوطني الجزائري وما يواجهه من تهديدات سيبرانية تطرحها ظروف البيئة الدولية وحتى الإقليمية؛ ومقالنا يأتي تزامناً وتطلع صانع القرار الجزائري إلى توسيع أجندته الأمنية تماشياً والتهديدات الجديدة؛ في

ظل زيادة تغلغل بعض الدول في إفريقيا وتبنيه لهجمات إلكترونية ضـــد أجهزة الأمن الوطني الجزائري.

نذكر أن الموضوع هو حديث نسبياً وتقل فيه الدراسات والبحوث؛ ومن بين الدراسات التي تناولت الموضوع نذكر:

- مذكرة ماجستير لـ مشيب ناصر محمد آل زيران الموسومة بـ "المواقع الإلكترونية ودورها في نشر الغلو الديني وطرق مواجهتها من وجهة نظر المختصين"، عن جامعة نايف العربية للعلوم الأمنية، الرياض، 2011

- أطروحة دكتوراه لـــ "سليم بلحاج" بعنوان "التهديدات الأمنية اللاتماثلية وتداعياتها على الأمن الوطني الجزائري"، عن جامعة باتنة 1، 2021، هدفت الدراســة إلى محاولة تحديد حجم ومصدر التهديدات اللاتماثلية على الأمن الوطني الجزائري بمختلف مستوياته وأبعاده، وطرح رؤية جديدة للاســتراتيجية الجزائرية في ظل التغيرات البيئية المحلية، الإقليمية والدولية، فضــلا عن التوصـــل إلى بناء اســتراتيجية أمنية قادرة على احتواء مثل هذا النوع من التهديدات ومواجهة التحديات، واستعان الباحث بالمنهج التفكيكي التركيبي، والمنهج التاريخي، وخلصت الدراسة إلى أن التحول في طبيعة التهديدات الأمنية إلى بناء المحتوى المعرفي والعملياتي للأمن، ومن ثم فهو مركب وشامل، أضف إلى ذلك أن الجزائر تعيش في بيئة إقليمية على درجة عالية من اللاستقرار، بسبب انتشر التهديدات اللاتماثلية، وأن هذا التنوع في التهديدات الأمنية فرض عليها توسيع تصورها لأمنها ليشمل الأمن الإقليمي.

- مذكرة ماستر لـــــــ آل سيد الشيخ فاطمة وموساوي صبيحة بعنوان "دور الإعلام الأمني وتكنولوجيا الاتصال الحديثة في الجزائر: الانترنيت نموذج"، عن جامعة مستغانم، 2016؛ هدفت الدراسة إلى تسليط الضوء على واقع الإعلام الأمني في الجزائر، وطرق تعامل المؤسسات الأمنية مع تكنولوجيات الاتصال الحديثة؛ واعتمدت الباحثتان على المنهج الوصفي لوصف الظاهرة ومعرفة خصائصها؛ وأداة تحليل المضمون الإعلامي الأمني كأداة للوصول إلى نتائج بحثية دقيقة؛ وحددت عينة الدراسة بتحليل مضمون المقالات التي تم نشرها من منتصف نوفمبر 2015 إلى بداية أفريل 2016؛ وقد خلصت الدراسة إلى ضرورة تكاثف الجهود الأمنية والإعلامية ناهيك أيضاً على استخدام أساليب اتصالية ونكنولوجية عالية الجودة.

- دراسة لـــ "حنين جميل أبو حسين" موسومة بـــ الإطار القانوني لخدمات الأمن السيبراني (دراسة مقارنة) عن جامعة الشرق الأوسط، 2021، هدفت الدراسة إلى التعرف على الإطار القانوني لخدمات الأمن السيبراني ومعرفة مفهوم الفضاء السيبراني وتأثيرها على دول العالم، واعتمدت على المنهج الوصفي لغايات الاستدلال، وقد خلصت الدراسة إلى أن الأمن السيبراني يقوم على حماية المنظمات والموظفين والأفراد، يجب على المنظمات والخدمات تنفيذ أدوات الأمن الســـيبراني والتدريب وأساليب إدارة المخاطر وتحديث الأنظمة باستمرار مع تغير التقنيات وتطورها.

- مذكرة ماستر لـــــــ "سليم دحماني" بعنوان "أثر التهديدات السيبرانية على الأمن القومي: الولايات المتحدة الأمريكية أنموذجاً 2001-2017"، عن جامعة المسيلة 2017، هدفت الدراسة إلى إبراز وتوضيح المفاهيم الجديدة في الفضاء السيبراني وإبراز إسهامات وجهود الدول وخاصة الولايات المتحدة الأمريكية في مواجهة التهديدات السيبرانية، استعان الباحث بالمنهج الوصفي،

منهج دراسة الحالة ومنهج تحليل المضمون؛ وقد خلصت الدراسة إلى أن الفضاء السيبراني أصبح مجالاً جديداً وهاماً للتفاعلات الدولية وازداد الصراع في الشبكات ليصبح حروباً جديدة لها طابعها التقني الخاص تهدد سيادة الدول، وأن الولايات المتحدة الأمريكية على الرغم من أنها أقوى دولة سيبرانية إلا أنها تواجه تهديدات سيبرانية ومنافسة في الفضاء السيبراني خاصة من الصين وروسيا.

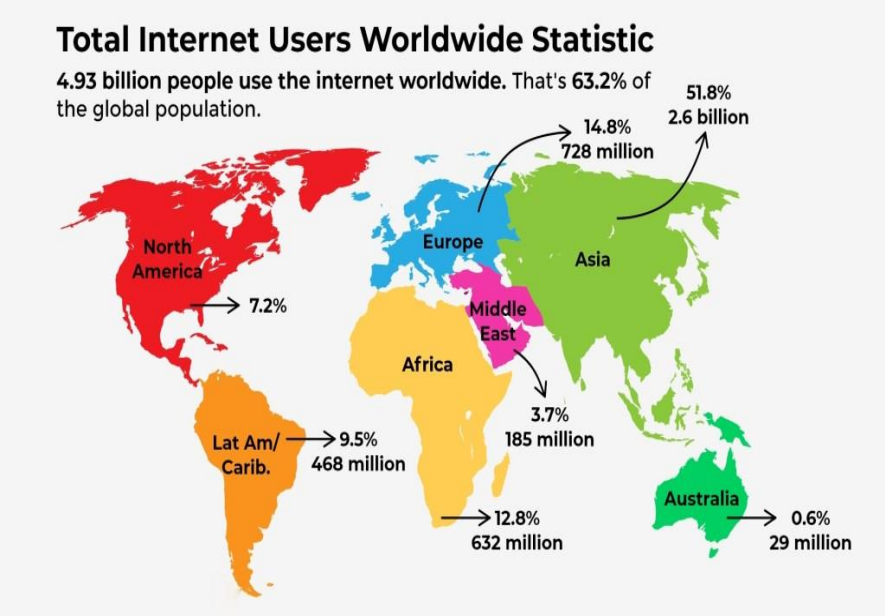
المحور الأول: الإطار النظري للبحث

دخل العالم مرحلة جديدة من التطور التقني والتكنولوجي في ظل الابتكارات الحديثة التي ترافق الحياة البشرية؛ على غرار الهواتف الذكية، نظم المعلومات، وأنظمة الذكاء الاصطناعي.

المبحث الأول: الفضاء الإلكتروني

تشير الاحصائيات إلى أن هناك 4.9 مليار مستخدم للإنترنيت بداية عام 2021، وأن قارة آسيا كان لها النصيب الأكبر بـ 51.8% ثم أوروبا بـ 14.8%، افريقيا بـ 12.8% في حين أن استراليا احتلت المرتبة الأخيرة بـ 0.6%.

خريطة رقم 01: إحصائيات حول عدد مستخدمي الأنترنيت عبر العالم



المصدر: https://thaqafati.com/

لعب الفضاء الإلكتروني دوراً أساسياً في تعظيم القوة والاستحواذ على عناصرها في العلاقات الدولية، حيث أصبح التفوق في ذلك المجال عنصراً حيوياً في تنفيذ عمليات ذات فعالية على الأرض والبحر والجو والفضاء الخارجي من خلال اعتماد القدرة القتالية في الفضاء الإلكتروني على نظم التحكم والسيطرة التكنولوجية، وهذا الأمر يستدعي بالضرورة تغيّرًا في مفهوم القوة حيث بات بالإمكان تعريفها بأنها: "مجموعة الوسائل والطاقات والإمكانيات المادية وغير المادية المنظورة وغير المنظورة التي بحوزة الدولة ويستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة وتوثر في سلوك الوحدات السياسية الأخرى(سعود، بلا تاريخ: 87).

أثر الفضاء الإلكتروني على بروز شكل جديد من أشكال القوة ممثلاً في القوة الإلكترونية؛ إلى جانب قوى أخرى السياسية، الاقتصادية، العسكرية وحتى الإعلامية؛ فالقوة الإلكترونية اليوم

حسب "ألفن توفلر" هي من تقود العالم نحو التأثير في السياسات العالمية وأن امتلاك المعرفة هو أساس لامتلاك للثروة والقوة العسكرية. وترتبط القوة السيبرانية بامتلاك المعرفة التكنولوجية والقدرة على استخدامها للتأثير في الأحداث على النحو الذي يحقق الأهداف المرجوة لاستخدام الوسائل والأدوات الإلكترونية(طالة، 2020: 59). وتبرز هذه الأهمية باتساع عدد مستعملي الفضاء الإلكتروني وشبكاته المعلوماتية، وكذا من خلال حجم وأهمية المعلومات المتاحة وقدرات الربط والاتصال اللحظيّة التي يمكن أن تبلور التصورات وتحدد المواقف(جعيجع، 2017: 60).

المبحث الثاني: التغيُّر في مفهوم التهديد الأمني

يؤدي التغيّر في مفهوم القوة بالضرورة إلى التغيّر في منظور الحرب، حيث انتقلت من نسق الحروب التقليدية القائمة على تدمير الخصم أو احتلال أرضه أو الاستيلاء على موارده، إلى حروب تعمل للاستحواذ على سباق التقدم التكنولوجي وسرقة الأسرار الاقتصادية والعلمية والتحكم بالمعلومات والعمل على اختراق الأمن القومي بدون طائرات أو متفجرات، أو حتى انتهاك الحدود وتدمير مواقع التجسس والتي قد يكون لها تأثير يفوق الحرب التقليدية لما تشكله من آثار مدمرة على الاقتصاد والبنية التحتيّة(سعود، د.ت: 87).

وبحسب "جوزيف ناي" Nye أن الفضاء الإلكتروني هو مجال فريد من نوعه، من حيث إنه وبخلاف الفضاءات والمجالات السيادية الأخرى هو من صنع الإنسان، حديث وأكثر ارتباطاً بالتغيّرات التكنولوجية مقارنة بالمجالات الأخرى، فجغرافية الفضاء الإلكتروني هي أكثر قابلية للتغيّر من البيئات الأخرى، حيث يصعب تحريك الجبال والمحيطات، لكن يمكن تشغيل وإيقاف أجزاء من الفضاء الإلكتروني بنقرة زر، ومن ثم فالتحكم في الأجهزة الإلكترونية هو أسهل، أقل كلفة وأسرع من تحريك السفن والأساطيل البحرية والطائرات والمقاتلات(شرايطية، 2020: 399).

أصبح الفضاء السيبراني اليوم من مسائل السياسات العليا، فممارسات كقطع الإنترنت في فترات عدم الاستقرار لدولة ما، أو تسريب وثائق حكومية سرية، أو هجوم سيبراني، كلها أمثلة تدل على أنه لا يمكن تجاهل وجود وقدرات الفضاء السيبراني؛ وقد بدأ التركيز على الفضاء السيبراني كتهديد أمني جديد بفعل أحداث دولية أهمها 11 سبتمبر 2001 وذلك مع استخدام تنظيم القاعدة له كساحة قتال ضد الولايات المتحدة، وفي عام 2007 برز بوضوح دور الفضاء الإلكتروني كمجال جديد في العمليات العدائية في الصراع بين استونيا وروسيا وفي 2008 في الحرب بين روسيا وجورجيا، وجاء الهجوم الإلكتروني بفيروس "ستاكسنت" على برنامج إيران النووي عام 2010 ليمثل نقطة هامة بالتطور في مجال الأسلحة الإلكترونية (بيرم، 2020: 794-796). وظهور الحرب السيبرانية يسمح بالتحول إلى تعريف "سان تزو" suntzu للحرب أي "إخضاع العدو دون قتال"، ووصف "فيليب ميلينجر" philipmeilinge الهجوم السيبراني بغير الدموي ولكنه يحتمل أن يكون طريقة جديدة للحرب، وأن الثورة الرقمية والمعلوماتية ستأتي بالتحول في طبيعة الحرب كما أكدها "روبرت ليوناردrobert leonard(شنوف، 2020: 97).

أحدث الفضاء السيبراني تغييرات في مجال وظائف الدولة، وبخاصة فيما يتعلق بوظيفة الدفاع الخارجية، التي تتعلق بسلامة الدولة وأفرادها من العدوان الخارجي، كما ساهم في وجود أشكال جديدة من العدوان على مواطني الدولة ومؤسساتها، عبر شبكات الاتصال والمعلومات، والتي

تعتمد عليها المنشآت الحيوية وهو ما يصيب الدولة بعجز في توفير الأمن على المستوى الداخلي، بحفظ سلامة الأفراد وممتلكاتهم وأموالهم، وكذلك مهمة الدفاع لعدم القدرة على تحديد مصدر الهجمات(بيرم، 2020: 801).

قد تعرض العالم لهجمات سيبرانية قوية أحدثت خسائر مالية وصلت للمليارات؛ ولعل أبرزها وأشهرها هجوم برامج الفدية العام 2017 واستهدف 150 بلداً وعطل أكثر من 200 ألف جهاز كمبيوتر وبلغت الخسائر سبعة مليارات دولار، وقبل ذلك تم استهداف قطاع الطاقة في العام 2012 من خلال زعزعة استقرار أنظمة الطاقة في "شركة أرامكو" السعودية واستهداف 30 ألف محطة عمل تابعة للشركة واستهداف شركة رأس غاز القطرية من خلال فيروس أدى لتعطل النظام التشغيلي، وبحسب الجريدة أيضاً فإن هناك 900 هجوم سيبراني خلال العام الماضي 2021، تقف خلفها دول وجهات مدعومة من دول أو تنظيمات إرهابية؛ واستهدفت مؤسسات سيادية وعسكرية وشركات كهرباء وطاقة واتصالات وشركات مالية ومواطنين(نوايسة، د.ت).

ترتب على الثورة التكنولوجية والاتصالية الحديثة أيضاً بروز مصطلح الجرائم العابرة للحدود، وزادت خطورتها وتعاظم حجم التأثير السلبي الذي باتت تخلفه، سواء من حيث تسهيل الاتصال بين الجماعات الإجرامية وتنسيق أعمالها في العالم الحقيقي، أو من حيث ابتكار أساليب وطرق إجرامية متقدمة، ووجدت الجماعات المتطرفة ضالتها في ترسيخ أعمالها وإبراز صورتها من أجل إيصالها إلى قطاع كبير من المنتمين إلى الفضاءات الافتراضية، وذلك رغبة منهم في توسيع قواعد نشاطها وكسب متعاطفين جدد وتجنيد آخرين وفق خططها(بشير، 2018: 209).

أصبح المجرمون يستغلون السرعة وعدم الكشف عن هوية الإنترنت لارتكاب مجموعة من متنوعة من الأنشطة الإجرامية التي لا تعترف بالحدود سواء أكانت حدود مادية أم افتراضية، وهذه الأنشطة تسبب ضرراً جسيماً وتشكل تهديدات حقيقية، فالمنظمات الإجرامية تتحول بشكل متزايد إلى الإنترنت لتسهيل أنشطتهم وتعظيم أرباحهم في أقصر وقت، فالجرائم مثل القرصنة، هجمات البرامج الضارة والابتزاز تشكل تهديدات حقيقية لأمن الحكومات، الشركات والأفراد (interpol,n.d : 05).

فكثير من الجماعات الإرهابية أتاحت لنفسها كثيراً من تطبيقات شبكة الإنترنت وطوعتها لخدمة أغراضها، حيث قامت باستغلال الفضاء الرقمي للترويج لأنشطتها وإعلام الناس بما تفعله، فتقوم عبر مواقع إلكترونية صممتها لنفسها أو عبر حسابات الشبكات الاجتماعية أو المنتديات بغية التأثير في المحيط الافتراضي الذي يتميّز بالاندماج السلس والمشاركة والانفتاح وغياب الحدود، حيث تنمو هذه الجرائم الإرهابية مع تقدم العولمة، وهي أشد خطورة وإثارة للقلق(بشير، 2018: 209)

ما يمكن ملاحظته أن التحولات ما بعد فترة الحرب الباردة أفضت إلى بروز أنماط وأشكال جديدة من التهديدات الأمنية، والتي تأتي في مقدمتها تهديدات الفضاء السيبراني الذي تفقد فيه الدول السيطرة؛ فهو ليس مجالاً ثابتاً؛ بالنظر إلى عدد مستخدميه وسرعة انتقال وتدفق المعلومات من جهة، وكذا القدرة العالية على اختراق أنظمة المعلومات.

تعد الجزائر كغيرها من الدول الأخرى مجالاً لاستهداف أمنها السيبراني ونظم معلوماتها؛ وما الهجمات الأخيرة التي تعرضت لها إلا خير دليل على ذلك، حيث إن الجهات المستهدفة تعمل على

ضرب أسس الأمن المجتمعي الجزائري بنشر الصور والفيديوهات محاولة منهم للمساس بالهوية والأخلاق؛ وسنحاول في العنصر الموالي تبيان أشكال التهديدات الأمنية التي تواجه الأمن الوطني الجزائري.

المحور الثاني: أنماط وأشكال التهديدات السيبرانية للأمن الوطني الجزائري

يعتبر تحدي الأمن السيبراني أعلى تحديات الأمن الوطني في القرن الواحد والعشرين، مع الإشارة إلى أن المفهوم الحديث للأمن لا يقتصر فقط على الجوانب العسكرية، بل يواكب كل التهديدات والتحديات التي يمكن أن تشكل حجر عثرة أمام الاقتصاد الرقمي وتدفق المعلومة، فقد أسقطت تكنولوجيا المعلومات والاتصالات مفهوم الحدود الجغرافية بين الدول مما يضع السيادة الوطنية على المحك، خاصة مع اختراق المواقع الحكومية الرسمية والتجسس الإلكتروني على الدول(كلاع، 2022: 304).سيتم تقسيم المحور إلى نقطتين الأولى تتعلق بأهم التهديدات السيبرانية في حين أن المبحث الثاني سيتم فيه تبيان أثر التهديدات السيبرانية على الأمن الوطني الجزائري.

المبحث الأول: أشكال التهديدات السيبرانية

أفضت التطورات التكنولوجية الجديدة وحركية الاتصالات إلى أشكال جديدة من التهديدات الأمنية التي أصبحت تركز بالأساس على استخدام الطرق والوسائل الحديثة في إدارتها؛ وتتنوع أشكال وأنماط التهديدات السيبرانية إلى (عطية، د.ت:108-110):

1- التجسس الإلكتروني: يعد أحد أشكال التجسس التقليدي باستخدام وسائل التكنولوجيا الفائقة، ومعظم الهجمات السيبرانية المتطورة التي تقع ضمن هذه الفئة، حيث تم الحصول على معلومات سرية بطرق غير مشروعة بهدف الحصول على أفضليّة اقتصادية، استراتيجية أو عسكرية. فالتجسس السيبراني هو ذلك التجسس الذي يعتمد على استخدام التقنيات الإلكترونية في الحصول على معلومات.

تعرضت ست على الأقل من الإدارات الحكومية الأمريكية للاختراق، من بينها الطاقة، التجارة، الخزانة والخارجية بالإضافة إلى شبكات إدارة الأمن القومي النووي. وذكرت وسائل الإعلام أن العشرات من شركات الأمن والتقنيّة، إلى جانب منظمات غير حكوميّة خارج الولايات المتحدة تأثرت أيضاً وذلك في كل من كندا، المكسيك، بلجيكا، إسبانيا، المملكة المتحدة، إسرائيل، والإمارات العربية المتحدة (للمستقبل، رقمنة البنية التحتية الحيوية، د.ت، صفحة 03)، ويكون التجسس على المعلومات العسكرية والخطط والأجهزة والمعدات، وكذا وعلى المعدات الاستخباراتية والسياسية والاقتصادية، بغية توظيفها لتحقيق مصلحة المخترق أو الإضرار بالطرف المتجسس عليه، مثلما حصل عندما أتهم الروس بزرع فيروس "تورلا" المعد للتجسس على دول الاتحاد الأوروبي في سياستها الخارجية تجاه أوكرانيا، الذي امتد من 2008 إلى 2011(جعيجع، 2017: 73)، ونشرت معلومات حول قيام وكالة الأمن القومي الأمريكي بالتجسس على نحو 35 من القادة على مستوى العالم، وأكثر من 60 مليون مكالمة هاتفيّة في دول مختلفة من بينها دول أوروبية، كما أعلن أمين مجلس الأمن الروسي "نيكولاي باتروشيف" في 26 أوت 2015 العثور على برامج تابعة للاستخبارات الأجنبية في نظم المعلومات للمؤسسات الحكومية الروسية(كلاع، 2022: 296).

وتنص المادة 61 من قانون العقوبات الجزائري في فقرتها رقم 03 وطبقاً للمادة 64 على أنه يعتبر جاسوساً كل من يقوم بإتلاف أو إفساد سفينة أو مركبات للملاحة الجوية أو عتاد أو مؤن أو مبان أو إنشاءات من أي نوع كانت وذلك بقصد الإضرار بالدفاع الوطني أو إدخال عيوب عليها أن التسبب في وقوع حادث وذلك تحققاً لنفس القصد (غريسي، 2022: 157).

2- الاحتيال الإلكتروني أو التصيد الإلكتروني: عبارة عن عمليتين متشابهتين من حيث الاستراتيجية، ويكمن الفرق الوحيد بينهما في أن التصيد الإلكتروني يستخدم رسائل البريد الإلكتروني كقناة، بينما يتم إجراء عمليّة الاحتيال الإلكتروني باستخدام الرسائل القصيرة، وغالباً ما تشبه رسائل الاحتيال الإلكتروني تلك الرسائل الصادرة عن موقع قانوني لبنك متنقل أو عبر متجر إلكتروني أو شبكة التواصل الاجتماعي؛ وأوضح المقدم "سيد علي سلمان" أن "مجرمي الإنترنت يستخدمون صياغة من جمل متشابهة وكلمات وعبارات تقليدية، كما يمكن أن تؤدي النقرات غير المقصودة وأرقام الهواتف المشبوهة والروابط الغريبة المذكورة في الرسالة إلى انتحال الشخصية، وذلك عن طريق دعوة المستخدم لإدخال المعلومات المتعلقة بهويته أو تفاصيل بطاقة الائتمان الخاصة به"(الجيش، 2021: 34).

3- الإرهاب السيبراني: هو ذلك الاستخدام للموارد المعلوماتية، المتمثلة في الإعلام وأجهزة الحاسوب وشبكة الإنترنت والفضائيات من أجل أغراض التخويف أو الإرغام لأغراض سياسية، أو الإقناع الفكري والتثقيف السلبي والعدواني، ويمكن أن يتسبب في إلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات وتعطيل أنظمة الدفاع الجوي وغيرها.

يعرف الإرهاب السيبراني بأنه نسخة إلكترونية من الإرهاب المادي الذي نشأ عن تكنولوجيا المعلومات والاتصالات والأنترنيت. استغل إرهابيون هذه التقنية لتنفيذ هجمات غير مشروعة ضد أهداف وهياكل تم إنشاؤها لصالح البشرية. وتشمل هذه الأهداف الطاقة والكهرباء وشبكات المياه وأنظمة الكمبيوتر والمعلومات والمواقع العسكرية والمدنية والحركة الجوية والنقل والبنية التحتية الأخرى، والهدف الأساسي من هذه الهجمات هو إخضاع الحكومة ونشر الخوف والرعب بين البشر من أجل تحقيق أهداف إرهابية سواء أكانت سياسية أم مدنية أو اجتماعية أو اقتصادية (Gunaratna, 2004: n.p).

4- الحروب السيبرانية: هي استخدام الهجمات الإلكترونية ضد دولة قومية، مما يتسبب في ضررها، بما في ذلك الحرب المادية وتعطيل أنظمة الكمبيوتر الحيوية. وتشير الحروب السيبرانية إلى هجمات ترتكبها دولة قوميّة على دولة أخرى، إلا أن أنها يمكن أن تصف أيضاً الهجمات التي تشنها الجماعات الإرهابية أو مجموعات المتسللين بهدف تعزيز أهداف دول معيّنة. وتتجلى أهدافها في إضعاف أو تعطيل أو تدمير دولة أخرى(katie terell hanna, s.d: n.p).

تعرف **حروب الجيل** الجديد على أنها مفهوم حديث لأحد أنواع الحروب، أُبتكر ليصير أداة رئيسية لفرض الهيمنة، حيث انتشر استخدامه بكثرة منذ مطلع هذا القرن من طرف أقوياء العالم لاستهداف ولتهديد سيادة الدول وإضعافها؛ فهي حروب تدار عن بعد وتستعمل فيها أدوات ووسائل مختلفة، معلوماتية، اقتصادية واجتماعية وعسكرية غايتها إجهاد النظام القائم وتفكيك الدولة من الداخل باتباع خطوات طويلة الأمد؛ فهي لا تقتصر على المسرح التقليدي للحرب بأبعاده البري، البحري والجوي؛ ويتم توظيف أحدث تكنولوجيات الإعلام والاتصال بما فيها الكمبيوتر،

الأقمار الصناعيّة، الرادارات، وأجهزة التنصت والمراقبة، بالإضافة إلى استعمال الذكاء الاصطناعي والتقنيات الخوارزمية(بليل، 2022: 45).

تشبه الحرب السيبرانية التجسس السيبراني، وفي بعض الأحيان يتم الخلط بين المصطلحين. يتمثل الاختلاف الأكبر في أن الهدف الأساسي لهجوم الحرب الإلكترونية هو تعطيل أنشطة الدولة القومية، في حين أن الهدف الأساسي لهجوم التجسس الإلكتروني هو بقاء المهاجم مخفيًا لأطول فترة ممكنة من أجل جمع المعلومات الاستخبارية. غالبًا ما يتم استخدام النشاطين معًا. على سبيل المثال، يمكن استخدام التجسس الإلكتروني لبناء معلومات استخباراتية تساعد الدولة القومية على الاستعداد لإعلان حرب فعلية أو إلكترونية. (katieterellhanna, s.d: n.p)

تعتمد على فريق من المتخصصين في المعارك الإلكترونية، حيث كل منهم يتميّز بمسؤولياته ومهاراته الخاصة لترسيخ القدرة على القتال والتحكم بها وإبرازه ضمن الفضاء السيبراني، ويقوم مشغلو الحروب السيبرانية بالتخطيط للنشاطات الهجومية والدفاعيّة وإدارتها وتنفيذها عبر الفضاء السيبراني.

حمل مفهوم الحرب الإلكترونية أبعادا جديدة وصار البعض يفضل مصطلح "الحرب السيبرانية" كتعبير عن ذلك التوجه الجديد وإن ظلت لفظة "الحرب" ذاتها محل جدل خاصة أن هناك مسميات عديدة تطلق على تلك الأنشطة العدائية الإلكترونية منها مثلا الهجمات الإلكترونية والإرهاب الإلكتروني وغيرهما، ووفقاً للمفهوم التقليدي للحرب فإنها تنطوي على استخدام الجيوش النظامية ويسبقها إعلان واضح لحالة الحرب وميدان قتال محدد بينما تبدو هجمات الفضاء الإلكتروني غير محددة المجال وغامضة الأهداف كونها تتحرك عبر شبكات المعلومات والاتصالات المتعدية للحدود الدولية إضافة إلى اعتمادها على أسلحة إلكترونية جديدة تلائم طبيعة السياق التكنولوجي لعصر المعلومات حيث يتم توجيهها ضد المنشآت الحيوية أو دسها عن طريق عملاء لأجهزة الاستخبارات (المرزوقي، د.ت).

المبحث الثاني: واقع الأمن السيبراني في الجزائر

عرفت الجزائر العديد من الهجمات السيبرانية، التي استهدفت مواقع حكومية، وأخرى تابعة لمؤسسات اقتصادية وحيوية استراتيجية، وازدادت هذه الهجمات حدة وكثافة، في الآونة الأخيرة، كما شكلت مواقع وتطبيقات التواصل الاجتماعي، ملاذا لشبكات إجرامية منظمة، لتشن حملات تحريضية، تهدف من خلالها إلى ضرب الاستقرار، وزرع الفتنة بين أفراد الشعب الواحد، وبث الرسائل الدعائية، والتسويق للأفكار الهدّامة، من طرف تلك الشبكات، خدمة لأجندات خبيثة أضحت مكشوفة للجميع (د.ذ.ك، د.ت).

ضمت مجلة الجيش إشارة واضحة للحرب السيبرانية المعلنة على الجزائر كنشر الإشاعات والفيديوهات المفبركة على المنصات الاجتماعيّة، وبث الأفكار الهدامة لتفكيك المجتمع ونشر الفوضى، وذلك من خلال ممارسة الضغط عليه وتوجيه الرأي العام الداخلي واللعب على وتر القناعات والتنوع الثقافي الموجود في المجتمع للتأثير على الوعي الجمعي للأفراد وإضعاف الجبهة الداخلية وتمزيق النسيج الاجتماعي(بليل، 2022: 38).

ففي العام الماضي من سنة 2021، تم تفجير قضية التجسس الإلكتروني على خلفية برنامج "بيغاسوس" الإسرائيلي وذلك حسب ما أوردته تقارير عن حكومات بعض الدول، حول عمليات جوسسة تعرّضت لها مصالح الجزائر وتنصّت طالت مواطنين وشخصيّات جزائريّة عن طريق برامج تجسّس مصمّمة لهذا الغرض (فرانس، الجزائر تعلن فتح تحقيق حول عمليات التجسس تعرضت لها باستخدام برنامج بيغاسوس، 2021)،. تأتي هذه القضية في خضم توتر العلاقات الجزائرية مع بعض الدول.

توضح شركة "كاسبرسكي- (Kaspersky) "المتخصصة في برامج الحماية من الفيروسات- أن بيغاسوس نوع من "البرامج الضارة المعيارية (modular malware) "؛ أي أنه مؤلف من وحدات، حيث يقوم أولا بـــ "مسح (Scan) "الجهاز المستهدف، ثم يثبت الوحدة الضرورية لقراءة رسائل المستخدم وبريده الإلكتروني، والاستماع إلى المكالمات، والتقاط صور للشاشة، كما أن بإمكانه الاستماع إلى ملفات الصوت المشفرة، وقراءة الرسائل المشفرة (الجزيرة، كيف يعمل برنامج التجسس بيغاسوس وهل فعلا أغلقته الشركة الإسرائيلية، د.ت). وكشف تقرير نشرته عدة وسائل إعلام غربية يوم 18 يوليو / تموز 2021 أن ناشطين وصحافيين وسياسيين حول العالم قد تعرضوا لعمليات تجسس بواسطة برنامج "بيغاسوس"، حيث أظهر عن تسرب بيانات 50.000 من أرقام الهواتف التي كان أصحابها مستهدفين للمراقبة منذ سنة 2016.(كلاع، 2022: 296)

وكانت الولايات المتحدة الأمريكية قد طورت فيروس الكمبيوتر Stuxnet، والذي كان قادرًا على القفز عبر الدفاعات المعروفة لتخريب الأبحاث النووية الإيرانية. ومع ذلك، فقد ألهم هذا إيران لإنشاء Shamoon، وهو فيروس كمبيوتر استخدمته في هجوم قضى على محركات الأقراص الصلبة في أكثر من 30 ألف جهاز كمبيوتر في شركة أرامكو السعودية(p.w.singer, s.d: n.p).

كشفت مصالح الدرك والشرطة الجزائرية في إحصائية مشتركة عن أن الجزائر سجلت 2500 جريمة إلكترونية في 2017 تتعلق بالقرصنة والابتزاز والتشهير والتحرش الإلكتروني والاحتيال؛ ذكر ذات المصدر أن الجرائم الإلكترونية ترتفع كلما ارتفع عدد مستخدمي الإنترنت، حيث تم تسجيل 29 مليون جزائري مستعمل للإنترنت مع نهاية 2017، من بينهم 19 مليون جزائري يستخدمون موقع التواصل الاجتماعي "فيسبوك" وأن 80% من الجرائم المرتكبة تمت عن طريق مواقع التواصل الاجتماعي، كما أن وزراء ونواب في البرلمان وإطارات عليا في الدولة الجزائرية لم يسلموا من الجرائم الإلكترونية، خاصة ما تعلق منها بالابتزاز والتشهير والتهديد، والفيديوهات أو وثائق ورسائل نصيّة (بورنان، د.ت).

وفي سنة 2018 راسلت مصالح الوزارة الأولى –الحكومة- جميع الوزارات والمؤسسات الرسمية حذرت فيها من "انتشار تطبيق خبيث" عبر شبكة الإنترنت يسمى.(Kik Messenger) وأن هذا التطبيق يعمل على الإيقاع بضحاياه عبر موقع التواصل الاجتماعي فيسبوك وماسنجر، من خلال "حسابات وهمية بهوية نسائية، ويعمل على سرقة جميع بيانات المستهدَف، من رسائل وصور، وله القدرة على تحديد أماكنهم"، وسجلت مصالح المديرية العامة للأمن الوطني، المختصة في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال خلال الـــ 8 أشهر الأولى من السنة الجارية،567 قضية تتعلق بجرائم الإنترنت، تورّط فيها 543 شخصا.

حيث تمكنت الفرق المتخصـصــة في مكافحة الجرائم الإلكترونية للأمن الوطني ومن خلال معالجة كافة المعطيات التقنية والأدلة المادية المرتبطة بالقضـايا السـالفة الذكر، من معالجة 385 جريمة إلكترونية من أصـل 567 قضـية مسـجلة ومحل متابعة لفك خيوطها، وهذا وفق ما توضـحه المعطيات الواردة في الجدول التالي:

جدول رقم 01: جدول يبين عدد الجرائم الإلكترونية المسجلة لدى المصالح الأمنية الجزائرية خلال عام 2021

نوع الجريمة	القضايا المسجلة	القضايا المعالجة	عدد المتورطين	النسبة المئوية للقضايا المعالجة
جرائم المساس بالأشخاص عبر الإنترنت	430	289	365	%68
جرائم الاعتداء على سلامة الأنظمة المعلوماتية	57	31	39	%55
جرائم الاحتيال عبر الإنترنت	25	17	32	%68
جرائم التحريض والتطرف عبر الإنترنت	14	14	31	%100
الجرائم المخلة بالحياء	12	08	22	%67
جرائم بيع السلع المحظورة عبر الإنترنت	06	05	15	%84
جرائم مختلفة (نسخ برامج دون حق، القرصنة)	23	21	39	%92
المجموع	567	385	543	%68

المصدر: المديرية العامة للأمن الوطني

تُشـــير إحصـــائيات الدرك الوطني إلى أنه تم ارتكاب أكثر من 40 حالة احتيال تحت ســـتار تطبيق **"بريدي موب"** الذي أطلقته وزارة البريد والمواصـلات السـلكية واللاسـلكيّة، حيث تعرض موظفون من مختلف القطاعات الحيوية لعمليات النصـب والاحتيال، حيث يسـتخدم مرتكبو هذه الجرائم حسـابات الفيسـبوك التي تم اختراقها من خلال ربط اتصـال مع أصـدقاء الفيسـبوك من تلك الحســابات نفســها بغرض إقناع الضــحايا أنهم ســيســتفيدون من منحة مخصــصــة لوباء كوفيد 19(الشرطة الجزائرية تتصدى لصناع الكراهيّة عبر المنصات الرقميّة، د.ت: 35).

تذكرُ ذات المصـالح أنه خلال شـهر كانون الثاني 2021 تم الكشـف عن العديد من الإعلانات والإصدارات الخاصة بالتوظيف في العديد من الشركات الوطنية، العمومية وخاصة تلك البارزة منها، حيث تم نشرها على صـفحات وهميّة في وسـائل التواصـل الاجتماعي، وبالنظر إلى نوعية المناصـب المفتوحة فإن زوار الموقع قاموا بإرسال كافة بياناتهم الشخصيّة وحتى نسخ من جوازات السفر بُغيَّة التواصـل مع مسـؤولي هذه الصـفحات(الشرطة الجزائرية تتصـدى لصـناع الكراهيّة عبر المنصـات الرقميّة، د.ت: 36). كما أن من بين التحديات التي تطرح أيضاً؛ هو إمكانية استخدام الفواعل من غير الدول للتكنولوجيات الحديثة للتأثير وتســويق أفكارها، بالإضــافة إلى التجنيد والتخطيط وحتى نقل

الموارد عن طريق اختراق الحسابات البنكية والمصرفيّة، وأيضاً استهداف البنية التحتية للمعلومات بغرض تخريبها والتشويش عليها.

المحور الثالث: الأمن والدفاع السيبراني داخل الأجهزة الأمنية الجزائرية

يرى "دومينيك دافيد" أن الأمن في مفهومه الواسع يتمثل في خلو وضع ما من التهديد أو أي شكل للخطر، وتوفر الوسائل اللازمة للتصدي لذلك الخطر في حال أصبح أمراً واقعاً(الطيب، 2020: 428)؛ وبالنظر إلى التحول الذي طرأ على البيئة الدولية ببروز ظواهر جديدة كالتهديدات السيبرانية فقد فرض هذا الوضع على الدول ضرورة الاستعداد الكلي لمواجهة هذا الخطر.

المبحث الأول: تعريف الأمن السيبراني وأبعاده

يعرف الأمن السيبراني بأنه "مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصيّة واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني"، وهو "سلاح استراتيجي بيد الحكومة والأفراد، لاسيما أن الحرب السيبرانية أصبحت جزء لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول"(عطية، د.ت: 104).

قدمت وزارة الدفاع للولايات المتحدة الأمريكية أيضاً تعريفاً للأمن السيبراني فاعتبرته "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم، الهجمات، التخريب، التجسس والحوادث. واعتبر الإعلان الأوروبي أن معنى الأمن السيبراني هو "قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات"، وهذا ما عبّر عنه أستاذ الاتصالات بجامعة كاليفورنيا "ريتشارد كمرر" حيث عرفه "عبارة عن وسائل دفاعيّة من شأنها أن تكشف وتحبط المحاولات التي يقوم بها القراصنة"(بوغرارة، 2018: 107). ويتحقق الأمن السيبراني بضمان سلامة المعلومات أثناء وجودها في الفضاء المعلوماتي وأثناء عمليات النقل والمعالجة والتخزين ضد كل التهديدات التي يمكن أن تمس سلامتها أو تؤدي إلى توظيفها لإلحاق أي ضرر مادي أو معنوي سواء بالأشخاص أم المجتمعات أم الهيئات أم الدول(جعيجع، 2017: 69)، ويطال الأمن السيبراني جميع المسائل العسكرية، الاقتصادية، الاجتماعية، السياسية والإنسانية بهدف تحقيق منظومة أمن متكاملة تعمل على الحفاظ على الأمن القومي للدولة، وعليه تنطوي أبعاد الأمن السيبراني على(طالة، 2020: 62-65):

أ- البعد العسكري: تكمن الميزة في القدرة على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الإلكتروني، بما يسمح بسهولة تبادل المعلومات وتدفقها، وسرعة اتخاذ القرارات العسكرية، ومن ثم فإن عدم استغلال هذه التكنولوجيا سيؤدي من دون شك إلى شن هجمات إلكترونية مضادة على شبكات القوات العسكرية، ومن ثم تدمير قواعد البيانات.

ب- البعد الاقتصادي: أصبح الفضاء الإلكتروني جاذباً لقطاعات المجتمع كافة، وأصبحت المعرفة محركًا للإنتاج والنمو الاقتصادي، كما أن التركيز على التكنولوجيا والمعلومات يعد عاملاً من العوامل الأساسية للنهوض الاقتصادي، وهو ما دفع بالدول إلى

زيادة استثماراتها في المعرفة، وأصبحت عصرنة الاقتصاد مرتبطة بالتحكم بالاقتصاد الرقمي من طرف مختلف الفاعلين الاقتصاديين والاجتماعيين.

ج- البعد الاجتماعي: يعتبر من الخطوات الضرورية لتعزيز الأمن، لذا يعد تنظيم الحملات الإعلامية والتثقيف المدني لأجل مجتمع معلومات مسؤول من الضرورة بمكان، بحيث تغطي التحديات والمخاطر، وتدابير الأمنية الوقائية الرادعة لأجل تثقيف الأفراد.

د- البعد القانوني: تفرض التطورات التكنولوجية المتسارعة مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية في الفضاء السيبراني.

هـ- البعد السياسي: في ظل التسريبات المختلفة للوثائق السياسية، الحركات الاحتجاجية الإلكترونية، التظاهرات الإلكترونية..، بالإضافة إلى استغلال المواقع من طرف العديد من الحكومات لتمرير سياساتها، واستخدام هذه المواقع أيضاً من طرف الحركات الإرهابية لتجنيد أفرادها وجمع التمويل لعملياتها، وهذا ما يستوجب على الدول العمل على حماية أمنها من التهديدات والمخاطر التي قد تتعرض لها من خلال شبكة الإنترنت.

حتى يتحقق الهدف من الأمن السيبراني، لا بد من توفر مجموعة من العناصر مع بعضها البعض لتكمل الدور في ذلك، ومن أهم عناصر الأمن السيبراني (الحياري، د.ت)

أ- التقنية:(technology) تشكل التكنولوجيا والتقنية دورًا في غاية الأهمية في حياة الأفراد والمنظمات، حيث توفر الحماية الفائقة لهم أمام الهجمات السيبرانية، وتشتمل حماية الأجهزة بمختلف أشكالها الذكية والحاسوبية والشبكات بالاعتماد على جدران الحماية واستخدام البرامج الضارة ومكافحة الفيروسات وغيرها.

ب- الأشخاص :(People) يستوجب الأمر لزومًا على الأشخاص من مستخدمي البيانات والأنظمة في منشأة ما استخدام مبادئ حماية البيانات الرئيسية كتحديد كلمة مرور قوية، وتفادي فتح الروابط الخارجية والمرفقات عبر البريد الإلكتروني، إلى جانبِ القيام بعمل نسخ حتياطية للبيانات.

ج- الأنشطة والعمليات :(Process) يتم توظيف الأشخاص والتقنيات للقيام بالعديد من العمليات والأنشطة وتسييرها بما يتماشى مع تطبيق أسس الأمن السيبراني والتصدي لهجماته بكل كفاءة.

ينحو العالم اليوم إلى اقتصاديات الرقمنة ونظم الأتمتة والذكاء الاصطناعي، فمثلاً خصصت الولايات المتحدة الأمريكية للعام 2019 مبلغ 19 مليار دولار للأمن السيبراني، بزيادة قدرها 583.4 مليون دولار عن العام 2018، وكان لوزارة الدفاع الحصة الأكبر في تلك الميزانية، إذ أعلنت في عام 2019 عن تخصيص مبلغ 8.5 مليار دولار لتمويل نظم الأمن السيبراني بزيادة قدرها 340 مليون دولار عن العام 2018.

في سنة 2008 تمت بلورة استراتيجية سميّت بـــ "الجزائر الإلكترونية 2013" وكان من أهم أهدافها: تسريع استعمال تكنولوجيا المعلومات والاتصالات في الإدارة العمومية، المؤسسات الاقتصادية وعند الأفراد، تطوير البنية التحتية الخاصة بالاتصالات ذات التدفق العالي، التكوين

وتطوير البحث والابتكار في هذا المجال، كما أطلقت عدة مشـــاريع منها؛ أسرتك، المدينة الذكية سيدي عبد الله، مشروع التعليم الإلكتروني لطلبة الجامعات(بشاري، 2020: 587).

المبحث الثاني: الدفاع السيبراني

يعرف الدفاع الوطني بأنه "التشكيلة الاستراتيجية الشاملة للدولة التي تهدف إلى المحافظة على الدوام وأمام كل أشكال التهديدات الداخلية والخارجية على حرية ممارسات النشاطات وإنجاز الأهداف السـياسـية وتحديد المسـاهمات الدبلوماسـيّة والاقتصـادية والمالية والتربوية والثقافية والعسكرية ضمن هذا النمط"(لخضاري، 2012-2013: 253).

يُعرف الدفاع السيبراني بأنه آلية دفاع لشبكة الكمبيوتر تتضمن الاستجابة للإجراءات وحماية البنية التحتية الحيوية وضـمان المعلومات للمؤسـسـات والهيئات الحكومية والشـبكات الأخرى الممكنة. يركز الدفاع الإلكتروني على منع الهجمات أو التهديدات واكتشافها وتقديم استجابات لها في الوقت المناســب حتى لا يتم العبث بالبنية التحتية أو المعلومات. مع النمو في حجم وتعقيد الهجمات الإلكترونية، يعد الدفاع الإلكتروني ضروريًا لمعظم الكيانات من أجل حماية المعلومات الحساسة وكذلك حماية الأصول.(techopedia, s.d: n.p)

يحلل الدفاع السـيبراني التهديدات المختلفة المحتملة على بيئة معينة. ثم يسـاعد في ابتكار وقيادة الاســتراتيجيات اللازمة لمواجهة الهجمات أو التهديدات الخبيثة. يتم تضــمين مجموعة واسعة من الأنشطة المختلفة في الدفاع السيبراني لحماية الكيان المعني وكذلك للاستجابة السريعة لمشهد التهديد. يقوم الدفاع الإلكتروني أيضًا بإجراء تحليل تقني لتحديد المسارات والمجالات التي يمكن للمهاجمين اسـتهدافها. يمكن أن يشـمل ذلك الحد من جاذبية البيئة للمهاجمين المحتملين، وفهم المواقع الحرجة والمعلومات الحســاســة، والقدرة على اكتشــاف الهجوم وقدرات رد الفعل والاســتجابة.(techopedia, s.d: n.p). عموماً يشــمل الدفاع الســيبراني على ثلاث فئات متكاملة(شنوف، 2020: 101):

1- الدفاع السيبراني الاستباقي: وهي الأنشطة التي تحمي البيئة السيبرانية، وتحافظ على أعلى كفاءة للبنية التحتية السـيبرانية والوظائف المهمة من خلال الابتكار لتعزيز الفعل السـريـع أسرع من المنافســين الاســتراتيجيين، وحماية الشــبكات والأنظمة والوظائف والبيانات، ومواكبة التهديدات، والتكنولوجيات سريعة التطور في الفضاء السيبراني، الحفاظ على السلام والأمن السيبراني من خلال تعزيز قدرة الدول، بالتنسيق مع الحلفاء والشركاء على ردع ومعاقبة أولئك الذين يستخدمون الأدوات السيبرانية لأغراض ضارة.

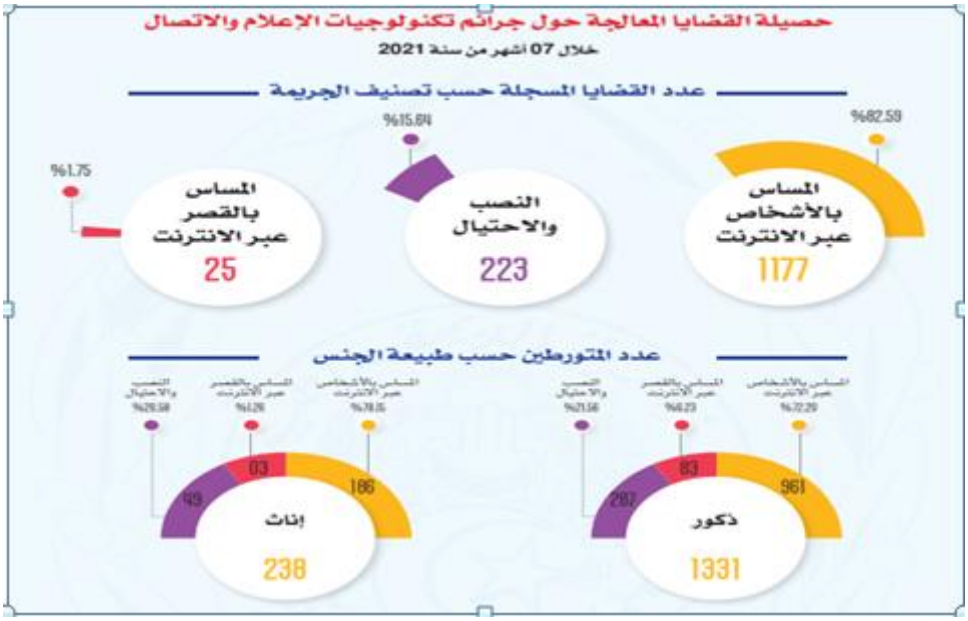
2- الدفاع الســيبراني النشــط: يوقف أو يحد من أضرار النشــاط الســيبراني للخصــم، وردع الأنشطة السيبرانية الضارة باستخدام جميع أدوات القوة الوطنية لردع الأعداء عن القيام بأي نشاط ضــار في الفضــاء الســيبراني، الذي يهدد المصــالح الوطنية، وإعطاء الأولوية لتأمين معلومات وزارة الدفاع.

3- الدفاع السـيبراني التفاعلي: يعمل على اسـتعادة الفعالية أو الكفاءة بعد الهجوم السـيبراني الناجح، هذه الفئات تشكل سلسلة متصلة من أنشطة الأمن السيبراني التي تحدث بشكل مستمر وفي وقت واحد على الشبكات، ووضع سياسات لأمن المعلومات ومراجعتها بشكل دوري.

شكل الأمن والدفاع السيبراني فلسفة جديدة في نظم الأمن والدفاع الوطني، فالدول الوطنية لم تعد تواجه أشـكال التهديدات الأمنية التقليدية وإنما عرفت هذه الأخيرة تطوراً وتحولاً في شـكلها ومصدرها، وبالتالي يتحتم على صناع الاستراتيجيات الأمنية بناء خطة استباقية لمجابهة التهديدات الأمنية الجديدة.

المبحث الثالث: الجهود الجزائرية في مكافحة التهديدات السيبرانية

تمكنت المصـالح العملياتية للأمن الوطني من ضـبط العديد من الشـبكات الإجراميّة التحريضيّة، الناشطة عبر الفضاء السيبراني، وذات الصلة بتنظيمات إرهابيّة تقوم ببث رسائل دعائية من شأنها التسويق لأفكار هدامة والترويج لسلوكيات وقناعات عدوانيّة منحرفة، مع إعادة مشاركة لمناشـير تحريضـية عبر مختلف التطبيقات ومواقع التواصـل الاجتماعي بغرض ضرب أمن الدولة (الشرطة الجزائرية تتصدى لصناع الكراهيّة عبر المنصات الرقميّة: 33).



شكل رقم 01: مصالح وزارة الدفاع الوطني

شـدد الفريق "شـنقريحة" على أن "مهمة حماية وتأمين الدفاع عن فضـائنا السـيبراني، هي مسـؤولية جماعية، تضـمن من خلال اسـتراتيجية وطنية شـاملة للأمن السـيبراني، يتعين أن ينخرط فيها الجميع، بداية من المواطن، من خلال وعيه بالمخاطر التي ينضـوي عليها هذا الفضـاء وتقيده الصارم بالإجراءات السليمة عند استخدام الوسائل التكنولوجية، فضلا عن دور المختصين في هذا المجال، عبر المساهمة بخبراتهم وآرائهم في إنجاح الاستراتيجية الوطنية، وصولاً إلى المسؤولين على كل المستويات.

وضـعت قيادة الدفاع الوطني الأمن السـيبراني أحد أولوياتها، على غرار باقي دول العالم التي سـارعت إلى مراجعة سـياسـاتها الأمنية، وإدراجها لآليات وميكانيزمات جديدة تعنى بهذه الوسـائل، بالموازاة مع تطوير البنيات الأسـاسـية المتعلقة بتكنولوجيات العالم الرقمي. وتجسـيداً لهذا بادرت

مؤسسة الدفاع الوطني إلى إعداد برامج خاصة لمجابهة الجريمة الإلكترونية والحد من انتشارها، وإنشاء أجهزة جديدة تنسجم في أدوارها وتجهيزاتها مع المتغيّرات الحاصلة في هذا المجال.

المصدر: وزارة الدفاع الوطني

استطاع الجيش الشعبي الوطني مسايرة التطورات التكنولوجية والإعلامية الحاصلة في العالم، ومن ثم تأمين وحماية نطاقه المعلوماتي، وتأمين الفضاء المعلوماتي لكل الناشطين فيه، وذلك من خلال التركيز على ثلاثة مرتكزات رئيسية وهي(سمير، 264:2017-270):

1- النص القانوني: أصدر قانون 04-15 المتضمن تعديل قانون العقوبات، حيث خصص قسمه السابع مكرر للمساس بأنظمة المعالجة الآلية للمعطيات.

أصدر قانون 09-04 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، يهدف هذا القانون إلى حماية أنظمة معالجة البيانات الآلية من الجرائم، ولديها أيضاً مجال للتحقيق نظراً إلى سرية الاتصالات، وخطورة التهديدات المحتملة، ويمكن أيضاً مراقبة الاتصالات الإلكترونية لمنع أفعال وصفت بأنها جرائم الإرهاب والتخريب والجرائم التي تطال أمن الدولة، أوتقديم معلومات حول هجوم محتمل على نظام معلومات بطريقة تهدد مؤسسات الدولة أو الدفاع الوطني، وكذلك لمتطلبات التحقيق في القضيّة، بحيث يصعب الوصول إلى استنتاج دون اللجوء إلى الوسائل الإلكترونية (Bahi Hichem, 2021).

جاء في نص المادة 394 مكرر 1 من قانون العقوبات الجزائري أنه "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"(غريسي، 2022: 163).

2- التطوّر التقني: تعتبر طبيعة الجريمة الإلكترونية وانفرادها بمميزات خاصة كانعدام الحواجز الجغرافية، وصعوبة الكشف عن هوية المستخدم من بين الدواعي التي تفترض التسلح بأحدث الوسائل التقنية للتمكن من مجابهة أخطارها، ولهذا يستلزم على الجهات المختصة بالتحقيقات في الجرائم المتصلة بالمعلوماتية أن تمتلك الوسائل والتقنيات اللازمة، ويمكن حصر ذلك في العناصر التالية:

- تنمية وتعزيز القدرات البشرية المكلفة بعمليات التحقيق في الجرائم الإلكترونية.
- توافر أحدث المعدات التكنولوجية في مجال الإعلام الآلي، الاتصالات اللاسلكية.
- التمتع بقاعدة بيانات واسعة محدثة باستمرار.
- القدرة على تصميم البرامج المعلوماتية وتطويرها.

3- الجهاز العملياتي: ويتمثل في المراكز والوحدات التي أنشأت لغرض مواجهة الجريمة الإلكترونية، ومدى استعدادها لأدائها من ذلك والمتمثلة أساساً في:

- **مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني؛** أنشأ في 2008، يوجد مقره ببئر مراد رايس، أهدافه تأمين منظومة المعلومات لخدمة الأمن العمومي، وهو بمثابة مركز توثيق، ويقوم بتحليل المعطيات والبيانات للجرائم المعلوماتية المرتكبة، ومحاولة تحديد هوية أصحابها، مما يُؤمن الأنظمة المعلوماتية للمؤسسات والبنوك والبيوت والشركات..، ويعمل على التنسيق الأمني بين الأجهزة الأمنية الأخرى، وقد استطاع المركز معالجة أزيد من 100 جريمة إلكترونية سنة 2014، وما يفوق 500 قضيّة رقميّة خلال سنة 2015(بوغرارة، 2018: 111).

- **المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:** يعتبر المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني مكسبا يدعم قدرات الدرك الوطني في مكافحة الجريمة بجميع أشكالها وذلك بإدراج العلوم في العدالة الجزائية، كما أن التحكم في التقنيات الحديثة من شأنه أن يدعم قدرات المؤسسة لمكافحة الإجرام المتطور باستمرار والذي يعتمد على التكنولوجيات الجديدة، من مهامه (الوطني، المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني، د.ت):

- انجاز الخبرات والتحاليل بناء على طلبات القضاة، المحققين والسلطات المؤهلة.
- الدعم التقني للوحدات أثناء التحقيقات المعقدة.
- تصميم بنوك معطيات وإنجازها وفقا للقانون.
- المشاركة في الدراسات والبحوث المتعلقة بالوقاية والتقليل من كل أشكال الإجرام.
- الإسهام في تحديد سياسة جنائية مثلى لمكافحة الإجرام.
- المبادرة بالبحوث المتعلقة بالإجرام وإجرائها باللجوء إلى التكنولوجيات الدقيقة.
- العمل على ترقية البحث التطبيقي وأساليب التحريات التي ثبتت فعاليتها في ميادين علمي الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي.
- المشاركة في تنظيم دورات تحسين المستوى والتكوين ما بعد التدرج في تخصصات العلوم الجنائية.

-المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني: له اختصاص وطني وطابع عملياتي بامتياز في مجال مكافحة الجريمة المنظمة في بعديها الوطني

والدولي، بالتنسيق مع الشركاء الأمنيين وتحت الإشراف الدائم للهيئات القضائية المختصة (المديرية العامة للأمن الوطني، د.ت)، من خلال تسخير تشكيل أمني مؤهل وكفء مهمته، جمع الأدلة والقيام بعمليات استباقيّة لوقف القرصنة ومختلف الجرائم الرقميّة، كما تعتمد على الأساليب الردعيّة من خلال التحريات وتقفي مجرمي المنصات الافتراضية وتسليمهم إلى الجهات القضائية المختصة من أجل تطبيق الإجراءات القانونية اللازمة(الشرطة الجزائرية تتصدى لصناع الكراهيّة عبر المنصات الرقميّة، د.ت: 32).

- **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها**: أنشا المشرع الهيئة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها سنة 2009 بموجب المادة 13 من القانون رقم 09-04 المؤرخ في 05 أوت 2009، وبالرجوع إلى المادة 14 من ذات القانون، فإنها حددت مهام الهيئة كالآتي(زكرياء، 2018: 421):

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم بتكنولوجيات الإعلام والاتصال.

- على مستوى الجيش الوطني الشعبي تم في نوفمبر 2015 استحداث مصلحة "الدفاع السيبراني ومراقبة أمن الأنظمة" على مستوى دائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي بهدف تأمين وحماية المنظومات والمنشآت الحيوية للبلاد، ضد التهديدات والإرهاب الإلكتروني (بليل، 2022:39) وتتمحّور استراتيجية الدفاع السيبراني للجيش الوطني الشعبي في محاور رئيسية(بوغرارة، 2018: 114):

1- الجانب الوظيفي والتنظيمي: لضمان فعالية وتناسق أعمال الدفاع السيبراني ضمن الجيش الوطني الشعبي، يعمل الجهاز على تأطير مجموعة من الآليات الوظيفية والتنظيمية.

2- الجانب القانوني: تعزيز وتحيين بصفة مستمرة للأطر القانونية التي تضمن التطوّر المتعلق باستعمال تكنولوجيات الإعلام والاتصال وتأمين منظومات الإعلام.

3- جانب الموارد البشرية: يتجلى نجاح بمدى جاهزية وتكوين المورد البشري وكفاءته العاليّة.

4- الجانب التقني: كفاءة الأجهزة والوسائل المستعملة، مع ضمان اليقظة عن الكشف والرد عن الهجمات السيبرانية.

- **تم استحداث في أوت 2021 قطب جزائي جديد مكلف بمتابعة الجرائم السيبرانية ومكافحتها**، في حين تتمحور استراتيجية الدفاع السيبراني للجيش الوطني الشعبي حول تعزيز وتحيين الإطار القانوني المتعلق باستعمال تكنولوجيات الإعلام والاتصال، وتأمين منظومات الإعلام، علاوة على تكوين مورد بشري تقني ذي كفاءة عالية في مجال الدفاع السيبراني(بليل، 2022: 22).

صـادقت الجزائر على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سـنة 2014 والتي توصي في مادتها الحادية والعشرـين على أن تلتزم كل دولة طرف بتشـديد العقوبات على الجرائم التقليدية في حالة ارتكابها بواسطة تقنية المعلومات.

أما على المسـتوى الإقليمي؛ احتضـنت الجزائر القمة الإفريقية للأمن السـيبراني (ACSS) في نسـختها الثالثة تحت شـعار "إفريقيا الرقمية الآمنة"، والتي نُظمت يومي 16 و17 نوفمبر 2022، بالمركز الدولي للمؤتمرات – "عبد اللطيف رحال"، وجمعت هذه القمة الإفريقية الرائدة في النظام البيئي لأمن تكنولوجيا المعلومات أكثر من 1000 مشارك يمثلون أكثر من 60 دولة. وسمحت القمة الإفريقية للأمن السـيبراني بمناقشة العديد من القضايا من مختلف الزوايا السـياسـية، الاسـتراتيجية، التقنية، القانونية والأخلاقية (زراقنية، الجزائر تحتضن القمة الإفريقية للأمن السيبراني في 16 نوفمبر 2022).

خطـت الجزائر خطوات كبيرة في مجـال الأمن والـدفـاع السـيبراني بـالنظر إلى التحـديـات السـيبرانية التي تواجه أجهزتها الأمنية، وذلك عقب الأحداث الأخيرة "حادثة بيغاسـوس" ومحاولة ضرب الأمن المجتمعي بنشرـ صـفحات مغرضـة تمس الأطفال؛ وعملت من جهة أخرى على إعداد الكوادر المؤهلة في هذا المجال، كما أولت القيادة العامة للدفاع الوطني أولوية لهذا المجال بعقدها للعديد من الندوات والحلقات النقاشية.

الخاتمة

تواجه الجزائر كغيرها من دول العالم تحديات جديدة تطرحها البيئة الدولية؛ فتهديدات الأمس لم تعد نفسـها تهديدات اليوم، ولم نعد أمام إمكانية تحريك الجيوش العسـكرية لتحقيق النصر، فيكفي فقط الضغط على زر الحواسيب الإلكترونية حتى تنجح عملية التخريب والتجسس؛ وبالتالي القضاء على النظم الدفاعيّة المعلوماتية.

تجدر الإشـارة إلى أنه يجب التعامل الجدي والأكثر صرامة مع هكذا نوع من التهديدات الجديدة التي أصـبحت تشـكل خطراً حقيقياً على الأمن بمفهومه الواسـع، حيث إن الأمر يقتضيـ تضافر جهود الجميع مؤسسات وأفراد، بالإضافة إلى القيام بحملات تحسيسيّة عبر تنظيم ملتقيات، اجتماعات وندوات وتنشـيط محاضرات، والأكثر من ذلك التركيز على وعي الأفراد بمدى خطورة الوضع، وأعلنت "فلة ڤوار"، رئيسة شركة« INTELLIGENT NETWOR »عن فتح أول مركز وطني للتكوين في قضايا الأمن السيبيراني في الجزائر، المعتمد من طرف المنظمات الدولية، والذي يهدف – حسـبها- إلى تعزيز تقنيات الدفاع والحماية ضـد مختلف أنواع الهجمات السـيبرانية التي تتعرض لها مختلف المؤسسات والبنى التحتية وحتى الأشخاص في الجزائر.

النتائج

- أن عجز المؤسسات الأمنية وأنظمة المراقبة فيها جعلها عرضة للتهديدات السيبرانية.
- كلما زاد حجم التهديدات السـيبرانية كلما شـكل ذلك تحدياً أمنياً للمنظومة الدفاعية الجزائرية.
- أن التهديدات الأمنية الجديدة والمرتبطة أسـاسـاً بالتكنولوجيا تفرض على المؤسـسـات الأمنية بناء خطة استراتيجية لمجابهتها.

- أن من يمتلك القوة المعلوماتية يعرف جيداً كيف يتحكم في الآخرين ويؤثر فيهم.
- برهن التصدي للهجمات الإلكترونية على مدى قدرة الأجهزة الأمنية الجزائرية وتأهبها.

التوصيات

ومن بين **التوصيات** التي خلصت إليها الدراسة نذكر:

- زيادة تأهيل العنصر البشري للتحكم في التكنولوجيات الرقميّة عن طريق فتح التكوينات الجامعية ذات الارتباط.
- الاستفادة من خبرات الدول المتقدمة كالولايات المتحدة الأمريكية، روسيا..، في مجال الأمن السيبراني.
- تنمية وتوعيّة الحس الوطني بمدى شدة وخطورة التهديدات السيبرانية عن طريق المنشورات، الحصص الإذاعية والتلفزيونية مع استضافة الخبراء.
- انفتاح المؤسسات الأمنية على الجامعة لتبادل الخبرات في مجال الأمن السيبراني ونظم الدفاع المعلوماتي، والمشاركة في صياغة البرامج التعليمية الأكاديمية في تخصص الأمن والدفاع السيبراني.

المراجع:

أولاً المراجع العربية

- الإذاعة الجزائرية. (د.ت). *الفريق شنقريحة: مواقع التواصل الاجتماعي ملاذ آمن لشبكات إجرامية معروفة بحقدها على الجزائر*. تاريخ الاسترداد 28 02, 2022، من https://radioalgerie.dz/
- إيمان الحياري. (بلا تاريخ). *ما هو الأمن السيبراني، وماهي معاييره؟* تاريخ الاسترداد 13 02, 2022، من https://www.mah6at.net/
- بارة سمير. (2017). الأمن السيبراني في الجزائر: السياسات والمؤسسات. *المجلة الجزائرية للأمن الإنساني*.
- بروال الطيب. (2020). إستراتيجية الجزائر للأمن والتنمية في منطقة الساحل الإفريقي. *المجلة الجزائرية للأمن الإنساني*.
- بشاري سلمى. (2020). تطوير الرقمنة في الجزائر كآلية لمواجهة مرحلة ما بعد جائحة كورونا 19. *Les cahiers du cread*.
- بليل سفيان. (2022). ترقية وتطوير الأمن والدفاع السيبراني. *مجلة الجيش*.
- بن خليفة إلهام، غريسي جمال. (2022). "التجسس الإلكتروني كجريمة ماسة بأمن الدولة في التشريع الجزائري"، *دفاتر السياسة والقانون. المجلد 14، العدد 01*.
- بوعون زكرياء. (2018). دور الهيئة الوطنية للوقاية من الجرائم الإلكترونية في حماية المستهلك. *مجلة العلوم الإنسانية*.

- بوغرارة يوسف. (2018). الأمن السيبراني: الإستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري. *مجلة الدراسات الإستراتيجية وحوض النيل*.
- بيرم, ف .(2020) .السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية .*المجلة الجزائرية للأمن الإنساني*.
- توفيق, سعد حقي .(2017) .*العلاقات الدولية* .بغداد: دار ومكتبة عدنان للطباعة والنشر.
- الجزيرة. (د.ت). *كيف يعمل برنامج التجسس بيغاسوس وهل فعلا أغلقته الشركة الإسرائيلية*. تاريخ الاسترداد 18 02, 2022، من https://www.aljazeera.net/
- جعيجع عبد الوهاب. (2017). *الأمن المعلوماتي وإدارة العلاقات الدولية*. الجزائر: دار الخلدونية.
- جيدور حاج بشير. (2018). تهاوي الحدود التقليدية بفعل الثورة الرقميّة الجديدة والتطوُّر الاتصالي والمعلوماتي. *الأزمات الحدودية: المعضلات والمخارج*.
- د.ذ.ك. (د.ت). *الأمن السيبرانية والدفاع السيبراني: رهانات وتحديات على ضوء التحولات الجديدة المتعددة الأبعاد*. تاريخ الاسترداد 13 02, 2022، من جريدة الجمهورية: https://www.eldjoumhouria.dz/art.php?Art=98918
- زراقنية مسعد. (د.ت). *الجزائر تحتضن القمة الإفريقية للأمن السيبراني في 16 نوفمبر 2022*. تاريخ الاسترداد 08 11, 2022، من https://edd-dz.net/126579.html
- سعود يحي ياسين. (د.ت). *الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني*. تم الاسترداد من المجلة القانونية: https://jlaw.journals.ekb.eg/
- شرايطية سميرة. (2020). السيادة السيبرانية في الصين بين متطلبات القوة وضرورات الأمن القومي. *المجلة الجزائرية للأمن والتنمية*.
- الشرطة الجزائرية تتصدى لصناع الكراهيّة عبر المنصات الرقميّة. (بلا تاريخ). *مجلة الشرطة*.
- شنوف زينب. (2020). الحرب السيبرانية في العصر الرقمي: حروب ما بعد كلاوزفيتش. *المجلة الجزائرية للأمن والتنمية*.
- طالة لامية. (2020). التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها. *مجلة معالم للدراسات القانونية والسياسية*.
- عطية إدريس. (د.ت). مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري. *مصداقية*.
- فرانس. (د.ت). *الجزائر تعلن فتح تحقيق حول عمليات التجسس تعرضت لها باستخدام برنامج بيغاسوس*. تاريخ الاسترداد 18 02, 2022، من https://www.france24.com/
- كلاع شريفة. (2022). الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني. *مجلة الحقوق والعلوم الإنسانية*.

- لخضاري منصور. (2012-2013). استراتيجية الأمن الوطني في الجزائر 2006-2011، أطروحة دكتوراه غير منشورة. جامعة الجزائر 03، كلية العلوم السياسية والعلاقات الدولية.
- للمستقبل, م. د .(s.d.) .رقمنة البنية التحتية الحيوية.
- مجلة الجيش. (2021). *التصيد الإلكتروني والقرصنة عبر الهاتف أو عبر شبكات التواصل الاجتماعي*.
- *المديرية العامة للأمن الوطني*. (بلا تاريخ). تاريخ الاسترداد 28 02, 2022، من https://www.algeriepolice.dz/
- المرزوقي ألاء. (د.ت). *الحرب السيبرانية: حرب المستقبل المفزعة*. تاريخ الاسترداد 13 02, 2022، من https://defense-arab.com/vb/threads/130964/page-4
- نوايسة زيد. (د.ت). *الهجمات السيبرانية التحدي القادم والأخطر*. تاريخ الاسترداد 05 11, 2022، من جريدة الغذ: https://alghad.com/
- وزارة الدفاع الوطني. (د.ت). *المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني*. تاريخ الاسترداد 12 02, 2022، من https://www.mdn.dz/

ثانياً: المراجع الأجنبية

- Bahi Hichem, M. W. (2021). Algerian LegislativeMechanisms to Combat Cybercrime and Achieve Information Security. *journal of right and fredoms, 09*(02), 1982.
- colard, d. (1977). *les relations internatinal de 1945 a nos jours*.paris: armand colin.
- Gunaratna, R. (2004). *The Changing Face of Terrorism*.Singapore: EasternUniversityPress.
- interpol. (s.d.). *cyber crime* .
- katieterellhanna, k. f. (s.d.). *cyberwarfare*. Consulté le 02 07, 2022, sur searchsecurity: https://www.techtarget.com/searchsecurity/definition/cyberwarfare
- p.w.singer. (s.d.). *darkterritory: the secret history of ciberwar by frdkaplan*. Consulté le 02 27, 2022, sur the new worktimes: https://www.nytimes.com
- seicherman, W. r. (1975). *technology and international politics*.london: lexington books.
- techopedia, d. (s.d.). *ciberdefence*. Consulté le 02 27, 2022, sur https://www.techopedia.com/definition/6705/cyber-defense

Bibliography:

First: Arabic References

- Al Jazeera. (n.d). How does Pegasus spy software work and has it been shut down by the Israeli government. Retrieved 18 February 2022, from https://www.aljazeera.net/
- Algerian police confront hate makers through digital platforms. (n.d). Police Journal.
- Algerian Radio. (n.d). *The Army General Chengriha:* Criminal networks known for their hatred of Algeria have found refuge on social media platforms. Retrieved February 28, 2022 from https://radioalgerie.dz/
- Almarzouki Alaa. (n.d). *Cyberwarfare:* A shocking future warfare. Retrieved February 13, 2022, from https://defense-arab.com/vb/threads/130964/page-4
- Al-moustakbel, (n.d). Digitisation of critical infrastructure.
- Atia Idris. (n.d). The status of cyber security in Algeria's national security system. *Credibility.*
- Bachari Selma. (2020). The development of digitalisation in Algeria as a response strategy to the post-COVID-19 a pandemic. *Les cahiers du cread.*
- Bara Samir. (2017). Cybersecurity in Algeria: Policies and institutions. The Algerian journal of Human security.
- Belil Sofiane. (2022). Enhancing and strengthening security and cyber defences. Army Journal.
- Benkhalifa Ilham and GhariciDjamal. (2022). “Electronic spying, a crime against state security in Algerian legislation”, Notebooks on Politics and Law. *volume fourteen- first issue-*
- Berouem Eltaieb (2020). The Algerian strategy for security and development in the African coast region. The Algerian journal of Human security.
- Bigram, F. (2020). National sovereignty regarding cyberspace and digital developments. The Algerian journal of Human security.

- Boughrara Youcef. (2018). Cyber defence: Algerian cybersecurity and defence strategy in cyberspace. *Journal of Strategic Studies and the Nile Basin.*
- Chenouf Zeineb. (2020). Cyberwarfare in the digital era: Post-Clausewitz Wars. Algerian Journal of Security and Development.
- *Cyber security and cyber defence:* Issues and challenges in the face of new multidimensional developments. (n.d). Retrieved 13 February 2022, from Al-Jumhuriya newspaper: https://www.eldjoumhouria.dz/art.php?Art=98918
- Djeidjaa Abdelouaheb. (2017). *Information security and international relations management.* Algeria: Khaldounia House.
- Frans. (n.d). Algeria announces the launch of a Pegasus software-based inquiry into the spying operations to which it has been subjected. Retrieved 02 18, 2022, from https://www.france24.com/
- Imane Al Hiyari. (n.d). *what are the definition and criteria of cybersecurity?* Retrieved February 13, 2022, from https://www.mah6at.net/
- Jaidor Haj Bashir. (2018). The disappearance of traditional boundaries with the new digital revolution and advancements in communication and information *Border crises:* Issues and solutions.
- Kelaa Cherifa. (2022). Cybersecurity, Spying Challenges and Cyber Hacks of states across Cyberspace. *Journal of Law and Human Sciences.*
- Lekdari Mensour. (2012-2013). National Security Strategy in Algeria 2006-2011, unpublished doctoral dissertation. University of Algiers 03, Faculty of Political Science and International Relations.
- Nouaissa Zeid. (n.d). Cyberattacks: the next and most dangerous challenge. Retrieved date 11 05, 2022, from Al-Ghad newspaper: https://alghad.com/
- Samira Cheraiteia. (2020). China's cyber sovereignty in light of force requirements and national security imperatives *Algerian Journal of Security and Development.*

- Saud Yahya Yassin. (n.d). Cyber warfare in light of the rules of international humanitarian law. Retrieved from the Legal Journal: **https://jlaw.journals.ekb.eg/**
- Tala Lamia. (2020). Cyberthreats and crimes: their impact on national security and counter-measures. *Maalem Journal for Legal and Political Studies.*
- The Army journal. (2021). Phishing and hacking by phone or via social networks.
- The Directorate General for National Security. (n.d). Retrieved February 28, 2022, from https://www.algeriepolice.dz/
- The Ministry of National Defence. (n.d). National Institute of Criminal Evidence and Criminology of the National Gendarmerie. Retrieved February 12, 2022, from https://www.mdn.dz/
- Toufik, saaf Haki. (2017). International Relations. Baghdad: Adnan Library and Publishing House.
- Zakaria Bouone. (2018). The role of the National Cybercrime Prevention Authority in consumer protection. Journal of Human science.
- Zerkania Mesaad. (n.d). Algeria hosts the African Cyber Security Summit on November 16, 2022. Retrieved 11 08, 2022, from https://edd-dz.net/126579.html

Second:Foreign references

- Bahi Hichem, M. W. (2021). Algerian Legislative Mechanisms to Combat Cybercrime and Achieve Information Security. *Journal of right and freedoms, 09*(02), 1982.
- Colard, d. (1977). International relations from 1945 to today.Paris: ArmandColin.
- Gunaratna, R. (2004). *The Changing Face of Terrorism.* Singapore: EasternUniversityPress.
- Interpol. (n.d). *cybercrime.*
- Katieterellhanna, k. f. (n.d). *Cyberwarfare*. Retrieved 02 07, 2022, fromsearchsecurity: https://www.techtarget.com/searchsecurity/definition/cyberwarfare
- p.w.singer. (n.d). *Dark territory: the secret history of ciberwar by frdkaplan*. Retrieved 02 27, 2022, from the New York Times: https://www.nytimes.com
- Seicherman, W. r. (1975). *Technology and international politics.*london: Lexington books.
- Techopedia, d. (n.d). *Cyber defence*. Retrieved 02 27, 2022, from https://www.techopedia.com/definition/6705/cyber-defense