وزارة التعليم العالي والبحث العلمي
Ministry of High Education and Scientific Research
جامعة محمد البشير الإبراهيمي – برج بوعريريج –
University of Mohamed el Bachir el Ibrahimi-Bba
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر مهني في الحقوق

تخصص: قانون إعلام آلي وانترنيت

الموسومة بـ :

الردع الإلكتروني كآلية لمواجهة الحروب السيبرانية

إعداد الطلبة:

- بلموهوب رياض
- قدوج نور الدين

إشراف الدكتور:

بركات مولود

- لجنة المناقشة

الاسم واللقب	الصفة	الرتبة
د/بن يحي بشير	أستاذ محاضر – أ –	رئيسا
د/ بركات مولود	أستاذ محاضر – أ –	مشرفا ومقررا
د/ بن شويحة علي	أستاذ مساعد – أ –	مناقشا وممتحنا

السنة الجامعية 2023/2022

*الملحق بالقرار رقم ....1082.... المؤرخ في ..... 2021 .....
الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،

السيد(ة): بلمحجوبة رياض ..... الصفة: طالب، أستاذ، باحث ..... طالب .....

الحامل(ة) لبطاقة التعريف الوطنية رقم: 180635791 والصادرة بتاريخ 2021/05/03 .....

المسجل(ة) بكلية / معهد ..... الحقوق ..... قسم ..... العلوم السياسية .....

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه)،

عنوانها: ..... الترويع الإرهابي كآلية لمواجهة الحروب السيبرانية .....

.....

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: ..... 25/06/2023 .....

توقيع المعني (ة)

2020 ... 27

*ملحق بالقرار رقم ......1082...... المؤرخ في ....

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،

السيد(ة): ممدوح نور الدين الصفة: طالب، أستاذ، باحث طالب

الحامل(ة) لبطاقة التعريف الوطنية رقم: 80441166.29 والصادرة بتاريخ 2017/05/07

المسجل(ة) بكلية / معهد الحقوق قسم الإعلام الآلي والأنترنت

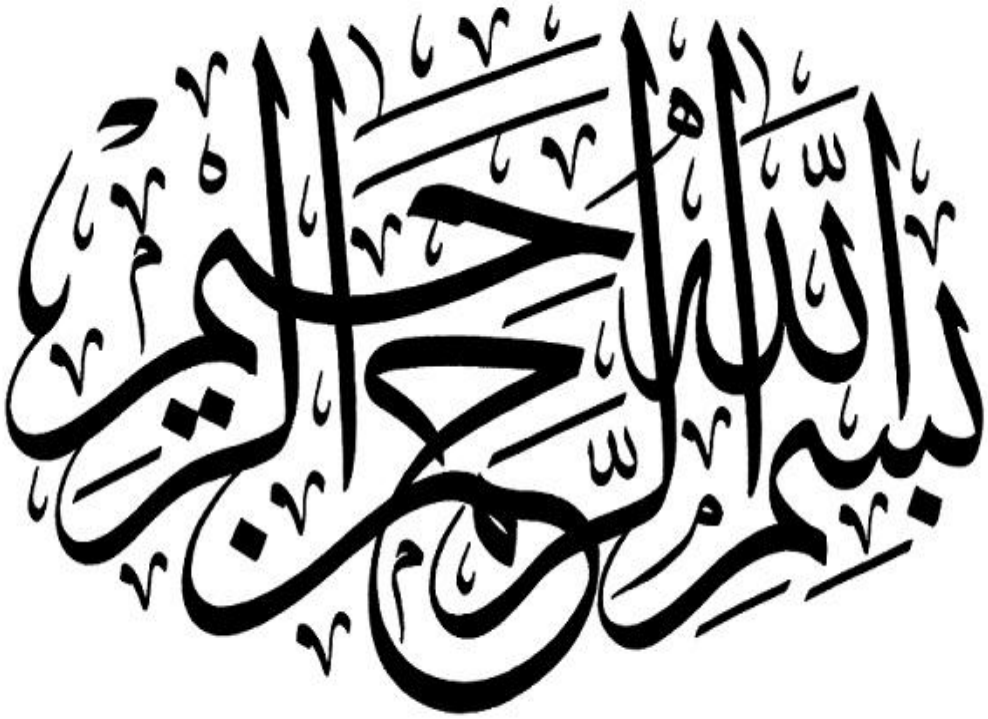
والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه)،

عنوانها: الترويج الإلكتروني كآلية لمواجهة الإرهاب السيبراني

أصرح بشرفي أني، ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: 25/06/2023

توقيع المعني (ة)


بسم الله الرحمن الرحيم

شكر وعرفان

الحمد لله على أنعم وسهل وأرشد فله الحمد كله وله الشكر كله على توصلنا

ومنحنا الصبر ومكننا لإنجاز هذا العمل

وبعد أتقدم بجزيل الشكر ووافر الامتنان والعرفان مع فائق الاحترام

والتقدير للأستاذ المشرف الدكتور: بركات مولود

على قبوله الإشراف على الموضوع، حيث لم يبخل علينا بتوجيهاته ونصائحه

رغم انشغاله وارتباطه ومد لنا يد العون وهو مأجور ومشكور

كما نتقدم بخالص الشكر للجنة المناقشة على قبولهم مناقشة هذا العمل

والشكر موصول إلى الأساتذة الكرام الذين رافقونا خلال المسيرة الدراسية

في قسم الحقوق تخصص إعلام آلي وانترنيت.

إهداء

الى التي أحبتني قبل أن أحبها وأعطتني دون أن أسألها، واحترقت حتى تنير لي الطريق وعلمتني أن الحياة عطاء ،الى رمز الحب ،الى أمي الغالية، الى من جرعة كأسا فرغا لتسقيني قطرة حب، الى من حصد الأشواك عن دربي ليمهد لي الطريق

أبي الغالي رحمه الله وأسكنه فسيح جناته

كما أهدي هذا العمل الى جميع أفراد عائلتي كبيرا وصغيرا

كما أتقدم بإهدائي هذا الى الأستاذ بركات مولود الذي قدم يد العون ولم يبخلنا

إلى كل طلبة قسم الحقوق وبالأخص دفعة 2023/2022 ماستر حقوق تخصص قانون الإعلام الآلي والأنترنيت .

إلى كل من وسعهم قلبي ولم يسعهم قلمي أهدي هذا العمل

• رياض •

إهداء

﴿ وَمَا يُلَقَّاهَا إِلَّا الَّذِينَ صَبَرُوا وَمَا يُلَقَّاهَا إِلَّا ذُو حَظٍّ عَظِيمٍ﴾ فصلت الآية – 35-

الحمد لله كما ينبغي لجلاله وعظيم سلطانه، الحمد لله الذي أنعم وأتم .

أهدي فرحة تخرجي.

إلى تلك الإنسانة العظيمة، قدوتي ومثلي الأعلى في الحياة، التي طالما تمنت أن تقر عينها برؤيتي في يوم كهذا .... أمي.

إلى من كلل جبينه وعلمني أن النجاح لا يأتي إلا بالصبر والإصرار ورفعت رأسي عاليا افتخارا به ..... أبي.

إلى الزوجة العزيزة و فلذتي كبدي" قصي " و" لؤي "

إلى كل من وسعهم قلبي ولم يسعهم قلمي أهدي هذا العمل.

نور الدين

قائمة المختصرات:

الرمز	الكلمة
م	مجلد
ط	طبعة
ق	قانون
ق إ ج	ق الإجراءات الجزائية
د ط	دون طبعة
ع	عدد
ص	صفحة

مقدمة

مقدمة.

لاتعد حرب الفضاء الإلكتروني تعبيرا رديفا للحرب الإلكترونية بمعناها التقليدي المتعارف عليه، بل هي نوع من الحرب يستهدف الشبكات الإلكترونية، التي قد تكون مدنية أو عسكرية. ويعد الفضاء الإلكتروني في وقتنا الراهن البعد الخامس للدفاع، بعد البر والبحر والجو والفضاء وإذا كانت الحرب بمفهومها العام امتحانا شاملا للقوى المادية والمعنوية للدولة، فإن الأمر ليس بالضرورة كذلك في حرب الفضاء الإلكتروني. إنها حرب أدمغة بالدرجة الأولى. وهي قد تنشب بين دولتين أو مجموعة دول. أو بين دولة وجماعة مدنية أو عسكرية. أو حتى بين دولة وبضعة أفراد[1].

هذه الحرب تستهدف على المستوى العملي تدمير شبكات دولة أو هيئة معينة، أو التجسس على محتوياتها، أو تعريضها للعطب أو الحجب أو الخداع.

ويمكن لبرمجيات التجسس المكوث في شبكات الجهة المستهدفة لسنوات طويلة وتجديد نفسها تلقائيا دون أن يشعر بها أحد. وفي فترة الاشتباك العسكري يمكن لحرب الفضاء الإلكتروني شل الاتصالات بين الجيوش وقياداتها، وإضعاف شبكات النقل والإمدادات اللوجستية.

ومن هنا، بدأت حرب الفضاء الإلكتروني تأخذ موقعها المتقدم في حسابات المخططين العسكريين والاستراتيجيين. وتشير التقارير الدولية إلى أنه من بين أكبر 15 جيشا في العالم، هناك اليوم 12 جيشا قام بإنشاء برامج خاصة بحرب الفضاء الإلكتروني.

[1] أنمار موسى جواد، حروب الفضاء الإلكتروني،(مفهوم، الأدوات، التطبيقات)، مجلة العلوم القانونية والسياسية، م 5 ع، الجزائر، جوان 2016، ص 264.

وقبل نحو عقد من الزمن، بدأت كل من الولايات المتحدة والصين وروسيا وبريطانيا وإسرائيل في تطوير قواعد أساسية للهجوم الإلكتروني. بيد أن أيا منها لم يبلور بصورة كاملة كيفية دمج هذه القدرات في العمليات العسكرية[1] .

ورغم عدم البلورة هذه، فإن الأسلحة الإلكترونية سوف تستخدم قبل أو أثناء الصراعات المسلحة، بهدف عطب شبكات العدو الحيوية. وقد تستخدم هذه الأسلحة أيضا في ذروة توتر سياسي أو نزاع تجاري.

وتعود أسباب اختيار هذا الموضوع إلى أسباب ذاتية وأخرى موضوعية ،أما الذاتية فهي الرغبة في معالجة هذا الموضوع والتي شكلت لنا حافزا ودافعا لتناوله بطريقة موضوعية ودقيقة ومتطابقة مع مبادئ وأسس إعداد البحوث الأكاديمية.

أما الموضوعية فهي محاولة إيجاد ربط علمي ممنهج عما هو متوفر حول موضوعنا بما هو موجود في الواقع العملي.

و تكمن أهمية هذه الدراسة في ظل ما تشهده مفاهيم الحرب الإلكترونية والأمن السيبيراني من رواج كبير على المستوى الدولي، حازت تلك المفاهيم على اهتمام كبير من قِبل الباحثين والأكاديميين والسياسيين على حد سواء . ويأتي ذلك الاهتمام استجابة للتهديد المتزايد من الحروب السيبرانية، وتأثيرها على الأمن القومي للدول.

أما الهدف الأساسي لهذا البحث هو دراسة مسألة تطبيق الردع الإلكتروني في المجال السيبراني، وكذلك الهدف من هذه الدراسة هو إثراء المكتبة القانونية المتخصصة في مجال الردع الإلكتروني، وذلك نظرا للنقص الملحوظ في البحوث التي تعنى بشرح هذا الموضوع.

[1] علي عبد الكريم العبودي، هاجس الحروب السيبيرانية وتداعياتها على الأمن والسلم الدوليين، مجلة قضايا السياسية، ع 57، الجزائر، د س ن، ص 105.

الدراسات السابقة.

من أجل فهم وبناء هذه الدراسة تم الاطلاع علي العديد من الدراسات السابقة، التي حاولت الجمع بين متغيرات الدراسة، ومن هذا المنطلق تم محاولة عرض بعض الدراسات التي تتقارب وتشبه موضوع بحثنا:

1: الدراسة الأولي: الدراسة التي قام بها الباحث أمين بولنوار من خلال رسالة ماجستير في العلوم السياسية والعلاقات الدولية، بعنوان الولايات المتحدة الأمريكية ومنطق الهيمنة، كلية العلوم السياسية للإعلام، قسم العلوم السياسية والعلاقات الدولية، جامعة الجزائر، سنة 2009.

2: الدراسة الثانية. التي قام بها الباحث وليد غسان سعيد جلعود من خلال رسالة الماجستير بعنوان دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، تخصص التخطيط والتنمية السياسية، كلية الدراسات العليا، جامعة النجاح الوطنية نابلس، فلسطين، سنة 2012.

تتمحور الإشكالية التي يثيرها موضوع الدراسة فيمايلي:

هل الردع الإلكتروني كاف لمواجهة الحروب السيبيرانية ؟.

إلى أي مدى يمكن للردع الالكتروني أن يضع حدا للحروب السيبرانية ؟.

للإمام بهذه الإشكالية ونظرا لتعقدها وتشعبها ومحاولة منا بجميع أبعاد وتفاصيل هذا الموضوع سلكنا **المنهج الوصفي** من خلال تحديد المفاهيم التي تنطوي عليها الدراسة، كما اعتمدنا على **المنهج التحليلي** المناسب ومقتضيات طبيعة موضوع بحثنا

وللإجابة عن الإشكالية وفق المناهج السابقة ارتأينا تقسيم البحث الي فصلين، نتناول في الفصل الأول الإطار النظري والمفاهيمي للردع الإلكتروني حيث قسم بدوره

الي مبحثين، تضمن المبحث الأول مفهوم الردع الإلكتروني والذي تفرع الي مطلبين،جاء في المطلب الأول التطور التاريخي لمفهوم الردع الإلكتروني، أما المطلب الثاني الاتجاهات الفكرية في تحديد جدوي الردع الإلكتروني، بينما تضمن المبحث الثاني مفهوم الحروب السيبرانية، والذي قسم الي مطلبين، تناولنا في المطلب الأول تعريف الحروب السيبرانية وطبيعتها القانونية، أما المطلب الثاني أنواع الحروب السيبرانية وخصائصها أما بالنسبة للفصل الثاني فيتضمن تحديات تطبيق الردع الإلكتروني وضرورة بلورة استراتيجية شاملة والذي قسم الي مبحثين، تناول المبحث الأول تحديات تطبيق الردع الإلكتروني، والذي تفرع الي مطلبين، في المطلب الأول الردع الإلكتروني بالمنع وتحديات تطبيقه في المطلب الثاني الردع الإلكتروني بالانتقام وتحديات تطبيقه أما المبحث الثاني بلورة استراتيجية شاملة للردع الإلكتروني وقد قسم الي مطلبين كذلك، تناول المطلب الأول الاستراتيجيات المعتمدة علي المستوي الدولي،أما الثاني الاستراتيجيات المعتمدة علي المستوي الداخلي وموقف الجزائر من الردع الإلكتروني.

وأنهينا الدراسة بخاتمة اشتملت علي أهم نتائج البحث وتوصياته.

الفصل الأول:

الإطار النظري والمفاهيمي للردع الالكتروني والحروب السبرانية.

الفصل الأول: الإطار النظري للردع الالكتروني والحروب السيبرانية:

في ظل ما تشهده مفاهيم الحرب الإلكترونية والأمن السيبراني من رواج كبير على المستوى الدولي، حازت تلك المفاهيم على اهتمام كبير من قِبل الباحثين والأكاديميين والسياسيين على حد سواء. ويأتي ذلك الاهتمام استجابة للتهديد المتزايد من الحروب السيبرانية، وتأثيرها على الأمن القومي للدول.

إنه عصر الردع الإلكتروني، هكذا يمكن تعريف الزمن الحاضر من المنظورين العسكري والاستراتيجي. هو عصر جديد في حسابات القوة والردع، ومفاهيم الحرب ذاتها. نحن الآن قد خرجنا للتو من المفهوم التقليدي للردع، الذي تعارف عليه الدارسون منذ عقود خلت. وخرجنا في الوقت نفسه من التقسيم الثلاثي للقوة: التقليدية وما فوق التقليدية والإستراتيجية. نحن اليوم بصدد نوع جديد من الحروب، هو حرب الفضاء الإلكتروني (أو حرب الشبكات)، يصاحبه سباق مستجد للردع، هو الردع الإلكتروني.

حيث سيتم التطرق في هذا الفصل إلى مفهوم الردع الالكتروني (المبحث الأول)، ثم مفهوم الحروب السيبيرانية (المبحث الثاني).

المبحث الأول: مفهوم الردع الالكتروني

أصبحت الهجمات الالكترونية مصدر قلق للأمن القومي وأداة جديدة في السياسة الخارجية تستلزم، التكثيف السريع معها عبر تطوير القدرات العسكرية والاستخباراتية السيبيرانية، وتماشيا مع هذا الوضع الجيوسياسي قامت القوي الكبرى بتكثيف استراتيجياتها العسكرية مع خصائص البيئة السبرانية لأن أمنها سيتحدد ليس فقط من خلال المواجهة على الأصعدة العسكرية والاقتصادية والدبلوماسية.

حيث سيتم التطرق إلى التطور التاريخي لمفهوم الردع الالكتروني (لمطلب الأول)، ثم إلى الاتجاهات الفكرية في تحديد جدوى الردع الالكتروني (المطلب الثاني).

المطلب الأول: التطور التاريخي لمفهوم الردع الالكتروني.

يعرف الردع الالكتروني على أنه "منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية[1]"ويرتكز الردع السيبراني على ثلاثة ركائز هي عماد استراتيجية الدفاع السيبراني، تتمثل في: مصداقية الدفاعCredibleDefense، والقدرة على الانتقامAn Ability to Retaliate، والرغبة في الانتقامA Will to Retaliate

ومع ظهور مفهوم "الدول المارقة"، ظهرت موجة ثالثة من "نظرية الردع"، والتي ارتبطت أيضاً بظهور "فاعلين من غير الدول" وانتشار الإرهابيين، مما يتطلب وجود تدابير وقائية.

حيث مّر مفهوم نظرية الردع بعدة مراحل أو موجات، منها الردع لتجنب الحروب عندما كانت الدول الغربية تمتلك الأسلحة النووية، وبرزت موجة ثانية مع صعود الاتحاد السوفياتي كقوة نووية وما نتج عنه من وجود عالم ثنائي القطبية، ثم مع ظهور مفهوم

[1]Michael Krepon, Space and NuclearDeterrence, In: Michael Krepon& Julia Thompson (Eds.), AntiSatellite Weapons, Deterrence and Sino-AmericanSpace Relations, United -States: Stimson Center, September2013, p. 15

الدول المارقة، ظهرت موجة ثالثة من نظرية الردع، والتي ارتبطت أيضا بظهور فاعلين من غير الدول والحكومات مما تتطلب وجود تدابير وقائية.

وانطلاقاً من ذلك، ونظراً للعواقب الوخيمة التي قد تسببها "الحروب السيبرانية"، وجد بعض الكتَّاب أن ثمة طريقاً لتطبيق نظرية الردع على الفضاء السيبراني، فيما يعرف بالردع السيبراني". وتشير الدراسة في هذا الصدد إلى أن مفهوم "الردع السيبراني" يعتمد على عنصرين هما: ردع الهجمات السيبرانية فيما يُعرف "الردع بالمنع"، والردع بالتهديد بشن هجمات سيبرانية فيما يُعرف بالردع بالانتقام."[1]

ويُميز الباحثان بين "الردع بالمنع" و"الردع بالانتقام"، حيث يصفان "الردع بالانتقام" أو الردع عن طريق العقاب، بأنه مثل القبض على الجاني في قضية ما وصولاً إلى محاكمته، وهو ما يؤثر على سلوك الجاني في المستقبل، وأيضاً على سلوك الآخرين في المجال الجنائي.

أما "الردع بالمنع"، فينطوي تحته "الردع بالمقاومةResistance "، و"الردع بالصمود " Resilience. و الصمود هنا يعني القدرة على استعادة الشيء بشكله الأصلي قبل الهجوم الذي تم، وهذا من شأنه أن يحد المكاسب المحتملة، ويمكن أن يقنع الخصم بعدم الهجوم خاصةً إذا كانت التكلفة مُفرطة. و يظل الهدف من "المقاومة والصمود" هو تقليل خيارات الطرف الذي ينوي الهجوم، سواء من خلال بناء هياكل دفاعية يصعب التغلب عليها أو من خلال ضمان الاستعادة السريعة لأصل الشيء بعد الهجوم.[2]

[1]. شفيق نوران ، أثر التهديدات الإلكترونية علي العلاقات الدولية (دراسة في أبعاد الأمن الإلكتروني)، د.ط، المكتب العربي للمعارف، القاهرة، 2016، ص 33.

[2]. بيتر سينجر، الحرب عن بعد (دور التكنولوجيا في الحرب)، ط 1، مركز الإمارات للدراسات والبحوث الإستراتيجية، الإمارات، 2010، ص 44.

فيما تعود أصول الردع الإلكتروني إلى عملية عاصفة الصحراء، عام 1991، عندما اكتسبت فكرة الثورة في الشؤون العسكرية شعبية كبيرة، فخلال المراحل الأولي من العملية شنت الولايات المتحدة لأمريكية حرب معلومات التي وصفها بيتز بأنها سلاح محتمل بحد ذاته لتتشكل بذلك أولي أدبيات الردع الإلكتروني في الحروب الحديثة.[1]

حيث تعود استراتيجية الردع على الأقل إلى ثيوسيديس والحرب البيوبونيسية، وكان للموضوع نهضة كبيرة خلال الحرب الباردة حيث سعت الولايات المتحدة والاتحاد السوفيتي إلي تجنب صراع نووي.

ويمكن الإشارة إلى واقعة حدثت في عام 1983 ويعتبرها نقطة فاصلة في تطور ترسانة الولايات المتحدة للحرب الإلكترونية التي استخدمتها بشكل فاعل في حرب الخليج عام 1991 ثم في صربيا في أواسط التسعينيات وقبل ذلك ضد الاتحاد السوفيتي السابق في سنين الحرب الباردة.[2]

وتتلخص الحادثة في أن الرئيس الأميركي الراحل رونالد ريجان كان يشاهد فيلم الخيال العلمي "ألعاب الحرب" عام 1983،واستعرض الفيلم قصة فتى يخترق منظومة أحد المؤسسات العسكرية الأمنية بدون أن يعلم، وكاد الفتى أن يشعل حرباً عالمية ثالثة بدون أن يدري، الأمر الذي أقلق ريجان؛ حيث استدعى ريجان في الأيام التالية كبار مساعديه وجنرالات الجيش، وسألهم بشكل مباشر "هل يمكن أن يحدث ذلك فعلا؟" في إشارة إلى قصة الفتى في فيلم "ألعاب الحرب". وبعد أيام جاء الجواب مباشراً وصاعقاً وعليه نتج عن النقاش بين ريجان وكبار مسؤولي الأمن والجيش زوبعة من ورش العمل والدراسات

[1]. حسين قوادري، الردع السيبراني بين النظرية والتطبيق، المجلة الجزائرية للأمن والتنمية ع 16، الجزائر، جانفي 2020، ص 27.

[2]. بيتر سينجر، المرجع السابق، ض 45.

والتحقيقات انبثقت عنها مذكرة لأمن القومي رقم 145 في 17 سبتمبر/أيلول عام 1984 وحملت عنوان "السياسة القومية للأمن الاتصالات وأنظمة المعلومات الأوتوماتيكية".[1]

وتجدر الإشارة إلى أنه في ذلك الوقت كانت الحواسيب المحمولة محدودة الانتشار للغاية، وخدمة الإنترنت لم تكن متاحة للجمهور بعد، إلا أن ذكرت المذكرة تحديداً مخاطر استخدام أجهزة الحاسوب وإمكانية اختراقها وسرقة المعلومات منها من قبل أجهزة استخبارات منافسة أو منظمات "إرهابية."

قد أثارت المهمة الجديدة للوكالة اعتراضات داخل الأجهزة التشريعية الأميركية،حيث إن الوكالة كانت تعمل بعيداً عن الأميركيين وغير مسموح لها التجسس عليهم أو اعتراض اتصالاتهم، وأراد دعاة الحريات المدنية التركيز على أن الخط الفاصل بين عدم التجسس على الأميركيين وتأمين منظوماتهم الإلكترونية هو خط واضح للوكالة.[2]

وأثيرت القضية بعد ذلك في عهد الرئيس الأسبق بيل كلينتون، إلا أنها لم تحتل حيزاً كبيراً حتى جاءت هجمات سبتمبر/أيلول عام 2001 والحرب الأميركية على أفغانستان ثم العراق. حيث كانت الولايات المتحدة منغمسة في حروب تقليدية تستخدم فيها كافة أنواع الأسلحة وكان الجنود الأميركيون يسقطون قتلى كل يوم.

وفي خضم تلك الظروف، كانت الحرب الإلكترونية في ذيل اهتمامات الأميركيين، ولكنها في الوقت ذاته كانت على رأس أولويات إدارة الرئيس الأميركي السابق جورج بوش الابن، حيث كان العمل على هذا النوع من الحروب يجري على قدم وساق خلف أبواب مغلقة،

[1]. حسين قوادري، المرجع السابق، ص 28.

[2]. علاء الدين فرحات، من الردع النووي إلي الردع اليبيراني (دراسة لمدي تحقيق مبدأ الردع في الفضاء السيبراني)، مجلة المفكر، م 16، ع 01، المدرسة الوطنية العليا للعلوم السياسية، الجزائر، 2021، ص 33.

ودأبت المؤسسة العسكرية الأميركية على وضعه في خدمة أهداف المعارك التقليدية على الأرض.[1]

المطلب الثاني: الاتجاهات الفكرية في تحديد جدوي الردع الالكتروني

يمكن تقسيم الاتجاهات الفكرية وفقًا لثلاثة محاور رئيسية، وذلك على النحو التالي:

1: **الاتجاه الأول** :يرى عدم جدوى نظرية الردع على صعيد الفضاء السيبراني، مشككًا في جدواها وفعاليتها، فطبيعة العمليات السيبرانية تُقوض من الدور المحتمل للردع، وقد تجعله عديم الفائدة كليًا. ويركز هذا الاتجاه على الإشكاليات التي تواجه الردع السيبراني، ومنها: صعوبة تحديد هوية مرتكبي الهجمات ابتداءًا، فضلًا عن غياب القوانين اللازمة والرادعة، على نحو يوفر لمرتكبيها الملاذ الآمن، مما يحول دون ملاحقتهم.[2]

2: **الاتجاه الثاني**:يرى أن نظرية الردع لا تنطبق فحسب في المجال السيبراني، لكنها ضرورةً أيضًا؛ فبدون الردع السيبراني، ستظل البيانات المفتوحة عرضة لأشكال بدائية وخطيرة من الاستغلال والاعتداء، ومنها سرقة البيانات، وانتهاك حقوق الملكية الفكرية، وتعطيل الأعمال التجارية، وإيقاف تشغيل النظم الحيوية. ذلك أن الردع السيبري لابد أن يكون جزءًا لا يتجزأ من استراتيجيات الأمن القومي للدول.[3]

---

[1]. شفيق نوران ، المرجع السابق، ص 34.

[2]. إسماعيل صبري مقلد، العلاقات السياسية الدولية، (دراسة في الأصول والنظريات)، المكتبة الأكاديمية، القاهرة:، 2010، ص 29.

[3]. Lotrionte, Catherine, A BetterDefense: Examining the United States New Norms-BasedApproach toCyber Deterrence, Georgetown Journal of International Affairs, 2013, pp. 71-84

الاتجاه الثالث :يرى أن نظرية الردع يمكن أن تتلاءم والفضاء السيبراني، ولكن بشروط وضوابط محددة، منها تبني مفهوم واسع للردع، والمزج بين خيارات عدة في سبيل الوصول إلى استراتيجية متكاملة له، أخذًا في الاعتبار أن الردع في عصر المعلومات يختلف كثيرًا عنه في عصر الحرب الباردة في النوع والنطاق، مما يتطلب نهجًا شاملًا يدمج كل المقومات العسكرية والاقتصادية والاستخباراتية والقانونية، تعزيزًا لأمن المعلومات من ناحية، وخلقًا للردع من ناحية أخرى.[1]

[1]. Kevin R. Beeker, StrategicDeterrence in Cyberspace: Practical Application, GraduateResearch ProjectPresented to the FacultyDepartment of Electrical& Computer Engineering GraduateSchool of Engineeringand Management, Air Force Institute of Technology Air Education and Training Command in Partial Fulfillmentof the Requirements for the Degree of Master of Cyber Warfare, 2009, p. 7; Report on Cyber Deterrence Policy,

المبحث الثاني: مفهوم الحروب السيبرانية

تزداد الهجمات الإلكترونية بفعل الفيروسات وتتضاعف كل يوم ومن بلد إلى بلد آخر، ومن الراجح هو عدم تمكن أغلب تلك الفيروسات من الاختراق، إلا نسبة ضئيلة منها قد تتمكن من الاختراق ومن شأن ذلك أن يحدث آثارا خطيرة، وقد أصبحت تلك الفيروسات، على اختلاف أنواعها، أسلحة حديثة تستخدم في شن هجمات إلكترونية على البنى التحتية الإلكترونية التابعة للدول والمؤسسات المختلفة، وفي أغلب الحالاتلا يدرك الضحايا وجود فيروسات أو ديدان إلكترونيةداخل أنظمة الحوسبة التي يستخدمونها، بل إنهم لن يدركوا ذلك إلا بعد أن يكون قد فات الأوان. وبعض تلك الهجمات يمكن التعافي منه مثل حجب الخدمة، لكن أغلبها تستعصي على العلاج في حالات التجسس، أو حملة التضليل المعلوماتي أو تشويه السمعة وغيرها مما يطلق عليه الحرب السيبرانية.

حيث سيتم التطرق إلي تعريف الحروب السيبرانية وطبيعتها القانونية (المطلب الأول)، ثم إلي أنواع الحروب السبرانية وخصائصها (المطلب الثاني).

المطلب الأول: تعريف الحروب السيبرانية وطبيعتها القانونية

ارتبط مسار الحروب عبر تاريخها الطويل، بالتطورات التقنية التي عرفتها الجماعات البشرية، وسخرتها في سبيل تطوير قدراتها القتالية، وصولا لتحقيق أهدافها، وتأمين مصالحها الحيوية المنشودة من خوض النزاع المسلح، ومع ولوج الحضارة الإنسانية عصر المعلومات والتقنيات الحديثة شهدت ساحات الحروب ظهور جيل جديد من المنظومات القتالية التي اعتمدت على الفضاء السيبراني في إدارة المعارك والتي صارت تعرف بالحرب السيبرانية، ومما تقدم أضحى من الضروري الوقوف على تعريف الحروب السيبرانية (الفرع الأول)، ثم بعد ذلك نتطرق إلى طبيعتها القانونية (الفرع الثاني).

الفرع الأول: تعريف الحروب السيبرانية

ليس هناك إجماع واسع على تعريف محدد ودقيق لمفهوم الحرب السيبرانية حتى الآن، وتكمن المشكلة الأساسية في غياب هذا التعريف إلى الطبيعة القانونية المتغيرة لمصطلحات متطورة ظهرت في الآونةالأخيرة في سياق النزاعات المسلحة، مثل الهجمات السيبرانية عن طريق الشبكة العنكبوتية من جهة، وحداثة الهجماتعلى شبكات الحواسيب التي تعد ظاهرة حديثة من جهة أخرى.[1]

وعلى الرغم من غياب إجماع واسع على تعريف محدد ودقيق لمفهوم الحرب السيبرانية، إلا أن ذلك لم يمنع الفقهاء كل في تخصصه من تقديم تعاريف للإحاطة بهذا المفهوم، ومن تلك التعاريف ما ذهب إليها خبراء ومختصين في القانون الدولي الإنساني، وأولهم الأستاذSHINالذي عرف الحرب السيبرانية بأنها: "استخداملطيف الإلكتروني أو

[1]. إيهاب خليفة، الحرب السيبرانية، الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، د.ط، العربي للنشر والتوزيع، القاهرة، 2021. ص 8.

الكهرومغناطيسي لتخزين وتعديل وتبادل البيانات وجها لوجه مع أنظمة تحكم في بنتحتية مرتبطة بها".[1]

وعرف الأستاذ ميشال الحرب السيبرانية بأنها: "مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية بهدف التأثير والإضرار بها، وفي الوقت نفسه للدفاع عن نظمالمعلومات الخاصة بالدولة المهاجمة".[2]

كما عرفها الأستاذ ريتشارد كلارك والأستاذ "روبرت كناكي" على أنها: " أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أوتعطيلها".[3]

ويعتبر آخرون أن الحرب السيبرانية هي:" امتداد للحروب التقليدية والمادية، إذ يتألف جندها من المدنيين والعسكريين في آن واحد، كما أنها حرب أدمغة بالدرجة الأولى، كونها تستهدف في المقام الأول تدمير البنية العلمية والمعلوماتية للهدف، وتأخذ أشكال عدة، كشكل الاتصالات بين الجيوش وقياداتها، وإضعاف شبكاتالنقل والإمدادات اللوجستية، وضرب المعلومات الاقتصادية، والعبث بالمحتوى التقني والرقمي وغيرها".[4]

وهناك من يربط مفهوم الحرب السيبرانية ببيئة الإنترنت فقط، كونها ساعدت على انتشار المعلومات في مختلف أرجاء المعمورة وسهلت الوصول إليها بشكل سريع. ويتم تعريف

---

[1]. أحمد عبيس نعمة الفتلاوي، "الهجمات السيبرانية:، (مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر)، مجلة المحقق الحلي للعلوم القانونية والسياسية، ع 4، الجزائر، ،2016 ص .616.

[2]. يحيى ياسين سعود، "الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني"، م4 ،ع 4، الجزائر، 2008، ص .84

[3]. يحيى مفرح الزهراني، "الأبعاد الاستراتيجية والقانونية للحرب السيبرانية"، مجلة البحوث والدراسات، ع 23، الجزائر، 2007، ص .235

[4]. حكيم غريب، صبرينة شرقي، تداعيات الحرب الإلكترونية على العالقات الدولية: (دراسة في الهجوم الإلكتروني على إيران) فيروس ستكنست")، دفاتر السياسة والقانون، م 12، ع 2، الجزائر، 2020، ص .96.

الحرب السيبرانية بناء على ذلك بأنها" :الحرب التي تستهدف المعلومات. وهي تعبير عن الاعتداءات التي تطال مواقع البيانات الموجودة على الإنترنيت، وتحاول الاستيلاء على معطياتها، بين أطراف متناقضة الأهداف، ومتعارضة المصالح، ومختلفة المواقف".[1]

ويرى بعض القانونيين أن أساليب عمل الحروب السيبرانية تتقارب من ناحية قانونية مع إشاعة الرعب والإرهاب، لذلك يمكن تعريف الحروب السيبرانية استنادا لهذه النظرة القانونية بأنها: " نظام قائم على الرعب المنتشر في شبكة الإنترنت، والتي تهدف إلى تنفيذ العديد من الأعمال لترويع أمن الأفراد والجماعات والمؤسسات والدول، وإدخالهم في أزمات نفسية واقتصادية وسياسية واجتماعية ناتجة عما يعرف بالإرهاب الصامت".[2]

ومن التعاريف الحديثة للحرب السيبرانية نذكر تعريف مجموعة الخبراء التابعين للناتو الوارد في القاعدة 30 دليل تالين المتعلق بتطبيقات القانون الدولي في مجالات الصراع والحروب السيبرانية[3] تنص على أنها:" كل العمليات السيبرانية سواء كانت دفاعية أو

[1]. وليد غسان سعيد جلعود، دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، رسالة ماجستير، تخصص: التخطيط والتنمية السياسية، كلية الدراسات العليا، جامعة النجاح الوطنية نابلس، فلسطين، 2013/2012، ص 82.

[2]. حكيم غريب، صبرينة شرقي، المرجع السابق، ص .96

[3] .Une vingtaine d'experts juristes internationaux dont les nationalités sont représentatives des nations membres de l'Otan a tenté une première analyse de l'interprétation des normes de droit international aux attaques cybernétiques. En s'appuyant ainsi sur le droit international préexistant notamment dans le domaine des conflits armés, du droit de l'espace, de la mer et de l'air, certaines règles applicables ont été étendues aux activités cyber. Cette première analyse constitue ainsi le socle futur de potentielles nouvelles normes juridiques internationales du cyberespace. Cette initiative, lancée au sein du Centre de cyberdéfense de l'Otan (CCD-CoE) situé à Tallinn en Estonie, est tout à fait innovante. Pendant trois ans, les experts ont travaillé sous la direction du professeur Michael Schmitt de l'US Naval WarCollege à la création d'un manuel de droit applicable à la cyberguerre, appelé communément Manuel de Tallinn (2013). Voir, Oriane BARAT- GINIES, "Existe-t-il un droit international du cyberespace ? ", La Découverte, n° 152-153, 2014/1, p. 202.

هجومية، والتي يعتقد أنها قد تسبب إصابات أو وفيات للبشر، أو تلف وضرر للأشياء المادية".[1]

الفرع الثاني: الطبيعة القانونية للحروب السيبرانية

أن البحث في امكانية تطبيق قواعد القانون الدولي الإنساني على الحرب السيبرانية التكييف القانوني لتلك المسألة من حيث شرعية وعدم شرعية الحرب السيبيرانية قد يستلزم في ضوء استخدام القوة في العلاقات الدولية، فالعلاقة بين حق اللجوء إلى الحرب وقانون الحرب تتسم بأنها علاقة توتر لابد منه، فالقواعد المعاصرة للقانون الدولي تحظر استخدام القوة، باستثناء حق الدول فرادى أو جماعات في الدفاع عن نفسها، أو بمقتضى استخدام تدابير انفاذ القانون التي يتخذها مجلس الأمن[2]، إما قانون الحرب فهدفه التوفيق بين ضرورات الحرب وقوانين الإنسانية من خلال فرض قيود واضحة على سير العمليات العسكرية، وبخالف ما تم الإشارة إليه، فأن استخدام القوة في العلاقات الدولية يعد عملا غير مشروع وفقاً لميثاق الأمم المتحدة حيث نص على ما يلي: (يمتنع أعضاء المنظمة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو أي وجه آخر لا يتفق ومقاصد الأمم المتحدة).[3]

هنا يثار التساؤل حول تفسير مصطلح (القوة) بين المقصود بهذا المصطلح، هو استخدام القوة المسلحة في إطار عدوان أو هجوم مسلح ترتكبه الدول باستخدام قواتها المسلحة أو

[1]. سعيد درويش، "الحروب السبرانية وأثرها على حقوق الإنسان: (دراسة على ضوء أحكام دليل " تالين"")، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، م 54، ع 5، الجزائر،2017، ص 181.

[2]. عمرو رضا بيومي، مخاطر اسلحة الدمار الشامل الإسرائيلية على الأمن القومي العربي، ط9، دار النهضة العربية، د.ب .ن، 2002، ص.25.

[3]. يحيى ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية) ، ع 2، مصر، 2020، ص 86.

جماعات منظمة تابعة لها أو مسندة من قبلها[1]، وبين من يرى انه ليس هناك سبب قانوني يدعو إلى اقتصار مفهوم القوة على القوة المسلحة فقط، بل يمكن أن يشمل الضغط الاقتصادي أو السياسي كذلك.[2]

والحقيقة أن الأخذ بالمعيار الأول المعتمد على العنصر الحركي للقوات المسلحة لا يستقيم والكثير من الاستخدامات للقوة أثناء الحروب، وبغض النظر عن مشروعية تلك الحرب من عدمها ومنها الهجمات البيولوجية والجرثومية وكذلك الهجمات السيبرانية مدار بحثنا، كما أن الاعتماد على المعيار الثاني قد يوسع كثير من مفهوم استخدام القوة والتهديد بها ليشمل الإكراه الاقتصادي والسياسي، وقد يخالف المقصود بما ورد في ميثاق الأمم المتحدة من مقاصد وفقاً لرأي اغلبية الفقهاء كونه يوسع من مفهوم العدوان بما يعطي مسوغاً الاستخدام القوة المضادة استناد الحق الدفاع الشرعي.[3]

على أن هناك من يذهب بخلاف الاتجاهين السابقين في تحديد المقصود بالقوة، لتشمل كافة صور استخدام القوة المسلحة، بالإضافة إلى صور أخرى يترتب عليها انتهاك أو تأثير واضح على الأمن القومي لدولة أخرى.[4]

وفي ضوء ما تقدم، فأن هناك مجموعة من الأطر التفسيرية المرتبطة بالحرب السيبرانية، منها ما يتعلق بمفهوم القوة، حيث لعب الفضاء الإلكترونيدورا اساسياً في تعظيمها والاستحواذ على عناصرها الأساسية في العلاقات الدولية، حيث اصبح التفوق في ذلك المجال عنصرا حيوياً في تنفيذ عمليات ذات فعالية على الأرض والبحر والجو والفضاء الخارجي من خلال اعتماد القدرة القتالية في الفضاء الإلكتروني على نظم التحكم

[1]. هشام بشير، المدخل للقانون الدولي الإنساني، ط، 1، المركز القومي للإصدارات القومية، القاهرة، 2012، ص 89.

[2]. عمرو رضا بيومي، المرجع السابق، ص 26.

[3]. سعيد درويش، المرجع السابق، ص 182.

[4]. هشام بشير، المرجع السابق، ص 90.

والسيطرة التكنلوجية، وهذا الأمر يستدعي بالضرورة تغير في مفهوم القوة حيث بات بالإمكان تعريفها بأنها: " مجموعة الوسائل والطاقات والإمكانيات المادية وغير المادية المنظورة وغير المنظورة التي بحوزة الدولة ويستخدمها صانع القرار في فعلمؤثر يحقق مصالح الدولة وتؤثر في سلوك الوحدات السياسية الأخرى".[1]

ومن هنا فأن عناصر القوة وفقاً للمنظور السابق يتمثل في التناغم بين القدرات التكنلوجية والسكانية والاقتصادية والصناعية والقوة العسكرية وارادة الدولة وغيرها مما يسهم في دعم امكانات الدولة على ممارسة الإكراه أو االإقناع أو ممارسة التأثير السياسي في أعمال الدول الأخرى بغرض الوصول للأهداف، سواء اكانت تلك الأهداف مشروعة متى ما توافقت مع القواعد القانونية، ومنها القواعد القانونية الدولية، أو غير مشروعة وما يستتبعه من مخالفة لقواعد القانون الدولي التي اوجبت على الجماعة الدولية من الامتناع في استخدام القوة أو التهديد بها في علاقاتهم الدولية، وبالتالي فأن التغير في مفهوم القوة يؤدي بالضرورة إلى تغير في منظور الحرب، حيث انتقلت من نسق الحروب التقليدية القائمة على تدمير الخصم أو احتلال ارضه أو الاستيلاء على موارده، إلى حروب تعمل للاستحواذ على سباق التقدم التكنلوجي وسرقة الأسرارالاقتصادية والعلمية والتحكم بالمعلومات والعمل على اختراق الأمن القومي بدونطائرات أو متفجرات، أو حتى انتهاك الحدود وتدمير مواقع التجسس والتي قد يكون لها تأثير يفوق الحرب التقليدية لما تشكله من آثار مدمرة على الاقتصاد والبنية التحتية.[2]

[1]. يحيى ياسين سعود، المرجع السابق، ص 87.

[2]. عمر بن عبد الله بن سعيد البلوشي، مشروعية اسلحة الدمار الشامل وفقاً لقواعد القانون الدولي، د.ط، منشورات الحلبي الحقوقية، بيروت، 2007، ص 33.

وإذا تبين لنا فيما تقدم أن مفهوم القوة في إطار الحرب السيبرانية له مدلولاته عن مفهومها التقليدي وفقاً لما قصده واضعي ميثاق الأمم المتحدة[1]، فأن هناك اطار تفسيري آخر مرتبط في أن استخدام القوة بصورة غير مشروعة، انما يتمثل بمعيار استخدام القوة المسلحة بالإضافة إلى انتهاك الأمن القومي لدولة أخرى، وفي ضوء انماط متعددة للحروب السيبرانية في كون جميع درجاتها يمكن أن تشكل استخدام غير مشروع للقوة؟ فقد يتم استخدام الفضاء الإلكتروني كساحة لصراع منخفض الشدة من خلال التأثير على النواحي الاقتصادية أو الثقافية أو الاجتماعية، وهي لا تتطور بالضرورة إلى استخدام الفضاء الإلكتروني كقوة مسلحة أو شن حرب الكترونية واسعة النطاق، حيث يمكن أن تتجسد تلك الصراعات بوسائل عدة، منها الحرب النفسية والاختراقات المتعددة والتجسس وسرقة المعلومات وشن حرب الأفكار وغيرها، ومثال ذلك ما تعرضت له روسيا من اتهام بالقرصنة الإلكترونية في الانتخاباتالأمريكية لدعم المرشح الجمهوري دونالد ترامب في مواجهة منافسته الديمقراطية هيلاري كلنتون.[2]

وهناك نمط آخر من الحروب السيبرانية يتمثل في تحويل الصراع عبر الفضاء الإلكتروني كساحة موازية أو مرافقة أو مرتبطة لحرب تقليدية دائرة على الأرض، ومنها ما تعرضت له سوريا في 2007/12/6 لهجمة سيبرانية على دفاعاتها الجوية في إحدى المنشئات التي يشتبه في انها منشأة نووية في مدينة دير الزور من قبل اسرائيل، مما ادى إلى

[1]. هشام بشير، المرجع السابق، ص 91.

[2]. افادات وكالة الاستخبارات الأمريكية بتدخل روسيا في الانتخابات الرئاسية الأمريكية لدعم (دونالد ترامب)، وان روسيا وراء الهجمات الإلكترونية والقرصنة المعلوماتية التي طالت حسابات البريد الإلكتروني لمرشحة الحزب الديمقراطي (هيلاري كلنتون) – 2018/8/10،الموقع الإلكتروني www.SaSapost.com .

تعطيل هذه الدفاعات لتمكين الطائرات الإسرائيلية من قصف هذا الموقع دون أن يتم الكشف عن الهجوم.[1]

ونمط ثالث يعبر عنه في نشوء حروب في الفضاء الإلكتروني بصورة منفردة، وإذا لم يشهد العالم هكذا نوع من الحروب وفقاً لآثارها المدمرة من خلال اختراق العمليات العسكرية عالية التقنية أو استهداف الحياة المدنية والبنية التحتية بالشكل الذي يمكن تصوره إلا أن هناك نماذج لتلك الحروب تتمثل على شكل رسائل تهديد مصحوبة بآثار محدودة جراء تلك الهجمات، ومنها ما تعرضت له جمهورية استونيا عام2007من هجومسيبراني مستقل بذاته موجه من روسيا الاتحادية وذلك عن طريق اغراق المواقع الإلكترونية بسيل من البيانات غير اللازمة، حيث وجهت ما يقارب من مليون حاسبة من عدة نقاط في العالم، واستهدفت المواقع الحكومية والصحف والجامعات والمستشفيات والمصارف وخدمات الإطفاء والإسعاف وذلك بهدف اسقاط وشل الحكومة الإستونية.[2]

المطلب الثاني: أنواع الحروب السبرانية وخصائصها

تعتبر الحرب السيبرانية من أهم وأخطر أنواع الحروب فب العصر الحالي، خصوصاً مع تطور وسائل الاتصال التكنولوجية، واقتحامها لكل ميادين حياة الشعوب والأفراد. فباتت جزءاً لا يتجزأ بل يتحكم، في كل مجالات القطاعين العام والخاص في الدول، في المنازل ووسائل النقل وخدمات البنية التحتية والقطاع الصحي، وصولاً الى قطاعات توليد الكهرباء والطاقة، هذه الأهمية الوظيفية، دفعت بأغلب دول العالم، الى وضع سياسات عسكرية وامنية، تلحظ هذا المجال من الحروب، عبر وضع خطط دفاعية وهجومية،

[1]. Heather Harrison Dinniss, The status and use of computer network attacks in international law, Phdthesis, London school of a economics and Political science, 2008, P 33

[2]. عمر بن عبد الله بن سعيد البلوشي، المرجع السابق، ص 34.

تؤمن هدف ردع الأعداء من تنفيذ أي هجوم على مصالحها، عبر التهديد بشن عمليات هجومية عليهم في حال اندلاع هكذا صدام.

حيث سيتم التطرق إلى أنواع الحروب السبرانية (الفرع الأول)، ثم إلي خصائصها (الفرع الثاني).

الفرع الأول: أنواع الحروب السيبرانية

تزداد الهجمات الإلكترونية بفعل الفيروسات وتتضاعف كل يوم ومن بلد إلى بلد آخر، ومن الراجح هو عدم تمّكن أغلب تلك الفيروسات من الاختراق، إلا أن نسبة ضئيلة منها قد تتمكن من الاختراق، ومن شأن ذلك أن يحدث آثارا خطيرة، وقد أصبحت تلك الفيروسات، على اختلاف أنواعها، أسلحة حديثة تستخدم في شن هجمات إلكترونية على البنى التحتية الإلكترونية التابعة للدول والمؤسسات المختلفة، وفي أغلب الحالاتلا يدرك الضحايا وجود فيروسات أو ديدان إلكترونيةداخل أنظمة الحوسبة التي يستخدمونها، بل إنهم لن يدركوا ذلك إلا بعد أن يكون قد فات الأوان. وبعض تلك الهجمات يمكن التعافي منه مثل حجب الخدمة، لكن أغلبها تستعصي على العلاج في حالات التجسس، أو حملة التضليل المعلوماتي أو تشويه السمعة وغيرها مما يطلق عليه الحرب السيبرانية[1] التي تتنوع حيث درجة الشدة، وإمكانية التنبؤ بالأزمات الناجمة عنها وأهم هذه الأنواع:

أولا: الحرب السيبرانية الباردة منخفضة الشدة

ويعبر هذا النوع عن صراع مستمر بين الفاعلين المتنازعين، وقد تكون ذات طبيعة ممتدة ذات بعد تاريخي وديني وإيديولوجي ممتد، كأن تكون امتدادا أو جزءا من الصراعات التقليدية الممتدة (الصراع العربي الإسرائيلي، الصراع الإيرانيالأمريكي، الصراع بين

[1]. محمدبكرارشوش، إستعدادات الجزائر لمقتضيات حروب الجيل الرابع بين الواقع والآفاق، دفاتر السياسة والقانون، م 13، ع 03، جامعة قاصدي مرباح ورقلة، الجزائر، 2021، ص 426.

الكوريتين). وخلالها عادة ما يتم اللجوء إلى القوة الناعمة التي تجمع بين الجيلين الرابع والخامس للحرب، حيث تشمل وسائل عدة، مثل الحروب النفسية وحرب الأفكار. ويستخدم هذا النوع من الحرب السيبرانية أساليب خلق الأزمات السياسية لإثارةالاضطرابات وإثارة الرأي العام ضد الدولة، وبث الإشاعاتللإضراربالاقتصاد القومي، وخلق مناخ غير آمن للاستثمار، وغيرها. وقد شهدنا نماذج منها مع بدء تنفيذ استراتيجية الفوضى الخلاقة عام 2011.[1]

ثانيا: الحرب السيبرانية متوسطة الشدة

ويبرز هذا النوع عند تحول الصراع عبر الفضاء إلى ساحة موازية لحرب تقليدية دائرة على الأرض .وينجم عن العمليات مجموعة متداخلة من الأزمات التقليدية، وهي ليست في حاجة إلى سيناريوهات أو بدائل كما في الأزمات السياسية، الأمر يتوقف على القدرات السيبرانية، وامتلاك برامج قادرة على الردع الإيجابي أو الهجوم المحدود أو الشامل، وينجم عنها بعض الأزمات نتيجة عدم القدرة والسيطرة على إدارة الشبكات، ومنها اختراق المواقع الإلكترونية، وسرقة المعلومات وتخريبها، وعرقلة شبكات الطاقة الكهربائية أو شبكات الطرق والمواصلات البرية والسكك الحديدية والطيران، وشبكات البنوك، وإدارة المفاعلات النووية. وشهد العالم بعض نماذج هذا النوع خلال الحرب بين روسيا وجورجيا 2008، وأمريكا وإيران 2010.[2]

ثالثا: الحرب السيبرانية مرتفعة الشدة وأزماتها الكارثية

ويعبر ذلك النوع عن نشوء حروب في الفضاء الإلكترونيمنفردة، وهي غير متوازية مع الأعمال العسكرية التقليدية. ولم يشهد العالم هذا النوع من الحروب، وإن كانت احتمالات

[1]. بوغرارة، الأمن السيبراني، مجلة الدراسات الإفريقية وحوض النيل، م 1، ع 3، الجزائر، سبتمبر 2018، ص ص 100 – 119.

[2]. محمدبكرارشوش، المرجع السابق، ص 427.

حدوثها واردة في المستقبل مع تطور القدرات التكنولوجية وزيادة الاعتماد عليها، وينطوي هذا النوع من الحروب على سيطرة البعد التكنولوجي على إدارة العمليات العسكرية، حيث يتم استخدام الأسلحةالإلكترونية فقط ضد منشآت العدو، والاستحواذ على القوة الإلكترونية. والهدف من وراء ذلك تحقيق الهيمنة الإلكترونية الواسعة بشكل أسرع ويرى بعض الخبراء شن إسرائيل هجمات فيروس ستاكسنت ضد المنشآت النووية الإيرانية بالتعاون مع الولايات المتحدة في عام 2010 نموذجا تقريبيا لهذا النوع من العمليات.[1]

الفرع الثاني: خصائص الحروب السبرانية

على الرغم من أن الحروب السيبرانية تتقاطع مع الحروب التقليدية في المبادئ والأهداف إلا أنها تكتسي طابعا خاصا بها من حيث أساليب القتال والمواجهة، هذه الخصائص يمكن إجمالها في النقاط التالية:

_تثير الحرب السيبرية عدة صعوبات وإشكالات قانونية تجعل تطبيق القانون الدولي الإنساني أمرا صعبا، ومن أبرز هذه الإشكالات أن تشن الحرب السيبرية ضمننزاع مسلح، أي ضرورة وجود نزاع مسلح سواء كان دولي أم غير دولي،حيث أن الممارسة الدولية أثبتت أن الدولتنفذ الهجمات السيبرية بمعزل عن النزاع المسلح[2].

_تشن الحرب السيبرانية في الفضاء السيبريالإلكتروني، الذي لا يعترف بالحدود الدولية، فبالرغم من أن القاعدة 21 من دليل "تالين" الخاصة بالحدود الجغرافية، تنص على أن العمليات السيبرية تتم ضمن الحدود الجغرافية المنصوص عليها في القانون الدولي الإنساني، إلا أنه من الصعب تطبيق هذه القاعدة على أرض الواقع.

[1]. بوغرارة، المرجع السابق، ص 120.

[2]. تناول دليل " تالين"(tallinde Manuel)هذا التقسيم في القاعدتين 22 و.23.

ونتيجة لذلك، فإن القتال بصورته الكلاسيكية، لا يمكن أن يجري إلا في مناطق معينة، ويميز بعض الفقهاء مثل Oppenheimفي هذا الصدد، بين المنطقة الحربية وهي المجال الذي يستطيع فيه المحاربون اعداد القتال وإنجازه، وبين ساحة الحرب وهي المكان الذي يجري فيه القتال فعليا.[1]

وعلاوة على ما سبق، وإجابة عن سؤال حول التحديات الأساسية التي تثيرها الحرب السيبرانية، أوضح المستشار القانوني للجنة الدولية للصليب الأحمر، بأنه يوجد فضاء إلكتروني واحد فقط تتقاسمه القوات المسلحة مع المستخدمينالمدنيين، وكل شيء فيه متشابك ومترابط. وتتمثل التحديات الرئيسية في ضمان توجيه الهجمات ضد الأهداف العسكرية فقط، وتوخي الحرص بشكل مستمر لحقن دماء السكان المدنيين والبنية التحتية المدنية.[2]

_كما تتميز الحرب السيبرية بنوعية الأسلحة التي يمكن استخدامها في القتال الإلكتروني، وفي هذا الصدد عرف دليل " تالين " في القاعدة رقم 41 الأسلحةالسيبرية، إذ صنف وسائل وطرق الحرب، بأنها تشمل من بين أمور أخرى: أسلحةوأساليب الحرب السيبريةالأخرى ذات الصلة، كالفيروسات والبرامج الخبيثة وأنظمة التجسس الإلكتروني...الخ. إضافة إلى مسألة المقاتل في الحرب الإلكترونيةوهل يمكن اعتبار القراصنة مقاتلين يمكن استهدافهم من قبل أطراف النزاع.[3]

---

[1]. شارل روسو، القانون الدولي العام، الأهلية للنشر والتوزيع، ترجمة شكر الله خليفة، عبد المحسن سعد، لبنان، 1987، ص 347.

[2]. اللجنة الدولية للصليب الأحمر، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟ الأسئلة الشائعة،، مقابلة مع السيد »لوران جيزيل« المستشار القانوني باللجنة الدولية للصليب الأحمر بتاريخ 2013/06/28، متاحة على الرابط التالي: resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm/ara/org.icrc.www://h أخر زيارة للموقع بتاريخ 12/ماي/ 2023، علي الساعة : 21 سا و38 د

[3]. شارل روسو، المرجع السابق، ص 348.

-الحرب السيبرانية هي استخدام الهجمات الرقمية لمهاجمة أصول دولة وكيان ما، ما يتسبب له في ضرر مادي مماثل لما يحصل في الحرب الفعلية، أو تعطيل أنظمة الكمبيوتر الحيوية.

_هناك العديد من الدول التي تهتم وتسعى لبناء قدراتها في هذا المجال، مثل الولايات المتحدة الأمريكية وبريطانيا وروسيا والصين وإيران وكوريا الشمالية وكيان الاحتلال الإسرائيلي.

__كما أن هنالك العديد من حركات وفصائل المقاومة التي بات لديها قدرات إلكترونية نشطة من أجل تنفيذ العمليات الهجومية والدفاعية. وتدعي إسرائيل أنها نفذت أول عمل عسكري ضد مركز سيبراني تابع للمقاومة الفلسطينية، في أيار من العام 2019، حيث أغارت عليه ودمرته.

-يمكن أن تشكل الحرب السيبرانية طرف دعم في الحرب التقليدية. على سبيل المثال، من خلال الهجوم على منشآت الرادار ومنظومات الدفاع الجوي وتعطيلها، ما يسمح لأذرع السلاح الجوي من تنفيذ عمليات قصف من دون التعرض لأي تصدي.[1]

-كما تساعد هذه الحرب كثيراً في الحروب الاستخباراتية المتنوعة، خصوصاً في هذا العصر الذي يتركز على جمع المعلومات والـ "Big Data". كما يسمح باكتشاف العديد من المعلومات الحساسة للدول والمنظمات.

وأكبر مثال على ذلك، ما استطاعت القيام به عدد من فصائل المقاومة الفلسطينية، من اختراق لأجهزة تخزين لملفات المعلومات الشخصية عن الضباط والجنود في جيش الاحتلال الإسرائيلي، والتمكن من الاستحواذ عليها ونشرها.

[1]. شارل روسو، المرجع السابق، ص 348.

_كما تساعد هذه الحرب في تنفيذ تكتيكات الحروب الناعمة والدعاية والبروبغندا، وضرب الروح المعنوية للأطراف المقابلة.[1]

_الحرب الرقمية هي حرب تقنية متطورة فباعتبار محورها هو شبكة الإنترنت بما تمتاز به من تطور مستمر وتنوع وابتكار في وسائلها وتقنياتها كما أنها ترتبط بالمصالح الحيوية للدول.

_تتميز بالسرعة وبإمكانية المراوغة والتي تعطي المهاجم أفضلية واضحة على المدافع.

_حرب غير محددة الأهداف والتأثير إذ قد تتعدى مخاطرها ميادين القتال التقليدية لتمس أكثر المواقع السيادية والحساسة تحصينا وبعيدا عن دائرة القتال.

_4-فشل نماذج الردع المعروفة كون الهجمات الإلكترونية في الغالب لا تترك أثرا أو دليلا على حصولها، كما أن الدمار الذي تخلفها الحروب السيبرانية قد يتضمن التجسس والتسلل والنسف بدون أي دماء أو أنقاض فضلا على أن أطرافه غير واضحة وتداعياته خطيرة من خلال تدمير المواقع على الإنترنت وقصفها بوابل من الفيروسات ونسفها كما أن سعة هذا الفضاء قد تسمح بزيادة عدد المهاجمين وامتداد الصراع في الزمان والمكان.[2]

وبالنسبة للفاعلين بهذا الفضاء. فيمكن أن تكون الدول والحكومات،الشركات متعددة الجنسيات، الجماعات الإرهابية، الفرد، الجماعات الاحتجاجية المنتشرة في العالم مثل Wikileaksتعمل في السياسة وهي جماعات تنتمي المنظمات غير حكومية وتقوم بنشر ملفات سرية عن الحكومات تحتوي معلومات حساسة ومهمة بدون ذكر هويتهم مجموعة

[1] محمدبكرارشوش، المرجع السابق، ص 429.

[2]. علي عبد الرحيم العبودي ،هاجس الحروب السيبرانية وتداعياتها علي الأمن والسلم الدوليين ،المجلة الأكاديمية العلمية، م 57، ع 2، ،كلية العلوم السياسية، جامعة النهرين بغداد، ،العراق،2019، ص 99.

مخترقين غير معروفي الهوية يدعون أنهم مجموعة دولية من كل دول العالم وقد قاموا بعدة هجمات ضد مواقع حساسة وأمنية للدول والحكومات مثل اختراقهم لمواقع الشرطة الأمريكية وتهديدها بفضح ملفات سرية.[1]

وعليه فإن خصوصية هذه الحروب تتصل بخصوصية الفضاء السيبراني من سرعة وسهولة ولا محدودية في الانتشار، فضلا على سريتها وصعوبة تتبعها أو الحصول على أدلة إثبات الأفعال المدمرة التي تخلفها وهذا الطابع غير المادي هو ما جعل التهديد أكبر وأكثر رعبا وإخلال بالعلاقات الدولية وجعل المتحكم في هذا الفضاء هو الطرف الأقوى ولو امتلك الآخر جيوشا قوية ،كل هذا تطلب إيجاد حلول فعالة من الدول تناسب هذا النمط من الحروب فاتجهت نحو تكريس أمنها السيبراني كمفهوم حديث للأمن والسلم الدوليين، وهو ما سنتناوله بالشرح والتفصيل.[2]

[1]. جيلالي شويرب ، دمراد فائزة، مفهوم الحروب السيبرانية والأمن السيبراني، مجلة الحقوق والحريات، م 11، ع 1، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي الأغواط، الجزائر، 2023، ص 164.

[2]. علي عبد الرحيم العبودي، المرجع السابق، ص 100.

الفصل الثاني:

تحديات تطبيق الردع الالكتروني وضرورة بلورة استراتيجية شاملة لمواجهة الحروب السيبيرانية .

الفصل الثاني: تحديات تطبيق الردع الالكتروني وضرورة بلورة استراتيجية شاملة

يهدف الردع إلى خلق مجموعة من المحفزات المانعة لقيام أحد أطراف الصراع من القيام باعتداء أو هجوم مستقبلا، وإذا كان ذلك هو هدف الردع في التفاعلات الدولية على أرض الواقع، فإنه مختلف جزئيا عن حالة الردع الإلكتروني، لأن أحد الفواعل غير قادر على إزالة تدمير الطرف الآخر كليا منا في حالة الردع النووي مثلا، كما أنه ليس من السهل تحقيق الردع الإلكتروني بسبب خاصية التخفي، والتي تمنع مستخدم القوة الإلكترونية من التعرف على خصمه أو التوقع من أين سوف تأتيه الضربة، وفي ظل نظام دولي يتميز بتعدد القطبية ما يزيد من حالات الصراع، فضلا عن تعدد الفاعلين من الدول وغير الدول الذين يستخدمون فضاء القوة السيبرانية في التفاعلات الدولية، بالإضافة إلى خاصية التخفي فإن احتمالات الصراع الدولي تزداد مع التقدم التقني.

حيث سيتم التطرق إلى تحديات تطبيق الردع الإلكتروني (المبحث الأول)، ثم إلى بلورة استراتيجية شاملة للردع الالكتروني (المبحث الثاني).

المبحث الأول: تحديات تطبيق الردع الإلكتروني

إنه عصر الردع الإلكتروني، هكذا يمكن تعريف الزمن الحاضر من المنظورين العسكري والاستراتيجي هو عصر جديد في حسابات القوة والردع، ومفاهيم الحرب ذاتها. نحن الآن قد خرجنا للتو من المفهوم التقليدي للردع، الذي تعارف عليه الدارسون منذ عقود خلت. وخرجنا في الوقت نفسه من التقسيم الثلاثي للقوة: التقليدية وما فوق التقليدية والاستراتيجية نحن اليوم بصدد نوع جديد من الحروب، هو حرب الفضاء الإلكتروني (أو حرب الشبكات)، يصاحبه سباق مستجد للردع، هو الردع الإلكتروني.[1]

في هذا الإطار، تناول الكاتبان تطبيق كل من "الردع بالمنع" و"الردع بالانتقام" والتحديات ذات الصلة بكل منهما، حيث سنتناول الردع الإلكتروني بالمنع وتحديات تطبيقه (المطلب الأول)، ثم نتطرق إلى الردع الإلكتروني بالانتقام وتحديات تطبيقه (المطلب الثاني).

المطلب الأول: الردع الإلكتروني بالمنع وتحديات تطبيقه

[1]. جيلالي شويرب ، دمراد فائزة، المرجع السابق، ص 170.

يمكن أن نميز بين بين الردع بالمنع والردع بالانتقام يكون فعالا بمجرد جعل حسابات التكلفة لدي المهاجمين سلبية، من خلال إقناع المهاجم بأنه لن تكون هناك مكاسب تتناسب مع تكلفة الهجوم، وبالتالي تتضح أهمية النظم الدفاعية الجيدة التي تجعل فرص نجاح أي هجوم ضئيلة، أما الردع بالانتقام أو العقاب فينطوي تحته الردع بالمقاومة، والردع بالصمود والصمود هنا يعني القدرة علي علي استعادة الشيء بشكله الأصلي قبل الهجوم.

حيث سيتم التطرق إلى الردع الإلكتروني بالمنع (الفرع الأول)، ثم تحديات تطبيقه (الفرع الثاني).

الفرع الأول: الردع الإلكتروني بالمنع

ترى الدراسة أنه يكون فعَّالاً بمجرد جعل حسابات "التكلفة" لدى المهاجمين سلبية، من خلال إقناع المهاجم بأنه لن تكون هناك مكاسب تتناسب مع تكلفة الهجوم. وبالتالي تتضح أهمية النظم الدفاعية الجيدة التي تجعل فرص نجاح أي هجوم ضئيلة، كما تضفي مصداقية على التدابير الانتقامية، وتحد من فكرة وجود الطرف الثالث. وهنا يلاحظ الكاتبان أن "الردع بالمنع" موجود بصفة "دفاعية" قبل وقوع الحدث، وبصفة "صمودية" بعد الحدث.

الهدف من الردع هو منع العمل العدواني من خلال قدرة الدولة على تطوير قدرات عسكرية موثوقة ومتبادلة ومتماثلة على الفضاء الإلكتروني تكون قادرة على التأثير على قرارات الخصم، وتمنعه من شن هجمات عسكرية عبر الفضاء الإلكتروني، وقد لعبت نظرية الردع دورا هاما في نظرية الأمن الوطني مع التطور الحديث للعمليات السيبرانية، فضلا عن الأكاديميين والممارسين، وقد تحول انتباههم إلى الإنترنت وقد تسببت طبيعة العمليات السيبرانية في بعض التقليل من دور محتمل للردع، ويطرح افتراض هو أن

تحقق الردع السيبراني ممكن مثل تحقق الردع النووي بعد الحرب العالمية الثانية، فالعمليات السيبرانية تبدو بطبيعتها مختلفة عن العديد من الأسلحةالأخرى التي تسخر العنف على مستوى الدولة، من حيث أنّها في متناول مجموعة واسعة من الجهات الفاعلة.[1]

وتفيد التقارير بأن أكثر من دولة لديها أسلحة إلكترونية أو تقوم بتطويرها، وأكثر من ثلاثين بلدا يقوم بإنشاء وحدات السيبرانية في جيوشها ورغم الاختلاف الذي يطرحه تغير الفواعل أن هناك تشابه على مستوى القوانين الضابطة لانتشار وطبيعة جغرافيا الفضاء الإلكتروني، ونوعية السلاحإلا هذه الأسلحة المستعملة بغرض التهديد، فكما هو موجود على مستوى استراتيجية الردع التقليدية والنووية فيما يخص التقنين ينطبق على الردع الإلكتروني أيضا، لأنه من الصعب تطبيق القوانين على العلاقات العابرة للحدود هذا من جهة، كما أّن ملامح الرقعة الجغرافية غير محّددة، وبالتالي من الصعب تحديد سيادة الدول ومن غير الممكن تحديد نوعية الأسلحة التي هي في تطّور مستمر والحد منها صعب.[2]

إن نظرية الردع السيبراني يجب أن تشمل كل الخصوم المحتملين لكونها قادرة على ردع الكثير، ويجب أن ينطبق الردع على مجموعة كاملة من الجهات الفاعلة، من الأفراد إلى الدول والأمم، والنظر في مجموعة كاملة من الإجراءات، من العمليات الصغيرة في أنظمة الكمبيوتر إلى الهجمات على نطاق واسع التي تنتج حركية كبيرة الآثار على المهاجمين[3].

[1]. محمدبكرارشوش، المرجع السابق، ص 432.

[2]. إيهاب خليفة، إمكانيات تحقيق الردع في صراعات الفضاء الإلكتروني، مجلة اتجاهات الأحداث، ع 13، الجزائر، 2013، ص .21.

[3]. أمين بولنوار، الولايات المتحدة الأمريكية ومنطق الهيمنة، رسالة ماجستير في العلوم السياسية والعلاقات الدولية، كلية العلوم السياسية للإعلام، قسم العلوم السياسية والعلاقات الدولية، جامعة الجزائر، 2010/2009، ص 32.

هذا النوع من الهجمات المحتملة والمهاجمين يتطلب الردع العام لتطبيق على نطاق واسع وقبل أي هجوم محتمل، فعلى سبيل المثال، وجود ترسانة نووية التي يمكن استخدامها ردا على مختلف الهجمات من مختلف الأنواع هو رادع عام يقابله في عالم الإنترنت بعض الإجراءات، مثل تثبيت جدار الحماية، التي تنطبق كرادع عام لجميع الجهات الفاعلة، ومنع جميع حركة المرور السيبرانية التي تأتي من خادم معين، أو التي تحمل معين نوع الملف. ألن الدولة المستهدفة يجب أن تدافع عن منظومتها وشبكاتها بكل قدراتها ضد كل الإمكانات الخصوم أو المهاجمين، والعوامل المذكورة تؤدي إلى استنتاج أن الردع يجب أن تغطي كمجموعة متنوعة من الجهات الفاعلة، وأنواع الهجمات، ومستويات العمل، وبعبارة أخرى، فالعمليات السيبرانية تتطلب هيمنة النوع الكامل إذا ما أريد لها تكون أكثر فعالية.[1]

وعلى الرغم من ذلك، يمكن تجاوز التدابير الدفاعية، فعلى سبيل المثال تم تجاوز إنشاء إيران هياكل متوازية لشبكة وطنية لمنع الهجمات الإلكترونية عالية المستوى، من خلال فيروس "ستكسنتStuxnet "الذي أصاب برنامج المفاعل النووي من خلال USB-sticks.[2]

الفرع الثاني: تحديات تطبيق الردع بالمنع

لقد شكل الفضاء السيبراني ميدان المعركة الخامس بين القوى الدولية، وذلك بعد الأرض، البحر، الجو والفضاء،فاستهداف الهجوم للبنية المعلوماتية يمكن أن يشكل ضربة قاضية

[1]. إيهاب خليفة، المرجع السابق، ص 23.

[2]. أمين بولنوار، المرجع السابق، ص 33.

لاقتصاد بلد من البلدان، أو يمكنه إلحاق الضرر الفادح في كل القطاعات التي يمكن التسلل لها إلكترونيا سواء كانت عسكرية أو مدنية، فمن خلال الاعتبارات السابقة الذكر حول طبيعة الفضاء السيبراني، يمكن أن تظهر توابع أخرى قابلة للنقاش، فلا تستطيع الدول أن تعبر عن سيادتها في الفضاء السيبراني، لأن اعتماد الناس على هذا البعد التكنولوجي يجعله عرضة بشكل خاص للأعمال العدائية، فلا يزال المهاجمون السيبرانيون يتمتعون بمميزات تفوق إمكانات المدافعين بسبب التأثير المفاجئ الذي لا يمكن أن يقلل من قوته أي أسلوب أمني أو دفاعي سلبي أو حتى إيجابي بشكل تام، كما أن هؤلاء المهاجمين يمتلكون القدرة على إخفاء آثارهم، ولا تسمح الحالة المعرفية بوضع توصيف دقيق للعمليات الهجومية التي تحدث في الفضاء السيبراني، الأمر الذي يجعلنا فيمواجهة جميع الاحتمالات.[1]

وفي الواقع لقد ساعدت عدة عوامل على تنامي التهديدات السيبرانية لمصالح الدول، ومن ثم إمكانية بروز حروب سيبرانية والذي يعتبر كتحدي لتطبيق الردع الالكتروني بالمنع، من هذه العوامل ما يلي:

_تزايد ارتباط العالم بالفضاء الإلكتروني (السيبراني)، الأمر الذي اتسع معه خطر تعرض البنية التحتية الكونية للمعلومات لهجمات إلكترونية في الفضاء السيبراني.

_تراجع دور الدولة في ظل العولمة وانسحابها من بعض القطاعات الاستراتيجية مع تصاعد أدوار الشركات متعددة الجنسيات، خاصة العاملة في مجال التكنولوجيا كفاعل مؤثر في الفضاء السيبراني.

[1] شريفة كلاع، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، م 15، ع 1، جامعة الجزائر 3، الجزائر، مارس 2022، ص 300.

_تزايد اعتماد الدول على الأنظمة الإلكترونية في جميع منشآتها الحيوية، الأمر الذي جعل من الممكن الإضرار بمصالحها من خلال الهجمات الإلكترونية في حالات العداء.

_قلة تكلفة الحروب السيبرانية مقارنة بنظيراتها التقليدية، مع إمكانية شن الهجوم في أي وقت، بحيث لا يتطلب تنفيذه سوى وقت محدود.

_تحول الحروب السيبرانية إلى إحدى أدوات التأثير في المعلومات المستخدمة في مستويات ومراحل القتال الإلكتروني والصراع المختلفة، سواء على الصعيد الاستراتيجي أو التكتيكي العملياتي بهدف التأثير بشكل سلبي على هذه المعلومات ونظم عملها.

_توظيف الفضاء السيبراني في تعظيم قوة الدول، من خلال إيجاد ميزة أو تفوق أو تأثير في البيئات المختلفة، وبالتالي ظهر ما يسمى الإستراتيجية السيبرانية للدول.

_اتساع نطاق مخاطر الأنشطة العدائية التي يمارسها الفاعلون، سواء من الدول أو من غير الدول في الحروب السيبرانية، فقد تشن الهجمات الإلكترونية عبر أجهزتها الأمنية الدفاعية، كما قد تلجأ إلى تجنيد قراصنة أو موالين لشن هجمات ضد الخصوم دون أي ارتباط رسمي.

وهو ما جعل مختلف دول العالم تتعرض إلى عمليات اختراق إلكترونية وجوسسة في الفضاء السيبراني للحصول على معلومات عسكرية كانت أو مدنية، وحتى القيام بالتعرض لعمليات إتلاف للبيانات وتدمير المنشآت، ونظرا لأن الدول تختلف فيما بينها من حيث أنظمة الحماية والدفاع الإلكتروني، وتبيان قدرات الدول الكبرى في مجال التحكم في الفضاء السيبراني ومحاولات الهيمنة والسيطرة عليه، ما خلق تحديات أمنية تتعرض لها الدول دونما استثناء، وفيما يلي يمكن تبيان مختلف تلك التحديات:[1]

[1]. مصطفى إبراهيم سلمان الشمري، ، "الأمن السيبراني وأثره في الأمن الوطني العراقي"، مجلة العلوم القانونية والسياسية، م. 10 ع.01، الجزائر، جوان 2021.، ص 78.

1: استهداف البنية التحتية للدول:

حيث يتم استهداف البنية التحتية للدول، سواء كانت مدنية أو عسكرية بهجمات إلكترونية[1]، بما يؤدي إلى شلل أنظمتها وتدمير أنظمة التشغيل الخاصةبها، والتأثير على تدفق المعلومات بما يؤدي إلى إرباك عمل البنية التحتية الحيوية، وينشأ عن مثل هذه الهجمات تعطيل العديد من مرافق الحياة في الدولوسيادة الفوضى، مثل استهداف محطات الطاقة والوقود والخدمات المالية والمصرفية ونظم الاتصالات والمواصلات، ومن أبرز الأمثلة على ذلك تعرض أوكرانيا خلال شهر جوان 2017 لهجمة إلكترونية شملت محطات الطاقة، بالإضافة إلى المؤسسات المالية وأحد أكبر محطاتها، ولقد شهدت السنوات القليلة الماضية العديد من الهجمات الإلكترونية على بعض البنى التحتية الحرجة والمؤسسات العسكرية، مثل محطات الطاقة النووية، كما هو الحال في قيام فيروس "ستاكسنت"بتعطيل حوالي ألف من أجهزة الطرد المركزي في منشأة لتخصيب اليورانيوم في مفاعل[2]"ناتانز" في وسط إيران سنة2010 فضلا عن تعرض أنظمة الكمبيوتر لشركة كوريا الجنوبية للطاقة المائية والنووية التي تديرها الدولة لهجمات إلكترونية في شهر ديسمبر 2014.

2:السيطرة على الأنظمة العسكرية وتعطيلها وإتلافها.

وذلك من خلال قيام قراصنة محترفين أو جيوش نظامية إلكترونية ووكلاء سيبرانيين بشن هجمات إلكترونية بغرض السيطرة على نظم القيادة والسيطرة عن بعد، الأمر الذي يؤدي

[1]. إيهاب خليفة، "تنامي التهديدات السيبرانية للمؤسسات العسكرية"، مجلة اتجاهات الأحداث، ع. 22، الجزائر، أوت 2017، ص 56.

[2]. عبد الجواد، أميرة عبد العظيم محمد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، مجلة الشريعة والقانون، ع 35،.الجزائر، 2020، ص 431.

إلى إخراج بعض منظومات الأسلحة عن سيرة القيادة المركزية، وإعادة توجيهها نحو أطراف داخلية أو ضد دول صديقة، كما يمكن أيضا السيطرة على الطائرات من دون طيار، أو الغواصات النووية في أعماق البحار، أو السيطرة على الأقمار الصناعية العسكرية في الفضاء الخارجي وإخراجها عن سيطرة الدولة التابعة لها هذه الأسلحة والمعدات، إذ تزداد خطورة مثل هذه الهجمات إثر التطور التكنولوجي واعتماد اللوجستيات ونظم القيادة والتحكم وتحديد الأهداف، وإصابتها على برامج الكمبيوتر وشبكات الاتصال.[1]

كما تقوم الهجمات السيبرانية بتدمير أنظمة إلكترونية لمنشآت حيوية عسكرية، وتعطيل أو إتلاف شبكات الدفاع العسكرية عن بعد، واختراق أو تعطيل أو تدمير شبكات القطاع الخاص ذا الصلة بالقطاع العسكري، وكذا التدخل في سلامة البيانات العسكرية الداخلية لدول أخرى، والقيام بمحاولات الإرباك والتشويش على أجهزتها[2].

3:جمع معلومات اقتصادية استخباراتية: ويتحقق عن طريق اختراق قواعد البيانات المالية والمصرفية وقواعد بيانات الشركات والبنوك وجمع المعلومات التي قد تؤثر على الأمن الوطني للدول، وكذلك من خلال التجسس على المسؤولين الماليين ووزراء المالية ورؤساء الشركات الكبرى، وفي هذا الصدد أصدر الرئيس الأمريكي السابق "باراك أوباما" أثناء فترة إدارته الثانية أوامره بوقف التنصت على مقري صندوق النقد الدولي والبنك الدولي، وذلك في إطار مراجعة أنشطة جمع المعلومات الاستخباراتية وذلك في أعقاب التسريبات التي كشف عنها المتعاقد السابق مع وكالة الأمن القومي "إدوارد سنودن" بشأن

[1]. محجوب الزويري، يارا نصار، "إيران والهجمات السيبرانية: فصل جديد في الحرب غير المعلنة"، مجلة رؤية تركية، م 09، ع 04، الجزائر، 2020، ص 124.

[2]. أميرة عبد العظيم، محمد عبد الجواد، المرجع السابق، ص 373

برامج لجمع كميات كبيرة من البيانات عن حلفاء وأعداء الولايات المتحدة الأمريكية والمواطنين الأمريكيين.[1]

المطلب الثاني: الردع الإلكتروني بالانتقام وتحديات تطبيقه

تعني العملية الانتقامية عملية فرض هجمات انتقامية سيبرانية سواء برد الفعل بنفس عملية الاعتداء، أو تجاوز الحد المطلوب من خلال الاتجاه للهجوم المسبق كغطاء لعملية متوقعة،وقد تتجاوز الانتقام في المجال الفضائي في مجالات أخرى أكثر قوة مثل المجال العسكري الذي يفترض وجود ضربات عسكرية بغرض الانتقام.[2]

حيث سيتم التطرق إلى الردع الإلكتروني بالانتقام (الفرع الأول)، ثم إلي تحديات تطبيقه (الفرع الثاني).

الفرع الأول: الردع الإلكتروني بالانتقام

حمل تطبيقه الكثير من التحديات، فرغم أن إظهار القوة وإمكانية استخدامها، عامل حيوي حتى يتم تخويف الخصم، فإن إظهارها قد يعني أن أي استخدام لتلك القوة قد يؤدي للكشف عن معلومات مهمة ضرورية للدفاع ضد الهجمات المستقبلية، وربما يفسر ذلك عدم كشف الدول الكبرى مثل ألمانيا أو فرنسا عن قدراتها الهجومية، وهناك قيود أخرى للانتقام في المجال السيبراني تتمثل في عدم التناسب بين كثافة الهجمات والضرر الناتج، وفكرة تطور الأنظمة عبر مرور الزمن، مما يجعل فرص الاختراق محدودة، لتعقد

[1]. عبد الجواد، المرجع السابق، ص 432.

[2] . Sico van der meer&franspaul van der putten , US deterrenceagainstchinese cyber espoinage, policybrief , clingendael , netherlandsinstitute of international relations , september 2015 , P 04

الأنظمة، وأيضاً مدة الهجمات، فكلما طالت الهجمات كان من الصعب تنفيذ هجمات لاحقة[1].

كما تظل فكرة التدمير المتبادل، غير واردة على الإطلاق في الردع السيبراني، حيث يُستفاد من الردع في إيقاف الهجمات فقط، ولكن يستمر "المهاجم" نفسه، فالهجمات السيبرانية يمكن القيام بها من خلال طرف ثالث مثل مقاهي الإنترنت أو شبكات الإنترنت اللاسلكية أو من خلال أجهزة مصابة بالفعل.

وهناك تحدٍ يرتبط بإشكالية "تحديد هوية الفاعلattribution "، فتحقيق الردع يتطلب أن يكون المعتدون مقتنعين بأنهم سوف يتم معرفتهم ومعاقبتهم، ويجب أن تكون مسألة تحديد هوية فاعل الهجمات دقيقة، لتجنب خلق أعداء جدد، وإقناع الأطراف الأخرى أن هذا الإجراء الانتقامي ليس هجوماً في حد ذاته .[2]

ويعتمد سياق "تحديد هوية الفاعل" على معرفة الصراع، والتاريخ، وتحديد من المستفيد من الهجوم، فهو يجمع بين التدابير التقنية والعمليات الاستخباراتية لتحديد الجاني، والاستفادة من الحوادث السابقة في التعامل مع الفاعلين الدوليين.

كما أن "الدفاع النشط" كأداة فعالة للانتقام السريع والفوري، لم يعد مناسباً لأسباب فنية وسياسية وقانونية مختلفة، فمثل هذه الهجمات الانتقامية الأوتوماتيكية قد تضر أجهزة الكمبيوتر، وذلك دون علم صاحبها. وعلاوة على ذلك، لا تقوم الدول بتقنين مثل هذه الآليات، حتى لا تتيح للقطاع الخاص انتهاك احتكار الحكومة لاستخدام القوة.[3]

---

[1]. محجوب الزويري، يارا نصار، المرجع السابق، ص 125.

[2] . حمزة برابح ، الاستراتيجية الأمنية الجزائرية لمواجهة التهديدات الأمنية الامتثالية في منطقة الساحل الإفريقي، مجلة الباحث للدراسات القانونية والسياسية، ع 6، الجزائر، جوان 2017، ص 262.

[3]. محجوب الزويري، المرجع السابق، ص 126.

الفرع الثاني: تحديات تطبيق الردع بالانتقام

إن متطلبات الردع الإلكتروني لا تزال غير كافية رغم وجود تحديات حقيقية، إذ لا تزال مشكلة تحديد الجاني تؤرق الكثير خاصة وأن الواقع المعلوماتي يشير إلى أن الفضاء السبرانيمفتوح وواسع ولا يقتصر على الأطراف الرسمية وكذا غياب آليات إلزامية لمعاقبة الأطراف المعتدية مما يجعل الردع أشبه بالعمليات العشوائية الانتقامية.

وهذا الصدداقترحت روسيا عام 1999 إنشاء معاهدة دولية لحضر الأسلحة الإلكترونية،وتم طرح ذات الموضوع مع الصين فيمنظمة شنغهاي للتعاون، وكذا الاتفاق 2003م فيالأمم المتحدة التي تقضي بتعيين خبراء حكوميين دوليين للحد من الصراع وتشكيل قواعد معيارية بين الدول ذات تفكير المتشابه يضاف لذلك بناء معايير أمنية مشتركة بين القطاع العام والخاص لإنشاء مدونات لقواعد السلوك.[1]

[1] . حمزة برابح ، المرجع السابق، 263.

المبحث الثاني: بلورة استراتيجية شاملة للردع الإلكتروني

تقدم استراتيجية الردع السيبراني وصفا عاما للقدرات الدفاعية للدول، التي باتت تنفق المزيد من مواردها لردع الهجمات السيبرانية المتنامية في السنوات الأخيرة، عبر تأمين القدرة على الصمود في كل من الشبكات الدفاعية والهجومية.

ويكون تركيز استراتيجية الردع السيبراني على قدرة مقاومة الهجمات السيبرانية من خلال تعزيز القدرات السيبرانية التي تحمي البنى التحتية للدول، حيث توصف تلك الاستراتيجية بالمرونة والقدرة على منع الجهات الفاعلة المعادية من شن الهجمات السيبرانية في المقام الأول.[1]

ويتم الردع السيبراني من خلال وضع استراتيجيات مضادة يدرك من خلالها الخصم أنه إذا قام بشن هجوم عبر الفضاء الإلكتروني سيواجه بهجوم آخر مضاد يفوق قدراته، كأن يتم مثلا استهداف البنية التحتية السيبرانية أو أنظمة الاتصالات والأنظمة المالية والمصرفية أو قطع خدمات الانترنت ومن ثم يرتدع الخصم عن محاولة التفكير في الاعتداء أو تكراره، ومثال على ذلك انقطاع اتصالات الانترنت في كوريا الشمالية لنحو عشر ساعات مما أثار تكهنات بأن الولايات المتحدة وراء هذا الحدث.[2]

وعليه سيتم التطرق إلى الاستراتيجيات المعتمدة على المستوي الدولي (المطلب الأول)، ثم بعد ذلك نتطرق إلى الاستراتيجيات المعتمدة على المستوي الداخلي وموقف الجزائر من الفضاء السبراني (المطلب الثاني).

---

[1]. حمزة برابح ، المرجع السابق، ص 263.

[2]. أميرة عبد العظيم، محمد عبد الجواد، المرجع السابق، ص 374.

المطلب الأول: الاستراتيجيات المعتمدة على المستوي الدولي

ثمة مجموعة من الخطوات تجب مراعاتها للوصول إلى استراتيجية شاملة للردع السيبراني على المستوي الدولي، حيث سيتم التطرق إلي التعاون الدولي بخلق بيئة قانونية مناسبة لمواجهة الحروب السبرانية (الفرع الأول)، ثم نتطرق بعد ذلك إلى توحيد المعايير الدولية لتقييد الحروب السيبيرانية (الفرع الثاني)، وأخيرا تبني حوار استراتيجي بين الدولة وشركائها لضمان الاستعداد للحروب السيبرانية (الفرع الثاني).

الفرع الأول: التعاون الدولي بخلق بيئة قانونية مناسبة لمواجهة الحروب السبرانية

التعاون الدولي من خلال خلق بيئة قانونية وتشريعية مناسبة لمواجهة الحروب السيبرانية، مما يزيد من فرص توقف شن مزيد من الهجمات السيبرانية، كما يجب تحديد قواعد عالمية واضحة للممارسة المقبولة وشرعية الأهداف في الفضاء السيبراني، فوجود خلاف حول وضع معايير دولية لتقييد الحرب الإلكترونية، لا تخدم سوى الفاعلين الإجراميين.

حيث تعاني دول شمال إفريقيا من تصاعد الحروب السيبرانية عليها لعوامل، أهمها: سهولة الاختراقات الإلكترونية، ضعف الإنفاق على نظم الحماية، والطبيعة غير المتماثلة للمواجهات العسكرية، وصعوبات اكتشاف الفاعلين، وانتفاء أدلة الإدانة المباشرة، وغياب الأطر القانونية لتحديد العقوبات لتوظيف الفضاء الافتراضي في الاعتداء على الدول، وكذا نقص التعاون الدولي من خلال خلق بيئة قانونية وتشريعية مناسبة لمواجهة الحروب السيبرانية، مما يزيد من فرص توقف شن مزيد من الهجمات السيبرانية.[1]

الفرع الثاني: توحيد المعايير الدولية لتقييد الحروب السيبرانية

[1]. توماس شيلينج، استراتيجية الصراع، ط 1، الدار العربية للعلوم والنشر، د.ب.ن، 2010، ص 521.

يجب تحديد قواعد عالمية واضحة للممارسة المقبولة وشرعية الأهداف في الفضاء السيبراني، فوجود خلاف حول وضع معايير دولية لتقييد الحرب الإلكترونية، لا تخدم سوى الفاعلين الإجراميين.

الفرع الثالث: تبني حوار استراتيجي بين الدولة وشركائها لضمان الاستعداد للحروب السيبرانية وموقف الجزائر من الفضاء السيبراني

ضرورة دخول الدول في حوار استراتيجي مع شركائها لضمان استعدادهم للحروب السيبرانية، وهذا يمكن أن يكون أساساً للردع "الممتد"، كما يجب على الحلفاء أن يوضحوا لـ"الجناة المحتملين" بأن الانتهاكات ضد حليف واحد سوف يؤدي إلى رد فعل مشترك.

فعلى سبيل المثال تم استهداف الصفحات الإيرانية للمنطقة المغاربية، عن طريق وسائل التواصل الاجتماعي في حالة التموقع في شمال أفريقيا كمدخل لأفريقيا ووسيلة ربط مع أوروبا.[1]

المطلب الثاني: الاستراتيجيات المعتمدة على المستوي الداخلي وموقف الجزائر من الفضاء السبراني

يواجه المجتمع الدولي نوعا جديدا من الحروب تستعمل فيه طرق مستحدثه في القتال بعيدا عن ارض المعركة التقليدية من بينها الحروب السيبرانية، التي جاءت كنتيجة منطقية لتطور وانتشار الأنظمة المعلوماتية والشبكات، وبروز معطيات حيوية كالفضاء السيبراني والأمن السيبراني واحتلالهما لمكانة بالغة الأهمية في مسار حياة الدول، لما يشكلانه من دور أساسي في مجالالحفاظ على أمنها واستقرارها.

[1]. محمد بكرارشوش ، المرجع السابق، ص 428.

حيث سيتم التطرق إلى الاستراتيجيات المعتمدة على المستوي الداخلي (الفرع الأول)، ثم إلى موقف الجزائر من الفضاء السيبراني (الفرع الثاني).

الفرع الأول: الاستراتيجيات المعتمدة على المستوي الداخلي

_التعاون المحلي من خلال شبكة دفاعية قوية قائمة على التعاون بين القطاع الحكومي والخاص، مثل "مجموعات الرد على الطوارئ الإلكترونيةCERT "وهي مرتبطة بوزارة الداخلية والدفاع والقطاع الخاص. ويتطلب هذا التعاون قدراً كبيراً من الثقة المتبادلة، لأن المساعدة التقنية لا يمكن أن تُقدم إلا إذا ضمنت تعاملاً فعالاً، كما يجب الاعتماد على أسلوب المنافسة لاستمالة القطاع الخاص.

_الجدية في نشر وتفعيل الأنظمة الدفاعية والهجومية معاً للشبكات الرئيسية، ومن ثم تحسين أساسيات أمن الشبكات، وحماية البنى التحتية الحيوية، وتحسين أمن الشبكات العسكرية والأسلحة.

_ التركيز على توعية الشعوب والعامة بمخاطر تلك الحروب، مما يحد منها. كما يتطلب ذلك وجود خبرات علمية لدى البرلمانات حتى يتم تبادل تلك المعلومات والخبرات بين البرلمان والقطاع الحكومي والقطاع الخاص.[1]

_تطوير نظم "للردع الضيق" narrowdeterrenceضد فاعلين محددين، لحماية أنظمة بعينها. وتُحدد الخطوات الانتقامية في حالة الهجمات السيبرانية ضد مجموعة ضيقة من الأهداف أو باستخدام مجموعة ضيقة من آليات الهجوم التي يمكن أن تجعل الردع فعالاً.

[1]. سميرة شرايطية، السيادة السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومي، المجلة الجزائرية للأمن والتنمية، م 9، ع 16، الجزائر، 2020، ص 183.

_عدم التركيز فقط على الجيش لمواجهة تلك الحروب، فالجيش جيد في الدفاع عن شبكاته الخاصة، لكنه لا يملك بالكاد أي خبرة في التعاون مع الجمهور، وخبرة أقل في التعاون مع القطاع الخاص. ومع ذلك، فهو جزء أساسي من الأمن السيبراني.[1]

حيث يتحقق التعاون الداخلي من خلال شبكة دفاعية قوية قائمة على التعاون بين القطاع العمومي والخاص، ويتطلب هذا التعاون قدرا كبيرا من الثقة المتبادلة، لأن المساعدة التقنية لا يمكن أن تقدم إلا إذا ضمنت تعاملا فعالا، كما يجب الاعتماد على أسلوب المنافسة الاستمالة القطاع الخاص، واعتماد الجدية في نشر وتفعيل الأنظمة الدفاعية والهجومية معا للشبكات الرئيسية، ومن ثم تحسين أساسيات أمن الشبكات، وحماية البنى التحتية الحيوية، وتحسين أمن الشبكات العسكرية والأسلحة، وكذا التركيز على توعية الشعوب والعامة بمخاطر تلك الحروب، مما يحد منها.[2]

كما يتطلب ذلك وجود خبرات علمية لدى البرلمانات حتى يتم تبادل تلك المعلومات والخبرات بين البرلمان والقطاع العمومي والقطاع الخاص، وأيضا تطوير نظم للردع الضيق ضد فاعلين محددين، لحماية أنظمة بعينها،وتحدد الخطوات الانتقامية في حالة الهجمات السيبرانية ضد مجموعة ضيقة من الأهداف أو باستخدام مجموعة ضيقة من آليات الهجوم التي يمكن أن تجعل الردع فعالا.[3]

كما يجب عدم التركيز فقط على الجيش لمواجهة تلك الحروب، فالجيش له مجاله في الدفاع عن شبكاته الخاصة، لكنه ال يملك بعض الخبرات الخاصة في التعاون مع الجمهور، وخبرة أقل في التعاون مع القطاع الخاص .ومع ذلك، فهو جزء أساسي من الأمن السيبراني.

---

[1]. توماس شيلينج، المرجع السابق، ص 522.

[2]. سميرة شرايطية، المرجع السابق، ص ص 183 – 184.

[3]. برابح حمزة، المرجع السابق، ص 266.

الفرع الثاني: موقف الجزائر من الفضاء السيبراني

تجدر الإشارة إلى أنه 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. وعليه ماهو دور الدفاع الوطني في تحقيق الأمن السيبراني في الجزائر.[1]

على غرار دول العامل لم تعد الجزائر بمنأى عن التهديدات السيبرانية التي لا تعترف بالحدود الجغرافية او القانونية، لذا فهي تعمل على تعزيز استراتيجيتها الوطنية السيبرانية في إطار تجسيد مشروع حوكمة الأنترنت ومجتمع معلوماتي منفتح وآمن في نفس الوقت، وتستند الآليات العملية لتنفيذ هذه الاستراتيجية عموما على دور الجيش الشعبي الوطني لما يملكه من قدرات ومؤهلات متقدمة في هذا المجال وقد اتخذ هذا النهج منذ نوفمبر 2015 أين تم استحداث مصلحة الدفاع السيبراني ومراقبة الأنظمة لأركان الجيش الشعبي الوطني التي جاءت تأكيدا على عزم القيادة العليا على إرساء بيئة سيبرانية أمنة ومستدامة ومحصنة من المخاطر والتهديدات، والتي تعمل على المستوى العسكري على تعزيز القدرات الدفاعية السيبرانية وتامين منظومة الأسلحة والإعلام والاتصال العسكرية، كما

[1]. محمد مختار، "هليمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية؟"، مجلة اتجاهات الأحداث. ع،6 يناير، الجزائر، ،2015 ص ص 6 – 7.

تسهر على التنسيق مع الهيئات الوطنية ذات الصلة على إعداد سياسة وطنية خاصة بتامين المنشاة الحساسة في المجال السيبراني .[1]

وعليه، فإن رهان التنمية الذي تتطلع إليه كافة الدول حاليا، تعترضه مجموعة من العراقيل، خاصة مع تزايد التهديدات السيبرانية، الذي تأخذ طابع الاختراق أحيانا وبث الدعايات من أجل التأثير على الجبهة الاجتماعية أحيانا أخرى، الأمر الذي دفع بالعديد من الدول ومنها الجزائر، إلى اتخاذ مجموعة من الإجراءات القانونية والمؤسساتية من أجل تأمين مصالحها في هذا الشأن.

من أجل التصدي للتهديدات السيبرانية الموجهة ضد قواعد وبيانات ومؤسسات الدولة، سيما الحساسة منها، قامت الجزائر بتبني حزمة من الإجراءات القانونية والمؤسساتية، بهدف تحقيق أمنها واحتواء كافة التهديدات، خاصة في ظل الرهان المرفوع من أجل التحول إلى حكومة إلكترونية، وكذا التزايد الكبير للجرائم الإلكترونية. وهي كالآتي:[2]

1: الإجراءات القانونية :وهذا من خلال سن مجموعة قوانين منها:

– القانون رقم 09–04[3]المؤرخ في 5 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي حدد مجال تطبيقه والمتمثل في وضع الترتيبات التقنية الهادفة إلى مراقبة الاتصالات الإلكترونية، وتجميع وتسجيل محتواها في حينها، وكذا القيام بإجراءات الحجز والتفتيش داخل المنظومة المعلوماتية.

---

[1] .Dan Craigen, Nadia Diakun-Thibault, and Randy Purse, DefiningCybersecurity. Technology Innovation Management Review, October 2014, pp 14-15.

[2]. محمد مختار،المرجع السابق، ص 8.

[3]. القانون رقم 09–04، المؤرخ في 5 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر، ع 47، الصادرة بتاريخ 16/أوت/2009.

_القانون رقم 14-01 المؤرخ في 4 فيفري 2014، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 8 جوان 1966، والمتضمن قانون العقوبات.

-القانون رقم 16-02[1] المؤرخ في 19 جوان 2016، المتمم للأمر رقم 66-156 المؤرخ في 8 جوان 1966، والمتضمن أيضا قانون العقوبات.

_القانون رقم 18-07 [2] المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

2: الإجراءات المؤسساتية:

وهذا من خلال استحداث هيئات مكلفة بالوقاية ومكافحة جميع أشكال التهديد السيبراني، ملحقة بجميع الأسلاك الأمنية من درك وطني، شرطة وجيش، وهي كالآتي:

_المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني، والمنشأ بموجب المرسوم الرئاسي رقم 04-183[3] المؤرخ في 26 جوان 2004 والمتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام وتحديد قانونه الأساسي. ويتكونهذا المعهد من إحدى عشرة دائرة متخصصة في مجالات مختلفة، مهامها إنجاز الخبرات وتقديم المساعدات التقنية. كما توجد دائرة متخصصة في الإعلام الآلي والإلكتروني، وهي مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة .

[1] . القانون رقم 16-02 المؤرخ في 19 جوان 2016، المتمم للأمر رقم 66-156 المؤرخ في 8 جوان 1966، والمتضمن أيضا قانون العقوبات، ج ر، ع 37، الصادرة بتاريخ 22/جوان/ 2016.

[2]. القانون رقم 18-07، المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر، ع 34، الصادرة بتاريخ 10/ جوان/ 2018.

[3]. المرسوم الرئاسي رقم 04-183، المؤرخ في، 2004/06/26، المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج ر، ع 41، الصادرة بتاريخ .2004/06/27.

_مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها، التابع لقيادة الدرك الوطني. دخل حيز الخدمة في 2006.

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تم التنصيص على إنشائها بموجب المادة 13 من القانون رقم 09-04[1]، المؤرخ في 5 أوت 2009. وتتمثل مهامها في تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك تجميع المعلومات، وإنجاز الخبرات القضائية، وتبادل المعلومات مع نظيراتها في الخارج، قصد التعرف على مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

إضافة إلى هذه المهام، فقد تم تكليفها أيضا، وبموجب المرسوم الرئاسي رقم 15-261[2]، المؤرخ في 8 أكتوبر 2015، والمحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، باقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وتنشيط وتنسيق عمليات الوقاية، وضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالإعمال الإرهابية الماسة بأمن الدولة.

_المصلحة المركزية لمكافحة الجريمة المعلوماتية، تم إنشائها في سنة 2011، والتي تم تطويرها بعدما كانت مجرد تشكيل أمني لمحاربة الجريمة الإلكترونية على مستوى

---

[1]. القانون رقم 04/09، المؤرخ في 2009/8/05، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهما، ج ر، ع 47، الصادرة بتاريخ 16/أوت/2009.

[2]. المرسوم الرئاسي رقم 15-261، المؤرخ في 8 أكتوبر 2015، والمحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج، ر، ع 53، الصادرة بتاريخ 2015/10/8.

المديرية العامة للأمن الوطني. وقد تم إلحاقها بالهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015.

هذه المصلحة تتكفل بمهام مباشرة التحريات في قضايا الإجرام المنظم والإرهاب والأعمال الهدامة، بالتنسيق مع الشركاء الأمنيين، كما تضطلع بمهمة مكافحة الإجرام الاقتصادي والمالي، إلى جانب باقي المصالح المتخصصة الوطنية الأخرى، على غرار الديوان المركزي لقمع الفساد، والهيئة الوطنية للوقاية من الفساد ومكافحته، وكذا خلية الاستعلام المالي. كما أنها تعتبر في مجال تخصصها، الجهة الرئيسية التي يتم التعامل معها لِمَرْكَزَة (Centralisation) التحري مع الأقطاب الجزائية المتخصصة، وتعزيز التعاون على المستوى الدولي.

_مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة، تم إنشاء هذه المصلحة بتاريخ 06 نوفمبر 2015 على مستوى دائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي، وهذا في إطار الاستراتيجية المتبناة من أجل تحقيق نظام دفاع سيبراني متكامل وفعال. وهدفها تأمين حماية المنظومات والمنشآت الحيوية للبلاد ضد التهديدات والإرهاب الإلكتروني والجوسسة، من خلال الرد السريع على الاختراقات والتشويش على أجهزة التجسس. وحسب آخر إحصاء لوزارة الدفاع الوطني، فإنها تجهض يوميا 3500 محاولة اختراق لمواقع قيادات قواتها من قبل الهاكرز، من مختلف أنحاء دول العالم.[1]

_المنظومة الوطنية لأمن الأنظمة المعلوماتية، والتي تم إنشائها بموجب المرسوم الرئاسي رقم 20-05، المؤرخ في 20 جانفي 2020، والمتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية. وهذه الأخيرة موضوعة لدى وزارة الدفاع، وتتكون من المجلس الوطني لأمن الأنظمة المعلوماتية، المكلف بإعداد الاستراتيجية الوطنية لأمن الأنظمة

[1]. شفيق نوران ، **أثر التهديدات الإلكترونية على العلاقات الدولية، دراسة في أبعاد الأمن الإلكتروني**، د.ط، المكتب العربي للمعارف، القاهرة، 2016، ص ص40-43.

المعلوماتية، والموافقة عليها وتوجيهها، ومن الوكالة الوطنية لأمن الأنظمة المعلوماتية، وهي التي تقوم بتنسيق تنفيذ الاستراتيجية الوكالة لأمن الأنظمة المعلوماتية. وهذه المنظومة تعد أداة الدولة في مجال أمن الأنظمة المعلوماتية، كما أنها تشكل الإطار التنظيمي لإعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتنسيق تنفيذها.[1]

كما تم إنشاء **الهيئات القضائية الجزائية المتخصصة** بموجب القانون رقم 04-14، المؤرخ في 10 نوفمبر 2004، المعدل والمتمم لقانون الإجراءات الجزائية، والمختصة بالنظر في الجرائم المعلوماتية المرتبطة بنظم المعالجة الآلية للمعطيات، المُستهدِفة لمؤسسات الدولة والاقتصاد والدفاع الوطنيين.[2]

[1]. المرسوم الرئاسي رقم 20-،05 المؤرخ في 20 جانفي 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج ر، ع 04، المؤرخة في 26 / 1/ 2020.

[2]. القانون رقم 04-14، المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 8 جوان 1966، المتضمن قانون الإجراءات الجزائية، ج ر ع 71، المؤرخة في 10 نوفمبر 2004.

خاتمة

خاتمة.

لطالما ركزت الولايات المتحدة على تعزيز قدراتها لحماية مواقعها الإلكترونية الحساسة وتقليص احتمالات تعرضها للهجوم والاختراق، ولكن في الآونة الأخيرة تصاعدت وتيرة الاهتمام لتتجه في منحى آخر، دافعة صناع القرار إلى إيجاد طرق ووسائل تمنع حدوث الهجمات والتصدي لها قبل أن تحدث أصلاً، ويبقى الهدف هو ردع الخطر برفع تكلفة الهجوم وتقليل فوائده حتى ينثني المهاجم عن المخاطرة. ويبدو أن الاستراتيجية الجديدة القائمة على الردع في مواجهة عمليات الاختراق الإلكتروني تعكس إدراكاً متقدماً لدى أعلى مستويات السلطة في أميركا بأن تنويع نماذج التصدي للهجمات الإلكترونية المتزايدة يقتضي عدم الاقتصار على الدفاع، بل يتجاوزه للتصدي الإيجابي والفعال، بل والهجوم عندما يكون ذلك ضرورياً. وحسب مقاربة وزارة الدفاع المحدثة بهذا الشأن تضطلع الوزارة بأدوار مهمة في استراتيجية الردع الإلكتروني المعتمدة على الهجوم، فأولاً سيكون على الوزارة اعتماد مقاربة أُطلق عليها اسم «الردع بالمنع»، وذلك من خلال التعاون والتنسيق مع القطاع الخاص، الذي يملك ويشغل 90 في المئة من البنية التحتية للإنترنت، لتكون قادرة على حماية ممتلكاتها وتعزيز دفاعاتها الخاصة، هذا بالإضافة إلى تشديد الاستراتيجية الدفاعية على عنصر المرونة. وعلى الرغم من أن وثيقة وزارة الدفاع لا تحدد التفاصيل المتعلقة بالمرونة وغيرها من التوصيات، فإنها مرتبطة بجملة من المفاهيم، منها حماية الحدود الإلكترونية، وأيضاً عزل الأجزاء بعضها عن بعض. فحماية الحدود الإلكترونية تعني إقفال الجزء الذي تعرض للهجوم تلقائياً وإعادة تشغيله لاحقاً، أما العزل فهو يعتمد مقاربة عزل الأجزاء حتى إذا تعرض أحدها لهجوم إلكتروني ظل الآخر بمنأى عنه ما يسهل التعامل معه ويقيه من الهجوم. وسواء أشرف البنتاجون نفسه على تطبيق الاستراتيجية، أو الجهات الخاصة المتعاونة معه، يبقى الهدف النهائي منها «إقناع الخصوم المحتملين بعدم جدوى شن هجوم على الشبكات والأنظمة الأميركية». وإذا كانت

المرونة التي تنص عليها الاستراتيجية تحد من نتائج وتداعيات الهجوم بتطويقها منذ البداية، إلا أن تعزيز حماية الشبكات في المجمل ينطوي على العديد من الصعوبات، ولا سيما أن استراتيجية البنتاجون لم توضح التفاصيل المتعلقة بتحقيق هذا الهدف. ولكن المهم واللافت أيضاً هو دور الحكومة الفيدرالية نفسها من خلال وزارة الدفاع في حماية الشبكات الأميركية حتى وإن كانت تشغلها جهات خاصة، إذ لا يمكن المجازفة بإيلاء عملية الحماية للشركات فيما ينطوي ضربها على خسارة لأميركا بأكملها ومس بسيادتها الإلكترونية التي قد تترتب عليها تداعيات أمنية واقتصادية خطيرة، هذا ناهيك عن القدرات المتطورة والإمكانات الكبيرة المتوفرة لدى الوزارة. والأكثر من ذلك وعندما يتعلق الأمر بمسألة بالغة الحساسية مثل حماية الأنظمة الإلكترونية الأميركية المسؤولة على عدد كبير من المهام سواء شبكات توزيع الكهرباء، أو تنظيم النقل، أو أسرار الشركات وغيرها، لا تقتصر الحماية على وزارة الدفاع، بل تشاركها أيضاً وكالة الأمن الوطني التي تعمل في انسجام تام مع استراتيجية البنتاجون، وهو ما أكده مديرها الأدميرال «مايك روجرز» في شهادة أدلى بها مؤخراً أمام الكونجرس وأشار فيها إلى أن تعظيم فرص حماية أميركا لشبكاتها الإلكترونية وتعزيز أمنها الإلكتروني لا تنفصل عن تقوية قدراتها الهجومية في هذا المجال. ولكن من السابق لأوانه تقييم مدى ملاءمة هذه الاستراتيجية، لأن أميركا بدأت لتوها التعامل مع الأخطار الإلكترونية بمنطق الردع، بمعنى إقناع الخصم بعدم جدوى الهجوم وارتفاع تكلفته حتى قبل الانطلاق فيه. ومع ذلك يمكن تلمس بعض جوانب النجاح التي ترجمتها أميركا في خطوات ملموسة لمعاقبة كل من سولت له نفسه المساس بالأمن الإلكتروني الأميركي، ومن بينها مثلاً توجيه وزارة العدل الأميركية قبل سنة تهماً واضحة لخمسة ضباط صينيين متورطين في الهجوم الإلكتروني على عدد من الشركات الأميركية الكبرى، وهي المرة الأولى التي تشير فيها أميركا بأصبع الاتهام لجهة صينية رسمية. وقبل أشهر قليلة فقط لوحت الولايات المتحدة بورقة العقوبات الاقتصادية عندما

تعرضت شركة «سوني السينمائية» لاختراق على يد كوريا الشمالية، حيث أصدر الرئيس أوباما قراراً تنفيذياً اعتمدت عليه وزارة الخزينة في استهداف الجهات الكورية الشمالية، التي يعتقد أنها تقف وراء الهجمات. ولكن الاستراتيجية الجديدة التي تحفز وزارة الدفاع على القيام بهجماتها الإلكترونية الخاصة كنوع من الدفاع المسبق عن النفس قد تنطوي على بعض المخاطر، التي من بينها توتير العلاقات الدبلوماسية بين أميركا ودول أخرى، وربما الدخول في حرب مفتوحة تصعب السيطرة عليها.

أولا: النتائج.

_أن طبيعة العمليات السيبرانية تُقوض من الدور المحتمل للردع، وقد تجعله عديم الفائدة كليًا. ورغم ذلك، تتزايد أهميته في ظل هشاشة الدول في الاستجابة للهجمات السيبرانية من ناحية، وقدرته على ردع بعض الفاعلين من ناحية أخرى. ولكنه إجمالًا لن يكون فعالًا تمامًا.

_يظل من الهام ردع الهجمات السيبرية؛ فلا يزال الردع ضروريًا ومناسبًا، ولكن النظرية الكلاسيكية للردع لم تعد كافية.

_أن من يسيطر على الفضاء السيبراني، سيسيطر ويتحكم في المجالات الجغرافية الأربعة (البر– البحر – الجو – الفضاء).

_لقد فرض الفضاء السيبراني تحديات مختلفة على دول العالم من دون استثناء، كما أوجد حدودا جديدة للقوة بين الدول.

–لقد خلق الفضاء السيبراني تحديدات جعلت من باب الالحاح أن تعتد الدول استراتيجيات مصممة لتحقيق الأمن السيبراني الوطني خاصة في ظل التحديات الراهنة.

_لقد فرضت الهجمات السيبرانية والجوسسة والاختراقات الإلكترونية على دول العالم فكرة النظر في سيادتها الكاملة، والتي أصبحت منكشفة وفي حالة انكشاف أمني إذا ما تم اختراقها والهجوم عليها.

_ستكون الحروب القادمة حروبا في الفضاء السيبراني، لصعوبة تحديد هوية المهاجمين عبره، ولصعوبة حدوث حروب تقليدية مباشرة على أرض الواقع.

_ستكون الغلبة في الفضاء السيبراني لمن يملك التقنيات المتقدمة ويتحكم بها بشكل منفرد، ما يجعل من يحقق ذلك يمتلك السيطرة في هذا المجال.

ثانيا: التوصيات.

_ضرورة أن تشمل استراتيجية الردع السيبرانية كلاً من آليات الردع بالمنع وبالانتقام، ويشمل هذا بصورة رئيسية أربعة عناصر؛ أولها المقاومة من خلال وضع مبادئ إرشادية قوية ضد الاضطرابات العرضية والفجائية، وثانيها القدرة على الصمود والتعافي بسرعة وبشكل كامل من الهجمات، وثالثها تعريف واضح المعالم لقواعد الممارسة المقبولة وشرعية الأهداف في الفضاء الإلكتروني، وأخيراً وجود استراتيجية وطنية للاستجابة والردود ضمن القواعد المنظمة، بدءاً من الملاحقة الجنائية والإدانة السياسية إلى العقوبات الاقتصادية، وكذلك اتخاذ تدابير للدفاع النشط والانتقام.

_الاكتفاء بالمراقبة وتكثيف الحماية وتأجيل الهجمات الوقائية لأوقات الطوارئ القصوى. ميلاني تيبلينسك" *كاتبة أميركية ينشر بترتيب خاص مع خدمة «كريستيان ساينس مونيتور".

_استراتيجية الردع الفعالة يحب أن تتضمن الإعلان عن استجابة واستعراض قدرات استجابة فاعلة مثل: فرض العقوبات، وتطوير ونشر قدرات دفاعية لمنع نجاح أي هجوم محتمل، فضلًا عن إنشاء قوات متخصصة للمهمات السيبرانية، وتطوير وتعزيز البنية

التحتية العسكرية والتجارية الهامة لكي تصد أي هجوم محتمل، ناهيك عن تعزيز وتطوير الاستخبارات لاكتشاف هوية المهاجم. ولا يكفي لتلك الاستراتيجية الاعتماد على القدرات السيبرانية أو النووية فحسب، بل يتطلب الأمر الاعتماد على الأسلحة غير النووية، على نطاق واسع، مثل: الضربات التقليدية والدفاع الصاروخي، والفضاء الهجومي.

_على الردع السيبراني التصدي لمختلف الطرق التي يحدث بها الاختراق، أو تُشن بها الهجمات، ومنها اختراق الأجهزة المستهدفة والشبكات والمعلومات، التي تعتمد على نقاط الضعف التقنية في الشبكات وأجهزة الكمبيوتر. إذ يعتمد عديد من العمليات عن بعد على احتمال أن يستقبل الضحايا رسالة أو ملف يتضمن برنامجًا ضارًا يهدد أنظمتها بشكل غير مقصود.

_جب تبني مفهوم واسع من الردع يستخدم نهجWhole-of-Governmentلدمج كل عناصر السلطة الوطنية، الدبلوماسية والعسكرية والاقتصادية، والاستخباراتية، والقانونية، لتعزيز أمن المعلومات وخلق حالة من عدم اليقين في أذهان الأعداء حول فعالية أي نشاط سيبراني، وزيادة تكلفته وعواقبه..

_لابد من نشر دفاعات قوية والاعتماد على أنظمة مرنة يمكن أن تتعافى سريعًا من الهجمات أو أي اضطراباتٍ أخرى. تلك التدابير لابد أن تتأسس على القدرة والرغبة في الرد على الهجمات السيبرانية من خلال جميع الوسائل اللازمة، على نحو يتسق والقانون الدولي. بحيث لا تقتصر تلك التدابير على متابعة تدابير إنفاذ القانون، بل تشمل فرض عقوبات على المهاجمين وشن عمليات سيبرانية هجومية ودفاعية، واستنفاد جميع الخيارات المتاحة لاستخدام القوة العسكرية.

_يجب تشديد الإجراءات القانونية الرادعة التي تحول دون التسبب في أضرار عابرة للحدود تتبع سيادة الدولة أو ولايتها القانونية، بل ومحاسبتها حال فشلها في وضع تدابير

تنظيمية لردع الهجمات السيبرانية داخل أراضيها. إن وضع قوانين للجرائم السيبرانية يعد خطوة كبرى نحو التصدي لها؛ فكل دولة عليها واجب اتخاذ التدابير المعقولة والمناسبة لتأمين مجتمع المعلومات، من خلال وضع تدابير قانونية لضمان أمن وفعالية شبكات الاتصالات الدولية. وهذا يؤكد المسئولية الجماعية للدول عن الأمن السيبراني.

قائمة المصادر والمراجع

قائمة المصادر والمراجع.

أولا: قائمة المصادر.

1: النصوص القانونية.

_القانون رقم 09-04، المؤرخ في 5 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر، ع 47، الصادرة بتاريخ 16/أوت/2009.

_القانون رقم 16-02 المؤرخ في 19 جوان 2016، المتمم للأمر رقم 66-156 المؤرخ في 8 جوان 1966، والمتضمن أيضا قانون العقوبات، ج ر، ع 37، الصادرة بتاريخ 22/جوان/ 2016.

_القانون رقم 18-07، المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر، ع 34، الصادرة بتاريخ 10/ جوان/ 2018.

_القانون رقم 04-14، المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 8 جوان 1966، المتضمن قانون الإجراءات الجزائية، ج ر ع 71، المؤرخة في 10 نوفمبر 2004.

2: النصوص التنظيمية.

_المرسوم الرئاسي رقم 20-،05 المؤرخ في 20 جانفي 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج ر، ع 04، المؤرخة في 26 / 1/ 2020.

_المرسوم الرئاسي رقم 04-183، المؤرخ في، 2004/06/26، المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج ر، ع 41، الصادرة بتاريخ .2004/06/27.

ـ المرسوم الرئاسي رقم 15-261، المؤرخ في 8 أكتوبر 2015، والمحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج، ر، ع 53، الصادرة بتاريخ 2015/10/8.

ثانيا: قائمة المراجع.

1: المراجع باللغة العربية.

أ: الكتب.

ـ نوران شفيق، أثر التهديدات الإلكترونية علي العلاقات الدولية (دراسة في أبعاد الأمن الإلكتروني)، د.ط، المكتب العربي للمعارف، القاهرة، 2016.

ـ نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية، دراسة في أبعاد الأمن الإلكتروني، د.ط، المكتب العربي للمعارف، القاهرة، 2016.

_إسماعيل صبري مقلد، العلاقات السياسية الدولية، (دراسة في الأصول والنظريات)، المكتبة الأكاديمية، القاهرة:، 2010.

_إيهاب خليفة، الحرب السيبرانية، الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، د.ط، العربي للنشر والتوزيع، القاهرة، .2021.

_بيتر سينجر، الحرب عن بعد (دور التكنولوجيا في الحرب)، ط 1، مركز الإمارات للدراسات والبحوث الاستراتيجية، الإمارات، 2010.

_شارل روسو، القانون الدولي العام، الأهلية للنشر والتوزيع، ترجمة شكر الله خليفة، عبد المحسن سعد، لبنان، ،1987.

_عمر بن عبد الله بن سعيد البلوشي، مشروعية اسلحة الدمار الشامل وفقاً لقواعد القانون الدولي، د.ط، منشورات الحلبي الحقوقية، بيروت، 2007.

_عمرو رضا بيومي، مخاطر اسلحة الدمار الشامل الإسرائيلية على الأمن القومي العربي، ط،9 دار النهضة العربية، د.ب .ن، 2002.

_هشام بشير، المدخل للقانون الدولي الإنساني، ط، 1، المركز القومي للإصدارات القومية، القاهرة، 2012.

ج: المقالات العلمية.

_ . بكرارشوش محمد، إستعدادات الجزائر لمقتضيات حروب الجيل الرابع بين الواقع والآفاق، دفاتر السياسة والقانون، م 13، ع 03، جامعة قاصدي مرباح ورقلة، الجزائر، 2021.

_. حسين قوادري، الردع السيبراني بين النظرية والتطبيق، المجلة الجزائرية للأمن والتنمية ع 16، الجزائر، جانفي 2020.

_أحمد عبيس نعمة الفتلاوي، "الهجمات السيبرانية:، (مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر)، مجلة المحقق الحلي للعلوم القانونية والسياسية، ع 4، الجزائر، ،2016.

_الشمري، مصطفى إبراهيم سلمان، "الأمن السيبراني وأثره في الأمن الوطني العراقي"، مجلة العلوم القانونية والسياسية، م. 10 ع.01، الجزائر، جوان 2021.

_إيهاب خليفة، "تنامي التهديدات السيبرانية للمؤسسات العسكرية"، مجلة اتجاهات الأحداث، ع. 22، الجزائر، أوت 2017.

_إيهاب خليفة، إمكانيات تحقيق الردع في صراعات الفضاء الإلكتروني، مجلة اتجاهات الأحداث، ع 13، الجزائر، 2013.

_برابح حمزة، الاستراتيجية الأمنية الجزائرية لمواجهة التهديدات الأمنية اللاتماثلية في منطقة الساحل الإفريقي، مجلة الباحث للدراسات القانونية والسياسية، ع 6، الجزائر، جوان 2017.

_بوغرارة، الأمن السيبراني، مجلة الدراسات الإفريقية وحوض النيل، م 1، ع 3، الجزائر، سبتمبر 2018.

_توماس شيلينج، إستراتيجية الصراع، ط 1، الدار العربية للعلوم والنشر، د.ب.ن، 2010.

_حكيم غريب، صبرينة شرقي، تداعيات الحرب الإلكترونية على العالقات الدولية: (دراسة في الهجوم الإلكتروني على إيران) فيروس ستكنست")، دفاتر السياسة والقانون، م 12، ع 2، الجزائر، 2020.

_سعيد درويش، "الحروب السبرانية وأثرها على حقوق الإنسان: (دراسة على ضوء أحكام دليل " تالين"")، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، م 54، ع 5، الجزائر،2017.

_شرايطية سميرة، السيادة السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومي، المجلة الجزائرية للأمن والتنمية، م 9، ع 16، الجزائر، 2020.

_شريفة كلاع، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، م 15، ع 1، جامعة الجزائر 3، الجزائر، مارس 2022.

_عبد الجواد، أميرة عبد العظيم محمد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، مجلة الشريعة والقانون، ع 35،.الجزائر، 2020.

_علاء الدين فرحات، من الردع النووي إلي الردع اليبيراني (دراسة لمدي تحقيق مبدأ الردع في الفضاء السيبراني)، مجلة المفكر، م 16، ع 01، المدرسة الوطنية العليا للعلوم السياسية، الجزائر، 2021.

_علي عبد الرحيم العبودي ،هاجس الحروب السيبرانية وتداعياتها علي الأمن والسلم الدوليين ،المجلة الأكاديمية العلمية، م 57، ع 2، ،كلية العلوم السياسية، جامعة النهرين بغداد، ،العراق،2019.

_محجوب الزويري، يارا نصار، "إيران والهجمات السيبرانية: فصل جديد في الحرب غير المعلنة"، مجلة رؤية تركية، م 09، ع 04، الجزائر، 2020.

_محمد مختار، "هليمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية؟"، مجلة اتجاهات الأحداث. ع،6 يناير، الجزائر، ،2015.

_يحيى مفرح الزهراني، "الأبعاد الاستراتيجية والقانونية للحرب السيبرانية"، مجلة البحوث والدراسات، ع 23، الجزائر، 2007.

_يحيى ياسين سعود، "الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني"، م4 ،ع 4، الجزائر، 2008.

_يحيى ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية) ، ع 2، مصر، 2020.

_شويرب جيلالي، دمراد فائزة، مفهوم الحروب السيبرانية والأمن السيبراني، مجلة الحقوق والحريات، م 11، ع 1، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي الأغواط، الجزائر، 2023.

ب: الرسائل الجامعية.

_أمين بولنوار، الولايات المتحدة الأمريكية ومنطق الهيمنة، رسالة ماجستير في العلوم السياسية والعلاقات الدولية، كلية العلوم السياسية للإعلام، قسم العلوم السياسية والعلاقات الدولية، جامعة الجزائر، 2010/2009.

_وليد غسان سعيد جلعود، دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، رسالة ماجستير، تخصص: التخطيط والتنمية السياسية، كلية الدراسات العليا، جامعة النجاح الوطنية نابلس، فلسطين، 2013/2012.

د: المواقع الإلكترونية.

_. www.SaSapost.com

_resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm
/ara/org.icrc.www://h

2: المراجع باللغة الأجنبية.

_Lotrionte, Catherine, A BetterDefense: Examining the United States New Norms-BasedApproach to Cyber Deterrence, Georgetown Journal of International Affairs, 2013

_ Michael Krepon, Space and NuclearDeterrence, In: Michael Krepon& Julia Thompson (Eds.), Anti Satellite Weapons, Deterrence and Sino-AmericanSpace Relations, United States: Stimson Center, September 2013

_ Kevin R. Beeker, StrategicDeterrence in Cyberspace: Practical Application, GraduateResearch Project Presented to the FacultyDepartment of Electrical& Computer Engineering GraduateSchool of Engineering and Management, Air Force Institute of Technology Air Education and Training Command in Partial Fulfillment of the Requirements for the Degree of Master of Cyber Warfare, 2009

فهرس المحتويات

فهرس المحتويات:

الملخص.

في السنوات الأخيرة، تزايد عدد الهجمات السيبرانية بشكلٍ حاد. ولذا، بحث الدارسون والمنظرون في قدرة نظريات الحرب الباردة – ومنها نظرية الردع – على التصدي لتلك الهجمات وردعها. ومن هنا تتجلي إشكالية الدراسة، والتي تتمثل في مدى انطباق تلك النظرية على الفضاء السيبراني. يقصد بالردع السيبراني منع الأعمال الضارة ضد الأصول الوطنية في الفضاء. ويرتكز على ثلاثة ركائز هي: مصداقية الدفاع، والقدرة على الانتقام، والرغبة فيه. إذ تدعو الحاجة إلى ردع الهجمات السيبرانية على اختلاف أنواعها وآثارها التدميرية ورغم ذلك، لا يزال الردع السيبراني فعالًا جزئيًا عبر خيارات جديدة، منها الردع السلبي، والاحتجاجات الدبلوماسية، والتدابير القانونية، والعقوبات الاقتصادية، والانتقام السيبراني أو العسكري وغيرها، وصولًا لبلورة استراتيجية متكاملة للردع.

الكلمات المفتاحية: الردع الإلكتروني، الجرائم السيبرانية، الحروب السيبرانية.

Résumé.

Ces dernières années, le nombre de cyberattaques a fortement augmenté. Par conséquent, les universitaires et les théoriciens ont examiné la capacité des théories de la guerre froide - y compris la théorie de la dissuasion - à affronter et à dissuader ces attaques. D'où la problématique de l'étude, qui se représente dans la mesure dans laquelle cette théorie s'applique au cyberespace. La cyberdissuasion vise à prévenir les actions malveillantes contre les actifs nationaux dans l'espace. Elle repose sur trois piliers : la crédibilité de la défense, la capacité à prendre sa revanche et le désir de la prendre. Il est nécessaire de dissuader les cyberattaques de toutes sortes et leurs effets destructeurs.Malgré cela, la cyberdissuasion est encore partiellement efficace à travers de nouvelles options, parmi lesquelles la dissuasion négative, les protestations diplomatiques, les mesures judiciaires, les sanctions économiques, les représailles cyber ou militaires, etc., menant à l'élaboration d'une stratégie intégrée de dissuasion.

.Mots clés : dissuasion électronique, cybercrimes, cyberguerres