السنة: السابعة المجلد:07 العدد: 01 ص ص: 130- 151
EISSN 2676-1645 ISSN 2543-375X

الدولة بين الهيمنة وتحقيق الأمن في الفضاء السيبراني

The State, between dominance and security attainment in cyberspace

فاتح حارك*، جامعة قسنطينة 3
fateh.harek@univ-constantine3.dz
رياض حمدوش، جامعة قسنطينة 3
riad.hamdouche@univ-constantine3.dz

تاريخ الاستلام: 2021/07/18 تاريخ القبول: 2021/09/18

ملخص:

يناقش هذا المقال الأهمية الأمنية والإستراتيجية للفضاء السيبراني ودوره في التأثير على واقع الهيمنة وتحقيق الأمن في العلاقات الدولية، حيث أصبحت القوة أكثر انتشارا بسبب الخصائص الفريدة للفضاء السيبراني وتصميم الانترنت الذي بني على سهولة الإستخدام بدلا عن تحقيق الأمن .وهو ما فتح المجال واسعا أمام صعود قوى جديدة قادرة على التأثير على أي فاعل من فواعل العلاقات الدولية، الأمر الذي عقد من مهمة تحقيق الأمن.

انطلاقا من ذلك يهدف المقال إلى وصف وتفصيل كيفية انتشار القوة وواقع الهجمات السيبرانية بين الدول والمكاسب الكبيرة التي تجنيها من ذلك، بالإضافة للتطرق إلى المأزق الأمني السيبراني الذي يجعل من رقمنة قطاعات الدولة نقطة قوة وضعف في نفس الوقت، خاصة مع ظهور ما يعرف بانترنت الأشياء.

يخلص المقال إلى إبراز أهم التغييرات التي حملها الفضاء السيبراني في مجال الأمن، من بينها تعاظم دور الدول الصغيرة، بالإضافة إلى تغير القواعد المرتبطة

* المؤلف المراسل

بالدفاع والهجوم في الفضاء السيبراني، مع إشكالية تحقيق الأمن القومي في ظل التوجه الكلي نحو رقمنة كل القطاعات.

الكلمات المفتاحية: الفضاء السيبراني – القوة السيبرانية – الأمن السيبراني – البنية التحتية التكنولوجية – الأمن القومي.

Abstract:

This article discusses the security and strategic importance of cyberspace and its role in influencing the realities of dominance and security in international relations where power has become more prevalent due to the unique characteristics of the cyberspace and the design of the Internet built on the simplicity of usage rather than security .This fact has opened up the way for the rise of new powers capable of influencing all the actors in international relations and has also complicated the task of achieving security.

Building on this idea, this article intends to describe and explain in detail how power is spread, the reality of cyber-attacks among countries and the significant gains they make. It seeks too to address the cybersecurity dilemma that makes the digitization of State sectors a point of strength and weakness at the same time especially with the advent of the Internet of Things.

This article concludes by trying to highlight the most important changes that cyberspace has brought about in the field of security including the growing role of the small States in addition to the changing of the rules linked to defence and offence in the cyberspace, and the problematic achievement of national security in light of the overall trend towards the digitization of all State sectors.

Keywords: Cyberspace, Cyber Power, Cybersecurity, Technological Infrastructure, National Security.

مقدمة:

مع بداية القرن الواحد والعشرين، تسارعت الأحداث وتغيرت المفاهيم وشهدت مختلف النشاطات البشرية ثورة حقيقية بسبب التطور التكنولوجي الهائل الذي يشهده العالم اليوم، حيث انتشرت التكنولوجيا في جميع المجالات وأصبحت ركيزة محورية يستحيل تحقيق التقدم من دونها، وكغيره من الميادين تأثر ميدان العلاقات الدولية بهذا التطور التكنولوجي لدرجة عجز الكثير من المداخل النظرية عن مسايرة التغيرات الحاصلة، فأصبح من الضروري جدا إعادة النظر في مختلف المفاهيم التقليدية مثل الأمن والحرب والسيادة والقوة وغيرها.

إن تعدد الفواعل السيبرانية وسهولة استخدام الفضاء السيبراني واستهداف الخصوم وقابلية التعرض للأضرار، جعلت منه ميدانا فريدا من نوعه، كما ساهم انتشار القوة السيبرانية بين الدول والأفراد والجماعات في ظهور صراعات عديدة، وأصبح الفضاء السيبراني الحل الأمثل لتحقيق المكاسب عبر تنفيذ الهجمات السيبرانية خاصة بالنسبة للدولة القومية، بالإضافة إلى ذلك، أدت صعوبة تحديد مصدر الهجوم في الفضاء السيبراني بالدول إلى التسابق لشن الهجمات على بعضها البعض واستغلال هذا المشكل الذي يعتبر نقطة قوة وفي نفس الوقت نقطة ضعف.

كل هذه الأحداث دفعت بالدول خاصة الكبرى منها إلى محاولة تحقيق التفوق في الفضاء السيبراني، وفي نفس الوقت تحصين أمنها القومي من الهجمات السيبرانية مجهولة المصدر، ومن خلال ما سبق يمكن طرح الإشكالية التالية: كيف أدى التطور التكنولوجي إلى التأثير على سلوك الدول المرتبط بالهيمنة وتحقيق الأمن في الفضاء السيبراني ؟

كما سنحاول اختبار صحة الفرضية التالية: يرتبط اكتساب القوة وتحقيق الأمن في الفضاء السيبراني بمدى قوة الدولة على أرض الواقع.

وللإجابة على الإشكالية المذكورة أعلاه، تم الاعتماد على المنهج الوصفي عند التطرق لمختلف المحاور المرتبطة بالبحث.

المحور الأول: الإطار المفاهيمي

سنحاول من خلال هذا المحور التطرق لمفهوم الفضاء السيبراني والتعريج على مفهوم القوة السيبرانية بشكل يجعلنا نفهم الإطار العام للدراسة.

1ـ مفهوم الفضاء السيبراني:

مفهوم الفضاء السيبراني كغيره من المفاهيم في العلوم الاجتماعية، لا يوجد تعريف دقيق له خاصة مع التطور السريع الذي يشهده هذا المجال، وعليه سنحاول التطرق إلى مجموعة من التعاريف المختلفة بغرض الإحاطة به وتقديم مفهوم أشمل له.

قدم الباحثان بيتر سينغر Peter W. Singer وآلان فريدمان Allan Friedman تعريفا بقولهما : الفضاء السيبراني هو عالم شبكات الكمبيوتر والمستخدمين الذين يقفون وراءها حيث يتم تخزين المعلومات ومشاركتها ونقلها عبر الإنترنت. (Singer & Friedman, 2014, p. 14)

هذا التعريف يمثل المفهوم الضيق للفضاء السيبراني، إذ اقتصر تعريفه على أن الفضاء السيبراني يتشكل من أجهزة الكمبيوتر والمستخدمين الذين يتحكمون في تلك الأجهزة، بالإضافة إلى المعلومات المتبادلة عبر الإنترنت.

تعريف آخر للفضاء السيبراني يصفه بأنه مجال عالمي ضمن بيئة المعلومات يتكون من الشبكات المترابطة للبنى التحتية لتكنولوجيا المعلومات والبيانات المرتبطة بها ، بما في ذلك الإنترنت وشبكات الاتصالات السلكية واللاسلكية وأنظمة الكمبيوتر والمعالجات المدمجة وأجهزة التحكم. (Department of the Army, 2017, p. 12)

يؤكد هذا التعريف على عالمية الفضاء السيبراني ويعني ذلك أنه لا مكان للحدود الجغرافية هنا، وقد ركز هذا التعريف على أن ارتباط البنية التحتية لتكنولوجيا المعلومات والبيانات المتعلقة بها اضافة إلى الانترنت وشبكات الاتصال والمعالجات وأجهزة الكمبيوتر وأجهزة التحكم، تشكل لنا مايعرف بالفضاء السيبراني، ويعتبر هذا التعريف أكثر شمولا كونه يركز على عدة

عناصر أساسية، رغم أنه قد أهمل العنصر البشري والذي يعتبر عنصرا أساسيا في تشكيل مفهوم الفضاء السيبراني.

يعرفه مايكل فانبوت Michael A. Van Putte، بأنه هو مجموعة أجهزة الكمبيوتر والأشخاص المترابطين من خلال أنظمة الاتصالات، توجد هذه الأجهزة سواء على الأرض أول على المياه عن طريق السفن، في الجو عن طريق الطائرات، وفي الفضاء الخارجي عن طريق الأقمار الصناعية، ويتم تخزين كل تعليمات الكمبيوتر والبيانات ومعالجتها ونقلها في أي وقت على جهاز مادي أو يتم نقلها عبر وسيلة اتصالات. (VanPutte, 2016, p. 33)

من خلال ما سبق نستنتج أنه يمكن تعريف الفضاء السيبراني على أنه مجال عالمي يتشكل من مختلف الأجهزة التي تمثل البنية التحتية التكنولوجية (أجهزة كمبيوتر أجهزة تحكم، أقمار صناعية...الخ) والتي يتم التحكم فيها عن طريق الشبكات السلكية (الكابلات) واللاسلكية ، تعمل هذه الأجهزة على معالجة ونقل والتأثير على البيانات والمعلومات في البيئة الإفتراضية عن طريق المستخدمين سواء كانوا أفرادا أو منظمات أو دول.

2. مفهوم القوة السيبرانية:

لا شك أن الفضاء السيبراني قد ساهم في بروز شكل جديد من القوة وهي القوة السيبرانية، وسنحاول في هذا العنصر التطرق لمختلف التعاريف المقدمة لها.

يعرفها كولين غراي Colin S. Gray ببساطة على أنها القدرة على تحصيل فائدة استراتيجية في الفضاء السيبراني. (Gray, 2013, p. 09)

كما يعرفها جين كريستوف نويل Jean-Christophe Noel بأنها قدرة أحد الفواعل مهما كانت طبيعته (دولة أو مؤسسة أو مجموعة أفراد) على استغلال البيانات الرقمية من أجل التأثير على سلوك فواعل أخرى على المستوى الدولي بغرض تحقيق أهداف معينة. (Noel, 2019, p. 11)

الملاحظ هنا أن التعريفين السابقين يحملان نفس المعنى تقريبا حيث تم تعريف القوة السيبرانية على أنها القدرة على التأثير على سلوكات فواعل أخرى عبر استغلال الفضاء السيبراني لتحقيق مكاسب سواء داخل الفضاء السيبراني بحد ذاته أو خارجه، أي في العالم الحقيقي.

في حين يعرف جوزيف ناي Joseph S. Nye, Jr القوة السيبرانية على أنها "القدرة على استخدام الفضاء السيبراني لخلق مزايا والتأثير على الأحداث في البيئات العملياتية الأخرى عبر أدوات القوة." ويضيف ناي بأنه يمكن استخدام القوة السيبرانية لتحقيق أهداف داخل الفضاء السيبراني كما يمكن استخدامها وعبر أدوات سيبرانية لتحقيق أهداف في مجالات أخرى خارج الفضاء السيبراني (Nye, p. 04).

وما يمكن استنتاجه من هنا هو أن القوة السيبرانية تستخدم للتحقيق أهداف إما داخل البيئة السيبرانية مثل تعطيل المواقع وتشفير الملفات واستغلال الثغرات في الأنظمة الأمنية السيبرانية للدول والشركات والمنظمات، وإما تستخدم للحصول على مكاسب في العالم الواقعي.

المحور الثاني: إشكالية الهيمنة على الفضاء السيبراني

إن الخصائص الفريدة للفضاء السيبراني، دفعت بالدول إلى إعادة ترتيب أولوياتها وفق ما يتطلبه هذا العالم الإفتراضي، فانتشار القوة وسهولة تنفيذ الهجمات وغياب قوانين رادعة، جعلت كل الفواعل يسارعون لاستغلال هذه الميزات لما قد تحققه من مكاسب.

1- انتشار القوة في الفضاء السيبراني

تاريخيا، ارتبطت قوة الدولة ونفوذها ومدى تأثيرها في النظام الدولي، بمساحتها الجغرافية وموقعها الجيوبوليتيكي وعدد سكانها إضافة إلى الموارد التي تمتلكها، إلا أن التطور التكنولوجي قد زاد من فرص الدول الصغيرة في لعب أدوار مهمة في العلاقات الدولية. (خليفة، 2019، ص 26- 27)

هذا مايعني العودة إلى نقطة الصفر، إذ من الواضح أن القدرات السيبرانية غير مرتبطة إطلاقا بمدى مساحة الدولة الجغرافية وعدد سكانها وقوتها

العسكرية، بالتالي الفضاء السيبراني يلغي فارق القوة العسكرية بين الدول، وهذا ما يدفعنا إلى اعتبار الفضاء السيبراني بمثابة طريقة جديدة للدول الصغيرة لفرض منطقها في العلاقات الدولية بعد أن عجزت عن ذلك عسكريا وعلى أرض الواقع، فبناء القدرات السيبرانية للدول لا يتطلب امتلاك اقتصادا قويا وامتلاك الأسلحة النووية بل يكفي الاستثمار في العنصر البشري أمن المعلومات وفتح المجال واسعا أمام البحث في تقنيات الذكاء الاصطناعي وتوفير الدعم اللازم لذلك.

تقول إيمي تشانغ Amy Chang بأن الحرب السيبرانية هي البديل الأمثل للأسلحة التقليدية بالنسبة للدول الصغيرة، فبالإضافة إلى سهولة الحصول عليها، فهي تسمح لهذه الدول بشن هجمات على دول أخرى دون إمكانية التعرض للعقوبات عند اكتشاف ذلك الهجوم. (Suciu, 2014) ويضيف ويليام لين William Lynn أن الجيش الأمريكي يعتمد على تكنولوجيا المعلومات في تشغيل كل شيء تقريبا بل إنها تمثل العمود الفقري للجيش، وهو ما يتيح للخصوم إلحاق أضرار كبيرة بالولايات المتحدة الأمريكية. (Lynn, 2010, p. 98) وهذه أهم مميزات الهجمات والحروب في الفضاء السيبراني، فبالإضافة إلى سهولة الاستخدام وانخفاض التكاليف، والفوائد المتوقع تحقيقها، هناك دائما إمكانية نفي المسؤولية عن الهجوم، وهو أكبر مشكل يواجهه النظام الدولي في الفضاء السيبراني، باعتبار أن تحديد مصدر الهجمات السيبرانية أمر في غاية الصعوبة، وغالبا ما يتم تحديد مصدر أي هجوم سيبراني على دولة ما، بناء على أحداث اقتصادية أو سياسية أو صراعات إيديولوجية.

يضيف جوزيف ناي Joseph S. Nye, Jr ، على أنه ليس هناك عوائق تحول دون امتلاك القوة في الفضاء السيبراني، أما فرض الهيمنة على الفضاء السيبراني، هو أمر غير قابل للتجسيد بسهولة، كما أن الإعتماد على الأنظمة السيبرانية المعقدة لدعم الأنشطة العسكرية والاقتصادية، يخلق نقاط ضعف جديدة في الدول الكبرى. (Nye, p. 04)

إن الفكرة الأساسية هنا هي دور الفضاء السيبراني في ربط مختلف ميادين الحرب السابقة (البر، البحر، الجو والفضاء الخارجي) مع بعضها البعض، بعبارة أخرى أصبح الفضاء السيبراني بمثابة قاعدة كبرى تربط ميادين الحرب كلها، بل إن الأمر يتعدى ذلك ليشمل مجالات أخرى كمجال الطاقة والشبكات ومختلف المواقع الحكومية، بالتالي فإن أي جهة أخرى سواء كانت دولة صغيرة بقدرات سيبرانية كبيرة، أو حتى مجموعة أفراد متخصصين في الأمن السيبراني، سيكونون قادرين على إيجاد أي ثغرة أو نقطة ضعف محتملة في النظام السيبراني للدولة واستغلالها واستهداف قطاعات عسكرية واقتصادية معينة.

هناك نقطة مهمة أيضا وهي أن أي نظام سيبراني لأي دولة قابل للتعرض لمختلف التهديدات السيبرانية سواء بالنسبة للأنظمة المتطورة أو الأكثر تطورا، في حين تتفاوت درجة الصعوبة في اختراق تلك الأنظمة، لكنها تبقى قابلة للاختراق، وحتى لو وجد هناك نظام سيبراني حصين ضد كل الهجمات السيبرانية، فإن حصانته لن تدوم طويلا، وذلك بسبب السرعة الكبيرة التي يتطور بها عالم التقنية والذكاء الاصطناعي.

2. واقع الدفاع والهجوم في الفضاء السيبراني

يؤكد كثير من الباحثين في مجال العلاقات الدولية على أفضلية الهجوم على الدفاع في الفضاء السيبراني، وتعتبر نظرية توازن الدفاع والهجوم أهم نظرية تفسر ذلك رغم تعرضها للعديد من الانتقادات، لكن الفكرة الأساسية لهذه النظرية، مرتبطة بتكاليف الدفاع والهجوم وعلاقة ذلك بتفضيل الهجوم على الدفاع أو الدفاع على الهجوم. فالدول تلجا للهجوم إذا كانت تكاليف الهجوم أقل من تكاليف الدفاع والعكس صحيح، تلجأ الدول للدفاع إذا كانت تكاليف الهجوم أعلى من تكاليف الدفاع. (Sean & Jones, 1995, p. 666) ومايمكن ملاحظته في الفضاء السيبراني هو أن الهجوم لا يكلف كثيرا، بالتالي تلجأ الدول إلى تنفيذ هجمات سيبرانية بغرض تحقيق مكاسب مختلفة بتكاليف بسيطة جدا.

أ- أفضلية الهجوم:

إن السبب الرئيسي الذي يمنح الأفضلية للمهاجم في الفضاء السيبراني هو انخفاض تكاليف تنفيذه، فمثلا دولة (أ) تقرر تنفيذ هجوم سيبراني على دولة (ب)، كل ما تحتاج إليه هو أجهزة كمبيوتر واتصال بشبكة الإنترنت وبعض الأفراد الذين يشترط فيهم امتلاك مهارات تقنية عالية وهذا هو الأساس، إذ أن نسبة نجاح الهجوم السيبراني تعتمد على مدى مهارة الأفراد في تنفيذه والتعامل مع برامج الحماية واكتشاف الثغرات في النظام السيبراني للدولة (ب)، ولهذا فالاستثمار في الموارد البشرية مهم جدا للدولة أمنيا واستراتيجيا.

يؤكد جوزيف ناي Joseph Nye أنه بسبب تصميم الإنترنت الذي يعتمد في جوهره على سهولة استخدام بدلا عن تحقيق الأمن، يجعل من الهجوم يتمتع بميزة الأفضلية على الدفاع. (Nye, p. 05) .بالتالي فإن عالمية المعلومات، وفرت للمهاجم فرصة كبيرة للقيام بعمليات تجسس أو عمليات تخريبية أو سرقة المعلومات، باعتبار أن حماية المعلومات في الفضاء السيبراني تتطلب جهدا أكبر. بالإضافة إلى أن صعوبة تحديد مصدر الهجوم قد ساهمت في تعزيز تلك الأفضلية.

إن الفضاء السيبراني خاضع للتطورات التكنولوجية التي تتسارع بشكل رهيب ، بالتالي فإن معالمه متغيرة بشكل متواصل، يسعى المهاجم دائما لبرمجة وأسلحة وفيروسات جديدة، ويقضي المدافع وقته في محاولة إيجاد حل لتلك البرمجيات الخبيثة، وفي نفس الوقت، لا يستطيع المدافع إيجاد برامج لحمايته من فيروسات أو برمجيات لم تصنع أو هجمات لم تنفذ بعد، غير أنه يستطيع فقط التقليل من آثار ذلك وتأمين البنية التحتية عن طريق وسائل وبرامج الحماية المختلفة.

ب- مأزق الدفاع:

جاء في تقرير القيادة السيبرانية للولايات المتحدة USCYBERCOM، في سنة 2018 أن الفضاء السيبراني عبارة عن بيئة مرنة من الاتصالات المستمرة والفرص الجديدة، حيث لا يبقى أي هدف ثابت، ولا تظل أي قدرة دفاعية أو

هجومية فعالة إلى الأبد. (USCYBERCOM, 2018, p. 04) بالإضافة إلى ذلك تتطور الأبحاث المتعلقة بالأسلحة والاستراتيجيات السيبرانية بطريقة سريعة جدا ما يعني أنه إذا كانت دولة ما منيعة إلى حد ما ضد الهجمات السيبرانية، فإن ذلك لن يدوم لوقت طويل لأن البرامج السيبرانية والأسلحة السيبرانية في تطور مستمر وسريع.

يؤكد الباحثين إيريك غارتزكي Erik Gartzke وجون ليندسي Jon R. Lindsay، على مشكل الدفاع في الفضاء السيبراني، فبينما يحتاج المهاجم للنجاح مرة واحدة في تنفيذ هجوم سيبراني، ينبغي على المدافع أن ينجح في كل مرة مع وجود الكثير من نقاط الضعف واحتمال إيجادها من طرف المهاجم. (Lindsay & Gartzke, 2015, p. 322)

في خضم كل ذلك، سيكون الدفاع عن الأمن القومي والأمن السيبراني في هذه الحالة صعبا جدا، لأن الدفاع في تلك الحالة يتطلب بحثا متواصلا ليس لضمان الأمن السيبراني بشكل شامل لأن الوصول لتلك المرحلة هو أمر مستحيل نظرا للبيئة المرنة للفضاء السيبراني، وإنما لضمان التعرض للحد الأدنى من الأضرار، والخروج بأقل الخسائر.

ويحدد لوكاس كيلو Lukas Kello العديد من العوامل التي تعقد من مهمة الدفاع في الفضاء السيبراني من بينها: (Kello, pp. 27-30)

- صعوبة التنبؤ بالهجوم السيبراني.
- احتمال بقاء الهجوم غير مكتشف.
- التعقيد الكبير الذي يتميز به الفضاء السيبراني وصعوبة اكتشاف كل الثغرات الموجود في النظام.
- المخاطر المتعلقة باستيراد الأجهزة والقطع التكنولوجية: حيث أن أنظمة الكمبيوتر تعتمد بشكل كبير على القطع التكنولوجية مثل المعالجات وبطاقات الرسومات وغيرها والتي تصنعها شركات مختلفة وبالتالي يتزايد

الشك حول إمكانية تحميل تلك القطع ببرامج ضارة بغرض استخدامها فيما بعد.

يلخص المدير السابق للمخابرات المركزية جورج تينيت George Tenet مشكلة الدفاع بقوله: "لقد بنينا مستقبلنا على قدرة لم نتعلم كيفية حمايتها. (Kello, p. 30) وعليه، فإن أزمة الدفاع في الفضاء السيبراني أزمة عميقة تتطلب مسايرة الأحداث والتطورات التكنولوجية خطوة بخطوة، خاصة مع الأسلحة السيبرانية التي تشهد تطورا كبيرا في كل وقت.

المحور الرابع: مفارقة الأمن في الفضاء السيبراني

مع دخول القرن ال21 بدا العالم وكأنه على أعتاب تحقيق ثورة رقمية جديدة، يكون فيها الذكاء الاصطناعي والروبوتات والعملات الإلكترونية وتقنيات البلوك تشين المحرك الأساسي، ومن الطبيعي أن هذه الثورة التكنولوجية الثانية ستساهم كسابقاتها في تطور وزيادة قوة الدولة، لكنها ستخلق مفارقة كبرى في تحقيق الأمن وخاصة الأمن القومي للدولة وهو ما سنناقشه في هذا المحور.

1- الأمن في الفضاء السيبراني

تاريخيا، ارتبط الأمن بمدى تطور الدولة، فكلما ازدادت الدولة تطورا كلما قل احتمال تعرضها للتهديد، خاصة عندما نتكلم عن التهديدات القادمة من الدول الصغيرة، حيث لا تملك تلك الدول الصغيرة أي فرصة في مواجهة القوى الكبرى، لكن يسير الأمر بشكل عكسي في الفضاء السيبراني، فكيف يتم ذلك ؟

يؤكد إيفو تسيكوف Ivo Tsecov أن المجال السيبراني هو ظاهرة فريدة من نوعها حيث كلما استثمرت الدولة وتوجهت نحو رقمنة قطاعاتها، كلما كانت أكثر عرضة للخطر (Tsecov, 2017, p. 05)، كانت إستونيا في سنة 2007 من أكثر الدول تطورا في المجال الرقمي، وكانت حكومتها تفتخر بكونها الأكثر تقدما في الاعتماد على تكنولوجيا المعلومات، وقد استخدم ما يقارب 60% من عدد السكان آنذاك الانترنت لتسيير حياتهم

اليومية، كما تفعل ذلك معظم الدول اليوم، واعتبرت الحكومة نفسها " حكومة بلا أوراق. (Connell & Vogler, 2017, p. 13). وكانت استونيا تعتمد على الإنترنت بشكل شبه كلي في تسيير بنيتها التحتية وكانت 97% من المعاملات المصرفية تتم عبر الانترنت كما أن شبكات الطاقة وحتى إمدادت المياه كانت مرتبطة بالبنية التحتية السيبرانية للعاصمة تالين، (Herzog, 2011, pp. 50-51) وهو ما يدل على التطور الرقمي الكبير الذي كانت ولاتزال تشهده استونيا في تلك الفترة.

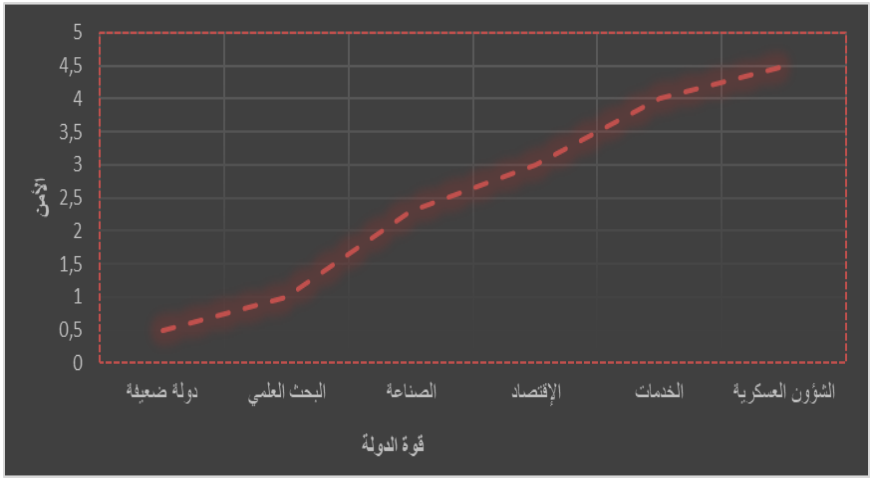
لكن تعرضت إستونيا في ذلك الوقت إلى هجمات سيبرانية متواصلة من روسيا، (Ottis, 2008, p. 163) وقد شملت تلك الهجمات تعطيل المواقع الإلكترونية الحكومية والبنوك والقدرات التكنولوجية للعديد من الوزارات وحالت تلك الهجمات دون حدوث معاملات بطاقات الائتمان وغيرها بالإضافة إلى تعطيل خوادم البريد الإلكتروني البرلماني مما شل قدرة الدولة على الاستجابة خلال تلك الأزمة (Herzog, pp. 51-52).

تعتبر سنغافورة كذلك من بين أكثر الدول رقمنة خاصة مع برنامج الأمة الذكية وسعيها لتصبح مركز بيانات، وهو نفس الشيء الذي يجعلها أكثر عرضة للتهديدات السيبرانية مقارنة بغيرها من الدول، (Eugene, 2019, p. 162) بالإضافة ذلك تعترف الولايات المتحدة الأمريكية بالتهديد الناجم عن الإعتماد الكلي على الفضاء السيبراني حيث جاء في رؤية القيادة السيبرانية الأمريكية USCYBERCOM أن الخصوم يملكون إمكانية تعطيل الإقتصاد والمجتمع وحتى الجيش الأمريكي، ويرجع ذلك إلى الإعتماد المتزايد على الفضاء السيبراني، (USCYBERCOM, p. 02) ، وبينما تتعرض الولايات المتحدة الأمريكية باستمرار لمختلف الهجمات السيبرانية، تبقى سنغافورة بعيدة نوعا ما عن الهجمات السيبرانية ويعود ذلك إلى أنها لا تمتلك أعداءا يشكلون تهديدا على أمنها القومي على عكس الولايات المتحدة الأمريكية التي تكن عداءا تاريخيا لدول مثل كوريا الشمالية وروسيا والصين، والملاحظ أن أغلبية التهديدات السيبرانية التي تتعرض لها الولايات المتحدة الأمريكية قادمة من تلك الدول الثلاث، وعليه يمكن القول أن احتمال تعرض دولة في الفضاء

السيبراني للتهديد، يرتبط ارتباطا وثيقا بطبيعة علاقاتها مع الدول الأخرى على أرض الواقع.

ويمكن توضيح العلاقة بين الرقمنة والأمن بطريقة أوضح من خلال المنحنيات التالية:

الشكل رقم1: يبين العلاقة بين التوسع في امتلاك قطاعات قوية ومدى



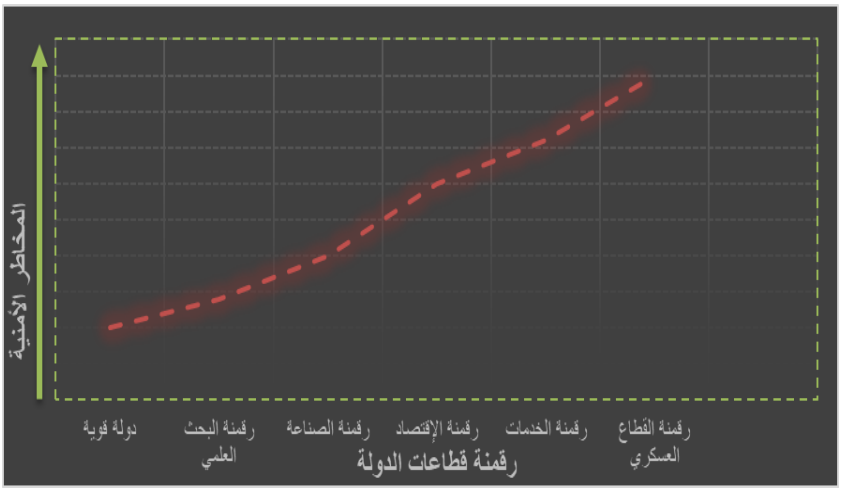
تحقيق الأمن بالنسبة للدولة قبل دخول عصر الفضاء السيبراني.

المصدر: إعداد الباحثين

في المنحنى البياني أعلاه، تتضح العلاقة بين قوة الدولة عبر مختلف القطاعات ومدى تحقيقها للأمن ضد مختلف الهجمات القادمة من الدول الأخرى، وللتوضيح أكثر وكمثال اعتمدنا الأرقام من 1 إلى 5 للتعبير عن درجة أمن الدولة واقترحنا نقطة لكل قطاع كمثال فقط حيث تمثل أعلى نقطة 5/5، بمثابة العلامة الكاملة ويعني ذلك دولة منيعة ضد كل الهجمات المختلفة، بينما تمثل النقطة 5/0.5 دولة هشة في جميع القطاعات. مثلا دولة تمتلك قطاع اقتصادي وصناعي وعسكري قوي مثل الولايات المتحدة الأمريكية تكون أكثر أمنا واحتمال تعرضها للضرر أقل من احتمال تعرض

دولة أخرى مثل إيران التي لا تتمتع بنفس القوة الاقتصادية والعسكرية للولايات المتحدة الأمريكية، هذا طبعا قبل إدخال متغير رقمنة القطاعات.

الشكل 2: يبين العلاقة بين الرقمنة وازدياد المخاطر الأمنية في عصر



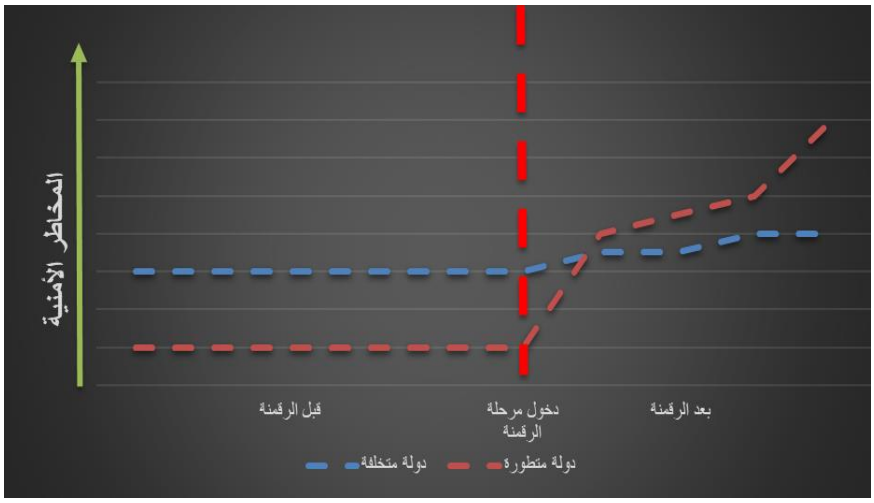
الفضاء السيبراني

المصدر: إعداد الباحثين

من خلال المنحنى اعلاه يمكن فهم العلاقة بين الرقمنة والمخاطر الأمنية حيث كلما توسعت الدولة في رقمنة مختلف القطاعات كلما كانت أكثر عرضة للتهديدات السيبرانية، إذ أن كل تلك القطاعات قد أصبحت مرتبطة بمجال واحد وهو الفضاء السيبراني والذي كما ذكرنا سابقا أن كل دولة تمتلك القوة السيبرانية، تستطيع الوصول إليه وتخريب المعلومات أو القيام بعمليات تجسس وغيرها، وعليه تصبح في هذه الحالة الدولة المتطورة أكثر عرضة للخطر من دولة متخلفة، لا تمتلك بنية تحتية سيبرانية.

لنلاحظ مسار دولة متطورة ودولة متخلفة قبل وبعد إدخال متغير الرقمنة في الرسم البياني التالي:

الشكل3: يوضع مسار دولة متطورة ودولة متخلفة قبل وبعد إدخال متغير الرقمنة.



المصدر: إعداد الباحثين

يوضح المنحنى أعلاه درجة المخاطر الأمنية التي تتعرض لها دولة متخلفة ودولة متطورة قبل وبعد الدخول إلى عصر الرقمنة، فالدولة المتخلفة تكون أكثر عرضة لمختلف التهديدات الأمنية بسبب هشاشة قطاعاتها الإقتصادية والعسكرية والخدماتية، والعكس بالنسبة للدول المتطورة ذات البنى التحتية المتماسكة. لكن بعد دخول مرحلة الرقمنة، أصبحت الدول المتطورة أكثر عرضة للتهديدات الأمنية بسبب رقمنة معظم القطاعات، حيث تشكل الهجمات السيبرانية أكبر تهديد على البنى التحتية لتلك الدولة ومازاد من حدتها هو سهولة القيام بالهجمات السيبرانية من طرف أي فاعل من الفواعل وأفضل مثال لتوضيح الفكرة، ما حدث في إستونيا التي عرفت باسم إستونيا الرقمية في سنة 2007 عندما أغرقتها روسيا بالعديد من الهجمات السيبرانية والتي تسببت في شلل تام لوظائف الدولة الإستونية لمدة أربعة أيام، بالتالي أصبحت المخاطر الأمنية تتزايد طرديا مع التطور الرقمي، ولو كانت دولة أخرى أقل اعتمادا على الإنترنت (الجزائر على سبيل المثال) في مكان إستونيا، لما تعرضت لكل تلك الأضرار، كما أن الدول المتخلفة أصبحت مجبرة على

إدخال عنصر التكنولوجيا إلى قطاعاتها ولكن لم تقم بذلك بالشكل الكافي بالتالي، وبالإضافة إلى المخاطر التقليدية زادت احتمالية تعرضها للتهديدات السيبرانية ولكن بقدر ضئيل مقارنة بالدول المتطورة نتيجة لمحدودية القطاعات الرقمية في تلك الدول.

2. انترنت الأشياء كتهديد جديد

تعتبر انترنت الأشياء آخر ما يتم التوصل إليه في مجال التكنولوجيا الرقمية ويمكن اعتبارها بمثابة ثورة تكنولوجية جديدة تجعل من الإنترنت تسيطر على أبسط وظائف البشر كتشغيل أو إطفاء مصباح منزل مثلا، ورغم المزايا العديدة التي تحملها إلا أنها لا تخلوا من مخاطر عديدة يمكن أن تتسبب في مشاكل غير مألوفة على الأقل بالنسبة لنا كمجتمع لم يصل بعد لتلك المرحلة.

أ. مفهوم انترنت الأشياء

تعرف شركة كاسبرسكي لاب Kaspersky Lab المتخصصة في الأمن السيبراني إنترنت الأشياء IoT (Internet of Things)، بأنها مجموعة من الأجهزة التي تتصل بالإنترنت. ولا تقتصر تلك الأجهزة على الأجهزة المعروفة مثل جهاز كمبيوتر أو تلفزيون ذكي، لكن إنترنت الأشياء تشمل أجهزة لم تكن لها أي علاقة بالإنترنت من قبل مثل آلات النسخ والثلاجات وغيرها، حيث يشير مصطلح انترنت الأشياء إلى جميع الأجهزة حتى التي يمكنها الاتصال بالإنترنت حتى الأجهزة غير المألوفة منها. ويمكن القول أنه تقريبا أي جهاز يحتوي على مفتاح تشغيل/إيقاف (ON/OFF) في الوقت الحالي وفي المستقبل، يحتمل أنه يستطيع الاتصال بالإنترنت، وهو ما يجعل تلك الأجهزة جزءا من انترنت الأشياء. (Kaspersky Lab, s.d.)

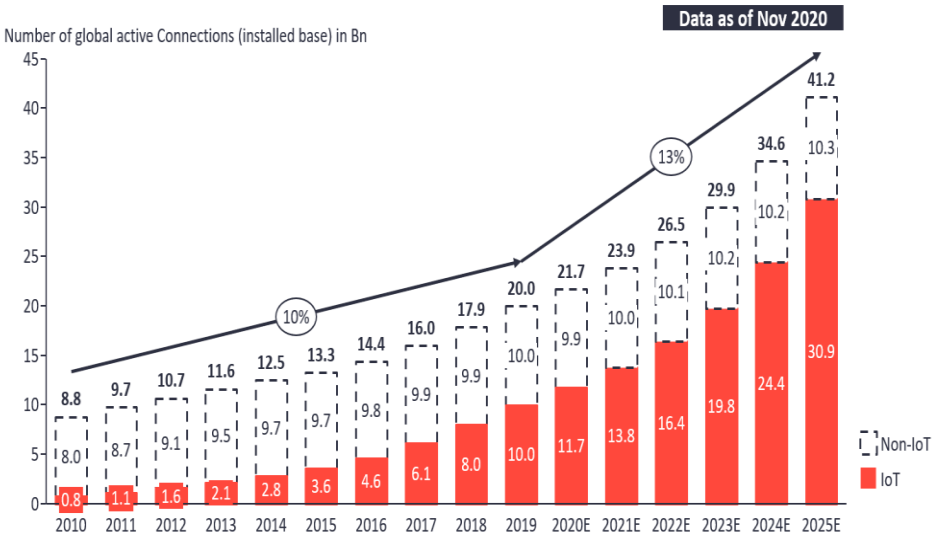
عموما تختلف التعاريف المقدمة لمفهوم انترنت الأشياء، ولكنها تحمل نفس المعنى، حيث يقصد قدرة مختلف الأشياء التي نستخدمها في حياتنا اليومية على الاتصال فيما بينها عبر الانترنت، وتشمل كلمة أشياء هنا كل شيء حرفيا، من الساعات الذكية التي تراقب الحالة الصحية لمرتديها من خلال قياس

الضغط ومراقبة ضربات القلب، إلى المنازل الذكية التي تتيح للمستخدم التحكم في كامل الأجهزة الموجودة بالمنزل مثل الثلاجة والغسالة وأجهزة التدفئة والأبواب وغيرها من خلال الهاتف أو الحاسوب، إلى السيارات المرتبطة بالانترنت والتي تتميز بالقدرة الذاتية على القيادة وتجنب الطرق المزدحمة والكثير من المميزات الأخرى وصولا إلى المدن الرقمية التي تستخدم التكنولوجيا لتحسين أوضاع السكان والرفع من كفاءة الخدمات.

ب- مخاطر انترنت الأشياء

ذكرنا سابقا أنه كلما توسعت الدولة في رقمنة قطاع معين كلما كانت أكثر عرضة للتهديدات الأمنية السيبرانية، لكن كيف سيكون الوضع عندما تتم رقمنة كل شيء تقريبا ؟ رغم أنه لم تصل أي دولة إلى الاستغلال الكامل لإنترنت الأشياء إلى أن عدد الأجهزة المتصلة بالانترنت يستمر في النمو بشكل سريع جدا، وهو ما يوضحه الشكل التالي:

الشكل4: يوضح تطور استخدام أجهزة انترنت الأشياء مقارنة مع أجهزة الهواتف والكمبيوترات واللوحات الإلكترونية.



المصدر: IoT Analytics Cellular IoT & LPWA Connectivity market tracker

تتضمن IoT : كل الأجهزة التي تتصل بالإنترنت ماعدا Non IoT.

تتضمن Non IoT: كل أنواع الهواتف، الأجهزة اللوحية (Tablets) وأجهزة الكمبيوتر.

من خلال الرسم البياني، نلاحظ النمو الكبير لأجهزة انترنت الأشياء منذ أكثر من 10 سنوات فمثلا في سنة 2010 كان هناك حوالي 800 مليون جهاز فقط يصنف ضمن أجهزة انترنت الأشياء بينما كان هناك حوالي 8.8 مليار جهاز اتصال (هاتف، كمبيوتر، جهاز لوحي)، لكن ومع مرور الوقت تضاعف العدد، إذ نلاحظ أنه في عام 2020، ولأول مرة ، هناك أجهزة إنترنت الأشياء (مثل السيارات المتصلة والأجهزة المنزلية الذكية والمعدات الصناعية المتصلة) أكثر من أجهزة الإتصال التي نعرفها (الهواتف الذكية وأجهزة الكمبيوتر وأجهزة الألواح الإلكترونية)، حيث بلغ عدد أجهزة انترنت الأشياء في سنة 2020، 11.7 مليار جهاز، بينما بلغ عدد أجهزة الكمبيوتر والهواتف والألواح الإلكترونية 9.9 مليار جهاز، وهو ما يدل على الانتشار السريع للرقمنة التي لن تتوقف حتى تشمل كل ما يحيط بنا تقريبا.

ومن المتوقع أن تستمر هذه الزيادة مع الوقت وبحلول عام 2025، من المتوقع أن يكون هناك أكثر من 30 مليار اتصال لأجهزة إنترنت الأشياء، أي ما يقرب من 4 أجهزة إنترنت الأشياء للشخص الواحد في المتوسط.

وهذا ما يدل على استمرار تشابك مختلف القطاعات بالإنترنت، وهو الأمر الذي يعقد من مهمة ضمان الأمن، باعتبار أن كل الفواعل سواءا على المستوى الفردي أو المؤسساتي أو المجتمعي أو الدولي، أصبحت تسير وظائفها عبر الإنترنت مع غياب أي ضمانات لتأمين مصالح أي طرف.

ويمكن أن تشكل انترنت الأشياء خطرا كبيرا على الأمن، حيث يزيد عدد الثغرات الأمنية مع زيادة الأجهزة المرتبطة بالانترنت، وهو ما يفتح المجال واسعا أمام الهجمات السيبرانية التي تهدد أمن كل قطاعات.

لتوضيح الرؤية أكثر، في عام 2015 أستطاع باحثان أمنيان اختراق سيارة Chrysler jeep cherokee، بعدها بأسبوع، كشف الباحثون عن القدرة على اختراق نظام OnStar الذي تستخدمه جنرال موتورز لتوفير مجموعة من الخدمات عبر الانترنت في السيارة، واستطاع الباحثون التحكم في أبواب السيارة والوصول إلى البريد الإلكتروني للمالك، وقد وصل الأمر في سيارات أخرى إلى إمكانية توقيف ناقل الحركة والتلاعب بالفرامل والوصول إلى جهاز الراديو ونظام المعلومات وتتبع السيارة عبر بيانات النظام العالمي لتحديد المواقع GPS. (Writer, 2016, p. 20)

من خلال ما سبق يمكن التأكيد على أمر مهم، وهو أننا في هذا العصر نستمر في الاعتماد بشكل أوسع على التكنولوجيا، وفي نفس الوقت نستمر في إحاطة أنفسنا بالعديد من الثغرات الأمنية التي تهدد خصوصيتنا وسلامتنا، وعليه وبناء على المعطيات الحالية، يمكن تصور مدى سيطرة التكنولوجيا على مختلف المجالات بعد عدة سنوات، وكذلك يمكن تخيل درجة الضعف التي سيصل إليها عالمنا باعتباره أصبح أكثر تشابكا.

الخاتمة:

أحدث الفضاء السيبراني ثورة من نوع خاص في مجال العلاقات الدولية، سواء عند التطرق إلى المفاهيم المختلفة كالهيمنة والأمن، أو عند الحديث عن موازين القوى، فأصبحنا نرى دول صغيرة بقدرات أكبر ودول كبرى عاجزة عن بسط الهيمنة على هذا المجال، بل حتى أنها عاجزة عن تحقيق أمنها القومي نتيجة لسهولة شن الهجمات السيبرانية وصعوبة اتخاذ الإجراءات الدفاعية، بالتالي تحقيق الهيمنة في الفضاء السيبراني ليس مرتبطا بالدول الكبرى التي تهيمن على العلاقات الدولية على أرض الواقع، بل إن الفضاء السيبراني أعاد تقسيم الفرص على الفواعل في العلاقات الدولية بطريقة متساوية وفي نفس الوقت أصبحت الدول الأكثر تطورا من الناحية الرقمية هي الدول الأكثر قابلية للتعرض للأضرار بسبب خصائص الفضاء السيبراني الفريدة من نوعها، وعليه أصبح على الدول التفكير بطرق مختلفة لتحقيق الأمن السيبراني باعتبار أن تحقيق الأمن في باقي القطاعات أصبح مرتبطا بتحقيق الأمن السيبراني،

ومع استمرار التطور التكنولوجي أصبحنا نتكلم عن ما يعرف بانترنت الأشياء والتي وجدت لتسهيل حياة المجتمعات لكن في نفس الوقت تعتبر تهديدا آخر على الأمن المجتمعي والأمن الفردي، بالتالي أصبحت الدول وفي الأخير يمكن الخروج بمجموعة من النتائج والتي نلخص أهمها في ما يلي:

- أتاح الفضاء السيبراني للدول الصغيرة فرصا عديدة لتحقيق مصالح استراتيجية ضد الدول الكبرى باعتبار أن القوة أصبحت أكثر انتشارا.
- قد تفشل الدول الصغيرة في الحصول على الأسلحة النووية، ولكنها تستطيع بناء أسلحة سيبرانية استراتيجية قادرة على تحقيق أهداف معينة.
- تحقيق الأمن السيبراني هو أمر في غاية الصعوبة وغير مرتبط بحجم الإنفاق، فالولايات المتحدة الأمريكية دائما ما تنفق في هذا المجال ولكنها تتعرض لهجمات سيبرانية في كثير من الأحيان.
- لا يوجد أي نظام سيبراني في أية دول تم تطويره بطريقة مثالية فكل الأنظمة معرضة للاختراق، بالتالي من غير الممكن تحقيق الأمن السيبراني الشامل على الأقل في الوقت الحالي.
- تتناسب آثار الهجمات السيبرانية طرديا مع التطور الرقمي، فكلما زادت درجة رقمنة قطاعات الدولة، كلما زادت درجة تأثرها بالهجمات السيبرانية.
- فكرة إنترنت الأشياء تعني العمل على توسيع نطاق الأجهزة التي ترتبط بالإنترنت لتشمل أجهزة أخرى مثل السيارات والمنازل والمدن وأجهزة منزلية مثل الثلاجات وغيرها.
- بالنظر إلى المعطيات الحالية، لا يمكن لأي دولة أن تفرض سيطرتها على الفضاء السيبراني نظررا لانتشار القوة السيبرانية بين مختلف الفواعل.

قائمة المراجع:

العربية:

الكتب:

خليفة إيهاب .(2019) .*مجتمع ما بعد المعلومات، تأثير الثورة الصناعية الرابعة على الأمن القومي* ط1 .القاهرة: العربي للنشر والتوزيع.

الفرنسية:

المقالات:

Noel Jean-Cristophe. (2019). *Qu'est-ce que la puissance numerique ?* Paris: Institut Français des relations internationales.

الإنجليزية:

الكتب:

Singer Peter & Friedman Allan. (2014). *Cybersecurity and cyberwar : what everyone needs to know.* New York: Oxford University Press.

VanPutte Michael A. (2016). *Walking Wounded Inside the U.S. Cyberwar Machine.* USA: Createspace Independent Publishing.

المقالات:

Connell Michael & Vogler Sarah. (2017). *Russia's Approach to Cyber Warfare , 2017,* CNA analysis & Solutions.

Eugene, E.G Tan. (2019). *A Small State Perspective on the Evolving Nature of Cyber Conflict: Lessons from Singapore* .the quarterly journal of complex operations Vol. 8. *PRISM*.

Gray Colin S. (2013). *Making a strategic sense of cyber power: Why the sky is not falling.* The Strategic Studies Institute (SSI). U.S. Army War College Press.

Herzog Stephen. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*.

Kello Lucas. (s.d.). The Meaning of the Cyber Revolution. *international security, 38*.

Lindsay Jon. Gartzke Eric. (2015). *Weaving Tangled Webs: Offense Defense, and Deception in Cyberspace*. Security Studies.

Lynn William J. (2010). Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*

Nye Joseph S. *Cyber Power.* Harvard Kennedy School. Cambridge: Belfer Center for Science and International Affairs.

Reveron Derek S. (2012). An introduction to national security and cyberspace. Dans *Cyberspace and national security; Threats, Opportunities, and Power in a virtual word*. Georgetown University Press.

Sean M. Lynn Jones. (1995). Offense-Defense Theory and Its Critics. *Security Studies.*

Tsecov Ivo. (s.d.). *The Changing Balance of Power in the Age of Emerging Cyber Threats.* Institute for Security and International Studies (ISIS), Sofia.

Writer Staff. (2016). Security and the Internet of Things: When your refrigerator steals your identity. *The Next Wave, National Security Agency review of emerging technologies.*

المؤتمرات:

Ottis Rain. (2008). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective,. *Proceedings of the 7th European Conference on Information Warfare and Security*. Estonia, Tallinn: Reading: Academic Publishing Limited.

المواقع الإلكترونية:

Kaspersky Lab. (s.d.). *What is IoT? Tips for IoT Security*. Consulté le 04 12, 2021, sur Kaspersky: https://bit.ly/3wxjIGP

Suclu Peter. (2014). *Why cyber warfare is so attractive to small nations*. Consulté le 02 22, 2021, sur Fortune: https://bit.ly/3wvXV20

التقارير:

Department of The Army. (2017). *Cyberspace and Electronic Warefare Operations.* Washington DC: Joint and Department of Defense publications.

US Cyber Command, (2018). *Achieve and maintain cyberspace superiority , Command vision for US Cyber Command.*