جامعة العربي التبسي -تبسة-

كلية الحقوق والعلوم السياسية

قسم: العلوم السياسية

الإستراتيجيات الدولية في مكافحة الجريمة السيبرانية

- دراسة حالة الجزائر -

مذكرة مكملة لنيل شهادة الماستر في العلوم السياسية والعلاقات الدولية

تخصص: دراسات إستراتيجية وأمنية

إعداد الطالبين:

- ✓ شعيب قاسمي
- ✓ فؤاد بلغيث

إشراف الأستاذ:

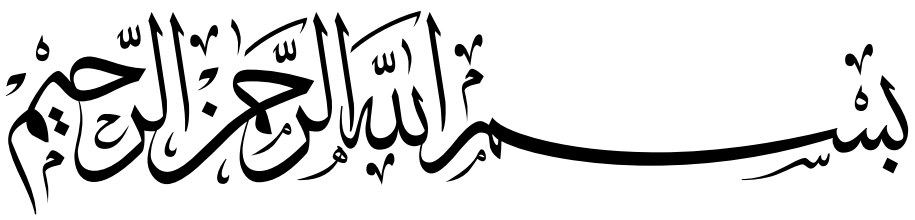
الدكتور: البار أمين

جامعة العربي التبسي - تبسة
Université Larbi Tebessi - Tebessa

لجنة المناقشة:

الاسم واللقب	الرتبة العلمية	الصفة
يوسف ازروال	أستاذ محاضر – أ –	رئيسا
أمين البار	أستاذ محاضر – أ –	مشرفا ومقررا
فتحي معيفي	أستاذ محاضر – ب –	مناقشا

السنة الجامعية 2020/2019


بسم الله الرحمن الرحيم

الملخص

تناولت هذه الدراسة الإستراتيجية الدولة لمكافحة الجريمة السيبرانية انطلاقا من دراسة حالة الجزائر، وهدفت إلى معرفة الجريمة السيبرانية التي ظهرت جراء التطور الهائل في عالم التكنولوجيا والمعلومات، فهذه الجرائم أصبحت تشكل خطرا كبيرا على الأمن القومي للدول، وفي الجزء الثاني فصلنا في الاستراتيجيات التي اتبعتها الدول لمواجهة هذه التهديدات الجديدة، خاصة الدول الكبرى مثل الولايات المتحدة الأمريكية وروسيا، بالإضافة إلى الدول العربية، ومن بين هذه الدول نجد الجزائر التي وضعت العديد من الاستراتيجيات تمثلت في آليات قانونية وتقنية، وإنشاء العديد من المراكز الأمنية لمكافحة هذه الجرائم، بالإضافة إلى التنسيق الإقليمي في إطار ثنائي أو جماعي للتصدي لهذه الجرائم السيبرانية.

ABSTRACT.

This strategic study examined the state's strategy to combat cyber crime from the case study of algeria and aimed to know the cyber crime that emerged asa result of the tremendous development in the world of technology and information, these crimes have become a major threat to the national security of countries, and in the second part we detailed the strategies that countries followed to confront these new threats, especially the major countries such as the united states of america and russia, in addition to the arab countries, and among these countries we find algeriq, which put many strategies represented in legal and technical mechanisms, and the establishment of many security centers to combat theses crimes, in addition to regional coordination in the framework of binary or collective to adress thèse cyber crimes.

شكر وعرفان

عملا بقول الرسول صلى الله عليه وسلم من لم يشكر الناس

و لم يشكر الله و أصالة عن أنفسنا نتوجّه بالشكر الجزيل إلى

" الدكتور البار أمين " على تفضله بالإشراف على هذا البحث

وعلى إعانته لنا وصبره وتفهّمه و فله كامل التقدير والعرفان

وتمنياتينا له بمزيد من العطاء

كما نتقدّم بالشكر الخالص إلى جميع أساتذة

قسم العلوم السياسية والعلاقات الدولية

بجامعة العربي التبسي تبسة

الإهداء

اهدي ثمرة جهدي وتعبي إلى من فطمني الموت منهما والدي العزيزان نسال الله لهما الرحمة والمغفرة.

إلى زوجتي الفاضلة حفظها الله.

إلى أبنائي وبناتي رعاهم الله:

سلسبيل، رقية، يوسف.

إلى جميع إخوتي وأخواتي سندي.

والى كل عزيز على قلبي.

عماد بلغيث

الإهداء

إلى ينبوع العطاء الذي زرع في نفسي الطموح والمثابرة والدي العزيز رحمه الله.

إلى نبع الحنان الذي لا ينضب أمي الغالية حفظها الله.

إلى من يحملون في عيونهم ذكريات طفولتي وشبابي إخوتي وأخواتي.

عبد المالك، العايش، سليمان.

وأختي "بية"

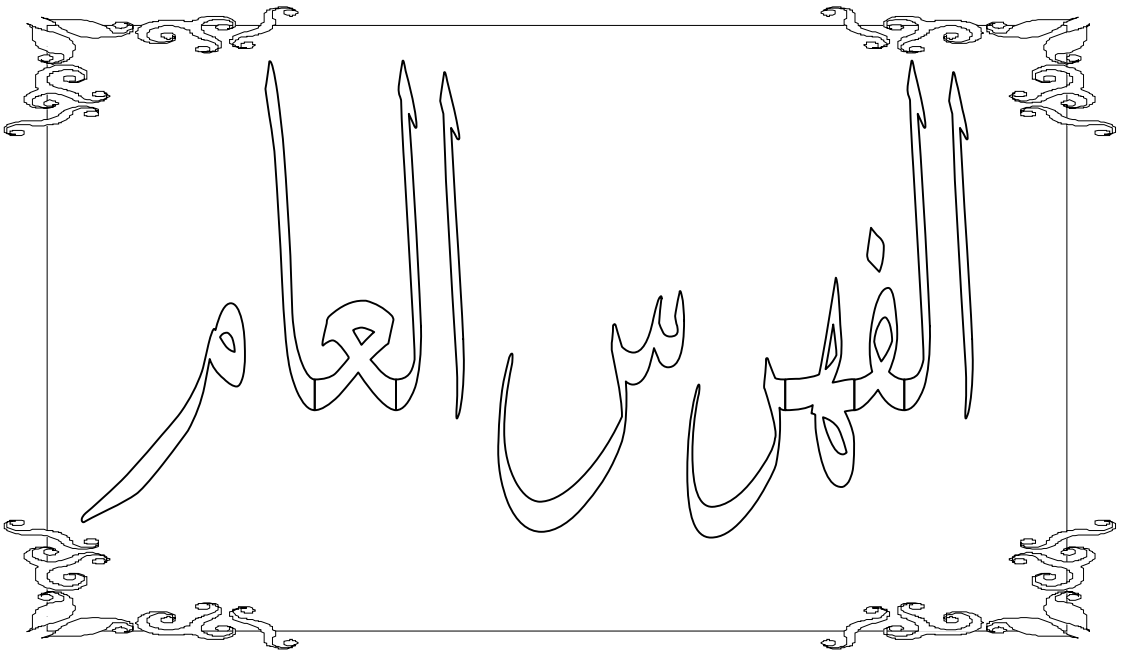
إلى من ضاقت السطور من ذكرهم فوسعهم قلبي أصدقائي.

إلى كل من قال لي "لا" فكان سببا في تحفيزي.

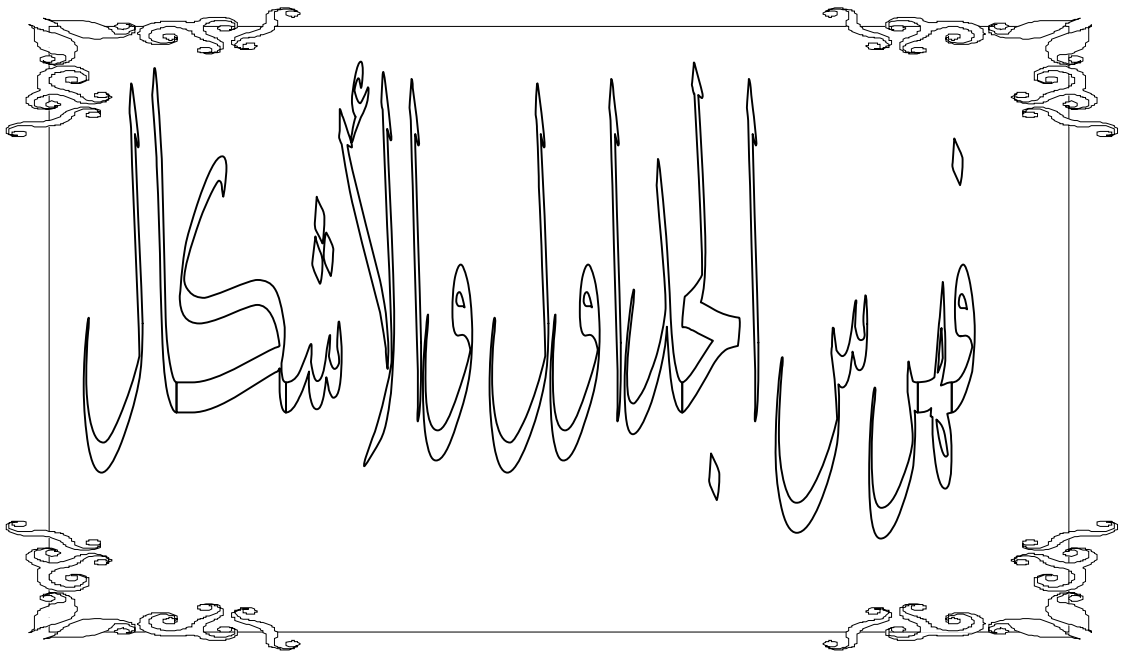
إلى كل من كان النجاح طريقه والتفوق هدفه والتّميُّز سبيله

إليكم جميعا الشكر والتقدير والاحترام.

قاسمي شعيب

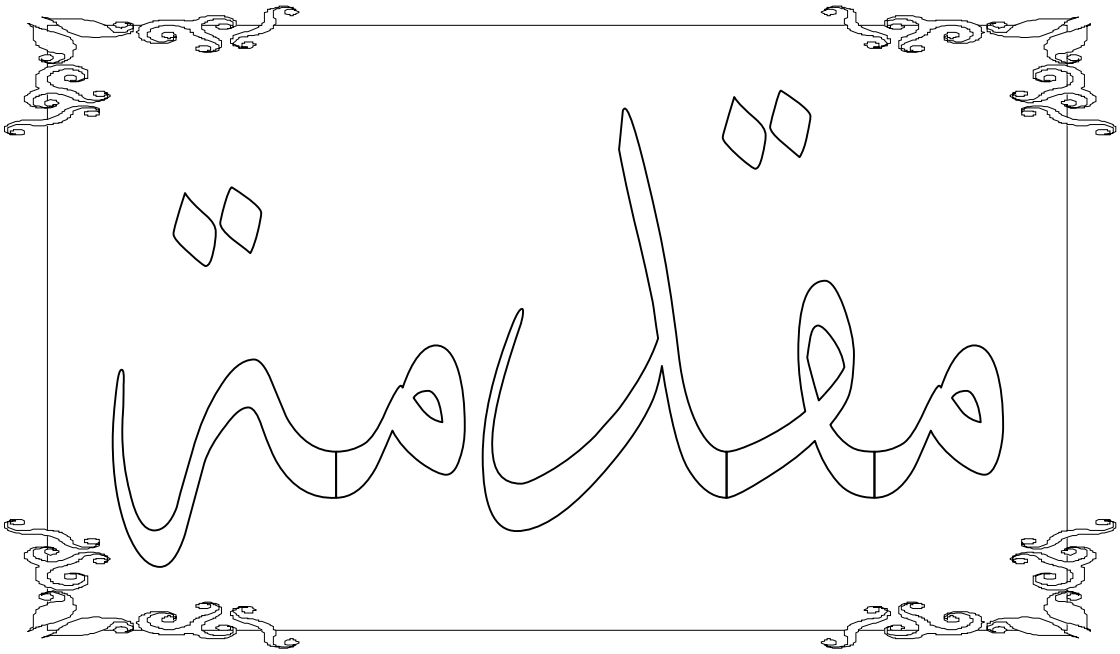

الفهرس العام

الفهرس العام


فهرس الجداول والأشكال

فهرس الجداول

فهرس الأشكال


مقدمة

مقدمة

يندرج موضوع بحثنا في سياق دراسة العلاقات الدولية عامة، ودراسة والدلراسات الاستراتيجية والامنية خاصة وبالتركيز على متغيرن هما الجرائم السيبرانية واستراتيجية مواجهتها.

عرفت العلاقات الدولية تطورا بارزا من حيث الفواعل والمواضيع المستخدمة في إدارة تفاعلاتها، وفي ظل هذه التطور الذي تزامن مع الثورة التكنولوجية والرقمية، اقتحمت شتى أنماط الحياة الإنسانية والتفاعلات الدولية ظهر نوع جديد من التهديدات المتمثلة في لجرائم السيبرانية، التي وجب على الدولة القومية التعامل معها وبالتالي محاولة مجابهتها، ومازاد تعقيد هذا النوع من التهديدات هو ذلك الترابط الذي فرضه هذا التعامل الكثيف في الفضاء الشبكي وحجم الخدمات المتوفر فيه، بالإضافة إلى ذلك الوضع الذي خلقه التطور التكنولوجي على مستوى البناءات الداخلية في الدولة بين السياسة الاقتصاد وقطاع التجارة والمال والثقافة وبالتالي فإن أي هجوم على قطاع من القطاعات من شأنه إحداث أضرار على أمن الدول، وبالتالي أصبحت الدول مجبرة على الاهتمام بالفضاء الإلكتروني كونه أضحى ساحة جديدة للتفاعلات الدولية.

ظهرت الجرائم السيبرانية بوصفها شكلا جديدا من أشكال التفاعلات الدولية وصورة جديدة من صور الحروب والتي اتسمت بمجموعة خصائص تجعلها مختلفة عن نظيرتها التقليدية، من حيث طبيعة الأنشطة العدائية والفواعل والتأثير في بنية الأمن العالمي.

وانطلاقا من هذا الشكل الجديد من التهديدات الذي تمثل في الجرائم السيبرانية، قامت الدول بمحاولة التصدي لهذه الجرائم عن طريق العديد من التشريعات القانونية التي تجر كل مستعمل لهذه الجرائم داخل الفضاء المعلوماتي كما وضع الدول العديد من الاستراتيجيات الاخرى لمواجهة هذه التهديدات، وكانت الهيئة العامة للامم المتحدة التي أصدرت قرار حول ضرورة نشر ثقافة الأمن السيبراني، وضرورة زيادة الوعي والمسؤولية لدى الدول بما يكفل ويضمن التعاون لمنع ورصد ومعالجة الحوادث السيبرانية، وبدأ اهتمام الدول بالتعاون واضحا من خلال مشاركتها في أعمال الجمعية العامة للأمم المتحدة التي ضم 193 دولة لمواجهة هذه الجرائم السيبرانية.

تعرضت الجزائر مثلها مثل باقي دول العالم الى تهديدات تمثلت في الجرائم السيبرانية مما شكل خطرا على امنها وجعلها عرضة الى الخطر، ما جعلها تقوم بالعديد من الاستراتيجيات لمواجهة هذه التهديدات، ومن

بين اليات المواجهة نجد الاليات الامنية متمثلة في مراقبة الفضاء السيبراني وردع التهديدات عن طريقه، بالاضافة الى وضع تشريعات قانونية لمواجهة مرتكبي هذه الجرائم السيبرانية.

❖ إشكالية الدراسة.

أضحى الفضاء الإلكتروني احد اهم الساحات الجديدة التي تدور فيها مختلف الصراعات ومازاد من تعقيد هذا النوع من الصراع، هو ذلك الترابط الذي كان نتيجة ظهور هذه الطفرة المعرفية في عصر المعلومات، ومع ازدياد درجة الجرائم السيبرانية في عدة مناطق من العالم، ، شكل أبرز ظواهر مشكلة البحث، ووفقا لذلك سارعت الدول لوضع استراتيجية لمواجهة هذه التهديدات سواء بشكل ثنائي او فردي، ومن بين هذه الدول نجد الجزائر.

وتنبع إشكالية الدراسة من العلاقة الوثيقة بين التهديات السيبرانية لذلك ستكون الاشكالية كالتالي:

الى أي مدى استطاعت الدول وضع استراتيجيات ناجحة في مكافحة الجرائم السيبرانية على ضوء حالة الجزائر؟

ويتفرع على هذا السؤال المركزي بعض الأسئلة الفرعية لتبسيط الإشكالية أكثر:

1/ ما هي الجرائم السيبرانية؟

2/ ما هي أبرز المخاطر الإلكترونية التي قد تؤثر على الأمن القومي للدول؟

3/ ماهي اهم الاستراتيجيات الدولية في مكافحة التهديدات السيبرانية؟

4/ هل أصبح الفضاء الإلكتروني ساحة جديدة للصراع الدولي؟

5/ كيف تواجه الجزائر الجرائم السيبرانية، وما هي أهم إستراتيجياتها للحد من هذه التهديدات؟

❖ فرضيات الدراسة.

نحاول من خلال موضوع **الإستراتيجيات الدولية في مكافحة الجريمة السيبرانية**، الإجابة على الإشكالية السابقة والأسئلة المتفرعة عنها، إرتأينا وضع الفرضيات التالية كإجابة مبدئية والتي نصوغها كما يلي:

1/ كلما زادت خطورة الهجمات السيبرانية التي تهدد امن الدول، كلما زادت الدول في وضع استراتيجيات جديدة لمكافحتها، ويبرز ذلك في الاستراتيجيات التي وضعتها الجزائر.

2/ هناك استجابة واسعة من طرف الجزائر لمواجهة التهديدات الإلكترونية الجديدة لحماية أمنها القومي سواء من خلال التشريع أو من خلال التعاون الدولي.

❖ اهمية الدراسة.

1/ الأهمية العلمية.

تظهر الأهمية العلمية للدراسة من خلال محاولة التعرض لظاهرة جديدة في العلاقات الدولية، والتي أصبحت تشغل حيزا كبيرا من الاهتمام لدى الدول، تتمثل هذه الظاهرة في الجريمة السيبرانية، كشكل من أشكال التفاعلات الدولية، من أجل ازالة الغموض المعرفي وتوضيح الحدود الفاصلة بينها وبين غيرها من المفاهيم المشابهة ومحاولة إخراجه من مدلوله التقني العلمي إلى مدلوله السياسي، باعتبار الحرب الإلكترونية تعبر عن واحدة من عمليات التفاعلات في السياسة الدولية.

2/ الأهمية العملية.

تكمن أهمية الموضوع في تزايد الجرائم السيبرانية في الفضاء الالكتروني، الذي يتوسع يوما بعد يوم وهذا نتيجة للمخاطر السلبية التي تشكلها هذه التهديدات على امن الدول، وبالتالي أصبح هذا النوع من الحروب أمرا واقعا وربما من أخطر أنواع الحروب لذلك تحاول جميع الدول وضع استراتيجيات لمكافحة هذه الظاهرة، ومن بين هذه الدول نجد الجزائر التي سارعت لوضع استراتيجيات سواء في اطار فردي او ثنائي لمواجهة الجرائم السيبرانية.

❖ مبررات اختيار الموضوع.

1/ المبررات الموضوعية.

محاولة تسليط الضوء على هذا النوع الجديد من الجرائم السيبرانية، ودورها في تهديد الأمن القومي للدول، فنظرا لتصاعد أهمية دور الفضاء الإلكتروني، أضحت التهديدات الإلكترونية حقيقة واقع ووجب على الدول التعامل معها بكل جدية ووضع استراتيجيات لمواجهته.

2/ المبررات الذاتية.

اهتمامات الباحث الشخصية بالتطورات التكنولوجية،بالاضافة الى فضول يدفعنا لمعرفة هذا النوع الجديد من الحروب الذي اصبح اليوم يه

دد جميع دول العالم، ومعرفة اهم الاستراتيجيات التي تقوم بها الدول لمواجهة هذا التهديد وبالاخص الجزائر.

❖ الدراسات السابقة.

نقصد بالأدبيات السابقة جميع البحوث والدراسات العلمية التي تتشابه مع البحث الراهن في جانب ما.

1/ Dan Craigen &Others, Defining Cybersecurity, Technology innovation Management Review (Octobre 2014)

تطرق الباحث في هذه الورقة الى تعريف الامن السيبراني، حيث وجد انه يوجد العديد من التعريفات لهذا المصطلح الحديث، وقام في هذه الورقة بتقديم تعريف جديد للامن السيبراني، وبدأ الورقة بالتهديدات التي ظهرت جراء الثورة المعلوماتية الكبيرة التي وصل لها المجتمع اليوم، ومع تزايد هذه الجرائم بدات الدول تبحث عن استراتيجيات لمواجهتها.

2/ محمد أمين الرومي، جرائم الكمبيورتر والانترنت، (الاسكندرية، دار المطبوعات الجامعية، 2004)

انطلق الكاتب من الثورة المعلوماتية الهائلة، وكيف انها اصبحت سلاح ذو حدين، فقد اصحب تحدث جرائم داخل الفضاء المعلوماتي او ما يطلق عليها بالجرائم السيبرانية، واصبحت هذه التهديدات تشكل خطرا كبيرا على الدول خاصة التي امنها المعلوماتي ضعيف، لذلك تم التفصيل في انواع هذه الجرائم لمواجهتها من طرف الدول.

3/ إلهام غازي، الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري، مجلة الجيش، مؤسسة المنشورات العسكرية العدد 630، (جانفي 2016)

فصلت الباحثة في الجانب القانوني لمحاربة الجرائم السيبرانية، حيث قامت الجزائر مثلها مثل بقية دول العالم بوضع العديد من التشريعات والقوانيين للحد من خطورة التهديدات الالكترونية، ومحاولة ردع الاطراف

التي تقوم بتهديد المصالح العليا للبلاد، وتعتبر هذه التشريعات احد اهم الاستراتيجيات التي تقوم بها الجزائر لمواجهة هذه الجرائم السيبرانية.

❖ حدود الدراسة.

1/ الحدود الزمنية.

تدور احداث هذه الدراسة حول الجريمة السيبرانية وكيف تحاول الدول وضع استراتيجيات لمواجهتها، لذلك فالفترة الزمنية للدراسة تنطلق منذ بداية الثورة الالكترونية وبالتحديد منذ زيادة التهديدات الالكترونية الى اليوم.

2/ الحدود المكانية.

مع انتشار التهديدات السيبرانية اصبحت الدول تضع استراتيجيات لمواجهتها واخترنا دراسة حالة الجزائر حيث تعتبر كنموذج.

3/ الحدود العلمية.

يندرج هذا البحث في إطار الدراسات الأكاديمية ضمن العلاقات الدولية، وبالتحديد ضمن مجال الدراسات الاستراتيجية والامنية، لذلك يسعى الباحث للتعمق في هذا الموضوع بشكل كبير.

❖ الإطار المنهجي للدراسة.

من أجل معالجة الموضوع استخدمنا في هذا البحث مجموعة من المقاربات المنهجية لما تفرضه أهداف ومستوى التحليل فقد استخدمنا:

1/ المنهج التاريخي.

هو عبارة عن إعادة للماضي بواسطة جمع الأدلة وتقويمها، وهو منهج علمي مرتبط بمختلف العلوم الأخرى حيث يساعد الباحث الاجتماعي خصوصا عند دراسته للتغيرات التي تطرا على البنى الاجتماعية وتطور النظم الاجتماعية، في التعرف على ماضي الظاهرة وتحليلها وتفسيرها علميا، في ضوء الزمان والمكان الذي حدثت فيه ومدى ارتباطها بظواهر أخرى ومدى تأثيرها في الظاهرة الحالية محل الدراسة ومن ثم الوصول إلى تعميمات.

وقد استخدمنا هذا المنهج في معرفة كيف ظهرت الهجمات السيبرانية وكيف تطور واصبحت تهدد امن الدول وحتى الكبرى منها.

2/ المنهج الوصفي.

يهدف هذا المنهج إلى تحقيق الفهم الدقيق والإحاطة بالأبعاد الواقعية للظواهر والموضوعات ومن هنا فالقواعد الأساسية التي يقوم عليها المنهج الوصفي تتمثل في تحديد الظواهر المراد بحثها، وجمع المعلومات الدقيقة عنها وفحصها ودراستها ومحاولة الإحاطة بعدد كبير من الأبعاد والعلاقات المرتبطة بالظاهرة من أجل الانتقال من مستوى الفهم البسيط إلى المستوى المركب، وما يرتبط بذلك من صياغة عدد من النتائج والتعميمات والتوصيات التي ترشد عملية البحث، وقد استخدمنا هذا المنهج في وصف ظاهرة الجريمة السيبرانية.

3/ منهج دراسة الحالة.

وهو منهج يهدف للوصول إلى معلومات شاملة عن الحالة المدروسة، وذلك بالاهتمام بمختلف جوانبها وكذا مختلف العوامل المؤثرة فيها، حيث يهدف للتعمق في ظاهرة معينة بهدف تثبيت الفهم، بناءا على كافة العوامل المؤثرة في تلك الحالة، من خلال البحث في موضوعنا استخدمنا هذا المنهج لدراسة حالة الجزئر التي ننتمي اليها بومعرفة اهم الاستراتيجيات التي تقوم بها لمواجهة التهديدات السيبرانية، وما هي اهم التشريعات التي قامت بها للتصدي لهذه الجرائم.

❖ تبرير خطة البحث.

للإجابة على هذه الإشكالية المركزية والأسئلة الفرعية للدراسة ولاختبار مدى صحة الفرضيات المقترحة ستتم دراسة الموضوع باعتماد خطة مكونة من ثلاثة فصول:

1/ نتطرق في **الفصل الأول** المعنون **الإطار المفاهيمي والنظري للدراسة**، أين قسم إلى ثلاثة مباحث خصصنا **المبحث الأول** للبحث حول **الضبط المفاهيمي للإستراتيجية** للتعمق في هذا الموضوع المرتبط بالاستراتيجية أما بالنسبة **للمبحث الثاني مفاهيم أساسية حول الجريمة السيبرانية**، وسنفصل فيها بشكل كبير من ذكر لأهم تعريفاتها وما هي اهم المفاهيم المشابهة لها، أما **المبحث الثالث** فيلقي الضوء على **مفاهيم أساسية حول الأمن السيبراني**، وكيف ان التهديدات السيبرانية جعلت الدول تسعى لتامين نفسها، اما **المبحث الرابع** فهو عبارة عن **اطار نظري للدراسة.**

2/ أما **الفصل الثاني** والذي عنوانه: **الجريمة السيبرانية في الاستراتيجيات الدولية**، قسم كذلك إلى ثلاثة مباحث وهي كالأتي: **المبحث الأول** وتطرقنا فيه إلى **الجريمة السيبرانية في القانون الدولي** لنحدد اهم القوانين للتحكم في هذه الظاهر الجديدة، كما عنون **المبحث الثاني: مكافحة الجريمة السيبرانية في الإستراتيجية الأمريكية والروسية**، وسنحاول التطرق فيه إلى كيف كافحا اكبر دولتان هذه الظاهرة، أما **المبحث الثالث: واقع الجريمة السيبرانية في الدول العربية وسبل مكافحتها** حيث سنقوم بدراسة بعض الدول العربية وكيف يتعاملون مع الهجمات السيبرانية.

3/ أما بالنسبة **للفصل الثالث: إستراتيجية الجزائر في مكافحة الجريمة السيبرانية**، وقد قسم إلى ثلاثة مباحث كذلك، **المبحث الأول: واقع الجريمة السيبرانية في الجزائر** ، وسنركز فيه على هذه الجرائم وكيف تكون عبر التجسس والقرصنة، أما **المبحث الثاني: الآليات المحلية لمواجهة الجرائم السيبرانية** فسنركز على الايات التشريعية واهم استراتيجيات المواجهة، **والمبحث الثالث والأخير: التنسيق الإقليمي لمكافحة الجريمة السيبرانية** فسنركز على الاليات الاقليمية وكيف سيكون مستقل الجريمة السيبرانية في الجزائر.

4/ أما **الخاتمة** فسنعرض فيها نتائج البحث، حيث سنحاول الإجابة على التساؤلات المكونة للإشكالية المطروحة في بداية الدراسة، وسبر مدى صدق الفرضيات التي قمنا باقتراحها.

الفصل الأول:

الإطار المفاهيمي والنظري للدراسة

تمهيد:

ينبغي لتناول أي بحث علمي وأكاديمي البدء في ضبط المفاهيم الأساسية لأن هذه العملية تسمح للباحث باستعاب المعنى الحقيقي للمفاهيم والمصطلحات المراد دراستها وتوضيحها بالشكل الذي يؤدي إلى فك الغموض والتعقيد، فكل مصطلح يحتاج إلى تقديم العديد من التعاريف لفهمه واستعابه ناهيك عن التطرق عن السياق التاريخي للموضوع محل الدراسة، إضافة إلى التطرق إلى المقاربات النظرية التي يتم تفسير أي موضوع من خلالها.

ويعتبر حقل العلاقات الدولية غني بالمفاهيم والمصطلحات الدالة على الظواهر، لذا سيتناول هذا الفصل الذي تم تقسيمه إلى أربعة مباحث مايلي :

- **المبحث الاول: مفاهيم أساسية حول الإستراتيجية؛**
- **المبحث الثاني: مفاهيم أساسية حول الجريمة السيبرانية.**
- **المبحث الثالث: مفاهيم أساسية حول الأمن السيبراني.**
- **المبحث الرابع: الإطار النظري للدراسة.**

المبحث الأول: الضبط المفاهيمي للإستراتيجية.

تحظى الإستراتيجية كموضوع باهتمام متزايد وواسع النطاق من قبل المفكرين والمثقفين والأكاديميين، فضلا عن اهتمام النخب القيادية، والمؤسسات الرسمية وغير الرسمية لما لها من تماس شديد وعلاقة وثيقة بالعديد من مجريات السياسة الدولية، فكلمة إستراتيجية تستخدم اليوم في مختلف ميادين الحياة وفي أنشطة وفعاليات عديدة حتى أصبح من الصعوبة بمكان تحديد ما المقصود بها على وجه الخصوص أوالتحكم في المصطلح من قبل الباحثين، لذا وجب التوقف عند مفهوم الإستراتيجية وبدايات الدراسة العلمية لهذا المصطلح والتطرق إلى بعض المفاهيم ذات الصلة. [1]

المطلب الأول: تعريف الإستراتيجية.

يمكن تناول أهم التعاريف التي تناولت موضوع الاستراتيجية وفقا لما يلي:

1- التعريف اللغوي.

الإستراتيجية (Strategy) مشتقة أصلا من الكلمة اليونانية (Strato) بمعنى جيش أوحشد، ومن مشتقات هذه الكلمة (Stratego) والتي تعني فن القيادة، ومن مشتقاتها أيضا (Stratagem) والتي تعني الخدعة الحربية التي تستخدم في مواجهة العدو. [2]

وانطلاقا من التحليل الكلاسيكي للمصطلحات نجد أن مفهوم أومصطلح الإستراتيجية يوجد في مختلف اللغات الأوروبية أواللغات الإغريقية اللاتينية.

ففي الألمانية نجد (Strategie) وفي الروسية (Strategya) وفي الهنغارية (Strategi)، وعندما نقول (Stratos agein) فمصطلح الإستراتيجية ذاته مقسم إلى جزئين ويعني: "الجيش الذي ندفع به إلى الأمام" وبوصل طرفي المصطلح (Stratos) و(agein) نحصل على (Strategos) وهذا يعني الجنرال وفعل (Stratególô) يعني قاد أوأمر. [3]

ويتضح من خلال ما تقدم ذكره في أصل كلمة إستراتيجية أنها قد ارتبطت بالجانب العسكري وبفن قيادة الجيوش وبفن الحرب وعلمها، لأن الإستراتيجية في تلك الفترة استحوذت على اهتمام القادة العسكريين، ثم انطلقت الاستراتيجية لباقي المجالات.

1- عبد القادر محمد فهمي،" **المدخل في دراسة الإستراتيجية**"، (عمان: دار مجدلاوي للنشر والتوزيع، 2009)، ص 07.
2- **المرجع نفسه**، ص 17.
3- صلاح نيوف، " **مدخل إلى الفكر الإستراتيجي**"، (الدنمارك: الأكاديمية العربية المفتوحة، د س ن)، ص 09.

2- التعريف الإصطلاحي.

يتفق معظم المفكرين والباحثين على أن الإستراتيجية هي مفهوم مثير للجدل في العلوم السياسية والفكر الإستراتيجي، ذلك أن هذا المصطلح ارتبط في البداية بالجانب العسكري وفنون القتال ونتيجة لتطور الدراسات والانفتاح على العلوم الأخرى أضحى هذا المفهوم واسع الانتشار، ومن بين ما قدم من قبل المفكرين والفلاسفة في تعريف الإستراتيجية نذكر ما يلي:

يقول المفكر الإستراتيجي الصيني "سان تزو" "Son Zi": "أن الأكثر تميزا من القادة بيننا هم هؤلاء الأكثر حكمة والأكثر استشرافا ورؤية".[1]

2-1- تعاريف المدرسة الغربية لمصطلح الإستراتيجية.

- يعرف المفكر الألماني "كلاوزفيتش" "Clausewitz" الإستراتيجية بأنها: "فن استخدام الاشتباك كوسيلة للوصول إلى غايات الحرب، أوإلى الأهداف التي شنت الحرب من أجلها".[2]

والملاحظ أن هذا التعريف قد اعتبر الإستراتيجية وسيلة لتحقيق أهداف العمل الحربي وغاياته من خلال وضع الخطط وتوفير الإمكانات للوصول لهذه الأهداف.

- أما "ليدل هارت" فقد عرف الإستراتيجية بكونها: "فن توزيع واستخدام الوسائط العسكرية لتحقيق هدف السياسة".[3]

هنا "ليدل هارت" يرى بأن الإستراتيجية هي استخدام وتوظيف الوسيلة العسكرية لتحقيق الأهداف السياسية التي تشن الحرب من أجلها وعلى فن استغلال هذه الوسائل.

وما يؤخذ على تعريف كل من "كلاوزفيتش" و"ليدل هارت" أنهما ربطا الهدف السياسي بالهدف الإستراتيجي للنشاط العسكري الميداني (أي الحرب)، أن هناك حالات وإن كانت استثنائية لا يتحقق فيها الهدف السياسي بمعناه الإستراتيجي عندما تكون الحرب وسيلة لتحقيقه.[4]

اذن فالمدرسة الغربية ركزت على الجانب الحربي، وكيف ان الاستراتيجيات الناجحة هي التي تحقق الاهداف الناجحة، ومنه تحقيق الاهدف السياسية.

1- صلاح نيوف، **المرجع السابق**، ص 06.

2- عبد القادر محمد فهمي، **المرجع السابق**، ص 13.

3- **المكان نفسه**.

4- **المرجع نفسه**، ص 14.

2 – 2– المدرسة الشرقية.

– يرى "لينين" في تعريفه أن: "الإستراتيجية الصحيحة هي التي تتضمن تأخير العمليات إلى الوقت الذي يسمح فيه الانهيار المعنوي للخصم للضربة المميتة بأن تكون سهلة وممكنة".[1]

– أما "ماوت سيتونغ" فيعرف الإستراتيجية بـــأنها: "دراسة قوانين الوضع الكلي للحرب".[2]

والملاحظ أن هاذين التعريفين المقدمين لم يخرجا الإستراتيجية عن المجال العسكري والحرب، غير أن "لينين" ركز على الجانب النفسي للخصم من خلال إرباكه وانتظار الوقت المناسب للعمليات والتي تكون فيها الضربة مميتة التي تكون سهلة وممكنة.

بينما ربطها "ماوت سيتونغ" بالحرب ودراسة قوانينها.

2– 3– المدرسة العربية.

تعريف المدرسة المصرية: "هي أعلى مجال في فن الحرب وتدرس طبيعة وتخطيط وإعداد وإدارة الصراع المسلح، وهي أسلوب علمي نظري وعملي يبحث في مسائل إعداد القوات المسلحة للدولة واستخدامها في الحرب، معتمدا على أسس السياسة العسكرية كما أنها تشمل نشاط القيادة العسكرية العليا بهدف تحقيق المهام الإستراتيجية للصراع المسلح لهزيمة العدو".[3]

ويتضح أن تعريف المدرسة العربية للإستراتيجية لا يبتعد عن الإطار العسكري لخدمة أهداف السياسة ولعل ما يؤخذ على هذه التعريفات أنها اعتبرت الحرب الأداة الوحيدة لتحقيق الهدف الإستراتيجي للدولة.

ولعل ارتباط الإستراتيجية بالمجال العسكري لدى منظري الفكر الإستراتيجي في القرنين 18م و19م له ما يبرره فالحرب كانت تعني زوال الدول أوبقائها، كما أن الشؤون السياسية والعسكرية كانت بيد شخص واحد وهو الملك وتمركز القرار الإستراتيجي في يد القادة العسكريين.

غير أن الوقت الحالي عرف تعددا لمجالات الإستراتيجية و لم تعد مرتبطة بالنشاط العسكري للدولة، بل تعدت ذلك لتشمل الجانب السياسي والاقتصادي والاجتماعي والأمني وذلك بفضل التطورات التي مر بها النظام الدولي، حيث باتت متطلبات بناء الدولة الحديثة لا تستند على متانة قاعدتها العسكرية فقط بل على قوة بناء قاعدتها الاقتصادية والتكنولوجية والاجتماعية أيضا.

1– عبد القادر محمد فهمي، **المرجع السابق**، ص 24.

2– **المكان نفسه.**

3– **المكان نفسه.**

بمعنى أن الدول أخذت ترسم إستراتيجياتها لا على أساس افتراضات الخيار العسكري حيث تقتضي ضرورة الحرب، وإنما في ضوء احتياجات ومتطلبات الواقع العملي وبمختلف معطياته السياسية والاقتصادية والاجتماعية والعسكرية وبشكل تؤلف فيه هذه الإستراتيجية كُلاًّ لا يتجزأ.[1]

وتتنوع الوسائل والأدوات بتنوع الأهداف والإستراتيجية في حد ذاتها، ذلك أن القدرة على تعبئة الموارد والإمكانيات اللازمة لتحقيق أهداف الإستراتيجية التي حددتها السياسة هوما يميز الإستراتيجية عن غيرها.

ويمكن تقسيم وسائل الإستراتيجية إلى مادية وتتمثل في الوسائل الجغرافية والاقتصادية والعسكرية وأخرى معنوية وتتضمن الثقافية والاجتماعية، وهنا يأتي دور صانع الإستراتيجية في التكييف والموازنة بين هذه الإمكانيات والأهداف المرجوة واحتواء ثغرات التفاوت الكمي والنوعي وانعكاسها على نسبة الإنجاز ومستواه.

وبالتالي وجب توفر مجموعة من الشروط لصياغة إستراتيجية شاملة وفعالة:

- وضوح الأهداف وتكاملها.
- واقعية الأهداف وتكاملها.
- الاختيار العقلاني بين الأهداف والوسائل.
- الاستمرارية: فأهداف الدولة لا نهاية لها لذا لابد أن تتصف عملية التخطيط بالاستمرارية.
- المرونة لمواجهة المواقف غير المحتملة أوغير المتوقعة في الظروف الاعتيادية مثل الحرب.
- الابتكار والاعتماد على الذات لأن الفكر الإستراتيجي يعتبر قمة الفكر الإبداعي.[2]

وكخلاصة فالحديث عن أي إستراتيجية يقودنا إلى أن:

- الإستراتيجية تعدت الجانب العسكري لتشمل مجالات أخرى.
- الإستراتيجية هي الموازنة بين الإمكانات المتاحة والأهداف المراد تحقيقها.
- الإستراتيجية هي علاقة بين الحاضر والماضي وتحديد المناهج والأدوات على ضوء رؤية مستقبلية للأهداف ونظرة فلسفية للتطور.[3]

1- خليل حسين، وحسين عبيد، "**الإستراتيجيا**"، (بيروت: منشورات الحلبي الحقوقية، 2013)، ص 30.

2- علي محمد إبراهيم كردي، "**المفهوم العسكري للإستراتيجية والتطور التاريخي**"، تم تصفح الموقع يوم : 15 فيفري 2018. الرابط: Renanaonline.com/users/alihordi/posts/352158

3- عبد القادر محمد فهمي، **المرجع السابق**، ص 11.

3- التعريف الإجرائي.

ويمكن تعريف الإستراتيجية من الناحية الإجرائية على أنها القدرة على الموازنة بين الإمكانات المتاحة للدولة وبين الأهداف المراد تحقيقها على المدى البعيد وفقا لمبادئ وقواعد معينة وتتسم بالاستمرارية والمرونة.

المطلب الثاني: التطور التاريخي للإستراتيجية.

يتفق المفكرون والباحثون الإستراتيجيون على أن الإستراتيجية مفهوم ليس حديث النشأة ويعود تأصيله التاريخي إلى قرون ماضية حيث مر بعدة مراحل، وهو ما ساهم في انتقال الإستراتيجية من الجانب العسكري وبفن الحرب وعلمها إلى مجالات أخرى، نتيجة التطورات التي شهدتها المجتمعات البشرية ويمكن إبراز هذه المراحل فيما يلي:

1- الفكر الإستراتيجي الآسيوي القديم – نموذج الفكر الصيني-

كان للكتابة مكانة رفيعة في الصين وقد كرس الكثير منها للأمور العسكرية حيث ظهر العديد من أعلام الفكر الإستراتيجي الصيني من أهمهم:

يعتبر الإستراتيجي الصيني "سان تزو" "Sun Tzu" في مؤلفه "فن الحرب" والذي يعتبر أقدم ما ألف في هذا المجال، حيث عرف الإستراتيجية على أنها: "يمكن مقارنة أي جيش بالماء فالماء يترك المرتفعات ويغزو الأماكن المنخفضة، وهكذا الجيش يتفادى القوة ويهاجم الضعف السيل ينتظم حسب تضاريس الأرض والانتصار يحرز بالتلاؤم مع وضعية العدو".[1]

ثم الجنرال "Caocao" في القرن السابع والثامن قبل الميلاد، إلى جانب "صان بن" "Sun Bin" أشهر أعماله "الإتفاقية العسكرية"، حيث يغلب الطابع العملي على رؤيته الإستراتيجية تحدث عن الدعم اللوجيستي وتأثير ذلك في زيادة فعالية إطالة الحملات العسكرية و"هي يانش" "Hi yanshi" أهم مؤلفاته الإستراتيجية:

كتاب "معلم الفروسية" "Simo-Fa": نص مختصر ظهر في القرن الرابع أوالخامس قبل الميلاد يتحدث عن إدارة الجيوش، وضرورة أن تكون الحرب عادلة.

كتاب "الإستراتيجيات الثلاث" "Sen Lue": يحلل في سيطرة الحكومة والأبعاد السياسية للإستراتيجية.[2]

1- نسيمة بوطويل، **"الإستراتيجية الأمنية الأمريكية في منطقة شمال شرق آسيا: دراسة لمرحلة ما بعد الحرب الباردة"**، رسالة مقدمة لنيل شهادة دكتوراه العلوم في العلوم السياسية، تخصص علاقات دولية، (جامعة: الحاج لخضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية والعلاقات الدولية، 2010)، ص 22.

2- **المرجع نفسه**، ص 24.

تعتبر مؤلفات هؤلاء المفكرين الإستراتيجيين الصينيين من ركائز الفكر الإستراتيجي الغربي رغم أن الغربيين تعاملوا دائما مع الفكر الصيني على أنه حكمة أكثر مما هو علم، ومع هذا ترجم كتاب "فن الحرب" لـــ"سان تزو" إلى كل اللغات الأوروبية إبتداء من الروسية سنة 1889 إلى الإنجليزية بداية القرن العشرين.[1]

2- الفكر الإستراتيجي الغربي القديم

يمكن الحديث عن الإستراتيجية في الفكر الغربي القديم عند كل من اليونانيين والرومان على اعتبار أن

2-1- الفكر الإستراتيجي اليوناني

امتلك اليونانيون العديد من التحليلات التكتيكية والإستراتيجية في عصرهم القديم، فكان الإسبارطيون أول من كتب في الصراعات وإستراتيجية خوضها وكانوا أول من علموا هذه الأفكار من خلال معلمين عسكريين سموهم بالتكتيكيين.

يعتبر كل من "إني" و"أندرسونس" أقدم من كتب في الإستراتيجية خلال العهد اليوناني حيث اعتمدوا كثيرا على الممارسات العملية أكثر من التنظير، رغم وجود هذا الأخير في كتابات "إكسنوفون" حيث ظهر التفكير التنظيري في مؤلفه "تحليل الفروسية" فكان أول من نظر في التكتيك.[2]

2-2- الفكر الإستراتيجي الروماني

كان لدى الرومان فكرا عسكريا أصيلا وجديدا وصل إلى عمق الأشياء والأمور الإستراتيجية وذلك حسب النصوص الرومانية، ودلالة ذلك التفوق التكتيكي الروماني من خلال قرون متتالية مما أوحى بوجود بنية تنظيمية دقيقة للعقيدة العسكرية، فيؤكد على ذلك "بوليب" قائلا: "المرشحون للوظائف العامة كان عليهم المشاركة في عشر حملات عسكرية قبل اختيارهم من قبل المواطنين".[3]

أشهر مؤلفات الرومان في المجال الإستراتيجي جاء بها كل من "كاتوا"،"بوليب" و"فرونتينوس" في مؤلفه "تعليقات عسكرية عند هوميروس".

اذن فالفكر الاستراتيجي الروماني كان ناجحا بشكل كبير، وتجسد ذلك من خلال النجاحات الهائلة التي حققها وتوسع الامبراطورية الرومانية لتشمل جزء كبير من الارض، واصبحت تعتبر اكبر مملكة على مدار فترة زمنية طويلة وذلك لنجاح استراتيجيتها.

1- نسيمة بوطويل، **المرجع السابق**، ص 24.

2- **المكان نفسه.**

3- **المرجع نفسه**، ص 25.

2-3- الفكر الإستراتيجي العربي الإسلامي.

معظم الكتابات والمؤلفات التي سبقت ابن خلدون والتي تتعلق بالفكر الإستراتيجي فقدت بعد تعرض الدول العربية للغزو المتكرر على يد المغول، لذلك تعتبر مؤلفات ابن خلدون عن الحروب والطرق المستخدمة في المعارك من قبل مختلف الشعوب أول ما ظهر في التراث العربي في هذا المجال.

عرف القرن 13م حتى القرن 16م العديد من المؤلفات التي تقترب من التكتيك والإستراتيجية من بينها "تعليمات رسمية للنخبة العسكرية"، كتاب "الفن العسكري" كتبه محمد بن عبد الله، كتاب "الفن العسكري والفروسية" كتبه علي بن عبد الشامان بن هزيل.[1]

الكتاب والسنة لم يحددا شيئا في هذا الموضوع، لكن الكُتَّاب الغربيون يرون أن وجود رسالة والرغبة في نشرها يساعد على تحديد مهام الإستراتيجية والأهداف العامة للأمة.

2-4- الفكر الإستراتيجي الأوروبي الحديث.

يعتبر العصر الحديث أخصب ما أُلِّف وكُتب في مجال الإستراتيجية، حيث صدر العديد من المؤلفات التي دفعت بهذا المجال المعرفي وتطوره.

فالفكر الإستراتيجي العسكري بدأ الإعلان عن نفسه بشكل واضح في إسبانيا مع كتاب " libro de la guerra" (كتاب الحرب) حوالي سنة 1420م، وقد كتبه الماركيز "vellena" وكتاب "تحليل الانتصار العسكري" حوالي سنة 1459م وقد ألفه "Alfonso Hernandez".

في فرنسا نجد العديد من الكُتّاب مثل "Robert de Balsac" وكتابه "مبادئ الصراعات النبيلة" في سنة 1502م، وفي انجلترا في نفس الفترة الزمنية نجد كتاب "تحليل لفن الحرب" وضعه "Béraud Stuart" وفي ألمانيا كتاب "الحرب" لمؤلفه "phlippe von Seldeneck" نحو نهاية القرن الخامس عشر وفي إيطاليا نجد كتاب "Semedeus liber tertuis de re militaire" سنة 1438م لمؤلفه "Catone Secco" "ميكيافلي" التكتيكي والإستراتيجي الذي ألّف الكتاب الأكثر شهرة في القرن السادس عشر ويحمل عنوان "فن الحرب" وفي الواقع هوكتابه الوحيد الذي نشر أثناء حياته، الكتابات العسكرية عند "ميكيافللي" هي بشكل أساسي كتابات سلبية أونقد للمؤسسات العسكرية التي كانت سائدة في عصره.[2]

1- نسيمة بوطويل، **المرجع السابق**، ص 24.

2- صلاح نيوف، **المرجع السابق**، ص 42.

والملاحظ هنا أن هذه الفترة كانت خصبة بالمؤلفات والكتابات حول الإستراتيجية وفن الحرب والتكتيك لأنها تأثرت بالحروب التي شهدتها تلك الفترة خاصة في القارة الأوروبية.

المطلب الثالث: الإستراتيجية وعلاقتها بالمفاهيم ذات الصلة.

هناك العديد من المصطلحات التي تتداخل مع مفهوم الإستراتيجية، لذلك تقتضي الضرورة العلمية التمييز بين مفهوم الإستراتيجية وبين هذه المفاهيم وتحديد العلاقة بينهم ويمكن إبراز أهم هذه المفاهيم فيما يلي:

1- التكتيك

كغيره من المفاهيم عرف التكتيك محاولات عدة لتعريفه، فهويعرف على أنه: "مجمل العمليات التي تقوم بها الدولة للوصول إلى الهدف الإستراتيجي، وعندما تؤدي الحرب إلى معركة حقيقية فإن الاستعدادات التي تتخذ لإعداد مثل هذا العمل وتنفيذه يشكل ما يسمى تكتيكا".[1]

ويقول "HAMLEY": "إن مسرح الحرب هو مجال الإستراتيجية أما ساحة المعركة فمجال التكتيك".[2]

ولذلك يمكن القول أن التكتيك هوتنفيذ الهدف الذي تحدده الإستراتيجية، وأن التكتيك هوجزء من الإستراتيجية بينما الإستراتيجية هي خطة شاملة وعامة.

ويمكن تحديد أوجه الاختلاف بين التكتيك والإستراتيجية فيما يلي:

- على مستوى الأهداف: تكون أهداف الإستراتيجية ثابتة وغير قابلة للتجزئة أوالمساومة، بينما تكون أهداف التكتيك متنوعة.

- على مستوى الحركات: قد تتضاعف الحركة في الإستراتيجية وقد تنعدم لثبوت الأهداف بينما في التكتيك تكون متعددة.[3]

2- الاستشرافالعمل دون هدف لا معنى له والاستباق يولد العمل، هكذا إذا يمكن أن يقترن الاستشراف بالإستراتيجية ويمثل الاستشراف استباقا يستعد للفعل (PREACTIVE) ويستحدث الفعل (PROACTIVE) وينير العمل الحاضر على ضوء المستقبلات الممكنة والمأمولة.[4]

1- حنان لبدي، **"التحولات الدولية الراهنة وتأثيرها على الإستراتيجية الأمنية في منطقة الساحل الإفريقي"**، مذكرة مقدمة لنيل شهادة الماجستير (جامعة: محمد خيضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية والعلاقات الدولية، 2015)، ص 22.

2- **المرجع نفسه**، ص 17.

3- عبد القادر محمد فهمي، **مرجع سابق**، ص 44.

4- ميشال غودي، وقيس الهمامي، **"الاستشراف الإستراتيجي والمشاكل والمناهج"**، مجلة ليبسور، العدد6، (2005)، ص 05.

الاستشراف من المفاهيم الحديثة ويعتبر أول ظهور له كمصطلح سنة 1953م من قبل "غاستون بيرجي" ليحل محل مفهوم علم المستقبل، فقد كان "غاستون بيرجي" "Gaston Berger" يقول: "إننا مع الاستشراف لابد أن ننظر نظرا بعيدا وفسيحا وعميقا وأن نفكر في الإنسان وأن نجازف"، ويضيف أن للاستشراف ثلاث خاصيات هي أن ننظر بطريقة مختلفة (أن نحضِر الأفكار المسبقة)، أن ننظر معا (التملك) وأن نستعمل مناهج صارمة.[1]

فالإستراتيجية تتحدث عن بعد النظر والتجديد والاستشراف يتحدث على تهيئة ظروف الفعل وعن استحداث الفعل، فكيف يمكن أن تتخيل فعل إستراتيجي دون أن يكون لنا بعد النظر وسعته وعمقه حسب "غاستون بيرجي" وبالتالي فالإستراتيجية تستدعي الاستشراف ولو لمجرد توضيح الخيارات التي تلزم المستقبل.

وخلاصة القول أن الغاية من الإستراتيجية هوتحقيق الأهداف التي تحددها السياسة باستخدام الوسائل والإمكانات التي تمكنها من تحقيقها فقد تكون هذه الإستراتيجية:

– **هجومية:** وهي قدرة الدولة على فرض إرادتها على دولة أخرى باستخدام الوسائل المتاحة لإيقاع التأثير وفرض الإرادة على الخصوم لتحقيق أهداف ذات طبيعة تكاد تكون عدائية، وذلك عبر سلوكيات متعددة منها امتلاك القدرات العسكرية والاقتصادية والتكنولوجية والثقافية المتفوقة.

ويكون هدف الدولة إخضاع الخصوم بذلك تغلب على هذه الإستراتيجية سمة العدوان، وتنطوي على مزايا منها أنها تمتلك عنصر المبادئة وحرية اختيار وقت الحركة وأدائها ونقل الحركة إلى ساحة الخصوم فضلا عن أنها تكسب الدولة النفوذ والمكانة.[2]

– **دفاعية:** عند الحديث عن الإستراتيجية الدفاعية يتبادر إلى الأذهان تنظيم القوات المسلحة وأسلحتها وأساليب قتالها، ولكن الدفاع عن الدولة لا ينحصر في الشق العسكري والقتالي فقط فلمؤسسات الدولة كافة دور فيه إذ لكل منها دور أساسي في إعداد الوسائل وتحفيز المجتمع وتعبئة القوى الداخلية والخارجية لمساندة الجهد الدفاعي.[3]

فالإستراتيجية الدفاعية تتسم بشمولها جميع مؤسسات الدولة ومواردها لتتمكن من العمل ضمن آليات متكاملة تعتمد على مركزية القرار ولا مركزية التنفيذ.

1- ميشال غودي، وقيس الهمامي ، **المرجع السابق**، ص 06.

2- سامر مؤيد، **"الإستراتيجية من منظور وظيفي إجرائي"**، تم تصفح الموقع يوم : 17 فيفري 2018. الرابط: Fcdrs.com/mag/issue-6-2.html

3- ميشال عون، **"دراسة موجزة عن الإستراتيجية"**، (الرابية، 2008)، ص ص 02-05.

المبحث الثاني: مفاهيم أساسية حول الجريمة السيبرانية

إن الثغرات ونقاط التعرض في التكنولوجيا الرقمية تجتمع معا لتحقيق بيئة من عدم الأمن فتطور شبكة الانترنت واكبها التطور في أشكال وأساليب الجرائم في الفضاء السيبراني، إذ من الممكن للتكنولوجيا الجديدة تسهيل جميع أنواع التهديدات السيبرانية والتي يمكن الإشارة إليها وإبرازها فيما يلي:

المطلب الأول: مفهوم الجريمة السيبرانية

تعتبر الجريمة السيبرانية من بين الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها الذي ارتبط بتقنية المعلومات، فقد أُصطلح على تسميتها في البداية بإساءة إستخدام الكمبيوتر ثم احتيال الكمبيوتر، فالجريمة المعلوماتية ثم جرائم الكمبيوتر والجريمة المرتبطة بالكمبيوتر ثم جرائم التقنية العالية إلى جرائم الهاكر، فجرائم الانترنت وأخيرا السايبر كرايم.

وتُعرف الجريمة الإلكترونية بأنها: "مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أوأجهزة إلكترونية أوشبكات الانترنت أوتبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أوالتحقيق فيها ومقاضاة فاعليها".[1]

وقد اتجه جانب كبير من الفقهاء إلى اعتماد التعريف الذي تبنته منظمة التعاون الإقتصادي والتنمية للجريمة المعلوماتية في إجتماع باريس سنة 1983م على أنها: "كل سلوك غير مشروع أوغير أخلاقي أوغير مصرح به، يتعلق بالمعالجة الآلية للبيانات أونقلها".[2]

ويمكن تعريف الجريمة الإلكترونية بأنها: "كل أشكال السلوك غير المشروع والمتعمد الذي يرتكب باستخدام الحاسب الآلي المرتبط بالانترنت والتي تمس به أوبمحتوياته أوبالعمليات التي تتم بواسطته بغرض إلحاق الضرر بالضحية أوالكسب المادي أوغير ذلك من الأغراض من طرف أفراد على دراية كاملة بتقنيات التكنولوجيا المعلوماتية وأسرارها".[3]

اذن مع التطور الهائل في الجانب المعلوماتي والرقمي ظهرت كذلك تهديدات جديدة ضمن هذا المجال من بينها الجرائم السيبرانية التي تكون داخل عالم المعلومات ولا تؤدي خسائر بشرية بل خسائر مادية ومن نوع اخر، لذلك تحاول الدول مواجهتها،

1- ياسمينة بونعارة، **"الجريمة الإلكترونية"**، (جامعة: الأمير عبد القادر للعلوم الإسلامية، د س ن)، ص 03.

2- **المرجع نفسه**، ص 04.

3- **المكان نفسه**.

المطلب الثاني: أشكال الجرائم السيبرانية

وتتمثل أهم أشكال الجرائم السيبرانية فيما يلي:

1- البرمجيات الخبيثة.

(MalWare) هي إختصار لـ (Malcious Software) وتعني برمجية خبيثة، البرمجيات الخبيثة هي برامج تهدف إلى إلحاق الضرر بالحاسوب أوتعطيله وجمع المعلومات والتجسس وعرقلة العمليات، وتتمكن بطريقة غير شرعية من عدوى نظام الحاسب بدون معرفة أوعلم المستخدم من أجل اختراق جهازه والتجسس عليه.[1]

ومن أنواع البرمجيات الخبيثة نذكر ما يلي:

أ- أحصنة طروادة: (Trojan Horses)

هي برامج تتضمن تعليمات خفية تهدف للتخريب وإلحاق الضرر بالنظام على الرغم من أنه في ظاهره يبدو كأنه يؤدي أعمالا عادية، فهي توحي للمستخدم بأنها تقوم بعمل معين في حين أنها في واقع الأمر تؤدي عملا آخر تخريبي في الغالب، فتقوم أحيانا بالتجسس ومتابعة كل ما يتم عمله من إجراءات وتسجيله من بيانات على الجهاز المصاب بها وتقوم أحيانا أخرى بإحداث أنواع أخرى من الأذى على الأجهزة المصابة مثل تشفير البيانات أومسحها أوغير ذلك، ولا تتمكن أحصنة طروادة من نسخ نفسها أوالالتصاق بالبرامج الأخرى ولكنها تؤدي عملا معينا تم تصميمها من أجله.[2]

ب- القنابل المنطقية (Logic Bombs) والقنابل الموقوتة (Time Bombs)

هي من أنواع أحصنة طروادة وتعمل القنابل المنطقية عند حدوث شرط منطقي محدد مثل بلوغ الموظفين عددا معينا أورفع اسم أحد الموظفين من كشف الرواتب، أوكتابة كلمة معينة أوعند تشغيل برنامج معين لعدد محدد من المرات، أما القنابل الموقوتة فتعمل وفقا لتوقيت معين مثل ساعة محددة أويوم محدد.[3]

1- جميل حسين طويلة، "**البرمجيات الخبيثة**"، (دليل عملي لإستخدام البرمجيات الخبيثة وبرمجيات التجسس وإجراءات الوقاية والحماية منها، د س)، ص 10.

2- فاتن سعيد بامفلح، "**حماية أمن المعلومات في شبكات المكتبات- دراسة حالة أم القرى**"،(جامعة: الملك عبد العزيز، د س ن)، ص 15.

3- **المكان نفسه.**

هذه البرمجيات استخدمت في العديد من الهجمات على الدول من طرف دول او منظمات مختصة في السرقة، وكمثال تعرض ايران للعديد من هذه البرمجيات التي تستخدم للسرق والافساد في مفاعلاتها النووية وعرضتها لخسائر كبرى.

ج- الديدان (worms).

لا تحتاج الدودة إلى برنامج آخر تلتصق به للقيام بدورها كما هوالحال بالنسبة للفيروس الذي يلزمه حاضن (Host) لتنفيذ مهمته، ولكنها تعمل بمفردها حيث لديها القدرة على إعادة توليد نفسها والانتقال من ملف إلى آخر ومن جهاز إلى آخر متصل بالشبكة لتحقيق الانتشار.

ولا تعمل الديدن على تخريب الملفات وإتلافها كما هوالحال بالنسبة للفيروسات ولكنها تسبب زيادة عبئ على تحميل الشبكة حيث تقوم باستهلاك الذاكرة أوالمعالج أوالأقراص أوسائر موارد الحاسب وقد تؤدي بالتالي إلى توقف النظام.

2- الاختراق

يشار إليه في اللغة الإنجليزية (Hacking) ويسمى باللغة العربية عملية التجسس أوالقرصنة، حيث يقوم أحد الأشخاص غير المصرح لهم بالدخول إلى نظام التشغيل في جهاز الحاسوب بطريقة غير شرعية ولأغراض غير مسموح بها مثل التجسس أوالسرقة أوالتخريب، حيث يتاح للشخص المتجسس (الهاكر) أن ينتقل أويمسح أويضيف ملفات أوبرامج، كما أنه بإمكانه أن يتحكم في نظام التشغيل فيقوم بإصدار أوامر مثل إعطاء أمر الطباعة أوالتصوير أوالتخزين[1]، وبالتالي يكون المستهدف عرضة لسرقة معلوماته وبياناته سواء أكان فردا أومنظمة أودول لإلحاق الضرر المادي في بناها التحتية أوتهديد أمنها.[2]

والمخترقون هم أشخاص يتمتعون بقدرة عالية على كتابة وتصميم البرامج وفهم عميق لكيفية عمل الحاسب الآلي مما يسهل عليهم اختراق أنظمتها وتغييرها، وهناك نوعين من المخترقين:

الأول: الهاكر (White Hat) هم في العادة أشخاص فائقوا الذكاء يسيطرون بشكل كامل على الحاسب ويجعلون البرامج التي تقوم بأشياء أبعد بكثير مما صمت له أصلا، لذلك نجد أن بعض الشركات العالمية توظف

1- شيماء جابر، "**الاختراق وطرق الحماية منه**"، تم تصفح الموقع يوم : 26 فيفري 2018. الرابط:
Https://download-internet-pDF-ebooks.com/4926.Free-book

2- أوس مجيد غالب العوادي، "**الأمن المعلوماتي السيبراني**"، (سلسلة إصدارات مركز البيان للدراسات والتخطيط، أوت 2016)، ص 19.

أمثال هؤلاء الهاكر لتستفيد من قدراهم سواء في الدعم الفني أوحتى لإيجاد الثغرات الأمنية في أنظمة هذه الشركات.[1]

الثاني: الكراكر (Black Hat)

هم من يُسخّرون ذكائهم بطريقة غير شرعية، وهم يهتمون بدراسة الحاسب والبرمجة ليتمكنوا من سرقة معلومات الآخرين الشخصية، ويغير أولئك المخربون أحيانا المعلومات المالية للشركات وتخريب أنظمة الأمان بالإضافة إلى أعمال تخريبية أخرى، وفي أسوأ الأحيان يقوم بالقضاء على النظام المعلوماتي الإلكتروني بشكل كلي والكثير منهم يقوم بسرقة برامج وتوزيعها مجانا لهدف، فمنهم من يضع ملف "الباتش" بين ملفات هذا البرنامج وفي الغالب يكون عمله تخريبي.[2]

وفيما يتعلق بأنواع الاختراقات يمكن تقسيمها إلى ثلاث أنواع وهي كالآتي:

– اختراق الخوادم والأجهزة الرئيسية للشركات والمؤسسات أوالجهات الحكومية وذلك عن طريق اختراق الجدار الناري للخوادم بعملية تدعى المحاكاة، والتي تعني انتحال شخصية للدخول إلى النظام إذ أن عنوان ال(IP) يحتوي على عناوين المرسل والمرسل إليه وهذه العناوين تشكل مادة أساسية وثغرة كبيرة للمحترفين.

– اختراق الأجهزة الشخصية واستراق ما تحويه من معلومات وتعد هذه الطريقة شائعة جدا من قبل الهواة والمحترفين.

– التعرض للبيانات أثناء انتقالها والتعرف على شفرتها في حال كونها مشفرة، وهذه الطريقة شائعة لدى المحترفين الذين يحاولون سرقة أرقام بطاقات الإئتمان البنكية وكشف الأرقام السرية لها.

الهجمات الإلكترونية التي تتم عبر الانترنت أوالفضاء السيبراني تمتاز بسهولتها لأن تلك الهجمات تتم عن بعد وأن عملية الاختراق لا تتم إلا بوجود عاملين أساسيين؛ الأول هوالبرنامج المسيطر ويكون في جهاز المخترق والثاني يسمى الخادم ويكون في جهاز الضحية يقوم بتسهيل عملية الاختراق.[3]

والجدير بالذكر أن طرق الإختراق تختلف وتتعدد وتتطور بتطور التقنيات، ولكن يبقى العنصر الأساسي هوضرورة وجود إتصال بين جهاز المخترق وجهاز الضحية.

1- فاروق فؤاد حسن، **" مدخل إلى أمن المعلومات وتعريف الجرائم الإلكترونية وكيفية الحماية والإستخدام الأمثل للموارد المتوفرة للوصول إلى أقصى درجات الحماية في دوائر وزارة الداخلية العراقية"**، (وزارة الداخلية: المديرية العامة للإتصالات والمعلوماتية، قسم التدريب والتطوير، شعبة الدراسات والبحوث، د س)، ص 12.

2- فاروق فؤاد حسن، **المرجع السابق**، 12، 13.

3- أوس مجيد غالب العوادي، **المرجع السابق**، ص 20.

3- الفيروسات

تعد الفيروسات من أخطر مهددات الأمن السيبراني لذا فإن مؤشر وجود فيروس يمثل جريمة سيبرانية من جرائم الحاسب، فالفيروسات تهدف إلى السيطرة على الجهاز والإضرار بالنظام وسرقة المعلومات وتمكين المخترقين من الوصول إلى المعلومات بسهولة وإتلاف محتويات النظام كافة.

والفيروسات من وجهة نظر برمجية هي عبارة عن برنامج أوتطبيق يتم تصميمه بواسطة أحد المبرمجين لتحقيق هدف معين من الأهداف التي تمت الإشارة إليها آنفا، لذلك يتم برمجته ليكتسب القدرة على التدمير أوفتح الثغرات للوصول إلى المعلومات وسرقتها أوالسيطرة على أنظمة معينة، ومن الممكن للفيروس استنساخ نفسه عدة مرات أوإعادة إنشاء نفسه والانتشار أوربط نفسه ببرامج أخرى ومن أهم أنواع هذه الفيروسات:[1]

– **باب المصيدة**: هورمز يتم توزيعه حين يتم تركيب باب الحماية كي يعطي للمخترق الحرية في اختيار الوقت المناسب لعملية التخريب، حيث يسمح هذا الرمز بالنفاذ من خلال الشبكات في ظل وجود نظم حماية معينة.

– **فيروس العتاد**: يعمل هذا النوع من الفيروسات على توليد ملايين العمليات الحسابية وعمليات الإدخال والإخراج المتتالية التي تؤدي إلى إرتفاع كبير في درجة حرارة المعالج المركزي وإحراقه.

– **الباتشيات (Trojans)**: عبارة عن برنامج صغير قد يكون مدمجا مع ملف آخر للتخفي، حينما يتم تتريله وفتحه يصيب الــRegistry ويفتح منافذ مما يجعل الجهاز الخاص بالمستخدم قابلا للاختراق بسهولة ويعد من أذكى البرامج.[2]

4- الهجمات الطمسية.

وتتمثل في استهداف صفحات الويب واستبدالها بصفحات أخرى، إذ يقوم المهاجم بخلق موقع شبكي مماثل للموقع الأصلي لاصطياد المشتركين واستدراجهم لمعرفة معلوماتهم أوبطاقات الإئتمان الخاصة بهم وغيرها.

5- الهجمات الخداعية.

تتم من خلال استخدام بروتوكولات النقل والتحكم (TCP/IP) في اختراق أمن النظام أثناء عمل العميل والخادم، حيث يعمل البروتوكول أعلاه على تأمين وصلة ربط آمنة بين أي عميلين من خلال أرقام المنافذ ومحددات الهوية المنطقية، حيث يقوم المهاجم بتخمين أرقام المنافذ التي تخص تبادل البيانات وبالتالي يحل

1- أوس مجيد غالب العوادي، **المرجع السابق**، ص 24.

2- **المرجع نفسه**، ص 25.

محل المستخدم القانوني ويخترق جميع الجدران الواقية للوصول إلى قواعد البيانات للضحية ويستغل المتسللون البروتوكولات في شل الشبكات وإعادة توجيه البيانات نحو مقصد زائف، تحميل الأنظمة فوق طاقاتها من خلال غمرها برسائل متعددة لمنع مرسل من إرسال بياناته.[1]

بالاضافة الى العديد من الهجمات الاخرى التي تظهر مع تطور شبكات المعلومات.

1- المرجع نفسه، ص 18.

المبحث الثالث: مفاهيم أساسية حول الأمن السيبراني.

تثير المسألة الأمنية إنشغال الكثير من الباحثين والمختصين في حقل العلاقات الدولية بصفة عامة والدراسات الأمنية والإستراتيجية بصفة خاصة، فالدول لاتزال تبحث عن أنجع السبل التي تمكنها من الحفاظ على أمنها واستقرارها، ومع ظهور الثورة التكنولوجية الحديثة وفي ظل تنامي التهديدات الأمنية الجديدة أصبحت مسألة الأمن السيبراني تحظى باهتمام الدول كافة، بحيث عمدت بصفة مستمرة على تطوير ودعم بينتها المعلوماتية وكذا حمايتها لضمان أمنها وأمن أفرادها.

وقبل الخوض في مفهوم الأمن السيبراني وجب البحث في أصل كلمة سبرانية وفي معناها اللغوي والاصطلاحي.

المطلب الأول: مفهوم الأمن السيبراني.

اتخذ مفهوم الأمنالسيبراني عدة اتجاهات يمكن وصفها فيما يلي:

1– التعريف اللغوي لكلمة سيبرانية.

كلمة سيبرانية مشتقة من الكلمة اليونانية (Kybernetes) التي وردت بداية في مؤلفات الخيال العلمي وكان يقصد بها قيادة ربان السفينة، وقد استخدمت هذه الكلمة سابقا من قبل الفيلسوف اليوناني "أفلاطون" أثناء محاوراته عن فن قيادة السفينة.[1]

وبالرجوع إلى قواميس اللغة يشير قاموس (المورد) إلى أن تعريف كلمة سيبرانية هوعلم الضبط، أي ضبط الأشياء والسيطرة عليها.[2]

ويعرف معجم "le petit la rousse" السيبرانية (Cyber) بأنها: "العلم الذي يدرس آليات الاتصال والتحكم في الآلات والكائنات الحية الأخرى".[3]

أما معجم "Oxford" الإنجليزي فيعرفها على أنها: "دراسة فاعلية العمل البشري بمقارنتها بفاعلية الآلات الحاسبة، وتتصل بسمات وخصائص الحواسيب وتكنولوجيا المعلومات والواقع الافتراضي".[4]

1– أحمد عيسى نعمة الفتلاوي، **"الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم المعاصر"**، (بحث مقبول للنشر في مجلة المحقق الحلي، جامعة الكوفة، كلية القانون، 2016)، ص 05.

2– منير البعلبكي ورمزي منير البعلبكي، **"المورد الحديث"**، (لبنان: دار العلوم للملايين)، ص 307.

3- **"la rousse dictionnaire de français"**, p 104.

4- **"Oxford dictionaries language"**, p 299.

أما الموسوعة العربية الإلكترونية فتعرف كلمة سيبرانية على أنها: "مجموعة من الدراسات النظرية للعمليات الناظمة لضبط الأجهزة الإلكترونية والميكانيكية بوجه عام والأجهزة البيولوجية على وجه الخصوص سواء أكانت آلية أم حيوية".[1]

إن معظم القواميس المتخصصة في المصطلحات العسكرية لم تُرجع كلمة (Cyber) إلى مصدرها بل عرفت في نطاق استخدامها الفعلي أي العسكري، كقاموس المصطلحات العسكرية الأمريكية إذ يعرفها بأنها: "أي فعل يستخدم عن طريق شبكات إلكترونية بهدف السيطرة أوالتعطيل لبرامج إلكترونية أخرى".[2]

فيما يعرفها قاموس مصطلحات الأمن المعلوماتي بأنها: "هجوم عبر الفضاء الإلكتروني يهدف إلى السيطرة على مواقع إلكترونية أوبنى محمية إلكترونيا لتعطيلها أوتدميرها أوالإضرار بها".[3]

أما في اللغة العربية وبالرجوع إلى المختصين فيها، فنجد أن هناك تحديا يواجهه هؤلاء المختصين في الوصول إلى مصطلح مقارب لمصطلح (Cyber) في اللغة الإنجليزية.

2- التعريف الاصطلاحي لكلمة سيبرانية.

كلمة سيبرانية في مفهومها الحديث استعملت لأول مرة من قبل عالم الرياضيات الأمريكي "نوربرت وينر" "Norbert wiener" وهوأستاذ الرياضيات في معهد ماساشوستس التقني (MIT) الذي أعطاها مفهومها الاصطلاحي الحديث وكان ذلك عام 1948م، من أجل وصف نظام التغذية الرجعية (Feed back) الذي وضعه والذي يعمل على الاستفادة من مخرجات الأنظمة في ضبط مدخلاتها وفي التحكم فيها واستقرار أدائها.

ورأى "وينر" أنه يمكن تطبيق هذا النظام على نطاق واسع في مختلف المجالات ليس العملية فقط بل الإنسانية أيضا، ووضع لذلك كتاب بعنوان "السيبرانية أوالتحكم والاتصال في الحيوان والآلة".[4]

وبالتالي فالمصدر الاصطلاحي الحديث لكلمة سيبرانية هوعلم القيادة أوالتحكم في الأحياء والآلات ودراسة آليات التواصل في كل منهما.

1- الموسوعة العربية، **"علم الحياة (الحيوان والنبات)، الاستقلالية"**، تم تصفح الموقع يوم : 03 فيفري 2018. الرابط:
http;//www.arab_ency.com/détails.php? Full=18nid=113

2- أحمد عيسى نعمة الفتلاوي، **المرجع السابق**، ص 05.

3- **المكان نفسه**.

4- سعد علي الحاج بكري، **"الأمن السيبراني ومعضلة حمايته"**، تم تصفح الموقع يوم : 03 فيفري 2018. الرابط:
www.aleqt.com/2017/08/24/article.1241506.html

ويعرفها "لوب كوفينال" "L.covinal" في كتابه "السبرنتيك" بأن الفكر السيبراني يتميز بهدفه ومنهجه:

- الهدف: هوفعالية قيادة وتوجيه الفعل.

- المنهج: هوالاستبدال التماثلي الذي يسمح بصنع نماذج فيزيائية تمثل بعض الوظائف العقلية التي تبين بالتحليل أنها وظائف آلية يمكن مكننتها، إذ أنه يمكن صنع نماذج تمثل الغريزة والتعلم والتصرف حسب سلوك الوسط الخارجي والتخيل كما أن الفعل الرجعي هوأساس هذه النماذج في أكثر الوظائف العقلية.[1]

ويعرفها "أوديل دافيد" "O.David" بأنها: "التوضيح الكامل والجوهري للفكر الخاضع لهدف منها".[2]

ويعرفها "براي والتر" "B.Walter" بأنها: "علم الآلات العقلية".[3]

لقد لخص "نوربورت وينر" الحدود التي لا ينبغي أن يتعداها إيماننا بقدرات الآلة أوالخوف من طغيانها بقوله: "أعط ما للإنسان للإنسان، وما للعقل الإلكتروني للعقل الإلكتروني"، وهويعني بذلك أن الإنسان يظل له دوره العام والأساسي في عصر التقدم التكنولوجي، وأن أرقى أنواع الآلات يظل على الدوام أداة طيعة في يد صانعها وهي تتجه في نفس الطريق الذي يريدها الإنسان أن تسلكه سواء أكان خيرا أم شرا.

وكان ظهور علم السيبرنطيقا (Cybernetics) هذا العلم الجديد، هوبدوره واحدا من المعالم البارزة لعصرنا الحاضر حيث كانت أبحاث "وينر" هي الأساس الأول لاختراع العقول الإلكترونية.

فقد كانت فكرة هذا العالم هي تطبيق ما يحدث في الإنسان بوصفه جهازا حيا متكاملا على الآلات من أجل بلوغ مرحلة جديدة في تطورها مختلفة عن كل ما استخدمت فيه الآلات من قبل، وعلى هذا الأساس فقد درس "وينر" الوظائف الذي يقوم بها الجهاز العصبي للإنسان والتي يتمكن الإنسان بواسطتها من أن يصحح مسار أفعاله ويعيد توجيهها وفقا لما يواجهه، وأن يأمر نفسه ويطيعها ويختبر نتائج سلوكه ويعدلها.[4]

وحين أمكن تطبيق نتائج هذه الدراسات في صنع جيل جديد من الآلات كانت تلك الآلات من نوع لم يألفه الإنسان من قبل، فهي ليست تلك الآلات التي تحتاج إلى إشراف دائم للإنسان ولا تعمل إلا وفقا لأوامره ولا تسير إلا في خط واحد يرسمه لها مقدما، بل أنها كانت آلات تصحح مسارها بنفسها وتتبادل مع

1- ضياء وراد، **مترجما**، **"الكون الرقمي: الثورة العالمية في الإتصالات"**، (المملكة المتحدة: مؤسسة هنداوي سي آي سي للنشر،2017)، ص 21.

2- **المرجع نفسه**، ص 22.

3 - **المكان نفسه**.

4- فؤاد زكريا، **"التفكير العلمي"**، الطبعة الثالثة، (الكويت: المجلس الوطني للثقافة والفنون، 1978)، ص 144.

نفسها الأوامر وتنفيذ الأوامر وتقوم بأعمال إنتاجية أعقد وأكمل بكثير مما كانت تقوم به الأجيال السابقة من الآلات سواء منها البخارية والكهربائية.

وهكذا كانت فكرة تلك الآلات تتضمن في داخلها عقلا حاسبا يراقب عملها ويعدله ويصححه ويعيد توجيه سيرها وفقا لما يجريه من حسابات.[1]

وقد نجحت هذه الآلات في إحداث تحول كبير في ميدان الإنتاج المادي فضلا على أنها توفر نسبة كبيرة من الأيدي العاملة، أي أنها كانت تحقيقا فعليا لحلم بشري هوحلم الآلة التي تقوم بكل أعمال الإنسان وتعفيه من مشقة العمل.

ويعد الإنجاز الأكبر الذي قامت عليه هذه الآلات الجديدة كان تطبيقها في ميدان العمل العقلي باختراع نوع جديد من الآلات هوالعقول الإلكترونية والذي يعد خطوة جديدة في طريق التقدم العلمي.[2]

3- تعريف الأمن السيبراني.

تعتبر مهمة تحديد المفاهيم أول تحد يواجهه المفكرون ويتعرض له الباحثون في جميع التخصصات وفي شتى الدراسات، وذلك لما تطرحه من إشكاليات تجعل من الصعوبة بمكان الإتفاق على تعريفات واضحة وشاملة وموحدة بين فرقاء المجتمع العلمي يمكن تعميمها على جميع الحقول المعرفية.[3]

ويعتبر مفهوم الأمن السيبراني من أكثر المفاهيم المثيرة للاهتمام والدراسة، حيث عرف تعددا في التعريفات المقدمة له والتي يمكن إبرازها فيما يلي:

- فقد عرفه "ريتشارد كمرر" "Richard A.Kemmerer" على أنه: "عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة".

- بينما يعرفه "إدوارد أمورسو" "Edward amoroso" على أنه: "وسائل من شأنها الحد من خطر الهجوم على البرمجيات أوأجهزة الحاسوب أوالشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها وتوفير الاتصالات المشفرة".[4]

---

1 - فؤاد زكريا، **المرجع السابق**، ص 147.

2 - **المرجع نفسه**، ص 153.

3- عنترة بن مرزوق، **"الأمن السيبراني كبعد جديد من السياسة الدفاعية الجزائرية"**، (محاضرات مقدمة لطلبة جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، د س)، ص 65.

4- محمد مختار، **"Cyber Security: هل يمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية؟"**، مجلة مفاهيم المستقبل، العدد 06، (يناير 2015)، ص 05.

الملاحظ أن كل من "ريتشارد كمرر" و"إدوارد أمورسو" قد ركزا في هذين التعريفين على اعتبار أن الأمن السيبراني هووسيلة دفاعية ضد الهجمات وعمليات القرصنة على مختلف الحواسيب والشبكات.

وطبقا لتعريف الاتحاد الدولي للاتصالات (International Télécommunication Union) فإن الأمن السيبراني هو: "مجموعة الأدوات والسياسات ومفاهيم الأمن والضمانات الأمنية ومناهج إدارة المخاطر والإجراءات والتدريبات وآليات الضمانات والتكنولوجيا التي يمكن استخدامها في حماية البيئة السيبرانية وأصول المؤسسات والمستخدمين".

وتشمل البيئة السيبرانية أجهزة الحاسب الآلي والبرمجيات والتطبيقات الموجودة عليه والشبكات المتصلة من خلالها والعناصر البشرية والبنية التحتية وأنظمة الاتصالات فيما بينها، بالإضافة إلى جميع المعلومات سواء كانت محفوظة على الأجهزة أومنقولة فيما بينها، وفي ذلك يسعى الأمن السيبراني للحفاظ عليها وحمايتها من المخاطر والتهديدات السبرانية.

ويتبين من خلال هذا التعريف أن الأمن السيبراني يشمل جميع السياسات والوسائل والأدوات والمناهج لإدارة المخاطر وكذا حماية البيئة السيبرانية من المخاطر والتهديدات السيبرانية.

فالأمن السبراني يعني حماية المعلومات من خلال ثلاث محاور رئيسية: محور المعلومات الشخصية، محور المعلومات داخل الشركة ومحور المعلومات عبر الدول.

ومن ناحيته يعرفه قاموس "أكسفورد" على أنه: "الإجراءات والتدابير المتخذة للحماية من الاستخدام الإجرامي أوالاستخدام غير المصرح به للمعلومات الإلكترونية".[1]

كما يمكن تعريف الأمن السيبراني على أنه: "الحد من خطر هجوم ضار للبرمجيات وأجهزة الكمبيوتر كذلك يشتمل على الأدوات المستخدمة للكشف عن عمليات الاقتحام ووقف الفيروسات ومنع المتطفلين من الوصول إليها".[2]

ويمكن تعريف الأمن السبراني انطلاقا من أهدافه بأنه: "النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حال

1 - محمد مختار، **المرجع السابق**، ص 05.

2 - Dan Craigen &Others, **"Defining Cybersecurity"**, (Technology innovation Management Review, Octobre 2014), p 14.

تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن بحيث لا تتوقف عجلة الإنتاج ولا تتحول الأضرار إلى خسائر دائمة".[1]

الملاحظ من هذا التعريف أن حماية الموارد البشرية والمالية وكل ما يرتبط بتقنيات الاتصالات والمعلومات هي من أهداف الأمن السيبراني، والغرض من ذلك هوالحد من الخسائر والأضرار والحيلولة دون وصول هذه الأضرار إلى خسائر دائمة تعيق حركة الإنتاج وديمومته.

وكخلاصة فإن الحديث عن الأمن السيبراني يقود إلى أن:

– الأمن السيبراني هوتلك الوسائل والأدوات والسياسات الدفاعية لمواجهة مختلف التهديدات السيبرانية ومختلف عمليات القرصنة من أجل حماية البيئة السيبرانية.

– الأمن السيبراني يضمن إمكانات الحد من الخسائر والأضرار والحيلولة دون وصول هذه الأضرار إلى خسائر دائمة واحتوائها في أسرع وقت ممكن.

– الأمن السيبراني هوسلاح إستراتيجي بيد الحكومات والأفراد لاسيما أن الحرب السيبرانية أصبحت جزءا لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول.

وتأتي أهمية الفضاء الإلكتروني كقضية تتعلق بالأمن القومي في ظل تزايد الاعتماد الدولي عليه فيما يتعلق بتسيير عمل البنية التحتية الكونية للمعلومات، ومن ناحية أخرى عكس حجم المخاطر المتزايدة أمام المنشآت المدنية والعسكرية مع تصاعد وتيرة الهجمات التي يقوم بها القراصنة أوتقف وراءها جهات أودول معادية أوحتى جماعات إرهابية، ليطرح بذلك أمن الفضاء الإلكتروني كقضية دولية وذلك مع أهميته على جميع الأصعدة الاقتصادية والسياسية والأمنية والاجتماعية.

وأدت علاقة الفضاء الإلكتروني بعمل عدد من المنشآت الحيوية سواء أكانت مدنية أوعسكرية في الوقت نفسه لإمكانية تعرضها لهجوم من خلاله، إما يستهدفه كوسيط وحامل للخدمات أوبشل عمل أنظمتها المعلوماتية ويكون من شأنه التأثير على القيام بوظيفتها ومن ثم فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة ونفوذ إستراتيجية بالغة الأهمية سواء في زمن السلم أوالحرب.[2]

1 – منى الأشقر جبور، **"الأمن السيبراني: التحديات ومستلزمات المواجهة"**، (جامعة الدول العربية: المركز العربي للبحوث القانونية والقضائية، 2012)، ص 03.

2- حنان علي سعادة، **"الأمن السيبراني والأمن المعلوماتي"**، تم تصفح الموقع يوم : 20 فيفري 2018. الرابط: http://ae.linkedin.com/sulse/D8A7D984D8A7

ومن خلال هذه المعطيات يتضح أن قضية أمن الفضاء الإلكتروني أضحت قضية دولية تحظى بالمزيد من الاهتمام بشكل جعلها إحدى أولويات الأمن الوطني في العديد من الدول بل ارتباطها بالأمن الدولي ككل وهذا يتطلب وجود إستراتيجية خاصة يتكون أهم عناصرها في:

– إدراك درجة العلاقة بين أمن الفضاء الإلكتروني والأمن الوطني وبقضايا التنمية الاقتصادية والاجتماعية والاستقرار السياسي.

– أهمية وجود فهم للقضايا القانونية التي تتعلق بتكنولوجيا الإتصال والمعلومات وسوء استخدامها.

– أهمية وجود هيكل تنظيمي أومؤسسي يتولى مواجهة تلك المخاطر في وقت الطوارئ.

– فهم الإمكانيات والقدرات التقنية لتكنولوجيا الاتصال والمعلومات والاستخدام السيئ لها وفهم الأخطار المرتبطة به وكيفية الاستجابة لها تكنولوجيا.

– أهمية دور الأفراد في عملية الأمن بمعرفتهم بالإجراءات الأمنية التي يمكن أن تستخدم لتأمين مصادر تكنولوجيا الإتصال والمعلومات.

– أهمية وجود تعاون من جميع الفاعلين في مجتمع المعلومات العالمي لترسيخ ثقافة عالمية لأمن الفضاء الإلكتروني.[1]

المطلب الثاني: الأمن السيبراني وعلاقته بالمفاهيم ذات الصلة

مفهوم الأمن السيبراني يتشابك ويتداخل معه مفاهيم ومصطلحات أخرى الأمر الذي يخلق اللبس والتعقيد لذلك لابد من توضيح مواطن اللبس من خلال تقديم تعريفات لهذه المصطلحات وما يفرقها عن مصطلح الأمن السيبراني.

1– الأمن المعلوماتي

يقصد بأمن المعلومات من زاوية أكاديمية العلم الذي يبحث في نظريات وإستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها، ومن زاوية تقنية فيقصد به الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية.

1– حنان علي سعادة، **المرجع السابق**.

ومن زاوية قانونية فإن أمن المعلومات هومحل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أواستغلال نظمها في إرتكاب الجريمة، وهوهدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها.[1]

ويعتبر الأمن السيبراني مفهوم أوسع من أمن المعلومات حيث يتضمن تأمين البيانات والمعلومات التي تتداول عبر الشبكات الداخلية أوالخارجية والتي يتم تخزينها في خوادم داخل أوخارج المنظمات من الاختراقات إضافة إلى ذلك فإن الأمن السيبراني يشمل بعض الأمور التي لا تندرج ضمن أمن المعلومات كحماية البنى التحتية والصواريخ الحربية وكاميرات المراقبة الرقمية، كما أن الأمن السيبراني يهتم بأمن كل ما هوموجود على السايبر من غير أمن المعلومات بينما أمن المعلومات لا يهتم بذلك، إلى جانب ذلك فأمن المعلومات يهتم بأمن المعلومات الفيزيائية الورقية بينما لا يهتم الأمن السبيراني بذلك.[2]

2- الأمن الإلكتروني

تعد الثورة الرقمية وعالم الانترنت في الوقت الحالي بيئة تنظم فيها الكثير من النشاطات الاقتصادية والإدارية والبحثية، كما تعد مجالا للتفاعل والتواصل والابتكار حيث لم يعد بالإمكان الاستغناء عن شبكات الانترنت ووسائل وتكنولوجيا الاتصال وحفظ البيانات والمعلوماتية في ظل الاتجاه نحوما يسمى بالإدارة والحكومة الإلكترونيتين والاقتصاد وكل هذه الأنواع من المعلومات والبيانات، حيث يتم تناقلها وحفظها في أغلب الأحيان عند شبكات الحواسيب، ومن هنا تأتي أهمية تأمين هذه الشبكات من مختلف التهديدات والمخاطر ولتجسيد ذلك ظهر ما يسمى بـــ"الأمن الإلكتروني" أوأمن المعلومات الإلكترونية، حيث بات يشكل جزءا أساسيا في أي سياسة أمنية وطنية وأصبحت الدول تنظر إليه كنظير منافس للأمن التقليدي ومُعَبر عن سيادتها وأمنها الوطني، لذلك أصبح صُنَّاع القرار في معظم دول العالم يصنفون مسائل أمن المعلومات الإلكترونية كأولوية في سياساتهم الدفاعية الوطنية.[3]

1- فتيحة ليتيم، ونادية ليتيم، **"الأمن المعلوماتي للحوكمة الإلكترونية وإرهاب القرصنة"**، مجلة الفكر، العدد 12، (د ش، د س)، ص 239.

2- فهد الدريبي، **" ما هو الأمن السيبراني"**، تم تصفح الموقع يوم : 21 فيفري 2018. الرابط:
Https://www.fadvisor.net/blog/2017/11/what is Cyber security/

3- د م، **"النظام القانوني للأمن الوطني الإلكتروني في ظل الثورة الرقمية"**، تم تصفح الموقع يوم : 22 فيفري 2018. الرابط:
www.univ-chlef.dz/fdsp/images/PDF/JE-DROIT-2017.PDF

فالأمن الإلكتروني يعني الحماية الناجمة عن جميع التدابير الرامية إلى منع الأشخاص غير المصرح لهم من الحصول على معلومات ذات قيمة يمكن أن تستمد من اعتراضهم.[1]

بينما يعتبر الأمن السيبراني مجموع الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به على شبكات الكمبيوتر، وسوء الاستغلال واستعادة المعلومات الإلكترونية التي تحتويها بهدف ضمان واستمرار عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات سواء الخاصة بالأفراد أوالجهات في الفضاء السيبراني.

والملاحظ من خلال التعرض إلى تعريف الأمن الإلكتروني والأمن السيبراني أن هناك تداخل وتقارب بين المصطلحين فكلاهما يرمي إلى نفس الأهداف وهي حماية أمن المعلومات وسلامتها من الهجمات والمخاطر، والسعي إلى تأمين وحماية خصوصية البيانات سواء تعلق الأمر بالأفراد أوالمؤسسات أوالدول.

المطلب الثالث: أبعاد الأمن السيبراني

يرتبط الأمن السيبراني بمجالات مختلفة سياسية وعسكرية واقتصادية وقانونية واجتماعية بهدف تحقيق منظومة أمن متكاملة تعمل على الحفاظ على الأمن القومي للدولة من أي تهديدات سيبرانية محتملة ويمكن توضيح ذلك من خلال ما يلي:

1- البعد العسكري

تكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الإلكتروني بما يسمح بسهولة تبادل المعلومات وتدفقها وبسرعة إعطاء الأوامر العسكرية والقدرة على إصابة الأهداف عن بعد وتدميرها، وقد تتحول هذه الميزة إلى نقطة ضعف إن لم تكن الشبكة الإلكترونية المستخدمة في ذلك مؤمنة جيدا من أي اختراق خارجي قد يتسبب في شن هجمات إلكترونية مضادة على شبكات القوة المسلحة وأجهزة الاستخبارات ومن ثم تدمير قواعد البيانات العسكرية وتعطيل قدرة الدولة على النشر السريع لقدراتها وقواتها أوقطع أنظمة الاتصال بين الوحدات العسكرية وتعطيل شبكات الكمبيوتر.

[1]- "**Electronics security**", Web Site Visited in : 22 Februay 2018. Link: https://www.thefreedictionary.com/electronics+security

كما يمكن أن يتم شل أنظمة الدفاع الجوي أوالتوجيه الإلكتروني للخصم فضلا عن إمكانية فقدان السيطرة على وحدات القيادة والتوجيه بالإضافة إلى فقدان العدو قدرته على التحكم أوالاتصال بالأقمار الصناعية.[1]

2- البعد الاقتصادي

يرتبط الأمن السيبراني ارتباطا وثيقا بالاقتصاد فالتلازم واضح بين إقتصاد المعرفة وتوسيع استخدام تقنيات المعلومات والاتصالات كما بالقيمة التي تمثلها البيانات والمعلومات المتداولة والمخزنة والمستخدمة على كل المستويات، كما تتيح تقنيات المعلومات والاتصالات تعزيز التنمية الاقتصادية لدول كثيرة عبر إفادتها من فرص الاستخدام التي تقدمها الشركات الدولية والشركات الكبرى التي تبحث في إدارة كلفة إنتاجها بأفضل الشروط.[2]

يضاف إلى ذلك دخول العالم عصر المال الإلكتروني ضمن بيئة تقنية متحركة بعد إطلاق الخدمات الإلكترونية، إذ تتزايد استثمارات المصارف والمؤسسات المالية في مجال المال الرقمي وتتنافس الشركات على إصدار تطبيقات تسمح بآليات دفع آمنة، وقد وضعت بعض الدول تشريعات خاصة بحماية أموالها وما يمكن أن يثيره هذا الأمر من صعوبات وما يتطلبه من تشريعات للحد من بعض الجرائم الاقتصادية والمالية الخطيرة والعابرة للحدود كتبييض الأموال والتهرب من الضريبة.

فالأمن السيبراني يضمن تقديم الخدمات التي تقدم بواسطة تقنيات المعلومات والاتصالات، كما يضمن الإقبال عليها بما يترجم عمليا بتطوير أسس اقتصاد سليم.[3]

3- البعد السياسي

يتمثل البعد السياسي للأمن السيبراني بشكل أساسي في حق الدولة في حماية نظامها السياسي وكيانها ومصالحها الاقتصادية التي تعني حقها وواجبها في السعي إلى تحقيق رفاه شعبها في وقت تؤثر موازين القوى داخل المجتمع نفسه، حيث أصبح بإمكان الفرد أن يتحول إلى لاعب أساسي في اللعبة السياسية كما أصبح بإمكانه الإطلاع على خلفيات ومبررات القرارات السياسية التي تتخذها حكومته عبر الكم الهائل من المعلومات التي يمكنه الوصول إليها.[4]

1- محمد مختار، **المرجع السابق**، ص 06.

2- مني الأشقر جبور، **المرجع السابق**، ص 30.

3- مني الأشقر جبور، **المرجع السابق**، ص 31.

4- **المرجع نفسه**، ص 29.

بالمقابل لا يتوانى العاملون في الشأن السياسي من الاستفادة مما تقدمه هذه التقنيات للوصول إلى أكبر شريحة ممكنة من الأفراد والترويج لسياساتهم في العالم، ومدى التأثير الذي يتركه هذا الأمر بغض النظر عن صحة السياسات والمبادئ والمواقف التي تروج لها، فقد استخدم "أوباما" مثلا الشبكات الاجتماعية بشكل مكثف خلال حملته الانتخابية كما تركت التسريبات لآلاف الوثائق الدبلوماسية السرية عبر الويكيليكس أثرا سلبيا على العلاقات بين الدول.[1]

4- البعد الإجتماعي

تساهم شبكات التواصل الاجتماعي بشكل خاص في فتح المجال للأفراد للتعبير عن تطلعاتهم السياسية وطموحاتهم الاجتماعية بأشكالها المختلفة، كذلك تشكل مشاركة جميع شرائح المجتمع ومكوناته وسيلة لتطوير المجتمع مما يتيح الفرصة للإطلاع على الأفكار والمعلومات وبما تكونه من حاجة لدى المجتمع في الحفاظ على استقرار الفضاء الإلكتروني والمجتمع الذي يرتكز إليه، كما أن انفتاح مجتمع ما على المجتمعات الأخرى يؤسس لتبادل خبرات وأفكار وتكوين آفاق للتعاون والتكامل.

يضاف إلى ذلك ما يقدمه هذا الفضاء من إمكانات وقدرات للمجالات العلمية والثقافية والخدماتية حيث يسمح للوصول إلى مناطق بعيدة وإلى فئات محددة، هذا فضلا عن الدور الذي يمكن أن يؤديه في تبادل المعلومات في أوقات الأزمات والكوارث بحيث تتأمن المساعدات في أسرع وقت.[2]

والمساهمة في الحفاظ على القيم الجوهرية في المجتمع كالإنتماء والمعتقدات والعادات والتقاليد عبر إنشاء مجموعات تهتم بنشر الوعي حول هذه المسائل، وفي هذا السياق يأتي التشديد من قبل المنظمات والهيئات الدولية على نشر ثقافة الأمن في الفضاء الإلكتروني وضرورة التعاون من قبل فئات المجتمع بكل مكوناته على تحقيقه وضمانه لحمايته من التهديدات السيبرانية ذات التأثير السلبي على أخلاقيات المجتمع والتجنيد لقضايا تمس الأمن والسلم الدوليين.

وعليه لابد من بناء مجتمع مسؤول ومدرك لمخاطر الفضاء الإلكتروني له القدرة على التعامل بحد أدنى من قواعد السلامة مع إدراك للعواقب القانونية التي يمكن أن تترتب على بعض التصرفات التي تمارس في الفضاء الإلكتروني.[3]

1- **المرجع نفسه**، ص 30.

2- منى الأشقر جبور، **المرجع السابق**، ص 31.

3- محمد مختار، **المرجع السابق**، ص 07.

5- البعد القانوني

تعد العلاقة بين القانون والتكنولوجيات علاقة تبادلية فالتطورات التكنولوجية المختلفة تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية منها ولكن بصورة عامة تفتقد الجريمة السيبرانية في الوقت الحالي للأطر القانونية الصارمة للتعامل معها، ولعل ذلك يعود لعوامل مثل طبيعة الجريمة الإلكترونية في حدا ذاتها وصعوبة تحديد هوية مرتكبي تلك الجرائم ومرونة التعريفات المرتبطة بتكنولوجيا المعلومات، إلى جانب ذلك فإن الجرائم السيبرانية غير مقيدة بحدود الدول، الأمر الذي يقتضي تفعيل التعاون الدولي المشترك لمكافحتها.[1]

المطلب الرابع: العلاقة بين الأمن السيبراني والأمن القومي.

في عصر الثورة التقنية والمعلوماتية وجب الوقوف على حدود التفاعل الرقمي القائم بين أمن المعلومات الإلكترونية والأمن القومي للدول، فمع انصهار الحدود الجغرافية وتقلص المسافات بين أركان المعمورة بفعل الثورة الإلكترونية؛ أحدثت هذه التغييرات العديد من التأثيرات على الأمن القومي نتيجة البيئة التكنولوجية التي أتاحت للدول إمكانية الولوج في فضاء إلكتروني يحوي العديد من عناصرها ومعلوماتها القومية والأمنية والاقتصادية والسياسية والاجتماعية وغيرها من المقومات.[2]

لقد أصبحت العلاقة بين الأمن والتكنولوجيا علاقة متزايدة مع إمكانية تعرض المصالح الإستراتيجية ذات الطبيعة الإلكترونية إلى أخطار إلكترونية وتهدد بتحول الفضاء الإلكتروني لوسيط ومصدرا لأدوات جديدة للصراع المتعدد الأطراف ودورها في تغذية التوترات الدولية، ومن جهة أخرى فرضت تلك التطورات إعادة التفكير في مفهوم الأمن القومي الذي يُعنى بحماية قيم المجتمع الأساسية وإبعاد مصادر التهديد عنها وغياب الخوف من خطر تعرض هذه القيم للهجوم، وبذلك يتوافر أمن الفضاء الإلكتروني حال تحقيق إجراءات الحماية ضد التعرض للأعمال العدائية والاستخدام السيئ لتكنولوجيا الاتصال والمعلومات.

فالأمن بمفهومه العام يشير نظريا وعمليا إلى: "السلام والطمأنينة وديمومة مظاهر الحياة واستمرار مقوماتها وشروطها بعيدا عن عوامل التهديد ومصادر الخطر".[3]

1- **المكان نفسه.**

2- وليد غسان سعيد جلعود، **"دور الحرب الإلكترونية في الصراع العربي الإسرائيلي"**، مذكرة مقدمة لنيل شهادة الماجستير في التخطيط والتنمية السياسية، (جامعة: النجاح الوطنية، كلية الدراسات العليا، 2013)، ص 53.

3- عادل عبد الصادق، **"الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي"**، (المركز العربي لأبحاث الفضاء الإلكتروني، 2017)، ص 02.

وإن للأمن القومي مفهوم خاص يشير نظريا وعمليا إلى:

"القيم النظرية والسياسات والأهداف العملية المتعلقة بضمان وجود الدولة وسلامة أركانها وديمومة مقومات استمرارها وشروط استقرارها وتلبية احتياجاتها وتأمين مصالحها وتحقيق أهدافها، وحمايتها من الأخطار القائمة والمحتملة داخليا وخارجيا مع مراعاة المتغيرات الداخلية والإقليمية والدولية".[1]

لقد أصبح الأمن السيبراني والإلكتروني جزءا لا يتجزأ من الأمن القومي خاصة مع تنامي حجم التهديدات وعلاقة البعد الإلكتروني بعمل المنشآت الحيوية سواء كانت مدنية أوعسكرية.[2]

ويمكن الإشارة هنا إلى أن الأمن القومي لأي دولة له محاوره الرئيسية والمتمثلة في المحاور العسكرية السياسية الجغرافية، الاجتماعية، الاقتصادية والأمنية وأخيرا التقنية، وهوالمحور الذي يهم الدول اليوم نظرا لاستنادها على منظومة تقنية وإلكترونية عالية الدقة وغزيرة التكنولوجيا تعتمد على صناعة المعلومات والبحث العلمي والمعلوماتي.

1- المكان نفسه.

2- عادل عبد الصادق، "**المجال الأعلى للأمن السيبراني خطوة في دعم إستراتيجية الأمن القومي**"، تم تصفح الموقع يوم : 23 فيفري 2018. الرابط: www.accronline.com/article-detal.aspx?!d=20284.

المبحث الرابع: الإطار النظري للدراسة.

شهد حقل العلاقات الدولية زخما فكريا ونظريا كبيرا عبر مراحل وفترات زمنية مختلفة من أجل تفسير الواقع الدولي بشكل مفهوم ومستصاغ، لذلك تعددت النظريات التي تحاول فهم وتفسير المتغيرات من جهة ومن جهة أخرى إبراز أهم ما تطرحه هذه النظريات.

وبناء على ذلك وجب التوقف عند أهم النظريات لفهم سلوك إسرائيل لمواجهة التهديدات السيبرانية ودوافع إستراتيجيتها وهوما يمكن إبرازه فيما يلي:

المطلب الأول: النظرية الواقعية.

الواقعية هي الطريقة التي يتم وفقها النظر إلى العلاقات الدولية كعلاقات قوة ويتعين علينا الرجوع إلى اليونان القديمة والصين إذا أردنا تتبع جذورها النظرية، إذ أسس "ثيوسيدس" للواقعية ولعلاقات القوة التي تقوم عليها عبر تأريخه للحرب التي دارت رحاها بين أثينا وأسبرطا والتي عرفت بـــ **الحروب البلوبونيزية**، وقد قال في هذا الصدد أن: "إرساء معايير العدالة يعتمد على نوع القوة التي تسندها وفي الواقع فإن القوي يفعل ما تُمكنه قوته من فعله أما الضعيف فليس عليه سوى تقبل ما لا يستطيع رفضه"، وبدوره أسدى "سان تزو" الإستراتيجي الصيني الذي عاش في زمن "موتي" النصح للحاكم وكيفية صيانة بقائه واستعمال القوة لتعزيز مصالحه خلال زمن الحرب.[1]

إضافة إلى كتابات كل من "هوبز" "Hobbes" الذي صور العلاقات بين الدول على أنها علاقات تصارعية نتيجة للطبيعة البشرية الشريرة في كتابه (leviathan)، وفي كتابات "نيكولا ميكيافللي" "N.Mackiavel" من خلال كتابه الأمير (Le prince) أين اعتبر أن سلطة الأمير لابد أن تكون محكمة وخالية من الأخلاق نظرا لما تتميز به الطبيعة البشرية من تصرفات عدوانية تمس سلامة الأشخاص لذلك يتوجب عليه ضمان الأمن لكل الأفراد.[2]

ويعتبر "هانس مورغانتو" أب الواقعية التقليدية فهو يرى بأن الدولة هي الوحدة المرجعية للتحليل ولا يمكن اعتبار الأفراد جزءا منفصلا عن الدولة، فمن خلال السعي لتحقيق الأمن تعمل الدول على تعظيم قوتها

1- عادل زقاع، مترجما، **"مفهوم الأمن في نظرية العلاقات الدولية"**، ، تم تصفح الموقع يوم : 17 فيفري 2018. الرابط: Bohothe.blogspot.com/2010/03/blog-spot-26.html.

2- زكرياء بودن، **"أثر التهديدات الإرهابية في شمال مالي على الأمن الوطني الجزائري وإستراتيجيات مواجهتها 2010-2014"**، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية والعلاقات الدولية، تخصص علاقات دولية ودراسات إستراتيجية، (جامعة: محمد خيضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، 2015)، ص 32.

العسكرية، كما يعتبر "كينث والتز" أب الواقعية الجديدة إلى جانب "جون ميرشايمر"، فـــ "كينث والتز" يؤكد عكس "مورغانتو" بأن النظام الدولي ذوطبيعة فوضوية نظرا لغياب سلطة دولية ذات سيادة، فالفوضى هي السبب في قيام الحرب بين الوحدات المشكلة للنظام الدولي، في حين يرى "مورغانتو" أن النظام الدولي يصبح فوضوي نتيجة التنافس بين الوحدات المشكلة له.

لدى معظم الواقعيين إجابة مباشرة عن مشكلة النظام العام (order) وهوالسلطة المركزية الفعالة، فالحكومات التي تدافع عن الحدود وتفرض تطبيق القوانين وتحمي المواطنين تجعل السياسة الداخلية أكثر سلمية مختلفة نوعيا عن السياسة الخارجية وتبقى الساحة الدولية نظاما من الفوضى السياسية والمساعدة الذاتية وساحة من العنف تبحث فيها الدول عن فرص لاستغلال بعضها بعضا.[1]

يمثل الواقعيون المنظور الأكثر دفاعا عن فكرة اعتبار الأمن من صميم اهتمام وصلاحيات الدولة وحدها أي أن مفهوم الأمن الوطني يرتبط مباشرة بالدولة، حيث يفسر الأمن على أنه أمن الدولة ضد الأخطار ذوالتهديدات الخارجية من خلال حماية حدودها الإقليمية وصيانة سيادتها الوطنية واستقرارها.[2]

من جهة أخرى عرف حقل الدراسات الأمنية جدالا واسعا بسبب ظهور مجموعة من المدارس الفكرية حسب تعبير "أولي ويفر" التي ارتبطت بشكل واسع بأماكن كـــ: باريس (أعمال "بيغو" المستوحاة من أعمال "بورديو") وكوبنهاغن (الأمننة) وتحديها للنقاش الأمني المهيمن في مراكز البحث الأمريكية المقتصر على النظريات الواقعية (الهجومية/الدفاعية) ومدرسة "أبريستويث" أوما يعرف بمدرسة "ويلز"، فالمقاربات الأوروبية الجديدة تشترك حسب "أولي ويفر" في الفرضيات التالية: [3]

- إعادة التفكير في مفهوم الأمن.
- الاهتمام بمسألة إمكانية توسيع وتعميق قطاعات ومرجعيات الأمن.
- الأمن كممارسة.
- الانعكاس الذاتي للمحلل الأمني واعتماده على الممارسة/الفاعل الأمني خلال المعضلة المعيارية.

1- ديما الخضرا، مترجما، "نظريات العلاقات الدولية: التخصص والتنوع"، (الدوحة: المركز العربي للأبحاث ودراسة السياسات، 2016)، ص 173.

2- جويدة حمزاوي، "التصور الأمني الأوروبي: نحو بنية أمنية شاملة وهوية إستراتيجية في المتوسط"، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية، تخصص دراسات مغاربية ومتوسطية في التعاون والأمن، (جامعة: الحاج لخضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، 2011)، ص 20.

3- أمينة مصطفى دلة، "الدراسات الأمنية النقدية"، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية والعلاقات الدولية، تخصص دراسات إستراتيجية، (جامعة: الجزائر3، كلية العلوم السياسية والإعلام، قسم العلوم السياسية والعلاقات الدولية، 2013)، ص 51.

واستجابة لهذه التحولات سيتم التطرق إلى كل من مدرسة كوبنهاغن وتوسيعها للقطاعات والمرجعيات الأمنية واستخدامها لمتغير الأمننة كأداة جديدة في التحليل الأمني، وكذلك مدرسة باريس التي تنظر للأمن كتقنية حكومية ومهنيوا الأمن كفواعل والاعتماد على التكنولوجيا المتطورة في إدارة المخاطر.

المطلب الثاني: مدرسة كوبنهاغن

على غرار النقاشات النظرية لفترة ما بعد الحرب الباردة والتي نادت بضرورة توسيع الأجندة الأمنية تجاوبت مدرسة كوبنهاغن مع هذه التغيرات الدولية خاصة بعد ظهور العديد من التهديدات الأمنية الجديدة التي تميزت باختلافها عن الطابع التقليدي للتهديد الذي كان سائدا أثناء الحرب الباردة، بالإضافة إلى انتفاء سيطرة البعد العسكري على مجال الدراسات الأمنية.[1]

ساهمت مدرسة كوبن هاغن في توسيع وتعميق مضامين الأمن من خلال أعمال "باري بوزان" في كتابة (People, States and fear) سنة 1983م، الذي سعى إلى توسيع مجال البحث في قطاعات أخرى غير العسكرية تتمثل في القطاع السياسي، القطاع الاقتصادي، القطاع المجتمعي والقطاع البيئي، بالإضافة إلى إسهامات المدرسة في مفهوم الأمن المجتمعي ونظرية الأمننة.

يرى "ميشال ويليامز" أن مدرسة كوبنهاغن تتبنى شكلا من أشكال البنائية الاجتماعية ولها جذور في النهج التقليدي الواقعي.[2]

تعد نظرية الأمننة (Securitization) من أهم الإسهامات النظرية للمدرسة حيث طورها "أولي ويفر" "Ole Waever"، ترى هذه النظرية أن الأمن لا يتم التعامل معه كشرط موضوعي لكن بوصفه نتيجة عملية اجتماعية محددة، وقد حدد "ويليامز" السياق الفكري لنظرية الأمننة فيقول بأنها: "تدمج بين أفكار الواقعية الكلاسيكية المتأثرة بأعمال "كارل شميت" وأفكار البنائية الأخلاقية".[3]

فحسب "أولي ويفر" الأمن يفهم كفاعل خطابي فهويعني اعتبار شيء ما كقضية أمنية يكسبها ذلك الإحساس بالأهمية والاستعجال الذي يضفي الشرعية لاستخدام الإجراءات الخاصة خارج العملية السياسية المعتادة للتعامل معه.

1- أمينة دير، "**أثر التهديدات البيئية على واقع الأمن الإنساني في إفريقيا: دراسة حالة دول القرن الإفريقي**"، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية والعلاقات الدولية، تخصص علاقات دولية وإستراتيجية، (جامعة: محمد خيضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، 2014)، ص 18.

2- **المكان نفسه.**

3- **المكان نفسه.**

إذا فالأمننة كعملية يتم فيها تحويل المشاكل إلى قضايا أمنية من خلال إضفاء الطابع الأمني عليها، تفترض أن الأمن يمكن أن يفهم على أنه نتيجة لأعمال خطاب (Speech Act)، أي عملية الاستخدام المتكرر لإظهار حدث ما على أنه تهديد وجودي من خلال لغة خطابية موجهة للجمهور العام تقدم من خلالها هذه القضية على أنها تمس المادي والمعنوي وتتطلب إجراءات استثنائية مستعجلة لتشريع الأفعال خارج العملية السياسية المعتادة، ويرى "بوزان" أن فواعل الأمننة (Securiting Actors) الأكثر شيوعا قد تكون حكومات، قادة سياسيين، لوبيات، جماعات ضغط، والحجة الرئيسية لنظرية الأمننة هوأن الأمن عبارة عن فعل كلام، حيث تصبح المشكلة الأمنية مهددة لوجود الدولة يستدعي ذلك اتخاذ تدابير إستثنائية لضمان بقاء الدولة، وذلك بتشريع الأفعال وانتقالها من مجال السياسة العامة إلى عالم السياسة الطارئة، وبالتالي يمكن التعامل مع المشكلة الأمنية بسرعة واتخاذ إجراءات إستعجالية اعتمادا على مجموعة من القواعد واللوائح لصنع السياسات لهذا الأمن.[1]

وحسب "باري بوزان" يكون ذلك من خلال إتباع ثلاث خطوات هي:

- تحديد التهديدات الموجودة.
- إعلان حالة الطوارئ.
- التأثير على العلاقات بين الوحدات عن طريق كسر القواعد.[2]

المطلب الثالث: مدرسة باريس

مع بداية التسعينات من القرن العشرين كان البناء السياسي للأمن محل اهتمام عدد من باحثي تحليل الممارسات الشرطية (أجهزة الرقابة والضبط الاجتماعي)، يعتبر تشكيل الأمن الداخلي أكثر الموضوعات تناولا في الأجندة البحثية المستندة إلى منظورات علم الاجتماع السياسي والنظرية السياسية، قدم هؤلاء الباحثون أجندة ترتكز على مهني الأمن (Security Professional)؛ أي العاملين في الأمن مثل: الجنود، الخبراء والعقلانية الأمنية وتأثيرات التنظيم السياسي للتقنية والمعرفة الأمنية.[3] اذن فمدرسة باريس من اهم المدارس التي تطرقت الى الامن من جانب تقني وهذا ما ينطق تمام مع موضوع دراستنا.

1- أمينة دير، **المرجع السابق**، ص 19.

2- Rita Taureck, **"Securitization Theory and Securitization Studies"**, (university of institutional repository, 2006), p 03.

3- سيد أحمد قوجيلي، **"تطور الدراسات الأمنية ومعضلة التطبيق في العالم العربي"**، (أبوظبي: مركز الإمارات للدراسات والبحوث الإستراتيجية، 2012)، ص 32.

تقوم مقاربة مدرسة باريس بتعديل المنظور السائد للأمن عبر ثلاثة طرق، أولا بدلا من تحليل الأمن كمفهوم حتمي تقترح مدرسة باريس معالجة الأمن باعتباره تقنية حكومية (Technique Government)، ثانيا بدلا من التحقيق في النوايا الكامنة وراء استخدام القوة تركز هذه المقاربة على تأثيرات ألعاب القوة (Power) (Games، ثالثا بدلا من التركيز على أفعال الكلام (Speech Acts) تؤكد على الممارسات والسياقات التي تسعى إلى تشجع أوتعميق إنتاج أشكال محددة من الحوكمة.[1]

على عكس المدارس السابقة يعود مصدر المنظور المقترح من قبل مدرسة باريس ليس إلى تغير الموضوع المرجع بقدر ما يعود إلى تغير طبيعة التهديد والطريقة الملائمة لمواجهته.

أدت الطبيعة الجديدة والمتغيرة للتهديدات إلى إظهار مدى ترابط واعتمادية العديد من المهن المختلفة التي قد تؤدي دورا فعالا في المهام الأمنية، قد تشمل هذه المهن: الاستخبارات، مكافحة التجسس وتكنولوجيا المعلومات ونظم مراقبة المسافات الطويلة، وكشف أنشطة حفظ النظام وإعادة إرسائه، كل هذه المهن كما يؤكد "ديديه بيجو" تتقاسم المنطق أوالخبرة والممارسة ذاتها كما تتلاقى في وظيفة واحدة تحت عنوان الأمن.[2]

الأمن في مدرسة باريس نمط من أنماط الحوكمة يختزل في ممارسة الشرطية عبر تقنيات المراقبة تعمل الشرطية عبر شبكات تجسد روابط بين مختلف المؤسسات الأمنية الوظيفية التي تتجاوز الحدود الوطنية، وفي عالم معولم أصبحت أنشطة الشرطة أكثر اتساعا، هذه الأنشطة تتم على مساحة تتجاوز الحدود الوطنية كما تتجاوز أيضا في طابعها بعض أنشطة الشرطة التقليدية وتصل إلى الأنشطة الخارجية.

تعتبر فكرة المراقبة أوالعين الإلكترونية حسب "دايفيد ليون" تجسيدا معاصرا لفكرة البانوبتية عند "فوكو" الفكرة الأساسية هنا أن السلطة يجب أن تكون منظورة وغير ملموسة، تتخذ هذه البانوبتية في مجتمعنا المعاصر أشكالا عديدة: استخبارات الإتصالات، الاستخبارات الإلكترونية، استخبارات الرادار واستخبارات الصور، كلها تعمل تحت علامة الاستخبارات التقنية التي تشكل نظاما جديدا للقوة في العلاقات الدولية.[3]

1- سيد أحمد قوجيلي، **المرجع السابق**، 32.

2- **المرجع نفسه**، ص 33.

3- **المرجع نفسه**، ص 34.

خلاصة الفصل

تقتضي الدراسة في الأساس الإحاطة بالجانب المفاهيمي والنظري للموضوع المراد دراسته من خلال ضبط المفاهيم الأساسية التي أثارت جدالا واسعا بسبب غموضها، ويرجع ذلك بصفة عامة لخضوعها للتحولات والتغيرات التي شهدتها الساحة الدولية، ويأتي في مقدمة هذه المفاهيم مفهوم الإستراتيجية بتعريفاتها التقليدية والتي تركز على المجال العسكري وبفن الحرب وعلمها ليتوسع هذا المفهوم إلى مجالات أخرى نتيجة تطور الوسائل المستخدمة في العلاقات بين الدول.

ويعتبر مفهوم الأمن السيبراني من أكثر المفاهيم المثيرة للاهتمام والذي يعبر عن الوسائل الدفاعية والسياسات التي تتبعها الدول من أجل الحد من خطر التهديدات السيبرانية.

أن التطورات الحاصلة في مجال المعلومات والتكنولوجيا ساهم في بروز تهديدات أصبحت تشكل هاجسا أمنيا أمام الدول تحتم عليها مواجهتها وإتباع إستراتيجيات للوقاية منها، أدى ذلك إلى تنوع مصادر هذه التهديدات وهي بدورها أخذت أشكالا مختلفة تهدف إلى إلحاق الضرر والتخريب والقضاء على النظام المعلوماتي الإلكتروني ككل.

من بين أهم المقاربات النظرية التي يمكن بها تفسير توجيه دولة ما لإستراتيجيتها لمواجهة التهديدات السيبرانية:

– ترى النظرية الواقعية أن على الدول حماية أمنها الوطني من أي تهديد باعتبار الدولة المرجعية الأساسية واعتبار الأمن من صميم اهتمامات وصلاحيات الدول.

– وابتعاداً عن المجال العسكري تجاوبت مدرسة كوبن هاغن مع التغيرات الدولية خاصة بعد ظهور العديد من التهديدات الأمنية الجديدة، حيث ساهمت في توسيع وتعميق مفهوم الأمن وتعتبر نظرية الأمننة من أبرز إسهامات مدرسة كوبن هاغن التي تتطلب إجراءات إستثنائية للتعامل مع المشكلة الأمنية.

– اعتبار الأمن تقنية حكومية واعتماد تقنيات المراقبة والتكنولوجيا المتطورة التي تقوم على فاعلية الممارسات الشرطية هي الأسس التي تقوم عليها مدرسة باريس لتحديد طبيعة التهديد وإدارة المخاطر.

الفصل الثاني:

الجريمة السيبرانية في الاستراتيجيات الدولية

تمهيد:

دخل العالم مرحلة جديدة فقد أصبح العالم قرية صغيرة وذلك راجع للتطور الكبير الذي حدث في عالم تكنولوجيا الاتصال، فقد انشات فضاءات جديدة للتعامل بين الدول، ومع هذا التطور ظهرت كذلك العديد من التهديدات الجديد داخل هذا الفضاء متمثلة في الجرائم السيبرانية بمختلف أنواعها (القرصنة، التجسس، السرقة) لكن الدول وضعت العديد من الاستراتيجيات لمواجهتها، بالإضافة إلى العديد من التشريعات القانونية وكل ذلك للتقليل من أضرار هذه الجرائم.

لذلك قمنا بتقسيم هذا الفصل إلى المباحث التالية:

- ✓ **المبحث الأول: الجريمة السيبرانية في القانون الدولي.**
- ✓ **المبحث الثاني مكافحة الجريمة السيبرانية في الإستراتيجية الأمريكية والروسية.**
- ✓ **المبحث الثالث: واقع الجريمة السيبرانية في الدول العربية وسبل مكافحتها.**

المبحث الأول: الجريمة السيبرانية في القانون الدولي

تشكل الجهود التي سعت إليها الدول ومختلف المنظمات العالمية من خلال التنسيق بين مختلف الوسائط التقنية والأكاديمية، وتكثيف آليات الاتصال والتعاون من خلال وضح استراتيجيات مختلفة لمواجهة التهديدات السيبرانية في نطاق ومسؤولية كل طرف وضرورة مراقبة استخدام تكنولوجيا المعلومات والاتصالات، في ظل انكشاف العالم على بعضه، حيث كانت الاتفاقية بشأن الجريمة السيبرانية* التي أبرمها مجلس أوروبا (واعتمدت في بروكسيل يوم 23 نوفمبر 2001) هي أول اتفاقية توضع للتعاطي مع الطابع الدولي للجريمة السيبرانية ودخلت تلك الاتفاقية حيز السريان في يوليو (في أعقاب التصديق عليها من جانب خمسة بلدان موقعة، كان من الضروري لثلاثة بلدان منها أن تكون من مجلس أوروبا). وتضم الاتفاقية النقاط التالية: [1]

المطلب الأول: الآليات الدولية لمواجة الجريمة السيبرانية

ويمكن توضيح أهم هذه الآليات وفقا لما يلي:

1- القانون الجنائي الأساسي

- المخالفات التي ترتكب ضد السرية، والسلامة والتوافر الخاص ببيانات ونظم الحاسوب
- المخالفات ذات الصلة بالحاسوب
- المخالفات ذات الصلة بمخالفات حقوق التأليف والنشر والحقوق ذات الصلة.

1-1- قانون الإجراءات:

- المحافظة المسرعة على بيانات الحاسوب وحركة البيانات والإفشاء السريع للأخيرة للسلطات المختصة
- حفظ وصيانة سلامة بيانات الحاسوب لفترة من الوقت تمتد حسب الضرورة وذلك لتمكين السلطات المختصة من طلب إشهارها.
- أمر الإنتاج

*الجريمة السيبرانية: **هي** مخالفة ترتكب ضد أفراد أو جماعات بدافع جرمي و نية الإساءة لسمعة الضحية أو لجسدها أو عقليتها، سواءً كان ذلك بطريقة مباشرة أو غير مباشرة، وأن يتم ذلك باستخدام وسائل الاتصالات الحديثة مثل الإنترنت غرف الدردشة أو البريد الإلكتروني أو المجموعات.

[1]- حسن بن أحمد الشهري،"**الإرهاب الالكتروني، حرب الشبكات**"، المجلة العربية الدولية للمعلوماتية، 2015، ص 19.

– البحث عن بيانات الحاسوب المختزنة والإمساك بها.

– جميع بيانات الحاسوب في الزمن الحقيقي.

– الحماية الكافية لحقوق الإنسان والحريات.

– وينبغي لكل دولة أن تعتمد التدابير التشريعية وغيرها من التدابير الضرورية لفرض ولايتها القضائية على المخالفات التالية ودون الإضرار بقانونها المحلي: [1]

– عندما يحدث عن قصد النفاذ إلى كل أو إلى أي جزء من النظام الحاسوبي بدون وجه حق.

– عندما يحدث عن قصد الاعتراض بدون وجه حق لعمليات إرسال البيانات غير العامة إلى أو من النظام حاسوبي أو داخله.

– عندما يحدث عن قصد، إتلاف، شطب، تدهور، أو تغيير أو كبت بيانات حاسوبية بدون وجه حق.

– عندما تحدث عن قصد، إعاقة خطيرة لأداء نظام بدون وجه حق.

– إنتاج، بيع، الشراء للاستخدام، استيراد، توزيع أو توفير البيانات بطرق أخرى لأداة مصممة أو مجهزة لغرض اقتراف أي من هذه المخالفات.

– عندما يحدث عن قصد وبدون قصد وجه حق، إدخال، تغيير، شطب أو كبت بيانات حاسوبية مما ينتج عنه بيانات غير يقينية وذلك بغرض النظر فيها، أو العمل على أساسها لأغراض قانونية كما لو كانت بيانات يقينية.

– عندما يحدث عن قصد وبدون وجه حق، التسبب في فقدان شيء مملوك لشخص آخر عن طريق أي مدخل تغيير، شطب أو كبت لبيانات حاسوبية، أي تدخل في أداء نظام حاسوبي بنية مخادعة أو غير شريفة للحصول بدون وجه حق، على منفعة اقتصادية للشخص أو لشخص آخر.

– التكييف كمخالفات جنائية مساعدة أو المساعدة على ارتكاب أي من تلك المخالفات، وكذلك أي محاولة لاقتراف أي من هذه المخالفات.

– وينبغي لكل طرف من الأطراف الموقعة أن يثبت ولايته القضائية على أي مخالفة تقترف:

[1] – حسن بن أحمد الشهري، **المرجع السابق**، ص 19.

– على يد أي من رعاياها، إذا كانت المخالفة يعاقب عليها جنائيا في مكان ارتكابها، أو إذا ارتكبت المخالفة خارج الولاية القضائية الإقليمية لأي دولة.[1]

1-2- قواعد التعاون الدولي المتصلة بـــ:

– تسليم المجرمين.

– المساعدة المتبادلة لأغراض التحقيق.

– الإجراءات الخاصة بالأعمال الجنائية ذات الصلة بنظم الحاسوب والبيانات.

– جمع القرائن الإلكترونية للعمل الإجرامي.

– خلق شبكة مساعدة متبادلة:

– متوافرة على مدار 24 ساعة/7 أيام في الأسبوع.

– ذات مراكز اتصال وطنية.

– بمساعدة فورية في حالة وقوع المخالفات.

تسود الإدارة السياسية للتعامل مع الجريمة السيبرانية على المستوى الدولي، وليست المشكلة هي دائما عدم وجود القوانين أو المبادئ التوجيهية كتلك التي أعلنتها منظمة التعاون والتنمية في الميدان الاقتصادي في عبارة "المبادئ التوجيهية لمنظمة التعاون والتنمية في الميدان الاقتصادي لأمن شبكات ونظم المعلومات- نحو ثقافة أمنية- 2002" (الجدول 1)، وإنما هي صعوبة وتعقد المهمة، والموارد الضرورية لتنفيذ أهداف النضال ليس فقط لمكافحة الجريمة السيبرانية وإنما أيضا الجريمة المنظمة التي تسفر عن تسخير شبكة المعلومات الدولية في أغراض خبيثة. [2]

[1]- حسن بن أحمد الشهري، **المرجع السابق**، ص 20.

[2]- حمدون تورين، **"دليل الأمن السيبراني للبلدان النامية"**، (الاتحاد الدولي للاتصالات، د.ب 2006)، جنيف، ص ص: 19-21.

الجدول1: مبادئ منظمة التعاون والتنمية في الميدان الاقتصادي بشأن أمن المعلومات

الوعي	جميع المشاركين مسؤولون عن أمن الشبكات ونظم المعلومات
المسؤولية	جميع الضالعين يشتركون في أمن النظم وشبكات المعلومات
الاستجابة	يجب على المشاركين العمل بصورة متعاونة ومنسقة زمنيا لمنع واكتشاف حوادث الأمن
الأخلاقيات	ينبغي للمشاركين احترام المصالح المشروعة للآخرين
الديمقراطية	ينبغي لأمن نظم وشبكات المعلومات أن يكون متوافقا مع القيم الأساسية للمجتمع الديمقراطي
تقييم المخاطر	ينبغي للمشاركين إجراء تقييمات للمخاطر
تصميم الأمن والتنفيذ	ينبغي للمشاركين إدراج الأمن كعنصر أساسي في نظم وشبكات المعلومات
إدارة الأمن	ينبغي للمشاركين اعتماد نهج شامل تجاه إدارة الأمن
إعادة التقييم	ينبغي للمشاركين استعراض، وإعادة تقييم أمن نظم وشبكات المعلومات، وإدخال التعديلات المناسبة على السياسات العامة للأمن وممارساته وإجراءاته وتدابيره.

المصدر: حمدون تورين، **"دليل الأمن السيبراني للبلدان النامية"**، (الاتحاد الدولي للاتصالات، د.ب 2006) ص 21.

2- على المستوى العربي

فالتشريع العربي بشأن الجريمة السيبرانيةة وضع نموذج لمكافحة جرائم تقنية أنظمة المعلوماتية والذي صادق عليه مجلس وزراء العدل العرب في2003/10/08 في دورته التاسع عشر:[1]

وقد جاء هذا القانون بجملة من الأحكام الموضوعية والإجرائية تعمل على الحد من الجريمة المعلوماتية.

واعتمد القانون في مجال الاختصاص على مبدأ العينية وفقا للمادة 26 التي تنص على أنه (تسري أحكام هذا القانون على أيا من جرائم المنصوص عليها فيه ولو ارتكبت كليا أو جزئيا خارج إقليم الدولة متى أضرت بإحدى مصالحها ويختص القضاء الوطني بنظر الدعاوى المترتبة عليه)

ومن خلال النص نلاحظ أن القانون أخذ بمبدأ العينية باعتماده على المصلحة الوطنية كمعيار أساسي لثبوت الاختصاص و بالتالي تطبيق القانون الجنائي الوطني.

كما نلاحظ أن هذا القانون لم يعين أي جهة تتولى عملية الضبط القضائي في جرائم المعلوماتية مما يعني ترك المجال مفتوحا للدول العربية من خلال إعطاء تلك السلطة لأي هيئة أو جهة تراها قادرة على اكتشاف ومتابعة تلك الجرائم.

المطلب الثاني: المساعي الدولية لمواجهة الجريمة السيبرانية.

إن الأطروحات الجديدة للأمن تستوجب علينا التوقف والتمعن في هذا المفهوم بما ينسجم والتغيرات الحاصلة في العالم لاسيما في ظل التطور الرهيب في مجال الإعلام الآلي وتكنولوجيا الاتصالات والمعلومات، إلى حد التوجه إلى إنشاء ما اصطلح على تسميته بالمدن الذكية، والتي تحولت فيها الخدمات من الشكل التقليدي إلى الالكتروني ، لتخلق بذلك ميدانا جديدا يختلف عن سابقيه، وعلى الرغم من ايجابياته إلا انه يستلزم توفير الأمن لنجاح هذه الخدمات. [2]

[1]- "**الجرائم الإلكترونية، وآفاق النمو المتسارع، المركز العربي للبحوث والدراسات**"، 2018، تاريخ التصفح: 01-04-2020، من الرابط https://www.google.com/url?sa

[2]- عادل عبد الصادق، "**أسلحة الفضاء الالكتروني في ضوء القانون الدولي**"، سلسلة أوراق ، العدد 23، مكتبة الإسكندرية، 2016، ص 64.

1- الحد من سباق التسلح السيبراني.

يلعب التسليح دورا هام في الإستراتيجية في توازن القوى على المستوى العالمي في ظل بيئة يسودها الشك وعدم اليقين، وهو ما يحمل خطورة عسكرة الفضاء السيبراني، وتتبنى عديد الدول إستراتيجية الحرب السيبرانية كحرب للمستقبل، لقد بدأ سباق تسلح خطير لتطوير الأسلحة السيبرانية، كانت بداية ظهوره (يعتبر المختصون هذه الأسلحة السيبرانية بدائية في الصراع الروسي – الاستوني، والروسي – الجورجي، والتطور البارز مع فيروس "ستاكست" الموجه ضد البرنامج النووي الإيراني والذي يتهم بتطويره كل من إسرائيل والولايات المتحدة.

واتجهت الدول لتعزيز قدراتها السيبرانية سواء في مجال الدفاع والردع أو الهجوم، بالإضافة إلى حماية بنيتها القومية للمعلومات وذلك من خلال العمل على تحقيق النفوق التقني. وعليه فان المشكلة في سباق التسلح السيبراني تكمن في تحديد ماهية تلك الأسلحة. [1]

وفي المجال السيبراني اقترحت روسيا في عام 1999، معاهدة للأمم المتحدة لحظر الأسلحة الالكترونية والمعلوماتية (بما في ذلك الدعاية). قومت الولايات المتحدة ما اعتبرته محاولة للحد من القدرات الأمريكية، ولا تزال تعتبر هذه المعاهدة عامة مظلة لا يمكن التحقق منها. وبدلا من ذلك اتفقت الولايات المتحدة وروسيا و13 دولة أخرى على أن يعين الأمين العام للأمم المتحدة مجموعة من الخبراء الحكوميين التي اجتمعت أولا في عام 2004.

وقد أسفرت تلك المجموعة في البداية عن نتائج هزيلة، ولكن بحلول جوان 2015 أصدرت تقريرا أقرته مجموعة العشرين، يقضي بوضع معايير مقترحة لبناء الثقة. [2]

وعلى الرغم من صعوبة عملية الرقابة والتفتيش على الأسلحة السيبرانية، فان السعي نحو الحد من انتشار هذه الأسلحة، يتطلب وجود إطار دولي تتشارك فيه العديد من الدول الجماعات عبر العالم، إلى جانب وجود

---

[1] - **المكان نفسه.**

[2] - جوزيف، س ناي، "**التحكم في الصراع الليبراني**"، مدونات الجزيرة على الرابط:
http://blogs.aljazeera.net/blogs (20/04/2020)،

الإطار القانوني الدولي الذي يحدد الالتزامات والواجبات لجميع الفاعلين، وان أي اتفاق من شانه تنظيم الاستخدام العسكري للفضاء السيبراني، يجب أن يعمل على منع نشر الأسلحة السيبرانية في وقت السلم .

إن الاعتداءات السيبرانية أخذت أبعاد عالمية ودولية، فبفضل ذلك ازداد الاهتمام بالتعاون الدولي من أجل مكافحتها وإدارة هذه التهديدات، وبذلك ظهرت فكرة لحماية الفضاء السيبراني ومواجهة المخاطر من التجمع الدولي للعلماء الذي أشار إلى هذا التعاون كنظام دولي للفضاء السيبراني يعمل على جميع مسائل الجريمة بما فيها الحرب السيبرانية وقد قادت الأمم المتحدة هذه الجهود سواء عبر إقراراها تنظيم القمة العالمية لمجتمع المعلومات أو إنشائها مجموعات عمل لمكافحة الجريمة السيبرانية.[1]

لعبت القرارات الصادرة عن الهيئة العامة للأمم المتحدة حول الأمن السيبراني وتقنيات المعلومات دور في جذب انتباه الدول الأعضاء من أجل إدراك مدى خطورة هذه التهديدات وسجلت حركة ناشطة لعدد من الأجهزة والإدارات وفرق العمل التابعة للأمم المتحدة في هذا المجال على مستويات عدة حيث يدعم مكتب مكافحة الجريمة والمخدرات جهود الأمم المتحدة في مجال تعزيز السلام، كما تهتم منظمة الجمارك العالمية بالترويج لاستراتيجيات حماية البنية التحتية الحرجة. والتي هي تعتبر نقطة قوة وضعف للدولة فإذا تم اختراقها سوف يؤثر ذلك على أمن الدول وزعزعة استقرارها. بينما تهتم اللجنة الاقتصادية والاجتماعية على تحسين تبادل المعلومات والممارسات الفضلى والتدريب على مكافحة الاستخدام الجرمي للشبكة.[2]

كذلك أصدرت الهيئة العامة للأمم المتحدة قرار حول ضرورة نشر ثقافة الأمن السيبراني وضرورة زيادة الوعي والمسؤولية لدى الدول بما يكفل ويضمن التعاون لمنع ورصد ومعالجة الحوادث السيبرانية.

وبدأ اهتمام الدول بالتعاون واضحا من خلال مشاركتها في أعمال الجمعية العامة للأمم المتحدة التي ضمن 193 دولة. والتي أصدرت عددا من القرارات التي يمكن إعتبارها قاعدة لانطلاق الجهود في مكافحة الجريمة السيبرانية، ونذكر هنا قرار أُصدر عام 1990 م حول قانون جرائم المعلوماتية، وأصدرت قرارا خاصا حول الأمن السيبراني عام 2003م ركز على القدرة على مكافحة الجريمة السيبرانية، ومن ثم أُصدرت قرارات حول الموضوع نفسه عام 2010 ملحقا حول ضرورة أن تلجأ الدول إلى إجراء تقييم ذاتي بمحض

[1] – عادل عبد الصادق، **المرجع السابق**، ص 69.

[2] – جوزيف ناي، **الموقع السابق**.

إرادتها لمعرفة مدى تناسب أطرها التشريعية وقدرتها على مكافحة الجريمة السيبرانية على ضوء التطورات السريعة الحاصلة في مجال تقنيات المعلومات والاتصالات، كذلك بذلت جهود عدة من قبل مجموعات متخصصة بدعم من الاتحاد الدولي للاتصالات حيث برزت الحاجة إلى تعاون الدول، وكانت روسيا قد أعدت مسودة عدد من القرارات وقدمتها إلى الأمم المتحدة لإقرار اتفاقية السيبرانية لكن هذه الاقتراحات لم تقرر. [1]

فجملة هذه التوصيات والجهود الدولية سواء منها تلك التي صدرت عن القمة العالمية أو عن المنتديات الدولية لحوكمة الأنترنت غير كافية بالرغم من وزنها سياسيا وإعلاميا على المستوى الدولي وعدم فاعليتها تعود لعدم إلزاميتها القانونية. وعدم إمكانيتها العقابية في حل المخالفات. فهذه التوصيات والقوانين صدر عن الهواة الرقمية (الهكرز Hackers)، وتزايد مفاجئ في اتساعها بين الدول والدعوة إلى ضرورة التعاون بين الدول التي لها قدرات وإمكانيات كبيرة على مستوى التقنيات والقدرات والخبرات مع الدول التي تملك قدرة محدودة في الإمكانيات التقنية وسبب محدودية القدرة في هذه الإمكانيات سمح بتزايد مجموعات الهواة الرقمية على هذه الدول ومنعها من الحفاظ على أمن فضائها السيبراني وبناء الثقة فيه. [2]

وعليه يبدوا التوصل إلى قرار نظام عالمي اليوم وفي المستقبل القريب بعيد المنال، فكيف يمكن لجميع دول العالم وإن اتفقت في إطار الأمم المتحدة على مكافحة الجريمة السيبرانية أن تتفق على تحديد واحد للأعمال السيبرانية غير الشرعية والشرعية سواء منها تلك التي تقوم بها الدول أم تلك التي يقوم بها الأفراد

2- قانون تالين Tallinn Law

تم إبرام نص قانوني عام 2013 يدعى "دليل تالين" (Tallinn Manual)، الذي أعدته مجموعة من خبراء القانون الدولي بدعوة من حلف شمال الأطلسي (NATO) وكذا قصور القانون الدولي والتشريعات الدولية في هذا المجال، ومن جهة أخرى عدم وجود أي أساس قانوني ينظم اللجوء إلى الحروب

[1] - المرجع نفسه.

[2] - المكان نفسه.

السيبرانية، وتم إبرام هذا القانون من اجل دراسة مدى إمكانية مدى تطبيق قواعد القانون الدولي الإنساني على الحروب السيبرانية وذلك اثر الهجوم السيبراني الشامل الذي شنته روسيا ضد استونيا عام 2007.[1]

ويحتوي دليل "تالين" على 95 قاعدة وتتمثل تحدياته الرئيسية في ضمان توجيه الهجمات ضد الأهداف العسكرية فقط.[2]

ويجيب دليل "تالين" على أهم النقاط الحساسة ذات الصلة بالحروب والهجمات السيبرانية كمفهوم النظام النزاع المسلح في إطار الحرب السيبرانية ومفهوم الجيوش السيبرانية، وكيفية إدارة الحبر السيبرانية من خلال قواعد الاشتباك السيبراني. وصفة المقاتلي السيبراني، إضافة إلى إمكانية مراعاة القانون الدولي الإنساني المعروفة كمبدأ التميز، ومدى شرعية استهداف المقاتل السيبراني بالوسائل العسكرية المايدة كالطائرات العسكرية بدون طيار.

يعتبر التعاون بين الدول، بشكل عام والتعاون الإقليمي بشكل خاص، عن طريق إقرار الاتفاقيات الإقليمية. أداة لتحفيز الحوار السياسي وحفظ الاستقرار وتنفيذ المشاريع الإقليمية، وتلبية احتياجات البلدان الشريكة، وتطوير القدرات والإمكانيات ومعالجة المشاكل والأولويات الخاصة بدول تتشارك إقليما وجغرافيا أو ثقافيا أو سياسية، ويهتم هذا التعاون بدراسة من إيجاد حلول للهموم وقضايا مختلفة المجالات (الأمنية، النقل، والموارد المائية والكهربائية والاقتصادية ...).

[1] – سعيد درويس، **"ماهية الحروب الالكترونية في ضوء قواعد القانون الدولي"**، حوليات جامعة الجزائر 1، العدد 29، ص 119.

[2] – اللجنة الدولية للصليب الأحمر، **"ماهية القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟"**، على الرابط:
http://accronline.com/article_detail.aspx?id=28958.(22/04/2020)

المبحث الثاني مكافحة الجريمة السيبرانية في الإستراتيجية الأمريكية والروسية.

مع تطور المعلومات وظهور الجريمة السيبرانية سارعت الدول لإيجاد استراتيجيات لمواجهة هذا التهديد الجديد.

المطلب الأول: الجريمة السيبرانية في الإستراتيجية الأمريكية.

كانت الولايات المتحدة من أوائل الدول التي بدأت في التعامل مع الأمن السيبراني كمهمة ذات أهمية إستراتيجية وذلك لتفادي التهديد المتنامي للاقتصاد المعتمد وبشكل متزايد على تكنولوجيا المعلومات والاتصالات مما أجبر الإدارة الرئاسية الأمريكية على العمل لتوفير الدفاعات السيبرانية وعلى إعادة تحديد مهمة ضمان أمن مرافق البنية التحتية الحيوية وكانت هناك حاجة إلى نهج متكامل فتمت صياغته في عام 2003 م بموجب إستراتيجية شاملة عرفت باسم " الإستراتيجية الوطنية لحماية الفضاء السيبراني" ووفقاً لها تم توزيع المسؤولية عن ضمان أمن الفضاء السيبراني بين الوكالات والوزارات الاتحادية وأصبحت وزارة الأمن الداخلي بالولايات المتحدة هي السلطة المنسقة, ووفقاً لفحوى الإستراتيجية قامت وزارة الدفاع الأمريكية ووكالات إنفاذ القانون بتطوير أنظمة الكشف عن التهديدات والهجمات السيبرانية لضمان الاستجابة الفعالة في الوقت المناسب بينما تقوم وزارة الخارجية بتطوير التعاون في جميع قضايا الأمن السيبراني على الساحة الدولية وتشدد لحماية فضاءها السيبراني عبر الحاجة إلى محورة بيئة دولية متعاونة على الأقل فيما بين الدول التي تتقاسم رؤية مشتركة حول عدد من القضايا كالمعايير التقنية والمعايير القانونية المقبولة بشأن الولاية الإقليمية والمسؤولية السيادية واستخدام القوة. وبدأت في عام 2008م مرحلة انتقالية جديدة في تطوير نظام الأمن السيبراني وكان الهدف من ذلك هو القضاء على المشاكل السيبرانية المتأصلة في النظام وبدأ تنفيذها بشكل معدّل ومعتدل قليلاً.[1]

وما إن أعلنت الإدارة الأمريكية أن أمن الفضاء السيبراني أحد أهم مهام الدولة حتى كان عليها مواجهة التحدي الآخر وهو تطوير الفرص الجديدة التي يوفرها الفضاء السيبراني لاستخدامها لأجل المصلحة الوطنية

[1] – ميثاق بيات ألضيفي، أمريكا والإستراتيجية السيبرانية، تصفح: (02/05/2020) متاح على الرابط :
https://m.annabaa.org/arabic/informatics/17712

ولذا تم تطوير " استعراض سياسة الفضاء الإلكتروني " والتي لا تحتوي فقط على تحليل لنظام الأمن السيبراني الحالي وإنما أيضًا على خطة لتحولها بهدف توفير دفاع إلكتروني أكثر ملائمة للولايات المتحدة وأُخذ الأساس الشامل لمبادرة الأمن السيبراني الوطني كأساس وتمت مراجعتها واستكمالها بشكل كبير باعتبارها واحدة من المشاكل الرئيسة وليتم تحديد التجزئة المستمرة لنظام الأمن السيبراني ولتوزيع المسؤوليات والمهام بين الوكالات والإدارات الاتحادية لتطوير النظام ولإنشاء موقف منسق سياسة الأمن السيبراني للدولة ما يسمى بالملك السيبراني. [1]

واعتمدت الإستراتيجية على مبدأ التقييس والمبادئ التوجيهية العامة والتي بموجبها توجب على رأس المال الخاص ضمان أمنها السيبراني والتركيز على تطوير الإمكانات البشرية ومحو الأمية الحاسوبية للسكان لكن التحرك الأكبر لها كان عبر تطوير التعاون في قضايا الأمن السيبراني على المستوى الدولي والذي أصبح العنصر المركزي لسياستها وضع" الاستراتيجية الدولية للفضاء السيبراني" في عام 2011م لإنشاء منصة موحدة للتفاعل الدولي بشأن قضايا الفضاء الإلكتروني لتعزيز سياسة الأمن السيبراني وإنشاء منصب منسق كبير على الإنترنت في وزارة الخارجية الأمريكية وكانت إحدى السمات المثيرة للاهتمام فيها هي ما يسمى "بناء القدرات" أي تقديم المساعدة إلى البلدان النامية من خلال توفير الموارد والمعارف والأخصائيين اللازمين بما في ذلك إعداد استراتيجيات الأمن السيبراني الوطنية.

لقد أصبحت الإستراتيجية الجديدة استمراراً منطقياً لسياسة السنوات الأخيرة وأول شيء يجذب الانتباه فيها هي تشكيل صورة تهديد خارجي للحرية والديمقراطية والتركيز على ضمان السلام بالقوة وإن إدارة مخاطر الأمن السيبراني لتحسين موثوقية واستدامة نظم المعلومات بما في ذلك المواقع الحساسة هي الهدف الرئيسي للدعامة الأولى في الإستراتيجية الجديدة التي تركز بضراوة على تحسين الأمن السيبراني في مجال النقل والبنية التحتية البحرية وكذلك في الفضاء ومع كل تحديث جديد لهذه القطاعات تصبح أكثر عرضة للهجمات السيبرانية ومن الأمور التي تثير القلق بشكل خاص سلامة النقل البحري إذ قد يؤدي التأخر في النقل أو إلغائه إلى تعطيل أداء الاقتصاد على المستويات الإستراتيجية وردا على ذلك توجب على الإدارة الأمريكية تقسيم

[1] – ميثاق بيات ألضيفي، **الموقع السابق**.

وتفعيل الأدوار والمسؤوليات الضرورية وتشجيع وتحسين الآليات المحفزة للتعاون الدولي وتبادل المعلومات والعمل على بلورة جيل جديد نابضا من البنية التحتية البحرية التي تقاوم التهديدات السيبرانية، ولذلك تعتبر الولايات المتحدة الوصول بحرية دون عوائق وحرية العمل في الفضاء عنصرا حيويا في ضمان أمنها وازدهارها الاقتصادي كما وتعتبر أيضا إن الأصول الفضائية والبنية التحتية الداعمة مهمة للغاية في مجالات الملاحة والاستطلاع والمراقبة والاتصالات والرصد, كما وانها تهدف إلى تكثيف الجهود لحماية الأصول الفضائية الحالية والمستقبلية ودعم البنية التحتية من التهديدات الإلكترونية المتطورة عبر التفاعل مع الصناعة والشركاء الدوليين.

ومن العناصر المهمة الأخرى في السياسة الموضحة في الإستراتيجية الجديدة هي تحديث التشريعات في مجال المراقبة الإلكترونية والجريمة الحاسوبية ومن المتأمل امريكيا تحديث التشريعات المتعلق بها لتوسيع قدرة وكالات إنفاذ القانون على جمع الأدلة اللازمة عن النشاط الإجرامي بصورة قانونية وإجراء مزيد من إجراءات التحقيق والقضاء التنفيذية وقد يتم جمع المعلومات الضرورية عن ذلك خارج أراضي الولايات المتحدة, ويتم التركيز بشكل كبير على الإستراتيجية على الإجراءات التي من شأنها أن تسهم في توسيع النفوذ الأمريكي في العالم وأحد هذه المجالات هو تطوير قدرات البلدان الشريكة لمواجهة الجريمة السيبرانية لتطوير التعاون الدولي في مجال مكافحة الجريمة السيبرانية وتطوير آليات متوافقة ومتبادلة المنفعة التي من شأنها تسهيل تبادل المعلومات وتعزيز استخدام الصكوك الدولية القائمة واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية وشبكة مجموعة السبعة ومراكز الاتصال التي تعمل على مدار متواصل، فإن الإدارة الأمريكية ستعمل على توسيع الإجماع الدولي لصالح الاتفاقية لتوسيع نفوذها وتعزيز التكنولوجيات الجديدة وتقديم المشورة بشأن نشر البنية التحتية وإدارة المخاطر والسياسات والمعايير لتوسيع تغطية الإنترنت والبرمجيات والأمن والاستقرار وإدخال معايير الخارجية الدراية والأمن السيبراني والتطورات التقنية الوطنية لا يمكن أن يؤدي إلا إلى فقدان السيادة التكنولوجية في هذا المجال الهام[1].

[1] - أميل أمين، " الأمن السيبراني العالمي... حروب خلفية ومساحات إرهابية "، تاريخ التصفح: (06/04/2020) متاح على الرابط : https://www.independentarabia.com/node/93586/

وتدرك الإدارة الأمريكية أن الفضاء السيبراني سيغير ميزان القوة الإستراتيجي وإن الفرص فيه سينظر إليها على أنها مرتبطة بعناصر أخرى من القوة الوطنية وبحملات الدعاية الخبيثة وحملات التضليل، وكانت قد أجرت وزارة الدفاع الأمريكية مراجعة شاملة للإستراتيجية العسكرية في مجال الفضاء السيبراني وإمكانيات وكانت النتيجة ظهور إستراتيجية سيبرانية جديدة لوزارة الدفاع تداخل العديد من عناصرها مع "إستراتيجية الإنترنت الوطنية" لتسريع تطوير القدرات السيبرانية الهادفة للقيام بعمليات قتالية مع الجهات الفاعلة الخبيثة في الفضاء السيبراني، ولذلك تركز استراتيجيات الأمن السيبراني الجديدة على تعزيز القوة وزيادة تأثير وتعزيز مصالح الولايات المتحدة في الساحة الدولية وفيما يتعلق بقواعد السلوك في الفضاء السيبراني التي طورتها مجموعة الخبراء الحكوميين للأمم المتحدة فستقوم بتعزيز هذه المعايير واستخدامها لمصلحتها. فلا تحدد الإستراتيجية خطط إنشاء آليات قانونية دولية بما يمكن أن تقوم بشكل مستقل وموضوعي وبكفاءة إجراء تحقيق مشروع واتخاذ قرار محكم بشأن الأعمال الكيدية في بيئات سيبرانية مما يعني أن الجناة السيبرانيين المزعومين معروفون بالفعل غير أنهم لا يخضعون لأية شكوك, كما لا تشير تلك الإستراتيجية إلى كيفية التغلب على الوضع الحالي للأزمات, لذا لابد أن نوضح بأن الانقسام بين الرؤية السيبرانية المؤيدة لأمريكا والرؤيا المؤيدة لإقرانها لا ينمو إلا نتيجة لما قد يؤدي ذلك إلى تجزئة المواجهات السيبرانية بينهما ويوزعها بين بيئات التكنولوجيا المعلومات والاتصالات والإنترنت.

المطلب الثاني: التغير والاستمرار في الإستراتيجية الروسية في المجال السيبراني.

لم تدشن روسيا قيادة عسكرية للفضاء السيبراني كما فعلت الولايات المتحدة، إلا أنها تعتمد على استراتيجيات جديدة لتعزيز قدراتها في مجال القوة السيبرانية ،وترتكز الرؤية الروسية على استخدام مصطلح "أمن المعلومات"كتعريف عن "الأمن السيبراني"،وذلك لأنها ترى انه مصطلح شامل يغطي الأمن السيبراني باعتباره جزء تابع له،وترى انه من الصعوبة ممارسة الدولة الرقابة والتنظيم الكامل للأمن السيبراني،وتسعى روسيا لبناء معايير دولية من خلال التعاون في الفضاء السيبراني،اما لتعزيز القدرات في مجال مواجهة التهديدات الداخلية لأمن المعلومات او مواجهة التهديدات الخارجية ،ومن ثم فان ابرز سمات الأمن السيبراني الروسي هو

تطبيق السيادة الوطنية على الفضاء السيبراني "'CyberSovereignty'" ،[1] لذا،فإن "السيادة السيبرانية"،ودور الدولة في مجال المعلومات والتنظيم والسيطرة،هي مرتكزات أساسية لإستراتيجية الأمن السيبراني الروسي.وهو ما يجعلها عامل معوق في بناء المعايير الدولية المتعلقة بالأمن السيبراني من وجهة نظر الدول الغربية .

بل وذكر هذا المنظور الروسي في العديد من الوثائق المعنية بعقيدة الاتحاد الروسي في "ضمان أمن المعلومات.والذي يظهر نية الحكومة الروسية لقيادة الجهود الدولية لتحقيق درجات عالية من الأمن،وذلك من خلال العديد من الطرق القانونية والمؤسسية والتكنولوجية وغيرها .[2]

وهو الأمر الذي يلاقي انتقادات حادة من قبل القوى الغربية مثل الولايات المتحدة،والتي ترى إنها تمارس سياسات استبدادية لقمع الحريات للمعارضة الروسية،وان ذلك يعبر عن "تحكم"مفرط في الفضاء السيبراني،وذلك على الرغم من تضمن المبدأ الأول في إستراتيجية الأمن السيبراني الروسي حرية المواطنين وحقوقهم الدستورية،وهو ما يعني عدم ممارسة سيادتها على الفضاء السيبراني إلى مستوى"السيطرة الكاملة"،ولكن يمكن أن يكون اقرب إلى مستوى"الرقابة".

وتحتفظ روسيا بعلاقات تعاونية مع الصين في مجال الفضاء السيبراني عبر اتفاقها عام 2015 وانضمامها لمنظمة شنغهاي للتعاون،بينما لا توجد علاقات متقاربة مع الولايات المتحدة بشأن التفاوض حول الفضاء السيبراني.

ورغم ذلك تصر روسيا على سعيها لإرساء قواعد دولية من خلال التوافق الجماعي الدولي،وهناك تناقض روسي مع القوى الغربية حول إنشاء معايير الإنترنت الدولية وبخاصة فيما يتعلق بالاختلاف بين تناول ومعالجه مفهومي "الفضاء السيبراني"و "السيادة السيبرانية".وذلك إلى جانب الخلاف بشأن استخدام السلطة السيادية في الفضاء السيبراني و"التهديدات السيبرانية والتي تعرّفها روسيا تحت مصطلح "التهديدات الأمنية

1 – عادل عبد الصادق،" صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية "،(26/04/2020) متاح على الرابط
http://accronline.com/article_detail.aspx?id=29415

2 – عادل عبد الصادق، **الموقع السابق**.

المعلوماتية".وتفصل بين تهديدات أمن المعلومات الخارجية والأخرى الداخلية ،وتري إنها أكثر حساسية ضد التهديدات السيبرانية الموجه إلى الداخل الروسي .

المطلب الثالث: اتجاهات مستقبل الصراع السيبراني بين روسيا والولايات المتحدة .

اختلفت اتجاهات الرؤية المستقبلية للتنافس السيبراني بين كل من الولايات المتحدة الأمريكية وروسيا وقد اتخذت عدة أبعاد واتجاهات يمكن توضيحها وفقا لما يلي:[1]

– **الاتجاه الأول**: الانتقال من الصراع على السيادة في الفضاء السيبراني إلى الفضاء الخارجي، وخاصة مع حالة التداخل بين كلا المجالين ولمواجهة التهديدات الروسية في مجال القوة الفضائية .– **الاتجاه الثاني**: التحول من الصراع "الناعم"على المعلومات والاستخبارات إلى صراع "صلب "على الاستحواذ على القوة السيبرانية ذات الطابع التدميري، والاستثمار في تطوير واستخدام الأسلحة السيبرانية من اجل تعزيز القيادة والسيطرة.

– **الاتجاه الثالث**: من الطابع العالمي المفتوح للفضاء السيبراني إلى الحمائية الدولية والدفع نحو فرض سيادة الدولة الوطنية في مقابل نظريه الفوضى.

– **الاتجاه الرابع**: تصاعد بناء القدرات في مجال شن الهجمات السيبرانية المنظمة والتحول من تبني السياسات الدفاعية إلى أخري هجومية ذات طابع استباقي وهو يهدد بعسكرة الفضاء السيبراني.

– **الاتجاه الخامس**: تأثير تزايد حالة الاحتقان بين روسيا والولايات المتحدة بسعي كل طرف أيجاد تكتل دولي داعم له وضاغط على الطرف الأخر وبخاصة إن العقوبات الأمريكية على روسيا ساعدت في التقارب مع الصين.

– **الاتجاه السادس**: توظيف الفضاء السيبراني لتحقيق أهداف خارجية والتدخل في الشئون الداخلية من خلال دعم حركات معارضة سياسية او مسلحة سواء عبر تقديم الدعم التقني أو السياسي أو الإعلامي. [2]

[1] – ساري محمد الخالد، اتجاهات في أمن المعلومات وأمانها –أهمية تقنيات (الشفرة)، شركة العبيكان للتعليم، ط11، المملكة العربيةالسعودية، 2018، ص 46.

[2] – عادل عبد الصادق، **المرجع السابق**.

– **الاتجاه السابع:** التوجه لتوظيف الفضاء السيبراني لفرض العقوبات الدولية على السلوك بمنع تصدير تكنولوجيا عسكرية او تجسسية او قطع كابلات الانترنت الواصلة للدولة او حجب مواقع مساندة للدولة في الداخل.

– **الاتجاه الثامن:** تصاعد الأنشطة السرية الاستخباراتية وتوظيف برمجيات التجسس والرصد والتحول من توجيه هجمات سيبرانية من الخارج إلى الداخل إلى توظيف عملاء الاستخبارات أو الدبلوماسيين المقيمين بشن هجمات من الداخل إلى داخل الدولة. [1]

وإجمالا يبدو تصاعد التوتر بين القوتين الأمريكية والروسية إلى جانب دول أخري سيعمل على تهديد الأمن الجماعي الدولي وهو ما يعزز اتجاه إعادة الاعتبار للقانون الدولي والمنظمات الدولية في حفظ الأمن والسلم الدوليين.

خصوصا وأنه من المرجح أن تنتقل الحرب الباردة الجديدة عبر الفضاء السيبراني إلى داخل المعسكر الغربي من قبل روسيا والصين لحين تحقيق التوازن الاستراتيجي في النظام الدولي.

[1] – ساري محمد الخالد، **المرجع السابق**، ص 47.

المبحث الثالث: واقع الجريمة السيبرانية في الدول العربية وسبل مكافحتها.

سارعت الدول العربية لوضع استراتيجيات لمواجهة الجرائم السيبرانية مثلها مثل باقي الدول.

المطلب الأول: تطور استخدام الانترنت وازدياد الجرائم السيبرانية في الدول العربية

أدى النمو السريع لاستخدامات الانترنت في الدول العربية إلى وزيادة عدد مستخدمي الانترنت، كما بينت الإحصاءات أـــن 40% من مستخدمي الانترنت في دول الشرق الأوسط وشمال أفريقيا يستخدمون الانترنت أكثر من 20 ساعة في الأسبوع، وهو ما يتوافق مع المعدل العالمي1، ويؤدي ازدياد أعداد مستخدمي الانترنت في المنطقة العربية بطبيعة الحال إلى ازدياد الأشخاص المعرضين للمخاطر السيبرانية، ومن ثم ازدياد الجرائم السيبرانية.

وتظهر الدراسات أن نسبة مستخدمي الانترنت الذين يقعون ضحايا الجرائم السيبرانية تتراوح ما بين 1 و17 في المائة، وهذه النسبة تزداد في الدول الأقل نموا. فقد أكد مسؤولو تطبيق القانون في دول آسيا، أن الجرائم السيبرانية وبدرجات تتفاوت بين ازدياد عادي وازدياد كبير .كما يعتقد 48 في المائة من المستطلعين في منطقة الشرق الأوسط، في مسح صدر أوائل عام 2014، أن مخاطر الجرائم السيبرانية في مؤسساتهم قد ازدادت في الأشهر الأربعة والعشرين الماضية ويبدي 44 في المائة من المستخدمين في دول منطقة الشرق الأوسط وشمال أفريقيا مخاوف كبيرة من تعرض حسابات بريدهم الإلكتروني أو غيره من الحسابات على الإنترنت للاختراق، وهذه النسبة هي أعلى قليلاً مما هي عليه في العالم عموما.[2]

ويبدو في دول المنطقة العربية أن الغالبية العظمى من الجرائم السيبرانية هي تلك التي تكون

المعلوماتية فيها وسيلة ارتكاب الجريمة وليس محلها .فوفق إحدى الدراسات لعام 2011، احتلت دولة الإمارات العربية المتحدة المرتبة 19 عالمياً، في حين جاء لبنان في المرتبة 25 عالمياً من حيث ترتيب الدول التي

[1] - ITU, Marco Gercke, Understanding Cybercrime: Phenomena, Challenges and Legal Response, September 2012, 90, p. 75-84.

[2]- Ministry of information and communications technology, Qatar, Rassed, The attitudes of online users in the MENA region cybersafety, security and data privacy, May 2014, http://www.ictqatar.qa/sites/default/files/Cybersafety,%20security%20, and%20data%20privacy.pdf, p. 22

تتعرض لهجمات سيبرانية. وفي لبنان تحديداً، لا تتجاوز جرائم التعدي على الأنظمة والبيانات 05 في المائة من المجموع، في حين أن 95 في المائة منها هي جرائم تقليدية بوسيلة معلوماتية، مثل الاحتيال والقدح .وكذلك في السودان، حيث لا تتجاوز نسبة جرائم التعدي على الأنظمة والبيانات في المائة، في حين تزيد نسبة جرائم شبكات التواصل الاجتماعي عن70 في المائة.[1]

وتبين عديد الأرقام والاحصاءات أن معدّل الجرائم السيبرانية هو أعلى نسبياً في منطقة الشرق الأوسط من

المعدّل العالمي، وهذا ناتج عن ضعف آليات محاربة هذه الجرائم، سواء على صعيد السياسات المطبقة، أو على الصعيد التقني أو التشريعي أو التوعوي .ويبدو أن المجرمين بدأوا يلجأون أكثر فأكثر في دول المنطقة إلى تكنولوجيا المعلومات لارتكاب أفعالهم لارتفاع عوائدها وتدني مخاطرها وإمكان القيام بها عن بعد وصعوبة إثباتها نسبياً .وفي هذا السياق، ووفقاً لإحصائية صادرة عن أبو ظبي، فإن نسبة 70 في المائة من الجرائم التي وقعت فيها خلال الأشهر الستة الأخيرة من عام 2010 استخدمت في ارتكابها تكنولوجيا المعلومات والاتصالات.

وقد أدى تزايد الجرائم السيبرانية في دول المنطقة إلى ارتفاع في أرقام بعض الجرائم التقليدية، باعتبار أن الجرائم السيبرانية يمكن أن تكون وسيلة لتسهيل ارتكاب الجرائم التقليدية .فعلى سبيل المثال، أثبتت بعض الدراسات في المجتمع السعودي أن 68.8% في المائة من المستطلعين يرون أن هناك علاقة بين الانحراف والجرائم المرتبكة، ومشاهدة محتوى الفيديو الجنسي .كما أثبتت إحدى الدراسات المتخصصة بتفسير ارتكاب الجريمة الجنسية في المجتمع السعودي والتي أجريت في الاصلاحيات المركزية في المملكة أن 22.2 في المائة .من مرتكبي الجرائم الجنسية كان لهم اهتمامات بالصور الجنسية. [2]

[1]- Hamadoun I. Touré Secretary-General, ITU, Cybersecurity Global status update, December 2011, http://www.un.org/en/ecosoc/cybersecurity/itu_sg_20111209_nonotes.pdf, p. 5.
[2]- Ibidi.

1- التحديات الإستراتيجية في المنطقة العربية.

يتيح وضع إستراتيجية شاملة للأمان السيبراني تحديد الأهداف المرجوة، وبيان الأنشطة المطلوبة لبلوغها، وتقسيمها على مراحل، وتحديد متطلباتها البشرية والمالية والتنظيمية والتقنية، وتنظيم وسائل تمويلها وفق خطط محدّدة .كما يساعد وضع الاستراتيجيات على تحديد آليات التنفيذ ووضع مخطط زمني للتنفيذ بالإضافة إلى تحديد المعنيين بالتنفيذ وإيجاد آليات لتنسيق الجهود في ما بينهم .وتفتقر معظم الدول العربية، إلى وجود إستراتيجية متكاملة للأمان السيبراني على بعض التجارب الدولية، وهي في طور استكمالها أما الدول الأخرى فلديها فقط استراتيجيات عامة لقطاع تكنولوجيا المعلومات والاتصالات.

2- معوقات وضع التشريعات وتحديثها.

يلاحظ في بعض بلدان المنطقة العربية أن المشرّع، إنفاذاً لقرارات من أعلى السلطات في البلاد، قد حزم أمره بإقرار التشريعات في مجال الجرائم السيبرانية ثم تطويرها، كما هو الحال في دولة الإمارات العربية المتحدة .أما في دول أخرى، فالتشريعات المتعلقة بالجرائم السيبرانية لم تصدر لغاية تاريخه 2014، وذلك إما بفعل عدم وجود استقرار سياسي وإعطاء الأولوية لملفات أخرى، أو بسبب عدم وجود ثقافة المعلوماتية لدى المسؤولين وعدم وعيهم لأهمية الموضوع .وبالانتظار يتم تطبيق بعض نصوص قانون العقوبات التقليدي وبعض النصوص الواردة في قوانين متفرقة أخرى على بعض الجرائم السيبرانية، فيما تبقى جرائم سيبرانية عديدة غير مجرمة .ونجد، أيضاً، تفاوت اً بين دول المنطقة من حيث تحديث تشريعاتها لتتلاءم مع المفاهيم المستجدة؛ فبعض هذه الدول، كدولة الإمارات العربية المتحدة، بلغت مرحلة متقدمة، ليس فقط بإقرار قانون منذ عدة سنوات، بل مراجعته وتحديثه عقب اختبار تطبيقه سنوات عدة، ومواكبة التطور التقني الحاصل والانتهاكات في هذا المجال.

ومن معوقات التشريع في دول المنطقة أيضاً وجود ضوابط مختلفة له في كل دولة، وكذلك الضوابط والمعايير العالمية التي لا تساعد على ضمان تناسقه بين الدول، وما يتعارض منها مع قواعد قانونية أساسية أو . دستورية أو دينية في البلاد أو مع تقاليد المجتمع أو غيرها.[1]

المطلب الثاني: إشكاليات الثقافة والتوعية حو الأمن السيبراني في الدول العربية.

وفيما يتعلق بممارسات مرتكبي الجرائم السيبرانية في دول المنطقة وردّ ات فعل الرأي العام عليها، فهي تبدو مشابهة أحياناً لتلك السائدة في العالم وتتفاوت معها أحياناً أخرى .إذ تتداخل معها عوامل اجتماعية أو ثقافية أو دينية أو اقتصادية، مرتبطة بخصوصيات المنطقة العربية .وتبرز تحديات تتعلق بالمفاهيم الاجتماعية والدينية والإنسانية السائدة في مجتمعاتنا الشرقية، والتي تفرض قواعد خاصة تختلف عن تلك المطبقة في دول الغرب . وهنا يتضح دور قواعد السلوك والتصرف المفترض مراعاتها من قبل الجميع في تعاملاتهم على الإنترنت، أي من قبل مزودي خدمات الاتصال والمستخدمين على حد سواء .إلا أن قواعد السلوك والتصرف هذه ما زالت غير مقننة وغير منشورة في كثير من دول المنطقة.[2]

وعلى سبيل المثال، يميل المستخدمون في المنطقة العربية في بعض الحالات إلى استعمال الإنترنت لتوسيع دائرة معارفهم الاجتماعية والمهنية، عبر الاتصال بأشخاص لم يعرفوهم من قبل، مما يعرضهم للمخاطر . وتظهر بين الحين والآخر إشكاليات عديدة تنتج عن عدم مراعاة قاعدة سلوكية معينة، فمثلاً قامت دولة الإمارات العربية المتحدة في الآونة الأخيرة بإلزام جميع المشتركين في موقع فيسبوك التقيّد بشروط قد تخالف قواعد الموقع ولكنها تلبي القانون الإماراتي، ومنها ألا يرفق المستخدم أسماء المستخدمين الآخرين عند نشر المحتوى دون الحصول على موافقتهم، وذلك باعتبار أن القانون الإماراتي يحمي خصوصية الأفراد وسمعتهم.[3]

[1] - .United Nations Office on Drugs and Crime, UNODC, Comprehensive study on cybercrime, draft, February 2013, p. 59

[2]- .ibidi

[3] – دولة الإمارات العربية المتحدة" ورقة عمل "حول استخدام موقع التواصل الاجتماعي" فيسبوك"، أنظر الرابط:

http://arabic.cnn.com/middleeast/2014/05/21/facebook-uae-law

3- إدراك المخاطر السيبرانية في دول المنطقة.

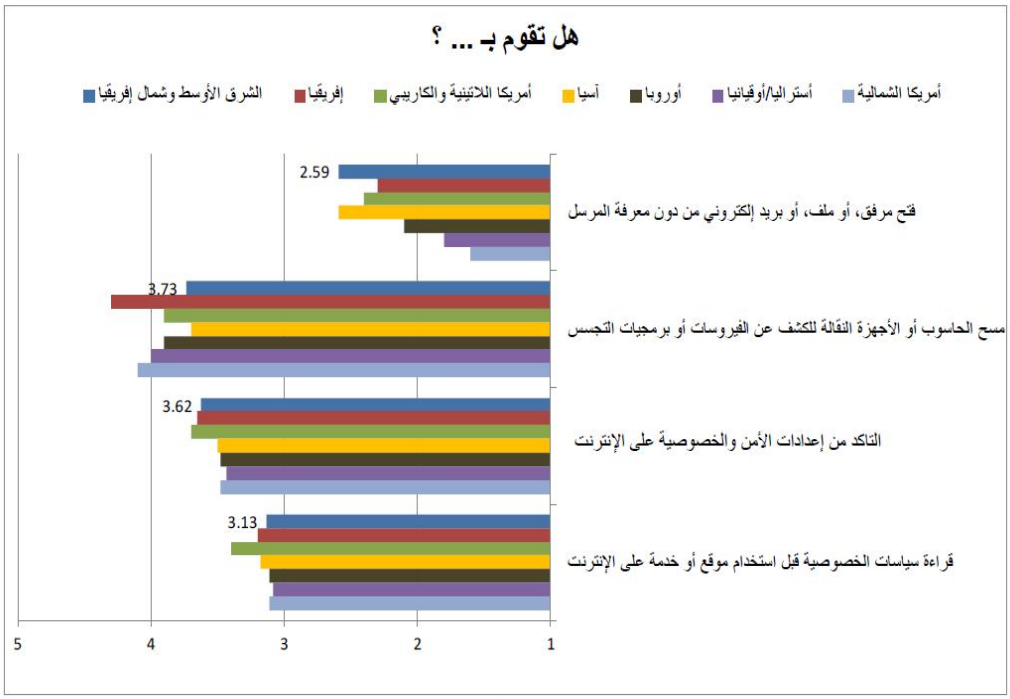
أشارت دراسة أجرتها وزارة الاتصالات وتكنولوجيا المعلومات في قطر عام 2014 في 14 بلدا، أن الأشخاص في المنطقة العربية لا يعون كثيراً المخاطر السيبرانية .فالأشخاص في دول منطقة الشرق الأوسط وشمال أفريقيا، وبالرغم من أن عدد اً كبير اً منهم (45 في المائة) يصرح أنه يتوخى الحذر بتصرفاته على الإنترنت، وأنه يتفحص ضبط الخصوصية والأمن على الخط، هم أكثر انفتاح اً من أولئك الذين هم في مناطق أخرى لإقامة اتصال على الخط مع أشخاص لا يعرفونهم أو لم يلتقوا بهم فعلي اً، كما أنهم يميلون أكثر من غيرهم إلى فتح رسائل بريد إلكتروني وملحقاتها الصادرة عن مصادر مجهولة، وإلى تنزيل ملفات عن الإنترنت، ولا يجرون مسحاً لحواسيبهم بالبرامج المضادة للفيروسات المعلوماتية وبرامج التجسس، مع أنهم أكثر تخوفاً من الإنترنت وأقل ميلاً لإجراء معاملات التجارة الإلكترونية أو العمليات المصرفية على الخط .[1]

وهم يعتقدون كباقي المستخدمين في العالم أن خدمات المصارف والمؤسسات المالية الإلكترونية على الإنترنت هي أكثر أمناً من غيرها من الخدمات، تليها الخدمات الصحية ومن ثم خدمات السلطات الحكومية.

وهذا ما سنراه في الشكل القادم.

[1] - Ministry of information and communications technology, Qatar, Rassed, The attitudes of online users in the 020
MENA region cybersafety, security and data privacy, May 2014,
http://www.ictqatar.qa/sites/default/files/Cybersafety,%20security%20
d%20data%20privacy.pdf,

الشكل رقم (01): تصرفات الأشخاص على الإنترنت في ما يخص الأمان السيبراني



المصدر: 20 15privacy.pdf.في المائة 51 data في المائة 51 and في المائة security في المائة
http://www.ictqatar.qa/sites/default/files/Cybersafety, :

ومن المعتقدات الشائعة لدى الرأي العام أن المخاطر على الأنظمة المعلوماتية تأتي من داخل المؤسسة لا من خارجها، ف 9 في المائة من المستطلعين في منطقة الشرق الأوسط هم من هذا الرأي،[1] كذلك يعتقد مستخدمو الهواتف النقالة أو الذكية والألواح الإلكترونية خطأً أنها أكثر أمن اً من الحواسيب .وتدل الدراسات على أن معظم مستخدمي الإنترنت في الدول المتقدمة والنامية يطبقون تدابير الأمن الأساسية؛ ويشذ عن ذلك القاصرون والأطفال الذين نادراً ما يستخدمون هذه التدابير، وكذلك الشركات الصغيرة والمتوسطة التي تعتقد أنها غير مستهدفة أو قلما تتخذ هذه التدابير.[2]

[1] - John Wilkinson, Tareq Haddad, PWC, Economic Crime in the Arab World, February 2014, http://www.pwc.com/m1/en/publications/gecs2014reportme.pdf, p. 18.

[2] - United Nations Office on Drugs and Crime, UNODC, Comprehensive study on cybercrime, draft, February 2013, p. 234, 237.

ولعل بعض الأشخاص في المنطقة العربية الذين لا يستعملون الحاسوب يعتقدون أنهم بغنى عن التعرف على هذا الحقل المستجد وكيفية الحماية فيه، إلا أنهم، كالغالبية العظمى من الناس، يستعملون أجهزة هاتف نقّال ذكية، وقد يقومون بتحميل تطبيقات عليها .إن مخاطر الهواتف النقّالة الذكية هي أكبر من مخاطر أجهزة الحاسوب التي تتمتع بحماية ضد الفيروسات والتجسس، في حين أن برامج الحماية في الهواتف هي برامج احتيالية malicious code كما أن شركات البرمجة هي أكثر سرعة في صنع التعديلات والتحديثات ضعيفة حالياً؛ لا بل إن معظم التطبيقات على الهواتف الذكية هي من صنع أفراد لا شركات، وقد يخفون داخلها للبرامج، وتوجيه التنبيهات للمستخدم على صعيد الحواسيب منها على صعيد الهواتف الذكية. [1]

4- عدم ملائمة أو كفاية برامج التوعية في دول المنطقة العربية.

بالرغم من عدم وجود وعي كاف في المنطقة العربية للمخاطر السيبرانية، يتبين أن دولا عديدة قد أطلقت حملات توعية أو حملات لتدريب المستخدمين .إلا أن هذه الحملات تعاني من الضعف أو عدم النجاح نسبياً نظراً لضعف التغطية أو التسويق، ولعدم تكرارها وكذلك عدم استهدافها الفئات المعنية حقيقةً ، وعدم استقطابها اهتمام الجمهور، وتعاني أيضا من حداثة مواضيعها وتقنيتها، أو سوء اختيار المحاضرين.

أما المناهج التعليمية، فلا تتضمن في كثير من المدارس والجامعات أية مواد حول الأمان السيبراني؛ ولا يجري تنظيم حملات إعلامية في وسائل الإعلام تعويض اً عن ذلك .كما يلاحظ ضعف في حملات التوعية الموجهة للنساء تحديداً، أو التوعية بالجرائم التي تطال النساء أكثر من الرجال.

ويوجد بعض المبادرات الناجحة في عدد من الدول العربية، إذ تتبنى اللجنة الوطنية لحماية النشء على الإنترنت في مصر مبادرات عديدة، وترعاها وتنفذها وزارة التربية والتعليم وفي لبنان، يقوم المجلس الأعلى للطفولة في وزارة الشؤون الاجتماعية بدور مشابه. [2]

---

[1] - United Nations Office on Drugs and Crime, **op.cit**.

[2] - John Wilkinson, op.cit.

المطلب الثالث: آفاق التعاون بين الدول العربية من أجل تعزيز الأمان السيبراني.

يُعد تعزيز التعاون بين الدول العربية، وكذا بينها وبين بقية الدول، حجر الأساس لمكافحة الجرائم السيبرانية ولتعزيز الأمان السيبراني، نظراً للطابع العابر للحدود لهذه الجرائم .ويمكن البدء بتفعيل الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 وتطبيقها؛ وقد تضمنت هذه الاتفاقية تنظيماً حديثاً لآليات التعاون .ويمكن كذلك الاسترشاد بإرشادات الإسكوا الخاصة بالتشريعات السيبرانية ومنها الاسترشاد الخاص بالجرائم الإلكترونية مضافاً إليه الجزء الإجرائي الموضح في المرفق الثالث لهذه الدراسة والمقتبس من اتفاقية بودابست .وتفيد هذه الاتفاقيات/الإرشادات في إعداد واعتماد اتفاقيات ثنائية أو صياغة تفاهمات بين الدول العربية أو في مراجعة الاتفاقية العربية لجرائم تقنية المعلومات .وقد تضمنت الاتفاقيات المذكورة قواعد خاصة حول التعاون القضائي بين الدول بخصوص جمع الأدلة المعلوماتية والتحقيق في الجرائم السيبرانية، وهذه القواعد تتلخص بالآتي: [1]

- التعاون إلى أقصى الحدود بين الدول في التحقيقات الجزائية وجمع الأدلة المعلوماتية، حتى في الجرائم التقليدية؛

- اعتبار الجرائم السيبرانية من الجرائم التي يقبل فيها استرداد المتهمين إذا كان معاقب اً عليها في الدولتين بعقوبة سالبة للحرية لمدة تزيد على سنة، أو بعقوبة أشد؛

الاستجابة لطلبات التعاون الموجهة بوسائل الاتصال السريعة، كالبريد الإلكتروني أو الفاكس، بشرط ضمان مستوى ملائم من الأمن والمصادقة على المصدر، ويمكن اشتراط تأكيد الطلب بمراسلة رسمية؛

- إرسال معلومات إلى دولة أخرى قد تفيدها في التحقيق في جريمة سيبرانية؛

- تسمية نقطة اتصال لدى كل دولة لإرسال طلبات المساعدة المتبادلة أو للإجابة عليها أو لتنفيذها؛

[1] - Michael A. Vatis, The Council of Europe Convention on Cybercrime, http://cs.brown.edu/courses/csci1950-p/ sources/lec16/Vatis.pdf,

– حفظ البيانات المعلوماتية الموجودة على أراضي دولة مدة لا تقل عن 60 يوماً، بناءً على طلب دولة أخرى، على أن يتم ضبط هذه البيانات بصورة لاحقة بناء على طلب الدولة الأخرى؛

– الاستجابة لطلبات المساعدة المتبادلة المقدمة من دولة أخرى للبحث عن بيانات معلوماتية أو لضبطها أو لإعطائها، عندما تكون موجودة على أراضي الدولة الموجه إليها الطلب. [1]

السماح لسلطات دولة بالوصول، عن طريق نظام معلوماتي موجود على أراضيها، إلى بيانات معلوماتية مخزنة على أراضي دولة أخرى، وذلك في حال موافقة الشخص صاحب السلطة على البيانات.

– تقديم المساعدة المتبادلة، عن طريق تقديم معلومات حركة البيانات الجارية على أراضي إحدى الدول في زمن الإرسال الحقيقي.

– تقديم المساعدة المتبادلة، عن طريق تقديم أو تسجيل محتوى الرسالة أو المعلومات المنقولة بواسطة نظام معلوماتي على أراضي إحدى الدول في زمن الإرسال الحقيقي بالقدر الذي تسمح به قوانين تلك الدولة؛

من ناحية أخرى يجب أيضاً العمل على توحيد المصطلحات الخاصة بالأمان والأمن السيبراني وكذلك التشريعات السيبرانية من أجل تسهيل تبادل المعرفة والخبرات، وكذلك من أجل التنسيق بين التشريعات، وتسهيل التعاون والتفاعل فيما بين القضاة ورجال الشرطة وخاصة عند مكافحة الجرائم السيبرانية

أخيراً، يدخل ضمن مفهوم التعاون، العمل بين دول المنطقة على تطوير آليات تبادل الخبرات والمعارف العلمية والتقنية والتجارب والحلول، عن طريق الزيارات المتبادلة والمؤتمرات الدورية وإنشاء قنوات اتصال دائمة .ويمكن أن يتم ذلك عن طريق توقيع بروتوكولات تعاون وتنسيق بين دول المنطقة العربية. [2]

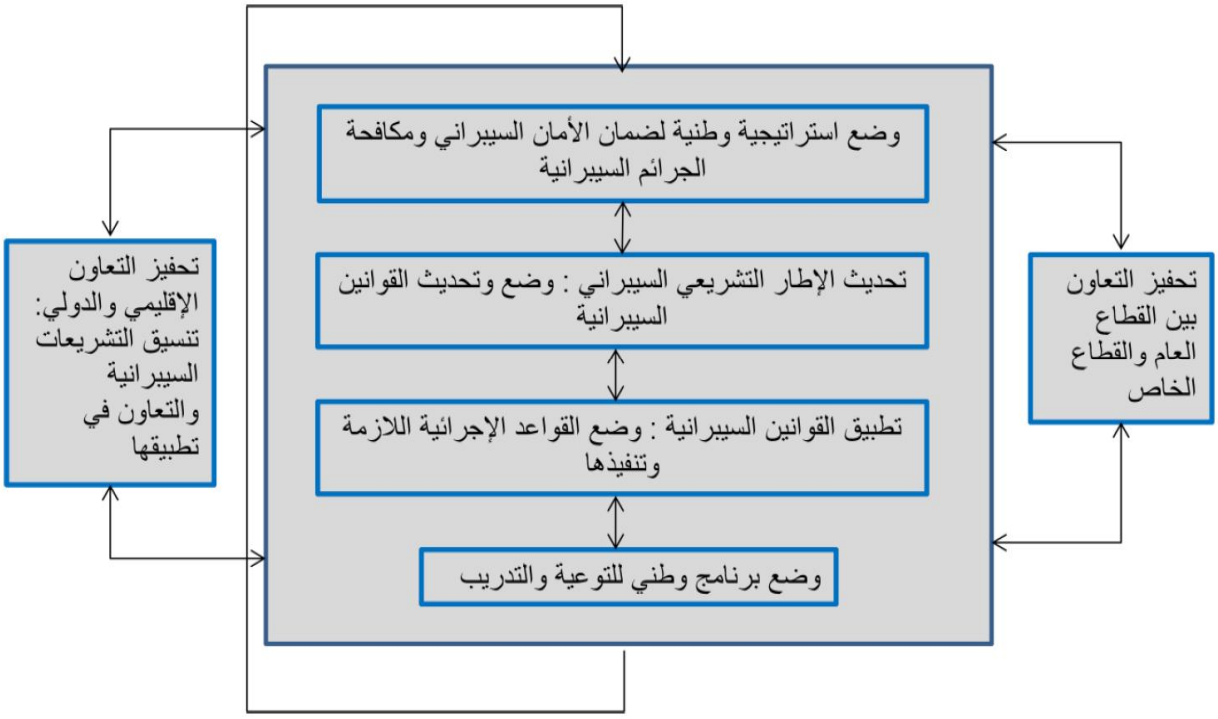
ويمكن توضيح أهم الآليات المقترحة لضمان الأمن السيبراني وفقا للخطة الموضحة في الشكل الموالي:

---

[1] - **ibidi**.

[2] - Micheal Barrett, Andy Steingruebl, Bill Smith, Combating Cybercrime: Principles, Policies and Programs, April 2011, https://www.paypalmedia.com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4.pdf,

الشكل رقم (02): خطة الأمان السيبراني للدول العربية



المصدر: Cabinet Office, *The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world*, November 2011,

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final

خلاصة الفصل

من خلال العرض الذي قدمناه حول الجريمة السيبرانية في الاستراتيجيات الدولية رأينا أن جميع الدول قامت بوضع العديد من الاستراتيجيات لمواجهة هذه التهديدات، ومن خلال ما سبق توصلنا إلى النتائج التالية:

-مع التطور الالكتروني ظهرت الجريمة الالكترونية التي انتشرت بشكل كبير وأصبحت تشكل خطرا على امن الدول، لذلك قامت الدول والهيئات والمنظمات بوضع العديد من القوانيين التي تجرم هذه العملية.

- قامت كل من روسيا والولايات المتحدة الأمريكية بمواجهة الجرائم السيبرانية عن طريق العديد من الاستراتيجيات، وذلك راجع لتطور هذه الدول وتغلغلها في الفضاء السيبراني بشكل كبير.

- لم تتخلف الدول العربية عن باقي الدول في مواجهة الجرائم السيبرانية لأنها تعرضت لها هي كذلك، وتلقت الدول العربية أضرار كبيرة نظرا لضعفها في الأمن السيبراني، لكنها تداركت ذلك بوضع العديد من الاستراتيجيات لمواجهتها.

الفصل الثالث:

إستراتيجية الجزائر في مكافحة الجريمة السيبرانية

تمهيد:

دخلت الجزائر في الفضاء السيبراني مثلها مثل باقي دول العالم، وبدات مراحل التطور عندها في مجال المعلوماتية حتى وصل لدرجات متقدمة، ومنه عانت الجزائر كذلك من العديد من الجرائم السيبرانية ماشكل خطورة كبيرة على امنها القومي، لذلك سارعت الى وضع العديد من الاستراتيجيات لمواجهة هذه التهديدات الجديدة التي تدور في عالم المعلوماتية، عن طريق اليات قانونية، بالاضافة الى اليات تقنية، والعديد من الاستراتيجيات الاخرى التي سوف نفصل فيها في هذا الفصل.

لذلك تم تقسيم هذا الفصل الى ثلاثة مباحث كما يلي:

- ✓ **المبحث الأول: واقع الجريمة السيبرانية في الجزائر.**
- ✓ **المبحث الثاني: الآليات المحلية لمواجهة الجرائم السيبرانية .**
- ✓ **المبحث الثالث: التنسيق الاقليمي لمكافحة الجريمة السيبرانية.**

المبحث الأول: واقع الجريمة السيبرانية في الجزائر.

تختلف نوعيّة الجرائم السيبرانية بين تلك التي هدفها الاعتداء والمساس بأمن وسلامة الأشخاص، أو تلك التي تهدف بالأساس إلى الإضرار بالأنظمة الحاسوبية والإلكترونية والتَجسّس على المعلومات الخاصة بالشركات والمؤسسات الإقتصادية أو التجارية أو المالية كالبنوك، وكذلك تلك الجرائم التي تتم من خلالها عمليات الابتزاز عن طريق الإنترنت التي من المفروض أن تكون وسيلة للتبادل الثقافي والمعرفي والحضاري بين الثقافات والشعوب المختلفة، وما تعانيه الجزائر اليوم من تفشي لظاهرة الجرائم السيبرانية فخاصة في ظل التقدم التكنولوجي الهائل واتاحة مختلف منصات التواصل وانكاشف المواطنين الجزائريين على مختلف بقاع الكرة الأرضية، ما جعل مجال التهديدات السيبرانية يتسع وينمو، هذا مع نقص آليات المراقبة وكذا المتباعة في ظل عدم تطرق خاصة المنظومة التشريعية والقانونية لهكذا جرائم مستجدة وهو ما سيتم توضيحه من خلال هذا المبحث من خلال إبراز أهم الجرائم السيبراني في الجزائر

المطلب الأول: الجرائم السيبرانية الإرهابية.

تعد الجرائم السيبرانية الإرهابية أحد أخطر التهديدات المحتملة على الأمن الجزائري في ظل الثورة التكنولوجية الحديثة حيث تشهد الساحة الامنية الجزائرية كغيرها من الدول العديد من المخاطر والتهديدات التي فوضتها الثورة التكنولوجية الحديثة، خاصة بعد انتشار وسائل التواصل الاجتماعي والعديد من المواقع الالكترونية التي تحمل أفكار هدامة تهدد استقرار الوطن ووحدته، وتدعوا إلى نشر الفوضى والعنف والتطرف والكراهية والانفصام، ومن أهم المخاطر التي تترتب عن استخدام التكنولوجيا الحديثة على الأمن الجزائري الإرهاب الالكتروني ويقصد به العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الالكترونية الصادرة من الدول أو الجماعات أو الافراد على الانسان في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق بشتى صنوفه وصور الإفساد في الأرض.[1]

لذلك الجزائر قامت بوضع العديد من التشريعات لمواجهة هذه لظاهرة، التي تشكل خطرا كبيرا لانها تستهدف الاجهزة الحساسة في الدولة.

[1] – أيسر محمد عطية، **" دور الآليات الحديثة للحد من الجرائم المستحدثة :الإرهاب الالكتروني وطرق مواجهته." ورقة مقدمة في الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية**، (عمان خلال الفترة 32-31 سبتمبر 2014)، ص 09.

ويعتبر أحد اخطر التهديدات التي تستهدف أمن جميع الدول بما في ذلك الدولة الجزائرية. وهذا ما أكده اللواء مناد نوبة القائد العام السابق للدرك الوطني الجزائري في كلمة له ألقاها بمناسبة افتتاح الندوة المحلية حول الأمن السيبراني حيث قال: "إن الإرهاب الالكتروني بات من أخطر الجرائم التي تستهدف الجزائر من خلال تنامي مظاهر الترويج لكل أشكال العنف والإرهاب والتطرف باستعمال أحدث التقنيات التكنولوجية خاصة شبكات التواصل الاجتماعي والمنتديات الالكترونية" وذلك دعا إلى إطلاق خلايا أمنية متخصصة هدفها العمل على تعزيز إجراءات الرقابة لحماية المواطن الجزائري، خاصة عنصر الشباب من مثل هذه الجرائم الالكترونية الخطيرة جدا على استقرار البلاد وذلك من خلال قيامها بتعقب وملاحقة كل الأنشطة المتعلقة بالتجنيد للإرهاب والإجرام المنظم العابر للحدود، وتكييفها بالوسائل التكنولوجية العصرية". وذلك يتطلب حسب ضرورة "التسلح بكل الوسائل التكنولوجية والفعالة لمحاربة إيديولوجيات العنف والتطرف وكل أشكال الجريمة المنظمة والعابرة للأوطان من خلال إعتماد آليات عملية للتعاون بين كل الأطراف والشركاء الفاعلين في هذا المجال".[1]

أما التنظيم الإرهابي "داعش" خلية أزيد من 50 ألف موقع الكتروني، 90 ألف صفحة باللغة العربية على موقع التواصل الاجتماعي "فيسبوك" و40 ألفا بلغات أخرى، وهذا ما ساهم حوالي 3400 شباب عبر حملاته الإلكترونية، وهذا حسب تقرير للخبير الأمني في ضحايا الارهاب الرقمي جيف باردين "Jeff Bardin".[2]

ورغم الخطورة الكبيرة التي تخلفها مثل هذه المواقع الالكترونية على أمن واستقرار المجتمعات، إلا أن تأثيرها على المجتمع الجزائري كان قليلا. فقد كشف السيد محمد عيسى وزير الشؤون الدينية والأوقاف أن التجنيد الالكتروني لداعش في الجزائر عن طريق شبكة الانترنيت ومواقع التواصل الاجتماعي لم يتجاوز 100 شباب جزائري، وهو رقم ضئيل إذ ما قورن بعدد المجندين في دول عربية أخرى مثل تونس وليبيا ومصر، لذلك الجزائر استطاعت مواجهة هذا الخطر.[3]

---

[1]- عنتر بن مرزوق، **"الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية"**، (محاضرة مقدمة لطلبة جامعة محمد بوضياف المسيلة، كلية الحقوق والعلوم السياسية، د.س)، ص67.

[2]- محمود خليل،" **50 ألف موقع الكتروني لداعش ... .والإرهاب يحاصر الانترنيت"**، تاريخ تصفح 2020/03/29، من الرابط: www.alittihad.ae/details.php=120l..

[3]- الاتحاد الدولي للاتصالات، "**دليل الامن السيبراني للبلدان النامية"**، (جنيف: مكتب تنمية الاتصالات 2009)، ص 08.

ويمكن تبرير ذلك بنتائج العشرية السوداء التي عاشها الجزائريون في القرن الماضي، وكذا التحصن الجزائري ضد الفكر التطرفي العابر للحدود، إضافة إلى الفشل الذريع الذي منيت به ما يعرف بثورات الربيع العربي، والذي كان له تأثير كبير على ضرورة البحث عن آليات أخرى للتغيير السلبي في المجتمعات بعيدا عن العنف والتطرف بشتى أشكاله. [1]

ولذلك فالانترنيت يجب أن تبقى فضاء لنشر ومشاطرة العلوم والمعرفة وأداة للإبداع والتقارب والتعاون بين الأفراد والشعوب والدول، وليس وسيلة وأداة تهديد تستغلها الجماعات الإرهابية من أجل بلوغ أهدافها الإجرامية ونشر أفكارها التطرفية، كما أشار إلى ذلك السيد وزير الشؤون المغاربية والاتحاد الإفريقي وجامعة الدول العربية السيد عبد القادر مساهل في كلمته خلال أشغال الورشة الدولية حول دور الانترنيت والشبكات الاجتماعية في مكافحة التطرف والإرهاب الالكتروني والوقاية منهما. ولا تقتصر التهديدات السيبرانية على قضية الإرهاب الالكتروني فقط وإنما تشمل العديد من المخاطر والتهديدات الأخرى التي ترتبط بأمن الدولة فقط بل تشمل المجتمع ككل، فهي متعلقة بأمن الأفراد والمنظمات أيضا.

المطلب الثاني: أنظمة التجسس والقرصنة.

سجلت الجزائر أزيد من 900 جريمة إلكترونية خلال سنة 2017، حسب ما أعلنه مركز الوقاية ومكافحة الجريمة الإلكترونية، التابع لمصالح الدرك الوطني.وشملت الجرائم الإلكترونية، حسب ذات الهيئة، "المساس بحياة الأشخاص، والتهديد والابتزاز، والتشهير بالإرهاب، وقرصنة البيانات ونظم الكمبيوتر، وسرقة الهوية، يؤكد خبير التكنولوجيات الحديثة للاتصال، إيهاب تيكور لـــ"أصوات مغاربية"، أن الرقم الذي أعلنته مصالح الدرك الوطني بشأن الجريمة الإلكترونية في الجزائر يتعلق بـــ "القضايا التي عالجتها المصالح الأمنية" مشيرا إلى أنها تخصّ القضايا المصرّح بها من طرف الضحايا، بينما الحقيقة أن "الرقم قد يكون مرتفعا جدا" موضّحا أن الاعتبارات الاجتماعية للعائلات، والأمنية لبعض الأشخاص، تجعلهم يتكتمون عن التصريح بها الجرائم الإلكترونية ترتفع بارتفاع عدد مستخدمي تكنولوجيا الاتصالات، معتبرا أنها لا تقتصر على جرائم مواقع التواصل، بل هناك جرائم أخرى تخص قرصنة المواقع والحسابات والبيانات. [1]

---

[1] – عنتر بن مرزوق ، **مرجع سابق**، ص20 .

[1] – عبد السلام البارودي، "**هل دخلت الجزائر عصر الجريمة الالكترونية؟**"، تصفح في: 2020/04/10. على الرابط:
https://www.maghrebvoices.com/a/algeria-cyber-criminality/414407.html

* تنص المادة 394 على: "كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسد أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها ".

ودعا خبير تكنولوجيا الاتصالات إلى تشريعات أكثر صرامة ووضوحا في محاربة الجريمة الإلكترونية، بعد دخول قضايا التجارة الالكترونية والعملة الافتراضية عل خط التعاملات اليومية لمستخدمي الشبكة العنكبوتية مذكّرا بجرائم خطيرة تسجل سنويا، كسرقة المعلومات والبيانات الشخصية للمتعاملين، وخلق أرضيات إلكترونية لمواقع شبيهة خاصة بالقرصنة.

فقد تبنى المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي بنص المادة 394* مكرر بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية، وعقوبة الاشتراك في الاتفاق تكون نفس عقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم تكون العقوبة هي عقوبة الجريمة الأشد.

يمكن أن نجمل أخطر التهديدات الالكترونية فيما يلي:

1. تعطيل الخدمة.
2. إتلاف المعلومات أو تعديلها.
3. التجسس على الشبكات.
4. تدمير الأصول والمعلومات. [1]

تلقت الأجهزة الأمنية خلال الثلاثي الأول من سنة 2017، أن أزيد من2000تبليغ عن متصلة بالإرهاب الالكتروني عبر المواقع الالكترونية وفقا لمصدر أمني مأذون ل البلاد ،وأفاد المصدر أن معظم التبليغات التي أرسلت حول شبهات الإرهاب بمحاولات اختراق حسابات مواقع تواصل اجتماعي، ودعوات التجنيد، وأفاد المعطيات أن تنظيم داعش يسيطر على عدد كبير من المواقع والمنتديات الالكترونية، وقد حذر من الهجمات والتحديات السيبرانية العديد من الجهات الرسمية والأكاديمية، حيث أكدت كاتب الدولة المكلف بالشؤون المغاربية والاتحاد الإفريقي وجامعة الدول العربية، أن الجزائر تحرص على حماية أمنها في محيطها الإقليمي الذي يتميز بتواصل وانتشار التهديد الإرهابي، وفي نفس السياق خلال أشغال الدولية حول دور الانترنيت والشبكات الاجتماعية في مكافحة التطرف الإرهاب الالكتروني والوقاية منها. [2]

[1] – فضيلة غاقلي، "**الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري**"، مركز جيل البحث العلمي، على الرابط:
تصفح في http://jilrc.com.2019/05/10

[2] – بن مرزوق عنترة، حرشاوي محي الدين، "**الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية**"، الملتقى الدولي حول سياسات الدفاع الوطني، (جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية،31/01/2017)، ص 12.

المبحث الثاني: الآليات المحلية لمواجهة الجرائم السيبرانية .

تعد الجرائم السيبرانية هي واحدة من أخطر الظواهر الإجرامية المستحدثة في المجتمع الجزائري كما في المجتمعات الأخرى، حيث شهدت الألفية الأخيرة ثورة تكنولوجية استغلها الجميع في تحقيق دوافع مشينة أحسنها الشغف بالتقنية وأسوءها الربح المادي، لهذا كان لزاما على الدولة الجزائرية التدخل عبر الإجراءات المختلفة لمواجهة هذه الظاهرة والحد من تناميها خاصة في ظل ما تشهده بلادنا اليوم من تحول داخلي وخارجي، وهو ما جعل المتربصين بها كثيرون في ظل الأحقاد التي تحيط بها والتي وجدت من البيئة الالكرتونية مجال مناسب لرزع سمومها ومحاولة استهداف أمن الجزائر وشعبها ويمكن وصف أهم الآليات المحلية لمواجهة التهديدات السيبرانية وفقا لما يلي:

المطلب الأول: الآليات الأمنية.

لقد وضعت قيادة الدفاع الوطني الأمن السيبراني أحد أولوياتها على غرار باقي دول العالم التي سارعت إلى مراجعة سياساتها الأمنية، وإدراجها الآليات وميكانزمات جديدة تعني بهذه المسائل، بالمؤازرة مع تطوير البنيات الأساسية المتعلقة بتكنولوجيات العالم الرقمي، ويفرض مطالب الأمن مضاعفة أنظمة الرقابة التي قد تشكل تهديدا ممكنا للحريات الفردية، ولهذا وجب مرافقة كل المقاربات الأمنية في مجال الأمن الرقمي للأطر القانونية والتكنولوجية الملائمة، وتؤخذ بعين الإعتبار دقة الهجمات الإلكترونية وتجسيدا لذلك بإشراف الدولة الجزائرية وفي مقدمتها مؤسسة الدفاع الوطني إلى إعداد برامج خاصة لمجابهة الجريمة الإلكترونية* والحد من انتشارها وإنشاء أجهزة جديدة تنسجم في أدوارها وتجهيزاتها مع المتغيرات الحاصلة في هذا المجال.

إذ أصبحت الحماية السيبرانية جزء مهما المضي قدما ومسايرة التطورات التكنولوجية والإعلامية في ظل التوجه الدولي نحو الحكومة السيبرانية أصبحت قضية الأمن السيبراني من بين الرهانات والتحديات الكبرى على الصعيدين الإقليمي والعالمي، وخاصة مع التزايد الهائل في التهديدات الأمنية الإلكترونية، والجزائر كغيرها من الدول التي سعت منذ انتهاجها للإدارة الإلكترونية ووضع الأمن السيبراني من بين أولويات الأمنية فقد قامت بإنجاز العديد من الأجهزة والخلايا الأمنية بغية حماية منظومتها المعلوماتية.

* **الجريمة الالكترونية:** هي فعل يتسبب بضرر جسيم للأفراد أو الجماعات والمؤسسات، بهدف ابتزاز الضحية وتشويه سمعتها من أجل تحقيق مكاسب مادية أو خدمة أهداف سياسية باستخدام الحاسوب ووسائل الاتصال الحديثة مثل الإنترنت.

لقد أصبح الأمن السيبراني ركن أساسي ضمن العقيدة الأمنية المعاصرة، والتي يجب على الدفاع الوطني من خلال أجهزتها كالدرك الوطني الجزائري بإعتباره جهاز أمني مهم مسؤوليته تحقيق الأمن المعلوماتي في ظل تنامي الجريمة الرقمية. ولا ننسى كذلك الجانب القانوني والمشرع الجزائري وكيف قام بمواجهة هذه الجرائم والاعتداءات الأمنية وتشير الإحصائيات المسجلة في الجزائر أن الجريمة الإلكترونية أخذت منحا تصاعديا في الآونة الأخيرة، ولهذا فإن السلطات الجزائرية ملزمة باتخاذ الاحتياطات الأمنية اللازمة لتفادي أي نوع من الجرائم السيبرانية.[1]

ومن خلال هذا الفصل الثالث سوف يتم التعرف عن هذه المناهج والإجراءات المتبعة لمواجهة ذلك في العالم، ومن ثمة تأمين وحماية نطاقه المعلوماتي، وتأمين الفضاء المعلوماتي لكل الناشطين فيه وذلك من خلال التركيز على النقاط التالية:

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

تنمية وتعزيز القدرات البشرية المكلفة بعمليات التحقيق في الجرائم الإلكترونية.

توافر أحدث المعدات التكنولوجية في مجال الإعلام الآلي، الاتصالات اللاسلكية.

التمتع بقاعدة بيانات واسعة محدثة باستمرار.

القدرة على تصميم البرامج المعلوماتية وتطويرها.

لقد لعبت هذه العناصر محور اهتمام مؤسسة الدفاع الوطني من الاستقلال، واستطاعت من خلال سعيها المتواصل إلى تطوير إمكاناته وقدراته على جميع الأصعدة.

[1]- ج .رضوان، **"الأمن السيبراني :أولوية في استراتيجيات الدفاع"**، **مجلة الجيش** .العدد 630، جانفي 2016،ص 41.

[2]- بارة سمير، **المرجع السابق**، ص ص6-7.

ويمكن نلحظ ذلك بشكل جلي، في درجة الاحترافية التي يتمتع بها أفراد الدرك الوطني، واستخدامهم لوسائل وتقنيات حديثة تساعد على إنجاز التحقيقات والتحريات في مجال التحقيق.

واستطاعت وحدات الدرك الوطني من اقتناء أحدث التجهيزات والبرامج التقنية لحماية البنى التحتية المعلوماتية ضد كل المخاطر الرقمية، وتكوين أفرادها على أعلى المستويات.

ويتضح ذلك في الأدوار التي تؤديها إنجازاتها، إذ يعتكف أفرادها على وضع التدابير اللازمة لمنع تسرب إمتحانات البكالوريا في 2017 وكذا تسرب إمتحانات المسابقات في جانب التربية والتعليم ومجالات أخرى. [2]

اذن فالتطور التقني ساعد الجزائر في مواجهة هذه الجرائم عن طريق مكافحتها من خلال نفس الاجهزة والذي تجسد في فرقة العمليات.

2- الجهاز العملياتي: ويتمثل هذا الأخير في المراكز والوحدات التي أنشئت لغرض مواجهة الجريمة الإلكترونية، ومدى استعداداتها لأدائها من ذلك والمتمثلة أساسا في :

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

وقد أنشئ في سنة 2008 ويعتبر الجهاز الوحيد المختص بهذا الصدد في الجزائر، وهدف إلى تأمين منظومة المعلومات لخدمة الأمن العمومي، واعتبر بمثابة مركز توثيق ومقره يوجد ببئر مراد رايس، وهذا المركز يعكف على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها سواء كانوا أشخاص فرادى أو عصابات، وهذا كله من أجل تأمين الأنظمة المعلوماتية والحفاظ عليها، لاسيما تلك المستعملة في المؤسسات الرسمية وللبنوك. [1]

كما يهدف إلى مساعدة باقي الأجهزة الأمنية الأخرى في أداء مهامها، واستطاعت قيادة الدرك الوطني من خلال التكوين المستمر والمتميز لأفرادها وكذا الملتقيات الدولية والوطنية وتبادل الخبرات مع دول أخرى أن توفر القوى المؤهلة وذات الكفاءة.وقد استطاع المركز من معالجة أزيد من 100 جريمة إلكترونية سنة 2014 وما يفوق 500 قضية رقمية خلال سنة 2015 منها 300 جريمة تتعلق بموقع التواصل الاجتماعي "فايسبوك"

[2]- .رضوان، **المرجع السابق**، ص 43.

[1]- بارة سمير، ال**مرجع السابق**، ص10.

و20 جريمة رقمية تعلقت باختراق مواقع رسمية لمؤسسات خاصة وعامة، وهي ارقام معتبرة ومجرموها أنظمة المعالجة الآلية للمعطيات. [1]

– المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني.

مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة لوزير الدفاع الوطني مكلفة بمهام متعددة كإجراء الخبرات والفحوص في إطار التحريات الأولية والتحقيقات القضائية، ضمان المساعدة العلمية أثناء القيام بالتحريات المعقدة. [2]

المساهمة في تنظيم دورات الإتقان والتكوين ما بعد التدرج في تخصص العلوم الجنائية، ولتأدية مهامه على أكمل وجه فإن المعهد الوطني للأدلة الجنائية وعلم الإجرام يحتوي على العديد من الأقسام والمصالح المختصة من أهمها: مصلحة البصمات؛ مصلحة البيئة؛ أما في ما يخص مجال الأمن السيبراني هناك مصلحة الإعلام الآلي: على مستوى هذه المصلحة يتم رصد ومراقبة وتتبع عمليات الاختراق والقرصنة المعلوماتية وكذا اكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية. [3]

–. المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني.

استجابت لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الإلكترونية قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الإلكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية، والتي كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة الإلكترونية وعلى مستوى المديرية العامة للأمن الوطني والتي أنشئت سنة 2011 ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بقرار من المدير العام للأمن الوطني وأضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015. [4]

---

[1] – **المرجع نفسه**، ص 12..

[2] – عز الدين عز الدين، **"الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها"**، قيادة الدرك الوطني، **مداخلة بالملتقى الوطني حول: الجريمة المعلوماتية بين الوقاية والمكافحة**، (جامعة محمد خيضر ببسكرة، 16 نوفمبر 1015)، ص 30.

[3] – **المرجع نفسه**، ص 31.

[4] – عز الدين عز الدين، **المرجع السابق**، ص 39.

– الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

تشكلت هذه الهيئة بمقتضى المرسوم الرئاسي رقم 15-261[1] وهي سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت إشراف ومراقبة لجنة مديرية يترأسها وزير العدل وتضم أساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

وكلفت الهيئة باقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما وتنشيط وتنسيق عمليات الوقاية منها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة هذه الجرائم، من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية، وضمان المراقبة الوقائية للاتصالات الإلكترونية، قصد الكشف عن جرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة[2].

المطلب الثاني: الآليات التشريعية والقانونية.

تركزت أساسا في مجال اتخاذ التدابير القانونية دون غيرها من التدابير الأخرى، ويتضح ذلك من خلال صدور القانون رقم 09-04 المؤرخ في 05 أوت 2009، الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، والتي تم فيه تحديد الحالات التي تسمح باللجوء إلى مراقبة الاتصالات الإلكترونية.

بناء على ما ورد في المادة 4 التي نصت على ما يلي:[3]

– للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والجرائم الماسة بأمن الدولة.

---

[1]– الجمهورية الجزائرية الديمقراطية الشعبية، مرسوم رئاسي15-261 مؤرخ في 2015/10/08، يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال والمكافحة الجريدة الرسمية، العدد 53، الصادرة بتاريخ 2015/10/08، ص ص16-20.

[2]– إلهام غازي، **"الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري"**، مجلة الجيش، مؤسسة المنشورات العسكرية، العدد630، جانفي 2016، ص44.

[3]– الجمهورية الجزائرية الديمقراطية الشعبية، قانون رقم 9-4 المؤرخ في 14 شعبان 1430، الموافق 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادرة بتاريخ 25 شعبان 1430 الموافق لـــ 16 أوت 2009، ص06.

– في حالة توفر معلومات عن احتمال اعتداء 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 اللجوء إلى المراقبة الإلكترونية في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

كما نصت المادة 13 على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. وهذا ما تم من خلال صدور المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر سنة 2015، والذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. ومن المهام التي تمارسها الهيئة ما ورد في المادة 4 من المرسوم التي نصت على ما يلي:[1]

– اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

– تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

– مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية.

– ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى.

– تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.

– المساهمة في تكوين المحققين المختصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال.

–المساهمة في تحديث المعايير القانونية في مجال اختصاصها.

[1]– الجمهورية الجزائرية الديمقراطية الشعبية، مرسوم رئاسي رقم 15-261 مؤرخ في 24 ذي الحجة عام 1436، مرجع سابق، ص ص16-17.

– المساهمة في تحديث المعايير القانونية في مجال اختصاصاتها.[1]

إضافة إلى اهتمامها بالجانب القانوني والمؤسساتي الذي تم ذكره، فقد نظمت مديرية الاتصال والإعلام والتوجيه أركان الجيش الوطني الشعبي جملة من ملتقيات حول "الجيش الوطني الشعبي ورهانات تداول المعلومة عبر شبكات التواصل الاجتماعي" وقد أجمع فيه على ضرورة تحلي العقيدة الأمنية الجزائرية بالمزيد من اليقظة والتحكم في التكنولوجيات الحديثة.

وكذلك التنبيه بمخاطر سوء استعمالها إضافة إلى توسيع إشراك فواعل جديدة من خارج المؤسسة العسكرية، والذين بوسعهم المساهمة في صيانة عقيدة الدفاع الوطني. فالفضاء السيبراني أصبح من بين الميادين الأكثر أهمية ويحتل المرتبة الخامسة للتراعات بعد البر والبحر والجو والفضاء.[2]

[1] – ب. بوعلام، ملتقى حول "**الجيش الوطني الشعبي ورهانات تداول المعلومات عبر شبكات التواصل الاجتماعي**"، مجلة الجيش، (مؤسسة المنشورات العسكرية، العدد 630، جانفي 2016)، ص39.

[2] – ب. بوعلام، **المرجع السابق**، ص ص38-39.

المبحث الثالث: التنسيق الاقليمي لمكافحة الجريمة السيبرانية.

إن بناء منظومة جدية لمواجهة الجرائم السيبرانية ينبغي تكاثف مختلف الجهود الدولية والاقيليمة، يغية التنسيق سواء من خلال القانون الدولي أو مختلف الاتفاقيات بين الدول سواء الثانية أة الجماعية، وهو ما سيتم توضيحه في الأتي:

المطلب الأول: آليات التعاون الاقليمي.

تتلاءم الاتفاقيات الإقليمية مع متطلبات مواكبة طبيعة وسرعة الجرائم السيبرانية، ويسجل في ذلك عدد من المبادرات كمبادرة شانغهاي، ومبادرة رابط البلدان المستقلة. ففي عام 2002 وضعت مجموعة بلدان الكومنولت، التي تضم 53 دولة، قانونا نموذجيا لمكافحة الجريمة السيبرانية، حرصت على أن يأتي منسجما مع الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية .

وفي العام 2009 بادرت المجموعة الاقتصادية بغرب إفريقيا المؤلفة من 15 دولة عضوا إلى إقرار توصيات لمكافحة الجريمة السيبرانية، وتشكيل الإطار القانوني لعمل الدول الأعضاء. مبادرة من قبل السوق المشتركة لشرق وجنوب إفريقيا في العام 2011، لوضع قانون نموذجي حول مختلف جوانب الجريمة السيبرانية. كما جاءت الاتفاقيات العربية لمكافحة جرائم تقنية المعلومات عام 2011، لتعزيز التعاون بين الدول العربية لمكافحة الجرائم السيبراينة والحفاظ على أمنها وأمن مجتمعاتها.[1]

اتفاقية بودابست (اتفاقية الأوروبية لمكافحة الجريمة السيبرانية) قد جاءت هذه الاتفاقية لتكلل جهود مجموعة من الخبراء الأوروبيين، وغير الأوروبيين، كالولايات المتحدة وإفريقيا الجنوبية واليابان إذ دخلت حيز التنفيذ عام 2004 كأداة إقليمية مهمتها مكافحة الجريمة السيبرانية عبر تحقيق الانسجام بين القوانين الوطنية، وقد ركزت بشكل خاص على تحسين تقنيات التحقيق والبحث وزيادة التعاون بين الدول، دخلت حيز التطبيق في 2007، وتوزعت بنود الاتفاقية، على محاور ثلاثة:

الانسجام بين التشريعات الوطنية التي تجرم الأعمال غير القانونية في الفضاء السيبراني.

تحديد وسائل التحقيق والملاحقة الجزائية.

[1]- عادل عبد الصادق، **المرجع السابق**، ص333.

وضع نظام تعاوني بين الدول، يتصف بالسرعة والفاعلية.

وترتكز أهمية هذه الاتفاقية بفعاليتها على إقرارها إجراءات عملية، تلتزم الدول المنظمة بإدراجها في قوانينها الوطنية مثل تلك الخاصة بجمع بيانات الاتصال وحفظها، بما يتيح تحديد مصدرها، ونقطة وصولها، وصلاحية الجهات القضائية المعنية، والمساعدة المتبادلة وتسليم المجرمين.[1]

لقد بذلت جهود عدة من قبل دول ومنظمات دولية وإقليمية بعمل متخصصين، وبدعم من الاتحاد الدولي للاتصالات لإقرار مجموعة من المعايير والقواعد التي تسير وتنظم المجال السيبراني وتضمن الاستخدام السلمي للمجال السيبراني، فبالرغم من قيمتها ووزنها دوليا فتبقى هذه الجهود والتوصيات غبر كافية ولا فاعلة نظرا لغياب فكرة الالتزام القانوني، وعدم إتاحتها إمكانية العقاب ما نتج عن الهوة الرقمية بين الدول التي تزرع الشك وغياب الثقة، خاصة مع سيطرة الولايات المتحدة الأمريكية لفضاء الانترنيت.[2]

وسيتم وضع بعض التوصيات التي يتبناها المرصد العربي للسلامة والأمن في الفضاء السيبراني وأهمها:

– التزام القرارات الصادرة عن الأمم المتحدة وعن القمة العالمية لمجتمع المعلومات والداعية إلى نشر ثقافة الأمن السيبراني.

– اتخاذ تدابير تعتمد الأمن كعنصر ضروري بين الإنتاج لاسيما ما يخص البرامج والأجهزة المستخدمة فقي تقنيات الاتصال.

– رفع إطار تعاون يضمن تبادل المعلومات ونقل الممارسات بين مجال الأمن.

تامين انسجام الأنظمة القانونية لمكافحة الجرائم السيبرانية، بما يمنع سوء جنات رقمية.

– استراتيجية لنشر الوعي وبنائه لدى مختلف شرائح المجتمع، سواء منهم المستخدمين العاديين أو المهنيين أو متخذي القرار، والمسؤولون عن سياسات الأمن والسلامة.

– اعتماد مبادئ أخلاقية السلوك السيبراني، على مثال أخلاقيات وأصول التعامل القائمة في المجتمع التقليدي، وتكون بمثابة عقد اجتماعي، يؤسس لسلوك يضمن سلامة الجماعة وسلامة مواردها.

[1]– مني الاشقر جبور، **"السيبرانية هاجس العمر"، مرجع سابق**، ص 103-104.

[2]– حمدون تورين، **مرجع سابق**، ص: 35.

– وضع استراتيجية، وسياسة أمنية واضحة وملزمة لكل المعنيين بصناعة المعلومات.

– اخذ جميع الأمن السيبراني بعين الاعتبار لدى وضع أي استراتيجية أو سياسة، بما في ذلك حاجات المواطنين والمؤسسات، كما حقوقهم وواجباتهم.

– الإقرار بالمسؤولية عن تحقيق الأمن السيبراني، كجزء لا يتجزأ من الأمن القومي والوطني.

– إنشاء مراكز للسلامة المعلوماتية ولطوارئ الاتصالات، تتعاون فيما بينها وفق آلية واضحة وشفافة وفعالة.

– تدريب وتأهيل وحدات عسكرية وأمنية خاص يمكنها مراقبة البني التحتية للاتصالات.

– تأهيل وحدات أمنية وعسكرية خاصة، تتولى التعاون على المستوى الخارجي مع الهيئات العاملة على مكافحة المخاطر والحد منها ومن أثارها.[1]

المطلب الثاني: سبل تعزيز التنسيق الإقليمي – الدولي لمكافحة الجريمة الالكترونية.

تحولت المخاطر السيبيرانية بما تمثله من تهديد للفرد والمجتمع والدولة، إلى مسألة تدرج على نواتج الطوارئ الدولية وكان الإتحاد الدولي للعلماء قد أدرجها على لائحة اهتماماته كواحدة من المسائل التي لابد من معالجتها، قبل أن تتحول إلى سبب اندلاع الحروب، ووقوع كوارث تضر كذلك الإنسانية جمعاء، دون أي تميز بين الدول المتقدمة تكنولوجيا، أو تلك الأقل تقدما، وللحد ومواجهة هذه المخاطر السيبيرانية وتهديداتها قدم الاتحاد بناء على ذلك، تقريرا في عام 2003 إلى القمة العالمية لمجتمع المعلومات، التي انعقدت في جينيف، بعنوان (نحو نظام عالمي للفضاء السيبيراني) اقترح فيه عددا من التوصيات التي تعتبر إجراءا دوليا لمواجهة هذه التهديدات السيبيرانية جاء فيها كالتالي: [2]

– حث الأمم المتحدة على قيادة الجهود بين الحكومات المختلفة، لتأمين عمل وسلامة الفضاء السيبيراني، بحيث لا يتحول إلى مرتفع للمخاطر، نتيجة استغلال الجريمة.

– إيجاد قانون شامل للفضاء السيبيراني، وتحقيق الانسجام بين التشريعات الوطنية، التي تحكم الجريمة السيبيرانية من خلال نموذج يمكن أن يكون الاتفاقية الأوروبية لمكافحة الجريمة السيبيرانية، ووضع قواعد تعاون دولي.

[1]– منى الأشقر، "**الأمن السيبري: التحديات ومستلزمات المواجهة**"، (اللقاء السنوي الأول للمتخصصين في أمن وسلامة الفضاء السيبراني، بيروت، 27-28- أغسطس 2012، جامعة الدول العربية: المركز العربي للبحوث القانونية والقضائية)، ص: 15.

[2]– منى الأشقر جبور، "**السيرانية هاجس العصر**"، **مرجع سابق**، ص48.

– تطبيق القوانين الدولية من قبل هيئات مختصة في الأمم المتحدة، على الاعتداءات السيبيرانية التي يمكنها أن تهدد السلم الدولي، مثل الإرهاب السيبيراني، والحرب السيبيراني، الجريمة السيبيرانية.

من الملاحظ أن التوصيات ركزت على مسائل سيبيرانية اتخذت ومازالت، طابع الضرورة والأهمية مثل الحرب السيبيرانية، والإرهاب، والنزاعات السيبيرانية بشكل عام، إضافة إلى ضرورة تحقيق التوازن في مجتمع المعلومات، بما يضمن بناء الثقة والاستقرار، من خلال حماية الحريات والخصوصية.

– دراسة السيناريوهات والمعايير والعقوبات السيبيرانية التي يمكن أن تطبق على مرتكبي الاعتداءات.

– دراسة إمكانية إنشاء وكالة دولية، تكون لها صلاحية دراسة ومراجعة قواعد السلوك في الفضاء السيبيراني وتسهيل تبادل الخبرات والتقنيات.

– تعزيز التعاون بين الدول، وإرساء شراكات بين القطاعين العام والخاص، والتنسيق بين مختلف المقاييس الدولية لتأمين إدارة أكثر فاعلية للمخاطر السيبيرانية، وتبادل المعلومات حول الاعتداءات السيبيرانية، كما تبادل الخبرات التقنية في مجال الحماية، بما يعزز أمن الأنظمة والشبكات وتبادل المعلومات.

– إلزام المسؤولين من إدارة الموارد المعلوماتية والاتصالات، في القطاعين العام والخاص، باتخاذ الإجراءات الضرورية للحماية، وبتقييم المخاطر، وبحماية البيانات والبنية التحتية الخاصة بمؤسساتهم، ويمكن للإجراءات أن تلحظ تأمين المخاطر، والحوادث التي يمكن أن تقع.

– تعزيز دور المؤسسات الدولية كالإنتربول والإقليمية كالأفريوبول Afripol، في مجال مكافحة الجريمة السيبيرانية.

– مقاربة المسائل العلمية والتقنية، الخاصة بالأمن السيبيراني، من جوانبها المختلفة، لاسيما منها تلك التي تتقاطع مع استخدام التقنيات، مثل الخصوصية، وحماية البيانات، والحريات العامة والخاصة.

– المبادرة إلى مساعدة الدول النامية، والجهات المتاحة على فهم تأثير التقنيات على التنمية، في بيئة تعزز السلامة والأمن، كما تساعد على هدم القوة الرقمية بين المجتمعات.[1]

[1]– الاتحاد الولي للاتصالات، "**البحث عن السلام السيبراني**"، تاريخ التصفح: 01-04-2020، من الرابط:
ww.itu.int/pub/s-gen-wfs ،

1- **أجهزة الحماية.**

يعتبر إنشاء حماية على جهاز المضيف، من أكثر الطرق فاعلية، وأقلها كلفة في تأمين حماية الأجهزة المتصلة عبر الشبكة. وغالبا ما يلجأ في هذا المجال إلى ما يعرف بجدار النار، وبرامج تقنية. وتعتبر هذه البرمجيات من الأدوات التي تستخدم في حماية الأنظمة، كما في منع الوصول إلى المواقع، أو معلومات معينة فالتقنية من الأدوات التي تستعمل لحماية بعض الفئات الاجتماعية والعصرية (الأطفال والشباب) إلا أنها تلعب دورا في الحماية عندما تمنع الدخول إلى مواقع يمكن أن تحتوي برامج وفيروسات، وغيرها من البرمجيات الضارة. ويعتمد في حماية البيانات أثناء عبورها، عدد من البروتوكولات، كنظام أمن الإتصالات SSL وتستخدم بروتوكولات الحماية، تقنيات تدعم الترميز والتشفير ليس سوى جزء من الحماية،(ISPEC) والتي يجب أن تطاول ليس فقط المعلومات وإنما البرنامج أيضا كما يفترض الانتباه هنا إلى المكان الذي يحفظ فيه مفتاح فك الشفرة والرمز، ومن الأفضل التعامل في هذا المجال مع الحل الأمني، الذي تواكبه عملية تصديق جهة ثالثة.

2- التشفير: يعتبر التشفير من التقنيات التي يمكن اللجوء إليها، كوسيلة أساسية في حماية المعلومات الشخصية والمعلومات السرية، فالتشفير تقنية تساعد على حماية المعلومات عبر تحويل النصوص إلى رموز لا يمكن قراءتها إلا بعد إعادة تحويلها إلى نصوص مقروءة من خلال عملية تفكيك هذه الرموز.[1]

ولتقنية التشفير دور هام، في الحماية من عدد من التهديدات السيبيرانية، لاسيما وأنها تحمي المعلومات، والبيانات الشخصية، كتلك المتعلقة ببطاقات الإئتمان والأسماء والعناوين، ومضمون الرسائل الإلكتروني، والمعلومات التي تنقل عبر شبكة الإنترنت وذلك في حال اعتراضها أو الوصول إليها دون رغبة صاحبها، كذلك تستخدم تقنيات التشفير في مجال تأكيد مصداقية الوثائق الإلكترونية وضمان صحة المعلومات والبيانات، لاسيما منها التوقيع. ما يمنع التلاعب بمصداقية الوثائق والمعلومات. ويعتمد على التشفير أيضا في العديد من برامج وأنظمة الدفع على الإنترنت، التي تستخدم العملة الرقمية ومعالجة الشبكات والتحويل الإلكتروني للأموال، وما إلى ذلك.[2]

---

[1]- **دليل عملي للعمل مع المنظمات الدولية**، من الرابط:

https://www.mandint.org/ar/guide-IO

[2]- منى الأشقر جبور، "**السيرانية هاجس العصر**"، **المرجع السابق**، ص ص62-63.

المطلب الثالث: مستقبل الأمن السيبراني في الجزائر على ضوء التحديات الراهنة .

تعتبر الجزائر كغيرها من الدول تسعى نحو تبني مقاربة الحوكمة الالكترونية، وعلى الرغم من حداثة التوجه، إلا أن عدد الجرائم المرتكبة يوحي بحجم الأخطار التي تتربصها، وهو ما يجعل مؤسسة الدفاع الوطني أمام تحديات وعوائق جديدة وهو تحقيق الأمن السيبراني حاليا ومستقبلا.

تواجه مصالح الدرك الوطني ومصالح الأمن الوطني العديد من العوائق والتحديات التي تعيقها في تحقيق الأمن السيبراني في الجزائر، يمكن أن نذكر أهمها بما يلي:

-زيادة عدد المشتركين في شبكة الانترنت (أكثر من 10 ملايين مشترك في الجزائر) ومع زيادة عدد مستخدمي الشبكة تزداد المخاطر، لتتحول عملية اكتشاف هوية مرتكبي الجرائم الالكترونية الى تحدي سبب صعوبة البحث والتحري ضمن هذا العدد الهائل والمتجه نحو الارتفاع باستمرار.

- انتشار تكنولوجيا الانترنيت فائقة السرعة والتدفق (VSAT/ADSL/SDSL) تتهم التكنولوجيا في سرعة انجاز الجريمة، وهذا يضع الجهات الأمنية المتخصصة أمام تحدي سرعة مباشرة التحقيقات ومتابعة الجناة، والتسلح بالأجهزة المتطورة في سرعة انجاز الجريمة وهذا يضع الجهات الأمنية المتخصصة أمام سرعة مباشرة التحقيقات ومتابعة الجناة، والتسلح بالأجهزة المتطورة والبرامج الحديثة السريعة الخدمة.

- التطور التكنولوجي وظهور الانترنيت لم يعد المجرم يحتاج للجلوس وراء الحواسيب الموصولة سلكيا بشبكة الانترنيت للقيام بجريمته مما يستدعي من الجهات الأمنية رفع التحدي والاستعداد بأحدث التقنيات.

- الاستعمال الواسع لشبكات التواصل الاجتماعي إذ وصل عدد مستعملي هذه المواقع في الجزائر الالكترونية لأكثر من 7 ملايين مستعمل ما ساهم بشكل كبير في ارتفاع أنواع متعددة من الجرائم الالكترونية مثل القذف، التحرش الجنسي، استغلال القصر، وغيرها وهذا ما يستوجب وضع استراتيجيات جد مكملة لضمان الآمن السيبراني عند استخدام مواقع التواصل الاجتماعي. [1]

- عمليات التخفي أثناء استعمال خدمات شبكة الانترنت (Proxy)، يعد من أكبر الإشكاليات التي تواجهها الجهات المتخصصة بالتحقيق، ويتطلب تعاون جهات متعددة والتسلح بالوسائل المتطورة التي يمكن لها رصد الجزئيات وفك الشفرات وتطوير البنى الخاصة بالمعلومات وتحديثها باستمرار، وتصميم برامج عالية التطور.

[1]- عز الدين عز الدين، **المرجع السابق**، ص 51.

-غياب التنسيق بين الدول والحكومات اذ من المعلوم أن الجريمة الالكترونية عابرة للحدود والقارات، وهو ما يعني أن مرتكبيها يمكنهم النفاذ إلى أنظمة الحاسوب في أحد الدول، يتم التلاعب واختراق البيانات في بلد آخر، تسجل النتائج في بلد ثالث، ناهيك عن أنه من الممكن وكل هذا يساعد المجرم الالكتروني في إخفاء هويته ونقل الموارد من خلال قنوات موجودة في بلدان مختلفة، وبالتالي ونتيجة القدرة على التنقل إلكترونيا من شبكة إلى أخرى والنفاذ إلى قواعد البيانات في قارات مختلفة، تصبح عدة دول ومحاكم وقوانين معينة بذلك، ما يشكل تحديا حقيقيا، وذلك فان المحاربة الفعالة للجريمة الالكترونية تستدعي تعاونا سريعا وفعالا على أعلى درجات التنسيق.[1]

-التطور التكنولوجي في مجال الأنترنيت والاتصالات وهو ما يفرض على الأجهزة الامنية المختصة بأن تساير هذا التطور، سواء من حيث إكتساب التكنولوجيا أو من حيث التمكن من استخدامها واستثمارها بالشكل اللازم ، هذا ما يرهق ميزانيتها المحدودة ولذلك يتوجب تركيز جميع الامكانيات المادية، المالية والبشرية اللازمة لتحقيق الامن السيبراني.

-نشر التوعية لمفهوم الامن السيبراني لمستخدمي شبكة الانترنيت، وهو ما يستوجب القيام بحملات توعوية بين مستخدمي شبكة الانترنيت لاتخاذ التدابير اللازمة لضمان الحد الأدنى من الأمان، وتعليمهم ضرورة التحلي بثقافة التبليغ في الوقت اللازم لتتمكن الجهات المعنية من القيام بدروها في الوقت المناسب، والتوصل الى مرتكبي الجرائم.

-تفعيل القوانين على أرض الواقع وتطبيقها بصرامة إذ من بين أكبر الاشكاليات التي تسهم في إنتشار الجريمة الالكترونية، هو الإفلات من العقاب، والتأخر في تفعيل القوانين وهو ما يمنح المجرم فرصا لتكرار جرائمه، ولذلك من الضروري تأكيد على تطبيق القوانين كما يجب أن تتكيف النصوص القانونية مع التغيرات الحاصلة في هذا المجال، كما يتوجب انشاء محاكم متخصصة بالجرائم الالكترونية نظرا للانتشار الواسع لهذه الجرائم. [2]

---

[1]- كريستينا سكولمان،" الإجراءات الوقائية والتعاون الدولي لمحاربة الجريمة الإلكترونية"، في: برنامج الأمم المتحدة، برنامج الأمم المتحدة، **برنامج تعزيز حكم القانون في بعض الدول العربية -مشروع تحديث النيابات العامة، أعمال الندوة الإقليمية حول: الجرائم المتصلة بالكمبيوتر**، المملكة المغربية، 19-20 يونيو 2007، ص 119.

[2]- بارة سمير، **المرجع السابق**، ص18.

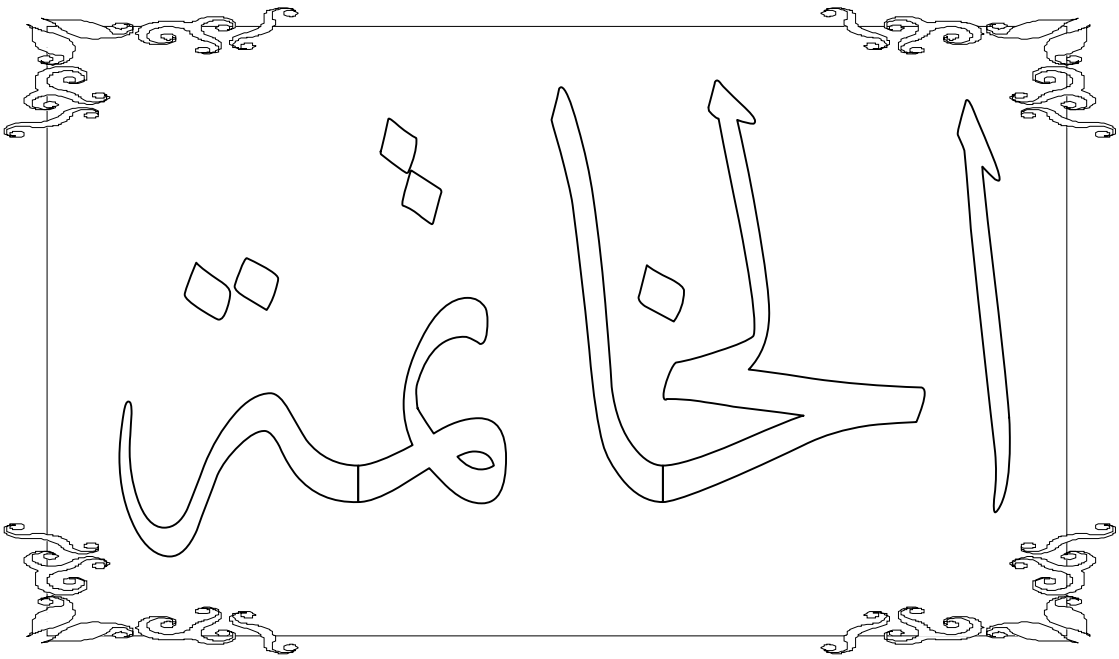
خلاصة الفصل.

بعد التطرق للاستراتيجية الجزائرية في مكافحة الجريمة السيبرانية وانطلاقا من ما تم سرده من معلومات في هذا الفصل توصلنا الى العديد من النتائج والتي نوضحا في التالي:

- كانت الجزائر من بين الدول التي تعرضت للعديد من الجرائم السيبرانية، وذلك اجع لدخولها العالم الرقمي لذلك حاولت الجزائر بالعديد من الطرق للتصدي لهذه الجرائم.

- قامت الجزائر بوع العديد من الاليات لمواجهة الجزائر السيبرانية تمثلت في الآليات الأمنية بوضع تشريعات قانونية، واستغلال التطور التقني باستخدام كافة الوسائل التكنولوجية المتاحة، ووضع جهاز للعمليات في العديد من الوحدات الامنية المختصة ي مواجهة هذه الجرائم.

- الجزائر لم تكتفي بالاستراتيجيات المحلية فقط، بل تعدت ذلك الى التنسيق مع العديد من الدول لمكافحة هذه الجرائم، والاستفادة من خبرة الدول خاصة المتطور منها.


الخاتمة

بعد دراستنا للاستراتيجيات الدولية في مكافحة الجريمة السيبرانية وبالتركيز على حالة الجزائر وبعد تحليل العلاقة التي ترتبط بين المتغيرين توصلنا إلى ان الدول ومنها الجزائر استطاعت ان تضع العديد من الاستراتيجيات لمواجه الجرائم السيبرانية، بالاضافة الى تطوير هذه الاستراتيجيات مع تطور انواع االتهديدات والجرائم السيبرانية، وكانت هذه الاستراتيجيات تتمثل في العديد من الاليات منها القانونية المتمثلة في تشريعات لمواجهة هذه الضاهرة بالاضافة الى استراتيجيات المواجهة عن طريق الفضاء السيبراني بردع المخترقين، ووضع شبكة امنية قوية لا تتعرض للاختراق.

❖ نتائج الدراسة.

ومن خلال الدراسة والاجابة على الإشكالية المطروحة والتأكد من صحة الفرضية توصلت الدراسة إلى النتائج التالية:

1. تعقدت مهمة إيجاد تعريف موحد كامل وشامل لمصطلح الجرائم السيبرانية نظرا لتعدد استخداماته والتطورات المعرفية التي مر بها واستخدامه من الباحثين بدلالة عدد غير محدود من المفاهيم المقاربة.

2. أصبح الفضاء السيبراني مجالا جديدا للتفاعلات الدولية مع التطور الهائل في الثورة المعلوماتية، كما أصبح الامن الإلكتروني إحدى أعلى أولويات الأمن القومي، وذلك راجع لكثرة التهديدات لتي انتشرت في هذا الفضاء.

3. تطورت التهديدات الإلكترونية وتنوعت أشكالها وتعددت آثارها وإنعكاستها لتشمل جميع المجالات، وعليه أصبحنا أمام جرائم حقيقية مست الأمن القومي للدول وأثرت عليه، ومن أمثلة تلك الجرائم، الجريمة الإلكترونية.

4. تعتبر التهديدات الإلكترونية تهديدات خطيرة جدا ،تهدد الأمن القومي للدول، وتمس قضايا السيادة الدولية وهي بذلك تهديدات عابرة للحدود الدولية، لذلك تسعى الدول لتامين نفسها الكترونيا، وظهر مصطلح جديد في ادبيات الدراسات الامنية يعرف بالامن السيبراني.

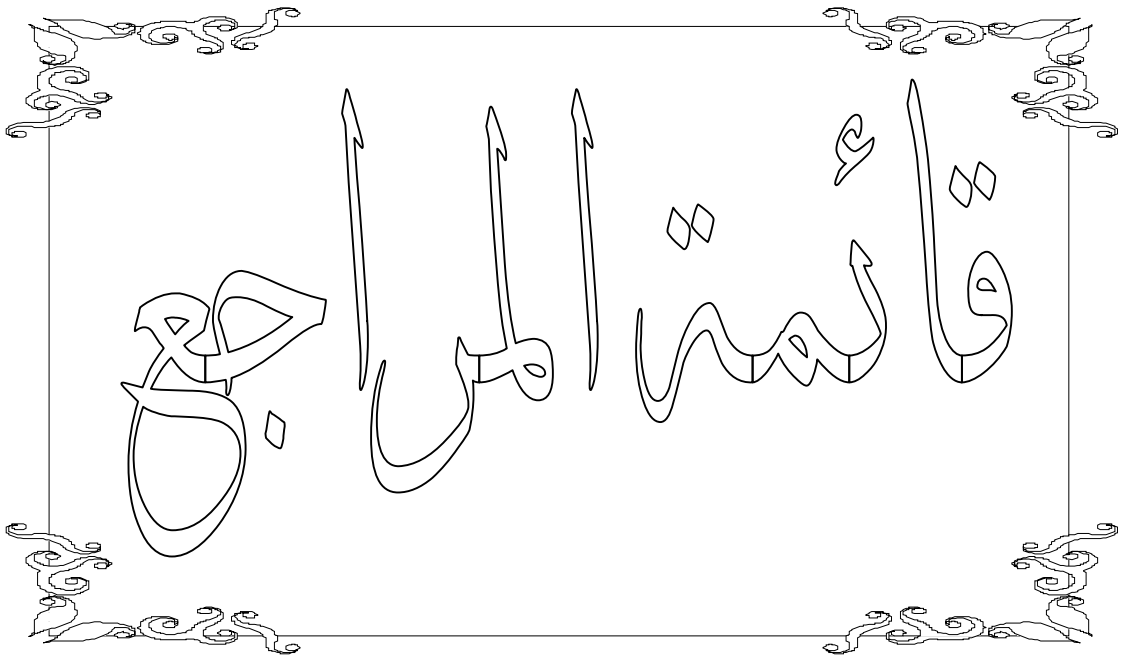
5. يمكن التمييز بين صورتين من الحروب الإلكترونية، تقليدية ارتبطت بعمليات التشويش الإلكتروني وكان استعمالها في ميدان القتال، وأخرى حديثة ارتبطت بظهور الحواسيب وشبكة الانترنيت ميدانها هو الفضاء السيبراني.

6. إن الاعتداءات السيبرانية أخذت أبعاد عالمية ودولية، فبفضل ذلك ازداد الاهتمام بالتعاون الدولي من أجل مكافحتها وإدارة هذه التهديدات، وبذلك ظهرت فكرة لحماية الفضاء السيبراني، ومواجهة المخاطر من التجمع الدولي للعلماء الذي أشار إلى هذا التعاون كنظام دولي للفضاء السيبراني، يعمل على جميع مسائل الجريمة بما فيها الجريمة السيبرانية وقد قادت الأمم المتحدة هذه الجهود سواء عبر إقراراها تنظيم القمة العالمية لمجتمع المعلومات أو إنشائها مجموعات عمل لمكافحة الجريمة السيبرانية

7. ابرم المجلس الاوروبي اتفاقية بشان الجريمة السيبرانية واعتمدت في بروكسيل يوم 23 نوفمبر2001، وهي أول اتفاقية توضع للتعاطي مع الطابع الدولي للجريمة السيبرانية، ودخلت تلك الاتفاقية حيز السريان في جوان.

8. قامت الدول العربية بوضع تشريعات بشأن الجريمة السيبرانية، ووضع نموذج لمكافحة الجرائم التقنية في أنظمة المعلوماتية والذي صادق عليه مجلس وزراء العدل العرب في 2003/10/08، وقد جاء هذا القانون بجملة من الأحكام الموضوعية والإجرائية تعمل على الحد من الجريمة السيبرانية.

9. انشات الجزائر مركز للوقاية من الجرائم المعلوماتية تحت اشراف الدرك الوطني، وقد أنشئ في سنة 2008 ويعتبر الجهاز الوحيد المختص بهذا الصدد في الجزائر، وهدف إلى تأمين منظومة المعلومات لخدمة الأمن العمومي وهذا المركز يعكف على تحليل معطيات وبيانات الجرائم السيبرانية المرتكبة.


قائمة المراجع

قائمة المراجع

➢ الكتب

1. البعلبكي منير رمزي البعلبكي منير، **المورد الحديث**، (لبنان: دار العلوم للملايين)

2. تورين حمدون، **دليل الأمن السيبراني للبلدان النامية**، (جنيف الاتحاد الدولي للاتصالات، د.ب 2006)

3. حسن فاروق فؤاد، **مدخل إلى أمن المعلومات وتعريف الجرائم الإلكترونية وكيفية الحماية والإستخدام الأمثل للموارد المتوفرة للوصول إلى أقصى درجات الحماية في دوائر وزارة الداخلية العراقية**، (وزارة الداخلية: المديرية العامة للاتصالات والمعلوماتية، قسم التدريب والتطوير، شعبة الدراسات والبحوث، د س)

4. حسين خليل، وحسين عبيد، **الإستراتيجيا**، (بيروت: منشورات الحلبي الحقوقية، 2013)

5. الخضرا ديما، **مترجما**، **نظريات العلاقات الدولية: التخصص والتنوع**، (الدوحة: المركز العربي للأبحاث ودراسة السياسات 2016)

6. الرومي محمد أمين، **جرائم الكمبيورتر والانترنت** ، (الإسكندرية، دار المطبوعات الجامعية، 2004)

7. زكريا فؤاد، **التفكير العلمي**، الطبعة الثالثة، (الكويت: المجلس الوطني للثقافة والفنون، 1978)

8. العوادي أوس مجيد غالب، **الأمن المعلوماتي السيبراني**، (سلسلة إصدارات مركز البيان للدراسات والتخطيط، أوت 2016)

9. عون ميشال، **دراسة موجزة عن الإستراتيجية**، (الرابية، 2008)

10. فهمي عبد القادر محمد، **المدخل إلى دراسة الإستراتيجية**، (عمان: دار مجدلاوي للنشر والتوزيع، 2010)

11. قوجيلي سيد أحمد، تطور الدراسات الأمنية ومعضلة التطبيق في العالم العربي، (أبوظبي: مركز الإمارات للدراسات والبحوث الإستراتيجية، 2012)

12. مراد علي عباس، **الأمن والأمن القومي: مقاربات نظرية**، (الجزائر: إبن النديم للنشر والتوزيع، 2017)

13. نيوف صلاح، **مدخل إلى الفكر الإستراتيجي**، (الدنمارك: الأكاديمية العربية المفتوحة، د س ن)

14. وراد ضياء، **مترجما، الكون الرقمي: الثورة العالمية في الإتصالات**، (المملكة المتحدة: مؤسسة هنداوي سي آي سي للنشر،2017)

15. الاتحاد الدولي للاتصالات، **دليل الامن السيبراني للبلدان النامية**، (جنيف: مكتب تنمية الاتصالات 2009)

➢ المجلات والدوريات.

أولا: باللغة العربية.

1. بوعلام، ملتقى حول " الجيش الوطني الشعبي ورهانات تداول المعلومات عبر شبكات التواصل الاجتماعي " **مجلة الجيش**، العدد 630،(جانفي 2016)

2. جبور منى الأشقر، " الأمن السيبراني: التحديات ومستلزمات المواجهة "، **المركز العربي للبحوث القانونية والقضائية**، (2012)

3. رضوان، " الأمن السيبراني :أولوية في استراتيجيات الدفاع"، **مجلة الجيش** .العدد 630، (جانفي 2016)

4. الشهري حسن بن أحمد،" الإرهاب الالكتروني حرب الشبكات "، **المجلة العربية الدولية للمعلوماتية** (2015)

5. طويلة جميل حسين، " البرمجيات الخبيثة "، (دليل عملي لإستخدام البرمجيات الخبيثة وبرمجيات التجسس وإجراءات الوقاية والحماية منها، د س)

6. عبد الصادق عادل، " أسلحة الفضاء الالكتروني في ضوء القانون الدولي "، **سلسلة أوراق**، العدد 23، مكتبة الإسكندرية، (2016)

7. عبد الصادق عادل،" الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي "، **المركز العربي لأبحاث الفضاء الإلكتروني**(2017)

8. غازي إلهام، " الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري "، **مجلة الجيش**، مؤسسة المنشورات العسكرية، العدد 630، (جانفي 2016)

9. غودي ميشال، قيس الهمامي، " الاستشراف الإستراتيجي والمشاكل والمناهج "، **مجلة ليبسور**، العدد 6 (2005)

10. الفتلاوي أحمد عيسى نعمة، " الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم المعاصر " **مجلة المحقق الحلي**، (جامعة الكوفة، كلية القانون، 2016).

11. ليتيم فتيحة، ونادية ليتيم، " الأمن المعلوماتي للحوكمة الإلكترونية وإرهاب القرصنة "، **مجلة الفكر**، العدد 12 (د ش، د س)

12. مختار محمد، " هل يمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية؟ "، **مجلة مفاهيم المستقبل**، العدد 06 (يناير 2015)

ثانيا: باللغة الاجنبية.

1. Craigen Dan &Others, **"Defining Cybersecurity"**, (Technology innovation Management Review, Octobre 2014)

2. Gercke Marco, Understanding Cybercrime: Phenomena, Challenges and Legal Response, September (2012)

3. Taureck Rita, **"Securitization Theory and Securitization Studies"**, (university of institutional repository, 2006).

4. Ministry of information and communications technology, Qatar, Rassed, The attitudes of online users in the MENA

5. United Nations Office on Drugs and Crime, UNODC, Comprehensive study on cybercrime, draft, February(2013)

6. Ministry of information and communications technology, Qatar, Rassed, The attitudes of online users

➢ المذكرات والرسائل الجامعية.

1. بودن زكرياء، **أثر التهديدات الإرهابية في شمال مالي على الأمن الوطني الجزائري وإستراتيجيات مواجهتها 2010–2014**، رسالة الماجستير (جامعة: محمد خيضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، 2015)

2. بوطويل نسيمة، **الإستراتيجية الأمنية الأمريكية في منطقة شمال شرق آسيا: دراسة لمرحلة ما بعد الحرب الباردة**، رسالة ماجستير (جامعة: الحاج لخضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية والعلاقات الدولية، 2010)

3. بونعارة ياسمينة، **الجريمة الإلكترونية**، (جامعة: الأمير عبد القادر للعلوم الإسلامية، د س ن)

4. جلعود وليد غسان سعيد، **دور الحرب الإلكترونية في الصراع العربي الإسرائيلي**، مذكرة مقدمة لنيل شهادة الماجستير في التخطيط والتنمية السياسية، (جامعة: النجاح الوطنية، كلية الدراسات العليا، 2013)

5. حمزاوي جويدة، **التصور الأمني الأوروبي: نحو بنية أمنية شاملة وهوية إستراتيجية في المتوسط**، رسالة ماجستير (جامعة: الحاج لخضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، 2011)

6. دلة أمينة مصطفى، **الدراسات الأمنية النقدية**، رسالة ماجستير (جامعة: الجزائر3، كلية العلوم السياسية والإعلام، قسم العلوم السياسية والعلاقات الدولية 2013)

7. دير أمينة، **أثر التهديدات البيئية على واقع الأمن الإنساني في إفريقيا: دراسة حالة دول القرن الإفريقي** رسالة ماجستير (جامعة: محمد خيضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، 2014)

8. فاتن سعيد، **حماية أمن المعلومات في شبكات المكتبات– دراسة حالة أم القرى**،(جامعة: الملك عبد العزيز، د س ن)

9. لبدي حنان، **التحولات الدولية الراهنة وتأثيرها على الإستراتيجية الأمنية في منطقة الساحل الإفريقي** رسالة ماجستير (جامعة: محمد خيضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية والعلاقات الدولية 2015)

➢ ملتقيات ومطبوعات.

1. الأشقر منى، " الأمن السيبري: التحديات ومستلزمات المواجهة "، (اللقاء السنوي الأول للمتخصصين في أمن وسلامة الفضاء السيبراني، بيروت، جامعة الدول العربية: المركز العربي للبحوث القانونية والقضائية، (27-28- أغسطس 2012)

2. بن مرزوق عنترة، " الأمن السيبراني كبعد جديد من السياسة الدفاعية الجزائرية "، (محاضرات مقدمة لطلبة جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، د س)

3. بن مرزوق عنترة، حرشاوي محي الدين، " الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية "، الملتقى الدولي حول سياسات الدفاع الوطني، (جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية (31/01/2017)

4. درويس سعيد، " ماهية الحروب الالكترونية في ضوء قواعد القانون الدولي "، حوليات جامعة الجزائر 1، العدد 01.

5. سكولمان كريستينا، " الإجراءات الوقائية والتعاون الدولي لمحاربة الجريمة الإلكترونية " ، في: برنامج الأمم المتحدة، برنامج الأمم المتحدة، برنامج تعزيز حكم القانون في بعض الدول العربية -مشروع تحديث النيابات العامة، أعمال الندوة الإقليمية حول: الجرائم المتصلة بالكمبيوتر، المملكة المغربية،(19-20 يونيو 2007)

6. عز الدين عز الدين، " الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها "، قيادة الدرك الوطني، مداخلة بالملتقى الوطني حول: الجريمة المعلوماتية بين الوقاية والمكافحة، (جامعة محمد خيضر ببسكرة، (16 نوفمبر 2015)

7. عطية أيسر محمد، "دور الآليات الحديثة للحد من الجرائم المستحدثة :الإرهاب الالكتروني وطرق مواجهته " ورقة مقدمة في الملتقى العلمي :الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، (عمان خلال الفترة32-31 سبتمبر 2014)

➢ مراسيم وقوانيين.

1. الجمهورية الجزائرية الديمقراطية الشعبية، مرسوم رئاسي15-261 مؤرخ في 2015/10/08، يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال والمكافحة الجريدة الرسمية، العدد 53، الصادرة بتاريخ 2015/10/08.

2. الجمهورية الجزائرية الديمقراطية الشعبية، قانون رقم 9-4 المؤرخ في 14 شعبان 1430، الموافق 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادرة بتاريخ 25 شعبان 1430 الموافق لـــ 16 أوت 2009.

➢المواقع الالكترونية.

اولا: باللغة العربية.

1. أمين أمين، **" الأمن السيبراني العالمي... حروب خلفية ومساحات إرهابية "**، متاح على الرابط :

https://www.independentarabia.com/node/93586/ (06/04/2020)

2. جوزيف، س ناي، **" التحكم في الصراع الليبيراني "**، مدونات الجزيرة ، تصفح في 2020/04/10، على الرابط: http://blogs.aljazeera.net/blogs

3. حنان علي سعادة، **" الأمن السيبراني والأمن المعلوماتي "**، تم تصفح الموقع يوم : 20 فيفري 2018. الرابط: http://ae.linkedin.com/sulse/D8A7D984D8A7

4. سامر مؤيد، **" الإستراتيجية من منظور وظيفي إجرائي "**، تم تصفح الموقع يوم : 17 فيفري 2018. الرابط: Fcdrs.com/mag/issue-6-2.html

5. سعد علي الحاج بكري، **" الأمن السيبراني ومعضلة حمايته "**، تم تصفح الموقع يوم : 03 فيفري 2018. الرابط: www.aleqt.com/2017/08/24/article.1241506.html

6. شيماء جابر، **" الاختراق وطرق الحماية منه "**، تم تصفح الموقع يوم : 26 فيفري 2018. الرابط: Https://download-internet-pDF-ebooks.com/4926.Free-book

7. عادل زقاع، **مترجما**، **"مفهوم الأمن في نظرية العلاقات الدولية "**، ، تم تصفح الموقع يوم : 17 فيفري 2018. الرابط: Bohothe.blogspot.com/2010/03/blog-spot-26.html.

8. عادل عبد الصادق، **" المجال الأعلى للأمن السيبراني خطوة في دعم إستراتيجية الأمن القومي "**، تم تصفح الموقع يوم : 23 فيفري 2018. الرابط:
www.accronline.com/article-detal.aspx?!d=20284.

9. عادل عبد الصادق،" صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية "، 26/04/2020 متاح على الرابط http://accronline.com/article_detail.aspx?id=29415

10. عبد السلام البارودي، **" هل دخلت الجزائر عصر الجريمة الالكترونية؟"**، تصفح في: 2020/04/10 على الرابط: https://www.maghrebvoices.com/a/algeria-cyber-inality/414407.html

11. علي محمد إبراهيم كردي، **" المفهوم العسكري للإستراتيجية والتطور التاريخي "**، تم تصفح الموقع يوم 15 فيفري 2018. الرابط: Renanaonline.com/users/alihordi/posts/352158

12. فضيلة غاقلي، **" الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري"**، مركز جيل البحث العلمي، على الرابط: http://jilrc.com تصفح في 2019/05/10.

13. فهد الدريبي، **" ما هو الأمن السيبراني "**، تم تصفح الموقع يوم : 21 فيفري 2018. الرابط:
Https://www.fadvisor.net/blog/2017/11/what is Cyber security/

14. محمود خليل،**" 50 ألف موقع الكتروني لداعش ... .والإرهاب يحاصر الانترنيت"**، من الرابط:
www.alittihad.ae/details.php=120l. تاريخ تصفح 2020./03/29

15. دليل عملي للعمل مع المنظمات الدولية، من الرابط: https://www.mandint.org/ar/guide-IO

16. الموسوعة العربية، **" علم الحياة (الحيوان والنبات)، الاستقلالية "**، تم تصفح الموقع يوم : 03 فيفري 2018. الرابط: http;//www.arab_ency.com/détails.php? Full=18nid=113

17. اللجنة الدولية للصليب الأحمر، **" ماهية القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟"** على الرابط: http://accronline.com/article_detail.aspx?id=28958.

18. ميثاق بيات ألضيفي، أمريكا والاستراتيجية السيبرانية،(02/05/2020) متاح على الرابط https://m.annabaa.org/arabic/informatics/17712

19. دولة الإمارات العربية المتحدة ، " ورقة عمل "حول استخدام موقع التواصل الاجتماعي " فيسبوك"، أنظر الرابط: http://arabic.cnn.com/middleeast/2014/05/21/facebook-uae-law

20. --" الجرائم الإلكترونية، وآفاق النمو المتسارع، المركز العربي للبحوث والدراسات "، 2018 من الرابط: https://www.google.com/url?sa

21. -- " النظام القانوني للأمن الوطني الإلكتروني في ظل الثورة الرقمية "، تم تصفح الموقع يوم : 22 فيفري 2018. الرابط: www.univ-chlef.dz/fdsp/images/PDF/JE-DROIT-2017.PDF

ثانيا: باللغة الاجنبية.

1. **Electronics security"**, Web Site Visited in : 22 Februay 2018. Link: https://www.the freedictionary.com/electronics+security

2. John Wilkinson, Tareq Haddad, PWC, Economic Crime in the Arab World, February 2014, http://www.pwc.com/m1/en/publications/gecs2014reportme.pdf

3. Hamadoun I. Touré Secretary-General, ITU, Cybersecurity Global status update, December 2011

http://www.un.org/en/ecosoc/cybersecurity/itu_sg_20111209_nonotes.pdf

4. MENA region cybersafety, security and data privacy, May 2014,

http://www.ictqatar.qa/sites/default/files/Cybersafety,%20security%20and%20data%20privacy.pdf,

5. Michael Vatis, The Council of Europe Convention on Cybercrime, http://cs.brown.edu/courses/csci1950-psources/lec16/Vatis.pdf,

6. Micheal Barrett, Andy Steingruebl, Bill Smith, Combating Cybercrime: Principles, Policies and Programs, April 2011, https://www.paypal-media.com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4.pdf,

7. region cybersafety, security and data privacy, May 2014, http://www.ictqatar.qa/sites/default/files/Cybersafety,%20security%20and%20data%20privacy.pdf