السيبرانيـــــة .... «الماهيـــة – الخصائـــص – الفواعـــل – الأَبعاد الاستراتيجية»

*** محمد أَكرم محسن**
***أ.م.د. مروان سالم علي**
باحثان من العراق

*جامعة الموصل/ كلية العلوم السياَسية
Marwanalali225@gmail.com

ملخص :

أَصبحت السيبرانية كغيرها مِن المجالات التقليدية ميداناً جديداً مِن ميادِين الصِراع، لها مفهومها وعناصرها وخصائصها وفواعلها، فضلاً عن أبعادها الاستراتيجية. إذ ادخلت الفواعل الدولية في فوضى مفاهيم السيبرانية ومكامن قوتها وعناصرها، فضلاً عن طرائق توظيفها بين ما هو مُفيد أو مُسبباً للضرر. فإلى جانب قوة الدولة الصلبة والناعِمة ظهرت القوة السيبرانية التي أصبحَ لها تأثيرها على المستويين المحلى والدولي، وأدت إلى تعدُد مستويات القوة بين الفاعلين دون حصرها بالدولة.

وأصبحَ واضِحاً لدى الفواعل الدولية أَنّ من يمتلك آليات توظيف البيئة السيبرانية يصبح في عالم اليوم الأكثر قدرة على تحقيق التأثير في سلوك الفاعلين المُستخدمين لهذه البيئة، هذا ما عمل على إدخال العالم في آليات ومفاهيم جديدة وصِراعات مُتجددة من التهديدات والحروب السيبرانية.

ومِن هُنا؛ يهدُف البحث إلى تقديم إطار نظري عن مفهوم السيبرانية والمفاهيم المُرتبطة بها واستعراض أهم خصائصها وتحديد أشكالها وعناصرها وفواعلها وأنماط الحروب السيبرانية، وأبعادها الاستراتيجية عبر ثلاثة محاور رئيسة تناول الأول: ماهية السيبرانية والمفاهيم المُرتبطة بها. أما الثاني فتعرض إلى خصائص الفضاء السيبراني (الإلكتروني) وعناصرهُ. أما المحور الثالث فتطرق إلى فواعل الفضاء السيبراني وأبعادهُ الاستراتيجية.

كلمات مفتاحية : السيبرانية، الفيروسات، فواعل الفضاء السيبراني (الالكتروني)، الأمن السيبراني، الأبعاد الاستراتيجية

Cyber: "What is it - Characteristics - Factors - Strategic Dimensions"

Mohammed Akram Muhsin
Prof. Dr. Marwan Salim Ali
College of Political Sciences/ University of Mosul

ABSTRACT

Like other traditional fields, cyber has become a new field of conflict, with its concept, elements, characteristics, and factors, as well as strategic dimensions. International actors have been plunged into the chaos of cyber concepts, their strengths, and elements, as well as the ways in which they are used between useful or harmful. In addition to the solid and soft power of the State, cyber power has emerged, which has had an impact on the domestic and international levels and has led to multiple levels of power among actors without limiting it to the State.

It has become clear to international actors that those who have the mechanisms to employ the cyber environment are now the most capable of influencing the behavior of the factors employed in this environment, bringing the world into new mechanisms and concepts and renewed conflicts of threats and cyber wars.

The research aims to provide a theoretical framework for the concept of cyber and associated concepts, to review its most important characteristics, to identify its forms, elements, parts and patterns of cyber warfare, and its strategic dimensions across three main themes: what cyber is and what concepts are associated with it. The second is related to the characteristics and elements of cyberspace. The third section touched on the satellites of cyberspace and its strategic dimensions.

KEY WORDS: cyber, viruses, cyberspace hubs, cybersecurity, strategic dimension

المُقدمة

في خضم التقدُم التقني والإلكتروني الـذي أَوجدته الثورة التكنومعلوماتية في العالم المُعاصر تحولت مُعظم الدول والمُنظمات والمؤسسات والشركات وحتى الأَفراد إلى مُنتجة ومُتلقية ومُستخدمة للقوة السيبرانية (الإلكترونية) الحديثة بشكلٍ كبير التي عملت بدورها على إحلال الأَنظمة الرقمية الإلكترونية من هواتف محمولة وحواسيب متطورة وشبكات إنترنت وأَنظمة تشغيل مكنت الدول أَن تحدث نقلة في معيار ما تملكهُ من قوة تُمكنُها من تهديد الأَمن الدولي بتوظيف القوة والفضاء السيبراني، ومما لاشك فيه إن هذه القوة السيبرانية قد أَدخلت الفواعل الدولية في فوضى مفاهيم السيبرانية ومكامن قوتها وعناصرها، فضلاً عن طرائق توظيفها بين ما هو مُفيد أَو مُسبباً للضرر. وأَصبح واضحاً لدى الفواعل الدولية أن من يمتلك آليات توظيف البيئة السيبرانية يصبح في عالم اليوم أَكثر قدرة على تحقيق التأَثير في سلوك الفاعلين المُستخدمين لهذه البيئة، هذا ما عمل على إدخال العالم في آليات ومفاهيم جديدة وصراعات مُتجددة من التهديدات والحروب السيبرانية، فرضت على الدول تغيير الاستراتيجيات الأَمنية والاقتصادية والعسكرية والسياسية ومن ثُم إعادة النظر والسعي قدُماً لإدراك القوة السيبرانية والمعايير المُتعلقة بها.

أَهمية البحث:

تتجلى أَهمية البحث في أَنهُ يجمع بين الشقين: العلمي (النظري)، والعملي (التطبيقي):

1. الأَهمية العلمية (النظرية)

- تظهر الأَهمية النظرية للبحث في تناوله أَحد أَهم القضايا الحديثة في الأَدبيات الاستراتيجية وعلم العلاقات الدولية، التي أَصبحت تشغل حيزاً كبيراً من اهتمامات المراكز البحثية الغربية بالأَساس وهي القوة السيبرانية (الإلكترونية) كأَحد أَهم المجالات التي تُمارس فيها التفاعُلات الدولية والتي فرضت نفسها بقوة ولم تزل

خصوصاً في العقدين الماضيين من القرن الحادي والعشرين.

- كما تنبع أهمية البحث في تقديم إطار نظري عن مفهوم السيبرانية والمفاهيم المُقاربة لها، وعناصر السيبرانية وفواعلها.
- الأهمية العملية (التطبيقية)
- نتائج الدراسة يمكن أن تسهم في تقديم رؤية لصُناع القرار في دول العالم للتعامُل مع مُتغيرات البيئة الدولية تلك، على نحوٍ يُقلل من تأثيرات السيبرانية السلبية على الأمن الدولي.
- كما إن البحث بإمكانه أن يسهم على نحوٍ كبير في الجانب العلمي والعملي في ظل غياب أو قلة الكتابات العربية الأكاديمية التي تخصصت في هذا الموضوع، وإغناء المكتبات بها، بما يخدم الطلبة.

هدف البحث:

يهدُف البحث إلى تحقيق عدد من الأهداف أهمها؛ تقديم إطار مفاهيمي عن مفهوم السيبرانية والمفاهيم المُرتبطة بها واستعراض أهم خصائص القوة السيبرانية وتحديد أشكالها وعناصرها وفواعلها وأنماط الحروب السيبرانية، بما يُساعد في إغناء المكتبات المعنية بتلك الأُطر المفاهيمية كإطار ثابت. وتسليط الضوء على أهم واخر تحولات القوة التي شهدها حقل العلاقات الدولية وانتقالها من القوة الصلبة ثُم الناعمة ثُم الذكية وصولاً إلى القوة السيبرانية. فضلاً عن المُساهمة في خلق وتطوير الوعي الجمعي بشأنَّ ظاهرة السيبرانية وتهديدها للأمن، فهي سلاحٌ ذو حدين.

إشكالية البحث:

يرتكز البحث حول إشكاليةٌ أساسيةٌ مفادها؛ إنَّ المُتغيرات التكنومعلوماتية العالمية غدت تُشكل تهديداً واضحاً للأمن الدولي وذلك نتيجة تزايُد انتشار الهجمات السيبرانية في الفضاء السيبراني، وبذلك تتمحور الإشكالية حول التساؤل الرئيس الآتي: من هُم الفاعلون الرئيسيون في مجال استخدام القوة السيبرانية؟ وتقودنا هذه الإشكالية إلى طرح مجموعة من التساؤلات الفرعية، ومنها ما

المقصود بالسيبرانية؟، وكيف يمكن تمييزها عن غيرها مِن المفاهيم المُقارِبة؟، وما هي خصائصها وعناصرها؟

فرضية البحث:

يقوم البحث على فرضيةٌ مفادها؛ انهُ بجانب قوة الدولة الصلبة والناعمة ظهرت القوة السيبرانية التي أَصبح لها تأثيرها على المستويين المحلى والدولي، وأدت إلى تعدُد مستويات القوة بين الفاعلين دون حصرها بالدولة، بعد أَنَّ أَصبح المجال السيبراني كغيره مِن المجالات التقليدية ميدان جديد مِن ميادين الصِراع، مجال له مفهومه وعناصره وخصائصه وفواعله الجدُّد، فضلاً عن أَبعاده الاستراتيجية.

مناهج البحث:

لسعة الموضوع وشموليته وتنوعه اعتمد الباحث مناهج عديدة، منها: (المنهج التاريخي) الذي كان لا بُد منه في الوقوف على استقراء تطورات القوة السيبرانية تاريخياً حتى وصلت إلى ما هي عليه اليوم. كما تم استخدام (المنهج الوصفي) لما يتطلبهُ موضوع من إعطاء وصفاً دقيقاً لمفهوم السيبرانية والمفاهيم المُقاربة لها وإبراز خصائصها وعناصرها وأَبرز فواعلها وتحديد إطارها العام. فضلاً عن إيلاء (المنهج التحليلي) أَهمية خاصة في هذا البحث للوقوف برؤية تحليلية على السيبرانية وتحليل أَبعادها الاستراتيجية.

هيكلية البحث:

للوقوف على ماهية السيبرانية وخصائصها وأَبرز فواعلها وأَبعادها الاستراتيجية تم تقسيم البحث، فضلاً عن المُقدمة والخاتمة والاستنتاجات إلى ثلاثة محاور رئيسة تناول الأَول: ماهية السيبرانية والمفاهيم المُرتبطة بها. أَما الثاني فتعرض إلى خصائص الفضاء السيبراني (الإلكتروني) وعناصره. أَما المحور الثالث فتطرق إلى فواعل الفضاء السيبراني وأَبعاده الاستراتيجية.

المحور الأَول

ماهية السيبرانية والمفاهيم المُرتبطة بها

يُعد الفضاء السيبراني المجال الحيوي الجديد الناتج من

التطورات التقنية والتكنولوجيا الحديثة، وهو يلي كُل المجالات البرية والبحرية والجوية، وإنَّ كان وجوده افتراضياً إلاَّ أنَّ ما يدور فيه من مُنافسة وصِراع وهجمات وحروب الكترونية جميعها حقيقية، بل ان من المتوقع ان من يتحكم في هذا المجال الافتراضي سيكون لهُ الصدارة في قيادة العالم، لأنه يؤثر في جميع جوانب الحياة، وللوقوف على ماهية السيبرانية والمفاهيم المُرتبطة بها تم اعتماد التقسيم الآتي:

يُعد الفضاء السيبراني المجال الحيوي الجديد الناتج من التطورات التقنية والتكنولوجيا الحديثة، وهو يلي كُل المجالات البرية والبحرية والجوية، وإنَّ كان وجوده افتراضياً إلاَّ أنَّ ما يدور فيه من مُنافسة وصِراع وهجمات وحروب الكترونية جميعها حقيقية

أَولاً: ماهية السيبرانية

تُشير المراجع العلمية إلى أَنَّ عالم الرياضيات نوربرت ونير (Norbert wiener) يُعد أَول من استعمل مُصطلح السيبرانية من خلال دراسته التي قدمها عـام1948 لموضوع القيادة والسيطرة والاتصال في عالم الحيوان، فضلاً عن حقل الهندسة الميكانيكية[1]. وهُناك رواية أخرى تُشير إلى أَنَّ أَول من استخدم مُصطلح الفضاء السيبراني كان ويليام جبسون عام1984 من رواية خيال علمي، وكان يقصد به شبكات الكمبيوتر والاتصالات الإلكترونية، وهي عبارة عن شبكات كمبيوتر خيالية تحتوي على كم هائل من المعلومات التي يمكن الحصول عليها لتحقيق الثروة والسلطة، وبعيداً عن رواية ويليام جبسون فالفضاء السيبراني لم يعد خيالاً علمياً، بل أَصبح واقعاً علمياً ذات تأَثيرات سياسية واقتصادية واجتماعية[2].

ومن خلال معاجم اللُغة يتضح أنَّ كلمة سايبر (cyber) لاتينية الأَصل وترجع إلى المُصطلح (cybernetic)، الذي ورد في مؤلفات الخيال العلمي ويعني القيادة أَو التحكُم عن بُعد[3]. ويُعرف قاموس (المورد) السيبرانية على انها: علم الضبط، ومصدرها (cybernetic) وتعني ضبط الأشياء عن بُعد والسيطرة عليها[4].

وهُناك من يُعرف السيبرانية في نطاق استخدامها الفعلي أَي العسكري، دون الرجوع إلى مصدر كلمة سايبر، ذلك بحسب ما ذُكر

(1) Norbert Wiener, Cybernetic or control communication in the animal and the machine, 2nd ed. (Cambridge: M.I.T Press, 1948), P.39.

(2) صباح عبد الصبور عبد الحي، استخدام القوة الإلكترونية في التفاعُلات الدولية تَنظيم القاعدة أَنموذجاً، ج2، (إسطنبول: المعهد المصري للدراسات السياسية والاستراتيجية، 2016)، ص20.

(3) Julia Creswell, Oxford Dictionary of Word Origins; Cybernetics, (USA: Oxford University Press, 2010), P.31.

(4) منير البعلبكي، المورد: قاموس انكليزي – عربي، (بيروت: دار العلم للملايين،2004)، ص243.

في مُعظم القواميس المُتخصصة في المُصطلحات العسكرية [5]. إذ عرف القاموس العسكري الأمريكي السيبرانية في نطاقها الفعلي أي العسكري بوصفها فعل يستخدم في الشبكات الإلكترونية وأدواتها بهدف السيطرة أو تعطيل لبرامج الكترونية أخرى[6]. أيضاً عرف قاموس مُصطلحات الأمن المعلوماتي، السيبرانية بأنها: «هجوم عبر الفضاء الإلكتروني يهدف إلى السيطرة على المواقع الإلكترونية أو البُنى المحمية إلكترونياً لتعطيلها أو تدميرها أو الإضرار بها»[7].

من كُل ما ذُكر، يمكن تعريف السيبرانية بأنها القدرة على التحكُم عن بُعد والسيطرة والحماية على النظام الإلكتروني أمنياً وسياسياً واقتصاديا وعسكرياً واجتماعياً.

ثانياً: نشأة السيبرانية وتطورها

أصبح اليوم المجال السيبراني كغيره من المجالات التقليدية ميدان جديد من ميادين الصراع، وذلك من خلال الاعتماد المُتزايد على القوة السيبرانية من جانب الفواعل الدوليين وغير الدوليين بوصفها قوة مجهولة الأطراف في كثير من الأحيان وإن التدمير الناتج عنها لا يُصاحبهُ وفيات من الأشخاص، إذ تسعى جميع الأطراف المُتصارعة عبر تلك القوة تحقيق أكبر قدر من المكاسب وإلحاق أكبر قدر من الخسائر بالخصوم، كذلك إمكانية مُمارسة النفوذ سواءً داخلياً أو خارجياً وهذا لا يكون إلاَّ بامتلاك الدول لمقومات وعناصر القوة السيبرانية وطريقة توظيفها ضمن نمطيها الصلب والناعم، فقد أرتبطت نشأة السيبرانية ارتباطاً وثيقاً بظهور شبكة الإنترنت، إذ تأسست شبكة الإنترنت في الولايات المُتحدة الأمريكية في أواخر ستينات القرن العشرين كمشروع تشرف عليه، ويُعد من مشاريع البحوث المُتقدمة التابعة لوزارة الدفاع الأمريكية، فكان يُطلق أسم (اربنت) على هذه الشبكة في بداية أمرها، ويُعد عام1969 أول تاريخ لهذه الشبكة، وأقيم أول عرض لها خلال المؤتمر العلمي حول اتصالات الحاسوب بواشنطن

أصبح اليوم المجال السيبراني كغيره من المجالات التقليدية ميدان جديد من ميادين الصراع، وذلك من خلال الاعتماد المُتزايد على القوة السيبرانية من جانب الفواعل الدوليين وغير الدوليين بوصفها قوة مجهولة الأطراف في كثير من الأحيان

(5) U.S. Department of Defense, Dictionary of Military and Associated terms, (USA: Joint Publication, 2010), P.201.

(6) وليام جورتني، قاموس المُصطلحات العسكرية، وزارة الدفاع الأمريكية، مقال منشور عبر شبكة معلومات الدولية (الانترنت)، مُتاح على الرابط الآتي: file//c:/users/discov-1/appdata

(7) Richard Kassel, Glossary of key information security terms, (USA: National Institute of Standards and Technology, Department of Commerce, 2013), P. 57.

عام 1972، أما شكل الرسائل الإلكترونية فقد حددت عام1977[8] .

ولكن عند الرجوع إلى النواة الأولى لنشأة السيبرانية عبر التاريخ نجد أنها تعود إلى مرحلة قيام الحرب الأهلية في الولايات المُتحدة الأمريكية عام1861، إذ استخدمت البرقية لأول مرة لإدارة الحرب، وأصبحت برقية التلغراف جزءً مُهماً من منظومة الحرب[9]. كذلك تُعد الحربان العالميتان الأولى والثانية اللتان شهدهما العالم في القرن العشرين نقطة الانطلاق للتفكير في دور التنمية في إدارة الصراع وتحقيق النصر، وعد السبب الذي من خلاله سعت الدول المُتصارعة على تطوير إمكاناتها التقنية المُتمثلة في الاتصال اللاسلكي (الرادار[10].

وفي النصف الثاني من القرن العشرين، ونتيجة للتنافُس يبين القطبين العالميين الولايات المُتحدة الأمريكية والاتحاد السوفيتي آنذاك، برز سباق في تطوير الأدوات الإلكترونية، إذ كانت الحصيلة تطوير منظومات التسليح واستخدام التقنية الحديثة في أنظمة الاتصال والسيطرة والتحكم عن بُعد[11].

وشهدت فترة تسعينات القرن العشرين غموضاً في مفهوم السيبرانية وعد غير واضح المعالم، لأنها كانت مُقتصرة على عمليات التشويش على أنظمة الرادار وأجهزة الإنذار، في الوقت نفسة وبسبب اتساع شبكة الانترنت فتح المجال للأجهزة المُخابراتية لاستغلال هذه الشبكة في حروبها الدولية، والتغلغل في أي شبكة من شبكات الانترنت وإمكانية السيطرة على هذه الشبكة وتعطيلها أو تغيير البيانات عليها أو اتلافها أو التحكُم فيها من خلال الضغط على بضع ازرار[12].

ومع نهاية القرن العشرين وبداية القرن الحادي والعشرون، ونتيجة الثورة المعلوماتية والتقنية المُتمثلة بالإنترنت ومن خلال التوظيف المُكثف لها، تزايد صدى السيبرانية، مما أدت إلى بروز الفضاء الإلكتروني أو السيبراني (cyberspace) كمفهوم جديد للصراع العالمي[13].

(8) حمزة غشوة ومعمر حمزة، دور المواقع الإلكترونية في الترويج السياحي، رسالة ماجستير غير منشورة، (الجزائر: جامعة قاصدي مرباح – ورقلة، كُلية العلوم الإنسانية والعلوم الاجتماعية،2015)، ص17.

(9) Rex Hugh, Towards a Global Regime For Cyber Warfare (London: Cyber Security project Chatham House, 2009), P. 3.

(10) Alfred price, the History of US Electronic Warfare, Is ted. (VA: Association of OLD crows, 1984), P. 6.

(11) H. Banks, R. Me Quillan, Electronic Warfare test and Evaluation, Flight Test Techniques Series, (Canada: Research and Technology Organization – North Atlantic Treaty Organization, 2000), P. 2.

(12) ريتشارد كلارك وروبرت نيك، حرب الفضاء الإلكتروني التهديد التالي للأمن القومي وكيفية التعامُل معهُ، (أبو ظبي: مركز الإمارات للدراسات وللبحوث الاستراتيجية،2012)، ص53.

(13) بيتر سينجر، الحرب عن بُعد: دور التكنولوجيا في الحرب، (أبو ظبي: مركز الإمارات للدراسات البحوث الاستراتيجية، 2010)، ص555.

نتيجة لِكُل ما ذُكِر، فقد عملت أَغلب الدول في الوقت الحاضر على تعزيز دفاعاتها ضد خطر التعرض للهجمات السيبرانية، بل اتجهت إِلى التحول مِن تبني السياسات الدفاعية الوقائية إِلى تبني سياسات هجومية، ويحمل ذلك في مضمونه مخاطر عسكرة الفضاء السيبراني، لاسيما وأَنَّ القدرة على السيطرة على مثل هذا النوع مِن الأَسلحة ضئيلة بالمُقارنة مع الأَسلحة التقليدية، كذلك مسأَلة صعوبة تحديد الأَسلحة التي يمتلكها الاخرون ومِن ثُم يتعذر على المُجتمع الدولي القدرة على التدخُل لاحتواء التقدُم في مثل هكذا أَسلحة[14].

ثالثاً: المفاهيم المُرتبطة بالسيبرانية

هُناك مفاهيم عديدة مُرتبطة ومُتداخلة مع مفهوم السيبرانية ولأهمية التعرُف عليها تم إِيجازها على النحو الاتي:

1. الفضاء السيبراني: يُعرف بانه بيئة تفاعُلية حديثة تشمل عناصر مادية وغير مادية، مكونة مِن مجموعة مِن الأَجهزة الرقمية، وأَنظمة الشبكات والبرمجيات والمُستخدمين لها، وهو البُعد الخامس للحرب ووسيلة جديدة للحروب الحديثة الذي يوصف بأَنهُ مجال افتراضي مِن صنع البشر يعتمد على نظُم الكمبيوتر وشبكات الأنترنت وكم هائل مِن المعلومات والبيانات والاجهزة[15].

2. الاستراتيجية السيبرانية: وهي طريقة وخطط إِدارة جميع العمليات السيبرانية بطريقة حكيمة في جميع مؤسسات وقطاعات الدولة تفادياً للتهديدات السيبرانية الداخلية والخارجية لتحقيق أَمن الدولة والوصول إِلى هدفها المُبتغى وتتغير هذه الاستراتيجية بتغير المُعطيات المُتحكمة بالبيئة الدولية[16]. ويُعد المُفكر الاستراتيجي الأَمريكي «جوزيف ناي» أَبرز المُهتمين بالاستراتيجية السيبرانية ويعرفُها بانها «القدرة على الحصول على النتائج المرجوة عن طريق استِخدام مصادر المعلومات المُرتبطة بالفضاء السيبراني»، أَي أَنها القدرة على استِخدام الفضاء السيبراني

الاستراتيجية السيبرانية: وهي طريقة وخطط إِدارة جميع العمليات السيبرانية بطريقة حكيمة في جميع مؤسسات وقطاعات الدولة تفادياً للتهديدات السيبرانية الداخلية والخارجية لتحقيق أَمن الدولة والوصول إِلى هدفها المُبتغى

(14) عادل عبد الصادق، «القوة الإِلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإِلكتروني"، مجلة السياسة الدَولية، العدد188، (القاهرة: مركز الأَهرام للدراسات السياسَية والاستراتيجية،2012)، ص33.

(15) عادل عبد الصادق، الفضاء الإِلكتروني والعلاقات الدولية: دِراسة في النظرية والتطبيق، (القاهرة: المكتبة الأَكاديمية،2016)، ص13. كذلك يُنظر: عباس بدران، الحرب الإِلكترونية: الاشتباك في عالم مُتغيرَ، ط1، (بيروت: مركز دراسات الوحدة العربية،2010)، صَ ص3-4.

(16) جوزيف هينروتين (وآخرون)، حرب واستراتيجية نهوج ومفاهيم، ترجمة أَيمن مُنير، (الكويت: المجلس الوطني للثقافة والفنون والآداب،2019)، ص70.

لخلق مزايا للدولة، والتأثير في الأحداث المُتعلقة بالبيانات التشغيلية الأخرى عبر ادوات سيبرانية، كما يُشير إلى أَنَّ مفهوم الاستراتيجية السيبرانية يقصد به «مجموعة الموارد المُتعلقة بالتحكُم والسيطرة على أجهزة الحاسوب والمعلومات والشبكات الإلكترونية والبُنية التحتية المعلوماتية والمهارات البشرية المُدربة للتعامُل مع هذه الوسائل[17].

3. الأمن السيبراني: وهو أَمن وحماية الشبكات والأنظمة المعلوماتية والبيانات والأجهزة المُتصلة بالإنترنت، فالمجال الذي يتعلق بإجراءات ومعايير الحماية المفروض اتخاذها أَو الالتزام بها لمواجهة التهديدات أَو على الأقل الحدُ من أثارها تُسمى بالأمن السيبراني[18]. والأمن السيبراني حسب تعريف الاتحاد الدولي للاتصالات في تقريره حول (اتجاهات الإصلاح في الاتصالات للعام2010– 2011) هو: «مجموعة من المهمات، مثل إجراءات أَمنية، ومبادئ توجيهية، ومُقاربات لإدارة المخاطر، وتدريبات،وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية، وموجودات المؤسسات والمُستخدمين»[19].

4. القوة السيبرانية : تُعرف بأنها: القدرة على استخدام الفضاء السيبراني لخلق الوسائل والتأثير على الأحداث في البيئات التشغيلية الأخرى وعبر أدوات القوة، أَي هي مجموعة الوسائل، والطاقات، والإمكانات المادية وغير المادية، المنظورة وغير المنظورة التي تمتلكها الدولة وتُمثل الموارد المُتعلقة بالتحكُم والسيطرة على أَجهزة الحاسبات والمعلومات، والشبكات الإلكترونية والبُنية التحتية المعلوماتية، والمهارات البشرية المُدربة للتعامُل مع هذه الوسائل وإمكانية استخدامها من جانب صانع القرار في إحداث فعل مؤثر يُحقق مصالح الدولة وتوثر في سلوك الوحدات السياسية الاخرى[20]. وعرف المُفكر الاستراتيجي الأمريكي «جوزيف ناي» (joseph s. Nye) القوة السيبرانية على أنها: «القدرة في الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المُرتبطة الكترونية بالفضاء السيبراني المعلوماتي والسيطرة على الأنشطة الإلكترونية

(17) نقلاً عن: عبد الكريم زهير عطية الشمري، الاستراتيجية الأمريكية للهيمنة على الفضاء السيبراني العالمي، رسالة ماجستير غير منشورة، (الموصل: جامعة الموصل، كُلية العلوم السياسية,2021)، ص ص29-30.

(18) مُنى الأشقر جبور، السيبرانية هاجس العصر، (بيروت: المركز العربي للبحوث القانونية والقضائية،2017)، ص35.

(19) الاتحاد الدولي للاتصالات، اتجاهات الإصلاح في الاتصالات، (جُنيف: الاتحاد الدولي للاتصالات،2008)، ص18.

(20) ITU, Cyber Security, (Geneva: ITU ,2008), P.39.

والحواسيب والبُنية التحتية المعلوماتية ذات الصلة بالفضاء الإلكتروني، أي انها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة، والتأثير على الأحداث المُتعلقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات سيبرانية»[21] .

5. الردع السيبراني : يُعرف على أنه مجموعة من الإجراءات التي تعمل على خلق عدد من المُحفزات التي تمنع قيام أحد أطراف الصراع باعتداء أو هجوم مُستقبلاً، مع العلم أنهُ لا يستطيع أحد الأطراف تدمير الطرف الآخر كُلياً ويتطلب الردع السيبراني مصداقية الدفاع عن أنظمة المعلومات وردع أي محاولات لاختراقها، القدرة على الانتقام، وكذلك وجود الرغبة في الانتقام بتكبيد المُهاجم ضرراً يفوق ما وقع على المُدافع من اضرار[22].

6. الهجمات السيبرانية: وهي إجراءات عديدة تتخذها الدولة، لغرض الهجوم على نظُم المعلومات المُعادية بهدف الإضرار بها والتأثير عليها وتحقيق عدد من الأهداف، وفي الوقت ذاته لغرض الدفاع عن النظُم والمعلومات الخاصة بالدول المُهاجمة[23] .

7. الصراع السيبراني: يُعد الصراع السيبراني أحد أوجه الصراع الدولي، إذ يستطيع أحد أطراف الصراع أن يوقع خسائر فادحة بالطرف الأخر، وأن يتسبب في فشل البُنية المعلوماتية والاتصال الخاص به وهو ما يُسبب خسائر عسكرية واقتصادية فادحة من خلال قطع أنظمة الاتصال بين الوحدات العسكرية بعضها ببعض أو تضليل معلوماتها أو سرقة معلومات سرية عنها[24].

8. الحروب السيبرانية : عرفها الباحثان الأمريكيان(ريتشارك كلارك) و(روبرت كناكي) بأنها: «أعمال تقوم بها الدول والفواعل من غير الدول تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة اخرى بهدف تحقيق أضرار بالغة أو تعطيلها»[25]. وكما يرى الباحث الاستراتيجي (بولو شاكريان) بأنها: «امتداد للسياسة من خلال الإجراءات المُتخذة في الفضاء السيبراني من قبل الدول أو الفاعلين غير الدوليين، إذ تُشكل تهديداً خطيراً للأمن القومي»[26].

(21) أيهاب خليفة، القوة الإلكترونية كيف يمكن أنَّ تُدير الدولة شؤنها في عصر (الانترنت)؟، (القاهرة: مطبعة العربي للنشر والتوزيع،2017)، ص24.

(22) Joseph S. Nye JR, Cyber power, (London: Harvard Kennedy School, 2010), P.10.

(23) نورة شلوش، «القرصنة الإلكترونية في القضاء السيبراني: التهديد المُتصاعد لأمن الدول»، مجلة بابل للدراسات الإنسانية، المُجلد8، العدد2، (بابل: مركز بابل للدراسات الحضارية والتاريخية،2018)، ص18.

(24) إيهاب خليفة، القوة الإلكترونية وأبعاد التحول في خصائص القوة، (الإسكندرية: مطبعة الاسكندرية،2014)، ص23.

(25) علي حسين باكير، المجال الخامس، الحروب الإلكترونية في قرن21، مركز الجزيرة للدراسات، نقلاً عن شبكة المعلومات الدولية (الانترنت)، مُتاح على الرابط الآتي: https://www.studies.aljazeera.com

(26) عادل عبد الصادق، الحروب السبرانية: تصاعد القدرات والتحديات للأمن العالمي، المركز العربي لأبحاث الفضاء الإلكتروني، نقلاً عن شبكة المعلومات الدولية (الانترنت)، مُتاح على الرابط الآتي: https://www.accronline.com.

وتُعد الحرب السيبرانية المستوى الأخطر للنزاع في الفضاء السيبراني، وتسعى تلك الحرب في التأثير على الإرادة السياسية للطرف المستهدف وعلى إمكانياتهُ في عملية صنع القرار، أيضاً القدرة على التأثير فيما يتعلق بالقيادة العسكرية أو توجهات المدنيين في مسرح العمليات الإلكترونية [27].

(27) هاري أر. يارغر، الاستراتيجية ومحترفو الأمن القومي، ترجمة راجح محرز علي، (أبو ظبي: مركز الإمارات للدراسات والبحوث الأستراتيجية،2011)، ص11.

9. الإرهاب السيبراني: وهو استخدام التنظيمات الإرهابية لشبكات التواصل الاجتماعي (الانترنت) للتواصل والدعاية والتضليل، بهدف تحقيق مكاسب سياسية من خلال الهجوم أو التهديد بالهجوم على اجهزة الكمبيوتر أو الشبكات وانظمة المعلومات لتدمير البنية التحتية وترهيب الحكومة أو المواطنين واجبارهم على تحقيق اهداف سياسية واقتصادية واجتماعية بعيدة المدى [28]. وتُعد هذه التنظيمات الإرهابية الأحدث والأكثر خطورة على الأمن الدولي، وذلك لان دافعهم ليس المال فقط إذ لديهم قضية يدافعون عنها، وغالباً ما يقومون بإرسال رسائل تهديد أو تدمير البيانات المخزونة في نظُم المعلومات الحكومية، من خلال تسجيل وجهة نظرهم إذ انَّ مكان تواجدهم ليس محدود فنشاطهم مُنتشر في كُل مكان من العالم وهذا ما يصعب اقتناصهم والقبض عليهم بسهولة.

الإرهاب السيبراني: وهو استخدام التنظيمات الإرهابية لشبكات التواصل الاجتماعي (الانترنت) للتواصل والدعاية والتضليل، بهدف تحقيق مكاسب سياسية من خلال الهجوم أو التهديد بالهجوم على اجهزة الكمبيوتر أو الشبكات وانظمة المعلومات لتدمير البنية التحتية

(28) Rrszard Zieba, Wspo czesne wyzwania I zagrocenia dla bezpieczenstwa miedzynarodowego, (USA, Stosunki Miedzynarodowe international Relation, 2003), P. 52.

المحور الثاني

خصائص الفضاء السيبراني (الإلكتروني) وعناصرهُ

يتمتع الفضاء السيبراني داخل شبكة الانترنت بعدة خصائص وميزات تحسن عمليات التواصل وتبادُل المعلومات، فضلاً عن امتلاكهُ لعناصر عديدة، ويمكن التعرف على هذه الخصائص والعناصر في ضوء التقسيم الآتي:

أولاً: خصائص الفضاء السيبراني

على الرغم من وجود بعض أوجه الشبه بين الفضاء التقليدي

والفضاء السيبراني، لكن هُناك عدد من الخصائص والعناصر للفضاء السيبراني تميزهُ عن الفضاء العام التقليدي، إذ أصبح يشكل الفضاء السيبراني ساحة جديدة للحرب بشكلهُ التقليدي ولكنهُ ذا طابع سيبراني، والحروب السيبرانية تقع داخل شبكات الاتصال والمعلومات عابرة للحدود التقليدية وسيادة الدول، على الرغم من أنَّ الحرب الفعلية تستعمل جميع أنواع الأسلحة المُتاحة، فأنها لم تتوان عن استخدام الفضاء السيبراني. يمكن تلخيص سمات وخصائص عدة للفضاء السيبراني والحروب السيبرانية على النحو الآتي:

1. الحُرية وغياب السيطرة الحكومية: يتيح الفضاء السيبراني للأَفراد والجماعات قدرة أكبر على التواصل والتشابُك وبناء مُجتمعات افتراضية بمظاهر مُختلفة للتأثير في القضايا عبر وسائل التواصل الاجتماعي والمُنتديات الإلكترونية وغيرها، وميزة كهذه لا تتوافر في المجال العام التقليدي، لاسيما مع القيود الصارمة التي تفرضها الأنظمة السلطوية على عملية التنظيم التي قد يقدم عليها الأفراد والجماعات[29].

يتيح الفضاء السيبراني للأَفراد والجماعات قدرة أَكبر على التواصل والتشابُك وبِناء مُجتمعات افتراضية بمظاهر مُختلفة للتأَثير في القضايا عبر وسائل التواصل الاجتماعي والمُنتديات الإلكترونية وغيرها،

2. الطبيعة الطوعية وليس الجبرية: هذه الخاصية مُمتدة من المجال العام التقليدي إلى السيبراني، لكنها اتسعت في المجال السيبراني، بل أيضاً تُفسر الإقبال الشديد عليه خصوصاً بأنه خالٍ من الإجبار الذي يُعانيه المواطن في العديد من مجالات حياته اليومية، خاصةً في علاقته بالدولة والقوانين، هذا ما يُساعد على خلق ساحة صِراع جديدة بين الدول يتشارك فيها المدنيين والعسكريين وترتبط بالتطورات المادية والعسكرية على الارض بأقل تكلُفة وأكثر تحديداً للهدف.
3. صعوبة الردع السيبراني: باعتبار الفضاء السيبراني ساحة افتراضية يصعب على الدول وضع الحدود لسيادتها وسيطرتها كما لو أنَّ الدول في الوقت الحاضر وفي ظل الفضاء السيبراني فاقدةً لركن

(29) ابتسام علي حسين، «فرص وقيود الأطـراف المُتنازعة على المجال العام السيبراني»، مجلة السياسة الدولية، العـدد208، (القاهرة: مركز الأهرام للدراسات السياسية والاستراتيجية،2017)، ص ص11–12.

مِن أَركان قيامها[30].

4. غياب الشفافية: مِن الصعوبة تحديد هوية المجموعة التي تُنفذ الهجمات السيبرانية في الكثير مِن الحالات، أَيضاً غياب التشريعات الدولية التي تضع الدول أَو المؤسسات أَو الجماعات التي تقوم بمثل هذه الأَنشطة تحت طائلة القانون الدولي، ذلك يعني عدم القدرة على مُلاحقتهم قانونياً على خِلاف مجالات الحرب التقليدية[31].

كما تتميز الحرب السيبرانية بمجموعة مِن الخصائص التي تُميزها عن الحروب التقليدية، ويمكن إجمالها بما يأتي[32]:

- انخفاض التكلُفة نسبياً للأَدوات اللازمة لنشأَة الحرب السيبرانية، فالدول لا تحتاج في سياق ذلك إِلى تخصيص ميزانيات ضخمة لإِنتاج الأَسلحة المُستخدمة في النِزاعات العنيفة التقليدية التي تكون تكلفتها عالية جداً كحامِلات الطائرات والمُقاتِلات المتطورة.

تتميز الحروب السيبرانية بالسرعة والمرونة والمراوغة، ومِن خِلالها يتمتع المُهاجم بأَفضلية على المُدافع، ومِن ثُم مِن الصعب جداً نجاح إِجراءات التحصين لوحدها

- تتميز الحروب السيبرانية بالسرعة والمرونة والمراوغة، ومِن خِلالها يتمتع المُهاجم بأَفضلية على المُدافع، ومِن ثُم مِن الصعب جداً نجاح إِجراءات التحصين لوحدها، فالتحصين في هذا المعنى سيجعل مِن هذا الطرف عرضة لمزيد مِن محاولات الاختراق، وبالتالي المزيد مِن الضغط.
- تتميز الحرب السيبرانية بانها غير مُحددة الأَهداف والتأَثيرات، فقد تتعدى مخاطرها ميادين القتال التقليدية لتنال بدمارها حتى أَكثر المواقع السيادية والحساسة تحصيناً وبعيداً عن دائرة القتال.
- تُعد حرب هلامية الشكل والملامح، فهي مُتعددة بميادينها، متنوعة ومتطورة بوسائلها المُرتبطة بأَكثر المجالات التقنية تطوراً وتبدُلاً في الحياة المُعاصِرة للدول.
- كذلك تتميز أَطرف الحرب السيبرانية بعدم الوضوح وتكون

(30) سماح عبد الصبور، «الصراع السيبراني: طبيعة المفهوم وملامح الفاعلين»، اتجاهات نظرية في تحليل السياسة الدولية، مجلة السياسة الدولية، العدد208، (القاهرة : مركز الأهرام للدراسات السياسية والاستراتيجية،2017)، ص6.

(31) شمويل ايفين ودافيد سيمان توف، حرب الفضاء الإلكتروني، المفاهيم والاتجاهات، (برلين:2011)، ص20.

(32) أَشرف السعيد أحمد، القرصنة الإلكترونية، (القاهرة: دار النهضة العربية،2013)، ص ص45-47.

تداعياتها خطيرة سواءً عن طريق تدمير المواقع على الانترنت ونسفها وقصفها بوابل من الفيروسات أَو العمل على استخدام أَسلحة الفضاء الإلكتروني المُتعددة، للنيل من سلامة تلك المواقع، وهي أَسلحة يسهل الحصول عليها من خلال مواقع الانترنت وكذلك تعلم كيفية استخدامها.

• تتميز الحرب السيبرانية بأن تدميرها لا تُصاحبهُ دماءً واشلاءً، إذ تقتصر في أَغلب حالاتها على التجسُس والتسلُل ثُم النسف، وسهولة الدخول إلى الفضاء الإلكتروني ساعد على توسيع دائرة استهداف المواقع الإلكترونية فضلاً عن زيادة عدد المُهاجمين، ولتدور تلك الهجمات المُتبادلة على نحو الكر والفر ليُعبر عن حالة صراع مُمتد يرتبط بطبيعة الفضاء الإلكتروني المُختلفة[33].

(33) نـورة شلوش، «القرصنة الإلكترونية في الفضاء السيبراني التَهديد المتصاعد لأَمن الدول»، مصدر سبق ذكرهُ، ص195.

ثانياً: عناصر الفضاء السيبراني

يتكون الفضاء السيبراني من عدد من العناصر أَهمها:[34]

(34) جميل حسين طويلة، البرمجيات الخبيثة، (دمشق: د.ن،2016)، ص4.

1. بنية الكترونية: وتتكون هذه البُنية من مراكز البيانات وأَجهزة الحاسوب وشبكات الحاسوب وأَجهزة إدارة قواعد البيانات، كذلك أَنظمة اللوائح التنظيمية وهي الأَجهزة المادية التي تُستخدم لربط أَجهزة الحاسوب والمُستخدمين وتشمل وسائط النقل بما في ذلك خطوط الهاتف وخطوط البث التلفزيوني عبر الكابلات والأَقمار الصناعية، الهوائيات وأَيضاً أجهزة التوجيه.

2. أسلحة الكترونية: هُنالك أَنواع عدة من الأَسلحة الإلكترونية منها ما يأَتي[35]:

(35) إيهاب خليفة، مُجتمع ما بعد المَعلومات: تأَثير الثورة الصناعية الرابعة على الأَمـن القَومي، (القاَهرة: دار العربي للنشر،2019)، ص ص117-119.

أ. الفيروسات: وهي برامج صُممت لغرض إلحاق الضرر في قواعد البيانات، وسرقتها وتخزينها أَو قطع الاتصال بالشبكة، ومن الصعب التعرف أَو اكتشاف هذه الأَسلحة، علماً انها برامج صُنعت عمداً لتغيير خصائص الملفات، وتُستخدم هذه الفيروسات لتعطيل شبكات الخدمات والبُنية التحتية للطرف المُستهدف كإحداث خلل وفشل في شبكة الاتصال لدولة ما .

ب. الديدان: برامج صغيرة جداً تتكون من الشبكات ولا تعتمد على

غيرها وغايتها القيام بقطع الاتصال عن الشبكات أَو القيام بسرقة البيانات وذلك مِن خِلال تصفح المُستخدمين للأنترنت[36].

ج. دودة ميليسا Melissa Worm: وهي فايروس أُنتشر بواسطة البريد الإلكتروني، مِن خِلال رسالة بريد إلكتروني مُزيفة تقوم بإرسال نفسها إِلى (50) بريد إلكتروني اخر عند فتحها، إِذ انتشر هذا النوع من الفايروسات عام 1999 وانتجت خسائر تقدر بملايين الدولارات[37].

د. دودة ستكسنتStuxnet Worm : أنتشر هذا النوع مِن الفايروسات عام 2010 مِن خِلال أجهزة USB drives)) عند وصلها بجهاز الحاسوب، وهذا النوع من الفيروسات لا يتطلب وجود اتصال بشبكة الانترنت لكي تتمكن من الانتشار، ومن الأمثلة التي تعرضت للإصابة من هذا النوع هي محطات توليد الطاقة النووية[38].

هـ. أحصنة طروادة **Trojan Horse:** نوع مِن البرمجيات الخبيثة التي لا تتناسخ مِن تلقاء نفسها إِذ يظهر لكي يؤدي وظيفة مرغوب فيها، فهو يعمل على نسخ حمولتهُ الخبيثة وفي أَغلب الأَحيان يعتمد على الأبواب الخلفية أَو الثغرات الأَمنية التي تساعده بالوصول غير المُصرح بِه إِلى الكمبيوتر أَو الجهاز المُستهدف، وهو على شكل شفرة صغيرة يتم تحميلها مع برنامج رئيس مِن البرامج ذات الشعبية العالية، ويقوم ببعض المهام الخفية وفي الغالب يرتكز على إِضعاف قوى الدِفاع لدى الضحية أَو اختراق جهازه وسرقة بياناته[39].

أحصنة طروادة Trojan Horse: نوع مِن البرمجيات الخبيثة التي لا تتناسخ مِن تلقاء نفسها إِذ يظهر لكي يؤدي وظيفة مرغوب فيها، فهو يعمل على نسخ حمولتهُ الخبيثة وفي أَغلب الأَحيان يعتمد على الأبواب الخلفية أَو الثغرات الأَمنية

و. الماكينات والميكروبات فائقة الصغر: وهي عِبارة عن (robots) فائقة الصغر تصيب أَساس النِظام، وهي عكس الفيروسات، تنتشر في مبنى نِظام معلوماتي، لدولة مُعادية أَو مُنافسة، إِذ تتفشى في الردهات والمكاتب حتى تجد حاسباً آلياً وتدخل إليه مِن خِلال الفتحات الموجودة به، لتقوم بإِتلاف

(36) عامر أَبو علي، فيروسات الكمبيوتر، (القاهِرة: دار حنين للنشر والتوزيع،1994)، ص46.

(37) أُسامة فتحي، فيروسات الحاسب، (د.م: د.ن،2008)، ص6.

(38) المصدر نفسهُ، ص7.

(39) Ken Dwight, Bug Free computing, (USA: The Teleprocessors Inc, 2005), P.P.1213-.

الدوائر الإلكترونية[40].

ز. الأبواب الخلفية back doors):) عبارة عن ثغرة تترك عن عمد من قِبل مُصمم النِظام ليستطيع الدخول إلى النظام عند الحاجة لذلك، علماً ان جميع البرامج والنظُم التي تنتجها الولايات المُتحدة الأمريكية تحتوى على أبواب خلفية تستخدمها عِند الحاجة[41].

الأبواب الخلفية (back doors): عبارة عن ثغرة تترك عن عمد مِن قِبل مُصمم النِظام ليستطيع الدخول إلى النظام عند الحاجة لذلك، علماً ان جميع البرامج والنظُم التي تنتجها الولايات المُتحدة الأمريكية تحتوى على أبواب خلفية تستخدمها عِند الحاجة

3. عمليات الكترونية: وهي القدرة على الدخول غير المشروع والتجسُس على شبكات الخصم عن طريق الحاسوب الآلي، وبهدف الحصول على المعلومات، إذ تشمل هذه المعلومات على خطط الدفاع العسكري وأسرار الحروب العسكرية كذلك معلومات استخبارية أو سياسية، كذلك إمكانية ترك ثغرات داخل البرامج الإلكترونية لحقن الشبكة بفيروسات للقيام بمهام مُعينة وذلك من خِلال الأبواب الخلفية إذ يمكن استخدامها للتأثير في سلوكيات الخصم وذلك بنشر الخطط العسكرية والبيانات أو إرسالها ليدرك انه مُخترق ما يدفعهُ للتفاوض أو الاستسلام وتحقيق المكاسب لصالح الطرف الذي قام بالعملية الإلكترونية[42].

4. مُهاجمة شبكات الحاسب الآلي: تقوم على أساس اختراق الشبكات لتعطيلها، ونشر فيروسات تدمرها، أو نشر معلومات محرفة، لإرباك العاملين عليها، أيضاً القيام بهجمات إلكترونية أو مادية لقطع خدمات الانترنت عن الخصم، ما يسمح بتدمير قواعد البيانات الإلكترونية، أو قطع أنظمة اتصال بث الوحدات العسكرية، أو العمل على شل أنظمة الدفاع الجوي، أو السيطرة على وحدات القيادة[43].

5. الدفاع عن شبكات الحاسب الآلي: هي القدرة على حماية الشبكات وأجهزة الكمبيوتر من التعرض للاختراق وتأمينها، إذ يكون ذلك على مستوى البرمجيات (Soft ware)، والمكون المادي للشبكات (Hard ware)، أي العمل على تأمين الشبكة والمكون

(40) مايا صبحي، الخيوط الخفية للماسونية في دائرة الضوء، نقلاً عن شبكة المعلومات العالمية (الانترنت)، مُتاح على الرابط الآتي: https://www.ar-ar.facebook.com/masonic.secret

(41) عامر أبو علي، فيروسات الكمبيوتر، مصدر سبق ذِكرهُ، ص 38.

(42) William T. Johen, Of Military Strategy,(Boston: Center for Strategic Leadership,2011), P.183.

(43) صباح عبد الصبور عبد الحي، استخدام القوة الإلكترونية في التفاعُلات الدولية..، مصدر سبق ذِكرهُ، ص25.

المادي لها، مثل الخوادم أَو الشرائح التي قد تكون برمجت من قبل المصمم لكي تعمل في ظروف غير عادية لصالحه[44]. والشكل ذو الرقم(1) يوضح عناصر الفضاء السيبراني.

(44) المصدر نفسهُ، الصفحة نفسها.

الشكل(1): عناصر الفضاء السيبراني

الشكل: مِن إعداد الباحثين.

المِحور الثالث

فواعل الفضاء السبيراني وأَبعادهُ الاستراتيجية

تشتق خصائص الفضاء السيبراني من طبيعة وسعة فواعله، إِذ إِنهُ لم يقتصر على الفواعل مِن الدول بل أَخذ ليشمل فواعل مِن غير الدول وأَصبح لهُ أَبعادهُ الاستراتيجية المُهدِدة للأَمن الدولي، وللوقوف على تلك الفواعل والأبعاد الاستراتيجية تم تحليلها على نحو دقيق، وفق التقسيم الآتي:

أَولاً: فواعل الفضاء السيبراني

ويمكن تقسيم الفواعل في الفضاء السيبراني والمالكين للقوة

السيبرانية إلى ما يأتي:

1. الدول والحكومات

تُعد الدول فاعلاً محورياً في تسيير الفضاء السيبراني، انطلاقاً من إمكاناتها المادية والبنيوية والبشرية والقانونية، واحتكارها القانوني والمُنظم للفضاء السيبراني وذلك من خلال أجهزتها المُختلفة

تُعد الدول فاعلاً محورياً في تسيير الفضاء السيبراني، انطلاقاً من إمكاناتها المادية والبنيوية والبشرية والقانونية، واحتكارها القانوني والمُنظم للفضاء السيبراني وذلك من خلال أجهزتها المُختلفة، فمع نهاية القرن العشرين أدركت الدول وخاصةً الكُبرى بضرورة العمل على تغيير استراتيجياتها أو إضافة استراتيجية إلى استراتيجياتها، بما يتناسب مع هيكلية القرن الحادي والعشرين وما حدث عليه من تطورات وإعادة ترتيب في سلم الأولويات، مما نتج عنهُ سباقاً محموماً بين بعض القوى لتعظيم الاستفادة من الفضاء السيبراني إذ عدت هذه الدول والحكومات القدرات السيبرانية وسيلة لبسط النفوذ وتحقيق مكاسب استراتيجية وسياسية واقتصادية ومالية لم تستطع تحقيقها عبر الوسائل العسكرية والدبلوماسية التقليدية[45].

فالدول لديها القدرة الكبيرة على تنفيذ الهجمات السيبرانية وتطوير البُنية التحتية ومُمارسة السلطات داخل حدودها، فبحسب التقسيم الذي قدمهُ «جوزيف ناي» لأنماط القوة، القوة الصلبة والقوة الناعمة والقوة الذكية، إذ عرف القدرات السيبرانية على انها جزء من القوة الناعمة، وبذلك تُعد القوة السيبرانية مظهر من مظاهر القوة في التفاعُلات الإقليمية والدولية، إذ تنطوي قوة دولة مُعينة سيبرانياً على ما تمتلكه من قدرات وإمكانيات في الفضاء السيبراني (الإلكتروني)[46]. إذ سعت أغلب الدول إلى تطوير قدراتها السيبرانية، مما نتج عنه اتساع قائمة الدول ذات القدرات السيبرانية المتطورة في الوقت الراهن فلم تعد تقتصر على قائمة الدول العظمى والكُبرى مثل الولايات المُتحدة والصين وبريطانيا وروسيا،بل ظهرت قوة سيبرانية جديدة يعتد بها مثل إسرائيل واستراليا والهند وإندونيسيا وكوريا الجنوبية والمكسيك والأرجنتين وإيران وتُركيا وغيرها[47].

(45) أحمد زكي عثمان، «تأثيرات القدرات السيبرانية في الصراعات الإقليمية»، مجلة السياسة الدولية، العدد208، (القاهرة: مركز الأهرام للدراسات السياسية الاستراتيجية،2017)، ص17.

(46) Joseph S. Nye, "Power and National Security in Cyberspace, Americas Cyber Future, Center For new America Security, Vo1.2, (2011),P.P.15-17.

(47) أحمد زكي عثمان، «تأثيرات القدرات السيبرانية في الصراعات الإقليمية»، مصدر سبق ذكره، ص16.

2. الشركات المُتعددة الجنسيات

تُعد الشركات المُتعددة الجنسيات من الفاعلين الرئيسيين داخل الفضاء السيبراني، وذلك لأنها تمتلك موارد للقوة تفوق بعض الدول ولا ينقصها غير الشرعية في مُمارسة القوة، التي هي حِكر على الدول، فخوادم شركات مثل جوجلGoogle، فيسبوكFacebook، ميكروسوفت Microsoft، أبلApple، أمازونAmazon، لديها موارد مالية ضخمة وأفرع في العديد من دول العالم مما يتيح لها السيطرة على التعليمات البرمجية الخاصة التي توفر لها مصادر وموارد مالية أكبر من مصادر العديد من الحكومات[48]. فقد تؤدي هذه الشركات بسهولة دوراً في صراعات الفضاء السيراني، وذلك بسبب انخفاض تكلُفة الاستثمار وصعوبة الكشف عن الهوية، كما تؤثر هذه الشركات في اقتصاديات الدول وثقافة المُجتمعات وتوجهاتها وهذا ما حدث في الأزمة بين شركة جوجل والصين حول (المحتوى)، أيضاً فضيحة تسريب بيانات مُستخدمي فيسبوك لصالح شركة كامبردج أنالايتيكا التي تم الاستعانة بها لصالح حملة الرئيس الأمريكي السابق (دونالد ترامب)[49].

3. الجماعات المُسلحة أو الإرهابية

تُعد من أحدث الفواعل الدولية خاصةً بعد أحداث الحادي عشر من أيلول/سبتمبر2001، إذ عملت على استغلال الفضاء السيبراني في عمليات التجنيد والتعبئة والرعاية وجمع الأموال والمتطوعين ونشر الأفكار والمُعتقدات، كذلك يسعى هذا الفاعل إلى توظيف الأدوات الإلكترونية في الفضاء السيبراني لتنسيق العمليات المسلحة على أرض الواقع[50]. ومثالاً على ذلك تنظيم القاعدة الذي كان لهُ السبق في الاعتماد على المواقع الإلكترونية لتحقيق أهداف استراتيجية وتسهيل القيام بالعمليات التكتيكية، من خلال استقطاب وتوجيه جنود جدد عبر المواقع الإلكترونية التابعة له كموقع النداء الإلكتروني وأيضاً مجلتهم الإلكترونية المُسماة (الينا).... وغيرها، فضلاً عن تنظيم دولة الإسلام في العراق والشام (داعش الإرهابي)

(48) Steve Lohr, Global Strategy Stabilized IBM Duing Downturn, The New York Time, available at: https://www.nytimes.com.

(49) إبراهيم أبو جازية، تمت السرقة بنجاح.. القصة الكاملة لفضيحة «كامبريدج أنالتيكا» التي هزت عرش «فيسبوك»، معلومة المنشورة عبر الشبكة المعلومات الدولية (الانترنت) مُتاح على الرابط الآتي: https://www.sasapost.com

(50) سماح عبدالصبور، «الإرهاب الرقمي استخدامات الجماعات المُسلحة لوسائل التواصل الاجتماعي»، دورية اتجاهات الأحداث»، العدد2، (القاهرة: مركز الأهرام للدراسات السياسية والاستراتيجية،2014)، ص8.

الذي يعد نوعاً اخر من الفاعلين المُسلحين من غير الدول فلهُ أكثر من (53) ألف موقع إلكتروني، و(90) ألف صفحة باللغة العربية، و(13) ألف باللُغات الأخرى، هذا ما ساهم في تجنيد حوالي (3400) شاب شهرياً عبر مواقعهم الإلكترونية، وذلك بحسب تقرير الخبير الأمني في قضايا الإرهاب الرقمي جيف باردين (Jeff bard in))[51].

4. الانونيموس وويكيليكس

الأنونيموس أو المجهولون هُم جماعات احتجاجية مُنتشرة حول العالم في الفضاء الإلكتروني، ولهُم أهداف سياسية ويقومون بتوزيع المعلومات السرية وتشوية المواقع وتوليد احتجاجات حول القضايا السياسية، فهُم نمط جديد من الفاعلين السياسيين الذين يعتمدون على إخفاء الهوية والقيادة بلا جسد وانخراط الأفراد بلا عضوية دائمة، وعلى هجمات افتراضية ضد أهداف مادية من أجل تشجيع التغيير السياسي، أما (ويكيليكس) موقع تم أنشائه عام2007 ويستهدف فضح الأنظمة السياسية من خلال تسريب الوثائق والأسرار حول الحكومات والشخصيات العامة، ومثل كُل من الانونيموس وويكيلكس نماذج لما قد يُسببه الفاعلون من غير الدول من تأثيرات صراعية محلية وإقليمية ودولية عبر الفضاء الإلكتروني وتهديد للأمن الدولي[52] . وخير مثال على ذلك، ما فعلهُ موقع ويكيليكس بنشر فيديو لمروحية أمريكية في إحدى القرى العراقية وهي تقصف المدنيين العراقيين وبينهم صحفي خلال فترة احتلال العراق عام2003، كذلك نشر العديد من المنشورات التي أظهرت السلوك السياسي الخارجي لبعض دول العالم التي تدعي الديمقراطية والحُرية، ما يمكن ان يسبب لهذه الدول أزمات عدة تعلقت بأمنها الاجتماعي والسياسي، ونظرتها للحُريات وحقوق الإنسان تجاه العالم الأخر[53].

5. الفرد

يُعد الفرد فاعلاً مُهماً وأساسياً في الفضاء السيبراني، على الرغم من قلة درجة تأثيرهُ بالنسبة للصراع داخل الفضاء السيبراني، إذ يمتلك

(51) بن مرزوق عنتر وحرشأوي محي الدين، الأمن السيبراني كبُعد جديد في السياسة الدفاعية الجزائرية، نقلاً عن شبكة المعلومات الدولية (الانترنت)، مُتاح على الرابط الآتي: https:// www.manifest.Univouargla

(52) Wendy H. Wong & Peter A Brown, E- Bandits In Global Activism: Wikileaks Anonymous and the Politics of No One, (Cambridge: Cambridge University, 2013), P. 111.

(53) السيد الحراني،ويكيليكس: حرب الوثائق وكشف الأنظمة العربية والعالمية،(مصر:دار الكتُب للنشر،2013)،ص132.

الأفراد القدرة على إحداث الثورة الرقمية، فتصبح تلك الثورة مجال استخدام للدولة نفسها، كمثال على ذلك ما قام به مارك زوكربيرغ (Markzoukerperg) عام2004 إذ أسس شبكة (فيسبوك) لتجمع أكثر من مليار مُستخدم حول العالم[54] فمواقع التواصل الاجتماعي كان لها دور كبير وبارز في تنظيم عدة مُظاهرات في مُختلف دول العالم، كذلك هُناك أفراد مُختصون في أعمال القرصنة والجرائم السيبرانية وأيضاً سرقة المعلومات والبيانات الشخصية والتلاعُب فيها أو الإساءة في استغلاله، ويطلق عليهُم تسمية (الهاكرز)[55].

ثانياً: الأبعاد الاستراتيجية للأمن السيبراني

يتسع مفهوم الأمن السيبراني على جميع المسائل السياسية والعسكرية والاقتصادية والاجتماعية والانسانية، بهدف تحقيق منظومة أمن مُتكاملة تعمل على الحفاظ على الأمن القومي للدولة من جميع التهديدات السيبرانية، عليه لا بُد من القيام بتوضيح أبعاد الأمن السيبراني بإيجاز على النحو الآتي[56]:

1. الأبعاد السياسية : بشكلٍ أساسي هي حق الدولة في حماية نظامها السياسي وكيانها ومصالحها الاقتصادية، إذ تعني حقها وواجبها في السعي لتحقيق رفاه شعبها، في الوقت الذي تؤثر فيه التقنيات بتغيير موازين القوى داخل المُجتمع نفسه، إذ اصبح المواطن بإمكانه الاطلاع على جميع القرارات السياسية وخلفياتها ومُبرراتها التي تتخذها الحكومة، عبر الكم الهائل من المعلومات التي يمكنه الوصول اليها أو من خلال ما ينشر على الانترنت وبقية الأجهزة التي توصل بها، كذلك فانَّ العاملين في الشأن السياسي لا يتوانون عن استعمال هذه التقنيات للوصول إلى أكبر شريحة مُمكنة من المواطنين والترويج لسياساتهم في العالم[57].

يرتبط الأمن السيبراني ارتباطاً وثيقاً بالاقتصاد، فالتلازُم واضِح بين اقتصاد المعرفة وتوسع استِخدام تقنيات المعلومات والاتصالات

2. الأبعاد الاقتصادية : يرتبط الأمن السيبراني ارتباطاً وثيقاً بالاقتصاد، فالتلازُم واضِح بين اقتصاد المعرفة وتوسع استخدام تقنيات المعلومات والاتصالات، كذلك بالقيمة التي تُمثلها البيانات

(54) قادر إسماعيل، إدارة الحروب النفسية في الفضاء الإلكتروني: استراتيجية الأمريكية الجديدة في الشرق الأوسط، تقرير منشور عبر شبكة المعلومات الدولية (الانترنت)، مُتاح على الرابط الآتي: https://www.manifest.univ-ouargla

(55) رفد عيادة الهاشمي، الإرهاب الإلكتروني، بحث منشور عبر شبكة المعلومات الدولية (الانترنت)، مُتاح على الرابط الآتي: https://www.mizandz.com.

(56) للاستزادة حول تلك الأبعاد يُنظر: عبد الكريم زُهير عطية الشمري، الاستراتيجية الأمريكية للهيمنة على الفضاء السيبراني العالمي، مصدر سبق ذكرهُ، ص ص54-57.

(57) مُنى الأشقر جبور، الأمن السيبراني: التحديات ومُستلزمات المواجهة، (القاهرة:جامعة الدول العربية،2012)، ص16.

والمعلومات المتداولة والمخزونة والمُستخدمة وعلى جميع المستويات، إذ تتوفر تقنيات المعلومات والاتصالات من تعزيز التنمية الاقتصادية لبلدان كثيرة، من خلال تحقيق الفائدة من فرص الاستخدام التي تقدمها الشركات الدولية والشركات الكُبرى، التي تبحث عن إدارة كُلفة إنتاجها بأفضل الشروط، غير أَنَّ هذا الواقع المُشرق يطرح وسائل عديدة سواءً ما يتعلق بحماية مُقدم الخدمة، العمل، وأَيضاً حماية المُستهلك على الانترنت[58].

3. الأبعاد الاجتماعية: إنَّ التطورات التقنية وطبيعة شبكات الانترنت المفتوحة وما تُقدمهُ من إمكانات وقدرات في المجالات العلمية والثقافية والخدماتية، عبر المدونات والشبكات الاجتماعية، إذ اتاحت الفرصة لكُل مواطن أَن يُعبر عن تطلعاته السياسية وطموحاتهُ الاجتماعية بأَشكالها كافة، ومن خلال ذلك يأتي التشديد من قبل المُنظمات والهيئات الدولية على نشر ثقافة الأَمن في الفضاء السيبراني، أَيضاً ضرورة تعاون المُجتمع بكُل مكوناته على تحقيق الأَمن السيبراني وضمانه، باعتبار المخاطر السيبرانية تطال المُجتمع بأجمعه سواءً بسبب ارتكاز الخدمات الحيوية مثل الطاقة والنقل والصحة والاتصالات وغيرها، أَو من خلال ما تُقدمهُ من تقنيات الاتصالات والمعلومات أَو من خلال ما يضخ من محتوى في الفضاء السيبراني، فان المحتوى غير المشروع وغير المرغوب فيه، ذات تأثير سلبي أَكيد على اخلاقيات مُجتمع مُعين، وأَيضاً يعمل على زيادة نسبة المُمارسات الإجرامية[59].

4. الأبعاد العسكرية : ويتمثل في قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية، وذلك ما يُساعد على تبادُل المعلومات والأَوامر وتدفقها «وهي جوهر الفكرة التي خلقت وطورت من أَجلها الشبكات ومن بعدها شبكة الانترنت»، وإصابة الأَهداف عن بُعد، على الرغم من كُل ما سبق، لا

(58) The Electronic Money Regulations 2011, available at: https://www.legislation.gov.uk.

(59) مُنى الأَشقر جبور، الأَمن السيبراني: التحديات ومُستلزمات المواجهة، مصدر سبق ذِكـرهُ، ص15.

يمكن تجاوز نقطة ضعف هذا البُعد خاصةً إذا لم تكُن مؤمنة بشكلٍ جيد مِن الاختراقات، التي ينتج عنها تدمير قواعد البيانات العسكرية وقطع الاتصال بين القيادة والوحدات العسكرية، كذلك إمكانية التحكُم في بعض الأسلحة وخروجها عن السيطرة مثل طائرات بدون طيار وصواريخ موجهة وأقمار صناعية.... وغيرها، إذ يُعد فيروس ستاكنت Stuxnet بداية لاستعمال القوة السيبرانية لتدمير البُنية المادية (هاجم حواسيب أجهزة الطرد المركزي الإيرانية)[60].

5. الأبعاد القانونية : إن التطورات التقنية والتكنولوجية المُتسارعة تفرض مواكبة التشريعات القانونية لها، من خلال سن أُطر وتشريعات للأعمال القانونية وغير القانونية في الفضاء السيبراني، فضلاً عن الحقوق الأساسية والحُريات الإنسانية المُعترف فيها في الدساتير والتشريعات الدولية، فأن ظهور الفضاء السيبراني أدى إلى ظهور حقوق أخرى كحق النفاذ إلى الشبكة العالمية للمعلومات، كذلك توسعت بعض المفاهيم لتشمل أساليب المُمارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، مثل الحق في إنشاء المدونات الإلكترونية والحق بإنشاء التجمُعات على الانترنت، أيضاً الحق في حماية ملكية البرامج المعلوماتية ومما لا شك فيه، ان السنوات القادمة لابُد وأن تشهد تصاعُداً في أعداد الأعمال الجرمية والمُمارسات غير القانونية في الفضاء السيبراني، هذا يعني عملياً أزدياد عدد القضايا التي سترفع أمام المحاكم وذلك يستدعي إعداد البيئة التنظيمية والتشريعية وبناء قدرات وهيئات المُكافحة والحكُم[61].

وفي ظل التقدُم التكنولوجي الذي أصبح يشغل حيزاً كبيراً في رسم معالم التحولات نحو دلالات ورؤى ترتبط بالطابع الإلكتروني يعُد هو الأخطر في مواكبة ديمومة هذا التقدُم الذي أتضحت معالمهُ في ظهور ما يُعرف بالقوة السيبرانية التي عدت نتيجة تحولات القوة

(60) عادل عبد الصادق، «القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني»، مصدر سبق ذكرهُ، ص32.

(61) مُنى الاشقر جبور، السيبرانية هاجس العصر، مصدر سبق ذكرهُ، ص56.

في بيئة النظام الدولي، التي أخذت طابعاً تنافُسياً حول الاستحواذ على سبق التقدُم التكنولوجي وسرقة الأسرار الاقتصادية والعلمية، إلى أن يمتد ذلك الصراع إلى محاولة السيطرة على الفضاء السيبراني من خلال سعي الفواعل الدولية للسيطرة على أسماء النطاقات وعناوين المواقع والتحكُم بالمعلومات والعمل على اختراق الأمن القومي للدول من دون استخدام طائرات أو مُتفجرات أو حتى انتهاك للحدود السيادية التي تتمثل بهجمات قرصنة الكمبيوتر وتدمير المواقع والتجسُس وأضرار بالبُنية التحتية بما يكون لذلك تأثير على تدمير الاقتصاد بنفس القوة التي قد يُسببُها تفجير تقليدي مُدمر وهذا ما يدعو إلى ضرورة الاهتمام بالقوة السيبرانية، بعد أن أصبح مفهوم الأمن السيبراني ضرورة حتمية في عالم اليوم، ولاسيما في ظل ارتباط التفاعُلات الدولية كافة بالجانب الرقمي والتكنولوجي، وهذا يتطلب من الدول حتمية إيجاد ميكانيكيات فعالة لمُراجعة المخاطر والتهديدات السيبرانية التي تتميز بالسرعة والغموض والدقة، ومن ثُم تحقيق الأمن السيبراني والحفاظ على مكاسب الدولة وأمنها القومي.

الخاتمة

ساهمت التحولات الاقتصادية والتكنولوجية المُتسارعة وغير المسبوقة في العقود الثلاثة الأخيرة وفي ظل العولمة، من زيادة تشظي القوة وانتشارها بعيداً عن الدول إلى الفواعل الأخرى من غير الدول، ولأسباب عدة منها، ما يتعلق بالدولة وطبيعتها، ومنها ما يتعلق بطبيعة المُتغيرات وقوتها وسرعة انتشارها، واخرى تتعلق بطبيعة الفواعل من غير الدول، فالشركات العابرة للقوميات استحوذت على القوة الصناعية والتجارية والمالية والمعلوماتية العالمية عن طريق عمليات التحول والاندماج وزيادة الأرباح بسبب التوسع في النشاط، كما أنَّ الثورة التكنولوجية خلقت ظروفاً مواتية للفواعل من غير الدول، فكما أنَّ الشركات المُتعددة الجنسيات وظفت مُخرجات هذه الثورة لغايات اقتصادية احتكارية، فإنَّ المجموعات الإرهابية وعصابات الجريمة العابرة للحدود وجدت لها خير وسيلة لتنفيذ

أَهدافها وتحقيق أَجندتها، كُل ذلك على حِساب تراجُع دور الدولة التي أَضرت بها هذه المُنافسة وقلصت مِن سيادتها لحِساب الفواعل الجدُّد في الساحة العالمية، وهو ما كان لهُ أَثاراً سلبية في الأَمن الدولي.

لذا فبجانب قوة الدولة الصلبة والناعِمة ظهرت القوة السيبرانية التي أَصبح لها تأَثيرها على المستويين المحلى والدولي، إذ أَدت إلى تعدُد مستويات القوى بين الفاعلين دون حصرها بالدولة، كما مكنت الفاعلين الأَصغر في السياسة الدولية مِن مُمارسة كُل مِن القوة الصلبة والناعِمة عبر الفضاء الإِلكتروني، وهو ما يعني تغيراً في علاقات القوى في السياسة الدولية. وفرض واقع الفضاء السيبراني إِعادة تعريف لبعض المفاهيم المُهِمة: مثل الأَمن والصِراع والقوة. فبدأَ الاهتِمام المُتصاعد بهذا الفضاء كتهديد أَمني.

فبجانب قوة الدولة الصلبة والناعِمة ظهرت القوة السيبرانية التي أَصبح لها تأَثيرها على المستويين المحلى والدولي، إذ أَدت إلى تعدُد مستويات القوى بين الفاعلين دون حصرها بالدولة

ومِن ضمن ما خرج به الباحث مِن استنتاجات:

- تتميز أَطرف الحروب السيبرانية بعدم الوضوح وتكون تداعياتها خطيرة سِواءً بتدمير المواقع على الإنترنت ونسفها وقصفها بوابل مِن الفيروسات أَو استِخدام أَسلحة الفضاء السيبراني المُتعدِدة.
- بفضل ثورة المعلومات والإنترنت بمواقعه المُختلِفة ظهر مفهوم الفضاء السيبراني (الإِلكتروني)، وأَصبح أَحد العناصر المؤثرة في النِظام الدولي نتيجة أَدواته الإِلكترونية والقادِرة على الحشد والتعبئة، بجانب التأَثير على القيم السياسية، نتيجة قلة تكلفتها، وأَصبحت مسأَلة أَمن الفضاء الإِلكتروني مسأَلةٌ مُهِمةٌ على أَجِندة الأَمن الدولي، خوفاً مِن تعرض المصالح الاستراتيجية ذات الطبيعة الإِلكترونية إِلى ساحة صِراع دولي تُهدد الأَمن الدولي.
- إِنَّ هُناك علاقة وثيقة ما بين الفضاء السيبراني (الإِلكتروني) والأَمن الدولي نتيجة التوسع في تبني الحكومات الإِلكترونية، واتِساع مُستخدمي وسائل الاتصال في العالم. فارتبطت التكنولوجيا

بالتحولات في القوة، وظهر مفهوم القوة السيبرانية/ الإلكترونية، وهذه القوة الجديدة مُرتبطة بامتلاك المعرفة التكنولوجية، والقدرة على استخدامها، ومِن ثُم أَصبحت حقيقةٌ أَساسيةٌ ومؤثرةٌ نتيجة التطور التكنولوجي السريع. وباتت المعلوماتية والإنجازات التقنية والمعرفية ذات الصلة، أَهم مُدخلات الفضاء السيبراني وأَدواتهُ، الذي أَتسم بها عالم اليوم.

- إنَّ استخدام الفضاء الإلكتروني يُعد مُتاحاً للفاعلين مِن غير الدول، والذي أَثر على سيادة الدولة وتحول الصراع إلى صراع إلكتروني، وهو يقوم على التجسُس، والتسلُل، ثُم النسف، أَي تدمير المواقع على الإنترنت، وقصفها بوابل مِن الفيروسات، للنيل مِن سلامتها. ومِن ثُم أَصبح تأَمين الفضاء الإلكتروني جزء لا يتجزأَ مِن استراتيجيات الأَمن القومي للعديد مِن الدول.

إنَّ استخدام الفضاء الإلكتروني يُعد مُتاحاً للفاعلين مِن غير الدول، والذي أَثر على سيادة الدولة وتحول الصراع إلى صراع إلكتروني، وهو يقوم على التجسُس، والتسلُل، ثُم النسف، أَي تدمير المواقع على الإنترنت

- إنَّ مفهوم الأَمن السيبراني له أَبعاده الاستراتيجية؛ السياسية والعسكرية والاقتصادية والاجتماعية والقانونية، الذي يسعى عبرها إلى تحقيق منظومة أَمن مُتكاملة تعمل على الحفاظ على الأَمن القومي للدولة مِن جميع التهديدات السيبرانية.

قائمة المصادر والمراجع

المصادر العربية

أَولاً: الوثائق الرسمية

1. الاتحاد الدولي للاتصالات، **اتجاهات الإصلاح في الاتصالات،** (جُنيف: الاتحاد الدولي للاتصالات،2008).

ثانياً: المعاجم والقواميس والموسوعات

1. مُنير البعلبكي، **المورد:** قاموس انكليزي – عربي، (بيروت: دار العلم للملايين،2004).

ثالثاً: الكتُب العربية والمُترجمة

1. أُسامة فتحي، فيروسات الحاسب، (د.م: د.ن،2008).

2. أَشرف السعيد أحمد، القرصنة الإلكترونية، (القاهِرة: دار النهضة العربية،2013).
3. أَيهاب خليفة، القوة الإلكترونية كيف يمكن أنَّ تُدير الدولة شؤنها في عصر (الانترنت)؟، (القاهِرة: مطبعة العربي للنشر والتوزيع،2017).
4. إيهاب خليفة، القوة الإلكترونية وأَبعاد التحول في خصائص القوة، (الإسكندرية: مطبعة الاسكندرية،2014).
5. إيهاب خليفة، مُجتمع ما بعد المعلومات: تأَثير الثورة الصناعية الرابعة على الأَمن القومي، (القاهرة: دار العربي للنشر،2019).
6. بيتر سينجر، **الحرب عن بُعد: دور التكنولوجيا في الحرب**، (أبو ظبي: مركز الإمارات للدراسات البحوث الاستراتيجية، 2010).
7. جميل حسين طويلة، **البرمجيات الخبيثة**، (دمشق: د.ن،2016).
8. جوزيف هينروتين (وآخرون)، حرب واستراتيجية نهوج ومفاهيم، ترجمة أَيمن مُنير، (الكويت: المجلس الوطني للثقافة والفنون والآداب،2019).
9. ريتشارد كلارك وروبرت نيك، حرب الفضاء الإلكتروني التهديد التالي للأَمن القومي وكيفية التعامُل معهُ، (أَبو ظبي: مركز الإمارات للدراسات وللبحوث الاستراتيجية،2012).
10. السيد الحراني، ويكيليكس: حرب الوثائق وكشف الأنظمة العربية والعالمية،(مصر: دار الكتُب للنشر،2013).
11. شمويل ايفين ودافيد سيمان توف، حرب الفضاء الإلكتروني، المفاهيم والاتجاهات، (برلين:2011).
12. صباح عبد الصبور عبد الحي، استخدام القوة الإلكترونية في التفاعُلات الدولية: تنظيم القاعدة أَنموذجاً، ج2، (إسطنبول: المعهد المصري للدراسات السياسية والاستراتيجية، 2016).
13. عادل عبد الصادق، الفضاء الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق، (القاهرة: المكتبة الأَكاديمية،2016).
14. عامر أَبو علي، فيروسات الكمبيوتر، (القاهِرة: دار حنين للنشر

والتوزيع،1994).
15. عباس **بدران**، الحرب الإلكترونية: الاشتباك في عالم مُتغير، ط1، (بيروت: مركز دراسات الوحدة العربية،2010).
16. مُنى الأشقر جبور، الأمن السيبراني: التحديات ومُستلزمات المواجهة، (القاهرة:جامعة الدول العربية،2012).
17. مُنى الأشقر جبور، السيبرانية هاجس العصر، (بيروت: المركز العربي للبحوث القانونية والقضائية،2017).
18. هاري أر. يارغر، الاستراتيجية ومحترفو الأمن القومي، ترجمة راجح محرز علي، (أبو ظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية،2011).

رابعاً: البحوث والدوريات العلمية

1. ابتسام علي حسين، «فرص وقيود الأطراف المُتنازعة على المجال العام السيبراني»، **مجلة السياسة الدولية**، العدد208، (القاهرة: مركز الأهرام للدراسات السياسية والاستراتيجية،2017).
2. أحمد زكي عثمان، «تأثيرات القدرات السيبرانية في الصراعات الإقليمية»، **مجلة السياسة الدولية**، العدد208، (القاهرة: مركز الأهرام للدراسات السياسية الاستراتيجية،2017).
3. سماح عبد الصبور، «الصراع السيبراني: طبيعة المفهوم وملامح الفاعلين»، **اتجاهات نظرية في تحليل السياسة الدولية**، مجلة السياسية الدولة، العدد208، (القاهرة : مركز الأهرام للدراسات السياسية والاستراتيجية،2017).
4. سماح عبدالصبور، «الإرهاب الرقمي استخدامات الجماعات المُسلحة لوسائل التواصل الاجتماعي»، دورية اتجاهات الأحداث»، العدد2، (القاهرة: مركز الأهرام للدراسات السياسية والاستراتيجية،2014).
5. عادل عبد الصادق، «**القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني**"، **مجلة السياسة الدولية**، العدد188، (القاهرة: مركز الأهرام للدراسات السياسية

والاستراتيجية،2012).

6. نورة شلوش، «القرصنة الإلكترونية في القضاء السيبراني: التهديد المُتصاعد لأمن الدول»، مجلة بابل للدراسات الإنسانية، المُجلد8، العدد2، (بابل: مركز بابل للدراسات الحضارية والتاريخية،2018).

خامساً : الرسائل والاطاريح العلمية

1. حمزة غشوة ومعمر حمزة، دور المواقع الإلكترونية في الترويج السياحي، رسالة ماجستير غير منشورة، (الجزائر: جامعة قاصدي مرباح – ورقلة، كُلية العلوم الإنسانية والعلوم الاجتماعية،2015).
2. عبد الكريم زهير عطية الشمري، الاستراتيجية الأمريكية للهيمنة على الفضاء السيبراني العالمي، رسالة ماجستير غير منشورة، (الموصل: جامعة الموصل، كُلية العلوم السياسية,2021).

سادساً: شبكة المعلومات الدولية (الانترنت)

1. إبراهيم أبو جازية، تمت السرقة بنجاح.. القصة الكاملة لفضيحة «كامبريدج أناليتيكا» التي هزت عرش «فيسبوك»، معلومة المنشورة عبر الشبكة المعلومات الدولية (الانترنت) مُتاح على الرابط الآتي: com.sasapost.www//:https
2. بن مرزوق عنتر وحرشأوي محي الدين، الأمن السيبراني كبُعد جديد في السياسة الدفاعية الجزائرية، نقلاً عن شبكة المعلومات الدولية (الانترنت)، مُتاح على الرابط الآتي: www//:https. Univouargla.manifest
3. رفد عيادة الهاشمي، الإرهاب الإلكتروني، بحث منشور عبر شبكة المعلومات الدولية (الانترنت)، مُتاح على الرابط الآتي: com.mizandz.www//:https
4. عادل عبد الصادق، الحروب السبرانية: تصاعد القدرات والتحديات للأمن العالمي، المركز العربي لأبحاث الفضاء الإلكتروني، نقلاً عن شبكة المعلومات الدولية (الانترنت)،

مُتاح على الرابط الآتي: https://www.accronline.com.

5. علي حسين باكير، **المجال الخامس، الحروب الإلكترونية في قرن21**، مركز الجزيرة للدراسات، نقلاً عن شبكة المعلومات الدولية (الانترنت)، مُتاح على الرابط الآتي: https://www. com.aljazeera.studies.

6. قادر إسماعيل، إدارة الحروب النفسية في الفضاء الإلكتروني: استراتيجية الأمريكية الجديدة في الشرق الأوسط، تقرير منشور عبر شبكة المعلومات الدولية (الانترنت)، مُتاح على الرابط الآتي: https://www.manifest-univ-ouargla

7. مايا صبحي، الخيوط الخفية للماسونية في دائرة الضوء، نقلاً عن شبكة المعلومات العالمية (الانترنت)، مُتاح على الرابط الآتي: https://www.ar-ar.facebook.com/masonic/secret

8. وليام جورتني، قاموس المُصطلحات العسكرية، وزارة الدفاع الأمريكية، مقال منشور عبر شبكة معلومات الدولية (الانترنت)، مُتاح على الرابط الآتي: file//c:/users/discov-1/appdata

المصادر الأجنبية

First : Official Documents

1. ITU, **Cyber Security,** (Geneva**:** ITU ,2008).

Second : Dictionaries, Dictionaries and Encyclopedias

1. Julia Creswell, **Oxford Dictionary of Word Origins; Cybernetics,** (USA: Oxford University Press, 2010)
2. Norbert Wiener, **Cybernetic or control communication in the animal and the machine,** 2nd ed. (Cambridge: M.I.T Press, 1948).
3. U.S. Department of Defense, **Dictionary of Military and Associated terms**, (USA: Joint Publication, 2010).

Third : Books

1. Alfred price, **The History of US Electronic Warfare, Is ted**. (VA: Association of OLD crows, 1984).
2. H. Banks, R. Me Quillan, **Electronic Warfare test and Evaluation, Flight Test Techniques Series,** (Canada: Research and Technology Organization– North Atlantic Treaty Organization, 2000).
3. Joseph S. Nye JR, **Cyber power**, (London: Harvard Kennedy School, 2010).
4. Ken Dwight, **Bug Free computing, (**USA: The Teleprocesses Inc, 2005).
5. Rex Hugh, **Towards a Global Regime For Cyber Warfare (**London: Cyber Security project Chatham House, 2009).
6. Richard Kassel, **Glossary of key information security terms**, (USA: National Institute of Standards and Technology, Department of Commerce, 2013).
7. Rrszard Zieba, **Wspo czesne wyzwania I zagrocenia dla bezpieczenstwa** miedzynarodowego**, (**USA, Stosunki Miedzynarodowe international Relation, 2003).
8. Wendy H. Wong & Peter A Brown**, E- Bandits In Global Activism: Wikileaks Anonymous and the Politics of No One**, (Cambridge: Cambridge University, 2013).
9. William T. Johen, **Of Military Strategy**,(Boston: Center for Strategic Leadership, 2011).

Forth : Research and Scientific Periodicals

1. Joseph S. Nye, "Power and National Security in Cyberspace, Americas Cyber Future, Center For new America Security, Vo1.2, (2011).

Fifth : Internet

1. Steve Lohr**,** Global Strategy Stabilized IBM Duing Downturn, **The New York Time,** available at: https://www.nytimes.com.
2. The Electronic Money Regulations 2011, available at: https://www.legislation.gov.uk.