حدود فعالية الحروب في تنفيذ أهداف السياسة الخارجية الروسية: دراسة حالة الحرب السيبرانية

The limits of the effectiveness of wars in the implementation of Russian foreign policy goals: a case study of cyber warfare

كيارا طه محمد

باحثة ماجستير بكلية السياسة والاقتصاد – جامعة بني سويف

نجاح عبدالفتاح الريس

أستاذ العلوم السياسية بكلية السياسة والاقتصاد – جامعة بني سويف

هشام محمد بشير

أستاذ العلوم السياسية ووكيل كلية السياسة والاقتصاد لشئون الدراسات العليا – جامعة بني سويف

المستخلص:

ينظر الاتجاه الواقعي للسياسة الدولية على أنها صراع من أجل القوة بمعناها التقليدي، ومع التطور التكنولوجي المتسارع الذي شهده العالم في العقود الأخيرة، تراجع احتكار القوة بمعناها التقليدي المتمثل في القوة الصلبة وظهر نوع جديد من القوة وهي القوة الإلكترونية أو الافتراضية، الأمر الذي ترتب عليه انتقال الحروب من صورتها التقليدية في ساحات القتال إلى ساحات الفضاء الإلكتروني، وبروز ما عرف باسم الحروب الإلكترونية، وقد كانت روسيا خير مثال للقوى العظمى التي استخدمت الحروب في سياستها الخارجية كوسيلة لتحقيق أهدافها الخارجية، ومن هذا المنطلق تهدف هذه الدراسة إلى تناول التدابير الحربية والتدابير ما دون الحربية التي تستخدمها روسيا كأداة لتحقيق أهدافها على المستوى الخارجي، وذلك من خلال دراسة أهمية تلك الحروب والفرق بينها.

الكلمات المفتاحية: التدابير الحربية في السياسة الخارجية الروسية ـ التدابير ما دون الحربية في السياسة الخارجية الروسية ـ الحروب التقليدية ـ الحروب الإلكترونية.

Abstract:

The realistic direction of international politics is seen as a struggle for power in its traditional sense, and with the rapid technological development that the world has witnessed in recent decades, the monopoly of power in its traditional sense of hard power has declined and a new type of power has emerged, which is electronic or virtual power, which resulted in the transition of wars from their traditional form on the battlefields to the battlefields. The emergence of what was known as electronic wars, and Russia was the best example of the great powers that used wars in Its foreign policy as a means to achieve its foreign policy goals. From this point of view, this study aims to address the military and sub-belligerent measures that Russia uses as a tool to achieve its goals at the external level, by studying the importance of these wars and the difference between them.
Keywords: War measures in Russian foreign policy - sub-war measures in Russian foreign policy - conventional wars - electronic wars.

المقدمة

مع انتهاء الحرب الباردة وتفكك الاتحاد السوفيتي وحلف وارسو العسكري، ورثت روسيا الاتحادية الاتحاد السوفيتي في مقعده الدائم في مجلس الأمن، والأسلحة النووية، وأصبحت لروسيا سياسة مستقلة قومها العمل على تعزيز الدور الروسي في مواجهة سياسات الغرب وخاصة الولايات المتحدة الأمريكية، وبصدد ذلك عملت روسيا على إظهار توازنها العسكري من أجل السعي إلى عالم متعدد الأقطاب تلعب فيه دورا محوريا، ومع التطور التكنولوجي المتسارع الذي شهده العالم في العقود الأخيرة، تراجع احتكار القوة بمعناها التقليدي المتمثل في القوة الصلبة وظهر نوع جديد من القوة وهي القوة الإلكترونية أو الافتراضية، ومن ثم انتقلت الحروب من صورتها التقليدية في ساحات القتال إلى ساحات الفضاء الإلكتروني، وبرز نوع جديد من الحروب عرف باسم "الحروب الإلكترونية"، وهي حروب تعتمد على الوسائل التقنية والتكنولوجية لا الأسلحة والعتاد، وقد كانت روسيا هي إحدى القوى العظمى التي استخدمت هذا النوع من الحروب لتحقيق أهداف سياستها الخارجية أيضًا بجانب الحروب التقليدية، وذلك عن طريق استخدام البرامج التقنية وبرامج التجسس المختلفة المعتمدة على الوسائل التكنولوجية الحديثة بغية التأثير في الرأي العام العالمي.

إشكالية الدراسة

تعتبر آلية الحروب من الآليات المهمة في دراسة السلوك السياسي الخارجي الروسي، حيث تعتبر روسيا من أهم القوى العظمى التي استخدمت الحروب بنوعيها كوسيلة في سياستها الخارجية، سواء من خلال التدابير الحربية

أو التدابير ما دون الحربية لخدمة مصالحها وتحقيق أهدافها، وفي هذا الاتجاه يثار التساؤل الرئيسي للدراسة حول: **ما مدى فعالية الحروب في تنفيذ أهداف السياسة الخارجية الروسية تطبيقا على الحرب السيبرانية...؟** وفي هذا الإطار تفرع عن التساؤل الرئيسي عدد من التساؤلات الفرعية التي سنحاول الإجابة عليها في طيات هذه الدراسة وذلك على النحو التالي:

- ما أنوع الحروب التي تستخدمها روسيا كوسيلة لتحقيق أهداف سياستها الخارجية؟
- ما مظاهر التقدم الروسي في مجال استخدامات الحروب السيبرانية؟
- ما مدى نجاح روسيا في استخدام الحروب السيبرانية في تنفيذ أهداف سياستها الخارجية؟

منهج الدراسة

انطلاقا من طبيعة الدراسة وأهدافها اعتمدت الباحث على المنهج الوصفي التحليلي ومنهج وذلك في محاولة للوصول إلى إجابة عن تساؤلات الدراسة كالتالي:

١/ المنهج الوصفي التحليلي

اعتمدت الدراسة على الاقتراب الوصفي التحليلي الذي هو أحد فروع المنهج الوصفي المتخصصة، حيث يقوم على دراسة الواقع أو الظاهرة كما هي ويقوم بوصفها وصفاً دقيقاً ويعبر عنها كيفياً بوصفها وتوضيح خصائصها، حيث يعتمد المنهج على تفسير الوضع القائم أي ما هو كائن وتحديد الظروف والعلاقات الموجودة بين المتغيرات، كما يتعدى المنهج الوصفي مجرد جمع بيانات وصفية حول الظاهرة إلى التحليل والربط والتفسير لهذه البيانات وتصنيفها وقياسها واستخلاص النتائج منها، وقد استفاد الباحث من هذا الاقتراب في جمع ورصد البيانات الوصفية حول آلية الحروب كوسيلة لتحقيق في السياسة الخارجية الروسية وبخاصة الحروب الإلكترونية وتحليلها وتصنيفها وقياسها واستخلاص مدي نجاحها في تحقيق أهداف متخذ القرار الروسي على المستوى الخارجي.[١]

٢/ منهج المصلحة الوطنية

يعد إقتراب المصلحة الوطنية إحدي الإقترابات البحثية الرئيسية في حقل العلاقات الخارجية و السياسة الخارجية، ويرتكز هذا المنهج على حقيقة أن المصلحة الوطنية هى الهدف النهائى والأسمى للسياسة الخارجية لأى دولة، فالسياسة الخارجية لأى دولة تعكس مصلحتها الوطنية، فهي تُصاغ وفقا لمصلحتها الوطنية، وقد ميز هانز مورجانثو

احد رواد هذا الاقتراب بين نوعين من المصلحة الوطنية: الأول هو المصلحة الوطنية الحيوية الأساسية الذي يهدف إلي بقاء الدولة و الحفاظ عليها، هذا النوع يقر بأن أي دولة علي استعداد للدخول في غمار الحرب لتحقيق مصلحتها الوطنية والحفاظ عليها لضمان استقلال و حرية الدولة، وحماية مؤسساتها وشعبها وقيمها الإجتماعية الأساسية. والثاني هو المصلحة الوطنية الثانوية التي لا تؤثر علي بقاء الدولة ولا تهدد سيادتها وبقائها لذا، وقد استفاد الباحث من هذا الاقتراب في تفسير استخدام روسيا للحروب السيبرانية كوسيلة في سياستها الخارجية وذلك انطلاقا من أن السياسة الخارجية للوحدة الدولية لا تنشاء من فراغ بل كنتيجة لبيئتها المحيطة بها، تلك البيئة التي تكون محددة بالمصالح القومية.[٢]

أهمية الدراسة

تأتي أهمية هذه الدراسة من كونها تحاول التركيز على آلية مهمة في دراسة السلوك السياسي الخارجي للدول بصفة عامة، والسلوك السياسي الخارجي الروسي بصفة خاصة آلا وهي آلية الحروب كوسيلة لتحقيق الأهداف، وذلك من خلال التطرق لتلك الحروب التي لجأت إليها روسيا في تحقيق أهدافها والتي في مقدمتها الحروب العسكرية التقليدية والتي تتناولها الدراسة في ضوء سباق التسلح في السياسة الخارجية الروسية في فترة الحرب الباردة وما بعدها، ثم تركز الدراسة على الحروب الإلكترونية كوسيلة فالسياسة الخارجية الروسية من خلال تناولها لمفهوم التدابير ما دون الحربية في السياسة الخارجية الروسية وأهميتها ووكلائها،

أهداف الدراسة

تهدف هذه الدراسة إلى تقديم رؤية تحليلية للحرب كأداة من ادوات تنفيذ السياسة الخارجية الروسية ولا سيما الحروب السيبرانية وتوظيف تقنيات الذكاء الاصطناعي فيها وذلك من خلال:

- ايضاح مدى فاعلية الحرب في تنفيذ أهداف السياسة الخارجية الروسية تطبيقا على الحرب السيبرانية.
- بيان الفرق بين مفهوم التدابير الحربية والتدابير ما دون الحربية في السياسة الخارجية الروسية وأهميتها.
- تناول أثر الحرب السيبرانية في السياسة الخارجية الروسية وأهميتها وكيف استخدمها متخذي القرار كأداة لتحقيق أهدافه.

تقسيم الدراسة

في إطار ما تقدم سوف يتم تناول آلية الحروب كوسيلة لتحقيق أهداف السياسة الخارجية الروسية بالتطبيق على الحروب السيبرانية من خلال مبحثين ، وذلك على النحو التالي:

المبحث الأول: الحروب التقليدية في السياسة الخارجية الروسية.

أولاً: سباق التسلح في السياسة الخارجية الروسية في فترة الحرب الباردة.

ثانيًا: سباق التسلح بعد إنتهاء الحرب الباردة.

المبحث الثاني: الحروب الإلكترونية في السياسة الخارجية الروسية.

أولاً: مفهوم التدابير ما دون الحربية في السياسة الخارجية الروسية وأهميتها.

ثانيًا: الحروب الإلكترونية كأداة في السياسة الخارجية الروسية ووكلائها .

المبحث الأول

الحروب التقليدية في السياسة الخارجية الروسية

بدأ سباق التسلح بين الولايات المتحدة الامريكية والاتحاد السوفيتي منذ نهاية الحرب العالمية الثانية، بعد قيام الولايات المتحدة بتدمير مدينتي هيروشيما ونجازاكي، باستخدام القنابل الذرية في تلك العملية، والتي اعتُبرت من أخطر القنابل وأسرعها في تحقيق نتائج عسكرية، ففي يوليو ١٩٤٥ نتجت أول قنبلة ذرية أمريكية، وأخبر الرئيس الأمريكي "ترومان" الزعيم السوفيتي "ستالين" بخططه لاستخدام السلاح النووي ضد اليابان وهو ما تم بالفعل في ٦ و٩ أغسطس ١٩٤٥، وبدأ الاتحاد السوفيتي معتمدًا على التوازن مع الولايات المتحدة بإجراء التجارب النووية والتي نتج عنها الإعلان في أغسطس عام ١٩٤٩، بأول قنبلة نووية كذلك وبدأ من ذلك الحين سباق التسلح بالدخول في مرحلة لتطوير الفئة الثانية من الأسلحة النووية.

أولاً: سباق التسلح في السياسة الخارجية الروسية في فترة الحرب الباردة.

في أواخر عام ١٩٥٢ احتدم التنافس الجيوسياسي للمعسكرين الشرقي والغربي، وبدأ الجانبان في تطوير القنابل الحرارية أو الهيدروجينية، وكان أول تفجير من نوع تلك الأسلحة للولايات المتحدة حينما أُعلن عن تفجير في نطاق جزر مارشال، وكان التفجير أقوى بمئات المرات مقارنة بالقنبلتين هيروشيما ونجازاكي، وخاضت بريطانيا أول تجربة نووية لها في العام نفسه ما، أضاف إلى سابق التسلح دولة ثالثة، وتمكنت واشنطن في ١٩٥٤ من استمراريتها في تطوير الأسلحة لاعتقادها أن الاتحاد السوفيتي لا يقف عند ما توصل إليه بل يستمر بشكل سريع في تطوير ترسانته النووية التي بدأها، وبالفعل بعد عام واحد أعلن الاتحاد السوفيتي في نوفمبر ١٩٥٥ عن أول جهاز نووي حراري، وهو ما شكل معضلة للقطبين نتيجة الانبعاثات الناتجة عن تطوير الأسلحة النووية. [٣]

وكانت الانبعاثات محور خطاب الرئيس الأمريكي "أيزنهاور" وعنوانه "الذرة من أجل السلام" أمام الجمعية العامة للأمم المتحدة في ديسمبر عام ١٩٥٣، ونتج عن الخطاب الأمريكي إنشاء وكالة الطاقة الذرية استجابة للمخاوف التي كان أسسها الاكتشافات الحديثة للتكنولوجيا النووية وما يمكن أن ينتج عنها من أضرار تؤثر على الأفراد، لذا قامت الوكالة بغرض المساهمة في تعزيز العمل السلمي وتطبيق ما توصلت إليه من نتائج لأغراض طبية، والتأكد من عدم استخدامها في الأعمال العسكرية، وساهم الخطاب الأمريكي في تشكيل النظام الأساسي للوكالة الدولية للطاقة الذرية، ووافقت حوالي ٨١ دولة على المقترح عام ١٩٥٦، وتم التصديق من قبل الولايات المتحدة في يوليو ١٩٥٧ ما مثل الولادة الحقيقة للوكالة، وانضم الاتحاد السوفيتي للوكالة في العام ذاته. [٤]

وفي سياق متصل وصل سابق التسلح بين الولايات المتحدة والاتحاد السوفيتي إلى إطلاق ما يسمى بالكذب بين الدول الذي عمد إليه الزعيم السوفيتي حينما نجح أول اختبار لصاروخ باليستي في العالم من نوع الصواريخ عابرة للقارات (ICBM)، في الرابع من أكتوبر عام ١٩٥٧، وبعد ايام تم إطلاق النسخة المعدلة من الصاروخ سبوتنيك ١، واستغل الزعيم السوفيتي ذلك لضمان عدم قيام الولايات المتحدة بضربة استباقية موجهة للأراضي السوفيتية وقت الأزمة، كذلك الضغط على حكومة الرئيس أيزنهاور للتخلي عن خطط تزويد ألمانيا الغربية بالسلاح النووي، وكان التفوق العسكري لصالح كفة الولايات المتحدة، واستمرت تلك الادعاءات السوفيتية وأظهرت الولايات المتحدة كقوة ثانية، وانتشر ما سُمي بفجوة الصواريخ، وانتقل سباق التسلح بينهما من إلى الفضاء، فبعد النتائج التي حققها الصاروخ الروسي ازداد الضغط على الرئيس أيزنهاور فقام بتحويل الأموال الفيدرالية إلى برنامج الفضاء الأمريكيين وبعد محاولات عديدة نجحت الولايات المتحدة في إطلاق أول قمر صناعي لها نهاية يناير ١٩٥٨، كما أنشأت في العام نفسه وكالة "ناسا "وهي وكالة مدنية

لاستكشاف الفضاء، كما أعتُبر عام ١٩٥٨ هو العام الأكثر نشاطًا في مجال التجارب النووية، إذ قامت الدول النووية الثلاث (الولايات المتحدة– الاتحاد السوفيتي– المملكة المتحدة) بإجراء أكثر من ١٠٠ تجربة، إلى أن توقفت تلك الدول طواعية عن تلك التجارب لحين مناقشة حظر دائم على تلك الأسلحة، ولم تمض فترة قليلة حتى لحقت فرنسا بركب الدول النووية عام ١٩٦٠، بعد إجراء أول تجربة لها لتصبح الدولة الرابعة في مجال حيازة الأسلحة النووية. [٥]

وفي سياق ما سبق أثر سباق التسلح بين الولايات المتحدة والاتحاد السوفيتي على غالبية الأزمات التي وقعت في العالم بشكل كبير، وقلل من فاعلية دور الأمم المتحدة في القضايا المتعلقة بسباق التسلح، وساهمت تلك العوامل في فترة ما بعد عام ١٩٦٠ في إحداث تحول في القدرات السوفيتية، وأصبحت أكثر شفافية عن السابق، وذلك نتيجة الأقمار الصناعية والاستخبارات الإلكترونية والبيانات المتبادلة بين القوتين تبعًا لمفاوضات الحد من الأسلحة النووية، ويمكن القول أن القدرات السوفيتية توسعت بشكل ملحوظ ففي عام ١٩٦٠ امتلك الاتحاد السوفيتي ما يقل عن عشرة قاذفات باليستية عابرة للقارات، وبحلول عام ١٩٦٥ بلغ حجم تلك القاذفات ٢٢٦ قذيفة، ثم استمر الرقم في التصاعد إلى أن وصل حجم تلك القذائف حوالي ١٤٣٤ بحلول عام ١٩٧٠، وفي نهاية السبعينيات استبدل الاتحاد السوفيتي البالستية من نوع SS–6/7/9، بصواريخ باليستية عابرة للقارات أكثر قدرة من نوع SS–17/18/19، وتميزت الصواريخ الباليستية السوفيتية بالعمل بالوقود السائل وكبر حجمها، واتقن السوفيت سهولة نشرها، ما جعلهم متقدمين على الولايات المتحدة في استخدام تلك التكنولوجيا. [٦]

واستكمالاً لما سبق لوحظ أن التحديث النووي السوفياتي في مجالات أخرى مهدد بنفس القدر، ففي عام ١٩٦٠ لم يكن لدى الاتحاد السوفيتي نظام إطلاق الصواريخ الباليستية من الغواصات والذي يُطلق عليه "SLBM" وفي عام ١٩٧٠ بلغ حجم تلك الغواصات أكثر من ٧٠٠ غواصة، وكان النوع SLBM SS–N–8 الجديد يبلغ ما يقرب من ثلاثة أضعاف مدى SS–N–6 الأقدم، وفي عام ١٩٨٠ دخلت SS–N–18 مع عشرة مركبات محملة ذات نظام استهداف مستقل، ومهد هذا السباق الطريق لأزمة في أواخر السبعينيات، كان الصاروخ الباليستي الجديد SS–20 ذو المدى المتوسط (IRBM) ، المسلح بثلاث صواريخ MIRV دقيقة ، أكثر قوة من الصواريخ (SS–4) و (SS–5) القديمة التي حلت محلها، ومع تولي ريجان رئاسة الولايات المتحدة خلفًا لجيمي كارتر، أثر في أحاديثه جدية التعامل مع الاتحاد السوفيتي باعتباره المسئول عن الاضطرابات التي وقعت في العالم نتيجة رفضه القبول بمكانة القوة العادية وانفراد الولايات المتحدة بالقوى العظمى والنظام أحادي القطبية. [٧]

وكانت التحديثات العسكرية السابقة نتيجة الثورة الصناعية الثالثة والتي تفجرت في سبعينيات القرن الماضي وأثرت بشكل كبير في مجال تكنولوجيا السلاح، والذي نتج عنه طرح نظريات تدعى إمكانية الانتصار في الحروب التقليدية برغم استحالتها في الحروب الشاملة، وظهر ذلك من خلال التطور التكنولوجي الذي حدث في نظم الأسلحة النووية والإنذار المبكر والمراقبة والاستطلاع، والتي عملت على تضليل الرادارات والدقة في إصابة الأهداف بعد أن كان يفشل معظم الصواريخ في ضرب الأهداف بدقة، كذلك التوجيه الذاتي والذي استُحدث فيما بعد في تصنيع الطائرات بدون طيار وكانت تلك التطورات ذات تأثير بالغ في نظم الإنذار المبكر، والتي اعتمدت على استخدام الأشعة تحت الحمراء في رصد الصواريخ، إلى جانب صناعة الأقمار الصناعية، والبدء في حرب النجوم. [٨]

ولم تكن العلاقات السوفيتية الأمريكية فترة حكم ريجان تتسم بالهدوء أو السلام البارد، بل كما أطلق عليه الزعيم السوفيتي أنها أيديولوجية عسكرية اجتاحت واشنطن، إلا أن تلك الأيديولوجية سيطرت على الإدارة الأمريكية وحدها ولم تكن معبرة عن جموع الشعب الأمريكي، فبعد قيام الولايات المتحدة بنشر صواريخ نووية على الأراضي الأوروبية قامت مظاهرات عديدة في البلدان الأوربية كألمانيا الغربية وفرنسا، وفي يونيو ١٩٨٢ قامت مظاهرة أمريكية بولاية نيويورك لنبذ سباق التسلح النووي، وقادت تلك المظاهرة "المجلس العالمي للكنائس" الذي دعا الدول للتخلي عن الأسلحة النووية، وقامت مجموعة "أطباء من أجل المسئولية" بترويج نموذج محاكاة لما سيترتب على ضرب قنبلة نوية بقدرة واحد ميجا طن، وما سيتبعه من موت مليون شخص، ناهيك عن الشتاء النووي والذي يؤدي إلى وفاة العديد من الكائنات، وأثر الرأي العام الأمريكي في التوجهات في السياسة الخارجية الأمريكية، وذلك بعد أن دعا الرأي العام أو بالأحرى تراجع عن استخدام القوة العسكرية وسباق التسلح بشكل دائم وغير محدد في السياسة الخارجية وبخاصة ضد الاتحاد السوفيتي. [٩]

ومع تولي "جورباتشوف" الحكم في الاتحاد السوفيتي، تطلع إلى التقارب مع الغرب، وكان لجورباتشوف قناعة مفادها أن سباق التسلح يعود على بلاده بالضرر، إذ يزيد من عبئها الاقتصادي، وأن الوسائل السياسية هي العامل الفعال لتحقيق الأمن لا الوسائل العسكرية، واعتمد الزعيم السوفيتي المنفتح على أن السوفيت لديهم ترسانة نووية تحقق لهم قدرًا كبيرًا من الحماية القومية لاعتمادها على مفهوم الردع، لذلك شارك الرئيس "إدوارد شيفرنادزه" هدف أسمى وهو التخفيض المشترك للأسلحة النووية بالاتفاق مع الولايات المتحدة، لوقف سباق التسلح، وكانت أفكار الزعيم السوفيتي محل إعجاب من الدوائر السياسية في المعسكر الغربي، فريجان المعروف عنه التأكيد على أهمية التفوق العسكري الأمريكي وجد زعيمًا سوفيتيًا يسعى لإرجاء الأيديولوجية الشيوعية عن السياسة الخارجية، ويقدم تنازلات تتعلق بالأسلحة التقليدية، وهو ما أجبر ريجان في النهاية على التخلي عن توجهاته وآرائه عن الشيوعية والعمل مع الزعيم الأخير للاتحاد السوفيتي

خاصة فيها يتعلق بالأسلحة النووية وتوحيد ألمانيا من جديد، والتي اعتبرت نهاية للحرب الباردة بين الولايات المتحدة والاتحاد السوفيتي، وهو ما تأكد عليه من خلال انهيار الاتحاد السوفيتي وتفككه عام ١٩٩١. [١٠]

ثانيًا: سباق التسلح بعد إنتهاء الحرب الباردة

بعد انتهاء الحرب الباردة وانهيار الاتحاد السوفيتي وتفككه إلى ١٥ دولة، ورثت روسيا الاتحادية النصيب الأكبر من الترسانة النووية السوفيتية والمقعد الدائم بمجلس الأمن، وعانت روسيا فترة التسعينيات من أزمات اقتصادية خلفتها سياسة الاعتماد التي انتهجها الاتحاد السوفيتي فكانت الدول المنضمة للاتحاد تعمل بشكل مشترك، ثم بعد ذلك انفصلت لتجد روسيا نفسها أمام عقبات اقتصادية وزادت من حدتها الحرب الروسية الشيشانية ديسمبر ١٩٩٤– أغسطس ١٩٩٦، وقبل انهيار الاتحاد السوفيتي بخمسة أشهر بدأت الدولتان في اجراء المباحثات حول سباق التسلح. [١١]

واستكمالاً لما سبق فقد نتج عن هذه المباحثات معاهدة الحد من الأسلحة الاستراتيجية بين الولايات المتحدة والاتحاد السوفيتي "ستارت ١"، والتي وقعت بين الرئيس الأمريكي "جورج بوش" والزعيم السوفيتي الأخير جورباتشوف في ١ يوليو ١٩٩١، وتضمنت المعاهدة وضع حد للأسلحة الاستراتيجية في كلا الدولتين، وأكدت على الاحتفاظ بالمركبات الإيصال موزعة بين القوات المختلفة بعدد ١٦٠٠ وسيلة، والاحتفاظ بعدد ٦ آلاف راس نووي لكل من الجانبين، والاحتفاظ بحوالي ١٥٤٠ رأس حربي عابر من الطائرات إلى جنب عدد ١١٠٠ رأس حربي على الصواريخ المتحركة، وعمدت المعاهدة إلى تساوي الأسلحة لكلا الجانبين، إلى جانب اجراء تفتيش دوري على المواقع العسكرية لضمان الالتزام بالمعاهدة، واعتُبرت تلك المعاهدة في صالح الولايات المتحدة لأنها تلزم الاتحاد السوفيتي بمنع توجيه صواريخ للمدن الأمريكية وهو ما استمر في التهديد به قبل المعاهدة، ودخلت المعاهدة حيز التنفيذ في عام ١٩٩٤، وتم تخفيض الرؤوس النووية في ٢٠٠٣ إلى ما بين ٣٠٠٠ و ٣٥٠٠ رأس نووي بعد أن نصت الاتفاقية على تخفيضها إلى ٦ آلاف رأس نووي لكل دولة، تم الاتفاق على أن تستمر هذه المعاهدة حتى عام ٢٠١٠. [١٢]

وفي ضوء ما سبق، تميزت فترة التسعينيات بالهدوء النسبي في العلاقات بين الولايات المتحدة ودول الاتحاد السوفيتي السابق –عدا روسيا والتي شابها بعض التوترات السياسية– ففي مارس ١٩٩٢، وقعت الولايات المتحدة وروسيا و٢٥ دولة أخرى على معاهدة الأجواء المفتوحة والتي تسمح للأعضاء بإجراء رحلات استطلاعية محددة فوق أراضي الدول المنضمين للمعاهدة، وأعلنت كلا من بيلاروسيا وكازاخستان وأوكرانيا في بروتوكول لشبونة المكمل لمعاهدة ستارت ١ التخلي عن أسلحتها النووية التي ورثتها عن الاتحاد السوفيتي، والتزمت تلك الدول بنقل الترسانة النووية إلى روسيا والانضمام

لمعاهدة حظر انتشار الأسلحة النووية كدول غير حائزة، وقامت الولايات المتحدة في إطار ذلك بتقديم مليارات الدولارات لتمويل عملية نزع السلاح النووي، وتم تسليم كافة الأسلحة لروسيا في نهاية عام ١٩٩٦، كما تم التوقيع على معاهدة ستارت ٢ بداية عام ١٩٩٣، والتي هدفت إلى الحد من الأسلحة النووية التي يمكن للأطراف امتلاكها إلى ٣٥٠٠، وصدق مجلس الشيوخ الأمريكي على المعاهدة عام ١٩٩٦، وصدق الدوما الروسي عام ٢٠٠٠، وفي عام ٢٠٠١ فرضت الاتفاقية قيودًا على الطرفين، والتي تضمنت الآتي: [١٣]

- عدم تجاوز العدد ٣٥٠٠ فيما يخص إجمالي للرؤوس الحربية الاستراتيجية المنشورة.
- عدم تحميل أي رأس حربي على الصواريخ الباليستية العابرة للقارات أو الثقيلة ذات قدراتMIR .
- عدم نشر صواريخ بالستية عابرة للقارات مزودة بقدرات MIRV.
- لا يُنشر أكثر من ١٧٥٠ رأسًا حربيًا على الصواريخ الباليستية التي تطلق من الغواصات.

وقد نتج عن عملية العولمة تداعيات على العلاقات الدولية منذ نهاية الحرب الباردة، والتي كان منها تقليل المسافات وزيادة التأثيرات الاقتصادية واتساع الفجوات في قوة الدولة والتي تضمنتها القوة الاقتصادية والسياسية والعسكرية، إلى جانب قوى مشابهة لها ذات تأثير غير قليل، وانعكست كل تلك الأمور على تطوير مفهوم الحرب التقليدية، والتي نتج عنها اتساع النطاق الجغرافي أو الموضوعي لتلك الحرب، والتي قد تتمثل في الحروب الإلكترونية أو الإعلامية، وبالتالي لن يكون لها مسرحًا محددًا، كذلك زيادة عدد الفاعلين من غير الدول والتي نشطت في نهاية القرن الماضي وبداية القرن الحالي، لتشمل شركات دولية وتنظيمات مسلحة وغير مسلحة، وحقق امتلاك التكنولوجيا بشكل عام للفاعلين الدوليين سواء أكانوا دولًا أو غير دول ميزة نسبية في القدرة على التأثير على الحروب التي تخوضها، القدرة على التحكم في مجريات الحرب، وكشف القدرات التي يمتلكها الخصوم، والتأثير المباشر في الرأي العام داخل الدولة الخصم. [١٤]

وبدأت الدول في التوجه نحو الهجمات السيبرانية للتأثير على الداخل في الدولة المستهدفة، وذلك لارتفاع تكلفة النتيجة المحققة من الحروب التقليدية والتي تتشابه نتائجها مع الهجمات السيبرانية، كذلك التوجه نحو هذا النوع من الهجمات لتحقيق لأغراض عدة والتي كان منها على سبيل المثال لا الحصر التأثير لمباشر في قارات الحكومة في الدولة المتأثرة بالهجمات السيبرانية نتيجة حشد الرأي العام تجاه قضية معينة، أو توجيه هجمات سيبرانية إلى النظام المالي والمصرفي للدولة المستهدفة، بغرض تعطيل العمل لفترات قد تستمر أسابيعًا، كتعرض المؤسسات المالية في الولايات المتحدة عام ٢٠١٢ إلى هجوم سيبراني

استهدف بنك أمريكا (Bank of America)، وموقع بنك سيتي جروب (Citi Group)، بغرض تعطيل المواقع الإلكترونية ، وبعد تحقيق دام أربع سنوات كشفت المصادر الأمريكية عن سبعة متسللين متمرسين عملوا نيابة عن الحكومة الإيرانية. [١٥]

المبحث الثاني

الحروب الإلكترونية كوسيلة لتحقيق أهداف السياسة الخارجية الروسية

تعتبر الحروب السيبرانية من أهم التطورات في مجال الحرب والأمن القومي، حيث تستخدم التكنولوجيا والشبكات الإلكترونية للهجوم على أهداف معينة، وقد اعتبرت روسيا واحدة من الدول التي نجحت في استخدام هذه الأساليب بشكل فعّال.

أولاً: مفهوم التدابير ما دون الحربية في السياسة الخارجية الروسية وأهميتها

بعد انتهاء الحرب العالمية الأولى وما شهده العالم من تطور في مجال نقل المعلومات وتكنولوجيا الاتصالات، وسهولة عمل أجهزة الاستخبارات، أدت كل هذا التطور إلى التغيير في طبيعة وخصائص الحرب التقليدية العسكرية التي تقوم على الاقتتال بين طرفين، ومحاولة طرف غزو الطرف الآخر والسيطرة على جزء من أراضيه، بل أصبحت تقوم باستخدام وسائل ومعدات سيبرانية في المحيط والمجال السيبراني، حيث المعلومات الرقمية وأجهزة الكمبيوتر وبرامجها وشبكات الاتصال والإنترنت، حيث تعتبر الحروب الإلكترونية محاولة اختراق من دولة إلى أخرى من خلال الشبكات وأجهزة الكمبيوتر، كما أنها تمتاز بأن تلك الحرب هي حرب في الفضاء الإلكتروني، مثل أعمال التخريب الإلكتروني أو القرصنة الإلكترونية مثل حذف ملفات، اختراق أجهزة وتهكير الصفحات، وتعديل بعض البيانات بما يؤثر في صحة الملفات والبيانات، بحيث يجعلها مغلوطة. [١٦]

وفي سياق ما تقدم، هناك فروق جوهرية بين الحروب التقليدية والحروب الإلكترونية بصفة عامة، والتي تنطبق على الحروب بنوعيها في سياسة روسيا الخارجية، وقد حاول الباحث إجمال تلك الفروق في التالي:

أولاً: تقوم مجموعة عسكرية رسمية بالحروب التقليدية الروسية مثل الجيوش، القوات المسلحة، أو المجموعات الخاصة، على عكس الحروب الإلكترونية الروسية والتي يقوم بها أعضاء غير معروفي الهوية، وأيضاً أشخاص غير رسميين، وغير معلنين جنسياتهم أو أسبابهم. [١٧]

ثانيًا: تعتمد الحروب التقليدية الروسية على القوة العسكرية مثل مدى جاهزية الجيوش، حجم المعدات ومدى تطورها، أنواع الأسلحة البرية والجوية والبحرية، وأيضا عدد القوات الاحتياطية الروسية، كما تعتمد على القوة الاقتصادية للدولة الروسية، أما الحروب الإلكترونية الروسية فيقوم بها عدد قليل جدا من الأشخاص المدربين جيدا باحترافية. [١٨]

ثالثًا: مدى تأثير الحروب التقليدية الروسية كان يعتمد على محددات متعددة، لكنها وقبل بداية الحرب لا يمكن ضمان نتيجة الحرب ومدى تأثيرها على أرض الخصم بشكل كامل وحسمي، لكن الحروب الإلكترونية الروسية تكون حروب نوعية على أهداف معينة، هجمات فريدة ويكون محددة بدقة أين يقع التأثير، مدة التأثير، مع عدم وضوح من الفاعل ومن الذي قام وتسبب في الاختراق. [١٩]

رابعًا: تقوم الحروب التقليدية الروسية بشكل أساسي على ميزانية مستقلة وكبيرة، وذلك لبناء المعدات العسكرية مثل الصواريخ، الطائرات، الدبابات، المدافع، الأسلحة الخفيفة، أو بناء شراء تلك المعدات العسكرية، بينما تحتاج الحروب الإلكترونية الروسية لميزانية كبيرة هي الأخرى، ولكنها ليست بضخامة ميزانية الحروب التقليدية وذلك بغية إعداد الخبراء والفنيين ومجموعة الهاكر، وشراء المعدات الإلكترونية.

خامسًا: تحتاج الحروب التقليدية الروسية إلى مناطق واسعة وشاسعة للقيام بعمليات مناورة من أجل عدم الخضوع لإرادة العدو، وقد تلجئ في ذلك إلى استخدام أراضي دولة أخرى للقيام بهجمات عسكرية على العدو في كثير من الأحيان، أما في الحرب الروسية الإلكترونية فلا حاجة لها إلى مساحات كبيرة أو صغيرة، بل فقط جهاز إلكتروني ومجموعة متخصصة وماهرة تقوم بجمع البيانات، ومن ثم استخدام تلك المعلومات والقيام بهجوم عبر الفضاء الإلكتروني على العدو. [٢٠]

سادسًا: اختلفت أهداف الحروب التقليدية الروسية عن أهدف حروبها الإلكترونية، حيث تقوم الحروب التقليدية الروسية باستهداف المناطق العسكرية خاصة، لأنها بين طرفين أو جهازين عسكريين محددين، بينما هدفت الحروب الإلكترونية الروسية إلى التأثير في البنية التحتية، مثل شركات الكهرباء والنقل العام ومؤسسات الطاقة والنظام المالي والنظام الصحي والمؤسسات النفطية. [٢١]

سابعًا: تختلف الحروب التقليدية الروسية عن الإلكترونية من ناحية مدة وزمن الحروب طالت أو قصرت، فالدول المعتدية بصفة عامة عند غزوها أو اعتدائها على دولة أخرى غالبا ما تضع خطة للغزو وكيفية التراجع والانسحاب، أما الحروب الإلكترونية الروسية فهي وقتية.

وفي سياق متصل، فإن الحروب الإلكترونية هي نوع من الحروب تدور في الفضاء الإلكتروني، حيث تتم المعارك والاشتباكات بين الأطراف المتنازعة عبر الشبكة العنكبوتية وأنظمة الحاسوب، ويكون هدف تلك الهجمات إما اختراق أنظمة المعلومات والتكنولوجيا، أو تعطيل أحد البرامج أو البنية التحتية، ومن ثم فأن أهمية الحروب السيبرانية بالنسبة للدولة الروسية تكمن في تحقيق الأهداف التالية:

١ ـ الأمن القومي

تلعب الحروب السيبرانية دورا حاسما في حفظ أمن الدول وحماية مصالحها، فهي تساهم في الحماية من الهجمات الإلكترونية المتطورة التي يمكن أن تستهدف البنية التحتية للدولة وأنظمتها الحيوية مثل الحكومة والبنوك والقطاع الصناعي، فإن الحكومة الروسية تمتلك جهاز Malwar، حيث يوفر البرنامج حلاً شاملاً للأمان، كما يقدم حماية ضد جميع أنواع البرامج الضارة، بما في ذلك الفيروسات وأحصنة طروادة وبرامج التجسس وبرامج الفدية والتهديدات الأخرى، ويساعد في توفير الحماية في الوقت الحقيقي وماسح ضوئي للكشف عن التهديدات. [٢٢]

٢ ـ الحماية الاقتصادية

يعتبر القطاع الاقتصادي هدفًا رئيسيًا للهجمات السيبرانية، حيث يمكن تعطيل الشركات والمؤسسات وسرقة المعلومات التجارية الحساسة، وبالتالي فإن حماية القطاع الاقتصادي من الهجمات السيبرانية تعزز الاستقرار الاقتصادي وتمكن التحول الرقمي، حيث تستهدف الدول المعادية المناطق والقطاعات الحساسة داخل الدول، مثل استهداف شركات النفط والتعدين، والشركات ذات العلاقة بالأمن القومي، لأن اقتصاد الدول قائم عليها مثل شركات أرامكو السعودية. [٢٣]

٣ ـ الجوانب العسكرية

تلعب الحروب السيبرانية دورا هاما في مجال الدفاع العسكري، حيث يمكن استخدامها لزيادة القدرة الهجومية والدفاعية للجيوش، وتشمل التكتيكات السيبرانية الهجمات على أنظمة القيادة والتحكم والتجسس الإلكتروني على الدول الأخرى، من خلال تدريب جاهز المخابرات السوفيتي KGP، أيام الحرب السوفيتية للعديد من المتطوعين والضباط، للتسلل داخل الشركات والهيئات والمؤسسات الغربية في محاولة سوفيتية لمعرفة المعلومات والتكنولوجيا الغربية، والقيام بصد وردع تلك الخطط العسكرية والمعلوماتية والتجهيز لمحاولة هجومية غير اعتيادية ضد الغرب. [٢٤]

٤ ـ الحفاظ على السلم والاستقرار

بوجود قوانين دولية متعددة الأطراف تحظر استخدام تكنولوجيا المعلومات في الأعمال العدائية، تُعَد الحروب السيبرانية وسيلة فعالة للحفاظ على السلم والاستقرار بين الدول من خلال الردع، منذ عام ٢٠١٠ وبدأت الدول بصفة عامة، وروسيا بصفة خاصة استخدام الحروب السيبرانية، ومن ثم تعمل الدول على زيادة تطور تكنولوجيتها لردع تلك الهجمات، علاوة على ذلك، تلعب الحروب السيبرانية أيضًا دورًا هامًا في الكشف عن واحتواء الهجمات السيبرانية وتحديد مصادرها ومحاسبة المسؤولين عنها، هذا يساهم في ردع الأعمال العدائية عبر الإنترنت وتقليل الانتهاكات السيبرانية التي يمكن أن تؤثر سلبًا على الاستقرار والسلم العام. [٢٥]

٥ ـ التجسس والاستخبارات

يمكن استعمال الحروب السيبرانية في تجميع المعلومات والتجسس على الأطراف الأخرى، وهو جانب مهم في مجال الأمن القومي للدول، وتستخدم الحكومات والجهات الاستخباراتية الحروب السيبرانية و الإلكترونية لاختراق أنظمة الحوسبة والشبكات الخاصة بالأهداف المحددة وسرقة المعلومات الحساسة والسرية، ويمكن استخدام التجسس السيبراني للوصول إلى معلومات الحكومات والشركات والأفراد ونقلها إلى الأطراف الأخرى، وتشمل أنشطة استخباراتية سيبرانية أخرى اختراق شبكات الاتصالات وجمع المعلومات عن الأعداء المحتملين وتتبع الأنشطة المشبوهة عبر الإنترنت، ويمكن أيضًا استخدام الحروب السيبرانية لزرع البرامج الخبيثة والتلاعب بالبيانات المصيبة وتعطيل الأنظمة الحاسوبية والبنية التحتية للأعداء. [٢٦]

ثانيًا: الحروب الإلكترونية كأداة في السياسة الخارجية الروسية ووكلائها

يعتبر استخدام الحروب السيبرانية تكتيكًا يُستخدم على نطاق واسع في العالم، وليست روسيا هي الدولة الوحيدة التي تنتهج هذه الاستراتيجية، وبالعودة إلى تاريخ استخدام السوفييت لتلك الآلية نجد أنه بعد سقوط الاتحاد السوفيتي بعد الحرب الباردة ١٩٩١ وسيطرة الغرب وخاصة الولايات المتحدة على النظام العالمي الذي أصبح أحادي القطبية، أدركت روسيا أن الصراع العسكري التقليدي في مواجهة الغرب مكلف وغير مجدي وذلك بسبب التطور العسكري في الغرب، لذلك قامت روسيا بتطوير مجموعات مدربة للقيام بحروب سيبرانية في الدول الغربية بدلا من الحروب العسكرية، وقد اعتبرت الحرب الباردة بين السوفييت والأمريكان، هي أول حرب تم استخدام الحرب السيبرانية بها، حيث عمل أهم جهاز في الاتحاد السوفيتي سابقا، وهو المخابرات السوفيتية KGP في ١٩٨٢، على سرقة المعلومات والتكنولوجيا الغربية

الحديثة عن التكنولوجيا السوفيتية، وتم تسمية هذه العملية باسم Line X، حيث دربت المخابرات الروسية العديد من الأفراد لكي يقوموا بالتسلل داخل الشركات والوكالات الغربية حتى يستطيعوا جلب المعلومات للاتحاد السوفيتي وبالتالي استخدام تلك المعلومات ضد المخططات الأمريكية. [٢٧]

وفي سياق ما سبق قامت الحروب الروسية الإلكترونية من خلال وكلاء لها ومنظمات غير حكومية وغير رسمية، كما كان هناك العديد من التنظيمات الروسية الخاصة التي تعمل في المجال السيبراني لصالح الحكومة والمخابرات الروسية، نذكرها كالتالي:

١. منظمة Fancy Bear

استخدمت روسيا هذه المنظمة في هجوم روسي على أهداف ومواطنين أمريكيين عام ٢٠١٨، حيث تم استهداف قطاع الطاقة الأمريكي، وتم استهداف موقع Microsoft office 365 لبعض المواطنين الأمريكان، وتم نشر البيانات التي حصلت عليها تلك المجموعة من برنامج الأوفيس، وكان هذا الهجوم الروسي من خلال تلك المنظمة الموجودة على الأراضي الأمريكية، بسبب حظر اللجنة الأولمبية الدولية روسيا من الاشتراك في تلك الألعاب بسبب استخدام الروس المنشطات لتحفيزهم داخل المباريات. [٢٨]

٢. منظمة Sandworm

هي إحدى المنظمات التابعة لوكالة المخابرات العسكرية الروسية GRU، وتعمل من خلال استهداف البنية التحتية للدول، حيث استهدفت روسيا من خلال تلك المنظمة شبكة الكهرباء الأوكرانية في عام ٢٠١٥ و٢٠١٦، حيث تم انقطاع الكهرباء على حوالي ربع مليون أوكراني، لساعات عديدة خلال الغزو الروسي لشبه جزيرة القرم وما بعد الغزو، ونشرت روسيا فيروس Not Petya في أوكرانيا ثم العالم أجمع، مما أدى إلى خسائر مادية حوالي ١٠ مليار دولار، ويعمل هذا الفيروس على سرقة المعلومات وبث المعلومات غير الصحيحة. [٢٩]

٣. منظمة Callisto Group

ترتبط هذه المنظمة بجهاز وكالة المخابرات العسكرية الروسية GRU، حيث إنها منظمة هاكرز متقدمة ومعروفة بأنشطتها في مجال القرصنة الإلكترونية والتجسس السيبراني، وتستخدمها روسيا في عملياتها غير العسكرية في سياستها الخارجية بحيث تحقق رؤيتها في النظام العالمي، وقد ظهرت هذه المجموعة في أواخر عام ٢٠١٥ وبداية عام ٢٠١٦

عندما استهدفت بعض الأشخاص الدوليين، من خلال إرسال رسائل بريد إلكتروني تصيد احتيالي عالية الاستهداف تحتوي على مرفقات ضارة، كما تحتوي على البرمجيات الخبيثة، التي تعمل على الوصول إلى المعلومات والبيانات ثم سحب تلك المعلومات. [٣٠]

٤. منظمة UNC2589

تدخل تبعية هذه المنظمة لوكالة المخابرات العسكرية الروسية GRU، وكان الهدف من إنشائها توجيه ضربات واستهداف الشركات الغربية في الدول الأوروبية وأمريكا وكل الدول الأعضاء في حلف شمال الأطلنطي، حيث تقوم هذه المنظمة بإرسال رسائل تشفيرية معاد توجيهها وهذه الرسائل تحمل معها فيروس يمكن تلك المنظمة من الحصول على المعلومات واستخدامها، وقد كان جدير بالذكر أن نشاطات هذه المنظمة تخريبية مدمرة، وتؤدي إلى وفيات في الدولة المعتدى عليها، فهذه المنظمة لا تقوم فقط على أنشطة إلكترونية بعيدة عن الدماء، لكن أحد أنشطتها هي قتل الأفراد. [٣١]

٥. منظمة Gamaredon Group

تم إنشاء هذه المنظمة في عام ٢٠١٣، وهي منظمة تقوم الدولة الروسية برعايتها، و تستخدمها في تحقيق وتنفيذ استراتيجيتها الدولية في السياسة الخارجية، وقد استخدمت روسيا هذه المنظمة من في القيام بعملية تجسس على أوكرانيا منذ ٢٠١٣ حتى تم اكتشاف هذه المحاولة في ٢٠١٦، حيث تم استهداف الحكومة الأوكرانية، الجيش الأوكراني، والمحاكم الأوكرانية التي كانت تصف روسيا بأنها دولة إرهابية تسعى لتدمير العالم، خاصة بعد الغزو الروسي لشبة جزيرة القرم، وقد قامت روسيا بهذه الهجمات كنوع من السيطرة والتحكم والديكتاتورية ليس فقط في الداخل، لكن أيضًا خارجيًا. [٣٢]

٦. منظمة Pushcka

تعمل المنظمة تحت رعاية وكالة الاستخبارات الروسية GRU، وتعتبر هذه المنظمة من أهم المنظمات التي تمارس روسيا بها ضغطا على الشعوب في الدولة المعتدية مما يؤثر على الأمن القومي لتلك الدول، حيث تم استخدام هذه المنظمة بعد الغزو الروسي لأوكرانيا في فبراير ٢٠٢٢، حيث عملت روسيا بعد اشتداد الحرب على محاولة التأثير على المواطنين الأوكرانيين والجيش الأوكراني، من خلال بث ١٤٠٠٠ رسالة إلكترونية مشفرة، بحيث يتم اختراق الأجهزة الحاسوبية ويتم مسح الأقراص والملفات على تلك الأقراص. [٣٣]

٧. منظمة Killnet:

تتميز هذه المنظمة بتخصصها في الأعمال السيبرانية والقرصنة، حيث تعتبر هذه الشركة خاصة تعمل في الأعمال الإلكترونية والمهارات السوداء، والكشف عن مرتبات العملاء المستهدفين، الدعم الفني، العلاقات العامة، تحليل البيانات وجمعها، واستخدام واستعمال النتائج ضد المستهدفين سواء كانوا دول أو أفراد، وتعمل على دعم المخابرات والمؤسسات الروسية حيث إنها أحد المنظمات التابعة لوكالة المخابرات الروسية. [٣٤]

الخاتمة:

تعتبر الحروب المسلحة القائمة على القوة العسكرية من الأليات الهامة التي قد تلجاء إليها الدول وتستخدمها في سياستها الخارجية من أجل بلوغ أهدافها، ونظراً للتطور التكنولوجي الذي شهده العالم انتقل مفهوم تلك الحروب من معناها التقليدي القائم على أساس استخدام القوة الصلبة إلى استخدام نوع جديد عرف بأسم الحروب الإلكترونية، والتي كانت روسيا من ضمن الدول التي استخدمتها ووظفتها في سياستها الخارجية من أجل تحقيق أهدافها، وقد استثمرت روسيا نفوذها في المجال التكنولوجي في تنفيذ بعض الهجمات السيبرانية ضد الدول الأخرى تأكيداً لسياستها الخارجية الداعية إلى عالم متعدد الأقطاب. وفي إطار ما سبق خلصت هذه الدراسة إلى عدد من النتائج كان أهمها:

- أن الحروب السيبرانية هي نوع من الحروب التي تدور في الفضاء الإلكتروني، حيث تتم المعارك والاشتباكات بين الأطراف المتنازعة عبر الشبكة العنكبوتية وأنظمة الحاسوب، ويكون هدف تلك الهجمات إما اختراق أنظمة المعلومات والتكنولوجيا، أو تعطيل أحد البرامج أو البنية التحتية، ومن ثم فأن أهمية الحروب بالنسبة للدول تكمن في كونها تحقيق أهداف لهذه الوحدات كحفظ أمنها وحماية مصالحها.
- أن التطور في مجال نقل المعلومات وتكنولوجيا الاتصالات، وسهولة عمل أجهزة الاستخبارات، أدت إلى التغيير في طبيعة وخصائص الحرب التقليدية العسكرية التي تقوم على الاقتتال بين طرفين، ومحاولة طرف غزو الطرف الآخر والسيطرة على جزء من أراضيه، وأصبحت تقوم باستخدام وسائل ومعدات سيبرانية في المحيط والمجال السيبراني، حيث المعلومات الرقمية وأجهزة الكمبيوتر وبرامجها وشبكات الاتصال والإنترنت.
- أن استخدام الحروب السيبرانية كان تكتيكًا يُستخدم على نطاق واسع في العالم، ولم تكن روسيا هي الدولة الوحيدة التي انتهجت هذه الاستراتيجية، وقد تمكنت روسيا من خلال استخدام التدابير ما دون الحربية والعسكرية في

تحقيق سياستها واستراتيجيتها الخارجية في النظام العالمي حيث عملت روسيا على تعزيز قدراتها السيبرانية، واستخدامها كبديل عن الحروب العسكرية المكلفة للتأثير في النظام العالمي.

- أن سقوط الاتحاد السوفيتي بعد الحرب الباردة ١٩٩١ وسيطرة الغرب وخاصة الولايات المتحدة على النظام العالمي الذي كان سبب من ضمن اسباب لجوء روسيا إلى استخدام الحروب السيبرانية في سياستها الخارجية، كما أن الإدراك الروسي لمدى كلفة وعدم جدوى الصراع العسكري التقليدي في مواجهة الغرب بعد انهيار الاتحاد السوفيتي كان من ضمن اسباب قيام روسيا بتطوير مجموعات مدربة للقيام بحروب سيبرانية في الدول الغربية بدلا من الحروب العسكرية.

الهوامش

[١] محمد تيسير، نبذة حول المنهج الوصفي التحليلي، المؤسسة العربية للعلوم ونشر الأبحاث، فبراير ٢٠٢٣.

[٢] نورهان الشيخ، نظرية العلاقات الدولية، المكتب العربي للمعارف، القاهرة، الطبعة الأولى، ٢٠١٨، ص١٥١.

[3] Council on foreign Relations, U.S.-Russia Nuclear Arms Control, 2021, Obtained 25/8/2023, Available at the following link: https://www.cfr.org/timeline/us-russia-nuclear-arms-control

[4] International Atomic Energy Agency, Creation of the International Atomic Energy Agency, 2020, Obtained 25/8/2023, Available at the following: https://www.iaea.org/about/overview/hist

[٥] جون جي ميرشايمر، **لماذا يكذب القادة؟: حقيقة الكذب في السياسة الدولية**، ترجمة غانم النجار، المركز الوطني للثقافة والفنون الآداب، الكويت: الطبعة الأولى ٢٠١٦، ص ٤٩.

[6] Helen Bury, **Eisenhower and the Cold War Arms Race: 'Open Skies' and the Military-Industrial Complex**, England: I.B. Tauris, 2014, p 168-169.

[7] Timothy Hoyt, "The United States and the Cold War Arms Race", Thomas Mahnken and other (Editor), **Arms Races in International Politics: From the Nineteenth to the Twenty-First Century,** United Kingdom: Oxford University, 2016 p 151.

[8] Timothy Hoyt, "**The United States and the Cold War Arms Race**", Loc.Cit**.**

[٩] عبد المنعم سعيد، **أمريكا والعالم: الحرب الباردة.. وما بعدها**، نهضة مصر، القاهرة، الطبعة الأولى ٢٠٠٣، ص ٨٤-٨٥.

[١٠] جيه ما كمان، **الحرب الباردة: مقدمة قصيرة جدًا**، ترجمة فتحي خضر، مؤسسة هنداوي، المملكة المتحدة، الطبعة الأولى ٢٠١٧، ص ١٤٩-١٥١.

[11] Archie Brown, **The Cold War Didn't Have to End. Gorbachev Made It Happen**, Time, AUGUST, 2022, Obtained 25/8/2023, Available at the following: https://time.com/6209992/mikhail-gorbachev-end-cold-war/

[١٢] الجزيرة، سقوط الاتحاد السوفياتي.. الأسباب والنتائج، بدون تاريخ، تاريخ الدخول ١٠/٨/ ٢٠٢٣، متوفر على الرابط التالي، https://shorturl.at/ipwGZ

[13] John Swift**,** The Soviet American Arms Race, History Today, March 2009, Obtained٢٠٢٣/٨/١٩ , Available at the following: https://www.historytoday.com/archive/soviet-american-arms-race

[14] Center for Arms Control and Non-Proliferation, Strategic Arms Reduction Treaty II, November 2022, Obtained 25/8/2023, Available at the following: https://armscontrolcenter.org/strategic-arms-reduction-treaty-ii/

[١٥] دلال محمود السيد، **تحولات الحرب التقليدية.. تصور في الأدوات أم تغير مفاهيمي؟**، القاهرة، مجلة السياسة الدولية، العدد ٢١١، ٢٠١٨، ص ٦.

[١٦] أحمد زكي عثمان، **تأثيرات القدرات السيبرانية في الصراعات الإقليمية**، القاهرة، مجلة السياسة الدولية، العدد ٢٠٨، ٢٠١٧ ص ١٩.

[17] Don E. Gordon, **Electronic Warfare Element of Strategy and Multiplier of Combat Power,** 1981. Chapter 3.

[١٨] قاسم خضير عباس، **"ديناميكيات الحروب الالكترونية وأثرها في الصراع الدولي"**، المركز الديمقراطي العربي، ٢٠٢١.

[19] Barry R. Posen, **The Sources of Military Doctrine,** Cornell Studies in Security Affairs, 1984

[٢٠] سوسن مهنا، **"الحروب السيبرانية وجه قبيح للتطور أم بديل رحيم للآلة العسكرية؟"**، Independentعربي، ٢٠٢٢. تم الحصو عليه في ٢٠٢٣/٨/١٩. متوفر على اللينك الآتي: https://2u.pw/uzdFXKr

[٢١] محمد عاطف إمام، **"الفضاء الإلكتروني وأثرة على الأمن القومي للدول: الحروب الالكترونية نموذجا"**، المركز العربي لأبحاث الفضاء الالكتروني، ٢٠٢٣.

[٢٢] **هل أصبحت الهجمات الإلكترونية بديلا عن الحروب التقليديّة؟"**، المركز الأوروبي لدراسة مكافحة الإرهاب والاستخبارات، ٢٠٢٠.

[٢٣] **بهذه الخطوات تحمي معطياتك من الاختراق"**، تيلي ماروك، ٢٠٢٣. تم الحصول عليه في ٢٠٢٣/٨/١٩، متوفر على الرابط التالي. https://2u.pw/cPMIqme

[٢٤] سعد علي الحاج بكري، **"الحرب السيبرانية وتوجهاتها الاستراتيجية"**، جريدة العرب الاقتصادية الدولية، ٢٠٢١. تم الحصول عليه في ٢٠٢٣/٨/١٩. ومتوفر على اللينك التالي: https://2u.pw/XBKXaS

[٢٥] د. كرار عباس متعب فرج، **الحرب السيبرانية: دراسة في استراتيجية الهجمات السيبرانية بين الواليات المتحدة الامريكية وإيران**، ٢٠٢١. مجلة حمورابي للدراسات، العدد ٤٠، ص١٩٩

[٢٦] أميرة عبد العظيم، **المخاطر السيبرانية وسبل مواجهتها في القانون الدولي**، جامعة الأزهر، مجلة الشريعة والقانون، العدد ٣٥، ٢٠٢٠، ص٣٦٦.

[٢٧] يحيى ياسين سعود، **الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني**، المجلة القانونية، ٢٠١٨، ص ٩٨.

[٢٨] **"الحرب الروسية الجورجية.. ٥ أيام طبعت ذاكرة شعب وفرضت الولاء لموسكو"**، العربي: ٢٠٢٢. تم الحصول عليه في ١٨/٨/٢٠٢٣. متوفر على الرابط التالي https://2u.pw/iXoOIKO

[29] Maxim Shemetov, "**US Indicts Sandworm, Russia's Most Destructive Cyberwar Unit",** Weird, 2020, Obtained 25/8/2023, available at https://2u.pw/HJSg5nn

[30] Ionut Arghire, "**Russian Espionage APT Callisto Focuses on Ukraine War Support Organizations",** Security week, 2022. Obtained 25/8/2023. The link available at https://2u.pw/0HouFhQ

[31] "**Evacuation and Humanitarian Documents used to Spear Phish Ukrainian Entities",** Mandiant, 2022. Obtained 25/8/2023. The link available at https://2u.pw/aPS73Cb

[32] **"The Top 5 Russian Cyber Threat Actors to Watch",** Rapid7, 2022. Obtained 25/8/2023. The link available at https://2u.pw/jB8BF0k

[33]AJ VICENS, **"Hacks, leaks and wipers: Google analyzes a year of Russian cyberattacks in Ukraine",** Cyberscoop, 2023. Obtained 25/8/2023. The link available at https://2u.pw/BcR41aH

[34] **"Black Skills' Is Killnet's Attempt to Form a 'Private Military Hacking Company'",** Flashpoint, 2023. Obtained 25/8/2023. The link available at https://2u.pw/pQq8f5q