الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
جامعة الشهيد حمّه لخضر- الوادي
Université Echahid Hamma Lakhdar - El Oued

كلية الحقوق والعلوم السياسية
مجلة العلوم القانونية والسياسية
ISSN: 2602-6260
الرقم : 83 /م.ع.ق.س/ ك.ح.ع.س/2022

الوادي في: 2022/05/24

شهادة نشر بالمجلة

يشهد رئيس تحرير مجلة العلوم القانونية والسياسية، بكلية الحقوق والعلوم السياسية، جامعة الشهيد حمّه لخضر الوادي، أنّ:

الإسم واللقب: إسماعيل زروقة (دكتور، جامعة المسيلة، الجزائر)

قد نشر (ت) مقالا بعنوان:

" الفضاء السيبراني والتحول في مفاهيم القوة والصراع "

وهو مقال محكّم بخبرة إيجابية وتمّ نشره في مجلة العلوم القانونية والسياسية، **المجلد:** العاشر (10)، **العدد:** الأول (01)، **شهر:** أفريل 2019.

رئيس التحرير

جامعة الشهيد حمة لخضر بالوادي
مجلة العلوم القانونية والسياسية
كلية الحقوق والعلوم السياسية
رئيس التحرير
زرقي عمار

سلمت هذه الشهادة للمعني (ة) بناء على طلبه (ها) لاستخدامها في ما يسمح به القانون

الفضاء السيبراني والتحول في مفاهيم القوة والصراع

Cyberspace and transformation of the concepts of power and struggle

الدكتور/إسماعيل زروقة
جامعة محمد بوضياف المسيلة، الجزائر
zerougaismail1@yahoo.fr

تاريخ الاستلام: 2018/06/24 تاريخ القبول للنشر: 2018/11/25

❖❖❖❖❖❖❖

ملخّص:

كانت ثورة المعلومات وظهور الانترنيت إيذانا ببزوغ العصر السيبري، وخلق بيئة جديدة هي الفضاء السيبراني (Cyber space)- إضافة إلى الأرض والبحر والجو والفضاء- الذي أصبح يؤثر في النظام الدولي، خاصة مع بروز شكل جديد من القوة هي القوة السيبرانية (Cyberpower)، التي توزعت وانتشرت بين عدد أكبر من الفاعلين على المستوى الدولي والمحلي، ما جعل الفضاء السيبراني مجالا جديدا للصراع بين الدول ، وبالتالي حاولت من خلال هذه الورقة البحثية اظهار الانعكاسات التي احدثها الفضاء السيبراني على التحولات في مفهوم القوة و الصراع، من خلال التحول من الصراع المادي الى الصراع الافتراضي، وهو ما ادى باهتمام الدول الى امننة الفضاء السيبراني.

الكلمات المفتاحية: الفضاء السيبراني؛ القوة السيبرانية؛ التهديدات السيبرانية؛ الامن السيبراني.

Abstract:

Globalization with the development of the internet mentioned the emergence of the Siberian era and leads to the creation of a new environment, Siberian space ,in addition to the land, sea, air and space, which became influential in the international system especially with the emergence of a new form of power, the Siberian power that was distributed and spread among a larger number of international and domestic actors have made Siberian space a new area of conflict between States .Thus ,this paper attempts to show the implications of space on the changes in the concept of power and conflict through the transition from physical conflict to virtual conflict, which led to the attention of States to the security of Cyberspace keywords Siberian space Siberian power Siberian threats Siberian security.

Keys words: *cyber space; cyber power; cyber threats; cyber security.*

مقـدّمـة:

لقد أحدثت تكنولوجيا المعلومات والاتصالات ثورة شاملة في جميع نواحي الحياة، اذ تزداد المخاطر السيبرانية في غالب الاحيان كلما زادت هيمنة تكنولوجيا المعلومات والاتصالات على النسق العام للحياة، فأصبحنا أمام جرائم حقيقية ومتكاملة الأركان تتم عن طريق شبكات الانترنت، أجهزة الحاسوب وشبكة الإنترنت بأشكال كثيرة، كسرقة الأموال، النصب والاحتيال، التخطيط لعمليات إرهابية، ترويج الأخبار الكاذبة، وكذلك القرصنة باعتبارها الجريمة الأكثر شيوعاً في العالم الرقمي.

وفي هذا السياق، فإن البحث في قضايا التهديدات السيبرانية والتحديات الأمنية يقتضي الغوص في حيثيات العصر الرقمي الجديد وتوصيف بيئة هذه التحديات، حيث إن شبكة الإنترنت تتوفر على 30 تريليون موقع إلكتروني.

مع انتشار واسع للابتكارات بالشبكة العنكبوتية. ففي تقرير صدر أخيراً عن مؤسسة "سيسكو" سنة 2015، يتبيّن أن أكثر من 40 مليار جهاز سوف يتحوّل على الإنترنت متمثلة في سيارات ذكية وأجهزة منزلية رقمية، وبالتالي الإشكالية التي نحاول معالجتها من خلال هذه الورقة البحثية هي : كيف أثر الفضاء السيبراني على التحول في مفاهيم و مضامين القوة والصراع؟

المبحث الأول

الفضاء السيبراني وتحولات القوة

المطلب الأول: مفهوم الفضاء السيبراني

الفضاء السيبراني مجال افتراضي من صنع الإنسان يعتمد على نظم الكمبيوتر وشبكات الانترنيت وكم هائل من البيانات والمعلومات والأجهزة، كما ان هناك من عرف الفضاء السيبراني بوصفه الذراع الرابعة للجيوش الحديثة[(1)]، وهناك من يرى أنه البعد الخامس للحرب، وهذا التعريف يحصر الفضاء السيبراني في المجال العسكري فقط دون التطرق للمجالات الأخرى.

كما عرَفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI) على أنه: "فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية"[(2)]، وهذا التعريف يركز على الجانب التقني كما يغفل العامل البشري، والذي يعد جزءا أساسيا في فهم الفضاء السيبراني.

كما يمكن الاعتماد على تعريف الاتحاد الدولي للاتصالات الذي يصف الفضاء السيبراني بأنه "المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي: أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكم، ومستخدموا كل هذه العناصر"[(3)].

وعليه يمكننا القول بأن: "الفضاء السيبراني هو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكون من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين" وتجدر الإشارة إلى أن مسألة تحديد مفهوم "الفضاء السيبراني"، هي مسألة نسبية

تتوقف على طبيعة إدراك وفهم كل من الدول والهيئات كل حسب رؤيته واستراتيجيته وقدرته على استغلال المزايا المتاحة ومواجهة المخاطر الكامنة في هذا الفضاء.

المطلب الثاني: التحولات في مضامين القوة وظهور القوة السيبرانية

أصبح الفضاء السيبراني احد العناصر الأساسية التي تؤثر في النظام الدولي، بما يتيحه من أدوات تكنولوجية مهمة لعمليات الحشد والتعبئة في العالم، فضلا عن التأثير في القيم السياسية، فسهولة الاستخدام ورخص التكلفة زادا من قدرته على التأثير في مختلف مجالات الحياة، سواء السياسية، الاقتصادية، العسكرية، الاجتماعية وحتى الايديولوجية، وبات جليا أن من يمتلك آليات توظيف البيئة السيبرانية يصبح أكثر قدرة على تحقيق أهدافه والتأثير في سلوك الفاعلين المستخدمين لهذه البيئة.

- سيسكو شركة أمريكية عملاقة متخصصة بعلم الشبكات بشكل عام.
- وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي تأسست في 7جويلية 2009.

من الأمور المتعارف عليها في العلاقات الدولية أن مصادر قوة الدولة وأشكالها تتغير، فإلى جانب القوة الصلبة ممثلة في القدرات العسكرية والاقتصادية، تزايد الاهتمام بالأبعاد غير المادية للقوة، ومن ثم بروز القوة الناعمة التي تعتمد على جاذبية النموذج والإقناع، ومع ثورة المعلومات ظهر شكل جديد من أشكال القوة هو القوة السيبرانية (Cyber power)، التي لها تأثير كبير على المستوى الدولي والمحلي، فمن ناحية أدت إلى توزيع وانتشار القوة بين عدد أكبر من الفاعلين مما جعل قدرة الدولة على السيطرة موضع شك، ومن ناحية أخرى منحت الفاعلين الأصغر قدرة أكبر على ممارسة كل من القوة الصلبة والقوة الناعمة عبر الفضاء السيبراني، وهو ما يعني تغيرا في علاقات القوى في السياسة الدولية.

يعد جوزيف.س ناي (Joseph S.Nye) من أبرز المهتمين بالقوة السيبرانية، حيث يعرفها بأنها :" القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة، والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات سيبرانية"[(4)]، كما يوضح جوزيف.س ناي أن مفهوم القوة السيبرانية يشير إلى "مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الالكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل".

ويتناول مفهوم القوة السيبرانية مجمل القضايا التي تتعلق بالتفاعلات الدولية العسكرية والاقتصادية والسياسية والثقافية والإعلامية وغيرها ، وحتى تتمكن الدولة من ممارسة النفوذ داخليا أو خارجيا عبر القوة السيبرانية يجب أن تتوفر على مجموعة عناصر أهمها:

- وجود بنية تحتية سيبرانية:

تشمل أجهزة الكمبيوتر، وشبكات الاتصالات، والبرمجيات، وقواعد البيانات لمختلف الأنظمة والقطاعات.

- بنية مؤسسية:

تتولى مهمة ممارسة القوة السيبرانية وتحقيق الأمن السيبراني للدولة.

- بنية تشريعية:

تكون ضامنة ومحددة لاستعمال القوة السيبرانية.

- إستراتيجية بأهداف واضحة:

تحدد طرق العمل والأهداف المرجوة.

وحتى تكتمل عناصر القوة السيبرانية لابد للدولة من القيام بتطوير أسلحة في مجال الحرب السيبرانية لاستعمالها سواء في العمليات الهجومية أو من أجل الردع(5).

المبحث الثاني

الفواعل في مجال القوة السيبرانية

يحدد جوزيف.س ناي ثلاثة أنواع من الفاعلين الذين يمتلكون القوة السيبرانية:

- الدول:

والتي لديها قدرة كبيرة على تنفيذ هجمات سيبرانية وتطوير البنية التحتية وممارسة السلطات داخل حدودها.

- الفاعلون من غير الدول:

ويستخدم هؤلاء الفاعلون القوة السيبرانية لأغراض هجومية بالأساس، إلا أن قدرتهم على تنفيذ أي هجوم سيبراني مؤثر تتطلب مشاركة ومساعدة أجهزة استخباراتية متطورة، ولكن يمكنهم اختراق المواقع الالكترونية واستهداف الانظمة الدفاعية.

- الأفراد:

الذين يمتلكون معرفة تكنولوجية عالية والقدرة على توظيفها، وعادة ما تكون هناك صعوبة في الكشف عن هوياتهم، ومن الصعب ملاحقتهم.

كما يمكننا التفصيل أكثر بخصوص الفاعلين من غير الدول كالتالي(6):

- الشركات متعددة الجنسيات:

تمتلك بعض شركات التكنولوجيا موارد للقوة تفوق قدرة بعض الدول، ولا تنقصها سوى شرعية ممارسة القوة التي مازالت حكرا على الدول، فخوادم شركات مثل: جوجل Google وفيسبوك Facebook وميكروسوفت Microsoft وآبلApple وأمازونAmazon، تسمح لها بامتلاك قواعد البيانات العملاقة التي من خلالها تستكشف وتستغل الأسواق، وتؤثر في اقتصاديات الدول وفي ثقافة المجتمعات وتوجهاتها، وهذا ما حدث في الأزمة بين شركة جوجل والصين حول المحتوى، أو فضيحة تسريب بيانات مستخدمي فايسبوك لصالح شركة "كامبردج أناليتيكا" التي تم الاستعانة بها لصالح حملة الرئيس الأمريكي ترامب.

- المنظمات الإجرامية:

تقوم هذه المنظمات الإجرامية بعمليات القرصنة السيبرانية، وسرقة المعلومات واختراق الحسابات البنكية وتحويل الأموال، كما توجد سوق سوداء على الانترنيت العميق Deep internet لتجارة المخدرات والأسلحة والبشر، حيث تكلف هذه الجرائم السيبرانية مليارات الدولارات سنويا.

- الجماعات الإرهابية:

تعد من أبرز الفواعل الدولية، خاصة بعد أحداث 11 سبتمبر، حيث تستغل الفضاء السيبراني في عمليات التجنيد والتعبئة والدعاية وجمع الأموال والمتطوعين، كما تحاول جمع المعلومات حول الأهداف العسكرية، وكيفية التعامل مع الأسلحة وتدريب المجندين الجدد عن بعد، رغم أنها لم تصل بعد إلى مرحلة القيام بهجوم سيبراني حقيقي على منشآت البنية التحتية للدول.

- الأفراد:

أصبح الفرد بفضل الفضاء السيبراني فاعلا مؤثرا في العلاقات الدولية، ومن أبرز النماذج ظاهرة الويكيليكس "Wikileaks" الذي نجح في نشر ملايين الوثائق السرية للإدارة الأمريكية وقنصلياتها، مما خلق مشاكل دبلوماسية بين الولايات المتحدة الأمريكية وحلفائها.

المبحث الثالث

الصراع السيبراني

اختصر الفضاء السيبراني حاجزا الزمان والمكان، وخلق مساحات للتفاعلات الداخلية والدولية في الواقع الافتراضي، ومن ثم، برزت فضاءات جديدة للصراع بأدوات مختلفة، وأنماط جديدة تختلف عن الصراعات التقليدية، بعد أحداث 11 سبتمبر 2001 – التي تعد مفصلية في تاريخ العلاقات الدولية لبداية استعمال الجماعات الارهابية للانترنت بشكل بارز في الترويج للفكر المتطرف - كان الفضاء السيبراني ساحة الصراع والقتال بين تنظيم القاعدة والولايات المتحدة، وفي عام 2007 جرت العمليات العدائية بين استونيا وروسيا في الفضاء السيبراني، وهو ما حدث أيضا في 2008 في الحرب بين روسيا و جورجيا، وجاء الهجوم الإلكتروني بفيروس "ستاكسنت" على برنامج إيران النووي عام 2012، ليبرز قوة الأسلحة السيبرانية في الصراعات الدولية.

ولعل أبرز ما يعزز انتشار الأنشطة غير السلمية في الفضاء السيبراني[7]:

1- ارتباط العالم المتزايد بالفضاء السيبراني وزيادة خطر تعرض البنية التحية الكونية للمعلومات لهجمات سيبرانية.

2- استخدام الفاعلين من غير الدول للفضاء السيبراني لتحقيق أهدافهم وتأثير ذلك على سيادة الدولة.

3- انسحاب الدولة من قطاعات استراتيجية لصالح القطاع الخاص.

4- إشكالية تعامل الدول مع الشركات التكنولوجية متعدية الجنسيات، والتي أصبحت تفوق قدراتها، مثل مواقع الشبكات الاجتماعية كالفيس بوك وتوتير واليوتيوب الذين أصبحوا فاعلين دوليين بامتياز.

وبالتالي أصبح الفضاء السيبراني ساحة جديدة للصراع بشكله التقليدي ولكنه ذو طابع سيبراني يعكس النزاعات التي تخوضها الدول أو الفاعلين من غير الدول على خلفيات دينية أو عرقية وإيديولوجية أو اقتصادية أو سياسية، ويتمدد الصراع السيبراني بداخل شبكات الاتصال والمعلومات متجاوزا الحدود التقليدية وسيادة الدول.

وكشف استخدام الفضاء السيبراني عن حالة التعارض الحقيقي للاحتياجات والقيم والمصالح بين العديد من الفاعلين، وساعد ذلك على ظهور أساليب جديدة للصراع الدولي، تباينت بين الطابع التقني والتجاري والاقتصادي والعسكري، إلى جانب ظهور طرق بديلة عن الحرب المباشرة بين الدول عبر شبكات الاتصال والمعلومات.

فهناك صراع سيبراني تحركه دوافع سياسية، ويأخذ شكلا عسكريا، ويتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء السيبراني ،ويوجد صراع سيبراني ذو طبيعة ناعمة، حول الحصول على المعلومات والتأثير في المشاعر والأفكار وشن حرب نفسية وإعلامية ،كما يأخذ الصراع السيبراني طابعا تنافسيا حول الاستحواذ على سبق التقدم التكنولوجي وسرقة الأسرار الاقتصادية والعلمية، والتحكم بالمعلومات، والعمل على اختراق الأمن القومي للدول، كهجمات قراصنة الكمبيوتر والتجسس بما يكون له من تأثير على تدمير الاقتصاد والبنية التحتية بنفس القوة التي قد يسببها تفجير تقليدي مدمر ،ويمكن أن يستخدم الفضاء السيبراني كوسيلة من وسائل الصراع داخل الدولة، بين مكوناتها، على أساس طائفي أو اقتصادي أو ديني.

المبحث الرابع

مفهوم الأمن السيبراني وأبعاده

المطلب الأول: تعريف الأمن السيبراني

يعرف الأمن السيبراني بأنه امن الشبكات والأنظمة المعلوماتية، والبيانات، والمعلومات، والأجهزة المتصلة بالأنترنيت، وعليه فهو المجال الذي يتعلق بإجراءات، ومقاييس، ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، او على الأقل الحد من آثارها[(8)].

فريتشارد كمرر Richard A.Kemmerer يعرف الأمن السيبراني بأنه :"عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة"[(9)].

بينما عرفه إدوارد أمورسو Edward Amorso على أنه :"وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها،.. إلخ"[(10)].

وبحسب تعريف الاتحاد الدولي للاتصالات في تقريره حول (اتجاهات الاصلاح في الاتصالات للعام 2010-2011)، هو " مجموعة من المهمات، مثل تجميع وسائل، وسياسات، وإجراءات أمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية، وموجودات المؤسسات والمستخدمين"[(11)]،وتهدف الحماية إلى جعل المعتدين يحجمون عن خططهم، أو منعهم من تحقيقها، وإلى ضمان حد مقبول من الأخطار، وذلك عبر وضع خطة تتلاءم والمحيط التقني، البشري، التنظيمي، والقانوني.

المطلب الثاني: أبعاد الأمن السيبران

يطال الأمن السيبراني جميع المسائل العسكرية، الاقتصادية، والاجتماعية، والسياسية، والإنسانية، بهدف تحقيق منظومة أمن متكاملة تعمل على الحفاظ على الأمن القومي للدولة من كل التهديدات السيبرانية، وعليه لابد من توضيح أبعاد الأمن السيبراني، التي نوردها كالآتي[(12)]:

- البعد العسكري:

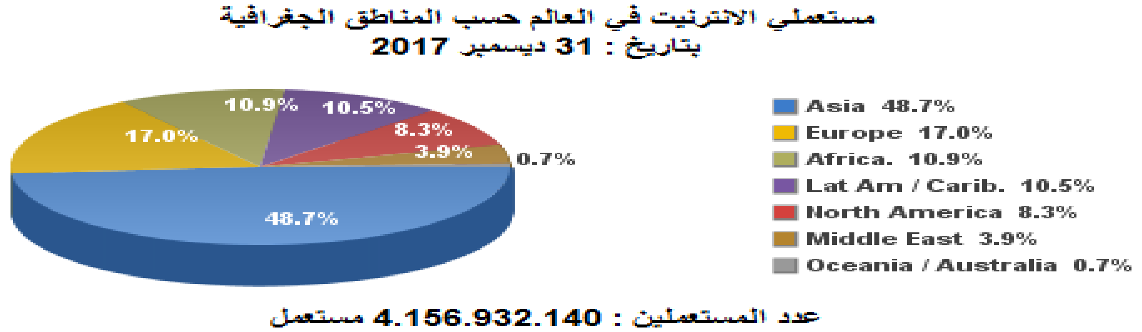
يكمن في الحفاظ على قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية، مما يسمح بتبادل المعلومات والأوامر وتدفقها (هي الفكرة التي خلقت وطورت من أجلها الشبكات ومن بعدها الانترنيت)، وإصابة الأهداف عن بعد، إلا أنها تمثل كذلك نقطة ضعف، خاصة إذا لم تكن مؤمنة جيدا من الاختراق، الذي قد يؤدي إلى تدمير قواعد البيانات العسكرية، أو قطع الاتصال بين القيادة والوحدات العسكرية، فضلا عن إمكانية التحكم في بعض الأسلحة وخروجها عن السيطرة (طائرات بدون طيار، صواريخ موجهة، أقمار صناعية.... إلخ)، ويعتبر فيروس ستاكسنت Stuxnet بداية لاستعمال القوة السيبرانية لتدمير البنية المادية (هاجم حواسيب أجهزة الطرد المركزي الإيرانية).

- البعد الاقتصادي:

أصبح الانترنيت أساسا للمعاملات التجارية والمالية والاقتصادية، كما تستعمل الحواسيب في تسيير وتطوير الصناعات وتحريك الاقتصاد، وأصبح الكل مترابطا عبر شبكات الكمبيوتر، مما يستدعي الحديث عن أهمية تحقيق الأمن السيبراني في المجال الاقتصادي.

- البعد الاجتماعي:

مستعملي الانترنيت حول العالم.



المصدر: Internet world statsعلى الموقع www.internetworldstats.com

يفوق مستخدمي الانترنيت 4 مليارات شخص في العالم، منهم أكثر من 2.6 مليار يستخدمون مواقع التواصل الاجتماعي، مما يجعلها أكبر تجمع للتفاعل البشري، ويفتح الباب واسعا لتبادل الأفكار والخبرات الجيدة، لكن في المقابل يعرض أخلاقيات المجتمع للخطر، نظرا لصعوبة مراقبة محتوى الانترنيت، كما يعرض الهويات لعمليات اختراق خارجي قد تتسبب في تهديد السلم الاجتماعي للدولة، وعليه فلابد من العمل على توعية المواطن بهذه المخاطر لتحقيق الأمن السيبري في بعده الاجتماعي.

- البعد السياسي:

يعد التدخل الروسي السيبراني في الانتخابات الأمريكية أبرز دليل على ضرورة وأهمية الأمن السيبري في بعده السياسي، إضافة إلى التسريبات للوثائق الحساسة والاختراقات التي غالبا ما تؤدي إلى أزمات دبلوماسية بين الدول، كما أن الفضاء السيبراني أصبح بيئة خصبة للحملات الانتخابية والدعاية لمختلف الفاعلين الدوليين.

- البعد القانوني:

إن التطورات التكنولوجية المتسارعة، تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية في الفضاء السيبراني، فالملاحظ أن الجريمة السيبرانية تفتقد في معظم البلدان الى الأطر القانونية الصارمة للتعامل معها، إضافة إلى ضرورة تفعيل التعاون الدولي المشترك لمكافحتها.

المبحث الخامس

أنماط التهديدات السيبرانية

تنقسم التهديدات السيبرانية التي تواجهها الدول والأفراد إلى أربعة أنماط رئيسية هي[13]:

هجمات الحرمان من الخدمة: حيث يتم إطلاق حزمة كبيرة من الطلبات والمهمات على خوادم الضحية بصورة تفوق قدرة الخادم أو الجهاز على معالجتها والاستجابة لها، مما يؤدي إلى توقفه بصورة جزئية أو كلية أو إبطاء عمله، وهذا ما يسبب ضررا للمستخدم النهائي، وهي تستعمل كثيرا ضد مواقع الانترنيت أو البنوك أو المؤسسات من أجل التأثير عليها أو لدفع فدية مالية.

1- إتلاف المعلومات أو تعديلها:

ويقصد به الوصول إلى معلومات الضحية عبر شبكة الانترنيت أو الشبكات الخاصة، والقيام بعملية تعديل البيانات الهامة دون أن يكتشف الضحية ذلك، فالبيانات تبقى موجودة لكنها مضللة قد تؤدي إلى نتائج كارثية خاصة إذا كانت خطط عسكرية أو مواعيد أو خرائط سرية.

2- التجسس على الشبكات:

ويقصد به الدخول غير المصرح والتجسس على شبكات الخصم، دون تدمير أو تغيير في البيانات، والهدف منه الحصول معلومات قد تكون خطط عسكرية أو أسرار حربية، اقتصادية ، مالية ، أو سياسية، مما يؤثر سلبا على مهام الخصم.

3- تدمير المعلومات:

ويتم في هذه الحالة مسح وتدمير كامل للأصول والمعلومات والبيانات الموجودة على الشبكة، يصطلح عليه " تهديد لسلامة المحتوى" ويعني بها إحداث تغيير في البيانات سواء بالحذف أو التدمير من قبل أشخاص غير مخولين.

وهناك من يميز بين عدة أنواع لمخاطر التهديدات السيبرانية نذكر منها[14]:

- التعرض لسرية الاتصالات التي تطال البريد الالكتروني، والدخول إلى الأنظمة والملفات دون إذن، وهذا يعتبر اعتداء على الحريات والحقوق الشخصية.

- التلاعب بالمعلومات الموجودة في نظام معين، وتشويهها أو إتلافها، سواء عبر الاختراق أو نشر الفيروسات.

- الجرائم العادية التي تستخدم الانترنيت، للسرقة والغش وسرقة الهويات، والاعتداء على الملكية الفكرية وغيرها.

- الجرائم التي تندرج في إطار الجريمة المنظمة، والتي تهدد امن الأفراد والدول، كتبييض الأموال والإرهاب...إلخ، كالتهديدات الأمنية الخاصة بنظام الفدية، وهي أداة إجرامية انتشرت عبر الإنترنت لعدة سنوات، مستمرة في التطور وتشمل كلاً من الأفراد والاقتصادات. على المستوى الفردي، حيث لا تزال حملات القرصنة بنظام الفدية تحقق عائدات كبيرة للقراصنة ففي الإمارات وحدها، تم خسارة حوالي 1.1 مليار دولار أمريكي من أفراد المجتمع لأنشطة الجريمة السيبرانية في عام 2017.

المبحث السادس

علاقة الأمن السيبراني بالأمن القومي

المطلب الأول: الأمن السيبراني رافد جديد للأمن القومي

تزايدت العلاقة بين الأمن والتكنولوجيا، ومعها تزايدت امكانية تعرض المصالح الاستراتيجية للدولة للتهديدات السيبرانية، وتهدد بتحول الفضاء السيبراني لوسيط ومصدر لأدوات جديدة للصراع الدولي المتعدد الاطراف.

بعد أحداث 11 سبتمبر بدأ التركيز على الفضاء السيبراني كتهديد أمني جديد، خاصة مع استخدام تنظيم القاعدة له كساحة قتال ضد الولايات المتحدة الامريكية، وفي 2007 و2008 على التوالي، كان الأمن القومي لكل من استونيا وجورجيا مهددا من طرف روسيا، حيث استعملت هجمات الحرمان من الخدمة لتقويض العمل في الإدارات والمؤسسات الحكومية لكلا الدولتين، وأصبح الفضاء السيبراني للدولتين مجالا للعمليات، وجاء الهجوم السيبراني بفيروس "ستاكسنت" على أجهزة الطرد المركزي الايرانية، من أجل تعطيل برنامج ايران النووي، ليمثل نقلة نوعية مهمة في تطوير واستخدام الأسلحة السيبرانية[15]،هذا إضافة الى الدور الكبير الذي لعبته شبكات التواصل الاجتماعي في حالة الثورات العربية في بداية 2011، حيث مثلت نقطة هامة في زيادة الاهتمام الدولي بأمن الفضاء السيبراني، وبرزت

محاولات للسيطرة عليه بعد تصاعد الاحتجاجات حتى في الدول الاكثر ديموقراطية كبريطانيا والولايات المتحدة الامريكية.

وإذا كان الأمن القومي يعنى بالحماية وغياب التهديد لقيم المجتمع الأساسية وغياب الخوف من خطر تعرض هذه القيم للهجوم، فإن الفضاء السيبراني قد فرض إعادة التفكير في مفهوم الأمن، والذي يتعلق بدرجة تمكن الدولة من أن تصبح في مأمن من خطر التعرض للهجوم، وإجراءات الحماية ضد تعرض المنشآت الحيوية للبنية التحتية للتهديد، من خلال الاستخدام السيئ لتكنولوجيا الاتصال والمعلومات.

إن العلاقة بين الأمن السيبراني والأمن القومي تزداد كلما زاد نقل المحتوى المعلوماتي والعسكري والامني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي إلى الفضاء السيبراني، خاصة مع التسارع في تبني الحكومات الالكترونية والمدن الذكية في العديد من الدول، واتساع نطاق وعدد مستخدمي الانترنيت في العالم، حيث تصبح قواعد البيانات القومية في حالة انكشاف خارجي، اضافة الى حملات الدعاية والمعلومات المضللة ونشر الشائعات أو الدعوة لأعمال تحريضية أو دعم المعارضة أو الاقليات، مما يساهم في تلاشي سيادة الدولة ويشكك في قدرتها على الحفاظ على أمنها القومي[16].

وعليه فلم يقتصر اهتمام الدول بالأمن السيبراني على البعد التقني وحسب بل تجاوزه إلى أبعاد أخرى مثل الإبعاد الثقافية والاجتماعية والاقتصادية والعسكرية وغيرها وهو ما عمل على دعم حقيقة ان الاستخدام غير السلمي للفضاء الإلكتروني يؤثر على الرخاء الاقتصادي والاستقرار الاجتماعي لجميع الدول التي أصبحت تعتمد على البنية التحتية الكونية لمعلومات.

إضافة الى ان تصاعد دور الفاعلين من غير الدول في العلاقات الدولية قد اثر بدوره على سيادة الدول وبخاصة مع بروز دور الشركات التكنولوجية عابرة للحدود الدولية وبروز أخطار القرصنة والجريمة السيبرانية والجماعات الإرهابية.

لقد أصبحت المصالح القومية التي ترتبط بالبنية التحتية الحيوية عرضة لخطر الهجوم، حيث جعل الفضاء السيبراني تلك المصالح مرتبطة ببعضها البعض في بيئة عمل واحدة، ومن ثم فإن أي هجوم على إحدى تلك المصالح يكون سببا لحدوث عدم توازن استراتيجي ومهددا خطيرا للأمن القومي، وهذا ما دفع العديد من الدول إلى إدخال الأمن السيبراني ضمن استراتيجيتها للأمن القومي.

المطلب الثاني: العقيدة الأمنية الجديدة

إن حالة انعدام الثقة واللايقين في العلاقات الدولية، هو ما يشجع تزايد النزاعات في العالم، إضافة إلى التطورات السريعة في الفضاء السيبراني، جعلت الدول تسارع إلى تبني تغييرات في العقيدة الامنية، وذلك بإدراج القوة السيبرانية كمحدد رئيس لمدى قوة الدولة، وقدرتها على حسم النزاعات لصالحها.

وكمثال على ذلك، نجد أن العقيدة الروسية الجديدة ، تكشف أنه تمت إضافة بند جديد يخص تهديدات الأمن السيبراني في المجالين العسكري والاقتصادي.

ووفقا للعقيدة الروسية الجديدة لأمن المعلومات، التي وقعها الرئيس الروسي فلاديمير بوتين، فإن إحدى التهديدات الرئيسية لروسيا تتمثل "بزيادة عدد الدول الأجنبية التي لديها تأثير على البنية التحتية لمعلومات الأغراض العسكرية في روسيا".

أحد الأهداف الرئيسية لواضعي هذه العقيدة للأمن السيبراني، هو "الردع الاستراتيجي والوقاية من النزاعات العسكرية، والتي يمكن أن تنجم عن استخدام تكنولوجيا المعلومات. [17]"

يقول أوليغديميدوف، وهو خبير في الأمن السيبراني، مؤسسة الرأي الروسية بي آي آر: "العقيدة في شكلها الحالي هي العقيدة الأفضل بما يخص التهديدات الموجهة للأمن العسكري والتكنولوجي في روسيا". على سبيل المثال، هي تعمل على الحماية من العمليات السيبرانية من قبل الأجهزة الخاصة الأجنبية، فضلا عن مكافحة النشاط الاستطلاعي الأجنبي في روسيا، ويشير الخبير إلى أن الحكومة الروسية أولت اهتماما خاصا لمواجهة "ثورات التويتر" الجديدة، كتلك التي حدثت في الشرق الأوسط في بداية العقد الحالي.

ارتبط تصاعد الصراع بين روسيا والدول الغربية بقيادة الولايات المتحدة، خلال السنوات الماضية، باستدعاء متنام لحرب المعلومات كأحد للمداخل الهامة للتأثير في مسارات الصراع.

كما يعتقد ديفيد سميث David J. Smith في دراسة له بعنوان "كيف تستخدم روسيا الحرب السيبرانية؟"، أن روسيا "تعتمد على مفهوم واسع للحرب المعلوماتية، يشمل: الاستخبارات، والتجسس المضاد، والخداع، والتضليل، والحرب الإلكترونية، وتدمير الاتصالات وأنظمة دعم الملاحة، والضغوط النفسية، بالإضافة إلى الدعاية وإلحاق الضرر بنظم المعلومات"[18].

ويفترض "بافل أنتونوفيتش" Pavel Antonovich أن "ترسيم الخطوط الفاصلة بين الحرب والسلام يمكن أن يتآكل بسهولة في الفضاء السيبراني، فيمكن أن يتم إلحاق أضرار، مهما كانت طبيعتها، بالخصم، وذلك دون تجاوز الخط الفاصل بين الحرب والسلام بشكل رسمي".

وفي الجهة المقابلة، نجد أن منظمة "حلف شمال الأطلسي NATO" سعت بدورها إلى تحديث عقيدته الأمنية، استجابة للتغيرات الحاصلة في طبيعة التهديدات، وطبيعة الحرب، حيث أقر بمجموعة من النقاط الأساسية من بينها:

- أن الدفاع السيبراني يمثل جزءا أساسيا من الدفاع الجماعي للحلف.
- الفضاء السيبراني يمثل مجالا لعمليات الحلف.
- بناء قدرات سيبرانية تعد مهمة اساسية للحلف وحلفائه[19].

بالإضافة الى ذلك ، نجد كلا من الصين، اسرائيل، بريطانيا، فرنسا، والولايات المتحدة الأمريكية، إيران، وكوريا الشمالية، قد طورت كل منها عقيدتها الأمنية، وأصبحت تعتبر الفضاء السيبراني مسرحا للعمليات العسكرية، كما أوجدت قيادة خاصة ومستقلة لقيادة العمليات السيبرانية.

المطلب الثالث: الحروب السيبرانية

تكمن خطورة الحروب السيبرانية في كون العالم أصبح يعتمد أكثر فأكثر على الفضاء السيبراني، لا سيما في البنى التحتية المعلوماتية، ولا شك أن ازدياد الهجمات السيبرانية يعني إمكانية تطورها لتصبح سلاحا حاسما في النزاعات بين الدول في المستقبل.

الفرع الأول: مفهوم الحرب السيبرانية

لا يوجد إجماع على تعريف محدد ودقيق لمفهوم الحرب السيبرانية، فيعرفها كل من "ريتشارك كلارك" و"روبرت كناكي" على أنها "أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها"[20].

ويعرفها "بولو شاكريان" Paulo Shakarian بأنها :" امتداد للسياسة من خلال الإجراءات المتخذة في الفضاء السيبراني من قبل دول أو فاعلين غير دوليين، حيث تشكل تهديدا خطيرا للأمن القومي"[21].

يقترح آخرون أن يتم التركيز بدلا من ذلك على أنواع وأشكال النزاع التي تحصل في الفضاء السيبراني، ويحددون مستوياتها كالتالي:

- **القرصنة السيبرانية:**

وتقع في المستوى الأول، ومن أمثلته القيام بعمليات قرصنة المواقع الإلكترونية أو بتعطيل الحواسيب الخادمة (Servers) من خلال إغراقها بالبيانات.

- **الجريمة السيبرانية والتجسس السيبراني:**

ويقعان في المستوى الثاني والثالث وغالبا ما يستهدفان الشركات والمؤسسات وفي حالات نادرة بعض المؤسسات الحكومية.

- **الإرهاب السيبراني:**

ويقع في المستوى الرابع ويعبر عن الهجمات غير الشرعية التي ينفذها فاعلون غير حكوميون ضد أجهزة الكمبيوتر والشبكات والمعلومات المخزّنة.

- **الحرب السيبرانية:**

وهي المستوى الأخطر للنزاع في الفضاء السيبراني، وتهدف إلى التأثير على إرادة الطرف المستهدف السياسية وعلى قدرته في عملية صنع القرار، وكذلك التأثير فيما يتعلق بالقيادة العسكرية و/أو توجهات المدنيين في مسرح العمليات الإلكتروني[22].

الفرع الثاني: خصائص الحروب السيبرانية

من المتوقع أن تصبح الحرب السيبرانية نموذجا تسعى إليه العديد من الجهات نظرا للخصائص العديدة التي تنطوي عليها، ومنها:

- حروب لا تناظرية (Asymmetric):

فالتكلفة المتدنية نسبيا للأدوات اللازمة لشن هكذا حروب يعني أنّه ليس هناك حاجة لدولة معينة او منظمة ما لقدرات ضخمة لتشكل تهديدا خطيرا وحقيقيا على دولة مثل الولايات المتّحدة الأمريكية.

- تمتع المهاجم بأفضلية واضحة:

فهذه الحروب تتميز بالسرعة والمرونة والمراوغة. وفي بيئة مماثلة يتمتّع المهاجم بأفضلية، ومن الصعوبة نجاح عمليات الدفاع.

- المخاطر تتعدى استهداف المواقع العسكرية:

هناك جهود متزايدة لاستهداف البنى التحتية المدنية والحسّاسة كاستهداف شبكات الكهرباء والطاقة وشبكات النقل والنظام المالي والمنشآت الحساسة النفطية أو المائية أو الصناعية بواسطة فيروس يمكنه إحداث أضرار مادّية حقيقية تؤدي الى دمار هائل.

الفرع الثالث: تداعيات الحروب السيبرانية على الامن القومي

سببت الحروب السيبرانية جملة من المخاطر والتداعيات على تفاعلات السياسة الدولية، يمكن طرح أبرزها على النحو الآتي[23]:

1- تصاعد المخاطر الإلكترونية، خاصة مع قابلية المنشآت الحيوية (مدنية وعسكرية) في الدول للهجوم، الأمر الذي يؤثر في وظائف تلك المنشآت. وبالتالي، فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة استراتيجية .

2- تعزيز القوة وانتشارها، عمل الفضاء السيبراني على إعادة تشكيل قدرة الأطراف المؤثرة، وأدى الى عملية انتشار القوة بين فاعلين متعددين.

3- عسكرة الفضاء السيبراني، حيث برز في هذا الإطار عدة اتجاهات، مثل التطور في مجال سياسات الدفاع والأمن السيبراني، وتصاعد القدرات في سباق التسلح السيبراني، وتبني سياسات دفاعية سيبرانية لدي الأجهزة المعنية بالدفاع والأمن في الدول، وتزايد الاستثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة[24].

4- إدماج الفضاء الإلكتروني ضمن الأمن القومي للدول، وذلك عبر تحديث الجيوش، وتدشين وحدات متخصصة في الحروب الإلكترونية، وإقامة هيئات وطنية للأمن والدفاع الإلكتروني، والقيام بالتدريب، وإجراء المناورات لتعزيز الدفاعات الإلكترونية.

5- الاستعداد لحروب المستقبل، حيث تبني العديد من الدول استراتيجية حرب المعلومات باعتبارها حربا للمستقبل، حيث تري الدول الكبرى أن من يحدد مصير تلك المعركة المستقبلية ليس من يملك القوة فقط، وإنما القادر على شل القوة، والتشويش على المعلومة.

الخاتمة:

نخلص إلى أن مفهوم الأمن القومي قد طرأ عليه الكثير من التعديل والتغيير، على مستوى التهديدات، الفاعلين، والقطاعات، فبعد أن بدأ عند الواقعيين محصورا في الدولة والقوة العسكرية، توسع في مفهومه الشامل، ليعم جميع مجالات الحياة، مركزا على أمن الافراد والمجتمعات، هذه الاخيرة التي دخلت العصر الرقمي بفضل ثورة المعلومات والاتصالات، فالكل مرتبط بالشبكة، مما خلق فضاءً جديدا للتفاعل، هو الفضاء السيبراني، الذي بدوره أحدث تغييرا في مفاهيم العلاقات الدولية، كمفهوم القوة والصراع والحرب، حيث انتشرت القوة بين الفاعلين، وتحول الصراع من المادي الى الافتراضي، واصبحت الحروب تخاض بالأصفار والآحاد، وبدا واضحا أن الدول تتجه نحو عسكرة الفضاء السيبراني، مما نتج عنه ظهور تهديدات جديدة تتزايد في الحجم والشدة، وتشكل تهديدا خطيرا للأمن القومي.

فكلما زاد التشابك، زادت التهديدات السيبرانية، وأثر ذلك على الأمن القومي، مما عجل بظهور مفهوم جديد هو الامن السيبراني، بأبعاده المختلفة، والذي تحاول الدول من خلاله الحد من المخاطر والتهديدات في الفضاء السيبراني.

كما نخلص إلى أن الأمن السيبراني أصبح على رأس أوليات قضايا الأمن القومي، حيث قامت معظم الدول بإعادة صياغة عقيدتها الأمنية لتتلاءم مع المتغير الجديد، وهذا في محاولة لمواجهة التهديدات السيبرانية التي تزداد وتتطور بسرعة، فالجريمة والارهاب والحرب في الفضاء السيبراني تعد من بين التحديات الأمنية الجديدة أمام الدول.

الهوامش:

(1) عباس بدران، الحروب الالكترونية: الاشتباك في عالم متغير، مركز دراسات الحكومة الالكترونية، بيروت،2010، ص 4.

(2) Olivier KEMPF, Introduction à la Cyberstratégie, Paris, Economica, 2012, P 9.

(3) The International Télécommunication Union, ITU Toolkit for CybercrimeLégislation, Geneva, 2010, P 12.

(4) Joseph S.Nye JR , Cyber Power, Harvard Kennedy School, 2010, P 03 .

(5) Joseph S.Nye JR , Cyber Power, Harvard Kennedy School, 2010, P 10 .

(6) ايهاب خليفة القوة الالكترونية وأبعاد النحول في خصائص القوة ، مكتبة الاسكندرية، مصر، 2014، ص 33-42.

(7) عادل عبد الصادق أسلحة الفضاء الالكتروني في ضوء القانون الدولي، سلسلة أوراق، العدد 23، مكتبة الاسكندرية، مصر، 2016، ص 17-18.

(8) منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت ، 2017، ص 25.

(9) Richard A. Kemmerer, Cyber security, University of California Santa Barbara, Department of Computer Science, 2003, P.3

(10) Edward Amoroso, Cyber Security, SiliconPress, 2007 , P01.

(11) ITU, Cyber security, Geneva: International Telecommunication Union (ITU),2008.

(12) عادل عبد الصادق، القوة الالكترونية: اسلحة الانتشار الشامل في عصر الفضاء الالكتروني، مجلة السياسة الدولية، العدد 188، مؤسسة الأهرام، مصر، 2012، ص 32.

(13) ايهاب خليفة، القوة الالكترونية: كيف يمكن ان تدير الدول شؤونها في عصر الانترنيت، دار العربي، 2017، ص 54.

(14) ما الجديد في عقيدة الأمن السيبراني الروسي؟، مركز دراسات ، على الموقع :
تاريخ النشر: 12-12-2016. http://katehon.com/ar/article/m-ljdyd-fy-qyd-lmn-lsybrny-lrwsy

(15) David Smith, How RussiaHarnesses Cyber Warfare,Defense Dossier, American Foreign Policy Council (August 2012: Issue 4), 9. Accessedathttp://www.afpc.org/files/august2012.pdf.

(16) حمد بسيوني، دوافع الاستراتيجية الروسية لحرب المعلومات ضد الدول الغربية، جريدة الصباحالجديد ، على الرابط:
http://newsabah.com/newspaper/138116 تاريخ النشر : 30-10-2017.

(17) Cyber defence, North Atlantic TreatyOnganisation, 19-02-2018, At :
https://www.nato.int/cps/en/natohq/topics_78170.htm

(18) Richard A. Clarke & Robert knake,CyberWar: The NextThreat to National Security and What to Do About It, HarperCollins, 2010, p:6.

(19) Paulo & Jana Shakarian, Andrew Ruef, Introduction to Cyber warfare, A multidisciplinaryApproach, Elsevier, 2013, P 02.

(20) المجال الخامس.. الحروب الإلكترونية في القرن الـ21، مركز الجزيرة للدراسات، على الموقع :
http://studies.aljazeera.net/ar/issues/2010/20117212274346868.html ، تاريخ النشر : 12-01-2011

(21) عادل عبد الصادق، الحروب السيبرانية : تصاعد القدرات والتحديات للأمن العالمي، المركز العربي لأبحاث الفضاء الالكتروني. على الموقع: http://accronline.com/article_detail.aspx?id=28395 ، تاريخ النشر : 12-03- 2017.

(22) محمد مختار، الأمن السيبراني ، مفاهيم المستقبل، اتجاهات الأحداث ، العدد 6 ، 2015، ص 6.

(23) محمد مختار، هل يمكن للدول أن تتجنب مخاطر الهجمات الالكترونية؟، مفاهيم المستقبل، العدد 6، مركز المستقبل للأبحاث والتطوير، 2015، ص 5-6.

(24) منى الأشقر جبور، السيبرانية هاجس العصر، مرجع سابق ، ص 35-36.

الفضاء السيبراني والتحول في مفاهيم القوة والصراع ـــــــ