مجلة تكريت للعلوم السياسية

اسم المقال: مطارحات هيمنة الاستراتيجية الأمريكية السيبرانية
اسم الكاتب: عبد الكريم زهير عطية الشمري، أ.م.د. حازم موسى الجنابي
رابط ثابت: https://political-encyclopedia.org/index.php/library/7760
تاريخ الاسترداد: 2026/11/02 14:07 +03

الموسوعة السياسيّة هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.
لمزيد من المعلومات حول الموسوعة السياسيّة - Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة - Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من موقع مجلة تكريت للعلوم السياسية جامعة تكريت ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

TJFPS

IRAQI Academic Scientific Journals

العراقية المجلات الاكاديمية العلمية

Contents lists available at Academic Scientific Journal
http://www.iasj.net

Tikrit Journal for Political Science



مطارحات هيمنة الاستراتيجية الأمريكية السيبرانية

Proposals for the Hegemony of US Cyber Strategy

Researcher: AbdEl-Kareem Zuhair Atiya Alshmari

Asst. Prof. Hazim Hamad Mousa aljanabi

الباحث: عبد الكريم زهير عطية الشمري (*)

جامعة الموصل / كلية العلوم السياسية

أ.م.د.حازم حمد موسى الجنابي

جامعة الموصل / كلية العلوم السياسية

A r t i c l e i n f o.

Article history:
- Received 2 April 2021
- Accepted 25 April 2021
- Available online: 30 June 2021

Keywords:
- US strategy
- Hegemon
- Cyberspace
- China
-Russia
- Iran
-North Korea

Abstract: The present study concentrates on the proposals for the strategy of the USA hegemony on cyberspace and the rejection of cyber hegemony by both the international and regional strategies. As a result, the interaction and the importance increased and we want to find an answer to the essential following questioning: Is it possible for the US strategy to dominate cyberspace without any rejection or argument with international and regional powers? Therefore, light has been shed on the present problem concerning the dynamic relationship between the US strategy and the interconnected international and regional strategies which might cause real conflict and collision. In order to find a solution for this problem, we have adopted the following hypothesis: The more US hegemony of the cyberspace increases, the more intense the arguments with international and regional strategies increase. In order to achieve a future vision for the conflicting US strategy internationally and regionally the analytical approach has been used. This approach analyzes the US cyber strategic paths in cyberspace and the consequences of cyberspace hegemony invoked in this study taking into consideration the arguments and the proposals in this study besides the most important regional and international cyber strategies.

(*)**Corresponding Author**: Researcher: AbdEl-Kareem Zuhair Atiya Alshmari , **E-Mail**: **Email**: sonse1992@yahoo.com ، **Tel**: **00964.7518582981** ,College of Political Sciences, University of Mosul

:.

معلومات البحث:

تواريخ البحث:

الاستلام: 2\04\2020

القبول: 25\04\2020

النشر : 30\6\2021

الكلمات المفتاحية:

– الاستراتيجية الأمريكية

– الهيمنة

– الفضاء السيبرني

– الصين

–روسيا

–ايران

–كوريا الشمالية

الملخص: يركز البحث على مطارحات الاستراتيجية الأمريكية للهيمنة على الفضاء السيبراني، وما يقابل ذلك من رفض للهيمنة السيبرانية من قبل الاستراتيجيات الدولية والإقليمية، فأزادا التفاعل وازدادت الأهمية، ويجيب عن التساؤل الأساسي الآتي: هل يمكن للاستراتيجية الأمريكية الهيمنة على الفضاء السيبراني دون مطارحات مع القوى الدولية والإقليمية؟ فسلطنا الأضواء على الإشكالية الدائر فيما يتعلق بالعلاقة الحراكية بين الاستراتيجية الأمريكية والاستراتيجيات الدولية والإقليمية المتداخلة التي تفضي إلى التداخل والتصادم؟ ولحل هذا الإشكالية تم تبني الفرضية الأتية" كلما ازدادت حراكات الهيمنة الأمريكية على الفضاء السيبراني ازدادت شدة التطارحات مع الاستراتيجيات الدولية والإقليمية"، وبهدف بناء رؤية مستقبلية للاستراتيجية الأمريكية المتصارعة دولياً وإقليمياً، وتحقيقاً استخدمنا المنهج التحليلي الذي يركز على تحليل مسارات الاستراتيجية الأمريكية السيبرانية في الفضاء السيبراني ومآلات التطارح التي يثيرها موضوع البحث، والتطرق إلى اهم الاستراتيجيات السيبرانية الإقليمية والدولية.

*بحث مستل من رسالة الماجستير المعنونة : الاستراتيجية الأمريكية للهيمنة على الفضاء السيبراني للطالب عبد الكريم زهيرعطية الشمري، بإشراف ا.م.د.حازم حمد موسى الجنابي، كلية العلوم السياسية، جامعة الموصل، 2020.

المقدمة:

إن نتيجة التطور التقني الإلكتروني الهائل في معظم الدول المتطورة الكبرى وفي مقدمتها الولايات المتحدة الأمريكية وروسيا الاتحادية والصين، أدى هذا التطور إلى بزوغ نوع أخر من الصراع والتطارح على الصعيد العالمي بعيداً عن استخدام الاستراتيجيات التقليدية في القرن العشرين وما تلاه، فظهور استراتيجية القوة السيبرانية كإحدى اعتى وسائل استراتيجيات الدول المتقدمة اثر بشكل كبير على الساحة الدولية وظهر بوصفه أحد حقول الاستراتيجية واحد فروع الاستراتيجية الشاملة، ونتيجة لذلك وفي غياب الرقابة القانونية على حرب المعلومات لذي حطم الكثير من وحدات الحماية الاستراتيجية للدول، ظهرت المطارحات بين الدول وفق أنماط عدة منها، التأثير المباشر والتأثير غير مباشر، فالمتتبع للشأن الدولي والاستراتيجيات السيبرانية يلحظ الكثير من الصراعات العالمية بدون خيوط للجريمة تذكر ولا يوجد دليل مادي على الهجمات السيبرانية، إن امتلاك القوة السيبرانية لم ينحصر بالدول الكبرى، بل تعدى ذلك، إذ إن دول إقليمية امتلكت هذه الاستراتيجية أمثال ايران وكوريا الشمالية وحقت نتائج هائلة في المقابل أعدت نفسها قوة منازعة للولايات المتحدة الأمريكية، أما فيما يخص الدول الكبرى أمثال الصين وروسيا الاتحادية والتي تمتلك بنية تحتية سيبرانية متطورة فهي عملت على إثارة نوع من الفوضى داخل النظام الدولي، بل وساهمت في تعزيز استراتيجياتها العامة، كما وأثرت في استراتيجيات الكثير من الدول الحليفة وغير الحليفة، عن طريق أدواتها وجيوشها السيبرانية، فنلحظ ظهور روسيا الاتحادية لاعب دولي سيبراني محترف اثر حتى في الداخل الأمريكي الذي يعد نفسه الأكثر احترافاً سيبرانياً، ففي العام 2016عندما تم انتخاب الرئيس الجديد دونالد ترامب رئيساً للولايات المتحدة الأمريكية، ظهرت الاستراتيجية السيبرانية على الساحة الدولية لتطغى على الفروع الاستراتيجية الأخرى وفق نمط الهيمنة الذي تحاول الولايات المتحدة الأمريكية فرضه ضد الدول الأخرى، وهذا ولد مطارحات على الساحتين الدولية والإقليمية في محاولة إلى كسر قيود الهيمنة الاستراتيجية الأمريكية، وقبل التفصيل لابد أن نذكر بعض المفردات لتكون لنا دليلاً في البحث، ولعل أهمها:

أولاً: الأهمية: تنبع من المكانة التي حظي بها الفضاء السيبراني في مطارحات الاستراتيجية الأمريكية، وما يقابل ذلك من رفض للهيمنة السيبرانية من قبل الاستراتيجيات الدولية والإقليمية، فأزادا التفاعل وازدادت الأهمية بفعل الانعكاسات الكبيرة على النظام الدولي.

ثانياً: الهدف: بناء رؤية مستقبلية للاستراتيجية الأمريكية المتصارعة دولياً وإقليمياً تفصح عن مستقبل الهيمنة الأمريكية.

ثالثاً: الإشكالية: سلطنا الأضواء على الإشكالية الدائر فيما يتعلق بالعلاقة الحراكية بين الاستراتيجية الأمريكية والاستراتيجيات الدولية والإقليمية المتداخلة التي تفضي إلى التحالف أو التصادم؟

رابعاً: تساؤلات: ينطرح تساؤل أساس هو: هل يمكن للاستراتيجية الأمريكية الهيمنة على الفضاء السيبراني دون مطارحات مع القوى الدولية والإقليمية؟ لتتفرع منه عدة أسئلة فرعية منها: ما هو موقف الاستراتيجيات الدولية من الهيمنة الأمريكية على الفضاء السيبراني؟ ما هو موقف الاستراتيجيات الإقليمية من الهيمنة الأمريكية على الفضاء السيبراني؟ وما هي انعكاسات المنافسة على الهيمنة السيبرانية على النظام الدولي؟

خامساً: الفرضية: تم تبني الفرضية الأتية" كلما ازدادت حراكات الهيمنة الأمريكية على الفضاء السيبراني ازدادت شدة التطارحات التصارعية مع الاستراتيجيات الدولية والإقليمية لرفض الهيمنة سيبرانياً".

سادساً: النطاق : تحدد البحث زمانياً في حقبة الرئيسين "باراك اوباما"، "دونالد ترامب"، ومكانياً : شمل الساحتين الدولية والإقليمية مُركز على الاستراتيجيات الفاعلة في الفضاء السيبراني بالتركيز الاستراتيجية الأمريكية السيبرانية على ابرز قوتين دولياً وإقليمياً.

سابعاً : تعريف المفاهيم والمصطلحات: من المتعارف عليه إن الدراسات والأبحاث تتطلب التعريف بالمفاهيم والمصطلحات لتحديد دلالاتها؛ وهذا ما حثنا إلى تعريف مصطلحات البحث وعلى النحو الاتي:

1.المطارحات: جاءت من مصدر تطارح، بمعنى تصارع في الأفكار والأفعال لإظهار الأقوى، فتطارحوا القوة تناظروا فيها وتناوروا لإثبات الأقوى، والمطارحات بين الدول هي التصارعات الفكرية والأدائية بين النظراء الأنداد –الأضداد لإبعادهم أو لإقصائهم من المكانة والدور، فالمطارحات الأمريكية جاءت بدلالة الأبعاد والإقصاء للقوى الدولية الكبرى الراغبة بالمنافسة على الهيمنة، والإقليمية الرافضة للهيمنة.

2.الهيمنـة: هـي كلمـة يونانيـة(Hegemonia) ، تعنـي الحكـم أو الأمـر، وفـي اللغـة الإنكليزيـة (Hegemony) تعني السيطرة على الأخرين، والهيمنة الأمريكية تعني سيطرة الولايات المتحدة الأمريكية على الدول جيوسياسياً وجيواستراتيجياً.

2. الفضاء السيبراني: هي مصطلح إنكليزي (Cyberspace) متكون من شقين (Cyber) و(Space)، الاول : سايبر يعني والثاني يعني سبيس ، فهو الحيزّ الافتراضي الذي تتم من خلاله وفيه مُجمل الأنشطة الرقمية–المعلوماتية.

ثامناً: المنهجية: استخدمنا المنهجان التاريخي والتحليلي، الأول يركز على بدايات الصراعات السيبرانية دولياً وإقليمياً والثاني يركز على تحليل مسارات الاستراتيجية الأمريكية السيبرانية في الفضاء السيبراني ومآلات التطارح الصراعية، التي يثيرها موضوع البحث، والتطرق إلى اهم الاستراتيجيات السيبرانية الإقليمية والدولية.

ثامناً: الهيكلية: اعتمدنا في خطة البحث (مقدمة ومبحثين وخاتمة ونتائج)، وعلى النحو الاتي : المبحث الأول: اختص بـ" الاستراتيجيات الدولية الكبرى المتطارحة مع الاستراتيجية الأمريكية سيبرانياً "، وجاء المبحث الثاني ليدرس: "الاستراتيجيات الإقليمية المتطارحة مع الاستراتيجية الأمريكية سيبرانياً"، لنختم البحث بجملة من النتائج.

المبحث الأول : الاستراتيجيات الدولية الكبرى المتطارحة مع الاستراتيجية الأمريكية سيبرانياً

، أدت الاستراتيجيات التقليدية دورها في الحرب الباردة وما قبلها من مراحل صراع وتنافس وصولاً إلى العصر الرقمي الذي افرز نوع من التطارح بين الدول الكبرى والولايات المتحدة الأمريكية ومراكز النفوذ الذي أفرزته القوة السيبرانية احد ابرز معالم القوة في القرن الواحد والعشرون برزت الصين وروسيا احد اهم الدول تطوراً واستخداماً للاستراتيجية السيبرانية في المنافسة الدولية والتطارح الدولي مع الولايات المتحدة الأمريكية، إذ كانت الاستخدامات كبيرة جداً وناجعة للحد من النفوذ الأمريكي العالمي ومحاولة الدول الكبرى إعادة ترتيب النظام الدولي وفق نهج جديد مبني على الاستفادة من تطورات الاستراتيجيات الحديثة وبعيداً عن الاستراتيجيات التقليدية، استخدمت المطارحات السيبرانية في مكامن عدة ذات علاقة بالعالم الرقمي، إذ كان لها الريادة في تغيير الكثير من الاهتمامات ذات الطابعين والإقليمي الدولي، فظهرت ملامح التصارع في الفضاء السيبراني بين الاستراتيجيات.

المطلب الأول: المطارحات الاستراتيجية الروسية –الأمريكية السيبرانية

يركز هذا المطلب على وضع الاستراتيجية الروسية وتطارحها مع الولايات المتحدة الأمريكية وصولاً إلى تقييم الأداء التفاعلي الروسي– الأمريكي سيبرانياً ذلك الأداء المحمل بالأحداث غير المتوقعة [1] ، الذي ابدع فيه الاستراتيجيون المخططون [2]، وبما إن التنوع الاستراتيجي هو السمة البارزة في استراتيجيات الدول الكبرى ففي خضم التحولات الدولية والاستراتيجية التي حدث في عام 1990 من تفكك الاتحاد السوفييتي وتربع الولايات المتحدة الأمريكية على قمة النظام الدولي[3]، أدت إلى التغيير في المفاهيم الاستراتيجية والتحول من الاعتماد المادي على الاستراتيجيات العسكرية إلى بزوغ فكر استراتيجي جديد يوظف تلك التحولات ومنها تحول الفكر الاستراتيجي العالمي من استخدام استراتيجية القوة التقليدية إلى استراتيجية القوة الناعمة والتي يرجع الفضل في ابتكارها إلى المفكر الاستراتيجي الأمريكي "جوزيف ناي" في عام 1990 الذي انتقل بالفكر الاستراتيجي الأمريكي والعالمي من استراتيجية القوة التقليدية إلى استراتيجية القوة الناعمة (الثقافية، الانجذاب العالمي، الإعلام، الدبلوماسية) وانتقالها وتطورها فيما بعد إلى القوة" الذكية إذ يعرف هذا المفهوم جوزيف ناي على انه" يقوم على الدمج والتفاعل بين القوة الصلبة والقوة الناعمة " ينتج لنا القوة الذكية تقوم على استخدام الوسائل الدبلوماسية والأعلام والقوة التقنية في رسم وتنفيذ استراتيجيات الدول الكبرى حول العالم[4] .إن الالتفاتة الروسية لاستراتيجية القوة الناعمة ظهر بشكل حقيقي حيث تم استخدام مصطلح "القوة الناعمة" لأول مرة في الخطاب الرسمي للدولة الروسية للرئيس الروسي "فلادمير بوتين " عام 2009، أمام مجلس الدوما، والذي حدد ان امتلاك روسيا للقوة الناعمة يهدف الى استعادة روسيا دورها العالمي ، والاستخدام الامثل وتهيئة الوسائل الفنية [5].

---

[1] نسيم طالب، *البجعة السوداء تداعيات الأحداث غير المتوقعة*، (بيروت: الدار العربية للعلوم ناشرون، 2009)، ص ص 9 -10.

[2]هاري أربارغر، *الاستراتيجية ومحترفو الأمن القومي التفكير الاستراتيجي وصياغة الاستراتيجية في القرن الحادي والعشرين*، ترجمة: محرز علي راجح ، (الإمارات: مركز الإمارات للدراسات والبحوث الاستراتيجية، 2011 ،(ص ص16-17.

[3]جهاد عودة، *النظام الدولي نظريات وإشكاليات*، (مصر: دار الهدى للنشر والتوزيع ،2005)، ص ص 21 - 22.

[4] جوزيف ناي، "مستقبل القوة"، حوار مع مجلة المجلة، عدد5، (سبتمبر 2011) .

[5]Nicu Popescu, "Russia's Soft Power Ambitions", *CEPS, policy brief*, No.115, (October 2006), PP. 11-12.

كما حصر الرئيس الروسي إجراءات وسياسات بلاده لاستخدام القوة الناعمة في الحفاظ على ثقافتها واستغلالها على نحو يجعل منها قوة فاعلة لتحقيق تقدم ملموس في الأسواق الدولية، وتحقيق تقدم ثقافي يرتكز على تصدير التعليم والثقافة الروسية للخارج، بما يخدم مصالح روسيا وأفكارها ومنتجاتها أيضا[1]، وفي الأول من ديسمبر 2011، نشر موقع وزارة الخارجية الروسية وثيقة رئاسية بتوقيع الرئيس فلاديمير بوتين، تتناول مفهوم السياسة الخارجية للدولة وأدواتها"، وجاء في بلدها التاسع (من أصل 108 بنود احتوت عليها الوثيقة) أن القوة الناعمة أصبحت جزءاً لا يتجزأ من الجهود المبذولة لتحقيق أهداف السياسة الخارجي[2].

وذكر وزير الخارجية الروسي الأسبق (سيرغي لافروف) مقال في عام 2009 على تبني بلادة استراتيجية القوة الناعمة والذكية واستخدامها بما يعيد ويضمن هيبة روسيا العالمية، عبر قوة جذب المجتمع المدني والمنظمات غير الحكومية ، كما حذر من استخدام استراتيجية القوة الناعمة في التدخل في سياسيات الدول ذات السيادة[3].

ومن تطبيقات القوة الناعمة قيام الجهات الرسمية وغير الرسمية في تطوير القوة الناعمة والذكية الاهتمام بالإعلام المرئي وتطوير القناة التلفزيونية "RT" التي كانت فيما مضى باسم قناة روسيا اليوم، إذ قامت بإضافة نسخ ناطقة بعدة لغات (العربية، الإنكليزية، الفرنسية) ، وأصبحت من كبرى الشبكات التلفزيونية العالمية وتغطي مساحات شاسعة من العالم، واتهمتها الولايات المتحدة الأمريكية بانها بوق السلطة الروسية ورئيسها بوتين، كما أنشأت المراكز الثقافية والعلمية في كثير من أرجا العالم، كما قامت بترجمة الكثير من الكتب والروايات، كما فعلت البرامج التعليمة وقدمت تسهيلات عالمية للذين يرومون الدخول في الجامعات الروسية [4]، وتشير الدوائر السياسية والاستخبارية الغربية إلى أن روسيا تستثمر شخصين اثنين، جوليان أسانج

---

(1) Andrew Radin & Clint Reach, “Russian Views Of The International Order,” *RAND Corporation*, (2017), PP. 5-7.

(2) Ulia Kiseleva,“Russia's Soft Power Discourse: Identity”, Status and the Attraction of Power, *Politic*,Vol. 35 ,No. 3-4, (2015), PP. 316-319.

(3) سيرجي لافروف، "العالم في مفترق طرق ونظام العلاقات الدولية في المستقبل"، *مجلة روسيا في الشؤون العالمية*، وموقع وزارة الخارجية الروسية، 20 أيلول/سبتمبر 2019.

(4) رضا محمد هلال،" أدوات وقيود القوة الناعمة الروسية"، *مجلة السياسة الدولية*، مج 55، عدد 218 ، (يناير 2020)، ص16.

وإدوارد سنودن لشن ما يسمونها الحرب الإلكترونية خدمة لأهدافها، وإحداث تغيرات سياسية في الأوساط الحاكمة بالولايات المتحدة وأوروبا، وعرفت بـ"عقيدة جيراسيموف The Gerasimov doctrine"، وهذه العقيدة تنطوي على مجموعة من الأفكار بشأن الأدوات غير التقليدية في الحروب الراهنة، والتي تتضمن أدوات مختلفة من بينها المعلومات، سواء من خلال الفضاء الإعلامي أو الفضاء الإلكتروني، واستهداف نقاط الضعف للخصوم، وتجنب المواجهة العلنية حتى المراحل النهائية للصراع. [1].

وفيما يتعلق بالاستراتيجية الرقمية(Digital Power) إذ تطورت الاستراتيجية الروسية الذكية الى الرقمية، فذكر وزير الاتصالات والتنمية الروسي " كونستانتين، نوسكوف " أن التطور الرقمي الروسي حقق طفرة نوعية تطارح الاستراتيجيات الرقمية العالمية، إذ إن محركات البحث الروسية تضاهي محركات البحث والتواصل الاجتماعي (جوجل، وفيسبوك) وان روسيا الاتحادية مستمرة بالتحديثات الرقمية للدجتل الروسي"[2].

وبحسب آخر تقرير لمؤسسة البيانات الدولية (International Data Corporation) فإن روسيا تجاوزت المملكة المتحدة والبرازيل بوصفها ثالث أكبر سوق للكتب الإلكترونية الرقمية في العالم، إلى جانب الولايات المتحدة والصين اللتين تحتلان المراتب الأولى. وخلال السنوات الأخيرة فقد حظيت الكتب الإلكترونية في روسيا بإقبال كبير من المستخدمين بنسبة وصلت إلى 25% والجدير بالذكر أن الكتب الروسية الرقمية لا تمثل إلا 1% من مجموع الكتب باللغات الأخرى، وقيل إن تزداد نسبة الكتب الروسية من مجموع الكتب الأخرى في سوق الكتاب الإلكتروني يصل إلى نسبة 5% في عام 2017 أي ما قيمته 3 بليون روبل روسي (90مليون دولار أمريكي)[3].

ففي خضم التطورات الدولية والتنافس الدولي اتجهت معظم الدول ذات القدرة السيبرانية ومنها روسيا الاتحادية التي تتميز بالقدرة الهائلة في هذا المجال ففي نهاية عام 2011 صدر

---

[1] محمد بسوني ، "عقيدة جيراسيموف: دوافع الاستراتيجية الروسية لحرب المعلومات ضد الدول الغربية"، مركز *المستقبل للأبحاث والدراسات المتقدمة*، (أكتوبر 2017)، ص5.

[2] كونستانتين نوسكوف، وزير الاتصالات الروسي، تصريح صحفي، بوابة الأهرام، شوهد بتاريخ 16 /5/ 2020 على الرابط: http://gate.ahram.org.eg/News/2155154.aspx .

[3] سوفان مندال، *روسيا تبرز كثالث اكبر سوق للكتب الإلكترونية في العالم*، ترجمة: المكتبة الرقمية السعودية، (السعودية: المكتبة الرقمية السعودية،2017)، ص3.

أول بيان رسمي حول مهام الاستراتيجية الروسية في الفضاء السيبراني [1]، وصدرت في عام 2012 وثيقة وزارة الدفاع الروسية "مفهوم الأنشطة الفضائية للمعلوماتية للقوات المسلحة بالاتحاد الروسي" The Russian Federation Armed Forces' Information Space Activities Concep لتعد تلك الوثيقة المسار الحقيقي الذي تمثله المعلومات والاستراتيجية السيبرانية في الإطار الاستراتيجي الروسي العام وتبنت الوثيقة تعريف فضاء المعلومات بأنه "مجال النشاط المتصل بتشكيل المعلومات ونقلها واستخدامها وتخزينها، مما يؤثر على الوعي الفردي والمجتمعي، فضلًا عن المعلومات في معناها الضيق، وكذلك الهياكل الأساسية للمعلومات[2].

ومن ابرز منظري الاستراتيجية الروسية السيبرانية "جيراسيموف*" الذي يعد سلاح الرئيس بوتين تجاه الغرب ، فاصدر نظريته تحت مسمى "عقيدة جيراسيموف للاستراتيجية الروسية السيبرانية" والتي أصدرها عام 2013 ويقول فيها: ((في العالم المعاصر تبدو الخطوط بين الحرب والسلام غير واضحة وغالباً ما تكون الصراعات غامضة غير معروفة المصدر فمهما بلغ حجم القوات التي يملكها العدو، ومهما بلغت درجة تطور قواته ووسائله الحربية، من الممكن إيجاد السبل والأدوات اللازمة للتغلب عليه، إذ سيكون دوماً لدى الخصم نقاط ضعف، وذلك يعني البحث عن وسائل مناسبة لمحاربته))[3].

ويختلف المنظور الروسي للاستراتيجية السيبرانية بشكل واضح عن المنظور الأمريكي والغربي، فالاستراتيجيون الروس مقتنعون بأن روسيا الاتحادية أمام صراع وجودي مستمر، فتسعى إلى تحصين أمنها في عالم المعلومات، ويرون في الإنترنت والتدفق الحر للمعلومات التي يولّدها إنها تشكّل فرصة لا تهديد، إذ عدها فرصة سانحة لبناء منظومتها الاستراتيجية العالمية، كما انهم يصورون العمليات السيبرانية ضمن الإطار الأوسع للاستراتيجية السيبرانية

---

[1] عبد الغفار الدويك، "تقرير التوازن العسكري 2019 قراءة تحليلية للقدرات السيبرانية في العالم"، *مجلة السياسة الدولية*، مج 54، عدد216، (أبريل 2019)، ص276.

[2] محمد بسيوني، "دوافع الاستراتيجية الروسية لحرب المعلومات ضد الدول الغربية"، مصدر سبق ذكره، ص4.

[3]Eugene Rumer, "The Primakov (Not Gerasimov) Doctrine in Action", *Carnegie Endowment for International Peace*,(2019),P.12.

*رئيس هيئة اركان الجيش الروسي ومسؤول ما يعرف بالحرب المعلوماتية الهجينة في ادارة الرئيس فلادمير بوتين.

والذي هو عبارة عن مفهوم شامل يتضمن عمليات شبكة الحاسوب والحرب الإلكترونية والأمن المعلوماتي والاستخباراتي والعمليات النفسية وعمليات المعلومات، وغيرها [1].

ولهذا الغرض روسيا الاتحادية أسست "وكالة أبحاث الأنترنت"، أو ما يُعرف باسم "جيش المتصيدين"(Troll Army)، تابع لوكالة الأمن الاتحادي الروسي، يضم آلاف الموظفين، ويخصص له سنوياً نحو(300) مليون دولار من ميزانية الدفاع، إذ يعد الجيش الإلكتروني الروسي خامس اقوى جيوش العالم الإلكترونية بعد كل من: الولايات المتحدة والصين وبريطانيا وكوريا الشمالية على التوالي، وتتلخص مهمات الجيش الإلكتروني الروسي[2] .

1- القيام بعمليات التجسس على الخصوم وكبار المسؤولين في الدول.

2- شن الهجمات الإلكترونية التي تسبب الضرر للبنى التحتية والاقتصاد والمواقع الحكومية في الدول الأجنبية المعادية والدول ذات التطور السيبراني الكبير، وحروب المعلوماتية في وسائل الإعلام والشبكات الاجتماعية.

3- القيام بعمليات اختراق الحسابات والبريد الإلكتروني، وجهود لتحديد قيادة الخصم وأنظمة مراقبتها وتحييدها بالاعتماد على وسائل الاستراتيجية السيبرانية [3].

وظهرت سلسلة تطارحات روسية –أمريكية في الفضاء السيبراني حتى سجلت نقاط لصالح استراتيجية روسيا الاتحادية باختراق العمق الاستراتيجي الأمريكي في عام 2013، إذ تمكن خبراء من روس اخذ عينات وتصاميم سلاحاً الإليكترونياً طورته "وكالة الأمن القومي الأمريكي " مستغلين نقاط الضعف في "مايكروسوفت ويندوز" التي قامت بحفظ هذه التصاميم للسلاح هذا الأمر كان احد ابرز نقاط تطور الاستراتيجية السيبرانية الروسية بعد سلسلة من العمليات على المستوى الإقليمي والدولي [4]، واستمراراً للحرب السيبرانية ففي السابع من تشرين الثاني/ 2016، نشر موقع "ويكيليكس" آلاف الرسائل الإلكترونية المسربة من بريد مدير الحملة الانتخابية لهيلاري كلينتون، وكشفت الوثائق المسربة أن الأخيرة ألقت خطابات مقابل

---

[1]Keir Giles, "Russia's public stance on cyberspace issues", *Cyber Conflict* (CYCON), (2019),P.70.

[3] سكوت بوسطن، وداور ماسكويت، "الطريقة الروسية في الحرب"، *مؤسسة راند للدراسات*، (2017)، ص7.

[4]Neri Zilber ,"The Rise of the Cyber-Mercenaries, Foreign Policy Magazine", (September 2018),P.5.

أجر لصالح مؤسسات مالية في عدد من بلدان العالم، ليتم فورها استدعاء كلينتون من قبل مكتب التحقيقات الفيدرالي الأمريكي (FBI) في أوج الحملة الانتخابية للحزب الديموقراطي، وهو ما أظهرها أمام الصحافة والرأي العام في أمريكا "مرشحة رئاسية مرتشية" وغير جديرة بالتصويت ليكون بذلك ترجيح كفة "دونالد ترامب"،وهذه نقطة ثانية لصالح روسيا [1] ، ومع ازدياد حدة التطارح السيبراني والاتهامات المتبادلة بتوجيه هجمات سيبرانية على أهداف حيوية، مثل ما أثير حول مقالة صحيفة "نيويورك تايمز" الأمريكية التي نُشرت في 15 يونيو/ حزيران 2018، (إن الجيش الأمريكي السيبراني يحضر لعمليات القراصنة العسكريين بتنفيذ نشاط عسكري سيبراني ضد أهداف حيوية روسية في حال تدهورت العلاقات بين البلدين)[2].

وبعد سلسلة من التدخلات الأمريكية في مناطق طوقها الجيوبولتيكي اتجهت روسيا إلى مسار الاستراتيجية السيبرانية لتتطارح معها، فمنذ أبريل – مايو 2007 (الحرب الإلكترونية الأولى) واحداث التوتر الكبيرة لردة فعل روسيا الاتحادية من فعل إستونيا (نقل النصب التذكاري للحرب العالمية الثانية الروسية ومقابر الجنود الروس)، فما كان من روسيا إلا أن تنتقم بشنّ هجمة سيبرانية تسبّبت في حدوث عُطل مؤقت بخدمة الإنترنت في إستونيا، في هجوم يُعرف باسم "هجوم حجب الخدمة" أو "هجمات الحرمان من الخدمة " مُستهدِفة المكاتب الحكوميّة والمؤسّسات المالية، ما أدى إلى تشويش الاتصالات وحدوث ضجة دولية لهذا الحدث، وحروبها تتطور سيبرانياً [3].

والتطارح الروسي –الأمريكي السيبراني في جورجيا فتضمنت هجمات سيبرانية روسية عدة، إذ كان مصدرها حسب التقرير المستقل الذي أصدرته الولايات المتحدة الأمريكية ، أجهزة حاسوبية لمستخدمين من روسيا الاتحادية وكان الهدف منها هو ضرب منظومة المؤسسات

---

[1] إف. ستيفن لارابي، وأخرون، بعد الأزمة الأوكرانية أوجه الضعف الأوروبية جراء الضغوط الروسية،(سانتا مونيكا، كاليفورنيا: مؤسسة رند، 2017)، ص ص8–9.

[2] نورهان الشيخ، "موسكو وواشنطن صراع سيبراني" ، *جريدة الخليج*، مقال منشور بتاريخ 6/27 2019 على الرابط : http://www.alkhaleej.ae

[3] Bilyana Lilly& Joe Cheravitch, "The Past, Present, and Future of Russia's Cyber Strategy and Forces", *International Conference on Cyber Conflict*,(12 th 2020),PP.139–140.

الحكومية لجورجيا والتي كان على اثرها وأثناء حرب أوسيتا الجنوبية التي اجتاحتها روسيا في العام 2008، فضلاً عن الهجمات السيبرانية في منطقة البلطيق [1].

وفي عام وفي خضم التطارح الروسي–الأمريكي حول قضية القرم اطلقت روسيا سلسلة من الهجمات السيبرانية في محاول لتعطيل وتأخير نتائج الانتخابات الرئاسة الأوكرانية وقبل ساعات من بث نتائج الانتخابات أعلنت قناة روسيا الأولى إن المرشح اليميني المتطرف الموالي لروسيا "ديمترو ياروش" هو من فاز في حين إن النتائج الانتخابات الأوكرانية تعكس غير ذلك لكن الهدف من هذا الأمر هو تغذية الجمهور الروسي في اوكرانيا الذي يؤيد انفصال جزيرة القرم هذا المنحنى الجديد المصاحب للعملية العسكرية في القرم هو بمثابة الحرب السيبراني وجزء من الاستراتيجية الروسية السيبرانية للتأثير سيبرانياً على مناطق النفوذ في العالم[2].

ومن هذا كله يمكن القول: إن الاستراتيجية الروسية السيبرانية من الاستراتيجيات الدولية الكبرى التي تطارحت مع الولايات المتحدة الأمريكية وسجلت لها نقاط في الانتخابات الأمريكية، وكذلك حسبت لها الكثير من النقاط في الطوق الجيوبولتيكي، وهذا يعني إن الاستراتيجية الروسية لها وزنها في التوازن الاستراتيجي السيبراني الدولي.

المطلب الثاني: مطارحات الاستراتيجية الصينية–الأمريكية السيبرانية

حققت الصين صعوداً تكنلوجياً سلمياً وتوسعت في مناطق كبيرة ومساحات واسعة من العالم في هذا المطلب نبين الصعود وكيف حدث التطارح التقليدي والسيبراني مع الولايات المتحدة الأمريكية، فكان للمفكر الاستراتيجي الصيني" مين هونك هاو" الريادة في تبيان استراتيجية القوة الناعمة الصينية والتي يذكرها وفقا لمبدأ الكونفوشيوسي الذي نادى "بالتناغم والانسجام" فان الاستراتيجية الناعمة والذكية هي تتكون من الثقافة والمفاهيم والنموذج التنموي والأنظمة الدولية، وذكر الرئيس الصيني السابق" هو جين تاو" في تقريره المقدم إلى المؤتمر

---

[1] أندرو رادن، *الحرب الهجينة في منطقة البلطيق: التهديدات والاستجابات المحتملة*، (سانتا مونيكا، كاليفورنيا: مؤسسة راند، 2017)، ص ص6–8.

[2] ليوبوف ستيبوشوفا، روسيا تؤثر على مصير 24 بلد في العالم ، مركز *نون بوست*، مقال منشور بتاريخ 2017/01/15:على الرابط : www.noonpost.org/content/16194

الوطني السابع عشر للحزب الشيوعي الصيني عام 2007 "استراتيجية القوة الناعمة الصينية على إنها تعتمد على السلام في العالم، المصالحة مع تايوان وتسوية المشكلات الأزلية، وتقوية أواصر الانسجام داخل المجتمع الصيني وتقوية أواصر الربط الدولي عبر تدعيم المشاريع التنموية وهذا يعني الحاجة إلى الطاقة[1]، فالصين تشهد تحولات كبيرة في قوتها الناعمة[2]، فمن الجدير بالذكر فان استراتيجية القوة الناعمة ليست حديثة العهد للصينين، بل تم الإشارة لها في الكثير من الإرث الصيني الثقافي والسياسي والفلسفي على إدارة العلاقة بين الحاكم والمحكوم، وذكرت الكونفشوسية وعظمت العقل وذكرت إن الحاكم الناجح هو من يكسب العقل ويكسب مواطنية بالمحبة وليست بالقوة ، ففي العام 1992 ترجم الصينيون أطروحة القوة الناعمة لجوزيف ناي ، لكن كان الحذر من هذه الأطروحة والتوجه الأمريكي، وتطرق الرئيس الصيني الأسبق" جيانغ زيمن" في عام 2002 أثناء مؤتمر الحزب، إذ ذكر إن عالم اليوم يمتزج ما بين الثقافة والاقتصاد والسياسة[3]

تبلورت استراتيجية القوة الذكية والناعمة للصين في العام 2007 في عهد الرئيس السابق "هو جين تاو"، وتكثف في عام 2011 في عهد الرئيس "شي جين بينغ"، موجه نشاطاها بالضبط من الولايات المتحدة الأمريكية ومناطق نفوذها، تبلور الصين هذه الانطلاقات في مؤسسات مثل بنك التنمية الجديد (مشروع تنظمه الصين مع البرازيل وروسيا والهند وجنوب إفريقيا) وبنك الاستثمار الآسيوي في البنية التحتية ومنطقة التجارة الحرة لمنطقة آسيا–المحيط الهادي وهو ما سيكون تكملة لمجموعة من الهيئات الإقليمية التي قامت الصين بتأسيسها بالفعل في آسيا وإفريقيا والشرق الأوسط وأمريكا اللاتينية وأوروبا الوسطى والشرقية عن طريق هذه المؤسسات، تبنى الصين بدقة بنية بديلة للنظام الغربي ما بعد الحرب، وفقا لنظريتها في استخدام استراتيجية القوة الناعمة [4].

---

(1) عبد القادر دندن ، *الصعود الصيني والتحدي الطاقوي : الأبعاد والانعكاسات الإقليمية* ،(الأردن، مركز الكتاب الاكاديمي، 2016)، ص ص 104-105.

(2) جانغ يون لينغ، وآخرون، *الحزام والطريق وتحولات الدبلوماسية الصينية في القرن 21*، ترجمة: آية محمد الغازي، (مصر: دار صفصافة للنشر، 2017) ، ص205.

(3) كاظم هاشم نعمة، "القوة الناعمة الصينية والعرب"، *مجلة سياسات عربية*، عدد 26 ،(أيار/مايو2017)، ص29.

(4) حنين جابر، حرب المبادرات الاقتصادية ...الصين أمريكا صراع على الاستثمار والجغرافيا ، صحيفة الاتحاد برس، 24/9/ 2020. على الرابط : https://aletihadpress.com

وتدعم الصين مشاريعها في استراتيجية القوة الناعمة باستخدام المال التنموي للتوسع فهي أنفقت 50 مليار دولار لبنك الاستثمار الآسيوي في البنية التحتية، و41 مليار دولار لبنك التنمية الجديد، و40 مليار دولار للحزام الاقتصادي لطريق الحرير، و25 دولار لملاحة طريق الحرير، وتعهدت بكين كذلك باستثمار 1.25 ترليون دولار في جميع أنحاء العالم بحلول عام 2025 وهذا الحجم من الاستثمار لم يسبق له مثيل حتى في الحرب الباردة، لم تنفق الولايات المتحدة والاتحاد السوفياتي في أي مكان ما يقترب مما تنفقه الصين اليوم، وبجمعها معًا، تضيف هذه التعهدات الأخيرة من جانب الصين ما يصل إلى 1.41 ترليون دولار، من الواضح أن بكين تستخدم أقوى أداة في صندوق أدواتها للقوة الناعمة: المال، أينما يسافر الزعماء الصينيون بما في ذلك، زيارة الرئيس" شي جين بينغ" ورئيس الوزراء "لي كه تشيانغ" أكثر من 50 دولة في عام 2014– ووقعا اتفاقيات تجارية واستثمارية ضخمة وقدما العديد من القروض السخية ووزعا من حزم المساعدات الضخمة [1].

إن القوى الكبرى دائماً في محاولة لاستخدام الأصول المالية لشراء النفوذ وتشكيل أفعال الآخرين ، إذ إن الصين لا تختلف عن غيرها، لكن ما يلفت النظر بشأن الاستثمارات الصينية هو كيف تضمن له إنتاجية عالية، تتحدث الأفعال بصوت أعلى من الكلمات، وفي أجزاء كثيرة من العالم، يناقض سلوك الصين على الأرض خطابها اللطيف[2].

وفيما يتعلق بالاستراتيجية الرقمية المتطورة الصينية، فان الصين تعد من أوائل الدول المتقدمة التي حققت تقدماً تقنياً واستطاعت تحويل استراتيجياتها من الناعمة ثم الذكية والرقمية التي هي تعد مفتاح الصعود السلمي الصيني إذ إن تقدم التطورات الرقمية والأقمار الاصطناعية في الصين فرصًا وتحديات إقليمية جديدة للولايات المتحدة في مواجهة النفوذ الرقمي المتطور في منطقة الشرق الأوسط.

ففي شهر يونيو 2020، أكملت الصين سعيها لتصبح قوة فضائية رقمية، بعد أن تم، بعد اطلاق القمر الصناعي تقديم شبكة الملاحة الساتلية (BeiDou) في عام 2015، وهي جزء من طريق الحرير الرقمي(DSR)، وهو ممر رقمي لمبادرة الحزام والطريق الصينية (BRI)، وتم

---

(1) اندروا سكوبيل ، وعليرظا نادر، *الصين في الشرق الأوسط : التنين الحذر* ،(سانتا مونيكا، كاليفورنيا : مؤسسة رند، 2020)،ص ص73-74.

(2) "أنماط القوة الناعمة الصينية، مركز الروابط للبحوث والدراسات الاستراتيجية، مقال منشور بتاريخ 2015/8/29 ، على الرابط : https://rawabetcenter.com/archives

طـرح هـذا البرنـامج الرقمـي، بـديل عـن نظـام تحديـد المواقـع العـالمي الأميركـي (GPS) وGLONASS الروسي و Galileo الأوروبي[1].

ومنطقة الشرق الأوسط، كانت ثمانية أقمار اصطناعية من نظام شبكة الملاحة الساتلية تقدم بالفعل خدمات ملاحية للدول العربية، وفقا لتقرير قدم في منتدى التعاون الصيني – العربي الثاني حول القمر الصناعي النهائي لنظام الملاحة الساتلية الذي عقد في تونس العام الماضي، وتم تقديم تغطية القمر الصناعي النهائي لنظام الملاحة الساتلية إلى الدول المشاركة في مشروع الممر الرقمي لمبادرة الحزام والطريق الصينية الضخم، وكانت الدول العربية من بين الدول الأولى التي تمكنت من الوصول إلى المرفق، إذ أنها كذلك أعضاء في منتدى التعاون الصيني العربي والحوار الاستراتيجي بين الصين ومجلس التعاون الخليجي، في الأساس، وفقًا لبكين "يمكن اعتبار أي نوع من التعاون الثنائي مع الصين جزءًا من الحزام والطريق"[2].

إن الاستراتيجية السيبرانية تقوم على التأثير عبر الفضاء الإلكتروني، فتعتمد على تطوير القدرات الحاسوبية وموارد العمل في الفضاء السيبراني، فقوة استراتيجية الدولة لا تقاس بقوتها العسكرية والاقتصادية إنما تقاس على أساس التقدم التقني والبنية التحتية المعلوماتية [3]، أما فيما يتعلق بالاستراتيجية السيبرانية الصينية فان الاهتمام زاد وبدأت الكلام حولها أثناء المؤتمر العاشر للحزب الشيوعي الصيني الذي أكد على تولي السلطات العليا اهتمام كبير بالمجال السيبراني وبالتحديد " الأنترنت" إذ عملت اللجنة المركزية في الحزب على تطويره وفي الوقت نفسه حوكمته، وقامت بترتيب القضايا التي تهتم بالأعلام والقوة السيبرانية في المجالات كافة، بما يتيح لساسة الصين بناء وتطوير استراتيجية سيبرانية قادرة على البناء السلمي وتطوير الصعود الصيني للمنافسة داخل الساحة الدولية

ووفقاً لمدير معهد دراسات المعلومات والتنمية الاجتماعية وتعزيز الابتكار في الصين "لي تشانغ" فان الاستراتيجية السيبرانية هي قدرة اتخاذ إجراءات وممارسة التأثير في الفضاء السيبراني، ففي عام 2010 أشار الكتاب "الأبيض للصين" إلى إن الأنترنت التي تتدفق إلى

---

(1) نايف المرزوقي، "طريق الحرير الرقمي ...مخاطر ومكافآت إلى الشرق الأوسط "، *القبس* ، 8/ 7/ 2020.

(2) الملاحة الساتلية هي الملاحة عبر الأقمار الصناعية ، للمزيد ينظر "طريق الحرير الرقمي مخاطر ومكافآت إلى الشرق الأوسط" ، تقرير منشور بتاريخ2020/7/8، على الرابط: https://uabonline.org

(3) "Amry war College Pensylvania :US Spade layson Information As power ",*China Cyber Power and National Security*, (2012),P.5.

الأراضي الصينية، يجب أن تخضع لسيادة الدولة الصينية، وينبغي احترام سيادة الأنترنت في الصين، وفي عام 2014 أعرب الرئيس الصيني "شي جين بينغ "Jinping عن استعداد الصبين للعمل مع جميع بلدان العالم لتعميق التعاون الدولي، واحترام سيادة الأنترنت والسلام والأمن والشفافية في الفضاء الإلكتروني وفي ديسمبر/كانون الأول 2015 صرح الرئيس الصيني في الخطاب الرئيسي في حفل افتتاح المؤتمر العالمي الثاني للأنترنت ((يجب تشجيع الالتزام العالي باحترام السيادة السيبرانية، والمشاركة المتساوية في الشبكات الدولية، ضمان الحق في الفضاء السيبراني وعدم الانخراط في الهيمنة السيبرانية، وعدم التدخل في الشؤون الداخلية والأنشطة السيبرانية للبلدان الأخرى، أو دعم الممارسات التي تعرض أمن الدولة للخطر بالنسبة إلى الصين، فان الأمن السيبراني جزء من السيادة السيبرانية، ويرتبط مفهوم السيادة السيبرانية بالحاجة إلى التحكم في أي نشاط يرتبط بالدولة، الأمة والحزب، فالحكومة الصينية تعمل على تركيز الرقابة والتحكم في الأنترنت ومحتواها))[1].

ووفقاً لمدير معهد دراسات المعلومات والتنمية الاجتماعية وتعزيز الابتكار في الصين "لي تشانغ" فان الاستراتيجية السيبرانية الصينية تقوم على:[2]

1- قدرات صناعة التكنلوجيا والمعلومات، جودة في الصناعة تكنولوجيا المعلومات ولديها تقدم تقني كبير عالميا، فهي تعتبر من الدولة المتقدمة تكنلوجيا وبأسعار اقل من الدول المنافسة.

2- القدرات البحثية التكنلوجية في المجال الصناعي، فهو قدرة الدولة على أجراء البحوث وتطوير التكنلوجيا الأنترنت ودور مراكز بحثية من شأنها زيادة الإنتاج، ووجود بنية تحتية متطورة للأنترنت، إذ تعد البنية التحتية هي من أركان الاستراتيجية السيبرانية .

3- وجود سوق الإلكتروني يعتمد على وجود أعداد كبيرة وهائلة من مستخدمي أجهزة الحاسوب والأجهزة اللوحية التي يوجد فيها الأنترنت، ووجود ثقافة الأنترنت لدى المواطنين والمسؤولين.

---

[1] سمير شرايطة، "السيادة السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومي"، *مجلة العلوم السياسة والعلاقات الدولية*، مج9، عدد 16،(كانون الثاني 2020)، ص 405.

[2]Munish Sharma, "China's, Emergence as a Cyber Power", *Journal of Studies*, Vol. 10,No.01,(2016)،PP.43-68.

4- شيوع ثقافة الأنترنت التي تعد الركن الأساسي من تطور الاستراتيجية السيبرانية في تغيير سلوكيات المواطنين وإيصال التوجيهيات عبر هذه الاستراتيجية، واستخدام الدبلوماسية الرقمية، فعادة ما تكون وتستخدم من قبل الأجهزة في السياسة الخارجية للدولة، والتأثير على المفاوضات في الدول الأخرى عن طريق استخدام القوة السيبرانية في التحشيد الشعبي أو عن طريق اللوبيات المتواجدة والجاليات للدولة في الدول الأخرى.

5- القدرة العسكرية السيبرانية، ومهمتها هي تطوير القدرات العسكرية الاستخبارية للحد من العمليات الاستخبارية الأخرى كم وتطويرا لقدرات العسكرية من حيث العمليات وتطوير الأسلحة واستخدام طائرات التجسس عن بعد وبدون طيار، ووجود الدافع القوي لامتلاك استراتيجية سيبرانية، وهو العنصر يعد الأبرز، إذ انه بدون دافع لا يمكن إن تتملك وتطور هذه الاستراتيجية.

ويسلط التقرير الذي اعده" نيلي صليبي" حول القدرات السيبرانية الصينية والذي جاء فيه التركيز على مجموعات القوة السيبرانية (ATP)التي تنسب نشاطاتها إلى الحكومة الصينية والتي هي جزء من النشاط الحكومي السيبراني والتي عملت على إثارة البلبلة فيما يتعلق بجائحة كورونا [1].

زاد اهتمام الجيش الشعبي الصيني والذي يعد من اقوى الجيوش وصاحب اكبر قدرات عسكرية عالمية إذ قام الجيش الشعبي الصيني بالهيكلة السيبرانية في عام 2015 بأنشاء ثلاث فروع دعم سيبراني جديدة الأولى هي كيف يتعامل استخباريا والدفاع في الفضاء السيبراني والعمليات الهجومية، والفرع الثاني المراقبة الرقمية للأقمار الصناعية والفرع الثالث هو مسؤول عن وحدة الذكاء الإلكتروني وازدادت عمليات التطوير ومن المؤمل تحقيق الهيكلية الكاملة في العام 2020[2].

واتسمت الاستراتيجية الصينية بالتطارح مع الولايات المتحدة الأمريكية بحالة من التنافر والتنافس في الفضاء السيبراني ففي تقرير سنوي صدر عن مكتب المخابرات الوطنية الأمريكية (DNI)، في كانون الثاني/عام 2019، إلى تصاعد أنشطة التجسس السيبراني التي تقوم بها

---

[1] نايلة صليبي، "ماهي خلفية استراتيجية الصين في الحرب السيبرانية"، *مونتكارلو الدولية*، مقابلة تلفزيونية أجريت بتاريخ 2020/8/4، على الرابط : https: www.mc-doualiya.com/chronicles

[2] عبد الغفار الدويك، "قراءة تحليلية للقدرات السيبرانية في العالم"، مصدر سابق ذكره، ص277.

الصين، ونص التقرير أن الحكومة الصينية "طورت" قدراتها في الهجمات السيبرانية، بما في ذلك توجيه آراء المواطنين الأمريكيين وفيما يتعلق بالمشكلات القائمة منتجات" شركتي هواوي" و"زد تي إي" الصينيتين إذ قال :"السيناتور مارك ورنر"، نائب رئيس لجنة الاستخبارات في مجلس الشيوخ الأمريكي، إن شركتي هواوي و"زد تي إي" الصينيتين للاتصالات، تشكلان تهديدا للولايات المتحدة ودعا في بيان مشترك مع السيناتور "ماركو روبيو"، العضو في اللجنة ((على السلطات الأمريكية إلى الاحتراس، لحماية التكنولوجيات الحساسة من أنشطة التجسس الأجنبية))، وتظهر بين حينة وأخرى، تحذيرات في الغرب من إمكانية استخدام أنظمة ومنتجات شركات الاتصالات الصينية العملاقة، لأغراض التجسس [1].

وذكرت صحيفة "نيويورك تايمز" الأمريكية إن الحكومة الأمريكية تتهم الصين بمحاولة سرقة معلومات عن أبحاث بخصوص لقاح لفيروس "كورونا" واستغلال وقت الوباء لعمل هجمات على البنية التحتية كونها تعد الوفرة الإلكترونية، وقالت الصحيفة، في تقرير لها، إن مكتب التحقيقات الفيدرالي (FBI) ووكالة الأمن القومي يستعدان لإصدار تحذير يفيد بأن أمهر المتخصصين في مجال اختراق المعلومات إلكترونياً الذين يعملون لحساب الصين يسعون لسرقة المعلومات الخاصة بالأبحاث الأمريكية المخصصة لإيجاد لقاح لفيروس كورونا، مشيرة إلى إن هذه الجهود تأتي كجزء من تصاعد السرقة والهجمات عبر الأنترنت من الدول التي تسعى للاستفادة من الوباء العالمي، ويقول خبراء أمنيون إن هناك تصاعداً في الهجمات من قبل القراصنة الصينيين الذين يسعون إلى الحصول على ميزة في السباق نحو لقاح لفيروس كوفيد-19 أو حتى علاج فعال له وإن الصينيين لوحدهم في سعيهم لاستغلال الفيروس، وهذا من اخطر التطارحات الصينية- الأمريكية [2].

وتظهر الاستراتيجية السيبرانية للصين بشكل فعال في التكنولوجيا في الاقتصاد الصيني إذ يعد سوق تكنولوجيا المعلومات والاتصالات في الصين من أكثر القطاعات ديناميكية في الاقتصاد، ومن المتوقع انه بحلول عام 2021، سيصل السوق إلى 8 . 1 تريليون دولار، وهو

---

[1]Michael E. DeVine, "Intelligence Community Spending: Trends and Issues", *Congressional Research Service*,(November 2019),PP.14-15.

[2]محمد هيكل، "زيادة وتيرة الهجمات السيبرانية بالتزامن مع جائحة كورونا ، *نيويورك تايمز*: الولايات المتحدة تتهم الصين بمحاولة اختراق معلومات عن لقاح لفيروس "كورونا، *نيويورك تايمز*، تقرير منشور على الرابط: https://covid-19.ecsstudies.com

مـا يمثـل 55 % مـن النـاتج المحلـي الإجمـالي للصـين، ووفقـا لشـركة استشـارات تكنولوجيـا المعلومات (IT) ، بلغت واردات الصين من تكنولوجيا المعلومات والاتصالات في عام 2017 حوالي 528 مليار دولار، في حين بلغت صادراتها 781 مليار دولار، المنافسة من الشركات الصينية قوية في مواجهة الشركات الغربية، إذ استثمر جودة الأجهزة والبرامج والخدمات المحلية في التحسن، ومع تطور سوف تكنولوجيا المعلومات والاتصالات في الصين، من المتوقع أن تصبح بعض القطاعات الفرعية التي كانت تقود النمو (مثل الهواتف الذكية مشبعة، وسيتم تعزيز النمو المستقبلي عبر دمج تقنيات تكنولوجيا المعلومات والاتصالات في الصناعات التقليدية وتحويلها[1].

المبحث الثاني: الاستراتيجيات الإقليمية المتطارحة مع الاستراتيجية الأمريكية سيبرانياً

إن الاستراتيجيات الإقليمية المتطارحة مع الولايات المتحدة الأمريكية(ايران، كوريا الشمالية) من المضادات الهيمنة الأمريكية، فبعد البرامج النووية التي تهدف إلى التطارح مع الولايات المتحدة الأمريكية ، تطور الأمر مع التطور العالمي وأخذت هذه الدول بالأخذ بالاستراتيجيات السيبرانية والعمل على تطوريها فكانت ذات ردة فعل قوية على الهيمنة الأمريكية على الفضاء السيبراني، إذ نفذت هذه الدول مئات من العمليات السيبرانية ضد الولايات المتحدة الأمريكية وبعض الدول العالمية، كما قامت الولايات المتحدة الأمريكية بتحييد قدرات سيبرانية كبيرة في هذه الدول، وهذا ما دعانا إلى تقسم المبحث على النحو الآتي :

المطلب الأول: الاستراتيجية الإيرانية السيبرانية

يرتكز هذا المطلب على ذكر تنوع الاستراتيجية التطارحية الإيرانية بالضد من الولايات المتحدة الأمريكية والمناورة في استخدام مختلف الاستراتيجيات لتحقيق المصلحة العليا لإيران، منذ تأسيس جمهورية ايران الحديثة بعد أسقاط حكم "الشاه بهلوي" في عام 1979، بدأت تُستخدم بفعالية أدوات استراتيجية القوة الناعمة في المطارحات الإقليمية والدولية، ولكي تتم فعالية تلك الأدوات، يجب أولًا أن تصل إلى عقول الشعب المستهدف، ولذلك فإن الدبلوماسيين الإيرانيين هم أكثر انفتاحًا مع شعوب المنطقة، وتحديدًا في النشاطات المجتمعية والثقافية التي تعد ركيزة استراتيجية القوة الناعمة الإيرانية، إذ يستخدم الدبلوماسيون الإيرانيون كل الأدوات

[1] سمير شرايطة، "السيادة السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومي"، مصدر سابق، ص406.

المتاحة لخلق صورة إيجابية عن إيران في الدول التي لها علاقات ارتباطية مع ايران ، فهناك ممثلون ثقافيون ومسؤولون عن الدبلوماسية العامة، وهذا دليل على أن صانع القرار في إيران يخطط لهذه الدبلوماسية بشكل دقيق ومنظم[1].

فبعد ثورة 1979 تم تغيير اسم وزارة الإعلام والسياحة إلى وزارة الإرشاد القومي، وبعد ذلك بعامين أصبح يطلق عليها وزارة التوجيه الإسلامي، كما أن وزارة الثقافة هي الأخرى قد تم دمجها في وزارة التوجيه، وفي عام 1987 تحولت وزارة التوجيه إلى وزارة الثقافة والإرشاد الإسلامية، نظرا لبعد الأيديولوجي الديني لنظام الحكم الإيراني قامت ايران بصناعة جماعات ضغط (لوبيات) تدار وفق استراتيجية القوة الناعمة داخل بعض الدول المستهدفة (العراق، سوريا، اليمن، بعض الدول الأوربية مهمتها هي تحويل القرارات لصالح ايران في المحافل العالمية والإقليمية وجلب المصالح الاقتصادية والسياسية[2]، إذ يعد تبنيها سياسة إدارة وتوجيه محور المقاومة في منطقة الشرق الأوسط الداعم الأساسي لاستراتيجيتها الناعمة من خلال جعل القضية الفلسطينية قضيتها الأولى، ومحاولة تشوية سياسة الولايات المتحدة الأمريكية في منطقة الشرق الأوسط[3]، وان توظيف القوة الذكية وفيما بعد القوة الرقمية (Digital power) ساعد كثير في تقوية الاقتصاد وتطوير برنامجها النووي أما فيما يتعلق بالاستراتيجية القوة الذكية الإيرانية ظهرت الاهتمامات السيبرانية ضمن خارطتها الاستراتيجية العامة، ازددت الاهتمامات السيبرانية بعد الاهتمام النووي الإيراني وبالتحديد في العام 2010 بعد أن تعرضت إلى هجوم سيبراني أمريكي وإسرائيلي استهدف برنامجها النووي محدثا أضرار جسيمة بعد الهجوم، وسميت هذه الهجمة بـ(ستوكس نيت Stuxnet) الخطير للغاية الذي حطم أجزاء كبيرة من برنامجها النووي، واحكمت جميع وحدات مفاعل نطنز لتخصيب اليورانيوم ببرامج فعالة ، وهذه البرامج ساعدها في التعرف بالتفصيل على شبكات الكمبيوتر الخاصة بالمنشأة، بما في ذلك أنظمة التحكم الصناعي المتصلة، واستهدف بالتحديد وحدات التحكم المنطقية القابلة للبرمجة، والتي

---

(1) سعد قاسمي ، "عوامل تراجع القوة الإيرانية الناعمة في المنطقة العربية"، *مجلة الدراسات الإيرانية*، عدد*10*، (أكتوبر *2019*)، ص*114*.

(2) فراس الياس، "الوجه الأخر للقوة الناعمة الإيرانية"، *المعهد الدولي للدراسات الإيرانية (رانش)*،8 /يوليو/2018، ص2.

(3) عبد الصبور سماح ، "القوة الذكية: أدوات السياسة الخارجية الإيرانية تجاه لبنان"، *مجلة السياسة الدولية*، مج*15*،عدد 2،(2014)، ص 147-148.

توفر التحكم في العمليات الكهروميكانيكية، وقد تسبب في تحطيم أجهزة الطرد المركزي سريعة الدوران، تسبب في أضرار جسيمة في البرنامج النووي الإيراني وأدى إلى تأخيره، و من المؤكد أنه أدى إلى تكاليف كبيرة ووقت إضافي لإصلاح الأضرار التي حدثت داخل أنظمة تكنولوجيا المعلومات، في جميع وحدات مفاعل نطنز للتخصيب اليورانيوم، والتي سيتطلب الكثير منها جهد لتطهير البرنامج، بل قد يصل الأمر إلى تدميره، وبالقدر نفسه من التكلفة سيكون من الضروري تغيير المعدات الصناعية، تلك المعدات التي لا تحصل عليها إلا من خلال شبكات بطيئة وسرية الانتشار [1]، وهنا سجلت الولايات المتحدة نقطة في مطارحاتها مع ايران.

تصدرت أدوات الاتصالات مكانة بارزة لدى المؤسسة الإيرانية، منذ عهد الشاه، إذ خصصت ميزانية ضخمة لتوطين تقنيات الاتصالات الحديثة قبل عام 1979، مما جعلها تتفوق بهذا المجال على الكثير من بلدان الشرق الأوسط، غير إن التغيير الإيراني وظف المعلومات والاتصالات لإضعاف دول المنطقة، غير إن الحرب مع العراق، حطمت كل البنى التحتية الإيرانية، لكن ما إن جاءت التسعينات حتى بدأت مرحلة بناء المنظومة المعلوماتية مرة أخرى، بيد آن ولادة تقنية فضاء الأنترنيت، والهواتف المحمولة أثارت المزيد من القلق لدى الحكومة بعد تهديد للأمن القومي بسبب الانكشاف الاستراتيجي، فتأرجحت استراتيجية الحكومية بين توسيع قاعدة الاتصالات والمعلومات من جهة، مع تضييق الخناق على فضاء التواصل والاتصالات، من جهة أخرى، فأصيبت الاستراتيجية بإرباك[2]، مباشرة تلقت درساً في الحرب الإلكترونية؛ وقد تلقته هذه المرة عندما كانت الحكومة في صدام مع شعبها، إذ نشأت حركة سياسية في إيران بعد الانتخابات الرئاسية الإيرانية عام 2009 ما تعرف (بالحركة الخضراء) طالب فيها المتظاهرون بإقالة محمود أحمدي نجاد من منصبه في أعقاب ما عدوة تزويراً للانتخابات، وأصبح هذا الحراك يعرف باسم "الحركة الخضراء" وهي من ضمن الجيوش الإلكترونية، وظهرت ساحة المعركة الجديدة هذه على "الإنترنت" كاشفه عن نقطة ضعف رئيسة في قدرة الدولة الإيرانية على الاستجابة لجأت الحكومة إلى "القمع الإلكتروني" للاحتجاجات؛ ما أدى إلى الحد من الوصول

---

[1]() " قدرا القرصنة السيبرانية الإيرانية"، تقرير خاص، مركز *الملك فيصل للدراسات والبحوث*،(كانون الأول 2020) ، ص10.

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

إلى الإنترنت، مع فرض الرقابة على المحتوى الذي ينشره المحتجون على شبكة الإنترنت، أو حذفه[1] .

وعلى اثر ذلك اصدر المرشد علي خامنئي امراً بإنشاء الهيئة الإلكترونية والتي تختص في معظم النشاط السيبراني في ايران، وفي العام2012 تمكنت شركة الأمن الإلكتروني ومكافحة الفيروسات (كاسبرسكاي) من التعرف على قطعة برمجية خبيثة على شبكات الكمبيوتر داخل إيران، لها القدرة على استخراج المعلومات سرية من أجهزة غير مؤمنة، ومن بين هذه المعلومات وثائق ومحادثات على وسائل التواصل الاجتماعي، وضغطات المستخدمين على لوحة المفاتيح، هذا البرنامج الضار، أطلق عليه فيما بعد اسم "فليم"، كان له القدرة على محو المعلومات، ويحتمل أن يكون نشط داخل إيران منذ عام 2010 ، وامتداد لما حدث أصدرت استراتيجيتها والتي تتكون من مراحل عدة فالمرحلة الأولى والتي خصص لها حوالي 19 مليار دولا لتطويرها وتشمل عدة استراتيجيات، تم رسمها وفق خطة خمسية من العام 2005–2009.

منها الاستراتيجية الوطنية لتطوير تقنيات الاتصال والأدوات والمعلومات كما تشمل استراتيجيات الأخرى الخدمة الإلكترونية وخصخصة قطاع الاتصالات وتحويل شبكات الاتصالات التقليدية إلى شبكات الجيل الجديد كذلك وتشجيع الاستثمارات الأجنبية في القطاع السيبراني.

وبعد التطورات الدولية السيبيرانية وازدياد الاعتماد الدولي على الخدمات السيبرانية فقد عمدت الحكومة إلى وضع خطة خمسية اكثر نجاعة ممن العام2011–2016، وشملت تطوير قواعد بيانات لملفات الرعاية الصحية الإلكترونية للمواطنين الإيرانيين، وتشييد قواعد وجيوش برمجية سيبرانية، وتوسيع نطاق شبكات الوطنية للمعلومات "شوما"، وطرح مزيد من الخدمات الحكومية السيبرانية، وتعزيز قواعد بيانات متكاملة تغطي المسائل القانونية، دعم برامج ومشاريع وضع قواعد لنظم المعلومات، والاهتمام بالمشاريع والأشخاص ذا المحتوى السيبراني، وتدريب الملاكات الإيرانية والتعاون مع بعض الدول المتطورة سيبرانيا مثل روسيا والصين.

ونتيجة للقدرات المعلوماتية غير المتكافئة بين الولايات المحددة الامريكية وإيران؛ طارحت الأولى الثانية سيبرانياً بعد إن طرحتها اقتصادياً بحزم العقوبات، ولذلك أولى الجانبان اعتباراً كبيراً لبناء منظومة سيبرانية قادرة على حماية شبكة معلومات من الهجمات السيبرانية [1].

[1] قدرات القرصنة الإيرانية السيبرانية، مصدر سبق ذكرة ، ص 13.

وما إن اقتربت الولايات المتحدة الأمريكية من ايران جغرافياً (العراق وأفغانستان) حتى شهدت تقاطع وهجمات سيبرانية بينهما، خلفت خسائر بمليارات الدولارات، بدأت بخطة "الألعاب الأولمبية" التي ابتكرها جورج بوش لضرب قوى الشر الإيرانية التي ترعى الإرهاب في شتى أنحاء العالم حسب وصفه، وتتآمر بشكل دائم على دول المنطقة كسبت أمريكا جولات عدة، ودمرت بيانات الحرس الثوري وأهدافاً حكومية بهدف ردع النظام ووقف نشاطاته السيبرانية، أثار الإيرانيون الفزع في مناطق كثيرة بالعالم عن طريق ضربات سيبرانية، تصاعدت التوترات بين الطرفين بشكل متزايد في الفضاء السيبراني، واعترفت الحكومتان بأن الهجمات السيبرانية كانت أساسية في استراتيجياتهما، على الرغم من إن النطاق غير معروف، لكن الفضاء الإلكتروني تحول إلى منطقة حرب شبه مقيدة، وبحسب نيويورك تاميز، بدأ البرنامج في 2006 تحت إدارة جورج بوش، واستهدف القدرات النووية الإيرانية، ووسع الرئيس باراك أوباما الألعاب الأولمبية لتشمل استخدام الأسلحة السيبرانية الهجومية ضد منشآت التخصيب النووي الإيرانية.

ومن المطارحات الأخرى التي كسبتها الولايات المتحدة الأمريكية في يونيو 2019، انتقمت "إدارة ترامب" من إسقاط إيران لطائرة أمريكية بدون طيار بهجوم الإلكتروني على قاعدة بيانات الحرس الثوري المستخدمة للتخطيط لشن هجمات على ناقلات النفط، وضربت الولايات المتحدة إيران مرة أخرى في سبتمبر 2019 بعد أن أطلقت إيران طائرات بلا طيار وصواريخ كروز على منشأتين نفطيتين، وبدورها كثفت إيران جهودها لاختراق بعض الأهداف الأمريكية وحسابات البريد الإلكتروني[2].

وفي المقابل سجلت ايران بعض النقاط في تلك ففي عام 2009 قام ما يسمى بـ"جيش الأنترنت الإيراني" بتشويه الصفحة الرئيسة لموقع (Twitter) رداً على احتجاجات "الثورة الخضراء" التي تدعمها الولايات المتحدة الأمريكية ضد انتخاب الرئيس "محمود أحمدي نجاد"، فمنذ عام 2009، نمت قدراتها السيبرانية، وسجلت نقطة تطارحية أخرى بعد أن استهدفت طهران بشكل أساسي القطاع الخاص بدلاً من الأنظمة الحكومية الأمريكية، وبحسب" نيويورك تايمز" في

---

[1]Clayton Thomas,"U.S. Killing of Qasem Soleimani: Frequently Asked Questions ", *Congressional Research Service*,(January 2020),PP.2-3.

[2] اماني يماني، "ضربات أمريكية سيبرانية موجعة لإيران"، مقال منشور بتاريخ 2020/1/22، على الرابط: https: //www.akkahnewspaper.com

سبتمبر 2012 وجه قراصنة إيرانيون هجوماً على خدمة الحرمان الموزع (DDoS) ضد البنوك الأمريكية، منعت الحملة، التي أطلق عليها اسم عملية "أبابيل"، الوصول إلى مواقع المؤسسات المالية الكبرى عن طريق غمر خوادمها بحركة مرور على الأنترنت، هذه الهجمات كلفت الشركات الغربية الملايين من الأعمال الضائعة، وفقاً لقرار اتهام من وزارة العدل، سارعت طهران في عملياتها الإلكترونية ضد حكومة الولايات المتحدة وشركائها الإقليميين بعد انتخاب الرئيس "دونالد ترامب"، وتزامنت هذه الهجمات مع زيادة التجسس الإيراني على الأنترنت، فايران لها جيش الإلكتروني[1].

إذ إن الولايات المتحدة الأمريكية التي عانت من هجمات سيبرانية، أقامت في السنين المنصرمة دفاعات محكمة ضد القراصنة المحتملين الراغبين في استهداف البنى التحتية شديدة الأهمية، وعززت قدرات الكشف عن التهديد، لتأمين تبادل معلومات آمنة بين القائمين على مشاريع البنية التحتية الحساسة، ولتأمين تعاون أكبر وأكثر سلاسة بين خبراء الدولة والقطاع الخاص، لكن اعتماد الولايات المتحدة الأمريكية المتزايد على شبكة الأنترنت لتسيير كل شيء، ابتداء من السدود، وصولاً إلى أسواق المال، يجعل منها أكثر انكشافاً أمام الهجمات السيبرانية من بلد مثل إيران التي ما زالت تعمل في مجالات كثيرة على أنظمتها التقليدية، لترد الولايات المتحدة مسجلة نقاط عدة أخرى لصالحها في تلك المطارحة، فبعد أن شهدت إيران منذ بداية حزيران2020، حوادث غامضة وحرائق متتالية طالت منشآت ومواقع كبرى، كشف المتحدث باسم الخارجية الإيرانية عباس موسوي، أن "عدة هجمات سيبرانية تعرضت لها البنية التحتية للبلاد خلال الأشهر الأخيرة حيث اكد موقع ياهو نيوز إن الرئيس الأمريكي دونالد ترامب أعطى أوامر بالهجمات السيبرانية[2] .

واستمرار لاستراتيجية التطارح الإيراني ضد الولايات المتحدة الأمريكية أسقطت ايران بواسطة أجهزتها السيبرانية والموجه عن بعد وعن طريق صاروخ ارض –جو طائرة بدون طيار أمريكية فوق مياه مضيق هرمز، وفي تصريح للقيادة المركزية الأمريكية وقال: الكابتن" بيل

---

[1] نبيل العتوم، الجيش الإلكتروني الإيراني،(الأردن: مركز أمية للبحوث والدراسات الاستراتيجية – دار عمار للنشر والتوزيع ،2015)،ص23 وما بعدها.

[2] صالح حميد ، طهران: "تعرضنا لهجمات سيبرانية"، *قناة العربية*، مقال منشور بتاريخ 2020/7/23، على الرابط الاتي: https:// ww.alarabiya.net

أوربان"، المتحدث باسم القيادة المركزية للجيش الأمريكي، إن الطائرة التي أسقطت هي طائرة استطلاع أمريكي في الأجواء الدولية ،وقال، وفي تصريح للرئيس الأمريكي عبر موقع تويتر غرد الرئيس الأمريكي دونالد ترامب قائلاً "لقد ارتكبت إيران خطأ كبيراً "، وقال: الحرس الثوري الإيراني إنه أسقط طائرة أمريكية بدون طيار بعد أن دخلت المجال الجوي الإيراني، قرب كوهمو باراك في إقليم هورموزكان الجنوبي فيما جاء الرد من وزارة الخارجية الإيرانية بانتهاك طائرة أمريكية بلا طيار لمجال إيران الجوي، محذرة الولايات المتحدة الأمريكية حسب التلفزيون الرسمي، وذكر الحرس الثوري الإيراني إن في إسقاط الطائرة "رسالة واضحة" للولايات المتحدة ،ونقلت وسائل إعلام إيرانية عن قائد الحرس الثوري، اللواء حسين سلامي، قوله: "حدودنا هي خطوط حمراء، وسوف نرد بقوة على أي اعتداء، إيران لا تسعى إلى الحرب مع أي بلد، لكننا مستعدون تماما للدفاع عنها[1].

المطلب الثاني: المطارحات الاستراتيجية الكوريا الشمالية-الأمريكية السيبرانية

النظام في كوريا الشمالية كان ومازال من ابرز أعداء الولايات المتحدة الأمريكية والتطارحات تطورت بشكل جدي من التهديدات النووية لامريكا وحلفائها اليابان وكوريا الجنوبية واستخدام الأفراد السيبرانيون من مختلف الأماكن لتنفيذ هجمات وفق تطلعات الاستراتيجية السيبرانية الكورية الشمالية.

إن التحول في الاستراتيجية الكورية الشمالية من القوة التقليدية إلى القوة الناعمة ثم القوة الذكية فالرقمية في ظل التعتيم الداخلي كان غير ملموس في كوريا الشمالية، إذ إن أدوات كوريا الشمالية وفق استراتيجية القوة الناعمة هي أدوات إعلامية بحتة موجهه لعدة دول تشاركها الرؤى وهي ايران وبعض الدول ذات التوجه الشيوعي التي تقف بالضد من الولايات المتحدة الأمريكية، فعلى سبيل المثال تتخذ كوريا الشمالية في ظل تصاعد التوترات عالمياً، عندما يكون لدى كوريا الشمالية نبأ مهم تود الإعلان عنه، عادة ما تكون مقدمة الأخبار ملهمة الشعوب الشيوعية" ري

[1] David E. Sanger & Julian E. Barnes, U.S. Tried a More Aggressive Cyberstrategy, and the Feared Attacks Never Came, New York Times, (Nov. 9, 2020),PP.2-3.

تشون هي، الشخص المسؤول عن ذلك، ويستمع العالم إلى أسلوب قارئة الأخبار المثير المتميز، وحدث ذلك مؤخراً حين كانت بلادها تطلق صاروخاً سراً، أو تجري تجارب نووية ،وقد أعلنت في آخر ظهور لها على الشاشة، بينما ترتدي ملابس باللون الوردي، أن كوريا الشمالية قد أجرت اختباراً على قنبلة هيدروجينية، حسبما وصفها نظام كوريا الشمالية، وقال إن قوتها أكبر بخمسة أمثال من القنبلة التي تم قصف نكازاكي بها أثناء الحرب العالمية الثانية[1].

وفيما يخص استراتيجية كوريا الشمالية السيرانية ترجع بداية مطارحات كوريا الشمالية السيبرانية، إلى عهد "كيم يونج إل"، والد رئيس كوريا الشمالية كان محباً للأفلام وصار مولعاً بالإنترنت، وكانت رفاهية مخصصة لنخبة البلاد فقط، في عام 2011 وبعد وفاة "كيم الأب"، قُدر عدد عناوين الـIP التي تملكها البلاد بـ1024 عنوانًا، وهو عدد أقل من العدد الموجود في معظم المربعات السكنية في نيويورك، وقال رئيس سابق للاستخبارات البريطانية أن كوريا الشمالية ربما تربح ما يصل إلى مليار دولار سنوياً من عمليات السطو السيبرانية، وهو ما يعادل ثلث قيمة صادراتها، فكان "كيم " يخشى "الإنترنت" في البداية ويراه تهديداً لقبضة نظامه الحديدية على المعلومات، لكن سلوكه تغير في بداية التسعينيات بعد عودة مجموعة من علماء الحاسوب لكوريا الشمالية من السفر، الذين اقترحوا استخدام الشبكة الإلكترونية للتجسس والهجوم على الأعداء مثل كوريا الجنوبية والولايات المتحدة الامريكية[2] .

وبعد التحول في أنماط الصراع بين كوريا الشمالية والولايات المتحدة الأمريكية إلى ميدان الفضاء السيبراني نتيجة للتطور التقني اصبح الصراع اكثر تعقيداً واقل كلفة ففي العام 2014 وضمن الاستراتيجية السيبرانية الكورية الشمالية قام قراصنة من وحدات ا"لجيش السيبراني الكوري الشمالي" بهجمات على المواقع الأمريكية، وفي سياق الجهود الأمريكية لتعزيز الأمن السيبراني ضد هجمات سيبرانية قد تنفذها القوى المنافسة للولايات المتحدة الأمريكية على قيادة النظام الدولي (روسيا والصين) أو دول تصنفها الولايات المتحدة الأمريكية على أنها أعداء لها (كوريا الشمالية وإيران)، أعلنت ليزا موناكو، مساعدة الرئيس الأمريكي للأمن الداخلي ومكافحة

---

[1] ري تشون ،"القوة الناعمة لكوريا الشمالية"، *جريدة الشرق الأوسط*، عدد 14167، منشور بتاريخ 11 /9/ 2017.

[2] محمد الحسيني ، "كيف أصبحت كوريا الشمالية ب6000 هاكرز إن تهدد امن الأنترنت"، *ترجمة ساسا بوست*، أكتوبر 2020 : على الرابط : https://www.sasapost.com/translation/north-korea-hacking-cyber

الإرهاب، عن اعتزام الإدارة الأمريكية تأسيس وكالة أمريكية جديدة مهمتها جمع وتحليل المعلومات لمنع هجمات تستهدف الأنظمة الإلكترونية للمؤسسات الحكومية والشركات داخل الولايات المتحدة، ودراسة العلاقات بين التهديدات السيبرانية التي تواجهها الولايات المتحدة الأمريكية حتى تصبح الوكالات والمؤسسات المعنية على دراية بهذه التهديدات بأسرع ما يمكن[1].

وحسب مصادر أمريكية فإن تأسيس تلك الوكالة التي ستحمل اسم "مركز التكامل الاستخباراتي للتهديدات السيبرانية (Cyber Threat Intelligence Integration Center) سيوحد جهود الأقسام الداخلية بالوكالات الأمريكية المناط بها حماية الولايات المتحدة الأمريكية من الهجمات السيبرانية مثل وكالة الاستخبارات المركزية، ووكالة الأمن القومي، ومكتب التحقيقات الفيدرالي[2]، وهذا يعني إن الولايات المتحدة الأمريكية وكوريا الشمالية في حالة تطارح سيبراني مستمر.

إن في مسار التطارح الكوري الشمالي ضد الولايات المتحدة الأمريكية وحلفائها في شبة الجزيرة الكورية وضمن استراتيجية كوريا الشمالية السيبرانية ذكرت هيئة الاتصالات الكورية الجنوبية إن الهجمات السيبرانية التي استهدفت بنوكا ومحطات تلفزة وشركة تقديم خدمات إنترنت في البلاد كان مصدرها أفراد من الوحدات السيبرانية الكورية الشمالية، على الرغم من هويات منفذي الهجمات لا تزال غير معروفة وقال المتحدث باسم الهيئة في مؤتمر صحفي بأن تتبع التسلل الذي انطلقت منه الهجمات أمس قادهم إلى خادم في الصين، وهي دولة استخدمها متسللون من كوريا الشمالية هجماتهم، ويأتي هذا الكشف بعد يوم من هجوم سيبراني ضخم منظم على خوادم في كوريا الجنوبية دفع السلطات لرفع حالة التأهب لدى الجيش وسط تخوفات بأن الهجمات شنتها جارتها كوريا الشمالية وكانت المواقع الرسمية الإلكترونية في كوريا الشمالية تعرضت قبل هذا الهجوم لهجمات سيبرانية أدت إلى تعطلها فترة طويلة، وقد اتهمت كوريا الشمالية جارتها الجنوبية وحليفتها الولايات المتحدة الأمريكية بتدبير الهجوم السيبراني الذي يعتبر

---

(1) كيف أصبحت كوريا الشمالية بـ 8 آلاف هاكر تهدد امن الأنترنيت؟ ،تقرير ، نيويورك تايمز، 17/ 8/ 2020.

(2) عمر عبد العاطي، "حرب أمريكية مضادة للإرهاب السيبراني"، *جريدة الخليج* ،مقال منشور 21/ 3/ 2013 ، 21/3/2013 ، على الرابط: https:www.alkhaleej.ae

ضمن استراتيجية التطارح الأمريكي الكوري الجنوبي ضد كوريا الشمالية[1]، ويدير جهاز المخابرات الرئيس في كوريا الشمالية خلية خاصة يطلق عليها اسم "الوحدة 180"، من المرجح أنها مسؤولة عن شن بعض الهجمات السيبرانية تعد من أنجح الاختراقات، بحسب ومسؤولين في الاستراتيجيات السيبرانية، اتجهت أصابع الاتهام إلى كوريا الشمالية، في سلسلة من الهجمات السيرانية أغلبها على شبكات مالية في كوريا الجنوبية، ونحو عشر دول أخرى، وقال باحثون في الأمن السيبراني" إنهم عثروا على أدلة تقنية يمكن أن تربط كوريا الشمالية بالهجوم العالمي بفيروس "الفدية" المعروف باسم (Wanna Cry)، الذي أصاب أكثر من 200 ألف جهاز كمبيوتر في 150 دولة، إذ ياتي هذا العمل الاستراتيجي المنظم ضمن استراتيجية التطارح من كوربا الشمالية ضد كوريا الجنوبية حليفة الولايات المتحدة الامريكية "[2] .

إن في النهج المستمر للإطاحة بشركاء الولايات المتحدة الأمريكية وفق مخطط الاستراتيجية للكورية الشمالية، أفاد تقرير لمكتب التحقيقات الفيدرالي الأمريكي (إف بي آي) في (19 كانون الأول 2014) أن كوريا الشمالية واذرعها السيبرانية هي المسؤولة عن عملية الهجوم السيبراني وقرصنة" شركة سوني " المعلوماتية الضخمة في (تشرين الثاني/نوفمبر 2014)، واختراق موقع شركة "سوني بيكتشرز" للأفلام السينمائية والأعمال التلفزيونية والتوزيع[3]، وذكرت وكالة الأنباء الحكومية في كوريا الشمالية "إنه عمل استفزازي يستحق عقوبة مشددة [4]، في ردها على عزم شركة "سوني بيكتشر" في اليابان الترفيهية عرض فيلم ساخر عن الرئيس" كيم يونج أون، أعلنت شركة سوني بيكتشر الأمريكية بعد أيام من التي تلت هذا التهديد عن تعطل نظام الحاسوب الخاص بالشركة ومسح بعض البيانات الخاصة بالشركة، وسرقة ما قيمته 10 سنوات من رسائل البريد الإلكتروني ونشر مقتطفات محرجة من هذه الرسائل، كما تم الإعلان عن سرقة

---

[1] "هجمات إلكترونية تستهدف كوريا الجنوبية"، *الخليج* ، تقرير منشور بتاريخ 2013/3/21، على الرابط: https:www.alkhaleej.ae_

[2] ايهاب خليفة ، *مجتمع ما بعد المعلومات : تأثير الثورة الصناعية الرابعة على الأمن القومي*، مصدر سبق ذكرة ، ص118.

[3] "كوريا الشمالية وراء قرصنة موقع شركة سوني"، *تقرير مكتب التحقيقات الفدرالي الأمريكي*، 2014/12/19، على الرابط: https://ww.dw.com/ar

[4] "الحرب الإلكترونية جيل جديد من الحروب لا نعرفه"، *نون بوست*، مقال منشور بتاريخ 2015/01/17، على الرابط : https://www.noonpost.com

بيانات شخصية لموظفي الشركة وكبار المسؤولين بها، كما تم تسريب مقتطفات من 5 أفلام من إنتاج الشركة من بينها 4 لم يتم عرضهم، ما سيؤدي إلى خسارة تتكبدها الشركة تصل إلى مليارات الدولارات في المقابل أعلنت الشركة عن الإلغاء عرض الفلم ، وضمن مسلسل الحرب السيبرانية استخدمت اليابان قدراتها الإعلامية بالاشتراك مع حليفتها الولايات المتحدة في بث أخبار حول صحة الرئيس الكوري الشمالي كيم جونغ أون في ظل الغموض الذي رافق في محاول منها لزعزعة الأوضاع داخل كوريا الشمالية واستمرت التحشيد الإعلامي وفق المخطط السيبراني الاستراتيجي، إذ ذكرت شبكات إعلامية يابانية إن رئيس كوريا الشمالية يكون فارق الحياة، متخذة هذا النهج لمنع كوريا الشمالية من التدخل السيبراني ضدها وأثار غياب الرئيس الكوري " كيم "لمدة 3 أسابيع في عام 2020تكهنات واسعة النطاق بأنه مريض أو خضع لعملية جراحية كبرى، إذ تعد معلومات صحة الرئيس أحد الأسرار الكبرى في هذا البلد المغلق [1].

[1]() بعد "حركة غريبة جدا.. اليابان تبدي شكوكا حول صحة زعيم كوريا الشمالية"، *قناة الحرة* ، مقال منشور في 26/06/2020، على الرابط: https//www.alhurra.com

الخاتمة :

إن الاستراتيجيات الدولية والإقليمية التي تعد بمثابة تهديد حقيقي للهيمنة الأمريكية على الفضاء السيبراني والتي تشير دلالاتها إلى مستقبل يحتمل عدة مشاهد لمستقبل تلك الاستراتيجية، أهمها تصاعد التطارح السيبراني بين الولايات المتحدة الأمريكية والروسية والصين دولياً، كوريا الشمالية وايران اقليمياً، وهذا التصاعد التطارحي سيعمل إلى رسم مستقبل قريب منفرد يتجه نحو نظام سيبراني متعدد القوى فوضوي يتجه نحو توازن القوى السيبراني متزن بالمستقبل البعيد، وهذا افضى بنا الى جملة من النتائج وهي:

1. يحتل الفضاء السيبراني العالمي موقعاً بارزاً في الاستراتيجية الأمريكية.
2. الاستراتيجية الأمريكية من اقوى الاستراتيجيات الدولية تأثيراً في الفضاء السيبراني.
3. الاستراتيجية الأمريكية ستتطارح مع القوى الدولية والإقليمية التي تعارض الهيمنة الأمريكية عالمياً، فتظهر "الحرب السيبرانية الباردة"، تفضي إلى ظهور "نظام دولي سيبراني تعددي".
4. إن جوهر الاستراتيجية الأمريكية للهيمنة على الفضاء السيبراني العالمي هو استكمال الهيمنة واستدامتها .
5. كلما ازدادت مساعي الاستراتيجية الأمريكية للهيمنة على الفضاء السيبراني ازدادت مساعي الاستراتيجيات الدولية والإقليمية لمنع الهيمنة.

واستناداً على النتائج التي خرج بها البحث صحت الفرضية" كلما ازدادت حراكات الهيمنة الأمريكية على الفضاء السيبراني ازدادت شدة التطارحات التصارعية مع الاستراتيجيات الدولية والإقليمية لرفض الهيمنة سيبرانياً".

قائمة المصادر

المصادر العربية

أولا: الكتب العربية والمترجمة:

1. إف. ستيفن لارابي، وآخرون، *بعد الأزمة الأوكرانية أوجه الضعف الأوروبية جراء الضغوط الروسية*، (سانتا مونيكا، كاليفورنيا: مؤسسة رند، 2017).
2. أندرو رادن، *الحرب الهجينة في منطقة البلطيق: التهديدات والاستجابات المحتملة*، (سانتا مونيكا، كاليفورنيا: مؤسسة راند، 2017).
3. اندروا سكوبيل، وعليرظا نادر، *الصين في الشرق الأوسط : التنين الحذر*، (سانتا مونيكا، كاليفورنيا: مؤسسة رند، 2020)،
4. إيهاب خليفة، *مجتمع ما بعد المعلومات : تأثير الثورة الصناعية الرابعة على الأمن القومي*، (القاهرة: العربي للنشر والتوزيع ،2019).
5. جانغ يون لينغ، وآخرون، *الحزام والطريق وتحولات الدبلوماسية الصينية في القرن 21* ، ترجمة: آية محمد الغازي، (مصر: دار صفصافة للنشر، 2017) .
6. جهاد عودة، *النظام الدولي نظريات وإشكاليات*، (مصر: دار الهدى للنشر والتوزيع ،2005).
7. حسن مظفر الرزو، *التهديد السيبراني الإيراني الملف المضاف إلى برنامجها* ، النووي،(برلين: المركز الديمقراطي العربي للدراسات الاستراتيجية والاقتصادية والسياسية، 2020).
8. سوفان مندال، *روسيا تبرز كثالث اكبر سوق للكتب الإلكترونية في العالم*، ترجمة: المكتبة الرقمية السعودية، (السعودية: المكتبة الرقمية السعودية،2017)،
9. عبد القادر دندن ، *الصعود الصيني والتحدي الطاقوي : الأبعاد والانعكاسات الإقليمية* ،(الأردن، مركز الكتاب الاكاديمي ، 2016).
10. نبيل العتوم، *الجيش الإلكتروني الإيراني*،(الأردن: مركز أمية للبحوث والدراسات الاستراتيجية – دار عمار للنشر والتوزيع،2015) .
11. نسيم طالب، *البجعة السوداء تداعيات الأحداث غير المتوقعة*، (بيروت: الدار العربية للعلوم ناشرون، 2009).
12. هاري أربارغر، *الاستراتيجية ومحترفو الأمن القومي التفكير الاستراتيجي وصياغة الاستراتيجية في القرن الحادي والعشرين*، ترجمة: محرز علي راجح ، (الإمارات: مركز الإمارات للدراسات والبحوث الاستراتيجية، 2011 .

ثانياً: المجلات/الدوريات العلمية:

1. جوزيف ناي، "مستقبل القوة"، حوار مع مجلة المجلة، عدد5، (سبتمبر 2011.(
2. رضا محمد هلال،" أدوات وقيود القوة الناعمة الروسية"، *مجلة السياسة الدولية*، مج 55، عدد 218، (يناير 2020).
3. سكوت بوسطن، وداور ماسكويت، "الطريقة الروسية في الحرب"، *مؤسسة راند للدراسات*، (2017).
4. سمير شرايطة، "السيادة السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومي"، *مجلة العلوم السياسة والعلاقات الدولية*، مج9 ، عدد 16، (كانون الثاني 2020).
5. سيرجي لافروف، "العالم في مفترق طرق ونظام العلاقات الدولية في المستقبل"، *مجلة روسيا في الشؤون العالمية*، وموقع وزارة الخارجية الروسية، (20 أيلول/سبتمبر 2019).
6. عبد الغفار الدويك، "تقرير التوازن العسكري 2019 قراءة تحليلية للقدرات السيبرانية في العالم"، *مجلة السياسة الدولية*، مج 54، عدد216، (أبريل 2019).
7. فراس الياس، "الوجه الأخر للقوة الناعمة الإيرانية"، المعهد الدولي للدراسات الإيرانية (رانش)،8 /يوليو/2018.
8. محمد بسوني ، "عقيدة جيراسيموف: دوافع الاستراتيجية الروسية لحرب المعلومات ضد الدول الغربية"، *مركز المستقبل للأبحاث والدراسات المتقدمة*، (أكتوبر 2017).
9. سعد قاسمي ، "عوامل تراجع القوة الإيرانية الناعمة في المنطقة العربية"، *مجلة الدراسات الإيرانية*، عدد10،(أكتوبر 2019).
10. عبد الصبور سماح ، "القوة الذكية: أدوات السياسة الخارجية الإيرانية تجاه لبنان"، *مجلة السياسة الدولية*،مج15 عدد 2،(2014).

ثالثاً: التقارير:

1." قدرات القرصنة السيبرانية الإيرانية"، تقرير خاص، مركز الملك فيصل للدراسات والبحوث،(كانون الأول ،2020).

رابعاً: الصحف والجرائد :

1. ري تشون،"القوة الناعمة لكوريا الشمالية"، جريدة الشرق الأوسط، عدد 14167، منشور بتاريخ 11 /9/ 2017.
2. نايف المرزوقي، طريق الحرير الرقمي ...مخاطر ومكافآت إلى الشرق الأوسط ، القبس ، 8/ 7/ 2020.

خامساً: الأنترنيت:

1. احمد يوسف الجميلي، "القدرات السيبرانية سلاح روسيا الفعال ضد الخصوم" ، *مركز صنع السياسات للدراسات الدولية والاستراتيجية*، مقال منشور بتاريخ 2018/6/19، على الرابط : https://www.makingpolicies.org/ar/posts/rusye.php

2. أماني يماني، "ضربات أمريكية سيبرانية موجعة لإيران"، مقال منشور بتاريخ 2020/1/22 ، على الرابط: https: //www.akkahnewspaper.com

3. "أنماط القوة الناعمة الصينية، مركز الروابط للبحوث والدراسات الاستراتيجية، مقال منشور بتاريخ 2015/8/29، على الرابط : https://rawabetcenter.com/archives

4. "إيران أسقطت بلا مبرر طائرة استطلاع أمريكية بدون طيار فوق المياه الدولية"، *قناة BBC*، خبر منشور بتاريخ 20/حزيران/يونيو/2019، على الرابط : https://www.bbc.com/arabic/middleeast

5. "بعد حركة غريبة جدا.. اليابان تبدي شكوكا حول صحة زعيم كوريا الشمالية"، *قناة الحرة* ، مقال منشور في 26/06/2020، على الرابط: https//www.alhurra.com

6. "الحرب الإلكترونية جيل جديد من الحروب لا نعرفه"، *نون بوست*، مقال منشور بتاريخ 2015/01/17، على الرابط : https://www.noonpost.com

7. "الحرب السيبرانية تهديدات حقيقية من العالم الافتراضي ،تقرير بتاريخ 2019/3/15,على الرابط: https: www.aa.com.tr

8. صالح حميد ، طهران: "تعرضنا لهجمات سيبرانية"، *قناة العربية*، مقال منشور بتاريخ 2020/7/23، على الرابط الاتي: https:// ww.alarabiya.net

9. طريق الحرير الرقمي مخاطر ومكافآت إلى الشرق الأوسط"، تقرير منشور بتاريخ2020/7/8، على الرابط: https://uabonline.org

10. عمر عبد العاطي، "حرب أمريكية مضادة للإرهاب السيبراني"، *جريدة الخليج* ،مقال منشور 21/ 3/ 2013 21/3/2013 ، على الرابط: https:www.alkhaleej.ae

11. "كوريا الشمالية وراء قرصنة موقع شركة سوني"، *تقرير مكتب التحقيقات الفدرالي الامريكي* ، 2014/12/19، على الرابط: https://ww.dw.com/ar

12. كونستانتين نوسكوف، وزير الاتصالات الروسي، تصريح صحفي، بوابة الاهرام، شوهد بتاريخ 16 /5/ 2020 على الرابط: http://gate.ahram.org.eg/News/2155154.aspx .

13. ليوبوف ستيبوشوفا، روسيا تؤثر على مصير 24 بلد في العالم، *مركز نون بوست*، مقال منشور بتاريخ 2017/01/15:على الرابط : www.noonpost.org/content/16194

14. محمد الحسيني ، "كيف أصبحت كوريا الشمالية ب6000 هاكرز إن تهدد امن الأنترنت"، *ترجمة ساسا بوست*، أكتوبر 2020 : على الرابط :
https://www.sasapost.com/translation/north-korea-hacking-cyber

15. محمد هيكل ، "زيادة وتيرة الهجمات السيبرانية بالتزامن مع جائحة كورونا، *نيويورك تايمز*: الولايات المتحدة تتهم الصين بمحاولة اختراق معلومات عن لقاح لفيروس "كورونا، *نيويورك تايمز*، تقرير منشور على الرابط: https://covid-19.ecsstudies.com

16. نايلة صليبي، "ماهي خلفية استراتيجية الصين في الحرب السيبرانية"، *مونتكارلو الدولية*، مقابلة تلفزيونية أجريت بتاريخ 2020/8/4، على الرابط : https: www.mc-doualiya.com/chronicles

17. نورهان الشيخ ، "موسكو وواشنطن صراع سيبراني"، *جريدة الخليج*، مقال منشور بتاريخ 6/27 2019 على الرابط : http://www.alkhaleej.ae

18. "هجمات إلكترونية تستهدف كوريا الجنوبية"، *الجزيرة* ، تقرير منشور بتاريخ 2013/3/21، على الرابط:https:www.alkhaleej.ae

19. ياسمين ايمن، "هل تشعل الحرب السيبرانية بين أمريكا وايران بعد مقتل سليماني؟" مقال منشور بتاريخ 2020/1/16، على الرابط: https://al-ain.com/article

English Sources

First: Journals &Magazine:

1. "Amry war College Pensylvania :US Spade layson Information As power ",*China Cyber Power and National Security*, (2012).
2. *Andrew Radin & Clint Reach ،"Russian Views Of The International Order", RAND Corporation ،(2017).*
3. Bilyana Lilly& Joe Cheravitch, "The Past, Present, and Future of Russia's Cyber Strategy and Forces", International Conference on Cyber Conflict,(12 th 2020).
4. Clayton Thomas," U.S. Killing of Qasem Soleimani: Frequently Asked Questions ", Congressional Research Service,(January 2020)..
5. David E. Sanger & Julian E. Barnes, U.S. Tried a More Aggressive Cyberstrategy, and the Feared Attacks Never Came, New York Times, (Nov. 9, 2020).
6. Eugene Rumer, "The Primakov (Not Gerasimov) Doctrine in Action", Carnegie Endowment for International Peace,(2019)..

7. Keir Giles, “Russia's public stance on cyberspace issues”, Cyber Conflict (CYCON), (2019)..
8. Michael E. DeVine, “Intelligence Community Spending: Trends and Issues”, Congressional Research Service,(November 2019)..
9. *Munish Sharma, “China's, Emergence as a Cyber Power”, Journal of Studies, Vol. 10,No.01,(2016).*
10. Neri Zilber ,”The Rise of the Cyber-Mercenaries”, Foreign Policy Magazine, (September 2018)..
11. *Nicu Popescu, “Russia's Soft Power Ambitions”, CEPS, policy brief, No.115, (October 2006).*
12. Ulia Kiseleva,“Russia's Soft Power Discourse: Identity”, Status and the Attraction of Power, *Politic*, Vol. 35 ,No. 3-4, (2015).