KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

تأثير التهديدات السيبرانية في الصراعات الإقليمية- نماذج مختارة

The Impact of Cyber Threats on Regional Conflicts - Selected Models

أ.د. بهاء عدنان السعبري

الباحثة شهد حمزة مير علي

كلية العلوم السياسية/ جامعة الكوفة

Prof. Dr. Baha Adnan Al-Saabari

Researcher Shahad Hamza Mir Ali

Faculty of Political Science / University of Kufa

DOI: https://doi.org/10.36322/jksc.176(A).19373

الملخص:

يتعرض الأمن الاقليمي إلى الكثير من التهديدات والتحديات التي تختلف باختلاف المجال التي تنبع منه ويرجع ذلك إلى التوسع في مفهوم التهديدات، وان ظهور الفضاء السيبراني كقوة جديدة في العلاقات الدولية وفاعل مؤثر في تلك العلاقات معتمداً على التقدم التكنولوجي، ونتيجة لانتقال جزء كبير من الصراعات الى مجال الفضاء السيبراني، ودخول المجتمع الإقليمي مرحلة جديدة تحاول فيه الدول الى تعزيز قدرتها من اجل ممارسة الهيمنة والسيطرة والتأثير في البيئة الاقليمية والدولية ظهرت فيها التهديدات تسمى بالتهديدات السيبرانية، إذ تحول الفضاء السيبراني الى ساحة للتأثير والتنافس والصراع بين الدول والمنظمات والشركات، أصبح الفضاء السيبراني أحد العناصر الرئيسية التي تؤثر في القيم السياسية والاجتماعية النظام الاقليمي، وبسبب ضئالة حجمها وقلة تكلفتها وعدم إمكانية معرفة أسباب ومصدر التهديدات إلا انها تسبب خسائر فادحة على كافة الأصعدة السياسية والاقتصادية والعسكرية، وان هذا ما

KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

دفع الدول من تطوير قدراتهم السيبرانية من اجل تعزيز قوتهم والسعي الى السيطرة على مجال الفضاء السيبراني.

الكلمات المفتاحية: التهديدات السيبرانية الإقليمية ـ العقيدة الأمنية السيبرانية الروسية ـ الأمن القومي الروسي

Abstract:

Regional security is exposed to many threats and challenges that differ according to the field from which it stems. This is due to the expansion of the concept of threats, and the emergence of cyberspace as a new force in international relations and an influential actor in those relations based on technological progress, and as a result of the transfer of a large part of the conflicts to The field of cyberspace, and the entry of the regional community into a new phase in which countries try to strengthen their ability to exercise hegemony, control and influence in the regional and international environment in which threats called cyber threats appeared, as cyberspace turned into an arena of influence, competition and conflict between states, organizations and companies, cyberspace has become one of The main elements that affect political and social values are the regional system, and because of their small size, low cost, and the inability to know the causes and source of threats, they cause heavy losses on all political, economic

ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

and military levels, and this is what prompted countries to develop their cyber capabilities through In order to consolidate their power and seek to dominate the domain of cyberspace.

Keywords: Regional Cyber Threats - Russian Cyber Security Doctrine - Russian National Security

المقدمة:

بعد انتهاء الحربين العالميتين وما خلفتهما من آثار وخسائر بشرية ومادية، بدأت الدول بالبحث عن وسائل وأساليب أخرى للقتال من شأنها أن تحقق لها الميزة العسكرية على الخصوم، ومن دون تحمل الخسائر والمخاطر التي يتحملها القائم بالهجوم في إطار استخدامه للأسلحة التقليدية. وقد توصلت هذه الدول في العقد الأخير إلى أحدث هذه الوسائل التي تتسم بالتعقيد واجتياز الحدود التقليدية، وهي الهجمات السيبرانية التي من شأنها تدمير البنية التحتية للخصم، والتسبب بآثار فادحة على البنية العسكرية والمدنية للخصم، وذلك كله من دون الحاجة إلى الدخول في أي اشتباك حقيقي ومادي مع الخصم، ومن دون الحاجة لتحمل أعباء مالية ومخاطر المواجهة المسلحة التي يتحملها المهاجم في إطار استخدام الأسلحة التقليدية.

يشهد العالم اليوم موجات من التغيرات و التطورات المتسارعة و لتعاظم وتيرة الابتكارات التقنية والإلكترونية والتي أضحت تضيف وبشكل يومي كل ما هو جديد ومتطور في عالم تكنولوجيا المعلومات، ولم يعد بالإمكان التخلي عن التقنيات الحديثة والتي دخلت في شتى المجالات وشكلت البنية التحتية لأغلب الدول المتقدمة ، و أحدثت انعطاف نحو تغيير الأفكار التقليدية ، حيث دخل الفضاء السيبراني كمجال جديدة في العلاقات الدولية وفاعل مؤثر في تلك العلاقات معتمداً على التقدم التكنولوجي الذي يعزز قدرة

الدولة على ممارسة الهيمنة والسيطرة والتأثير في البيئة الاقليمية والدولية ، و مكنت من ان تحدث نقله في معيار ما تمتلكه الدول من قوة تمكنها من مواصلة الاستجابة و القدرة على مواجهة التهديدات السيبرانية في بيئة الفضاء السيبراني .

أهمية الموضوع:

إن أهمية الموضوع تنبثق من أهمية بيئة التطور التكنولوجي وانعكاساتها على البنية التحتية المعلوماتية للدول الاقليمية، ويعد الفضاء السيبراني مجالاً عاماً بين من يستخدمونه ويتفاعلون معه، مع الأخذ بنظر الاعتبار على أهمية التركيز على مقدار الخطر المحدق بمستخدمي الفضاء الإلكتروني وهذا ما جعل الفضاء السيبراني بيئة جاذبة لمستخدميها، ويمكن توظيفها لتحقيق أهداف في غاية الأهمية من خلال:

١. فهو يسعى الى فهم وتفسير العلاقات الدولية والسياسة الإقليمية والعالمية المعاصرة، خاصة في ظل الطبيعة المتغيرة للتهديدات الأمنية المختلفة.

٢. ويعد الفضاء السيبراني مجالاً عاماً، بسبب انتقال كافة مجالات الحياة الى الفضاء السيبراني أثرت على البيئة الأمنية فيه وأفرزت عدة تداعيات أثرت على أمن.

٣. ارتفاع مستوى التهديدات السيبرانية بعد الاعتماد الكلي للدول في استراتيجياتها في مجالات الأمن والقوة العسكرية على الفضاء السيبراني وتؤدي بالتالي الى زيادة انتشار الصراع الدولي.

الإشكالية:

في ظل تزايد الاعتماد على التكنولوجيا و توظيفها في القطاعات السياسية و العسكرية و الاقتصادية أصبحت هذه القطاعات عرضة للتهديد و الهجوم من خلال المنافذ الالكترونية، فأن إشكالية الدراسة تكمن

KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

في ان التهديدات السيبرانية أصبحت احد وسائل الدول و الفواعل الإقليمية و الدولية في فرض التهديدات و بذلك أضحت البنية الإقليمية متأثرة بتوظيف هذه الأسلحة السيبرانية في صراعاتها الإقليمية و يتفرع من هذه الإشكالية مجموعة تساؤلات.

١. كيف يمكن التعامل مع واقع التهديدات السيبرانية التي فرضت واقعاً جديداً يعرض الامن الإقليمي للخطر؟

٢. ما القدرات السيبرانية للدول وكيف وظفت استراتيجيات خاصة بالأمن السيبراني لتطوير قدراتها السيبرانية؟.

٣. كيف تؤثر الحروب الالكترونية على الامن الإقليمي؟.

الفرضية:

إن الدراسة تنطلق من فرضية مفادها أن في ظل الاعتماد المتزايد للدول على التكنلوجيا والبنية التحتية المعلوماتية، فأن الفرضية تحاول إثبات ما يأتي: ان تزايد التهديدات السيبرانية بين الفواعل من الدول تؤدي بالنتيجة الى زيادة حدة انتشار الصراع الاقليمي وذلك من خلال الاستخدام المتزايد من قبل الدول الكبرى والإقليمية والجماعات والأفراد للقوة السيبرانية .

منهاج الدراسة:

تقتضي ضرورة البحث العلمي عند دراسة أي ظاهرة، تحديد المنهج الانسب لها لكي يكون الوسيلة أو الطريق الصحيح للوصول الى النتائج، وقد تم الاستناد في هذه الدراسة على المنهج الاستقرائي، بوصفه منهجا اساساً، فضلا عن استخدام بعض المناهج الاستدلالية بطريقة علمية أساسا لتحقيق النتائج المرجوة

KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

من هذه الدراسة، وضمن هذا السياق، لذلك كان لابد من استخدام المنهج الوصفي لغرض وصف الظاهرة وتحليلها. وبعدها تمت الاستعانة بالمنهج التحليلي عبر عرض إشكالية البحث ومناقشتها والبرهنة عليها عن طريق معرفة المدخلات والمخرجات، وكيفية التأثير المتبادل فيما بينها وصولاً إلى الاستنتاجات.

المبحث الأول

روسيا والتهديدات السيبرانية الإقليمية

تولي روسيا أهمية كبيرة المناطق التي كانت تابعة للاتحاد السوفيتي ، فمن الصعب عليها التخلي عن طموحاتها بأن تكون وريثة للاتحاد السوفيتي في موقع القوة الكبرى المؤثرة ، فروسيا تعد المناطق التي كانت فيما مضى جزءاً من الاتحاد السوفيتي مجالاً حيوياً لها ، تسعى روسيا استعادة نفوذها في بعض المناطق والدول التي كانت تحتفظ بعلاقات صداقة تقليدية معها لأوقات طويلة من الزمن ، وذلك من اجل تكوين عوامل قوة مضافة لاستعادة الأدوار الخارجية التي كان الاتحاد السوفيتي ، حيث تسعى روسيا لاستعادة نفوذها الاقليمي، و رغبة وسيا في إعادة وجودها العسكري من اجل الوقوف امام مواجهه حلف(الناتو).فقد اتبعت روسيا منذ مطلع الألفية الجديدة استراتيجية جديدة لإدارة ما يجري في مجالها الحيوي التي حاول الغرب إثارتها، حيث جعل الفضاء السيبراني تلك المصالح مرتبطة ببعضها البعض في بيئة عمل واحدة، ، استغلت روسيا تحسن امكاناتها وقدراتها الاستراتيجية ، للوقوف بوجه تلك المخططات الغربية عن طريق توظيف وسائل القوة الشاملة في المدرك الاستراتيجي الروسي لإحباط أي تحد لها في جوارها القريب وتأكيد هيمنتها[1].

KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

وعلى أساس هذا تم تقسيم المبحث الى مطلبين:

المطلب الأول: العقيدة الأمنية السيبرانية الروسية.

المطلب الثاني: توظيف التهديدات السيبرانية والأمن القومي الروسي.

المطلب الأول

العقيدة الأمنية السيبرانية الروسية

أدى تفكك الاتحاد السوفيتي عام (١٩٩١) إلى قلب موازين القوة لدى الدولة الروسية، وبالتالي الثقافة الروسية، بمجرد اعتبار نفسها مركزاً لحركة شيوعية تاريخية عالمية، اضطرت النخبة السياسية في موسكو إلى التكيف مع الحدود المتضائلة والتحالفات المتقلبة والاقتصاد الوطني الراكد الذي كان يتمتع بمزايا قليلة على منافسيها العالميين.

حصل بوتين على دعم شعبي واسع النطاق في جميع أنحاء روسيا، وذلك بسبب ومناشداته للفخر الوطني، وانتشار عبادة الشخصية. سعى بوتين إلى ترسيخ هذه الموافقة من خلال الحد بشكل منهجي من التدفق الحر للمعلومات وفرض الرقابة أو حتى سجن خصومه السياسيين . مع الحفاظ على سيطرة صارمة على السياسة الروسية المحلية، إضافة إلى توسيع نفوذ روسيا ومكانتها وازدهارها على المسرح العالمي ، كان بوتين أكثر من راغب في استخدام القوة العسكرية الروسية وخدمات المخابرات لمواجهة الأهداف الدبلوماسية والعسكرية الغربية في الشرق الأوسط. وأوروبا الشرقية وأماكن أخرى. تمثل العمليات السيبرانية وسيلة فريدة للحكومة الروسية لتكافؤ الفرص مع منافسيها العالميين، وقد تمكنت من الاستفادة من هذه القدرات بنجاح باهر[2].

KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

إن روسيا قد حققت تطوراً مهماً في مجال الفضاء الإلكتروني وذلك بسبب التطورات السريعة التي حصلت في الفضاء السيبراني ، جعلت الدول تسارع إلى تبني تغييرات في العقيدة الامنية ، وذلك بإدراج القوة السيبرانية كمحدد رئيس لمدى قوة الدولة ، وقدرتها على حسم النزاعات لصالحها ، وان روسيا لا تتردد باستخدام القوة السيبرانية من اجل تعظيم قوة روسيا وتحقيق أهدافها التي تعجز أدوات القوة التقليدية عن تحقيقها ،من اجل تعزيز استقرارها الاستراتيجي ، خاصة بما تتميز به هذه القوة من خاصية القدرة على إصابة أهداف الخصم ، واتساع نطاق تدمير الأهداف الالكترونية مع التحكم في امكانية إصابة الاهداف من دون وقوع خسائر بشرية غير مقصودة [٣] .و تم توسيع مفهوم الإقليم ليشمل "الفضاء السيبراني" أو "الفضاء السيبراني الوطني" ، والجيش مكلف على وجه التحديد بحماية جميع الفضاء السيبراني داخل الاتحاد الروسي وتشمل حماية الأراضي الروسية منطقة المعلومات ، إن الأمن السيبراني في روسيا ليس مفهوماً قائماً بذاته ولكنه جزء لا يتجزأ من أمن المعلومات القومي ، حيث الأمن السيبراني مصطلح شائع، تميل روسيا إلى عدم استخدام هذا المصطلح في وثائقها القانونية الرسمية على عكس الاتحاد الأوروبي، في عام ، ٢٠١٤حاول مجتمع الأعمال الروس بتغيير نهج الدولة للأمن السيبراني تم اقتراح استراتيجية وطنية للأمن السيبراني حيث تشارك الشركات والمجتمع المدني في تطوير معايير وسياسات الأمن السيبراني ، وسيزداد التعاون الدولي في الأمن السيبراني والدول الأخرى سيتم تنفيذ التجربة ومع ذلك ، تم انتقاد الاستراتيجية من قبل خدمة الأمن الفيدرالية ولم يتم تبنيها مطلقاً [٤].

وبدلاً من ذلك تم اعتماد مبدأ أمن المعلومات الخاص بالاتحاد الروسي بعد ذلك بعامين الذي لا ينص على مشاركة مجتمع الأعمال في تطوير معايير الأمن السيبراني ، ولكنه يحدد مبادئ عامة مثل حماية الحقوق الدستورية ، وحماية البنية التحتية للمعلومات الحيوية في روسيا ، وتطوير العلوم وتكنولوجيا المعلومات

KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

الروسية ، وتقديم معلومات دقيقة عن الدولة الروسية المواقف السياسية والرسمية للمجتمع المحلي والدولي، والمساعدة في إنشاء نظام دولي لأمن المعلومات ، وحماية السيادة الروسية في مجال المعلومات [٥].

حيث تركز عقيدة أمن المعلومات على اعتبار الأمن السيبراني كأحد الوسائل التي تضمن أمن المعلومات، هذا و ان امن المعلومات يتم تعريفها و فهمها على أنها حماية الفرد والمجتمع أو الدولة من تهديدات المعلومات الداخلية والخارجية، وبالتالي الحفاظ على الحقوق و الحريات الدستورية ، ونوعية ومستوى معيشة المواطنين ، فضلاً عن السيادة والسلامة الإقليمية و التنمية الاقتصادية والاجتماعية المستدامة للاتحاد الروسي ، والدفاع والأمن للدولة . لذلك يفهم الأمن السيبراني في روسيا على أنه أحد عناصر أمن المعلومات، أي أن متطلبات الأمن السيبراني يتم تنفيذها في سياق سياسة أمن المعلومات هذا الاختلاف مهم لفهم النهج الروسي في مسائل الأمن السيبراني ، وان أمن المعلومات في روسيا تحكمه الدول وتنظمه إلى حد كبير لصالح الدولة ، مما يجعل هذه المنطقة متأثرة سياسياً تماماً وهو ويهدف إلى تحقيق الاستقلال عن الفضاء الإلكتروني الدولي ، وسيادة روسيا في مجال المعلومات، وتطوير البنية التحتية المحلية لتكنولوجيا المعلومات [٦].أحد الأهداف المنصوص عليها في عقيدة أمن المعلومات هو تقديم (Runet) ، أي إنترنت روسي مستقل. في عام ٢٠١٩ ، تم اعتماد ما يسمى بقانون الإنترنت السيادي الذي يهدف إلى الوظيفة المستقلة للجزء الروسي من الإنترنت ، وضع قانون الإنترنت السيادي الأساس القانوني لقطاع الإنترنت الروسي يمكن أن تعمل بشكل مستقل عن الإنترنت العالمي السلطات الروسية مما أدى إلى خلق نظام بأسماء النطاقات الوطنية و تم تزويد تكنولوجيا المعلومات ووسائل الإعلام بصلاحيات جديدة لجمع المعلومات من مالكي البنية التحتية للإنترنت ، و إنشاء بنية تحتية إضافية لصيانة حركة المرور ومراقبتها

KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

(بما في ذلك إدارة شؤون الإعلام)[٧]. تكشف العقيدة الروسية الجديدة، أنه تمت إضافة بند جديد يخص تهديدات الأمن السيبراني في المجالين العسكري والاقتصادي، ووفقا للعقيدة الروسية الجديدة لأمن المعلومات، التي وقعها الرئيس الروسي (فلاديمير بوتين) ، فإن إحدى التهديدات الرئيسية لروسيا تتمثل " بزيادة عدد الدول الأجنبية التي لديها تأثير على البنية التحتية لمعلومات الأغراض العسكرية في روسيا "،أحد الأهداف الرئيسية لواضعي هذه العقيدة الجديدة، هو " الردع الاستراتيجي والوقاية من النزاعات العسكرية، والتي يمكن أن تنجم عن استخدام تكنولوجيا المعلومات " [٨] . وقد بدأ الاهتمام الروسي بالأبعاد السياسية للأمن الإلكتروني في التسعينات من القرن الماضي بعد تأسيس مجلس الأمن الروسي في عام (١٩٩٢)، وإضافة إلى المؤسسات الأمنية الروسية تم إنشاء مؤسسات أخرى تختص فقط بالقضايا الإلكترونية وبحماية الأمن الإلكتروني الروسي ، و صرح المتحدث باسم وزارة الدفاع الروسية "ايجور يجوروف " (في تشرين الأول (٢٠١٤) بان روسيا تخطط لبناء نظام الكتروني شامل على مراحل إذ يتم الانتهاء منه في (٢٠١٧) وذلك بهدف حماية البنية الأساسية للقوات المسلحة من الهجمات السيبرانية ، ولقد تبلور الاهتمام الروسي بقضايا الأمن الإلكتروني في (عام ٢٠٠٠) [٩] ، أنشأت روسيا الاتحادية (وكالة أبحاث الأنترنت)، أو ما يعرف باسم جيش المتصيدين (Troll Army) ، تابع لوكالة الأمن الاتحادي الروسي، يضم آلاف الموظفين، ويخصص له سنوياً نحو (٣٠٠) مليون دولار من ميزانية الدفاع الروسية وعندما قامت روسيا بتطوير استراتيجية أمنية تبنى على أساس الإيمان الكامل بالدور الذي يلعبه الأمن الإلكتروني في تحقيق المصالح القومية وتعزيز الاستقرار الاجتماعي والسياسي ومن أهم المؤسسات المسئولة عن الأمن الالكتروني في روسيا هي مجلس الأمن ، وجهاز الأمن الفيدرالي ، جهاز الحرس

الفيدرالي ، والجهاز الفيدرالي للتحكم التقني ، ووزارة الاتصالات وتكنولوجيا المعلومات [١٠]. حيث ان روسيا قد حددت ادوات الحرب السيبرانية لها وهي مكافحة التجسس , توحيد الذكاء واعتماد التضليل ، أضعاف اتصالات العدو ، تدهور ملاحة العدو , الضغط النفسي على العدو تدمير قدرات كمبيوتر الخصم، وعليه تعتبر روسيا ان هذه الادوات ستكون سلاحاً مخيفاً بالمستقبل بآثار متنوعة وعديدة ، فإن فاعلية الحرب السيبرانية الى جانب الاسلحة الدقيقة تكون اثارها مشابهة لأسلحة الدمار الشامل[١١]. وقد أعلنت روسيا أيضا في عام (٢٠١٠) عن العقيدة العسكرية الخاصة بها، والتي أشارت إلى أن الصراعات العسكرية الحديثة تتضمن الاستخدام المتكامل للقدرات العسكرية وغير العسكرية، مع الاهتمام بإبراز دور أكبر لحرب المعلومات. وقد تم تشكيل قيادة مستقلة للأمن السيبراني، هذا علاوة على الإدارة السيبرانية داخل الجيش الروسي لتعزيز جاهزية القوات المسلحة الروسية للدفاع ضد الهجمات السيبرانية. وفي عام (٢٠١٤) صرحت وزارة الدفاع الروسية بأنها تخطط لبناء نظام الكتروني شامل ينتهي العمل منه عام (٢٠١٧) حيث يعمل على حماية البنية الأساسية للقوات المسلحة من الهجمات السيبرانية, كما ان روسيا تمتلك عناصر بشرية مؤهلة للقيام بعمليات سيبرانية ، ولديها الكثير من القراصنة المتطوعين , والذين يتم توظيفهم لخدمة الأغراض العسكرية [١٢]. ويسعى الرئيس الروسي فلاديمير بوتين " في التأكيد على ان من المحتمل جداً الوصول الى الوسائل النهائية للحرب المستقبلية، التي تبتعد عن النزاعات المسلحة التقليدية، والتوجه الى قمع القيادة العسكرية وايقاف عمليات الملاحة والاتصالات الخاصة بالعدو، في الفضاء الالكتروني، والتوجه نحو اختراق المعلومات التي تعتمد عليها الدولة المستقرة، وان استراتيجية روسيا حول الأمن الالكتروني هو الهجوم، وذلك باعتقادها ان الترهيب والتجسس في الفضاء السيبراني يحقق نصف الانتصار في اعين الخصوم والاعداء [١٣].حيث تظهر التقارير أن قوات الأمن السيبراني الروسية

KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

وصلت إلى ١٠٠٠ موظف، وتنفق وزارة الدفاع الروسية حوالي ٣٠٠ مليون دولار سنويا على مثل هذه الأنشطة [١٤]، و ان مهام الأجهزة الالكترونية الروسية هي القيام بعمليات التجسس على الخصوم و شن الهجمات الالكترونية التي تسبب الضرر للبنى التحتية والاقتصاد والمواقع الحكومية في الدول الاجنبية المعادية [١٥] . وتستخدم روسيا الإنترنت كسلاح في العمليات العسكرية التقليدية، إذ أتاحت تجربتها مع كل من جورجيا وأوكرانيا فرصاً لتحسين تقنياتها وإجراءاتها في مجال الحرب السيبرانية وعمليات الارهاب السيبراني، واستعراض قدراتها على الساحة العالمية وشكلت هذه القدرات في عده مناسبات قوة ردع مهمة ضد خصوم روسيا[١٦].

و من اجل تعزيز أمن لسيبراني لروسيا في مواجهة أي هجمات محتملة من الطرف الآخر ، حيث تم انشاء في ١٠ ايلول ٢٠١٨ جهاز الأمن الفيدرالي الروسي مركزا وطنيا لتنسيق مكافحة الهجمات السيبرانية على البنية التحتية الحيوية في روسيا ، يتولى مهام الكشف والوقاية والفضاء على تداعيات الهجمات الإلكترونية ، وتبادل المعلومات بين الهيئات المتخصصة في الداخل والخارج ، وتحليل الهجمات السيبرانية الماضية وتطوير أساليب مكافحتها ، وجار العمل على فصل روسيا كلها عن الإنترنت بهدف زيادة فاعلية دفاعاتها ضد الهجمات الإلكترونية والقرصنة ، حيث إن تداول البيانات بين المواطنين والمؤسسات في هذه الحالة سيكون داخل البلاد لا عن طريق مراكز توجيه دولية . إذ تحتفظ روسيا بعلاقات تعاونية مع الصين في مجال الفضاء السيبراني عبر اتفاقها عام (٢٠١٥) وانضمامها لمنظمة شنغهاي للتعاون ، وكان البرلمان الروسي قد وافق في ١٢ من شباط (٢٠١٨)على قانون عزل البلاد عن شبكة الإنترنت العالمية، لجعل البلاد في موقع أفضل لصد أي هجمات إلكترونية محتملة من الخارج [١٧] .

KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

ومن ناحية أخرى اعتزمت روسيا من خلال منظمة " البريكس * " تأسيس فضاء إلكتروني خاص بها مستقل عن شبكة الانترنت الحالية بهدف التخلص من الهيمنة وعمليات التجسس الالكتروني الامريكية ، وبذلك يتم انشاء شبكة انترنت جديدة موازية لشبكة الانترنت الحالية ، وتكون منافسا قويا للولايات المتحدة[١٨].أطلقت روسيا في (٣٠ ايلول ٢٠١٥) حملتها العسكرية ضد التنظيمات الإرهابية في سوريا ، والتي تمثلت أهدافها الرسمية في حماية الجيش العربي السوري من الانهيار حتى لا تسقط مؤسسات الدولة الحالية، فضلاً عن القضاء على تنظيمي " داعش " ، و "جبهة النصرة " التابعين لتنظيم القاعدة وغيرها من التنظيمات الإرهابية الأقل نفوذا وانتشاراً ، تمتلك روسيا مجموعة واسعة من الأدوات والموارد السيبرانية ، بما في ذلك القدرة على تنفيذ هجمات رفض الخدمة وتطوير برامج ضارة معقدة واستغلال نقاط ضعف البرامج غير المعروفة سابقًا .إن محاربي الإنترنت في الكرملين قادرون على استهداف كل شيء من الهواتف المحمولة الفردية إلى البنى التحتية لتكنولوجيا المعلومات لحكومات بأكملها .تعرضت دول البلطيق لهذه الأنواع من التهديدات لبعض الوقت وهي على دراية بالخطر[19] .

تستهدف الهجمات الروسية في الولايات المتحدة والدول الغربية الأخرى الصناعات والمنظمات أبحاث " COVID-19" ، والحكومات ، والمنظمات الانتخابية ، والرعاية الصحية والأدوية ، والدفاع ، الطاقة وألعاب الفيديو والمرافق النووية والتجارية والمياه والطيران والتصنيع الحرج، واستهداف عام ٢٠٢٠ للشركات الأمريكية التي تطور لقاحات " COVID-19" .

KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

المطلب الثاني

توظيف التهديدات السيبرانية والأمن القومي الروسي

الأمن السيبراني هو رافد جديد للأمن القومي وتزايدت العلاقة بين الأمن والتكنولوجيا، ومعها تزايدت امكانية تعرض المصالح الاستراتيجية للدولة للتهديدات السيبرانية، وهددت بتحول الفضاء السيبراني لوسيط ومصدر لأدوات جديدة للصراع الدولي المتعدد الاطراف.

ان العلاقة بين الأمن السيبراني والأمن القومي تزداد كلما زاد نقل المحتوى المعلوماتي والعسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي إلى الفضاء السيبراني ، خاصة مع التسارع في تبني الحكومات الالكترونية والمدن الذكية في العديد من الدول ، واتساع نطاق وعدد مستخدمي الانترنيت في العالم ، والثورة الكبرى في انترنيت الأشياء ، حيث أصبحت قواعد البيانات القومية في حالة انكشاف الخارجي ، اضافة الى حملات الدعاية والبيانات المضللة ونشر الشائعات أو الدعوة لأعمال تحريضية أو دعم ومساعدة المعارضة أو الاقليات ، مما يساهم في تلاشي سيادة الدولة ويشكك في قدرتها على الحفاظ على أمنها القومي [٢٠].

تعد التقنيات الجديدة من بين أدوات السياسة الخارجية الحديثة لأنها تشكل تهديدات للأمن القومي ،من بين الوثائق الرسمية "مفهوم الأمن القومي" ، الذي دخل حيز التنفيذ في ٢١ كانون الثاني (٢٠٠٠)، و "عقيدة أمن المعلومات" التي اعتمدها الرئيس الروسي فلاديمير بوتين في ٩ أيلول(٢٠٠٠). الوثيقة التي تحمل عنوان "وجهات النظر المفاهيمية حول أنشطة القوات المسلحة الروسية في مجال المعلومات" المنشورة في عام ٢٠١١ استندت إلى أنشطة الجيش الروسي في عصر المعلومات على بعض المبادئ مثل الشرعية

KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

والتعاون والابتكار والتفاعل. يحتوي نص "مفهوم السياسة الخارجية لروسيا" ، الذي تم تبنيه في عام ٢٠١٣ ، أيضًا على معلومات مهمة حول دبلوماسية الشبكات.

وأعلنت روسيا قبل سنوات قليلة، عن عزمها على استعادة موقع الزعامة في كافة التكنولوجيات العسكرية وتطوير السلاح الجوي والفضائي، وقد خصصت مبالغ ضخمة لإعادة التسليح [٢١].

وعملت على ربط "كوزي بير" التي تسمى أيضا و"ذي ديوكس" (The Dukes) بجهاز الأمن الفدرالي الروسي وجهاز المخابرات الخارجية. وتدير روسيا مجموعات الاختراق هذه بطريقة تنافسية باستخدام هذه المجاميع من القراصنة، إذ يتم تشجيع وكالات الاستخبارات المنفصلة على خرق نفس الأهداف وحيث تم توجيهه عدة لقراصنة الظل في القوة السيبرانية الروسية بالآتي [٢٢] :

❖ القيام بعمليات التجسس على الخصوم من اجل الحصول على المعلومات والبيانات في مختلف المجالات التكنولوجية.

❖ شن الهجمات السيبرانية والتي تسبب الضرر للبنى التحتية والاقتصاد والمواقع الامنية الحساسة.

وفي ٢٧ حزيران من عام ٢٠١٧ ، بدأت سلسلة من الهجمات السيبرانية الروسية القوية ضد مواقع حكومية في اوكرانيا باستخدام البرمجيات الخبيثة (بيتيا) ، استهدفت الهجمات بنوك ووزارات وصحف وشركات كهرباء ، وقد تأثرت العديد من الوزارات الأوكرانية والمصارف ونظم المترو والشركات المملوكة للدولة (مطار بوريس بيل الدولي ، أوكرتيليكوم ، أوكربوشتا ، بنك الادخار الحكومي الأوكراني ، السكك الحديدية الأوكرانية) ، ولوحظ أن الهجوم الالكتروني على الأرجح يهدف إلى شل عمل الدولة الأوكرانية وليس لأسباب مادية ، حيث جاء الهجوم يوم العطلة الرسمية الأوكرانية احتفالا بالذكرى السنوية لإقرار

KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

البرلمان الأوكراني دستور أوكرانيا في ٢٨ حزيران من العام (١٩٩٦) ، وقد توجه الاتهام الى روسيا بتدبير ذلك الهجوم[٢٣].

تعد روسيا الاتحادية على مستوى التنظيم الدولي من أقوى دول العالم التي يمكنها إدارة الحروب الإلكترونية على مستوى العالم، ولكن خلافاً للولايات المتحدة فإنها ترى إن السبيل لمنع الكوارث والنزاعات الناشئة عن الهجمات السيبرانية يكمن في الحظر التام لاستخدام النشاطات الإلكترونية في العمليات العسكرية، لا فقط تقييد استخدامها على مستوى القانون الدولي. قال مركز الدراسات الدولي إن روسيا تنفذ نشاطاً إلكترونياً ضاراً من أجل تأكيد نفسها بقوة - من خلال محاولة التدخل في انتخابات البلدان الأخرى ، وحذر التقرير من أن المتسللين الروس قد تمكنوا من الوصول إلى البنية التحتية الوطنية الحيوية لدول أخرى أظهرت الجهات الفاعلة السيبرانية الروسية التي ترعاها الدولة قدراتها على تعريض شبكات تكنولوجيا المعلومات للخطر وتطوير آليات للحفاظ على وصول طويل الأجل ومستمر إلى شبكات تكنولوجيا المعلومات ، سرقة البيانات الحساسة من شبكات تكنولوجيا المعلومات والتكنولوجيا التشغيلية ، وتعطيل وظائف أنظمة التحكم الصناعية والتي يمكن استخدامها لاحقًا للتأثير التخريبي [٢٤]. واستخدمت قدرانها الإلكترونية في الهجوم على العديد من الدول وهي :

أولا -الهجوم الروسي على إستونيا : بدأ الهجوم السيبراني الاستوني يوم الجمعة ، ٢٧نيسان ، ٢٠٠٧وانتهى يوم الجمعة ١٨ايار ، ٢٠٠٧واستمر لمدة ثلاثة أسابيع ، وكانت العلاقة بين إستونيا التي كانت تعد احدى جمهوريات الاتحاد السوفيتي السابق و روسيا في البلاد تتسم بالتوتر المستمر في البلاد وذلك بعد استقلالها وذلك بسبب تقلّد العديد من الروس لمناصب مهمة في الحكومة، و تحول هذا مؤخراً إلى أداة للاستفزاز وزعزعة استقرار النظام القائم ، كانت نظرة الأستونيين للروس كمحتلين غزوا بلادهم لتحريرها من

KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

النازيين ولكن أعادوا احتلالها لنصف قرن ، لكن بالنسبة للأستونيين العرقيين لم يكن السوفييت محررين لهم بل محتلين، كان الغرض من الهجوم الإلكتروني الروسي على استونيا هو معاقبة إستونيا على عدم احترام الثقافة والتاريخ والهوية الروسية عن طريق ازالة استونيا للتمثال البرونزي هو رمز مؤلم لنصف قرن من القمع السوفييتي، اما بالنسبة للروس كان يمثل التمثال الجندي البرونزي التذكاري، الذي شيدته الحكومة السوفييتية في عام ١٩٤٧، يطلق عليه في الأصل "النصب التذكاري لمحرري تالين". انتصار الاتحاد السوفييتي على النازية ، و رأى بعض الروس في إزالته محاولة لمحو تاريخهم [٢٥].وجهت روسيا هجوماً هجيناً شاملا على إستونيا في عام ٢٠٠٧ شملت هجمات إلكترونية وحملات تضليل ، والتي أعقبت أيضًا قرارًا حكوميًا بنقل تمثال يخلد تضحيات جنود روس في الحرب العالمية الثانية من العاصمة تالين الى مكان آخر مجهول ، صدم الحادث المسؤولين في البلاد مما دفعهم الى التوجه في تعزيز دفاعاتهم الإلكترونية ، ونتيجة لشدة وتعقيد هذه الهجمات اضطر إستونيا – التي هي من أعضاء حلف الناتو – لاستدعاء خبراء من حلف الشمال الاطلسي لمساعدتها وعقد اجتماع طارئ لأعضاء الحلف [٢٦].ووردت تقارير بأن قراصنة الإنترنت اخترقوا ما يصل إلى ربع أجهزة الكومبيوتر في العالم واستعانوا بروبوت برمجي لإغراق المواقع الإستونية بمعلومات وهمية عن وقوع هجوم حجب الخدمة (وهو هجوم يستهدف وقف خدمة إلكترونية ما بإغراقها بسيل من المعلومات من مصادر متعددة) بالإضافة إلى ذلك، انضم إلى القراصنة أشخاص عاديون حصلوا على تعليمات من مواقع روسية بشأن كيفية شن هجوم حجب الخدمة، وتم اختراق بعض المواقع وإعادة توجيه مستخدميها و تزامن مع تلك الهجمات نشر معلومات خاطئة، اذ

KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

نشرت مواقع إلكترونية أخرى مخترقة أخبارا كاذبة بأن الحكومة الإستونية طلبت العفو من روسيا ووعدتها بإعادة النصب التذكاري إلى موقعه الأصلي [٢٧].

كما وجهت إستونيا اتهامات الى روسيا وقد وجه الاتهام الى روسيا الإتحادية ، إذ عدتها إستونيا هجمات انتقاميه وبانها تقوم بتضليل الروابط التي تستخدمها الحكومة الاستونية في المؤسسات وذلك من خلال عرض صور للجنود السوفييت ، فبدأت سلسلة من الهجمات يطلق عليها (DDOS attacks) باستهداف المواقع التي تديرها الحكومة الإستونية، استمر هذا الهجوم لمدة ثلاثة أسابيع تم خلالها استهداف المواقع الإلكترونية الحكومية والبنوك و وسائل الإعلام مما أدى الى شلل تام في الخدمات الإلكترونية والأنظمة البنكية وتسبب الهجوم في عرقلة وصول المواطنين إلى بعض المواقع [٢٨]، واستهداف مواقع رئيس الوزراء والرئيس والبرلمان والوزارات، ومؤسسات الدولة الأخرى كالشرطة، وموقع الائتلاف الحاكم ، وتم اختراق عديد من المواقع الأخرى، والتي كان من بينها موقع حزب الاصلاح الذي قام المهاجمون من خلاله بنشر اعتذار رسمي مزور باللغة الروسية على انه صادر من رئيس الوزراء الإستوني أدى الى ذلك شل نشاط الدولة بالكامل ، وعلى الرغم من انكار روسيا لصلتها بالهجوم، إلا انها اعترفت أنه من الممكن أن يكون شن من داخل روسيا من قبل منظمات إجرامية غاضبة من القرار الإستوني بنقل التمثال [٢٩].في حين أن ما نتج عن هذا الهجوم هو توجيه انتباه إستونيا وغيرها من الدول إلى خطورة التهديدات الالكترونية، وكيف أن بإمكانها شل حركة الدولة تماماً حتى وان كان لفترة محدودة [٣٠].

ثانياً -الهجوم الروسي على جورجيا : بدأ الهجوم الإلكتروني الجورجي يوم الجمعة ٨ آب ٢٠٠٨ وانتهى يوم الخميس ٢٨ آب ٢٠٠٨ واستمر الهجوم ثلاثة أسابيع ، جرى ذلك إثر التوتر الذي شهده إقليم أوسيتا

KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

الجنوبية بسبب إعلانه الانفصال عن جورجيا ، قامت القوات الروسية بشن هجوم سيبراني على جورجيا ، حيث أضعف هذا الهجوم قدرة وسائل الدفاع الجوي الجورجية ، قالت وزارة الخارجية الجورجية إن روسيا تستخدم قراصنة الكمبيوتر لحجب أو إغلاق مواقع الحكومة الجورجية منذ أن شنت روسيا هجوماً عسكرياً ضد القوات الجورجية في أوسيتيا الجنوبية التي تقع في وسط جورجيا في الطرف الشمالي -الجبلي ، وتعد مدينة (تسخينفالي) عاصمتها [٣١]. قام مخترقون محترفون من روسيا عام ٢٠٠٨ بإعادة توجيه الاتصالات بشبكة الإنترنيت من جورجيا الى أجهزة خوادم في روسيا مما أدى الى زعزعة نشاط الحكومة في جورجيا ، حيث توقفت شبكة الانترنت الجورجية عن العمل في آب ٢٠٠٨، وتم الاعتداء على الموقع الإلكتروني للرئيس الجورجي ، وقد اتخذ الهجوم الالكتروني الذي تعرضت له جورجيا شكلين ، الأول هو اختراق بعض المواقع الالكترونية السياسية ، من بينها موقع رئيس الجمهورية، البرلمان والرئاسة ، وكذلك الصفحات الرئيسية لوزارة الخارجية ووزارة الدفاع ، كما تم اختراق بعض المواقع التجارية [٣٢]، ثم ظهرت على الموقع صورة الزعيم النازي ادولف هتلر بجانب صور لرئيس الجمهورية وغيره من الحكام الديكتاتوريين [٣٣]، الثاني هي تتمثل بهجمات الحرمان من الخدمة والتي وجهت ضد مواقع حكومية كموقع وزارة التربية والتعليم ، والمواقع التي تم تقدم اختبارات للطلاب، وموقع وأكبر بنك تجاري في جورجيا ، كما تمت مهاجمة مواقع الأخبار ووسائل الاعلام والتي شملت أكبر مواقع أخبار باللغة الإنجليزية في جورجيا ، وشبكات إخبارية من بينها BBC، CBC [٣٤]، وتزامناً مع تلك الهجمات قامت روسيا بشن هجمات عسكرية على جورجيا فضلاً عن الإضرار بمواقع الكترونية كوسائل الإعلام ، البنى التحتية ، المواصلات وغيرها من المواقع مما أدى الى إرباك واسع في

KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

جورجيا وتزامناً مع تلك الهجمات قام الجيش الروسي بتنفيذ عمليات عسكرية على جورجيا ، ويعد هذا النزاع المسلح الأول من نوعه الذي تزامنت فيه الهجمات السيبرانية مع الهجمات العسكرية معاً بهذا الشكل الواسع [٣٥] .

كان الضرر الأكبر في الجورجيا هو الحد من قدرة الدولة على إيصال رؤيتها للعالم ، وإيصال المعلومات للمواطنين من خلال الانترنت ويرجع السبب وراء هذا الهجوم الروسي رداً على إرسال الحكومة الجورجية الموالية للغرب قوات للحكومة الانفصالية المدعومة من موسكو[٣٦].

ثالثاً -الهجوم على أوكرانيا : تعتبر أوكرانيا هي دولة على خط المواجهة وموقع ذو أهمية كبيره لروسيا ، كان لدى روسيا سبب رئيسي على الأقل للتدخل في الانتخابات الأوكرانية ، ولسياستها العدوانية تجاه أوكرانيا بشكل عام ، هو إن نجاح أوكرانيا في أتصبح ديمقراطية مزدهرة وعملية وليبرالية ودولة أوروبية يمثل تهديداً وجوديًا للاستبداد الروسي الحالي ، طموحا بوتين الإمبريالية والجيوسياسية لهذا السبب استخدمت روسيا ، وستواصل باستخدام كل قدراتها ، ، بسبب ان الهجمات الإلكترونية الروسية أدت إلى اختراق شبكة لجنة الانتخابات المركزية عام ٢٠١٤ ، حيث تم شن العيد من حملات تضليل المعلومات على شرق أوكرانيا ، إزالة موقع المعارضة الروسية على الإنترنت من الإنترنت ، و قصف قراصنة مؤيدون لروسيا مواقع قادة المعارضة بالإضافة الى هجمات الكترونية متقطعة حتى قبل الإطاحة بـ(فيكتور يانوكوفيتش) [٣٧]. وقد استخدمت روسيا عدة آليات من أجل تحقيق من خلال تسخير الفضاء الالكتروني بدءا من محاولة التأثير على الرأي العام الروسي وصولا الى اختراق الانتخابات الأوكرانية [٣٨].بدأ الجيش الروسي باستخدام الطائرات المسيرة هذه في المهمات القتالية عن طريق ربط أربع قذائف متشظية شديدة

KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

الانفجار بالأجنحة لاستهداف المركبات الأوكرانية ، والمعدات ، والجنود [٣٩].تعرض نظام الانتخابات المركزي الوطني الأوكراني قبل أربعة أيام من التصويت للخطر وتم حذف الملفات الهامة ، رصد مسؤولو اللجنة الهجوم قبل أقل من ساعة من موعد الإعلان عن النتائج ، ومنعوا عرض النسخة المزورة علنًا. قامت وسائل الإعلام الحكومية الروسية ، بالتنسيق مع (Cyber Berkut)، ببث النتائج المزيفة ، ، حيث ، نشر (CyberBerkut) تعلن فوز " دميترو ياروش" بنسبة ٣٧ في المائة من الأصوات على بوروشنكو بنسبة ٢٩ في المائة .كذلك تعرضت أوكرانيا لعملية إلكترونية أخرى ضد شبكة الكهرباء الأوكرانية ، في ٢٣ كانون الاول ٢٠١٥ ، أن انقطاع الخدمة الذي عانى منه عملائها كان بسبب الدخول غير القانوني إلى أنظمة الكمبيوتر والتحكم الإشرافي واكتساب البيانات الشركة مما أدى الى تأثير الهجوم السيبراني على توزيع الكهرباء [٤٠]. تعرضت الى مسح البيانات الحكومية الحيوية وتدمير المواقع الحكومية ، بما في ذلك وزارتي التعليم والشؤون الخارجية.

مما تقدم يتضح أن القيادة الروسية وعلى راسها الرئيس (فلاديمير بوتين) عملت في السنوات القليلة الماضية بشكل دؤوب على تنمية قدرات روسيا في المجال السيبراني وتطويرها بشكل كبير، وسخرت تلك القدرات بصورة ذكية كسلاح فعال لإيقاع الضرر المطلوب في قدرات خصومها، بالشكل الذي جعل من تلك القدرات السيبرانية أحد عناصر الردع الاستراتيجي للدولة الروسية.

KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

الخاتمة:

إن الثورة التكنلوجية والمعلوماتية قد أوصلتنا إلى نتيجة مفادها أن أشكال التهديدات قد تتغير وذلك بظهور ما يعرف بالفضاء السيبراني الذي يعد بمثابة الميدان يتنافس عليه الدول من اجل زيادة قوتهم الالكترونية لاسيما في ظل اعتماد الدول بشكل تام على التكنلوجيا والمعلومات وربط أمنها القومي و الإقليمي بالفضاء السيبراني ، حيث خلقت هذه التطورات التقنية والتكنولوجية الحديثة العديد من التهديدات الأمنية والمعلوماتية، خاصةً على مستوى الأمن الاقليمي، والذي أصبح أكثر عرضةً للخطر نظراً لسهولة الانكشاف المعلوماتي الذ ي وفرته وسائل الاتصال والتواصل الحديثة، وانتشار مختلف أنواع المعلومات بزخم كبير على شبكات الإنترنيت، تحولت أدوات الإنترنت ، ووسائل الاتصال الحديثة، وصفحات المواقع الاجتماعية إلى أسلحة إلكترونية جندتها العديد من الدول لتخوض غمار حروبها الرقمية والمعلوماتية، في ظل التحولات التكنولوجية التي يشهدها العالم، لتكون هذه الأدوات والتقنيات الحديثة سلاحاً ذو حدين فهي من جهة ضرورية لمواكبة تغيرات العصر الحديثة، ومن جهة أخرى نافذةً للانكشاف الأمني والمعلوماتي، والعمل على تدمير البنية التحتية المعلوماتية للعدو ، وقد أدى هذا الى ظهور تحديات عدة على المستوى الإقليمي منها عدم القدرة على الحفاظ على سلامة البنية التحتية المعلوماتية و المواقع والانظمة والبيانات الرقمية من خطر التجسس او تعديل المعلومات أو أتلافها . وسعي روسيا الامتلاك زمام الريادة في مجال الفضاء السيبراني من خلال تطوير قدرتها السيبرانية من اجل فرض سيطرتها على المستوى الإقليمي او الدولي و كذلك العمل على تطوير ما لديها من موارد بشرية ومعرفية لتكون على قدر كاف من الجاهزية للرد على أية مخاطر قد تواجهها في المستقبل.

KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

الاستنتاجات:

١) إن أهمية المجال الإلكتروني في تشكيل قدرة الأطراف المؤثرة، وانتقال التهديدات وانتشارها، من النطاق التقليدي (البر والبحر والجو)، إلى الفضاء السيبراني، وللدول المتقدمة الأسبقية في الوجود والسيطرة والتحكم، والمجتمع الاقليمي يتابع اتجاهات التحول في قضية التعامل مع تهديدات الفضاء الإلكتروني، وإمكانية تحوله نحو العسكرة، وهذا الأمر بات واضحا من خلال تصاعد الهجمات الإلكترونية ومخاطرها على أمن الفضاء الإلكتروني وما فيه من معلومات لذلك فإن تصاعد القدرات في سباق التسلح السيبراني عبر الفضاء الإلكتروني وتبني سياسات دفاعية سيبرانية لدى الأجهزة المعنية بالدفاع والأمن، وتصاعد حجم الاستثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة، كله ينبئ بأن المستقبل لن يكون مضمونا أمام أطماع المقتدرين، ما لم تقدم الدول نحو المزيد من التكافؤ في المقدرات السيبرانية.

٢) هناك ارتباط بين امن المعلومات والامن الإقليمي باعتبار ان المعلومات هي ركيزة أساسية للأمن الإقليمي لأن هذه المعلومات جزء من السياسة الأمنية للدول واي اختراق قد يحدث يتسبب بتهديد وتوجيه هجمات تخترق البنية التحتية للدول ويخلق حالة من الاستقرار.

٣) تمثل البيئة الاستراتيجية السيبرانية بيئة جديدة مختلفة عن البيئة الاستراتيجية التقليدية، إن الأمن السيبراني هو عبارة عن أمن المعلومات، والذي يطبق على أجهزة الكمبيوتر والشبكات الحاسوبية أو على الانترنت ككل، وذلك يهدف المجتمع الإقليمي الى مكافحة الهجمات السيبرانية وغيرها من المحاولات غير المشروعة التي تحاول إتلاف أو تدمير أنظمة الكمبيوتر أو أنظمة الشبكات بكافة أنواعها.

KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

٤) ان انتشار الفضاء الإلكتروني ، وسهولة الدخول إليه ، اتسعت دائرة الصراعات السيبرانية ، وزاد عدد المهاجمين ، وكذلك الهجمات السيبرانية بسبب تطوير القدرات الهجومية الإلكترونية من اجل حيازة القوة والتفوق والهيمنة وتعزيز التنافس حول السيطرة والابتكار والتحكم في المعلومات وتعظيم القدرات القادرة على زيادة النفوذ والتأثير في المستويين الإقليمي والدولي وبما أن المتنازعين يتجهون في الصراعات التقليدية إلى استخدام شتى أنواع أسلحة التدمير الممكنة فقد انتقلت جبهات القتال بشكل مواز إلى ساحة الفضاء الإلكتروني .

٥) تتمثل الهجمات الإلكترونية بشكل عام في مجموعة الاختراقات الموجهة الشبكات الحاسب الآلي لسرقة أو تغيير معلومات ، أو تدمير النظام الإلكتروني ، أو استخدام الشفرات الخبيثة والتي تنتقل من حاسب آلي إلى آخر وتقوم بتعطيل الوظائف التي تقوم بها تلك الأجهزة ، أو إيقاف عمل الشبكات . وباستخدام هذه الوسائل يستطيع القائمون بالهجوم الإضرار والبنى التحتية ، والمؤسسات الحكومية ، وهو ما يترتب عليه تعطيل المحركات الرئيسة لاقتصاد الدولة والإضرار بمواطنيها وتهديد أمنها الاقليمي بشكل عام . ولذا تكون التداعيات الدولية لتلك الهجمات خطيرة وواسعة النطاق وتتخطى حيز الدولة لتؤثر في الأمن الإقليمي ككل، وقد أدى تزايد اعتماد الدول على أجهزة الحاسب الآلي إلى زيادة قابلية تعرضها للهجمات الإلكترونية واتساع نطاق التأثيرات المحتملة المترتبة على هذه الهجمات.

الهوامش:

١ بافل باييف ، لقوة العسكرية وسياسة الطاقة : بوتين والبحث عن العظمة الروسية ، مركز الإمارات للدراسات والبحوث الاستراتيجية ، أبو ظبي ، ٢٠١٠ ، ص ٦٩ .

2Adam Hlavek and Kimberly Ortiz ,The Russian Threat, In Brief , Threat Intelligence Report , IRONNET , 21 December 2020, pp 2-4 .

٣ كريستوفر س.تشسفيس ، وآخرون ، تعزيز الاستقرار الاستراتيجي مع روسيا ، مؤسسة راند ، ٢٠١٧ ، ص ٧.

4 Federation Council of the Federal Assembly of the Russian Federation's official website (2013) , Transcript of Parliament hearings on the topic of Legislative Procurement of National Cyber security in the Russian Federation held on 29 November 2013, Date Of Visit 1/8/2022., At The Link : http://council.gov.ru/media/files/ .

٥ كنوت دورمان ، بعد عشرين عامًا: القانون الدولي الإنساني وحماية المدنيين من آثار العمليات السيبرانية أثناء النزاعات المسلحة ، المجلة الدولية للصليب الأحمر ، تاريخ الزيارة ٢٠٢٢/٨/١، متاح على الرابط :

https://international-review.icrc.org/ar/articles/twenty-years-international-humanitarian-law-and-protection-civilians-against-effects-cyber.

6 Alexander Chernykh , Maria Stroiteleva, , The Internet is being controlled byPeople who do not know how to use Email are attempting to regulate the Internet, Kommersant ,Date Of Visit 2/7/2022,At The Link : https://www.kommersant.ru/doc/3907444 .

7 Runet resilience exercises postponed until the end of the pandemic , Interfax , 26 january 2021_, Date Of Visit 2/8/2022, At The Link : Runet resilience exercises postponed until the end of the pandemic (interfax.ru) .

8 NIKOLAI LITOVKIN , What is the updated Russian cyber-security doctrine about? , Russia Beyond , Date Of Visit 3/8/2022, At The Link :

https://www.rbth.com/defence/2016/12/07/what-is-the-updated-russian-cyber-security-doctrine-about_654407 .

٩ ايهاب خليفة ، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي ، المستقبل للأبحاث والدراسات المتقدمة، العربي للنشر والتوزيع ، ابو ظبي ،٢٠١٦، ص ١٥٣.

١٠ نوران شفيق ، اثر التهديدات الإلكترونية على العلاقات الدولية : دراسة في ابعاد الامن الالكتروني ، مكتب العربي للمعارف ، القاهرة ، ٢٠١٦ ، ص ١٠٣ .

11 Cornish , paulone cyber war far , Achatham House Report , The Royal institute of international Affairs , London , 2011 , p 18 .

١٢ إيهاب خليفة ، مجتمع ما بعد المعلومات ...، مصدر سبق ذكره ، ص ١٥٣.

13 Cornish , paulone cyber war far , Ibide ,p19 .

١٤أفضل خمسة جيوش الكترونية في العالم ، مركز الدراسات كاتيخون ، تاريخ الزيارة ٢٠٢٢/٧/٦ ، متاح على الرابط : Катехон № 5. 2020. Специальный выпуск | مركز دراسات كاتيخون (katehon.com).

١٥ الاستخبارات ـ ماهو الدور الذي تلعبه خلال الحروب والنزاعات الدولية. ملف؟،المركز الاوربي ، تاريخ الزيارة ٢٠٢٢/٧/٦ ، متاح على الرابط :https://www.europarabct.com/ .

16 Military Doctrine of the Russian Federation , approved by Russian Federation President V. Putin " , EMBASSY OF THE RUSSIAN FEDERATION, 31 December 2014, Date Of Visit 6/8/2022,At The Link : https://thailand.mid.ru/en/military-doctrine-of-the-russian-federation

١٧نورهان الشيخ ، " موسكو وواشنطن .. صراع سيبراني " ، الخليج، تاريخ الزيارة ٢٠٢٢/٨/٥.
، متاح على الرابط :
http://www.alkhaleej.ae/supplements/page/3c792d51-a025-437d-9f36.

١٨ نوران شفيق ، أثر التهديدات الالكترونية على العلاقات الدولية : دراسة في ابعاد الامن الالكتروني ، مصدر سبق ذكره ، ص١٠٤ .

19 Bobo Lo, “Russia’s Crisis: What It Means for Regime Stability and Moscow’s Relations with the World,” Policy Brief, Centre for European Reform, Date Of Visit 10/8/2022 , At The Link:
at https://www.cer.eu/sites/default/files/publications/attachments/pdf/2011/policybrief_russia_19feb09-771.pdf .

٢٠ ايهاب خليفة ، القوة الالكترونية : كيف يمكن ان تدير الدول شؤونها في عصر الانترنيت ، دار العربي ، ٢٠١٧ ، ص ٥٤ .

٢١ بوتين يطلق سباق التسلح مع الغرب صحيفة الجمهورية، تاريخ الزيارة ٨/ ٨ /٢٠٢٢ متاح على الرابط : http://www.aljoumhouria.com/article/print-article/29687 51 ،.

٢٢ كوزي پير وفانسي بير مجموعات اختراق روسية متعددة الرؤوس وهدفها واحد ، مقال منشور على موقع الجزيرة ، تاريخ الزيارة ٢٠٢٢/٨/٨ ، متاح على الرابط :
https://www.aljazeera.net/amp/news/scienceandtechnology/2019/10/17 .

23 " Russian Space Launch Vehicles " Globalsecurity.Org , Date of visit 9/8/2022, At The Link , Https:www.globalsecurity.org/space/world/russia/launch.htm .

24 Steve Ranger , Russian Cyberattacks An 'Urgent Threat' To National Security , ZDNET , 21 July 2020 , Date Of Visit 9/8/2022, At The Link: https://www.zdnet.com/article/russian-cyberattacks-an-urgent-threat-to-national-security/ .

٢٥ اسراء تريسي ، هجمة إلكترونية تشلّ مؤسسات الدولة بأكملها.. قصة "تمثال الأحرار" الذي أشعل الحرب السيبرانية بين إستونيا وروسيا ، موقع عربي بوست ، ، تاريخ الزيارة ٢٠٢٢/٨/٩ ، متاح على الرابط https://arabicpost.net: .

26 Estonia Fines Man For 'Cyber War' , BBC News , Date Of Visit 9/8/2022,At The Link : http://news.bbc.co.uk/2/hi/technology/7208511.stm .

27 Heather A. Conley Et Al , Russian Soft Power In The 21st Century : An Examination Of Russian Compatriot Policy In Estonia . Center For Strategic And International Studies, Washington, 2011,P23.

28 Estonia Repels Cyberattacks Claimed By Russian Hackers , Date Of Visit 11/8/2022 , At The Link : https://www.aljazeera.com/news/2022/8/18/estonia-says-it-repelled-cyber-attacks-claimed-by-russian-group.

29 ANTOANETA ROUSSI ،Estonia Fends Off 'Extensive' Cyberattack Following Soviet Monument Removal ،Politico ، Date Of Visit 24/8/2022, At The Link : https://www.politico.eu/article/estonia-extensive-cyber-attack-following-soviet-war-monument-removal/ .

٣٠ نوران شفيق ، أثر التهديدات الالكترونية على العلاقات الدولية دراسة في أبعاد الأمن الإلكتروني ، مصدر سبق ذكره ، ص ١٤٣ .

31 Travis Wentworth , How Russia May Have Attacked Georgia's Internet , Newsweek , Date of visit 20/8/2022, At The Link : https://www.newsweek.com/how-russia-may-have-attacked-georgias-internet-88111.

32 Jon Swaine , Georgia: Russia 'Conducting Cyber War' ,The Telegraph , Date of visit 20/8/2022, At The Link : https://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html.

33 Dancho Danchev , Coordinated Russia vs Georgia cyber attack in progress , zdnet, Date of visit 20/8/2022: https://www.zdnet.com/article/i-just-spent-a-week-with-a-robot-cat-and-my-life-will-never-be-the-same/ .

34 Donald L. Buresh, A Critical Evaluation Of The Estonian Cyber Incident , JOURNAL OF ADVANCED FORENSIC SCIENCES , Vol-1 , Issue 2 , P 17-19 Pdf , Date Of Visit 20/8/2022 https://openaccesspub.org/jafs/article/1686#ridm1849989524 .

35 JOHN MARKOFF , Before The Gunfire, Cyberattacks , The New York Times , Date Of Visit 20/8/2022, At The Link : https://web.archive.org/web/20190330172829/https://www.nytimes.com/2008/08/13/technology/13cyber.html .

٣٦ خالد خميس عبدالسالم السحاتي، التدخل العسكري الروسي في جورجيا عام ٢٠٠٨ -دراسة في الاسباب والنتائج، مجلة العلوم والدراسات الإنسانية ،العدد(٣٦) ، كلية الآداب والعلوم، جامعة بنغازي، ليبيا، ٢٠١٧ ،ص٢.

37 Elmar Brock: Ukraine’s Success—Worst Thing that Could Happen to Russia, Interfax-Ukraine, December 23, , Date of visit 15/8/2022, At The Link : https://interfax.com.ua/%20news/interview/392660.html.

٣٨ مايكل كوفمان وآخرون ، عبر من عمليات روسيا في شبه جزيرة القرم وشرق أوكرانيا ،مؤسسة راند ، ترجمة مؤسسة راند ، كاليفورنيا ، ٢٠١٧، ص ١٢ .

KUFA STUDIES CENTER JOURNAL
UNIVERSITY OF KUFA
مجلة مركز دراسات الكوفة - جامعة الكوفة
KSCJ OPEN ACCESS
ISSN (P) : 1993-7016
ISSN (E) : 2708-728X
www.journal.uokufa.edu.iq

٣٩ صاموئيل بالدين وحفري إيدموندر ، مركبات ذاتية القيادة للجيش الروسي في اوكرنيا ،ترجمة مركز الخطابي للدراسات ، منظمة أبحاث و تحليل عسكري – الولايات المتحدة الامريكية ٦/٧/ ٢٠٢٢ ، ص ص ١-٦ .

40 GREGORY BARBER , The Race To Rescue Ukraine's Power Grid From Russia , Wired , , Date of visit 5/10/2022 , At The Link : https://www.wired.com/story/the-race-to-rescue-ukraines-power-grid-from-russia/.