استراتيجية الامن السيبراني الروسي

Russia's Cyber security Strategy

م.م. زينب ضياء محمد امين

مركز الدراسات الاستراتيجية والدولية – جامعة بغداد

zainab.d@cis.uobaghdad.edu.iq

تاريخ استلام البحث: ٢٠٢٤/١١/٥ تاريخ قبول النشر: ٢٠٢٥/٢/٢٤

الملخص:

يعد مفهوم الأمن السيبراني أحد أهم المفاهيم التي طرأت على السياسة الدولية والتي تسعى الدول الى تحقيق الوصول أليها في العالم خصوصاً في ضوء التطور التكنولوجي والمعلوماتي والذي أحدث نقلة نوعية في جميع المجالات (السياسية، الاقتصادية، العسكرية، الأمنية) حيث أن لهذا التطور تأثيراً واضحاً على العلاقات الدولية وتحديداً في مجال التنافس والصراع، حيث أصبح للحروب والجرائم شكلاً جديداً (الحروب السيبرانية، الجرائم السيبرانية) والتي باتت اليوم تشكل تهديداً للنظام الدولي بصورة عامة وللدول خاصتاً، اذ انها تمثل أحد التحديات التي تواجه الدول مهما كانت متقدمة سواء اقتصادياً او عسكرياً أو تكنولوجياً، وهذا ما دفع بالعديد من الدول الى اعادة صياغة رؤيتها الاستراتيجية المرتبطة بالأمن القومي ومنها روسيا والتي تعمل على تطوير مجال مفهوم الأمن السيبراني وتوظيفه في عدة مجالات (الأمني، العسكري، الاقتصادي، التكنولوجي) كذلك ومواجهة الحروب السيبرانية والتي تشكل خطراً على الأمن القومي الروسي.

الكلمات مفتاحية: الامن السيبراني، الحروب السيبرانية، الاستراتيجية الروسية، الارهاب السيبراني.

Abstract:

The concept of cyber security has become one of the most important notions in international politics, as countries strive to achieve and maintain it in light of the technological and informational advancements that have brought about a qualitative shift across various fields (political, economic, military, security). This progress has had a significant impact on international relations, particularly in the areas of competition and conflict. Wars and crimes have taken on a new form (cyber wars, cybercrimes), now posing a threat to the international system in general and to individual states in particular. Cyber security challenges are a concern for all countries, regardless of their level of economic, military, or technological development. This has led many nations to reshape their strategic visions related to national security, including Russia, which is actively working to develop cyber security and employ it across various sectors (security, military, economic, technological) to confront cyber warfare that poses a threat to Russian national security.

Keywords: Cybersecurity, Cyber Wars, Russian Strategy, Cyber Terrorism

المقدمة:

لقد لعبت الثورة التكنولوجية دوراً مهماً على المستويات كافة (الاقتصادية،السياسية، الأمنية، المعلوماتية) فلم تعد تقتصر على التفاعلات السياسية والاقتصادية فحسب، بل أثرت بالعديد من المجالات أهمها التنافس والصراع غير التقليدي والمرتبط بالفضاء السيبراني، و التي تعد أحد أهم الأدوات التي تستعملها الدول في مجال التنافس والصراع الدولي فضلاً عن توظيفها في تحقيق مصالحها وأهدافها الاستراتيجية، إضافة للحروب السيبرانية والتي تعد حروب المستقبل المقبلة، فهي تمثل احد اهم الحروب التي تشكل خطراً وتهديداً اكثر من الحروب التقليدية نتيجة حجم التخريب والتدمير الذي تنتجه هذه الحروب، ولم تعد هذه الحروب قاصرة على الفاعلين الدوليين فحسب بل توسعت لتضم فاعليين آخرين كالشركات التكنولوجية والمعلوماتية والتي تهيمن بدرجة او بأخرى على المقومات التكنولوجية والمعلوماتية، وكذلك على المهارات البشرية المدربة على التعامل مع مثل هذه الوسائل، لذلك فتعد روسيا الاتحادية أحد أهم الدول التي تستخدم وتوظف هذا المفهوم كأداة لإدارة صراعاتها وتفاعلاتها مع الدول الإقليمية والدولية، حيث ان الأمن السيبراني يشكل أحد المقومات الاستراتيجية في رسم سياساتها الخارجية اتجاه الدول المنافسة لها فضلا عن تحقيق مصالحها وأهدافها المنشودة، لذلك فنجد استراتيجية الأمن السيبراني الروسي تعمل على تطوير مفهوم الأمن السيبراني بهدف حماية البنية التحتية للمعلومات الاستخباراتية الخاصة بها، فضلاً عن الوقوف بوجه المخاطر والتهديدات السيبرانية التي تمس أمنها القومي.

أهمية الدراسة: تكمن أهمية الدراسة وذلك من خلال توظيف روسيا للقوة السيبرانية في ادارة تفاعلاتها الدولية، وقدرة هذه القوة على التكيف مع المتغيرات والتحولات التي تطرء على النظام الدولي، لذلك فأن أهمية الدراسة تكمن في العلاقة بين التطور التكنولوجي والمعلوماتي وبين ادراك صانع القرار الروسي لأهمية الأمن السيبراني في ادارة التفاعلات الدولية لروسيا، كما وأنها تعد أحد مقومات الاستراتيجية الروسية في تحقيق المصالح والاهداف المرتبطة بالاستراتيجية العليا للدولة.

اشكالية الدراسة: تكمن إشكالية الدراسة وذلك من خلال طرح عدة تساؤلات والمتمثلة بما يلي:

١. ما الأمن السيبراني وماهي خصائصه؟
٢. ما الحروب السيبرانية وماهي خصائصها وأشكالها؟
٣. هل أثرت استراتيجية الأمن السيبراني الروسي على مكانة روسيا الدولية؟
٤. ما التهديدات السيبرانية وكيف واجهت روسيا تلك التهديدات؟
٥. ما هي أهم سيناريوهات الحروب السيبرانية القادمة؟

فرضية الدراسة: تقوم الدراسة على فرضية مفادها (كلما تزايدت التهديدات السيبرانية لروسيا الاتحادية كلما سارعت الى صياغة عدة أستراتيجيات سيبرانية لتصدي للتحديات الافتراضية بكل أشكالها)

منهج الدراسة: اعتمدت الدراسة على منهجين مهمين في تحقيق الاهداف واثبات الفرضية وهي كالتالي:

١. **المنهج الوصفي (التحليلي):** حيث استخدم هذا المنهج لتحليل ووصف جميع مقومات القوة السيبرانية الروسية وكيفية توظيفها في مواجهة التهديدات والحروب السيبرانية وعلى الصعيدين الاقليمي والدولي.
٢. **المنهج الاستشرافي:** والذي يضمن أهم السيناريوهات المستقبلية والتي ستوضح شكل الحروب السيبرانية القادمة ومدى تأثيرها على أستراتيجية الامن السيبراني الروسي.

هيكلية الدراسة: تقوم هيكلية الدراسة على ثلاثة محاور والمتمثلة بما يلي: المحور الاول: ما هية الامن السيبراني، اما المحور الثاني: التهديدات السيبرانية التي تواجه روسيا الاتحادية، اما المحور الثالث: استراتيجية روسيا الاتحادية في مواجهة التهديدات السيبرانية

المطلب الأول: ما هية الامن السيبراني

المحور الاول: مفهوم الامن السيبراني وخصائصه:

يعرف الأمن السيبراني على أنه المجال المتعلق بالإجراءات والمقاييس والمعايير الخاصة بالحماية المتصلة بالشبكات، كما ويعرف على أنه أمن المنظومات والشبكات المعلوماتية فضلا عن الأمن المتصل بالبيانات والمعلومات الخاصة بالدولة، فقد عرف العالم والمفكر ريتشارد (Richard) الأمن السيبراني على أنه "كافة الوسائل الدفاعية والتي بإمكانها كشف الاختراقات و احباط المحاولات التي يقوم بها القرصنة"، بينما عرف أدوارد أمورسو (Edward Amros) الأمن السيبراني على أنه "جميع الوسائل والأساليب والتي بإمكانها الحد والوقوف بوجه الهجمات التي تصيب أجهزة الحاسوب وكافة البرمجيات والشبكات والمتمثلة بالوسائل والأدوات التي تستخدم في الوقوف بوجه القرصنة والكشف عن الفيروسات التي تصيب الشبكات والبرمجيات" كما وقد عرف الاتحاد الدولي للاتصالات الأمن السيبراني في تقرير نشره عام ٢٠١١ على أنه " مجموعة من المهام والوسائل والأساليب وكذلك السياسات والإجراءات الأمنية التي تنتهجها الدول لأدارة المخاطر السيبرانية "[١].

لذلك فنجد مفهوم الأمن السيبراني وبحسب تقارير قدمها الخبراء المختصين في هذا المجال على أنه مفهوم غامض وواسع المدى وشامل فهو يهدف الى ثلاثة مفاهيم، الأول يشير الى مجموعة الأنشطة والأدوات التي تهدف الى حماية الشبكات والبرمجيات من اي هجوم او تهديد محتمل بالإضافة الى البرامج والمعلومات المتعلقة بالفضاء السيبراني، اما الثاني فيشير إلى المجال الواسع الذي يهدف الى مجموعة الأنشطة والإجراءات للحد من اي خرق يصيب البيانات والمعلومات الخاصة بدولة ما اما الثالث فيشير إلى أمن المعلومات والذي يهدف الى حماية المعلومات وأنظمة المعلومات من الوصول اليها او الكشف عنها وحماية الخصوصية للمعلومات المتعلقة بأمن الدول[٢].

كما أن مفهوم الامن السيبراني هو اشمل واوسع من المفاهيم الاخرى لأنه يهتم بتأمين كل ما هو مادي من منشآت واجهزة وانظمة وبرمجيات من التهديد والهجوم، لذلك فأن مفهوم الامن السيبراني هو مجموعة من الادوات والممارسات التي تهدف الى حماية الاجهزة والبيانات والبرامج من الهجمات السيبرانية، والتي بإمكانها التعرف عليها لذلك فأن الامن السيبراني يهتم بتأمين الانظمة ومكافحة ما يسمى بالجرائم السيبرانية وكذلك الدفاع السيبراني[٣].

كما وقد اهتم علماء السياسة بتفسير هذا المفهوم حيث ظهرت العديد من الدراسات والتقارير التي تبين لنا مدى اهمية الامن السيبراني خصوصا بعد اقبال العديد من الدول على استخدامها في مجالات عدة أهمها المجال الامني والعسكري لأحداث قفزات تنموية عالية في التطور التكنولوجي، لذلك فأن الامن السيبراني يعني أمن

المعلومات الذي يهتم بحماية الانظمة والشبكات والاجهزة الامنية الخاصة بالدولة، ويعرف ادوارد أمورسو صاحب كتاب "الامن السيبراني" الذي صدر عام ٢٠٠٧ حيث عرف الامن السيبراني على أنه "مجموعة من الوسائل والاجراءات التي بإمكانها الحد من مخاطر الهجوم والتهديد على الشبكات وانظمة الحاسوب " لذلك فالأمن السيبراني هو عملية ممارسة الدفاع عن أجهزة الحاسوب والشبكات والبيانات من الهجمات المنظمة(الهجمات السيبرانية) كونه يمثل احد اهم التحديات التي تواجه الامن القومي لأي دولة ومدى تأثيره على السلم والامن الدوليين، فحسب الإحصائيات التي قدمها المعهد الدولي للدراسات الاستراتيجية في لندن فأنه من الممكن ان تصل حجم الخروقات السيبرانية الى ما يقارب ١٠,٥ ترليون دولار بحلول عام ٢٠٢٥ ووفقاً لتقرير Edsurge، لذا فأن الهدف الرئيسي للأمن السيبراني هو تعزيز قدرة الدولة على مواجهة التحديات والتهديدات التي تصيب الفضاء السيبراني بشكل عام والأمن القومي للدولة بشكل خاص، وهذا ما دفع بعض الدول كروسيا والولايات المتحدة الامريكية والصين لوضع منظومات واجندة تعمل على مواجهة التهديدات والجرائم السيبرانية[٤].

كما وقد قدم المختصان بالشأن السيبراني بيتر سينز والان فريدمان تعريفاً للأمن السيبراني على أنه "عالم شبكات الحاسوب والمستخدمون الذين يقفون وراءها حيث يتم تخزين المعلومات ومشاركتها ونقلها عبر شبكات الانترنيت" ويعتبر هذا التعرف ضيقاً لمفهوم الامن السيبراني أو ما يسمى بالفضاء السيبراني حيث اقتصر تعريفه على الاجهزة والمستخدمون فقط هم من يتحكمون في تلك الاجهزة، اما المفهوم الشامل والاوسع فهو الذي لا يقتصر على حدود جغرافية واحدة بل يمتد ويشمل البنى التحتية لتكنلوجية المعلومات والبيانات المرتبطة بها، خلال ما سبق يمكن ان نستنتج يمكن تعرف الفضاء السيبراني على انه مجال دولي يضم مختلف الاجهزة والتي يتم التحكم بها عن طريق الشبكات السلكية واللاسلكية، حيث تعمل هذه الاجهزة على التصدي لأي هجوم محتمل للبيانات والمعلومات والتي تتم عن طريق المستخدمين سواء كانوا افراد او منظمات او شركات متعددة الجنسية او دول [٥].

ويمكن تحديد خصائص الامن السيبراني بالنقاط التالية:

١. يعد مفهوم شامل وواسع ومعقد وقابل للتغير وفق المتغيرات التي تطرأ عليه.

٢. يضم العديد من الفاعلين "الدول، الشركات متعددة الجنسية، المنظمات من غير الدول، التنظيمات الارهابية".

٣. يعد مفهوم الامن السيبراني من المفاهيم التي تواكب التطورات والتغييرات التي تطرأ على النظام الدولي بشكل عام.

٤. يعد فضاء غير محدد يضم خصوم متعددة.

٥. يضم هجمات سيبرانية " جرائم سيبرانية" اضافة الى امكانية في خلق حروب سيبرانية معقدة.

٦. يعد من أخطر المفاهيم التي تواجه النظام الدولي وكذلك الدول نتيجة الاضرار التي يسببها بما فيها خرق النظام الأمني.

اما بالنسبة لتحديات الامن السيبراني فهنالك العديد من التحديات التي تطرآ على الامن السيبراني وهي تحديات كبيرة ومتعددة والمتمثلة بما يلي [٦]:

اولا/ الافراد: ويعد الفرد من أخطر التحديات التي تطرأ على الامن السيبراني ولديه القدرة على ما يلي:

١. قدرته على التحكم في ردود الافعال العاطفية.

٢. البيانات الامنية متعددة ومعقدة وتخضع الى احكام الافراد.

٣. أن الانظمة الامنية هي من تضم الافراد بالتالي فهم من يتحكمون بها وباستعمالاتها.

٤. أن الانظمة الامنية يمكن ان يتم خرقها عن طريق الافراد او الاشخاص وكذلك خرق حقوقها.

ثانيا/ خطورة استعمال الفضاء السيبراني من قبل المنظمات.

ثالثاً/ يمكن خرق الشيفرات الخاصة بالنظام.

رابعاً/ التطور التكنلوجي الحاصل قد يستخدم في شن هجمات سيبرانية وهذا ما يشكل تهديداً في المستقبل.

خامساً/ ظهور تقنيات جديدة ومتطورة بالتالي سيشكل تهديداً للأمن الدول.

سادساً/ زيادة الهجمات السيبرانية نتيجة التطورات على الشبكات الخاصة بالأنترنيت وهذا ما سيؤدي الى زيادة الحروب السيبرانية اضافة الى التجسس السيبراني من جهة اخرى

سابعاً/ المرونة السيبرانية والتي تعد أحد المميزات التي تتمتع بها الشركات والتي تمكنها من القدرة على مواجهة التهديدات والتكيف معها.

المحور الثاني: مفهوم الحروب السيبرانية وخصائصها

ويعد مفهوم الحروب السيبرانية من المفاهيم المعاصرة، والتي شغلت أهمية كبيرة في مفهوم الأمن السيبراني فالعالم اليوم أصبح عالم المعلومات والبيانات فمن يملك المعلومة يمتلك القوة، وبالتالي يسيطر على الكثير من مرافق الدولة والمؤسسات، لذلك أصبح من أولويات الدولة حماية المعلومات من الاختراقات الإلكترونية خصوصاً المعلومات التي تخص أمن الدول والأمن الاستخباراتي للدولة، حيث أصبح آمن المعلومات والأمن السيبراني وكذلك الحروب السيبرانية احد خصائص السياسات الأمنية التي تسعى الدول الى تحقيقها، وقد عرف ميشال ثمين الحروب السيبرانية على أنها مجموعة من الإجراءات التي تتخذها الدولة من أجل الوقوف بوجه الهجمات و اختراق المعلومات [٧].

كما وتعرف على أنها "نزاع مسلح بكونه عملية الكترونية سواء كانت هجومية او دفاعية مما قد تؤدي الى أحداث أصابات او قتل أشخاص أو الاضرار بالممتلكات وتدميرها ووفقاً للقانون الدولي، كما وتتصف الحروب السيبرانية على انها حرب بعيدة المدى وغير محددة ومعقدة كونها توجه نحو الشبكات العابرة للحدود الدولية مما يؤدي الى اضرار كبيرة في المنشآت الحيوية للدول [٨].

وتعرف الحروب السيبرانية على أنها "مجموعة من الإجراءات التي تتخذها أطراف النزاع المسلح لتفوق على خصومهم وذلك من خلال عدة إجراءات يتخذونها اهمها اختراق أنظمة الحواسيب الخاصة بالخصم والحصول على معلومات سرية "التجسس السيبراني" مما يؤدي الى نشوب حرب سيبرانية متكافئة [٩].

وتكمن خطورة الحروب السيبرانية بالاستغلال غير المشروع لأنظمة الحاسوب والشبكات والبرمجيات والتي تعتمد عملها على البرامج الرقمية بغرض احداث اضرار وذلك من خلال عمليات اختراق وتدمير مصادر النظم

المعلوماتية والبيانات، كما وأن جذور الحروب السيبرانية ظهرت منذ انهار الاتحاد السوفيتي عام ١٩٩١ حيث بدأت المواجهات تظهر بين كل من روسيا وأوكرانيا، لذلك نجد روسيا تعمل على تطوير برمجيتها، حيث أن أول الحروب السيبرانية التي قامتها روسيا ضد مؤسسات الدولة الاوكرانية كانت عام ٢٠١٣[١٠].

كما أن مفهوم الحروب السيبرانية مرتبطاً بقيادات عسكرية مختصة بتدمير واختراق أنظمة المعلومات الى الحد الذي قد يسبب حدوث حروب نووية، أضافة لذلك فقد عرف المركز الالماني لاستراتيجيات الامن السيبراني الحروب السيبرانية بأنها" هجوم عابراً للحدود الفضاء الالكتروني، غايته الاضرار بالأنظمة التكنولوجية والمعلوماتية في دولة ما وذلك عن طريق تدميرها وهذه الاثار ناتجة عن ما يسمى بالقنبلة الذكية وهي عبارة عن برامج الكترونية تهدف الى اغلاق نظام الكتروني او شبكة الكتروني بحد ذاتها أو محو بيانات او المعلومات المتوفرة على الشبكات"[١١].

أما بالنسبة للخصائص الجريمة السيبرانية فأن الجريمة السيبرانية تتصف بعدة خصائص والمتمثلة بما يلي:

١. تتصف بأنها حروب رقمية غير تقليدية بعيدة المدى محورها ونقطة ارتكازها هو التطور التكنولوجي والتقني فضلاً عن الوسائل الحديثة المستخدمة فيها.

٢. تتصف بأنها حرب غير محددة الاهداف حيث تتعدى مخاطرها ساحات القتال التقليدية لتمس أكثر المواقع الحساسة بالدولة "السيادة، الاستخبارات".

٣. تتصف بالسرعة وامكانية المناورة والتي تعطي المهاجم أفضلية واضحة على المدافع [١٢].

٤. تتصف بخطورتها على البنى التحتية حيث تعد أحد المهددات التي تستهدف "الافراد، الدول، الحكومات".

٥. تتطلب استراتيجيات خاصة لمكافحتها كما وتتطلب اجهزة وقوة قانون [١٣].

لذلك فأن الحروب السيبرانية تعد أخطر أنواع الحروب في السياسة الدولية كونها حرب بعيدة المدى قابلة لتغير وتغير الاهداف والوسائل تمس بالدرجة الأولى الجانب الأمني والسياسي وهذا ما يندرج تحت مسمى السيبراني والذي يضم أبعاداً عديدة منها:-

اولا/ البعد العسكري: يعد أهم الأبعاد في الأمن السيبراني حيث يوفر الأمن السيبراني للقوات العسكرية أمكانية الصد لأي هجوم محتمل اضافة الى تبادل المعلومات والأوامر عن بعد وبشكل آمن وسلس، وكذلك الصد للهجمات السيبرانية الأخرى المحتملة وكما حدث في ايران عندما اخترقت منشئاتها النووية.

ثانياً/ البعد الاقتصادي: يعد أحد الأبعاد المهمة للأمن السيبراني وتظهر اهميته بشكل واسع وكبير في الجانب الاقتصادي والمتضمن المعاملات التجارية والمالية والاقتصادية حيث أصبح الأمن السيبراني أحد اهم الوسائل والأدوات المستخدمة في مجال الاقتصاد ومجالات التنمية المستدامة.

ثالثاً/ البعد الاجتماعي: حيث يأخذ الأمن السيبراني بعداً اجتماعيا ومختلفا، ان اصبحت مواقع التواصل الاجتماعي أحد الأدوات التواصل بين الأفراد والتي تمد بالمعلومات والافكار من ناحية ومن ناحية فهي تعرض المجتمع الدولي للخطر اذ بإمكانها أن تمس هوية الاشخاص وأحد أدوات التهديد للسلم المجتمعي، وهذا ما يتطلب زيادة الوعي لدى الأفراد ومدى معرفتهم بمخاطر اختراقه [١٤].

رابعا/ البعد السياسي: ويعد أحد أهم الأبعاد الرئيسية في الأمن السيبراني والتي تشكل محوراً مهماً في العلاقات الدولية، كما وتعد وسيلة تبادل المعلومات والوثائق الحساسة بين الدول، لذلك لا بد من تفعيل هذا البعد لتلافي أي خلافات وأزمات سياسية بين الدول، كما وقد شهدت العلاقات الدولية حروب فعلية شرسة نتيجة اختراق الأمن السياسي للدولة ومثال ذلك الحرب الروسية _ الاوكرانية عام ٢٠٢٢ والتي بدأت بحرب سيبرانية شرسة انتهت بحرب مدمرة.

خامسا/ البعد القانوني: ويعد هذا البعد بمثابة اداة ضبط للمجتمعات، اذ لابد من الدول ان تشرع قوانين وتفعيل اجراءاتها اتجاه أي خروقات سيبرانية تواجهها الدولة وكذلك تفعيل دورها في مكافحته مثل هكذا جرائم اضافة الى وجود قوانين تواكب هذا التطور [١٥].

لذلك فأن القوة السيبرانية بشكل عام وكما عرفها "جوزيف ناي" بأنها "كافة الموارد المتعلقة بالتحكم والسيطرة على اجهزة الحاسوب وكذلك البيانات والمعلومات والشبكات الالكترونية والتكنولوجية والبنى التحتية والمعلوماتية والمهارات والموارد البشرية والمادية وكيفية تعاملها مع هذه الوسائل "، كما وأن القوة السيبرانية يحكمها اتجاهين [١٦]:

الاتجاه الاول: دعم القوة الناعمة للدول بمعنى أن بإمكان القوة السيبرانية أن تصبح مجالاً لشن الحروب السيبرانية والهجمات التي تتضمن نشر البيانات والمعلومات، فضلاً عن ممارستها حرب نفسية وكذلك تأثيرها على الرأي العام وكذلك النشاط السري والاستخباراتي الخاص بالدول.

الاتجاه الثاني: يتضمن زيادة الانفاق على مكافحة الجريمة السيبرانية وحماية الشبكات الوطنية من خطر التهديدات السيبرانية، وبناء نظام امن سيبراني يهدف الى مكافحته أي خروقات وتهديدات سيبرانية تمس الأمن الاقليمي للدولة وكذلك أمنها القومي.

وتعد الحروب السيبرانية من أخطر انواع الحروب والتي طرأت على الساحة الدولية، حيث انها تمثل أحد المتغيرات المؤثرة في رسم السياسة الدولية، اذ يمكن تقسيمها الى عدة انواع والمتمثلة بما يلي:

اولاً: الحروب السيبرانية الباردة: يتصف هذا النوع من الحروب بانها حروب مستمرة بين الفاعلين كما وأنها ذات طبيعة ممتدة ودائمة النشاط العدواني، حيث انها تتخذ ابعاداً عدة قد تكون حرب ذات طابع اقتصادي او سياسي او اجتماعي او ذات طابع ثقافي، فهي تعد احد انواع الحروب ذات القوة الناعمة والمستخدمة في العديد من الصراعات والنزاعات فهي لا تصل الى حد الحروب التقليدية ومستوى الحرب السيبرانية الشاملة انما هي مقتصرة على القوة الناعمة في تحقيق المصالح والاهداف المنشودة للدول، ومثال هذه الحروب الصراع والتوتر بين استونيا وروسيا عام (٢٠٠٧) وكذلك التهديدات المتبادلة بين الصين والولايات المتحدة الامريكية وروسيا [١٧].

وقد تعرضت روسيا الى توجيه عدة اتهامات والتي تضمنت قيامها بالقرنصة السيبرانية في الانتخابات الامريكية في عام ٢٠٢٠ لدعم المرشح "دونالد ترامب" الرئيس الامريكي الفائز في تلك الانتخابات، في مواجهة منافسته في الحزب الديمقراطي "هيلاري كلنتون"، كما اتهمت روسيا بشن هجمات سيبرانية على كل من النرويج والتشيك وبريطانيا وهذا ما دفع بالدول للدفاع عن نفسها وبنفس الطريقة [١٨].

ثانيا/ الحروب السيبرانية غير التقليدية: تتصف هذا النوع من الحروب على أنها حروب غير تقليدية وتتضمن شن هجمات متوسطة الشدة بدل من الحرب العسكرية المتبادلة كما وتتضمن شن هجمات وحروب نفسية ضد العدو وتستمد هكذا نوع من الحروب شدتها من قوة الأطراف المشاركة فيها وأنها تتصف بانها أقل تكلفة من الحروب التقليدية التي تستخدم الأسلحة والدبابات العسكرية، وقد تم استخدام مثل هكذا حروب عام ١٩٩٩ والتي وقعت بين حلف الناتو ويوغسلافيا وكان هدفها تعطيل وسائل الاتصال كما هو الحال بين روسيا وجورجيا عام ٢٠٠٨.

ثالثاً/ الحروب السيبرانية الاكثر شدة: وتعد هذه الحروب من أخطر أنواع الحروب كونها تستخدم القوة الصلبة والأعمال العسكرية التقليدية، وإلى الآن لم يشهد العالم مثل هذه الحروب ولاكن في حال حدوثها خصوصاً في ضل التطور التكنولوجي وتطور القدرات العسكرية ستؤدي الى اضرار كبيرة في العالم، حيث تعتمد هذه الحروب على الفضاء السيبراني اضافة الى توظيف كافة الأدوات السيبرانية في الحرب مستقبلاً والتي ستقدم في حروبها الطائرات من دون طيار " طائرات مسيرة" بعيدة المدى، وتعد هذه الوسائل في الحروب السيبرانية وهذا ما سيودي الى تحقيق ما يسمى "بالهيمنة السيبرانية الواسعة"[١٩].

المطلب الثاني: التهديدات السيبرانية التي تواجه روسيا الاتحادية

المحور الاول: الاستراتيجية السيبرانية الروسية (الاهمية والاهداف)

أن استراتيجية الأمن السيبراني الجديدة أصبحت موضع اهتمام من قبل الدول الكبرى (روسيا الاتحادية، الولايات المتحدة الامريكية)، خصوصاً وأنها بمثابة تهديد للعديد من المبادئ اهمها الحرية وتعزيز الديمقراطية وبناء السلام وذلك من خلال استخدام القوة السيبرانية من جهة وتعزيز قوة الدولة وتوفير الحماية لنظم المعلوماتية والاستخباراتية من جهة اخرى، والتي يمكن وصفها بأنها احد الاهداف الرئيسية للاستراتيجية الدول الكبرى، وتعتمد هذه الرؤيا على ما تقدمه الدول من دعم وعلى كافة المستويات فضلاً عن توفير الامكانيات والمقومات التي تعزز من قوتها السيبرانية ازاء التهديدات الخارجية، لذلك فقد ابدت الحكومية الروسية اهتماماً واضحاً بمفهوم الفضاء السيبراني وذلك لحماية مؤسساتها وانظمتها الالكترونية مما قد تتعرض له من تهديدات وهجمات سيبرانية، ووفقاً لذلك فقد اتصفت استراتيجية روسيا الاتحادية المرتبطة بأمنها السيبراني بقدر عال من السرية على جميع انشطتها السيبرانية بشكل يعيق اعطاء رؤية واضحة لاستراتيجيتها السيبرانية في مواجهة التهديدات والتحديات المرتبطة بالأمن السيبراني [٢٠].

كما ان المنظور الروسي لمفهوم الامن السيبراني والتهديدات السيبرانية يختلف بشكل واضح عن النظريات الغربية، حيث ان ذلك يبدوا واضحاً في تفسير مفهوم الامن السيبراني الروسي، أذ يشير الى كيفية استخدام كافة القدرات والإمكانيات لتحقيق الاهداف القومية لروسيا الاتحادية، فصانع القرار الروسي يؤكد على ان روسيا تخوض عملية صراع مستمر ومتطور مع فواعل داخلية وخارجية لغرض حماية أمنها السيبراني، اضافة الى اغتنام الفرص من تدفق المعلومات، حيث بإمكانها توظيفها في خدمة اهدافها

القومية الى حد سواء، كما وانها ترى الحروب السيبرانية احد اهم الحروب في صنع السياسات وتحقيق المصالح والاهداف المنشودة، والتي تمثل مفهوم شامل وواسع يتضمن شبكة الحاسوب والحروب الالكترونية والعمليات النفسية والعمليات الاستخباراتية، حيث يرى الرئيس الروسي "فلاديمير بوتين" "ان الصراع داخل مجال المعلومات مستمراً ولا يقتصر عند حد معين"، لذلك فأن استراتيجية روسيا السيبرانية تتصف بطبيعتها الهجومية والاستباقية وبالتالي فهي تختلف عن الاستراتيجية السيبرانية في الولايات المتحدة الامريكية وكذلك الدول الاوروبية(٢١).

كما وقد أكد الرئيس الروسي "فلاديمر بوتين" بأن استراتيجية روسيا تقوم على عدة اوليات اهمها (٢٢):

١. اعادة تسليح روسيا لمواجهة سياسة الولايات المتحدة الامريكية وحلف شمال الاطلسي (الناتو) في مجال الدفاع الصاروخي وهذا ما يتطلب من روسيا تعزيز قدراتها ومقوماتها الامنية والعسكرية للردع الاستراتيجي.

٢. تعزيز امنها السيبراني في مواجهة التهديدات الخارجية.

لذلك فأن الاستراتيجية الروسية تسعى الى بناء معايير دولية وذلك من خلال التعاون في مجال الامن السيبراني اضافة الى تعزيز قدراتها في مواجه التحديات والتهديدات الداخلية والمختصة بأمن المعلومات من جهة ومواجهة التهديدات الخارجية (الحروب السيبراني) من جهة اخرى، وعليه فأن من اهم سمات الامن السيبراني الروسي هو تحقيق مفهوم (السيادة القومي) على الفضاء السيبراني cyber.sovereighty، لذلك فأن السيادة السيبرانية لا يمكن تحقيقها ما لم تتوفر فيها سمات اساسية، وكذلك تبنى وفق مرتكزات مرتبطة باستراتيجية الامن السيبراني الروسي، وهي تعد احد اهم العوامل المؤثرة في التوجهات الاستراتيجية الروسية، وكذلك احد اهم المعوقات بالنسبة للمعايير الدولية المرتبطة بالأمن السيبراني.

كما وان هنالك عدة سمات للاستراتيجية الروسية تتمثل بما يلي (٢٣):

١. **الواقعية:** حيث تتصف استراتيجية الروسية بالواقعية وذلك من خلال سعي القيادة الروسية في بناء سياسة برغماتية مستندة على اسس ايديولوجية فضلاً عن تطلعات روسيا المستقبلية من خلال تعزيز امكانياتها وعلى كافة المستويات (السياسية، العسكرية، الاقتصادية، الامنية، المعلوماتية).

٢. **الديناميكية:** وذلك من خلال التطور التكنولوجي والذي أحدث قفزات تنموية في سياسة روسيا الخارجية، حيث اتبعت روسيا سياسة العولمة وحرية السوق وفي الوقت نفسه استطاعت من المحافظة على وحدة روسيا الداخلية وعدم التفريط بها وذلك من خلال اتباعها العديد من الوسائل واهمها القوة العسكرية.

٣. **المنافسة:** وهي أحد اهداف الاستراتيجية الروسية والتي تتضمن اعادة ترتيب اولويات سياستها الخارجية والذي انعكس في خطط الاصلاح التنموية وحركة الانفتاح المالي والاقتصادي الخارجي.

٤. **الهيمنة:** تسعى روسيا الى اعادة هيكلة النظام الدولي حيث لم يقتصر على الولايات المتحدة فحسب او نظام القطبية بل تسعى الى جعل النظام الدولي متعدد الاقطاب، وتكون فيها أحد الاقطاب المؤثرة في هذا النظام لتحقيق مصالحها واهدافها الاستراتيجية (٢٤).

اما بالنسبة للأهداف الاستراتيجية الروسية فتتمثل بما يلي [٢٥]:

١) ابراز مكانة روسيا الجيو سياسة ومحاولاتها لتحجيم الدور الامريكي في المنطقة، فهي تسعى الى اتباع خطة استراتيجية واقعية وعقلانية تسعى من خلالها الى احلال التعددية القطبية في النظام الدولي على النحو الذي يتوافق مع مصالحها واهدافها في المنطقة.

٢) اقامة علاقات استراتيجية وطيدة وكذلك تفعيل التعاون المشترك بين كل من روسيا وإيران والصين والهند.

٣) تعزيز النفوذ الروسي في المنطقة.

٤) الواقعية في التفكير الاستراتيجي وتعزيز التعاون المشترك مع الدول (اقليمية ودولية).

٥) التطور التكنولوجي وتوظيفه في مجالها العسكري والامني (الفضاء السيبراني).

٦) تقوية منظمة الامن والتعاون الأوروبي (osce) لتتمكن من ممارسة دوراً اساسياً في الوقت الذي تسعى فيه دول حلف الناتو للتوسع وبسط النفوذ.

٧) ابراز المكانة الروسية كقوة اوراسية، اضافة الى الوقوف بوجه التوسع الاوروبي (حلف الناتو) وما يشكله من تهديداً لروسيا ومصالحها الاستراتيجية.

المحور الثاني: التهديدات السيبرانية التي تواجه روسيا الاتحادية.

في ضوء التطور التكنولوجي والمعلوماتي وتنامي دور الفاعلين من جيوش الكترونية وفواعل دولية في مجال الأمن السيبراني زادت التهديدات السيبرانية ولم تعد تقتصر على اختراق البيانات والمعلومات أنما امتدت لتشمل المنشآت العسكرية وكذلك البنى التحتية كالمفاعلات النووية وهذا ما أثر على الأمن القومي للدول من بينها روسيا، كون هذه التهديدات تشكل تهديداً و تحدياً اقليمياً ودولياً يمس بالأمن القومي للدول، اذ أن هذا التطور الحاصل أتاح للفواعل من الدول زيادة قدراتها الأمنية حيث أصبح بإمكانها شراء الأسلحة والمتفجرات عبر شبكات الأنترنيت، أضافة الى قدراتها على طباعة الأسلحة وتحميلها على الطائرات من دون طيار وتوجيهها عبر الهواتف الذكية للمواقع معينة، بالتالي فأنها تشكل تهديداً واضحاً لأمن الفرد والمجتمع وهذا يعد أحد التحديات التي تواجه الدول، نتيجة ما تمتلك هذه الفواعل من أمكانية عالية من المناورة فضلاً عن امتلاكها ادوات سيبرانية ومعلوماتية تمس بأمن الدول و المجتمع[٢٦].

لذا فان العقيدة الروسية التي أقرها الرئيس الروسي "فلاديمير بوتين" والتي نصت على أمكانية أعادة النظر في أحكام العقيدة العسكرية بالتغير والتعديل بما يتناسب مع حجم التهديدات التي تواجه روسيا الاتحادية، ووفقاً لذلك فأن العقيدة العسكرية الروسية تعتمد وبشكل رئيسي على تطور قدراتها السيبرانية في مواجهة التحديات والتهديدات التي تواجه أمن روسيا القومي، وهذا ما عملت به مؤخراً في حربها مع أوكرانيا، أذ اعتمدت وبالدرجة الأساس على قدراتها السيبرانية في الرد على أي مجرم أوكراني محتمل[٢٧].

كما وأن عقيدة روسيا العسكرية والتي أقرها الرئيس الروسي بوتين تتضمن فقرة تخص التهديدات السيبرانية وعلى المستويين العسكري والاقتصادي والتي تمس القيم الأخلاقية التقليدية الروسية، ووفقا لهذه العقيدة المتعلقة بأمن المعلومات والتي مضى عليها الرئيس الروسي عام ٢٠١٤، فأن أحد اهم التهديدات

التي تمس روسيا تتمثل في زيادة عدد الدول الغربية والتي لديها القدرة على التأثير للبنى التحتية الروسية والمتمثلة بـ(الولايات المتحدة الأمريكية، حلف الناتو)، كما ونصت هذه العقيدة والتي تعد بمثابة وثيقة وقعت من قبل مجلس الأمن الروسي على وجود قيود على الخدمات التي تخص وسائل الأعلام التي تستخدمها الدول الأخرى بهدف زعزعة الأمن والاستقرار في الداخل الروسي، كما ونصت على عدة أهداف اهمها الردع الاستراتيجي وحماية أمن المعلومات من التهديدات السيبرانية [٢٨].

ومن خلال ذلك تمكنت روسيا من ادارة تفاعلاتها الدولية وفقا لما تمتلكه من قدرات سيبرانية استطاعت من خلالها تحقيق أهدافها ومصالحها في المنطقة، كما وتعد روسيا أن التهديدات السيبرانية الداخلية والتي تمس الداخل الروسي هي اكثر خطورة من التهديدات السيبرانية الخارجية كونها تؤثر على الرأي العام وتهدد أمن واستقرار روسيا داخليا وهذا ما يشكل خطراً واضحا لاستهداف أمنها القومي، ومما لاشك فيه فان عقيدة روسيا العسكرية استطاعت من التصدي للتهديدات السيبرانية وأهمها أوكرانيا والولايات المتحدة الأمريكية، وذلك من خلال القوة السيبرانية التي تمتلكها والتي بإمكانها توظيفها في حروبها السيبرانية اضافة الى تعزيز مكانتها ونفوذها في النظام الدولي فضلاً عن تحقيق مصالحها وأهدافها الاستراتيجية[٢٩].

وعليه فأن روسيا الاتحادية استطاعت من شن هجمات سيبرانية خصوصاً بعد التهديدات التي تعرضت لها روسيا والتي اتهمت فيها روسيا الولايات المتحدة الامريكية بأنها من المحتمل ان تكون وراء الهجمات السيبرانية التي استهدفت الشبكات الكهربائية، وهذا ما اكده المتحدث باسم الرئاسة الروسية الكريملين (ديميتري بيكون) قائلاً " أن التقارير تبين أن الولايات المتحدة الامريكية وراء التهديدات السيبرانية، وأن هنالك جنود امريكيون الكترونيون وراء اختراق شبكات المعلومات وكذلك البيانات التي تمس امن الدولة، مؤكداً أن الولايات المتحدة الامريكية هي من استهدفت محطات الطاقة الروسية ايضاً"[٣٠].

في المقابل فان روسيا تمتلك قيادة مستقلة للأمن السيبراني منذ عام ٢٠١٠ والتي أكدت أن الحرب السيبرانية لعبت دوراً مهماً في النزاعات المسلحة وغير المسلحة، كما وان الانفاق المالي في مجال الأمن السيبراني بدأ بالازدياد منذ عام ٢٠١٧ ولغاية عام ٢٠٢٣ اذ وصل معدل الانفاق العالمي ما يقارب ١٠٠ مليار دولار امريكي في عام ٢٠١٧ وما يقارب ٢٠٠ مليار دولار لغاية عام ٢٠٢٣، ومن المتوقع أن يصل الاتفاق على البنى التحتية والخدمات الامنية الى ما يقارب ٩٠ مليار دولار امريكي بحلول عام ٢٠٢٤، اضافة لنمو سوق امن المعلومات بحلول عام ٢٠٣٠ يقابله معدل انفاق ضخم وكبير يصل الى ثلاث اضعاف عما كان عليه في عام ٢٠١٧، وهذا ما دفع بروسيا الى تخصيص ميزانية لتمويل أمنها السيبراني للوقوف بوجه أي تهديدات داخلية كانت ام خارجية [٣١]

أضافة لذلك فأن الحرب الروسية–الاوكرانية تمثل أحد أهم التهديدات السيبراني التي واجهت روسيا الاتحادية، كون الحكومة الاوكرانية تمكنت من اختراق عدة منشأت عسكرية تابعة للجيش الروسي وذلك من خلال الدعم المقدم لها من قبل حلف الناتو، ولكن سرعان ما تمكنت روسيا من مواجهة هذه

التهديدات والخروقات، حيث أن النشاط السيبراني لروسيا يهدف الى الضغط على الدول الغربية وبما فيها حلف الناتو، اضافة الى زيادة التوتر بين دول الاعضاء، لذلك فأن الهجمات السيبرانية الروسية ممكنة، نتيجة ما تمتلكه من مقومات القوة السيبرانية وهي نفس الوقت فأن أي هجوم محتمل من قبل روسيا سيزيد من حدة الصراعات وهذا ما سيفتح المجال أمام روسيا لرد بهجوم سيبراني محتمل[٣٢].

المطلب الثالث: استراتيجية روسيا الاتحادية في مواجهة التحديات السيبرانية

المحور الاول: سبل توظيف الاستراتيجية الروسية في مواجهة التحديات

تعد روسيا احد اهم الدول التي تمكنت من توظيف الامن السيبراني في مواجهة التهديدات السيبرانية منذ عام ٢٠٠٠ وبعد تولي بوتين السلطة في روسيا، حيث عملت روسيا على تطوير استراتيجية أمنية مبنية على مجموعة من الاسس والاعتراف بالدور الذي يلعبه الأمن السيبراني في تحقيق مصالح روسيا القومية وتعزيز أمنها واستقرارها في المنطقة وعلى الصعيدين الأمني والسياسي، اذ تعد روسيا من أوائل الدول التي سعت الى عقد العديد من الاتفاقيات الدولية والتي تهدف الى الحد من المخاطر السيبرانية والحيلولة من حدوث سباق لتسلح السيبراني نتيجة التطور التكنولوجي والذي دفع بالدول بالتنافس في مجال التسلح، ففي عام ٢٠١١ قدمت روسيا مشروعاً دوليا، مختصاً بالأمن السيبراني الا ان هذا المشروع حمل في طياته العديد من المعايير والاهداف التي تتعارض مع رؤى واهداف الرؤيا الدول الغربية للأمن السيبراني، ومن بين اهم نقاط الخلاف حيث ان روسيا كالصين في ضمان سيادة الدولة في مجال الفضاء السيبراني، وهذا ما يتعارض مع رؤى الدول الغربية التي تؤمن بالحرية في تداول المعلومات والبيانات عبر برامج الانترنيت على العكس من روسيا كونها اكثر تعقيداً في اتاحة المعلومات [٣٣].

وفي نطاق ذلك عملت روسيا على انشاء (وكالة ابحاث الانترنيت) او ما تعرف باسم جيش المتصدين "Army-trall" والتابع لوكالة امن الاتحاد الروسي، حيث يضم الالاف المتطوعين ويخصص لهم سنوياً (٣٠٠) مليون دولار من حجم الانفاق العسكري الروسي، كما يحتل الجيش السيبراني الروسي خامس اقوى جيوش العالم في التقارير العالمية المختصة بالفضاء السيبراني بعد كل من الولايات المتحدة الامريكية والصين وبريطانيا وكوريا الشمالية [٣٤].

ويمكن تحديد مهام هذا الجيش على النحو الاتي:

١. القيام بالعديد من عمليات التجسس ضد الخصم

٢. شن الهجمات السيبرانية والتي تهدف الى اضعاف البنى التحتية للخصم والاضرار بالجانب الاقتصادي والسياسي.

٣. القيام بشن الحروب السيبرانية وذلك عن طريق اختراق الحسابات والمعلومات الالكترونية وانشاء حسابات وهمية غرضها الأضرار بالبرامج الالكترونية وكذلك مواقع التواصل الاجتماعي (فيس بوك، تويتر، وغيرها).

وهذا ما عملت به روسيا في هجماتها السيبرانية مع كل من اوكرانيا وجورجيا، حيث ان روسيا تقدم الحروب السيبرانية كسلاح في عملياتها العسكرية التقليدية، اذ اتاحت تجربتها مع كل من جورجيا واوكرانيا فرصاً لتطوير تقنياتها في مجال التسليح السيبراني وكذلك عمليات الارهاب السيبراني، حيث شكلت لها هذه القدرات قوة ردع مهمة وشاملة ضد خصوم روسيا [٣٥].

كما أن هنالك العديد من الهجمات السيبرانية الروسية – الاوكرانية ففي عام ٢٠١٤ تمكن الجيش السيبراني الروسي من الوصول الى عدد الاصوات في اوكرانيا في انتخاباتها مما ادى الى تدمير السجلات الالكترونية من قبل الجانب الروسي وهذا ما دفع بالحكومة الاوكرانية الى فرز الاصوات يدوياً، وفي عام ٢٠١٥ قامت السلطات الروسية بشن هجوم سيبراني في اوكرانيا اسفر عن قطع التيار الكهربائي لعدة ساعات غرب اوكرانيا، وفي عام ٢٠١٧ شنت الاستخبارات الروسية هجوماً سيبرانياً ضد اوكرانيا ونجحت في اضرار ما يقارب ١٠ % من انظمة الكمبيوتر الالكترونية، وفي عام ٢٠٢٢ اعلن micro sofit عن وجود برامج ضارة تسمى "whispergate" تهدف المنظمات الحكومية وغير الربحية كذلك مؤسسات تكنلوجيا المعلومات الموجودة في اوكرانيا، اما في اوائل فبراير من عام ٢٠٢٢ فقد كشف مايكروسفت عن استهداف المؤسسات العسكرية الاوكرانية من قبل ما يسمى بـ(اكتينيوم) والمرتبط بأجهزة الامن السيبراني الروسي، حيث بدأ هذا الاستهداف من عام ٢٠٢١ وتم الاعلان عنه في عام ٢٠٢٢ حيث يعمل في مهمتين التجسس وجمع المعلومات الاستخباراتية [٣٦].

ووفقاً لذلك فيمكن تحديد الهجمات السيبرانية الروسية على اوكرانيا على النحو الاتي [٣٧]:

اولاً: عملية هرمجدون والتي شنتها روسيا على اوكرانيا عام ٢٠١٣.

ثانياً: عملية سيناك والتي شنتها القوات السيبرانية الروسية عام ٢٠١٤.

ثالثاً: خرق النظام الانتخابي في اوكرانيا عام ٢٠١٤.

رابعاً: اختراق شبكة الكهرباء في ديسمبر عام ٢٠١٥ والتي استخدمت فيه القوات السيبرانية الروسية فايروس حصان طروادة بلاك إنرجي (black energy).

خامساً: الاختراق الثاني لشبكة الكهرباء في اوكرانيا من قبل القوات السيبرانية الروسية عام ٢٠١٦.

سادساً: الهجمات السيبرانية الروسية على المؤسسات الحكومية الاوكرانية عام ٢٠١٦.

سابعاً: الهجمات السيبرانية الروسية عام ٢٠٢٢ والتي استهدفت مواقع الحكومة الاوكرانية.

ثامناً: الهجمات السيبرانية الروسية عام ٢٠٢٢ والتي استهدفت المؤسسات المعرفية الاوكرانية مستخدماً برنامج (foxplade) اثناء الغزو الروسي للأوكرانية، ومن خلال ما سبق فيمكن القول إن الحروب السيبرانية الروسية قد تمت من خلال ما يعرف بالوكلاء ومنظمات حكومية وغير حكومية، كما أن هنالك العديد من التنظيمات الروسية التي تعمل في مجال الفضاء السيبراني لصالح الحكومة والمخابرات الروسية والمتمثلة بـ [٣٨]:

١. منظمة (fancy bear): حيث قامت هذه المنظمة بشن هجوم سبراني روسي استهدف مواقع ومواطنين امريكيين عام ٢٠١٨، كذلك وقد استهدف قطاع الطاقة الامريكي وموقع (micro soft office) التابع للولايات المتحدة الامريكية.

٢. منظمة (sand worm): وتعد أحد المنظمات التابعة لوكالة المخابرات الروسية (gru)، حيث عملت هذه المنظمة على استهداف البنى التحتية التابعة للدول ومنها أوكرانيا ومن خلال هذه المنظمة تم استهداف قطاع الكهرباء في اوكرانيا عام ٢٠١٥ وعام ٢٠١٦ مما أدى الى انقطاع التيار بشكل تام ويعد من اهم الهجمات السيبرانية الروسية ضد اوكرانيا.

٣. منظمة (callisto grouo): وهي أحد المنظمات التي لها ارتباط مباشر بوكالة المخابرات العسكرية الروسية (gru)، وتعد أحد منظمات الهكرز والمعروفة بأنشطتها الاستخباراتية وتعمل في مجال التجسس السيبراني ومجال القرنصة والتي ظهرت عام ٢٠١٥ وبداية عام ٢٠١٦، حيث استهدفت العديد من الدول واهمها جورجيا واوكرانيا.

٤. منظمة (unc2589): وهي أحد المنظمات التابعة لوكالة المخابرات الروسية حيث تعمل على توجيه ضربات واستهداف شركات ومنظمات تابعة للدول الاوروبية وذلك من خلال ارسال رسائل مشفرة حاملة معها فايروسات تتمكن من خلالها الحصول على المعلومات والبيانات المرتبطة بالدول الاوروبية ومنها دول حلف شمال الاطلسي (حلف الناتو).

٥. منظمة (pushcka): وتعد من اهم المنظمات التابعة لوكالة المخابرات الروسية، حيث انها تعمل على ممارسة الضغط على الشعوب مما يؤدي الى المس بالأمن القومي للدول الخصوم، حيث تم استخدام هذه المنظمة بعد الغزو الروسي على اوكرانيا عام ٢٠٢٢، حيث عملت على التأثير على الرأي العام الاوكراني ومحاولة خلق نوع من زعزعة الأمن والاستقرار بين المواطنين من خلال نشر رسائل مشفرة.

المحور الثاني: سيناريوهات الحرب السيبرانية الروسية

هنالك عدة سيناريوهات توضح لنا التطور المحتمل لنشوب حروب سيبرانية ذات تأثير مباشر على الأمن العالمي:

١. **الحروب السيبرانية المرتبطة بالذكاء الاصطناعي:** فمن الممكن ان يحدث الذكاء الاصطناعي ثورة مهمة ومؤثرة في الحروب السيبرانية، اذ يمكن توظيف الذكاء الاصطناعي في تطوير برامج ذات اضرار كبيرة في أي هجوم سيبراني (٣٩).

٢. **سباق التسلح السيبراني:** فمن الممكن أن يؤدي التطور التكنولوجي والسيبراني سباق تسلح سيبراني وذلك من خلال توظيف كافة القدرات والإمكانيات السيبرانية الهجومية والدفاعية، وهذا سيؤدي الى زعزعة العلاقات الدولية وزيادة الهجمات والحروب السيبرانية بين الدول.

٣. **صراعات جيو سياسية وجيو سيبرانية:** فمن الممكن ان تستخدم الدول الحروب والهجمات السيبرانية كأداة لتحقيق اهدافها ومصالحها الجيو سياسية، وهذا ما سيؤدي الى تزايد النزاعات والصراعات الدولية مما ستؤثر وبشكل مباشر على هيكلية النظام الدولي (٤٠).

٤. **استهداف البنى التحتية:** أن الهجمات السيبرانية التي تستهدف البنى التحتية بإمكانها ان تؤدي الى اضرار كبير فعلى سبيل المثال انقطاع التيار الكهربائي لمدينة جوهانسبرغ، واستهداف اجهزة الطرد المركزي بالمفاعلات النووية الايرانية وتوقف شركة الارمكو النفطية، وهذا ما عملت به روسيا موخراً مع حربها ضد اوكرانيا اذ تمكنت من استهداف البنى التحتية الاوكرانية والمتضمنة قطاع الكهرباء ووزارتي الدفاع والمالية (٤١).

وعليه فأن الدول تستخدم الحروب السيبرانية او التهديد بها كأداة للمحافظة على بقائها، فالحرب السيبرانية هي أحد المحاور المهمة في السياسات الدولية (سياسات القوى) والتي تمكنت روسيا من استخدامها لتحقيق اهدافها ومصالحها اضافة الى المحافظة على أمنها القومي وتعزيز مكانتها الاقليمية والدولية.

الخاتمة:

يعد التطور التكنولوجي احد الادوات المهمة التي اتاحت للدول تحقيق اهدافها والتحرك والتأثير في الهياكل الحيوية الخاصة بالدول، اذ انها تعد احد المقومات المهمة في السياسة الخارجية للدول والتي تمكنت روسيا في توظيفها في أدارة تفاعلاتها الدولية، ونتيجة لذلك حضي الأمن السيبراني الروسي باهتمام كبير من قبل الدول الغربية واهمها الولايات المتحدة الامريكية، اذ تمكنت روسيا من تحقيق مكانة متميزة ومهمة في التمكن من هذه القوة واستخدامها في تحقيق مصالحها واهدافها المنشودة، اذ استطاعت من القيام بالعديد من العمليات السيبرانية واهمها عملية التجسس والتدخل في الشأن الداخلي للدول، فقد اصبحت تكنلوجيا المعلومات ترسم خارطة طريق جديدة للدول في تحقيق السيادة وجذب الداعمين والاقتراب من نقاط صنع القرار وتقوية العلاقات الدولية مع الحلفاء وحماية مصالحها الوطنية من جهة والرد على التهديدات السيبرانية من قبل دول الخصوم من جهة اخرى.

الاستنتاجات: من خلال ما سبق يمكن أن نستنتج ما يلي:

اولاً: ان العديد من الدول ومنها روسيا تمكنت من انشاء جيوش رقمية استطاعت من خلالها تغيير قواعد الحرب في المستقبل والتحول من الحروب التقليدية الى الحروب السيبرانية الالكترونية.

ثانياً: نجحت روسيا في بناء استراتيجية سيبرانية لمواجهة التهديدات والحروب السيبرانية سواء كانت داخلية او خارجية او متداخلة بين الداخل والخارج.

ثالثًا: تمكنت روسيا من انشاء حكومة الكترونية لمواجهة التهديدات السيبرانية.

رابعاً: أدركت الاجهزة الروسية المختصة في مكافحة التهديدات السيبرانية ان يتوجب عليها تأمين المعلومات والبيانات من خلال انشطة حماية مرتبطة بالتطور التكنولوجي والمعلوماتي.

خامساً: أن مفهوم الأمن السيبراني من اهم المفاهيم التي طرأت على الساحة الدولية، حيث أن الأمن السيبراني أصبح أحد المحاور المؤثرة في رسم سياسات الدول وكذلك أحد محاور العلاقات الدولية.

سادساً: أن مقومات روسيا الجيو سيبرانية والجيوسياسية من اهم المقومات التي تمكنت روسيا من توظيفها في حروبها السيبرانية تجاه دول الخصوم.

الهوامش:

(١) أسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، المجلد ١٠، العدد ١، ٢٠١٩، ص ٦-٧.

(٢) مقال بعنوان قضايا وتحديات الامن السيبراني، خدمة ابحاث الكونجرس، ٢٠١٦، متاح على الرابط ادناه: https://crsreports.congress-gov

(٣) ساعد بوقرص، الامن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة، مجلة الابحاث في الحماية الاجتماعية، جامعة العلوم والتكنولوجيا – هوادي بومدين، العدد ١، ٢٠٢٢، ص ٦٦.

(٤) هبة جمال الدين، الامن السيبراني والتحول في النظام المالي، دراسات، معهد التخطيط القومي، العدد ١، المجلد ٢٤، ٢٠٢٣، ص ٩٠.

(٥) رياض حمدوش، الدولة بين الهيمنة وتحقيق الامن في الفضاء السيبراني، المجلة الجزائرية للأمن الإنساني، العدد ١، المجلد ٧، ٢٠٢٢، ص ١٣٣-ص١٣٤.

(٦) ساعد بوقرص، مصدر سابق، ص٦٤.

(٧) شوريب جيلاني، مفهوم الحروب السيبرانية والامن السيبراني، مجلة الحقوق والحريات، جامعة ثلجي الاغوط، كلية الحقوق والعلوم السياسية، المجلد ١١، العدد١، ص١٦٠.

(٨) نسيب نجيب، الحرب السيبرانية من منظور القانون الدولي الانساني، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، العدد ٤، المجلد ١٩، ٢٠٢١، ص٢٢٢.

(٩) نسيب نجيب، مصدر سبق ذكره، ص ٢٢٣.

(١٠) علي عبد الرحيم، هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، المجلة الاكاديمية العلمية، كلية العلوم السياسية، المجلد ٧، العدد ٣، ٢٠٠٩، ص٩٦.

(١١) عبد الستار شاكر سلمان، جرائم الامن السيبراني وأثر الجهود الدولية في مكافحتها، دار هاتريك للنشر والتوزيع، الطبعة الاولى، العراق، اربيل، ٢٠٢٣، ص٣٥.

(١٢) شويرب جيلاني، مصدر سابق، ص١٦٣.

(١٣) عبد الستار شاكر، مصدر سبق ذكره، ص٦٣.

(١٤) محمود علي عبد الرحمن، اسامة فاروق، الفضاء الالكتروني وأثره على مفاهيم القوة والامن والصراع في العلاقات الدولية، مجلة كلية السياسة والاقتصاد، جامعة محمد البشير الابراهيمي، المجلد ١٦، العدد ١٥، الجزائر، ٢٠٠٢، ص ٤٣٨.

(١٥) شوريب جيلاني، مصدر سابق، ص١٦٧.

(١٦) عادل عبد الصادق، الفضاء الالكتروني والتحول في سياسات اجهزة الاستخبارات الدولية، مركز الاهرام للدراسات الدولية والاستراتيجية، العدد ٢٤٧، القاهرة، ٢٠١٣، ص ١٠-١٢.

(17) Davide Sanger, confrontand Conceal: Obama secret Wasand surprising use of American power (New York: Crownb 2012): 188.

(١٨) مايكل فالوف وزير الدفاع البريطاني، بإمكان بريطانيا شن هجمات الكترونية للدفاع عن نفسها ضد روسيا، موقع تلي غراف، ٢٠١٧، متاح على الرابط الاتي: https://translate.google.com/translate?hl=ar8=en8u=https

(١٩) حازم جري الشمري، توظيف القوة السيبرانية في استراتيجيات الدول الكبرى (الولايات المتحدة الامريكية وروسيا انموذجا)، ط١، دار انكي للنشر والتوزيع، العراق، بغداد، ٢٠٢٢، ص ١٠٦-١٠٧.

(٢٠) أنغام عبد الرضا سلطان العكابي، الدور الدولي في تعزيز الامن السيبراني في ضوء التحديات المعاصرة، المجلة العراقية للعلوم السياسية، العدد ٩، ٢٠٢٣، ص ٢٦٦-٢٦٧.

(٢١) احمد يوسف الجميلي، الشؤون العسكرية والامنية في روسيا، مركز صنع السياسات للدراسات الدولية والامنية، العدد ١، ٢٠١٩، ص ٢.

(٢٢) احمد ذياب، (عودة بوتين: تحديات وطموحات روسيا بعد الانتخابات الرئاسية)، مجلة السياسة الدولية، مركز الدراسات السياسية والاستراتيجية، العدد ١٨٨، ٢٠١٢، ص ١٠٦.

(٢٣) حازم جري الشمري، مصدر سابق، ص ١٨٣.

(٢٤) بعلوج السعيد، رزقي جلال، الاستراتيجية الروسية لمكافحة التهديدات الالكترونية (الامن السيبراني في عهد فلاديمير بوتين للمدة ٢٠٠٦-٢٠١٤)، رسالة ماجستير منشورة، جامعة العربي التبسي، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، الجزائر، ٢٠١٩، ص ٣٠-٣١.

(٢٥) عبد العزيز مهدي، توجهات السياسة الخارجية الروسية في مرحلة ما بعد الحرب الباردة، دراسات دولية، العدد ٣٥، ٢٠٢٢، ص ١٦٥-١٦٦.

(٢٦) أيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الامن القومي، المستقبل للأبحاث والدراسات المتطورة، العربي للنشر والتوزيع، ط١، مصر، ٢٠٢٠، ص ١٨٦.

(٢٧) بعلوج السعيد، مصدر سابق، ص٣٧.

(٢٨) ما الجديد في عقيدة الأمن السيبراني الروسي، مقال منشور على الرابط الالكتروني الاتي:
https://katehon.com/ar/article/m-ljdyd-fy-qyd-lmn-lsybrny-lrwsy

(٢٩) أنغام عبد الرضا سلطان الكعبي، توظيف، الحرب السيبرانية في تطوير مفهوم القوة للدول الكبرى، مجلة قضايا سياسية، العدد ٧٣، ٢٠٢٠، ص ٤٢٥.

(٣٠) روسيا تشك أن الولايات المتحدة سعت لقرصنة شبكتها الكهربائية، مقال منشور على الرابط الاتي:
https://www.bbc.com/arabic/science-and-tech-48686046

(٣١) جودي ملاك، التكنولوجيا الحديثة تحولات القوة في العلاقات الدولية: دراسة تحليلية نظرية، رسالة ماجستير منشورة، جامعة الجزائر، كلية العلوم السياسية والعلاقات الدولية، قسم الدراسات الدولية، ٢٠٢، ص ٩٦-٩٧.

(٣٢) علي حسين حميد، أنغام عادل حبيب، ملامح توظيف الفضاء، مجلة قضايا سياسية، جامعة النهرين، العدد٧٢، ٢٠٢٣، ص ١٦٣.

(٣٣)حازم جري الشمري، مصدر سابق، ص ١٨٥.

(٣٤)

(٣٥) بعلوج السعيد، رزقي جلال، مصدر سابق، ص ٣٥-٣٦.

(٣٦) علي حسين حميد، أنغام عادل حبيب، مصدر سابق، ص ١٦٠.

(٣٧) احمد عثمان محمد، الحرب السيبرانية وأثرها في العلاقات الدولية: روسيا والولايات المتحدة الامريكية انموذجاً، مجلة الجامعة العراقية، العدد ٥٩، المجلد ٢، ٢٠٢٣، ص ٤٦٧.

(٣٨) كيار طه محمد، نجاح عبد الفتاح الريس، هشام محمد بشير، حدود فعالية الحروب في تنفيذ اهداف السياسية الخارجية الروسية: دراسة حالة الحرب السيبرانية، مجلة كلية السياسية والاقتصاد، العدد ٢٣، ٢٠٢٤، ص ٢١٧-٢١٨.

(٣٩) مؤنس حواس، هاكرز بدرجة جنود: الحروب السيبرانية، ٢١ يوليو، ٢٠٢٤، مقال متاح على الرابط الاتي:
https://n9.cl/wg5cq

(٤٠) علي حسين حميد، أنغام عادل حبيب، مصدر سابق، ص١٦٩.

(٤١) الامن الاوروبي: دراسة التغييرات في مفهوم وقضايا الأمن بعد الحرب الباردة، مجلة كلية السياسة والاقتصاد، العدد ١٧، ٢٠٢٣، ص ١١.

المصادر:

١) أسماعيل زروقة، الفاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، المجلد ١٠، العدد ١، ٢٠١٩.

٢) مقال بعنوان قضايا وتحديات الامن السيبراني، خدمة ابحاث الكونجرس، ٢٠١٦، متاح على الرابط ادناه: https://crsreports.congress-gov

٣) ساعد بوقرص، الامن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة، مجلة الابحاث في الحماية الاجتماعية، جامعة العلوم والتكنولوجيا – هوادي بومدين، العدد ١، ٢٠٢٢.

٤) هبة جمال الدين، الامن السيبراني والتحول في النظام المالي، دراسات، معهد التخطيط القومي، العدد١، المجلد ٢٤، ٢٠٢٣.

٥) رياض حمدوش، الدولة بين الهيمنة وتحقيق الامن في الفضاء السيبراني، المجلة الجزائرية للأمن الإنساني، العدد ١، المجلد ٧، ٢٠٢٢.

٦) شوريب جيلاني، مفهوم الحروب السيبرانية والامن السيبراني، مجلة الحقوق والحريات، جامعة ثلجي الاغوط، كلية الحقوق والعلوم السياسية، المجلد ١١، العدد١.

٧) نسيب نجيب، الحرب السيبرانية من منظور القانون الدولي الانساني، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، العدد ٤، المجلد ١٩، ٢٠٢١.

٨) علي عبد الرحيم، هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، المجلة الاكاديمية العلمية، كلية العلوم السياسية، المجلد ٧، العدد ٣، ٢٠٠٩.

٩) عبد الستار شاكر سلمان، جرائم الامن السيبراني وأثر الجهود الدولية في مكافحتها، دار هاتريك للنشر والتوزيع، الطبعة الاولى، العراق، اربيل، ٢٠٢٣.

١٠) محمود علي عبد الرحمن، اسامة فاروق، الفضاء الالكتروني وأثره على مفاهيم القوة والامن والصراع في العلاقات الدولية، مجلة كلية السياسة والاقتصاد، جامعة محمد البشير الابراهيمي، المجلد ١٦، العدد ١٥، الجزائر، ٢٠٠٢.

١١) عادل عبد الصادق، الفضاء الالكتروني والتحول في سياسات اجهزة الاستخبارات الدولية، مركز الاهرام للدراسات الدولية والاستراتيجية، العدد ٢٤٧، القاهرة، ٢٠١٣.

12) Davide Sanger, confrontand Conceal: Obama secret Wasand surprising use of American power (New York: Crownb 2012).

١٣) مايكل فالوف وزير الدفاع البريطاني، بإمكان بريطانيا شن هجمات الكترونية للدفاع عن نفسها ضد روسيا، موقع تلي غراف، ٢٠١٧، متاح على الرابط الاتي:
https://translate.google.com/translate?hl=ar8=en8u=https
١٤) حازم جري الشمري، توظيف القوة السيبرانية في استراتيجيات الدول الكبرى (الولايات المتحدة الامريكية وروسيا انموذجا)، ط١، دار انكي للنشر والتوزيع، العراق، بغداد، ٢٠٢٢.
١٥) أنغام عبد الرضا سلطان العكابي، الدور الدولي في تعزيز الامن السيبراني في وء التحديات المعاصرة، المجلة العراقية للعلوم السياسية، العدد ٩، ٢٠٢٣.
١٦) احمد يوسف الجميلي، الشؤون العسكرية والامنية في روسيا، مركز صنع السياسات للدراسات الدولية والامنية، العدد ١، ٢٠١٩.
١٧) احمد ذياب، (عودة بوتين: تحديات وطموحات روسيا بعد الانتخابات الرئاسية)، مجلة السياسة الدولية، مركز الدراسات السياسية والاستراتيجية، العدد ١٨٨، ٢٠١٢.
١٨) بعلوج السعيد، رزقي جلال، الاستراتيجية الروسية لمكافحة التهديدات الالكترونية (الامن السيبراني في عهد فلاديمير بوتين للمدة ٢٠٠٦-٢٠١٤)، رسالة ماجستير منشورة، جامعة العربي التبسي، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، الجزائر، ٢٠١٩.
١٩) عبد العزيز مهدي، توجهات السياسة الخارجية الروسية في مرحلة ما بعد الحرب الباردة، دراسات دولية، العدد ٣٥، ٢٠٢٢.
٢٠) أيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الصورة الصناعية الرابعة على الامن القومي، المستقبل للأبحاث والدراسات المتطورة، العربي للنشر والتوزيع، ط١، مصر، ٢٠٢٠.
٢١) ما الجديد في عقيدة الأمن السيبراني الروسي، مقال منشور على الرابط الالكتروني الاتي:
https://katehon.com/ar/article/m-ljdyd-fy-qyd-lmn-lsybrny-lrwsy
٢٢) أنغام عبد الرضا سلطان الكعبي، توظيف، الحرب السيبرانية في تطوير مفهوم القوة للدول الكبرى، مجلة قضايا سياسية، العدد ٧٣، ٢٠٢٠.
٢٣) روسيا تشك أن الولايات المتحدة سعت لقرصنة شبكتها الكهربائية، مقال منشور على الرابط الاتي:
https://www.bbc.com/arabic/science-and-tech-48686046
٢٤) جودي ملاك، التكنولوجيا الحديثة تحولات القوة في العلاقات الدولية: دراسة تحليلية نظرية، رسالة ماجستير منشورة، جامعة الجزائر، كلية العلوم السياسية ولعلاقات الدولية، قسم الدراسات الدولية، ٢٠٢، ص ٩٦-٩٧.
٢٥) علي حسين حميد، أنغام عادل حبيب، ملامح توظيف الفضاء، مجلة قضايا سياسية، جامعة النهرين، العدد ٧٢، ٢٠٢٣.
٢٦) احمد عثمان محمد، الحرب السيبرانية وأثرها في العلاقات الدولية: روسيا والولايات المتحدة الامريكية انموذجاً، مجلة الجامعة العراقية، العدد ٥٩، المجلد ٢، ٢٠٢٣.

٢٧) كيار طه محمد، نجاح عبد الفتاح الريس، هشام محمد بشير، حدود فعالية الحروب في تنفيذ اهداف السياسية الخارجية الروسية: دراسة حالة الحرب السيبرانية، مجلة كلية السياسية والاقتصاد، العدد٢٣، ٢٠٢٤.

٢٨) مؤنس حواس، هاكرز بدرجة جنود: الحروب السيبرانية، ٢١ يوليو، ٢٠٢٤، مقال متاح على الرابط الاتي: https://n9.cl/wg5cq

٢٩) الامن الاوروبي: دراسة التغييرات في مفهوم وقضايا الأمن بعد الحرب الباردة، مجلة كلية السياسة والاقتصاد، العدد ١٧، ٢٠٢٣.