جامعة العربي التبسي -تبسة-

كلية الحقوق والعلوم السياسية

قسم: العلوم السياسية

إنعكاسات التهديدات السيبرانية على الأمن الوطني الجزائري

مذكرة مقدمة لاستكمال متطلبات لنيل شهادة الماستر في العلوم السياسية

تخصص دراسات إستراتيجية وأمنية

إعداد الطالبة:

- بكوش الروميساء

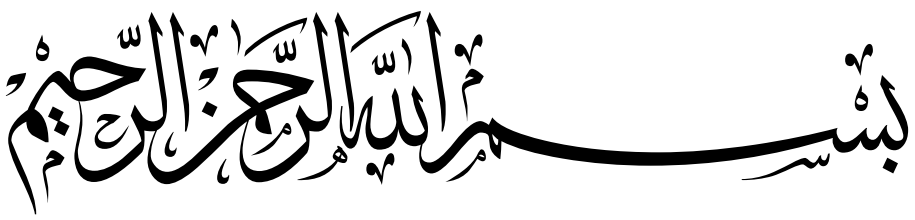
إشراف الأستاذ:

بن حدة باديس

لجنة المناقشة:

الاسم واللقب	الرتبة العلمية	الصفة
معيفي فتحي	أستاذ محاضر -ب-	رئيسا
بن حدة باديس	أستاذ مساعد -أ-	مشرفا ومقررا
لعجال ليلى	أستاذ محاضر -ب-	عضوا مناقشا

السنة الجامعية 2019/2018


بسم الله الرحمن الرحيم

الملخص

في ظل التطورات الحاصلة في مجال التكنولوجيا، أصبحت قضية الأمن المعلوماتي السيبراني من التحديات الكبرى على الصعيدين الإقليمي والعالمي، لا سيما مع تزايد التهديدات السيبرانية التي تعتبر من التهديدات الجديدة التي تصيب أمن معلومات الدول، ما يؤدي إلى انهيار أمنها الوطني واختراقه وبالتالي تنهار الدولة تماما.

إن الجزائر من بين الدول التي قد تتعرض إلى التهديدات السيبرانية، لذلك أصبحت الجزائر تهتم بالأمن السيبراني بشكل كبير بوضع مجموعة من الآليات المحلية وكذا التنسيق الدولي للحد من إنتشار هذه الظاهرة، كما تحاول وضع استراتيجيات مبنية على التعاون مع العديد من الدول الإقليمية والعالمية للتصدي لهذه التهديدات، وذلك عن طريق إنشاء مراكز تعنى بمكافحة التجسس وحماية أمن المعلومات.

الكلمات المفتاحية:

الأمن السيبراني، الجريمة الإلكترونية، الأمن القومي الجزائري

Summary

In light of developments in technology, the issue of cybersecurity has become a major challenge at the regional and global levels, especially with the increasing cyber threats, which are considered new threats to the security of state information, leading to the collapse of national security and penetration and thus the collapse of the state completely.

Algeria is one of the countries that may be exposed to cyber threats. Therefore, Algeria is interested in cybersecurity by developing a set of local mechanisms as well as international coordination to reduce the spread of this phenomenon. It is also trying to develop strategies based on cooperation with many regional and global countries to address these threats , Through the establishment of anti-espionage and information security centers.

key words:

Cyber Security, Cyber Crime, Algerian National Security

شكر وعرفان

قال عمر بن الخطاب رضى الله عنهُ

«الدنيا ملعونة والملعون فيها إلا ذكر الله وعلم المتعلم»

الحمد لله الذى أنار لنا درب العلم والمعرفة وأعاننا على أداء هذا الواجب ووفقنا إلى انجاز هذه المذكرة التى لم تكن لترى النور لولا توفيق الله سبحانه وتعالى

نتقدم بأسمى عبارات الشكر والتقدير لكل من زرع بذرة العلم فى قلبى

نخص بالذكر الأستاذ **باديس بن حدة** رئيس قسم العلوم السياسية الذى تفضل بقبول الإشراف على هذه المذكرة وذلك بكثير من التشجيع والحرص على إتمام العمل وإتقانه ومدى رحابة صدره وتحمله الإشراف على المذكرة حتى نهايتها ولم يبخل علينا بنصائحه وتوجيهاته القيمة التى كانت عونا لنا فى إتمام هذا العمل

إلى من علمونا حروفا من ذهب وكلمات من نور وعبارات من أسمى وأحلى كلام فى العلم إلى من صاغوا لنا علمهم حروفا ومن فكرهم منارة تنير لنا سيرة العلم والنجاح

إلى من وقفوا على المنابر وأعطوا لنا من حصيلة فكرهم لينيروا دربنا

نتقدم بالشكر إلى كل أساتذتنا فى قسم العلوم السياسية لجامعة تبسة الذين نفتخر بهم لكوننا تكونا على أيديهم فى سبيل تشجيع العلم والمعرفة فلهم منا جميعا جزيل الشكر والعرفان والتقدير

كما نتوجه بجزيل الشكر لأعضاء لجنة المناقشة لقبولهم مناقشة هذا المذكرة الأستاذة **ليلى لعجال** والأستاذ **فتحى معيفى**

وشكر الخاص إلى الأستاذة رقية بلقاسمى

إلى طاقم مكتبة النور الدكتور **أحمد الحمزة** **الأستاذ كمال مباركة**

نتوجه بجزيل الشكر والامتنان إلى كل من ساعدنا من قريب أو من بعيد على انجاز هذا العمل

الإهداء

الحمد لله الذي وفقنا في انجاز هذا العمل الذي أهديه إلى من قال فيهما الله عز وجل "وبالوالدين إحسانا"،

إلى التي سهرت الليالي من أجلي وعانت الكثير لإسعادي ،إلى الكلمة الطيبة واللحن الشجي والصدر الحنون ،إلى التي دعواتها ترافقني في كل مكان ،أمي الغالية حفظها الله

إلى القلب الكبير الذي غمرني والي أجمل إنسان في الوجود إلى الصديق والأخ الحنون وكان له الفضل في تحقيق أحلامي والدي العزيز حفظه الله

إلى إخوتي وسندي في الحياة "عبد الرزاق، كمال"

إلى من اشكوا لهن أحزاني متى ضاقت بيا الدنيا إلى من تمنياتهن لي دوما بالتوفيق والنجاح أخواتي "هادية، صبرينة"

إلى صديقاتي العزيزات "آمنة وأميمة"

إلى أبناء أختي أمينة "أيمن، أمين"

إلى كل الأقارب والأحباب

إلى جميع أساتذة قسم العلوم السياسية

إلى كل من نسيهم قلمي ولم ينسهم قلبي

إلى كافة دفعة العلوم السياسية لسنة 2019

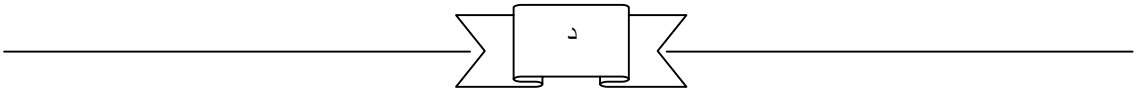
الروميساء

فهرس الجداول

فهرس الجداول

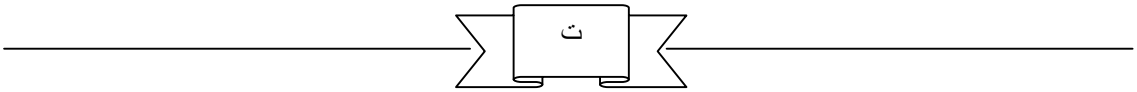
قائمة المختصرات

س.خ.ج: السياسة الخارجية الجزائرية



د.ب: دون بلد نشر

د.ط: دون طبعة



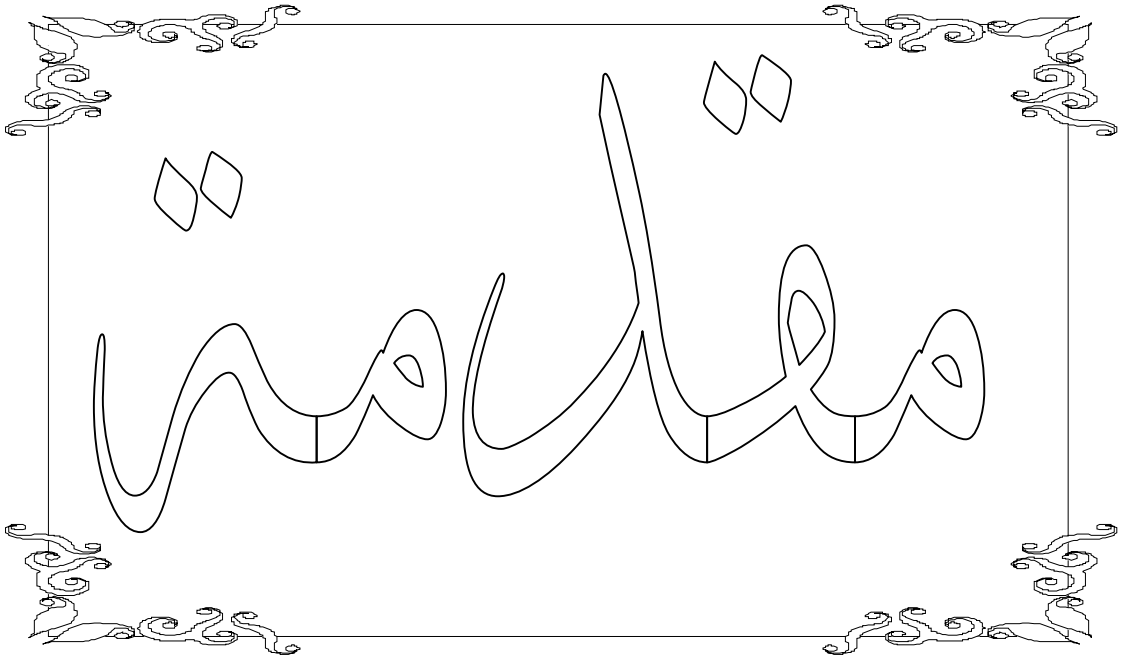
تر: ترجمة

ع: عدد

ط: الطبعة

ص: صفحة

د.ص: دون صفحة


مقدمة

يندرج هذا البحث في سياق دراسة العلاقات الدولية خاصة، ودراسة وتحليل الدراسات الأمنية والتركيز على أحد القطاعات الحديثة للأمن، وهو الأمن السيبراني.

حيث احتل موضوع الأمن اهتماما كبيرا من الباحثين المختصين في الدراسات الأمنية خاصة، وباحثي العلاقات الدولية عامة، أين كان ينظر للأمن من المنظور التقليدي القائم على فكرة حماية الدولة من التهديدات الداخلية الخارجية وذلك بالوسائل العسكرية فقط، فكانت هذه النظرة سائدة لفترة طويلة حتى بدأت تتغير مع ظهور تهديدات وتحديات جديدة مثل: النزاعات الداخلية، التلوث البيئي، الفقر والتفاوت في توزيع الثروات، الجريمة الالكترونية والتهديدات السيبرانية، هذا ما جعل بعض المفكرين البحث في تطوير مجالات الأمن، فقاموا بتوسيع قطاعات الأمن لتشمل قطاعات أخرى منها: القطاع العسكري، القطاع السياسي، القطاع المجتمعي، القطاع البيئي، بالإضافة إلى قطاع أخر وهو موضوع بحثنا ويركز على الجانب الالكتروني، **"الأمن السيبراني"**.

وتعاطيا مع الاختلاف والتنوع في طبيعة التهديدات الأمنية تبرز لنا التهديدات السيبرانية لتأخذ بعدا إقليميا ودوليا، خاصة بعد اتجاه العديد من دول العالم إلى الاعتماد على التكنولوجيا الإلكترونية والرقمية في إدارة وتسيير منشآتها الحيوية ومؤسساتها بشكل جعلها تُدخلها ضمن حساباتها الإستراتيجية وأمنها القومي، لكن بالرغم من المميزات التي تقدمها هذه الأخيرة إلا أن هذه الدول نفسها أصبحت عرضة للعديد من الاختراقات والهجمات الإلكترونية والتي تهدد بذلك أمنها وقطاعاتها الحساسة، الأمر الذي جعل هذه الدول تعيد قراءة العديد من حساباتها وتحاول تكييف إستراتيجياتها وفقا للتغيرات الحاصلة حتى تستطيع الحفاظ على أمنها القومي أو التقليل من حجم الخسائر المترتبة عن مثل هذه التهديدات المتفاقمة.

وفي هذا السياق فإن دراسة التهديدات السيبرانية، يقودنا إلى دراسة أحد الدول التي يتعرض أمنها الوطني لهذه التهديدات وهذه الدولة هي الجزائر، وتحاول الجزائر تجاوز هذه التهديدات بدءا بالاهتمام أكثر بالجانب الخاص بالأمن السيبراني، وذلك عن طريق وضع قوانيين وتشريعات خاصة باستخدامات الالكترونية الحديثة، التي فيها عديد الايجابيات إلا أنها حملت معها العديد من التهديدات والمخاطر التي تُرجمت في شكل جرائم إلكترونية، لم تفرق بين الأشخاص والمؤسسات والدول.

وتشير الإحصائيات المسجلة في الجزائر أن الجريمة الإلكترونية أخذت منحا تصاعديا في الآونة الأخيرة، وهو ما ينبأ بخطورة الوضع، لا سيما في ظل توجه الجزائر نحو تبني مقاربة الحكومة الإلكترونية-e) (Gouvernement، ومن هذا المنطلق فإن السلطات الجزائرية ملزمة باتخاذ الاحتياطات الأمنية اللازمة

لتفادي أي نوع من الجرائم الإلكترونية المهددة لها، فهي عبر محاولة وضع حلول وإجراءات لمواجهة هذا التهديد الذي يترصد أمنها الوطني، كما تسعى جاهدة للتعاون مع باقي دول العالم خاصة المتطورة منها في مجال الحماية السيبرانية.

أهمية الدراسة

يكتسب موضوع الدراسة أهمية بالغة بالنظر لمدى حداثته، وضرورة البحث فيه وتكمن أهميته في:

1- الأهمية العلمية

يمثل هذا الموضوع أحد أبرز مواضيع الساعة فالتهديدات السيبرانية أصبحت تحتل صدارة اهتمامات الباحثين والمختصين، ويعد موضوع الأمن السيبراني وإستراتيجيات مواجهة التهديدات السيبرانية من أهم المواضيع في اختصاص الدراسات الإستراتيجية و الأمنية.

2- الأهمية العملية

وتكمن في إعطاء تصور واضح لعلاقة الأمن السيبراني بأمن الدولة وكيف يتحول هذا الجانب لتهديد لا تستطيع الدول مواجهته منفردة بالإضافة إلى دراسة الجزائر ومعرفة أهم التهديدات السيبرانية التي تتعرض لها.

- أهداف الدراسة

يمكن التعرف على أهداف الدراسة من خلال متغيرات الموضوع في حد ذاتها، فما أصبحت تشكله التهديدات الالكترونية على مختلف المستويات خاصة على العالم الثالث، في ظل انتشار التكنولوجيا الحديثة،وعدم وعي أفراد المجتمع بمخاطرها وتأثيراتها، جعلنا نتجه بالدراسة إلى ضرورة التعرف على انعكاسات التهديدات السيبرانية على الأمن الوطني الجزائري، فمتغير التهديد يأتي متضاد مع تحقيق الأمن فغياب أحدهما يؤدي إلى تحقيق الآخر، ونظرا لما تشهده الجزائر من أحداث متتالية، يأتي هدف الدراسة الأساسية للتعرف على مفهوم الأمن السبراني وتأثيراته المختلفة على البيئة الداخلية والخارجية الجزائرية، خاصة بعد انتشار الإعلام الموازي والشبكات الاجتماعية المختلفة، التي أصبحت منبر لمن لا منبر له، وما يشكله تأثيرها على أمن المجتمع ثم أمن الدول، وهو ما سيتم التعرف عليه في موضوع البحث.

أسباب اختيار الموضوع

هناك العديد من الأسباب التي تبرر اختيار موضوع ما، وموضوع التهديدات السيبرانية من المواضيع الهامة التي أصبحت محل نقاش على مستويات عالمية، فلم يعد التهديد مقتصرا على الجانب العسكري فقط بل تعداه إلى قطاعات أخرى، لذلك فاختيار هذا الموضوع جاء نتيجة عدة عوامل يتمثل أبرزها فيما يلي:

1- أسباب الموضوعية

الإحاطة بأحد المواضيع المهمة والمتمثل في الأمن والتعمق في أحد قطاعاته والمتمثل في الأمن السيبراني لمحاولة ربطه التهديدات السيرانية وتأثيرها على الأمن الوطني للدول واخترنا الجزائر كدراسة لنا.

2- أسباب الذاتية

شكل موضوع الأمن السيبراني اهتماما خاصا للبحث من خلال ما تقدمنا به سابقا، بالإضافة إلى أن الموضوع يعتبر من أحدث المواضيع على الساحة البحثية كون التهديدات السيبرانية تزداد يوما بعد يوم، بالإضافة إلى أن هذا الموضوع يؤثر بشكل كامل على اهتمامنا، واخترنا دراسة حالة الجزائر كونها الدولة التي ننتمي لها ومحاولة منا أن نفيد بهذا البحث ونبرز أهم مكامن الخلل في المنظومة الأمنية السيبرانية الجزائرية، وكذلك لإضافة هذا العمل العلمي لرفوف المكتبات الجامعية الوطنية لإفادة الباحثين والدارسين لهذا الموضوع.

مشكلة الدراسة

في العصر الرقمي تزيد مخاطر التهديدات السيبرانية وتتباين أثارها وانعكاساتها على العالم عامة وفي الجزائر خاصة حيث مست هذه التهديدات معظم الدول لتطال عبرها مختلف القطاعات الاقتصادية والعسكرية والسياسية وأصبحت بذلك تهدد الأمن الوطني للدول بشكل دائم ومستمر.

مما تقدم، يمكن طرح السؤال المركزي التالي:

إلى أي مدى يمكن أن تؤثر التهديدات السيبرانية المعاصرة على الأمن الوطني الجزائري في ظل توجه الدولة الجزائرية نحو تفعيل الحوكمة الإلكترونية لمختلف القطاعات الإستراتجية للدولة؟

ويتفرع عن هذا السؤال المركزي عديد الأسئلة الفرعية منها:

- ما هي أبرز المضامين الإيتيمولوجية لدراسة الأمن والتهديدات السيبرانية ؟
- ما هي أبرز وسائل التهديدات السيبرانية؟ وما هي أنجع السبل والإجراءات لمواجهتها ؟
- فيما تتمثل أهم أساليب تعامل الجزائر مع التهديدات السيبرانية ؟
- فيما تكمن أبرز مرتكزات العقيدة الأمنية الجزائرية؟

– كيف تأثر التهديدات السيبرانية على الأمن الوطني الجزائري؟.

فرضيات الدراسة

للإجابة عن السؤال المركزي للأسئلة التي تم طرحها في إشكالية الدراسة، يقترح الباحث الفرضيات التالية:

1– الفرضية المركزية

كلما زادت مخاطر التهديدات السيبرانية على الأمن الوطني الجزائري كلما أدى ذلك إلى ضعف المنظومة الأمنية الجزائرية مما يستوجب إعادة ضبط إستراتيجية المواجهة .

2– الفرضيات الفرعية

– تعتبر الاختراقات السيبرانية بمثابة تهديد للأمن الوطني الجزائري بالنظر لإمكانية المساس بالبنية التحتية الإلكترونية للدولة ومنظومتها الإستراتيجية؛

– إن التعاون والتنسيق بين الدول في الفضاء السيبراني يؤدي حتما إلى التقليل من التهديدات للأمن الوطني.

مجال الدراسة

1– الحدود الزمنية

تدور أحداث هذا البحث حول التهديدات السيبرانية التي تتعرض لها دول العالم ومن بينها الجزائر وسوف نقوم بالدراسة انطلاقا من الفترة المحددة إلى ما بعد أحداث 11 سبتمبر 2001 و الممتدة إلى غاية سنة 2018.

2– الحدود المكانية

بالنظر لطبيعة انتماء الباحث اخترنا دراسة حالة الجزائر وهي دولة مساحتها 2.378.341 كلم^2 وعدد سكانها يقدر بـــ 42 مليون نسمة وهي تتعرض للتهديدات السيبرانية وبالتالي يتعرض أمنها الوطني إلى خطر كبير.

3– الحدود الموضوعية

يندرج هذا البحث في إطار الدراسات الأكاديمية وبالتحديد ضمن مجال الدراسات الأمنية، فموضوع التهديدات السيبرانية طرح فيه عدة أطر نظرية ودراسات وأبحاث تعنى بالبحث في ماهيته وكيف يتأثر الأمن القومي للدولة به .

– مناهج وإقترابات الدراسة

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

1– المنهج الوصفي التحليلي

يستخدم هذا المنهج بصفة عامة في العلوم الاجتماعية والإنسانية عامة والعلوم السياسية بصفة خاصة، حيث يتم من خلاله تحديد خصائص وأبعاد الظاهرة المدروسة ووصفها وصفا موضوعيا من خلال جمع الحقائق والبيانات وعلى استخدام أدوات وتقنيات البحث العلمي ومن ثم تحليل المعطيات التي تم وصفها.

وتم استخدامه بشكل كبير في الدراسة من خلال تفسير ظاهرة التهديدات السيبرانية وتحديد خصائصها بالإضافة إلى طبيعة ونوعية العلاقة بين الأمن السيبراني ومفاهيم مشابهة من خلال جمع البيانات الوصفية حول التهديدات السيبرانية في العالم بشكل خاص وتحديد مفهوم الأمن السيبراني وغيرها ومن ثم تحليل المعلومات المتحصل عليها بما يخدم الدراسة.

2– منهج دراسة حالة

يقوم منهج دراسة الحالة بدراسة الظاهرة بشكل معمق وذلك بجمع بيانات ومعلومات شاملة ومفصلة عنها بهدف الوصول إلى فهم أعمق للظاهرة المدروسة، وذلك بجمع المعلومات والبيانات عن الوضع الحالي والماضي لفهم أعمق وتفسير أفضل للأسباب وكشف الحقائق والمعلومات التفصيلية الدقيقة عن الظاهرة المدروسة، وقد تم استخدامه في هذه الدراسة من خلال الاعتماد على الجزائر كحالة تستحق الدراسة والإلمام بمجموعة من التفاصيل والمعلومات والبيانات حول التهديدات السيبرانية التي تمس الجزائر والإجراءات ومناهج المجابهة.

3– منهج تحليل المضمون

هو أسلوب وأداة يستخدمها الباحث ضمن أساليب وأدوات أخرى في إطار منهج متكامل هو منهج الحصر في الدراسات الإعلامية تم الاعتماد عليه في دراستنا من اجل تفسير أهم المضامين والخطابات وكذا القوانين والتشريعات والوثائق الرسمية والاتفاقيات الدولية لمواجهة التهديدات السيبرانية.

– إقترابات الدراسة

يمكن تناول موضوع الدراسة كذلك وفقا للمقتربات التالية:

– **الاقتراب النسقي:** حيث تم الاعتماد على هذا المقترب لتبيان النسق العام للتهديدات السيبرانية وكيفية مواجهتها عبر الاعتماد على أحدث الآليات المعتمدة في ذلك.

– **الاقتراب الوظيفي:** يبرز هذا المقترب الوظيفة الوقائية التي تتبناها الدولة الجزائرية في مواجهة التهديدات السيبرانية والحد من تأثيراتها على المجتمع الجزائري.

– **الاقتراب الاتصالي:** يأتي هذا المقترب من توضيح كيفية نقل المعلومات المتوفرة في البيئة المحيطة بالنظام إلى داخل النظام أو النسق السياسي، بالتركيز على حالة الأمن الجزائري وكيفية التعامل مع التهديدات السيبرانية في ظل توسع نطاقها وتحديد العلاقة بين النظام والمجتمع والواقع الاتصالي بينهما وما تشكله هذه اللحمة في التصدي لمختلف الظواهر.

– الدراسات السابقة

نقصد بها جميع البحوث والدراسات العلمية التي تتشابه مع البحث الراهن أو تقترب منه في جانب ما والتي تأثر بها الباحث في إعداده لهاته الدراسة.

1– دراسة قامت بها منى "الأشقر جبور" جاءت على شكل كتاب بعنوان "السيبرانية هاجس العصر"، تطرقت فيه الباحثة إلى المفاهيم والوسائل التي ترتبط بالأمن السيبراني عبر تحديد مفهومها ورصد أبعادها وتشخيص وقائعها، وكذا التطرق إلى ما تم انجازه حتى اليوم على المستوى الإقليمي والدولي والجهود الدولية والعربية في مجال إرساء الأمن في الفضاء السيبراني والخطوات العملية التي لا تدرك المخاطر السيبرانية.

2– دراسة قام بها الكاتب "فيصل محمد عبد الغفار" جاءت على شكل كتاب بعنوان "الحرب الإلكترونية " عن الدولة: دار الجنادرية للنشر والتوزيع، 2016. اعتبر فيها الكاتب أن ظهور ثورة تكنولوجيا الإلكترونيات واستخدامها في الأغراض العسكرية يعد نقطة تحول كبيرة، سواء في فن الحرب أوفي إدارة الصراع المسلح ويضيف أن أسلحة القتال الحديثة ووسائله قد اتخذت مكان الصدارة في حسم أي صراع مسلح وخاصة أسلحة الهجوم الجوي الحديثة .

3– قام بها الدكتور "بارة سليم" في كتابه: "الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر (الدور والتحديات)" تكلم فيه على تبني الجزائر كغيرها من الدول "لفكرة الحوكمة الالكترونية" وحمايتها لجهازها المعلوماتي ومنظومتها المعلوماتية من خلال العديد من الأجهزة والخلايا الأمنية وتكلمت عن دور أجهزة الدفاع الوطني في الجزائر لتحقيق الأمن السيبراني وأبرز التحديات الوطنية والعالمية التي يفرضها الفضاء السيبراني حلا مستقبليا.

– تحديد المفاهيم والمصطلحات

– **البنية التحتية الإلكترونية:** عبارة عن سلسلة من الجهود التي تبذل للوصول إلى مصادر الحوسبة، وتمثل البنية التحتية للإنترنت وتطبيقاتها مثل التجارة الالكترونية والبريد الالكتروني عصب الحياة في الوقت الراهن ولا يمكن للحكومات او المؤسسات التجارية وحتى الأفراد الاستغناء عنها. وقد أدى التطور الهائل في تكنولوجيا المعلومات والذي يشمل تطبيقات الانترنت بأنواعها المختلفة وكذلك تطور المعدات المادية للحاسوب إلى عدم كفاية البنية التحتية للإنترنت الحالية لتلبية الاحتياجات المطلوبة منها.

– **الجريمة الإلكترونية:** لجريمة الإلكترونية 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 الإتصال الحديثة مثل الإنترنت.

المدخل النظري للدراسة

يشكل المدخل النظري أهم منطلق ياتي بعد الجانب المفاهيمي وهدفه التعرف على مختلف آراء المفكرين والباحثين حول موضوع البحث، وموضوع بحثنا يمكن توضيح الإطار النظري الخاص به وفقا لما يلي:

1– 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.

ساهمت مدرسة كوبن اغن في توسيع وتعميق مضامين الأمن من خلال أعمال" باري بوزان "في كتابة الشعب الدولة والخوف، سنة 1983، 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 الأممنة.

2– 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.

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، **ثانيا** بدلا من التحقيق في النوايا الكامنة وراء استخدام القوة تركز هذه المقاربة على تأثيرات ألعاب القوة، **ثالثا** بدلا من التركيز على أفعال الكلام تؤكد على الممارسات والسياقات التي تسعى إلى تشجع أوتعميق إنتاج أشكال محددة من الحوكمة. 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 أو الخبرة والممارسة ذاتها كما تتلاقى في وظيفة واحدة تحت عنوان الأمن.

تبرير خطة الدراسة

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

تطرقنا في **الفصل الأول** المعنون مقاربة معرفية حول الأمن السيبراني، أين قسم إلى أربعة مباحث خصصنا المبحث الأول: مقاربة مفاهيمية للأمن السيبراني، للتعمق في مفهوم الأمن وكيف تم توسيع قطاعاته لتشمل المجال الالكتروني، أما بالنسبة المبحث الثاني: أشكال الأمن السيبراني تطرق إلى البحث والتعرف على أشكال الأمن السيبراني والتعمق فيها، أما المبحث الثالث فيلقي الضوء على ضبط مفاهيم التهديدات السيبرانية ومعرفة خطر هذه التهديدات، أما المبحث الرابع حول الأمن السيبراني والوسائل الفتاكة.

أما **الفصل الثاني** والذي عنوانه: الأمن السيبراني في الجزائر دراسة تحليلية ، قسم كذلك إلى ثلاثة مباحث وهي كالأتي: المبحث الأول وتطرقنا فيه إلى السياسة الأمنية الجزائرية بين العقيدة الأمنية والتطورات التكنولوجية ، أين بحثنا حول السياسة المنتهجة من طرف الجزائر في ظل التطورات التكنولوجية، كما عنون المبحث الثاني الأمن السيبراني الجزائري، والحديث عن العوامل التي تتخذها الجزائر لحماية أمنها السيبراني، أما المبحث الثالث أبرز التهديدات السيبرانية التي تواجه الأمن الجزائري.

أما بالنسبة **للفصل الثالث** والذي تمحور حول المناهج المستخدمة لمواجهة التهديدات السيبرانية وقد قسم إلى المبحث الأول الوسائل الجزائرية لمواجهة التهديدات السيبرانية، أما المبحث الثاني التعاونات الدولية

كآلية لمواجهة التهديدات السيبرانية، أما المبحث الثالث آليات التعاون الدولي والإقليمي في مواجهة التهديدات السيبرانية.

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:

مقاربة معرفية حول الأمن السيبراني

تطور الأمن بشكل ملحوظ حيث تم الانتقال من مفهوم الأمن الصلب إلى الأمن اللين، كما أن مجالات الأمن توسعت بشكل كبير وظهر لنا جانب يتمثل في الأمن السيبراني، أين أصبح يشكل خطرا كبيرا على الدول، لقد تميز هذا النوع بالعديد من الأشكال، إن التطور الحاصل في مجال التكنولوجيا جعل من هذا البعد يصبح من أخطر التهديدات التي تواجه دول العالم، لذلك تسعى جميع الفواعل الدولاتية.

ففي هذا الفصل سوف يدرس الباحث الجوانب المتعلقة بهذا البعد الجديد للأمن ومحاولة معرفة التهديدات التي تتعرض لها الدول.

وسوف يتم تقسيم الفصل إلى أربعة مباحث كالتالي:

- ❖ المبحث الأول: مقاربة مفاهيمية للأمن السيبراني؛
- ❖ المبحث الثاني: أشكال الأمن السيبراني؛
- ❖ المبحث الثالث: ضبط مفاهيم التهديد السيبراني؛
- ❖ المبحث الرابع: وسائل وإجراءات التهديدات السيبرانية.

المبحث الأول: مقاربة مفاهيمية للأمن السيبراني

تناولت العديد من الدراسات والباحثين مفهوم الأمن السبراني وفقا عدة توجهات يمكن توضيحها وفقا لما يلي:

المطلب الأول: التعريف اللغوي والاصطلاحي لكلمة سيبرانية

في هذا المطلب سيتم التطرق إلى التعريف اللغوي والإصطلاحي للسيبرانية وكذا التطرق إلى مفهوم الأمن السيبراني كما يلي:

الفرع الأول: التعريف اللغوي لكلمة سيبرانية

السيبرانية: مأخوذة من كلمة (سيبر) وتعني صفة الأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي فالسيبرانية تعني (فضاء الإنترنت) [1]. وهي كلمة مشتقة من الكلمة اليونانية Kybernetes التي وردت بداية في مؤلفات الخيال العلمي، وكان يقصد بها قيادة ربان السفينة[2].

ويعرف المعجم الفرنسيLe Petit Larousse السيبرانية 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 تتصل بسمات وخصائص الحواسيب وتكنولوجيا المعلومات والواقع الافتراضي".[4] فيما يعرفها قاموس مصطلحات الأمن المعلوماتي بأنها: "هجوم الفضاء الإلكتروني يهدف إلى السيطرة على المواقع إلكترونية أو بني محمية إلكترونيا لتعطيلها أو تدميرها أو الإضرار بها".[5]

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

[1]-أحمد عيسى، نعمة الفتلاوي، "**الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم المعاصر**"، (بحث مقبول للنشر في مجلة المحقق الحليلي،العراق: جامعة الكوفة، كلية القانون، 2016)، ص05.

[2]- منير البعلبكي ورمزي منير البعلبكي، "**المورد الحديث**"، (لبنان: دار العلم الحديث، د.س)، ص307.

[3]-**Dictionnaire français Le petit Larousse**, (France, Edition, 2001), p104.

[4]-**English dictionary Oxford dictionaries language,** P299.

[5]-أحمد عيسى نعمة الفتلاوي، **مرجع سابق**، ص 05.

الفرع الثاني: التعريف الإصطلاحي لكلمة سيبرانية

كلمة سيبرانية في مفهومها الحديث استعملت لأول مرة من قبل عالم الرياضيات الأمريكي نوربرت وينر Norbert Winer وهو أستاذ الرياضيات في معهد ماساشوستس التقني MIT الذي أعطاها مفهومها الاصطلاحي الحديث وكان ذلك عام 1948، ومن أجل وصف نظام التغذية الرجعية Feedback الإستفادة من مخرجات الأنظمة out puts في ضبط مدخلاتها in puts وفي التحكم فيها واستقرار أدائها.

ورأى "وينر" أنه يمكن تطبيق هذا النظام على نطاق واسع في مختلف المجالات ليس العملية فقط بل الإنسانية أيضا.[1]

وبالتالي فالمصدر الإصطلاحي الحديث لكلمة سيبرانية وهو "**علم القيادة والتحكم في الأحياء والآلات ودراسة آليات التواصل**".

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

لقد لخص نوربورت وينر الحدود التي لا ينبغي أن يتعداها إيماننا بقدرات الآلة أو الخوف من طغيانها بقوله: "أعط ما للإنسان للإنسان، وما للعقل الإلكتروني للعقل الإلكتروني" وهو يعني 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 كان خيرا أم شرا.

وكان ظهور علم السيبرنطيقا (Cybernetics) هذا العلم الجديد، هو بدوره واحد من المعالم البارزة لعصرنا الحاضر حيث كانت أبحاث "وينر" هي الأساس الأول لإختراع العقول الإلكترونية. فقد كانت فكرة هذا العالم هي تطبيق ما يحدث في الإنسان بوضعه 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 أن يصحح مسار أفعاله ويعيد توجيهها وفقا لما يواجهه وأن يأمر نفسه ويطوعها ويختبر نتائج سلوكه ويعدلها.[2]

---

[1]– سعد علي الحاج بكري، "**الأمن السيبراني ومعضلة حمايته**"،الرابط: www.alegt.com/article1241506.html، تاريخ التصفح يوم 2019/03/04.

[2]– فؤاد زكريا، "**التفكير العلمي**"، الطبعة الثالثة، (الكويت: المجلس الوطني للثقافة والفنون، 1978)، ص144.

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 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]

الفرع الثالث: تعريف الأمن السيبراني

ويعرف الأمن السيبراني على أنه: "عبارة عن مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني"[2].

والأمن السيبراني هو: "سلاح استراتيجي بيد الحكومة والأفراد، لاسيما أن الحرب السيبرانية أصبحت جزء لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول"[3].

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

فقد عرفه "ريتشارد كمرر" Richard A Kemmerr على أنه: "عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة".[4]

[1]- فؤاد زكريا، **مرجع سابق**، ص147.

[2]- عنترة بن مرزوق، "**الأمن السيبراني كبعد جديد من السياسة الجزائرية**"، محاضرات مقدمة لطلبة جامعة محمد بوضياف – المسيلة، كلية الحقوق والعلوم السياسية، د س، ص65.

[3]- **صحيفة المرصد، "ما هو الأمن السيبراني"، موقع إلكتروني**

https://al-marsd.com/168664.html، **تاريخ التصفح 2019/3/11.**

[4]- محمد مختار، "**Cyber Security، هل يمكن تجنب الدولة مخاطر الهجمات الإلكترونية؟**"، مجلة مفاهيم المستقبل، العدد 06، بيوت، لبنان، يناير2015، ص5.

* **المجال الجديد الخامس**: وهو المجال الإلكتروني حيث أصبح منافسا لمجالات البث والاتصال البرية والبحرية والجوية والفضائية بل وأصبح أحد ميادين الحرب بين الأمم خصوصا وأن هيئات استراتيجية مثل الجيوش والمصارف والشركات وغيرها صارت تعتمد على المجال الإلكتروني في تخزين بنياتها التحتية مما يجعلها عرضة لهجمات إلكترونية وذلك خلال القرن 21.

الأمن السيبراني هو : "المجال الجديد الخامس* للحروب الحديثة بعد البر والبحر والجو والفضاء الحقيقي وهو يمثل جميع شبكات الحاسب الآلي الموجودة حول العالم ويشمل ذلك الأجهزة الإلكترونية المرتبطة من خلال شبكة الألياف البصرية والشبكات اللاسلكية، الفضاء السيبراني ليس الإنترنت فقط وإنما شبكات أخرى كثيرة متصلة".[1]

بينما يعرفه "إدوارد أمورسو" Edward Amoroso على أنه: "وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها وتوفير الاتصالات المشفرة".[2]

الملاحظ هنا أن كل من "ريتشارد كمرر" و"إدوارد أمورسو" قد ركزوا في هذين التعريفين على أن الأمن السيبراني هو: "وسيلة دفاعية ضد الهجمات وعمليات القرصنة على مختلف الحواسيب والشبكات. الأمن السيبراني يعني حماية المعلومات من خلال ثلاث محاور رئيسية محور المعلومات الشخصية، محور المعلومات داخل الشركة ومحور المعلومات عبر الدول".

كما يمكن تعريف الأمن السيبراني على أنه: "الحد من خطر هجوم ضار للبرمجيات وأجهزة الكمبيوتر كذلك يشمل على الأدوات المستخدمة للكشف عن عمليات الإقتحام ووقف الفيروسات ومنع المتطفلين من الوصول إليها".[3]

ويمكن تعريف الأمن السيبراني انطلاقا من أهدافه بأنه: "النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الإتصالات والمعلومات، ويتضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن بحيث لا تتحول الأضرار إلى خسائر دائمة"[4].

الملاحظ أن هذا التعريف يستنتج منه أن حماية الموارد المادية والمالية وحتى البشرية كلها مرتبط بتقنيات الإتصالات والمعلومات فهي من أهداف الأمن السيبراني. والغرض من ذلك هو الحد من الخسائر والأضرار.

---

[1]– صالح بن علي بن عبد الرحمان الربيعة، الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت. متاح على الرابط: https://www.google.com/url?sa=، تاريخ التصفح: 28-04-2019.

[2]– صالح بن علي بن عبد الرحمان الربيعة، مرجع سابق.

[3] - Dan Craiyen and others, "**Defining cybrescurity**", Technology innovation management review, Montreal, Canada, (october 2014).p14.

[4]– منى الأشقر جبور، "**الأمن السيبراني: التحديات ومستلزمات المواجهة**"، (جامعة الدول العربية: المركز العربي للبحوث القانونية والقضائية، 2012)، ص03.

وكخلاصة فإن الحديث على الأمن السيبراني يقود إلى أن:

– الأمن السيبراني هو عبارة عن مجموعة الوسائل والتنظيمية الإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به، الأمن الدفاعي؛

– الأمن السيبراني هو سلاح استراتيجي بيد الأفراد والحكومة لاسيما أن الحرب السيبرانية أصبحت جزأ لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول، حروب الجيل الخامس؛

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

المطلب الثاني: الأمن السيبراني والمفاهيم ذات الصلة

إن مفهوم الأمن السيبراني يتداخل ويتشابك مع مفاهيم ومصطلحات مختلفة كالأمن المعلوماتي ، والأمن الالكتروني ما يسمح بضبط مفهوم الأمن السيبراني ومجالاته، وإبراز أوجه التشابه والاختلاف بينها.

الفرع الأول: الأمن المعلوماتي

يقصد بأمن المعلومات من زاوية أكاديمية العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الإعتداء عليها، ومن زاوية تقنية فيقصد به الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية.[1]

وأمن المعلومات هي الإجراءات والتدابير الوقائية التي تستخدم للمحافظة على المعلومات وسريتها والمحافظة عليها من السرقة أو الإختراق Hack. ويعتبر الأمن السيبراني مفهوم أوسع من أمن المعلومات حيث يتضمن تأمين البيانات والمعلومات التي تتداول عبر الشبكات الداخلية أو الخارجية والتي يتم تخزينها في خوادم داخل أو خارج المنظمات من الإختراقات، إضافة إلى ذلك فإن الأمن السيبراني يشمل بعض الأمور التي لا تندرج ضمن أمن المعلومات كحماية البنى التحتية[2].

الفرع الثاني: الأمن الإلكتروني

تعد الثورة الرقمية وعالم الإنترنت في الوقت الحالي بيئة تنظم فيها الكثير من النشاطات الاقتصادية والإدارية، كما تعد مجالا للتفاعل والتواصل والإبتكار حيث لم يعد بالإمكان الإستغناء عن شبكات الإنترنت

---

[1]– فتيحة ليتيم، ونادية ليتيم، "**الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة**"، (جامعة بسكرة، مجلة المفكر، العدد 12، (د.س.ن) ص239.

[2]– فهد الدريبي، "**ماهو الأمن السيبراني**"، من الرابط: www.fadvisor.net/blog/2017/11/whatiscyberhack تاريخ التصفح 2019/02/26.

ووسائل تكنولوجيا الاتصال وحفظ البيانات والمعلوماتية في ظل الإتجاه نحو ما يسمى بالإدارة والحكومة الإلكترونيتين والاقتصاد وكل هذه الأنواع من المعلومات والبيانات، حيث يتم تناقلها وحفظها في أغلب الأحيان عن طريق شبكة الحواسيب، ومن هنا تأتي أهمية تأمين هذه الشبكات من مختلف التهديدات والمخاطر، ولتجسيد ذلك ظهر ما يسمى بـــ"الأمن الإلكتروني" أو أمن المعلومات الإلكترونية، حيث بات يشكل جزء أساسيا في أي سياسة أمنية وطنية وأصبحت الدول تنظر إليه كنظير منافس للأمن التقليدي ومعبر عن سيادها وأمنها الوطني، لذلك أصبح صناع القرار في معظم دول العالم يصنفون مسائل أمن المعلومات الإلكترونية كأولوية في سياستهم الدفاعية الوطنية. 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.

بينما يعتبر الأمن السيبراني مجموعة 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 أو الجهات في الفضاء السيبراني. والملاحظ من خلال التعريف نستنتج أنه هناك تقاربا وتداخلا بين المصطلحين، فكلاهما يرمي إلى هدف حماية أمن المعلومات وسلامتها من الهجمات والمخاطر ووضع التدابير اللازمة لتأمين خصوصيات وبيانات الأفراد والمؤسسات والدولة. [1]

الفرع الثالث: 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 ومعلوماها القومية والأمنية والاقتصادية والسياسية والاجتماعية وغيرها من المقومات. [2]

[1] محمد مختار، مرجع سابق، ص7.

[2] – عادل عبد الصادق، "**الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي**"، (المركز العربي لأبحاث الفضاء الإلكتروني، د.ش، 2017)، ص02.

لقد أصبحت العلاقة بين الأمن والتكنولوجيا علاقة متزايدة، مع إمكانية تعرض المصالح الإستراتيجية ذات الطبيعة الإلكترونية إلى أخطار إلكترونية وتهدد بتحول الفضاء الإلكتروني الى وسط ومصدر الأدوات الجديدة للصراع المتعدد الأطراف ودورها في تغذية التوترات الدولية.[1]

ومن جهة أخرى فرضت تلك التطورات إعادة التفكير في مفهوم الأمن القومي الذي يعنى بحماية قيم المجتمع الأساسية وإبعاد مصادر التهديد عنها وغياب الخوف من خطر تعرض تلك القيم للهجوم، وبذلك يتوافر أمن الفضاء الإلكتروني حال تحقيق إجراءات الحماية ضد التعرض للأعمال العدائية وللإستخدام السيئ لتكنولوجيا الإتصال والمعلومات[2].

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

لقد أصبح الأمن السيبراني والإلكتروني جزء لا يتجزأ من الأمن القومي خاصة مع تنامي حجم التهديدات وعلاقة البعد الإلكتروني بعمل المنشآت الحيوية سواء كانت مدنية أو عسكرية.[4]

ويمكن الإشارة هنا إلى أن الأمن القومي لأي دولة له محاوره الرئيسية والمتمثلة في المحاور العسكرية السياسية، الجغرافية، الاجتماعية، الاقتصادية والأمنية وأخيرا التقنية، وهو المحور الذي يهم الدول اليوم نظرا لإستنادها على منظومة تقنية وإلكترونية عالية الدقة وغزيرة التكنولوجيا تعتمد على صناعة المعلومات والبحث العلمي والمعلوماتي في جميع الجوانب، وبهذا يمكن الإشارة إلى أن الأمن القومي المعلوماتي هو عبارة عن "مدى جاهزية الدول من الناحية التقنية والمعلوماتية لحماية مخزونها الإلكتروني من المعلومات وعدم الوصول إليها بأية طريقة تقنية أو تقليدية".[5]

لقد أدخلت ثورة المعلومات دول العالم في هاجس أمني قوي خاصة وأن هذه الدول قد قامت بوضع مدخراتها القومية على شكل معلومات رقمية عبر فضاء مذاب الخصوصية وضعيف الأمن لبعض دول العالم وفائق السرعة ومتغيرة بشكل كبير، مما زاد من الفجوة المعلوماتية القومية بين الدول. شكل هذا التعاون

---

[1]– عادل عبد الصادق، "**المجال الأعلى للأمن السيبراني خطوة في دعم استراتيجية الأمن القومي**"، الرابط: www.aceronline.com/article-detal.Aspxd=20284 تاريخ التصفح 2019/03/01.

[2]– عادل عبد الصادق، "**الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي**"، مرجع سابق، ص04.

[3] علي عباس مراد، "**الأمن والأمن القومي، مقاربات نظرية**"، (الجزائر: ابن النديم للنشر والتوزيع، 2017)، ص12.

[4]– عادل عبد الصادق، **موقع سابق**.

[5]– وليد غسان سعيد جلعود، "**دور الحرب الإلكترونية في الصراع العربي الإسرائيلي**"، أطروحة ماجستير في التخطيط والتنمية السياسية (بكلية الدراسات العليا، جامعة نابلس، فلسطين، 2013)، ص53.

المعلوماتي القومي بين دول العالم هاجس الخوف من الطرف الآخر ومدى امتلاكه للأسلحة التكنولوجية والمعلوماتية المدمرة والتي لم تعد حكرا على القطاعات العسكرية للدول فحسب، بل أصبحت سلاحا تتقن استخدامه غالبية مستخدمي الحواسيب ووسائل الاتصال الحديثة، وفي صورة زادت من تفاعل المعلومات الإلكترونية والأمن القومي بحيث رفعت من وتيرة الخوف الذي تعاني منه شعوب العالم المعاصر.

ومن هنا نستنتج أن الأمن السيبراني والأمن القومي يتشابكان من ناحية الهدف، حيث يسعى كل منهما إلى حماية البنى التحتية والحدود من كل الاختراقات التكنولوجية والتخوف من زعزعة أمن الدولة. [1]

المطلب الثالث: أبعاد الأمن السيبراني

سيتم التطرق في هذا المطلب إلى أبرز أبعاد الأمن السيبراني ويشمل العديد من الأبعاد سيتم ذكرها كالتالي:

الفرع الأول: البعد العسكري

تكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الالكتروني، بما يسمح بسهولة تبادل المعلومات وتدفقها، وكذا السرعة وإعطاء الأوامر العسكرية والقدرة على إصالة الأهداف عن بعد وتدميرها، وقد تتحول هذه الميزة إلى نقطة ضعف لا قوة إن لم تكن شبكة الإلكترونية المستخدمة في ذلك مؤمنة جيدا من أي اختراق خارجي قد ينسب في شن هجمات إلكترونية مضادة على شبكات القوات المسلحة وأجهزة الاستخبارات، ومن ثم تجسس على أمن العسكري للدول، وتعطيل قدرة الدولة على النشر السريع لقدراتها وقواتها، أو قطع أنظمة الاتصال في ما بين الوحدات العسكرية وتعطيل شبكات الكمبيوتر، كما يمكن أن يتم شل وتعطيل عمل أنظمة الدفاع الجوي أو التوجيه الالكتروني فضلا عن إمكانية وفقدان السيطرة على وحدات القيادة[2].

كما أن من أبرز مميزاته تعطيل قدرة الدولة على النشر السريع لقدراتها وقواتها أو قطع أنظمة الإتصال بين الوحدات العسكرية وتعطيل شبكات الكمبيوتر. كما يمكن أن يتم شل أنظمة الدفاع الجوي أو التوجيه الإلكتروني للخصم فضلا عن إمكانية فقدان السيطرة على وحدات القيادة والتوجيه[3].

---

[1]- وليد غسان سعيد جلعود، **مرجع سابق**، ص54.

[2]- د.م، **"النظام القانوني للأمن الوطني الالكتروني في ظل الثورة الرقمية"**، من الرابط: www.univ-chlef.dz/fdsp/pdf/je-droits2017.pdf تاريخ التصفح: 2019/02/28

[3]- محمد مختار، **مرجع سابق**، ص6.

الفرع الثاني: 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 الإستخدام التي تقدمها الشركات الدولية والشركات الكبرى التي تبحث في إدارة كلفة إنتاجها بأفضل الشروط.

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[1].

الفرع الثالث: 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. وبالمقابل لا يتوانى العاملون في الشأن السياسي من الإستفادة 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

[1]- مني أشقر جبور، **مرجع سابق**، ص31.

الشبكات الاجتماعية بشكل مكثف خلال حملته الإنتخابية كما تركت التسريبات لآلاف الوثائق الدبلوماسية السرية عبر الويكيليكس* أثرا سلبيا على العلاقات بين الدول.[1]

الفرع الرابع: البعد الاجتماعي

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 إنفتاح 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. والمساهمة في الحفاظ على القيم الجوهرية في المجتمع كالإنتماء والمعتقدات والعادات والتقاليد عبر إنشاء مجموعات تهتم بنشر ثقافة الأمن في الفضاء الإلكتروني وضرورة التعاون من قبل فئات المجتمع بكل مكوناته على تحقيقه وضمانه لحمايته من التهديدات السيبرانية.

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 تترتب على بعض التصرفات التي تمارس في الفضاء الإلكتروني[2].

الفرع الخامس: البعد القانوني

تعد العلاقة بين القانون والتكنولوجيات علاقة تبادلية فالتطورات التكنولوجية علاقة تبادلية فالتطورات التكنولوجية المختلفة تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية

---

* **الويكيليكس**: هي منظمة دولية غير ربحية تنشر تقارير وسائل الإعلام الخاصة والسرية من مصادر صحفية وتسريبات أخبارية مجهولة. بدأ موقعها على الإنترنت سنة 2006 تحت مسمى منظمة سن شاين الصحفية، وادعت بوجود قاعدة بيانات لأكثر من 1.2 مليون وثيقة خلال سنة من ظهورها ، وتصف ويكيليكس مؤسسيها بأنهم مزيج من المنسقين الصينيين والصحفيين والرياضيين وتقنيون مبتدؤون لشركات عاملة في الولايات المتحدة وتايوان وأوروبا وأستراليا وجنوب أفريقيا . ومديرها جوليان أسانج وهو ناشط إنترنت استرالي، أنطلق الموقع كويكي للتحرير، ولكنه انتقل تدريجيا نحو نموذج نشر أكثر تقليدية و لم يعد يقبل بتعليقات المستخدمين أو كتاباتهم.

[1]– منى أشقر جبور، **مرجع سابق**، ص30.

[2]– محمد مختار، **مرجع سابق**، ص7.

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 حد 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].

يضم الأمن جميع المسائل الاقتصادية، والاجتماعية والسياسية والإنسانية، وإنطلاقا من مفهوم الأمن السيبراني على أنه قدرة الدول في حماية مصالحها وشعبها، في مختلف مجالات حياته اليومية ومسيرته نحو التقدم، ومن كونه يرتبط ارتباطا وثيق بسلامة مصادر الثروة في العصر الحال ونعني بها البيانات والمعلومات والقدرة على الاتصال والتواصل وهي المحور التي تبنى على أساسها الإنتاج والإبداع والقدرة على المنافسة.

المبحث الثاني: أشكال الأمن السيبراني

يتخذ الأمن السبراني عدة أشكال من خلال التعرف على أهم الآليات والبرمجيات التي يمكن من خلالها الحد من انتشار مختلف تهديداته والتي يمكن التطرق لأهمها وفقا لما يلي:

المطلب الأول: القرصنة الالكترونية

من خلال هذا المطلب سيتم التطرق إلى مفهوم القرصنة الإلكترونية وكذا تاريخها ومختلف تصنيفاتها كما يلي:

الفرع الأول: مفهوم القرصنة الإلكترونية

عندما يتبادر إلى سماعنا كلمة قرصنة فإننا نتخيل عصابات سرق السفن البحرية والسطو عليها ونهب ما فيها وأسر طاقمها، وهو ذاته ما يفعله قرصان الأنظمة الإلكترونية بالضبط لكن بوسائل حديثة ودون أن يعرض نفسه للخطر، ودون أن يدركه أحد أو يتعرف على شخصيته.

فالقرصنة الإلكترونية أو المعلوماتية هي عملية إختراق لأجهزة الحاسوب تتم عبر شبكة الإنترنت غالبا، إلا أن أغلب حواسيب العالم مرتبطة عبر هذه الشبكة، أو حتى عبر شبكات داخلية يرتبط فيها أكثر من جهاز حاسوب ويقوم بهذه العملية شخص أو عدة أشخاص متمكنين في برامج الحاسوب وطرق إدارتها، أي إنهم

---

* **الجريمة الإلكترونية** 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

[1] محمد مختار، **مرجع سابق**، ص 7.

مبرمجون ذو مستوى عال يستطيعون بواسطة برامج مساعدة إختراق حاسوب معين والتعرف على محتوياته ومن خلالها يتم إختراق باقي الأجهزة المرتبطة معها في نفس الشبكة.[1]

الفرع الثاني: تاريخ القرصنة

من شيوع استخدام الكمبيوتر أواخر سبعينات القرن الماضي برزت ظاهرة القرصنة الإلكترونية، وسرعان ما تحول السلوك الذي بدأ في بدايته إنحرافا لمراهقين شغوفين بالتكنولوجيا، وهي تهدد منشآت حيوية كالمفاعلات النووية ومحطات الكهرباء كما تدمر المخزونات النقدية لبنوك ودول وتهتك أسرار لا يراد لها الخروج إلى العلن.

لا يمكن فعليا تحديد الفترة الزمنية لأول عملية إختراق، وذلك لأن مفهوم الإختراق قديما لم يكن يعني مجرد إختراق شبكة حاسوب أو موقع إلكتروني، وإنما كان إختراق أي جهاز لتحقيق هدف خاص.

وفي عام 1903 كان الفيزيائي "جون أمبرون فلمنج" يستعد لعرض إحدى العجائب التكنولوجية المستجدة وهي نظام "تلغراف لاسلكي" بعيد المدى ابتكره الإيطالي "جوليلمور ماركوني" في محاولة الإثبات أن رسائل شفرة مورس يمكن إرسالها لاسلكيا عبر مسافات طويلة، وكان ذلك أمام جمهور غفير في قاعة محاضرات المعهد الشهيرة بلندن.

وفي عام 1932 تمكن خبراء التشفير البولنديون ماريان ريجيوسكي وهنري زيجلاسكي وروزيكي من فك شفرة جهاز إنيغما الذي استخدمه بشكل خاص الألمان خلال الحرب العالمية الثانية لإرسال واستقرار وسائل سرية.

وفي عام 1971 إبتكر جون درابر الملقب بكابتن كرنتش وصديقه جو أنغريسيا الصندوق الأزرق الذي استخدماه للتحايل على نظام الهاتف وإجراء مكالمات هاتفية بعيدة المدى مجانا.

في عام 1981 تشكلت مجموعة قراصنة في ألمانيا، ومجموعة أسياد البرامج في أمريكا، المكونة من المتسللين المراهقين ومحترفي الهاتف والمبرمجين والعديد من قراصنة الحاسوب الذين يعملون في الخفاء.

وفي عام 1988 ظهرت "دودة موريس" إحدى أوائل دايدن الحواسيب المعروفة التي في البنية التحتية للإنترنت وانتشرت في الحواسيب وعلى نطاق واسع داخل الولايات المتحدة الأمريكية. واستغلت الدودة نقطة

[1] – كريم حميد، **"القرصنة الإلكترونية"**، من الرابط: https://www.alakah.net/culturel/0/52639/ تاريخ التصفح 2013/04/04.

ضعف في نظام يونيكس "ناون وان" واستنسخت ذاتها بإنتظام وتسببت بإبطاء أداء الحواسيب لدرجة عدم القدرة على استخدامها.

وفي عام 1994 تمكن قرصان روسي يدعى فلاد يمبرليفين من اختراق بنك "سيتي بنك" الأمريكي وتحويل عشرة ملايين دولار من حسابات عملاء إلى حساباته الشخصية في فنلندا وإسرائيل مستخدما حاسوبه المحمول.

في يناير 2009 وخلال العدوان الإسرائيلي على قطاع غزة تعرضت بنية الإنترنت التحتية في إسرائيل لهجمات إلكترونية عديدة تركزت على موقع إلكتروني حكومة، ونفذت الهجمات بإستخدام نحو خمسة ملايين حاسوب على الأقل وفقا لمجلة "ناتوريفيوا" الإلكترونية، وتبنت مجموعة القراصنة المجهولين أنونيموس الكثير من تلك الهجمات[1].

الفرع الثالث: تصنيفات القرصنة الالكترونية

يمكن ّأخذ اهم تصنيفات القرصنة الالكرتونية وفقا لما يلي:

1- الهواة (الهاكرز – Hackers) يعتمد الهواة على برامج التجسس الجاهزة والمتاحة في كل مكان سواء عن طريق الشراء أو التحميل من شبكة الإنترنت، ويقوم الهاكرز بزرع ملفات التجسس (Patches&Trojans) في حواسيب الضحايا عن طريق البريد الإلكتروني أو ثغرات الويندوز التي يكشفها البرنامج. هذا الصنف من الهاكرز أهدافه طفولية؛ حيث يسعى لإثبات نجاحه في استخدام هذه البرامج وانضمامه إلى قائمة الهاكرز، بهدف التفاخر بين الأصحاب كشخص يمتلك مواهب يفتقدها بعضهم، وهؤلاء كل ما يشغلهم هو التسلل إلى الحواسيب وسرق بريدهم الإلكتروني. وللهكرز مهارات، وهي أنهم يستطيعون إختراق مواقع الشركات، وإختراق كلمة السر، سواء الخاصة بالبريد الإلكتروني أو موقع الشركة على الإنترنت، أو فك "السيريل نمبر" عند تثبيت برنامج.

2-المحترفون (الكراكرز-Crackers) أما المحترفون فهم الفريق الأخطر لأنهم يعلمون ماذا يريدون وماذا يفعلون، وكيفية الوصول إلى أهدافهم بإستخدام ما لديهم من علم يطورونه بإستمرار، بالإضافة إلى استخدام البرامج الجاهزة المتطورة، إلا أنهم يعتمدون على خبرتهم في لغات البرمجة والتشغيل، وتصميم وتحليل وتشغيل البرامج بسرعة، كما أن هوايتهم الأساسية معروفة كيفية عمل البرامج لا تشغيلها.

[1] - **"القرصنة الالكترونية ... سلاح العصر الرقمي"**، من الرابط: www.aljazeera.net/knowledg/newscoverage، تاريخ التصفح: 2019/03/14.

إن أهداف هذا الفريق أكبر وأخطر من الفريق السابق، فأهدافهم المصارف وسحب الأموال من حساب العملاء، أو الولوج إلى أخطر المواقع وأكثرها حساسية والتلاعب ببياناتها أو تدميرها. [1]

المطلب الثاني: الإرهاب السيبراني

يمكن تحديد مفهوم الأمن السبراني وفقا لما يلي:

الفرع الأول: مفهوم الإرهاب السيبراني

إن الإرهاب السيبراني مفهوم يتضمن العديد من التعقيدات، ويمكن تفسير هذا المصطلح على أنه استخدام تكنولوجيا المعلومات من قبل الجماعات أو الأفراد الإرهابيين لتحقيق أهدافهم، وتنظيم وتنفيذ هجمات ضد الشبكات وأنظمة الكمبيوتر والبنية التحتية للاتصالات، وتبادل المعلومات وأداء تهديد إلكتروني، ويتجلى هذا النوع من التهديد الأمني في العديد من الطرق مثل إختراق أنظمة الكمبيوتر ونشر فيروسات أو تعطيل نظام إلكتروني متعلق بمؤسسة معينة كمؤسسة الصحة أو الطيران[2].

وتعرفه دوروثي داميغ Dorothy E Deming مديرة معهد جورج تاون لتأمين المعلومات في جامعة جورج تاون بالولايات المتحدة الأمريكية بأنه:" التقارب بين الإرهاب والفضاء السيبراني، ويعني تلك الهجمات غير المشروعة والتهديدات التي تستهدف أجهزة الكمبيوتر والشبكات والمعلومات المخزنة وتعمل على تخويف الحكومة وشعبها، وذلك من أجل تحقيق أهداف سياسية أو دينية أو عقائدية، وينبغي أن تكون الهجمات لديها القدرة على تعطيل أو تخريب خدمة ضرورية، أو تشكل إزعاجا من الناحية الاقتصادية للخصم بحيث تكون مشابهة للأفعال المادية للإرهاب".

ويعرف الإرهاب السيبراني أيضا على أنه "الفعل المتعمد الذي تقوم به جهات فاعلة في الأنترنت قصد تدمير أو تخريب أو تعديل البيانات أو تدفق المعلومات، أو نظم المعلومات الحيوية للدولة أو الشركات، بحيث أن الغرض من إحداث الضرر يكون للأسباب سياسية أو دينية أو إيديولوجية"[3].

وإنطلاقا من التعريفات المقدمة المستخلص بأنه الإرهاب السيبراني هو أحد الأنماط المستخدمة للإرهاب الذي يعبر عن تكيف الجماعات الإرهابية مع تكنولوجيا المعلومات وشبكة الإنترنت، وبالتالي أنتج لنا ما يسمى الإرهاب السيبراني، هو مصطلح يعبر عن استخدام الجماعات الإرهابية لتكنولوجيا المعلومات لشن

---

[1]- **"القرصنة الالكترونية ... سلاح العصر الرقمي"، موقع سابق.**

[2]- جارش عادل، **"مقاربة معرفية حول الإرهاب السيبراني"**، مجلة المستقبل العربي، العدد20، بيروت، لبنان،2000، ص73.

[3]- جارش عادل، **مرجع سابق**، ص 76.

هجمات ضد أجهزة الكمبيوتر والبنى التحتية للدولة والأفراد بغرض تحقيق أهداف سياسية. ويطلق عليه أيضا الإرهاب الإلكتروني أو الإرهاب الصامت أو الناعم.

الفرع الثاني: خصائص الإرهاب السيبراني

يعتبر الإرهاب السيبراني خيارا جذابا للإرهابيين المحاربين نظرا لعدة نقاط يمكن إبرازها على النحو التالي:

– من حيث التكلفة يعتبر الإرهاب السيبراني أرخص من الأساليب الإرهابية التقليدية، وكل ما يحتاجه الإرهابي هو كمبيوتر وشبكة إنترنت، ولا يحتاج إلى شراء أسلحة ومتفجرات باهضة الثمن.

– الإرهابي السيبراني هو طرف مجهول يرمز له ب(X) فعادة ما يستخدم أسماء مستعارة أثناء هجومه، مما يجعل من الصعب للغاية على وكالات الأمن وقوات الشرطة تعقب هويته الحقيقية عكس للأساليب التقليدية التي يمكن فيها معرفة هوية الإرهابي بسهولة.

– القيام بالهجوم عن بعد، وهي ميزة جذابة بشكل خاص للإرهابي، وهو ما يجعله أقل عرضة للموت والمواجهة المباشرة مع الأمن.

– سهولة تجنيد الأتباع عبر شبكات التواصل الاجتماعي عكس الطرق التقليدية التي كانت تعتمد على الأسلوب المباشر، فعلى سبيل المثال أحدث تنظيم داعش تنظيما فرعيا تحت إسم "الخلافة السيبرية" تمكن من خلاله سنة 2015 من إختراق موقع التواصل الخاصة بالقيادة المركزية الأمريكية.

– القدرة على تولي تغطية أكثر عبر الإنترنت، وبالتالي زيادة القدرة على التأثير في الأشخاص.

– تنوع وتعداد الأهداف واسع في الفضاء السيبراني عكس الفضاء التقليدي الذي يعد صعب ومحدود، فمثلا يستطيع الإرهابي عبر شبكة الإنترنت المساس بحركة الطيران والمرور، السدود، والمرافق العامة وغيرها[1].

– شبكة الإنترنت ألغت الحدود الجغرافية بين الفواعل الدولية، فحاليا يستطيع الأشخاص التواصل فيما بينهم من عدة دول في نفس الوقت من خلال الدردشة أو وسائط إلكترونية أخرى، وعليه فإن الجماعات الإرهابية استطاعت أن تزيد من الصبغة الدولية في هجماها وتأثيراها من خلال هذه الميزة، وأصبحت السيادة بالنسبة لها ليس صعب المنال خاصة وأن الفضاء السيبراني أتاح لها مرونة في إرتكاب الجرائم في أي منطقة في العالم[2].

---

[1] – جارش عادل، **مرجع سابق**، ص 77.

[2] – عبد الحميد ابراهيم، محمد العريان، **"العلاقة بين الارهاب المعلوماتي والجريمة المنظمة ما هو رد القطاع الخاص"**، من الرابط: ص17، repository.nauss.edu.sa/bitstream/handies/9.pdf تاريخ التصفح 2019/04/10

الفرع الثالث: وسائل الإرهاب السيبراني

البريد الإلكتروني: ظهر البريد الإلكتروني في عام 1972 عندما قام راي توملنسون بتقديم أول برنامج للبريد الإلكتروني، ليصبح فيما بعد من خلال سلسلة من التحديات أحد أكثر الشبكات والخدمات انتشارا واتساعا على الإنترنت وهو بمثابة نقلة نوعية في عملية التراسل بين الفواعل، إذ ساهم البريد الإلكتروني في الإنتقال من النمط التقليدي للتراسل الذي كان يعتمد بشكل كبير على الفاكس إلى البريد الإلكتروني[1].

ويستخدم الإرهابيون البريد الإلكتروني للتواصل بينهم وتبادل المعلومات بينهم كما يستغلونهم في نشر أفكارهم والترويج لها وتجنيد أفراد في صفوفهم.

وعموما يقوم الإرهابيون في هذا الجانب بإنشاء وتصميم مواقع لهم على شبكة الأنترنت تنشر أفكارهم والدعوة إلى مبادئهم، بل لتعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية، ومن الأمثلة على بعض المواقع الإلكترونية العربية التي قام بإنشائها وتصميمها بعض التنظيمات الإرهابية نجد:

- موقع النداء: وهو الموقع الرسمي لتنظيم القاعدة بعد أحداث 11 سبتمبر 2011، ومن خلاله يتم إصدار البيانات الإعلامية للتنظيم.

- ذروة السنام: وهي صحيفة إلكترونية دورية للقسم الإعلامي لتنظيم القاعدة في جزيرة العرب، وهي وتتضمن مجموعة من البيانات والحوارات مع قادة التنظيم ومنظريه تصدر بصيغتي (PDF) و(Word) .

- البتار: وهي مجلة عسكرية إلكترونية متخصصة تصدر عن تنظيم القاعدة وتختص بالتجنيد والمسائل العسكرية[2].

- شبكات التواصل الإجتماعي Social networks: تعرف شبكات التواصل الاجتماعي بأنها شبكات تفاعلية افتراضية تتيح لمستخدميها التواصل في أي وقت وفي أي مكان من العالم، وتتسم بأنها شبكات عالمية فرضت أنفسها بقوة خاصة في العشر سنوات الأخيرة، وذلك لأن أغلب تلك الشبكات متاحة للجميع وبالمجان. ولأنها صممت أساسا لتكون سهلة الإستخدام وبدون تعقيدات، ومن بين الشبكات نجد الفيسبوك،

---

[1] - وجيه دسوق مرسي، **"الأساليب الالكترونية الحديثة التي تستخدمها التنظيمات الارهابية في الجرائم الارهابية"**، من الرابط: ص154،repository.nauss.edu.sa/bitstream/handies/1.pdf تاريخ التصفح 2019/04/10

[2] - بكر أبو بكر، **"الإرهاب الالكتروني من الدعاة والاستقطاب الى اكتساح المجال الافتراضي"**، (المغرب، مجلة ذوات، العدد46، 2018)، ص23.

والتويتر، والإنستغرام، الواتساب وغيرها، ومما لا شك فيه أنه مع انتشار شبكات التواصل الاجتماعي فإن ذلك أتاح الفرصة للإرهابيين لتوظيفها في أنشطتهم[1].

وتستخدم التنظيمات الإرهابية شبكات التواصل الاجتماعي لأغراض منها: الدعاية، نشر التطرف، التجنيد أو جذب جهاديين جدد، من حيث تجند الجماعات الإرهابية بعض الصفحات على موقع التواصل الاجتماعي، ومن ثم تعمل على محاولة جذبهم ودعوتهم للإنضمام إليها، فعلى سبيل المثال تشير التقارير إلى أن 80% من الذين انتسبوا لداعش ثم تجنيدهم عبر شبكات التواصل الاجتماعي، وأن نحو 200 ألف مستخدم يقرؤون يوميا رسائل التنظيم، وأن داعش ينشر ما يزيد عن 90 ألف مادة إعلامية دعائية يوميا على الشبكات الاجتماعية، وأن أكثر من 2600 موقع إنترنت وشبكة تواصل اجتماعي ترتبط بالتنظيم وتخاطب العالم بلغات متعددة منها الإنجليزية والعربية والفرنسية.

لقد بنت شبكات التواصل الاجتماعي ما يسمى بالإستقطاب السريع Rapid polarization للجماعات الإرهابية، ويعبر عن مدى قدرة التنظيم على الحفاظ على الأعضاء وإستمالة أكثر عدد من الأفراد للإنضمام، وقد يكون ذلك عبر الإقناع العلمي المنطقي، أو بالأسلوب النفسي العاطفي أو بإستثمار الترعة الدينية أو القومية أو الإيحاء غير المباشر، وذلك كله عبر هذه الشبكات التي أصبحت الفضاء المميز للجماعات الإرهابية[2].

وأهم ثلاث تطبيقات تستخدمها التنظيمات الإرهابية في مجال شبكات التواصل الاجتماعي كالآتي:

- **الفايسبوك Facebook**: يعتبر الفايسبوك الشبكة الاجتماعية الأضخم والأكبر بمليار مستخدم، وحسب مجلة محرك البحث فإن عدد المستخدمين يصل إلى 03مليار مستخدم سنة 2016، 8.7% و7.4 عام 2017، يبلغ معدل عمر مستخدمي الفايسبوك 30 سنة، وتبلغ نسبة انتشاره في الشرق الأوسط 67%، ولقد اهتمت الجماعات الإرهابية بإستخدام الفايسبوك ودعت إلى غزوه نظرا لفاعليته وتحقيق الأهداف المختلفة من خلاله كتقديم المعلومات الخاصة بصناعة القنابل والقيام بعمليات القتل وتقديم مختلف المعلومات للمنتسبين والقيام بالدعاية واستخدامه كذلك كبنك للمعلومات.

---

[1] - يوسف بن أحمد الرميح، "**الإرهاب في شبكات التواصل الاجتماعي**"، من الرابط، www.aljazeera.com/ar2.htm تاريخ التصفح 2019/04/11

[2] - أماني المهدي، توظيف التنظيمات "**الإرهابية لشبكات التواصل الاجتماعي في استقطاب الشباب "الاستراتيجيات وآلية المواجهة"**"، الرابط: www.kitabat.com/culturel تاريخ التصفح 2019/04/11،

تويتر Tweter: أحد أشهر الشبكات الاجتماعية ووسائل التواصل الاجتماعي، يقدم خدمة التدوين المصغر والتي تسمح لمستخدميه بإرسال "تغريدات" عن حالتهم أو عن أحداث حياهم أو إبداء أرائهم .

المواقع الإلكترونية Web sites: الموقع الإلكتروني هو عبارة عن معلومات مخزنة بشكل صفحات وكل صفحة تشمل على معلومات معينة تشكلت بواسطة مصمم الصفحة بإستعمال مجموعة من الرموز تسمى لغة (Html). تحديد النص الأفضل html ولأجل رؤية هذه الصفحات يتم طلب استعراض شبكة المعلومات العنكبوتية Browser ويقوم بحل الرموز.

مما سبق نستنتج أن الإرهاب السيبراني يعد من الأنماط الجديدة للإرهاب (الجيل الخامس) يمثل المهدد الناشئ، له تأثيرات راهنة وأخرى مستقبلية محتملة تؤثر بشكل سلبا على الأمن البشري خاصة، والأمن الدولي خاصة، وتؤثر كذلك على استقرار كل القطاعات داخل الدول، كالقطاعات الاقتصادية والأمنية والسياسية والاجتماعية والثقافية. للإرهاب السيبراني جملة من الخصائص التي تميزه من حيث التكلفة لا يكلف كثيرا، بعكس الإرهاب التقليدي ومن حيث الفاعل فاعله مجهول ، والهدف أوسع في الفضاء السيبراني عكس الفضاء التقليدي الذي يعد صعب ومحدود.

المطلب الثالث: مفهوم الحرب السيبرانية

تحولت الساحة الإلكترونية العالمية إلى أرض معارك حقيقية، في عالم افتراضي تقني يعتمد على كل ما هو جديد من صيحات التكنولوجيا الرقمية والإتصالية الحديثة، وتعددت أشكالها ما بين الفرعي والجماعي، والدولي والمؤسساتي، والسياسي والاقتصادي والاجتماعي، والمتهمة بالإرهاب.

الفرع الأول: مفهوم الحروب السيبرانية

تعرف الحرب السيبرانية "الحرب الإلكترونية ترتبط بالأساس بالتطبيقات العسكرية للفضاء السيبراني، وهي تعني في إحدى تعريفاها أن تقوم دولة أو كيان ما بشن هجوم إلكتروني، وذلك في إطار متبادل، أو حتى من طرف واحد". وعلى الرغم من انتشار مصطلح "الحرب الإلكترونية" على نطاق واسع على المستوى الإعلامي، فإن المصطلح ذاته يعد قديما، خصوصا مع إقترانه مع رصد حالات التشويش على أنظمة الاتصال، والرادار، وأجهزة الإنذار المعروف إبان حروب القرن العشرين، أما في الوقت الراهن فإنه يرتكز على تفاعلات الفضاء الإلكتروني، مع دخول شبكات الاتصال والمعلومات الرقمية إلى المجال العسكري.

وبناء على ما سبق، ومع تمدد الأعمال العدائية في الفضاء الإلكتروني، ووصولها إلى البنية التحتية المعلوماتية للدول، لتحقيق العديد من الأغراض فقد تجاوز الأمر مفهوم الحروب الإلكترونية، ليحلو للبعض

تسميته ب"الحرب السيبرانية"، تعبيرا عن الشكل الجديد للحروب الإلكترونية. وهي "هجمات الفضاء الإلكتروني وتكون غير محدودة المجال، ولا التوقيت، ولا حتى بدايتها أو نهايتها، وتكون أهدافها غامضة، علاوة على اعتمادها على أسلحة إلكترونية تناسب طبيعة المهام التي تقوم لأجلها"[1].

تعرف الحرب السيبرانية بأنها "حرب تخيلية Virtual&wor أو افتراضية ذات طبيعة غير ملموسة، تحاكي الواقع بشكل شبه تام، وهي حرب بلا دماء، بحيث تتلخص أدوات الصراع فيها بالمواجهات الإلكترونية، والبرمجيات التقنية، وجنود من برامج التخريب المحسوبة، وطلقات من لوحات المفاتيح ونقرات المبرمجين في بيئة اصطناعية تحاول ما أمكن للوصول إلى صورة حقيقية لملامح الحياة المادية والملموسة".[2]

الفرع الثاني: القطاعات التي تستهدف الحروب السيبرانية

إن تطور التكنولوجيا في العالم وتكاثر احتياجات الفرد، عمل على تغير الفكر عنده حيث أصبح من المستحسن توفير جانب التكنولوجيا المتطور في حياة الفرد. مثل وجود الحواسيب خاصة في المرافق الحكومية والغير حكومية وأن تكون معاملاتها الخدماتية متاحة لجماهيرها عبر الإنترنت، وأن تتوفر بياناتها الضرورية عبر شبكات الفضاء الرقمي، إلا أن كل هذا قد تكون عليها دفعه، فمخاطر الفضاء الإلكتروني عالية، الأمر الذي يدفع بدول أن تكشف عن خاطرتها الضعيفة خصوصا إذا ما تعلق الأمر بتلك المرافق التي يكون فيها الضغط الإلكتروني عليها كثيرا.

1- قطاع الاتصالات الحديثة والمعلومات: يشمل هذا القطاع جميع شبكات الاتصالات العامة للدولة، وعلى رأسها الإنترنت والحاسبات، والشبكات الحكومية والأكاديمية والمدنية والتجارية، والشبكات المحلية والخارجية ومحطات البث التلفزي، وشبكات الخلوي، ومراكز استقبال الموجات السلكية واللاسلكية والألياف البصرية fiber-obtique، وجميع ما يمكن إدراجه تحت هذا القطاع الاتصالي والمعلوماتي، تعد هذه القطاعات أكثر ملائمة للحروب السيبرانية، لإعتمادها بشكل كبير على وسائل الإتصالات الحديثة.

تحاول الحكومات الإلكترونية اليوم الخروج بقالب من الثقة التي تغريها من جمهور المتلقي، كما وتحاول التغلب على القطاعات الخاصة المنافسة لها في النواحي الخدماتية والإدارية والفنية، لما لذلك من مكاسب مادية واقتصادية واجتماعية تصب في الصالح السياسي والاقتصادي والاجتماعي والأمني لحكومات دول العالم،

---

[1]- حسام السبكي، "**الحروب السيبرانية، المفهوم، والأنماط والتداعيات على الأمن الدولي**"، جريدة الأخبار (13 أوت 2015) ، من الرابط: www.royenhenews.com/articles/4809 تاريخ التصفح 2019/04/09

[2]- مساعد كمال، "**الحروب الإفتراضية وسيناريوهات محاكاة الواقع**"، (لبنان، مجلة الجيش اللبناني(ع: 253، يوليو 2006م)، من الرابط: www.lebarmy.gov.ib/article.ospfind=11575 تاريخ التصفح 2019/04/09

لذلك فإن ضرب الخدمات الإلكترونية التي تقدمها هذه الحكومات يعني كسر قالبها الأمني، ونزع الثقة عنها، وبالتالي خسارتها لجمهورها المتلقي[1].

2- قطاعات الطاقة والتوزيع الفيزيقي: تشكل هذه القطاعات الفيزيقية البناء الأساسي للبنية التحتية الكاملة لأي دولة في العالم، حيث تضم باقة من القطاعات الهامة، كالأمن الوطني، والاقتصاد السياسي القومي، وترابط الطرق عبر الخرائط الإلكترونية، ومراكز تسيير حركات النقل في القطاعات البرية والجوية والبحرية ومراكز مراقبة الكوارث الطبيعية، ومصادر توزيع الطاقة والبنوك وبنوك الأهداف المعلوماتية وغيرها من الادارات المسؤولة عن قطاعات توليد الطاقة داخل أي بلاد في العالم[2].

3- قطاع الأعمال العسكرية والحربية: شهدت القطاعات العسكرية والحربية تطورات عديدة جعلت منها مجالات ذات اعتمادية كبيرة على عنصر المعلوماتية والرقمية، وحولتها إلى بناءات تتسلح بأجيال جديدة من الأسلحة التكنولوجية والاتصالية، وزادت من قدراتها وفاعليتها على الدعم اللوجستي، والتواصل المعلوماتي والاستخباراتي القائم على توفر عنصر التقنية الحديثة، والذي أضفى على الوسائل والأدوات العسكرية والحربية قدرا كبيرا من الدقة الجاهزية[3].

5- قطاع الأعمال والأنظمة الحكومية وغير الحكومية: كما هو الحال في جميع القطاعات الإلكترونية المحسوبة، والتي تعتبر هدفا مباشرا لنيران وقذائف الحروب السيبرانية، فإن القطاعات الحكومية بشكل عام، وتلك التي تتعلق بالعمل المدني والإداري، وتقديم الخدمات للجماهير بشكل خاص، معرضة لتلقي ضربات إلكترونية كونها أحد أهداف الصراعات التقنية في عالمنا اليوم، خاصة بين الحكومات التي تتسابق إلى الدخول في تطبيق منظومات الحوكمة الإلكترونية، أو تلك الشركات التي تعيش القالب التنافسي الرقمي[4].

6- قطاعات المعلومات الإعلامية والمجتمعية: تشترك الصحافة ووسائل الإعلام مع باقي أدوات الاتصال في تقديم العديد من المعلومات والبيانات للجمهور المتلقي، وذلك عبر الوسائل التقنية والرقمية الحديثة، والتي

---

[1] - جلعود، غسان، **مرجع سابق**، ص90.

[2] - ذياب البداينة، **"الأمن وحرب المعلومات"**، ط1، (دار الشرق للنشر والتوزيع، دب، 2006)، ص40.

[3] - بورجيلي ريمون، **"التكنولوجيات الحديثة في المجالات العسكرية"**، (مجلة الجيش اللبناني، عدد236، شباط 2009) ، من الرابط: www.lebenarmy.gov.lb/article.asp=arfid=7066 تاريخ التصفح 2019/04/18

[4] - **الموقع نفسه**.

تغذي البشرية بكل ما يجول في عالمها الحاضر، بحيث تختزل المسافات والأحداث للإنسان وتقدمها له بقالب معلوماتي له أهمية كبرى في ديمومة بقائه بصدارة ما يجري من أحداث في عالمه بشكل إلكتروني.[1]

7- قطاعات الاقتصاد والمال والأعمال: تحظى قطاعات المال والأعمال في عقدنا الحالي بأهمية كبيرة، خاصة بعد التحولات الاقتصادية والرأسمالية التي شهدها العالم في عقده الأخير، واندفاع البشرية نحو العمل الاقتصادي والمالي، وسهولة التبادلات التجارية المعتمدة على التجارة الإلكترونية والإدارة الدولية، انتشار القيم الرأسمالية الداعية للإستهلاك والإنفتاح الاقتصادي المرتكز على العنصر التكنولوجي، والذي أدخل البشرية جمعاء في عصر اقتصادي معتد بالرقميات التكنولوجيا والإلكترونية الحديثة تقيس الاقتصاديات المتقدمة اليوم في دول العالم، وتلك التي تحاول اللحاق بركب المعلوماتية، مرحلة التحول إلى الاقتصاديات الرقمية المرتكزة على عنصر المعرفة و المعلوماتية، مشكلة مجتمعات اقتصادية شبكية، واقتصاديات افتراضية، قائمة على العمل التقني وشبكات الإنترنت، وغيرها من وسائل التواصل الرقمي، والتجارة الدولية، والسلع الرقمية وكافة أشكال العمل المالي والاقتصادي الموجود عبر الفضاء الإلكتروني.[2]

8- القطاعات الإنسانية والاجتماعية: تتحلى هذه القطاعات بالطابع المعنوي، والذي يقوم بتعزيز القيم الإنسانية، والإعتبارات الوطنية والاجتماعية والولاء للدولة والأمن الفكري. وغيرها من القيم التي يحتاجها الإنسان لتعزيز صموده في ظل التأثيرات التي قد يتعرض لها أثناء تجواله عبر الفضاء الإلكتروني،[3] تأخذ هذه القطاعات شكل مواقع التواصل الاجتماعي المنتشرة عبر الإنترنت، والمدونات الاجتماعية والسياسية، وقنوات التواصل الرقمية، والفضائيات التلفزية. والتي تعتبر منافسا سياسيا اجتماعيا في كثير من بلدان العالم، ووسائل جماهيرية وشعبية لإيصال الرسائل المجتمعية لصانعي القرارات، سجلت هذه القطاعات حضورا متميز في مسيرة الإنسان المعاصر وقدمت له العديد من الخدمات، وأتاحت له ساحة ومساحة من الحرية، وأداة فعالة لكسر حواجز الخوف، وفاضحة لممارسات الفساد ضد الإنسانية في العديد من دول العالم، وأهلت له الوصول الافتراضي والرقمي إلى منابع المشاكل الاجتماعية والاقتصادية والسياسية.[4]

---

[1]- غسان، جلعود، **مرجع سابق**، ص106.

[2]- اليحياوي، يحيى، "**في الاقتصاد الرمادي**"، من الرابط: www.elyahyauc.erg/savoirs.htm. تاريخ التصفح 2019/04/18

[3]- جعفر، "**حرب المعلومات بين الإرث الماضي وديناميكية المستقبل**"، مرجع سابق، ص94.

[4]- وليد غسان، سعيد جلعود، **مرجع سابق**، ص 96.

الفرع الثالث: أنماط الحرب السيبرانية

1- الحرب السيبرانية الباردة: فالحرب السيبرانية الباردة أو منخفضة الشدة يتم استخدامها في حالة الصراعات ذات الطبيعة الممتدة وطويلة الأجل وعميق الجذور بين الدول ولها جوانب مختلفة ثقافية أو اجتماعية أو اقتصادية. وفي العادة، يتم اللجوء إلى نوع من القوة الناعمة في هذا النمط من الحروب السيبرانية ولا تتطور على الأرجح إلى استخدام القوة المسلحة بالشكل المعروف، أو حتى بشن حروب إلكترونية على نطاق واسع. وكمثال على هذا النمط نجد الصراعات مثل "الصراع الهندي الباكستاني"، أو "الصراع بين الكوريتين الشمالية والجنوبية".

وتنشط هذا النمط أيضا، جماعات دولية للقرصنة للتعبير عن مواقف سياسية، أو حقوقية مثل "ويكيليكس"، و"أنونيموس" كما يستخدم في حالات الأزمات الدولية، كالتوتر الذي وقع بين إستونيا وروسيا في عام 2007 إلى جانب الإختراقات المتبادلة بين الصين والولايات المتحدة الأمريكية وروسيا، وكذا ما بين الولايات المتحدة وإيران. وتعتبر الإتهامات الموكلة لروسيا بالقرصنة الإلكترونية في الإنتخابات الرئاسية الأمريكية الأخيرة، لدعم المرشح الجمهوري "دونالد ترامب" على حساب "هيلاري كلينتون".

2- الحرب السيبرانية متوسطة الشدة: وهو يعبر عن تحول الصراع في الفضاء الإلكتروني إلى ساحة مشابهة للحروب التقليدية على الأرض، وقد يمهد لعمل عسكري حقيقي، ويتم فيه إختراق المواقع الإلكترونية، وتخريبها وشن حرب ضد الخصوم وغيره. ويستمد ذلك النوع من الحروب السيبرانية شدة من قوة أطرافه وارتباطها بعمل عسكري تقليدي، وتشير بعد التقديرات إلى أن تكلفة هذه الحروب قد تشكل من إنفاق نظيرتها التقليدية، بما يمكن من تمويل حملة حربية كاملة عبر الإنترنت بتكلفة. وقد تم اللجوء إلى هذا النمط من "الحروب السيبرانية" في هجمات حلف الناتو في عام 1995 على يوغسلافيا، حيث استهدفت الهجمات الإلكترونية تعطيل شبكات الاتصالات للخصوم.

3- الحروب السيبرانية "الساخنة": يعبر هذا النمط تحديدا عن الحروب في الفضاء الإلكتروني بشكل منفرد، ولا يرتبط بالجوانب أو العمليات العسكرية التقليدية، وهو نوع متقدم من الحروب، لم يسبق أن شهدها العالم، رغم بقاء احتمالية حدوثها قائما في المستقبل خصوصا مع تطور قدرات التكنولوجيا، واتساع الاعتماد بين الدول والكيانات والأفراد على الفضاء الإلكتروني.

وينطوي هذا النمط من الحروب على سيطرة البعد التكنولوجيا على إدارة العمليات الحربية، حيث يتم استخدام الأسلحة الإلكترونية فقط ضد منشآت العدو، وكذا اللجوء إلى الروبوتات الآلية في الحروب

والطائرات دون طيار، وإدارتها عن بعد بخلاف تطوير القدرات في مجال الدفاع والهجوم الإلكتروني، والإستحواذ على القدرة الإلكترونية[1].

المبحث الثالث: ضبط مفاهيم التهديد السيبراني

أصبحت التهديدات السيبرانية إحدى التحديات الرئيسية التي يتحتم على الدول مواجهتها خلال الفترة الحالية، ومع تزايد الإعتماد على الإنترنت خاصة في المجالات التي تتعلق بالأمن القومي مثل الشبكات العسكرية والبيانات المالية والمصرفية وتزايد الحديث عن أهمية مواجهة هذه التهديدات[2].

وفي هذا الإطار سيتم التعرض إلى ماهية التهديدات السيبرانية التي يمكن أن تتعرض لها الدول، وسيتم توضيح ذلك فيما يلي:

المطلب الأول: مفهوم التهديدات السيبرانية

سيتوجب التطرق إلى موضوع التهديدات السيبرانية توظيف بعض المفاهيم الأساسية التي لابد من التدقيق في استعمالها ومعرفة فحواها، ومن بين هذه المفاهيم مفهوم التهديد.

ومن أبرز التعريفات التي قدمت لهذا المصطلح نذكر ما يلي:

الفرع الأول: تعريف التهديد الأمني

اشتقت كلمة تهديد من الناحية اللغوية من لفظ "هدد" ويقصد به محاولة إلحاق الضرر والأذى بشيء معين قصد الإخلال بالأمن.[3]

ويرى "بيتري دبيل" أن التهديد "عمل نشط وفعال تقوم به دولة معينة للتأثير على سلوك دولة أخرى ويشترط نجاحه توفر عدة عوامل أبرزها الصداقة والجدية والقدرات التي تتناسب مع التهديد وهناك ثلاث سمات يشهد بها وهي درجة الخطورة ومدى احتمالية وقوع التهديد وعنصر الوقت".[4]

ويمكن الإشارة إلى أن التغيرات التي شهدتها البيئة العالمية ساهمت في بروز قواعد جديدة غير الدولة ترى من ذلك التغير من طبيعة التهديدات الأمنية ونزوحها من النمط التقليدي العسكري إلى نمط جديد كتعبير عن

---

[1]- حسام السبكي، "**الحروب السيبرانية المفهوم والأنماط وتداعياتها على الأمن الدولي**"،)الإمارات، جريدة رؤية للأخبار، العدد6(، 13 أوت 2018، دص.

[2]- محمد مختار، **مرجع سابق**، ص05.

[3] – عادل جارش، "**مقاربة معرفية حول التهديدات الأمنية الجديدة**"، مجلة العلوم السياسية والقانونية، من الرابط:
www.democraticar.de/p=43831:2019/03/22 تاريخ التصفح

[4]- **الموقع نفسه**.

زيادة التعقيد والتطور المستمر الذي يمس الظاهرة الأمنية خاصة مع التطورات الحاصلة من مجال التكنولوجيا والتقني والمعارفي. ومن أبرز هذه التهديدات السيبرانية التي أصبحت تشكل هاجسا أمنيا بالنسبة للدول التي تحركها الكثير من الأحيان قواعد أمنية غير تقليدية تحاول توفيق أهدافها المنشودة وتعبر عن مجرى جديد للبعد الأمني في العلاقات الدولية.

الفرع الثاني: تعريف التهديدات السيبرانية

عندما نواجه التهديدات السيبرانية فنحن هنا نجد أن هناك أوجه للتشابه إلى حين يبين الجيوش فطوال التاريخ قد اختلفت المعارك في نطاق التعقيد والإستراتيجية والتكتيكات، ولكن الشيء المشترك لكل هذه المعارك هو العدو الذي يسعى إلى الاستفادة من البنية التحتية وقدرات لشن هجوم آخر وهو نفس الشيء بالنسبة للتهديدات السيبرانية، هي قدرة العدو على الإستفادة من البنية التحتية لاستغلال نقاط الضعف كما هو الحال مع الجيوش في المعركة وكل عدو يوظف مختلف التكتيكات والتقنيات والإجراءات.

ويعرف قاموس " أوكسفورد" التهديدات السيبرانية على أنها "إمكانية محاولة إلحاق الضرر عن قصد وبنية سيئة أو تعطيل عمل شبكات الكمبيوتر أو النظام"[1].

ومن الناحية الاصطلاحية يمكن تقديم تعريف أكثر شمولا يرتبط بنقطة ضمان الحكومات بأنها: "أي ظرف أو حدث ينطوي على إمكانية التأثير سلبا على العمليات التنظيمية أو الأفراد من خلال نظام معلومات عن طريق الدخول غير المصرح به أو التدمير أو الكشف أو تعديل الحكومات والخدمات".[2]

وبالتالي فالتهديدات السيبرانية هي: "أي فعل ضار الذي يحاول الوصول إلى شبكات الحاسوب بدون ترخيص أو إذن من أصحابها".[3]

وتهدف هذه التهديدات إلى الإضرار بسمعة شركة أو شخص، وسرقة تصميمات المنهج وبراءات الاختراع والتأثير على البيانات الحكومية، كما تتسبب هذه التهديدات في تدمير البنى التحتية والاقتصاديات والتحكم في نظام الطاقة والشبكات وأنظمة التحكم الصناعية والبيانات الخاصة بالمدنيين. وفي معظم الحالات يتم استخدام العديد من هذه التهديدات لاستغلال نقاط الضعف في المؤسسات أو الشركات والوصول إلى الأصول فعلى سبيل المثال يمكن استخدام البرمجيات الخبيثة لسرقة بطاقات الإئتمان والبيانات الشخصية كما

[1]-**What is cyber threat how to explain cyber threat your CEO**, Date de visite 22/03/2019, www.threatcomment.com/bloghowtoexplainwahtisacyberthreat.

[2] -www.threatcomment.com Op cit, Date de visite 22/03/2019,

[3] -I bid.

يمكن استخدامها في حملات متعددة كما هو الحال في مجال التحايل وتتميز التهديدات السيبرانية بالسرعة وتحدث في وقت واحد وتتخذ أشكالا عديدة.

ويمكن أن يكون التهديد السيبراني غير مقصود ويمكن أن يكون متعمدا أو مستهدف أو غير مستهدف ويمكن أن يأتي من مصادر متنوعة بما في ذلك الدول التي تقوم بعمليات التجسس وحرب المعلومات والقرصنة وقد تنشأ من أفراد أو منظمات. وتشمل التهديدات المتعمدة، الهجمات المقصودة و غير مقصودة، الهجومات المقصودة عندما يقوم فرد أو مجموعة بمهاجمة نظام البنية التحتية، ويكون هجوم غير مقصود عندما يكون الهدف المقصود من الهجوم غير مؤكد.[1]

وانطلاقا مما سبق ذكره يمكن استخلاص النقاط التالية:

- أن التهديد السيبراني هي جهد محدد يهدف إلى إلحاق الضرر دون ضابط قانوني.
- قد تنشأ التهديدات السيبرانية في إطار داخليا وخارجيا وقد يكون سببها أفراد أو حتى منظمات.
- تعمل على إلحاق الأضرار والـــتأثير على السياسات الحكومية وتدمير البنى التحتية للدول.
- التهديدات السيبرانية تعمل على أشكال كثيرة ومتعددة.
- تتميز بسرعة التطور بإستمرار.

المطلب الثاني: مصادر التهديدات السيبرانية

هناك مجموعة متنوعة من مصادر التهديدات السيبرانية يمكن تلخيصها فيما يلي:

1- مشغلو شبكة بوتنيت: وهي شبكة تسيطر عليها أنظمة التحكم عن بعد لتنسيق الهجمات ولتوزيع مخططات التصيد الإحتيالي والرسائل غير مرغوب فيها والهجمات الخبيثة.

2- الشركات المنافسة: وهي التي تقوم باستهداف شركات أخرى حيث تسعى للحصول على معلومات حساسة لتحسين ميزاتها التنافسية في مجالات مختلفة.

3- الجماعات الإجرامية: تسعى الجماعات الإجرامية إلى مهاجمة الأنظمة لتحقيق مكاسب نقدية وعلى وجه التحديد تستخدم هذه الجماعات المنظمة الرسائل غير المرغوب فيها والتصيد الاحتيالي وبرامج التجسس، البرامج الضارة و الاحتيال عبر الإنترنت.

---

[1]– **مصادر التهديد السيبراني، الإرهابيون، والمجرمون، والحكومات المعادية، والساخطون الداخليون يشكلون تهديدات على أنظمة المعلومات، من الرابط:**

http://centcom.unipath-magazine.com

4- الدول: تستخدم أجهزة الاستخبارات لجمع المعلومات والتجسس، كما أن العديد من الدول تعمل بقوة على تطوير عقيدة حرب المعلومات والبرامج والقدرات، حيث تمكن هذه القدرات الدول من إحداث أثر كبير وخطير من خلال تعطيل الإصدادات والاتصالات والهياكل الأساسية والاقتصادية التي تدعم القوة العسكرية.

5- قرصنة إقتحام الشبكات: وتهدف هذه المجموعات إلى الإنتقام، مطاردة الآخرين، الربح النقدي، والحصول على المعلومات غير المصرح بها ويتطلب ذلك قدرا كبيرا من المهارة والمعرفة بالحواسيب ويمكن للقراصنة تحميل البرامج النصية للهجوم والبروتوكولات من الإنترنت وإطلاقها ضد مواقع الضحايا، في حين أصبحت أدوات الهجوم أكثر تطورا وأصبحت أيضا أسهل للإستخدام

6- برامج التجسس: حيث يقوم الأفراد أو المنظمات بتنفيذ الهجمات ضد المستخدمين من خلال إنتاج وتوزيع برامج التجسس والبرمجيات الخبيثة والعديد من الفيروسات المدمرة في الكمبيوتر بما في ذلك فيروس ميلس، دودة نيمدا، كود الأحمر، ودودة الناسف.

7- الجماعات الإرهابية: تسعى هذه الجماعات إلى تدمير البنى التحتية الحيوية أو تعطيلها أو استغلالها لتهديد الأمن القومي ويسبب خسائر جماعية وإضعاف اقتصاديات الدول، لكن رغم ذلك ترى وكالة المخابرات الأمريكية أن هذه الجماعات تشكل تهديدا سيبرانيا محدودا وستبقى ترتكز على الأساليب التقليدية للهجوم[1].

المطلب الثالث : أنواع التهديدات السيبرانية

تتنوع الممارسات التي تهدد الأمن السيبراني بتنوع الهدف وبإختلاف المصادر الممارسة له والتي سوف نتعرف على بعض أنواع هذه المخاطر والتي تعمل على الحاق الضرر في الجانب رالسيبراني تتوفر هناك جملة من طرق والامكانيات التي تتيحها تكنولوجيا الانترنات وتبرز هذه التهديدات في جملة من الهجمات التالية:

1- سرقة كلمات مرور المستخدمين للتسلسل في النظام: وفي ما يلي الطرق الرئيسية التي تستخدم في الحصول على معلومات اتصال المستخدمين الشرعيين للنفاذ الى النظام.

2- التخمين: كلمة المرور تكون واضحة جدا (كاسم المستعمل، تاريخ ميلاده، اسم زوجته...الخ) بحيث يكون حسابه غير محمي اساسا.

3- الخداع (الهندسة الاجتماعي) حيث يظهر المهاجم بمظهر المسؤول ثم يطلب كلمة المرور تحت أي ذريعة تقنية.

---

[1] – مصادر التهديد السيبراني، **الموقع السابق.**

4- الاستماع الى حركة المرور: حيث يتعرض المهاجم أو يستمع الى البيانات غير مرسلة الى الشبكة عبر بروتوكولات الاتصال (التلصص، الترصد).

5- البرمجيات: حيث يتم تسريب "حصان طروادة Trojan" الى محطة عمل المستعمل، حيث يقوم سرا بتسجيل المعلومات المستخدمة للارتباط بالنظم البعيدة؛

6- النفاذ الى مختلف تخزين كلمة المرور؛

7- السطو على كلمة المرور المرسلة بشكل مشفر، التجسس على المستخدمين عن طريق تنشيط طرفياتهم متعددة الوسائط لتسجيل معلومات اتصالهم.

8- الهجمات الطمسية: وتتمثل في استهداف صفحات الويب واستبدالها بصفحات أخرى، إذ يقوم المهاجم بخلق موقع شبكي مماثل للموقع الأصلي لاصطياد المشتركين واستدراجهم لمعرفة معلوماتهم أو بطاقات الإئتمان الخاصة بهم وغيرها.

9- الهجمات الخداعية : يتم من خلال استخدام بروتوكولات النقل والتحكم في اختراق أمن النظام أثناء عمل العميل والخادم، حيث يعمل البروتوكول أعلاه على تأمين وصلة ربط آمنة من أي عميلين من خلال أرقام المنافذ ومحددات الهوية المنظمة حيث يقوم المهاجم بتحصين أرقام المنافذ التي تخص تبادل البيانات وبالتالي يحل 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 طاقاتهم من خلال غمرها برسائل متعددة لمنع مرسل من إرسال بياناته.[1]

10- هجمات رفض اداء الخدمة: ينفذ هجوم رفض الخدمة عادة عن طريق تحميل النظام بما يفوق طاقته، ذلك أن الانظمة المستهدفة التي يتم غمرها بطلبات تزيد كثيرا عما تسمح طاقتها بمعاملته تنهار وتصبح غير متوافرة الخدمة. ويمكن إرتكاب هذه التهديدات عن طريق استغلال تصدعات موجودة في النظام الجاري تشغيله، وباستغلال جوانب معينة في النظام مثل ادارة الذاكرة (هجوم فيض الذاكرة) مما يتسبب في تعطيل التشغيل الأمر الذي يمكن أن يؤدي الى اقفال النظام).[2]

11- الهجمات على البنية التحتية الحرجة: إن مدى تعرض البنيات التحتية الاساسية لمجتمع ما (امدادات الكهرباء، المياه، النقل، لوجستيات الاغذية، الاتصالات، الرادوية والمالية، الصحة، الخ) يزداد بازدياد تجذر

---

[1]- أوس مجيد غالب العوادي، "**الأمن المعلوماتي السيبراني**"، (سلسلة أصدرت مركز البيان للدراسات والتخطيط ، أوت 2016، ص 18.

[2]- حمدون ، توريه، "**دليل الأمن السيبراني للبلدان النامية**"، الجزء الاول، (سويسرا: جنيف، 2006)، ص 59.

تكنولوجيات الانترنت وتصبح تلك البنيات نفاذة عن طريق "شبكة الشبكات" وثمة حاجة إلى التشديد على تعرض توليد الطاقة الكهربائية ونظم التوزيع الضرورية لتشغيل الجزء الأكبر من البنية التحتية القومية ذات الأهمية الحيوية . أن تعقد واتساع نطاق العلاقات بين مختلف البنيات التحتية الحرجة جزء من قوتها ، وفي نفس الوقت مصدر من مصادر تعرضها للأخطار .[1]

المبحث الرابع: الأمن السيبراني ووسائل الفتك

يعني الأمن السيبراني عمل كل الوسائل اللازمة لحماية الفضاء السيبراني ، وتعني وسائل الفتك تلك التقنيات المستخدمة في الهجمات السيبرانية والتي لها عدة أشكال يمكن توضيحها وفقا لما يلي:

المطلب الأول: وسائل التهديد الأمن السيبراني للدول

وتشمل الفيروسات الأسلحة الأساسية في الحرب، حيث تؤدي إلى تعطيل عمل الشبكات الإلكترونية، والخوادم الرئيسية أو تؤدي إلى استخدامها لإرسال مختلف المعلومات، من الأماكن التي تغزوها ويمكن نشر الفيروسات عبر الرسائل الإلكترونية أو نقل الملفات الإلكترونية، أو تحميلها على أداة لحفظ البيانات. ويشار هنا إلى أن فيروس Stuxnet الذي ضرب المفاعل النووي الإيراني، قد تم عبر استخدام هذه الطريقة الأخيرة لاسيما وأن، هذا المفاعل غير موصول بالشبكة العنكبوتية العالمية. ولا تقتصر هذه الوسائل مستخدم على الفيروسات والبرامج المعادية، فهي تشمل أيضا التشويش المادي المباشر، المتعلق بموجات البث السلكي اللاسلكي وشبكات الطاقة[2].

1- التجسس المعلوماتي : تمثل وسائل التجسس التقني والمعلوماتي أحد أشهر الوسائل وأسلحة الحرب السيبرانية، والتي تهدد الدول تم استخدام هذا السلاح منذ بداية الاستعمال الإنساني لوسائل الاتصال والتواصل.[3]

تتخذ وسائل التجسس المعلوماتي عدة أشكال، منها ما يتم عبر التجسس والتصنت على المعلومات الصادرة من أجهزة الحواسيب أو الصادرة عن الأقمار الصناعية، والهواتف المحمولة، وغيرها من وسائل التجسس المعلوماتي ذات الطابع القديم أو الحديث.[4]

[1] المرجع نفسه، ص 61.

[2]- مني أشقر جبور، "**السيبيرانية هاجس العصر**"، (دش، دس)، ص70.

[3] - جفعر، **مرجع سابق**، ص171.

[4]- **المرجع نفسه**.

2- الإختراق الإلكتروني: وهي عبارة عن إنشاء نظام أو برنامج إلكتروني يهدف إلى استغلال معلومات الخصم وتدميرها، إضافة إلى فساد نظامه الحاسوبي والآلي، وذلك بهدف التقدم عليه أمنيا وعسكريا واقتصاديا وسياسيا، وقد تكون هذه المواجهة على المستوى الفردي، أو المؤسساتي، أو على مستوى الدول[1].

3- زرع الفيروسات التقنية في البيئات المعلوماتية: وهي عبارة عن برامج إلكترونية مدمرة، تعمل ضمن آلية معينة يحددها صانع هذه البرامج، ولها أشكال وأنواع متعددة، تهدف هذه الفيروسات الإلكترونية إلى إحداث فوضى في نظام تشغيل الضحية المنوي ضربه إلكترونيا، وتلويث بيئته المعلوماتية، وذلك بغية تعطيل الوصول المعلوماتي للضحية، وفقدانه لغالبية مخزونه الرقمي، وربما ضرب الأجزاء المادية من أنظمة التشغيل الخاصة به[2].

4- القرصنة الإلكترونية: من أضخم وأكثر الأسلحة ووسائل التهديد عبر الفضاء الرقمي، يشتمل هذا السلاح التقني على غالبية وسائل الصراع الإلكتروني في يومنا هذا، وذلك لشمولية مفهومه و مضمونه، حيث تقوم آلية عمله على تجنيد العديد من الأشخاص المؤهلين والقادرين على التعامل مع الحاسوب بخبرة ودراية عالية جدا، تمكنهم من اقتحام مختلف وسائل الاتصالية، والنظام التكنولوجي من حواسيب وهواتف وموجات وآليات ضوئية وغيرها، كما يطلق على هؤلاء الأشخاص المؤهلين للعمل الحاسوبي والإلكتروني في عالم البرمجيات والإلكترونيات اسم الهاكرز.[3]

5- الرسائل الصامتة: عبارة عن برمجة تقنية مخصصة للهواتف المحمولة من فئة الجيل الثالث. وهي رسائل يتم برمجيتها بشكل لا يشعر حامل الهاتف أو المحمول بوصولها، بحيث تساعد مرسلها على التحديد الدقيق لمكان تواجد الشخص، وذلك عبر استخدام معادلة تقوم بإحتساب قوة إشارة الموجات المنبعثة من الجهاز المحمول تبعا لأقرب ثلاث مراكز مستقبلية لهذه الموجات.[4]

6- شبكات التواصل الاجتماعي: وهي تركيبات اجتماعية تقنية ذات محتوى رقمي، تقوم بربط الحلقات الاجتماعية ببعضها البعض، كالعمل والدين وغيرها، والتي تضم في طياتها مختلف الفئات العمرية، وجميع المستويات الاجتماعية والاقتصادية، وكافة الدرجات الثقافية، والتعليمية، استخدم أدولف هتلر الزعيم النازي

---

[1]- الشهري، نوال، "**حرب المعلومات**"، في مركز تميز الأمن المعلوماتي، (جامعة الملك سعود)، دن، من الرابط: www.coeia.edu.sa/index.php/ar/assur_awess/data_privacy/1263_influance_warfare.html تاريخ التصفح 2019/03/16

[2]- حسين فاروق، "**فيروسات الحساب الآلي**"، (القاهرة: العربية للطباعة والنشر، ط1، 1999)، ص7.

[3]- غسان، جلعود، **مرجع سابق**، ص111.

[4]- الرسائل الصامتة، "**سلاح الرقابة السرية**"، 23 يونيو/ حزيران 2016م، من الرابط: www.almaged.ps/3 ،2019/03/17 تاريخ التصفح

البث التلفزي إبان الحرب العالمية الثانية لنشر خطاباته، وتحميس جنوده والجماهير، وهي نفسها التي ركز عليها الحميني إبان الثورة الإسلامية في إيران، وهي نفس المشهد الذي ألقي بظلاله اليوم على الصراع التقني المناسب عبر الفضاء الإلكتروني العالمي، ولكن بسلاح جديد وهو شبكات التواصل الاجتماعي.[1]

7- الأقمار الصناعية: وهي أسلحة ذات دلالات استحواذية، هدفها السيطرة على أكبر قدر ممكن من المعلومات وذلك عبر إلتقاط ملايين الصور للهدف، وإرسالها للقاعدة المعلوماتية الموجودة على الأرض. تعتبر الأقمار الصناعية من أكفئ الوسائل التقنية، وأكثرها تعقيدا في حسم المعارك، فهي قادرة على توجيه الصواريخ والقاذفات النارية صوب أهدافها على الأرض، وقد بلغت ذروة استخدامها إبان الحرب الباردة والتي هددت العالم بإندلاع حرب كونية ثالثة، وتستخدم اليوم في التشويش على المحطات الفضائية ومنها البث، وذلك بأجندة وأهداف سياسية، في تعبير جديد عن الحرب السيبرانية الدائرة في العالم الإفتراضي، كالتشويش الذي تعرضت له بعض القنوات الفضائية العربية (العربية، الجزيرة) خلال الثورات العربية.[2]

8- الحقيبة الكهروستاتيكية: أحد أنواع التكنولوجيا العسكرية وهي عبارة عن أجهزة صناعية على شكل حقائب صغيرة، تقوم بتوليد نبضات كهرومغناطيسية فائقة القدرة، يمكن من خلالها تدمير الوحدات الإلكترونية في أية إدارة أو محطة إرسال. مما يفقدها قدرتها العلمية والإنتاجية والتشغيلية، هناك أبحاث جارية على هذه الحقيبة وذلك بهدف تطوير نواتها الخاصة، والتي تسمى ميكروبات إلكترونية، بحيث يتم تصويبها ضد التقنيات السيليكونية، بغية تدمر المعدات الإلكترونية الخاصة بها.[3]

9- الخداع الإلكتروني: وهو من أهم وسائل تأمين الصراعات الإلكترونية وبه تحقق المعارك الإلكترونية عنصر المفاجأة. يشتمل هذا السلاح الرقمي على عدة وسائل أهمها: التقليد الصوتي، التشويش الإلكتروني، التضليل المعلوماتي، الخداع ونشر الشائعات، انتحال الشخصيات افتراضيا، الإبتزاز الإلكتروني، وغيرها من أساليب الخداع الرقمي.[4]

---

[1]- غسان، جلعود، **مرجع سابق**، ص113.

[2]- شبكة النبأ المعلوماتية، **"حرب الفضاء والأقمار الصناعية"**، من رالرابط:

www.annaba.org/nbanes/69/022/htm2019/03/19 تاريخ التصفح

[3]- إسماعيل كاخيل، **"الحرب الإلكترونية"**، موقع مجلة الدفاع العربي، من الرابط:

www.arahdefancejournal.com/article560.htm 2019/03/18 تاريخ التصفح ،

[4]- غسان، جلعود، **مرجع سابق**، ص115.

10- قنابل التعتيم الميكروويفية: يصوب هذا النوع من الأسلحة الإلكترونية نحو مولدات الطاقة، كالمزودات الكهربائية، والرادارات، ومحطات التزويد بخدمات الإنترنت، ومراكز الاتصالات، والشبكات السلكية واللاسلكية، ومحطات البث الخلوي، وغيرها من وسائل تزويد الطاقة والمعلومات، يقوم مبدأ عمل هذه القنابل على إطلاق نبضات من الطاقة المغناطيسية قصيرة الموجة، والتي تعمل على قطع كافة مصادر الطاقة والمعلومات في الكيان المستهدف، مما يؤدي إلى فصله عن العالم الخارجي.

11- الأسلحة النانو تكنولوجية: يعد هذا المجال العلمي من أكثر المجالات إثارة، وأوعدها صعودا، فهو يتم بتصميم أجهزة تقنية في غاية الدقة والصغر، وذلك من خلال رصد الذرة بجوار الذرة للحصول على الشكل أو التكنولوجيا المطلوبة، تسلط هذه التكنولوجيات العسكرية على الأجزاء المادية للأجهزة الحاسوبية والتقنية بحيث تنتشر داخلها، لتتسلل إلى أنظمة التشغيل، وتفرغ ما بحوزتها من أنظمة تدميرية قادرة على هدم البناء المعلوماتي للنظام بسرعة فائقة، في صورة تشبه آلية عمل الفيروسات لهذا، والتي تخصص لمهاجمة الأجزاء المادية للنظام المعلوماتي، ومنها ما يسمى بالميكروبات الرقمية، والتي تحدد لمهاجمة النظام التشغيلي لبيئة المعلومات المنوي استهدافها.[1]

12- الطائرات الإلكترونية (دون طيار): دخلت هذه الطائرات الحرب الإلكترونية لتشكل فوارق عديدة في قدرات الجيوش ومدى امتلاكها للمنظمات المعلوماتية، والتي وبالتالي سهولة اقتحامه والسيطرة عليه بشكل كامل، أحدثت مثل هذه الأسلحة الجامعة بين مبادئ العمل الحربي والمعلوماتي صيحات إنسانية وحقوقية عديدة في العالم كونها تحوي العديد من التأثيرات السلبية على جسم الإنسان، ناتجة عن الموجات التي تطلقها، والأصوات المزعجة الصادرة عنها[2].

المطلب الثاني: نماذج التهديدات السيبرانية

إن الأحداث الدولية الاخيرة ساهمت بشكل أو بآخر في رفع وعي الباحثين والدراسين وكذا صناع القرار بشان التهديدات السيبرانية التي تطورت وسائلها وممارسيها وشمل جملة من مجالات الحياة. أبرز هذه الحالات فيما يلي:

- أستونيا أبريل 2007 : بدأت سلسلة من الهجمات التي يطلق عليها DDOS TTACKS ضد المواقع التي تديرها الحكومة الاستونية، وتسبب الهجوم في عرقلة ولوج المواطنين الى بعض المواقع مثل موقع

[1]- جعفر، "**حرب المعلومات بين إرث الماضي وديناميكية المستقبل**"، **مرجع سابق**، ص128.

[2]- غسان، جلعود، **مرجع سابق**، ص117.

الحزب السياسي الذي ينتمي اليه رئيس الوزراء. واستخدام الروابط التي ترعاها الحكومة في تضليل المستخدمين واعادة توجيههم الى صور للجنود السوفيين.

- كوريا الجنوبية والولايات المتحدة يوليو 2009: تم استهداف مواقع البيت الابيض، ووكالة الامن القومي والإدارة الاتحادية للطيران Administration Federal Aviation وزارة الخارجية ، والخدمة السرية Secret Service، والخزانة ، ولجنة التجارة الاتحادية Federal Trade Commission ، فضلا عن جهاز المخابرات الوطني في كوريا الجنوبية.

- وكذلك الهجوم على شركة سوني بيكتشرز الامريكية في عام 2014 ، بسبب فيلم من انتاج هوليود عن زعيم كوريا الشمالية كيم يونغ اون . واستخدام فيروس " ستكسنت" – سابقا – لمهاجمة برنامج ايران النووي في نوفمبر 2007، ويعتقد أنه من تطوير الولايات المتحدة واسرائيل، وقد تم اكتشافه في عام 2010.[1]

- وفي يوليو 2011 أعلنت نائب وزير الدفاع ويليام لين أن اكثر من 24 الف ملف من ملفات وزارة الدفاع قد سرق، قبل ذلك ببضعة اشهر تم اختراق احدى المختبرات العلمية الرئيسية التابعة لحكومة الولايات المتحدة، و لم تعلن الحكومة الامريكية عن هوية مرتكبي الهجوم

- وفي عام 2012، تم تدمير 35 الف جهاز كمبيوتر في شركة النفط السعودية "ارامكو"، لتخريب صادرات النفط والقت المخابرات الامريكية اللوم على ايران، وفي عام 2016، هاجم القراصنة احدى الوكالات الحكومية السعودية، بالاضافة الى منظمات في قطاعات الطاقة والصناعة والنقل، والهيئة العامة للطيران المدني التي تنظم الطيران السعودي.

- وشهدت عام 2016، التسلل الروسي إلى خوادم البريد الالكتروني للجنة الوطنية الديمقراطة، كما تم اختراق البريد الالكتروني الخاص بجون بوديستا رئيس الحملة الانتخابية الرئاسية لهيلارى كلينتون، وقام الوسطاء بتسريب رسائل الكترونية الى موقع Wikileaks وعلى إثرها قامت الولايات المتحدة الأمريكية بطرد 35 دبلوماسيا روسيا.[2]

[1]- العربية سكاي نيوز، "**اسكسنت فيروس ضد إيران**"، فبراير 2013، من الرابط:

www.Synewsarabia.com/web/article/114276/%d8%b3%d8%%d9%.2019/3/21 تاريخ التصفح

[2]- العربية سكاي نيوز، "**تفاصيل الهجوم ....قراصنة يدمرون كومبيوترات في وكالة الطيران السعودي.. ويستبدلون البيانات بصورة الطفل السوري الان كريد**"، من الرابط:

www.Skynewsarabia.Comweb/article/114276/d. تاريخ التصفح 2019/03/21

ويمكن القول في ضوء تلك الحالات أنه رغم اختلاف غرض وهدف كل حالة من الحالات السابقة، إلا أنه من الواضح ان حجم الهجمات السيبرانية يتزايد بشكل حاد وكبير، ولذا يصعب تحديد حجمها الحقيقي وبخاصة أن عديد منها لا يتم التبليغ عنه. وتتمثل القواسم المشتركة بين تلك الحالات في صعوبة تحديد مرتكبي تلك الهجمات على وجه الدقة، وغياب الرد المضاد، كنتيجة لها. والاهم أنها ليست حكرا على الدول المتقدمة ذات الانظمة المعلوماتية الهائلة والمتطورة فحسب بل قد تمس أيضا الدول المتخلفة.

خلاصة واستنتاجات

إن الأمن السيبراني يشكل تهديدا خطير على امن الدول، لذلك وجب علينا أن نتطرق إلى دراسة مفصلة حول المفاهيم المتعلقة به وأشكاله وكيف يتحول إلى تهديد للدول، ومن خلال المباحث الأربعة السابقة نصل إلى الاستنتاجات التالية:

– إن الأمن السيبراني مصطلح حديث نسبيا، فقد بدا يظهر وينظر له إلا مع فترة التطور التكنولوجي والثورة الرقمية أين أصبح العالم كقرية صغيرة.

– للأمن السيبراني العديد من الأشكال التي تتعرض له الدول من بينها القرصنة الالكترونية أين يستطيعون اختراق جميع الأنظمة غير المؤمنة وتهديدها للدول، كما أصبح هذا يعرف بالإرهاب الالكتروني.

– لقد أصبحت الدول تتعرض لتهديدات جديد دون دخول حدودها، فأصبح المقرصن يتجسس على الدولة ويسرق جميع معلوماتها وأموالها دون التحرك من مكانه، لذلك فهو من اخطر التهديدات الحديثة على امن الدول.

الفصل الثاني:

الأمن السبراني الجزائري

دراسة تحليلية

إن العقيدة الأمنية للدولة يقصد بها مجموعة الآراء والاعتقادات والمبادئ التي تشكل نظاما فكريا لمسألة الأمن في الدولة، وتتبنى الدول هذه العقيدة عندما يتعلق الأمر بتعاطيها مع التحديات والقضايا التي تواجهها وتواجه الجزائر تهديدا بالغ التطور والصعوبة والمتمثل التهديدات السيبرانية، فالجزائر تحاول دائما أن تطور أنواع دفاعاتها ومواجهته هذه التحديات بإعادة صياغة قوانين تتماشى مع الواقع والتطور الحاصل.

وسوف نفصل في هذا الفصل هذه العقيدة الجزائرية وكيف أنها تحاول التطور مع التطورات التكنولوجية الحاصلة، بالإضافة إلى معرف هل الجزائر تمتلك منظومة سيبرانية للدفاع عن نفسها ضد التهديدات التي تتعرض لها.

وسيتم التطرق إلى المباحث التالية:

- ❖ المبحث الأول: السياسة الأمنية الجزائرية بين العقيدة الأمنية والتطورات التكنولوجية؛
- ❖ المبحث الثاني: الأمن السيبراني الجزائري؛
- ❖ المبحث الثالث: أبرز التهديدات السيبرانية التي تواجه الأمن الجزائري.

المبحث الأول: السياسة الأمنية الجزائرية بين العقيدة الأمنية والتطورات التكنولوجية

تكتسي العقيدة الأمنية أهميتها من اعتبارها دليلا موجها انطلاقا من المصالح الجيو سياسية للدولة، وذلك من خلال تحديد الأوليات والتحديات البارزة والكامنة التي تواجه أمنها في ظل ما يشهده العالم من تطور الكرتوني وظهور أنواع جديدة من التهديد، أصبح لازما دراستها والتصدي لها،وهو ما سيتم توضيحه في الآتي:

المطلب الأول: العقيدة الأمنية الجزائرية

إن العقيدة الأمنية للدولة يقصد بها مجموعة الآراء والاعتقادات والمبادئ التي تشكل نظاما فكريا لمسألة الأمن في الدولة، وتتبنى الدول هذه العقيدة عندما يتعلق الأمر بتعاطيها مع التحديات والقضايا التي تواجهها، كما تمنحها هذه العقيدة إمكانية تفسير مجمل الأحداث ذات الطابع الأمن، فالعقيدة الأمنية تمثل تصورا أمنيا يحدد المنهجية التي تقارب بها الدولة أمنها، كما يحدد كذلك أفضل السبل لتحقيقه، وعليه عادة ما تكون مرجعية هذه العقيدة عبارة عن أطروحات نظرية تتبناها الدولة وصناع القرار فيها كما يمكن أن تأخذ صيغة إيديولوجية إذ وصلت حد النظام الفكري المتجانس والمتناغم الذي يوفر تفسيرات معينة للواقع، ويترتب على ذلك تبني القوى النافذة في المجال الأمني لهذه التفسيرات والرؤى.[1]

العقيدة الأمنية: هي مجموعة القواعد والمبادئ والنظم العقائدية المنظمة والمرتبطة، التي توجه سلوك الدولة الأمني (تعاوني/ غير تعاوني) وقرارا تاما على المستوى المعلي والدولي، وتعمل على كيفية استخدام القادة للقوة (العسكرية، الاقتصادية، السياسية...) من أجل الوصول للأهداف الإستراتيجية للدولة.

وبالرجوع إلى العقيدة الأمنية الجزائرية يمكن القول أن هناك تعدد وتنوع في المرتكزات والعوامل التي ساهمت في تحديد طبيعة العقيدة الأمنية الجزائرية منذ الأيام الأولى لإستقلال الجزائر فجملة التهديدات والمخاطر قد لعبت دور كبير في تحديد طبيعة هذه العقيدة، وأدت إلى اعتماد على مفهوم الأمن بشقيه الصلب واللين.[2]

---

[1]- صالح زياني، "**مرتكزات عقيدة الأمن القومي الجزائري بين الثبات والتحول**"، (محاضرة مقدمة لطلبة جامعة باتنة، كلية الحقوق والعلوم السياسية، د.س)، ص3.

[2]- عبد النور بن عنتر، "**عقيدة الجزائر الأمنية: ضغوطات البيئة الإقليمية ومقتضيات المصالح الأمنية**"، **من الرابط:**

http://studies.aljazeera.net/ar/reports/2018/05/180502110656159.html.2019-05-24 تاريخ التصفح: 24-05-2019

وبهدف توضيح أهم المرتكزات التي تقوم عليها العقيدة الأمنية الجزائرية، سوف نحاول أن نذكرها في النقاط التالية:

- احترام سيادة الدول وعدم التدخل في شؤونها الداخلية كمبدأ أساسي.
- الحل السلمي للنزاعات الدولية والإقليمية بالطرق المباشرة وغير المباشرة بين الأطراف المتنازعة.
- التركيز على مفهوم الأمن بشقيه (الصلب، اللين) للحفاظ على السلم والاستقرار وفض النزاعات.

ينطلق مبدأ عدم التدخل في الشؤون الداخلية من العامل التاريخي حيث تعتبر الجزائر من بين الدول التي كافحت من أجل نيل استقلالها، فبعد نهاية الثورة اتبع القادة السياسيين سياسة الاعتماد على نفس المبدأ في بناء دولة الجزائر الحديثة ورسم سياستها المستقبلية، لذلك تم اتخاذه كمبدأ يصون ويدافع عن سيادة الدولة خاصة في الساحة الإقليمية التي تتواجد بها وعدم التدخل في شؤونها سواء على الصعيدين السياسي والعسكري، وهو ما يفسر عدم إبرامها لأي معاهدات أو اتفاقيات دفاعية مع القوى الأجنبية لأنها لا تتناسب مع الخطاب الرسمي والتوجهات السياسية لاستقلالية للبلاد.[1]

كما كان للدبلوماسية الجزائرية دور الوساطة في العديد من النزاعات والأزمات كالأزمة الإيرانية الأمريكية بسبب حادثة الرهائن، وكذا دورها في النزاع العراقي الإيراني واستطاعت إنهاء النزاع الإثيوبي الإريثيري فضلا عن إحكامها للقوانين والمواثيق الدولية والإقليمية كمنظمة الوحدة الإفريقية وحركة عدم الإنحياز ومنظمة المؤتمر الإسلامي والأمم المتحدة وبعد التحولات الجديدة عملت جاهدة لإبراز دور الإتحاد الإفريقي في صيانة وحفظ أمن إفريقيا وفض النزاعات فيها من مبدأ إفريقيا للإفريقيين.

وبعد ظهور التهديدات الجديدة المصاحبة للتحولات التي مست البيئة الإقليمية وجدت الجزائر نفسها أمام ساحل أزماتي، تتبع كل دولة تحت وطئة أزمة الفقر والنزاعات، لتجد نفسها مرة أخرى مجبرة على لعب دورها ومكانتها الريادية، حيث سعت من أجل تلك الأزمات وكذا بذلت جهود حثيثة لجمع الفرقاء الليبيين من مبدأ حسب الجوار لإيجاد حل ينهى حالة الفوضى والإنقسام الذي تعاني منه دولة ليبيا.

كما تقوم العقيدة الأمنية الجزائرية على مفهوم الأمن الشامل بحيث ترتكز على المفهوم التقليدي الصلب، بل تتبنى مقاربة تنموية في إطار مفهوم الأمن اللين بجوانبه الاجتماعية والاقتصادية والبيئية وغيرها من الجوانب التي تؤثر في أمن الدول والجماعات. ويعود التركيز على مقاربة الأمن الصلب لدى صناع القرار

[1]- عبد النور بن عنتر، "**البعد المتوسطي للأمن الجزائري: الجزائر، أوربا، الحلف الأطلسي**"، (الجزائر: مكتبة العصر للطبع والنشر والتوزيع، 2005)، ص120.

الجزائري إلى فترة حرب التحرير خاصة جيش التحرير الوطني حرب شرسة طويلة المدى لنيل الاستقلال، بعد انضمام الجزائر إلى مجموع الدول المستقلة ظهرت العديد من المخاطر التي بإمكانها تهديد الأمن الوطني ورقعته الجغرافية لترسم حرب الرمال مع الجار المغرب صفحة جديدة من التهديد التقليدي لا يمكن تجاهله، حيث أصبح عامل موجه للعقيدة الأمنية في شقها العسكري.[1]

مع بروز التهديدات الجديدة المتتابعة من الساحل الإفريقي حتم على الجزائر مواصلة سياسة التسلح النوعية لمواجهة تلك التهديدات على رأسها مكافحة الإرهاب والجريمة المنظمة، حيث ركزت على ضرورة امتلاك آليات وأجهزة للرصد بتأمين الحدود والاستطلاع، لإختراق الجماعات الإرهابية والعصابات المنظمة وإبطال مفعولها وتهديداتها الأمن الوطني وحدوده.

أما المقاربة التنموية التي تندرج في إطار الأمن الشامل فقد حاولت الجزائر تمرير رؤيتها على أن المشاكل التي تعاني منها إفريقيا من نتاج لسياسات الاستعمار ونهب الثروات التي تعرضت لها أثناء الحقبة الاستعمارية، كما أكدت في العديد من المرات أن محاولة القضاء على ظاهرة الإرهاب والجريمة المنظمة في منطقة الساحل وإفريقيا لا يكون بالترسانة العسكرية، بل عن طريق معالجة الخلل البنيوي التي تعانيه معظم الأنظمة الإفريقية، فقامت الجزائر بإيجاد الحل في هذا الجانب وهو إقامة سياسات تنموية كالشركة الجديدة لتنمية إفريقيا ويعد الرئيس السابق عبد العزيز بوتفليقة أحد أبرز زعمائها وهي مبادرة جادة لإيجاد حلول لمشاكل الساحل الإفريقي على العموم.

كما كانت الجزائر طرفا في البرامج التنموية التي تبنتها المنظمات الدولية والإقليمية الموجهة للدول الإفريقية. على منها دول الجوار. كما تحافظ على تقديم مساعدات سنوية للعديد من الدول الإفريقية على رأسها مالي والنيجر. من أجل إقامة مشاريع تنموية في المناطق التي تتواجد بها وذلك تخاوف من زعزعة أمن الجزائر من طرف الطوارق فعملت على المشروع التنموي.[2]

ولعبت الجغرافيا دورا كبير في توجيه العقيدة الأمنية الجزائرية إذ تعد هذه الأخير بدورها كاملا محددا لهذا الأمن. فموقع الجزائر في نقطة تقاطع إستراتيجية مهمة بتوسطها لعدة دول مغاربية، وكذلك توسطها لكيانين ضخمين الأول في الشمال يمثله الإتحاد الأوروبي والثاني في الجنوب ويمثله في العمق الإفريقي، إن هذا

---

[1]– بورعة على جهاد، "**الجزائر بين توجه إستراتيجي وعقيدة أمنية**"، من الرابط:

تاريخ التصفح www.maspolitiques.com/mas/index.phpcontent=article8id=123.2019/04/26

[2]– مليكة خ، "**الإستراتيجية الأمنية للجزائر تعزيز المقاربة التنموية**"، موقع جريدة المساء ، من الرابط:

تاريخ التصفح www.el-massa.com/dz.2019/04/27 ،

الموقع أو بعبارة أخرى هذه النقطة الإستراتيجية أمنيا جعلت الأمن الجزائري ينكشف الأمني، إن مستويات تأثير عامل الجغرافيا على طبيعة العقيدة الأمنية للجزائر متنوعة. فإن غاية انتهاء الحرب الباردة مثلت قضايا دعم حركات التحرر في العالم والدفاع عن مكانة الجزائر كقوة إقليمية أحد أهم عناصر هذه العقيدة.

أما في ظل التحولات التي أعقبت نهاية الحرب الباردة وعلى رأسها الإنكشافات الأمنية للجزائر، وازدياد عملية الإعتماد المتبادل والترابط والتشابك على العديد من الأصعدة، اتجهت هذه العقيدة للإرتكاز على عناصر جديدة وعلى رأسها قضايا تتعلق بمحاربة الإرهاب وتجارة المخدرات وأمن الدولة، أي الإنتقال من البعد الخارجي كمحدد لهذه العقيدة إلى البعد الداخلي الذي أثر بشكل واضح في صياغتها.[1]

أما الجانب الإيديولوجي فقد ظل بثقله أحد مرتكزات العقيدة الأمنية للجزائر منذ الأيام الأولى للاستقلال، فقد مثلت الاشتراكية بمبادئها المضادة للاستقلال والاستعمار، مصدرا ذا قيمة لهذه العقيدة الأمنية وذلك لعدة عقود.[2]

كما كان لخيار الحزب الواحد، إقتداء بعد تجارب أخذت بها العديد من الدول، دوره في بلورة هذه العقيدة. إنه وبحسب الإديولوجيا تم النظر إلى جبهة التحرير الوطني على أنها وعاء لتحقيق الوحدة الوطنية بعد الإنشقاقات الأولى التي عرفتها الجزائر عقب حصولها على الاستقلال، وعليه أكدت المواثيق الوطنية لسنوات 1964و 1976 و 1986 على أن الاشتراكية كنظام وإيديولوجيا هي المنهج الوحيد الكفيل بتحقيق الاستقلال التام والقضاء على الاستغلال.

لقد رسمت الأيديولوجية الاشتراكية مبادئ وأهداف العقيدة الأمنية الجزائرية لفترة تقارب ثلاثة عقود منذ الاستقلال، ولعل من أبرز تلك الأهداف مناصرة حركات التحرر في العالم. ونصرة القضية الفلسطينية...إلخ، والعمل على المحافظة على مكانة الجزائر كقوة إقليمية، وكذلك الإستعانة بالمؤسسة العسكرية، أو الجيش الوطني الشعبي في مجهودات التنمية الوطنية.

وأثرت التحولات العالمية وحتى الداخلية للجزائر مع نهاية الثمانينات على التوجهات الإيديولوجية التي ضلت مصدرا للعقيدة الأمنية للجزائر لعدة عقود، فأحداث 05 أكتوبر 1988 التي شهدتها البلاد، وضعت أمنها القومي أمام محك صعب ويحكم ذلك الإنفجار مع تحولات هامة على المستوى الدولي كانهيار المعسكر

---

[1] – هربرت بوبون، "**نطاق التهدي الغير العسكري في: التسللح ونزع السلاح الأمني الدولي، (مجموعة من المؤلفين)**"، تر: فادي محمود وآخرون، (بيروت: مركز دراسات الوحدة العربية، 2004)، ص ص 120-124.

[2] – الطاهر حرف الله، "**النخبة الحاكمة في الجزائر 19*62-1982، بين التصور الإيديولوجي والممارسات السياسية**"، ج1، (الجزائر: دار هومة، 2007)، ص 105.

الشرقي وأفول إيديولوجية، لتحل محل الإيديولوجية اللبرالية، فإن ذلك انعكس بشكل واضح على طبيعة الإيديولوجية التي ظلت مصدر إلهام للعقيدة الأمنية للجزائر منذ الاستقلال.

فمن أجل الحفاظ على أمنها ورغبة منها لمباشرة العديد من الإصلاحات سواء كانت سياسية أو اقتصادية وحتى على مستوى الإحتراف داخل المؤسسة العسكرية، حدث تحولا هاما في هذه العقيدة لتتلاءم وعملية التحول المرن نحو الديمقراطية، وتزامنت عملية إعادة صياغة بعض المبادئ التي تقوم عليها العقيدة الأمنية للجزائر لتواكب السياسة الجديدة، وكذا الأزمات السياسية اقتصادية حادة. تهديدا حقيقيا للأمن القومي الجزائري، وهو ما استلزم بلورة عقيدة أمنية تؤخذ في الحسبان كلا من جانبي الأمن الصلب والناعم وللتعاطي مع هذه الظاهرة المعقدة (كلا ظاهرة الإرهاب، الجريمة المنظمة وتجارة واستهلاك المخدرات) ساهمت كلها في إعادة تشكيل هذه العقيدة الأمنية.

وبذلك يمكن القول أن العوامل والمرتكزات التي ساهمت في تحديد طبيعة العقيدة الأمنية للجزائر كانت متنوعة وكل عامل كان له تأثير معين من جانب من الجوانب اهتماماتها الأمنية، فالبرغم من تنوع العوامل المؤثرة والمحركة للعقيدة الأمنية للجزائر، فإن المبادئ الكبرى لهذه العقيدة لم تتغير بل يتم في كل مرة تكيف هذه المبادئ لتتماشى مع التحولات الداخلية والدولية لتبقي النخب الحاكمة تراهن على:

- عدم التدخل في الشؤون الداخلية للدول واحترام سيادتها
- دعم الحل السلمي للنزاعات الدولية وتجنب الحل العسكري
- وأخيرا الاعتماد على مقارنة الأمن بشقيه (الصلب واللين) في حل النزاعات وإرساء السلم.

فإستعانة بجانب العسكري لتأمين حدود البلاد جغرافيا يعد من الضروريات القصوى، كما أن للمشاريع التنموية في مختلف الجوانب داخليا أو خارجيا تعمل على الحد من ظاهرة الإرهاب والتطرف والانخراط في الجريمة المنظمة وبالتالي الحد من النزاعات الداخلية والدولية وفي المجال الإقليمي للأمن الوطني الجزائري.[1]

المطلب الثاني: الاهتمامات الأمنية للجزائر

يعتبر الموقع الجغرافي لأي دولة من المحددات الأساسية في صياغة سياستها الخارجية، وهذا ما تعكسه الدراسات في الجغرافية السياسية، حيث تهدف هذه الأخيرة إلى إبراز القيمة الفعلية للموقع الجغرافي، لأنه يعطي للدولة شخصية خاصة ويوجه سياستها باتجاهات معينة، إذ تعد الجزائر من الدول ذات الموقع الإستراتيجي

[1]- صالح زياني، **مرجع سابق**، ص6.

والمساحات الشاسعة، والامتداد الحدودي الكبير وهو الأمر الذي جعل منها الدولة تتصف بــ "القارة الغنية"،[1] بتنوع مواردها وثرواتها حيث جعل هذا الآخر منها منطقة لطمع واستقطاب من جهة بالإضافة إلى أنها تواجه تهديدات داخلية وخارجية من البيئة الإقليمية التي تهدد أمنها واستقرارها خاصة في ظل التغيرات السياسية والأمنية التي تشهدها دول الجوار الشرقية (ليبيا وتونس) وكذا تنامي الإشكاليات الأمنية في منطقة الساحل الإفريقي، خاصة مع الأزمات كأزمة مالية وأزمة ليبيا، ويضاف إلى ذلك تنامي التهديدات اللاتماثلية في البيئة الإقليمية للجزائر من الإرهاب والجريمة المنظمة والهجرة الغير شرعية وتجارة وتهريب الأسلحة والمخدرات...إلخ.

تأثرت الجزائر بعمق بالتحولات التي عرفتها المنظومة الدولية منذ انتهاء الحرب الباردة، فقد توسعت مضامين الأمن القومي الجزائري في زمن العولمة واتسمت أكثر بالطبيعة اللينة، بحي لم تعد التهديدات العسكرية وحدها تحض بنفس الأهمية كما كان الأمر في السابق، بحكم التهديدات الجديدة التي أخذت بالظهور والتنوع والتطور سواء على المستوى السياسي أو الاقتصادي أو الاجتماعي أو الثقافي أو البيئي أكان ذلك محليا أو إقليما أو عالميا.

إن ارتباط الأمن القومي الجزائري بالقضايا اللينة في ظل تنامي العولمة بتداعيتها المختلفة لا يعني بقاء واستمرار العديد من التهديدات ذات الطبيعة الصلبة، أي التهديدات العسكرية وذلك في الوقت الراهن وحتى في المستقبل، وهي تهديدات ذات علاقة مباشرة بالأمن القومي الجزائري ومنها على الخصوص قضية الصحراء الغربية المرتبطة بمطالب ترابية مغربية والتي لازالت تفرض علينا تواتر، كما لا ينبغي أن نغفل كذلك تأثير وتداعيات الاستراتيجية الاورو – أطلسية والتي تبني توجهات وقائية لاسيما ما يتعلق ببناء القدرات التسليحية للدول العربية وعلى رأسها امتلاك هذه الدول الصواريخ طويلة المدى أو تطويرها لأنشطة نووية بإمكانها أن تشكل مصدرا لتحديد الأمن الأوروبي أو الإسرائيلي.[2]

إضافة إلى كل ما سبق يتعين أن نشير إلى تهديد هام للغاية وله ارتباط بكل من الأمن القومي في شكله الصلب وفي شكله اللين كذلك ألا وهو التهديد الإرهابي، إذ تعد الجزائر من الدول التي تأثرت وعانت من التهديد بشكل لافت في مقابل بقية الدول الأخرى، فقد وصل التهديد الإرهابي في لحظات معينة إلى حد تهديد

---

[1]– لخضر زازة ، عبد الحليم بوقرين، **"سياسة المشرع الجزائري في مواجهة التهديدات الأمنية الجديدة"**، مجلة العلوم الإنسانية، (جامعة أم البواقي ، العدد4، 2016)، ص 103.

[2]– زيد موسى أبو زيد، **الأمن القومي العربي وخطر المروع الصهيوني**، من الرابط:
http// :www.zaidabuzaid.jearan.com/archive/2009/7/906812.html،2019-05-25 تاريخ التصفح،

كيان الدولة الجزائرية لاسيما خلال النصف الأول من تسعينات القرن الماضي، فان هذه المشكلة لازالت تمثل أولوية أمنية بالنسبة لمختلف المؤسسات السياسية والأمنية في الجزائر والتي تربط استفتاء شروط الأمن القومي. إن التهديدات الإرهابية تتعدى مخاطرة الجوانب العسكرية الصلبة، تداعياته السلبية على النسيج السياسي والاجتماعي وعملية التنمية الاقتصادية في الجزائر[1].

ومن أهم التهديدات التي تتعرض لها الجزائر:

الفرع الأول: التهديدات السياسية

تميز الدراسات الأمنية الحالية عادة بين أمن النظام وأمن المجتمع، حيث بقدر ما تكون الدولة تسلطية وشمولية بقدر ما يتم التركيز فيها أكثر على حماية النظام، وبقدر ما تميل الدولة اكثر لتحسين مبادئ الديمقراطية كالمشاركة والشفافية والمساءلة والمحاسبة بقدر ما تكون بصدد التمكين لمضمون أعمق لأمنها وهو الأمن المجتمعي.

وتجدر الملاحظة إلى أنه عادة ما تكون أمام وضعيات معينة تميز الأنظمة التسلطية، وهي تحول النظام إلى تهديد أمني للمجتمع في الحالات التي يمر فيها هذا النظام بأزمات حادة حيث يلجأ الى إجراءات وحلول أمنية تكون انعكاساتها خطيرة على أمن المجتمع في الحالات التي يتم فيها انغلاق النظام السياسي وتحجيم قواعد التنافس السياسي والمشاركة السياسية.

أدى إنغلاق النظام السياسي الجزائري خلال مطلع التسعينات إلى استفعال ظاهرة الارهاب التي تزامنت مع ظروف دولية محفزة لها، وعليه أصبح هاجس أمن النظام وأمن الدولة من الهواجس الأمنية للجزائر، ورغم التنوع في الأساليب التي اعتمدتها النخبة الحاكمة في الجزائر لتطويق هذه الظاهرة وهي الأساليب التي تراوحت بين استخدام القوة العسكرية واللجوء إلى أساليب المعالجة السياسية من خلال مبادرات سياسية معينة كسياسات الوئام المدني والمصالحة الوطنية، إلا أن هذا التهديد لازال قائما بفعل تعدد أسبابه وعلى رأسها عجز الشرعية السياسية في الجزائر والتي لازالت مستمدة من الخارج اكثر من الداخل.[2]

---

[1] - صالح زياني، **مرجع سابق**، ص3.

[2] - مصطفى الخلفي، **أزمة العلاقات المغربية الجزائرية ومشكلة الصحراء المغربية .**على الرابط:

http://www.aljazeera.net.2019-05-19 ، تاريخ التصفح: 19-05-2019

الفرع الثاني:التهديدات الاجتماعية

لعل من أبرز التهديدات التي يتواجه الأمن القومي الجزائري تلك المتعلقة بتحقيق الإندماج الاجتماعي وتحصين الأمن الهوياتي، رغم أن قضايا الهوية والثقافات والمشروع المجتمعي ومصادر تهديدها ظلت قائمة في الجزائر منذ الاستقلال إلا أن ارتباطها في الوقت الحاضر بتأثيرات العولمة يجعل من هذه الحكومات مصدر تهديد حقيقي للأمن القومي الجزائري.[1]

إن رغبات المشروع المجتمعي في الجزائر يمثل تحديا حقيقيا للأمن الاجتماعي والثقافي وبالتالي على الأمن القومي، فلا زالت عناصر الهوية والوطنية كاللغة والدين والإرث التاريخي محل استخدام سياسي، سواء من قبل النخبة الحاكمة أو من قبل قوى المعارضة كالأحزاب السياسية ومؤسسات المجتمع المدني، إن التعاطي السلبي مع هذه المكونات ساهم بقدر وافر في تجسيد المشروع المجتمعي، والذي من خلاله يتم إنتاج وبلورة تكامل واندماج اجتماعي يكون فيه لمؤسسات المجتمع المدني دورا بارزا وفعالا من خلال اضطلاعها بمهمة تحديث الأمن والمجتمع الجزائري[2].

الفرع الثالث: التهديدات الاقتصادية والتكنولوجية

يعد هذا الصنف من التهديد محوريا ومؤثرا للغاية في عصر يتم فيه مقايضة السياسة بالاقتصاد فتحقيق الأمن القومي يستدعي بلورة استراتيجية اقتصادية وتكنولوجية دقيقة وفعالة وبعيدة المدى، إلا أن ما يلاحظ ضمن الحالة الجزائرية قصورا في هذه الاستراتيجية، وما المؤشرات التي سيتم ذكرها الا دليل كاف على هذا القصور. إذ لا يزال الاقتصاد الجزائري اقتصادا ريعي يحكم اختلال انتاج المحروقات بنسبة تفوق 95% من الصادرات الجزائرية، بل وان الجزائر لا تمتلك السلطة المطلقة على حقول النفط التي تخضع أكثر لسلطة الشركات المتخطية القوميات.

إن عدم التنوع في مداخيل الجزائر وإعتمادها على الاقتصاد الريعي وفي حالة استمرار تصديرها للمحروقات بهذه الوترة فلن يكون هناك ما نصدره بعد ربع قرن من الآن. وهنا نطرح فعلا غياب استراتيجية أمنية لتامين حياة الأجيال القادمة، من ناحية أخرى فان الجزائر لا تمتلك السلطة الكاملة على مواردها وعلى احتياطاتها المالية التي تتعرض لإشراف مستمر بفعل تنامي مشكلة الفساد لمختلف أشكاله فقد أصبح الفساد

---

[1]- محمد الصالح بوعافية، **دور الجيش في تأمين المنشآت الإستراتيجية: حالة الجزائر منشأة تيقنتورين النفطية**، (الملتقى الدولي حول الدفاع الوطني بين الالتزامات والتحديات الاقليمية .جامعة -قاصدي مرباح – ورقلة،) 2014، ص: 127.

[2]- صالح زياني، **"تحولات العقيدة الأمنية الجزائرية في ظل تنامي تهديدات العولمة"**، (مجلة الفكر، عدد5، الجزائر، د.س.ن) ص ص293-294.

مؤسسة في الجزائر التي ترهن مستقبل الأجيال القادمة، أما من ناحية ثالثة فإن الجزائر مهددة في أمنها الغذائي بين العجز المتنامي في هذا القطاع الحيوي الحساس، إذ تشكل واردات الجزائر الغذائية ما يزيد من ربع وارداتها السنوية.

أما على مستوى التهديدات التكنولوجية، فإن التطورات السريعة التي يشهدها هذا المجال يساهم في بروز تهديدات للأمن القومي الجزائري، وهي تهديد تمس كلا من مؤسسات وكذلك أفراد المجتمع، وهناك كذلك الجرائم المتعلقة بالمواقع المعادية سيما المواقع السياسية التي وان كانت من جهة تعبر عن تنامي القيم الحضارية الديمقراطية لكنها كثيرا ما تكون مصدرا للأخبار الفاسدة التي تخلق شرخا بين النظام السياسي ومواطنيه، إضافة الى كل ذلك هناك جرائم القرصنة والنسخ غير المشروع أين تعد الجزائر من الدول التي أهلكتها هذه المعضلة.

ويمكن أن نذكر كذلك جرائم التجسس الالكتروني بفعل وجود تقنيات عالية التقدم يتم استثمارها للتجسس على الدولة، وهناك أخيرا ما يعرف حاليا بالإرهاب الالكتروني، والذي يتم من خلاله الاستيلاء على المعلومات والقيام بتدميرها أو تعطيلها في عصر الازدهار الالكتروني.[1]

الفرع الرابع: التهديدات البيئية

تعد مشكلة التصحر تهديدا آخر للأمن القومي الجزائري، فظاهرة التصحر تقترب أكثر فأكثر من شمال البلاد مما سيخلق تأثيرات بيئية خطيرة للغاية[2].

[1]- صالح زياني،" **مرتكزات عقيدة الأمن القومي الجزائري بين الثبات والتحول**"، الملتقى الدولي حول الدفاع الوطني بين الالتزامات والتحديات الإقليمية .(جامعة -قاصدي مرباح -ورقلة، 2014)،ص 06.

[2] - **المرجع نفسه**، ص 10.

المبحث الثاني: الأمن السيبراني الجزائري

في ظل التوجه الدولي نحو الحكومة الإلكترونية أصبحت قضية الأمن المعلوماتي السيبراني من التحديات الكبرى على الصعيدين الإقليمي والعالمي، لا سيما مع تزايد التهديدات الأمنية الإلكترونية، والجزائر كغيرها من الدول سعت منذ انتهاجها للإدارة الإلكترونية حماية منظومتها المعلوماتية من خلال العديد من الأجهزة والخلايا الأمنية. لقد أصبح الأمن المعلوماتي السيبراني ركن أساسي ضمن المنظومة الأمنية المعاصرة، والتي يجب على الدفاع الوطني من خلال أجهزته كالدرك الوطني الجزائري باعتباره مسؤول أمني داخلي تحقيقه في ظل تنامي الجريمة الرقمية، وكذا نظرا للاستغلال المتنامي للشبكات الالكترونية لأهداف إجرامية، والتي تؤثر سلباً على سلامة البنى التحتية للمعلومات الوطنية الحساسة لا سيما على المعلومات الشخصية. [1]

المطلب الأول: مكانة الأمن السيبراني في السياسة الأمنية الجزائرية

وضعت الجزائر خطوة جديدة نحو مجابهة الجرائم الإلكترونية التي شهدت أرقاما قياسية في السنة الماضية وأخذت أشكالا جديدة، جعلت مسؤوليها يعلنون حالة استنفار لمجابهة الظاهرة الإلكترونية، وبهدف محاربة الجرائم الإلكترونية، كشفت الجزائر عن أنها جهزت أكثر من 24 ألف مهندس وتقني مختص في الأمن السيبراني الجزائر شرعت في تكوين أعداد أخرى "ذات كفاءة عالية في مكافحة الجريمة الإلكترونية وحماية الشبكات والأنظمة المعلوماتية تبدأ بتكوين الموارد البشرية ذات كفاءة عالية، ففي سنة 2002 في إبرام اتفاقيات مع عملاقة في هذا المجال على غرار Huawei،Microsoft، Cisco في إطار الإستراتيجية الوطنية لتطوير الاقتصاد الرقمي والأمن السيبراني المرافق له. [2]

في هذا الإطار فان الجزائر قد وضعت أجهزتها الأمنية لحماية منظومتها السيبرانية اعتمادا على مؤسسة الدفاع الوطني أحد أولوياتها، على غرار باقي دول العالم التي سارعت إلى مراجعة سياساته الأمنية، وإدراجها لآليات وميكانيزمات جديدة تعني بهذه المسائل ،بالموازاة مع تطوير البنيات الأساسية المتعلقة بتكنولوجيات العالم الرقمي ،ويفرض مطلب 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 وتأخذ بعين الاعتبار دقة الهجمات الالكترونية وتعقيداتها والتي يزداد خطرها مع التطور التكنولوجي واستخداماتها اليومية،

1- سمير بارة،" **الأمن السيبراني في الجزائر السياسات والمؤسسات** "، **المجلة الجزائرية للأمن الإنساني**، العدد الرابع، (جويلية 2017) ص255.

2- يونس بورنان، "**الجزائر24 ألف مختص في الأمن السيبراني لمواجهة الجرائم الالكترونية**"، على الرابط:

https://www.searchnewworld.com. تصفح في: 2019/05/10

وتجسيدا لذلك باشرت الدولة الجزائرية وفي مقدمتها مؤسسة الدفاع الوطني إلى إعداد برامج خاصة لمجابهة الجريمة الالكترونية والحد من انتشارها ،وإنشاء أجهزة جديدة تنسجم أدوارها وتجهيزاتها مع المتغيرات الحاصلة في هذا المجال، إذا أصبحت الحماية السيبرانية جزءا مهما في أي منظومة للدفاع ،وقد استطاع الجيش الوطني الشعبي المضي قدما ومسايرة التطورات التكنولوجية والإعلامية الحاصلة في العالم، ومن ثمة تأمين وحماية نطاقه المعلوماتي لكل الناشطين فيه من خلال التركيز على مرتكزات رئيسية وهي :

النص القانوني: استدرك المشرع الجزائري في السنوات الأخيرة ولو نسبيا الفراغ القانوني في مجال الجريمة الالكترونية، وذلك لما أصدر القانون 04-15 المتضمن تعديل قانون العقوبات، حيث خصص قسمه السابع مكرر للمساس بأنظمة الآلية للمعطيات، لقد أخص المشرع الجزائري تنظيم الجرائم الالكترونية بقوانين عامة وخاصة ، حيث تمثلت القوانين العامة في: [1]

أ/ **الدستور الجزائري**: كفل دستور 2016، بالتعديل الطارئ على حماية الحقوق الأساسية و الحريات الفردية ذلك عن طريق أهم المبادئ الدستورية في مواده.

المادة 38: الحريات الأساسية وحقوق الإنسان والمواطنة مضمونة.

المادة 44: حرية الابتكار الفكري والعلمي مضمونة للمواطن .حقوق المؤلف يحميها القانون تتمثل القوانين الخاصة التي أقرها المشرع الجزائري في مجال الجريمة الالكترونية. [2]

ب/ **قانون البريد والاتصالات السلكية واللاسلكية**: حيث نصت عدة مواد منه فيما يخص المجال السيبراني المادة 87، و التي نصت على سهولة التحويلات المالية الكترونيا والمادة 84/ 2 على استعمال حوالات الدفع العادية والالكترونية، كما نصت المادة 105 على احترام المراسلات، أما المادة 127 بجزاء كل من يفتح أو يخرب بريد.

ج/ **قانون التأمينات**: وقد نص هذا القانون على تنظيم الجريمة الالكترونية من خلال مؤسسات وهيئات الضمان الاجتماعي ،وذلك في عدة نصوص تخص بطاقة الكترونية.

د/ **القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها**:حيث جاء هذا القانون منظما للجرائم المتصلة بتكنولوجيا الإعلام والاتصال وكل ماله علاقة بالمنظومة المعلوماتية[3].

[1]- ج. رضوان،" **الأمن السيبراني: أولوية في استراتيجيات الدفاع** "، **مجلة الجيش**. العدد 630 ،(جانفي 2016) ص 41،40.

[2]- القانون 04-15من الجريدة الرسمية رقم 14 المؤرخة في 7 مارس 2016.

[3]- يوسف بوغرارة،" **الأمن السيبراني: الإستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري** "، **مجلة الدراسات الإفريقية**، العدد الثالث (سبتمبر/أيلول2018) ص110.

المطلب الثاني: أسباب اهتمام الجزائر بالأمن السيبراني

من بين أساب اهتمام الجزائر بالأمن السيبراني يتجلى فيما يلي:

الفرع الأول: أسباب سياسية

هناك أمثلة كثيرة تدفع نحو الاهتمام بهذا الجانب كالتسريبات المختلفة للوثائق الحساسة التي تؤدي إلى مشكلات عويصة جدا على المستوى الخارجي والدولي كما أنه لا ينكر أحد الدور المتعاظم لشبكات التواصل الاجتماعي على المستوى السياسي (حملات انتخابية، تظاهرات الكترونية ،حركات احتجاجية الكترونية.

كما يتم استغلال هذه المواقع من طرف العديد من الحكومات لتمرير سياستها وفي سياق اخر يجب أن لا نغفل عن استخدام هذه المواقع من طرف الحركات الإرهابية لتجنيد أفرادها وجمع التمويل لعملياتها ،واليه للاتصال بينها كأفراد وكجماعات، وهو ما استوجب على الدول العمل على حماية أمنها من التهديدات والمخاطر التي تتعرض لها من خلال شبكات الانترنت.

الفرع الثاني: أسباب عسكرية وأمنية

شكل التطور الاهتمام التقني بالشبكات وبرامج المعلوماتية أهم عناصر لفك ألغز الجرائم السيبرانية محور اهتمام مؤسسة الدفاع الوطني في تطوير إمكاناته وقدراته على جميع الأصعدة ،ويكمن أن يلاحظ بشكل جلي في درجة الاحترافية التي يتمتع بها أفراد الدرك الوطني فقد استطاعت لحماية البنى التحتية المعلوماتية ضد كل المخاطر الرقمية ،وتكوين أفرادها على المستويات ويتضح ذلك في الأدوار التي تؤديها انجازاتها، إذا يعتكف إفراجها وضع التدابير اللازمة لمنع تسرب امتحانات البكالوريا 2017.[1]

واستطاعت قيادة الدرك الوطني من خلال التكوين المستمر والمتميز لأفرادها والملتقيات الدولية والوطنية وتبادل الخبرات مع دول أخرى أن توفر القوى المؤهلة وذات الكفاءة من مهندسي الإعلام الآلي، رجال القانون، وهذا من أجل التصدي لها في ذات السياق استطاع مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني رصد أزيد من 100جريمة الكترونية سنة2014 وما يفوق 500 قضية رقمية خلال سنة 2015، منها 300 جريمة تتعلق بمواقع التواصل الاجتماعي "فيسبوك"و20 جريمة رقمية تعلقت باءختراق مواقع رسمية لمؤسسات خاصة وعامة ،استهدف مجرموها أنظمة المعالجة الآلية للمعطيات ويتحقق الدفاع الوقائي الالكتروني وفق ثلاث أساليب رئيسية:

[1]- 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.

1- الكشف المبكر عن الهجمات في وقتها الحقيقي: وذلك باستخدام sensorsعلى شبكات والبرامج والتطبيقات مع توظيف المعلومات الاستخبارتية.

2- الهجوم الالكتروني ألاستباقي: وذلك بنشر الديدان البيضاء white wormsباعتبارها برامج قادرة على اكتشاف التطبيقات الضارة وتدميرها قبل التوظيف، وإطلاق هجمات الكترونية مضادة Hack Back

3- التضليل والإخفاء والتضليل والخداع: وذلك بإخفاء هويات الأهداف الإستراتجية للدولة للانترنيت عن ذريق تضليل الخصوم بأدوات التمويه والخداع وتغيير ملامح الأهداف واستجابة لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الالكترونية قامت مصالح الأمن بانشاء المصلحة المركزية للجريمة الالكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية لمحاربة الجريمة الالكترونية على مستوى المديرية العامة للأمن الوطني والتي أنشئت سنة2011، ليتم بعدها انشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وأضيف هيكل تنظيمي لمديرية الشرطة القضائية.

الفرع الثالث: أسباب قانونية

يترتب على النشاط الفردي والمؤسساتي والحكومي، في الفضاء السيبراني، نتائج قانونية وموجبات تستدعي اهتماما خاص ،لحل التزاعات التي يمكن أن تنشأ عنها وتستدعي مواكبة التحولات التي رافقت ظهور مجتمع المعلومات ،فظهرت حقوق أخرى،كحق النفاذ إلى الشبكة العالمية للمعلومات توسعت بعض المفاهيم، لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات كالحق في إنشاء المدونات الالكترونية، والحق في إنشاء التجمعات على الانترنت، والحق في ملكية البرامج المعلوماتية كما ظهرت موجبات جديدة ذات انعكاسات اقتصادية مثل: موجب الاحتفاظ ببيانات الاتصالات وموجب الإبلاغ عن مخالفات وجرائم خاصة بالمحتوى كل هذه التغيرات والتحولات تستدعي وجود ترسانة قانونية تنسجم مع التطورات الحاصلة على المستوى الحقوق أو على مستوى البيئات والعمليات.[1]

1 بارة سليم، **المرجع السابق**، ص 14.

المبحث الثالث: أبرز التهديدات السيبرانية التي تواجه الأمن الجزائري

في ظل الأوضاع الأمنية غير المستقرة التي تشهدها المنطقة العربية عموما، ودول الجوار الجزائري خصوصا، ومع تسارع التطورات التكنولوجية الكبيرة التي يشهدها عالم اليوم، والتي أدت إلى إحداث تغيرات جذرية مست الكثير من الأصعدة الاجتماعية والسياسية والإقتصادية، فقد ساهمت الثورة التكنولوجية الحديثة في تجاوز الحدود وتقريب المسافات وزيادة حرية التواصل بين الشعوب وتسهيل الحصول على الخدمات وغير ذلك من الانعكاسات الايجابية التي أفرزتها هذه الثورة، كما ترتب عنها العديد من المخاطر التي تهدد أمن واستقرار الدول والمجتمعات، لعل من أهمها انتشار ظاهرة الارهاب الإلكتروني التي برزت بشكل كبير بعد انتشار وسائل التواصل الاجتماعي والعديد من المواقع الالكترونية التي تحمل أفكارا هدامة، وتدعو الى نشر الفوضى والعنف والتطرف والكراهية والانقسام، وهو ما سيتم توضيحه في هذا المبحث.

المطلب الأول: الإرهاب السيبراني

يعد الإرهاب السيبراني كأحد أخطر التهديدات المحتملة 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]

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

---

[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.

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 ولبيا ومصر[3].

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[4].

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

---

[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"**، من الرابط: www.alittihad.ae/details.php=120l..2019/04/30 تاريخ تصفح

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

[4]- عنتر بن مرزوق ، **مرجع سابق**، ص20 .

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: القرصنة السيبرانية

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 وكذا تحريض القصر على الدعارة.

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]

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.

---

[1] – عبد السلام البارودي، "**هل دخلت الجزائر عصر الجريمة الالكترونية؟**"، على الرابط:

تصفح في: https://www.maghrebvoices.com/a/algeria-cyber-criminality/414407.html.2019/05/10

* 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 ".

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:

- تعطيل الخدمة.
- إتلاف المعلومات أو تعديلها.
- التجسس على الشبكات.
- 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. [1]

فقد حذر الباحث الأكاديمي غي العلوم السياسية والعلاقات الدولية "أحمد عظيمي" خلال محاضرة ألقاها بمركز الشعب للدراسات الإستراتجية حول موضوع الإرهاب الالكتروني القاعدة كنموذج ،أن مواقع الانترنيت الداعية للعنف في تزايد،وبين تنظيم القاعدة استغل الانترنيت إلى أقصى الحدود لنشر أفكاره بتأسيس ما يسمى الجبهة الإعلامية في 2003. [2]

---

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

[1]- 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

[2]- سمير بارة، **المرجع السابق**، ص 251.

خلاصة واستنتاجات

لقد أصبحت الجزائر دولة سائرة في طريق النمو والتطور وذلك راجع للعديد من الإجراءات والتحديثات التي قامت بها لكي تبقى مستعدة لمواجهة التحديات والتهديدات التي تحيط بها، ومن خلال ما سبق سرده في المباحث السابقة نصل إلى النتائج التالية:

– مع بروز التهديدات الجديدة المتتابعة أصبح على الجزائر مواصلة سياسة التسلح النوعية لمواجهة تلك التهديدات على رأسها مكافحة الإرهاب والجريمة المنظمة، حيث ركزت على ضرورة امتلاك آليات وأجهزة للرصد بتأمين الحدود والاستطلاع، لاختراق الجماعات الإرهابية والعصابات المنظمة وإبطال مفعولها وتهديداتها الأمن الوطني وحدوده، كما طور نفسها في الجانب التكنولوجي ومحاولة الوصول إلى الحكومة الالكترونية.

– إن الجزائر تهتم بشكل مباشر بالأمن السيبراني وذلك راجع التسريبات المختلفة للوثائق الحساسة التي تؤدي إلى مشكلات عويصة جدا على المستوى الخارجي والدولي.

– سجلت الجزائر أزيد من 900 جريمة إلكترونية خلال سنة 2017، حسب ما أعلنه مركز الوقاية ومكافحة الجريمة الإلكترونية، لذلك فهي تعاني في هذا الجانب وتحاول إيجاد حلول تساعدها على تامين منظومتها السيبرانية.

الفصل الثالث:

المناهج المستخدمة لمواجهة التهديدات السيبرانية

لقد وضعت الجزائر الأمن السيبراني كأحد أولوياتها على غرار باقي دول العالم التي سارعت إلى مراجعة سياساتها الأمنية، حيث أصبح كهوية للجزائر وذلك لأهمية وتشكيله تهديدا كبيرا، وقامت بإدراج آليات وميكانزمات جديدة تعني بهذه المسائل، بالمؤازرة مع تطوير البنيات الأساسية المتعلقة بتكنولوجيات العالم الرقمي، بالإضافة إلى التعاون على المستوى الدولي والإقليمي.

لذلك في هذا الفصل سوف نفصل في طريقة الجزائر للاهتمام بهذا الجانب وتطوير لذلك تم تقسيم هذا الفصل إلى المباحث التالية:

- ✓ المبحث الأول: وسائل الدولة الجزائرية في مواجهة التهديدات السيبرانية؛
- ✓ المبحث الثاني: آليات التعاون الدولي والإقليمي في مواجهة التهديدات السيبرانية؛
- ✓ مستقبل الأمن السيبراني الجزائري.

المبحث الأول: الوسائل الجزائرية لمواجهة التهديدات السيبرانية

نظرا لخطورة التهديدات السيبرانية أولت الجزائر أهمية كبيرة لمسألة توفير وسائل تحقيق الأمن السبراني، خاصة بعد دخول خدمة الجيل الثالث والرابع وتنامي استخدام شبكات التواصل الاجتماعي، ويظهر ذلك من خلال ما يلي:

المطلب الأول: الجانب الأمني والمؤسساتي

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.

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 في الأمن الداخلي 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

* **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.

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.

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.

---

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

[2]- بارة سمير، مرجع سابق، ص ص6-7.

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" و20 جريمة رقمية تعلقت باختراق مواقع رسمية لمؤسسات خاصة وعامة، ومجرموها أنظمة المعالجة الآلية للمعطيات

-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.

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

[1]- بارة سمير، **مرجع سابق،** ص10.

الإعلام الآلي: على مستوى هذه المصلحة يتم رصد ومراقبة وتتبع عمليات الاختراق والقرصنة المعلوماتية وكذا اكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية.[1]

-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.[2]

-الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

تشكلت هذه الهيئة بمقتضى المرسوم الرئاسي رقم 15-261[3] 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[4].

[1]- 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.

[2]- عز الدين عز الدين، **مرجع سابق**، ص 39.

[3]- 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.

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

المطلب الثاني: الجانب القانوني

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:[1]

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

– 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:[2]

– 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.

[1] – 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 لــ 16 أوت 2009، ص06.

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

– 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.

– 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 للنزاعات بعد البر والبحر والجو والفضاء.[2]

المطلب الثالث: معيقات تحقيق الأمن السيبراني الجزائري في ظل التحديات الأمنية والمستقبلية

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 إيجابياته إلا أنه يستلزم توفير الأمن لنجاح هذه الخدمات.

[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، **مرجع سابق**، ص ص38-39.

والجزائر 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 (WiFi/3G/4G) عبر هذه التقنيات لم يعد المجرم يحتاج للجلوس وراء الحواسيب الموصولة سلكيا بشبكة الانترنيت للقيان بجريمته مما يستدعي من الجهات الأمنية رفع التحدي والاستعداد بأحدث التقنيات لمواجهة والتصدي لهذه التطورات.

- 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

* **الحوكمة الالكترونية**: الحوكمة الإلكترونية هي استخدام تكنولوجيا المعلومات والاتصالات لتقديم الخدمات الحكومية، وتبادل معلومات معاملات الاتصالات، وتكامل مختلف الأنظمة والخدمات القائمة بذاتها بين الحكومة والمواطن، وبين الحكومة والشركات، وبين الحكومات وبعضها البعض، وكذلك عمليات الأقسام الإدارية والتفاعلات داخل إطار عمل الحكومة بأكمله

[1]- عز الدين عز الدين، **مرجع سابق**، ص 51.

لها رصد الجزئيات وفك الشفرات وتطوير البنى الخاصة بالمعلومات وتحديثها باستمرار، وتصميم برامج عالية التطور.

-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 متزايدا 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، **مرجع سابق**، ص18.

المطلب الرابع: رؤية مستقبلية للأمن السبراني الجزائري

إن الأطروحات الجديدة للأمن تستوجب علينا التوقف والتمعن في هذا المفهوم، بما ينسجم والتغيرات الحاصلة في العالم، لا سيما في ظل التطور الرهيب في مجال الإعلام الآلي وتكنولوجيا الاتصالات والمعلومات، إلى حد التوجه إلى إنشاء ما أصطلح على تسميته بالمدن الذكية، والتي تحولت فيها الخدمات من الشكل التقليدي إلى الإلكتروني، لتخلق بذلك ميدانا جديدا يختلف عن سابقيه، وعلى الرغم من إيجابياته إلا أنه يستلزم توفير الأمن لنجاح هذه الخدمات. والجزائر كغيرها من الدول يجب أن تتجه نحو تبني مقاربة الحكومة الإلكترونية، وعلى الرغم من حداثة التوجه إلا أن عدد الجرائم المرتكبة، يوحي بحجم الأخطار التي تتربصها، وهو ما يجعل مؤسسة الدفاع الوطني أمام تحدي جديد، وهو تحقيق الأمن السيبراني حاليا ومستقبلا[1].

المبحث الثاني: آليات التعاون الدولي في مواجهة التهديدات السيبرانية

تعتبر جهود التعاون الكبيرة التي تبذلها الحكومات والدول 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،وهو ما سيتم توضيحه في هذا المبحث.

المطلب الأول: التشريعات الدولية بشأن الجريمة السيبرانية

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: [2]

[1] – بن مرزوق عنترة وآخرون، "البعد الالكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب"، مجلة العلوم الإنسانية، العدد 38، جوان 2018، ص 41.

***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، و أن يتم ذلك باستخدام وسائل الاتصالات الحديثة مثل الإنترنت) غرف الدردشة أو البريد الإلكتروني أو المجموعات.

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

- **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.

– 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

– 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:

– 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:

– داخل إقليمه

– على ظهر سفينة ترفع علم ذلك البلد

– 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]

– 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

[1]– حسن بن أحمد الشهري، مرجع سابق، ص ص 19، 20.

عبارة "المبادئ التوجيهية لمنظمة التعاون والتنمية في الميدان الاقتصادي لأمن شبكات ونظم المعلومات- نحو ثقافة أمنية- 2002"[1] (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.

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، **مرجع سابق**، ص: 21.

- على المستوى العربي

فالتشريع العربي بشأن الجريمة السيبرانية وضع نموذج لمكافحة جرائم تقنية أنظمة المعلوماتية والذي صادق عليه مجلس وزراء العدل العرب في2003/10/08 في دورته التاسع عشر:[2]

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

[2]- **"الجرائم الإلكترونية، وآفاق النمو المتسارع، المركز العربي للبحوث والدراسات"**، 2018، من الرابط:

https://www.google.com/url?sa=.2019-06-01 :تاريخ التصفح

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: الجهود الدولية

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.

الفرع الأول: الحد من سباق التسلح السيبراني

يلعب التسليح دورا هام في الاستراتيجية في توازن القوى على المستوى العالمي في ظل بيئة يسودها الشك وعدم اليقين، وهو ما يحمل خطورة عسكرة الفضاء السيبراني، وتتبنى عديد الدول استراتيجية 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. [1]

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

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.

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.[1]

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 الإطار القانوني الدولي الذي يحدد الالتزامات والواجبات لجميع الفاعلين، وان أي اتفاق من شانه تنظيم الاستخدام العسكري للفضاء السيبراني، يجب ان يعمل على منع نشر الاسلحة 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 كنضام 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 مجنوعات عمل لمكافحة الجريمة السيبرانية.[2]

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

[1]– جوزيف، س ناي، "**التحكم في الصراع الليبيراني**"، مدونات الجزيرة على الرابط: http://blogs.aljazeera.net/blogs، بتاريخ: 29-05-2019.

[2]– عادل عبد الصادق، **مرجع سابق،** ص 69.

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.[1]

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 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 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.

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

[1]- جوزيف، س ناي، **موقع سابق**.

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.

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

الفرع الثاني: 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 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

---

[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.

وجغرافيا أو ثقافيا أو سياسية، ويهتم هذا التعاون بدراسة من إيجاد حلول للهموم وقضايا مختلفة المجالات (الأمنية، النقل، والموارد المائية والكهربائية والاقتصادية ...).

وفي كل مرة يظهر فيها هم دولي، أو إقليمي مشترك، تظهر الدول ميلا إلى التعاون، ولا يخرج هم مكافحة الجريمة السيبرانية عن هذه القاعدة، لذا نجد أن العالم ممثلا بالأمم المتحدة، يدفع بهذا الاتجاه كما نلاحظ بروز العديد من المبادرات الجهود التي تصب في خانة إرساء قواعد التعاون. [1]

المبحث الثالث: آليات التعاون الاقليمي في مواجهة التهديدات السيبرانية

تأتي آليات التعاون الإقليمي أكثر نجاعة وفعالية بحكم الخوف من انتشار التهديد وتكون طرق المواجهة أكثر جدية وتنسيق بين الأطراف،وهو ما سيتم توضيحه وفقا للآتي:

المطلب الأول: الجهود الإقليمية

تتكيف 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.[2]

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:

---

[1]- سعيد درويش ، **مرجع سابق**، ص 133.

[2]- عادل عبد الصادق، **مرجع سابق**، ص333.

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

– تحديد وسائل التحقيق والملاحقة الجزائية.

– 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]

المطلب الثاني: الوسائل الإقليمية لمواجهة التهديدات السيببرانية

ونورد 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 حبور، "**السيبراينية 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، بحيث نقوم بتحديد المخاطر المحتملة وإزالتها.

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

الفرع الأول: التنسيق الإقليمي الدولي لمواجهة التهديدات السيبرانية

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.

[1]– مني 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]– مني الأشقر جبور، "**السيرانية هاجس العصر**"، **مرجع سابق**، ص48.

– 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.

– تطبيق القوانين الدولية من قبل هيئات مختصة في الأمم المتحدة، على الاعتداءات السيبيرانية التي يمكنها أن قمدد 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 بمؤسساقم، ويمكن للإجراءات أن تلحظ تأمين المخاطر، والحوادث التي يمكن أن تقع.

– تعزيز دور المؤسسات الدولية كالإنتربول والإقليمية كالأفريبوبول 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**"، من الرابط:

www.itu.int/pub/s-gen-wfs.2019-05-26 :تاريخ التصفح ،

الفرع الثاني: تقنيات 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 SSLوتستخدم 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.

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 السيبرانية، 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]– مني الأشقر جبور، "**السيرانية هاجس العصر**"، **مرجع سابق**، ص ص62-63.

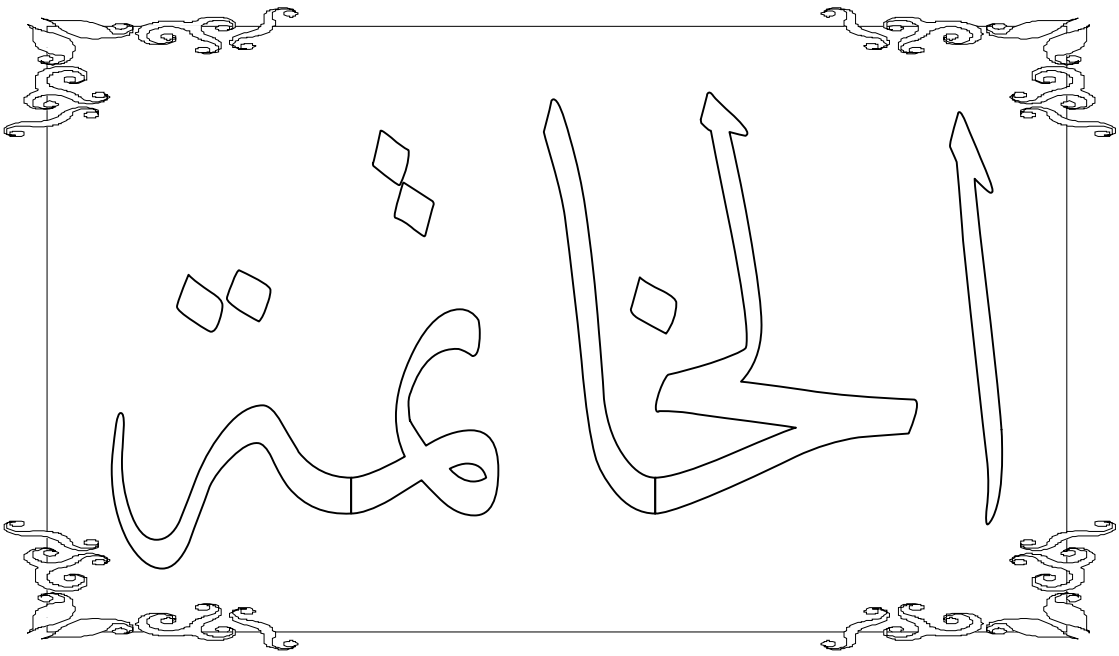
خلاصة واستنتاجات

لقد انتهجت كل دولة وسيلة لمواجهة التهديدات السيبرانية ومن بينها الجزائر التي اعتمدت على أسلوب ناجح وذلك ساعدها على عدم التعرض للاختراق دائما، ومن خلال ما تم التطرق إليه في المباحث السابق نصل إلى الاستنتاجات التالية:

– لقد قامت الجزائر بإنشاء العديد من المراكز التي تعنى بالتأمين السيبراني وتهديداته ومن بينها، المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني، ومختص في الجرائم الالكترونية، بالإضافة إلى المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني وهي مختصة في اعتقال ومتابعة الجرائم الالكترونية.

– لقد سارعت الجزائر لإيجاد حلول لهذه التهديدات لكنها لم تستطع وحدها وانتقلت الى التعاون الإقليمي والدولي مع بقية الدول الصديقة والتي لا تستخدم التكنولوجيا للتهديد.

– سايرت الجزائر مختلف الجهود الدولية والإقليمية والمبادرات ذات الطابع الدولي والاقليمي لمواجهة التحديات السيبرانية سواء من حيث التصدي لها قبل وقوعها أو التنسيق الدولي مع الأخذ بعين الاعتبار الإمكانيات والأطر التشريعية المحلية.


الخاتمة

في الأخير وبعد دراستنا لموضوع الأمن السيبراني وأهم تهديداته المتعلقة به، على الصعيد الدولي والاقليمي والوطن ، فالتهديد السيبراني في الجزائر يعد أحد أهم التحديات الجديدة للسياسة الأمنية الجزائرية، التي فرضتها التطوراتالتكنولوجية المتسارعة، ورغم الجهود المبذولة في سبيل تحقيق ذلك إلا أن المراتب التي تحتلها الجزائر عربيا ودوليا تشير إلى أنها بحاجة إلى المزيد من الجهود، وهذا حتى يمكن لها أن تنجح في مجال مكافحة مختلف المخاطر التي يفرزها الفضاء الالكتروني.

– وقد تم التوصل إلى جملة النتائج التالية:

– إن دراسة الأمن السيبراني التي تم الوصول لها بعد التطرق الى توسيع قطاعات الأمن، من أهم المجالات التي تواجه الدول، حيث إن تحقيق الأمن السيبراني للدولة يؤدي بالدولة إلى الاستقرار في المجال التكنولوجي وتحقيق امنها ومنعه من التعرض للاختراق.

– أصبحت التهديدات السيبرانية أحد أهم التحديات التي يتحتم على الدول مواجهتها خلال الفترة الحالية خاصة مع تزايد الاعتماد على شبكات الانترنت والحواسيب لإلحاق الضرر بها عن قصد، كما تتنوع أشكال ومصادر هذه التهديدات حيث يصبح بإمكان فرد أو مجموعة أفراد في أي مكان من العالم أن يحاول بشكل سري اختراق الأنظمة التي تحتوي على معلومات حيوية أو شن هجمات على البنى التحتية الحيوية.

– لقد أصبحت العلاقة بين الأمن والتكنولوجيا علاقة متزايدة مع إمكانات تعرض المصالح الإستراتيجية ذات الطبيعة الالكترونية إلى أخطار وتهديدات الكترونية، تؤدي إلى تحول الفضاء الالكتروني لوسيط ومصدر لأدوات للصراع المتعدد الأطراف.

– من بين العوامل التي تساهم في تطور المقاربة الأمنية الجزائرية دور العولمة والثورات التكنولوجية في مجالات الاتصالات، السايبر والفضاء الخارجي، وما لا يلاحظ أن العقيدة الأمنية لجزائرية تحاول التكيف مع ما هو مستجد من تهديدات أمنية خاصة تلك التي تتعلق بالتهديدات السيبرانية والتكنولوجية التي أصبحت هاجسا يهدد أمن الدول

– إن الدولة التي تعتمد على الاستراتيجيات التقليدية لمواجهة التهديدات لن تستطيع للتصدي للتهديدات الجدية والمتمثلة في التهديدات السيبرانية.

– تعتبر الجزائر من بين الدول التي تعتمد على التكنولوجيا والتطور في جميع المجالات، لذلك فهي تتعرض للعديد من التهديدات الأمنية من بينها السيبرانية لذلك تعتمد على العديد من الاستراتيجيات لمواجهة هذا الخطر والتصدي له.

– الجزائر كغيرها من الدول اتجهت نحو تبني مقاربة الحكومة الإلكترونية، وعلى الرغم من حداثة التوجه إلا أن عدد الجرائم المرتكبة، يوحي بحجم الأخطار التي تتربص بها، وهو ما يجعل مؤسسة الدفاع الوطني أمام تحدي جديد وهو تحقيق الأمن السيبراني حاليا ومستقبلا.

-رغم الجهود الجزائرية المبذولة في مجال تحقيق الأمن ومواجهة جريمة الإرهاب الالكتروني سواء في شقيها القانوني أو المؤسساتي إلا أنها تبقى بحاجة إلى مزيد من الجهود التشاركية بين مختلف فواعل المجتمع.

التوصيات

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

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

– أخذ جميع أبعاد الأمن السيبراني، بعين الاعتبار، لدى وضع أي إستراتيجية أو سياسة، بما في ذلك حاجات المواطنين والمؤسسات، كما حقوقهم وواجباتهم، بحيث تأتي الخطة متكاملة، ومنسجمة مع ما يمكن توقع الالتزام به من قبل المعنيين بأمن مجتمع المعلومات.

– تدريب وتأهيل وحدات عسكرية وأمنية خاصة، يمكنها مراقبة البنى التحتية للاتصالات، بحيث تقوم بتحديد المخاطر المحتملة وإزالتها

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

– -تحقيق الأمن الالكتروني يتطلب ضرورة نشر الوعي المجتمعي بخطورة جريمة الارهاب الالكتروني وتشجيع التكوين العلمي والجامعي المتخصص في دراستها.

– -تؤدي وسائل الإعلام دورا محوريا في معالجة أهم القضايا والمشكلات التي تواجه المجتمع، ولذلك وجب العمل على تشجيع تناولها لمواضيع متعلقة بهذه الجريمة الخطيرة وتوضيح آليات الوقاية منها.

– يتطلب نجاح سياسة تحقيق الأمن ومكافحة جريمة الارهاب الالكتروني ضرورة الاستفادة من التجارب الرائدة في هذا المجال.

– تؤدي التنشئة الاجتماعية دورا هاما في مكافحة مختلف الجرائم سواء التقليدية أو الالكترونية، وهنا وجب الاهتمام بالأسرة، المدرسة، المسجد والجامعة، وحتى تنظيمات المجتمع المدني من أجل المشاركة معا في بناء مجتمع خال من التطرف والإرهاب.


قائمة المصادر والمراجع

أولا: المصادر

1- الجريدة الرسمية لالجمهورية الجزائرية

ثانيا: المراجع باللغة العربية

1- الكتب

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

2- الطاهر خرف الله، "**النخبة الحاكمة في الجزائر 19*62-1982، بين التصور الإيديولوجي والممارسات السياسية**"، ج1، (الجزائر: دار هومة، 2007).

3- أوس مجيد غالب العوادي، "**الأمن المعلوماتي السيبراني**"، (سلسلة أصدرت مركز البيان للدراسات والتخطيط ، أوت 2016.

4- حسين فاروق، "**فيروسات الحساب الآلي**"، (القاهرة: العربية للطباعة والنشر، ط1، 1999).

5- حمدون ، توريه، "**دليل الأمن السيبراني للبلدان النامية**"، الجزء الاول، (سويسرا: جنيف، 2006).

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

7- ذياب البداينة، "**الأمن وحرب المعلومات**"، ط1، (دار الشرق للنشر والتوزيع، دب، 2006).

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

9- عبد النور بن عنتر، "**البعد المتوسطي للأمن الجزائري: الجزائر، أوربا، الحلف الأطلسي**"، (الجزائر: مكتبة العصر للطبع والنشر والتوزيع، 2005).

10- علي عباس مراد، "**الأمن والأمن القومي، مقاربات نظرية**"، (الجزائر: ابن النديم للنشر والتوزيع، 2017).

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

12- منى أشقر جبور، "**السيبيرانية هاجس العصر**"، (دش، دس).

13- منير البعلبكي ورمزي منير البعلبكي، "**المورد الحديث**"، (لبنان: دار العلم الحديث، د.س).

14- هربرت بوبون، "**نطاق التهدي الغير العسكري في: التسلح ونزع السلاح الأمني الدولي، (مجموعة من المؤلفين)**"، تر: فادي محمود وآخرون، (بيروت: مركز دراسات الوحدة العربية، 2004).

2- المذكرات والرسائل

1- منى الأشقر جبور، "**الأمن السيبراني: التحديات ومستلزمات المواجهة**"، مذكرة ماجستير، جامعة الدول العربية: المركز العربي للبحوث القانونية والقضائية، 2012.

2- وليد غسان سعيد جلعود، "**دور الحرب الإلكترونية في الصراع العربي الإسرائيلي**"، أطروحة ماجستير في التخطيط والتنمية السياسية (بكلية الدراسات العليا، جامعة نابلس، فلسطين، 2013).

3- المجلات والملتقيات

1- إلهام غازي، "**الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري**"، مجلة الجيش، مؤسسة المنشورات العسكرية، العدد630، جانفي 2016.

2- 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.

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

4- بكر أبو بكر، "**الإرهاب الالكتروني من الدعاة والاستقطاب الى اكتساح المجال الافتراضي**"، (المغرب، مجلة ذوات، العدد46، 2018).

5- بن مرزوق عنترة وآخرون، "البعد الالكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب"، مجلة العلوم الإنسانية، العدد 38، جوان 2018.

6- 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).

7- 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) .

8- ج .رضوان، "**الأمن السيبراني :أولوية في استراتيجيات الدفاع"، مجلة الجيش** .العدد 630، جانفي 2016.

9- ج. رضوان،" **الأمن السيبراني: أولوية في استراتيجيات الدفاع** "، **مجلة الجيش.** العدد 630 ،(جانفي 2016) ص 41،40.

10- جارش عادل، "**مقاربة معرفية حول الإرهاب السيبراني**"، مجلة المستقبل العربي، العدد20، بيروت، لبنان،2000.

11- حسام السبكي، "**الحروب السبيرانية المفهوم والأنماط وتداعياتها على الأمن الدولي**"،)الإمارات، جريدة رؤية للأخبار، العدد6)، 13 أوت 2018.

12- حسن بن أحمد الشهري،"**الإرهاب الالكتروني، حرب الشبكات**"، المجلة العربية الدولية للمعلوماتية، 2015.

13- سعيد درويس، "**ماهية الحروب الالكترونية في ضوء قواعد القانون الدولي**"، حوليات جامعة الجزائر 1، العدد 29.

14- سمير بارة،" **الأمن السيبراني في الجزائر السياسات والمؤسسات** "، **المجلة الجزائرية للأمن الإنساني**، العدد الرابع، (جويلية 2017)

15- صالح زياني، "**تحولات العقيدة الأمنية الجزائرية في ظل تنامي تهديدات العولمة**"، (مجلة الفكر، عدد5، الجزائر، د.س.ن) ص ص293-294.

16- صالح زياني، "**مرتكزات عقيدة الأمن القومي الجزائري بين الثبات والتحول**"، (محاضرة مقدمة لطلبة جامعة باتنة، كلية الحقوق والعلوم السياسية، د.س).

17- صالح زياني،" **مرتكزات عقيدة الأمن القومي الجزائري بين الثبات والتحول**"، الملتقى الدولي حول الدفاع الوطني بين الالتزامات والتحديات الإقليمية .(جامعة -قاصدي مرباح -ورقلة، 2014).

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

19- 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).

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

21- عنترة بن مرزوق، "**الأمن السيبراني كبعد جديد من السياسة الجزائرية**"، محاضرات مقدمة لطلبة جامعة محمد بوضياف – المسيلة، كلية الحقوق والعلوم السياسية، د س.

22- فتيحة ليتيم، ونادية ليتيم، "**الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة**"، (جامعة بسكرة، مجلة المفكر، العدد 12، (د.س.ن) .

23- 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.

24- لخضر زازة ، عبد الحليم بوقرين، "**سياسة المشرع الجزائري في مواجهة التهديدات الأمنية الجديدة**"، مجلة العلوم الإنسانية، (جامعة أم البواقي ، العدد4، 2016).

25- محمد الصالح بوعافية، **دور الجيش في تأمين المنشآت الإستراتيجية: حالة الجزائر منشأة تينقتورين النفطية**، (الملتقى الدولي حول الدفاع الوطني بين الالتزامات والتحديات الاقليمية .جامعة - قاصدي مرباح – ورقلة،) 2014.

26- محمد مختار، "**Cyber Security، هل يمكن تجنب الدولة مخاطر الهجمات الإلكترونية؟**"، مجلة مفاهيم المستقبل، العدد 06، بيوت، لبنان، يناير2015.

27- 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).

28- يوسف بوغرارة،" **الأمن السيبراني: الإستراتجية الجزائرية للأمن والدفاع في الفضاء السيبيري** "، **مجلة الدراسات الإفريقية**، العدد الثالث (سبتمبر/أيلول2018) .

29- -أحمد عيسى، نعمة الفتلاوي، "**الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم المعاصر**"، (بحث مقبول للنشر في مجلة المحقق الحليلي،العراق: جامعة الكوفة، كلية القانون، 2016).

4- المواقع الإلكترونية

1- إسماعيل كاخيل، "**الحرب الإلكترونية**"، موقع مجلة الدفاع العربي، من الرابط:
www.arahdefancejournal.com/article560.htm

2- "**الجرائم الإلكترونية، وآفاق النمو المتسارع، المركز العربي للبحوث والدراسات**"، 2018، من الرابط:

https://www.google.com/url?sa.

3- "**القرصنة الالكترونية ... سلاح العصر الرقمي**"، من الرابط:

ww.aljazeera.net/knowledg/newscoverage ،

4- الاتحاد الولي للاتصالات، "**البحث عن السلام السيبراني**"، من الرابط: ww.itu.int/pub/s-gen-wfs.

5- الرسائل الصامتة، "**سلاح الرقابة السرية**"، 23 يونيو/ حزيران 2016م، من الرابط:
www.almaged.ps/3

6- الشهري، نوال، "**حرب المعلومات**"، في مركز تميز الأمن المعلوماتي، (جامعة الملك سعود)، دن، من الرابط:

www.coeia.edu.sa/index.php/ar/assur_awess/data_privacy/1263_influance_warfare.html

7- العربية سكاي نيوز، "**اسكسنت فيروس ضد إيران**"، فبراير 2013، من الرابط:

www.Synewsarabia.com/web/article/114276.

8- العربية سكاي نيوز، "**تفاصيل الهجوم ....قراصنة يدمرون كومبيوترات في وكالة الطيران السعودي.. ويستبدلون البيانات بصورة الطفل السوري الان كريد**"، من الرابط:
www.Skynewsarabia.Comweb/article/114276/d.

9- اللجنة الدولية للصليب الأحمر، "**ماهية القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟**"، على الرابط:

http://accronline.com/article_detail.aspx?id=28958.

10- اليحياوي، يحيى، "**في الاقتصاد الرمادي**"، من الرابط:
www.elyahyauc.erg/savoirs.htm.

11- عادل جارش، "**مقاربة معرفية حول التهديدات الأمنية الجديدة**"، مجلة العلوم السياسية والقانونية، من الرابط:

www.threatcomment.com

12- أماني المهدي، توظيف التنظيمات "**الإرهابية لشبكات التواصل الاجتماعي في استقطاب الشباب** "**الاستراتيجيات وآلية المواجهة**"، الرابط:

www.kitabat.com/culturel

13- بورجيلي ريمون، "**التكنولوجيات الحديثة في المجالات العسكرية**"، (مجلة الجيش اللبناني، عدد236، شباط 2009) ، من الرابط:

www.lebenarmy.gov.lb/article.asp=arfid=7066

14- بورعة على جهاد، "**الجزائر بين توجه إستراتيجي وعقيدة أمنية**"، من الرابط:

www.maspolitiques.com/mas/index.phpcontent=article8id=123.

15- جوزيف، س ناي، "**التحكم في الصراع الليبيراني**"، مدونات الجزيرة على الرابط:

،http://blogs.aljazeera.net/blogs

16- حسام السبكي، "**الحروب السيبرانية، المفهوم، والأنماط والتداعيات على الأمن الدولي**"، جريدة الأخبار (13 أوت 2015) ، من الرابط:

www.royenhenews.com/articles/4809

17- د.م، "**النظام القانوني للأمن الوطني الالكتروني في ظل الثورة الرقمية**"، من الرابط:

www.univ-chlef.dz/fdsp/pdf/je-droits2017.pdf

18- دليل عملي للعمل مع المنظمات الدولية، من الرابط:

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

19- زيد موسى أبو زيد، **الأمن القومي العربي وخطر المروع الصهيوني**، من الرابط:

http// :www.zaidabuzaid.jearan.com/archive/2009/7/906812.html

20- سعد علي الحاج بكري، "**الأمن السيبراني ومعضلة حمايته**"،الرابط:

،www.alegt.com/article1241506.html

21- شبكة النبأ المعلوماتية، "**حرب الفضاء والأقمار الصناعية**"، من الرابط:

www.annaba.org/nbanes/69/022/htm

22- صالح بن علي بن عبد الرحمان الربيعة، الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت. متاح على الرابط:

https://www.google.com/url?sa=

صحيفة المرصد، "ما هو الأمن السيبراني"، موقع إلكتروني **https://al-marsd.com/168664.html**

23- عادل عبد الصادق، "**المجال الأعلى للأمن السيبراني خطوة في دعم استراتيجية الأمن القومي**"، الرابط:

www.aceronline.com/article-detal.Aspxd=20284

24- عبد الحميد ابراهيم، محمد العريان، "**العلاقة بين الارهاب المعلوماتي والجريمة المنظمة ما هو رد القطاع الخاص**"، من الرابط:

repository.nauss.edu.sa/bitstream/handies/9.pdf،

25- عبد السلام البارودي، "**هل دخلت الجزائر عصر الجريمة الالكترونية؟**"، على الرابط:

https://www.maghrebvoices.com/a/algeria-cyber-criminality/414407.html

عبد النور بن عنتر، "**عقيدة الجزائر الأمنية: ضغوطات البيئة الإقليمية ومقتضيات المصالح الأمنية**"، من الرابط:

http://studies.aljazeera.net/ar/reports/2018/05/180502110656159.html

26- فضيلة غاقلي، "**الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري**"، مركز جيل البحث العلمي، على الرابط:

http://jilrc.com.

27- فهد الدريبي، "**ماهو الأمن السيبراني**"، من الرابط:

www.fadvisor.net/blog/2017/11/whatiscyberhack

28- محمود خليل،" **50 ألف موقع الكتروني لداعش ... .والإرهاب يحاصر الانترنيت**"، من الرابط:

.www.alittihad.ae/details.php=120l.

29- مساعد كمال، "**الحروب الإفتراضية وسيناريوهات محاكاة الواقع**"، (لبنان، مجلة الجيش اللبناني(ع: 253، يوليو 2006م)، من الرابط:

www.lebarmy.gov.ib/article.ospfind=11575

30- مصطفى الخلفي، **أزمة العلاقات المغربية الجزائرية ومشكلة الصحراء المغربية .**على الرابط:

http://www.aljazeera.net

31- مليكة خ، "**الإستراتيجية الأمنية للجزائر تعزيز المقاربة التنموية**"، موقع جريدة المساء ، من الرابط: ،

www.el-massa.com/dz

32- وجيه دسوق مرسي، "**الأساليب الالكترونية الحديثة التي تستخدمها التنظيمات الارهابية في الجرائم الارهابية**"، من الرابط: repository.nauss.edu.sa/bitstream/handies/1.pdf،

33- يوسف بن أحمد الرميح، "**الإرهاب في شبكات التواصل الاجتماعي**"، من الرابط،
www.aljazeera.com/ar2.htm

34- يونس بورنان، "**الجزائر24 ألف مختص في الأمن السيبراني لمواجهة الجرائم الالكترونية**"، على الرابط:

https://www.searchnewworld.com.

35- كريم حميد، "القرصنة الإلكترونية"، من الرابط:
https://www.alakah.net/culturel/0/52639/

ثالثا: المراجع باللغة الأجنبية

*1- Dan Craiyen and others, "**Defining cybrescurity**", Technology innovation management review, Montreal, Canada, (october 2014).*

*2- -**Dictionnaire français Le petit Larousse**, (France, Edition, 2001).*

*3- -**English dictionary Oxford dictionaries language**.*

*4- -**What is cyber threat how to explain cyber threat your CEO**, www.threatcomment.com/bloghowtoexplainwahtisacyberthreat*

.