مجلة

كلية التـــراث الجامعة

مجلة علمية محكمة

متعددة التخصصات نصف سنوية

العدد السابع والثلاثون

15 حزيران 2023

ISSN 2074-5621

رقم الايداع في دار الكتب والوثائق 719 لسنة 2011

مجلة كلية التراث الجامعة معترف بها من قبل وزارة التعليم العالي والبحث العلمي بكتابها المرقم (ب 3059/4) والمؤرخ في (2014/ 4/7)

التحول في استراتيجية الحرب السيبرانية الروسية بعد عام 2008: جورجيا انموذجاً

م.م نورالدين عبدالله نايف

جامعة النهرين – كلية العلوم السياسية

المستخلص:

ان قضية الأمن السيبراني برزت كأحد التحوطات من الصراعات السياسية والاقتصادية بين الدول نتيجة الحروب الالكترونية أو الحروب السيبرانية التي باتت تستهدف البنى التحتية والمنشآت والمؤسسات الحكومية والغير حكومة والشبكات الصناعية والأبحاث وهي قادرة بشكل أو بآخر على تعطيل تشغيل البنى التحتية الحيوية، وفي هذا الجانب، كان لروسيا دوافع عديدة للقوة السيبرانية وتعزيزها منها سياسية، اقتصادية، عسكرية وأمنية، والتي اخذت تستخدمها في حروبها، وتزيد من مقوماتها ومؤهلاتها السيبرانية، لأنها أصبحت الحروب السيبرانية سمه مميزة لجميع الدول في حروبها.

كلمات مفتاحية: روسيا، الاستراتيجية السيبرانية، العقيدة السيبرانية، جورجيا.

Abstract:

The issue of cyber security has emerged as one of the precautions against political and economic conflicts between countries as a result of electronic wars or cyber wars that are now targeting infrastructure, governmental and non-governmental facilities and institutions, industrial networks and research, and they are capable in one way or another of disrupting the operation of vital infrastructures, and in this aspect, Russia had There are many motives for cyber power and its enhancement, including political, economic, military, and security, which it used in its wars, and increased its cyber components and qualifications, because cyber wars have become a distinctive feature of all countries in their wars.

Keywords: Russia, cyber strategy, cyber doctrine, Georgia.

المقدمة:

يمكن اعتبار تحدي الأمن السيبراني أعلى تحديات الأمن القومي في القرن الواحد والعشرين، مع الإشارة إلى أن المفهوم الحديث للأمن لا يقتصر فقط على الجوائب العسكرية، بل يواكب كل التهديدات والتحديات التي يمكن أن تشكل حاجزا أمام الاقتصاد الرقمي وتدفق المعرفة، فقد أسقطت تكنولوجيا المعلومات والاتصالات مفهوم الحدود الجغرافية، السياسية والثقافية بين الدول، ما يضع السيادة الوطنية في خطر شديد، خاصة مع اختراق المواقع الحكومية الرسمية والتجسس المعلوماتي على الدول، كما يبرز التحدي الثقافي والفكري كأحد أهم بوابات التهديدات السيبرانية، وذلك عن طريق الغزو الفكري في شبكات التواصل ونشر ثقافة العنف والإقصاء، والتحريض على الإجرام تحت ذرائع دينية، طائفية أو عصبية، ومن هنا اهتمت روسيا الاتحادية في الجانب السيبراني كونها قوى كبرى ومن الدول الساعية لتغيير النظام الدولي وذلك يتطلب منها إيلاء الاهتمام في الامن السيبراني لذا وضعت استراتيجية امنية سيبرانية محددة لها، كما استخدمت التكنلوجيا في حروبها التي خاضتها في جورجيا واوكرانيا وفي تحقيق هجمات محددة على الدول لتعتبر الأداة السيبرانية احدى الأدوات لتحقيق اهداف سياستها الخارجية.

اولا: اشكالية البحث

تنطلق اشكالية البحث من ماهي الاستراتيجية الروسية للأمن السيبراني؟ وكيف وظفتها في حروبها لتحقيق اهدافها؟ ماهي الامكانات الروسية في بناء استراتيجيتها الامن السيبراني ؟ وهل استخدمت روسيا في حربها على اوكرانيا الامن السيبراني؟

ثانيا: فرضية البحث

تنطلق فرضية البحث من ان لروسيا الاتحادية استراتيجية تهتم بالأمن السيبراني لتعزيز امنها ومصالها القومية، كما انها استخدمتها في حربها في جورجيا وتنافسها مع القوى الاخرى.

ثالثا: هيكلية البحث: قسم البحث الى ثلاث مباحث فضلاً عن المقدمة والخاتمة والاستنتاجات:

المبحث الاول: التدابير الاستراتيجية الروسية للأمن السيبراني:

المطلب الاول :التدابير الداخلية لاستراتيجية الامن السيبراني الروسي

المطلب الثاني :التدابير الخارجية الروسية للأمن السيبراني

المبحث الثاني: الاهتمام والعقيدة الجيوسيبرانية والقدرات الروسية للأمن السيبراني:

المطلب الأول :الاهتمام الروسي في الأمن السيبراني

المطلب الثاني :العقيدة الجيوسيبرانية والقدرات الروسية

المبحث الثالث :النموذج مختار (جورجيا):

المطلب الأول :الحرب السيبرانية الروسية –الجورجية

المطلب الثاني :مظاهر الحرب السيبرانية الروسية تجاه جورجيا ٢٠٠٨

المبحث الاول:

التدابير الاستراتيجية الروسية للأمن السيبراني

المطلب الاول: التدابير الداخلية لاستراتيجية الامن السيبراني الروسي:

يعد الامن السيبراني من اهم مجالات الامن في القرن الحادي والعشرين، ومن المعروف ان الهيمنة السيبرانية ترسم ملامح الحروب في القرن القائم مما يستلزم تغيير الاستراتيجية في اتجاه التصعيد مع قوى اخرى معادية في ساحة الحرب السيبرانية، ولكن هذا يتوقف على ما تمتلكه الدولة من قدرات تجعلها قادرة على الصمود والمواجهة وحماية امنها السيبراني.

اولا: التدابير التقنية الروسية:

بدأ الاهتمام الروسي بالأبعاد السياسية للأمن الإلكتروني في التسعينات، بعد تأسيس مجلس الأمن الروسي في عام 1992، وإضافة إلى المؤسسات الأمنية الروسية تم إنشاء مؤسسات أخرى تختص فقط بالقضايا الإلكترونية وبحماية الأمن الإلكتروني الروسي، ومن أهم المؤسسات المسؤولة عن الأمن الإلكتروني في روسيا هو مجلس الأمن، وجهاز الأمن الفيدرالي، جهاز الحرس الفيدرالي، والجهاز الفيدرالي للتحكم التقني، ووزارة الاتصالات وتكنولوجيا المعلومات، وتنقسم المهام ما بين الإدارات المختلفة في الأنشطة المتعلقة بالأمن الإلكتروني كالتالي: تختص وزارة الداخلية بمواجهة الجرائم الإلكترونية، ووزارة الدفاع مسؤولة عن كل ما يتعلق بأخطار الحروب الإلكترونية وتطوير القدرات الإلكترونية الهجومية للجيش الروسي، ويهتم جهاز الأمن الفيدرالي بالإرهاب الإلكتروني، هذا التقسيم قائم بالأساس على التفرقة ما بين الأبعاد الإجرامية، والارهابية، والعسكرية، والسياسية للأمن الإلكتروني[1].

اعلنت روسيا عزمها عن تطوير السلاح الجوي والفضائي رداً على الدرع الصاروخي في العام 2005، لإعادة التسليح خلال العقد المقبل والعمل على استعادة موقع الزعامة في كافة التكنولوجيات العسكرية[2].

وقد عرفت روسيا نتيجة لتطور تقنياتها بما يسمى بحرب التضليل، اذ شهدت استخدام التقنيات للتأثير على هياكل الدولة والسكان بمساعدة شبكات المعلومات، محاولة للتأثير على الرأي العام بالدرجة الاساس، وتقليل ارادة الخصم للمقاومة، بما

[1] .اماني عصام، استخدام روسيا للقوة السيبرانية في إدارة تفاعلاتها الدولية، مجلة كلية الاقتصاد والعلوم السياسية، العدد(4)، المجلد(22)، كلية الاقتصاد والعلوم السياسية، جامعة حلوان، مصر، 2021، ص173.

[2] .اميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد(35)، كلية الشريعة والقانون، جامعة الامارات، الامارات، 2020، ص520.

يحقق لروسيا اهدافها وبنفس الوقت يحافظ على درجة معقولة من الانكار فيما بتعلق بمشاركتها في حملات التضليل، والنقطة الاساس هنا هو ان روسيا تلجأ لهذا الاسلوب قبل بدء عملياتها العسكرية التقليدية كوسيلة لأعداد ساحة المعركة المحتملة، ذا ان الحرب النفسية ستضع اساساً للنصر الى حد كبير[3].

لقد شنت روسيا حربها على اوكرانيا في 24 فبراير 2022، لكن الهجمات الالكترونية الروسية استمرت منذ ضم روسيا لجزيرة القرم في العام 2014، ولكنها تكثفت قبل عام في 2022 على البنى التحتية الاوكرانية مثل وسائل الاعلام والمالية والطاقة، حيث عانت هذه القطاعات، ومن اهم الهجمات الروسية هي محاولة منع اوكرانيا للوصول الى بياناتها الخاصة والمعلومات الاساسية، او نشر معلومات مزيفة على مواقعها الخاصة[4].

ثانيا: الوكالات الروسية المتخصصة:

توجد في روسيا اربعة وكالات رئيسية متخصصة في حرب المعلومات وهي[5]:

1. دائرة الحماية الاتحادية FSO : وهو الجهاز المختص في ضمان الامن الالكتروني للموظفين الحكوميين ورجال الدولة، وتتركز مهمته في الدفاع عن الشبكات الحكومية.
2. جهاز الامن الاتحاديFSB : وهو جهاز مسؤول عن الامن داخل الدولة.
3. الاستخبارات الخارجية SVR : هو المسؤول عن جمع الاستخبارات الاجنبية باستخدام الطرق البشرية والاشارات والالكترونية والسيبرانية، وهو جهاز تابع للرئيس، وهو الذي يوفر المعلومات الاستخبارية.
4. جهاز الاستخبارات العسكرية GRU : وهو نظام استخبارات يستخدم بشكل شامل جميع قوى ووسائل الاستخبارات تقريباً، على اعتباره يقوم بالعديد من الانشطة الاستخباراتية.

ان هذا التقسيم قائم بالأساس على التفرقة ما بين الابعاد الاجرامية والارهابية والعسكرية والسياسية للأمن السيبراني، ولقد تبلور الاهتمام الروسي بقضايا الامن السيبراني في عام 2000، عندما قامت روسيا بتطوير استراتيجية امنية تبنى على اساس الايمان الكامل، بالدور الذي يلعبه الامن السيبراني في تحقيق المصالح القومية وتعزيز الاستقرار الاجتماعي والسياسي، وتتصدر روسيا الدول الساعية لتطوير اتفاقية دولية لمواجهة المخاطر السيبرانية والحيلولة من دون حدوث سباق للتسلح الالكتروني نتيجة لتزايد التنافس التكنولوجي ما بين الفواعل على المستوى الدولي، ويتم من خلالها وضع تعريفات واضحة ويقبلها المجتمع الدولي لكافة المفاهيم المحورية ذات الصلة بالفضاء السيبراني[6].

المطلب الثاني: التدابير الخارجية الروسية للأمن السيبراني:

اتخذت روسيا عقيدة مختلفة عن الغرب، من اجل مواجهة التهديدات الخارجية في مجال الامن السيبراني، وهذه العقيدة لها مرتكزات اساسية اقامت عليها استراتيجية الامن السيبراني الروسي في تدابيرها الخارجية.

اولا: العقيدة الروسية الخارجية للأمن السيبراني:

تدور مضامين العقيدة الروسية على الآتي[7]:

1. اثارة المشكلات الداخلية، حيث تنطوي حرب المعلومات الروسية على التكريس لأوضاع داخلية وازمات في المجتمعات الغربية.
2. مواجهة العقوبات الغربية بعد الازمة الاوكرانية.
3. تشويه القوى المناهضة، حيث وظفت روسيا المعلومات لتشكيل سرديات وروايات تشوه القوى المناهضة لها.

---

[3] Michael Connell and Sarah Vogler, Russia's Approach to Cyber Warfare, Center for Strategic Studies, International Affairs Group, (March 2017), P.4.

[4] Jakub Przetacznik with Simona Tarpova, Russia's war on Ukraine: Timeline of cyber-attacks, EPRS | European Service, (June 2022), p.1. Parliamentary Research

[5] حارك فاتح، الفضاء السيبراني والتحول في شكل الحروب: دراسة حالة روسيا، دار فاضي للنشر والترجمة، الجزائر، 2019، ص ص 58-59.

[6] Keir Giles, Russia Public Stance on Cyberspace Issues Conference on Cyber Confict, Publications, Tallinn, pp 63- 75.

[7] علي زياد فتحي، رؤية استراتيجية العمليات السيبرانية الاوروأطلسية ومهددات الجيوسيبرانية الروسية" رؤية في الاشتباك السيبراني الاورو-روسي"، مجلة حمورابي، العدد(30)، بغداد، 2019، ص ص5-6.

4. خلق بنية متسامحة، وهذا يجري عبر وسائل الاعلام الجماهيري والاجتماعي لإحداث تأثير في اراء وتوجهات الافراد العاديين.
5. تقويض القدرة على المواجهة، فكثيراً من حرب المعلومات الروسية وخاصة القرصنة الالكترونية تضعف من امكانيات خصوم روسيا.

ان احد الاهداف الرئيسة لواضعي العقيدة للأمن السيبراني، هو الرد الاستراتيجي والوقاية من النزاعات العسكرية، والتي يمكن ان تنجم عن استخدام تكنلوجيا المعلومات، وكما يقول (اوليغد يميدوف)، وهو خبير في الامن السيبراني، مؤسسة الرأي الروسية بي اي ار:" العقيدة في شكلها الحالي هي العقيدة الافضل بما يخص التهديدات الموجهة للأمن العسكري والتكنولوجي في روسيا، على سبيل المثال هي تعمل على الحماية من العمليات السيبرانية من قبل الاجهزة الخاصة الاجنبية، فضلا عن مكافحة النشاط الاستطلاعي الاجنبي في روسيا، ويشير الخبير الى ان الحكومة الروسية اولت اهتماماً خاصا لمواجهة " ثورات تويتر" الجديدة كتلك التي حدثت في الشرق الاوسط في بداية العقد الحالي[8].

واقر مجلس الدوما الروسي في عام 2017، مشروع قرار يهدف الى عزل روسيا عن شبكة الانترنيت العالمية، وان الادارة الروسية تدعي ان الغاية من هذا المشروع هو تحصين الامن القومي الروسي وامن المواطنين، من الاعداء وبذلك تحصن البلاد من اي هجمات سيبرانية خارجية، خاصة من قبل الولايات المتحدة الامريكية، التي يعتقد الروس انها تتبع بشكل متزايد استراتيجية سيبرانية عدائية، والى جانب ذلك طالبت الحكومة الروسية شركات الاتصالات الروسية بتوفير تقنيات تكنلوجية متطورة تستطيع الحكومة المركزية التحكم من خلالها، كما طالب الشركات بتطوير شبكات الانترنيت لتلبي احتياجاتها الامنية وامن المعلومات للمستخدمين والدوائر وللوزارات الحكومية والبنية التحتية الالكترونية، وان هذه الخطوة تهدف الى حماية الجانب الروسي من الشبكة العالمية في الوقت المطلوب[9].

ومن ثم ابرز سمات الامن السيبراني الروسي هو تطبيق السيادة الوطنية على الفضاء السيبراني، لذا فأن السيادة السيبرانية، ودور الدولة في مجال المعلومات والتنظيم والسيطرة، هي مرتكزات اساسية لاستراتيجية الامن السيبراني الروسي، وهو ما يجعلها عاملاً معوقاً في بناء المعايير الدولية المتعلقة بالأمن السيبراني من وجهة نظر الدول الغربية، بل وذكر هذا المنظور الروسي في العديد من الوثائق المعنية بعقيدة الاتحاد الروسي في ضمان امن المعلومات، والذي يظهر نية الحكومة الروسية لقيادة الجهود الدولية لتحقيق درجات عالية من الامن، وذلك من خلال العديد من الطرق القانونية والمؤسسية والتكنلوجية وغيرها[10].

ثالثا: نقاط الضعف السيبرانية الروسية الداخلية والخارجية

تواجه روسيا تحديات كبيرة في العمليات السيبرانية وهي[11]:

1. تواجه الاجهزة الامنية الروسية تحديات في توظيف موظفين مؤهلين، حيث تتنافس فرص القطاع الخاص والوكالات المنافسة على المواهب.
2. تشتهر الاجهزة الروسية ايضا بمستويات عالية من الفساد.
3. غالبا ما تستعين روسيا بأجهزة امن خارجية من القراصنة المدنيين.
4. تم الكشف عن العديد من العملاء داخل استخبارات الامن الروسية، وقيل عنهم ضباط امن فاسدين، وكانوا مسؤولين عن العديد من عمليات الاغتيالات لشخيصات مهمة، مثل ما حدث في العام 2020 حينما حددت وسائل الاعلام عملاء داخل FSB الذين ورد انهم مسؤولين عن محاولة اغتيال المعارض الروسي (اليكسي نافالني) .

---

[8].اسماعيل زروفة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، العدد(1)، كلية العلوم القانونية والسياسية، جامعة محمد بوضياف المسيلة، الجزائر، 2016، ص1026.

[9].افتكار مانع، قانون سيادة الانترنت في روسيا هل هو بداية لحرب الكترونية، موقع الجزيرة ، 2019، متوفر على الموقع: www.aljazeera.net

[10]. Franz – Stafan Greg and Greg Autsin , Russia the United States and Cyber Diplomacy; Opening the Doors the Doors , East West Insttiute, pp 5-6.

[11]. Russian Cyber Units, Congressional Research Service(IN FOCUS), (February 2022), p.2.

5. ما زالت روسيا تفتقر الى المعرفة الكافية لدعم وتطوير التكنولوجيا.

فضلا عن ان روسيا الاتحادية تواجه مشاكل اخرى مثل العامل الديمغرافي ومناخ الاعمال الغير مناسب للابتكار، علاوة على ذلك تعاني روسيا من العديد من الانخفاضات في مجال العلوم والتكنولوجيا والابتكار، انخفاض القدرة التنافسية العالمية، وانخفاض مستوى انشطة الابتكار، وانخفاض مستوى القيمة المضافة في الصادرات التكنولوجية، والمستوى المنخفض العام للإنتاج عالي التقنية والمعرفي المكثف، فضلا عن انخفاض مستوى براءات الاختراع التجارية القابلة للتطبيق عالمياً، اذ يستثمر القطاع الخاص بشكل متواضع فقط في البحث والتطوير ولا ينفق سوى نسبة منخفضة من هذه الاستثمارات على اكتساب التقنيات الجديدة وبراءات الاختراع والترخيص[12].

المبحث الثاني:

الاهتمام والعقيدة الجيوسيبرانية والقدرات الروسية للأمن السيبراني:

المطلب الأول: الاهتمام الروسي في الأمن السيبراني:

تبلور الاهتمام الروسي بقضايا الأمن السيبراني في عام ٢٠٠٠، عندما طورت روسيا استراتيجية أمنية تقوم على الإيمان الكامل بالدور الذي يلعبه الأمن السيبراني في تحقيق المصالح الوطنية وتعزيز الاستقرار الاجتماعي والسياسي، تسعى روسيا لتطوير اتفاقية دولية لمنع سباق التسلح الإلكتروني نتيجة المنافسة التكنولوجية المتزايدة بين الجهات الفاعلة على المستوى الدولي[13].

عمل بوتين على ان الأمن السيبراني أولوية قصوى على المستوى الوطني خلال عقدين من حكمه كرئيس لروسيا، بدءا من عام ٢٠٠٠؛ صدر أول ميثاق لأمن المعلومات في غضون أشهر من تنصيبه كرئيس في عام ٢٠٠٠ ونظرا في العدد المتزايد للهجمات الإلكترونية الخارجية التي نسبتها الحكومات والشركات الغربية إلى القوات المسلحة الروسية والجهات الفاعلة الروسية الأخرى من خلال عمليات معقدة تقنيا فمن الأمن أن نفترض أن روسيا تمتلك أيضا امكانات استخباراتية إلكترونية إقليمية وعالمية واسعة النطاق[14].

وتعتمد الاستراتيجية الروسية على محاولة تعطيل البنية التحتية للمعلومات لدى الخصم، والاتصالات المدنية والعسكرية قبل بدء العمليات العسكرية التقليدية، وبحسب العقيدة العسكرية الروسية، فإن الهجوم العسكري الناجح يجب أن يسبقه عمليات أخرى تهدف إلى منع الخصم من الحصول على معلومات من مصادر خارجية وتعطيل عمليات التجارة المالية والائتمانية، ومحاولة التأثير في الرأي العام في دولة الخصم من خلال عمليات كاذبة للمعلومات والدعاية التي تخدم المصالح الروسية، وأبرز مثال على تلك الهجمات التي اتهمت روسيا بها عام ٢٠٠٨ ضد جورجيا قبل توجيه ضربة عسكرية لها[15].

من ناحية أخرى، تعتزم روسيا من خلال منظمة (بريكس)، إنشاء فضاء إلكتروني خاص بها مستقل عن الإنترنت الحالي من أجل التخلص من الهيمنة وعمليات التجسس الإلكتروني الأمريكية، وقد اتخذت خطوات فعلية للقيام بذلك إذ تقوم البرازيل ببناء نظام كابلات يمكنه ربطها بروسيا والصين وجنوب إفريقيا يبلغ طوله ٣٤ ألف كيلومتر، ويربط بين مدينة (فلاديفوستوك) شرقي روسيا و(فورتاليزا) في البرازيل ، مروراً بشانتو بالصين و(تشيناي) الهندية و(كيب تاون) بجنوب إفريقيا يوفر المشروع خدمات الإنترنت في ٢١ دولة أفريقية وبالتالي خلق إنترنت جديد مواز للإنترنت الحالي، ولكي يكون منافسا قويا للولايات المتحدة وتعتزم دول البريكس أيضا تمرير تشريعات تلزم القوى الرئيسة في الإنترنت مثل (Facebook) (Google) و (Yahoo) لتخزين جميع المعلومات التي يتم جمعها داخل دول المجموعة محليا بحيث لا تتمكن وكالة الأمن القومي الأمريكية من الوصول إليها[16].

---

[12] .Santtu Lehtinen, Sinikukka Saari, Arho Suominen (Eds.), Russia's technological policy and knowhow in a competitive global context, Prime Minister's Office, Finland, 2022, P.33.

[13]. أماني عصام محمد، مصدر سبق ذكره، ص١٧٣.

[14]. دراسة حديثة: كيف تشكل القدرات السيبرانية موازين القوى محلياً ودولياً؟، موقع كيوبوست، ٢٠٢١، متاح على الرابط التالي: https://www.qposts.com

[15]. أماني عصام محمد، مصدر سبق ذكره ، ص ص١٧٤-١٧٥.

[16]. أماني عصام محمد ، المصدر نفسه، ص١٧٤.

كما أنشأت روسيا الاتحادية وكالة أبحاث الإنترنت، أو ما يعرف باسم Troll Arm جيش المتصيدين التابعة لوكالة الأمن الفيدرالية الروسية، التي تضم آلاف الموظفين، وتخصص سنويا حوالي (٣٠٠) مليون دولار من ميزانية الدفاع الروسية، ويحتل الجيش السيبراني الروسي المرتبة الخامسة بين أقوى الجيوش الإلكترونية في العالم بعد كل من الولايات المتحدة الأمريكية، والصين، وبريطانيا، وكوريا الشمالية على التوالي وتتلخص مهام الجيش الإلكتروني الروسي في ما يأتي[17]:

- القيام بعمليات تجسس على المعارضين.
- حروب المعلومات في وسائل الإعلام والشبكات الاجتماعية، من خلال اختراق الحسابات والبريد الإلكتروني، وإنشاء حسابات وهمية على شبكة المعلومات الدولية، وفتح آلاف الحسابات الوهمية على مواقع التواصل الاجتماعي، للرد على الآلاف من التعليقات والمقالات ونشر الشائعات وتظليل الحقائق في محاولة لدعم الموقف الروسي وتوجيه الرأي العام ضد المعارضين.
- شن هجمات إلكترونية من شأنها إلحاق الضرر بالبنية التحتية والاقتصاد والمواقع الحكومية في دول أجنبية معادية.

وان من أبرز سمات الأمن السيبراني الروسي تطبيق السيادة الوطنية على الفضاء السيبراني؛ لذلك فإن (السيادة الإلكترونية) ودور الدولة في مجال المعلومات والتنظيم والرقابة هي ركائز أساسية لاستراتيجية الأمن السيبراني الروسية، مما يجعلها عاملاً معوقا في بناء المعايير الدولية المتعلقة بالأمن السيبراني من وجهة نظر الدول الغربية، وحتى هذا المنظور الروسي ورد ذكره في العديد من الوثائق حول عقيدة الاتحاد الروسي لـ (ضمان أمن المعلومات)، مما يدل على نية الحكومة الروسية لقيادة الجهود الدولية لتحقيق درجات عالية من الأمن وهو ما تنتقده بشدة قوى غربية مثل الولايات المتحدة، التي ترى أنها تمارس سياسات استبدادية لقمع حريات المعارضة الروسية، وأن هذا يعبر عن سيطرة مفرطة على الفضاء الإلكتروني على الرغم من حقيقة أن المبدأ الأول في استراتيجية الأمن السيبراني الروسية يتضمن حرية المواطنين وحقوقهم الدستورية18.

المطلب الثاني: العقيدة الجيوسيبرانية والقدرات الروسية:

أولاً: العقيدة الجيوسيبرانية في الاستراتيجية الروسية:

لقد تبلورت العقيدة الجيوسيبرانية الروسية من خلال الوثيقة الخاصة بوزارة الدفاع الروسية والتي تحمل عنوان مفهوم الأنشطة الفضائية المعلوماتية للقوات الروسية المسلحة لتوضح الإطار المهم الذي تقوم به المعلومات في صياغة الإطار الاستراتيجي الروسي، وتبنت الوثيقة - كما سبق وأن تم توضيحه من قبل تعريف الفضاء المعلوماتي على أنه هو ذلك المجال الخاص بالأنشطة المتصلة بتكوين المعلومات واستخدامها ونقلها، فضلاً عن ما يطلق عليها عقيدة "جيراسيموف"، والتي تحتوي على عدد من الأفكار التي تخص الوسائل الغير تقليدية في الحروب الحالية حيث تزايد اللجوء إليها في روسيا خلال الفترة السابقة مع السعي الحثيث لروسيا كي تستعيد الإرث التقليدي كقوة مؤثرة في النظام الدولي، ما يستلزمه ذلك من توظيف أدوات الحرب السيبرانية، وفي هذا السياق، اعتمدت روسيا على عقيدة أمن المعلومات في الاتحاد الروسي، وأكدت الوثيقة على البعد العسكري لمسالة المعلومات كأساس لأمن الدولة، وتحدد أسلحة المعلومات باعتبارها إحدى الأدوات لتحقيق الأهداف السياسية، وتتمثل مفردات هذه العقيدة في19:

١. تقويض القدرة على المواجهة: فالعديد من عمليات الحرب المعلوماتية التي تقوم بها روسيا وعلى وجه الخصوص المتعلقة بـالقرصنة الإلكترونية تهدف في المقام الأول إلى إضعاف إمكانات خصوم روسيا، وتقليل القدرة على المواجهة، وهو ما بدا واضحاً في الحرب الروسية الجورجية عام ٢٠٠٨ ؛ حيث أن التهديدات السيبرانية التي قامت بها روسيا في الدولة الجورجية في نفس وقت دخول القوات الروسية أدت إلى تعطيل الاستجابة الجورجية للغزو الروسي لها؛ حيث أضعفت عمليات القرصنة التي قامت بها روسيا قنوات تواصل الحكومة مع المواطنين، وإيقاف المعاملات المالية وعرقلة انتقال المعلومات حول ما يحدث في مناطق الحرب إلى العالم الخارجي.

---

[17] . احمد يوسف الجميلي ، القدرات السيبرانية، مركز صنع السياسات للدراسات الاستراتيجية، ٢٠١٨، متاح على الرابط التالي: https://www.makingpolicies.org/ar/posts/rusye.php

[18] . عادل عبد الصادق ، صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية ، مقال منشور على موقع المركز العربي لأبحاث الفضاء الإلكتروني، ٢٠١٩، متاح على الرابط التالي: https://accronline.com/article_detail.aspx

[19] . علي زياد فتحي، مصدر سبق ذكره، ص ص٥-٦.

٢. توظيف المعلومات ضد القوي المناهضة: ويتضح ذلك من خلال ما قامت به روسيا من توظيف المعلومات ضد القوي المناهضة لها مثلما حدث في جورجيا وأوكرانيا، بأن ما حدث كان نتاجاً للتدخلات الأمريكية، وفي الوقت ذاته تشييد صور إيجابية لحلفائها.

٣. مواجهة العقوبات الغربية وهذا ما يمكن ملاحظته عقب التدخل الروسي في أوكرانيا عام ٢٠١٤، بعد استفتاء مارس ٢٠١٤م ، وضم شبه جزيرة القرم، وتزايد العزلة الأوروبية المفروضة على روسيا، وفي عام ٢٠٢٢ أيضاً عقب تدخلها في أوكرانيا والتي تضمنت عدداً من العقوبات التجارية والاقتصادية.

ثانيا: القدرات والامكانيات السيبرانية الروسية:

عند تحليل العقيدة الإلكترونية الروسية أنه لا توجد كلمة (cyber) ولا مصطلح (الحرب المختلطة) موجودان بشكل مستقل في الإطار المفاهيمي الروسي بدلاً من تلك يتم استخدامه بشكل حصري تقريبا للإشارة إلى الأنشطة الغربية، وتعامل روسيا الفضاء الإلكتروني كعنصر ثانوي في عقيدة حرب المعلومات الشاملة، والعمليات الإلكترونية في نظر العقل الروسي، على نطاق أوسع "الية لتمكين سيطرة الدولة حول مشهد المعلومات بدلاً من عده آلية ضيقة لتحقيق تأثيرات منفصلة على أنظمة الاتصالات يتضح هذا التمييز في الاستخدام الروسي لمصطلح (أمن المعلومات) بدلاً من المفهوم التقني الضيق لـ (الأمن السيبراني) السائد في المناقشات الأمريكية20.

تستند الاستراتيجية الروسية إلى حقيقة أن الأمن السيبراني والعمليات ذات الصلة هي ركائز أساسية في مواجهة المعلومات مع الغرب وإذ تشير المصادر الروسية إلى (فضاء المعلومات) بدلا من (القضاء الإلكتروني) فقد تم تصميم الاستراتيجية في جوهرها بهدف دمج العمليات الإلكترونية التقنية مع وسائل أخرى لتحقيق التميز المعلوماتي فضلا عن ذلك روسيا قوة فضائية مكتفية ذاتيا وهي تدير شبكات الاتصالات الخاصة بها وتقنيات الملاحة عبر الأقمار الصناعية التي تخدم كلا من الأغراض المدنية والعسكرية فضلاً عن الأقمار الصناعية المخصصة لخدمة مجموعة من الوظائف الأخرى، يعادل نظام الملاحة الأقمار الصناعية الروسي قوة نظام تحديد المواقع العالمي في الولايات المتحدة، مع وجود ٢٤ قمراً صناعياً عاملاً توفر تغطية عالمية كاملة21.

المبحث الثالث: النموذج مختار (جورجيا):

المطلب الأول: الحرب السيبرانية الروسية – الجورجية:

هاجمت روسيا مجموعة من المواقع إلكترونية جورجية وغربية عام ٢٠٠٨، أثناء حربها مع جورجيا بما في ذلك مواقع حكومية ومصرفية وبرلمانية وقضائية، والسفارات البريطانية والأمريكية في جورجيا وذلك لعرقلة الاتصالات الداخلية والخارجية بين الحكومة والشعب الجورجي بحيث تكون هذه الهجمات من أولى الهجمات في سلسلة حروب جديدة في القرن الحادي والعشرين.

تقع أوسيتيا الجنوبية في وسط جورجيا في الشمال وحدودها متاخمة لجمهورية أوسيتيا الشمالية، غالبية الأوسيتيين في جمهورية الجنوب هم من المسيحيين، استولت روسيا على أوسيتيا بأكملها بعد الثورة البلشفية قسمتها إلى كيانين، ضمت الشمال إلى الاتحاد الروسي والجنوب الى جورجيا، وجورجيا تمنع توحيد أوسيتيا الجنوبية والشمالية، وبدأ التوتر في العلاقة بين أوسيتيا الجنوبية وجورجيا مع ميل الأخيرة للاستقلال عن الاتحاد السوفيتي مع بداية التسعينيات، أعلنت أوسيتيا الجنوبية عزمها إعلان المنطقة تحت النفوذ الروسي، وهو ما اعترض عليه البرلمان الجورجي فبدأت المواجهات بين الانفصاليين في أوسيتيا والشرطة الجورجية، التي أسفرت عن مقتل أكثر من عشرة أشخاص22.

وفي عام ١٩٩١ فرضت جورجيا استخدام اللغة الجورجية في جميع الإدارات الأوسيتية وهذا يشكل تحديا للقادة الانفصاليين الذين يطالبون باستخدام اللغة الأوسيتية في منطقتهم، ظلت هذه المنطقة منطقة توترات مستمرة حتى وقعت حرب الأيام الخمسة في ٧ آب ٢٠٠٨ و عبرت القوات الروسية بشكل غير قانوني الحدود الروسية الجورجية ودخلت منطقة الصراع

---

[20] Sarah P.White .Understanding Cyberwarfare, Lessons from the Russia-Georgia War. modernwar institute at west point, 2018, p 2.

[21]. دراسة حديثة: كيف تشكل القدرات السيبرانية موازين القوى محليا ودولياً ، مصدر سبق ذكره.

[22]. أحمد نزيه، حكاية اوسيتيا الجنوبية (أرض الحرب) التي راقبتها (ميركل) بالمنظار، موقع أخبار اليوم، ٢٠١٨ ، متاح على الرابط التالي: https://m.akhbarelyom.com

في أوسيتيا الجنوبية، ثم اتهمت جورجيا بـ (العدوان على أوسيتيا الجنوبية) وشنت غزوا واسع النطاق لجورجيا، ونظم الجيش الروسي غارات جوية وغارات برية ضد قوات الجيش الجورجي في أوسيتيا الجنوبية فضلا عن إلى الأراضي الجورجية غير المتنازع عليها، وكان أهمها قصف مدينة جوري التي تبعد أميال قليلة عن العاصمة الجورجية تبليسي، كما فتحت القوات العسكرية الروسية والأبخازية جبهة ثانية بشن هجوم على وادي (كودوري) في غرب جورجيا، على الحدود الفعلية في أبخازيا ثاني منطقة انفصالية في جورجيا، لقد دخلت البحرية الروسية أيضا في الغزو، وحاصرت جزءا من الساحل الجورجي على البحر الأسود بالقرب من منطقة أبخازيا[23].

أوقفت الحكومة الجورجية بث القنوات التلفزيونية الروسية ومنعت الوصول إلى المواقع الروسية أثناء الحرب وبعدها ، مما حد من التغطية الإخبارية في جورجيا، في ٨ - ١٠ أغسطس ٢٠٠٨ بثت قناة RT عدة تقارير إخبارية حول الحرب في جورجيا، و في ٩ أب ٢٠٠٨ ، وصف السفير الروسي لدى جورجيا (فياتشيسلاف كوفالينكو) الإجراءات الجورجية بأنها (أكثر عمل تخريبي حقيقي) وزعم أن مدينة (تسخينفالي) لم تعد موجودة، وأن الجيش الجورجي قد دمرها، وفي ١٠ آب ٢٠٠٨ ، اتهم نائب وزير الخارجية الروسي (غريغوري كاراسين) وسائل الإعلام الأجنبية بالتحيز المؤيد لجورجيا في تغطيتها للصراع بين جورجيا وروسيا حول أوسيتيا الجنوبية الانفصالية.

و ابتداء من اليوم الثاني للحرب، استشهد المسؤولون في الحكومة الروسية وأوسيتيا الجنوبية مرارا وتكرارا بأرقام الوفيات المدنية في أوسيتيا الجنوبية من الهجمات الجورجية التي تراوحت بين ١٤٠٠، الى أكثر من ٢٠٠٠ وفاة، وقد استخدم هذا كأحد المبررات الرئيسة بالنسبة للتدخل الروسي، إذ أشار (ديمتري ميدفيديف) في ١٠ أب ٢٠٠٨، الشكل الذي اتخذه هذا العنوان ليس أقل من إبادة جماعية لأن جورجيا ارتكبت أبشع الجرائم[24].

المطلب الثاني: مظاهر الحرب السيبرانية الروسية تجاه جورجيا ٢٠٠٨:

تم تنفيذ الموجة الأولى من الهجمات الإلكترونية في ٦-٧ آب ٢٠٠٨ بوساطة شبكات الروبوت وأنظمة القيادة والتحكم التي ارتبطت بروسيا، وبعد يومين بدأت العمليات العسكرية الروسية ومن ضربت الموجة الثانية من خلال المنشورات على مواقع الويب، وعلى الرغم من اقتصار الهجمات الإلكترونية على الحرمان من الخدمة وعمليات تشويه المواقع الإلكترونية ، وهي أنواع غير معقدة نسبيًا من الهجمات إلا أنها نفذت على نطاق واسع جدا وبعد أن استمكنت القوات الروسية مواقعها في جورجيا تم توسيع قائمة الهجمات لتشمل العديد من المواقع الإلكترونية للوكالات الحكومية والمؤسسات المالية ومجموعات الأعمال والمؤسسات التعليمية ووسائل الإعلام الإخبارية ومنتدى القرصنة الجورجي لمنع أي استجابة فعالة أو منظمة للوجود الروسي[25].

وفي تقرير صادر من معهد أبحاث الولايات المتحدة الأمريكية الذي أكد على أن هذه الهجمات السيبرانية على جورجيا نفذتها الاستخبارات الروسية وقراصنة يستخدمون أجهزة كمبيوتر موجودة في كل من روسيا واوكرانيا ولاتيفيا، استهدفوا الشبكات المالية والإعلامية لجورجيا أثناء حرب أوسيتيا الجنوبية[26].

لقد تميز الهجوم السيبراني الروسي على جورجيا بتعدد الجنسيات للمهاجمين، مما يثير قضايا قانونية متنوعة ريما ستترافق أي استخدام لطرف ثالث في ساحة المعركة الإلكترونية ، كون استخدام المواطنين المتسللين وغيرهم من الجهات الفاعلة غير الحكومية يعقد اختيار الإطار القانوني المناسب الذي سيحكم الاستجابة الدولية كما وضح مركز التميز للدفاع السيبراني التعاوني CCD COE فإن الأعمال العدائية الجسدية تواجه بتطبيق قانون النزاعات المسلحة، الذي يعرف بأنه (أي اختلاف ينشأ بين دولتين يؤدي إلى تدخل القوات المسلحة) في حين نظر كل من اتفاقية مجلس أوروبا (COE) والقانون الأمريكي

---

[23]. مايا أوتاراشفيني، حزب روسيا وجورجيا بعد مرور 10 أعوام هل تعلم الغرب؟، مجلة المجلة، ٢٠١٨، متاح على الرابط التالي: https://arb.majalla.com/node

[24]. تقرير، حرب المعلومات خلال الحرب الروسية الجورجية، متاح على الرابط التالي: https://stringfixer.com/ar/Infomation_war_during_the_Russo-Georgian_War.

[25]. Stephen Blank, Cyber War and Information War à la Russe, From Understanding Cyber Conflict: Fourteen Analogies George Perkovich and Ariel E. Levite, Editors, Published by Georgetown University Press, November 2017, p 90.

[26]. علي زياد فتحي، مصدر سبق ذكره، ص ١٢ .

الحالي إلى الهجوم السيبراني ضد جورجيا بوصفة جريمة إلكترونية ، بينما استفادت إستونيا من إطار قانوني أكثر تطوراً لتكنولوجيا المعلومات والاتصالات ساعد في توجيه استجابتها للهجوم الإلكتروني الروسي في عام ٢٠٠٧ ، ولم تستفد جورجيا من أي شيء مشابه في قانونها المحلي[27].

نتيجة قلة اعتماد جورجيا نسبيا على تقنية المعلومات والاتصالات، إلا أن هذا الهجوم أكد على أنه حتى تلك الدول التي لا تعتمد بشكل كبير على تكنولوجيا المعلومات يمكن أن تتضرر في حالة تعرضها لهجوم سيبراني وذلك من حيث ضمان دقة تدفق المعلومات للشعب داخل البلد، ومع ذلك يلاحظ أن الهجوم السيبراني كان محدودا، ولم يستهدف أهدافا أكثر حيوية، مثل أنظمة التحكم والتشغيل، مما قد يتسبب في خسائر فادحة للبنية التحتية الجورجية، مما يعني أن الهدف لم يكن تدمير الإنترنت بشكل دائم، والبنية التحتية لجورجيا ولكن فقط لتحقيق هدف عزلها عن العالم الخارجي، بمعنى إذا تعرضت البنية التحتية لجورجيا للهجوم، فإن الخسائر الاقتصادية الهائلة ستؤثر حتما في البلدان التي ترتبط معها بعلاقات اقتصادية وثيقة ولاسيما روسيا لذلك إذا نسبنا هذا الهجوم إلى الجهات الرسمية الروسية فمن المنطقي ألا تضر روسيا بجورجيا اقتصاديا حتى لا تمس مصالحها[28].

لم تتوقف الهجمات السيبرانية الروسية على جورجيا فقط في حقبة الحرب عام ٢٠٠٨ ، إذ اتهمت وزارة الخارجية الجورجية روسيا بشن هجمات إلكترونية في ٢٨ تشرين الأول ٢٠١٩، ضد مواقع مؤسسات رسمية وأدان وزير الخارجية الأمريكي السابق (مايك بومبيو) في تغريده على توتير الهجوم السيبراني الروسي على جورجيا ودعا بومبيو الجانب الروسي إلى وضع حد لموقفه تجاه جورجيا، وإلى جانب الولايات المتحدة أدانت دول عديدة هذا الهجوم، ولكن روسيا ومن خلال نائب وزير خارجيتها (أندريه رودنكو) دحضوا صحة هذه الاتهامات[29].

فوفقاً للعقيدة العسكرية الروسية لابد وإن يسبق الهجوم العسكري الناجح عمليات أخرى تهدف إلى منع الخصم من الحصول على معلومات من مصادر خارجية، ومحاولة التأثير على الرأي العام في الدولة الخصم عن طريق المعلومات الخاطئة والدعاية التي تخدم المصالح الروسية، ومن ثم يساعد التخطيط في مرحلة ما قبل الهجوم للقيام بعملية الاختراق السري لأنظمة الخصم في تحقيق هذا الأهداف، وأبرز مثال على ذلك هي تلك الهجمات التي اتهمت روسيا بشنها عام(2008) ضد جورجيا قبل توجيه ضربة عسكرية[30].

وقد استخدمت روسيا الهجمات السيبرانية بحروبها المختلفة، إذ يبدو إنّ روسيا تستخدم الإنّترنت كسلاح في العمليات العسكرية التقليدية، حيث أتاحت تجربتها مع جورجيا فرصاً لتحسين تقنياتها وإجراءاتها في مجال الحرب السيبرانية واستعراض قدراتها على الساحة العالمية وشكلت هذه القدرات في عدة مناسبات قوة ردع مهمة ضد خصوم روسيا[31].

الخاتمة:

أحدث القرن الحادي والعشرين نقلة نوعية في ترتيب أولويات معظم الدول، وكذلك في الخيارات المتوفرة لدى صناع القرار، والتي بدورها أثرت على أدوات السياسة الخارجية كوسائل لبسط النفوذ وإبراز المكانة على الساحة الدولية، وتعتبر التكنولوجيا واحدة من القوى التي أتاحتها العولمة لتحقيق أهداف بعيدة المدى، والتحرك الخفي والتأثير في الهياكل الحيوية الخاصة بالدول، وهو ما أوجب على الدول ضرورة الانتباه لتلك الأداة، ومعرفة كيف تعمل، وإلى أي مدى يمكن أن تصل ومدى تحقق منافع أو تهديدات، ونتيجة لذلك، حظي الأمن السيبراني باهتمام كبير من مختلف دول العالم، ومنها وروسيا، وحققت مكانة متميزة في التمكن من هذه القوة، واستخدمتها في تحقيق أهدافها المنشودة، كما وأن روسيا وضفت الامن السيبراني في حربها على جورجيا عام 2008، وأصبحت التكنولوجيا ترسم خريطة ثقل دول العالم، وتعطي صورة عن

---

27. Sarah P. White Understanding Cyberwarfare. Lessons from the Russia-Georgia War modernwar institute at west point, March 20, 2018, p 9.

28. أماني عصام محمد، مصدر سبق ذكره، ص ص١٧٧-١٧٨.

29. وكالة الأناضول، جورجيا تتهم روسيا بتنفيذ هجوم سيبراني على مواقعها الرسمية، ٢٠٢١/٢/١٢، متاح على الرابط التالي: https://www.aa.com.tr/ar

30. أحمد علو، العقيدة العسكرية الروسية الجديدة، مجلة الجيش، دراسات وأبحاث :العدد(356)، 2015، متوفر على الرابط التالي: https://www.lebarmy.gov.lb/ar/content/ %D8%A7%D9%84%

31. احمد يوسف الجميلي, القدرات السيبرانية سلاح روسيا الفعال ضد الخصوم, مركز صنع السياسات للدراسات الدولية والاستراتيجية، 2018، متوفر على الرابط التالي https://www.makingpolicies.org/ar/posts/rusye.php

مكانة الدولة؛ حيث إن امتلاك أسلحة المعلومات يعطي ميزة استراتيجية خاصة للدولة، وعلى النقيض تعتبر الدول الضعيفة رقميا تفتر لقوة مهمة؛ خاصة أن فضاء المعلومات يختلف تماماً عن المجالات التقليدية للعلاقات الدولية.

الاستنتاجات :

١. اصبح استخدام القوة الصلبة مع استخدام القوة السيبرانية تتم في فضاء سيبراني افتراضي.
٢. التحول في فن الحرب والياتها والاسلحة المستخدمة فيها اذ اصبح العامل التقني والمعلوماتي هو معيار اساسي للقوة .
٣. ان الحرب السيبرانية باتت سمه مميزة لحروب القرن الحادي والعشرين.
٤. ظهور أدوات جديدة تمثلت في الأدوات التقنية والتكنولوجية والمعلوماتية والتي تدار تلك الوسائل والأدوات من خلال فضاءات افتراضية وشبكية .
٥. ان الحرب السيبرانية تنطوي على تحقيق مجموعة من الأهداف أهمها ضرب البنية التحتية الحيوية للدول سواء كانت هذه عسكرية او مدنية.
٦. أصبح الأمن السيبراني ضمن إستراتيجيات الأمن القومي للدول، ولاسيما الدول الكبرى وذلك من اجل زيادة قوتها وقدرتها وبالتالي توظيفها لممارسة التأثير والسيطرة والنفوذ على الآخرين.
٦. استخدمت روسيا القوة السيبرانية في حربها على جورجيا في جميع جوانبها.
٧. الفضاء السيبراني كان له الدور كبير في زعزعة الاستقرار داخل جورجيا قبل وأثناء الحملة العسكرية من قبل روسيا.

قائمة المصادر:

1. اماني عصام، استخدام روسيا للقوة السيبرانية في إدارة تفاعلاتها الدولية، مجلة كلية الاقتصاد والعلوم السياسية، العدد(4)، المجلد(22)، كلية الاقتصاد والعلوم السياسية، جامعة حلوان، مصر، 2021.
2. اميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد(35)، كلية الشريعة والقانون، جامعة الامارات، الامارات، 2020.
3. حارك فاتح، الفضاء السيبراني والتحول في شكل الحروب: دراسة حالة روسيا، دار فاضي للنشر والترجمة، الجزائر، 2019.
4. علي زياد فتحي، رؤية استراتيجية العمليات السيبرانية الاوروأطلسية ومهددات الجيوسيبرانية الروسية" رؤية في الاشتباك السيبراني الاورو- روسي"، مجلة حمورابي، العدد(30)، بغداد، 2019.
5. اسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، العدد(1)، كلية العلوم القانونية والسياسية، جامعة محمد بوضياف المسيلة، الجزائر، 2016.
6. Franz – Stafan Greg and Greg Autsin, Russia the United States and Cyber Diplomacy; Opening the Doors the Doors, East West Insttiute.
7. Russian Cyber Units, Congressional Research Service(IN FOCUS), (February 2022).
8. Santtu Lehtinen, Sinikukka Saari, Arho Suominen (Eds.), Russia’s technological policy and knowhow in a competitive global context, Prime Minister’s Office, Finland, 2022.
9. Michael Connell and Sarah Vogler, Russia’s Approach to Cyber Warfare, Center for Strategic Studies, International Affairs Group, (March 2017).
10. Jakub Przetacznik with Simona Tarpova, Russia's war on Ukraine: Timeline of cyber-attacks, EPRS | European Parliamentary Research Service, (June 2022).
11. Sarah P.White .Understanding Cyberwarfare, Lessons from the Russia-Georgia War modernwar institute at west point, 2018.
12. Stephen Blank, Cyber War and Information War à la Russe, From Understanding Cyber Conflict: Fourteen Analogies George Perkovich and Ariel E. Levite, Editors, Published by Georgetown University Press, November 2017.
13. Keir Giles, Russia Public Stance on Cyberspace Issues Conference on Cyber Confict, Publications, Tallinn.
14. دراسة حديثة: كيف تشكل القدرات السيبرانية موازين القوى محلياً ودولياً؟، موقع كيوبوست، ٢٠٢١، متاح على الرابط التالي: https://www.qposts.com

15. افتكار مانع، قانون سيادة الانترنت في روسيا هل هو بداية لحرب الكترونية، موقع الجزيرة ، 2019، متوفر على الموقع: www.aljazeera.net
16. احمد يوسف الجميلي ، القدرات السيبرانية، مركز صنع السياسات للدراسات الاستراتيجية، ٢٠١٨، متاح على الرابط التالي: https://www.makingpolicies.org/ar/posts/rusye.php
17. عادل عبد الصادق ، صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية ، مقال منشور على موقع المركز العربي لأبحاث الفضاء الإلكتروني، ٢٠١٩، متاح على الرابط التالي:
18. https://accronline.com/article_detail.aspx
19. أحمد نزيه، حكاية اوسيتيا الجنوبية (أرض الحرب) التي راقبتها (ميركل) بالمنظار، موقع أخبار اليوم، ٢٠١٨ ، متاح على الرابط التالي: https://m.akhbarelyom.com
20. مايا أوتاراشفيني، حزب روسيا وجورجيا بعد مرور 10 أعوام هل تعلم الغرب؟، مجلة المجلة، ٢٠١٨، متاح على الرابط التالي: https://arb.majalla.com/node
21. تقرير، حرب المعلومات خلال الحرب الروسية الجورجية، متاح على الرابط التالي: https://stringfixer.com/ar/Infomation_war_during_the_Russo-Georgian_War.
22. وكالة الأناضول، جورجيا تتهم روسيا بتنفيذ هجوم سيبراني على مواقعها الرسمية، ٢٠٢١/٢/١٢، متاح
23. على الرابط التالي: https://www.aa.com.tr/ar
24. أحمد علو، العقيدة العسكرية الروسية الجديدة، مجلة الجيش، دراسات وأبحاث :العدد(356)، 2015، متوفر على الرابط التالي: https://www.lebarmy.gov.lb/ar/content/ %D8%A7%D9%84%

احمد يوسف الجميلي, القدرات السيبرإنية سلاح روسيا الفعال ضد الخصوم, مركز صنع السياسات للدراسات الدولية والاستراتيجية، 2018، متوفر على الرابط التالي https://www.makingpolicies.org/ar/posts/rusye.php