الدراسات

الأمن السيبراني في استراتيجية الامن القومي الروسي

نهي علي امير

باحثة متخصصة في الشئون الدولية

ا لملخص :

يعد مفهوم الأمن السيبراني من أهم وأخطر المفاهيم التي تسعى الدول إلى تحقيقيها، والوصول إليها في عالمنا اليوم، لاسيما في ضوء التقدم التكنولوجي الهائل الذي تشهده مختلف مجالات الحياة، فقد كان لهذا التقدم تأثيرًا واضحًا على العلاقات الدولية، وتحديدًا في حالة الصراعات والحروب، حيث ظهر شكل جديد للحروب عرف باسم «الحروب السيبرانية»، والتي باتت تشكل خطرًا عالميًا لا تستثنى منه أي دولة مهما بلغ تقدمها العسكري والاقتصادي والتكنولوجي، ومن ثم فقد أدى ذلك إلى قيام العديد من الدول إلى إعادة النظر في رؤيتها لمفهوم الأمن القومي في محاولة لتضمينه عنصرًا استراتيجيًا جديدًا، وهو العنصر الأمن السيبراني في محاولة منها لمواجهة هذه الحروب والهجمات، وذلك من خلال توظيف إمكانياتها الاقتصادية والتقنية والبشرية.

حيث تطرح روسيا الاتحادية تحت قيادة الرئيس فلادمير بوتين نموذجًا واضحًا كأحد تلك الدول، التي سعت إلى تنمية قدراتها في هذا المجال السيبراني الجديد خلال السنوات القليلة الماضية، وتطويرها كسلاح فعال لمواجهة خصومها ، وفي مقدمتهم الدول الغربية متمثلة في الولايات المتحدة الأمريكية، ودول الاتحاد الأوروبي، بل وفي إدارة تفاعلاتها الدولية والإقليمية.

كلمات مفتاحية: الأمن السيبراني، روسيا، استراتيجيات الأمن القومي، الحروب السيبرانية، الفضاء السيبراني

Abstract:

The concept of cyber security is one of the most important and dangerous concepts that countries seek to achieve and reach in our world today, especially in light of the tremendous technological progress witnessed in various fields of life. This progress has had a clear impact on international relations, specifically in the case of conflicts and wars, where A new form of warfare known as “cyber wars”, which has become a global threat from which no country is excluded, regardless of its military, economic and technological progress. Hence, this has led many countries to reconsider their vision of the concept of national security in an attempt to include a strategic component in it. New, which is the element of cyber security in an attempt to confront these wars and attacks, by employing its economic, technical and human capabilities.

Where the Russian Federation, under the leadership of President Vladimir Putin, presents a clear model as one of those countries, which has sought to develop its capabilities in this new cyber field during the past few years, and develop it as an effective weapon to confront its opponents, led by the Western countries represented in the United States of America, and the European Union countries, Rather, in managing its international and regional interactions.

المقدمة:

لم يعد هناك مجال للشك في أن تأثيرات الثورة التكنولوجية على مجالات الحياة المختلفة، لم تعد قاصرة على التفاعلات المجتمعية والاقتصادية والسياسية فحسب، بل امتدت لتخلق ساحة جديدة للصراعات غير التقليدية، والبعيدة عن ساحات البر والبحر والجو ومنها ساحة "الفضاء السيبراني"، والتي حفزت العديد من الفاعلين من الدول، وغيرها لاستخدامها كأحد أهم أدوات الصراع والتنافس والهيمنة غير التقليدية، وظهر للمرة الأولى مفهوم "الحرب السيبرانية" [1]، والتي وصفها العديد من المحللين بأنها حروب المستقبل، فهي لا تقل خطورة عن الحروب التقليدية من حيث التهديد الذي تنطوي عليه وحجم التدمير الذي يمكن أن تؤدي إليه، لاسيما وأنها تنفذ بأساليب يصعب تتبعها في كثير من الأحيان مثل الهجمات الإلكترونية على أجهزة الحاسبات والشبكات الإلكترونية، والبنى التحتية المعلوماتية، كذلك فلم تعد تلك الحروب والصراعات قاصرة على الفاعلين الدوليين التقليديين «الدول» بل امتد مداها ليشمل فاعلين آخرين مثل شركات تكنولوجيا المعلومات العملاقة، والتي تسيطر بدرجة أو بأخرى على المقومات التكنولوجية، وكذلك المهارات البشرية المدربة على التعامل مع مثل هذه الوسائل.

وعليه، فقد بات واضحًا أن من يملك آليات توظيف تلك البيئة الإلكترونية الجديدة، أو ما يطلق عليه "الفضاء السيبراني" يصبح الأكثر قدرة على تحقيق أهدافه الإستراتيجية، والتأثير في سلوك الفاعلين الآخرين المستخدمين لذلك الفضاء الجديد، بل وفرض هيمنته عليهم من خلاله.

وأصبح صناع القرار في العديد من الدول الكبرى والمتقدمة كالولايات المتحدة الأمريكية ودول الاتحاد الأوروبي وروسيا والصين والهند وغيرها، يصنفون الأمن السيبراني كأولوية في استراتيجيات سياساتهم الدفاعية الوطنية، حيث أعلنت أكثر من 130 دولة عن تخصيص أقسام خاصة بسيناريوهات تتعلق بالهجمات والحروب السيبرانية ضمن فرق الأمن الوطني، وتطوير استراتيجيتها للأمن السيبراني بهدف حماية البنية التحتية للمعلومات الحساسة الخاصة بها، وردع المخاطر والتهديدات بل والهجمات السيبرانية، وذلك على الصعيدين

الداخلي: من خلال التعاون الوطني بين الحكومة، ومجتمع صناعة الاتصالات والمعلومات وخلق قدرات وطنية لإدارة الحاسب الآلي، والخارجي: من خلال التعاون الدولي ومحاولات تبني استراتيجيات دولية لمواجهة، وردع المخاطر والتهديدات والاختراقات السيبرانية [2].

وتقدم روسيا الاتحادية تحت قيادة الرئيس فلادمير بوتين نموذجًا واضحًا كأحد تلك الدول، التي سعت إلى تنمية قدراتها في هذا المجال السيبراني الجديد خلال السنوات القليلة الماضية، وتطويرها كسلاح فعال لمواجهة خصومها، وفي مقدمتهم الدول الغربية متمثلة في الولايات المتحدة الأمريكية، ودول الاتحاد الأوروبي، بل وفي إدارة تفاعلاتها الدولية والإقليمية بشكل عام، لاسيما في ضوء سعيها الحثيث على استعادة إرثها التقليدي كقوة مؤثرة في النظام الدولي، بل ومحاولاتها أن تصبح أحد أقطابه الرئيسيين.

أهمية الدراسة:

تتشكل أهمية هذه الدراسة في كونها تلقي الضوء على أحد أهم وأخطر ساحات الصراع الدولي في الوقت الحالي وهو الفضاء السيبراني، الذي لا يقل أهمية عن ساحات الصراع التقليدية (البر والبحر والجو والفضاء)، بل أنه يعد أكثرهم خطورة من حيث التهديد الذي ينطوي عليه، وحجم التدمير الذي يمكن أن يؤدي إليه، إذا أخذنا في الاعتبار السرعة الفائقة والانتشار الواسع كونه ينفذ بأساليب يصعب تتبعها في كثير من الأحيان، وهو ما حدا بالدول الكبرى والتي تمتلك مفاتيح والأدوات التكنولوجية الحديثة في التأثير على غيرها من الدول والتي لا تمتلك مثل هذه الأدوات، بعبارة أخرى يعد الفضاء السيبراني أحد أبرز أدوات الدول الكبرى لإعادة تشكيل العالم الافتراضي، بما يخدم مصالحها دون غيرها.

وتسعى الدراسة إلى التركيز على دراسة مدى اهتمام أحد الدول الكبرى وهي روسيا بهذه الأداة، ومدى استخدامها لها في إدارة صراعاتها وتفاعلاتها الدولية والإقليمية، وما هي المظلة التي تنطلق منها في رؤية تلك الأداة وهل نجحت في استخدامها لتحقيق أهدافها الاستراتيجية...

ولا تتوقف خطورة الأمر على الدول، بل امتد ليشمل فاعلين دوليين آخرين

ليسوا دولاً قد يكونوا أشخاصًا أو جماعات أو شركات لديهم من الخبرات التكنولوجية، التي تؤدي إلى ما لا يحمد عقباه، وهو ما بدا واضحًا مع ظهور الجماعات الإرهابية، والشركات التكنولوجية العملاقة، وبعض جماعات القرصنة، التي انتشرت مؤخرًا في هذا المجال، وأصبحت تمثل خطرًا واضحًا على الأمن والسلم الدوليين، وهذا يفتح مجالاً لدراسات مستقبلية حول كيفية استخدام هؤلاء الفاعلين من غير الدول لهذا الفضاء لتحقيق مصالحهم الخاصة.

إشكالية الدراسة:

انطلاقًا مما سبق، فإن هذه الدراسة تسعى للإجابة على عدد من التساؤلات حول ماهية الأمن السيبراني، وموقعه في استراتيجيات الأمن القومي الروسي، وتطور الرؤية الروسية لهذا المفهوم، وكيف استخدمته من أجل تحقيق أهدافها الاستراتيجية وفي إدارة صراعاتها الدولية والإقليمية، وهل اختلف تناوله في استراتيجية الأمن القومي الروسية الجديدة والتي وقعها الرئيس بوتين وأُعلن عنها في العام 2021 عن سابقتها؟

منهج الدراسة:

اعتمدت الدراسة على المنهجين الوصفي والتحليلي من حيث قراءاتها التفصيلية الدقيقة لماهية الأمن السيبراني وتعريفاته المتعددة وصولاً إلى عناصره الرئيسية، كذلك استخدمت القراءة التحليلية للكيفية التي نظرت بها روسيا لهذا المفهوم ومدى أهميته في استراتيجيات الأمن القومي الروسي، وكذلك لبعض الأمثلة التي استخدمت فيها روسيا الأداة السيبرانية لتحقيق أهدافها الاستراتيجية وإدارة صرعاتها الدولية والإقليمية، هذا فضلاً عن استخدامها المنهج المقارن في المقارنة بين رؤية موسكو لمفهوم الأمن السيبراني في استراتيجيات الأمن القومي السابقة، وما مدى الاختلاف بين تلك الرؤية وبين ما أعلنه الرئيس بوتين في استراتيجية الأمن القومي الأخيرة في مارس 2021، كذلك المقارنة بين الرؤيتين الروسية والغربية في تحقيق الأمن السيبراني على الصعيد الدولي.

ولهذا سيتم تناول ماهية مفهوم الأمن السيبراني، وكيفية تناولت الاستراتيجيات الروسية المختلفة لمفهوم الأمن السيبراني، واستخدام روسيا الأمن السيبراني في إدارة تفاعلاتها الدولية والإقليمية، والرؤية الجديدة في استراتيجية

الأمـن القومـي الروسـية الأخـيرة فيـما يتعلـق بمفهـوم الأمـن السـيبراني.

المحور الأول: مفهوم الأمن السيبراني

تعـددت تعريفـات الأمـن السـيبراني، فهنـاك مـن يـراه تعبـيرًا عـن القـدرة عـلى حمايـة بيانـات الدولـة وشـبكاتها مثـل تعريـف (LEWIS J. A) بأنـه «حمايـة شـبكات الحاسـب والمعلومـات التـي تحتويهـا من الاختـراق أو التدمـير أو الاضطرابات الضـارة»، بينـما يـراه آخـرون عـلى أنـه» الدفـاع عـن اسـتخدام الفضـاء السـيبراني مـن الهجـمات السـيبرانية»، أو أنـه «فـن ضـمان وجـود واسـتمرارية مجتمـع المعلومـات في دولـة مـا وضـمان حمايـة المعلومـات والبنيـة التحتيـة الحيويـة في الفضـاء الإلكـتروني»[3]، كـما عرفـه البعـض بأنـه «الحـد مـن خطـر الهجـمات الضـارة عـلى برامـج وأجهـزة الكمبيوتـر والشـبكات مـن خـلال اسـتخدام أدوات كشـف الاختراقـات، ووقـف أنشـطة الفيروسـات، ومنـع الدخـول غـير المـصرح بـه، وتأكيـد الهويـات، وتمكـين الاتصـالات المشـفرة».

ومـن جانبـه، قـدم الاتحـاد الـدولي للاتصـالات تعريفًـا للأمـن السـيبراني بأنـه «مجمـوع الأدوات والسياسـات والمفاهيـم الأمنيـة، والضمانـات، والمبـادئ، ومناهـج إدارة المخاطـر، والإجـراءات، والتدريبـات، وأفضـل الضمانـات والممارسـات التكنولوجيـة، التـي يمكـن اسـتخدامها لحمايـة البيئـة السـيبرانية، والمسـتخدم والمنظمـة بصفـة عامـة".

كـما عرفتـه وزارة الدفـاع الأمريكيـة بأنـه "جميـع الإجـراءات التنظيميـة اللازمـة لضـمان حمايـة المعلومـات بجميـع أشـكالها الماديـة والإلكترونيـة مـن مختلـف الجرائـم، والهجـمات، التخريـب، التجسـس، والحـوادث، فالأمـن السـيبراني مجموعـة مـن الوسـائل التقنيـة والتنظيميـة والإداريـة التـي تسـتخدم لمنـع الاسـتخدام الغـير مـصرح بـه، ووقـف عمليـات سـوء الاسـتغلال وحمايـة خصوصيـة البنايـات الشـخصية" [4].

وتتكون منظومة الأمن السيبراني من ثلاثة عناصر رئيسية، هي[5]:

- القـوة السـيبرانية: والتـي عرفهـا جوزيـف نـاي أسـتاذ العلاقـات الدوليـة الشـهير بأنهـا «القـدرة عـلى الحصـول عـلى النتائـج المرجـوة مـن خـلال اسـتخدام مصـادر المعلومـات المرتبطـة بالفضـاء الإلكـتروني»، بينـما عرفهـا دنيـال كويـل

بأنها «القدرة على استخدام الفضاء الإلكتروني لخلق مزايا، والتأثير على الأحداث المتعلقة بالبيئة الواقعية عبر أدوات إلكترونية».

- الدفاع السيبراني: ويقصد به مجموعة القدرات النظامية التي تمتلكها القوات المسلحة للحماية من تأثير الهجمات السيبرانية، والتخفيف من حدتها والتعافي منها بسرعة، وقد عرفت العقيدة الفرنسية الدفاع الإلكتروني على أنها مجموعة الوسائل الفنية وغير الفنية التي تسمح للدولة بالدفاع في الفضاء الإلكتروني عن نظم المعلومات الحرجة، ويعرفه البرلمان الأوروبي بأنه «عمليات تطبيق الإجراءات الأمنية من أجل الحماية من الهجمات السيبرانية والتعامل معها».

- الردع السيبراني: نتيجة للطبيعة الخاصة للفضاء السيبراني، فإنه من الصعوبة منع الهجمات السيبرانية بصورة كلية، فضلاً عن صعوبة تعقب مصدر الهجمة، ومعرفة الفاعل من الناحية الفنية، لذا فإن تحقيق الردع بالطرق التقليدية لا يتحقق في أفضل الأحوال في الفضاء الإلكتروني كما في حالات الردع التقليدي، لذلك فإن الردع في الفضاء الإلكتروني يتحقق من خلال تبني خطط، واستراتيجيات للتعامل مع الهجمات السيبرانية في حالة حدوثها تشمل:

- التخفيف من حدتها.
- عدم التأثير على البنى التحتية الحرجة، والخدمات الرئيسية ،والمعلومات المهمة التي تشكل ركيزة للأمن القومي للدولة.

المحور الثاني: مفهوم الأمن السيبراني في استراتيجيات الأمن القومي الروسي

هناك توجهًا غير معلن لدى روسيا الاتحادية بقيادة بوتين لاستعادة أمجادها السوفيتية، ومحاولة حسم صراعها مع الغرب على قيادة النظام الدولي، هذا التوجه مفاده أن الانتصار في الصراع مع الغرب لن يتحقق بالاعتماد القاصر على الأدوات العسكرية التقليدية، ولكن يتطلب أيضًا الاعتماد على أدوات الحرب الحديثة.

وقد كشفت وثيقة لوزارة الدفاع الروسية بعنوان "مفهوم الأنشطة الفضائية

المعلوماتية للقوات المسلحة الروسية"، عن الحيز الذي تمثله المعلومات، والأمن السيبراني ضمن إطار استراتيجية الأمن القومي الروسي، وتبنت الوثيقة تعريف فضاء المعلومات بأنه «مجال النشاط المتصل بتشكيل المعلومات ونقلها واستخدامها»، بالإضافة إلى من ما يطلق عليه "عقيدة جيراسيموف" – الرئيس السابق لهيئة الأركان العامة الروسية - وهذه العقيدة تنطوي على مجموعة من الأفكار بشأن الأدوات غير التقليدية في الحروب الراهنة، والتي تتضمن أدوات مختلفة من بينها المعلومات، سواء من خلال الفضاء العالمي أو الفضاء الإلكتروني، واستهداف نقاط الضعف للخصوم وتجنب المواجهة العلنية حتى المراحل النهائية للصراع[6].

وبصفة عامة، يمكن القول بأن الاهتمام الروسي بالأبعاد السياسية للأمن الإلكتروني، قد بدأ في التسعينات من القرن الماضي بعد تأسيس مجلس الأمن الروسي في عام 1992، حيث تم بالإضافة إلى المؤسسات الأمنية الروسية إنشاء مؤسسات أخرى تختص فقط بالقضايا الإلكترونية، وبحماية الأمن الإلكتروني الروسي، ومن أهمها: مجلس الأمن الروسي، جهاز الأمن الفيدرالي، جهاز الحرس الفيدرالي، الجهاز الفيدرالي للتحكم التقني، ووزارة الاتصالات، وتكنولوجيا المعلومات.

وتنقسم المهام ما بين الإدارات المختلفة في الأنشطة المتعلقة بالأمن الإلكتروني على النحو التالي: تختص وزارة الداخلية بمواجهة الجرائم الإلكترونية، ووزارة الدفاع مسئولة عن كل ما يتعلق بأخطار الحروب الإلكترونية وتطوير القدرات الإلكترونية الهجومية للجيش الروسي، ويهتم جهاز الأمن الفيدرالي بالإرهاب الإلكتروني، وهو تقسيم قائم بالأساس على التفرقة ما بين الأبعاد الإجرامية، والإرهابية، والعسكرية، والسياسية للأمن الإلكتروني.

وفي بداية الألفية الجديدة، تبلور الاهتمام الروسي بقضايا الأمن الإلكتروني، عندما قامت روسيا بتطوير استراتيجية أمنية تبنى على أساس الإيمان الكامل بالدور، الذى يلعبه الأمن الإلكتروني في تحقيق المصالح القومية وتعزيز الاستقرار الاجتماعي والسياسي، وقد تصدرت روسيا آنذاك الدول الساعية لتطوير اتفاقية دولية لمواجهة المخاطر الإلكترونية، والحيلولة دون حدوث سباق للتسلح

الإلكتروني نتيجة لتزايد التنافس التكنولوجي ما بين الفاعلين على المستوى الدولي، يتم من خلالها وضع تعريفات واضحة يقبلها المجتمع الدولي لكافة المفاهيم المحورية ذات الصلة بالفضاء الإلكتروني.

ومع إعلان موسكو في العام 2010 عن العقيدة العسكرية الخاصة بها، تم الإشارة إلى أن الصراعات العسكرية الحديثة تتضمن الاستخدام المتكامل للقدرات العسكرية وغير العسكرية، مع الاهتمام بإبراز دور أكبر لحرب المعلومات، وتم تشكيل قيادة مستقلة للأمن السيبراني، بالإضافة إلى الإدارة السيبرانية داخل الجيش الروسي لتعزيز جاهزية القوات المسلحة الروسية للدفاع ضد الهجمات السيبرانية، واتخاذ الاجراءات الاحترازية ضد تلك الهجمات من خلال الشبكات، وقامت روسيا بشراء آلات كاتبة لاستخدامها في المكاتبات الحيوية، حتى لا تتعرض المكاتبات السرية للاختراق، وبلغ الانفاق العسكري الروسي على حرب الفضاء الإلكتروني آنذاك 127 مليون دولار من إجمالي إنفاق عسكري بلغ 40 مليار دولار، حيث تحتل روسيا المركز الرابع عالميًا في مجال تطوير قدرات الاسلحة الإلكترونية[7].

وفي سبتمبر 2018 قام جهاز الأمن الفيدرالي الروسي بتأسيس مركزًا وطنياً لتنسيق مكافحة الهجمات السيبرانية على البنية التحتية الحيوية في روسيا، يتولى مهام الكشف والوقاية والقضاء على تداعيات الهجمات الإلكترونية، وتبادل المعلومات بين الهيئات المتخصصة في الداخل والخارج، وتحليل الهجمات السيبرانية الماضية وتطوير أساليب مكافحتها[8]

وعلى صعيد موازٍ، أعلنت روسيا من خلال منظمة «البريكس» - التي تضم البرازيل ، روسيا، الهند، الصين، وجنوب إفريقيا، و تأسست عام 2008 ، وتم عقد أول قمة لها في يونيو 2009 - عزمها إنشاء فضاء إلكتروني خاص بها مستقل عن شبكة الانترنت العالمية الحالية، وذلك بهدف التخلص من الهيمنة الغربية، وعمليات التجسس الإلكتروني الأمريكية، واتخذت خطوات فعلية لذلك؛ حيث قامت البرازيل ببناء منظومة الكابلات، التي يمكن أن تربطها بروسيا والصين وجنوب إفريقيا بكابل طوله 34 ألف كيلو متر، وهو يربط بين مدينة «فلاديفوستوك" في شرق روسيا و"فورتاليزا" في البرازيل، مرورًا بشانتو الصينية

و"تشينای" الهندية و"كيب تاون" في جنوب ريقيا، ليس هذا فحسب، بل من المتوقع أن يوفر المشروع خدمات الإنترنت في 21 دولة افريقية، وبذلك يتم انشاء شبكة إنترنت جديدة موازية لشبكة الانترنت الحالية، وتكون منافسًا قويًا للولايات المتحدة، وتعتزم دول «البريكس» أيضًا إصدار تشريعات تجبر القوى الرئيسية في الانترنت مثل «جوجل» و«فيسبوك» و«ياهو» على تخزين المعلومات كافة التي يتم جمعها داخل دول المجموعة محليًا، كي لا تتمكن وكالة الأمن القومي الأمريكية من الوصول إليها [9].

وبصفة عامة، يمكن القول بأن استراتيجيات الأمن القومي الروسية السابقة، وضعت المخاطر الإلكترونية في المرتبة الخاصة بالتطرف، والمخاطر البيئية، والجريمة المنظمة العابرة للحدود، وقد جاءت الهجمات الإلكترونية ضمن قائمة أكثر عشرة مخاطر تهدد البنية التحتية، ثم تلا ذلك ضرورة تطوير القدرات التكنولوجية للقوات المسلحة حتى يتحقق الردع الإلكتروني، وقد اعتمدت تلك الاستراتيجيات على عدد من الأدوات لتحقيق أهدافها [10]:

- استخدام الأسلحة الإلكترونية الهجومية باعتبار أنها قوة مضاعفة Fore Multiplier في الحروب، بمعنى أنها تزيد من القدرات القتالية للدولة إذا ما تم استخدامها إلى جانب قدرات عسكرية أخرى.
- تعطيل البنية التحتية المعلوماتية للخصوم، والاتصالات المدنية والعسكرية لهم قبل البدء في العمليات العسكرية التقليدية، فوفقاً للعقيدة العسكرية الروسية، لابد وأن يسبق الهجوم العسكري الناجح عمليات أخرى تهدف إلى منع الخصم من الحصول على معلومات من مصادر خارجية.
- تعطيل عمليات التداول المالية والائتمانية، ومحاولة التأثير في الرأي العام في الدولة الخصم عن طريق المعلومات الخاطئة والدعاية التي تخدم المصالح الروسية، ومن ثم يساعد التخطيط في مرحلة ما قبل الهجوم للقيام بعملية الاختراق السري لأنظمة الخصم في تحقيق هذه الأهداف.

المحـور الثالـث اسـتخدام روسـيا للقـوة السـيبرانية في إدارة تفاعلاتهـا الدوليـة والإقليميـة

تعـددت الأمثلـة التـي توضـح كيفيـة اسـتخدام روسـيا للقـوة السـيبرانية في إدارة تفاعلاتهـا الإقليميـة والدوليـة، وذلـك عـلى مـدار العقديـن الماضيـين انطلاقًـا مـن رؤيتهـا الاسـتراتيجية للأمـن السـيبراني عـلى النحـو الموضـح بعاليـه، ومـن أبرزهـا:

1- على صعيد التفاعلات الدولية العسكرية:

أ. تعطيـل الخدمـات والتأثـير البنـى التحتيـة: وهـو مـا بـدا واضحًـا في التعامـل مـع اسـتونيا، حيـث قامـت موسـكو في العـام 2007 بشـن حـرب سـيبرانية شـاملة عليهـا، بـدأت بسلسـلة مـن الهجـمات يطلـق عليهـا DDOS at-tacks ضـد المواقـع التـي تديرهـا الحكومـة الإسـتونية، وتسـبب الهجـوم في عرقلـة دخـول المواطنـين إلى بعـض المواقـع مثـل موقـع الحـزب السـياسي، الـذي ينتمـي إليـه رئيـس الـوزراء. كذلـك لم يعـد المواطنـون قادريـن عـلى إجـراء معاملاتهـم البنكيـة الإلكترونيـة، التـي يتـم 97% منهـا عـبر الانترنـت، أو التواصـل مـع بعضهـم بالبريـد الإلكـتروني لأيـام عديـدة، وتـم تعطيـل البنيـة التحتيـة للاقتصـاد الرقمـي الإسـتوني [11].

1. ورغـم أن الهجـوم الـروسي السـيبراني عـلى البنيـة التحتيـة الإسـتونية لم يسـتمر طويـلاً، إذ اسـتعانت الأخـيرة بحلـف شـمال الأطلـسي لمواجهـة تلـك الهجـمات والسـيطرة عليهـا، إلا أن هـذا الهجـوم لفـت الانتبـاه إلى خطـورة التهديـدات الإلكترونيـة، ومـدى قدرتهـا عـلى شـل حركـة الدولـة تمامًـا حتـى وإن كان لفـترة محـدودة.

ب. الاخـتراق والحرمـان مـن الخدمـات: قبـل الغـزو الـروسي لجورجيـا عـام 2008 قامـت موسـكو بالهجـوم الإلكـتروني عليهـا مـن خـلال أداتـين رئيسـيتين، هـما:

- اخـتراق بعـض المواقـع الإلكترونيـة السياسـية منهـا كموقـع الرئيـس الجورجـي، ووزارة الخارجيـة، ووزارة التعليـم، وموقـع البرلمـان الجورجـي.
- هجـمات الحرمـان مـن الخدمـة كالتـي تقدمهـا البنـوك التجاريـة الكـبرى في جورجيـا، فضـلاً عـن المواقـع الإخباريـة ووسـائل الإعـلام والتـي شـملت أكـبر

المواقع الإخبارية باللغة الإنجليزية مثل: CBC & BBC ومواقع التواصل الاجتماعي.

وقد اختلف الهجوم السيبراني الروسي في الحالة الجورجية عن مثيلتها الإستونية، ففي حين كان الهدف من الهجوم على إستونيا هو الحيلولة دون قدرة المواطنين على الوصول إلى الخدمات الإلكترونية الحيوية، التي يقدمها القطاعان العام والخاص، كان الهدف من الإضرار بالمواقع الإلكترونية الجورجية، هو الحد من قدرة الدولة على إيصال رؤيتها للعالم ولمواطنيها عبر الإنترنت.

ورغم أن نتائج الهجوم الإلكتروني الروسي على جورجيا لم تكن أثاره التدميرية فادحة بالنسبة لتقديم الخدمات الحكومية، نظرًا لعدم الاعتماد الجورجي على البنية الإلكترونية بشكل كبير، فهدف الدب الروسي كان تحقيق العزلة الداخلية والخارجية للنظام الجورجي، وليس إلحاق الضرر الدائم ببنيته التحتية الإلكترونية لما له من خسائر اقتصادية طائلة قد تطول الدول المرتبطة اقتصاديًا بجورجيا وفي مقدمتها روسيا، إلا أنه لفت الانتباه أيضًا حتى الدول التي لا تعتمد على تكنولوجيا المعلومات والاتصالات بشكل كبير يمكن أيضًا أن تتعرض للضرر حال وقع هجوم إلكتروني عليها من حيث ضمان تدفق المعلومات للمواطنين داخل الدولة، وعليه فإنه وعلى العكس من الهجمات العسكرية التقليدية يمكن الاعتماد على الهجمات الإلكترونية بحيث تحدث آثارًا مؤقتة في إطار زمني محدد [12].

ج. الضغط على الدول لاتخاذ قرارات تتماشى مع المصالح الروسية: في يناير 2009 توقّف اثنين من مزوّدي خدمة الإنترنت في قرغيزستان عن العمل، بعد قيام قراصنة روس بشن هجمة DDOS، في إطار الجهود التي كانت تبذلها روسيا آنذاك، من أجل الضغط على رئيس قرغيزستان لإزالة قاعدة عسكرية أمريكية كانت تستخدمها واشنطن كداعم رئيسي في عملياتها العسكرية في أفغانستان، بيد أن تلك الهجمة قد أتت ثمارها بعد قيام الجمهورية القيرغيزية بإزالة القاعدة الأمريكية، وهو ما دفع

الكرملين إلى منح قرغيزستان قروضًا ومساعدات مالية بقيمة 2 مليار دولار لاحقًا [13].

د. الاختراق وإحداث الفوضى الشاملة (أوكرانيا - 2014): بدأت الاحتجاجات في أوكرانيا عام 2013 للمطالبة بالانضمام للاتحاد الأوربي، وذلك بعد إعلان الرئيس الأوكراني فيكتور يانوكوفيتش - والمقرب من دوائر الحكم في موسكو - تعليق التوقيع على اتفاقية الشراكة مع الاتحاد الأوروبي، ومع بداية العام 2014 ، ازدادت وتيرة تلك الاحتجاجات، ووصل الأمر إلى وقوع ضحايا بين صفوف الحكومة والمعارضين، ومع تزايد الاشتباكات اتخذ مجلس النواب الأوكراني قرارًا في فبراير 2014 بعزل الرئيس يانوكوفيتش، وتلا ذلك اندلاع الثورة الأوكرانية التي أطاحت بالرئيس الأوكراني وحكومته نهائيًا، وتم اتخاذ بعض الإجراءات التي اعتبرتها الأقليات الموالية لروسيا بمثابة لإعلان الحرب العنصرية في مواجهتها، ومن ذلك إلغاء لغات الأقليات، ومن ضمنها اللغة الروسية، واعتماد اللغة الأوكرانية اللغة الرسمية الوحيدة للبلاد.

وفي الأول من مارس من نفس العام قدم الرئيس الروسي بوتين طلبًا وافق عليه الاتحاد الروسي بالاجماع، وهو استخدام القوات الروسية في أوكرانيا، ثم قامت الأقليات التابعة للقومية الروسية في شبه جزيرة القرم بإجراء استفتاء في مارس حول الانفصال عن أوكرانيا والانضمام إلى روسيا الاتحادية، وكانت نتيجته الموافقة على ذلك المقترح بنسبة 95%، ويمكن القول بأن روسيا قد قامت بتوظيف أدوات القوة السيبرانية، والفضاء الإلكتروني لتحقيق أهدافها في أوكرانيا، وذلك على النحو التالي[14]:

1) التأثير على الرأي العام:

كان هناك حملة معلومات سبقت العمليات العسكرية في شبه جزيرة القرم، استهدفت بالأساس الرأي العام الروسي في الداخل يليه المقيمين في شبه جزيرة القرم، وكانت الحملات الإعلامية الروسية تهدف تشويه بالأساس إلى: سمعة الحكومة الأوكرانية، التي تولت الحكم عقب اندلاع الثورة في 2014، والتشديد على الخطر المحدق بالروس المقيمين في أوكرانيا، والدعم الكبير لفكرة عودة شبه جزيرة القرم إلى روسيا.

2) نشر معلومات مضللة:

استفادت موسكو كثيرًا من وسائل التواصل الاجتماعي لحشد دعم داخلي، ونشر كميات هائلة من المعلومات المضللة حول احتجاجات الميدان الأوربي، ونوايا الحكومة الجديدة في كييف، وقد اعتمدت روسيا في حملتها الدعائية خلال الصراع مع أوكرانيا على خمسة عناصر[15].

- التأثير الهائل والطويل الأمد.
- المعلومات المرغوب بها (التلاعب بالرسائل لاستغال مخاوف الروس العرقيين في أوكرانيا).
- التحريك العاطفي (استخدام موضوعات ستجعل الروس العرقيين يتصرفون بدافع من غضب غير عقلاني).
- الوضوح (عرض الصراع الأوكراني بمصطلحات بسيطة من الخير والشر).
- الجلاء المفترض (مطابقة الرسائل الدعائية مع الخرافات والأساطير الروسية التي يتم الاعتقاد بها على نطاق واسع).

وقد ساعدت وسائل الاعلام الروسية ايضاً المرئية والإلكترونية على ضمان تحقيق الموافقة الداخلية، على عملية انتقالية سريعة من صراع مربك إلى استيلاء على أراضٍ مقبول سياسيًا، واستخدم بوتين تلك الوسائل لتحقيق تأثير كبير في عرض الحجج التاريخية والعاطفية، بشأن كيفية انتماء شبه جزيرة القرم إلى روسيا في خطاب بتاريخ 18 مارس 2014.

3) الاختراق وقطع الخدمات والتلاعب في بيانات الانتخابات الأوكرانية:
قبيل الإطاحة بالرئيس الأوكراني بيانكوفيتش تم شن حملات معلوماتية متعددة على شرق أوكرانيا، حيث نجح قراصنة المعلومات الموالين لروسيا في أكتوبر 2014 في قطع النظام الإلكتروني لجمع نتائج الانتخابات، واختراق الحواسب المسجل عليها بيانات التصويت، والاقتراع في محاولة للتلاعب بنتائج الانتخابات، وإحداث فوضى سياسية، وهو ما اضطر إلى فرز الأصوات يدويًا، وتأخير الإعلان عن نتائج الانتخابات[16].

2- على صعيد التفاعلات السياسية الدولية:

لم تتوانى روسيا عن استخدام القوة السيبرانية في إدارة تفاعلاتها الدولية السياسية والاقتصادية بما يساعد في تعظيم قوتها، وتحقيق أهدافها، التي تعجز أدوات القوة التقليدية عن تحقيقها، لاسيما في ضوء ما تتميز به هذه القوة السيبرانية من خاصية كالتخفي والقدرة على إصابة أهداف الخصم، واتساع نطاق تدمير الأهداف الإلكترونية مع التحكم في إمكانية إصابة الأهداف من دون وقوع خسائر بشرية غير مقصودة، وتتنوع تطبيقات روسيا في استخدامها للقوة السيبرانية في التفاعلات الدولية السياسية، وهناك العديد من الأمثلة على ذلك ومنها:

أ. الحرب السيبرانية على ألمانيا:

باردات روسيا بتنظيم هجمات إلكترونية ضد أحزاب ومؤسسات سياسية ألمانية، بغية إضعافها قبيل الانتخابات، وذلك من خلال تسريب وثائق سرية، مثل تلك التي تمت سرقتها من البرلمان الألماني (البوندستاغ) في عملية قرصنة كبرى تعرض لها في سنة 2015، ويعتقد أن فريقًا من القراصنة يدعى «سوفاسي» يقف وراء تلك العملية، ومن المرجح أنهم ينتمون إلى المخابرات الروسية، وقد أدت الحملات الدعائية الروسية إلى حالة من الارتباك في الداخل الألماني، حيث اكدت الحكومة الألمانية على أن الحكومة الروسية تشن حملات إعلامية عبر قناتها الرسمية «روسيا اليوم»، وموقع «سبوتنيك» الإخباري، فضلاً عن توظيف أساليب ساخرة في مواقع التواصل الاجتماعي، لنشر دعايتها فيما يتعلق بالانتخابات الألمانية، وكانت تلك الحملات الروسية بدرجة أولى إلى الناخبين الألمان الذين يتكلمون الروسية، والذين يبلغ عددهم حوالي 3 ملايين، فضلاً عن الناخبين القوميين والمحافظين، على غرار أنصار حزب «البديل من أجل ألمانيا» اليميني المتطرف، وتعد حادثة الاعتداء على الفتاة الروسية ليزا خير مثال على التلاعب الروسي بالرأي العام في ألمانيا، حيث تواترت في العام 2016 قصة مفادها أن فتاة روسية عمرها 13 عامًا قد تعرضت لاختطاف، والاغتصاب على يد مجموعة من اللاجئين في ألمانيا، واتهمت وسائل الإعلام الروسية ألمانيا بإخفاء القصة، والتستر على جنسية

الضحية، من جانبه، أدلى وزير الخارجية الروسي سيرغي لافروف بدلوه في القضية، وطالب الجانب الألماني بتقديم توضيحات، كما خرجت مظاهرات احتجاجية في ألمانيا، على الرغم من أن التحقيقات أظهرت في النهاية أن القصة برمتها تم اختلاقها، ودفع ذلك الحكومة الألمانية للاحتجاج لدى نظيرتها الروسية، ومطالبتها بالتوقف عن بث الدعايات السياسية [17].

ب. الهجمات السيبرانية على نتائج الانتخابات الأمريكية:

أكد تقرير استخباراتي أمريكي قيام الحكومة الروسية بالتدخل بغرض التأثير على نتائج الانتخابات الرئاسية الأمريكية عام 2016، وأشار التقرير الذي صدر عن مكتب مدير الاستخبارات الأمريكية في يناير 2017 ، أن القيادة الروسية كانت تفضل المرشح الرئاسي دونالد ترامب على نظيرته هيلاري كلينتون، وأن الرئيس الروسي فلاديمير بوتين قد أمر شخصيًا بـ «حملة تأثير» لإلحاق الضرر بفرص كلينتون الانتخابية، و"إضعاف" الرأي العام في العملية الديمقراطية الأمريكية، وفي 7 أكتوبر 2016، ذكرت وزارة الدفاع الوطني ووزارة الأمن الداخلي أن وكالة الاستخبارات الأمريكية كانت على ثقة من أن الحكومة الروسية، قد أدارت عمليات قرصنة للرسائل الإلكترونية بقصد التدخل في سير الانتخابات الأمريكية، ووفقا لتقرير أوندي ODNI في 6 يناير 2017، فإن المخابرات العسكرية الروسية (GRU) قد اخترقت خوادم اللجنة الوطنية الديمقراطية (DNC) ، وحساب البريد الإلكتروني الشخصي لمدير حملة كلينتون جون بوديستا وإحالة محتوياتها إلى ويكيليكس، وعلى الرغم من أن المسؤولين الروس كانوا قد نفوا تورطهم في أي اختراقات أو تسريبات للـ DNC، إلا أن هناك أدلة قوية تفيد بأن عملية اختراق DNC مرتبطة بعمليات روسية معروفةK في يناير 2017، وشهد مدير المخابرات الوطنية جيمس كلابر أن روسيا تدخلت أيضًا في الانتخابات من خلال نشر الأخبار مضللة، التي تم الترويج لها على وسائل التواصل الاجتماعي [18].

ومن يونيو 2016 وحتى مارس 2019، أجرى كل من مكتب التحقيقات الفيدرالي FBI والمستشار الخاص تحقيقات عديدة، أسفرت عن توجيه اتهامات لستة وعشرين مواطنًا روسيًا وثلاث منظمات روسية، كما قام

المستشار الخاص بالتحقيق في العلاقات بين روسيا وشركاء ترامب، وأشارت أصابع الاتهام إلى كل من ريك جيتس وروجر ستون، وأدين كل من بول مانافورت، مايكل فلين، جورج بابادوبولوس، أليكس فان دير زوان، وكر صامويل باتن ومايكل كوهين بالتآمر[18].

ج. تعبئة الرأي العام لصالح التدخل العسكري في سوريا:

بدأت روسيا في سبتمبر 2015 حملتها العسكرية ضد ما أسمته بالتنظيمات الإرهابية في سوريا، وقد أعلنت أن أهدافها الرسمية تتمثل في حماية نظام الأسد، والجيش العربي السوري من الانهيار حتى لا تسقط مؤسسات الدولة، فضلاً عن القضاء على تنظيمي «داعش»، و»جبهة النصرة» التابعين لتنظيم القاعدة، وغيرها من التنظيمات الإرهابية الأقل نفوذاً وانتشاراً، وقد قوبل هذا التدخل الروسي العسكري بموجة من الرفض الشعبي، وتصاعد الجدل الداخلي بشأن جدواه ومدى انعكاسه على الداخل الروسي، واختلفت اتجاهات الرأي العام تجاه هذه الخطوة، خاصة في ضوء الذكرى السلبية للتدخل السوفيتي في أفغانستان، وقد نجحت الحكومة الروسية في تهدئة مخاوف الرأي العام من التدخل العسكري في سوريا، ونجحت في تعبئته لصالح تأييد هذا القرار، وذلك من خلال الخطوات التالية [19]:

- سعى وزارة الدفاع الروسية لإصدار بيانات صحفية عن العلميات العسكرية في سوريا، ونشرها من خلال موقع الفيس بوك يومياً، فضلاً عن كتابة تغريدات على موقع تويتر عن العمليات العسكرية الروسية في سوريا، وذلك بهدف تقديم معلومات مفصلة عن الضربات الجوية، كما تم عرض مقاطع فيديو للعمليات العسكرية، وللظروف المعيشية على اليوتيوب، التي يعيش في ظلها أفراد الجيش الروسي في سوريا، وهدفت هذه الخطوة إلى زيادة الشفافية، وتقديم انطباع بأن المناطق التي توجد فيها القوات المسلحة الروسية آمنة ومحمية.

- التأكيد على استخدام الجيش الروسي أسلحة ومعدات عسكرية متقدمة تقنياً، مما يقلل إلى حد كبير من خطر الإصابات والخسائر في صفوف الجيش الروسي، فضلاً عن استبعاد القيادة الروسية إمكانيه إرسال قوات برية إلى

سـوريا.

- توظيـف الكرملـين حـادث اسـتهداف الطائـرة المدنيـة الروسـية في سـيناء بعمـل إرهـابي، للتأكيـد عـلى ضرورة توجيـه ضربـات انتقاميـة ضـد داعـش، وهـو مـا يتسـق مـع توجهـات الـرأي العـام في هـذا الإطـار.

د. الهجـمات السـيبرانية عـلى نتائـج اسـتفتاء بريطانيـا الخـروج مـن الاتحـاد الأوروبي:

أشـارت العديـد مـن أصابـع الاتهـام البريطانيـة إلى قيـام الكرملـين بدعـم سرًا تصويـت إيجـابي بخـروج بريطانيـا مـن الاتحـاد الأوروبي في عـام 2016، وادعـى نائـب البرلمـان البريطـاني بـن برادشـو أن روسـيا تدخلـت في حملـة الاسـتفتاء عـلى خـروج بريطانيـا مـن الاتحـاد الأوروبي، وفي عـام 2017 أصـدرت لجنـة الإدارة العامـة والشـؤون الدسـتورية التابعـة لمجلـس العمـوم، تقريـرا يشـير إلى انهيـار موقـع تسـجيل الناخبـين الحكومـي في يونيـو 2016 قبـل أقـل مـن سـاعتين مـن الموعـد النهـائي للتسـجيل المقـرر أصـلاً)، مؤكـدًا دور الاسـتخبارات السـيبرانية الروسـية في هـذا الفعـل، كـما كشـف التقريـر دورهـا في انشـاء وتمويـل حركـة الدعائيـة الإلكترونيـة التـي تحـث الناخبـين للتصويـت بنعـم للخـروج مـن الاتحـاد الأوروبي[21].

المحور الرابع: الأمن السيبراني في استراتيجية الأمن القومي الروسي:

بعـد سـقوط الاتحـاد السـوفيتي، رسـمت روسـيا الاتحاديـة اسـتراتيجياتها للأمـن القومـي بوتـيرة متصاعـدة، بهـدف اسـتعادة قوتهـا كدولـة في الدرجـة الأولى، ودورهـا الخارجـي عـلى أسـاس تبنـي قاعـدة أساسـية وهـي بنـاء قوتهـا الداخليـة، وهـذا يتضـح فيـما يـلي :

أ. استراتيجيات الأمن القومي الروسي منذ 1993 وحتى 2020

صـدرت مجموعـة مـن اسـتراتيجيات الأمـن القومـي، أولهـا الاسـتراتيجية التـي صـدرت عـام 1993، وثانيهـا تلـك التـي صـدرت عـام 2000، وثالثتهـا التـي صـدرت عـام 2012، واسـتمر تنفيذهـا حتـى عـام 2020، وأُجـري عليهـا تعديـلان في نهايـة عام 2014 ونهايـة عـام 2015، قبـل أن يوقّـع الرئيـس الـروسي فلاديمـير بوتـين الاسـتراتيجية الجديـدة في 3 يوليـو 2021.

وبقـراءة سريعـة للاسـتراتيجيات السـابقة، يمكـن القـول بـأن هنـاك اختلافًـا واضحًـا فيـما بينهـا مـن حيـث المضمـون، مـن خـلال تحديـد مصـادر الخطـر عـلى الدولـة، وأشـكال هـذه المخاطـر والتهديـدات، كذلـك مـدى قدرتهـا عـلى تحقيـق أهدافها والمحـددة في كل اسـتراتيجية عـلى حـدى، والتـي تمثلـت في رغبتهـا اسـتعادة قوتهـا داخليًـا وفضـلاً عـن مكانتهـا الإقليميـة والدوليـة، بـل وطموحهـا في العـودة كلاعـب أسـاسي في النظـام الـدولي.

وعليـه، فقـد تمحـورت أهـداف اسـتراتيجية عـام 1993 بصـورة أساسـية حـول تقويـة أواصر الدولـة، وإدارة انفـراط عقـد الاتحـاد السـوفياتي، وتحديـداً إدارة وراثـة روسـيا الاتحاديـة للاتحـاد المنهـار، وتضمّنـت اسـتراتيجية عـام 2000 تطلعًـا روسـيًا واضحـاً نحـو اسـتعادة مكانتهـا الدوليـة، بالتـوازي مـع انطـلاق حكـم الرئيـس بوتـين الـذي فـاز في الرئاسـة في العـام نفسـه، بعـد سـنتين مـن تكليفـه رئاسـة الـوزراء، والدولـة فيـما بعـد، وهـو مـا بـدا واضحًـا في خطابـه التاريخـي في مؤتمـر ميونيـخ للأمـن الـدولي، عـبر إعلانـه أن بـلاده لـن تقبـل الأحاديـة القطبيـة بعـد ذلـك الوقـت، وأنهـا تسـعى لعـالمٍ متعـدد الأقطـاب، لتتبلـور منـذ ذلـك التاريـخ رغبـة روسـيا في التعدّديـة القطبيـة وعـودة «روسـيا العالميـة»، وهـو الأمـر الـذي ورد صراحـةً هدفـاً رئيسـاً مـن أهـداف اسـتراتيجية الأمـن القومـي الـروسي، 2012-2020.[20]

استراتيجية الأمن القومي الروسي الجديدة 2021:

جـاءت الاسـتراتيجية الروسـية الجديـدة للأمـن القومـي، والتـي وقـع عليهـا الرئيـس بوتـين في الثالـث مـن يوليـو 2021، اسـتكمالاً لمـا بدأتـه الاسـتراتيجيات السـابقة، فقـد اتفقـت معهـا في الأهـداف والمنطلقـات، إلا أنهـا كانـت أكـثر تركيـزًا عـلى المخاطـر والتهديـدات التـي تواجـه الأمـن القومـي الـروسي، وكان لافتًـا شـمول تلـك الوثيقـة لأنـواع جديـدة مـن المخاطـر إلى جانـب المخاطـر والتهديـدات التقليديـة، وهـو مـا أكـده بوتـين عنـد إعلانـه لتلـك الوثيقـة عندمـا أشـار إلى أن بـلاده تتعـرض لـ "محاولـة لفـرض حصـار متنـوع يـتراوح بـين التهديـدات العسـكرية،والهجمات السـيبرانية، والتدخـل في الشـئون الداخليـة للدولـة لزعزعـة النظـام السـياسي، والاسـتقرار الأمنـي للبـلاد وذلـك مـن قبـل أعدائهـا في الداخـل

والخـارج»[21].

هـذا التطـور الـذي اشـتملت عليـه وثيقـة الأمـن القومـي الجديـدة جعـل العديـد مـن المهتمـين بالشـأن الـروسي يصفهـا بأنهـا «بيـان لحقبـة جديـدة»[22] ،ويعتبرهـا خارطـة طريـق تسـعى لتكييـف روسـيا مـع عـالم مـا يـزال متداخـلًا ومليئًـا بالانقسـامات التـي ترسـم خطـوط الـصراع بـين الـدول وداخلهـا.

وقـد حسـمت روسـيا في تلـك الوثيقـة موقفهـا تجـاه الـدول الكـبرى في النظـام الـدولي، حيـث أعلنـت تأكيدهـا عـلى أولويـة تأمـين موقعهـا المهيمـن في مجالهـا الجيوسـياسي، وذلـك عـبر تقويـة الهيـاكل والمؤسسـات الإقليميـة «لتنسـيق عمليات التكامـل» بـين الـدول الواقعـة في المجـال، وهـذا يعنـي أن روسـيا حسـمت أمورهـا بالتوجـه شرقًـا، فالتصـور الجديـد يعتـبر أن تعميـق التعـاون «المفيـد للطرفـين»، و"تطويـر شراكـة شـاملة" تقـوم عـلى "التفاعـل الاسـتراتيجي" مـع الصـين والهنـد والمؤسسـات غـير الغربيـة مثـل منظمـة شـنغهاي للتعـاون ومنظمـة البريكـس المشـار إليهـا بعاليـه، وفي هـذا الإطـار، قامـت روسـيا برفـع الهنـد إلى مسـتوى الشريـك الاسـتراتيجي في محاولـة روسـية للتـوازن مـع الصـين، وذلـك لعـدم رغبتهـا في لعـب دور الشريـك الأصغـر للصـين، وفي المقابـل وصفـت الاسـتراتيجية الجديـدة الولايـات المتحـدة الأمريكيـة، وبعـض حلفائهـا بحلـف شـمال الأطلـسي بأنهـم أطـراف غـير وديـة حيـث أسـمتهم في الوثيقـة بـ «البلـدان غـير الصديقـة" ،معتـبرة إياهـم يسـعون إلى إضعـاف روسـيا سياسـيًا، وعسـكريًا، وتكنولوجيًـا، واقتصاديًـا [25].

الأمن السيبراني أولوية في استراتيجية الأمن القومي الروسية الجديدة:

خلافـاً للنسـخ السـابقة مـن اسـتراتيجية الأمـن القومـي الـروسي، أعـارت النسـخة الجديـدة اهتمامًـا خاصًـا بملـف الأمـن السـيبراني، وبهـذا المعنـى، بـات أمـن المعلومـات يشـغل أولويـة عـلى جـدول أعـمال روسـيا، ليـس فقـط عـلى المسـتوى الخارجـي، بـل عـلى المسـتوى الداخـلي أيضًـا، ويلاحـظ أن الرؤية الروسـية الجديـدة حرصـت عـلى اسـتخدام مصطلـح «أمـن المعلومـات» بديـلاً لـ «الأمـن السـيبراني»، تأكيـدًا منهـا عـلى أنـه أكـثر شـمولاً، لـذا فـإن مـن أبـرز وسـائل تحقيـق أمـن المعلومـات لـدى موسـكو هـو «تطبيـق السـيادة الوطنيـة كاملـة عـلى الفضـاء السـيبراني" Cyber Sovereignty وفي هـذا، الشـأن حـذرت الوثيقـة مـن أن

"التطور السريع لتكنولوجيات المعلومات والاتصالات يفاقم من احتمال ظهور مخاطر على أمن المواطنين والمجتمع والدولة، وأن توسيع نطاق استخدام تكنولوجيا المعلومات والاتصالات للتدخل في شؤون دول وتقويض سيادتها ووحدة أراضيها بات يشكل خطرًا على الأمن والسلام الدوليين" [26].

حيث ترى الاستراتيجية الجديدة أن الجهود الروسية الرامية إلى تعزيز «السيادة الوطنية الرقمية» تواجه تحديًا قويًا، لأنه لا توجد «لا توجد حلول قادرة على تنفيذ وصيانة نظام مغلق تمامًا غير متصل بالعالم الخارجي» ، ذلك أن فضاء المعلومات لا حدود له، ومستوى التطور التكنولوجي لا يسمح بعزلة كاملة للبلد بأكمله.. فقد أصبح العالم شفافًا للغاية [27].

وقد توقفت الاستراتيجية عند "تزايد عدد الهجمات على الموارد المعلوماتية الروسية، ومعظمها ينفّذ من خارج البلاد"، لتلفت الأنظار إلى أن "المبادرات الروسية الرامية إلى ضمان الأمن المعلوماتي الدولي تواجه معارضة من قبل دول أجنبية، تسعى إلى الهيمنة في الفضاء المعلوماتي العالمي"، وأظهر نص الوثيقة معارضة روسيا الكاملة للاتهامات الغربية لموسكو، وفي المقابل، قامت باتهام أجهزة استخباراتية أجنبية بتكثيف أنشطتها الرامية إلى تنفيذ عمليات تخريبية في المجال المعلوماتي الخاص بروسيا.

كذلك، ترى الوثيقة أن روسيا تواجه "حملات تضليلية وتخريبية" في الإنترنت تستهدف بالدرجة الأولى الشباب، (منها تداول أنباء كاذبة عن خطر تنفيذ هجمات إرهابية ودعوات للانتحار ونشر مواد متطرفة، والتحريض على ارتكاب أعمال غير قانونية، وترويج تناول المخدرات وغيرها)، كما توقفت الوثيقة عند اتهام شركات دولية عملاقة مثل "جوجل"، ادّعت أنها "تسعى إلى ترسيخ احتكارها في الإنترنت، والسيطرة على كل الموارد المعلوماتية، من خلال فرض الرقابة غير القانونية وإغلاق موارد معلوماتية بديلة"، ورأت أيضاً أن "رواد الإنترنت الروس يواجهون محاولات تهدف إلى فرض رؤية مشوّهة عليهم إزاء الحقائق التاريخية، والتطورات في روسيا، والعالم لدواعٍ سياسية"، وخلُصت إلى التحذير من أن «استخدام تكنولوجيات المعلومات والاتصالات الأجنبية في روسيا، يزيد من خطر تعرّض الموارد المعلوماتية في البلاد لمحاولات التأثير

عليها من الخارج.

وبهذه التحذيرات والاتهامات للغرب، تدفع استراتيجية الأمن القومي الروسي الجديدة عملياً إلى وضع ملف المواجهة السيبرانية، وأمن المعلومات في مقدمة معركتها الحالية مع الغرب، رافعة شعار "حماية روسيا من التأثير الغربي الضار على المجتمع"، ولذلك يظهر الهدف الرئيسي في "تعزيز سيادة البلاد في المجال المعلوماتي"، ويدفع هذا الهدف المعلن، إلى سلسلة من التدابير التي حددتها الوثيقة لحماية روسيا، وتعزيز سيادتها الرقمية، حيث بدأ منحى هدم جدران من "العزلة الرقمية" يتجسّد أكثر وأكثر في توجهات الاستراتيجية الروسية.

آليات حماية الأمن السيبراني في الإستراتيجية الروسية الجديدة [28]:

- إنشاء فضاء آمن لتداول المعلومات الموثوق بها.
- تحصين البنى التحتية الخاصة بالمجال المعلوماتي في روسيا.
- منع التأثير التخريبي بالوسائل المعلوماتية والتكنولوجية على الموارد المعلوماتية الروسية.
- تهيئة الظروف الملائمة لكشف ومنع الجرائم في الإنترنت.
- زيادة تحصين القطاع الروسي لشبكة الإنترنت ومنع أي سيطرة أجنبية على أنشطته.

هذا بالإضافة إلى أهداف أخرى، تمثلت في تقليص عدد حالات تسرب بيانات سرية وشخصية إلى أدنى حد ممكن، وتعزيز الأمن المعلوماتي الخاص بقوات الجيش الروسي ومنتجي الأسلحة والمعدات العسكرية، وتطوير وسائل وأساليب ضمان الأمن المعلوماتي باستخدام تكنولوجيات حديثة، منها الذكاء الاصطناعي، وإعطاء الأفضلية إلى استخدام التكنولوجيات محلية الصنع في البنى التحتية المعلوماتية في روسيا... وأخيراً، تعزيز التعاون مع الشركاء الأجانب في مجال ضمان الأمن المعلوماتي، بما يخدم خاصة إنشاء نظام دولي جديد خاص بهذا الشأن[29].

استراتيجية الأمن القومي الجديدة...والدعوة إلى تعزيز التعاون الدولي في مجال الأمن السيبراني:

انطلاقًا من رؤية موسكو بالأهمية الاستراتيجية للأمن السيبراني لتحقيق أمنها القومي، فقد دعت إلى معاهدة دولية مُلزِمة تنظم آليات الرقابة والمحافظة على أمن المعلومات، ولتحقيق ذلك استخدمت عددًا من الأدوات، منها:

- استغلال المنصات الدولية لحشد المجتمع الدولي لتبني فكرة ضرورة صياغة آلية تنظيمية ملزمة، وذلك بشأن مكافحة الاستخدام الإجرامي لتقنيات المعلومات، والاتصالات تحت رعاية الأمم المتحدة، حيث قدمت موسكو مشروع اتفاقية للتعاون في مكافحة الجرائم المعلوماتية، وذلك في محاولة لاستبدال اتفاقية بودابست لعام 2001، والتي وقعت عليها الولايات المتحدة الأميركية إلى جانب 55 دولة أخرى وترفضها روسيا، بل وتراها تهديداً مباشراً لسيادتها، وبخاصة ما يتعلق بالمادة 32 (ب) ،والتي تسمح لأصحاب البيانات بالسيطرة على استخدامها بدلاً من الحكومات، ويحاول المقترح الروسي وضع قواعد السلوك المتبعة في الفضاء السيبراني، والتحقيق المشترك في الأنشطة الخبيثة، وهو ما ترفضه واشنطن وغيرها من العواصم الغربية، التي رأت أن الاتفاقية المقترحة ستعزز من قدرات روسيا وغيرها من البلدان السلطوية في السيطرة على الاتصالات في الداخل، و في بلدان أخرى[30].
- عقد جولات للحوار مع العديد من الدول ذات الشأن في المجال السيبراني، لاسيما تلك التي لا تتفق مع وجهة النظر الروسية، وترى موسكو أنها تمثل تهديدًا على أمنها المعلوماتي وفي مقدمتها واشنطن، وبعض العواصم الأوروبية الأخرى، فخلال جولات الحوار الروسي الأمريكي التي بدأت في 2021 في جنيف كان الملف الأساسي المطروح على «أجندة» النقاشات يتعلق بأمن المعلومات، إلا أنه سرعان ما أبرز الحوار عن اختلاف وجهة النظر الروسية عن مثيلتها الغربية، إذ رأت موسكو أن واشنطن وعددًا

من الدول الغربية تدفع باتجاه أن ينحصر النقاش حول "الهجمات التي تعرّضت لها مواقع في الغرب من جانب قراصنة روس"، في حين تدعو موسكو إلى مناقشة أسس للتعاون المستقبلي في هذه القضية، عبر وضع آليات دولية ملزمة على شكل معاهدة خاصة بالأمن السيبراني، أيضاً ترى موسكو أن المدخل الأميركي للحوار، ليس فقط مجتزأ، بل أيضاً "يركز على قضية الهجمات السيبرانية بغرض الابتزاز السياسي، ولتوجيه الأنظار فقط إلى ملاحقة من يقفون وراء تلك الهجمات"، كما أوضح المسؤولون الروس.

ويمكن القول أن الفرق بين المطلبين الروسي والغربي في هذا الملف واضح، فروسيا لا تريد الخوض في الاتهامات المباشرة التي وُجِّهت ضدها، ولا تريد فتح تحقيق يؤدي إلى الكشف عن أشخاص محددين متورّطين - وفقاً للادعاءات الأمريكية والغربية - بمهاجمة مواقع غربية، بل تريد تحويل النقاش نحو تأسيس قواعد قانونية عامة وملزمة لجميع الأطراف الدولية، وكان لافتاً أن الإشارات التي وجّهتها موسكو حول مدى استعدادها للتعاون مع الغرب في مجال أمن المعلومات، وقد ارتبطت دائماً بشروط واضحة تفرض على كل الأطراف الالتزام بتعهدات مسبقة، وهو ما أوضحه الرئيس الروسي فلاديمير بوتين خلال لقاءه مع نظيره الأمريكي جو بايدن، بالإشارة إلى أن موسكو مستعدة لتسليم مرتكبي الجرائم السيبرانية إلى واشنطن في حال إبرام الطرفين اتفاقية رسمية تنصّ على التزاماتهما المتبادلة في هذا الصدد.

- عولى صعيد مقابل، اتجهت موسكو إلى تعزيز التعاون مع الدول التي تتفق ورؤيتها الاستراتيجية في مجال الفضاء السيبراني وتكنولوجيا المعلومات، كما هو الحال مع الصين، حيث يرى محللون أن ثمة تآلفًا واضحًا بين رؤية الدولتين فكلاهما تسعى إلى «السيادة التكنولوجية» كهدف رئيسي، بحيث تكون القوتان الشرقيتان قوتين متناغمتين استراتيجياً من ناحيتي الأهداف ومصادر التهديد [31]، ولتحقيق تلك الأهداف قامت موسكو في العام 2015 بالانضمام إلى منظمة شنغهاي للتعاون.

الخاتمة:

بصفة عامة ومما سبق يمكن الوصول إلى عدد من النتائج البحثية المهمة، وهي:

1- أن الطفرة الهائلة في تكنولوجيا المعلومات، والتي تعد سمة أساسية من سمات القرن الحادي والعشرين، قد أحدثت نقلة نوعية في ترتيب أولويات الأمن القومي للعديد من الدول، كذلك الخيارات المتوفرة لدى صناع القرار في تلك الدول لتحقيق أهدافها الاستراتيجية وبسط نفوذها وإبراز مكانتها على الساحة الدولية، وأصبح أمن المعلومات أو ما يطلق عليه «الأمن السيبراني" في مقدمة العناصر التي تتحدث عنها استراتيجيات الأمن القومي لتلك الدول، سواء كان مصدرًا للقوة وأداة تستخدمها لتحقيق منافع وأهداف داخلية وخارجية أم كان مصدرًا من مصادر تهديد لأمنها القومي قد يصل إلى حد التجسس عليها والتدخل في شأنها الداخلي.

بطريقة أخرى فإن تكنولوجيا المعلومات باتت ترسم خريطة ثقل الدول وتعطي صورة عن مكانتها على الساحة الدولية، حيث أن امتلاك أسلحة المعلومات يعطي ميزة استراتيجية خاصة للدولة، في حين تعتبر الدولة الضعيفة رقميًا سهلة الاصطياد.

2- أصبحت الحروب السيبرانية هي الأكثر بروزًا وانتشارًا على الساحة الدولية، وأصبح الفضاء السيبراني من أهم الأسلحة الاستراتيجية التي تستخدمها الدول في الحروب الحديثة، حيث باتت تلك أحد الأدوات الرئيسية لتحقيق الأهداف السياسية والعسكرية والاقتصادية للدول.

3- تعتبر روسيا الاتحادية تحت قيادة بوتين أحد أهم وأبرز الدول التي يحتل فيها الأمن السيبراني أولوية في استراتيجيات الأمن القومي بشكل معلن وصريح، وهو ما عبرت عنه استراتيجية الأمن القومي الروسية الأخيرة لعام 1202 والتي لا تزال معتمدة لدى صانع القرار الروسي حتى تاريخه، حيث تؤمن بفاعلية الحرب السيبرانية لما لها من آثار تدميرية على الدول الأعداء تشبه تلك التي تخلفها أسلحة الدمار الشامل.

4- تسعى الاستراتيجية الروسية الجديدة إلى التأكيد على اقتراب الوصول

إلى الوسائل النهائية للحروب المستقبلية والتي تبتعد عن النزاعات المسلحة التقليدية وتتوجه إلى قمع القيادة العسكرية وإيقاف عمليات الملاحة والاتصالات الخاصة بالعدو في مجال الفضاء الإلكتروني والتوجه نحو اختراق المعلومات التي يعتمد عليها، وعليه فإن استراتيجية روسيا حول الأمن السيبراني تقوم على «الهجوم» وذلك لاعتقادها بأن الترهيب والردع والتجسس على المعلومات لا يحقق الانتصار الكامل على الخصوم والأعداء.

5- لا يوجد حتى الآن اتفاق واضح على وضع آلية تنظيمية دولية ملزمة لمكافحة الاستخدام الإجرامي لتقنيات المعلومات والاتصالات، حيث تنقسم الدول الكبرى فيما بينها إلى معسكرين رئيسيين، هما: الغرب بقيادة الولايات المتحدة الأمريكية، والشرق بقيادة روسيا والصين، حيث يتصارع الطرفان فيما بينهما من أجل فرض وجهة نظره ورؤيته لكيفية تشكيل تلك القواعد والمبادئ الدولية التي من شأنها تنظيم التعامل مع التهديدات المحتملة في الفضاء السيبراني، ويزيد الأمر تعقدًا هو تحول كل من روسيا والصين من العزلة عن السياسات العالمية إلى الانخراط وبشدة بها بل والسعي تكتل قوي في مواجهة التكتل الغربي.

6- مستقبل الواجهة (الحروب) السيبرانية على الساحة الدولية:

مع بروز الحروب والصراعات السيبرانية على الساحة الدولية والتي لم تقتصر مخاطرها وآثارها السلبية على الفاعلين الدوليين التقليديين فحسب بل امتدت لتشمل المجتمعات والأفراد، انقسم المحللون حول مستقبل تلك الحروب ما بين الدفع بأنها ستشهد تقدمًا وسيطرة واضحين على الصعيد الدولي وآخر يدفع بانحسارها وتراجعها لتكون جزءًا من كل.

المشهد الأول: تقدم وسيطرة الحرب السيبرانية

إذا ما استمرت الحروب والهجمات السيبرانية في استهداف البنى التحتية وأنظمة الطاقة وإصابة شبكات المعلومات الحكومية والعسكرية، سيكون مستقبل الجميع معرض للتهديدات المتزايدة، وسيضحى جميع الأفراد والمؤسسات التي تعتمد على تكنولوجيا المعلومات في الخط الأمامي لتلك الحروب ولن يسلم من آثارها التدميرية أحد، وقد ذهب البعض

بـأن الحـرب السـيبرانية قـد بـدأت بالفعـل وأنهـا أصبحـت حقيقيـة وعالميـة النطـاق.

المشهد الثاني: تراجع وانحسار الصراعات والحروب السيبرانية

مـن المحتمـل ان يأخـذ الـصراع في المسـتقبل أشـكالاً صامتـة مختلفـة سـتبدأ بالهجمات السـيبرانية واسـتخدام أسـلحتها كالتشـويش علـى الأقمار الصناعية، والاختراقـات الخاصـة بعرقلـة الخصـوم، لكـن سـيكون دور هـذه الهجمـات مؤقتـًا ثـم يـتم الانتقـال بعـد ذلـك إلى الهجـمات الماديـة الفعليـة المدمـرة التـي ستسـتهدف الأصـول الفضـائية، وهـو مـا يثـير القلـق لـدى العديـد مـن الخـبراء حيـث سـتؤدي إلى انـدلاع حـرب فضائيـة باهظـة الثمـن.

7- مـع تزايـد حـدة الـصراع الـدولي عـلى الفضـاء السـيبراني، وتعـدد الفاعلـين القادريـن عـلى شـن الحـروب السـيبرانية مـع صعوبـة تحديـد جهـة الهجـوم، وحتـى في أوقـات السـلم يصبـح لهـا آثـارًا تخريبيـة واضحـة عـلى مختلـف مجـالات الحيـاة، أصبـح مـن الـضرورة بمجـال تكثيـف الجهـود الدوليـة للحـد مـن تلـك الآثـار فعـلى الصعيـد الـدولي: مـن خـلال التعـاون للوصـول إلى اتفـاق دولي ملـزم ينظـم اسـتخدام الفضـاء السـيبراني ويضـع آليـات لإيقـاف والحـد مـن الجرائـم السـيبرانية، كـما يضـع حـدًا للـصراع بـين الـدول في هـذا المجـال ويفتـح البـاب أمـام التعـاون فيـما بينهـا لمـا فيـه مـن تقـدم للبشريـة جمعـاء، وداخليًـا: مـن خـلال إنشـاء أقسـام خاصـة في الـدول لمواجهـة الهجـمات السـيبرانية عـلى أيـدي متخصصـين في هـذا المجـال.

المراجع

1. بدأت الإرهاصات الأولى لإطلاق مفهوم الحرب السيبرانية منذ عام 1993 عندما كتب كل من (John Arquilla and David Ronfeldt) مقالا تحت عنوان "الحرب السيبرانية قادمة!"، والتي توقعا فيها العديد من التحديات التي سيواجها الأمن القومي الغربي مستقبلاً، ومن بينها أن المفاهيم المرتبطة بالفضاء السيبراني ستحدث تغييرات جذرية في دور الجيوش وآليات عملها، وعرف الكاتبان الحرب السيبرانية بأنها "إجراء والاستعداد لإجراء العمليات العسكرية بالاعتماد على المبادئ والآليات المعلوماتية، ما يعني تعطيل – إن لم يكن تدمير – نظم المعلومات والاتصالات على أوسع نطاق لتشمل حتى العقيدة العسكرية للعدو".
2. العلي زياد علي, الصراع والأمن الجيوسبراني في السياسة الدولية: دراسة في استراتيجيات الاشتباك الرقمي ،عمان، دار المجد للنشر والتوزيع، المملكة الهاشمية الأردنية .
3. الموسوعة السياسية، الأمن السيبراني، متاحة على الإنترنت على الرابط
www.polotical encyclopaedia.org
4. سري غضبان غيدان، الأمن السيبراني وسياسات المواجهة الدولية، المركز الديمقراطي العربي – مجلة الدراسات الاستراتيجية والعسكرية، العدد التاسع، برلين، ديسمبر 2020.
5. إيهاب خليفة: الأمن السيبراني. الماهية والإشكاليات، مركز المستقبل للأبحاث والدراسات المتقدمة، أبو ظبي، أكتوبر 2019.
6. أماني عصام، استخدام روسيا للقوة السيبرانية في إدارة تفاعلاتها الدولية، مجلة كلية الاقتصاد والعلوم السياسية، المجلد 22 العدد 4، أكتوبر 2021
7. عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الانساني، (الإسكندرية: وحدة الدراسات المستقبلية، 2017).
8. د. عبد الغفار عفيفي، "الأزمات والحروب السيبرانية... تهديدات تتجاوز الفضاء الإلكتروني"، دراسة، مركز صقر للدراسات، العراق، 15 فبراير 2019.
9. نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية: دراسة في أبعاد الأمن الإلكتروني (القاهرة: المكتب العربي للمعارف، 2018).
10. أماني عصام، مرجع سابق.
11. رغدة الهبي، "الردع السيبراني: المفهوم والإشكاليات والمتطلبات"، مفاهيم

استراتيجية، القاهرة: المركز العربي لأبحاث الفضاء الإلكتروني، 2017،
12. نوران شفيق، مرجع سابق
13. أماني عصام، مرجع سابق.
14. أماني عصام، مرجع سابق.
15. مايكل كوفمان، كاتيا ميجاشيفا، برايان نيشيبوروكج، أندرو رادين "عبر من عمليات روسيا في شبه جزيرة القرم وشرق أوكرانيا"، (كاليفورنيا: مؤسسة راند، 2017)،
16. مايكل كوفمان وآخرؤون، مرجع سابق
17. علي زياد فتحي، العمليات السيبرانية الأوروأطلسية ومهددات الجيوسيبرانية الروسية. رؤية في الاشتباك الجيوسيبراني الأورو- روسي، مجلة رويه استراتيجية، العدد 30 ربيع 2019)
18. عادل عبد الصادق، صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية، الموقع الإلكتروني للمركز العربي لأبحاث الفضاء الإلكتروني، 24/5/2022
19. موقع وكالة الأنباء رويترز باللغة العربية، 27/1/2018.
20. ليكسى كلينيكوف، "متلازمة أفغانستان: اتجاهات الرأي العام الروسي تجاه التدخل العسكري في سوريا"، اتجاهات الاحداث، فبراير 2016، العدد 15.
21. علي زياد فتحي، مرجع سابق.
22. محمد سيف الدين، ماذا حققت استراتيجية الامن القومي الروسي 2020-2012 (2-1)، 22/7/2021 - موقع الميادين على الإنترنت
https://www.almayadeen.net/butterfly-effect.
23. معركة الأمن السيبراني تحدد مسار الحوارات الروسية الغربية، مصدر سابق
24. ديميتري كرنين مدير مركز كارنيجي في موسكو
25. فراس بورزان، روسيا "القطب": قراءة في وثيقة الأمن القومي الجديدة، 12/2/2022
26. صراع السيادة السيبرانية بين التوجهات الأمريكية والروسية- مرجع سابق
27. حوار أجرته صحيفة الشرق الأوسط مع لايما جيرمانوفا – مدير مؤسسة كريبروم للأبحاث في روسيا، بتاريخ 31/7/2021
28. معركة الأمن السيبراني، صحيفة الشرق الأوسط. مصدر سابق
29. محمد سيف الدين، أمن روسيا: اتجاه استراتيجي أكثر ثقة، 16/7/2021
30. د. عادل عبد الصادق، صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية، مرجع سابق
31. أمن روسيا: اتجاه استراتيجي أكثر ثقة، مصدر سابق