رقم الترميز الدولي / ISSN (P): 2710-2653
ISSN (E): 2960-253X /
رقم الايداع الوطني / 2375 / 2019

تاريخ استلام البحث 3 / 2 / 2024
تاريخ قبول البحث 20 / 2 / 2024
تاريخ النشر 30 / 3 / 2024

استخدام القُـوة السيبرانيـة في سياسات الــدول الكبـرى

The Use of Cyber Power in the Policies of the Major Countries

أ.د.عماد خليل ابراهيم
جامعة الموصل/ كلية العلوم السياسية
Prof. Dr. Imad Khalil Ibrahim
University of Mosul/College of Political Sciences
dr.emadalmukhtar@uomosul.edu.iq

م.م. نجوان هاني محمود
جامعة الموصل/ كلية العلوم السياسية
Nagwan Hani Mahmoud
University of Mosul/College of Political Sciences
nahjwanhani@uomosul.edu.iq

IRAQI Academic Scientific Journals
https://www.iasj.net/iasj/journal/393/issues

الملخص

لا شك إن القوة تعدّ محوراً رئيساً في العلاقات الدولية ، وبما إنها تستهدف تحقيق المصالح القومية للدول ،كان عليها أن تطور مفاهيمها بما يُلائم تطور الحياة الدولية وتعقّد العلاقات الدولية بناءً على ذلك، وقد تطورت إستخداماتها إنطلاقاً من القوة العسكرية ثم الإقتصادية مروراً بالقوة المعلوماتية والرقمية وإنتهاءً بالقوة السيبرانية.

وعلى الرغم من التغيّر الذي طرأ على بنية الحرب التقليدية وتصنيفها الى نزاع مسلح دولي وآخر غير دولي وأحياناً الى حرب أهلية ، إلاّ إن لجوء الدول الى إستخدام القوة الالكترونية في تزايد مستمر وذلك لما توفره من التقليل من تكلفة الحروب بإستخدام أدوات جديدة فيها مثل الفيروسات وبرامج التجسس وقرصنة المعلومات العسكرية والإستراتيجية.

ونتيجةً لذلك، حظي الأمن السيبراني بإهتمام كبير من دول العالم المختلفة، كالولايات المتحدة الأمريكية وروسيا والصين، إذ تحاول هذه الدول تحقيق مكانةً متميزة في التمكّن من هذه القوة، واستخدامها في تحقيق أهداف سياساتهما الدولية المنشودة.

كلمات مفتاحية : " القوة السيبرانية " , " الدول الكبرى " , " استوكس نيت " , " روسيا "،" الولايات المتحدة "

Abstract

There is no doubt that the power is considered to be a major axis in the international relations, and since it aims to fulfil the national interests of states, it had to develop its concepts to suit the development of international life and the complexity of international relations. Accordingly, the uses of power have developed, starting with military power, then economic power, passing through informational and digital power, and ending with cyber power.

Despite the change that has occurred in the structure of traditional war and its classification into an international armed conflict, a non-international armed conflict, and sometimes a civil war, countries' resort to the use of electronic force is constantly increasing due to the reduction it provides in the cost of wars by using new tools such as viruses, spyware, and piracy of military and strategic information.

As a result, cybersecurity has received a great attention from many countries around the world, such as the United States of America, Russia, and China, where these

countries are trying to achieve a distinguished position in mastering this power, and using it to achieve the goals of their desired international policies

Keywords: "**Cyber Power**", "**Major Powers**", "**StocksNet**", "**Russia**", "**United States**"

المقدمة

لقد تطورت إستخدامات القوة إنطلاقاً من القوة العسكرية ثم الاقتصادية مروراً بالقوة المعلوماتية والرقمية ثم أخيراً القوة السيبرانية ،لذلك حرصت الدول الكبرى على إمتلاك التقنية الالكترونية فالأنظمة المعلوماتية ووسائل الاتصالات والأنظمة الالكترونية أصبحت متاحة ويمكن الوصول اليها وعن بعد وبذلك تحولت الى هدف للمهيمنين الكبار ،فالتجسّس والمراقبة ومعرفة التحركات باتت وسيلة مهمة لدى الدول الكبرى من أجل فرض هيمنتها على العالم بأسره ،إذ تتعدد استخدامات القوة السيبرانية في التفاعلات الدولية، وهناك اليات مختلفة تدير بها الدول تفاعلاتها وذلك وفقاً لطبيعة الظروف الدولية المحيطة، سواءً في شكل تفاعلات سياسية أم عسكرية، أم اقتصادية أم غيرها.

لذلك، فالدول تسعى لحماية أمنها القومي ومواجهة التهديدات السيبرانية، من خلال العمل على مسارين: الأول تقني، عِبر تطوير الجيوش السيبرانية، وإنشاء هيئات الأمن السيبراني، والثاني قانوني، من خلال سنّ تشريعات وطنية، إقليمية، دولية لمكافحة الجريمة والإرهاب السيبراني، والعمل على الحدّ من سباق التسلح وعسكرة الفضاء السيبراني.

أهمية البحث : تكمن بدراسة ظاهرة معاصرة تلجأ إليها الفواعل الدولية المختلفة وخاصة الدول الكبرى وهي القوة السيبرانية بوصفها قضية محورية ضمن موضوعات الدراسات الإستراتيجية والأمنية لهذه الدول وتوظيفها في سياساتها الدولية.

إشكالية البحث :تستخدم الدول الكبرى القوة السيبرانية من أجل تحقيق مصالحها القومية من جهة ، ومحاولة فرض إرادتها وهيمنتها على الدول الأخرى من جهةٍ ثانية ، وهنا يندرج السؤال الرئيس للبحث: كيف تُوظّف الدول الكبرى (القوة السيبرانية) في إدارة سياساتها الدولية ؟

فرضية البحث :أصبحت الدول تركز في سياساتها على القوة السيبرانية وهي في ذلك تكون في حالة تأهب قصوى إستعداداً لأية حرب سيبرانية مما أثر في مفهوم الأمن الدولي ، إذ إستند موضوع البحث على فرضية أساسية قوامها علاقة عكسية مفادها: إنه كلما حاولت الدول الكبرى إستخدام القوة السيبرانية في سياساتها الدولية بهدف توطيد أمنها الوطني، إنعكس ذلك على زيادة التنافس فيما بينها

هيكلية البحث : إندرج البحث في محورين : الأول: ماهية القوة السيبرانية وأبعادها والثاني : نماذج لإستخدام الدول الكبرى للقوة السيبرانية

المحور الأول: ماهية القوة السيبرانية وتطور إستخدامها

مع ثورة المعلومات والتقدم التكنلوجي وظهور الانترنيت تداولت على الساحة الدولية مجالا جديدا وهو الفضاء الالكتروني الذي اصبح احد العناصر المؤثرة في النظام الدولي مما جعل التنافس بين الدول الكبرى اكثر قوة مما كان عليه

أولاً : ماهية القوة السيبرانية

تعددت التعاريف حول مفهوم القوة بمختلف أنواعها فنجد إن مفهوم القوة الصلبة مرتبط بالمفهوم التقليدي للقوة ويقصد بها" القدرة على فرض السيطرة على الآخرين عن طريق الإكراه، أو الحوافز المادية والمصادر الأساسية للقوة الصلبة هي: القوة العسكرية، والقوة الاقتصادية" ،أما القوة الناعمة فيقصد بها "إستخدام الجاذبية بدلاً من الإرغام أو دفع المال"[1]، وبالنسبة للقوة الإفتراضية، فهي ترتبط بامتلاك المعرفة التكنولوجية، والقدرة على استخدامها، وهي القدرة على استخدام الفضاء السيبراني والمعلومات للتأثير في الأحداث ، على النحو الذى يُحقّق الأهداف المرجوة بإستخدام الوسائل والأدوات السيبرانية، أما القوة الذكية فهي قدرة الفاعلين الدوليين على الجمع بين عناصر القوة الصلبة والقوة الناعمة بطريقة تضمن تحقيق أهداف الفاعلين الدوليين بكفاءة وفعالية[2] ،منذ ظهور هذا المفهوم بدأ المفكرين والباحثين بالتعرف على مدى أهمية القوة السيبرانية وإزالة الغموض عنه على إعتبار إن الموضوع له إرتباط كبير بالقوة الناعمة والقوة الذكية ، وكما هو معروف ان مصادر القوة الصلبةتتغير في كثير من الاحيان بمرور الزمن ،اذ برز الى جانب القوة الصلبة التقليدية(العسكرية والاقتصادية) القوة الناعمة التي تعتمد على الاقناع والتأثير غير المباشر ،ومع التقدم التكنلوجي وظهور ثورة المعلومات والاتصال والانترنيت ،ظهر شكل جديد لإشكال القوة ،وهو القوة السيبرانية (cyber power) ،والتي بدأت تحدث تأثير بشكل كبير على المستوى الوطني والدولي ،فَمن جهة اخرى ادى استخدام الفضاء السيبراني الى زيادة القوة لدى عدد من الفاعلين سواء الحكوميين وغير الحكوميين مما ادى الى ضعف سيطرة الدولة على مختلف المستويات وايضا زيادة القوة لدى بعض الدول وتمكينها من شن ضربات الى الدولة المعادية او التي لا ترضخ لمصالحها وبالتالي ادى ذلك الى احداث تَغيُر في ميزان القوة في العلاقاتِ الـدَولية [3].وبعد أن كان مفهوم "القوة الصلبة" هو السائد لتحقيق تلك المصالح القومية ، جاء (جوزيف ناي) بمفهوم "القوة الناعمة" ليُلائم التطورات المعاصرة في القرن الحادي والعشرين ولتصبح المعلومات هي عملة العالم الرئيسة ولتكون سمة جديدة في أجيال الحروب المتعددة لذلك فإن كل الفواعل من الدول وغير الدول أخذت تعتمد بصورة كبيرة على تكنولوجيا المعلومات، ومن ذلك تقنيات الحاسوب والاتصالات التي تُستخدم في إدارة العمليات العسكرية ، ومنها على سبيل المثال في القيادة والتحكم وفي الأمور اللوجستية ، ويُعرِفّها بأنها :" القدرةُ على الـحصولِ على النتائج المرجوة بواسطة استخدام مصادِر المعلومات المُرتبِطة بِالفضاء السيبراني"، أي إنها القدرة على استخدام الفضاءُ السِيبراني لإيجاد مزايا اكثر للدولة، من اجل التأثير على الأحداثِ المتعلقة بِالبيئات التشغيلية الأخرى ،وذلك عِأبر أدوات سيبرانية،

كما يُوضّح (ناي) بأن مفهوم القوة السيبرانية يُشير إلى "مجموعة الموارد المتعلقة بالتحكّم 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" [4].

بمعنى إن (جوزيف ناي) يرى إن القوة السيبرانية فرضت تحديات على الأطراف الدولية خاصة (الكبرى)التي كانت تحتكر مصادر القوة والتحديات وبذلك تعدّ انتقالاً للقوة وانتشارها بين أطراف متعددة سواءً أكانت دول أم غير دول[5].

من هنا يتبين لنا ان احد العناصر الاساسية التي بدأت تؤثر في العالم هو القوة السيبرانية لما لها من اداوات تكنلوجية تؤثر في العلاقات الدولية فضلا عن ميزتها الاساسية والمهمة وهي قلة التكلفة مقارنة مع القوة العسكرية ، وبات جلياً إن من يمتلك آليات توظيف البيئة السيبرانية يصبح أكثر قدرة على تحقيق أهدافه والتأثير في سلوك الفاعلين المستخدمين لهذه البيئة[6].

وتم تعريف الفضاء السيبراني من قبل وزارة الدفاع الامريكية "بأنه مجال يتّسم باستخدام الإلكترونيات والطيفْ الكَـهرومِغناطيسي لتخزين وحفظ البيانات او العمل على تعديلها أو القيام بتبادلها بواسطة أنظمة شبكاتِ الاتصال فضلاً عنِ البُنية التحتية المادية المرتبطةُ بها ،وعليه وبالاستناد على هذا التعريف، تستخدم الكيانات المدنية والعسكرية والإرهابية القوة السيبــرانيةُ من اجل تنفيذ لأنشطتها وعملياتها فضلاً عن مصالِحها [7].

إن القوة السيبرانية تُركز على وجود نظام متماسك فيه تناغم بين القدرات التكنلوجية والإقتصادية والقوة العسكرية وإدارة الدولة وغيرها من العوامل التي تُسهم في دعم إمكانيات الدولة على مُمارسة الإكراه أو الإقناع أو التأثير على الدول الأخرى من خلال السيطرة على الفضاء الالكتروني، فضلاً عن إن تكلفة الحصول على القوة أصبح مرهوناً بالتطور التكنلوجي ، مما جعل الدول في حالة إنكشاف أمني ومن ثم ستكون أمام مشكلة أمنية سيبرانية [8].

ثانياً: أبعاد القوة السيبرانية وفواعلها

للقوة السيبرانية أبعاداً عدة ،فضلاً عن إن لها فواعل مختلفة ، وتتمثل بالآتي :

1- أبعاد القوة السيبرانية: [9]

أ-البعد العسكري : تعمل القوة السيبرانية في الوحدات العسكرية على الاعتماد الكامل على تبادل المعلومات ووسائل الاتصال الذي ينعكس بصورة إيجابية على تحقيق الأهداف العسكرية المرغوب بها .

ب–البعد الإجتماعي: يُمكن لكلّ مواطن عِبر الفضاء السيبراني أن يُعِبر عن تطلعاته السياسية وطموحاته الإجتماعية إذ تُمثّل مشاركة جميع الأفراد فرصة الإطلاع على المعلومات والأفكار المختلفة.

ج– البعد السياسي: هناك دور كبير لشبكات التواصل الإجتماعي على المستوى السياسي (حملات انتخابية ،تظاهرات ،حركات إحتجاجية الكترونية) لذلك نلاحظ إهتمام الجانب السياسي بالقوة السيبرانية.

د–البعد الإقتصادي: تعزيز التنمية الاقتصادية تتم من خلال توسيع استِخدام تقنيات المعلومات والأتِصالات التي تعمل على توسيع الاستخدام التي تعمل الشركات الدولية والشركات الكُبرى على تقديمها مِن أجل الأنتاج بأفضل الشروط.

2–الفواعل الرئيسة في ممارسة القوة السيبرانية : حدّد (جوزيف ناي) ثلاثة أنواع من الفاعلين وهم :الدولة والفاعلون من غير الدول والأفراد.

أ.الدولة: تعتبر الدولة الفاعل الرئيسي في استخدام القوة السيبرانية لما تتمتع به من امكانيات بشرية وبنية تحتية وارادة فالدولة تستطيع ات تتحكم بنظم المعلومات بواسطة اجزتها لذلك نلاحظ في الفترة الاخيرة زيادة التنافس الدولي وذلك نتيجة تزايد استخدام القوة السيبرانية(10).

ب.الفاعلون من غير الدول: وهم الأفراد والجماعات والمنظمات غير الحكومية والشركات الذين يعملون على التحكّم في سياسات الدول وإدارتها وفق توجهات معينة من خلال الفضاء السيبراني وأهم الفواعل هي :

–الشركات متعددة الجنسيات: هناك شرِكات تمتلك إمكانيات وقدرات تتفوقبها على قدرة بعض الدول ولا ينقصها الا شرعيةُ ممارسة القـوة التي تعد حكراً على الدول، فمثلاً نجد شركات (كـوكِـل– Google) ،و(ميكْـروسـوفت/ Microsoft ، وأبـلْ/ Apple) المُنتشِرة في دولِ العالـم المختلفة تملك قـواعِد مِن البيانات التي تستطيع عن طريقها التأثير في اقتصادياتِ الكثير من دولِ العالم وقوتها الناعمة ، لا سيما ان مُعظم دول العالم تتجه صوب جذب هكذا شركات دولية بغية ضمان ايجاد استثماراتٌ جديدةٌ فيها لأنها تستغل أدواتِ الـدفع عِبر الانترنت [11].

–المنظمات غيرُ الحكومية : تستند هذه المُنظمات بصورة كبيرة على شبكة المعلومات الولية الانترنتفضلاً عن الوسائل التكنولوجيةُ الحديثة من اجل تعبئة الرأي العام، والضغط على الحكوماتعن طريق ترتيب الحملاتْ الاجتماعية فضلاً عن تعبِئة المجتمع المدني ليمارس ضغطاً على الحكومات ،ولتغيير سياسات معينة ،كمثل ما تقوم به اليوم معظم منظمات البيئة العالمية على أثر قـرار الرئيس الأمريكي الأسبق (دونالد ترامب) بِالتخلّي عن اتفاقياتُ التغير المُناخِي[12].

–حركاتِ التحرر الــوَطني: تعد من افضل الفواعل الدولية مِن غير الدول، مثل(حركة حماس وحزب الله) ، يشارك هذه الحركات عدد كبير من الأفراد بصفاتهم الشخصية ويقومون بإرسال هجمات سيبرانية ضد أهداف العدو على الإنترنت دفاعاً عن قضية معينة [13].

ج.الأفراد : يعدّ الفرد فاعلاً مهماً في الفضاء السيبراني، إذ إن له القدرة على إحداث الثورة في المعلوماتية وتُصبح مجالاً لإستخدام الدولة نفسها، ومثال عى ذلك ما قام به (مارك زوكربارغ/ Zoukerberg Mark) عام 2004 ، بتأسيسه لشبكة التواصل الاجتماعي الـ (فيس بوك) لِتستقطب أكثرُ مِن مِليارُ مُستخدِم عِبر العالم، فمواقع التواصل الاجتماعي كان لها دوراً كبيرا في تنظيم مظاهرات عدة في مختلف دول العالم، كما إن هناك أفراد مختصون في أعمال القرصنة أو الجرائم السيبرانية وسرقة المعلومات والبيانات الشخصية والتلاعب فيها أو الإساءة في استغلالها، ان زيادة استخدام الفضاء السيبراني ادى الى ازدياد انتشار القوى بين الفاعلين من غير الدول للتأثير في سياسات دول معينة لذلك نلاحظ زيادة التهديدات والمخاطر التي تتعرض لها الدول في الاونة الاخيرة واصبح من الضروري ان تسيطر كل دولة علىقوتها التكنلوجية التي تمكنها من الرد على اي هجوم خارجي [14]

اصبح العامل الالكتروني له دور مهم وفاعل في تحديد قوة ومكانه الدولة اذ ان السيطرة على اسلحة المعلومات امر مهم للغاية في ظل التنافس الدولي ،وعلى العكس من ذلك تعد الدولة ضعيفة رقميا اذا لم تمتلك اسلحة فضاء الكتروني مما يعرضها لمشاكل كثيرة مع الدول الاقوى [15]، وعلى سبيل المثال ، نجد إن حلف شمال الأطلسي سعى بدوره الى تحديث عقيدته الأمنية إستجابة للتغيرات الحاصلة في طبيعة التهديدات وطبيعة الحرب ، إذ أقرّ مجموعة من الآليات لتنفيذها من بينها ، إن الدفاع السيبراني يُمثّل جزءاً أساسياً من الدفاع الجماعي ولعملياته، وبناء القدرات السيبرانية بوصفها مهمة أساسية له ، فضلاً عن ذلك ، نجد إن كلاّ من الولايات المتحدة وروسيا والصين وبريطانيا وفرنسا وإيران وكوريا الشمالية، قد طورت كلّ منها عقيدتها الأمنية، وأصبحت تعدّ الفضاء السيبراني مسرحاً للعمليات العسكرية التي تحقق مصالحها من خلاله، كما أوجدت قيادة خاصة ومستقلة لقيادة العمليات السيبرانية [16].

وعلى الرغم من عقد الاتفاق المبدئي بين (تشي جين بينغ– Xi Jinping) ، و (باراك أوباما– Barack Obama) في واشنطن في أيلول 2015 ، إلاّ هناك أسئلة جوهرية تُثار حول العلاقة بين الدولتين فيما يخص الفضاء السيبراني، ففي غياب مجموعة معايير وإجراءات تفصيلية كاملة لضبط النشاطات المثيرة للقلق وقواعد رأسية خاصة به، ستستمر المشكلة في تشكيل خطر كبير على العلاقة الثنائية وعلى السلام والإستقرار الإقليميين وعلى النظام العالمي أيضاً[17].

في عام 2014 أجرت كوريا الشمالية هجوماً إلكترونياً ضدّ شركة Sony Pictures Entertainment ، فقد تم إختراق المعلومات السريّة لهذه الشركة وتعطيل الآف عدة من أجهزة الكمبيوتر عن للعمل، فضلاً عن ذلك، سرقت كوريا الشمالية نسخ رقمية لعدد من الأفلام التي لم يتم إطلاقها، بالإضافة إلى

آلاف المستندات التي تحتوي على بيانات حساسة تتعلق بالشخصيات الشهيرة وموظفي الشركة، ويعدّ هذا الهجوم واحداً من أكثر الهجمات الإلكترونية خطورة، إذ أدى إلى مزيد من النقاش حول طبيعة التهديد السيبراني والحاجة إلى تحسين الأمن السيبراني(18).ترتيب الدول القوية سيبرانيا حسب مؤشر القوة الإلكترونية الوطنية للعام 2022 جاء كالآتي:

التسلسل	الدولة
الاول	• الولايات المتحدة الأميركية
الثاني	• الصين
الثالث	• روسيا
الرابع	• المملكة المتحدة
الخامس	• أستراليا

يتضح من الأرقام والمعطيات الواردة في المؤشر تقدّم روسيا على بريطانيا في المركز الثالث، وبينما بقيت الصين في المرتبة الثانية، قفزت أستراليا من المرتبة العاشرة في عام 2020 إلى المرتبة الخامسة في مؤشر هذا العام 2022؛ في حين تراجعت فرنسا ثلاث درجات من المركز السادس إلى التاسع.

الجدير ملاحظته أنه في تصنيف 2022، جاءت أوكرانيا في المرتبة 12 بعد أن حققت قفزة هائلة من المرتبة 29 في عام 2020، ويبدو أن الحرب في أوكرانيا ساهمت في زيادة المواقف لكل من روسيا وأوكرانيا، وأدت إلى صعود روسيا وتفوقها على المملكة المتحدة في التصنيف العالمي.

أحد أهم العناصر الرئيسية التي أشار إليها التقرير هو أن الولايات المتحدة الأميركية لا تزال تتربع على رأس القائمة الأقوى من حيث امتلاكها القوة السيبرانية، وقد احتلت مكانة بارزة لا مثيل لها في شؤون الفضاء السيبراني العالمية خلال الأعوام السابقة، ولطالما احتفظت واشنطن بتفوقٍ واضح على جميع البلدان الأخرى من حيث قدراتها في تكنولوجيا المعلومات والاتصالات، وقد كانت الهيمنة على الفضاء السيبراني هدفا إستراتيجيا للولايات المتحدة منذ منتصف التسعينيات؛ وهي الدولة الوحيدة التي لها بصمة عالمية بارزة في كل من الاستخدامات المدنية والعسكرية للفضاء السيبراني، على الرغم من أنها تعتبر نفسها الآن مهددة في هذا المجال بشكل خطير من قبل الصين وروسيا.

اكثر الدول تعرضا للهجمات الالكترونية هي:

	اكثر الدول تعرضا للهجمات	عدد الهجمات
1	بولندا	114
2	استونيا،لاتفيا،ليتوانيا،	157
3	السويد والنرويج	95
4	المانيا	58
5	بريطانيا	18
6	فرنسا	14
7	اسبانيا	4

وبحسب ما تقدم، يمكن أن يفضي استخدام القوة السيبرانية الموجَّه لدولة ما إلى عدد من العواقب لعل من أهمها[19]:

–الإطاحة بنظام الحكم أو تهديد أمنها القومي.

–التمهيد لبدء الحرب التقليدية خلال المستقبل القريب.

–القيام بعمليات تخريب في قطاعات حيوية، تؤثر في حياة السكان.

–الإضرار بالعلاقات السياسية والدولية أو الإساءة إلى مكانتها.

–التسبب بحدوث عدد من الإصابات البشرية أو إلحاق الخطر على الصحة والسلامة العامة.

–نشر الفوضى الداخلية والاضطراب واسع النطاق.

–تقويض ثقة الجمهور بمعتقداتهم الدينية والسياسية والقومية والعرقية.

–إلحاق أضرار جسيمة بالاقتصاد الوطني.

–تدمير واسع النطاق أو تعطيل في أداء الأصول الإلكترونية الوطنية

المحور الثاني: نماذج لإستخدام الدول الكبرى للقوة السيبرانية

أصبحت القوة السيبرانية تمتاز بدور كبير في حركة التفاعلات والتحولات البنيوية في العلاقات بين الدول ،وبدأ ينتقل تأثيرها الى إحداث تغيرات في النظام الدولي وأصبح العالم يشهد تطوراً في تهديد الأمن العالمي، إذ أصبحت (القوة السيبرانية) مصدر إهتمام على أجندة القضايا الأمنية الدولية خاصة بعد أحداث 11 أيلول، إذ تعدّ روسيا والصين والولايات المتحدة الامريكية من أقوى الدول التي تستحوذ على القوة السيبرانية القادرة على توفير الحدّ الأعلى من الأمن الالكتروني ثم ظهرت قوى اقليمية سيبرانية مثل: ايران وكويا الشمالية وهو ما فرض على هذه الدول تبنّي سياسات سيبرانية دفاعية خوفاً من التهديد الأمني وحماية المعلومات والبرمجيات وتعزيز القدرة الالكترونية[20]..

أولاً : سياسات روسيا السيبرانية

أدى تفكك الإتحاد السوفيتي عام 1990 الى حدوث تحولات دولية جذرية وتغيير في مفاهيم القوة التقليدية والاتجاه نحو القوة الناعمة ،وقد إستخدم هذا المفهوم (فلاديمير بوتين) عام 2009 في خطابه أمام مجلس الدوما والذي عدّ فيه إن إمتِلاك دولة روسيا الاتحادية للقوةِ الناعِمة يهدف الى استعادتها لِدورها العالمي[21].

وفي ظل التنافس الدولي اتجهت روسيا الى تعزيز قدراتها السيبرانية ، فقد صدر في العام 2011 البيان الرسميُ الأول بخصوص المهامُ الاستراتيجية لروسية الاتحادية في الفضاء السيبراني، وتم تأسيس جيش (المتصيّدين) التابع لوكالة الأمن الإتحادي الروسي الذي يضم الآف الموظفين ويُخصّص له سنوياً 300 مليون دولار من ميزانية الدفاع[22].

وقد إستخدمت (روسيا) القوة السيبرانية من خلال أنماط عديدة تتمثل في: تعطيل الخدمة، السيطرة على الأنظمة العسكرية، إتلاف المعلومات أو تعديلها، سرقة المعلومات والبيانات العسكرية، جمع معلومات اقتصادية استخباراتية، التكّم بالعقل والسيطرة عن بعد، وأخيراً الحرب النفسية[23].

" ويُعدّ الجيشُ الإلكتروني لروسيا الاتحادية خامِسُ أقوى الجيوش في العالم الإلكتروني بعد الولايات المتحدةُ وبريطانيا والصين وكوريا الشمالية ،وتتلخّص مُهِمات الجيش الإلكتروني الروسي بـ :[24]

1-القيامُ بعمليات تتمثل بالتجسّس الخاص على الخصوم وكِبار المسؤولين في بعض الدول .

2-شنّ الهجمات الإلكترونية التي تحدث وتتسبب بالاضرار للبُنى التحتية وتضرب الاقتصاد والمواقع الحكومية الخاصة في الدول الأجنبيةُ المعادية فضلاً عن الدول ذاتِ التطور السيبرانيُ الكبير، وحروب المعلوماتية في وسائلِ الإعلامِ وكذلك الشبكاتُ الاجتماعية .

3- ايضاً تنفيذ عدد من عمليات الاختراقِ للحساباتِ والبريد الالإلكتروني ،وبذل الجهود لتحديد قيادات الخصم والعمل على تحييـدها بواسطة الاعتماد على وسائل الإسترتيجية السيبرانيةُ .

إن لروسيا تاريخ سابق في شنّ هجمات سيبرانية ، ففي عام 2007 قامت بشنّ حرب سيبرانية على أستونيا بسبب تغيير مكان التمثال الذي يخلد الجنود الروس في الحرب العالمية الثانية ،إذ شنّت هجمات ضد بعض المواقع التي تديرها الحكومة الاستونية مما أدى الى عرقلة معاملات المواطنين البنكية الالكترونية التي كان نحو 97% منها يتمّ عِبر الأنترنيت فضلاً عن تعطيل البنية التحتية للإقتصاد الأستوني[25].

ونتيجة الى تعطّل الى كافة الخدمات التي تقدمها الدولة للمواطنين بسبب الإعتماد على الأنظمة الالكترونية لإدارة شؤون الدولة ، حاولت أستونيا اللجوء الى دول حلف شمال الأطلسي لمواجهة الحكومة

الروسية، وعلى الرغم من إنكار روسيا للهجوم إلاّ انها إعترفت بأن من قام بالهجوم يُعتقد إنها منظمات اجرامية رافضة لنقل التمثال[26].

كذلك ،شنّت روسيا هجمات سيبرانية على بعض المواقع الحكومية لجمهورية جورجيا ، كردّ على إرسال الحكومة الجورجية (الموالية للغرب) قوات للحكومة الإنفصالية ،إذ توقفت شبكة الأنترنيت عن العمل وتم إختراق (الموقع الألكتروني لرئيس الجمهورية) حيث ظهرت صورة الزعيم النازي (أدولف هتلر) بجانب صور رئيس الجمهورية، فضلاً عن الهجوم على أكبر بنك تجاري في جورجيا مما ادى الى قطع الصلة بينها وبين والعالم الخارجي[27].

وفي عام 2014، أطلقت روسيا الاتحادية هجمات سيبرانية متعددِة لمحاولة تعطيل وتأخير إنتخابات الرئيس الأوكراني آنذاك ،وقبلْ ان تبث النتائج بساعات أعـلنت(قناةُ روسيا الأولى) بأن المُرشح للانتخابات اليميني المتطرف المُوالي لِروسيا (ديمترو ياروش) هو الذي فاز ولكن النتائج غير صحيحيه ولم تكُن كذلك ،وكان الهدف من هذا هو من اجل تعبئةُ الجمهور الروسي في اوكرانيا والذي كان يُؤيد انفصال جزيرةُ القِرم ،وقد عُدّ هذا الإعــلان الذي صاحب هده العمليةُ العسكرية في القِرم بمثابة حرب سيبرانية وجزءٌ من الإستراتيجية الروسية من اجل التأثير على مناطقِ النفوذ في العالم [28].

شهدت أوكرانيا هجمات إلكترونية متواصلة على مدار العقد الماضي، ونُسبت العديد من الهجمات إلى روسيا، ففي عام 2020، واجهت أوكرانيا حوالي 397 ألف هجمة ونحو 280 ألف هجوم في الأشهر العشرة الأولى من عام 2021 وكانت الهجمات واسعة النطاق لدرجة أن الاتحاد الأوروبي أرسل فريق الاستجابة الإلكترونية السريع لتقديم الدعم لكييف.

كن من الواضح جدا أن روسيا تستعمل الحرب السيبرانية من خلال أسلوب الحرب المختلطة أو ما يعرف بالهجينة، ليس فقط من خلال توجيه الهجمات إلى البنية التحتية لتكنولوجيا المعلومات. بل من خلال توجيه المعلومات الكاذبة أيضا من قبل روسيا نفسها. إذ تصبح الهجمات السيبرانية جزءا من الحرب النفسية الحديثة، ويوضح ذلك هيربيغ بأن "الأمر يتعلق بزعزعة ثقة السكان لتحطيم قدرتهم على المقاومة."

في بعض الحالات يمكن أن يكون للهجمات الرقمية تأثير محدد للغاية على مسار الحرب. لكن كلما زادت رقمنة الجيش، زادت نظريا مساحة الهجوم التي يوفرها على سبيل المثال، حاول القراصنة الروس اختراق التطبيقات المستخدمة للسيطرة على سلاح المدفعية الأوكرانية مع مثل هذا الإجراء، بحسب هيربيغ، يمكن للمرء على سبيل المثال الحصول على بيانات جغرافية من أجل قصف مواقع المدافع[29].

أطلقت روسيا فى 30 سبتمبر 2015 حملتها العسكرية ضد التنظيمات الإرهابية فى سوريا، والتى تمثلت أهدافها الرسمية فى حماية الجيش العربى السورى من الانهيار حتى لا تسقط مؤسسات الدولة الحالية، فضلاً عن القضاء على تنظيمى "داعش"، وجبهة النصرة التابعين لتنظيم القاعدة وغيرها من

التنظيمات الإرهابية الأقل نفوذاً وانتشاراً. وفى مواجهة هذا التدخل الروسى، تصاعد الجدل الداخلى بشأن جدواه ومدى انعكاسه على الداخل الروسى، واختلفت اتجاهات الرأى العام تجاه هذه الخطوة، خاصة فى ضوء الذكرى السلبية للتدخل السوفيتى فى أفغانستان.

هذا وقد نجحت الحكومة الروسية فى تهدئة مخاوف الرأى العام من التدخل العسكرى فى سوريا، ونجحت فى تعبئة الرأى العام لصالح تأييد هذا القرار، وذلك من خلال الخطوات التالية[30]:

– سعى وزارة الدفاع الروسية لإصدار بيانات صحفية عن العلميات العسكرية فى سوريا، ونشرها من خلال موقع الفيس بوك يومياً، فضلاً عن كتابة تغريدات على موقع تويتر عن العمليات العسكرية الروسية فى سوريا، وذلك بهدف تقديم معلومات مفصلة عن الضربات الجوية، كما يتم عرض مقاطع فيديو للعمليات العسكرية وللظروف المعيشية على اليوتيوب التى يعيش فى ظلها أفراد الجيش الروسى فى سوريا. وتهدف هذه الخطوة إلى زيادة الشفافية وتقديم انطباع بأن المناطق التى توجد فيها القوات المسلحة الروسية آمنة ومحمية.

– التأكيد على استخدام الجيش الروسى أسلحة ومعدات عسكرية متقدمة تقنياً، مما يقلل إلى حد كبير من خطر الإصابات والخسائر فى صفوف الجيش الروسى فى سوريا، فضلاً عن استبعاد القيادة الروسية إمكانية إرسال قوات برية إلى سوريا.

– توظيف الكرملين حادث استهداف الطائرة المدنية الروسية فى سيناء بعمل ارهابى، للتأكيد على ضرورة توجية ضربات انتقامية ضد داعش، وهو ما يتسق مع توجهات الرأى العام فى هذا الإطار.

ومما سبق، يتضح ان طريقة إدارة الكرملين التغطية الإعلامية الالكترونية للحرب الروسية فى سوريا حتى الآن، نجحت فى إيجاد مواقف إيجابية وداعمة من جانب أغلب فئات الشعب الروسى، خاصة أنه ليس من المتوقع أن تواجه القوات الجوية الروسية خسائر بشرية تذكر نتيجة عملياتها العسكرية فى سوريا، وقد انعكس هذا النجاح فى التغطية الإعلامية للحرب على نتائج استطلاعات الرأى العام التى قامت بها بعض مؤسسات قياس الرأى العام الروسية.

لا تتوانى روسيا عن استخدام القوة السيبرانية فى إدارة تفاعلاتها الدولية السياسية والعسكرية بما يساعد فى تعظيم قوة روسيا وتحقيق أهدافها التى تعجز أدوات القوة التقليدية عن تحقيقها، خاصة بما تتميز به هذه القوة من خاصية التخفى والقدرة على إصابة أهداف الخصم، واتساع نطاق تدمير الأهداف الالكترونية مع التحكم فى امكانية إصابة الاهداف من دون وقوع خسائر بشرية غير مقصودة، وفى مايو 2015 اكتشف مُحقّقون ألمان تعرّض شبكة الكمبيوتر الخاصة بالبرلمان الألماني (البوندستاغ) للاختراق من جانب مجموعة من الهاكرز، في هجوم سيبراني يُعد الأبرز في تاريخ ألمانيا، وقال دائرة الاستخبارات الاتحادية الألمانية BfV، لاحقًا، إن روسيا كانت تقف وراء هذا الهجوم في مسعى للحصول على معلومات لا تتصل بأعمال مجلس النواب الاتحادي الألماني فقط، بل معلومات تخُص القادة

الألمان، وحلف شمال الأطلنطي (الناتو) أيضًا، وقال خبراء الأمن إن الهاكرز حاولا اختراق أجهزة الحاسب الخاصة حزب الاتحاد الديمقراطي المسيحي للمستشارة الألمانية أنجيلا ميركل[31].

ويعتقد خبراء الأمن أن الروس يحاولون تدمير المُستشارة الألمانيّة الحالية أنجيلا ميركل، على خلفيّة مواقفها الداعمة لفرض عقوبات ضد الرئيس الروسي فلاديمير بوتين بعد ضم روسيا لشبه جزيرة القرم.

واخيرا، تبيّن إن روسيا لجأت الى استخدام القوة السيبرانية بدلاً عن الحروب التقليدية ، ومن ثمّ سيُجنّبها الوقوع في إتهامات إرتكاب جرائم الحرب وفرض العقوبات عليها من المجتمع الدولي فضلاً عن التعويضات التي ستخلفها الحرب.

ثانياً: سياسات الولايات المتحدة الأمريكية السيبرانية

تُعدّ الولايات المتحدة الأمريكية الدولة الأكثر تفوقاً في مجال إمتلاك القدرات العسكرية السيبرانية،إذ تم تشكيل قيادة سيبرانية موحدة في وقت مبكر من عام 2018 بإشراف مدير وكالة الأمن القومي، من أجل التماشي مع التطور الكبير والواسع في القدرات السيبرانية الأمريكية، وقد كان هذا أحد أهداف الاستراتيجية السيبرانية الوطنية لوزارة الدفاع الأمريكية[32].

تعتمد القيادة السيبرانية الأمريكية على خمسة مكونات أساسية: "القيادة السيبرانية للجيش، وقيادة الأسطول السيبراني، والقيادة الإلكترونية للقوات الجوية، والقيادة الإلكترونية لقوات مشاة البحرية وخفر السواحل، بالإضافة إلى وحدات الحرس الوطني" وترتكز استراتيجية الفضاء الإلكتروني الأمريكي على مبدأ "الدفاع المتقدم"، لذا ينظر البعض إلى القوة السيبرانية الأمريكية على إنها قوة هجومية في المقام الأول، فالولايات المتحدة الأمريكية أصبحت تركز بشكل متزايد على دمج القدرات التكنولوجية في جميع مراحل العمليات التي تقوم بها قواتها المسلحة، وفي كل مستوى من مستويات القيادة[33].

لقد ظهرتِ الاهتماماتُ الامـريكية السيبرانية في اهداف استراتيجيتها العامة ، وازدادت عام 2010 ، بعد أن تعرّض البرنامج النووي الإيراني إلى هجوم سيبراني أمريكي ، مُحدثاً أضراراً جسيمة ، وسُمى هذا الهجوم بـ (ستوكس نيت–Stuxnet) وهو عبارة عن برنامج كمبيوتر خبيث يهاجم أنظمة التحكم الصناعية المستخدمة على نطاق واسع في مراقبة الوحدات التي تعمل آليا، وعلى الرغم من أنه تم اكتشاف هذا الفيروس لأول مرة من قبل شركة بيلاروسية تدعى (VirusBlockAda) إذ قالت انها عثرت على التطبيق الخبيث في جهاز كمبيوتر يعود لأحد عملائها الإيرانيين(34)، إن الهجوم كان دقيقاً إلى درجة تحديد عدد أجهزة الطرد المركزي، وقد احتاج تفعيل هذا الهجوم مجرد تشغيل أجهزة الكمبيوتر في المنشآت الإيرانية، وبمجرد أن تسلل الفيروس إلى الأجهزة أخفى وجوده واستطاع تعطيل أجهزة الطرد المركزي بمهارة فائقة، إذ عمل على تغيير الضغط داخل أجهزة الطرد المركزي، وجعل سرعة الدورات داخل الأجهزة متفاوتة، مما أدى إلى انهيارها، ويعدّ البعض إن نجاح هذا الهجوم انتقل بالعالم إلى مرحلة

توظيف الهجمات السيبرانية في تحقيق أضراراً مادية متعمدة، وهو ما يفتح الباب أمام الكثير من التكهنات بأن مثل هذه الأسلحة المتطورة يمكن أن تصبح أمراً شائعاً في المستقبل[35].

وفي 25 أيلول /سبتمبر من عام 2010 ، أكدت إيران إن العديد من وحداتها الصناعية تعرّضت لهجوم إلكتروني بعد إصابتها بفيروس" ستكوس نيت "ويعد هذا الفيروس وفق العديد من التقارير التي صدرت مؤخراً، واحداً من أعقد الأدوات التي تم استخدامها ، الذي دمر أجزاء كبيرة من البرنامج، وأحكمت جميع وحدات مُفاعِل (نطـنز) الخاص بِتخصيب اليُورانيوم من خلال برامج فعاله ،والتي كان لها دور في مساعدتها بالتعرف على التفاصيل على شبكاتِ الكومبيوتر التي تخص المنشأة، بما في ذلك أنظمةُ التحكُّم الصناعي المتصلة ، كما استهدف أيضاً وحداتُ التحكم المنطقية القابلة لِلبرمجة والموفرة للتحكم بالعمليات الكهروميكانيكية، وان هذا أدى الى تحطيم اجهزةُ الطردِ المركزي السريعةُ الدورانِ بصورة كبيرة ،واحدثت أضرار جسيمة في البرنامِج النووي الإيراني فضلاً عن ما تسببت فيه بتكاليف كبيرة وان الوقت اللازم لإصلاح الأضرار التي حدثت داخل الأنظمة التكنولوجية والمعلومات في جميع وحدات المُفاعِل لتخصيب اليورانيوم ، وسيتطلب هذا إعادة تأهيلهُ جُهداً كبيراً ،فضلاً عن التغيير في المعداتِ الصناعية والتي لا يُمكن ابداً الحصول عليها إلاّ بواسطة شبكات بطيئة وكذلك سرية الانتشار(36) ،وبسبب هذا الهجوم، إستهدفت إيران المصالح الأمريكية المتمثلة بشركة أرامكو في الخليج[37].

إذ كان الخبراء يعتقدون إنّ مهمّة البرنامج هي التجسس الصناعي ونقل المعلومات التي تساعد على تقليد المنتجات، لكن تبيّن لخبراء الهندسة العكسيّة فيما بعد أنّ الأمر مختلف كليا فالبرنامج وعلى عكس الكثير من البرامج المعروفة إلى الآن ليس مخصصاً للتجسس وسرقة المعلومات الصناعية لمحاولة كسب المال أو لسرقة الملكية الفكرية، فبعد نحو أربعة أشهر من العمل، ظهر أن الأمر أكثر تعقيداً مما كان متصوراً، اذ ظهر نوع جديد من البرامج التي من الممكن أن تتحول إلى نموذج للأطراف التي تنوي إطلاق هجمات إلكترونية تؤدي إلى دمار حقيقي وواقعي في البلد المستهدف [38] فالبرنامج لا يعمل بشكل عشوائي كما هي العادة وإنما بشكل محدد جدا، إذ يقوم بعد اختراق الأجهزة والحواسيب بالتفتيش عن علامة فارقة تتعلق بأنظمة صنعتها شركة" سيمنز الألمانية"، فإذا ما وجدها يقوم عندها بتفعيل نفسه ويبدأ بالعمل على تخريب وتدمير المنشأة المستهدفة من خلال العبث بأنظمة التحكم وقد تتعدد المنشآت التي يستطيع مهاجمتها من خطوط نقل النفط إلى محطات توليد الكهرباء وحتى المفاعلات النووية وغيرها من المنشآت الاستراتيجية الحسّاسة، أمّا إذا لم يجدها، فيترك الحاسوب وشأنه، فالبرنامج كبير ومشفّر جدا ومعقد جدا ويوظّف تقنيات ذكية وجديدة، ولا يلزمه للعمل أي تدخل بشري في أي مرحلة من المراحل، ويكفي أن يكون هناك بطاقة ذاكرة تخزين إلكترونية مصابة به حتى يبدأ عمله، ولأنه على هذه الدرجة من التعقيد والتطور ولأنّه يعمل بشكل محدد جدا، حيث يرى البعض أنه من صنع دولة، ومن البديهي أن تكون المنشأة أو المنشآت الأساسية التي يبحث عنها لتدميرها أو تخريبها قيّمة للغاية وعلى

درجة عالية من الأهمية، وبناء على هذا الاستنتاج ذهبت العديد من المصادر إلى التخمين بأنّ مفاعل بوشهر الإيراني قد يكون الهدف الأساسي الذي يبحث البرنامج عنه لتدميره[39].

وأشارت شركة" سيمناتيك "التي تعمل في مجال برامج الأمن الإلكتروني والبرامج المضادة للفيروسات إن إيران تأتي في طليعة الدول المستهدفة من ناحية الإصابات التي حققها برنامج" ستكس نيت[40]" ،وإن ما يقارب 60 من أجهزة الكمبيوتر التي تعرضت لهجوم من هذا التطبيق الخبيث كانت في إيران ،وعلى الرغم من إن إيران نفت عِبر مدير مشروع بوشهر محمود جعفري أن يكون الفيروس قد أصاب المفاعل أو تسبّب في أي ضرر في أنظمة التحكّم فيه، إلاّ إنها كانت قد أقرّت إصابة بعض الحواسيب الشخصية المحمولة لموظفي المحطة بهذا الفيروس إضافة إلى إصابته لأكثر من 30 ألف نظام حاسوبي لمنشآت صناعية متعددة داخل إيران ،إن هدف الفيروس الأساسي هو مفاعل بوشهر، وإنّ الفيروس قد حقّق هدفه من التخريب بدليل إن إيران أعلنت أنها ستؤجّل العمل في المفاعل عدّة أشهر حتى بداية عام2011[41].

الخاتمة

حظيت القوة السيبرانية باهتمام كبير من مختلف دول العالم، وعلى رأسها الولايات المتحدة الأمريكية، وروسيا، وغيرها، وحقَّقت بعض الدول مكانةً متميزةً في التمكُّن من هذه القوة، واستخدمتها في تحقيق أهدافها المنشودة، كما لم تسلم أيضاً من التهديدات التي وصلت إلى حد التجسّس والتدخل في الشأن الداخلي.

من خلال ماتقدم توصل الباحثان الى استنتاجات عدة منها :

1-باتت القوة السيبرانية حقيقة مساندة للقوة التقليدية لبعض الدول وداعمة لها في العمليات الحربية والأنشطة السياسية والإقتصادية والدبلوماسية للدول.

2-تدعيم القوة الناعمة للدول.

3-القدرة على الوصول للأهداف المرجوة بأقل التكاليف والوقت.

4-وفرت للدول مجالاً حركياً تتجاوز فيها الحدود الجغرافية للوصول الى أهداف قد يصعب وصولها عن طريق القوة التقليدية.

6-زيادة الإنفاق في مجال السياسات الدفاعية الهجومية، وحماية الشبكات الوطنية من خطر التهديدات، وبناء مؤسسات وطنية رصينة للحماية الإلكترونية.

الهوامش

(3) جيمس دورت وروبرت بالستغراف، النظريات المتضاربة في العلاقات الدولية (ترجمة: وليد عبد الحي)،ط (1 بيروت: مكتبة شركة كاظمة للنشر والترجمة) 1995 ص 6 .

(2) جُـوزيف س.ناي ،القـوةِ الناعِمة وسيلـةُ النجاح في السياسة الدوليـة (ترجمة : محمـد تـــوفيقْ البجيرمي) ، (الــرياض :العبيكان للنشِر) ، 2007، ص12.

(3)محمد سيد ريان،الإعلام الجديد،ط1،(القاهرة،مركز الأهرام للنشروالترجمة والتوزيع،2012)،ص7.

(4) joseph s.nye jr , cyber power, harvard kennedy school, 2010, p 03 .

(5) منى الأشقر جبور ، السيبرانية هاجس العصر (دم : دت) ، ص66 ، على الموقع:

https://www.carjj.org/sites/default/files/ebooks/cyber.ebook.pdf

6)نصيرة صالحي،التنافس العالمي على قوة الفضاء الالكتروني والقدرات السيبرانية،دفاتر السياسة والقانون ،العدد (1)،المجلد 13،الجزائر ،2021،ص376

(7) هربرت لين ،النزاع السيبراني والقانون الدولي الإنساني ،مختارات من المجلة الدولية للصليب الأحمر ، مجلد/ 94 (886) صيف 2012.

(8) هربرت لين ،مصدر سبق ذكره.

(9) محمد مختار،"هل يُمكِن للدول أن تتَجنبْ مخاطِر الهجماتِ الإلكترونية؟ "، مفاهيم المُـستقبل، العدد6 ، مركز المستقبل للأبحاث والتطوير،2015 ، ص5-6

(10) إسماعيل قادير"إدارة الحروب النفسية في الفضاء الإلكتروني: الإستراتيجية الأمريكية الجديدة في الشرق الأوسط " .عولمة الإعلام السياسي وأثرها على الأمن القومي للدول النامية ،(كلية الحقوق والعلوم السياسية : قسم العلوم السياسية ، جامعة قاصدي مرباح : ورقلة)،2017،ص5.

(11) Steve Lohr, Global Strategy Stabilized IBM During Downturn,(New York:2010),p(44).

(12) لطفي أمين بلفرد، "التهديدات الأمنية في الفضاء السيبراني" ، أقلام شرطية ، العدد129،(الجزائر) ، ديسمبر2015 ،ص3.

(13) محمد عصمان ،" دور المنظمات غير الحكومية في حماية حقوق الإنسان" ،19-12-2017، على الموقع: http://www.pointjuridique.com/2017/02/19/%D8%AF%D9%88

(14) فاطمة عوامر، تأثير القوة السيبرانية على الإستراتيجيات الأمنية للدول الكبرى دراسة حالة – الصين، رسالة ماجستير غير منشورة،جامعة قاصدي مرباح ورقلة :كلية الحقوق والعلوم السياسية،2018،ص24.

(15) لطفي امين بلفرد ،الفضاء السيبراني:هندسة وفواعل،المجلة الجزائرية للدراسات السياسية،الجزائر، العدد 5، ،حزيران-2016،ص149.

(16) إسماعيل زروقة ،الفضاءُ السيبراني والتحوّل في مفاهيمُ القــوة والصراع ،مجلة العلــوم القانونية والسياسية، المُجلد 10 ،العدد 1، جامِعة محمد بوضياف المسيلة ،الجزائر ، 2019، ص1020.

(17) علاء الدين فرحات،الفضاء السيبراني :تشكيل ساحة المعركة في القرن الحادي والعشرين،مجلة العلوم القانونية والسياسية ،المجلد10،العدد3،ديسمبر 2019،ص93.

(18) Department of Defense Cyber Stratigy, Department of Defense, April 2015, p 2. Book online, available from https://goo.gl/g4hpuA.

(19) الهجمات السيبرانية وتصاعد المنافسة الدولية،على الموقع/ الكتروني،https://www.aljundi.ae

(20)عــادِل عبد الصادق ،القــوة الالكترونيــة :اسلِحة الانتشار الشامل في عصر الفضاءُ الالكتروني ،مجلة السياسةُ الدولية ،العدد 188 ،مؤسسة الأهرامْ ،مِصر ،2012،ص2.

(21)nicu popescu ,"russias soft power ambitions ,ceps ,policy. brief ,no ,115 ,(october , 2016) , p.p 11,12.

(22) سكوت بوسطن ، داور ماسكويت ،" الطريقةُ الروسيةُ في الحرب "، مؤسسةُ راند للدراسات ،(2017)، ص7.

(23) عادل عبد الصادق، مصدر سبق ذكره ، ص 32.

(24) سكوت بوسطن، وداور ماسكويت، مصدر سبق ذكره ، ص7.

(25) إيهاب خليفة ،الحربُ السيبرانية مُراجعة العقيدة العسكرية استعداداً للمعركة القادمة ،مجلةُ السياسة الدولية ،العدد 211،مصر، 2018،ص20.

(26) نوران شفيق ،اثر التهديدات الالكترونية على العلاقات الدولية دراسة في ابعاد الامن الالكتروني،(القاهرة ،المكتب العربي للمعارف ،2018)،ص 141.

(27)عادل عبد الصادق،انماط الحرب السيبرانية وتداعياتها على الامن العالمي،مجلة السياسة الدولية ،العدد 208،المجلد 52،مصر،ابريل 2017،ص34.

(28) ليوبوف ستيبوشوفا ،روسيا تُؤثِر على مصير 24 بلد في العالم مركز نون بوست ،المقال منشور بتاريخ : (15/1/2017 على الــــرابِط : www.noonpost.org//content

29 https://www.annabaa.org/arabic/informatics/30480

اماني عصام استخدام روسيا للقوة السيبرانية فى إدارة تفاعلاتها الدولية،على الموقع الالكتروني [30]https://jpsa.journals.ekb.eg/

إبراهيم سيف منشاوي ،دمج القدرات السيبرانية في تقرير التوازن العسكري ،مركز المستقبل، كلية الاقتصاد والعلوم السياسية – جامعة القاهرة ، آذار2021. [31]

([32]) سكـوتْ وارينْ هارولد، وآخرون، التوصلْ الى اتِفاق مع الصين بِشأن الفضَاءُ الإلكتروني، تقارير مؤسسة راند ،2016،ص ص8-9.

([33]) إبراهيم سيف منشاوي ،مصدر سبق ذكره

(34)thomas rid, (november / december 2013). cyberwar & peace: hacking can reduce real world violence, foreign affairs, vol. 92, no. 6.

([35]) غريب حكيم وشرقي صبرينه ،تداعيات الحرب الإلكترونية على العلاقات الدولية:دراسة في الهجوم الإلكتروني على إيران (فيروس ستكنست)،دفاتر السياسة والقانون،المجلد 12 ،العدد 2،الجزائر،2020،ص92-107.

([36]) قُدرات القرصنة السيبرانية الإيرانية ، " تقـريـــر خاص ،مركز الملك فيصل للدِراسات والبحوث ،كَانون الأول 2020 ،ص10.

([37]) رغدة البهى ،الوكالة السيبرانية: عوامل النشاة وانماط التفاعل، ملحق بعنوان اتجاهات نظرية ،مجلة السياسة الدولية،مركز الاهرام –القاهرة،العدد 218،تشرين الاول 2018،ص16.

[38] حسن مظفر الرزو، التهديد السيبراني الايراني الملف المضاف إلى برنامجها النووي ،(برلين :المركز الديمقراطي العربي للدراسات الاستراتيجية والاقتصادية والسياسية) 2020 ، ص151

([39]) مُحمد مختار ، "الأمنُ السِيبراني مَفاهيمُ المستقبل" ، إتجـــاهاتْ الأحداث ، العدد6 ،2015، ص6.

([40]) فيصلْ مُحمد عبد الغفار ،الحربُ الإلكترونية ،ط1،(الأردنْ :الجنادرية للنشر والتوزيع،2015)،ص162.

([41]) شكر عمر حامد، المجال الخامس- الفضاء الإلكتروني،(القاهرة: المعهد المصري للدراسات)، 2010 ، ص11.

المصادر

اولا:الكتب

محمد سيد ريان،الإعلام الجديد،ط1،(القاهرة،مركز الأهرام للنشروالترجمة والتوزيع،2012)

-جيمس دورت وروبرت بالستغراف، النظريات المتضاربة في العلاقات الدولية (ترجمة: وليد عبد الحي)،ط (1 بيروت: مكتبة شركة كاظمة للنشر والترجمة) 1995

جوزيف س.ناي ،القوة الناعمة وسيلة النجاح في السياسة الدولية(ترجمة : محمد توفيق البجيرمي) ،(الرياض : العبيكان للنشر)،2007

-نوران شفيق ،اثر التهديدات الالكترونية على العلاقات الدولية دراسة في ابعاد الامن الالكتروني،(القاهرة ،المكتب العربي للمعارف ،2018)

حسن مظفر الرزو، التهديد السيبراني الايراني الملف المضاف إلى برنامجها النووي ،)برلين: المركز الديمقراطي العربي للدراسات الاستراتيجية والاقتصادية والسياسية 2020

فيصل محمد عبد الغفار،الحرب الالكترونية،ط1،(الاردن:الجنادرية للنشر والتوزيع،2015)

شكر عمر حامد، المجال الخامس- الفضاء الإلكتروني،(القاهرة: المعهد المصري للدراسات)، 2010

ثانيا :المجلات والدوريات

1-هربرت لين ،النزاع السيبراني والقانون الدولي الإنساني ،مختارات من المجلة الدولية للصليب الأحمر ، مجلد/ 94 (886) صيف 2012.

2- محمد مختار،"هل يمكن للدول أن تتجنب مخاطر الهجمات الالكترونية؟"، مفاهيم المستقبل، العدد6 ، مركز المستقبل للأبحاث والتطوير،2015

3-إسماعيل قادير"إدارة الحروب النفسية في الفضاء الإلكتروني: الإستراتيجية الأمريكية الجديدة في الشرق الأوسط" .عولمة الإعلام السياسي وأثرها على الأمن القومي للدول النامية ،(كلية الحقوق والعلوم السياسية : قسم العلوم السياسية)

4-لطفي امين بلفرد ،الفضاء السيبراني:هندسة وفواعل،المجلة الجزائرية للدراسات السياسية،الجزائر، العدد 5، ،حزيران-2016.

5- اسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع ،مجلة العلوم القانونية والسياسية، المجلد 10 ،العدد 1، جامعة محمد بو ضياف المسيلة ،الجزائر ، افريل 2019.

6-سكوت بوسطن، وداور ماسكويت،" الطريقة الروسية في الحرب"، مؤسسة راندا للدراسات، (2017)

7-ايهاب خليفة،الحرب السيبرانية مراجعة العقيدة العسكرية استعدادا للمعركة القادمة،مجلةالسياسة الدولية ،العدد 211، يناير 2018،ص20.

8-علاء الدين فرحات،الفضاء السيبراني :تشكيل ساحة المعركة في القرن الحادي والعشرين،مجلة العلوم القانونية والسياسية ،المجلد10،العدد3،ديسمبر 2019.

9- سكوت وارين هارولد وآخرون، التوصل إلى اتفاق مع الصين بشأن الفضاء الالكتروني، تقارير مؤسسة راند 2016،

10- إبراهيم سيف منشاوي ،دمج القدرات السيبرانية في تقرير التوازن العسكري ،مركز المستقبل، كلية الاقتصاد والعلوم السياسية – جامعة القاهرة ، مارس آذار2021.

11- لطفي أمين بلفرد، "التهديدات الأمنية في الفضاء السيبراني" ، أقلام شرطية ، العدد129،(الجزائر) ، ديسمبر2015

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

13- غريب حكيم وشرقي صبرينه ،تداعيات الحرب الإلكترونية على العلاقات الدولية:دراسة في الهجوم الإلكتروني على إيران (فيروس ستكنست)، دفاتر السياسة والقانون،المجلد 12 العدد 2،الجزائر،1،6 ،2020

14-قدرات القرصنة السيبرانية الإيرانية"،تقرير خاص،مركز الملك فيصل للدراسات والبحوث ،كانون الأول 2020،ص10.

15-رغدة البهى ،الوكالة السيبرانية: عوامل النشاة وانماط التفاعل، ملحق بعنوان اتجاهات نظرية ،مجلة السياسة الدولية،مركز الاهرام –القاهرة،العدد 218،تشرين الاول 2018،ص16.

16-محمد مختار،"الأمن السيبراني مفاهيم المستقبل"، إتجاهات الأحداث ، العدد6 ،2015

الرسائل والاطاريح

1- فاطمة عوامر، تأثير القوة السيبرانية على الإستراتيجيات الأمنية للدول الكبرى دراسة حالة – الصين، رسالة ماجستير غير منشورة،جامعة قاصدي مرباح ورقلة :كلية الحقوق والعلوم السياسية،2018.

الانترنيت

1-محمد عصمان ، "دور المنظمات غير الحكومية في حماية حقوق الإنسان "،19-12-2017،على الموقع: http://www.pointjuridique.com/2017/02/19/%D8%AF%D9%88/?print=pdfامعة قاصدي مرباح : ورقلة)،2017

2-منى الأشقر جبور ، السيبرانية هاجس العصر (دم : دت) ، ص66 ، على الموقع:
https://www.carjj.org/sites/default/files/ebooks/cyber.ebook.pdf

3-ليوبوف ستيبوشوفا،روسيا تؤثر على مصير24 بلد في العالم ، مركز نون بوست،مقال منشور بتاريخ : (15/1/2017) على الرابط : www.noonpost.org/content/

المصادر الاجنبية

.1-Thomas Rid, (November / December 2013). Cyberwar & Peace: Hacking Can Reduce Real World Violence, Foreign Affairs, Vol. 92, No. 6.

2-Joseph S.Nye JR , Cyber Power, Harvard Kennedy School, 2010

3-NICU POPESCU , "Russias soft power ambitions , CEPS ,POLICY. brief,no,115, (October , 2016)

4-Department of Defense Cyber Stratigy, Department of Defense, April 2015, p 2. Book online, available from https://goo.gl/g4hpuA,(New York:2010)