أثر الأمن السيبراني في التدابير الخارجية لروسيا الاتحادية بعد العام ٢٠٠٠

أ.د إسراء شريف جيجان الكعود

جامعة بغداد / كلية العلوم السياسية / قسم الدراسات الدولية

dr.israashareef68@gmail.com

https://doi.org/10.61884/hjs.v14i57.694

ملخص :

شهد العالم منذ أحداث ١١أيلول٢٠٠١ سباقاً محموماً بين القوى الكبرى والإقليمية ولاستغلال الفضاء السيبراني والإفادة من المزايا التي يوفرها في تحقيق مكاسب إستراتيجية حيوية وأصبحت قضية الأمن السيبراني واحدة من أهم وأعقد القضايا التي تهم هذه القوى المتقدمة على الصعيد التكنولوجي ومنها روسيا الاتحادية التي عملت على تنمية قدراتها السيبرانية وتطويرها بشكل كبير وسخرت تلك القدرات كسلاح فعال لإيقاع الضرر في قدرات خصومها، بالشكل الذي جعل من تلك القدرات السيبرانية أحد عناصر الردع الإستراتيجي لروسيا وتمثل الأهداف القومية الروسية في أمنها القومي مزيجاً من الأهداف المتوازنة للفرد والمجتمع والدولة وعلى كافة الأصعدة.

الكلمات المفتاحية: الأمن السيبراني، التدابير الخارجية، روسيا الاتحادية.

The Impact of Cybersecurity on the Foreign Policy MeasuresOf the Russian Federation after 2000

A Research Paper Submitted by

Prof. Dr. Israa Sharif Jijaan Al-Kaoud

Department of International Studies, College of Political Science, University of Baghdad

dr.israashareef68@gmail.com

ABSTRACT:

Since the events of September 11-2001 the world has witnessed an intense competition among major and regional powers to exploit cyberspace and capitalize on the strategic advantages it offers in achieving vital national interests. Cybersecurity has emerged as one of the most significant and complex issues confronting technologically advanced states, including the Russian Federation. Russia has devoted considerable effort to developing and expanding its cyber capabilities, employing them as an effective instrument to inflict damage on the capabilities of its adversaries. As a result, cyber capabilities have become a central component of Russia's strategic deterrence posture. Russian national objectives in the realm of national security reflect a balanced integration of individual, societal, and state-level interests across multiple dimensions. Within this context, the present study examines the conceptual framework of cybersecurity and related concepts, before followed by an analysis of cybersecuritys impact on the Russian Federation foreign policy and strategic measures

KEYWORDS: cyber security, external measures, Russian federation.

المقدمة:

يعد موضوع الأمن السيبراني من الموضوعات المهمة التي تثير جدلاً واسعاً في العلاقات الدولية وهو أحد العناصر المؤثرة في السياسة والاقتصاد على الصعيد الدولي بسبب تحول الصراعات بين القوى الفاعلة إلى أدوات ووسائل جديدة انتجتها التطورات التقنية والعلمية المتمثلة بالشبكة العنكبوتية والوسيط الرقمي أو الفضاء السيبراني.

وقد أصبح الأمن السيبراني في ظل الثورة التكنولوجية والمعلوماتية مجالاً واسعاً للتنافس والصراع بين الدول الكبرى وظهر لأول مرة مفهوم الحروب السيبرانية التي تقع ضمن خانة حروب المستقبل فتداعياتها أخطر من الحروب التقليدية من حيث التهديد وحجم الدمار.

في ضوء هذه المعطيات جاء البحث بالعنوان الذي أشرنا إليه لحيويته وأهميته ودخوله كعامل مهم وجديد في العلاقات الدولية ودور روسيا الاتحادية كقوة فاعلة تحاول وأن تحمي أمنها القومي وتستعيد قوتها كما كانت في ظل الثنائية القطبية (Bipolarity) ومحاولة إيقاف فرص التفرد الأمريكي في العالم.

إشكالية البحث:

ينطلق البحث من إشكالية متمثلة بسؤال مركزي:

ما هو أثر الأمن السيبراني في التدابير الخارجية لروسيا الاتحادية بعد العام ٢٠٠٠؟

يتشظى من هذا السؤال عدة تساؤلات فرعية:

ما هو مفهوم الأمن السيبراني؟

ما هي المفاهيم المقاربة له؟

ما هو تأثير متغير الأمن السيبراني في التدابير الخارجية لروسيا الاتحادية؟

فرضية البحث:

ينطلق البحث من الفرضية التي تعد مخرج للإشكالية وهي: أن الأمن السيبراني يعد متغيراً فاعلاً ومؤثراً في التدابير لروسيا الاتحادية وخاصة بعد عام ٢٠٠٠ بعد الوصول لرئاسة روسيا والتحولات الكبيرة التي حدثت ومنها التدابير الخارجية في مجال الأمن السيبراني والتي تعد عنصراً أساسياً في الإستراتيجية العسكرية الروسية وقد نجحت روسيا في الحفاظ على أمنها القومي من خلال تطوير إمكانياتها الأمنية في ميدان الفضاء السيبراني.

المبحث الأول:

الأمن السيبراني والتدابير الخارجية (إطار مفاهيمي)

النشأة والظهور

أثار مفهوم الأمن السيبراني جدلاً واسعاً أمام المعنين بالدراسات الدولية ومثل تحدياً صريحاً في فهم طبيعته وقضاياه بخلاف طرح المقاربات التفسيرية لكيفية نشوئه، إذ انتشرت العديد من المفاهيم المعاصرة وثيقة الصلة بالثورة التقنية والاتصالات بشكل خاص بعد انتشار الهجمات الالكترونية وحوادث القرصنة التي أصبحت تمثل جيلاً جديداً من وسائل الحروب والتهديد على الصعيد الدولي[١].

ظهر الأمن السيبراني مع نهاية الحرب الباردة (Cold war) وظهور مصطلح حرب الانترنت أو الحرب السيبرانية التي برزت مع بداية اعتماد الدول على أجهزة الكومبيوتر في مؤسساتها وتطوير وحدة المعالجة المركزية في هذه الأجهزة.

اقتصر دور الأمن السيبراني في المدة الأولى على الحماية من الفيروسات والبرمجيات الخبيثة.

وظهر أول فيروس رقمي في سبعينيات القرن الماضي وذلك على شبكة (أربانت) إحدى أوائل الشبكات في العالم لنقل البيانات باستخدام تقنية تبديل الرزم وكان على شكل رسالة نصية بسيطة لم تحدث أضراراً تقنية لكنها دفعت إلى اتخاذ تدابير وقائية[٢]. في مطلع الثمانينات من القرن الماضي وتحديداً عام (١٩٨٣) طور معهد (ماساتشوستس) للتقنية نظام اتصالات يعتمد على التشفير أصبح أساساً لتطوير تقنيات الأمن السيبراني الحديثة، وشكل ظهور الإنترنت ثورة جديدة شكلت طفرة نوعية عندما تم استخدامه في المجالات المهمة كالمجال العسكري والمجال الأمني وتسابقت الدول في تطويره مع مطلع عقد التسعينات وظهرت الحاجة إلى وجود قوة جديدة غير مادية جنباً إلى جنب مع القوة العسكرية والاقتصادية وبدأت الدول تولي اهتماماً ملحوظاً بالقوة السيبرانية لتأثيرها في المضمارين المحلي والدولي[٣].

ومع بروز الثورة المعلوماتية ودخول العصر الرقمي واعتبار عدد من الباحثين الفضاء

---

(١) علي زياد العلي، الصراع والأمن الجيوسيبراني في السياسة الدولية، ط١، (دار أمجد للنشر والتوزيع، عمان – الأردن، ٢٠١٩)، ص٥٣.

(٢) الأمن السيبراني: https : // political.www – encyclopedia.org.

(٣) الأمن السيبراني مفهومه وتاريخه Net.Aljazeera تاريخ الزيارة ٢٠٢٥/١/٢٦.

السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء، ظهرت الحاجة لتوفير ضمانات أمنية خاصة مع بداية ظهور التهديدات والجرائم السيبرانية ومع ولوجنا في القرن الحادي والعشرين، عندها دخل الأمن السيبراني ضمن حقل الدراسات الأمنية وظهرت تقنيات متطورة مثل التشفير والأمان السحابي والكشف عن التهديدات بـ الذكاء الاصطناعي ورغم ذلك فإن الهجمات السيبرانية مجال معقد وسريع التطور مما يستلزم استجابات أمنية سريعة تضاهي وتيرة نموه السريع.

نتيجة ذلك اكتسب الأمن السيبراني (Cyber Security) أهمية قصوى كمتغير جديد في العلاقات الدولية[١].

بدأت الدول بخطوات حثيثة لمواجهة هذا المتغير المهم في سن التشريعات الخاصة بالجرائم السيبرانية وإصدار الأحكام الجنائية على المُدانين.

وتتجسد الجهود الحالية لمعظم الدول بشركاتها ومؤسساتها في محاولة دمج الذكاء الاصطناعي في عمليات مكافحة هجمات الفيروسات من خلال إنشاء جدار أمني عالي المستوى والكفاءة لتقليل الآثار الكارثية لأي هجمة سيبرانية[٢]، وأصبح تعزيز أمن ومرونة القضاء السيبراني عملاً مهماً للأمن الوطني لدول العالم كافة وبات يشكل جزءاً أساسياً في السياسة الداخلية والخارجية ويتم تصنيف الأمن السيبراني من قبل صناع القرار كأولوية في سياساتهم الدفاعية لذا أصبح لزاماً عليهم وضع استراتيجيات خاصة في هذا المجال.

تعريف الأمن السيبراني

يعرف الأمن السيبراني (بأنه عبارة عن مجموع الوسائل التقنية والتنظيمية المستخدمة لحماية الأنظمة والشبكات الالكترونية من التهديدات والهجمات السيبرانية.

وكذلك بأنه أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والأجهزة المتصلة بالإنترنت وعليه فهو المجال الذي يتعلق بإجراءات ومقاييس ومعايير الحماية المفروض اتخاذها والالتزام بها لمواجهة التهديدات أو على الأقل الحدّ من آثارها[٣].

لقد تعددت تعريفات الأمن السيبراني على وفق رؤى وتصورات عدد من الباحثين في مجال المعلوماتية إذ عرفه إدوارد امورسو (Edward Amorso) بأنه وسائل من شأنها الحد من خطر

(١) الأمن السيبراني مفهومه وتاريخه Net.Aljazeera تاريخ الزيارة ٢٠٢٥/١/٢٦.

(٢) جهاد دحام، تاريخ الأمن السيبراني https://www.Mawdoo٣.com.، تاريخ الزيارة ٢٠٢٥/١/٣٠.

(٣) منى جبور الأشقر: السيبرانية هاجس العصر، (المركز العربي للبحوث القانونية والقضائية، بيروت، ٢٠١٧)، ص٢٥.

الهجوم على البرامجيات أو أجهزة الحاسوب أو الشبكات وتشمل تلك الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات[١].

في حين عرفه ريتشارد (Richard A. Kemmerey) : بأنه عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة[٢]. وهنالك من يعرف الأمن السيبراني هو ممارسة حماية أجهزة الكومبيوتر والشبكات وتطبيقات البرامج والأنظمة الهامة والبيانات من التهديدات الرقمية المحتملة.

وقدمت وزارة الدفاع الأمريكية (البنتاغون) تعريفاً آخر لمفهوم الأمن السيبراني فوصفته (أنه يشمل الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والالكترونية من مختلف الجرائم كالهجمات التخريبية والتجسس والحوادث).

في حين عرفه الإعلان الأوربي، الأمن السيبراني على أنه قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات[٣].

(السيبرا) عملية انعكاسية نشطة تعكس مداخلات التفاعلات الالكترونية في بيئة لا يستطيع الإنسان إدراكها

أما ما يتعلق بالمدلول اللغوي فإن الأمن السيبراني نسبة إلى السيبرانية (Cyber) * التي توصف بـ (التخيلية) وهي البيئة الالكترونية غير الملموسة ومعقدة التفاعل، يتم فيها بناء نماذج لظواهر أو صور الكترونية و(السيبرا) عملية انعكاسية نشطة تعكس مداخلات التفاعلات الالكترونية في بيئة لا يستطيع الإنسان إدراكها، بمعنى آخر هي عبارة عن شبكة الكترونية لمجموعة من الخوادم الالكترونية لها قاعدة بيانات متاحة للجميع تتفاعل فيما بينها متجاوزة الحدود الجغرافية والسياسية وذلك لتحسين قدرة الاتصال والتعامل الالكتروني في المجتمعات كالشبكات الافتراضية وأسواق البورصة[٥] السيبرانية يمكن للمستخدم التعامل مع بيئتها الافتراضية.

---

(1) Edward Moroso ,Cyber Security ,Silicon press ,2007 ,P.1.

(2) Richard A .Kemmerer ,Cyber Security ,University of California ,2003 ,P.3.

(٣) الموسوعة السياسية، تعريف الأمن السيبراني، www.encyclopedia.org // https.

* Cyber: هو مصطلح درج استخدامه لوصف الفضاء الذي يضم الشبكات المحوسبة وشبكات الاتصال والمعلومات وأنظمة التحكم عن بُعد، وكمفردة فإنه يعد كلمة يونانية وتعني الدفة التي تدير السفينة إشارة إلى التحكم.

(٥) علي زياد العلي، (مصدر سابق)، ص٦٠ – ٦١.

التدابير الخارجية

يعد مصطلحاً يستخدم غالباً في العلاقات الدولية والسياسات العامة ويشير إلى الإجراءات أو السياسات التي تتخذها دولة ما خارج حدودها بهدف حماية مصالحها أو تعزيز نفوذها أو تحقيق أهداف أمنية، اقتصادية أو سياسية تفرض العقوبات على دول أو كيانات أجنبية أو الدعم الدبلوماسي أو العسكري لحلفاء في نزاع ما أو التدخل الإنساني في دول تشهد أزمات كإرسال مساعدات أو قوات حفظ سلام وقد تكون تلك التدابير عبر تحالفات ومعاهدات دولية أو الدعاية والحرب الإعلامية.

المبحث الثاني

الاشتقاقات والمفاهيم المقاربة للأمن السيبراني

هنالك العديد من المفاهيم المرتبطة والمقاربة بالأمن السيبراني ومن أهمها :

الفضاء السيبراني

عرفت الوكالة الفرنسية بأنه (فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية، فهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية مكون من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرامجيات والمستخدمين سواء مشغلين أو مستعملين)[١].

يرتبط الفضاء الالكتروني السيبراني بالمعلومات ولذلك فإن احتمالية استخدامها كأداة للحروب عبر تكنولوجيا المعلومات والتي تمتاز بالقوة العسكرية والدقة في تنفيذ العمليات العسكرية ولعل مصطلح الحرب المعلوماتية أقرب إلى الحروب الالكترونية الحديثة[٢].

وعرف جوزيف ناي الفضاء الالكتروني على أنه (نطاق تشغيلي محكم باستخدام الالكترونات لاستكشاف المعلومات عبر أنظمة مترابطة ببعضها البعض وبنية تحتية لها، وعرفته جامعة الدفاع الوطني الأمريكية بأنه مجال تشغيلي تجري فيه مجموعة من العمليات ذات الطابع الالكتروني الفريد والمحكم بمجموعة من الاستخدامات التي تعتمد على الالكترونات والأطياف الكهرومغناطيسية لإنشاء وتخزين وإبدال وتبادل واستغلال المعلومات من خلال مجموعة من نظم المعلومات المترابطة والمتصلة عبر الانترنت والبنى التحتية الخاصة)[٣].

(١) منى عبد السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، (مجلة كلية التربية، العدد (١١)، جامعة المنصورة، ٢٠٢٠)، ص١١.

(٢) فادية عباس هادي، استراتيجية اوباما في الحرب المعلوماتية، أوراق دولية، (مركز الدراسات الدولية، جامعة بغداد، ١٩٣، ٢٠١٠)، ص١٥.

(٣) ايهاب خليفة، القوة الالكترونية، كي يمكن أن تدير الدول شؤونها في عصر الانترنت، (دار العربي للنشر والتوزيع، بيروت، ٢٠١٧)، ص٢٧.

القوة السيبرانية

عرف جوزيف ناي القوة السيبرانية بأنها القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء الالكتروني، أي أنها القدرة على استخدام الفضاء الالكتروني والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات الكترونية، كما يوضح جوزيف ناي بأن مفهوم القوة الالكترونية يشير إلى مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الالكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل[١].

الردع السيبراني

طوال الحرب الباردة، كانت نظرية الردع هي الإطار المفضل للتحليل والعقيدة العسكرية ولتفسير تأثير الأسلحة النووية ودفع ذلك القوة النووية، خوفاً من العواقب بأن لا تخوض حرباً مع بعضها البعض ومنذ ذلك الحين، طبق المؤلفون الإطار النظري على الفضاء الالكتروني والمتمثل بالردع الالكتروني.

الجريمة السيبرانية على أنها نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ فعل إجرامي أو سلوك غير مشروع مرتبط بالشبكات المعلوماتية العالمية

يعرف الردع السيبراني (Deterrence Cyber) على أنه منع الأعمال الضارة ضد الأصول الوطنية في الفضاء الرقمي والأصول التي تدعم العمليات الفضائية[٢] ويمكن تعريف الردع على أنه ثني أو منع شخص ما أو دولة ما عن فعل شيء عن طريق خلق اعتقاد لديهم بأن التكاليف التي ستحملونها ستتجاوز المنفعة المتوقعة في مجال الأمن السيبراني.

الجريمة السيبرانية

تعرف الجريمة السيبرانية على أنها نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ فعل إجرامي أو سلوك غير مشروع مرتبط بالشبكات المعلوماتية العالمية ففهي جرائم العصر الرقمي التي تطال المال والمعرفة والثقة

(١) يونس مؤيد يونس، استراتيجية الولايات المتحدة للأمن السيبراني، (مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، العدد ٥٥، ٢٠١٨)، ص١٢٤.

(٢) الأمن السيبراني، هيئة الإعلام، (قسم الدراسات والاتصال والعلاقات العامة، الأردن، ٢٠٢١)، ص٢.

والسمعة وكلها عبر وسائل اتصالات تستخدم فيها التقنية الحديث[١]، إذن هي بالمجمل أعمال غير قانونية تتم عبر معدات وأجهزة الكترونية عبر الانترنت أي بواسطة الكومبيوتر أو أحد وسائل التقنية الحديثة على كومبيوتر آخر أو أحد وسائل التقنية الحديثة مع ضرورة توفر شبكة اتصال فيما بينهما.

وهنا لابد لنا من التفريق ما بين الجريمة السيبرانية والهجمات السيبرانية فعلى الرغم من أنهما متشابهات من حيث المجال السيبراني إلا أنهما يختلفان معاً في نقطتين هما[٢] :

١- بالنسبة للأشخاص ما يكون مرتكبي الجرائم السيبرانية هم الأفراد وتوجه نحو المؤسسات المالية أو الشركات وحتى أفراد داخل أو خارج إقليم الدولة، بخلاف الهجمات التي تتم من قبل دول أو مجموعات حكومية أو غير حكومية ضد دولة أخرى.

٢- أما بالنسبة للأهداف غالباً ما يكون الهدف من الجرائم السيبرانية هو إثبات مهارة الفاعل تقنياً وقدرته على اختراق أجهزة الكومبيوتر أو بهدف التسلية أو تحقيق مكاسب شخصية كسرقة الملكية الفكرية عن طريق شبكات الحاسب الآلي أو التسلل إلى أنظمة المصارف والتلاعب بأرقام الحسابات وتحويل الأموال دون الحاجة إلى تدمير وتعطيل شبكة الكومبيوتر المستهدفة وتكون هذه الأفعال مجرمة بموجب القانون الوطني بخلاف الهجمات السيبرانية التي يستهدف مرتكبوها الأمن القومي والسياسي للدولة ويقوم هؤلاء بتخريب الشبكات التي تتحكم بالبنى التحتية الأساسية في الدولة وتدميرها بقصد إرباكها وزعزعة النظام فيها لتحقيق أهداف أمنية أو عسكرية أو سياسية.

الأمن السحابي

إن التقنية السيبرانية تعتمد على حفظ المعلومات في الفضاء السيبراني وهو جزء من الأمن السيبراني والاعتماد المتزايد على الخدمات السحابية يخلق نقاط ضعف للدول، إذ تشن في اليوم الواحد الآلاف من الهجمات للاستحواذ على المعلومات المرفوعة في البنية التحتية السحابية العالمية ويوصف الأمن السحابي بأنه السياسات والتقنيات والضوابط التي تعمل جميعها لحماية البيانات المشفرّة والتطبيقات المرتبطة بها والمكونة للحوسبة السحابية،

(١) روان بنت عطية الله الصحفي، الجرائم السيبرانية، المجلة الالكترونية الشاملة متعددة الاختصاصات، العدد الرابع والعشرون، (جدة، أيار، ٢٠٢٠)، ص٩.

(٢) نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني،(رسالة ماجستير غير منشورة، كلية القانون، جامعة دمشق، ٢٠٢١(، ص١٤.

واجبها حماية البيانات وأمن التطبيقات والأنظمة السرية وغيرها من الواجبات[١].

أمن المعلومات أو البيانات

يمثل فرعاً من فروع الأمن السيبراني، إلا أنه يخص بعض جوانب قطاعات الاقتصاد والمصارف العالمية، حيث تعاني هذه البنية من هجمات افتراضية كثيرة للحصول على الحسابات المصرفية للمؤسسات والأفراد.

الهدف من الجرائم السيبرانية هو إثبات مهارة الفاعل تقنياً وقدرته على اختراق أجهزة الكومبيوتر أو بهدف التسلية أو تحقيق مكاسب شخصية كسرقة الملكية الفكرية عن طريق شبكات الحاسب الآلي أو التسلل إلى أنظمة المصارف والتلاعب بأرقام الحسابات وتحويل الأموال

واختراق هذه البيانات يلحق بلا شك خسائر مالية قاسية أكثر فداحة مما تسببه الجرائم التقليدية، ليس على مستوى المنظمات والجهات والمؤسسات بما يؤثر سلباً على اقتصاديات الدول والمؤسسات والمنظمات والأفراد على حد سواء، إذ يتعرض الأفراد إلى سرقة المعلومات الخاصة بهم (الهوية، بطاقة الإئتمان)، كذلك الابتزاز والتهديد وعمليات الاحتيال، تحويل أو نقل حساب مصرفي أو نقل ملكية الأسهم، أما على صعيد أبعد فقد تتعرض المؤسسات والمنظمات والبنوك والشركات إلى عملية اختراق للمعلومات السرية للصفقات والمناقصات والتسويق، كذلك العبث بمخازن المعلومات الخاصة أو حذفها أو تعديلها أو تعطيل الوصول إليها، وسرقة الأموال وتحويل الحسابات المصرفية[٢].

(١) سامر جمال حسن، أثر متغير الأمن السيبراني في العلاقات الأمريكية – الروسية ما بعد أحداث (١١ أيلول ٢٠٠١)، بحث ترقية مقدم إلى معهد الخدمة الخارجية، (وزارة الخارجية العراقية، ٢٠٢٠)، ص٤٩.

(٢) علي زياد العلي، مصدر سابق، ص٩٧، وكذلك: حسن سعدي، القرصنة الإلكترونية، سلاح العصر الرقمي، (مركز الجزيرة للدراسات، ٢٠١٦).

المبحث الثالث

أثر الهجمات السيبرانية الروسية في تعزيز الأمن القومي

الخطوات الأولى للتدابير الروسية الخارجية ومتغير الأمن السيبراني

عملت روسيا بشكل كبير على تنمية قدراتها السيبرانية وتطويرها، وقد سخرت تلك القدرات كسلاح فعال لإيقاع الضرر في قدرات الردع الإستراتيجي الأمريكي.

على الصعيد الدولي تتمثل مصالح روسيا القومية في ضمان السيادة ودعم مركزها كقوة عظمى وأحد مراكز الثقل في العالم متعدد الأطراف وفي مجال المعلومات تتمثل مصالحها القومية، في الالتزام بالحقوق والحريات المدنية الدستورية والخاصة بالحصول عل المعلومات واستخدامها وتطوير تقنيات الاتصال الحديثة[١].

إن مصادر المعلومات باتت تمثل البيئة الإستراتيجية الجديدة أو البديلة للإستراتيجية الدولية التقليدية التي تضم في دائرتها الواسعة مسلمات التفاعلات الدولية[٢]، وقد سعت القوى الفاعلة بمختلف مستوياتها إلى التعامل مع الإستراتيجية السيبرانية كمجال واسع للتفاعل والانغماس فيه.

لذا بدأ الصراع بين الدول الفاعلة حول امتلاك أدوات الحماية والدفاع وتطوير القدرات السيبرانية لاستهداف حيازة القوة والتفوق والهيمنة وتعزيز التنافس حول السيطرة والابتكار على المستويين المحلي والدولي.

بدأت روسيا الاتحادية أولى خطواتها على الصعيد الدولي بهدف تأسيس بعض قواعد التعاون الأمني السيبراني، إذ قدمت عام (١٩٩٨) مشروع قرار إلى الجمعية العامة للأمم المتحدة حول التطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في إطار الأمن الدولي وقد تضمن ذلك المشروع تحذيراً من التهديدات القائمة والمحتملة في مجال الأمن السيبراني ودعوة الدول الأعضاء كافة إلى إعلام الأمن العام للأمم المتحدة بوجهات نظرهم بهذا الخصوص.

إن أحد الأهداف الرئيسية لعقيدة الأمن السيبراني الروسية هو (الردع الإستراتيجي) والوقاية من النزاعات العسكرية التي يمكن أن تنجم عن استخدام تكنولوجيا المعلومات

(١) ايميل خوري، صراعات الجيل الخامس، (الطبعة الأولى، شركة المطبوعات للتوزيع والنشر، بيروت، ٢٠١٧)، ص٨٧.

(٢) كمال مساعد، عقيدة عسكرية روسية جديدة، على الرابط الالكتروني : https://:com.akhbar-al، تاريخ الزيارة ٢٠٢٥/١/١٢.

ومواجهة التهديدات للأمن العسكري والتكنولوجي في روسيا وسبق ذلك أن أكدت العقيدة للمدة (٢٠٠٥ - ٢٠١٠) مكانة روسيا على الصعيد الدولي وكذلك التركيز على العوامل الجيوسياسية وهي أقرب ما تكون إلى الاستنفار والمواجهة مع الغرب منها إلى الموقف الدفاعي[١].

لقد أعلن الرئيس فلادمير بوتين في مؤتمر ميونخ في (١٠ / شباط / ٢٠٠٧) ((أن روسيا غير راضية عن شكل البيئة الدولية ولن تقبل بالأحادية القطبية (Unipolarity) وقيادة العالم من قبل قوة واحدة وقد عده وضعاً شاذاً لابد أن يتغير ويصبح العالم متعدد الأقطاب (Multipo-larity) والقانون الدولي هو المرجع الأساس لحل النزاعات والصراعات والحروب في العالم))[٢].

وقد حدث ذلك التصريح بشكل متسق مع محاولات روسيا لتعزيز دورها دولياً بعد تأمين ساحتها الداخلية ومجالها الحيوي. وضمن الأحداث المتتابعة والمترابطة التي تتعلق بالأمن السيبراني الروسي كان الفضاء السيبراني المجال الأرحب في التنافس والصراع بين القوى الفاعلة واستخدامه كمجال لشن الهجمات السيبرانية ضد الدول الأخرى وتوظيفه سياسياً لتحقيق مصالح تلك القوى وذلك ما أقدمت عليه روسيا في هجماتها السيبرانية على استونيا عام (٢٠٠٧) وعلى جورجيا (٢٠٠٨) وعلى ألمانيا عام (٢٠١٥) وعلى المملكة المتحدة عام (٢٠١٦).

إلا أننا سنتناول تلك الهجمات السيبرانية التي قامت بها روسيا الاتحادية بشنها على أوكرانيا والخلاف السيبراني الروسي – الأميركي.

الهجمات السيبرانية الروسية على أوكرانيا

شنت روسيا الاتحادية سلسلة من الهجمات السيبرانية على مدى أيام وذلك لتعطيل نتائج الانتخابات الأوكرانية في (آذار ٢٠١٤)، وعمدت إلى تعطيل الأنظمة الأوكرانية لفرز الأصوات بشكل مؤقت، فضلاً عن محاولة التدخل في نتائج الانتخابات في محاولة لتغييرها وتأخير النتيجة النهائية للانتخابات[٣].

ويبدو أن روسيا قد أطلقت برامجها وذلك لإعلان نتائج مزيفة وموجهة لفئات من الشعب الأوكراني بعينها من أجل دعم الرواية الروسية، التي ادعت منذ البداية أن المتطرفين والنازيين

---

(١) أحمد دهشان، الرؤية الروسية لملف الإرهاب، تعريفه وآليات مكافحته، الرابط الالكتروني : https : // al net.amesbar، تاريخ الزيارة : ٢٠٢٥/١/٢٣.

(٢) سامر جمال حسن، (مصدر سابق)، ص٥٠ - ٥١.

(3) Maria Malksso ,Countering hybrid warfare as anthological Security Management, The emerging Practices of The Eu and NATO ,vol ,27 ,No3 ,2018 ,p.374 .

كانوا وراء أحداث أوكرانيا[١].

ترجع أسباب التدخل الروسي في أوكرانيا لأنها تمثل أهمية قصوى لروسيا الاتحادية، كونها المعبر الرئيس لتمرير النفط والغاز إلى قارة أوربا، ما يوفر من تكاليفه الباهضة، فضلاً عن أن أوكرانيا تعد ثاني البلدان الأوربية من حيث المساحة وتتمتع بموارد مائية مهمة كالبحر الأسود، وشبكة واسعة من الأنهار، وقد مثلت منتجات القطاع الزراعي نحو (٤٥٪) من إجمالي الصادرات الأوكرانية فعادت على البلاد نحو (٢٢,٥) مليار دولار وأبرزها كانت صادرات الحبوب (القمح والشعير والذرة)[٢].

وكذلك تأتي أهمية الجيوستراتيجية لأوكرانيا من كونها الجدار الفاصل بين روسيا الاتحادية وأوربا الشرقية وضمن حدودها تبدأ محاصرة النفوذ الروسي، حسب الإستراتيجية الأمريكية لتحول دون صعود روسيا من جديد كقوة فاعلة وعظمى على المستوى الدولي، وقبل وقت قصير من الغزو الروسي الكامل لأوكرانيا عام (٢٠٢٢) شنت روسيا عدد من الهجمات الالكترونية ضد أوكرانيا وفي إطار ضمها لشبه جزيرة القرم عام (٢٠١٤) استخدمت روسيا الهجمات السيبرانية لاستهداف إمدادات الطاقة في كييف.

وتستند العمليات السيبرانية الروسية لأهداف إستراتيجية في أوكرانيا على التعطيل والتسبب في حوادث منخفضة التكلفة ومنخفضة التأثير والتجسس قصير المدى (الوصول إلى التأثير الفوري) والتجسس طويل المدى (الاستفادة من المعلومات) في إطار العمليات المستقبلية وكذلك التدهور (السعي إلى التدمير المادي والإعاقة).

وفقاً للدراسات فقد تم تسجيل (٣٠) حادثة سيبرانية ثنائية بين روسيا وأوكرانيا بين عامي (٢٠٠٠ – ٢٠٢٠) من بينها (٩٣٪) قامت بها روسيا وتركزت غالبية هجمات روسيا (٥٧٪) على جهات فاعلة خاصة وغير حكومية كما استهدفت (١١٪) فقط أهداف عسكرية حكومية داخل أوكرانيا لأغراض التعطيل والتجسس وهي جزء من إستراتيجية شاملة لشن حرب سيبرانية روسية ضد أوكرانيا[٣].

---

(١) ليوبون ستيوشوفا، روسيا تؤثر في مصير انتخابات (٢٤) بلداً في العالم، مركز نون بوست ٢٠١٧، منشور على الرابط الالكتروني: http://www.noonpost.org، تاريخ الزيارة: ٢٠٢٥/١/٣٠.

(٢) ايمان أشرف شلبي، الأبعاد الدولية للأزمة الأوكرانية على الرابط الالكتروني: https://democraticac.de، تاريخ الزيارة: ٣٠/١/٢٠٢٥.

(3) Grac B. Muller, Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, Jose M. Macias Cyber Operations during The Russo – Ukrainian war, Center for strategic and international studies, Jul,2023.

الخلاف السيبراني الروسي – الأمريكي

إن مسار العلاقات الروسية – الأمريكية وصلت أدنى مستوياتها منذ تولي ترامب الرئاسة في الولايات المتحدة الأمريكية في الولاية الأولى والوثائق الصادرة عن البيت الأبيض ووزارة الدفاع الأمريكية تؤكدان التوتر بين الجانبين ليس من قبيل الخلافات العابرة وإنما تناقضات جوهرية وهيكلية يصعب تجاوزها **وقد تركز هذا التناقض في ثلاث محاور**[١] :

- **التنافس الإستراتيجي وصراع المكانة الدولية وزعامة العالم.**
- **الاختلافات بشأن القضايا الإقليمية.**
- **التنافس في سوق الطاقة.**

تبرز أوجه الخلاف السيبراني بين الدولتين في خضم التنافس المتصاعد ويمكن أن نلخصها بالآتي:

١- **الاتجاه الأول:** تحول الصراع (الناعم) على المعلومات والاستخبارات إلى صراع (صلب) للاستحواذ على القوة السيبرانية ذات الطابع التدميري واستثمار تطوير أدوات هذه القوة في استخدام الأسلحة السيبرانية من أجل تعزيز القيادة والسيطرة.

٢- **الاتجاه الثاني:** تأثير تزايد حالة الاحتقان بين روسيا والولايات المتحدة الأمريكية، يسعى كل طرف لإيجاد تكتل دولي داعم له وضاغط على الطرف الآخر[٢].

٣- **الاتجاه الثالث:** توظيف الفضاء السيبراني لتحقيق أهداف وغايات أخرى عبر التدخل في الشؤون الداخلية من خلال دعم حركات معارضة سياسية أو مسلحة وتقديم الدعم التقني أو السياسي أو الإعلامي لها.

٤- **الاتجاه الرابع:** تصاعد النشاطات السرية والاستخباراتية وتوظيف برامجيات التجسس والرصد والتحول من توجيه هجمات سيبرانية من الخارج إلى الداخل، فضلاً عن توظيف عملاء الاستخبارات أو الدبلوماسيين المقيمين بشن هجمات إلى داخل الدولة المقيمين فيها.

(١) نورهان الشيخ، العلاقات الروسية – الأمريكية من الحرب الباردة إلى السلام البارد، (المكتب العربي للمعارف، القاهرة، ٢٠١٨)، ص٥٢.

(٢) جوزيف. س. ناي، القوة الناعمة، وسيلة النجاح في السياسة الدولية، ترجمة محمد توفيق البجيرمي، العبيكان للنشر، (المملكة العربية السعودية، ٢٠١٥)، ص٢٢ – ٢٥.

ثمة تحذير تشير إليه إحدى مراكز البحوث الأمريكية ومخاوف من التصعيد في الصراع السيبراني باستخدام بدائل للعمليات الالكترونية لدرجة عدم القدرة على التنبؤ بنشوب الصراع استناداً إلى شكوك في قدرات روسيا في هذا المجال وعدم انضباط الفاعلين وضعف السيطرة على نشاطاتهم من قبل الحكومة الروسية وتخشى الولايات المتحدة الأمريكية بأن يمتلك الخصوم قدرات سيبرانية تقترن بقوة تخريبية بعيدة المدى، تزيد بدورها حوافز التصعيد وتكون مقدمات لمزيد من الهجمات التي ليست في الواقع قيد التحضير وقد يحدث الانتقام من جديد وصراع بسبب أخطاء يرتكبها الفاعلون[١].

لقد أدى الخلاف بين كلا الجانبين إلى عدم التوصل إلى اتفاق حول الأمن السيبراني والاختلاف في الرؤية للإستراتيجيات والمبادئ وخاصة في عهد الرئيس (جو بايدن) عندما أثرت التهديدات السيبرانية على كل جانب من جوانب العلاقات العسكرية والأمنية بين روسيا وأمريكا، وعندما وصل الرئيس الأمريكي (دونالد ترامب) إلى الإدارة الأمريكية في ولاية ثانية في (٢٥/يناير/٢٠٢٥) تم إيقاف الحملات السيبرانية الهجومية ضد روسيا في وقت تتواصل فيه المساعي الدبلوماسية لوقف الحرب الروسية – الأوكرانية.

نستنتج من ذلك أن التهديدات السيبرانية تشكل تحدي كبير للعلاقات الأمريكية – الروسية على مستويات متعددة وفي ظل هذه التحديات يجب على البلدين السعي نحو تعزيز الحوار والتعاون في مجال الأمن السيبراني لتجنب تصعيد التوترات وتحقيق استقرار أكبر في العلاقات الدولية.

وأخيراً يمكن القول: إن انتقال السياسة الخارجية الروسية إلى استخدام التهديدات السيبرانية بديلاً عن الحروب والتهديدات العسكرية وهذا له أبعاد اجتماعية وإنسانية، حيث يجنب الدول الوقوع تحت طائلة عقوبات القانون الدولي الإنساني وجرائم الحرب وتعويضات عن الضحايا التي تخلفها الحروب، كما أنه يعمل أكثر على التكوين النفسي للشعوب، وإثارة القلق والترقب لوقوع أخطار محتملة لا يمكن التكهن بمداها.

(١) كريستوفر. س. تشينيس وآخرون، تعزيز الاستقرار الاستراتيجي مع روسيا، (مؤسسة راند الأمريكية، كاليفورنيا، ٢٠١٧)، ص٩ – ١٠.

الخاتمة:

ظهرت الحاجة لدى الدول إلى تأمين الفضاء السيبراني وحمايته بإجراءات وتدابير متعددة لمواجهة الاختراقات والتهديدات والهجمات (الالكترونية) لما يعرف بـ (الأمن السيبراني) بعد أن أصبحت المخاطر جدية وتهدد حياة الملايين من البشر فأصبح تعزيز أمن ومرونة الفضاء السيبراني عملاً أساسياً لتعزيز الأمن القومي لدول العالم كافة وبات يشكل ركيزة أساسية للسياسات الأمنية الوطنية ولا يخفى عن ذي لب أن مسائل الأمن السيبراني أصبحت من الثوابت كأولوية في السياسة الدفاعية للدول ومن ضمنها روسيا الاتحادية التي اتخذت حزمة من التدابير الخارجية لتعزيز أمن وحماية الشبكات وأجهزة الحاسوب والاتصال والبرامج والبيانات من الهجوم والتلف ولكي تكون بمنأى عن التعطيل أو التشويش والإعاقة.

وعملت روسيا الاتحادية بشكل دؤوب على تعزيز قدراتها السيبرانية وذلك لإيقاع خسائر جسيمة في قدرات الخصوم بشكل يجعل من تلك القدرات إحدى أهم مرتكزات الردع الإستراتيجي الروسي وهذا بلا شك مرتبط بالمصالح الروسية العليا في ضمان السيادة ودعم مكانتها الدولية كإحدى القوى العظمى.

لقد شكلت الحرب السيبرانية الروسية الأوكرانية إحدى مكونات المواجهة بين روسيا وأوكرانيا منذ انهيار الاتحاد السوفيتي في ٢ ايلول ١٩٩١ وبالفعل فقد حققت روسيا نتائج كبيرة في مجال التأثير في الرأي العام وإضعاف الروح المعنوية للشعب الأوكراني واستهداف البنية التحتية المدنية وضرب أوكرانيا اقتصادياً وإضعاف الثقة في الحكومة الأوكرانية وبالمقابل حاولت أوكرانيا صد تلك الهجمات بالاستعانة بالغرب لمواجهة الهجمات الروسية وقد حقق الجانبان أهداف أخلت نوعاً ما بالمنظومة المضادة.

أما ما يتعلق بجانب الخلاف الروسي الأمريكي فعلى الرغم من أوجه التشابه في مجال الاستهداف السيبراني ومرت كل من الولايات المتحدة الأمريكية وروسيا الاتحادية بمسارات مختلفة في تطوير قدراتهما وسياستهما في هذا المجال، بسبب اختلاف العقيدتين السيبرانيتين لكل منهما، الأمر الذي نجمت عنه فجوة في استخدام العمليات السيبرانية ومع ذلك لا يمكن ردع الخطر السيبراني في إرادة كل الطرفين، وسوء الفهم المتبادل، إلا أن روسيا استطاعت تحقيق اختراقات غير مقيدة لمنظومة المعلومات الأمريكية.

في ظل تلك المعطيات يستمر الشد والجذب بين روسيا والولايات المتحدة الأمريكية إذ تحاول الأخيرة تأكيد نفوذها في مجال الأمن السيبراني يقابله رفض روسي لـ (أمركة الانترنت) من جانب وامتناعها عن قبول هيمنة الشركات الأمريكية من جانب آخر واستمرار روسيا في فرض قيود صارمة على ما يمكن أن يُعد تهديداً لأمنها القومي.

قائمة المصادر

اولا: المصادر العربية

أ- الكتب العربية والمترجمة:

١- علي زياد العلي، الصراع والأمن الجيوسيبراني في السياسة الدولية، ط١، (دار أمجد للنشر والتوزيع، عمان – الأردن، ٢٠١٩).

٢- منى جبور الأشقر: السيبرانية هاجس العصر، ا(لمركز العربي للبحوث القانونية والقضائية، بيروت،)٢٠١٧.

٣- ايهاب خليفة، القوة الالكترونية، كي يمكن أن تدير الدول شؤونها في عصر الانترنت، (دار العربي للنشر والتوزيع، بيروت، ٢٠١٧).

٤- الأمن السيبراني، هيئة الإعلام، (قسم الدراسات والاتصال والعلاقات العامة، الأردن، ٢٠٢١.

٥- نورهان الشيخ : العلاقات الروسية – الأمريكية من الحرب الباردة إلى السلام البارد،(المكتب العربي للمعارف، القاهرة، ٢٠١٨).

٦- جوزيف. س. ناي، القوة الناعمة، وسيلة النجاح في السياسة الدولية، ترجمة محمد توفيق البجيرمي، العبيكان للنشر، (المملكة العربية السعودية، ٢٠١٥).

٧- كريستوفر. س. تشينيس وآخرون، تعزيز الاستقرار الاستراتيجي مع روسيا،(مؤسسة راند الأمريكية، كاليفورنيا، ٢٠١٧).

ب- الاطروحات والرسائل العلمية:

١- نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، (رسالة ماجستير غير منشورة، كلية القانون، جامعة دمشق، ٢٠٢١).

ج- المجلات والصحف:

١- منى عبد السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، (مجلة كلية التربية، العدد (١١)، جامعة المنصورة، ٢٠٢٠.

٢- فادية عباس هادي، استراتيجية اوباما في الحرب المعلوماتية، أوراق دولية، (مركز الدراسات الدولية، جامعة بغداد، ١٩٣، ٢٠١٠.

٣- يونس مؤيد يونس، استراتيجية الولايات المتحدة للأمن السيبراني، (مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، العدد ٥٥، ٢٠١٨.

٤- روان بنت عطية الله الصحفي، الجرائم السيبرانية، المجلة الالكترونية الشاملة متعددة الاختصاصات، العدد الرابع والعشرون، جدة، أيار، ٢٠٢٠).

٥- سامر جمال حسن، أثر متغير الأمن السيبراني في العلاقات الأمريكية – الروسية ما بعد أحداث (١١ أيلول ٢٠٠١)، بحث ترقية مقدم إلى معهد الخدمة الخارجية، وزارة الخارجية العراقية، ٢٠٢٠(.

د- المو اقع الالكترونية:

١- الأمن السيبراني: https : // www.political – encyclopedia.org.

٢- الأمن السيبراني مفهومه وتاريخه Aljazeera.Net تاريخ الزيارة ٢٠٢٥/١/٢٦.

٣- الأمن السيبراني مفهومه وتاريخه Aljazeera.Net تاريخ الزيارة ٢٠٢٥/١/٢٦.

٤- جهاد دحام، تاريخ الأمن السيبراني ٣com.https://www.Mawdoo.، تاريخ الزيارة ٢٠٢٥/١/٣٠.

٥- الموسوعة السياسية، تعريف الأمن السيبراني، https // www.encyclopedia.org.

٦- علي زياد العلي، مصدر سابق، ص٩٧، وكذلك: حسن سعدي، القرصنة الإلكترونية، سلاح العصر الرقمي، مركز الجزيرة للدراسات، ٢٠١٦.

٧- ليوبون ستيوشوفا، روسيا تؤثر في مصير انتخابات (٢٤) بلداً في العالم، مركز نون بوست ٢٠١٧، منشور على الرابط الالكتروني : http://www.noonpost.org، تاريخ الزيارة : ٢٠٢٥/١/٣٠.

٨- ايمان أشرف شلبي، الأبعاد الدولية للأزمة الأوكرانية على الرابط الالكتروني : https:// democraticac.de، تاريخ الزيارة : ٣٠ / ١ / ٢٠٢٥.

ثانياً: المصادر الأجنبية:

1- Edward Moroso, Cyber Security, Silicon press, 2007.

2- Richard A. Kemmerer, Cyber Security, University of California, 2003.

3- Maria Malksso, Countering hybrid warfare as anthological Security Management, The emerging Practices of The Eu and NATO, vol, 27, No3, 2018.

4- Grac B. Muller, Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, Jose M. Macias Cyber Operations during The Russo – Ukrainian war, Center for strategic and international studies, Jul, 2023.