جامعة قاصدي مرباح - ورقلة -

كلية الحقوق والعلوم السياسية

قسم العلوم السياسية

مذكرة تخرج لاستكمال متطلبات نيل شهادة الماستر في ميدان الحقوق والعلوم السياسية

شعبة العلوم السياسية

تخصص: دراسات أمنية و إستراتيجية

واقع الفضاء السيبراني و إشكالية الدفاع الوطني في الجزائر

إعداد الطالبة:

نورة العقون

إشراف الدكتور:

د/ عبد الكريم باسماعيل

أعضاء لجنة المناقشة

(الرتبة العلمية) اسم ولقب الأستاذ	الصفة
د/ محمد خميس	رئيسا
د/ عبد الكريم باسماعيل	مشرفا ومقررا
د/ فريدة طاجين	مناقشا

نوقشت وأجيزت يوم: 2019/06/11

السنة الجامعية: 2019/2018م

بسم الله الرحمن الرحيم

﴿ وَقُلِ اِعمَلُواْ فَسَيَرَى اَللّهُ عَمَلَكُم وَرَسُولُهُ
وَالمُومِنُونَ وَسَتُرَدونَ إِلَى عَلِمِ اِلغَيْبِ وَ
الشهَدَةِ فَيُنَبِئُكُم بِمَا كُنتُمْ تَعْمَلُونَ ﴾

صدق الله العظيم

سورة التوبة الأية 105

شكر وعرفان

الحمد لله الذي هدانا لهذا وما كنا لنهتدي لولا أن هدانا الله القائل في كتابه العزيز

"**ولا تنسوا الفضل بينكم** "الآية 237 من سورة البقرة،

والصلاة والسلام على نبينا محمد عليه أفضل الصلاة وأزكى التسليم وبعد

ارفع أسمى عبارات الشكر والعرفان إلى كل من ساندني في انجاز هذه المذكرة واخص بالذكر أستاذي العزيز "**باسماعيل عبد الكريم**" الذي كان له الفضل في إنجاز هذه العمل من خلال توجيهاته و أفكاره البناءة ونصائحه الدقيقة فشكر الله سعيك يا أستاذ وجعلك الله منارة من منارات العلم الخالدة.

وشكري الموصول إلى أعضاء لجنة المناقشة الموقرين على قبولهم مناقشة هذا العمل، كما لا يفوتني أن أتقدم بالشكر الجزيل إلى كل أعضاء هيئة التدريس والموظفين في جامعة قاصدي مرباح ورقلة.

والشكر موصول كذلك إلى جميع زملائي في العمل الذين لم يبخلوا علي بالمساعدة رغم كل مسؤولياتهم

الإهـداء

إلى من أمرني ربي أن أخفض لهم جناح ألذلي من الرحمة

"والداي الكريمين"

إلى جميع من ضحوا في سبيل العلم والمعرفة

إلى كـل عـائلة **"العقون"**

إلى جميع الأصدقاء والأحبة

اهدي هذا العمل المتواضع

نورة

الملخص:

تهدف هذه الدراسة إلى معالجة تأثير الفضاء السيبراني على إستراتجيات المنظومة الدفاعية في الجزائر، وبالتالي التعرف على هذا الفضاء وخصائصه وما نتج عنه من تهديدات سيبرانية تمس بالأمن القومي الجزائري ، مما فرض على الدولة الجزائرية تبني إستراتجية خاصة لمواجهة هذه التهديدات .

الكلمات المفتاحية: الجزائر ، الفضاء السيبراني ، التهديد ، الجريمة ، الأمن ، الدفاع ، القانون

Abstract:

This study aims to addressing body the find out the effect of Cybers pace on the defence strategies of the body in Algeria , in order to have a clear image of this space , its characteristics and what has resulted from it including cybernetic threats which targets the Algerian national security . this latter has obliged the Algerian government to adopt a specific strategy to face these threats .

Key words: Algeria , Cybers pace, the threat , the crime, Security , defence , Law.

Résumé :

Le but de cette étude est d'aborder l'impact du cyberespace sur les stratégies du système de défense en Algérie , Et ainsi d'identifier cet espace et ses caractéristiques et les cybermenaces qui en résultent pour la sécurité nationale algérienne , Ce qui a contraint l'Etat algérien à adopter une stratégie spécifique pour faire face .

Mots clés

Algérie, cyber espace, menace, défense, sécurité, criminalité, droit.

مقدمـة

أمام التطور الهائل الذي عرفته تكنولوجيا الإعلام والإتصال و إنعكاستها الإيجابية على جميع مناحي الحياة الإجتماعية ، الإقتصادية ، السياسية ، الثقافية ... و التي غيرت معالم القرن الواحد والعشرين وهذا بإيجاد بيئة مغايرة للبيئات الأربع (البحر ، البر، الجو ، الفضاء) ، والتي تعرف بيئة الفضاء السيبراني التي صنعها الإنسان إعتماداً على الأدوات التكنولوجية لينقلنا من العالم الواقعي إلى الفضاء الإفتراضي خاصةً بعد تعدد وسائل إمستخدمها هواتف ذكية ، أجهزة حاسوب ، لوحات تحكم . هذا الفضاء الذي فتح للجميع: أفراد ، مؤسسات الباب على مصرعيه لسباحة في بحر لا يعرف قواعد أو قيود مما أتاح لهم الفرصة لممارسة أعمالهم الإجرامية بكل حرية .

وفي المقابل أصبح مفهوم الدفاع يجلب إهتمام الكثير من الباحثين والأكاديميين في العلاقات الدولية ، وهذا ناتج عن طبيعته المتغيرة التي لاتعرف الثبات . فحياة المجتمعات البشرية مرتبطة بضرورة توفر الأمن والإستقرار ، وذلك لا يكون إلا بتوفر القدرات الدفاعية . ويعود تبلور مفهوم الدفاع بمدلوله الإستراتيجي إلى معاهدة وستفاليا سنة 1648 التي أسست معالم الدولة القومية ، وتطور إلى أن أصبح من إهتمام القانون الدولي بعد إلغاء حق الدول المشروع في الحرب ، وحل محله حق الدفاع المشروع من أجل الأمن الوطني للدولة .1

وبعد الحرب الباردة والإنتشار الواسع الذي عرفته الأسلحة النووية إتجهت الدول للحديث عن الدفاع النووي وكيفية بناء قدرات دفاعية نووية للحفاظ على مكانتها وردع أي تهديد من قبل الدول المعادية . إلا أنه ومع الألفية الجديدة ومواكبة لتطور الهائل لتكنولوجيا المعلومات وظهور ما يعرف بالفضاء السيبراني كان من الضروري أن تتجه الدول نحو بناء سياسة دفاعية تتلائم والتطور الحاصل في هذا المجال من أجل مكافحة تهديداته السيبرانية و هذا بتبني

---

1 –أسماء حداد ،<< الدفاع الوطني الجزائري:الواقع و الرهانات الاستراتجية >>، المركز الديمقراطي العربي ،207/05/24 ، على الموقع : https://democraticac.de/?p=4673 ، تم الإطلاع على صفحة الويب بتاريخ: 2018/07/12 .

نظاماً دفاعياً سيبرانياً يمكنها من الحفاظ على أمنها القومي .
وضمن هذا السياق ونظراً للتطور المتسارع الذي تشهده الجزائر في مجال التكنولوجيات الجديدة والتي مست جميع القطاعات فاصبح الحديث عن حكومة إلكترونية، تجارة إلكترونية ، بطاقات إلكترونية وتعداه هذا حتى للخدمات الإلكترونية ، إلا أن هذا لم يحيد الجزائر من التأثر بالجانب السلبي لهذه التكنولوجيا ومن هنا جاءت هذه الدراسة كمحاولة لمعرفة تأثير الفضاء السيبراني على المنظومة الدفاعية في الجزائر .

❖ **أهمية و أهداف الموضوع**

أ/ الأهمية العلمية:

يندرج موضوع البحث ضمن الدراسات الأمنية والإستراتجية و تبرز أهميته العلمية من خلال التعريف بالفضاء السيبراني و أشكال تهديداته التي تخل بالأمن القومي للدولة ودور هذه الأخيرة في رسم استراتجيتها الدفاعية.

ب/ الأهمية العملية:

إن موضوع الفضاء السيبراني من المواضيع التي تعنى بأهمية كبيرة لدى النظام ، باعتبار أن له تأثير على الأمن القومي الجزائري ، ومن هنا تبرز الأهمية العملية لهذه الدراسة من خلال معرفة كيفية تعامل الجزائر مع الفضاء السيبراني ، ومدى قدرتها في مواجهة تهديداته المختلفة .

و تهدف هذه الدراسة إلى :

- التعرف على أشكال التهديدات السيبرانية التي تواجهها الجزائر
- التعرف على جهود الدولة الجزائرية في التصدي لهذه التهديدات
- التوصل إلى بعض المقترحات والتوصيات لخدمة وتنمية الإستراتجية الدفاعية في المجال السيبراني .

❖ **مبررات اختيار الدراسة**

إن اختيار موضوع واقع الفضاء السيبراني وإشكالية الدفاع الوطني في الجزائر ، جاء مدفوعا بجملة من الأسباب منها ما هو موضوعي ومنها ما هو ذاتي، والتي يمكن حصرها في الآتي:

أ/الأسباب الموضوعية: تهدف هذه الدراسة إلى تقديم تصور تحليلي لواقع الدفاع الوطني في الجزائر في ظل الفضاء السيبراني ، من خلال توضيح جهود الدولة الجزائرية في مكافحة التهديدات التي أوجدها هذا الفضاء .

ب/ الأسباب الذاتية: إن الميول الشخصي لمختلف القضايا التي تمس الجزائر دفعني لإختيار هذا الموضوع من ضمن قائمة المواضيع المقترحة من قبل الأستاذ المشرف وهذا بهذف الا طلاع المعمق عليه خاصة انه موضوع حديث يعكس الوجه الأخر لتكنولوجيا وأخطارها إذا ما استعملت بطريقة غير مشروعة ، وكذا من أجل إثراء الرصيد العلمي والمعرفي باللغة العربية في هذا الموضوع .

❖ **الدراسات السابقة:**

إن أية دراسة علمية أو بحث أكاديمي يتطلب الرجوع والإطلاع على الدراسات السابقة في نفس المجال وهذا لفهم الموضوع وتوجيه الباحث للمسار الصحيح ، ومن الدرسات السابقة التي رجعت إليها بغرض الاستفادة :

✓ **دراسة لـ يوسف بوغرارة بعنوان : الأمن السيبراني : الإستراتجية الجزائرية للامن والدفاع في الفضاء السيبراني** مقال بمجلة الدراسات الإفريقية وحوض النيل، الصادرة عن المركز الديمقراطي العربي ، المجلد الأول ، العدد الثالث ، سبتمبر/ أيلول 2018 حيث حاول الباحث في هذه الدراسة الإجابة على الإشكالية الأتية : إلى أي مدى إستطاعت الجزائر أن تحقق الأمن والدفاع السيبراني في الفضاء السيبري ؟ إنطلاقاً من الفرضية الأتية : أدت الاصلاحات الجزائرية إلى تحقيق مستوى عالي من الأمن والدفاع السيبراني في الفضاء السيبري. وقد تطرق الباحث في هذه الدراسة إلى الأليات القانونية والمؤسساتية لمكافحة الجريمة السيبرانية في الجزائر ، و استراتجيات الدفاع وتحقيق الأمن

السيبراني للجيش الوطني الشعبي ، وفي الأخير أختتم الباحث هذا المقال بتقيم دور الجزائر في مجال الأمن السيبراني.

- ✓ **دراسة لـ سمير بارة بعنوان : الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر – الدور والتحديات –** ، مداخلة بالملتقى الدولي الثاني حول سياسات الدفاع الوطني بين الإلتزامات السيادية والتحديات الإقليمية ، جامعة قاصدي مرباح ورقلة يومي 30 و 31 جانفي 2017 . حيث عالج الباحث من خلال هذه الدراسة الإشكالية الأتية : ما هو دور الدفاع الوطني في تحقيق الأمن السيبراني في الجزائر أمام التحديات الوطنية والعالمية التي يفرضها الفضاء السيبراني حالياً و مستقبلاً ، حيث تم التطرق إلى النقاط الأتية : أساسيات عن الأمن السيبراني و الجريمة السيبرانية ، الدفاع الوطني وأليات تحقيق الأمن السيبراني ، عوائق تحقيق الأمن السيبراني وفي الأخير أختتمت الدراسة ببعض التوصيات التي يتبناها المرصد العربي للسلامة و الأمن في الفضاء السيبراني كوضع إستراتجية لنشر الوعي وبنائه لدى مختلف شرائح المجتمع ، وكذلك الإلتزام بالقرارات الصادرة عن الأمم المتحدة وعن القمة العالمية لمجتمع المعلومات ونشر ثقافة الأمن السيبراني .
- ✓ **دراسة لـ عنترة بن مرزوق ،" الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية"** ، مداخلة بالملتقى الدولي الثاني حول سياسات الدفاع الوطني بين الإلتزامات السيادية والتحديات الإقليمية ، جامعة قاصدي مرباح ورقلة يومي 30 و 31 جانفي 2017 . حيث عالج الباحث من خلال هذه الدراسة مفهوم الأمن السيبراني ، الإرهاب الإلكتروني كأحد أخطر التهديدات المحتملة على الأمن الجزائري في ظل الثورة التكنولوجية الحديثة ، والجهود الجزائرية في مجال الأمن السيبراني ، والأخير أختمت المداخلة بمجموعة من التوصيات : كإقامة العدة العسكرية السيبرانية بتكليف عدد كبير من الأفراد العسكريين بمهمة القتال الإفتراضي ، تكوين نخب وطنية مختصة في مجال الأمن السيبراني ، التعاون الإقليمي والدولي بتسيير تبادل المعلومات في مجال مكافحة الإرهاب الإلكتروني ، منع تحول الفضاء السيبراني إلى فضاء للحروب والنزاع بين الدول.

من خلال إطلاعنا على الموضوع تبين لنا أن هذه الدراسات تناولت النصوص القانونية لمكافحة الجريمة الإلكترونية وكذلك التطرق لجهود الجزائر على المستوى الداخلي من خلال الأجهزة الأمنية المختلفة (الأمن الوطني ، الدرك الوطني ، الجيش الوطني الشعبي) ، فحاولنا من خلال دراستنا هذه التطرق إلى جهود الدولة الجزائرية داخليا وخارجيا من خلال القوانين والإتفاقيات هذا من الناحية القانونية ، أما فيما يخص الجانب الأمني تم التطرق إلى مختلف الهياكل التنظيمية على المستوى الداخلي والخارجي .

❖ إشكالية الدراسة

إن الإستعمال غير المشروع من قبل العديد من الفواعل للفضاء السيبراني خلق تهديدات لاتمس بأمن الأفراد فقط بل مس كيان الدول بكامله ، والجزائر بإعتبارها جزاءا لا يتجزاء من الكيان الدولي لم تأخد موقف المتفرج في الساحة الدولية بل حاولت من خلال أجهزتها الأمنية المختلفة إلى الدفاع عن كيانها .

انطلاقا مما سبق نحاول في هذه الدراسةإثارة الجدل والنقاش الدائر حول إشكالية الدفاع الوطني في الجزائر في ظل الفضاء السيبراني ، وذلك بطرح الإشكالية التالية:

- **كيف يؤثر الفضاء السيبراني على منظومة الدفاع الوطني في الجزائر ؟**

❖ حدود الدراسة

أ/ **الحدود المكانية:** تتمثل حدود الدراسة في الفضاء السيبراني ، الجزائر بما أن الدراسة مخصصة للفضاء السيبراني وإشكالية الدفاع الوطني في الجزائر .

ب/ **الحدود الزمنية** : إبتداءا من شهر سبتمبر 2018 وهي بداية دراسة الموضوع إلى غاية ماي 2019 .

❖ فرضيات الدراسة

للقيام بتحليل موضوعي ومنطقي وللإجابة على إشكالية الدراسة وضعت الفرضية التالية:

*** كلما زاد عدد التهديدات السيبرانية بالجزائر كلما أثر ذلك على إستراتجيتها الدفاعية .**

❖ مناهج الدراسة

يعرف المنهج عند **عبد الرحمان بدوي** بأنه: " الطريق المؤدي إلى الكشف عن الحقيقة في العلوم ، بواسطة مجموعة من القواعد العامة تهيمن على سير العقل وتحدد عملياته حتى يصل إلى نتيجة معلومة " [1] ، وعليه فالمنهج هو الطريق الذي يسلكه الباحث للبحث عن الحقيقة والوصول إلى نتيجة .

ولدراسة الموضوع دراسة علمية تتماشى وطبيعته ولمعالجة كل الجوانب المتعلقة به تم إعتماد المناهج التالية:

* **المنهج الوصفي :** يعد أكثر المناهج اعتمادا في الدراسات الخاصة بالواقع الاجتماعي وهو يعتبر طريقة لوصف الظاهرة المدروسة وتحليلها و إخضاعها للدراسة الدقيقة و تم إستخدامه في الجانب النظري وهذا لوصف وتفسير الظاهرة محل الدراسة من خلال وصف الفضاء السيبراني وتبيان علاقته بالدفاع الوطني.

كما تم الاعتماد على **منهج دراسة الحالة:** والذي يعرف بأنهّ " المنهج الذي يتجه إلى جمع البيانات العلمية المتعلقة بأية وحدة كانت سواء فرداً أو مؤسسة أونظاماً إجتماعياً أو مجتمعاً محلياً أو مجتمعاً عاماً " [2] . وقد تم إستخدامه في الجانب التطبيقي من الدراسة .

---

1 –عبد الرحمان بدوي ، **مناهج البحث العلمي** ، ط3 ، الكويت : وكالة المطبوعة ، 1977 ، ص5.

2 –محمد شلبي ، **المنهجية في التحليل السياسي (مفاهيم – المناهج– الاقترابات)** ، الجزائر : ديوان المطبوعات الجامعية ، 1997 ، ص.87 .

3 - الإطار النظري

تم الإستعانا ببعض النظريات التي تمكننا من تحليل تاثير الفضاء السيبراني على المنظومة الدفاعية في الجزائر:

* **النظرية الواقعية الجديدة** : تركز هذه النظرية على إقامة التحالفات المتوازنة والقوة الدفاعية الرادعة هي التي تتحقق الأمن الدولي.

* **نظرية الحروب اللاتماثلية**: تقوم هذه النظرية على الانتقال من سلوك التهديد التماثلي إلى انتشار مظاهر التهديد اللاتماثلي، فتعدد الفواعل في الفضاء السيبراني ، ساهم في زيادة التهديدات على الدولة الجزائرية بشكل بات يتجاوز قدرة الدولة على مواجهتها.

كما تم الإعتماد على **الإقتراب القانوني المؤسسي** من خلال تناول النصوص القوانين و إنشاء الهياكل التنظيمية .

4 -مصطلحات الدراسة

حاولت تقديم بعض التعريفات الإجرائية لبعض مصطلحات الدراسة:

* **الفضاء السيبراني**: هو عالم إفتراضي يقوم على علاقة تفاعلية بين الإنسان و الألة ، يرتبط بالعالم الواقعي يؤثر فيه ويتأثر به .

* **التهديد** : هو كل فعل يراد به إلحاق الضرر بطرف آخر ، ويكون الغرض منه خلق حالة من الخوف و الرهبة قصد الإخلال بالأمن الداخلي للدولة المهددة

* **الأجهزة الأمنية** : هي مجموعة الهياكل التنظيمية ، المنشأة من قبل الدولة هدفها الدفاع عن الأمنها القومي.

❖ خطة الدراسة

تنقسم الدراسة محل البحث إلى مقدمة و فصلين وتليهما خاتمة:

حيث يتناول **الفصل الأول** الإطار النظري والمفاهيمي للدراسة في ثلاثة مباحث، المبحث الأول منها يتناول مفهوم الفضاء السيبراني وعلاقته بالمفاهيم ذات الصلة، بدءا من تعريف الفضاء السيبراني وتوضيح الفارق بينه وبين بعض المفاهيم شائعة الارتباط به. بينما يتعرض المبحث الثاني مفهوم الدفاع الوطني وعلاقته بالمفاهيم ذات الصلة ، أما المبحث الثالث فيبحث في العلاقة بين الفضاء السيبراني والدفاع الوطني .

أما **الفصل الثاني** فيتناول واقع الدفاع السيبراني في الجزائر انطلاقا من التهديدات السيبرانية المتربصة بالجزائر وهذا في مبحث أول. وتم تناول جهود الدولة الجزائرية في مجال الدفاع السيبراني في مبحث ثاني من خلال التطرق إلى جهود الدولة الجزائرية في الجانب القانوني و الجانب الأمني داخلياً و خاريجياً.

❖ صعوبات الدراسة

ليس من السهل التعرض بالدراسة لإشكالية الدفاع الوطني في الجزائر في ظل الفضاء السيبراني ، فالدراسات الأكاديمية ذات الصلة المباشرة بهذا العنوان قليلة جدا ، و الإنعدام الكلي لها بمكتبة الكلية ، نظرا لحداثة الموضوع وتوفر المراجع باللغة الإنجليزية أدى إلى تعدد الترجمات مما صعب من عملية إيجاد المصطلح الدقيق ، هذا بالنسبة للجانب النظري والمفاهيمي .

أما بالنسبة للجانب التطبيقي واجهت صعوبة في الحصول على المعلومة وهذا لطبيعة الموضوع الحساسة وكذلك لتكتم الجهات الأمنية على المعلومة مما دفعني للبحث في عدد كبير من مجلات الجيش لعلي أجد ضالتي وهذا ما أخد مني وقت طويل .

الفصل الأول

الإطار النظري والمفاهيمي للدراسة

الفصل الأول : مفهوم الفضاء السيبراني وعلاقته بالدفاع الوطني

من الواضح أن تواجد ثورة المعلومات وظهور الانترنات قد فاجأ جميع الدول وفرض عليها الكثير من التحديات خاصة مع بروز بيئة مغايرة للبيئات الأربع (البر ، البحر ، الجو ، الفضاء) وهي بيئة الفضاء السيبراني ومن أهم هذه التحديات ضرورة تطوير الجانب الدفاعي مواكبةً مع هذه التطورات ، وهذا ما سنعالجه من خلال هذا الفصل وذلك بتقسيمه إلى ثلاث مباحث ، الأول تناولت من خلاله مفهوم الفضاء السيبراني ، والثاني تحت عنوان التعريف بالدفاع الوطني ، أما المبحث الثالث لدراسة العلاقة بين الفضاء السيبراني و الدفاع الوطني .

المبحث الأول: مفهوم الفضاء السيبراني وعلاقته بالمفاهيم ذات الصلة

إن قدرة الفضاء السيبراني على التأثير في النظام الدولي والتغيير في مفاهيمه التقليدية الإرهاب ، الجريمة ، الحرب ، الدفاع ، الردع، الأمن أتاح للجميع: دول ، منظمات ، أفراد الفرصة للاستفادة منه وهذا نتيجة لما يتميز به من سهولة الإستعمال وقلة التكلفة .

- **تعريف الفضاء السيبراني**

- **تعريف الفضاء**

لغةً: مصدر مأخوذ من الفعل الثلاثي (فضا ، يفضو ، فضواً ، فهو فاض) و **الفضاء** : هو المكان الواسع ، والفضاء الخارجي الفارغ الواسع من الأرض ، يقال : أفضيت إذ خرجت إلى الفضاء[1] .

1 – أبي منصور محمد بن أحمد الأزهري . **تهذيب اللغة** ، الدار المصرية للنشر ، مادة " فضا " .

✓ **إصطلاحاً** : هو كل ما يقع خلف الغلاف الجوي للأرض ، أو هو كل ما يقع في الإرتفاع حوالي (1000كم) فوق سطح البحر ، فهو يضم سائر الأجرام السماوية في الكون بما فيها الشمس والقمر والنجوم والمذنبات [1].

ويشير مصطلح " الفضاء" إلى مجالات التفاعلات التي :[2]

- تنشئ مصادر محتملة للقوة
- توفر توسيع النفوذ و التأثير
- تمكن الخدمات الجديدة أو الموارد أو المعرفة أو الأسواق
- تحقق المزيد من الإمكانات عند تعزيزها و إستمرارها من خلال التقدم التكنولوجي .

➢ تعريف السيبرانية:

✓ **لغةً** : مشتقة من كلمة سيبرنتيك أو كيبرنتيك وهي مفردة مشتقة من اللغة الإغريقية القديمة من كيبرنتسين أي القائد أو قائد السفينة كما قد تكون مشتقة من كيبرنتيكا أي فن قيادة السفن أو من كيبرنيسيس أي منصب قيادي في الكنيسة.[3]

و عرفها قاموس المورد بأنها" علم الضبط و مصدرها Cy-ber.net.ics "[4].

✓ **إصطلاحاً** :

أصل المصطلح " **السيبرنتيك**" وهو مصطلح له أصل يوناني قديم في البداية

1- عبد الله عبد الطائي عبيد ، **أحكام الفضاء في الفقه الإسلامي** ، بيروت : دار الكتب العلمية . د ت، ، ص 14 .

2- Nazli Choucri , **Cyberpolitics International Relations** , The Mitpress Cambridge , Massachusets , London , p.05.

3- د م ، **سيبرنيتيك** ، على الموقع : https:/m,marefa.org ، تم الإطلاع على صفحة الريب بتاريخ : 2018/08/12 .

4- رمزي منير البعلبكي ، **المورد الحديث : قاموس إنكليزي – عربي حديث** ، بيروت : دار العلم للملايين ، ص 307 .

كان يعني إدارة القوارب ، وفيما بعد القرن التاسع عشر إستعمله العالم الفرنسي الشهير " أمبير" للتعبير عن علم خاص للادارة الإجتماعية السياسية[1].

فالخطوة الأولى المحددة والحاسمة للسيبرنتيك كعلم مرتبطة قبل كل شيء بإسم العالم الرياضي الأمريكي " نوربرت وينر **Norbert Weiner** ، فبظهور كتاب " وينر " المنشور عام 1948 تحت عنوان " السيبرنيتك أو الإدارة والرابطة في الحيوانية و الآلية " قدم من خلاله تعريف لـ **cybernetics** مفاده أن التفاعل بين الحيوان و الألة يخلق لنا بيئة مغايرة للإتصال .[2]

ومن التعريفات الموجودة في المؤلفات حول موضوع السيبرنتيك نجد أن أكثر تعريفين مستخلصين من خصائص السيبرنتيك التي عرضها " وينر" :[3]

التعريف الأول : وهو تعريف يقوم على مقولة الإدارة ، وضع من قبل العالم السيبرنتيكي السوفياتي " أبيرج Birg " وحسبه فإن **السيبرنتيك** هو علم إدارة الجمل* الديناميكية المعقدة ، فالإدارة هي مقولة أساسية لسيبرنيتيك ، ولهذا فإن التعريف المشار إليه يعبر بشكل ملائم عن حقيقتها .

التعريف الثاني : وهو تعريف يقوم على مقولة الإعلام ، حيث يعرف **السيبرنتيك** كعلم لعمليات إستلام (جمع) ، إرسال (نقل) ، إعادة تشكيل (تحليل) حفظ و إستعمال المعلومات في الجمل الديناميكية المعقدة .

فمن خلال هاتين التعريفين يتضح أن جوهر السيبرنتيك وموضوعه مرتبطان بالعمليات الإدارية الإعلامية .

فالسيبرنتيك : هو علم التوجيه و التحكم بالآلات ولا سيما الأتوماتكية ، هو الحال في الآلات الحاسبة الإلكترونية و الطائرات الأسرع من الصوت و

1- م يانكوف، ل يوتوفا ، **السيبرنتيك والاعلام** ، (ترجمة : برهان العلى)، بيروت : دار الطليعة ، ط 1 ، 1979 ، ص 07 .

2 - **المرجع نفسه** ، ص 10 .

3- **المرجع نفسه** ، ص 14.

* بمعنى الأنظمة أو الأنساق .

الطائرات بدون طيار ، والصواريخ الموجهة والمركب الفضائية والأقمار الصناعية . وقد أصبحت السيبرنتيك منهجاً أو مدخلاً علمياً في دراسة الظواهر شديدة التعقيد وذات الطابع المنظومي أكثر منه فرعاً علمياً متخصصاً في دراسة ظواهر محددة[1] .

ومن خلال المفاهيم المقدمة لكل من المصطلحين " **السيبرانية** " و " **الفضاء** " و بالربط بينهما يعتبر الكاتب الإمريكي وليام جيبسون William Gibson (1984) أول من قدم تسمية رسمية للساحة الجديدة ، وهو التفاعل الذي نعرفه الآن بإسم " الفضاء السيبراني " ، في حين أن تعيين الفضاء السيبراني يمثل تحولاً في الفهم ، والأكثر أهمية هي ميزاته التي تسمح بالتفاعلات بين البشر بطرق لم تكن ممكنة من قبل . ومن الأهمية بشكل خاص هي الطرق التي تستخدم بها المواقع السيبرانية لتشكيل الأفكار، وتبادل المعلومات وزيادة الوصول إلى المعرفة وطرق بديلة لتفكير .[2]

فإختلاف التعريفات حول الفضاء السيبراني يرجع لطبيعة كل دولة أو كيان وما الإمكانيات المكتسبة لتعامل مع مجال الفضاء السيبراني و إمكانية إستغلال مزياه والقدرة على مواجهة الأخطار الكامنة فيه.

وفيما يلي مجموعة من التعريفات الواردة عن الفضاء السيبراني :

- **معجم أوكسفورد :** عرفه على أنه " البيئة الإفتراضية التي يتم عبرها إتمام عملية الإتصال عبر شبكات الكمبيوتر"[3].
- **معجم كامبردج :** فعرفه على أنه " منطقة وهمية بلا حدود ، حيث يمكننا

---

1 – يوسف لازم كماش ، عبد الكاظم جليل حسان ، **سيكولوجية التعلم والتعليم** ، ط 1 ، عمان: دار الخليج ،2018 ، ص 324. .

2– Nazli Choucri , **op.cit** , p. 07.

3– **معجم أوكسفورد** ، الفضاء السيبراني على الموقع :

http://en.exforddictionaris.com /définition/cyberspace. تم الإطلاع على صفحة الويب بتاريخ : 2018/09/10 .

التعرف على الناس و إكتشاف المعلومات حول أي موضوع " [1]

❖ و عرفه قاموس " **Glassary Of Key Information Security Terms** " على أنه " نطاق عالمي في بيئة المعلومات يتألف من شبكة الإعتماد المتبادل للبنى التحتية لأنظمة المعلومات بما في ذلك الانترنت وشبكات الإتصالات والكمبيوتر ، الأنظمة و المعالجات المضمنة ووحدات التحكم "[2]

❖ وعرفته **الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI)** *: أنه " فضاء التواصل من خلال الربط البيني العالمي لمعدات المعالجة الألية للمعطيات الرقمية " [3]

❖ وعرفه **المعهد الوطني للمعايير والتقنية الأمريكية (NIST)** : أنه الشبكة المترابطة من البنى التحتية لتكنولوجيا المعلومات ، والتي تشمل الأنترنت وشبكات الإتصالات السلكية والاسلكية والنظم الحاسوبية والمعالجات المدمجة وأجهزة التحكم"[4]

وهناك من يرى أنه يمثل البعد الخامس للحرب كما يعرف على أنه " المجال المادي وغير المادي الذي يتكون من عناصر أجهزة الكمبيوتر ، والشبكات والبرمجيات وحوسبة المعلومات والمحتوى ومعطيات النقل والتحكم و مستخدمو كل هذه العناصر ، حيث تعد كل هذه العناصر العامل المشترك في جميع

1- معجم كامبردج ،الفضاء السيبراني، على الموقع:
http://dictionory.combridage.org/fr/dictionnaire/englais/cyberpace
تم الإطلاع على صفحة الويب بتاريخ : 2018/09/10 .

2- Richard Kissel , "Glassory Of Key Information Security Terms " ,National Institute Of Standards and Tchnology , U S , Department of commerce ,Revision,2,May,2013 , p.57 .

* وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي .

3- إسماعيل قادير، " إدارة الحروب النفسية في الفضاء الإلكتروني : الإستراتجية الأمريكية الجديدة في الشرق الأوسط " ، مداخلة ضمن فعاليات الندوة الدولية الموسومة بـ عولمة الإعلام السياسي وتحديات الأمن القومي للدول النامية ، جامعة الجزائر 03 ، ص04 .

4- جيه جي إي تريمبلاي ،<< الأمن السيبراني منهج مرجعي عام>> ، **مجلة أكاديمية الدفاع الكندي** ، أكتوبر 2016 ، ص17 .

محاور إستخدام الفضاء السيبراني ، سواءا كانت الجهات المستخدمة قادرة على تعظيم قيمتها وقدرتها بما في ذلك رفع كفاءة العنصر البشري أم كانت في مرحلة متأخرة .[1]

برغم من وجود العديد من التعريفات للفضاء السيبراني إلا أنه لم يتكمن حتى الآن من إيجاد تعريف مشترك له وهذا لإختلاف الرؤى حوله ، إلا أن كل التعريفات تتفق في أن هناك علاقة تأثير وتأثر بين الألة و العنصر البشري.

ويمكن القول أن **الفضاء السيبراني** هو عالم افتراضي يعتمد على نظم الكمبيوتر وشبكات الأنترنت يتداخل مع عالمنا الواقعي يتأثر به ويؤثر فيه فهو يعرف بساحة المعركة الخامسة للحرب بعد الجو ، البحر، البر و الفضاء والذي يعتبر العنصر البشري جزاء لا يتجزأ منه.

❖ الفضاء السيبراني و المفاهيم ذات الصلة

لحداثة مصطلح الفضاء السيبراني أعترف العديد من المختصين في مجال الكمبيوتر بوجود تداخل بين مصطلح الفضاء السيبراني مع من مجموعة المصطلحات المشابها له مثل الفضاء الإلكتروني ، المعلوماتي و الرقمي.

➢ **الفضاء السيبراني و الإلكتروني :**

عرفته **هيئة الأركان الأمريكية** على أنه " مجال يتميز بإستخدام الالكترونيات الكهرومغناطسية لتخزين تأثيرات متحركة أو ساكنة ضد الإشارات (الرادار، وأجهزة الاتصال) ونقاط ربط وشبكات النظام الدفاعي حيث يتم الوصول إلى الهدف بسرعة الصوت أو بسرعة الضوء عند إستعمال قدرتها الفضائية الإلكترونية.[2]

1- ربيع محمد يحي ،<< إسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط >>، **رؤى إستراتجية** ، المجلد رقم: 1، العدد رقم: 2 ، يونيو 2013، ص67 .

2- عادل عبد الصادق ، << الفضاء الالكتروني وتهديدات جديدة للأمن القومي >> **قضايا إستراتجية**، المركز العربي لأبحاث الفضاء الإلكتروني ، فبراير 2012 ، 2013/02/11 ، على الموقع : www.accronline.com/print-aspx?id=8745 تم الإطلاع على صفحة الويب بتاريخ 2018/012/12:

كما يعرف على أنه " المجال الكهرو مغناطيسي لتخزين وتعديل أو تغيير البيانات المتصلة والمرتبطة بشبكة البنية التحتية الطبيعية ، ويتضمن عملية الإندماج مابين الأنترنات و المحمول و أجهزة الاتصالات والأقمار الصناعية ، والفضاء الإلكتروني أكبر من الانترنت ، لما يحتويه من قدرات توجيهة للطاقة التي توجد في جزء من الموجات الكهرو مغناطسية .[1]

ويعمل الفضاء الالكتروني تحت ظروف مادية غير تقليدية حيث يكون وسيطاً عبر العمل من خلال أجهزة الكمبيوتر وشبكات الاتصال .[2]

فإذا كان الفضاء الإلكتروني يهتم بالأحداث داخل الجهاز الإلكتروني والتفاعلات الحاصلة بين أجهزته المختلفة أو الأجهزة المتصلة به ، في حين أن الفضاء السيبراني يدرس التفاعل الحاصل بين الأنترنت و الأجهزة الإلكترونية و العنصر البشري من أجل إتمام عملية الإتصال .

- **الفضاء السيبراني و المعلوماتي :**

المعلوماتية عرفها **كلود شانون** * على أنها عبارة عن سيل من النبضات الرقمية التي تقاس كميتها بدلالة المقاييس الرقمية (Bits . Bytes).

أو أنها عبارة عن كل أنواع البيانات التي تم تجميعها بالملاحظة أو المراقبة او التدوين مسموعة كانت أو مرئية وتمتاز بكونها قابلة للمعالجة بتقنيات الحاسوب والأليات المعلوماتية المتاحة فتتحول إلى خطاب يحمل دلالة معرفية قابلة للتغيير والتداول بما تضمن إكتساب الجهات التي تستخدمها معارف

1- عادل عبد الصادق ،<< الفضاء الالكتروني والرأي العام تغير المجتمع والأدوات ، و التأثير>> ، **قضايا إستراتجية** ، المركز العربي لأبحاث الفضاء الالكتروني ، 2011/08/26 ، على الموقع : www.accronline.com/article-detail.aspx?id=2725 تم الإطلاع على صفحة الويب بتاريخ : 2018/12/12

2- إيهاب خليفة ،<< القوة الإلكترونية و أبعاد التحول في خصائص القوة >>، 2014/06/30 ، على الرابط : https://www.middle-east-online.com ، تم الإطلاع على صفحة الويب بتاريخ: 2019/01/21 .

* خبير معلوماتية أمريكي من مواليد 1916/04/30 توفي في 2001/02/24 .

وحقائق قابلة للاستثمار في شتى ميادين الأنشطة المعاصرة [1].

فالمعلوماتية هي عملية ترجمة البيانات داخل الحاسوب وتحويلها إلى خطاب يحمل العديد من الدلالات في حين أن السيبرانية تعني جمع البيانات ونقلها وتحليلها ، فإذا كان الفضاء المعلوماتي يهتم بترجمة الكم الهائل من المعلومات وتحويلها إلى خطاب له معنى ، فإن الفضاء السيبراني التفاعل الحاصل بين المعلومات المترجمة داخل الجهاز والعنصر البشري وكيفية التعامل مع المعلومة ، فما يميز مصطلح الفضاء السيبراني عن الفضاء المعلوماتي والإلكتروني فهو يشمل المصطلحين وذلك بإعتباره بنية ذي ثلاث طبقات هي :[2]

01 – **الطبقة المادية** : تشمل معدات الحواسيب ، والبرمجيات ، والمعدات الضرورية لعملية الربط البيني للأجهزة .(الفضاء الإلكتروني)

02 – **الطبقة المنطقية** : تشمل مجموعة البرامج المترجمة للمعلومة على شكل معطيات رقمية حيث يتم الإنتقال من لغة الإنسان إلى لغة الآلة في شكل خوارزمية ومنها إلى برامج مطورة بلغة مبرمجة .(الفضاء المعلوماتي)

03 – **الطبقة الإعلامية** : و تتمثل هذه الطبقة في البعد البشري الذي يضاف إلى الطبقتين السابقتين ، حيث أنه في الفضاء السيبراني يظهر تفاعل الإنسان مع الأنترنات وهذا من خلال (عنوان بريد إلكتروني ، رقم هاتفه النقال ، صورة رمزية على مواقع التواصل الإجتماعي .

1– كريمة شافي جبر الكعبي ، << مجتمع المعلومات في العالم العربي – العراق أنموذجا – >> ، **مجلة كلية الأدب** ، الجامعة المستنصرية ، قسم المجتمع المدني ، العدد 98 ، ص. 718 .

2– إسماعيل قادير ، **نفس المرجع السابق** ، ص 5 .

➢ خصائص الفضاء السيبراني:

ينفرد الفضاء السيبراني بمجموعة من الخصائص التي تميزه عن البر، البحر، الجو و الفضاء ويمكن إجمال هذه الخصائص فيما يلي:[1]

- ✓ الفضاء السيبراني يعتمد على المجال الكهرو مغناطيسي ، فبدون هذا المجال تفقد تكنولوجيا المعلومات والإتصالات (HCT) ، القدرة على العمل.
- ✓ تتوفر البدائل بإستمرار في الفضاء السيبراني على عكس الجو ، البحر، البر، الفضاء والذي يوجد فيه ميدان واحد ، ففي ميدان الجو مثلاً يحسم الأمر بتدمير طائرة العدو ، في حين أن في الفضاء السيبراني عند إغلاق مواقع لأشخاص مثلا تبقى أمال هؤلاء إمكانية فتح موقع جديد بإسم مختلف في ساعات قليلة.
- ✓ سهولة إصلاح الشبكات و إعادة بنائها، بفضل قلة تكلفة الأجهزة وتوفرها .
- ✓ أسبقية الهجوم على الدفاع في الفضاء السيبراني ، لأسباب متعددة ، منها أن الهجوم يحدث بسرعة كبيرة ، ومن أي مكان في العالم ، دون تحديد المصدر ،أو المسؤول عنه.
- ✓ الفضاء السيبراني يتألف من أربع طبقات ، و السيطرة على إحداهما لايعني السيطرة على بقية الطبقات : البنى التحتية ، البنى المادية ، و طبقتان السيميائية و النحوية .

مع إستثناء يتعلق بما ينوي اللاعب القيام به ، فإذا كان المقصود تعطيل الشبكة يكفي تدمير البنى التحتية ليصبح ذلك فعلياً .

- ✓ يعتمد الفضاء السيبراني (cyber pace) كمجال إفتراضي على نظم الكمبيوتر وشبكات الأنترنت ومخزون هائل من البيانات والمعلومات بحيث يتم الإتصال بالشبكات غير الحواسيب أو الهواتف أو غيرها من

1- أنديرا عراجي ، **القوة في الفضاء السيبراني : فصل عصر من التحدي والإستجابة** (رسالة لنيل دبلوم دراسات عليا في العلوم السياسية و الإدارية ، جامعة لبنان: كلية الحقوق والعلوم السياسية والإدارية)، 2015/ 2016 ، ص. 18 .

دون تقيد بالحدود الجغرافية [1].

ويتكون الفضاء السيبراني من :[2]

- **المكون الأول** : الطبيعي أو المادي وهو الذي يتمثل في الأسلاك والمحولات والبنية التحتية كالكبلات .

- **المكون الثاني** : يتمثل في المحتوى والذي يعكس شكل المعلومة في لفضا السيبراني .

- **المكون الثالث** : فيتمثل في عملية التوصيل بين المعلومات والبشر وحركة التفاعل ما بين البرمجيات والمعدات ، و إرتباط ذلك بتصورات وقيم وسلوك المستخدمين من البشر ، كما أصبحت المعلومات متوافرة لها قيمة إقتصادية وقيمة ميدانية بالنسبة إلى الجهات وكلما زادت فعالية إدارة تلك المعلومات زادت الفائدة التي يمكن الحصول عليها و أصبح تفوق المعلومات إحدى القيم الأساسية للقوة العسكرية و أصبحت المعلومات مجالا لسيطرة والتحكم ، ويتعلق ذلك بعمليات المعلومات التي تشير للبيئة التي يمكن من خلالها شن عمليات الهجوم والدفاع والتي تكون متصلة ومستخدمة عبر الشبكات .

فالفضاء السيبراني ليس محض إفتراضية ، وهو يشمل على أجهزة كمبيوتر التي تخزن البيانات بالإضافة إلى الأنظمة والبنية التحتية التي تسمح بالتدقيق وهو يشمل الأنترنت من أجهزة الكمبيوتر المتصلة بالشبكة المغلقة ، الشبكة الداخلية والتقنيات الخلوية وكابلات الالياف الضوئية والإتصالات الفضائية .[3]

1- دويب حسين صابر، " القوانين العربية وتشريعات تجريم الجرائم السيبرانية وحماية المجتمع "، مداخلة بجمعية المكتبات والمعلومات ، الرياض ، 3-2009/11/4 ، ص 02 .

2- عادل عبد الصادق ،<< الفضاء الالكتروني وتهديدات جديدة للأمن القومي >>، ص3.

3- Peter w Singer And Allanfriedam , **Cybersecurity And Cyberwar, what Everyone Needs to know**, USA:University of oxfordpress,2014,p13 .

المبحث الثاني : مفهوم الدفاع الوطني وعلاقته بالمفاهيم ذات الصلة

ظهر مفهوم الدفاع مع وجود الإنسان على وجه الأرض و صراعه مع الحياة ، حيث ارتبطت حياة المجتمعات البشرية بضرورة توفير الأمن والاستقرار ، و لا يكون ذلك إلا بتوفر القدرات الدفاعية .[1]

❖ تعريف الدفاع الوطني

من الصعب أن نجد تعريف موحد لدفاع الوطني وهذا لتعقيد هذا المصطلح وصعوبة إستعابه من زاوية واحدة .

فقد ميز الأستاذ " **برنارد شانتيو** " بين ثلاث تصورات مختلفة لمصطلح " الدفاع الوطني" [2]:

الأول : مصطلح الدفاع الوطني يعني الجيش .

الثاني: يعني مجمل العوامل المؤثرة في مصير نزاع مسلح ما .

الثالث : يتخد معنى واسعاً لدرجة الخلط بينه وبين مفهوم السياسة العامة للأمة ، ومن أنصار هذا التصور الجنرال الفشي " **توني ألبورد** " لدرجة أنه اقترح إستبدال مصطلح الدفاع الوطني بمصطلح القوة الوطنية .

وعرفته **الموسوعة العالمية** على أنه " مجمل الإجراءات بمختلف أوجهها (السياسية و العسكرية والإقتصادية) المتخذة من قبل الدول بغية ضمان إستقلالها وتأمين سلامة و أمن إقليمها وكذا حياة شعبها أمام جميع أصناف الإعتداءات " [1]

1- أسماء حداد ، **نفس المرجع السابق .**

2- العميد محند الصالح إسريق ، " مفهوم الدفاع الوطني في القانون الجزائري" ، مداخلة ضمن فعاليات ملتقى الدفاع الوطني بين الالتزامات السيادية والتحديات الإقليمية، كلية الحقوق والعلوم السياسية ، جامعة ورقلة ، 13/12 نوفمبر 2014 ، ص46 .

3- **المرجع نفسه** ، الصفحة نفسها .

ومن هنا يمكن القول أن مجمل التعاريف تتفق اليوم وعلى نطاق واسع ، على أن مفهوم الدفاع الوطني يتمحور حول مقاربتين أساسيتين [1]:

أ) **المقاربة الأولى** : تتمثل في جرد الوسائل المسخرة للدفاع والتي تقوم على إعداد جرد أو مدونة للقطاعات والنشاطات وأشكال الحياة الوطنية التي تهم الدفاع ، إلا أن ما يميز هاته المقاربة هو أنها ناقصة ، قليلة الدقة ، ويشوبها الغموض .

ب) **المقاربة الثانية**: تتمثل في الأهداف المسندة للدفاع الوطني ، وتتمحور حول حماية سلامة الإقليم والأمن والإستقرار و الوحدة الوطنية .

رغم إختلاف المقاربتان في السياق إلا أنهما تبقيا متكاملتان في لغاية .

ومن خلال ماسبق يمكن تعريف الدفاع الوطني على أنه جميع الإجراءات المتخذة من قبل الدولة والشاملة لجميع القطاعات لمواجه التهديدات المحيطة بها من أجل المحافظة على إستقرار أمنها القومي .

- **أبعاد الدفاع الوطني** :

للدفاع العديد من الأبعاد التي تشترك في بناء الدولة

- ✓ **الطابع الشمولي و المستديم :**

ينبني مفهوم الدفاع تبعاً للتهديدات العسكرية و غير العسكرية ما يستدعي القيام بدراسة طبيعة تلك التهديدات وكذلك الإستعداد لها في مجال التراتيب القانونية والموارد والهياكل القاعدية ولا يتعلق الأمر فقط بالتخفيف من مواطن الضعف والهشاشة وتقليص الخسائر والأضرار في حالة النزاع أو الكوارث و التزود بوسائل الرد والهجوم لأي عدوان محتمل .[2]

1- **نفس المرجع السابق** ، ص: 47 .

2- جان لوك ماتيو ، **الدفاع الوطني** ، كوساج للمنشورات الجامعية .1996 .ص .03

✓ **الطابع المواطني:**

يعد الدفاع تعبيراً عن الإرادة الجماعية لمجتمع ما أين تقتسم الأمة نفس الموروث التاريخي والمصير وتدافع عن وجودها بشكل تضامني وتحمي وسائلها ومواردها المادية والمعنوية . وهذا التعريف يعطي مكانة خاصة للمواطنة كعنصر مركزي للمفهوم .[1]

➢ **المؤسسات المشاركة في سياسات الدفاع الوطني**

في وقتنا الحالي لم يعد تجسيد الأبعاد الدفاعية للدولة المعاصرة مقتصراً عن المراكز والمؤسسات الرسمية لدولة بخلاف مايراه البعض من أن المؤسسات العسكرية هي وحدها التي ترسم معالم الدفاع الوطني ، فحقيقة هذه المؤسسات هي الجهاز العملي والأداة التي من خلالها تتجسد الرؤي الإستراتجية للدولة [2].

فسياسات الدفاع الوطني تشترك فيها العديد من المؤسسات والجهات نجد أهمها:[3]

✓**مراكز البحوث والمؤسسات التعليمية** : التي يوكل إليها أمر البحث عن حلول للمشكلات بمختلف أشكالها سواء تعلق الأمر بالأبعاد الإجتماعية أو السياسية أو الإقتصادية ، هذه المؤسسات التي ينبغي أن تسعى من خلال الأموال المرصدة لها إلى البحث عن الحلول لكل الإشكالات العالقة و إيجاد آليات عملية لذلك دون الوقوف عل الأبعاد النظرية التقليدية.

1- أسماء حداد، **نفس مرجع سابق** .

2- براهيم بن داود، عبد الكريم جمال ، "الدفاع الوطني بين متطلبات الأمن الفكري ومقومات الأمن الإستراتجي" ،مداخلة ضمن فعاليات ملتقى الدفاع الوطني بين الالتزامات السيادية والتحديات الإقليمية، كلية الحقوق والعلوم السياسية ، جامعة ورقلة ، 13/12 نوفمبر 2014 ، ص470 .

3- **المرجع نفسه** ، ص ص ، 470-471 .

✓**المخابر ومراكز الدراسات الإستشرافية** : سياسة الدفاع الوطني تتبني على النظرة المستقبلية للأمور فالوقاية أهم من العلاج ، فالدراسات الإستشرافية تجعلنا في منأى عن العديد من المخاطر وتضعنا أمام أهذاف و إستراتجيات ينبغي تحقيقها .

✓**المجتمع المدني** : يعد المجتمع المدني أبرز وأهم الكيانات التي من خلالها يتم الوصول إلى بعد توعوي متكامل يجمع بين المنظور المجتمعي ولو كان بسيطاً والمنضور المؤسساتي.

✓**المؤسسات الإعلامية** : يلعب الإعلام دوراً هاماً في الإشادة بالجهود المبذولة وفي توعية المجتمع أيضاً بالأدوار المنوطة به في تحقيق السياسات العامة للدولة في تحقيق الرؤى الدفاعية المتكاملة .

وبهذا نجد أن السياسات الدفاعية تقود إلى مجموعة من الأفكار التي ينبغي أن تكون ملقحة ومتكاملة ولا يقتصر الأمر على البعد التنفيذي الإجرائي المتمثل في العمليات العسكرية فحسب ، فلابد أيضاً من إستخدام البعد المعلوماتي التقني في الترصد والبحث والمراقبة .

❖ الدفاع الوطني والمصطلحات ذات صلة

يرتبط بمصطلح الدفاع العديد من المصطلحات التي يمكن إجمالها فيما يلي:

➢ **الأمن والدفاع :**

الأمن من المفاهيم الأساسية في الدراسات الأمنية ، فهناك العديد من التعريفات لهذا المصطلح ، فقد عرفته **موسوعة العلوم الإجتماعية** على أنه : " قدرة الدولة على حماية قيمها الداخلية من التهديدات الخارجية " [1] .

وعليه فإن الأمن يتعلق بالحماية والدفاع عن كيان الدولة ووحدة أرضيها من

1- محمد شلبي ، " الأمن الوطني في ظل التحولات الدولية الراهنة "، مداخلة ضمن فعاليات ملتقى الدولة الوطنية والتحولات الدولية الراهنة ، جامعة الجزائر، كلية العلوم السياسية والإعلام ، 2004 ، ص157.

التهديدات الداخلية والخارجية ، وتحصيل أهذاف المواطنين عامة و إهتماماتهم المتعلقة بالإستقرار والطمأنينة والتمسك الإجتماعي والتنمية الإقتصادية [1].

فتحقيق الأمن صار مند مدة طويلة يقوم على الإمكانيات العسكرية و أسلحة الردع الذي صارا من صميم الدفاع ، هذا الأخير الذي أعطى السلاح مكانة هامة في مجال توفير الأمن ، لذا فإن فكرة الأمن ومصطلح الدفاع يؤديان إلى تكوين فكرة الإستمرار في الوجود بالنسبة للدولة . كما أن وحدة الدولة وقوتها تقوم على أساس الأمن ، فمن أجل توفير الأمن للدولة لابد لها أن تكون في أتم الاستعداد للحرب ، مهما كان نوعها و وسائلها خاصة ما تعلق بالجانب الدفاعي ، فلا يمكن الحصول على الأمن إلا بسياسة دفاعية قوية تكون متكئة على الجيش والقيادة اسياسية المتحكمة في زمام الأمور .[2]

- **الردع و الدفاع**

الردع مفهوم سياسي ويقصد به " فن إستخدام الوسائل و القوى لتحقيق الهذف دون الوصول إلى مرحلة الإشتباك ، ويكون هذف الردع ، منع إي قوة معادية من إتخاد قرار بإستخدام الأسلحة ، أو منعها – أي القوة المعادية – من الإقدام على فعل (أو رد فعل) إزاء موقف معين . ويفشل الردع عندما يبداء القتال"[3].

1- **نفس المرجع السابق** ، ص 157.

2- محمد غربي،<< من أجل مفهوم جديد لنظرية الدفاع والأمن: حالة منطقة البحر الأبيض المتوسط >> ، جامعة الشلف ، على الموقع :

www.Revws-Univ-Ouargla.dz/index-php/numero-01-2009-dafater/511-2013-05-02 10-48-57 ، تم الإطلاع على صفحة الويب بتاريخ :2019/02/24

3- بوحنية قوي و أخرون ، **فهم الأمن القومي من مذخلي الأمن الوطني والدفاع الوطني** (عمان : دار ومكتبة الحامد ، ط . 1 ، 2015) ص 50 .

فالحقيقة أن دعم المقدرة الدفاعية للدولة يدعم في نفس الوقت من قدرتها على الردع وهو ما يمكنها من إحباط الهجوم قبل أن يبداء فعلاً لأن الردع يسبق الدفاع ، و إخفاق الردع هو الذي يؤدي بالدولة التي يستهدفها الهجوم إلى الانتقال إلى المرحلة التالية عليه وهي اللجؤ إلى الدفاع الفعال عن كيانها ومصالحها وسيادتها الإقليمية في مواجهة أعدائها [1].

- **الهجوم والدفاع**

إنطلاقا من العبارة المشهورة " أفضل وسيلة للدفاع الهجوم " لا طالما إرتبط مصطلح الدفاع بالهجوم فلا يمكننا التحدث عن الدفاع إذ لم يكن هناك هجوم ، فالحديث عن العلاقة التي تربط الدفاع بالهجوم تدفعنا للحديث عن مصطلح الدفاع الوقائي .

فالدفاع الوقائي هو مبادرة دولة ما بالهجوم إستجابة لتهديد وشيك بإستخدام القوة من قبل دولة أخرى وقبل أن يتم فعلياً ولا يلزم أن تصل الأعمال الدفاعية إلى حد شن حرب على الطرف الآخر.[2]

---

1 –نصر الدين الاخضري ، " الجيش الوطني الشعبي بين واجب حماية الحدود والالتزام بالمشاركة في بعث أسباب التنمية" ،مداخلة ضمن فعاليات ملتقى الدفاع الوطني بين الالتزامات السيادية والتحديات الإقليمية، جامعة ورقلة ، كلية الحقوق والعلوم السياسية ، 13/12 نوفمبر 2014 ، ص 61 .

2 –سامي الزبيدي ، << الدفاع عن النفس في ضوء القانون الدولي ميثاق الأمم المتحدة >> ، 2018/07/02 ، ، على الرابط: www.azzaman.com ، تم الإطلاع على صفحة الويب بتاريخ 2018/12/04.

المبحث الثالث : علاقة الفضاء السيبراني بالدفاع الوطني

بتحول مفهوم التهديدات بالفضاء السيبراني (الجريمة ، الإرهاب ، الحرب) و إنتقالها من المفهوم التقليدي إلى السيبراني سمح بتغير في مفاهيم مواجهة هذه التهديدات (الدفاع ، القوة ، الأمن ، الردع ، الهجوم) بما يتلائم معها .

❖ التهديدات السيبرانية

➢ الجريمة السيبرانية

نتيجة ازدياد استخدام شبكة الانترنت في كثير من المعاملات ا لإلكترونية أصبحت مجالاً خصباً لكثير من الأفعال الإجرامية والتي أطلق عليها الجريمة الإلكترونية Cyber Crime والتي تجد مكانها في الفضاء السيبراني Cyber Space عبر شبكة الانترنت.

والمقصود بجرائم الانترنت ، والمسماة أيضاً الجرائم السيبرانية Cyber Crime هو " أي نشاط غير مشروع ناشئ من مكون أو أكثر من مكونات الانترنت مثل : مواقع الانترنت ، البريد الإلكتروني "[1] .

وتتعدد الجرائم السيبرانية وتتنوع حسب أهدافها مابين جرائم ذات دافع سياسي أو ذات ارتباط بالأمن القومي أو العسكري ، وبين جرائم ذات طبيعة جنائية والتي بدورها تتنوع مابين جرائم إقتصادية أو جرائم متعلقة بأمن وسلامة الأشخاص ، ومن أهم هذه الجرائم جريمة القرصنة والاحتيال ألمعلوماتي ، وتبيض الأموال ، والجرائم المخلة بالآداب والجرائم المتعلقة بسلامة شبكة المعلومات كتعطيل أو فساد أنظمتها والإستلاء على المعلومات التي بها ، وجرائم السرقة والقتل [2] .

1- خالد ممدوح إبراهيم ، **أمن الجريمة الإلكترونية** ، الإسكندرية : الدار الجامعية ، 2008 ، ص. 56.

2- **المرجع نفسه** ، ص57 .

✓ **مرتكبو الجريمة السيبرانية :**

يغزو الفضاء السيبراني مجموعة من القراصنة الذين ينشطون بكل حرية و إستقلالية ،و لكل واحد منهم أهدافه الخاصة ، ثراءه غير الشرعي ، سياسته ، إيديولوجيته ...الخ ، [1]

ومن أنواع القراصنة نجد :[2]

* **الهاكرز** : أو الهواة ويطلق هذا الإسم على القراصنة الذين يتخدون من الجرائم الالكترونية والقرصنة هواية أو فضول ليس أكثر ويكون غرضها تخريبيا ليس لتحقيق غايات ، وتكون غالبا من الفئة الشبابية المصابة بهوس التعمق بالمعلومات الإلكترونية والحاسوب .

* **الكراكرز**: وهم القراصنة المحترفون ويعد هذا النوع من أكثر أنواع مرتكبي الجرائم السيبرانية خطورة ، ويكون القراصنة من هذه الفئة ذوي مكانة إجتماعية عادية أو متخصصة في العلوم الالكترونية .

* **الطائفة الحادقة**: تستهذف غالبا هذه الفئة المنظمات والمنشآت و أرباب العمل ، ويكون الهدف من إرتكابها للجريمة ضد الاطراف بغية الانتقام والحصول على المنفعة المادية أو السياسية ، وقد يكون ترف أو جاسوس أو مخترق الأنظمة .

✓ **الحرب السيبرانية :**

إن الحروب التقليدية تغير مفهومها اليوم بوجود التطور التكنولوجي حيث أصبحت الجيوش االعسكرية تهتم بحرب المعلومات ودورها في حرب المستقبل.[1]

---

1 –لطفي لمين بلفرد ، <<التهديدات الأمنية في الفضاء السيبراني الجزء الثاني>> ، **مجلة الشرطة** ، العدد رقم: 129 ، الجزائر، ديسمبر 2015 ، ص 138 .

2 –فضيلة عاقلي ، " الجريمة الالكترونية و إجراءات مواجهتها م خلال التشريع الجزائري "، مداخلة ضمن فعاليات مؤتمر الجريمة الإلكترونية ، طرابلس لبنان ، 24-2017/03/25 .

3 –نسرين الصباحي ، << الحروب السيبريانية و تحديات الأمن العالمي >>، المركز العربي للبحوث و الدراسات ، على الموقع : http://www.acrseg.org/40594 ، تم الإطلاع على صفحة الويب بتاريخ: 2019/01/12

فالعنف ألمعلوماتي يمارس اليوم عن طريق قوى إفتراضية إشتهرت بحرب المعلومات وهي تختلف جوهرياً عن القوى التقليدية الصلبة ، أو الحرب التقليدية ، فحرب المعلومات تعمل بالجدب والترغيب لا بالضغط والترهيب وتخاطب العقول والقلوب ، من أجل إكتساب الآراء لا كسب الأرض ، ومن أجل إنتزاع الإرادة الجماعية لا نزع السلاح والملكية ، ومن أجل فرض المواقف و الآراء بدلاً من فرض الحصار والجوع ، لذا أصبح توسيع نطاق الإعلام في مقام نشر القوات ، وأصبحت الأجندة في مقام التكتيك والهوائيات والفضائيات في مقام ترسانات الأسلحة ومضادات الصواريخ ، وأصبح التلفزيون ، والأنترنات ، وغيرها من وسائل الإعلام آلات حرب ، ومن حيث أسلوب الممارسة ، تختلف حرب المعلومات عن نظيراتها في القدرة الهائلة من المناورة زمنياً وجغرافياً ، وتمارس بصورة مستمرة ودائمة ، بينما لاتستخدم القوة في الحرب التقليدية إلا في حالة الضرورة [1].

فهناك العديد من التعريفات للحرب السيبرانية تستند أولاً إلى البيئة التي تتم فيها عمليات الإعتداء فنجد من يعتبرها " صراعات و إعتداءات ترتكز على الأنترنات وتحركها أهذاف سياسية على المعلومات و أنظمتها ، ويمكنها أن تؤدي فيما تؤدي ، إلى وقف الخدمات الأساسية ، وسرقة المعلومات السرية ، وشل النظام المالي ، تعطيل المواقع الرسمية وشبكات الإتصال .[2]

كما يمكن أن تفهم بصورة عرضية على أنها حرب تجرى في الفضاء السيبراني بإستعمال واستهداف تكنولوجيا المعلومات والإتصالات .[1]

---

1 – محمد طوالبية ، <<إيديولوجية الفضاء الرقمي دراسة في الخلفيات المرجعية>> ، **الأكاديمية لدراسات الإجتماعية و الإنسانية** ، جامعة الشلف،ع 21 ، جانفي 2019 ، ص ص . 47-48

2- منى الأشقر جبور، **السيبرانية هاجس العصر**، المركز العربي للبحوث القانونية والقضائية ، ص 66 على الموقع : https://www.carjj.org/sites/default/files/ebooks/cyber.ebook.pdf

3- 1- حمدون إ توريه ، << البحث عن السلام السيبراني>> ، **الإتحاد الدولي للاتصالات**، يناير 2011 ، ص 7

ويعرفها كل من **ريتشارد كلارك و روبرت كناكي** على أنها " أعمال تقوم بها دولة تحاول من خلالها إختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها "[1].

وتعتبر الحرب السيبرانية المستوى الأخطر للنزاع في الفضاء السيبراني ، فهي تهدف إلى التأثير على الإرادة السياسية للطرف المستهدف وقدرته في عملية صنع القرار، وكذلك التأثير فيما يتعلق بالقيادة العسكرية وتوجهات المدنين في مسرح العمليات الإلكترونية .[2]

✓ **خصائص الحرب السيبرانية :**

تتميز الحرب السيبرانية بالعديد من الخصائص ومنها: [3]

- حروب لاتناظرية (Asymmeric) : فالتكلفة المتدنية نسبياً للأدوات اللازمة لشن هكذا حروب يعني أنه ليس هناك حاجة لدولة ما مثلاً وقدرات هائلة ومتطورة لتفرض تهديداً خطيرا وحقيقياً على دولة قوية.
- تمتع المهاجم بأفضلية واضحة : فهذه الحروب تتميز بالسرعة والمرونة والمراوغة، وبأفضلية المهاجم عن المدافع، وصعوبة نجاح عمليات الأخير.
- فشل نمادج الردع المعروفة : إن صعوبة تحديد الهجمات الإلكترونية ، وإستغراق الوقت الطويل لرصدها وعدم إمكانية تتبع مصدرها كلها عوامل تلغي مفهوم الردع بالإنتقام أو العقاب.

1- Richarda Clarke & Rebert Knake , **Cyber War : The Next Threat to National Security and What to de about it** , Harper Collins , 2010 , p.06 .

2- سليم دحماني ، **أثر التهديدات " السيبرانية " على الأمن القومي الولايات المتحدة الأمريكية أنموذجاً (2001- 2017)** ، (مذكرة ماستر ، جامعة محمد بوضياف المسيلة ، كلية الحقوق والعلوم السياسية) ، 2018/2017 ، ص 49 .

3- << المجال الخامس ..الحروب الإلكترونية في القرن ال 21>> ، مركز الجزيرة لدراسات ، 2011/01/12 ، على الموقع :
http://www.studies.aljazeera.net/ar/issues/2010/20117212274346868.htm
تم الإطلاع على صفحة الويب بتاريخ ، 2018/11/12

- المخاطر تتعدى استهداف الواقع العسكرية : وهذا بإستهداف البنى التحتية المدنية والحساسة كشبكات الكهرباء والطاقة والنقل والنظام المالي والمنشآت الحساسة النفطية أو المائية أو الصناعية وهذا بواسطة فيروس يمكنه إحداث أضرار مادية حقيقية تؤدي إلى إنفجارات أو دمار هائل.

❖ **الأسلحة السيبرانية :**

وتتمثل الأسلحة التي تستخدم في هذا الفضاء في الفيروسات بأنواعها المختلفة ، حيث تعرف **الفيروسات** على أنها برامج تم تصميمها لإلحاق الضرر بقواعد البيانات، أو سرقتها وتخريبها أو قطع الإتصال بالشبكة علماً أنه يصعب التعرف أو إكتشاف هذه الأسلحة ، هي برامج صنعت عمداً لتغيير خصائص الملفات[1].

ومن أنواع الفيروسات نجد :

* **الديدان Worms** : وهي برامج صغيرة تتكون من الشبكات وهي لا تعتمد على غيرها ، هدفها قطع الإتصال عن الشبكة أو سرقة البيانات وذلك أثناء تصفح المستخدمين للأنترنات[2] .

* **أحصنة الطروادة Trajan horse** : ويعتبر برنامج طروادة من البرامج الخطرة ، والتي تستخدم عملية القرصنة و إختراق أجهزة الحاسبات الالية فهي برامج توحي لمستخدم بأنها تقوم بعمل معين بينما هي في حقيقة الأمر تقوم بعمل أخر وتتمز عن الفيروسات بكونها غير قادرة على استنساخ نفسها ، إذ تقوم بعمل واحد هو إتلاف القرص الصلب أو فتح بعض المنافد ، للسماح للمحترفين بالتحكم في الجهاز الصلب أو لسرقة البيانات منه .[3]

---

1 -جميل حسين طويلة ، **البرمجيات الخبيثة (سوريا ، 2016)** ، ص 4. على الموقع : http://dounload.internet-bdf-ebooks.com/14777-free-book تم الإطلاع على صفحة الويب بتاريخ : 2018/12/12 .

2 -عامر أبو علي، **فيروسات الكمبيوتر**، مصر : دار حنين ، ط1 ، 1994 ، ص 46 .

3 -فتيحة ليتيم ، نادية ليتيم ،<< الأمن المعلوماتي للحكومة الالكترونية و إرهاب القرصنة >> ، **مجلة الفكر** ، جامعة محمد خيضر بسكرة ، كلية الحقوق والعلوم السياسية ، العدد رقم: 12 ، ص. 246

* **القنابل المنطقية Logie Bombs:** هي جزء من أحصنة الطروادة ، وهي تعمل في ظل ظروف معينة وتؤدي لمسح جميع بيانات الطرف المستهدف . [1]

* **برامج التجسس Spyware:** [2] وهي برامج تقوم بتحميل نفسها تلقائيا على جهاز الخاص بالهدف ، وتستخدم هذه البرامج لمراقبة ما يقوم به الهدف وجمع المعلومات عنه دون علمه وتتمثل أخطار هذه البرامج في :

- **إختطاف المتصفح** : والتي يتم من خلالها تغيير إعدادات المتصفح الخاص بالهذف وهذا بإستبدال الموقع الرئيسي الذي يستخدمه الهذف بوقع أخر ، او عرقلة دخوله لمواقع معينة .

- **برامج الزومبي** : وهي برامج يتم من خلالها التحكم بجهاز الهدف وتحويله إلى زومبي أي إستخدامه في القيام بهجمات الحرمان من الخدمة ، أو لنشر الفيروسات.

➢ الارهاب السيبراني:

هو مصطلح ليس بالحديث ، ظهر وشاع إستخدامه مع ثورة المعلومات و إستخدام الحواسيب الألية والأنترنت حيث عرفه **حلف الشمال الأطلسي** على أنه " هجموم سيبراني يستخدم أو يستغل شبكات المعلومات أو شبكات الاتصال لإحداث تدمير كاف لاثارة الرعب و إرهاب مجتمع لأهذاف إيديولوجية "[3]

1- نسرين الشحات الصباحي علي ، << الأبعاد العسكرية للقوة السيبرانية على الأمن القومي للدول دراسة حالة إسرائيل مند عام 2010 >>، المركز ادمقراطي العربي ، على الموقع: https://democaticac.de/?p=30262، تم الإطلاع على صفحة الويب بتاريخ: 2019/01/12

2- نوران شفيق ، <<أثر التهديدات الالكترونية على العلاقات الدولية : دراسة في أبعاد الأمن الإلكتروني >> ، **السياسة الدولية و الإستراتجية** ، ص28 .

3- منى الأشقر جبور ، **السيبرانية هاجس العصر** ، نفس مرجع سابق ، ص 85 .

فالإرهاب السيبراني هو التقارب بين الإرهاب والفضاء السيبراني وهو يعني هجمات غير مشروعة وتهديدات بالهجوم على الحواسيب والشبكات والمعلومات المخزنة فيها وهذا لتخويف الشعب و إكراه الحكومة على تحقيق أهداف سياسية أو إجتماعية .[1]

❖ **خصائصه** : يتميز الإرهاب السيبراني بالعديد من الخصائص التي تختلف عن بقية الجرائم بما يلي:[2]

- لا يحتاج في إرتكابه الجرائم للعنف والقوة بل يتطلب وجود حاسوب متصل بالشبكة المعلوماتية مزودة ببعض البرامج الضرورية .
- يمتاز بكونه جريمة متعدية الحدود عابرة للدول والقارات غير خاضعة لنطاق إقليمي محدد فهو جريمة دولية يمارسها مجرمين دوليين .
- صعوبة إثبات جرائمه نظراً لسرعة غياب الدليل الرقمي وسهولة إتلافه أو تدميره ما يصعب من عملية التعقب و إكتشاف الجريمة .

❖ **طرائق إستخدام الانترنت في أغراض إرهابية :**

يستخدم الإرهابيون العديد من الطرق لتنفيذ إستراتجيتهم وتتمثل هذه الطرق في :[3]

* **الدعاية** : من خلال الترويج لتنظيمات الإرهابية وهذا بتقديم شروح للأنشطة الإرهابية أو تسوق المبررات لها أو تشجيع على القيام بها من أجل التأثير على نفسية الفرد لإضعاف إيمانه ببعض القيم الإجتماعية الجماعية ، أو لبث شعور بالقلق أو الخوف في مجتمع من المجتمعات وذلك عبر نشر معلومات مضللة

1-Sarah Ggordon, Richard Ford , **Cyberterrorism**?, http://www.symantec.com, page web consultee le12/03/2018 , p. 04.

2- أمال بن صويلح ، "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الالكتوني بالجزائر" ، مداخلة ضمن فعاليات ملتقى الإجرام السيبراني المفاهيم والتحديات ، قالمة، جامعة 08 ماي 1945 ، 12/11 أفريل 2017 ، ص3 .

3- د م ، **إستخدام الانترنت في أغراض إرهابية** ، مكتب الأمم المتحدة المعني بالمخدرات والجريمة ، نيويورك ، 2012 ، ص 04 .

أو شائعات ، أو تهديدات بإستخدام العنف صور لأعمال عنف تثير المشاعر.

التمويل : تستخدم التنظيمات الإرهابية الانترنت لتمويل أعمالها ، وهذا بـ: طلب التبرعات من الأنصار أو عن طريق التجارة الإلكترونية من خلال بيع الكتب وتسجيلات صوتية ومرئية وغيرها من المواد للأنصار أو من خلال إستغلال المنظمات الخيرية بإنشاء المنظمات الإرهابية شركات تحت غطاء مشاريع خيرية لطلب التبرعات عبر الانترنت وهذا لتمويل الأعمال الإرهابية.

* **التدريب**: تستخدم التنظيمات الإرهابية الانترنت بوصفها مساحة تدريب بديلة للإرهابين تنشر من خلالها موضوعات تنص عن كيفية الإنضمام إلى التنظيمات الارهابية وكيفية صنع المتفجرات والتخطيط للهجمات الارهابية وتنفيذها وبهذا تكون منصات النشر بمثابة معسكر تدريبي إفتراضي .

* **التخطيط**: وهذا بإستخدام تكنولوجيا الانترنت من أجل التسهيل لتحضير لأعمال إرهابية ، بوسائل منها إجراء إتصالات مكثفة داخل التنظيمات التي تروج للتطرف العنيف فيما بينها وكذلك عبر الحدود .

* **التنفيذ**: وتستخدم شبكة الانترنت لتنفيذ أعمال إرهابية وهذا عن طريق تهديدات صريحة بإستخدام العنف ، بما في ذلك التهديد بإستخدام السلاح لاشاعة القلق والخوف بين الأفراد.

ومن أهم المواقع الالكترونية التي تدعو إلى التعبئة والتجنيد والدعوة إلى الإنضمام إلى التنظيمات الإرهابية نجد :[1]

- **موقع النداء** : وهو الموقع الرسمي لتنظيم القاعدة بعد أحداث الحادي عشر من سبتمبر عام 2001 ، ومن خلاله تصدر البيانات الإعلامية للقاعدة .

- **ذروة السنام** : وهي صحيفة إلكترونية للقسم الإعلامي لتنظيم القاعدة .

1- إيهاب شوقي ، << الإرهاب الإلكتروني وجرائمه>> ، 2015/12/07 ، ،على الموقع : www.anntv.tv/new/showsubject.aspx?ib=121062 تم الإطلاع على صفحة الويب تاريخ: 2018/11/04.

.

- **صوت الجهاد** : وهي مجلة نصف شهرية ، يصدرها ما يسمى بتنظيم القاعدة في جزيرة العرب ، وتتضمن مجموعة من البيانات والحوارات مع قادة التنظيم .

- **البتار**: وهي مجلة عسكرية إلكترونية متخصصة ، تصدر عن تنظيم القاعدة و تختص بالمعلومات العسكرية و الميدانية والتجنيذ .

مفهوم الدفاع والأمن والردع و الهجوم في الفضاء السيبراني

- **الفضاء السيبراني والدفاع**

تطور مفهوم الدفاع في وقتنا الحالي بشكل ملفت ، إذ لم يعد يرتبط بالأمن ووحدة الإقليم فحسب ، وإنما تعداه ليشمل معاني أخرى من أمن الشبكات المعلوماتية وإثراء الرصيد العلمي والتكنولوجي[1] ،

فيعرف الدفاع في الفضاء السيبراني على أنه " القدرة على إستباق الهجمات وتعطيلها والإستجابة لها "[2]. وهذا من خلال رصد الهجمات الإلكترونية – الأمن الوقائي – ، ويتحقق الدفاع الوقائي وفق ثلاث أساليب أساسية :

* **الكشف المبكر عن الهجمات في وقتها الحقيقي** : وذلك بإستخدام حساسات – **Sensors** – على شبكات والبرامج والتطبيقات .

* **الهجوم الإلكتروني الإستباقي** : وذلك بنشر الديدان البيضاء – **White Worms** – بإعتبارها برامج قادرة على إكتشاف التطبيقات الضارة وتدميرها قبل التوظيف ، و إطلاق هجمات إلكترونية مضادة –**Hack Back** – .

* **التضليل والإخفاء والدفاع** : وذلك بإخفاء هويات الأهداف الإستراتجية للدولة على الأنترنت عن طريق تضليل الخصوم بأدوات التمويه والخداع وتغيير ملامح الأهداف .

1– حميدة فضيل شريف ،<< صناعة الدفاع بين : البحث والتطوير، التكنواوجيا والإزدواجية >> ، **مجلة الجيش** ، العدد: 645 ، الجزائر، أفريل 2017 ، ص.53 .

2 – **دليل المرونة السيبرانية للتعاون بين القطاعين الحكومي والخاص** ، المنتدى الإقتصادي العالمي (WEF) ، دم ، دت .

3– يوسف بوغرارة ،<< الأمن السيبراني : الإستراتجية الجزائرية للامن والدفاع في الفضاء_السيبيري>> ، **مجلة الدراسات الإفريقية وحوض النيل** ، المجلد رقم: 1 ، العدد رقم: 3 ، سبتمبر/أيلول،2018 ، ص 114 .

ويتطلب الدفاع أدوات وتقنيات تسعى إلى منع طرف معاد من أن يقوم بالهجوم وهي نوعان: [1] تقنية وبشرية ، وتتمثل الأدوات التقنية في: جدار الحماية الإلكترونية حيث تغلق طرق الوصول لتي قد تترك بطرق السهو مفتوحة و إصلاح مواطن الضعف قبل أن يستطيع طرف معاد إستغلالها هذا وب تشفير الملفات بحيث أنه حتى في حالة إذا سرقت نسخة منه من نظام الحاسوب يصبح عديم الجدوى للطرف المعادي .

وتتضمن التقنيات الدفاعية المستندة إلى البشر في معظمها في حث الناس على عدم التصرف بالطرق التي تدفعهم للخطر، توعية مستخدمي الأنترنت بعمليات الإحتيال والمقصود منها الحصول على المعلومات السرية ، الإقناع بعدم إستخدام تكنولوجيا المعلومات على نحو مثير للشبهات ، التشجيع على إبلاغ السلطات المختصة عن أي نشاط مخالف للقانون .

ولا يقتصر مجال الدفاع السيبراني على سلامة وأمن الحواسيب بل يتعداه للحد الذي يكون له تأثير مباشر على الأمن القومي وبتالي العمل على الدفاع على مختلف النظم الالكترونية الخاصة بالدولة ، وما تواجهه من حرب إلكترونية ، كما يسمح الدفاع السيبراني بالتصدي للتهديدات المحدقة بالشبكات والأجهزة الرقمية الحساسة للمؤسسات الكبرى .

فمن خلال الدفاع السيبراني و إستغلال الأنترنت يمكن التحكم والسيطرة على العديد من الأنظمة الإستراتجية من ضمنها :مراقبة ورصد العمليات الصناعية المراقبة والتحكم في نقل المواد الكيميائية ، التحكم في أنظمة إمدادت المياه ، السيطرة على إنتاج الطاقة الكهربائية ، التحكم في أنظمة التوزيع الكهربائي ، السيطرة على إنتاج النفط والغاز . [2]

---

1 –هربت لين ،<< النزاع السيبراني والقانون الدولي الإنساني >>، **مجلة الصليب الأحمر** ، المجلد: 94 ، صيف 2012 ، ص 518 .

2 –إلهام غازي ، << الدفاع السيبراني >> ، **مجلة الجيش** ، العدد: 663 ، الجزائر، أكتوبر 2018 ، ص47 .

- **الفضاء السيبراني و الأمن**

إن مفهوم الأمن مفهوم واسع يطال جميع عمليات الدخول والخروج ، والبقاء أو التصرف في مكان ما ، وعليه فإنه في الفضاء السيبراني يشمل مختلف قواعد و أصول ضبط الإتصال ، و إنتقال المعلومات ، وتخزينها وحفظها ، كما يشمل أمن المواقع ، وأمن الأنظمة الإلكترونية ، وعمليات إستثمارها ، إضافة إلى أمن الإتصالات .[1]

وعرفته وزارة الدفاع في الولايات المتحدة الأمريكية على أنه " جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها (الإلكترونية و المادية)، من مختلف الجرائم ، الهجمات ، التخريب ، التجسس، والحوادث .[2]

فهو يعني مجمل القوانين السياسية ، الأدوات ، النصوص ، المفاهيم و مكانيزمات الأمن وطرق تسيير الأخطار و الممارسات التكنولوجية المتعلقة بتكنولوجيا المعلومات والإتصالات المستخدمة لحماية الدول والمنظمات والأشخاص ، كما يعرف على أنه الحالة المرغوب فيها لعمل أنظمة المعلومات و الإتصالات والتي تمنحها القدرة على المقاومة و التصدي لكل ما ينجم عن الفضاء السيبراني والذي من شأنه أن يعرض المعلومات المخزنة أو المعالجة أو المنقولة للتلف أو التغيير أو التحسس .[3]

---

1 –منى الأشقر جبور ، الأمن في الفضاء السيبيري ، على الموقع :

www.Xa.yimg.com/kq/groups/166186325/1096065403/name/ÇãÃä+ýí+ÇáýÖÁ+ÇáÓíÉíÑí.doc ، تم الإ طلاع على صفحة الويب بتاريخ 2018/12/24 .

2– عنترة بن مرزوق ، محي الدين حرشاوي ، " الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية" ، مداخلة ضمن فعاليات ملتقى سياسة الدفاع الوطني بين التحديات الإقليمية والإلتزامات السيادية ، جامعة ورقلة ،كلية لحقوق والعلوم السياسية ، ، ط 2 ، 30–2017/01/31 ، ص 66 .

3– ج رضوان ، << الأمن السيبراني : أولوية في إستراتجيات الدفاع >> ، **مجلة الجيش** ، العدد 630 ، الجزائر، جانفي 2016 ، ص41 .

❖ **أبعاد الأمن السيبراني :**

وللأمن السيبراني أبعاده المختلفة :

* **البعد العسكري** : و تتجلى الميزة النسبية للأمن السيبراني في بعده العسكري عن طريق قدرة القوة السيبرانية على ربط الوحدات العسكرية مع بعضها البعض عبر العالم الإفتراضي ، وهذا ما يسهل عملية تبادل المعلومات ، مما ينعكس بالإيجاب على تحقيق الأهداف العليا للمؤسسات العسكرية .[1]

* **البعد السياسي** : لدولة الحق في حماية نظامها السياسي ومصالحها ،

وتجدر الإشارة إلى أن موازين القوى تغيرت وأن أي شخص أصبح بإمكانه التحول إلى لاعب أساسي وهذا من خلال تمكنه من الإطلاع على خلفيات القرارات التي يسطيع الحصول عليها بسهولة نتيجة الكم الهائل من المعلومات المنتشرة والمسربة عبر الأنترنت ، و أيضا دور شبكات التواصل الإجتماعي في تنظيم الدعايات السياسية والإنتخابية ، وتنظيم التظاهرات الإفتراضية ، و إفتعال الإحتجاجات الإلكترونية .[2]

* **البعد القانوني** : ويتمثل البعد القانوني للأمن السيبراني في إيجاد القواعد القانونية لتنظيم التفاعلات في الفضاء السيبراني وحل النزاعات التي تنشأ عنها ، وترتب عن إستخدام الأنترنت العديد من الممارسات كإنشاء المدونات وتجمعات على الأنترنت والخق في حماية ملكية البرامج المعلوماتية و الإبلاغ عن المخالفات والجرائم السيبرانية وهذا ما أدى إلى تواجد ترسانة قانونية تتلائم مع ماهو موجود .[3]

1- يوسف بوغرارة ، **نفس المرجع السابق** ، ص 108 .

2 -**المرجع نفسه** ، ص 109 .

3- سمير بارة ، "الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر " الدور والتحديات " ، مداخلة ضمن فعاليات ملتقى سياسة الدفاع الوطني بين التحديات الإقليمية والإلتزامات السيادية ، كلية لحقوق والعلوم السياسية ، جامعة ورقلة ، ط 2 ، 30-2017/01/31 ، ص .431 .

* **البعد الإقتصادي** : يرتبط الفضاء السيبراني إرتباط وثيق بالإقتصاد ، فتقنية المعلومات تعزز من التنمية الإقتصادية للدول وهذا ما دفع عديد الدول إلى الإستثمار في المعرفة ، واصبحت عصرنة الإقتصاد مرتبطة بالتحكم الرقمي في الإقتصاد من طرف مختلف الفاعلين الإقتصادين والاجتماعيين .[1]

➢ **الفضاء السيبراني و الردع**

غير الفضاء السيبراني من مفهوم الردع حيث عرف على أنه " منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية"[2] .

فقواعد الردع المتعارف عليها دولياً لا تتغير بالإنتقال من المجالين النووي التقليدي إلى المجال السيبراني فالردع في عصر المعلومات يختلف كثيراً عنه في عصر الحرب الباردة في النوع والنطاق ، ففي زمن الحرب الباردة تميزت الساحة الدولية بقلة الدول المالكة للأسلحة النووية لكن حاليا عدد الدول التي تسعى لتطوير أسلحتها السيبرانية 140 دولة كما أدخلت 30 دولة الوحدات السيبرانية في جيوشها.[3]

ويرتكز الردع السيبراني على ثلاث ركائز وهي : مصداقية الدفاع ، القدرة على الإنتقام ، و الرغبة في الإنتقام .

ووفقاً للمعهد الألماني للشؤون الأمنية والدولية في دراسة له نشرها سنة 2015 بعنوان"نظرية الردع في القرن السيبراني " يرتكز اردع على عنصرين هما: [4]

- ردع الهجمات السيبرانية فيما يعرف " الردع بالمنع " وينطوي تحت الردع

---

1 -**نفس المرجع السابق** ، ص 430 .

2 -يوسف بوغرارة ، **نفس المرجع السابق** ، ص 107 .

3 – محمد بوكبشة ،<< الأمن والدفاع السيبراني (أولوية قصوى)>> ، **مجلة الجيش** ، العدد: 651 ، الجزائر ، أكتوبر 2017 ، ص.34.

4 -**المرجع نفسه** ، الصفحة نفسها .

بالمقاومة والردع بالصمود ويعني الصمود القدرة على إستعادة الشئ بشكله الأصلي قبل الهجوم الذي تم وهذا من شأنه أن يحد من المكاسب المحتملة ، ويمكن أن يقنع الخصم بعدم الهجوم خاصةً إذا كانت التكلفة مفرطة ويظل الهذف من المقاومة والصمود هو تقليل خيارات الطرف الذي ينوي الهجوم ، سواء من خلال بناء هياكل دفاعية يصعب التغلب عليها أو من خلال ضمان الاستعادة السريعة لأصل الشيء بعد الهجوم .

- الردع بالتهديد بشن هجمات سيبرانية فيما يعرف " الردع بالإنتقام " أو الردع عن طريق العقاب فهو بمثابة القبض على الجاني ومحاكمته و هو ما يؤثر على سلوك الجاني في المستقبل و أيضاً في سلوك الأخرين في المجال الجنائي .

خلاصة الفصل الاول:

أن ظهور مصطلح الفضاء السيبراني في الساحة الدولية لقي إهتمام كبير من قبل الدارسين والباحثين الأكاديميين وهذا لتأثيره الكبير في تغيير مفهوم العديد من المصطلحات : الجريمة ، الإرهاب ، الحرب وإنتقالها من الواقع التقليدي إلى الواقع السيبراني ، مما ألزم تغيير إستراتجيات التصدي لها بوسائل تتلاءم مع التطور الحاصل فأصبح الحديث عن مصطلحات : الدفاع ، الردع ، الأمن في الفضاء السيبراني .

الفصل الثاني

واقع الدفاع السيبراني في الجزائر

تمهيد:

إدراكاً للتهديدات التي أصبح يحملها الواقع الافتراضي ، والرغبة الجادة من قبل المنظومة الدفاعية الجزائرية في التصدي لكل هاته التهديدات من خلال وضع إستراتجية دفاع سيبراني شاملة لكل الجوانب ذات الصلة بتحقيق الأمن القومي .

المبحث الأول: التهديدات السيبرانية في الجزائر

عرفت الساحة الأمنية الجزائرية العديد من التهديدات التي أفرزتها الثورة التكنولوجية الحديثة والإنفتاح على العالم الإفتراضي من خلال وسائل التواصل الإجتماعي خاصة و أن الجزائر غير معزولة عن هذا العالم التي تتأثر بكل ما يحيط به من أحداث و تحديات .

❖ الجريمة السيبرانية :

إن إرتفاع معدل الجريمة السيبرانية بالجزائر له علاقة كبيرة بزيادة عدد المستخدمي لشبكة الأنترنت ، حيث يفوق عدد مستخدمي شبكة الأنترنت 33 مليون جزائري من بينهم 19 يستخدمون مواقع التواصل الإجتماعي فايسبوك ، 13 مليون يبحرون في الأنترنت يومياً ، 18 مليون حساب ccp ، التجارة الإلكترونية الحكومة الإلكترونية... [1]، وهي أرقام تعكس خطورة هذا الفضاء الذي بات بؤرة خصبة لكل أنواع الجرائم .

وتنوعت أشكال الجريمة السيبرانية بالجزائر من الإعتداء و المساس بأمن وسلامة الأشخاص كالسب والقذف والمساس بالحرمة الخاصة في الفضاء السيبراني ، جرائم إبتزاز ، جرائم متعلقة بالإعتداء على القصر متعلقة بأفعال غير أخلقية ومخلة بالحياء ، إعتداء على الأنظمة المعلوماتية و البريد الإلكتروني و مواقع إلكترونية لمؤسسات خاصة .

1- يونس بورنان ،<< قانون جديد في الجزائر لمكافحة الجرائم الإلكترونية >>، 2018/03/28 على الموقع: http://al-ain.com ، تم الإطلاع على صفحة الويب بتاريخ 2019/04/12 .

وفيما يلي بعض الإحصائيات عن الجريمة السيبرانية بالجزائر التي سجلت من طرف بعض المؤسسات الأمنية

✓ سجلت مصالح الشرطة القضائية بالمديرية العامة للأمن الوطني خلال سنة2017 أزيد من2130 قضية تتعلق بجرائم إلكترونية وهي تنقسم إلى:[1]

* 1511 قضية متعلقة بالمساس بالأشخاص كالسب والقذف والمساس بحرمة الحياة الخاصة في الفضاء الإفتراضي عبر الأنترنت وتضرر من هذا النوع من السلوكيات المنحرفة 2381 ضحية .

* 47 قضية متعلقة بجرائم الإبتزاز عن طريق شبكة الانترنت أغلبها يتعلق بعروض عمل وهمية للحصول على المال .

* 49 قضية متعلقة بالإعتداء على القصر متعلقة بأفعال غير أخلاقية ومخلة بالحياء .

* 28 قضية إعتداء على الأنظمة المعلوماتية وبريد الكتروني لمؤسسات وخواص من خلال محو أو تغيير البيانات .

✓ وعلى مستوى المصلحة المركزية لمكافحة الإجرام السيبراني لدرك الوطني عالجت المصلحة من بداية سنة 2018 إلى شهر نوفمبر 1140 قضية متعلقة بالجريمة الإلكترونية منها 136 قضية خاصة بالأطفال.[2]

✓ وسجل مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها التابع للقيادة العامة للدرك الوطني في سنة 2017 يزيد عن 900 قضية جريمة إلكترونية تتعلق أساساُ بالقرصنة والإحتيال عبر شبكة الانترنت[3]

1- << مجلة الشرطة : معالجة 2130 جريمة الكترونية خلال 2017 >> ، 2018/04/17 ، على الموقع : www.radioalgerie.dz ، تم الإطلاع على صفحة الويب بتاريخ 2019/03/02

2- << الدرك يدعو ضحايا " الإبتزاز الإفترصي " إلى التبليغ عن المتورطين>> ، 2018/11/27، على الموقع ، https://www.tsa-algerie.com تم الإطلاع على صفحة الويب بتاريخ 2019/03/14 .

3- بهاء الدين آيت صديق ، << الكشف عن عدد الجرائم الالكترونية المعالجة بالجزائر سنة 2017 >>، 2018/01/18 ، على الموقع : https://www.android-dz.com ، تم الإطلاع على صفحة الويب بتاريخ 2019/02/01 ،

- ✓ تعرض موقع قاعدة بيانات وزارة البريد لعملية قرصنة سنة 2016 وتكررت العملية على مستوى إتصالات الجزائر سنة 2017 .[1]
- ✓ تعرض موقع وكالة الأنباء الجزائرية في الخارج للقرصنة في شهر مارس 2017 .[2]
- ✓ كشفت إحدى الدراسات بعنوان بارومتر 2018 حول الأمن السيبراني في المؤسسات الجزائرية عن إحصائيات تكشف التهديدات السيبرانية الموجهة ضد المؤسسات الجزائرية :[3] .

-27% من المؤسسات التي شملها سبر الأراء تعرضت لاختراق أنظمة معلوماتها خلال 12 شهر بواسطة فيروسات.

- 15% فقدت بياناتها جراء أخطاء بشرية .

وتعود أسباب تعرض المؤسسات الجزائرية إلى الإختراقات إلى الجهل بوجود قوانين في هذا المجال ، عدم تخزين المؤسسات بياناتها في شبكات معلوماتية جزائرية ، كما أن معظم المؤسسات أكدت أنها تتعامل مع مؤسسات أجنبية في مجال التزود بالخدمة و إيواء المواقع .

1- << الجرائم الالكترونية تهدد أمن الجزائريين >> ، 2018/04/10 ، على الموقع : www.djazairess.com/akhabrelyoum/240271 تم الإطلاع على صفحة الويب بتاريخ 2019/05/01 .

2 -الموقع نفسه .

3 - << الأمن السيبراني بالجزائر >> ، **مجلة الجيش** ، العدد: 663 ، الجزائر ، أكتوبر 2018 ، ص 44 .

❖ **الإرهاب السيبراني**

حسب تقرير معهد " راند كوربورايش " بشأن الإرهاب الجديد فإن قدرات إبن لادن تعززت وتطورت بفضل التكنولوجيا الحديثة وذلك في إتجاهين هما :[1]

1) شبكة إتصالاته 2) إمكانية القيام بنشاطات هجومية على المصالح الإعلامية .

وقد عبر هاتين الاتجاهين عن دور التكنولوجيا في تهديد الأمن الوطني وهذا ما عانت منه المؤسسات الأمنية الجزائرية خاصةً أن الجماعات الإرهابية وجدت من يمونها في العالم الغربي المتطور ، فمن خلال إستخدامها لتكنولوجيا تعمل الجماعات الإرهابية على :[2]

- تعطيل التمويل الإعلامي للمؤسسات العسكرية وذلك عن طريق شن هجمات على هذه المؤسسات الاعلامية و رجالاتها .
- إستعمال أجهزة التصنت .
- إقتحام البرامج والأنظمة الاستراتجية العسكرية .

فتغيير إستراتجيات الإرهاب والتطرف وإنتقاله من البيئة المادية الطبيعية إلى البيئة الإفتراضية السيبرانية ، أضحى يشكل تحدياً أمنياً للجزائر وهو ما أكده رئيس الجمهورية السيد عبد العزيز بوتفليقة *قائلاً: " **لقد أضحى هذا الفضاء الإفتراضي تحدياّ أمنياّ لبلداننا العربية ، خصوصا و أنه يمثل ملاذاً للتنظيمات الارهابية وكل الشبكات الاجرامية لكونه غير مرئي لا سيما تلك التي تنشط في الاتجار بالبشر والأعضاء البشرية والمهاجرين غير الشرعيين و المتاجرة**

---

1 -بوحنية قوي وآخرون ، **المرجع السابق** ، ص.448 .

2 -**المرجع نفسه** ، الصفحة نفسها .

* رئيس الجزائر للفترة (1999-2019) .

بالمخدرات والأسلحة والمتفجرات وتزوير الهويات والمستندات ، فضلا عن دوره في تجنيد المقاتلين الجدد وربط شبكات المقاتلين بعضهم ببعض وتوفير مصادر تمويل خارج الرقابة المنتهجة في إطار تجفيف منابع تمويلها التقليدية ".[1]

فالجزائر مستهدفة من قبل الجماعات الإرهابية وبصورة دائمة وهذا ما صرحت به بعض الأجهزة الأمنية :[2]

- ✓ حيث سجلت الأجهزة الأمنية خلال الثلاثي الأول من سنة 2017 أزيد من 2000 تبليغ عن أنشطة متصلة بالإرهاب عبر المواقع الإلكترونية ، وفقاً لما أفاد به مصدر أمني مأذون لـ " البلاد " حيث أقر أن معظم التبليغات التي أرسلت إلى المصالح الأمنية حول " شبهات الإرهاب " تتعلق بمحاولات اختراق لحسابات مواقع التواصل الإجتماعي أو دعوات للتجنيد في صفوف تنظيمات مجهولة أم إرهابية أو طوائف دينية .
- ✓ سيطرة تنظيم " داعش " على عدد من المواقع والمنتديات الإلكترونية ، التي تحتوي على مكتبو هائلة وواسعة تختص بالإيديولوجيا والخطاب وآليات التجنيد والتمويل والتدريب والتخفي وصنع المتفجرات وكل ما يلزم " الإرهابيين" في عمليات المواجهة في إطار حرب العصابات وسياسات الاستنزاف .
- ✓ كشفت ذات المصدر أن تنظيم داعش لديه فريق من الخبراء التقنيين مهمتهم الرئيسية تتمحور حول إختراق البريد الإلكتروني للآخرين وهتك أسرارهم والاطلاع على معلوماتهم وبياناتهم والتجسس عليهم لمعرفة مراسلاتهم ومخاطباتهم والإستفادة منها في عمليات إرهابية .
- ✓

---

1 –<< رسالة الرئيس بوتفليقة بمناسبة إنعقاد الدورة 35 لمجلس وزراء الداخلية العرب>>، 2018/03/07 على الموقع : www.radioalgerie.dz ، تم الإطلاع على صفحة الويب بتاريخ 2019/05/12.

2 –<< الإرهاب الالكتروني يهدد الجزائر >>، 2017/05/13 ، تم الإطلاع على صفحة الويب بتاريخ 2018/12/01 ، على الموقع : www.m.elbilad.net

المبحث الثاني: الجانب القانوني في مواجهة التهديدات السيبرانية

لقد أبدت الجزائر مند سنوات عديدة إستعدادها الكامل لمكافحة الجرائم السيبرانية و المعلوماتية لذا عكفت على إعداد النصوص القانونية و الانخراط في العديد من الإتفاقيات .

❖ النصوص القانونية

هناك محاولات جادة من طرف الجزائر لتطوير المنظومة القانونية و إصدار تشريعات تواكب التطور الحاصل في المجال التكنولوجي ، حيث سارع المشرع الجزائري بإحتواء هذا التطور و إحاطة الجريمة السيبرانية بأطر قانونية تحكمها .

- ✓ **القانون رقم 04-15 المؤرخ في 27 رمضان عام 1425 الموافق لـ 10 نوفمبر 2004 المعدل والمتمم للامر رقم 156/66 المتضمن قانون العقوبات[1].**

حيث خطا المشرع الجزائري خطوة هامة بالمبادرة إلى تعديل قانون العقوبات بإدراج القسم السابع مكرر المتعلق بالمساس بأنظمة المعالجة الألية للمعطيات بمحتوى المادة 394 مكرر إلى 394 مكرر 7 والذي نص على العقوبات التالية :

- المادة 394 مكرر 1: عقوبة الإدخال بطريق الغش معطيات في نظام المعالجة الألية أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها.[2]
- المادة 394 مكرر 2: عقوبة كل من يقوم عمداً وعن طريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها إحدى الجرائم

1- الجمهورية الجزائرية الديمقراطية الشعبية ، القانون رقم 04-15 المعدل والمتمم للأمر 66-156 المتعلق بقانون العقوبات، المؤرخ في 2004/11/10 ، **الجريدة الرسمية** ، العدد 71 ، 10/ 2004/11 ، ص 8 .

2- **المرجع نفسه** ، ص 12 .

المنصوص عليها في هذا القسم ، و حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم .[1]

– المادة 394 مكرر 3: مضاعفة العقوبات المنصوص عليها في هذا القسم ، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام ، دون الإخلال بتطبيق عقوبات أشد .[2]

– المادة 394 مكرر 4: معاقبة الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.[3]

– المادة 394 مكرر 5 : معاقبة كل من شارك في مجموعة أو في إتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسداً بفعل أو عدة أفعال مادية ، بنفس العقوبات المقررة للجريمة ذاتها.[4]

– المادة 394 مكرر 6 : مصادرة الأجهزة والبرامج و الوسائل المستخدمة مع إغلاق المواقع التي تكون محلاً لجريمة من الجرائم المعاقب عليها وفقاً لهذا القسم ، علاوة على إغلق المحل أو مكان الإستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها .[5]

– المادة 394 مكرر 7 : عقوبة الشروع في إرتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها.[7]

---

1 –**نفس المرجع السابق** ، ص12 .

2 –**المرجع نفسه** ، الصفحة نفسها .

3 –**المرجع نفسه**، الصفحة نفسها.

4 –**المرجع نفسه** ، الصفحة نفسها.

5 –**المرجع نفسه** ، الصفحة نفسها.

6 –**المرجع نفسه** ، الصفحة نفسها.

✓ **القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ 05 أوت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها [1].**

هذا القانون الذي جاء لتكريس إطار قانوني يتلائم مع خصوصية وخطورة جرائم العالم الإفتراضي ، يهدف إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، جاء في 19 مادة تندرج تحت ستة(06) فصول تضمن **فصله الأول** أهداف القانون ومفهوم المصطلحات التقنية الواردة فيه كالجرائم المتصلة بتكنولوجيا الإعلام والإتصال ، منظومة معلوماتية ، معطيات معلوماتية ، مقدمو الخدمات ، المعطيات المتعلقة بحركة السير ، الاتصالات الالكترونية "، والأحكام القانونية المتعلقة بمجال تطبيقه والتي تضمن سرية المرسلات وإتصالات . مع وضع ترتيبات تقنية لمراقبة الإتصالات الالكترونية ، ليتناول الفصل الثاني المادة 4 منه الحالات التي تسمح باللجوء إلى المراقبة الالكترونية حسب ما نصت عليه المادة 3 من هذا القانون وتتمثل في :

* للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة .

* في حالة توفر معلومات عن إحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني .

* لمقتضيات التحريات والتحقيقات القضائية ، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجؤ إلى المراقبة الإلكترونية.

وفي إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة ويشترط إذن

---

1 –الجمهورية الجزائرية الديمقراطية الشعبية ، القانون رقم 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها ' ، المؤرخ في 2004/08/05 ، **الجريدة الرسمية** ، العدد 47 ، الصادرة بتاريخ: 2009/08/16، ص5.

مكتوب من السلطة القضائية المختصة حيث خولت المادة 5 من الفصل الثالث للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية ، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 ، الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها ، ومنظومة تخزين معلوماتي .

وفي حالة تبين تخزين المعطيات المبحوث عنها والتي يمكن الدخول إليها إنطلاقا من المنظومة الأولى في منظومة معلوماتية تقع خارج الإقليم الوطني ، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقاً للاتفاقيات الدولية ذات الصلة ووفقا لمبداء بالمثل .[1]

كما نص الفصل الرابع على التزام مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية مع كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.[2]

ويقترح القانون في فصله الخامس إنشاء هيئة الوطنية للوقاية من الجرائم المتصل بتكنولوجيا الإعلام والإتصال ومكافحتها والتي من شأنها مكافحة الجرائم ومصاحبة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم . كما يخول القانون لهذه الهيئة تولي جانب تجميع المعلومات و إنجاز الخبرات القضائية وتبادل المعلومات مع نظيراتها في الخارج قصد محاربة هذا النوع من الجرائم .[3]

أما الفصل السادس من هذا القانون فتناول التعاون والمساعدة القضائية الدولية ومن خلاله تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيا

---

1 –الجمهورية الجزائرية الديمقراطية الشعبية ، القانون رقم 09/04 ، **المرجع السابق** ، ص06.

2 –**المرجع نفسه** ، ص07.

3 –**المرجع نفسه** ، ص08.

الإعلام والإتصال المرتكبة خارج الإقليم الوطني ، عندما يكون مرتكبها اجنبياً وتستهذف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتجية للإقتصاد الوطني ، هذا بالإضافة إلى تبادل المساعدات القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني ، وقد وضعت الجزائر من خلال هذا القانون قيود على طلبات المساعدة القضائية والدولية وهذا ما نصت عليه المادة 18 حيث ترفض الجزائر تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام ، كما يمكن أن تكون الإستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم إستعمالها في غير ما هو موضح في الطلب [1].

ويعتبر القانون 09/04 والقانون 15/10 أهم قانونين سنتهم الجزائر في مكافحة الجريمة الإلكترونية بصفة عامة .

هذا بالإضافة إلى قوانين أخرى أقرها المشرع الجزائري في مجال الجريمة الإلكترونية والمتعلقة بمؤسسات الدولة وتمثلت في :

✓ **قانون البريد والإتصالات السلكية واللاسلكية:** حيث نصت عدة مواد منه فيما يخص المجال السيبراني ؛ المادة87 ، و التي نصت على سهولة إجراء التحويلات المالية إلكترونيا ، و المادة 84/ 2 على إستعمال حولات الدفع العادية والإلكترونية ، كما نصت المادة 105 من القانون على إحترام المراسلات أما المادة 127 منه فنصت على جزاء كل من يفتح أو يخرب بريد .[2]

✓ **قانون التأمينات :** وقد نص هذا القانون على تنظيم الجريمة الإلكترونية

---

1 -**نفس المرجع السابق** ، نفس الصفحة السابقة .

2 -يوسف بوغرارة ، **نفس المرجع السابق** ، ص110 .

من خلال مؤسسات و هيئات الضمان الإجتماعي ، و ذلك في عدة نصوص تخص البطاقة الإلكترونية .[1]

وجهود الجزائر متواصلة في هذا المجال حيث تقوم الجزائر مند جانفي 2015 من أجل تكييف إطارها التشريعي والتنظيمي من خلال تبني مجموعة من القوانين الهامة منها الخاصة بالتوقيع والمصادقة الإلكترونية التي من شأنها تطوير الخدمات المقدمة عبر الأنترنت مثل الإدارة الإلكترونية ، التجارة الإلكترونية وكذا البنوك الإلكترونية ، فضلا عن سعي الجزائر الحثيث إلى إرساء قاعدة قانونية لإستخدام التكنولوجيا الجديدة للإعلام والإتصال في تطوير قطاع العدالة .[2]

❖ الإتفاقيات

✓ الإتفاقية العربية لمكافحة جرائم تقنية المعلومات

من أجل تعزيز التعاون فيما بين الدول العربية لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامه مجتمعاتها ، وإقناعاً بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهذف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات .تم إنشاء الإتفاقية العربية لمكافحة جرائم تقنية المعلومات حررت بمدينة القاهرة في 2010/12/21 موقعة من طرف مماثلين وزراء الداخلية العرب و وزراء العدل لـ 22 دولة ، تم التوقيع عليها من الجانب الجزائري كل من دحو ولد قابلية ممثل عن وزارة الداخلية والطيب بلعيز ممثل عن وزارة العدل.[3]

تحتوي هذه الإتفاقية على خمس فصول و ثلاثة وأربعون مادة ، تناول الفصل الأول أحكام عامة حول الإتفاقية ، وتضمن الفصل الثاني التجريم وهذا بعرض

---

1 –**نفس المرجع السابق** ، نفس الصفحة السابقة .

2 –إسماعيل جنادي ، << الأمن السيبراني التحدي القادم للإتحاد الإفريقي>> ، **مجلة الجيش** ، العدد: 663 ، الجزائر ، أكتوبر2018 ، ص 45 .

3 –**الإتفاقية العربية لمكافحة جرائم تقنية المعلومات** ، جامعة الدول العربية ،2010/12/31 ، ص25.

لأنواع الجرائم المرتبطة بالاستخدام السيئ لتقنية المعلومات ، كما تناول الفصل الثالث الأحكام الإجرائية ، أما الفصل الرابع فتطرق إلى التعاون القانوني والقضائي بين الدول الموقعة لهذه الإتفاقية وهذا من خلال المساعدة المتبادلة حسب ما نصت عليه الجزائر من خلال الفصل السادس من القانون 09/04 كما نصت المادة 39 من الإتفاقية على التعاون والمساعدة الثنائية بالوصول إلى معلومات تقنية المعلومات المخزنة :[1]

– يجوز لأي دولة طرف أن تطلب من دولة طرف أخرى البحث أو الوصول أو الضبط أو التأمين أو الكشف لمعلومات تقنية المخزنة والواقعة ضمن أرضي الدولة الطرف المطلوب منها.

– تلتزم الدولة الطرف المطلوب منها بأن تستجيب للدولة الطرف الطالبة وفقاً للأحكام الواردة في هذه الإتفاقية .

– تتم الإجابة على الطلب على أساس عاجل إذا كانت المعلومات ذات العلاقة عرضة للفقدان أو التعديل .

❖ إتفاقية الإتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي

وهي إتفاقية مستوحاة من الإتفاقية الأوروبية لبودابست إعتمدها الإتحاد الإفريقي خلال قمته الـ 23 التي انعقدت بمالابو بجمهورية غينيا الإستوائية ، تعكس هذه الإتفاقية درجة وعي الدول الإفريقية بالخطر الذي يهددها ، بحيث يندرج تبنيها ضمن حرص دول الإتحاد الإفريقي على تحيين قوانينها وتشريعاتها الإقليمية في مجال الأمن السيبراني ومن أهمها[2]:

---

1 –**نفس المرجع السابق** ، ص.22.

2 –إسماعيل جنادي ، **نفس مرجع سابق** ، نفس الصفحة السابقة .

القرار بشأن تكنولوجيا الإعلام والإتصال في إفريقيا : التحديات والأفاق المستقبلة للتنمية سنة 2010* ، إعلان " أوليفر تامبو " ** بتاريخ 2009/11/09 ،" إعلان أبيدجان "* بتاريخ 2012/02/22 و إعلان أديس بابا بتاريخ 2012/06/22.

وتهدف هذه الإتفاقية إلى تعزيز وتنسيق التشريعات الحالية للدول الأعضاء والمجموعات الإقتصادية الإقليمية في مجال تكنولوجيات الإعلام والإتصال ، خلق إطار معياري ملائم للبيئة القانونية ، الثقافية ، الإقتصادية والإجتماعية للقارة ، تسليط الضوء على مسألة حماية البيانات الشخصية والخصوصية حيث تلتزم كل دولة طرف بوضع إطار قانوني يهدف إلى تعزيز الحقوق الأساسية والحريات العامة وقمع أية جريمة متعلقة إنتهاك الخصوصية والمعاقبة عليها دون المساس بمبداء حرية حركة البيانات ذات الطابع الشخصي [1]، التأكيد على ضرورة التوفيق بين حماية البيانات الشخصية واحترام الحريات الأساسية للأفراد وتعميم إستخدام تكنولوجيا الإعلام والاتصال ، إلى جانب مرعاة مصلحة الفاعلين العموميين والخواص على حد السواء .

ويتضمن الفصل الثالث من الإتفاقية تعزيز الأمن الإلكتروني ومكافحة الجريمة الإلكترونية حيث تناول في قسمه الأول تدبير الأمن الإلكتروني الواجب إتخاذها على المستوى الوطني فيما يتعلق بالجانب القانوني المؤسساتي والتعاون الدولي لمواجهة التهديدات الإلكترونية ' كذلك النظم الوطني لتأمين الفضاء الإلكتروني وهذا من خلال ثقافة تأمين الفضاء الإلكتروني و دور الحكومات و الشراكة بين

---

* الصادر عن الدورة الرابعة عشر لمؤتمر رؤساء دول وحكومات الإتحاد الإفريقي المنعقدة في أديس بابا بإثيوبيا من 31 جانفي إلى 2 فيفري 2010 .

** أعتمد في مؤتمر الإتحاد الإفريقي الإستثنائي للوزراء المسؤولين عن تكنولوجيا المعلومات والاتصالات المنعقد في جنوب إفريقيا بجوهانسبيرغ في 05 /2009/11 .

1 -**إتفاقية الإتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي** ، ملابو غينيا ، 2010/06/27 ، المادة 8 ، ص 18 .

القطاعين العام والخاص وكذلك التعليم والتدريب في مجال أمن الفضاء الإلكتروني .[1]

وقد تم إعداد مجموعة من المبادئ التوجيهية في ماي 2018 قصد تسهيل تنفيذ إتفاقية الإتحاد الإفريقي حول الأمن السيبراني وحماية البيانات الشخصية، وتسعى هذه المبادئ إلى خلق جو من الثقة في مجال الخدمات المقدمة بواسطة الأنترنت بإعتبارها عاملاً رئيسياً في حماية الإقتصاد الرقمي ، كما تسعى إلى تحسيس مستخدمي الأنترنت بشكل عام ومساعدتهم على مضاعفة الحيطة والحذر لغرض حماية بياناتهم الشخصية .[2]

وهذه الإتفاقية تعكس إهتمام السلطات الإفريقية بالفضاء السيبراني وتحدياته وتعزيز أليات التعاون في مجال مكافحة الجريمة السيبرانية .

❖ **الإتفاقية الجزائرية الفرنسية :**

اتخذت الجزائر الإجراءات اللازمة من أجل مقاومة الجريمة المعلوماتية المنصوص عليها في الاتفاقية الأورو متوسطية المؤرخة في 2002/04/22 والتي كانت تهذف إلى ربط الجهود بين الوحدة الأوربية والدول الأعضاء فيها وما بين الحكومة الجزائرية من جهة أخرى [3].

وبهذا صادقت الجزائر على الإتفاق مع الحكومة الفرنسية بالتعاون في مجال الأمن ومكافحة الإجرام المنظم ، الموقعة بالجزائر في 2003/10/25 .

حيث نصت المادة الأولى من الإتفاق على إقامة الطرفان تعاوناً عملياتياً وتقنياً .

---

1 –**نفس المرجع السابق** ، المادة 26، ص ص، 35– 35 .

2 –إسماعيل جنادي ، **مرجع سابق** ، ص. 45 .

3 –مختارية بوزيدي ، " ماهية الجريمة الإلكترونية"، مداخلة ضمن فعاليات الملتقى الوطني أليات مكافحة الجرائم الإلكترونية في التشريع الجزائري ، مركز جيل البحث العلمي ، الجزائر العاصمة، 2017/03/29 ، ص. 12 .

المبحث الثاني : الجانب الأمني في مواجهة التهديدات السيبرانية

❖ الهياكل التنظمية على المستوى الداخلي

ولمكافحة تهديدات الفضاء السيبراني قامت المنظومة الدفاعية من خلال مؤسساتها المختلفة: الأمن الوطني ، الدرك الوطني، الجيش الوطني الشعبي من أنشات عديد الهياكل التنظيمة أو تكيف هياكلها الموجودة مواكبة مع التحديات الجديدة التي فرضها الفضاء السيبراني .

✓ على مستوى الدرك الوطني

قامت فرق الدرك الوطني بإنشاء هياكل لمكافحة الجرائم السيبرانية ومن هذه الهياكل نجد :

- **المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني**

يعد المعهد الوطني للأدلة الجنائية وعلم الإجرام مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والإستقلال المالي موضوع تحت وصاية وزير الدفاع الوطني يديره مدير عام ، ويخضع إلى جميع الأحكام التشريعية والتنظيمية المطبقة على المؤسسات العسكرية .[2]

ليدخل حيز التنفيذ إبتداءا من 2009/01/01 ، أما الفترة بين 2004 و 2009 فكرست لتكوين الموارد البشرية و إقتناء المعدات العلمية والتقنية الضرورية[3]

---

1 –الجمهورية الجزائرية الديمقراطية الشعبية ، المرسوم الرئاسي رقم 375/07 المتعلق المتضمن التصديق على الإتفاق بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الفرنسية المتعلق بالتعون في مجال الأمن ومكافحة الإجرام المنظم ، المؤرخ في 2004/08/05 ، **الجريدة الرسمية** ، العدد 77 ، الصادرة بتاريخ :2007/12/09 ، ص ص 5– 6 .

2 –الجمهورية الجزائرية الديمقراطية الشعبية ، المرسوم الرئاسي رقم 183/04 المتعلق بتأسيس المعهد الوطني للأدلة الجنائية ، المؤرخ في 2004/08/26 ، **الجريدة الرسمية** ، العدد 41 ،الصادرة بتاريخ: 2004/06/27 ، ص.18.

3 –نسيمة سحواد، مقابلة مع العقيد سيد أحمد بوزمالة ، المدير العام لمعهد الأدلة الجنائية وعلم الإجرام للدرك الوطني ، 2014/12/08 ، 18:29سا، على الموقع :
www.ar–dk news–dz.com/index– php/nation/actualite 25768. 2014.12.17

و نصت المادة 06 منه على الهيكل التنظيمي للمعهد حيث يتكون من مديرية للأدلة الجنائية ، مديرية للدراسات والبحوث الإجرامية ، مصلحة للتنظيم والمناهج ،مصلحة للإدارة والوسائل .ويحتوي على (11) دائرة متخصصة في عدة مجالات متباينة تضمن جميعها الخبرة والتكوين والتعليم ، وتقديم جميع المساعدات التقنية . حيث تقوم دائرة الإعلام الآلي و الالكترونيك برصد ومراقبة وتتبع عمليات الإختراق والقرصنة المعلوماتية وكذا إكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية، كما يقوم بهمة معالجة تحليل وتقديم للعدالة كل دليل رقمي وتماثلي كما تقدم مساعدة تقنية للمحققين في التحقيقات المعقدة ، ولإنجاز المهمة المنوط بها تنقسم الدائرة إلى ثلاث مخابر وهي : مخبر الإعلام الآلي ، مخبر الفيديو ، مخبر الصوت .[1]

- **مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني**

أنشأته قيادة الدرك الوطني في سنة 2008 ، وهو مركز متخصص في محاربة الجريمة السيبرانية ، ويعتبر عصب الجهاز المختص في مكافحة الجريمة السيبرانية مقره بئر مراد رايس ، وهو بمثابة مركز توثيق حيث يعمل المركز على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة وتحديد هوية أصحابها ، ويهدف المركز إلى تأمين الأنظمة المعلوماتية والحفاظ عليها لاسيما تلك المستعملة في المؤسسات الرسمية والبنوك والبيوت [2]، كما يهدف إلى مساعدة باقي الأجهزة الأمنية الأخرى في أداء مهامها ، حيث يسعى المركز إلى: [3]

-تعميم و إستكمال نشر فرق المحققين في الجريمة المعلوماتية وتعميم نظام اليقضة على المستوى الوطني عبر كافة الوحدات التابعة للدرك الوطني.

-

---

1 - إبتسام بغو ، **إجراءات المتابعة الجزائية في الجريمة المعلوماتية** ، (مدكرة ماستر في القانون ، جامعة العربي بن مهيدي أم البواقي، قسم الحقوق) ، 2016/2015 ، ص 23 .

2 -سمير بارة ، **نفس المرجع السابق**، ص.435 .

3-العقيد بن رجم جمال، << حماية منظومتنا الوطنية للمعلومات من خلال تطبيق القانون>> ، **مجلة الجيش** ، العدد: 599 ، الجزائر ، جوان 2013 .ص 14.

- تكوين مجموعة مختصة في مهام أمن الأنظمة المعلوماتية وحمايتها .
- تكوين المكونين في المجال و إعداد برامج المواد المتعلقة بالتكنولوجيا الجديدة ومكافحة الجريمة المعلوماتية على صعيد كافة مستويات التكوين

ويضم المركز ثلاث مكاتب يتولى المكتب الأول مهام التحقيق في الجريمة السيبرانية ، والمكتب الثاني مختص في تأمين شبكة الأنترنت أما المكتب الثالث فهو مختص بالأمن الرقمي .

وفي مايلي إحصائيات للجرائم المعالجة على مستوى المركز

الجدول رقم 01 : عدد القضايا التي تمت معالجتها على مستوى المركز

سنة معالجة القضايا	2009	2010	2011	2012	2016	2017
عدد القضايا المعالجة	82	146	269	349	500	900

المصدر : من إعداد الطالبة إعتمادا على الموقع : www.android-dz.com ، https://el-massa.com و مجلة الجيش جوان 2013 .

فمن خلال الإحصائيات المذكورة نلاحظ تزيادة في عدد القضايا المعالجة على مستوى المركز من 82 قضية سنة 2009 وهي بداية عمل المركز ليتزايد عدد القضايا المعالجة 146 قضية سنة 2010 ويرتفع سنة 2011 بـ 269 قضية ليصل سنة 2012 إلى 349 قضية ويسجل المركز 500 قضية سنة 2016 أما في سنة 2017 إرتفع عدد القضايا إلى 900 قضية .

فالإرتفاع في عدد القضايا المعالجة على مستوى المركز يعكس التركيبة البشرية المؤهلة التي يكتسبها الجهاز من التكوين المستمر لمؤهلين في مجال متابعة وتقصي الجريمة عبر الأنترنت ومن خلال الملتقيات الوطنية والدولية و تبادل الخبرات مع الدول الأخرى في هذا مجال .[1]

1- سمير بارة ، **نفس المرجع السابق** ، ص 435 .

✓ على مستوى الأمن الوطني

- **المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني**

إستجابةً لمطلب الأمن السيبراني ومكافحة التحديات الأمنية الناجمة عن الجرائم الإلكترونية ، قامت مصالح الأمن الوطني بإنشاء هذه المصلحة سنة 2011 . وقد كانت المصلحة في البداية عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة الإلكترونية على مستوى المديرية العامة لأمن الوطني ، ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال بقرار من المدير العام للأمن الوطني أضيفت للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015 [1].

وتقوم المصلحة بمعالجة القضايا المتعلقة بالجرائم المعلوماتية على المستوى المحلي و الدولي ، حيث كانت أول قضية عالجتها المصلحة ذات بعد دولي في التعاون مع مكتب التحقيقات الفيدرالية أف بي أي وهذا بتقديم بلاغ إلى السلطات الجزائرية بسبب تعرض شركة أمريكية إلى عملية قرصنة بخصوص بيانات بنكية ، وتبين من التحقيق أنها منظمة إجرامية تنشط في مجال الإختراق والقرصنة ولها شريك بالجزائر، وبعد وصول البلاغ تم توجيه الملف لمصالح اللشرطة القضائية فيتم تشكيل فوج لللتحقيق مكون من ثلاث عناصر حيث تم بعد التحريات التعرف على مكان الشخص وتحديد هويته و تقديمه للعدالة ، ونفس الحالة بالنسبة لإختراق البنك الكندي .[2]

---

1 –<< المصلحة المركزية للجريمة الإلكترونية في مواجهة مجرمي العالم الإفتراضي>> ، **السلام اليوم** ، 2016/02/13 ، على الموقع:

https://www.djaziress.com/essalam/52564. ، تم الإطلاع على صفحة الويب بتاريخ :2019/01/12 .

2 –**المرجع نفسه** .

أما على المستوى الوطني المصلحة على إستعداد دائم لمعالجة القضايا المتعلقة بالجريمة الإلكترونية والجدول الأتي يبين عدد القضايا المعالجة من طرف المديرية العامة للأمن الوطني

الجدول رقم 01 : يبين عدد القضايا المعالجة على مستوى المديرية العامة للأمن الوطني

السنة	عدد القضايا المعالجة	عدد الأشخاص المتورطين
2007	31	31
2008	06	10
2009	29	21
2013	91	/
2014	245	/
2015	409	347
2016	1055	/
2017	2130	2101

المصدر: من إعداد الطالبة إعتمادا على الموقع:- www.radioalgerie.dz

- يوسف بوغرارة ، نفس المرجع السابق

نلاحظ من خلال الجدول وتتبع عدد القضايا المعالجة من قبل المديرية العامة للأمن الوطني خلال عشر سنوات من 2007 إلى غاية 2017 تزايد في عدد الجرائم السيبرانية فهي في تصاعد دائم ويعكس هذا زيادة عدد المستخدمين للأنترنت على المسوى الوطني ، وتتنوع القضايا المعالجة ففي سنة 2017 كما هو موضح في الجدول أعلاه سجلت مصالح المديرية العامة للأمن الوطني 2130 قضية تتعلق بالجرائم السيبرانية وشملت 1511 قضية متعلقة بالمساس بالأشخاص كالسب والقذف والمساس بحرمة الحياة الخاصة في الفضاء الإفتراضي عبر الأنترنات وتضرر من هذا النوع من السلوكيات المنحرفة 2381 ضحية ، كما بلغ عدد القضايا المتعلقة بجرائم الإبتزاز عن طريق شبكة الأنترنت 47 قضية أغلبها يتعلق بعروض عمل وهمية للحصول على المال ، و 49 قضية

متعلقة بالإعتداء على القصر متعلقة بأفعال غير أخلاقية ومخلة بالحياء ، و 28 قضية إعتداء على الأنظمة المعلوماتية وبريد إلكتروني لمؤسسات وخواص من خلال محو أو تغيير البيانات .[1]

فزيادة عدد القضايا المعالجة في كل سنة يعكس نجاعة المجهودات المبذولة من قبل مصالح الأمن الوطني في تتبع الجرائم السيبرانية ومعالجتها ، وهذا ناتج عن الخبرات المكتسبة في هذا المجال والكفاءات المؤهلة المتواجدة على مستوى المصلحة .

ولمعالجة القضايا بأكثر فعالية تم توسيع التشكيل الأمني بتكوين فصائل على مستوى أمن الولايات 48 وتعرف بـ :

- ✓ **فرقة مكافحة الجريمة المعلوماتية** : وهي فصائل **أمنية** تقوم بمعالجة الجرائم التي تمس الأفراد والمتعلقة بالنصب والإحتيال عبر الأنترنات والتهديد والمساس والإعتداء على الحياة الخاصة للأشخاص وغيرها من أنواع الجرائم الإلكترونية .

والقضايا المعالجة نواعان مباشرة أو عن طريق تعليمات نيابية ..

وفيما يلي جدول يوضح مجهودات فرقة مكافحة الجريمة الإلكترونية على مستوى أمن ولاية ورقلة .

جدول رقم 03: حصيلة نشاطات فرقة مكافحة الجريمة المعلوماتية لسنة 2017-2018 .

طبيعة الجريمة	عدد القضايا المسجلة		عدد القضايا المنجزة	
	سنة 2017	سنة 2018	سنة 2017	سنة 2018
المساس بحرمة الحياة الخاصة للأشخاص	04	09	04	08

1- << مجلة الشرطة : معالجة 2130 جريمة إلكترونية خلال 2017>>، **نفس الموقع السابق** .

الدخول عن طريق الغش إلى منظومة المعالجة الآلية للمعطيات	08	08	06	05
إنتحال إسم الغير عن طريق شبكة الأنترنت	02	00	02	00
القذف والسب والشتم عن طريق شبكة الأنترنت	05	06	04	02
النصب والإحتيال	02	01	02	01
الجموع	22	30	19	20

المصدر : من إعداد الطالبة إعتماداً على صور مقتطفة من معرض بدار الثقافة مفذي زكرياء ورقلة بمناسبة اليوم الوطني للشرطة 2018/12/18 .

نلاحظ من خلال الجدول أعلاه ان أكبر عدد من القضايا المسجلة في السنتين كانت موجهة ضد منظومة المعالجة الآلية للمعطيات وهذا بالدخول عن طرق الغش ، لترتفع حصيلة قضية المساس بحرية الحياة الخاصة للأشخاص من 04 قضايا سنة 2017 إلى 09 قضايا سنة 2018 ويفسر النسبة الضئيلة للقضايا المعالجة هو عدم التبليغ عن الجرئم من قبل الأفراد الضحايا وهذا لعدة أسباب ابرزها الخوف من الفضيحة .

وإن معالجة هذا النوع من القضايا على مستوى فرق مكافحة الجريمة الإلكترونية يتم بالتنسيق مع المجالس القضائية ، وهذا من خلال التعليمات النيابية المقدمة إلى فرق مكافحة الجريمة الإلكترونية .

وفيما يلي جدول مقارنة بين القضايا المباشرة ، التعليمات النيابية

الجدول رقم 04 : حصيلة نشاطات فرقة مكافحة الجريمة المعلوماتية بين القضايا المباشرة والتعليمات النيابية

طبيعة الجريمة	عدد القضايا المسجلة		عدد القضايا المنجزة	
	سنة 2017	سنة 2018	سنة 2017	سنة 2018
القضايا المباشرة	22	30	19	20
التعليمات النيابية	45	62	45	47

المصدر: من إعداد الطالبة إعتماداً على صور مقتطفة من معرض بدار الثقافة مفذي زكرياء ورقلة بمناسبة اليوم الوطني للشرطة 2018/12/18.

من خلال الجدول نلاحظ أن عدد القضايا المعالجة من قبل الفرقة والتي يكون مصدرها التعليمات النيابية ضعف القضايا المعالجة مباشرة ، وهذا يعكس التعاون بين المؤسستين في مجال مكافحة الجريمة .

فالنسب الورادة في الجدولين رقم: 03 و رقم : 04 يعكس المجهودات المبذولة من طرف فرقة مكافحة الجريمة المعلوماتية لمواجهة الجرائم المعلوماتية على مستوى ولاية ورقلة وهذا ينطبق على كل الفرق على المستوى الوطني .

✓ على مستوى الجيش الوطني الشعبي

حيث تم إستحداث مصلحة لمكافحة الجريمة السيبرانية وتتمثل في:

*** مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة**

قامت قيادة الجيش الوطني الشعبي بوضع إستراتجية دفاع سيبراني تغطي كل الجوانب التي لها صلة بتحقيق نظام دفاع سيبراني متكامل وفعال وبهذا أنشأة القيادة بتاريخ 2015/11/06 على مستوى دائرة الإستعمال والتحضير لأركان الجيش الوطني الشعبي " مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة "

- **مهمتها** : تكلف المصلحة بالعديد من المهام أهمها

1 -التخطيط و إدراج ومتابعة حالة تقدم نشاطات تجسيد السياسة الشاملة للدفاع السيبراني الهادفة لتحقيق بفاعلية الحماية ضد التهديدات السيبرانية التي تستهدف أنظمة المعلومات ومنظومات الإتصال وكذا منظومات الأسلحة للجيش الوطني الشعبي.[1]

2 إحباط كل محاولة للتجسس على أسرار الجزائر.

وتتمحور إستراتجية الدفاع السيبراني للجيش حول سبع محاور وهي :[2]

1 - **جانب وظيفي و تنظيمي** : حتى تكون أعمال الدفاع السيبراني ضمن الجيش الوطني الشعبي موجهة و منفذة في إطار سلسلة وظيفية أو تنظيمية مكرسة لضمان تجانس وفعالية هذه الأعمال .

2 -**جانب قانوني:** تحين وتعزيز بإستمرار الإطار القانوني المتعلق بإستعمال

---

1 -محمد بوكبشة ، **المرجع السابق** ، ص .35 .

2 -المرجع نفسه ، الصفحة نفسها .

تكنولوجيا الإعلام و الإتصال بشكل عام ، و تأمين منظومات الإعلام بشكل خاص .

3 -**جانب تقني:** تقوية وتكثيف القدرات التقنية للحماية وكشف والرد على الهجمات السيبرانية مع ضمان يقضة دائمة فيما يخص الطرق والوسائل المستعملة من طرف المهاجمين .

4 -**جانب الموارد البشرية** : العمل على إيجاد مورد بشري تقني معتبر وذي كفاءة عالية في مجال الدفاع السيبراني هذا من خلال عمليات التكوين وتبادل الخبرات وهذا يعتبر هذفاُ أساسياُ لضمان نجاح إدخال هذا المجال في النشاطات العملياتية والتسيير الحسن للجيش الوطني الشعبي .

5 -**جانب الوقاية والتحسيس** : وهذا من خلال الوقاية وتحسيس مستخدمي الجيش الوطني الشعبي من المخاطر والتهديدات التي تنجر عن إستعمال تكنولوجيا الإعلام والإتصال في الإطار المهني والشخصي بطريقة مستمرة .وهذا من خلال التنظيم المستمر التي تقوم به قيادة الجيش الوطني الشعبي في إقامة ملتقيات ومحاضرات عبر كل ولايات الوطن .

6 -**جانب البحث والتطوير** :إن إستقلالية إستعمال وسائل تقنية خاصة ومشخصة من طرف هياكل البحث والتطوير للجيش الوطني الشعبي ، لاسيما تلك المستعملة للحماية ضد التهديدات السيبرانية عنصرا حاسماُ في إستراتجية الدفاع السيبراني .

7 -**جانب التعاون** : وهذا من خلال تعزيز التعاون في مجال الدفاع السيبراني مع جيوش الدول الشريكة من أجل إعطاء فرصة للجيش الوطني الشعبي للإستفادة من الخبرات والوسائل التكنولوجية المتطورة. ولتعزيز إستراتجية الدفاع الوطني لمكافحة التهديدات السيبرانية وقصد الإلمام بكل التطورات في مجال الدفاع السيبراني وحماية المنشآت الحساسة ضد الهجمات السيبرانية ، تعمل المصلحة دورياً على تنظيم ملتقيات ومحاضرات وورش عمل تطبيقية من أجل خلق نقاش بين مختلف الفاعلين في الفضاء السيبراني على

المستويين الوطني والدولي من أجل تحسين و إثراء المعارف في مجال الوقاية ومكافحة التهديدات السيبرانية ومن أجل تحديد أثرها على الأمن الوطني .

- ✓ **على مستوى وزارة العدل**

وهذا بإنشاء **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها** ، وهي بمثابة سلطة إدارية مستقلة تم إنشاؤها بموجب المرسوم الرئاسي رقم 15-261 المؤرخ في 2015/10/08 يوجد مقرها بالجزائر لدى الوزير المكلف بالعدل.[1]

مهامها: تمارس الهيئة العديد من المهام وهذا حسب مانصت عليه المادة 14 من المرسوم وتتمثل في :[2]

1 - تنشيط وتنسيق عمليات الوقاية عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها .

2 - مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والإتصال وهذا من خلال جمع المعلومات وإنجاز الخبرات القضائية

3 - تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والإتصال

4 - ضمان المراقبة والوقاية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي المختص .

---

1 -الجمهورية الجزائرية الديمقراطية الشعبية ، المرسوم الرئاسي رقم 15-261 المتعلق بتحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها' ، المؤرخ في 2015/10/08 ، **الجريدة الرسمية** ، العدد 53 ، 2015/10/08 ، ص 16.

2 -**المرجع نفسه** ، الصفحة نفسها .

5- تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيا الإعلام والإتصال .

6- المساهمة في تحديث المعايير القانونية في مجال إختصاصها .

وتزود الهيئة عند القيام بمهامها بقضاة وضباط و أعوان للشرطة القضائية من المصالح العسكرية للإستعلام والأمن والدرك الوطني يتم تحديد عددهم بموجب قرارات مشتركة بين وزير العدل والدفاع و الداخلية كما تزود بمستخدمي الدعم التقني والإداري ضمن مستخدمي المصالح العسكرية للإستعلام والأمن والدرك الوطني كما يمكن لها الإستعانة بأي خبير أو أي شخص يمكن مساعدتهم في أعمالها شرط التزامهم بالسر المهني وواجب التحفظ وخضوعهم لإجراءات التأهيل.[1]

* **تشكيلة الهيئة و تنظيمها** :تضم الهيئة من حيث تشكيلها مايلي:

1 - **اللجنة المديرة** :حيث نصت المادة 07 على تأسيسها يرأسها الوزير المكلف بالعدل تتشكل من الوزير المكلف بالداخلية ، الوزير المكلف بالبريد و تكنولوجيا الإعلام والإتصال ، قائد الدرك الوطني المدير العام للأمن الوطني ، ممثل عن رئيس الجمهورية ، ممثل عن وزارة الدفاع الوطني ، قاضيان من المحكمة العليا .[2]

مهامها: نصت المادة 08 على المهام الموكلة إليها :[3]

- الإشراف والتوجيه ومراقبة عمل الهيئة وضبطه وتحديد شروط تنفيذه.
- دراسة كل مسألة تخضع لمجال إختصاص الهيئة .
- القيام بشكل دوري بتقييم حالة الخطر في مجال الإرهاب و التخريب والمساس بأمن الدولة للتمكن من تحديد مشتملات عمليات المراقبة الواجب القيام بها والأهداف المنشودة بدقة.

1- **المرجع السابق** ، ص.17.

2- **المرجع نفسه** ، الصفحة نفسها .

3- **المرجع نفسه** ، الصفحة نفسها ،

- إقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها .

- دراسة التقرير السنوي لنشاطات الهيئة والمصادقة عليه و إبداء رأيها في كل مسألة تتصل بمهام الهيئة مع تقديم كل إقتراح مفيذ يتصل بمجال إختصاصها .

2- **المديرية العامة :** يتولى إدارتها مدير عام يعين بموجب مرسوم رئاسي وتنهى مهامه بنفس الطريقة .

03 - **مديرية المراقبة و الوقاية واليقضة الإلكترونية :**

وحسب المادة 11 تقوم بتنفيذ عمليات المراقبة والوقاية للإتصالات الالكترونية من أجل الكشف عن الجرائم المتصلة بتكنولوجيا الإعلام الإتصال وهذا بناءاً على رخصة مكتوبة من السلطة القضائية وتتم تحت مراقبتها ، كما تقوم بإرسال المعلومات المحصل عليها إلى السلطات القضائية ومصالح الشرطة القضائية المختصة ، وتعمل على تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة ، كما تعمل الهيئة على جمع المعطيات في تحديد مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والإتصال والتعرف عليهم ، هذا بالإضافة إلى المشاركة في عمليات التوعية حول كيفية إستعمال تكنولوجيا الإعلام والإتصال وحول المخاطر المتصلة بها [1].

1 - **مديرية التنسيق التقني :** حيث تقوم هذه المديرية بإنجاز الخبرات القضائية في مجال إتصاص الهيئة ، تكوين قادة معطيات تحليلية للإجرام المتصل بتكنولوجيا الإعلام والإتصال وإستغلالها ، و إعداد الإحصائيات الوطنية المتعلقة بتكنولوجيا الإعلام الإتصال وهذا ما نصت عليه المادة 12 من المرسوم . [2]

---

1 -نفس المرجع السابق ، ص18.

2 -المرجع نفسه ، الصفحة نفسها .

2 -**مركز العمليات التقنية :** يتم تزويده بالمنشأت والتجهيزات والوسائل المادية و بالمستخدمين التقنيين الضروريين لتنفيذ العمليات التقنية لمراقبة الاتصالات التكنولوجية . يتبع المركز مديرية المراقبة الوقائية واليقضة الإلكترونية التي تكون تابعة لها.[1]

إن إنشاء الهيئة ومن خلال هياكلها المختلفة مكن بالفعل من تزويد العدالة بالمزيد من الموارد البشرية المؤهلة ومراجعة الترسانة التشريعية بما في ذلك في مجال الجزائي من تحسين حماية حقوق وحريات المواطنين وتشديد العقوبات على أي تقصير في هذا المجال .[2]

---

1 - **نفس المرجع السابق** ، نفس الصفحة السابقة .

2- أمنة محمدي بوزينة ، " **إجراءات التحري الخاصة في مجال مكافحة الجريمة المعلوماتية**"، مركز جيل البحث العلمي، 24 /2017/04 ، على الموقع : www.jilrc.com تم الإطلاع على صفحة الويب بتاريخ: 2018/12/12 .

❖ الهياكل التنظيمية على المستوى الخارجي :

✓ المنظمة الدولية لشرطة الجنائية:

تعمل المنظمة الدولية لشرطة الجنائية المسماة الأنتربول على مكافحة الجريمة بمختلف أنواعها، حيث تعمل على تجميع البيانات والمعلومات المتعلقة بالمجرمين وتبادلها مع شرطة الدول 182 الأطراف ، حيث تتيح مجالات تسهيل الإجراءات القضائية المتعلقة بتسليم المجرمين، وكذا مباشرة الإنبات القضائية الدولية و نشر أوامر القبض للمبحوث عنهم دوليا خاصة بالنسبة للجرائم المشتركة بين الدول من بينها جرائم الأنترنت ، ونظرا للبعد الدولي الذي عادة ما يتخذه هذا النوع من الجرائم أكدت الجزائر عضوتها الفعالة في المنظمة من خلال مجهوداتها الجبارة.[1]

وهذا ما تم تأكيده في الإجتماع ال 10 لرؤساء المصالح المختصة في مكافحة الجرائم المعلوماتية لدول الشرق الأوسط وشمال إفريقيا المنعقد يومي 10 و 11 ماي 2017 بفرنسا بتعين رئيس المصلحة المركزية لمحاربة ، الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال للمديرية العامة للأمن الوطني على رأس مجموعة خبراء الأنتربول المختصة في مكافحة الجريمة المعلوماتية و هذا إعترافا من الهيئات الدولية للمستوى العالي و الإحترافية التي أضحت تتميز بها الشرطة الجزائرية في مختلف المجالات .[2]

1- فضيلة عاقلي ، " الجريمة الإلكترونية ومواجهتها من خلال التشريع الجزائري" ، مداخلة ضمن فعاليات المؤتمر الدولي الربع عشر الجرائم الإلكترونية ، مركز جيل البحث العلمي، لبنان: طرابلس ، 24-2017/03/25 ، ص133 .

2- << مكافحة الجريمة المعلوماتية : تعيين خبير من الشرطة الجزائرية لترأس مجموعة خبراء الأنتربول>> ، وكالة الأنباء الجزائرية ، 28أيار2017 ، على الموقع : www.aps.dz ، تم الإطلاع على الويب بتاريخ 2019/04/12.

✓ **الإتحاد الدولي للإتصالات:**

هو مؤسسة متخصصة تابعة لمنظمة الإتحاد الدولي لتكنولوجيا الإعلام و الإتصال تم إنشاؤها سنة 1869 يوجد مقرها بجنيف (سويسرا) وهي تضم أكثر من 193 بلد عضو بالإضافة إلى منظمي قطاع تكنولوجيا الإعلام و الإتصال و مؤسسات القطاع العمومية و الخاصة و الهيئات الجامعية و الأكادمية[1]، يعمل الإتحاد الدولي للإتصالات على مساعدة الدول الأعضاء في الإتفاق على مبادئ مشتركة في مجال تكنولوجيا المعلومات و البنية التحتية للإتصالات، حيث وضع الإتحاد مخطط لتعزيز الأمن السيبراني من خلال تقليص الفجوة الرقمية عن طريق تشجيع دعم الكفاءة ورفع مستوى الثقة في إستعمال الفضاء السيبراني بفضل تأمين أحسن للنت، وكذا تطوير التشريعات في مجال الأمن السيبراني يكون قابلا للتطبيق المحلي و الدولي و أخرى لتحديد الحد الأدنى المقبول عالميا في معايير الأمن و نظم تطبيق البرامج و الأنظمة بالإضافة إلى تقديم مشورة بشأن إمكانية اعتماد إطار إستراتيجي عالمي لأصحاب المصلحة من أجل التعاون الدولي و الحوار و التنسيق[2] .

✓ **إسهامات الجزائر بالإتحاد:**

1- مؤتمر المندوبين المفوضي:

وهو الهيئة العليا للإتحاد حيث يعقد دوراته كل 4 سنوات من أجل تحديد المبادئ الأساسية و تقرير دوره المستقبلي، شاركت الجزائر في الدورة 19 للمؤتمر من 20 أكتوبر إلى 7 نوفمبر 2014، خلال هذه الدورة عرضت الجزائر مشروعين لتعديل الوائح و قرارات تم إعتمادها من قبل أعضاء الإتحاد يتعلق الأمر بـ:

1- << التعاون الدولي>> ، د ت ، على الموقع : www.mpttn.gov.dz/ar/content ، تم الإطلاع على صفحة الويب بتاريخ : 2019/02/04 .

2- فاتح حارك ، زكريا قطوش ، **تأثير الفضاء السيبراني على السياسة الأمنية للدول نمودج (الولايات المتحدة الأمريكية)** ، (مذكرة ماستر ، جامعة صالح بوبنيدر قسنطينة 3 ، كلية العلوم السياسية)، 2018/2017 ، ص 47 .

-القرار 174 تحت عنوان:دورة الإتحاد الدولي للإتصالات بخصوص مسائل السياسات العمومية الدولية ذات الصلة بأخطار إستعمال تكنولوجيا الإعلام و الإتصال لأغراض غير مشروعة

- القرار 130 تحت عنوان تعزيز دور الإتحاد الدولي للإتصالات في إرساء الثقة و الأمن في إستعمال تكنولوجيا الإعلام و الإتصال.

2) **المجلس:**

وينعقد مرة واحدة في السنة بمقر الإتحاد من أجل بحث مسائل سياسية الإتصالات،وضمان السير الحسن للإتحاد ويتم إنتخاب أعضائه من طرف مؤتمر المنذوبين، وينقسم إلى 5 مناطق و قد تم إنتخاب الجزائر بعنوان منطقة إفريقيا، كما أعيد إنتخابها عضو لمجلس الإتحاد و هذا لمساهماتها المفيذة و الفعالة لأشغال الإتحاد الذي تم عقده من 12 إلى 22 ماي 2015 أين حثت الجزائر المجتمع الدولي على العمل من أجل تفعيل اللائحة 174 التي تم من خلالها تعيين الإتحاد مشرفا على القيام بتنفيذها[1].

- ✓ **المكتب العربي للشرطة الجنائية :**

إنشاء مجلس وزراء العرب المكتب العربي للشرطة الجنائية بهدف تأمين و تنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة و ملاحقة المجرمين في حدود القوانين المعمول بها في كل دولة، بالإضافة إلى تقديم المعونة في مجال دعم و تطوير أجهزة الشرطة في الدول الأعضاء[2].

1- << التعاون الدولي>> ، **نفس الموقع السابق** .

2- أمال بوجليدة ،<<المعاهدات الدولية المتعلقة بالانترنت : مكافحة الجريمة الإلكترونية >> ، **مجلة الجيش**، العدد: 650 ، الجزائر، سبتمبر 2017 . ص ص. 46-47 .

✓ **التعاون الجزائري الأمريكي:**

ويعتبر التعاون الجزائري الأمريكي النموذج للتعاون الدولي التي تعمل الجزائر في نهجه للقضاء على الإرهاب، لما للولايات المتحدة الأمريكية من مكانة كقوة عسكرية عالمية في العالم كما أن هذا التعاون الثنائي يتم التفاعل بين البلدين في المجالات التالية:[1]

- موافقة الجزائر على المشاركة في الحرب التي تقودها الولايات المتحدة الأمريكية على الإرهاب لأنها كانت على قناعة بأنه لايمكن إلحاق الهزيمة بهذا الخطر المبهم و الغامض إلا عبر مشاركة جماعية عابرة للقوميات بتفويض دولي واضح.

- تبادل المعلومات الإستخبارية: فقد أسست الجزائر معرفة عميقة بالشبكات الإسلامية الإرهابية في جميع أنحاء العالم، وذالك كجزء من إستراتجية و طنية لهزيمة هذا الخطر من خلال عزله على خطوط دعمه الخارجية.

- التعاون بين وكالات الأمن و الإستخبارات ووزارتي دفاع البلدين

- التعاون العسكري في مجال التدريب في مختلف المدارس العسكرية و المعاهد و الجامعات الأمريكية لكن على الرغم من الطلبات الجزائرية المتكررة إلا أن الولايات المتحدة الأمريكية لاتزال مترددة في تزويد الجزائر بالأسلحة المتطورة اللازمة لمكافحة الإرهاب ولا سيما تجهيزات الرؤية الليلية.

كما يندرج التعاون الجزائر الأمريكي في تبادل المعلومات و تسليم المجرمين بخصوص الجرائم الإلكترونية .

1- قوي بوحنية و آخرون ، **نفس المرجع السابق** ، ص.461 .

✓ **مبادرة 5+5 دفاع:**

إنخرطت الجزائر التي تعمل بإستمرار على تهيئة مناخ من الأمن و الإستقرار في منطقة البحر المتوسط في هذه المبادرة بشكل كامل، وقامت بالتوقيع خلال إجتماع باريس 2004/9/30 على الوثيقة التأسيسية للمبادرة (5+5 دفاع) وهي إعلان النية الذي حدد إطار التعاون الأمن متعدد الأطراف في المنطقة لترقية النشاطات العملية في المجالات ذات الإهتمام المشترك و تشجيع تبادل وتقاسم المعارف و التجارب بين الدول الأعضاء و تسهيل التعاون البيني للقوات المسلحة ، و إقامة علاقة الثقة و التفاهم المتبادل بين الدول المبادرة للإستجابة بفعالية للتحديات المطروحة.

بالإضافة إلى جعل منطقة البحر االأبيض المتوسط منطقة سلام و إستقرار،وتغير الجريمة الإلكترونية من بين محالات التعاون ذات الإهتمام و الأولوية في المبادرة و هذا مايتضح من خلال تبادل الخيرات و المعارف و المشاريع المشتركة التي تنظمها المبادرة سنويا[1].

وكمثال لهذه التظاهرات نظمت الجزائر 22و23 أفريل 2015 بالنادي الوطني للجيش ملتقى دوليا حول "الجريمة المعلوماتية: شبكات التواصل الإجتماعي و الأمن العمومي" وقد حضر هذا الملتقى ممثلون عن الدول العشر الأعضاء في المبادرة لكل من فرنسا و إسبانيا،و إيطاليا،البرتغال،و مالطا عن الصفة الشمالية للمتوسط و الجزائر و تونس و المغرب و ليبيا و موريتانيا عن الضفة الجنوبية للمتوسط، و ممثلو وزراة الداخلية و الجماعات المحلية و العدل و البريد و تكنولوجيا الإعلام و الإتصال.[2]

1- إلهام غازي ، << التحديات الأمنية في البحر الأبيض المتوسط >> ، **مجلة الجيش** ،_العدد : 668 ، الجزائر ، مارس 2019 ، ص 53 .

2 -<< مبادرة (5+5 دفاع) الجريمة المعلوماتية ، شبكات التواصل الإجتماعي و الأمن العمومي >> ، **مجلة الجيش** ، العدد: 41 ، الجزائر ، ماي 2015 ، ص 41.

و تهدف أشغال هذا الملتقى الدولي المخصص لمكافحة الجريمة المعلوماتية و الوقاية منها إلى تحقيق الأهداف الآتية:[1]

– الإستفادة من الإستراتجيات المنتجة من طرف قوات الدرك و القوات المماثلة لها لدو الأعضاء في مبادرة 5+5 دفاع في مجال الوقاية و مكافحة الجريمة المعوماتية

– تبادل الخيرات و التجارب الميدانية بغرض التقليل من مخاطر شبكات التواصل الإجتماعي على الأمن العمومي للبلدان الأعضاء في المبادرة

– تبادل المعلومات حول السياسات و الإجراءاتو الوسائل التقنية للتحري ومكافحة الجريمة المعلوماتية .

– التشاور حول فرص و آليات تجسيد تعاون ميداني بين الهياكل المختصة للدول الأعضاء في المبادرة في مجال مكافحة الجريمة المعلوماتية.

و تمثل الهدف الأساسي من هذا الملتقى هو بحث العلاقة بين شبكات التواصل الإجتماعي و الأمن العمومي من منظور إستخدام هذه الشبكات من طرف المجرمين قصد تسهيل نشاطهم الإجرامي هذا بالإضافة إلى المخاطر الأخرى لهذه الشبكات و التي من شأنها أن تؤثر سلبا عن الأمن العمومي.

وتم إختتام أشغال هذا الملتقى بتبني العديد من التوصيات تنص على ضرورة تكثيف الجهود لمحاربة هده الآفة بكل أشكالها و ترجمة هذه الجهود و تجسيدها قصد الوصول إلى مكافحة أكثر فعالية للجريمة المعلوماتية بالإعتماد على التطور التكنولوجي في هذا المجال .

1– **نفس المرجع السابق** .نفس الصفحة السابقة .

خلاصة الفصل الثاني:

إن تزايد عدد مستخدمي الأنترنت بالجزائر و الذي فاق 33 مليون جزائري منهم 19 مليون لديهم موقع تواصل اجتماعي ، يعكس تزايد عدد التهديدات السيبرانية المتربصة بالجزائر ، و أمام التزايد الهائل التي تعرف هـ الجريمة السيبرانية بمختلف أشكالها تعمل الجزائر على مكافحتها وهذا بتكثيف جهودها والتي مست جميع الجوانب ، حيث عملت الجزائر على إستحداث وتحيين القوانين والتشريعات الوطنية ،وكذا إقامة إتفاقيات وهذا من الناحية القانونية ، أما من الجانب الأمني عملت الجزائر على مكافحة هذه التهديدت بإنشاء العديد من الهياكل التنظيمية على المستوى الوطني من خلال أجهزتها الأمنية المختلفة الأمن الوطني ، الدرك الوطني ، والجيش الوطني الشعبي ، كما إنخرطت في العديد من المنظمات الدولية ذات الإهتمام المشترك . فإنخراط الجزائر في هكذا منظمات عزز من قوة الجزائر في مجال الدفاع السيبراني .حيث تندرج نقاط التعاون ضمن تبادل الخبرات ، تقديم المساعدات في إطار المعاملة بالمثل .

الخـاتـمـة

الخــاتمة

يعد الدفاع الوطني العمود الفقري للدولة الجزائرية ، فبتكوين منظومة دفاعية قوية تستطيع الجزائر الحفاظ على مكانتها . فلم يعد الدفاع الوطني يقتصر على الجانب العسكري بل تعداه إلى مختلف الجوانب الأخرى ، فوجود الفضاء السيبراني وما أفرزه من تهديدات غير بطريقة ديناميكية في الإستراتجية الدفاعية للجزائر ، وهذا بإدراج الفضاء السيبراني ضمن أولوياتها

النتائـــج

من خلال الدراسة الفضاء السيبراني وإشكالية الدفاع الوطني في الجزائر " الواقع والأفاق " وللإجابة على الإشكالية المطروحة و التأكد من صحة الفرضية توصلت الدراسة إلى النتائج الأتية :

- الفضاء السيبراني بإعتباره ساحة جديدة للصراع غير من مفاهيم عديد المصطلحات التقليدية .
- التهديدات الأمنية تتغير وذلك بالتطور التكنولوجي المتسارع و الإعتماد المتزايد للدول على الفضاء لسيبراني.
- صعوبة التعرف على معلومات الخصم في الفضاء السيبراني و إمكانياته و قدراته التدميرية على عكس ما كان في الواقع التقليدي .
- عدم تحصين الدولة لبنيتها التحتية يجعلها عرضة للهجمات والتهديدات السيبرانية (الإختراق ، القرصنة ، التخريب ، التلاعب ....) وهذا ما ينعكس بالسلب على أمنها القومي .
- اقامة الجزائر للعلاقات تعاون ثنائية ودولية للمواجهة تهديدات الفضاء السيبراني يعزز من من قدراتها الدفاعية من خلال تبادل الخبرات ، تقديم مساعدات في إطار المعاملة بالمثل .

- الاهتمام الجديد للمنظومة الدفاعية الجزائرية بات يركز على الدفاع السيبراني خاصة مع انتشار مختلف التهديدات الأمنية عبر الفضاء السيبراني.
- مساهمة الجزائر في عديد المنظمات الأمنية مثل الإتحاد الدولي للإتصالات والمنظمة الدولية للشرطة الجنائية يجعلها رائدة في مجال الدفاع السيبراني .
- القوانين المستحدثة والمحينة من قبل الدولة الجزائرية لاتزال قاصرة في مكافحة الجريمة السيبرانية خاصة وأن هذه الأخيرة في تطور متسارع .
- إذا أرادت الجزائر فعلا تعزيز أمنها السيبراني ، عليها العمل جديا في تطوير منظومتها الدفاعية في مجال الدفاع السيبرني وهذا من خلال إستحداث العديد من المصالح والتي تمس كافة ولايات الوطن .
- ستستمر الجزائر في إقامة علاقات تعاون ثنائية و دولية وهي "علاقات تتمنى أن تخدم المصالح الجزائرية وتزيد من تعزيز دفاعها السيبراني .

التوصيات :

وأخيرا نورد بعض التوصيات :

- تكثيف المشاركة في الجهود الدولية والإقليمية لتحفيز الوقاية الوطنية والتحضير لمواجهة الحوادث السيبرانية .
- إدراج مقياس الأمن السيبراني لتدريسه بالجامعات ومركز التكوين وهذا من أجل التعريف بالفضاء السيبراني وخطورته وطرق الوقاية .
- تحصين مختلف المؤسسات العامة والخاصة من الهجمات السيبرانية بالبرمجيات والأدوات المتطورة وهذا من اجل رصد الهجمات وتحليلها والوقاية منها .
- إعداد دراسات مقارنة مع الدول السباقة في مجال الدفاع السيبراني وإستخلاص نقاط القوة والضعف والإستفادة منها .

- نشر الوعي والثقافة في التعامل مع التكنولوجيا المتطورة عبر جميع المؤسسات التربوية مدرسة ، جامعة ، معاهد ، وتفعيل دور المسجد في مكافحة التطرف .
- إرسال بعثات إلى الخارج لتكوينهم وتدريبهم في مجال مكافحة التهديدات السيبرانية والإستفادة منهم بأرض الوطن .

قائمة المراجع

الوثائق الرسمية:

- الجمهورية الجزائرية الديمقراطية الشعبية ، المرسوم الرئاسي رقم 183/04 المتعلق بتأسيس المعهد الوطني للأدلة الجنائية ، المؤرخ في 2004/08/26 ، **الجريدة الرسمية** ، العدد رقم: 41 ، الصادرة بتاريخ: 2004/06/27 .

- الجمهورية الجزائرية الديمقراطية الشعبية ، القانون رقم 04-15 المعدل والمتمم للأمر 66-156 المتعلق بقانون العقوبات، المؤرخ في 2004/11/10 ، **الجريدة الرسمية** ، العدد 71 ، الصادرة بتاريخ : 10/ 2004/11 .

- الجمهورية الجزائرية الديمقراطية الشعبية ، المرسوم الرئاسي رقم 375/07 المتعلق المتضمن التصديق على الإتفاق بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الفرنسية المتعلق بالتعون في مجال الأمن ومكافحة الإجرام المنظم ، المؤرخ في 2004/08/05 ، **الجريدة الرسمية** ، العدد رقم : 77 ،الصادرة بتاريخ: 2007/12/09 .

- الجمهورية الجزائرية الديمقراطية الشعبية ، القانون رقم 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها' ، المؤرخ في 2004/08/05 ، **الجريدة الرسمية** ، العدد رقم : 47 ، الصادرة بتاريخ : 2009/08/16 .

- الجمهورية الجزائرية الديمقراطية الشعبية ، المرسوم الرئاسي رقم 15-261 المتعلق بتحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها ' ، المؤرخ في 2015/10/08 ، **الجريدة الرسمية** ، العدد رقم: 53 ، الصادرة بتاريخ: 2015/10/08 .

- **إتفاقية الإتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي** ، ملابو غينيا ، الصادرة بتاريخ : 2010/06/27 .

- **الإتفاقية العربية لمكافحة جرائم تقنية المعلومات** ، جامعة الدول العربية، الصادرة بتاريخ:2010/12/31 .

المصادر :

- الأزهري أبي منصور محمد بن أحمد. **تهديب اللغة** ، الدار المصرية للنشر ، مادة " فضا " .
- البعلبكي رمزي منير ، **المورد الحديث : قاموس إنكليزي – عربي حديث** ، بيروت : دار العلم للملايين .دت .
- يانكوف م ، يوتوفا ل ، **السيبرنتيك والاعلام**،(ترجمة: برهان العلى)، ط 1، بيروت دار الطليعة ، 1979 .

الكتب:

باللغة العربية :

- أبو علي عامر ، **فيروسات الكمبيوتر**، مصر : دار حنين ، ط$_1$ ، 1994 .
- بدوي عبد الرحمان ، **مناهج البحث العلمي** ، ط3 ، الكويت : وكالة المطبوعة ، 1977.
- كماش يوسف لازم ، عبد الكاظم جليل حسان ، **سيكولوجية التعلم والتعليم** ، ط $_1$ ، عمان: دار الخليج ،2018 .
- ماتيو جان لوك ، **الدفاع الوطني** ، كوساج للمنشورات الجامعية ، 1996 .
- ممدوح إبراهيم خالد ، **أمن الجريمة الإلكترونية** ، الإسكندرية : الدار الجامعية ، 2008.
- عبد الطائي عبيد عبد الله ، **أحكام الفضاء في الفقه الإسلامي** ، بيروت : دار الكتب العلمية . د ت.
- قوي بوحنية و أخرون ، **فهم الأمن القومي من مذخلي الأمن الوطني والدفاع الوطني** ، عمان : دار ومكتبة الحامد ، ط . 1 ، 2015 .
- شلبي محمد ، **المنهجية في التحليل السياسي (مفاهيم – المناهج– الاقترابات)** ، الجزائر : ديوان المطبوعات الجامعية ، 1997.

باللغة الأجنبية

- Choucri Nazli, **Cyberpolitics International Relations** , The Mitpress Cambridge , Massachusets , London .
- peter w Singer And Allanfriedam , **Cybersecurity And Cyberwar, what Everyone Needs to know,** USA: University of oxfordpress,2014 .
- Clarke Richarda & Knake Rebert, **Cyber War : The Next Threat to National Security and What to de about it** , Harper Collins , 2010.

المقالات:

- باللغة **العربية** :

- الكعبي كريمة شافي جبر ، << مجتمع المعلومات في العالم العربي – العراق أنمودجا >> ، **مجلة كلية الأدب** ، الجامعة المستنصرية ، قسم المجتمع المدني ، العدد 98 .

- إ توريه حمدون ، << البحث عن السلام السيبراني>> ، **الإتحاد الدولي للاتصالات**، يناير 2011 .
- بلفرد لطفي لمين ،<< التهديدات الأمنية في الفضاء السيبراني الجزء الثاني>> ، **مجلة الشرطة** ، ع 129 ، ديسمبر 2015.

- بوجليدة أمال <<المعاهدات الدولية المتعلقة بالانترنت : مكافحة الجريمة الإلكترونية >> ، مجلة الجيش، العدد: 650 ، الجزائر، سبتمبر 2017 .
- بوكبشة محمد ، << الأمن والدفاع السيبراني (أولوية قصوى)>> ، **مجلة الجيش** ، العدد رقم: 651 ، الجزائر، أكتوبر 2017 .

- بوغرارة يوسف ،<< الأمن السيبراني : الإستراتجية الجزائرية للامن والدفاع في الفضاء السيبيري>> ، **الدراسات الإفريقية وحوض النيل** ، المجلد رقم: 1 ، العدد:3 ، سبتمبر/أيلول،2018

- العقيد بن رجم جمال، << حماية منظومتنا الوطنية للمعلومات من خلال تطبيق القانون>>، **مجلة الجيش** ، العدد رقم: 599 ، الجزائر ، جوان 2013.

- جنادي إسماعيل ،<< الأمن السيبراني التحدي القادم للإتحاد الإفريقي >>، **مجلة الجيش** ، العدد: 663 ، الجزائر ، أكتوبر 2018.

- ج رضوان ، << الأمن السيبراني : أولوية في إستراتجيات الدفاع >> ، **مجلة الجيش** ، العدد: 630 ، الجزائر، جانفي 2016 .

- طوالبية محمد ، << إيديولوجية الفضاء الرقمي دراسة في الخلفيات المرجعية >> ، **الأكاديمية للدراسات الإجتماعية و الإنسانية** ، جامعة حسيبة بن بوعلي الشلف ، العدد: 21 ، جانفي 2019 .

- ليتيم فتيحة ، ليتيم نادية ، << الأمن المعلوماتي للحكومة الالكترونية و إرهاب القرصنة>> ، **مجلة الفكر** ، كلية الحقوق والعلوم السياسية ، جامعة محمد خيضر بسكرة ، العدد رقم: 12 .

- لين هربت ،<< النزاع السيبراني والقانون الدولي الإنساني >> ، **مجلة الصليب الأحمر** ، المجلد رقم : 94 ، صيف 2012.

- محمد يحي ربيع ، << إسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط >> ، **مجلة رؤى إستراتجية** ، المجاد رقم :1، العدد رقم :2 ، يونيو 2013.

- شفيق نوران ،<< أثر التهديدات الالكترونية على العلاقات الدولية : دراسة في أبعاد الأمن الإلكتروني>> ، **السياسة الدولية و الإستراتجية** .دت ، دم.

- شريف حميدة فضيل ، << صناعة الدفاع بين : البحث والتطوير، التكنواوجيا والإزدواجية >> ، **مجلة الجيش** ،الجزائر، العدد رقم: 645 ، أفريل 2017.

- تريمبلاي جيه جي إي ، << الأمن السيبراني منهج مرجعي عام >> ، **مجلة أكاديمية الدفاع الكندي** ، أكتوبر 2016 .

- غازي إلهام ،<< الدفاع السيبراني >>، **مجلة الجيش** ، العدد: 663 ، الجزائر، أكتوبر 2018 .

- غازي إلهام ،<< التحديات الأمنية في البحر الأبيض المتوسط >> ، **مجلة الجيش** ، العدد : 668 ، الجزائر ، مارس 2019 .

- << الأمن السيبراني بالجزائر >> ، **مجلة الجيش** ، العدد: 663 ، الجزائر ، أكتوبر 2018.

- د م ،<< إستخدام الانترنت في أغراض إرهابية>> ، **مكتب الأمم المتحدة المعني بالمخدرات والجريمة** ، نيويورك ، 2012 .

-<< دليل المرونة السيبرانية للتعاون بين القطاعين الحكومي والخاص >> ، المنتدى الإقتصادي العالمي (WEF) .

- << مبادرة (5+5 دفاع) الجريمة المعلوماتية ، شبكات التواصل الإجتماعي و الأمن العمومي>> ، **مجلة الجيش** ، العدد: 41 ، الجزائر ، ماي 2015 .

- باللغة الأجنبية :

- Kissel Richard, <<Glassory Of Key Information Security Terms National Institute Of Standards and Tchnology>> , U S , Department of commerce ,Revision,2,May,2013 .

المذكرات :

– بغو إبتسام ، **إجراءات المتابعة الجزائية في الجريمة المعلوماتية** ، (مذكرة ماستر في القانون ، جامعة العربي بن مهيدي أم البواقي، قسم الحقوق)، 2016/2015.

– دحماني سليم ، **أثر التهديدات السيبرانية على الأمن القومي الولايات المتحدة الأمريكية أنموذجاً (2001– 2017)** ، (مذكرة ماستر ، جامعة محمد بوضياف المسيلة : كلية الحقوق والعلوم السياسية) ، 2018/2017 .

– حارك فاتح ، قطوش زكريا ، **تأثير الفضاء السيبراني على السياسة الأمنية للدول نمودج (الولايات المتحدة الأمريكية)** ، (مذكرة ماستر ، جامعة صالح بوبنيدر قسنطينة 3 : كلية العلوم السياسية) ، 2018/2017 .

– عراجي أنديرا ، **القوة في الفضاء السيبراني : فصل عصر من التحدي والإستجابة** (رسالة لنيل دبلوم دراسات عليا في العلوم السياسية و الإدارية ، جامعة لبنان: كلية الحقوق والعلوم السياسية والإدارية) ،2015/ 2016 .

الملتقيات :

– الاخضري نصر الدين ، " الجيش الوطني الشعبي بين واجب حماية الحدود والالتزام بالمشاركة في بعث أسباب التنمية" ملتقى الدفاع الوطني بين الالتزامات السيادية والتحديات الإقليمية، كلية الحقوق والعلوم السياسية ، جامعة ورقلة ، 13/12 نوفمبر 2014 .

– إسريق محند الصالح ، " مفهوم الدفاع الوطني في القانون الجزائري: الجدور والأركان" ، مداخلة ضمن فعاليات الملتقى الموسوم بـ الدفاع الوطني بين الالتزامات السيادية والتحديات الإقليمية، كلية الحقوق والعلوم السياسية ، جامعة ورقلة ، 13/12 نوفمبر 2014.

– بارة سمير ، "الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر – الدور والتحديات– " ، مداخلة ضمن فعاليات ملتقى سياسة الدفاع الوطني

بين التحديات الإقليمية والإلتزامات السيادية ، كلية لحقوق والعلوم السياسية ، جامعة ورقلة ، ط 2 ، 30-2017/01/31

- بوزيدي مختارية ، " ماهية الجريمة الإلكترونية "، مداخلة ضمن فعاليات الملتقى الوطني الموسوم بـ أليات مكافحة الجرائم الإلكترونية في التشريع الجزائري ، مركز جيل البحث العلمي ، الجزائر العاصمة، 2017/03/29 ..

- بن داود براهيم ، جمال عبد الكريم ، " الدفاع الوطني بين متطلبات الأمن الفكري ومقومات الأمن الإستراتجي " ،مداخلة ضمن فعاليات الملتقى الموسوم بـ الدفاع الوطني بين الالتزامات السيادية والتحديات الإقليمية، كلية الحقوق والعلوم السياسية ، جامعة ورقلة ، 13/12 نوفمبر 2014 .

- بن مرزوق عنترة ، حرشاوي محي الدين ، " الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية" ، مداخلة ضمن فعاليات ملتقى سياسة الدفاع الوطني بين التحديات الإقليمية والإلتزامات السيادية ، كلية لحقوق والعلوم السياسية ، جامعة ورقلة ، ط 2 ، 30-2017/01/31.

- بن صويلح أمال ، " الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الالكتوني بالجزائر" ،مداخلة ضمن فعاليات الملتقى الإجرام السيبراني المفاهيم والتحديات ، جامعة 08 ماي 1945 قالمة ، 12/11 أفريل 2017 .

- دويب حسين صابر، مداخلة بعنوان : **القوانين العربية وتشريعات تجريم الجرائم السيبرانية وحماية المجتمع** ، (جمعية المكتبات والمعلومات ، الرياض ، 3-2009/11/4) .

-عاقلي فضيلة ،" الجريمة الإلكترونية ومواجهتها من خلال التشريع الجزائري" ، مداخلة ضمن فعاليات المؤتمر الدولي الربع عشر الموسوم بـ الجرائم الإلكترونية ، مركز جيل البحث العلمي، لبنان: طرابلس ،24-2017/03/25 .

- قادير إسماعيل ، " إدارة الحروب النفسية في الفضاء الإلكتروني : الإستراتجية الأمريكية الجديدة في الشرق الأوسط " محاضرة بـالندوة الدولية عولمة الإعلام السياسي وتحديات الأمن القومي للدول النامية ، جامعة الجزائر 03 .
- شلبي محمد ، " الأمن الوطني في ظل التحولات الدولية الراهنة " ، مداخلة ضمن فعاليات الملتقى الموسوم بـ الدولة الوطنية والتحولات الدولية الراهنة ، كلية العلوم السياسية والإعلام ، جامعة الجزائر ، 2004.

الواب غرافيا :

- معجم اكسفورد: على الموقع:

http://en.exforddictionaris.com /définition/cyberspace. تم الإطلاع على صفحة الويب بتاريخ : 2018/09/10

-معجم كامبرادج، على الموقع :

http://dictionory.combridage.org/fr/dictionnaire/englais/cyberpace تم الإطلاع على صفحة الويب بتاريخ : 2018/09/10

- آيت صديق بهاء الدين ، << الكشف عن عدد الجرائم الالكترونية المعالجة بالجزائر سنة 2017 >>، 2018/01/18 ، على الموقع : https://www.android-dz.com ، تم الإطلاع على صفحة الويب بتاريخ 2019/02/01 .

- بوزينة أمنة محمدي ،<< إجراءات التحري الخاصة في مجال مكافحة الجريمة المعلوماتية>>، مركز جيل البحث العلمي، 24 /2017/04 ، على الموقع : www.jilrc.com . تم الإطلاع على صفحة الويب بتاريخ: 2018/12/12 .

- بورنان يونس ، << قانون جديد في الجزائر لمكافحة الجرائم الإلكترونية>> ، 2018/03/28 على الموقع: : http://al-ain.com ، تم الإطلاع على صفحة الويب بتاريخ 2019/04/12 .

- جبور منى الأشقر ، **السيبرانية هاجس العصر** ، المركز العربي للبحوث القانونية والقضائية >>، على الموقع :
https://www.carjj.org/sites/default/files/ebooks/cyber.ebook.pdf

- جبور منى الأشقر ،<< الأمن في الفضاء السيبيري>> ، على الموقع :
www.Xa.yimg.com/kq/groups/166186325/1096065403/name/ÇãÃä+ýí+ÇáýÖÁ+ÇáÓíÉíÑí.doc

- الزبيدي سامي ، << الدفاع عن النفس في ضوء القانون الدولي ميثاق الأمم المتحدة>> ، 2018/07/02 ، على الرابط: www.azzaman.com تم الإطلاع على صفحة الويب بتاريخ: 2018/12/04.

- حداد أسماء ،<< الدفاع الوطني الجزائري: الواقع و الرهانات الاستراتجية >> ، المركز الوطني الديمقراطي ، 207/05/24 ، على الموقع :
https://democraticac.de/?p=4673، تم الإطلاع على صفحة الويب: 2018/07/12 .

- طويلة جميل حسين ، **البرمجيات الخبيثة (سوريا ، 2016)** ، على الموقع :
http://dounload.internet-bdf-ebooks.com/14777-free-book تم الإطلاع على صفحة الويب بتاريخ : 2018/12/12 .

- عبد الصادق عادل ،<< الفضاء الالكتروني والرأي العام تغير المجتمع والأدوات ، و التأثير>> ، **قضايا إستراتجية** ، المركز العربي لأبحاث الفضاء الالكتروني ، 2011/08/26 ، على الموقع :
www.accronline.com/article-detail.aspx?id=2725 تم الإطلاع على صفحة الويب بتاريخ : 2018/12/12.

- عبد الصادق عادل ، << الفضاء الالكتروني وتهديدات جديدة للأمن القومي >> **قضايا إستراتجية** ، المركز العربي لأبحاث الفضاء الإلكتروني ، فبراير 2012 ، 2013/02/11 ، على الموقع :
www.accronline.com/print-aspx?id=8745 تم الإطلاع على صفحة الويب بتاريخ :2018/12/12.
- الصباحي نسرين ، <<الحروب السيبريانية و تحديات الأمن العالمي >>، المركز العربي للبحوث و الدراسات على الرابط :
http://www.acrseg.org/40594 تم الإطلاع على صفحة الويب بتاريخ2019/01/12
- شوقي إيهاب ، << الإرهاب الإلكتروني وجرائمه>> ، 2015/12/07 ، تاريخ الإطلاع : 2018/11/04 ،على الرابط :
www.anntv.tv/new/showsubject.aspx?ib=121062
- الشحات الصباحي علي نسرين ، <<الأبعاد العسكرية للقوة السيبرانية على الأمن القومي للدول دراسة حالة إسرائيل مند عام >> ، المركز ادمقراطي العربي. على الرابط: https://democaticac.de/?p=30262 ، تم الإطلاع على صفحة الويب بتاريخ 2019/01/12 .
- خليفة إيهاب ، << القوة الإلكترونية و أبعاد التحول في خصائص القوة>> ، 2014/06/30 ، على الرابط :
https://middle-east-online.com ، تم الإطلاع على صفحة الويب بتاريخ: 2019/01/21 .
- غربي محمد ، << من أجل مفهوم جديد لنظرية الدفاع والأمن : حالة منطقة البحر الأبيض المتوسط >>، جامعة الشلف ،. على الرابط :
Revws-Univ-Ouargla.dz/index-php/numero-01-2009-dafater/511-2013-05-02 10-48-57

، تم الإطلاع على صفحة الويب بتاريخ :2019/02/24

– سحواد نسيمة ، مقابلة مع العقيد سيد أحمد بوزمالة ، المدير العام لمعهد الأدلة الجنائية وعلم الإجرام للدرك الوطني ، 2014/12/08 ، 18:29سا، على الموقع :

ar– dk news–dz.com/index– php/nation/actualite25768.
2014.12.17

– << الإرهاب الالكتروني يهدد الجزائر >>، 2017/05/13 ، تم الإطلاع على صفحة الويب ب تاريخ 2018/12/01 ، على الرابط :
www.m.elbilad.net/article/detail?id=70386

– << رسالة الرئيس بوتفليقة بمناسبة إنعقاد الدورة 35 لمجلس وزراء الداخلية العرب>>، 2018/03/07 على الوقع : www.radioalgerie.dz ، تم الإطلاع على صفحة الويب بتاريخ 2019/05/12.

–<< مجلة الشرطة : معالجة 2130 جريمة الكترونية خلال 2017 >>، 2018/04/17 ، على الموقع : www.radioalgerie.dz ، تم الإطلاع على صفحة الويب بتاريخ 2019/03/02

– << الدرك يدعو ضحايا – الإبتزاز الإفترصي– إلى التبليغ عن المتورطين>> ، 2018/11/27، على الموقع ،https://www.tsa– algerie.com تم الإطلاع على صفحة الويب بتاريخ 2019/03/14 .

– << الجرائم الالكترونية تهدد أمن الجزائريين >> ، 2018/04/10 ، على الموقع www.djazairess.com/akhabrelyoum/240271 تم الإطلاع صفحة الويب بتاريخ 2019/05/01 .

– << التعاون الدولي>> ، على الموقع :
www.mpttn.gov.dz/ar/content ، تم الإطلاع على صفحة الويب بتاريخ : 2019/02/04 .

– << سيبرنيتيك>> . على الموقع https://www.m,marefa.org تم الإطلاع على صفحة الريب بتاريخ : 2018/08/12 .

– << المجال الخامس ..الحروب الإلكترونية في القرن ال 21 >>. على الموقع: : http://studies.aljazeera.net/ar/issues/2010/20117212274346868.html

تم الإطلاع على صفحة الويب:2018/12/25

–<< المصلحة المركزية للجريمة الإلكترونية في مواجهة مجرمي العالم الإفتراضي>> ، **السلام اليوم** ، 2016/02/13 ، على الرابط: https://www.djaziress.com/essalam/52564.

تم الإطلاع على صفحة الويب بتاريخ :2019/01/12 .

– << مكافحة الجريمة المعلوماتية : تعيين خبير من الشرطة الجزائرية لترأس مجموعة خبراء الأنتربول>>، وكالة الأنباء الجزائرية ، 28أيار 2017 ، على الموقع : www.aps.dz ، تم الإطلاع على الويب بتاريخ 2019/04/12.

–Sarah Ggordon, Richard Ford , **Cyberterrorism**? , http://www.symantec.com page web consultee le12/03/2018 .

الفهرس

فهرس الجداول

رقم الجدول	عنوان الجدول	الصفحة
01	عدد القضايا المعالجة على مستوى مركز الوقاية من جرائم الإعلام الألي و الجرائم المعلوماتية للدرك الوطني	59
02	عدد القضايا المعالجة على مستوى المديرية العامة للأمن الوطني	61
03	حصيلة نشاطات فرقة مكافحة الجريمة المعلوماتية لسنة 2018/2017	62
04	حصيلة نشاطات فرقة مكافحة الجريمة المعلوماتية بين القضايا المباشرة والتعليمات النيابية	64

فهرس العام

العنوان		رقم الصفحة
مقدمة		02
الفصل الأول	مفهوم الفضاء السيبراني وعلاقته بالدفاع الوطني	10
المبحث الأول	مفهوم الفضاء السيبراني وعلاقته بالمفاهيم ذات الصلة	11
المبحث الثاني	مفهوم الدفاع الوطني وعلاقته بالمفاهيم ذات الصلة	21
المبحث الثالث	علاقة الفضاء السيبراني بالدفاع الوطني	27
الفصل الثاني	واقع الدفاع السيبراني بالجزائر	42
المبحث الأول	التهديدات السيبرانية بالجزائر	43
المبحث الثاني	الجانب القانوني في مواجهة التهديدات السيبرانية	48
المبحث الثالث	الجانب الأمني في مواجهة التهديدات السيبرانية	57
الخاتمة		79
قائمة المراجع		84
فهرس الجداول		97
الفهرس العام		98