ISSN : 2543-3938 - EISSN : 2602-7771

التهديدات الأمنية السيبرانية: دراسة في انعكاسات الحرب الإلكترونية على الأمن القومي للدول وإستراتيجيات المقاومة

Cybersecurity Threats: A Study into the implications of cyberwarfare for countries national security and resistance strategies

سميــر بلي

جامعة الجزائر3 (الجزائر)، bey.samir@univ-alger3.dz

تاريخ الاستلام: 2023/02/02 **تاريخ القبول**: 2023/05/25 **تاريخ النشر**: 2023/06/10

ملخص:

تهدف هذه الدراسة للبحث في طبيعة التهديدات الأمنية السيبرانية التي تواجه المنظومات المعلوماتية للدول، وذلك من خلال التطرق لمفاهيم الأمن السيبراني وخصائصه، والإستراتيجيات الوطنية والدولية التي عملت عليها الدول والحكومات بهدف التصدي للحرب الإلكترونية لتحقيق أمنها السيبراني، مع البحث في الإسقاط القانوني الدولي لهذا النوع من التهديدات فضلا عن تكييفها مع الواقع للوصول إلى السبل الأنجع لمعالجته.

أدت شمولية التهديدات الأمنية السيبرانية إلى قيام المجتمع الدولي بما فيه الدول والحكومات والمنظمات المختلفة، بالتعاون وتنسيق الجهود وابتكار ميكانيزمات مضادة من أجل التصدي للانعكاسات السلبية المصاحبة للحرب الإلكترونية، ومنه التخفيف من تداعياتها.

الكلمات المفتاحية: الأمن السيبراني؛ التهديدات السيبرانية؛ الحرب الإلكترونية؛ انعكاسات السيبرانية.

* * *

Abstract:

This study aims to investigate the nature of cyber security threats facing states, information systems by addressing the concepts and characteristics of cyber security, and the national and international strategies that states and governments have worked to address cyber warfare to achieve their cyber security, while researching the international legal projection of this type of threat as well as adapting it to reality to reach the most effective ways to address it.

The comprehensiveness of cyber security threats has led the international community, including States, Governments and various organizations, to cooperate, coordinate efforts and devise counter-mechanics to address and mitigate the negative repercussions of cyber warfare.

Keywords: *Cyber Security; Cyber Threats; Cyber warfare; Cyber Reflections.*

مقدمة

شهد العقد الأخير من القرن الماضي تطورات معتبرة على مستوى تكنولوجيا المعلومات والاتصالات وشبكات الإنترنت على اختلاف استعمالاتها، صاحب ذلك تطورٌ ملحوظ في نشاطات الجريمة الإلكترونية والتهديدات الأمنية التي تستهدف المجال السيبراني للدول ضمن الفضاء الإلكتروني في إطار ما يسمى بـ "الحرب الإلكترونية".

مما حتم على دول العالم على اختلاف مستوياتها الاقتصادية والاجتماعية للتعاون البيني، في سبيل البحث عن إستراتيجيات وميكانيزمات فعالة كفيلة بالتصدي لهذا النوع من التهديدات، التي تعمل على تحطيم البنية التحتية الإلكترونية للدول ومنظوماتها الأمنية، الاقتصادية والعسكرية وتعطيل مصالحها المادية والمعنوية، خاصة في وقت شملت فيه الرقمنة والتكنولوجيا معظم القطاعات السيادية للدول، ومنه فقد توجب على الباحثين والدارسين في هذا المجال الإحاطة بالجوانب المفاهيمية والنظرية للأمن السيبراني، والإحاطة بالتهديدات ذات العلاقة لتسهيل عملية التحكم أو على الأقل التصدي لمجموعة الاعتداءات التي تسعى لشل المنظومات الأمنية الإلكترونية للدول والحكومات، ومنه فالإشكالية التي يتوجب معالجتها في هذا المقال تتمحور حول: **ما مدى خطورة انعكاسات التهديدات الأمنية السيبرانية على الأمن القومي للدول؟**

يتم دراسة حلول الإشكالية من خلال اقتراح فرضية كإجابة مؤقتة قائمة على ضرورة معرفة مكنونات الأمن السيبراني لتيسير محاولات الإحاطة بمضامين الهجومات السيبرانية، وهي: كلما كانت التهديدات الأمنية السيبرانية معقدة ومكثفة وموجهة ضد المنظومات الإلكترونية للدول الخصم، كلما كانت تداعياتها خطيرة على الأمن القومي لهذه الدول، لذلك بالاستعانة بمجموعة من المناهج والمقاربات منها: المقاربة التاريخية التي تبحث في تطور التهديدات الأمنية من التقليدية إلى الحديثة ثم السيبرانية، والمقاربة القانونية التي تسعى لتأصيل التهديدات الإلكترونية وفق القانون الدولي والاتفاقيات الإطارية، والمنهج المقارن للمقارنة بين مختلف التهديدات وسبل المواجهة، بهدف الوصول إلى إجابات دقيقة وشاملة.

أولا: الأمن السيبراني

تسعى الدولة الوطنية في ظل التطور التكنولوجي والرقمنة إلى ضمان أمنها السيبراني الوطني، في وقت أصبحت فيه التهديدات الأمنية ذات العلاقة تتحكم في مصير الدول والشعوب.

1. مفهوم الأمن السيبراني Cyber Sécurity

بدأ مفهوم الأمن السيبراني يحظى بالاهتمام الواسع منذ استخدامه من طرف الرئيس الأمريكي "باراك أوباما" عام 2009، واعتبره سببا لتعزيز الأمن القومي لبلاده، كما اعتبرت التهديدات القادمة من الفضاء السيبراني من أكبر التحديات الأمنية والاقتصادية التي واجهتها الولايات المتحدة الأمريكية (سلمان الشمري، 2021، صفحة 154).

فالصعود المتسارع لتكنولوجيا المعلومات زاد من حجم التعقيد وتغلغل الإنترنت والتقنيات المتصلة بالشبكة، أثر ذلك على الحياة اليومية للسكان خاصة باستعمال ذلك في المجال العسكري والدفاع، بسبب كون هذه التطورات تمثل عالما تقنيا بحتا مما عقد من آثارها الاجتماعية والثقافية، إضافة إلى ظهور

التهديدات السيبرانية بلغة الخيال العلمي مما صعب فهمه على الفنيين وغيرهم (Richards, 2014, pp. 7-8).

1.1. تعريف الأمن السيبراني والفضاء السيبراني

يشير مفهوم الأمن السيبراني إلى مجموعة الأدوار الجديدة للقوانين والسياسات والأجهزة والآليات، التي تعمل على إدارة المخاطر وتنظيم وتطوير الإجراءات والممارسات التكنولوجية المستخدمة لحماية السكان وممتلكاتهم المادية والمعنوية، كما يعتبر الأمن السيبراني مجموعة من العمليات التقنية الحديثة التي تحمي الشبكات والبيانات وأجهزة الكمبيوتر من الهجمات الإلكترونية وطرق الوصول غير المصرح بها(كاظم السدحان، أفريل 2021، صفحة 193).

أما "الفضاء السيبراني" فهو: "المجال العالمي لبيئة المعلومات الذي يتميز من خلال استخدام الاليكترونيات والطيف الكهرو - مغناطيسي، بهدف إنشاء وتخزين واستغلال وتبادل المعلومات عبر شبكات مترابطة باستعمال وسائل الاتصال المعلوماتية، وهذا الفضاء كبيئة افتراضية يتم فيه إنشاء أنواع مختلفة من المعلومات وتخزينها ونقلها عند الحاجة، يؤثر ويتأثر بالعالم المادي بعلاقة قائمة على نظرة تكاملية بين العالمين ذات مزايا ومخاطر معينة"، كما ساهم في جعل الأمن السيبراني ينتقل من مستوى الدولة إلى مستوى النظام الدولي، ليشكل بذلك نوعا من الأمن الجماعي العالمي (حسن المشهدي، د.س.ن، صفحة 241)، بالنظر إلى وجود تهديدات سيبرانية عالمية مشتركة تهدد المجتمعات قاطبة.

وهذا الفضاء يختلف عن الفضاء الجغرافي المعروف لكنه يتشارك معه في خصائص متعددة، فالمركب الأمني حسب كل من "بوزان" و"وايفر" و"جاب دو وايلد" ليس موضوعيا بمعنى الاستقلال عن الجهات الفاعلة في كثير من التحليلات الأمنية التقليدية، فهو يخضع إلى إعادة تعريف متكررة في ظل ظهور تهديدات جديدة يصعب التحكم في تغيراتها، فالمنطقة أصبحت ببساطة ساحة للأمن غير متأثرة بالسياسات الأمنية، حيث يقولان إننا نجادل هنا بأن الأمن ليس قضية موضوعية بل هو نتاج سلوك الفاعلين، وينظر إلى المركب الأمني كبناء استطرادي من قبل الجهات الفاعلة(Buzan, Waever, & De Wild, 1998, p. 20) .

2.1. تأمين البنية التحتية الإلكترونية

ينظر إلى البنية التحتية الحيوية Critical Infrastructure باعتبارها الأنظمة والوظائف الرئيسية التي يؤدي تعطيلها أو تدميرها إلى آثار كبيرة على الصحة العامة، التجارة والأمن القومي للبلد، فالأمن السيبراني يتكون من عناصر مادية تقنية كالمرافق والمباني وغرف البيانات وأخرى افتراضية ذكية.

فالبنية التحتية كمسألة حاسمة في وظائف الدول الأساسية تقدم خدمات مختلفة في عدة مجالات متعددة وفي نفس الوقت تعتبر مستهدفة ومعرضة للتهديدات السيبرانية، أهمها:

- الاتصالات وتكنولوجيا المعلومات: كشبكات الاتصالات المتعددة، والكوابل البحرية الأرضية والأقمار الصناعية... التي تشكل صلب الاقتصاد الرقمي، كونها تعتمد في تشغيلها على برامج الحاسبات كنظام "سكادا" Scada في محطات الطاقة الكهربائية، إضافة إلى قطاعات الطاقة الأخرى وقطاع الصحة.

وبالتالي فإن حدوث أي عطل في البنية التحتية الحيوية للمعلومات ينعكس ذلك على قدرة الدولة في أداء مهامها في قطاعات متعددة، فمن شأن برامج الحماية أن توفر السلامة والصيانة الدائمة للمكون الافتراضي للمعلومات (زهير البابلي، جوان 2021، صفحة 31).

2. عناصر الأمن السيبراني

تتمثل عناصر الأمن السيبراني خصوصا في عناصر الجغرافيا السياسية التي أصبحت مجالا لمساحة المعلومات، وتجاوزت المكانية التقليدية كما أثرت بعمق في الفضاء الجغرافي المكاني التقليدي، ففضاء المعلومات جعل من الجغرافيا السياسية ذات ميزة مكانية جديدة، حيث كان التحدي السابق يتمثل في البحث عن كيفيات الدفاع عن الحدود التقليدية بين الدول، فساهمت التقنيات الحديثة ونظم الشبكات والمعلومات في إضعاف الجغرافيا وأصبحت من السهل اختراقها، كما تغيرت مجالات السيادة الوطنية من المناطق البرية والبحرية والمجال الجوي إلى حدود المعلومات فتغير التفكير الجيو-سياسي التقليدي القائم على العوامل الطبيعية، وأصبحت حدود المعلومات جزء مهما من الأمن القومي للدول (حسن المشهدي، د.س.ن، صفحة 242).

1.2. الركائز الإستراتيجية للأمن السيبراني

تتطلب الإستراتيجية الوطنية للأمن السيبراني استمرارية سياسية ورؤية طويلة الأمد، لذلك فقد تكاتفت الجهود الدولية من أجل تعزيز الثقافة العالمية حول الأمن السيبراني، ومنه تطوير "الإتحاد الدولي للاتصالات" مؤشرا عالميا للأمن السيبراني GCI يقيس مستويات التنمية في كل بلد في هذا المجال، مهمته تقييم مدى التزام الدول بالأمن السيبراني من خلال خمسة ركائز أساسية، هي:

- التعاون بين الدول في هذا المجال.

- استخدام تقنيات حديثة في القضاء على الهجمات السيبرانية.

- تنظيم العمل المشترك للحد من هذه الهجمات.

- استخدام الأساليب التوعوية، وكذا استخدام الإطار القانوني بهدف تعزيز الشراكة والتعاون وتعيين الحد الأدنى من متطلبات الأمن ودعم تنفيذ القانون (كاظم السدحان، أفريل 2021، صفحة 198).

2.2. الأمن السيبراني والأمن القومي

نتيجة التقدم العلمي في المجال التكنولوجي اتخذت التهديدات أشكالا جديدة كالجريمة الإلكترونية والإرهاب الإلكتروني، وتعد هذه الجرائم موجهة ضد الأمن العام بالدول والمؤسسات التي تضمن الأمن القومي لأفرادها، لذا فقد تطور هذا الأخير ليواجه هذا النوع من التهديدات واتسع مجاله ليشمل مجالات غير عسكرية لحماية أجهزة الحكومة الإلكترونية التي أصبحت تتعرض لهجمات الهاكرز، أو لهجمات أجهزة الاستخبارات والجوسسة للبلدان المعادية الساعية لاختراق المنظومة الأمنية المعلوماتية للدول الخصم (حسن المشهدي، د.س.ن، صفحة 244)، مما حتم ضرورة البحث في إيجاد الطرق الكفيلة للردع السيبراني.

3. مفهوم الردع السيبراني Cyber Deterrence

عمليا يحمل الردع معنى المنع، فهو مانع للفعل من الحصول بناء على مخاوف وشكوك من النتائج، وغالبا ما يشير المصطلح إلى نوعين من الأفعال هما: العقاب والمنع، فالأول يعني شل قدرة الطرف الآخر على الهجوم أو رد الفعل، أما الثاني فيدل على عملية التحضير للدفاع عبر جملة من الإجراءات المضبوطة.

ومنه فالردع السيبراني هو "منع الأعمال الضارة الممارسة ضد الأصول الوطنية في الفضاء والتي تدعم العمليات الفضائية"، يقول الجنرال الأمريكي "كارتيرايت" Catwright عن الردع السيبراني "إننا بحاجة لتطوير قدراتنا في الفضاء السيبراني لمواجهة ما قد يريده الآخرون فعله تجاهنا" (بونيف، جوان 2019، صفحة 128).

1.3. خصائص الردع السيبراني ومرتكزاته

يختلف الردع بالمفهوم التقليدي عن الردع السيبراني نظرا لوجود عدة عوامل أهمها:

1.1.3. وجود فواعل جديدة من غير الدولنظرا لتغير طبيعة النزاعات والصراعات الدولية وتحول مستوياتها وفواعلها من دولية إلى ما دون الدول، يمكن تمييز الفواعل البارزة في الفضاء الإلكتروني من مجموعات المصالح الخاصة والناشطين من أجل قضية واحدة، وحركات الاستقلال الذين اكتسبوا منابر عالمية عبر الانترنت مكنتهم من تعزيز وجهات نظرهم من جهة، كما حددوا سكان الفضاء الإلكتروني، ومنه يمكن للأشخاص أن يكونوا مستخدمين للإنترنت ومواطنين في الوقت نفسه من جهة أخرى، لكن فقط في شبكة الإنترنت تتآكل جنسية الدولة القومية نظرا لخصائصها المحددة.

2.1.3. طبيعة الفضاء السيبراني: ليس له مساحة ملموسة ولا حدود لطبيعته ويعتمد على البنية التحتية المادية المتمثلة في الكابلات وأجهزة الكمبيوتر، وحلول الإنترنت محل المفاهيم التقليدية للأراضي والملكية في ظل غياب أية حدود إقليمية في هذا الفضاء الجديد.

3.1.3. مصداقية التهديد: كسمة بارزة لإستراتيجية الردع في ظل الاشتراط على الطرف الأول أن يظهر التهديد الحقيقي، فقد كتب "توماس شيلينغ" Thomas Schelling في هذا المعنى "كقاعدة عامة يجب على المرء أن يهدد بأنه سوف يتصرف وليس أنه قد يتصرف إذا فشل التهديد"، لكن في حالة الفضاء السيبراني وعدم مرئية وسائل التهديد على خلاف الأسلحة التقليدية فيجعل تلك التهديدات افتراضية.

4.1.3. عدم الكشف عن الهوية: وهي ميزة قد منحت القدرة على التصرف بشكل مجهول عبر الإنترنت كقيام الإرهاب والكيانات الأخرى استعمال الفضاء الإلكتروني لتمرير رسائلهم والقيام بعمليات التجسس وتنظيم وتنفيذ الأعمال التخريبية، في ظل فشل المسئولين في حماية الأفراد ومتابعة الجناة جزائيا(قوادرة، 2020، صفحة 129).

يقوم الردع السيبراني على مجموعة مرتكزات تتمثل في:

- **الردع من حيث النوع:** ومن خلاله يمكن التمييز بين نوعين من الردع يشير الأول لعملية الردع بالمنع، ينطوي تحته ما يسمى الردع بالمقاومة، أما الثاني فهو الردع بالصمود وهو القدرة على استعادة الشيء بشكله الأصلي قبل الهجوم ما من شأنه أن يحد من المكاسب المحتملة.

- **الردع من حيث الفعل:** يستند حدود الفعل في الردع على ثلاث (03) ركائز أساسية هي:

- مصداقية الدفاع عن أنظمة المعلومات ومنع أي محاولة لاختراقها عبر توافر أنظمة نسخ احتياطية، مما يعني أن أي هجوم لن يسفر عن التدمير الكلي في ظل إمكانات الاستعادة الذاتية.
- القدرة على الانتقام التي تتطلب وجود آليات للرد على الهجمات ما يمنح الطرف المتعرض للهجوم القدرة على إعادة بناء الذات وتحقيق التوازن مع الطرف المهاجم.
- عملية الرغبة في الرد، أي وجود نوايا للرد مع وجود القدرة على القيام بالفعل.

- **الردع من حيث المتطلبات:** وهي مجموعة من الأساليب التي تضمن عملية الردع السيبراني في شكل خيارات وإجراءات تتخذ لمواجهة الهجمات المحتملة، تتمثل في:

- **الردع السلبي:** وهو الرد على الهجمات مع الاعتراف بأن مسألة أمن المعلومات المتعلقة بها لا تزال غير كافية.
- **الإجراءات الدبلوماسية والقانونية:** وهي مجموعة الخطوات التي تعتمد على الاستجابة الرمزية ضد الطرف المهاجم، بطرد البعثة الدبلوماسية مما قد يتسبب في زعزعة الطرف المعتدي دوليا، أو توجيه اتهامات ضد الأفراد والمنظمات التي تضطلع بهجوم سيبراني.
- **العقوبات الاقتصادية والأعمال الانتقامية:** بفرض عقوبات مالية أو غرامات ضد المتسببين، سواء برد الفعل بنفس وتيرة الهجمات أو تجاوز الحد المطلوب (بونيف، جوان 2019، صفحة 129).

2.3. تحديات الردع السيبراني

يواجه الردع السيبراني في مرحلة التنفيذ مجموعة من التحديات والعراقيل، أهمها:

1.2.3. مشكلة الإسناد: التي تجعل من عملية الردع السيبراني عديم الجدوى بسبب ضعف القدرة على معرفة المتسبب، لذا اعتبرت هذه المشكلة عاملا حاسما في الحد من فعالية الردع مما يقوض مصداقية التهديد بالانتقام.

2.2.3. تحدي فهم الدوافع العدوانية ومستوى تحمل المخاطر: وفقا لهذه المشكلة يجب تصنيف التهديدات السيبرانية إلى عدة فئات، تبعا لطبيعة الفواعل التي سيكون لكل منها دوافع وقدرات مختلفة، وهي: الفواعل الإجرامية، الفواعل العنيفة من غير الدول والفواعل الحكومية أو التي ترعاها الدول، كما أن القدرة على المعاقبة محدودة وتعتمد على إنفاذ القانون والتعاون الفعال من قبل الدول الأجنبية (قوادرة، 2020، صفحة 524).

ثانيا: التهديدات السيبرانية- مقاربة نظرية

يعتبر ظهور الفضاء الإلكتروني سببا في تغيير ضوابط ومحددات السياسة الدولية وتفاعلاتها، فظهر الأمن السيبراني كتحدي و/أو كحاجة أمنية ملحة للدول ذات السيادة، فعلى المستوى الأكاديمي فإن الصراع السيبراني قد بدأ مع قيام كل من "رونالدت" Ronaldt و"أركيلا" Arquilla بتطوير مفهوم الحرب الإلكترونية Netwar في تسعينيات القرن الماضي، واعتبر هذا الأخير موضوعا هاما في نظريات العلاقات الدولية لكونه يتضمن مواضيع السيادة والأمن القومي والقوة.

وعلى الرغم من كون العنصر الأكثر حضورا في الحرب هو "عمل القوة" في صورتها المادية وأنه يمكن لنظام الأسلحة المبرمج تحديد الهدف بشكل شبه ذاتي، إلا أن الاستخدام الفعلي للقوة في الحرب الإلكترونية يكون أكثر تعقيدا في تسلسل الأسباب والتداعيات، حيث يمكن مثلا للقوات الصينية تغطية مدينة أمريكية كبيرة بانقطاع في التيار الكهربائي عن طريق تفعيل ما يسمى بـ "القبائل المنطقية" Logic Bombs المركبة مسبقا في شبكة الكهرباء الأمريكية (Rid, 2013, p. 3) ، والمتحكم فيها إلكترونيا عن بعد وذات تداعيات خطيرة على الاقتصاد، والسياسة والأمن القومي الأمريكي.

1. مدخل نظري للفضاء الإلكتروني ومضامينه

يرى "جوزيف ناي" Josef S.Nye أن القوة ارتبطت بالسياق والنمو السريع للفضاء السيبراني الذي أصبح مجالا مهما في السياسة الدولية، حيث أن انخفاض تكلفة الدخول وعدم الكشف عن الهوية وعدم التماثلية في الإنكشافية أعطى فرصا متساوية للفواعل على اختلاف أحجامها وأهميتها لتكون لها القدرة على ممارسة القوة الصلبة والناعمة في هذا الفضاء مقارنة بالواقع التقليدي السابق.

1.1 الواقعية الجديدة: ركزت الواقعية الجديدة على الفضاء السيبراني كضابط لتوازنات القوة الداخلية والخارجية، فاعتبر "روبرت جيرفيس" Robert Jervis التكنولوجيا أحد أهم محددات التوازن الهجومي-الدفاعي للدول وبأقل تكلفة وذات فعالية في التسبب في حالات اللاأمن، أما "ريتشارد" Richard فقد أكد على أن الدول تعمل على زيادة قوة دفاعها السيبراني كجزء من دفاعها العسكري كالصين وروسيا، من خلال التحكم في الإنترنت وتصفية الفضاء السيبراني على أراضيها بما يضمن لهما الدفاع السيبراني الضروري (شرايطية، 2020، صفحة 399).

2.1 الليبرالية الجديدة: يرى النيو- ليبراليون أن الفضاء الإلكتروني يضعف من سيادة الدول في ظل وجود فواعل دولاتية وغير دولاتية متعددة، ازدادت قوتها وقدراتها بسبب ثورة المعلومات، كما أكدوا على أنه يجب على الدول من أجل تأمين فضائها الإلكتروني إبرام العديد من المساقات والتنظيمات والاتفاقات الدولية لخلق السلام عبر الإنترنت والتعامل بفعالية مع الحروب الإلكترونية وتحقيق الأمن.

3.1 البنائية: اعتقد البنائيون أن تكوين الهويات والمصالح يكون من خلال مسار اجتماعي مثلها مثل الحروب السيبرانية، وركزوا على دور البناء الهوياتي في الحرب الإلكترونية، فالتعرض لهجوم من جهة تحمل نفس الهوية يعتبر تجسسا، لكن إذا صدر الفعل من عدو فإنه يعتبر هجوما إلكترونيا، ومنه فإن مشاركة القيم والمعايير واحترام الهويات يقلل من احتمالية حدوث حروبا إلكترونية أو هجمات سيبرانية، كما اعتبر كل من "وندت" Wendt و"دوفال" Duvall أن عالم الإنترنت يتطور فيجب معه الاستمرار في توسيع المسئولية لدى الحكومات بهدف السيطرة على فضائها الإلكتروني (شرايطية، 2020، صفحة 400).

2. نظرية القوة السيبرانية العالمية

من خلال تقييم مقاربات الجيو- بوليتيك تم التوصل إلى نظرية القوة السيبرانية، التي رأت أن القوة السيبرانية يجب أن تركز على أربعة (04) عوامل رئيسية، هي: التقدم التكنولوجي، سرعة نطاق العمليات، السيطرة على السمات الرئيسية والتعبئة الوطنية، وتماشيا مع هذه الميزات تبين أن الاعتماد على الفضاء الإلكتروني أدى إلى نقاط ضعف كونه عرضة لمجموعة من التهديدات، كهجمات رفض الخدمة والفساد المحتمل للبيانات الحساسة، لكن نظرا لانتشار التكنولوجيا المتطورة للفضاء الإلكتروني، فقد تعززت سرعة

ونطاق العمليات مثل القدرة على إشراك أهداف حساسة بنجاح في أي مكان من العالم، مما حسن في القدرة على التحكم والقيادة وقلل من تركيز عمليات مراقبة الأزمنة الكلاسيكية (حسن المشهدي، د.س.ن، صفحة 252).

1.2 الحرب السيبرانية Cyber Warfare: يعد مصطلح الحرب السيبرانية مفهوما جديدا على صعيد النزاعات المسلحة في القرن الـ 21م، تشتمل هذه الحرب على أساليب ووسائل قتالية تتألف من عمليات إلكترونية ترقى إلى مستوى النزاع المسلح أو تستخدم في سياقه، تعمل هذه الحرب على الإخلال أو التدمير الكلي لأنظمة المعلومات وشبكات الاتصال التابعة للعدو، عرفتها مؤسسة "راند" RAND بأنها: "حرب الدول والمنظمات الدولية ضد دول أخرى من أجل تدمير شبكات الكمبيوتر والمعلومات، تتم عن طريق الفيروسات، أحصنة طروادة والبرمجيات الخبيثة"، كما لا يمكن تحديد وقت بدئها وانتهائها (عبيس نعمة و كلنتر، د.س.ن، صفحة 52).

2.2 قياس القوة السيبرانية/ العسكرية: أدى تطور المجال السيبراني إلى تعقيد هذه الصورة من حيث كيفية تبني القوات المسلحة للتكنولوجيا، والبحث فيما يشكله الاستخدام العسكري في مجال يكون فيه المستخدمون المدنيون والعسكريون متشابكا بشكل كبير، فقد عملت الدول القومية لامتلاك أفضل فهم ممكن لقدرات الأعداء المحتملين، على إبراز القوة في المجال العسكري كأداة حيوية في فن الحكم، والعمل على إنشاء فروع منفصلة كقوة الدعم الإستراتيجي في الصين أو القيادة السيبرانية في الولايات المتحدة الأمريكية (حسن المشهدي، د.س.ن، صفحة 248).

ثالثا: التهديدات الأمنية السيبرانية وانعكاساتها

تختلف التهديدات الأمنية السيبرانية باختلاف مصادرها والفواعل التي تقف ورائها، لذلك وجب تحديد تعريفاتها ومدلولاتها على اختلافها وسبل مواجهة انعكاساتها على الأمن القومي للدول.

1. مفهوم التهديدات السيبرانية

هناك اتجاهين رئيسيين مختلفين في تعريف هذا النمط من التهديدات هما: الاتجاه الضيق الذي يركز على موضوع الهجوم وهو ما تبنته الولايات المتحدة الأمريكية وحلفائها، كما تبنت منظمة "شنغهاي للتعاون" نهجا أكثر توسعا بينت فيه عن قلقها بشأن التهديدات التي تشكلها إمكانية استخدام وسائل المعلومات والاتصالات الحديثة لأغراض تتنافى مع ضمان الأمن والاستقرار الدوليين.

1.1 تعريف الجريمة السيبرانية وأنواعها Cybercrime: جاء ضمن إرشادات "الإسكوا" ESKWA للتشريعات السيبرانية، أن الجريمة السيبرانية تنقسم إلى نوعين أساسيين هما: النوع الأول الذي يكون فيه الحاسوب أداة تنفذ بواسطتها الجريمة، والنوع الثاني يكون فيه جهاز الحاسوب وشبكاتها وبرامجها موضوعا للجريمة، أي أن الفعل الإجرامي ارتكب على هذا الجهاز"، بهدف تحقيق مكاسب مادية أو إثبات الفاعل لمهارته الفنية وقدرته على التحكم والاختراق (عبيس نعمة و كلنتر، د.س.ن، صفحة 52).

2.1 مظاهر التهديد السيبراني للأمن الدولي وخصائصه تعتبر التطورات التكنولوجية والرقمية أحد الإفرازات العولمية التي تم الاستعانة بها في الصراعات الدولية، من خلال التوظيف الفعال لمختلف الأسلحة المتطورة، كما مثل تنظيم "داعش" أكبر تهديد لسلامة شبكة الإنترنت العالمية، وبالتالي فإن أهم مظاهر هذه التهديدات السيبرانية للأمن الدولي والأمن القومي للدول تتمثل في:

- استخدام نظم المعلومات في الدعاية والتجنيد والتمويل وجمع المعلومات.

- تنسيق الهجمات الإرهابية وحشد المتعاطفين ونشر أفكار التطرف وسط الشباب، ففي هذا الإطار حدد "أبو بكر ناجي" في كتابه "إدارة التوحش" أساليب توظيف الإعلام الجهادي لتنظيم داعش من خلال:

1.2.1. فئة الشعوب: وذلك بالعمل على دمج أكبر عدد منهم في صفوف الجهاد ودعمها.

2.2.1. جنود العدو: بالتركيز على الفئات الهشة والموظفين ذوي الدخل الضعيف للزج بهم في صفوف الجهاد (حكيم، 2018، صفحة 108).

أما خصائص الجرائم والتهديدات السيبرانية فتتمثل في:

- التهديدات السيبرانية تتم ضمن بيئة رقمية معلوماتية من خلال أجهزة ومعدات الحاسب الآلي ومكوناته البرمجية.

- يقوم بالجريمة الإلكترونية مجرمون ذو طبيعة خاصة وبإمكانات خاصة –معلوماتية- شديدة التطور والتعقيد، وبأساليب بالغة الاحترافية وصعبة المقاومة.

- أسلوبها هادئ لا يتطلب العنف كالجرائم التقليدية من خلال التعامل الدقيق مع التقنية.

- صعوبة الحصول على دليل مادي لإثبات هوية مرتكبيها بسبب غلبة الطبيعة الإلكترونية.

- لا يخضع هذا النوع من التهديدات للحدود الوطنية ولا للأبعاد الجغرافية ولا تحكمها عوامل الزمان والمكان (الردفاني، 2014، صفحة 163).

2. تكييف التهديدات السيبرانية في القانون الدولي

إن تنامي استخدام شبكات المعلومات في شتى المجالات وتنوع التهديدات الناجمة عنها شكل تحديا كبيرا للتنظيم الدولي المعاصر مما دعا إلى تكييف هذه التهديدات ضمن القوانين الدولية.

1.2. الحرب السيبرانية في القانون الدولي الإنساني: تم تكييف الهجمات السيبرانية ضمن "قانون الحرب" والقانون الدولي الإنساني، بسبب أن القانون الدولي يميز بين النزاع المسلح وأسباب النزاع المسلح، لأن الغاية من القانون هو منع الحروب والناعات و/أو حماية ضحايا النزاعات المسلحة بغض النظر عن انتماءاتهم، من خلال تنظيم جوانب النزاع ذات الأهمية الإنسانية، وتسري أحكامه على أطراف النزاع، أما قانون الحرب فيبحث في مدى مشروعية اللجوء إلى القوة المسلحة لأن الهجمات السيبرانية تشكل تهديدا للمبادئ الرئيسية في القانون الدولي، لما تتضمنه من اختراق لمعلومات أمنية وعسكرية سرية وتقويض الامتناع عن الاستخدام غير المشروع للقوة نظرا لما تخلفه من أضرار بالغة على السير الحسن والعادي لعمل الدول والحكومات(عبيس نعمة و كلنتر، د.س.ن، صفحة 55).

2.2. دليل "تالين" بشأن الحروب السيبرانية: صيغ هذا الدليل من طرف مجموعة خبراء بناء على طلب "مركز الامتياز التعاوني للدفاع عن الفضاء الإلكتروني"، وسمي تالين - نسبة إلى عاصمة استونيا- وهو الإجراء الأمثل لتفسير قواعد القانون الدولي.

قدم تالين رؤى حول الحرب الإلكترونية من خلال تمسكه بالثنائية التقليدية للنزاعات المسلحة غير الدولية، ويقر بأن العمليات الإلكترونية قد تشكل وحدها نزاعات مسلحة تبعا للظروف، كما ركز الدليل على "الضرر" الذي من الممكن أن تحدثه هته الحرب، وأكد على ضرورة احترام مبدأي "الاحتياط" و"التناسب" في حال تعرض شبكة الإنترنت إلى الهجوم، مع الاستعانة بالخبرة التقنية الموجودة لمساعدتهم في تحديد ما إذا كانت التدابير الاحتياطية الملائمة قد اتُخذت، ومن ثم القدرة على تقييم طبيعة الهجوم والخسائر والأضرار العرضية بين المدنيين غير متاحة، فقد يتعين على المهاجم أن يقوم بالامتناع عن الهجوم (بن تغري، 2020، صفحة 210).

3. الجهود الوطنية والدولية لمكافحة التهديدات السيبرانية

على المستوى الوطني معظم الحكومات تعترف بضرورة إعادة توزيع الموارد وإصلاح الإستراتيجيات الأمنية الوطنية، من خلال زيادة التمويل لبحث الموارد التكتيكية والدبلوماسية لتعزيز أمنها السيبراني، أما دوليا فيعتبر الحوار العالمي والتعاون ضروري نظرا لكون المعايير القانونية الدولية غير مجهزة للتعامل مع هكذا تهديدات. بابتكار تطبيقات ذكية مع مسح "ببليومتري" لأحدث تقنيات البرمجة السيبرانية لتحليل الحالات الطارئة المتعلقة بالإنترنت والمهددة لأنظمة الطاقة الذكية كإستراتيجية هجومية قادرة على المساومة على مستوى الشبكة(Karimipour & Other, 2020, p. 3) .

1.3. أساليب مواجهة الحرب السيبرانية: من الضروري بمكان أن تعمل الدول على التنسيق من أجل مواجهة الحروب السيبرانية، وذلك من خلال:

- وضع إطار قانوني وتنظيمي مشترك مع إقامة نظام لتحديث هذه القوانين لمعالجة الطبيعة المتغيرة للتهديدات.

- إصدار معايير دولية وقواعد سيبرانية كوسيلة لتحسين الأمن السيبراني على الصعيد الدولي بإصدار مبادئ توجيهية لتحقيق هذا النوع من الأمن.

- ضرورة النظر في الخصائص المميزة للفضاء السيبراني وإبراز التحديات التي تطرحها هذه السمات، وذلك بالعمل على تطوير نموذج للتشريعات المتعلقة بالجرائم السيبرانية يكون قابلا للتطبيق على الصعيد العالمي (بن تغري، 2020، صفحة 211).

- إجراءات التشغيل المعيارية لحوادث الإنترنت والتهديدات تشمل الأنشطة التي وضعها الخبراء والمتخصصون السيبرانيون خلال فترت الاستقرار النسبي، بالرجوع إلى معرفة طبيعة الهجمات التي تستهدف تعطيل الأنشطة التجارية للدول(Kacprzyk, 2021, p. 2) .

2.3. الإجراءات الاستباقية لمواجهة خطر التهديدات السيبرانية: تتعدد الأساليب الاستباقية للتصدي للهجمات السيبرانية وتختلف باختلاف طبيعتها، فتنقسم إلى صنفين هما:

1.2.3. الإجراءات الهجومية: يتم استخدامها ضد أطراف معينة قد تشكل خطرا مستقبلا على بياناتها، تعتمد على عملية إطلاق فيروسات أو ديدان إلكترونية تهاجم الخصم بشكل فجائي، كما يتم الاعتماد على طريقة

الأبواب الخلفية القائمة على استغلال ثغرات أنظمة العدو وإستراتيجية حجب الخدمة، تهدف كلها بشكل عام إلى زعزعة القدرات الهجومية للعدو.

2.2.3. الإجراءات الدفاعية: تتمثل في تطوير الذات وتقوية القدرات لمواجهة الأخطار المحتملة، تتمثل في عدة أبعاد أهمها:

1.2.2.3. البعد العسكري: وهو عملية الحماية الأمنية للمعلومات من خلال بلورة أنظمة للدفاع السيبراني ذات مستوى عالي من الدقة والسرية.

2.2.2.3. البعد الاجتماعي: من خلال تأمين البيانات للأفراد تتراوح ما بين أساليب الردع القانوني كمعاقبة المخترقين للحسابات الشخصية وسرقة ملكية المعلومات.

3.2.2.3. البعد السياسي: يتمثل في امتلاك الدولة لحق حماية نظامها السياسي ومصالح مواطنيها بإتباع إجراءات محلية أو خارجية قائمة على التوافق الدولي لحماية الأمن السيبراني (بونيف، جوان 2019، صفحة 127).

خاتمة:

تعتبر التهديدات الأمنية السيبرانية وما ينجر عنها من حروب إلكترونية مهددة للأمن الدولي بصفة عامة والأمن القومي للدول بصفة خاصة، وليدة التطور الكبير الذي شهدته نظم المعلومات والاتصالات كصورة من صور الحركيات العولمية التي جعلت من العالم عبارة عن "قرية صغيرة".

ونظرا لما باتت تشكله هذه التهديدات من عراقيل وصعوبات في سبيل تطور وازدهار الدولة في محيطها الإقليمي، فقد دأبت الجهود الدولية لتكثيف التعاون والتنسيق في مجال البرمجيات والصناعات الإلكترونية المجهرية، إلى البحث في الإستراتيجيات والميكانيزمات التي يمكن من خلالها التصدي لمخاطر وانعكاسات هذه التهديدات على المجالات الحيوية للسكان.

ومنه نستنتج أنه كلما كانت التهديدات السيبرانية والهجمات والحروب الإلكترونية شديدة التعقيد والتشابك والتطور التكنولوجي، كلما أثر على أمن الدول واستقرارها في مختلف المجالات السياسية والاقتصادية، والذي يتطلب معه لمقاومة هذه الحروب والتقليل من تداعياتها تسخير كافة الطاقات المادية– تكنولوجيا ووسائل حديثة ومتطورة-، وطاقات بشرية –تشتمل على الخبراء والتقنيين في مجالات الحوسبة والحروب الهجينة بالغة التطور والتعقيد.

المراجع:

- Buzan Barry & Waever Ole & De Wild Jaap, **Security: A New Framework For Analysis**, (United Kingdom: Lynne Rienner Publishers, Inc, 1998).

- Kacprzyk Janusz, **The Syber Security Network Guide**, (S. N. Suitzerland, Ed: Systems research institute, Polish academy of sciences, 2021).

- Karimipour, Hadis, & Other, **Security of Syber- phisical Systems**, (Springer nature Switzerland, 2020).

- Richards Julian, **Cyber- War: The Anatomy of the Global Security Threat**, (United kingdom: palgrave makmilian university buckigham, 2014).

- Rid Thomas, **Cyber War Will Not Take Place**, (New York: University Oxford Press, 2013).

- أحمد عبيس نعمة وزهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي ، **مجلة الكوفة** ، جامعة الكوفة، العدد 44/1، د.س.ن.

- تغريد معين حسن المشهدي ، الأثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة ، **مجلة البحوث الجغرافية**، العدد 30، د.س.ن.

- حسين قوادرة، الردع السيبراني بين النظرية والتطبيق، **المجلة الجزائرية للأمن والتنمية** ، المجلد 09، العدد 16، جانفي 2020.

- سامي محمد بونيف، دور الإستراتيجيات الاستباقية في مواجهة الهجمات السيبرانية- الردع السيبراني أنموذجا- ، **المجلة الجزائرية للحقوق والعلوم السياسية**، المجلد 04، العدد 07، جوان 2019.

- سميرة شرايطية، السيادة السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومي ، **المجلة الجزائرية للأمن والتنمية**، المجلد 09، العدد 16، جانفي 2020.

- ضحى العيبي كاظم السدحان، البعد الجيوسياسي للأمن السيبراني، **مجلة العلوم الإنسانية**، المركز الجامعي- علي كافي، تندوف، المجلد 05، العدد 01، أفريل 2021.

- عمار ياسر زهير البابلي، التحديات الأمنية المعاصرة للهجمات السيبرانية ، **مجلة الفكر الشرطي** ، مصر، المجلد 30، العدد 118، جوان 2021.

- غريب حكيم، الإرهاب السيبراني والأمن الدولي: التهديدات العالمية الجديدة وأساليب المواجهة ، **المجلة الجزائرية للدراسات السياسية**، المجلد 05، العدد 02، 2018.

- محمد قاسم أسعد الردفاني، تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية ، **المجلة العربية للدراسات الأمنية والتدريب**، الرياض، المجلد 31، العدد 61، 2014.

- مصطفى إبراهيم سلمان الشمري ، الأمن السيبراني وأثره في الأمن الوطني العراقي ، **مجلة العلوم القانونية والسياسية**، المجلد 10، العدد01، 2021.

- موسى بن تغري، الحرب السيبرانية والقانون الدولي الإنساني، **مجلة الاجتهاد القضائي**، العدد 22، أفريل 2020.