استخدام روسيا للقوة السيبرانية فى إدارة تفاعلاتها الدولية

د. أمانى عصام محمد *

مستخلص

لم تقتصر تأثيرات اختراق الثورة التكنولوجية لمجالات الحياة المختلفة على التفاعلات المجتمعية والاقتصادية والسياسية فقط، بل امتدت لتخلق ساحة جديدة من الحروب غير التقليدية بعيداً عن ساحات البر والجو البحر، وهى ساحة الفضاء السيبرانى التى توافرت فيها عدة عوامل حفزت بعض الدول والفاعلين من غير الدول على استخدامها كإحدى أدوات الصراع والتنافس والهيمنة والإرهاب غير التقليدى، لدرجة تدعو بعض المحللين إلى القول بأن ما يشهده العالم من هجمات إلكترونية مختلفة قد ينقلنا إلى نموذج جديد من الحروب يطلق عليه اسم الحرب السيبرانية Cyber War، وهو ما استخدمته روسيا بجدارة فى اكثر من دولة واكثر من حالة كما يتضح فى البحث. فالقيادة الروسية عملت في السنوات القليلة الماضية بشكل دؤوب على تنمية قدرات روسيا في المجال السيبراني وتطويرها بشكل كبير، وسخرّت تلك القدرات بصورة ذكية كسلاح فعّال لإيقاع الضرر المطلوب في قدرات خصومها، بالشكل الذي جعل من تلك القدرات السيبرانية احد عناصر الردع الاستراتيجي للدولة الروسية.

كلمات مفتاحية: القوة السيبرانية- روسيا- الثورة التكنولوجية- الفضاء السيبرانى- هجمات الكترونية- الاستراتيجية الروسية السيبرانية.

Abstract:

The effects of penetrating the technological revolution in different spheres of life have not only affected societal, economic and political interactions, but have spread to create a new arena of unconventional wars away from the land and sea, the Cyberspace arena, where several factors have been available that have motivated some states and non-state actors to use them as instruments of conflict, competition, domination and unconventional terrorism, to the point

* مدرس بقسم العلوم السياسية – كلية التجارة وادارة الاعمال – جامعة حلوان
Email: amanyessam@yahoo.com

where some analysts argue that the world's various cyber attacks may move us to a new model. From wars is called cyber war, which Russia has well used in more than one country and more than one case, as evidenced in the research. In the past few years, the Russian leadership has worked tirelessly to significantly develop and develop Russia's cyber capabilities, cleverly harnessing those capabilities as an effective weapon to inflict the required damage on the capabilities of its adversaries, making such cyber capabilities one of the strategic deterrents of the Russian State.

Key Words: Cyber Power – Russia – Technological Revolution – CyberSpace – Cyber Attacks – Russian Cyber Strategy.

مقدمـــة:

من المؤكد أنه من بين أهم القضايا التي باتت تشغل العالم قضية العالم الافتراضي والفضاء السيبراني، ذاك الذي أضحى واقعا موازيا للعالم الحقيقي، بل لا نغالي إن وصفناه أنه في بعض الأوقات يكون خطره أكثر دموية ، لا سيما وأن صداماته تجري بعيدا عن الأعين، وإن كانت لا تغيب بالطبع عن القائمين عليه من خبراء متمرسين وراء الشاشات، في محاولة للتأثير على مجريات العالم السياسية والاقتصادية من جهة، والمعطيات الأمنية والعسكرية من جهة ثانية، ومرد هذا وذاك أن جزءا كبيرا من الصراعات بين القوى العظمى في العالم، قد انتقلت من ميادين القتال الكلاسيكية إلى شبكات الإنترت والعالم السيبرانى.[١]

فقد أدت الثورة التكنولوجية والمعلوماتية إلى بروز الفضاء السيبرانى ليكون أحد مجالات التنافس والصراع بين القوى الكبرى، وظهر لأول مرة مفهوم الحرب السيبرانية التى يعتبرها البعض حروب المستقبل، وأنها لا تقل خطورة عن الحروب التقليدية من حيث التهديد الذى تنطوى عليه وحجم التدمير الذى يمكن أن تؤدى إليه أخذاً فى الاعتبار السرعة الفائقة، والانتشار الواسع، وكونها تُنفَّذ بأساليب يصعب تتبعها فى كثير من الأحيان. مثل هذه الهجمات الإلكترونية تكون بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الإلكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل. ففي خضم التوتر المتصاعد بين موسكو وواشنطن

[١] د. عبدالغفار عفيفي الدويك، "الأزمات والحروب السيبرانية... تهديدات تتجاوز الفضاء الإليكتروني"، دراسة، مركز صقر للدراسات، العراق، ١٥ فبراير ٢٠١٩.

حول مدى واسع من القضايا الثنائية والإقليمية، تزداد حدة المواجهة السيبرانية بينهما في ضوء الاتهامات المتبادلة بتوجيه هجمات إلكترونية على أهداف حيوية مختلفة.

يتزامن هذا مع تسابق البلدين لتعزيز أمنهما السيبرانى فى مواجهة أى هجمات محتملة من الطرف الآخر، ففى ١٠ سبتمبر ٢٠١٨ أنشأ جهاز الأمن الفيدرالى الروسى مركزاً وطنياً لتنسيق مكافحة الهجمات السيبرانية على البنية التحتية الحيوية فى روسيا، يتولى مهام الكشف والوقاية والقضاء على تداعيات الهجمات الإلكترونية، وتبادل المعلومات بين الهيئات المتخصصة فى الداخل والخارج، وتحليل الهجمات السيبرانية الماضية وتطوير أساليب مكافحتها. وجار العمل على فصل روسيا كلها عن الإنترنت بهدف زيادة فاعلية دفاعاتها ضد الهجمات الإلكترونية والقرصنة، حيث إن تداول البيانات بين المواطنين والمؤسسات في هذه الحالة سيكون داخل البلاد لا عن طريق مراكز توجيه دولية.

وكان البرلمان الروسى قد وافق فى ١٢ من فبراير ٢٠١٨ على قانون عزل البلاد عن شبكة الإنترنت العالمية، لجعل البلاد فى موقع أفضل لصد أى هجمات إلكترونية محتملة من الخارج، وبخاصة من الولايات المتحدة، وذلك على غرار نظام جريت فايروول الصينى، الذى ينظم الإنترنت لتعزيز السيادة الوطنية، من ناحية أخرى، تعزز واشنطن من دفاعاتها السيبرانية أيضاً، حيث أنشأت القيادة الإلكترونية الأمريكية مجموعة عمل خاصة لمواجهة أنشطة روسيا فى الفضاء السيبرانى، ووقع الرئيس الأمريكى دونالد ترامب مرسوماً فى ١٦ أغسطس ٢٠١٨ يلغى بموجبه التوجيه الرئاسى لسلفه باراك أوباما لتنظيم استخدام الأسلحة السيبرانية ضد معارضى الولايات المتحدة، رقم ٢٠ لعام ٢٠١٢، على النحو الذى يخفف القيود المفروضة على شن هجمات سيبرانية ضد معارضى واشنطن. وقد ظل مضمون هذه الوثيقة سرياً حتى عام ٢٠١٣، عندما كشف الموظف السابق فى وكالة الأمن القومى الأمريكية إدوارد سنودن عن عدد من الوثائق السرية المتعلقة بعمل أجهزة الاستخبارات الأمريكية والبريطانية. كذلك أصدر البنتاجون مطلع عام ٢٠١٨ قائمة «لا تشتر» متضمنة أسماء عدد من الموردين الذين ربما استهدفتهم مجموعات القراصنة المعادية الذين تدعمهم روسيا والصين، وجرى تعميمها على مسؤولى عمليات الشراء الذين يعملون مع الجيش الأمريكى لتزويده بالخدمات المرتبطة بالتكنولوجيا وغيرهم من الفرق المسؤولة عن توفير البرمجيات للقوات المسلحة الأمريكية.

على الرغم من كل الجهود من الجانبين لتعزيز الأمن السيبرانى يظل سباق الهجمات السيبرانية قائماً، وربما يتصاعد فى ظل التوتر المتزايد بين موسكو وواشنطن، وإعلان ترامب تخليه عن حيادية شبكة الإنترنت، وهو الأمر الذي يثير مخاوف القوى الكبرى في

النظام الدولى، وخصوصاً الصين وروسيا اللتين تطالبان بانفتاح أمريكي في التعامل مع فرص السيطرة الدولية على أمن الفضاء الإلكتروني.[٢]

أهمية الدراسة:

- **الأهمية العلمية:**

تبرز أهمية البحث من الناحية العلمية كونه يشكل دراسة تشخيصية وتحليلية لما يعيشه عالمنا المعاصر اليوم من تخمة فى التطورات التكنولوجية التى فاقت حد الحاجات الضرورية لواقع الانسان فى دوله المختلفة، الامر الذى أغرى دولاً وجماعات كثيرة على استغلال هذا الفائض من التقدم التكنولوجى والمعرفى ليصب فى اتجاهات سلبية تعرض الكثير من دول العالم الى القرصنة غير المحسوبة أو الخارجة عن نطاق قدراتها بما يغرى الدول العظمى أو من يملكون مثل هذه القدرات أن يحققوا أهدافهم على حساب قوى لم تلحق بهذا التطور العلمى للحد من اثاره السلبية، وإعادة تشكيل العالم الافتراضى بما يخدم مصالحهم دون غيرهم.

- **الأهمية العملية:**

تتمثل الأهمية العملية فى بروز دور الفضاء الإلكترونى بوضوح كمجال جديد فى العمليات العدائية، كان أهم صوره الصراع بين أستونيا وروسيا فى ٢٠٠٧، والحرب بين روسيا وجورجيا فى عام ٢٠٠٨، وبين كوريا الجنوبية والولايات المتحدة الأمريكية فى عام ٢٠٠٩ والتى شهدت هجمات إلكترونية كورية على شبكات البيت الأبيض. وجاء الهجوم الإلكترونى بفيروس "ستاكسنت" على برنامج إيران النووى عام ٢٠١٠ ليمثل نقلة مهمة فى تطور واستخدام الأسلحة الإلكترونية، ثم الدور السياسى الذى لعبته شبكات التواصل الاجتماعى فى إدارة الفوضى فى عدد من الدول العربية خلال عامى ٢٠١١، ٢٠١٢، والهجوم على آلاف من أجهزة كمبيوتر فى شركة النفط السعودية "أرامكو" فى عام ٢٠١٦، وهجمات القراصنة ضد قطاعات الطاقة والصناعة والنقل وشركات الطيران المدنى فى بعض دول الخليج.

وهكذا، أصبحت الحروب اليوم حروبا هجينة، تلعب الأدوات والساحة السيبرانية فيها دورا رئيسيا. كما أصبحت "الحرب السيبرانية" تتسم بدرجة كبيرة من التطور السريع والمنافسة الشديدة، بسبب المنافسة القائمة بين شركات البرمجيات الكبرى، والتعاون بين هذه الشركات وشركات تصنيع السلاح، وفرص التكامل الكبيرة بين الجانبين.

---

[٢] د. نورهان الشيخ، "موسكو وواشنطن.. صراع سيبراني"، الخليج، 27/06/2019.
http://www.alkhaleej.ae/supplements/page/3c792d51-a025-437d-9f36-36d361c7cd33

اشكالية الدراسة:

أصبح الفضاء الالكترونى أحد العناصر الرئيسية التى تؤثر فى النظام الدولى بما يحمل من أدوات تكنولوجية تلعب دوراً مهماً فى عملية التعبئة والحشد فى العالم، فضلاً عن التأثير فى القيم السياسية، فسهولة استخدامها ورخص تكلفتها ساعدا على قيامها بأدوار مختلفة فى الحياة البشرية، سواء تجارية او اقتصادية او معلوماتيه او سياسية او عسكرية او ايديولوجية، ومن هنا قامت بعض دول العالم في السنوات الأخيرة بتطوير استخدام مهارات الإنترنت والحواسيب كأدوات هجوم ودفاع واستخبارات وحروب نفسية. فقد أنشأت الولايات المتحدة وبريطانيا وفرنسا وكوريا الجنوبية وروسيا وحدات خاصة في قوّاتها المسلحة مسؤولة عن الحرب الإلكترونية أو حرب المعلومات. وتجمع هذه الوحدات الخاصة ما بين العقل العسكري والمهارات التقنية التي تمكّنها من الدفاع وصدّ الهجمات أو إحداث خسائر.

من ناحية أخرى، يتزايد استخدام الإنترنت بشكل عام، ووسائل التواصل الاجتماعي بشكل خاص، كأداة فعالة في الحرب التي تشنها التنظيمات المسلحة لا سيما في الشرق الأوسط. فقد وجدت هذه المجموعات في الفضاء الإلكتروني وسيلة مفيدة في صراعها، فاستخدمت وسائل التواصل الاجتماعي لتجنيد المقاتلين. كما استفادت هذه التنظيمات من الفضاء الإلكتروني كمنصّة لإطلاق الحرب النفسية ضد الخصوم بتصوير مشاهد العنف ونشرها على نطاق واسع لبثّ الرعب والذعر. كذلك، يُستخدم الإنترنت في شن هجمات إلكترونية **Cyber attacks** من شأنها إلحاق خسائر بالخصم، غالبًا ما تكون مالية، فيجري استهداف البنوك أو المواقع الحكومية التي تحتوي على بيانات مهمة، أو حتى استهداف منشآت صناعية، كما حدث لبرنامج إيران النووي[٣].

هذا فضلاً على أنها لم تعد حكراً على الدول فقط، بل ان شركات التكنولوجيا العملاقة هى التى تسيطر بدرجة ما على المقومات التكنولوجية، وقد أصبح جلياً أن من يمتلك آليات توظيف هذه البيئة الالكترونية الجديدة يصبح الأكثر قدرة على تحقيق أهدافه والتأثير فى سلوك الفاعلين المستخدمين لهذه البيئة. ومن هنا فقد استطاعت روسيا توظيف التكنولوجيا الحديثة فى تعظيم قوتها من خلال القوة الالكترونية **Cyber Power**، حيث سعت إلى الاستفادة من تلك القوة فى تطوير استراتيجياتها العسكرية والسياسية من أجل حماية مصالحها الوطنية.

---

[٣] وفق تقرير شركة سيمانتك العاملة في مجال الأمن الإلكتروني، فإنّ نسخة من فيروس الكمبيوتر «ستكسنت **Stuxnet**» استُخدمت لمهاجمة وتدمير برنامج إيران النووي في العام ٢٠١٠، بالتعاون بين الولايات المتحدة والكيان الإسرائيلي.

التساؤل البحثى:

من خلال ما تم توضيحه فى اشكالية الدراسة نتطرق الى التساؤل الرئيسى كالتالى:
كيف تستخدم الدول (روسيا) القوة السيبرانية فى إدارة تفاعلاتها الدولية؟

منهج الدراسة:

تعتمد الدراسة على:

المنهج الوصفي التحليلي: حيث يهدف هذا المنهج إلى تحقيق الفهم الدقيق والإحاطة بالأبعاد الواقعية للظواهر والموضوعات. ومن هنا فالقواعد الأساسية التي يقوم عليها المنهج الوصفي هي تحديد الظواهر المراد بحثها، وجمع المعلومات الدقيقة عنها وفحصها ودراستها، ومحاولة الإحاطة بعدد كبير من الأبعاد والعلاقات المرتبطة بالظاهرة للإنتقال من مستوى الفهم البسيط إلى المستوى المركب، وما يرتبط بذلك من صياغة عدد من النتائج والتعميمات والتوصيات التي ترشد عملية البحث، وذلك من خلال محاولة وصف وتحليل مفهوم القوة السيبرانية (الإلكترونية) والأسس والمرتكزات التي قامت عليها إستراتيجية القوة السيبرانية الروسية مع الدول المختلفة.

منهج المصلحة الوطنية: يعتبر المنهج أن الهدف الآساسى للدولة هو تحقيق المصلحة الوطنية، وعلى هذا الأساس أنصار هذا المنهج يركزون فى دراسة العلاقات الدولية على كل مايتعلق بالمصلحة الوطنية، وهى تتضمن الاستمرارية بمعنى المصالح.

التحديد الزمنى والمكانى:

تطبق الدراسة على روسيا واستخدامها للقوة السيبرانية، وتبدأ فترة الدراسة من عام ٢٠٠٧، حيث الهجوم الروسى على استونيا بسلسلة من الهجمات ضد المواقع التى تديرها الحكومة الإستونية، حتى عام ٢٠١٥، حيث قضية حزب الاتحاد الديمقراطى الالمانى.

اسخدام روسيا للقوة السيبرانية فى إدارة تفاعلاتها الدولية

تتعدد استخدامات القوة السيبرانية فى إدارة التفاعلات الدولية، وتختلف الآلية التى تدير بها روسيا تفاعلاتها وفقاً لطبيعة الظروف الدولية المحيطة، سواء فى شكل تفاعلات سياسية او عسكرية، او اقتصادية أو غيرها. وقد استخدمت روسيا تلك القوة من خلال أنماط عديدة تتمثل فى: تعطيل الخدمة، السيطرة على الأنظمة العسكرية، إتلاف المعلومات أوتعديلها، سرقة المعلومات والبيانات العسكرية، جمع معلومات اقتصادية استخباراتية، التحكم فى العقل والسيطرة عن بعد، وأخيراً الحرب النفسية.

أولاً: الاستراتيجية السيبرانية الروسية للأمن السيبرانى:

يعد الهدف الأسمى للأمن السيبرانى هو القدرة على مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافى، وبالتالى التحرر من الخطر أو الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا المعلومات والاتصالات أو بسبب إساءة استخدام تكنولوجيا المعلومات والاتصالات ويتطلب حماية الشبكات وأجهزة الكمبيوتر،

والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به، ونتيجة لأهمية الأمن السيبرانى فى واقع مجتمعات اليوم فقد جعلته العديد من الدول على رأس أولوياتها، خاصة بعد الحروب الإلكترونية التى بدأت تظهر تجلياتها بين بعض الدول الكبرى، فى إشارة صريحة إلى نهاية الحروب التقليدية التى كانت تستخدم فيها الأسلحة الثقيلة، والإعلان عن بداية حروب جديدة هي الحروب الإلكترونية.

وقد بدأ الاهتمام الروسى بالأبعاد السياسية للأمن الإلكترونى فى التسعينات من القرن الماضى بعد تأسيس مجلس الأمن الروسى فى عام ١٩٩٢، وإضافة إلى المؤسسات الأمنية الروسية تم إنشاء مؤسسات أخرى تختص فقط بالقضايا الإلكترونية وبحماية الأمن الإلكترونى الروسى. ومن أهم المؤسسات المسئولة عن الأمن الالكترونى فى روسيا هى مجلس الأمن، وجهاز الأمن الفيدرالى، جهاز الحرس الفيدرالى، والجهاز الفيدرالى للتحكم التقنى، ووزارة الاتصالات وتكنولوجيا المعلومات.

وتنقسم المهام ما بين الإدارات المختلفة فى الأنشطة المتعلقة بالأمن الإلكترونى كالتالى: تختص وزارة الداخلية بمواجهة الجرائم الالكترونية، ووزارة الدفاع مسئولة عن كل ما يتعلق بأخطار الحروب الإلكترونية وتطوير القدرات الإلكترونية الهجومية للجيش الروسى، ويهتم جهاز الأمن الفيدرالى بالارهاب الإلكترونى. هذا التقسيم قائم بالأساس على التفرقة ما بين الأبعاد الإجرامية، والارهابية، والعسكرية، والسياسية للأمن الإلكترونى.

ولقد تبلور الاهتمام الروسى بقضايا الأمن الإلكترونى فى عام ٢٠٠٠، فعندما قامت روسيا بتطوير استراتيجية أمنية تبنى على أساس الإيمان الكامل بالدور الذى يلعبه الأمن الإلكترونى فى تحقيق المصالح القومية وتعزيز الاستقرار الاجتماعى والسياسى. وتتصدر روسيا الدول الساعية لتطوير اتفاقية دولية لمواجهة المخاطر الإلكترونية والحيلولة دون حدوث سباق للتسلح الإلكترونى نتيجة لتزايد التنافس التكنولوجى ما بين الفواعل على المستوى الدولى، ويتم من خلالها وضع تعريفات واضحة يقبلها المجتمع الدولى لكافة المفاهيم المحورية ذات الصلة بالفضاء الالكترونى.[١]

وقد أعلنت روسيا أيضاً فى عام ٢٠١٠ عن العقيدة العسكرية الخاصة بها، والتى أشارت إلى أن الصراعات العسكرية الحديثة تتضمن الاستخدام المتكامل للقدرات العسكرية وغير العسكرية، مع الاهتمام بإبراز دور أكبر لحرب المعلومات. وقد تم تشكيل قيادة مستقلة للأمن السيبرانى، هذا علاوة على الإدارة السيبرانية داخل الجيش الروسى لتعزيز جاهزية القوات المسلحة الروسية للدفاع ضد الهجمات السيبرانية، واتخاذ الاجراءات الاحترازية ضد الهجمات السيبرانية من خلال الشبكات. وقامت روسيا بشراء آلات كاتبة لاستخدامها فى المكاتبات الحيوية حتى لا تتعرض المكاتبات السرية للاختراق، وبلغ الانفاق العسكرى الروسى على حرب الفضاء الالكترونى ١٢٧ مليون دولار من إجمالى إنفاق عسكرى بلغ ٤٠ بليون دولار فى روسيا، التى تحتل المركز

الرابع عالمياً فى مجال تطوير قدرات الاسلحة الالكترونية.[٢] وفى عام ٢٠١٣، توافقت كل من الولايات المتحدة الامريكية وروسيا على انشاء "الخط الساخن السيبرانى" للمساعدة فى نزع فتيل أى أزمات تتعلق بالانترنت فى المستقبل.[٣]

ومن ناحية أخرى اعتزمت روسيا من خلال منظمة "البريكس"[٤] تأسيس فضاء إلكترونى خاص بها مستقل عن شبكة الانترنت الحالية بهدف التخلص من الهيمنة وعمليات التجسس الالكترونى الامريكية، واتخذت خطوات فعلية لذلك، حيث تقوم البرازيل ببناء منظومة الكابلات التى يمكن أن تربطها بروسيا والصين وجنوب افريقيا، بكابل طوله ٣٤ ألف كيلو متر، وهو يربط بين مدينة "فلاديفوستوك" فى شرق روسيا و"فورتاليزا" فى البرازيل، مروراً بشانتو الصينية و"تشيناى" الهندية و"كيب تاون" فى جنوب افريقيا، ليس هذا فحسب، بل من المتوقع أن يوفر المشروع خدمات الإنترنت فى ٢١ دولة افريقية، وبذلك يتم انشاء شبكة انترنت جديدة موازية لشبكة الانترنت الحالية، وتكون منافساً قوياً للولايات المتحدة، وتعتزم دول "البريكس" أيضاً إصدار تشريعات تجبر القوى الرئيسية فى الانترنت مثل "جوجل" و"فيسبوك" و"ياهو" على تخزين المعلومات كافة التى يتم جمعها داخل دول المجموعة محلياً، كى لا تتمكن وكالة الأمن القومى الأمريكية من الوصول إليها.[٥]

وفى السنوات الأخيرة، قامت الحكومة الروسية بعمليات تقييم لمخاطر التهديدات الإلكترونية، إلا أن نتائجها وما أسفرت عنه من سياسات لم يتم الاعلان عنه للعامة. ولكن بشكل عام يمكن القول بأن روسيا تضع المخاطر الإلكترونية فى المرتبة الخاصة بالتطرف والمخاطر البيئية والجريمة المنظمة العابرة للحدود، وتأتى الهجمات الإلكترونية ضمن قائمة أكثر عشرة مخاطر تهدد البنية التحتية، وذلك وفقاً لاستراتيجية الأمن القومى الروسية. وتأتى فى المرتبة الثانية، ضرورة تطوير القدرات التكنولوجية للقوات المسلحة حتى يتحقق الردع الإلكترونى.[٦]

وتعتمد الاستراتيجية الروسية الخاصة بالحروب الإلكترونية مثل الصين على استخدام الأسلحة الإلكترونية الهجومية باعتبار أنها قوة مضاعفة **Fore Multiplier** فى الحروب، بمعنى أنها تزيد من القدرات القتالية للدولة إذا ما تم استخدامها إلى جانب قدرات عسكرية أخرى. كما تعتمد الاستراتيجية الروسية على محاولة تعطيل البنية التحتية المعلوماتية للخصم، والاتصالات المدنية والعسكرية له قبل البدء فى العمليات العسكرية التقليدية. فوفقاً للعقيدة العسكرية الروسية، لابد وأن يسبق الهجوم العسكرى الناجح عمليات أخرى تهدف إلى منع الخصم من الحصول على معلومات من مصادر خارجية، وتعطيل عمليات التداول المالية والائتمانية، ومحاولة التأثير فى الرأى العام فى الدولة الخصم عن طريق المعلومات الخاطئة والدعاية التى تخدم المصالح الروسية. ومن ثم يساعد التخطيط فى مرحلة ما قبل الهجوم للقيام بعملية الاختراق السرى لأنظمة

الخصم فى تحقيق هذه الأهداف. وأبرز مثال على تلك الهجمات التى اتهمت روسيا بشنها سنة ٢٠٠٨ ضد جورجيا قبل توجيه ضربة عسكرية ضدها.[٧]

ثانياً: استخدام القوة السيبرانية الروسية فى التفاعلات الدولية العسكرية:

لقد تعددت أدوات القوة السيبرانية متمثلة فيما يلى..

١.تعطيل الخدمة- وشل البنية التحتية (الهجوم على استونيا):

قامت روسيا فى عام ٢٠٠٧ بشن حرب سيبرانية شاملة على استونيا بسبب نقل تمثال يخلد تضحيات جنود روس فى الحرب العالمية الثانية[٨]، فبدأت سلسلة من الهجمات يطلق عليها DDOS attacks ضد المواقع التى تديرها الحكومة الإستونية، وتسبب الهجوم فى عرقلة ولوج المواطنين إلى بعض المواقع مثل موقع الحزب السياسى الذى ينتمى إليه رئيس الوزراء.[٩] من جهة أخرى، استخدمت الروابط التى ترعاها الحكومة فى تضليل المستخدمين، وإعادة توجيههم إلى صور للجنود السوفييت، واقتباسات من مارتن لوثر كينج عن محاربة الشر، مما أدى إلى دمار لوجيستى كبير.[١٠] ولم يعد المواطنون قادرين على إجراء معاملاتهم البنكية الإلكترونية التى يتم ٩٧% منها عبر الانترنت، أو التواصل مع بعضهم بالبريد الالكترونى لأيام عديدة، وتم تعطيل البنية التحتية للاقتصاد الرقمى الاستونى.[١١]

ونتيجة لشدة تعقيد هذه الهجمات، وما أحدثته من شلل كامل لكافة أجهزة الدولة، استعانت استونيا بحلف شمال الاطلنطى لمواجهتها، ووجهت استونيا الاتهامات للحكومة الروسية بأنها تقف ما تعرضت له من هجمات بعد أن اكتشفت ان انظمة التحكم التى شنتها موجودة فى روسيا، وعلى الرغم من انكار روسيا لصلتها بالهجوم، إلا انها اعترفت انه من الممكن ان يكون قد شن من داخل روسيا من قبل منظمات إجرامية غاضبة من القرار الإستونى بنقل التمثال. هذا وقد انقسمت الهجمات الالكترونية التى تعرضت لها استونيا فى ٢٠٠٧، الى مرحلتين:[١٢]

أ. المرحلة الاولى: الرد المباشر من 27-29 ابريل .

بدأت الهجمات باستهداف المواقع الالكترونية الحكومية والاعلامية التى بثت أخبار عن العمل فى استونيا، كموقع رئيس الوزراء، والرئيس والبرلمان والوزارات، ومؤسسات الدولة الأخرى كالشرطة، وموقع الائتلاف الحاكم. وتم اختراق عديد من المواقع الأخرى، والتى كان من بينها موقع حزب الاصلاح الذى قام المهاجمون من خلاله بنشر اعتذار رسمى مزور باللغة الروسية عن نقل التمثال والذى يبدو وكأنه صادر من رئيس الوزراء الإستونى، ولكن اتسمت هذه الهجمات فى هذه المرحلة ببساطتها، إذ كانت أشبه بالاحتجاج الشعبى.

ب. المرحلة الثانية: من 30 ابريل الى 18 مايو.

شهدت تلك الفترة هجمات أكثر تعقيداً وتنظيماً، تم فيها استخدام البوتنتس Botnets[١٣] وهجمات الحرمان من الخدمة الموزعة، والتى اتسع نطاق استهدافها لتهاجم اكبر البنوك الموجودة فى إستونيا، ولقد فاق عدد طلبات الدخول الى هذه المواقع ٤٠٠ ضعف المستوى الطبيعى. كما استهدفت أيضاً البنية التحتية القومية للإنترنت، وخط الطوارىء القومى للحيلولة دون تلقى الشكاوى من المواطنين.

هذا وكان للهجوم الالكترونى الذى تعرضت له استونيا آثاراً قصيرة المدى وطويلة المدى، سواء على المواطنين أم الأجهزة الحكومية، أم البنوك، فمن جهة. ترتب على الهجوم تعطيل كامل لكافة الخدمات التى تقدمها الحكومة للمواطنين لفترة طويلة نسبياً حتى تمكنت الدولة من استعادة سيطرتها على المواقع التى تمت مهاجمتها. ونتيجة لاعتماد استونيا بشكل كبير على الانظمة الالكترونية لإدارة شؤون الدولة، وتقديم خدمات للمواطنين، كان من شأن هذا الهجوم أن يعطل مصالح المواطنين بشكل كامل، وأن يشل حركة الاقتصاد والمعاملات البنكية الخاصة والحكومية.[١٤]

ولكن يلاحظ هنا أن الأثر كان معنوياً أكثر منه مادياً إذ لم ينتج عن الهجوم أى أثر تدميرى على البنية التحتية الإلكترونية لإستونيا، فلقد انتهت آثار الهجوم فور السيطرة عليه، ولم تمتد الى فترة أبعد. فى حين أن ما نتج عن هذا الهجوم هو توجيه انتباه استونيا وغيرها من الدول إلى خطورة التهديدات الالكترونية، وكيف ان بامكانها شل حركة الدولة تماماً حتى وان كان لفترة محدودة.[١٥]

٢.الاختراق- وتعطيل الخدمة. (الهجوم على جورجيا).

قبل بداية الغزو الروسى لجورجيا فى اغسطس ٢٠٠٨ توقفت شبكة الانترنت الجورجية عن العمل، وتم الاعتداء على الموقع الإلكترونى للرئيس الجورجى، وقد اتخذ الهجوم الالكترونى الذى تعرضت له جورجيا شكلين رئيسين هما:

أ. اختراق بعض المواقع الالكترونية:

والتى وجهت ضد مواقع إلكترونية سياسية، حكومية، من بينها موقع رئيس الجمهورية ووزارة الخارجية، ثم ظهرت على الموقع صورة الزعيم النازى ادولف هتلر بجانب صور لرئيس الجمهورية، وغيره من الحكام الديكتاتوريين.

ب. هجمات الحرمان من الخدمة:

والتى وجهت ضد مواقع حكومية كموقع وزارة التربية والتعليم، والمواقع التى تم تقدم اختبارات للطلاب، وموقع البرلمان والرئاسة، وأكبر بنك تجارى فى جورجيا، كما تمت مهاجمة مواقع الأخبار ووسائل الاعلام والتى شملت أكبر مواقع أخبار باللغة الانجليزية فى جورجيا، وشبكات إخبارية من بينها CBC، BBC، حتى ان وزارة الشؤون الخارجية الجورجية- خروجاً من أزمة انقطاع التواصل الالكترونى- وضعت

لنفسها بريداً الكترونياً مجانياً على موقع البحث الالكترونى جوجلGoogle واستبدلت كذلك الموقع الالكترونى الذى توقف فجأة بمدونة الكترونية مجانية من جوجل ايضاً.[١٦] ويرجع السبب وراء هذا الهجوم الروسى كرداً على إرسال الحكومة الجورجية الموالية للغرب قوات للحكومة الانفصالية المدعومة من موسكو.[١٧]

وقد اختلفت تداعيات الهجوم الالكترونى فى حالة إستونيا عن جورجيا، ففى استونيا كان الضرر الاكبر هو الحيلولة دون قدرة المواطنين على الوصول الى خدمات الكترونية حيوية يقدمها كل من القطاع العام والخاص، أما فى الحالة الجورجية كان الضرر الأكبر هو الحد من قدرة الدولة على إيصال رؤيتها للعالم، وإيصال المعلومات للمواطنين من خلال الانترنت.[١٨]

فالشركتان المقدمتان لخدمات الانترنت فى جورجيا فى تلك الفترة توقفا عن العمل ولم تتمكنا من تقديم الخدمة للمواطنين لعدة أيام بعد الهجوم. كما أن ايقاف المواقع الحكومية الرسمية عن العمل نتيجة لهجمات الحرمان من الخدمة قد أدى إلى قطع الصلة ما بين جورجيا والعالم الخارجى، وحال دون قدرة الحكومة الجورجية على الحفاظ على وسائل نقل المعلومات لمواطنيها والعالم فى الأيام الأولى الأكثر أهمية فى الصراع الروسى- الجورجى. كما أن للهجوم الالكترونى على جورجيا تداعيات على الخدمات العامة، فعلى سبيل المثال فور وقوع الاعتداءات أعطى البنك الوطنى الجورجى أمراً كافة البنوك بالتوقف عن تقديم الخدمات الالكترونية للمواطنين، واستمر ذلك لمدة ١٠ ايام. إلا أن الآثار المترتبة على انقطاع الخدمات الالكترونية تختلف فى الحالتين الجورجية والإستونية، نتيجة لاختلاف درجة اعتماد كلتا الدولتين على تكنولوجيا المعلومات والاتصالات فى إدارة شئون الدولة، والتى بدورها تجعل الدولة أكثر عرضة للهجوم الالكترونى.[١٩]

ولذا لم تكن نتائج الهجوم الالكترونى على جورجيا ذات آثار فادحة على تقديم الخدمات الحكومية والتى لم تعتمد بالأساس على البنية الالكترونية بشكل كبير، نتيجة للإنخفاض النسبى لاعتماد جورجيا على تكنولوجيا المعلومات والاتصالات. بيد ان الهجوم الالكترونى على جورجيا كان له دور كبير فى التأكيد على انه حتى تلك الدول التى لا تعتمد بشكل كبير على تكنولوجيا المعلومات من الممكن أن تتعرض للضرر حال وقوع هجوم الكترونى عليها من حيث ضمان دقة تدفق المعلومات للمواطنين داخل الدولة.

فعلى الرغم من أن الهجمات لم ينتج عنها أى آثار دائمة، أو حتى بعيدة المدى، إلا أن ما أحدثته من أضرار على قدرة الدولة فى التواصل مع مواطنيها ومع العالم الخارجى جاءت فى أكثر وقت كانت جورجيا فيه فى حاجة للاعتماد على بنيتها التكنولوجية والمعلوماتية. فعلى عكس الهجمات العسكرية التقليدية، يمكن الاعتماد على الهجمات الالكترونية بحيث تحدث آثاراً مؤقتة فى إطار زمنى محدد. ولكن هناك صعوبة فى تحديد

مبالغ محددة لكافة الخسائر التى ترتبت على الهجوم وخاصة فى الحالة الجورجية، إذ جاء الهجوم الإلكترونى مصاحباً لهجوم عسكرى مما يصعب الفصل ما بين الآثار المترتبة على كل منهما.

ولكن يلاحظ ان الهجوم الالكترونى كان محدوداً، ولم يستهدف أهدافاً أكثر حيوية كأنظمة التحكم والتشغيل والتى كان من شأنها أن ترتب خسائر ضخمة على البنية التحتية الجورجية، أى إن الهدف لم يكن إلحاق أضرار دائمة ببنية الانترنت الخاصة بجورجيا، وإنما فقط تحقيق هدف عزلها عن العالم الخارجى. فإذا ما تمت مهاجمة البنية التحتية لجورجيا سيترتب على ذلك خسائر اقتصادية ضخمة ستطول حتماً الدول المرتبطة بها بعلاقات اقتصادية وثيقة وعلى رأسها روسيا. وعليه، إذا ما أرجعنا هذا الهجوم الى السلطات الرسمية الروسية، يكون من المنطقى ألا تقوم روسيا بالإضرار اقتصادياً بجورجيا حتى لا يؤثر ذلك فى مصالحها.[٢٠]

٣. تعطيل الخدمة- وإجبار الدولة لتغيير قرار (قرغيزستان):

فى يناير ٢٠٠٩ 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 أمريكيّة. بيد أن تلك الهجمة قد أتت ثمارها بعد قيام الجمهورية القيرغيزية بإزالة القاعدة الأمريكيّة، وهو ما دفع الكرملين إلى منح قرغيزستان قروضًا ومساعدات مالية بقيمة ٢ مليار دولار لاحقًا.

٤.الاختراق- وإحداث الفوضى (اوكرانيا).

بدأت احتجاجات الميدان الأوروبي في كييف عام ٢٠١٣ للمطالبة بدخول أوكرانيا إلى الاتحاد الاوربي بعد تعليق حكومة الرئيس فيكتور يانوكوفيتش التوقيع على اتفاقية الشراكة مع الاتحاد، وازدادت وتيرة هذه الاحتجاجات مع بداية ٢٠١٤ وأدت إلى مقتل العديد من المحتجين والقوى الحكومية، تأججت الاشتباكات بين قوات الأمن والمحتجين ابتداءً من يوم ٢٠ فبراير. وفي ظل تلك الظروف صوت مجلس النواب الأوكراني على عزل الرئيس يانوكوفيتش في ٢٢ فبراير.

وعقب الثورة الأوكرانية في ٢٠١٤ التي أطاحت بالرئيس فيكتور يانوكوفيتش وحكومته، تظاهر محتجون، معظمهم ينتمي للقومية الروسية، اعتراضاً على الأحداث الجارية في كييف وطلباً للمزيد من التكامل مع روسيا، بالإضافة إلى حكم ذاتي موسع أو استقلال للقرم عن أوكرانيا. على الجانب الآخر تظاهرت جماعات إثنية أخرى لتأييد الثورة. وفي ١ مارس من نفس العام، وافق مجلس الاتحاد الروسي بالإجماع على طلب الرئيس الروسي فلاديمير بوتين استخدام القوات الروسية في أوكرانيا. وفي ٢ مارس، استدعى مجلس الأمن القومي الأوكراني كامل قوات احتياط القوات المسلحة، وتصاعد التوتر في

القرم بين الأطراف المؤيدة لروسيا والمؤيدة لأوكرانيا استجلب ردود فعل من حلفاء أوكرانيا الغربيين[٢١].

هذا التغيير في كييف لم يرق لسكان العديد من المناطق في جنوب وشرق البلاد. وفي يوم ٢٣ شباط وكجزء من نتائج الثورة الأوكرانية ألغي قانون اللغة للأقليات (والذي يشمل الروسية) وتم إعلان اللغة الأوكرانية لغة رسمية وحيدة للبلاد. فجاء هذا القرار ليصب الزيت على النار في تلك الأقاليم المستاءة أصلا من التغييرات الحاصلة في عاصمتهم. وقد رأت تلك الاقاليم وخاصة شبه جزيرة القرم أن خطوة إلغاء قانون اللغات هي دليل على أن المحتجين في كييف يحملون اجندة معادية لروسيا ولهم توجه عنصري. وفي ١٦ مارس، أُجري استفتاء في القرم للانفصال عن أوكرانيا والانضمام لروسيا الاتحادية، جاءت نتيجة الاستفتاء لصالح الانضمام لروسيا بنسبة ٩٥%. وقد استخدمت روسيا عدة آليات من أجل تحقيق أهدافها فى تلك الازمة من خلال تسخير الفضاء الالكترونى بدءاً من محاولة التأثير على الرأى العام الروسى وصولاً الى اختراق الانتخابات الاوكرانية:[٢٢]

أ. التأثير فى الرأى العام:

كانت هناك حملة معلومات سبقت العمليات العسكرية الروسية فى شبه جزيرة القرم وصاحبتها وتلتها، وقد استهدفت هذه الحملة بشكل أساسى الرأى العام الروسى فى الداخل، واستهدفت بشكل ثانوى المقيمين فى شبه جزيرة القرم. لطالما حافظت وسائل الاعلام الروسية على بعض التغطية للأحداث في شبه جزيرة القرم للرأى العام الروسى الذى يتابعها، ولكن ذلك تكثف مع زيادة حدة العنف الذي شهدته الاشتباكات بين القوات الموالية للحكومة والمحتجين فى كييف، وقد نشطت حركة احتجاج الميدان، التي بدأت في نوفمبر ٢٠١٣، مع تلاعب روسيا بالمعلومات الذي كان حاداً بالفعل، وكان يستهدف المواطنون الروس، محذرة إياهم من مخاطر بناء روابط أوثق مع الاتحاد الأوروبى EU. شملت حملتها تضمين وسائل الإعلام المستقلة الداخلية المتبقية القليلة أو تهميشها، مكتسبة بذلك المزيد من السيطرة والقوة لتشكيل وجهات النظر في روسيا حول الأحداث في أوكرانيا، تم دمج وسائل الإعلام الحكومية القائمة على غرار "ريانوفوستى" RIA Novosti، و"صوت روسيا" Voice of Russia، وفى روسيا اليوم التى تعرف حالياً بـ" RT".[٢٣]

في ذلك الوقت، شاهدت أغلبية شرق أوكرانيا وشبه جزيرة القرم التلفاز الروسي، وكما كان الحال في الاتحاد السوفيتى سابقاً، حصلت الأغلبية الساحقة من الشعب على أخبارها من وسائل الإعلام المتلفزة ووسائل التواصل الاجتماعى، وتنازلت أوكرانيا إلى حد كبير عن

معلومات باللغة الروسية لمنافذ مقرها فى روسيا منذ استقلالها عن الاتحاد السوفيتى فى العام ١٩٩١، وبالأخص فى شبه جزيرة القرم، فى حين لم تعزز موسكو رسمياً وسائل الاعلام الروسية فى اوكرانيا، كانت الأسواق الاعلامية الروسية أكبر بكثير من الأسواق باللغة الروسية فى اوكرانيا، لدرجة أن قنوات المعلومات والترفيه التابعة لها كانت مهيمنة بين الأوكرانيين الناطقين بالروسية، وأغلقت القوات الروسية تسع محطات تلفزيونية أوكرانية فى ٩ مارس متيحة الوصول إلى القنوات الروسية فقط، وأصبح بالإمكان الوصول إلى القنوات من اوكرانيا عبر أجهزة استقبال الاقمار الاصطناعية.

وعندما انهارت حكومة يانوكوفيتش في بداية عام ٢٠١٤ أصبحت التصريحات الروسية بشأن الأحداث فى اوكرانيا أكثر حدة، حيث أشارت وسائل الإعام الروسية بشكلٍ نموذجى إلى حكومة أوكرانيا الانتقالية (المرحلية) وحركة الاحتجاج التي أتت بها بعبارة "مجلس فاشي". وكان لحملة معلومات روسيا ثلاثة أهداف أساسية، الأولى: تشويه سمعة الحكومة الجديدة في أوكرانيا، والثانية: التشديد على الخطر الكبير المحدق بالروس في أوكرانيا، والثالثة: ضمان عرض دعم واسع لعودة شبه جزيرة القرم للعيش في سلام في الوطن الأم روسيا.

وفى ٢٦ فبراير بدأت روسيا تروج بشدة لرسالتها بأن تغيير النظام في أوكرانيا كان غير مشروع. وسبق هذا اليوم مباشرة السيطرة العسكرية الروسية على المبانى الحكومية فى شبه جزيرة القرم تم تقديم هذه الرسالة من قبل عدد من الشخصيات والنخبويين الروس، على غرار سيرجى مونوروف Sergei Mironov، وهو قائد الحزب السياسى الروسى "روسيا عادلة".

بالإضافة إلى ذلك أدت أيضاً حملة تعبئة على مستوى الشعب فى شبه جزيرة القرم لمكافحة حركة الميدان دوراً فى اتصالات روسيا الاستراتيجية. ونشأت هذه الحملة من سكان شبه جزيرة القرم الناطقين باللغة الروسية، على الرغم من أن البعض زعم ان الحكومة الروسية كانت وراءها.[٢٤]

ب. نشر معلومات مضللة:

استفادت موسكو بفعالية من وسائل التواصل الاجتماعي لحشد دعم داخلى ونشر كميات هائلة من المعلومات المضللة حول احتجاجات الميدان ونوايا الحكومة الجديدة فى كييف. وقد كشف تحليل العمليات معلومات روسيا فى الصراع الاوكرانى عن خمسة عناصر لحملتها الدعائية، وكانت: [٢٥]

- التأثير الهائل والطويل الأمد (إعادة المواضيع نفسها مراراً وتكراراً).

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

وقد ساعدت وسائل الاعلام الروسية ايضاً المرئية والالكترونية فى ضمان الموافقة الداخلية على عملية انتقالية سريعة من صراع مربك إلى استيلاء على اراض مقبول سياسياً. واستخدم بوتين تلك الوسائل لتحقيق تأثير كبير فى عرض الحجج التاريخية والعاطفية بشأن كيفية انتماء شبه جزيرة القرم إلى روسيا فى خطاب بتاريخ ١٨ مارس ٢٠١٤.

ومن الصعب تمييز أى مزايا عملياتيه ملموسة اكتسبتها روسيا من حملة المعلومات الخاصة بها خلال ضم شبه جزيرة القرم. وجدت عمليات المسح التى أجراها خبراء أمريكيون أنه، وعلى عكس الكثيرين من الاوكرانيين ٨٥% من سكان شبه جزيرة القرم لم ينظروا الى انفسهم على أنهم أوروبيون،[٢٦] تشير استطلاعات للرأى بشكل أكثر عموماً إلى ان سكان شبه جزيرة القرم كانوا على الأرجح نظاماً سياسياً منفصلاً أكثر من أوكرانيين كثيرين آخرين.[٢٧] على الأرض كان العملاء الروس ومساعدوهم بدلاً من حملة المعلومات، القوة المنظمة خلف التعبئة. وعلى الرغم من أنه وبدون شك كان لحملة المعلومات تأثير استقطاب على السكان، نتجت نقاط التحويل الخاصة بها عن الأخطاء الأوكرانية بدلاً من النجاحات الروسية. استخدمت موسكو هذه الأخطاء لتحقيق تعبئة أكبر وخلاف داخلى، ولكن حرب المعلومات كانت عرضاً جانبياً للعملية بحد ذاتها.

ركزت الحملة المعلوماتية الروسية على جمهورها الداخلى أكثر من التأثير على الرأى العام الأوكرانى داخل شبه جزيرة القرم وخارجها. لم تؤسس روسيا وكالات أو أدوات أو وسائل خاصة لإشراك الأوكرانيين منتجاً ثانوياً لحملة معلومات روسيا لإدارة رأيها الداخلى الخاص. خلال الضم سعت القوات الروسية إلى قطع إمكانية الوصول إلى وسائل الاعلام الاوكرانية والأخبار الالكترونية، مرغمه السكان المحليين على الاعتماد على مصادر أخبار تراقبها موسكو. على الرغم من ذلك، تشير الدراسات الاستقصائية إلى أن اغلبية سكان شبه جزيرة القرم حصلوا على معلوماتهم من التليفزيون الروسى فى البداية- وهم مازالوا يقومون بذلك اليوم.[٢٨] بالنظر إلى قرب شبه جزيرة القرم من روسيا، كانت هذه المقاربة كافية وفعالة ويمكن إعادة إنتاجها فى أماكن أخرى على طول حدود روسيا.[٢٩]

جـ. الاختراق- قطع الخدمة- التلاعب فى البيانات فى الانتخابات الاوكرانية:

تم شن حملات معلومات متعددة على شرق أوكرانيا، بالإضافة الى هجمات الكترونية متقطعة حتى قبل الاطاحة ببيانكوفيتش، عانى الميدان الاوروبى فى خاركيف، الذى ساعد على تنظيم المنتدى الأوكرانى للميادين الأوروبية العام الأول من هجوم قطع موزع للخدمة رئيسى Denial of Service (DDoS) Distributed فى فبراير بعد الإطاحة ببيانكوفيتش، استهدفت هجمات القطع الموزع للخدمة المواقع الالكترونية التابعة للحكومة. ولم تكن الهجمات الأولية تعطيلية إلى حد كبير، ولكن القراصنة الإلكترونيين تمكنوا فى اكتوبر ٢٠١٤ من تعطيل النظام الإلكترونى لجمع نتائج الإنتخابات، واختراق الحواسيب المُسجّل عليها بيانات التصويت والاقتراع، في محاولة للتلاعُب في النتائج وإحداث الفوضى، مما اضطر إلى فرز الأصوات يدوياً، وتأخير الإعلان عن النتائج.

أصبحت وسائل التواصل الاجتماعى أيضاً محط تركيز حملة المعلومات، وبما أنه كانت تتم استضافة منصّتى وسائل التواصل الاجتماعى الأكثر شعبياً فى أوكرانيا فى كونتاكنتى وأودنوكلاســـنيكي على خوادم روسية، كانت السلطات الروسية قادرة على حجب الصفحات الموالية للميدان وإرغام مزودى الخدمات على تشارك معلومات شخصية بشأن الذين نقروا "إعجاب" LIKE لها.[٣٠]

باع بافيـــل دوروف Pavel Durov وهـــو مؤســـس فـــي كونتاكتـــي حصته المتبقية وفرّ إلى روسيا فى ابريل ٢٠١٤.[٣١] ومع تصعيد العنف على الارض، وفّرت فى كونتاكنتى وأودنوكلاســـنيكي أداة لطلب المساهمات والتجنيد فى روسيا لمجموعات على غرار "مكافحة الميدان" AntiMaidan، و"ميليشيا دونباس الشعبية" Donbas People's Militia و"صنـــدوق مســـاعدة نوفوروســـيا" Fund to HelP Novorossiya. التقتت وسائل التواصل الاجتماعى أيضاً نشاطات الانفصاليين، والمعـــدات الروســـية التـــي تـــم توفيرهـــا لهـــم وأغلبيـــة أعمـــال العنـــف الممـــارس ضدهم. يتمثل عنصر مهم فى حملة المعلومات الروسية بإعادة إحياء مصطلح نوفوروسيا (روسيا الجديدة). ذكر بوتين هذا المفهوم فى خطاب ألقاه فى ١٧ ابريل ٢٠١٤، مذكراً أن شرق أوكرانيا وجنوبها- أو ثلث البلد من دونباس إلى أوديسا، بما فى ذلك المناطق الناطقة بالروسية بشكل أساسى- كانا تاريخياً جزئين من الإمبراطورية الروسية. كان تفسير بوتين لتاريخ نوفوروسيا يخدمه ذاتياً، علماً أن المصطلح كان موجوداً فحسب على هوامش البنية السياسية الروسية منذ العام ١٩٩٠، على الرغم من أن بعض مسؤولى الدولة تخيلوه حافزاً محتملاً ضد أوكرانيا فى حال تحولها بشكل حاد الى الغرب.

أثار استخدام هذا المصطلح مخاوف فى الغرب حيث أنه أشار ضمناً إلى أن روسيا تنتوى تقطيع أوصال أوكرانيا سعياً وراء قضية تحريرية أكبر. وقد كانت حملة معلومات

روسيا أكثر نجاحاً فى تحريض الغرب منه فى تقديم نتائج ملموسة فى أوكرانيا، وجدت دراسات تستخدم بيانات استطلاع وتحليل تقنى لاختراق مؤشرات البث الروسى أنه قد تم الافراط بتقدير تأثير الحملة إلى حد كبير. واتضح أن الرسالة تسعى إلى الاستقطاب بدلاً من التعبئة، حتى عندما كان لمؤشرات التلفاز الروسى المستوى الأعلى من التغطية ونسبة المشاهدة. فى حين زادت الحملة العداء تجاه الحكومة الوطنية الأوكرانية وعدم الثقة بها، حققت القليل من أجل تعبئة الدعم العام للانفصالية. فى نهاية المطاف حظرت أوكرانيا البث الروسى فى باقى البلد، فى حين تراجعت نسبة المشاهدة الوطنية للأخبار الروسية ووسائل الاعلام الاخرى بشكل كبير.

وفى دونباس كان الدعم للحكومة الوطنية والقضية الانفصالية فاتراً بالتساوى. كان على الانفصاليين المدعومين من روسيا اللجوء إلى القوة لأن حملة المعلومات قد فشلت فى تجميع انتفاضة أصلية قد تجتاح شرق أوكرانيا، وبعيداً عن كونها عنصراً متكاملاً، بقيت حملة المعلومات عرضاً جانبياً على مدى الصراع، فى توصيف أهمية حملة المعلومات، يفترض عادة أن النشاط ترجم إلى إنجاز وأنه، وبما أن روسيا قد استثمرت فى الجهد كان يجب ان تترك تأثيراً.[٣٢]

ثالثاً: استخدام القوة السيبرانية الروسية فى التفاعلات الدولية السياسية – والاقتصادية:

لا تتوانى روسيا عن استخدام القوة السيبرانية فى إدارة تفاعلاتها الدولية السياسية والعسكرية بما يساعد فى تعظيم قوة روسيا وتحقيق أهدافها التى تعجز أدوات القوة التقليدية عن تحقيقها، خاصة بما تتميز به هذه القوة من خاصية التخفى والقدرة على إصابة أهداف الخصم، واتساع نطاق تدمير الأهداف الالكترونية مع التحكم فى امكانية إصابة الاهداف من دون وقوع خسائر بشرية غير مقصودة. وتتنوع تطبيقات روسيا فى استخدامها للقوة السيبرانية فى التفاعلات الدولية السياسية نتناول بعضها فيما يلى:

١.التجسس- حزب الاتحاد الديمقراطى الالمانى:

فى مايو ٢٠١٥ اكتشف مُحقّقون ألمان تعرّض شبكة الكمبيوتر الخاصة بالبرلمان الألماني (البوندستاغ) للاختراق من جانب مجموعة من الهاكرز، في هجوم سيبراني يُعد الأبرز في تاريخ ألمانيا. وقال دائرة الاستخبارات الاتحادية الألمانية BfV، لاحقًا، إن روسيا كانت تقف وراء هذا الهجوم في مسعى للحصول على معلومات لا تتصل بأعمال مجلس النواب الاتحادي الألماني فقط، بل معلومات تخُص القادة الألمان، وحلف شمال الأطلنطي (الناتو) أيضًا. وقال خبراء الأمن إن الهاكرز حاولا اختراق أجهزة الحاسب الخاصة حزب الاتحاد الديمقراطي المسيحي للمستشارة الألمانية أنجيلا ميركل.

ويعتقد خبراء الأمن أن الروس يحاولون تدمير المُستشارة الألمانيّة الحالية أنجيلا ميركل، على خلفيّة مواقفها الداعمة لفرض عقوبات ضد الرئيس الروسي فلاديمير بوتين بعد ضم روسيا لشبه جزيرة القرم.

٢. السيطرة على الأفكار (حالة الصراع الامريكى- الروسى).

تمكنت روسيا من تطوير أساليب متعددة لإدارة "الحروب الإعلامية" فى مواجهة الغرب، حيث عززت روسيا من انتشار وسائل الإعلام التابعة لها، مثل "روسيا اليوم" و"سبوتنيك" لمواجهة الحملات الاعلامية الغربية، خاصة فى أوروبا الشرقية، كما اتبعت روسيا عدة أساليب وتكتيكات فى إدارة الحرب الإعلامية، تتمثل فيما يلى:

أ. كثافة تدفق المعلومات: تعتمد الاستراتيجية الاعلامية الروسية على نشر المعلومات الواحدة عبر أكثر من قناة، وبأكثر من صيغة، حيث يتم تكرار بث الرسالة نفسها من عدة مصادر، مثل المنتديات والقنوات الاخبارية على الانترنت والمنصات على مواقع التواصل الاجتماعى، مما يزيد مصداقية التغطية الإعلامية باعتبار أن "الكم الضخم للمعلومات عادة ما يكون مرادفاً للمصداقية".

ب. سرعة التغطية الإخبارية: تنشر وسائل الاعلام الروسية تغطيات إخبارية سريعة ومتتابعة على مدار الساعة، مما يؤدى لتعزيز ارتباط المتابعين بها وإيمانهم بمصداقية الأخبار والتحليلات الصادرة عنها، كما تتعزز مصداقية القصة بنشر رسائل متكررة ومستمرة على مواقع التواصل الاجتماعى بالتزامن مع البث التليفزيونى.

ج. الاستشهاد الانتقائى بالمصادر: تعتمد وسائل الاعلام الروسية على اجتزاء الحقائق وصياغة روايات غير دقيقة عن الواقع وتحرير الصور، بالإضافة للاستشهاد الخاطىء بالمصادر الموثوق بها، وعلى سبيل المثال نشرت روسيا اليوم تصريحاً نسبته إلى براون موسز المعروف بموقفه المعارض لنظام الأسد، يتضمن ادعاءات بأن المعارضة السورية نفذت هجمات بالأسلحة الكيماوية فى ٢١ اغطسطس ٢٠١٣، وهو ما تبين أنه تصريح مفبرك، وأن التصريح الحقيقى لموسز يتضمن انتقاداً لنظام الأسد.

د. التغطية التراكمية للأحداث: تقوم وسائل الاعلام الروسية بتغطية التطورات بصورة تراكمية من خلال متابعة الأحداث منذ بدايتها ونشر التطورات فور حدوثها، وهو ما يعزز ارتباط الجمهور بها واعتماده عليها، ويتم التغلب على التناقضات فى المتابعات المنشورة لبعض الأحداث بعرض وجهات نظر مختلفة وآراء متعددة حول القضية الواحدة فى محاولة لنفى اتهامات التضليل والانحياز.[٣٣]

هـ. مراقبة مواقع التواصل الاجتماعى: تسعى روسيا للسيطرة على النقاشات الافتراضية "السيبرية" حول السياسات الروسية على مواقع التواصل الاجتماعى، وتعمل فرق الرصد والمتابعة الروسية للانترنت على مدار الساعة فى فترتى عمل متتابعتين تصل كل منهما إلى ١٢ ساعة، وينبغى أن يستوفى كل منهم حصة يومية قدرها ١٣٥

تعليقاً بحد أدنى ٢٠٠ حرف لكل تعليق للرد على الآراء والتعليقات العدائية الموجهة للسياسات الروسية. وتجدر الإشارة فى هذا الصدد إلى وجود ١,٧ مليار مستخدم نشط على فيس بوك وحده يعتمدون على صفحات الأخبار فى متابعة الأحداث والتطورات، وتتميز هذه المنصات الاعلامية الافتراضية بسرعة انتشار المعلومات بسبب إعادة نشرها من جانب ملايين المستخدمين حول العالم.[٣٤]

٣. تعبئة الرأى العام (التدخل العسكرى فى سوريا).

أطلقت روسيا فى ٣٠ سبتمبر ٢٠١٥ حملتها العسكرية ضد التنظيمات الإرهابية فى سوريا، والتى تمثلت أهدافها الرسمية فى حماية الجيش العربى السورى من الانهيار حتى لا تسقط مؤسسات الدولة الحالية، فضلاً عن القضاء على تنظيمى "داعش"، وجبهة النصرة التابعين لتنظيم القاعدة وغيرها من التنظيمات الإرهابية الأقل نفوذاً وانتشاراً. وفى مواجهة هذا التدخل الروسى، تصاعد الجدل الداخلى بشأن جدواه ومدى انعكاسه على الداخل الروسى، واختلفت اتجاهات الرأى العام تجاه هذه الخطوة، خاصة فى ضوء الذكرى السلبية للتدخل السوفيتى فى أفغانستان.[٣٥]

هذا وقد نجحت الحكومة الروسية فى تهدئة مخاوف الرأى العام من التدخل العسكرى فى سوريا، ونجحت فى تعبئة الرأى العام لصالح تأييد هذا القرار، وذلك من خلال الخطوات التالية:

– سعى وزارة الدفاع الروسية لإصدار بيانات صحفية عن العلميات العسكرية فى سوريا، ونشرها من خلال موقع الفيس بوك يومياً، فضلاً عن كتابة تغريدات على موقع تويتر عن العمليات العسكرية الروسية فى سوريا، وذلك بهدف تقديم معلومات مفصلة عن الضربات الجوية، كما يتم عرض مقاطع فيديو للعمليات العسكرية وللظروف المعيشية على اليوتيوب التى يعيش فى ظلها أفراد الجيش الروسى فى سوريا. وتهدف هذه الخطوة إلى زيادة الشفافية وتقديم انطباع بأن المناطق التى توجد فيها القوات المسلحة الروسية آمنة ومحمية.[٣٦]

– التأكيد على استخدام الجيش الروسى أسلحة ومعدات عسكرية متقدمة تقنياً، مما يقلل إلى حد كبير من خطر الإصابات والخسائر فى صفوف الجيش الروسى فى سوريا، فضلاً عن استبعاد القيادة الروسية إمكانية إرسال قوات برية إلى سوريا.

– توظيف الكرملين حادث استهداف الطائرة المدنية الروسية فى سيناء بعمل ارهابى، للتأكيد على ضرورة توجية ضربات انتقامية ضد داعش، وهو ما يتسق مع توجهات الرأى العام فى هذا الإطار.[٣٧]

ومما سبق، يتضح ان طريقة إدارة الكرملين التغطية الإعلامية الالكترونية للحرب الروسية فى سوريا حتى الآن، نجحت فى إيجاد مواقف إيجابية وداعمة من جانب أغلب

فئات الشعب الروسى، خاصة أنه ليس من المتوقع أن تواجه القوات الجوية الروسية خسائر بشرية تذكر نتيجة عملياتها العسكرية فى سوريا، وقد انعكس هذا النجاح فى التغطية الإعلامية للحرب على نتائج استطلاعات الرأى العام التى قامت بها بعض مؤسسات قياس الرأى العام الروسية.[٣٨]

خاتمة:

أحدث القرن الحادي والعشرين نقلة نوعية في ترتيب أولويات معظم الدول، وكذلك في الخيارات المتوفرة لدى صُنَّاع القرار، والتي بدورها أثَّرت على أدوات السياسة الخارجية كوسائل لبسط النفوذ وإبراز المكانة على الساحة الدولية.

وتعتبر التكنولوجيا واحدةً من القوى التي أتاحتها العولمة لتحقيق أهداف بعيدة المدى، والتحرك الخفي والتأثير في الهياكل الحيوية الخاصة بالدول، وهو ما أوجب على الدول ضرورة الانتباه لتلك الأداة، ومعرفة كيف تعمل، وإلى أيّ مدى يمكن أن تصل أو تحقّق منافع أو تهديدات.

ونتيجةً لذلك، حظي الأمن السيبراني باهتمام كبير من مختلف دول العالم، وعلى رأسها الولايات المتحدة الأمريكية، وروسيا، وغيرها، وحقَّقت بعض الدول مكانةً متميزةً في التمكُّن من هذه القوة، واستخدمتها في تحقيق أهدافها المنشودة، كما لم تسلم أيضاً من التهديدات التي وصلت إلى حد التجسّس والتدخل في الشأن الداخلي.

فلقد أصبحت التكنولوجيا ترسم خريطة ثقل دول العالم، وتعطي صورة عن مكانة الدولة؛ حيث إن امتلاك أسلحة المعلومات يعطي ميزة استراتيجية خاصة للدولة، وعلى النقيض تعتبر الدول الضعيفة رقميًّا سهلة الاصطياد؛ خاصة أن فضاء المعلومات يختلف تماماً عن المجالات التقليدية للعلاقات الدولية، ولذلك فقد دعا المجتمع الدولي والشركات المتخصصة في المجال الإليكتروني للتعامل مع مفهوم القوة السيبرانية من حيث تهديداتها ومحاولة التطوير لمجارتها. حيث كوّن "حلف الناتو" وحدة للدفاع الإليكتروني ومقرها "تالين" عاصمة استونيا، بعدما عجز عن مواجهة الهجمات الإليكترونية على استونيا ٢٠٠٧، وجورجيا ٢٠٠٨ من قِبَل روسيا.

وقد استخدمت روسيا هذه الآلية، إلى جانب الآليات الاقتصادية والسياسية المعنية؛ من أجل تحقيق أهداف سياستها الخارجية؛ حيث يمكن تصنيفها ضمن الأدوات الناعمة لفرض السيادة، وجذب الداعمين، والاقتراب من نقاط صنع القرار، وتقوية العلاقات الدولية مع الحلفاء، وحماية المصالح الوطنية، وكانت تلك الآلية هي الاختيار الأول بالنسبة لروسيا عندما تدخلت في شؤون بعض الدول الكبرى؛ بهدف التأثير على الرأي العام؛ لترجيح الخيار الأنفع بالنسبة لروسيا، ويُظهر ذلك خلفية الاختيار التكنولوجي، ونجاحه في تمرير الأجندة الروسية.

ومن الجدير بالذكر أن روسيا لم تدرك فقط أن الأداة التكنولوجية هي المحرّك الأكثر فعَّالية مع الغرب بل أيضاً على سبيل المثال في إطار توسُّعاتها في إفريقيا من خلال شركة فاجنر، وقد استخدمت تلك الشركة في حملاتها مواطنين محليين بهدف تجنيدهم كعملاء سريين لروسيا، وخلق حلفاء أفارقة تضمن دعمهم وولائهم، كما أنهم استولوا على بعض الصفحات الموجودة بالفعل للاستفادة من عدد المتابعين، وأنفقوا أكثر من ٨٧٠٠٠ دولار على إعلانات الفيسبوك التي اجتذبت أكثر من مليون متابع. وعملت فاجنر من خلال تلك الحملات على الدعاية لأنشطتها في إفريقيا والصفقات الروسية للذهب والماس والموارد الطبيعية الأخرى، وإبراز أهميتها لتحقيق التنمية الإفريقية، وتتبع في آلياتها تقديم الدعم العسكري أو الاستقرار السياسي في مقابل النفوذ السياسي، أو فرص التوسع الجيوستراتيجي، أو تنازلات الموارد، وصنع روابط سرية مع ممثلي الدول، ومن خلال جهود موسكو لتحويل إفريقيا جنوب الصحراء الكبرى إلى مركز استراتيجي، وإضعاف النفوذ الغربي في المنطقة، بالإضافة إلى تزويدها بالجنود المرتزقة، والظهور كمصدر للاستقرار الإقليمي، وتعزيز العلاقات مع زعماء القارة؛ حيث شارك بريجوزين في اجتماع للسلطات الروسية مع اللواء حفتر في موسكو، كما لعبت روسيا وخاصة المديرية العامة لهيئة الأركان العامة (GRU) دورًا رئيسيًّا في تدريب مقاولي فاجنر المتوجهين إلى إفريقيا.

ومثلت التكنولوجيا غطاءً لتأمين مصالح روسيا في إفريقيا؛ من خلال التوغل فيها، ومواجهة التحديات التي تقف عائقاً أمام استثماراتها؛ حيث تحرص روسيا دائماً على مساعدة الدول الإفريقية في بناء منشآت الطاقة، ولطالما لجأت إلى القادة الأفارقة باستثمارات كبيرة في البنية التحتية في قطاعات استخراج المعادن والتقنيات، والطاقة (بما في ذلك توليد الطاقة الكهرومائية والطاقة النووية)، والتعاون العسكري التقني وصيانة الأصول العسكرية، والأمن السيبراني والخدمات الإلكترونية.

ومن هنا أصبح واضحاً أن التكنولوجيا هي أحد أهم الموارد الاستراتيجية للدول، والتي يجب تأمينها، وتحقيق الكفاية منها، وصنع برامج الحماية اللازمة لها؛ للتصدي لأيّ أخطار أو هجمات إلكترونية؛ كاختراق نُظم الأمان الخاصة بالدول، الإرهاب، استخدام المعلومات والتكنولوجيا لأغراض عسكرية، الاتجار غير المشروع، تنفيذ عمليات التجسس، وتهديد أمن المعلومات بهدف الوصول إلى المعلومات السرية، وتغييرها، وتدميرها، أو تعطيل التشغيل العادي للشركات الكبرى.

وأخيرا يمكن القول ان انتقال السياسة الخارجية الروسية إلى استخدام التهديدات السيبرانية بديلاً عن الحروب والتهديدات العسكرية له بُعْد اجتماعيّ وإنسانيّ؛ حيث يجنّب الدول الوقوع تحت طائلة عقوبات القانون الدولي الإنساني، وجرائم الحرب، وتعويضات عن الضحايا التي كانت تُخلِّفها الحروب، كما أنه يعمل أكثر على التكوين النفسي للشعوب، وإثارة القلق والترقُّب لوقوع أخطار محتملة لا يمكن التكهُّن بمداها.

هوامش الدراسة:

[1] وفعلاً قدمت روسيا مقترحاً لاتفاقية دولية للأمن الإلكتروني فى سبتمبر ٢٠١١، إلا أنها تضمنت عديداً من النقاط الخلافية التى تتعارض والرؤية الغربية للأمن الإلكترونى واستراتيجيات الدفاع من أجل تحقيقه. ويرجع ذلك إلى أن روسيا تماما كالصين تؤمن بضرورة ضمان سيادة الدولة فى مجال الانترنت، بمعنى احتفاظ الدولة بسيادتها فى الفضاء الإلكتروني كما هو الحال فى المجالات التقليدية. ولذا جاء المقترح يعكس الرؤية الروسية لضرورة تحكم الدول فى المحتوى الذي تم تداوله عبر الانترنت، باعتبار أن فى ذلك ما يمكن الدول من حماية أمنها الإلكترونى. فى حين أن الدول الغربية تدعو إلى حرية تداول المعلومات والتواصل عبر الانترنت كإحدى الحريات الأساسية التى لابد وأن تكفل للمواطنين. انظر: نوران شفيق، "الفضاء الإلكترونى وأنماط التفاعلات الدولية: دراسة فى أبعاد الأمن الإلكترونى"، مرجع سابق، ص ١٠٣.

[2] عادل عبدالصادق، اساحة الفضاء الإلكتروني في ضوء القانون الدولي الانساني، (الاسكندرية: وحدة الدراسات المستقبلية، ٢٠١٧)، ص ٦٩.

[3] **Cristina, Carmen. (October 2014). "Cyber Defence in The EU Preparing for cyber warfare?", European Parliamentary Research Service Briefing, pp 4-5. http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf**

[4] بريكس هو مختصر للحروف الأولى باللغة اللاتينية **BRICS** يتم كتابة المختصر بالعربية "برهجص" لأول الحروف باللغة العربية المكونة لأسماء الدول صاحبة أسرع نمو اقتصادى بالعالم، وهي :البرازيل وروسيا والهند والصين وجنوب أفريقيا.

[5] ايهاب خليفة، "الدوائر المغلقة: لماذا تتجه الدول لتأسيس شبكات إنترنت وطنية"، اتجاهات الأحداث، فبراير ٢٠١٥، العدد ٧، ص ٦١.

[6] **Patrick Smith, Russian Electronic Warfare: A Growing Threat to U.S. Battlefield Supremacy, American Security Project, April 2020, p. 3.**

[7] نوران شفيق، "الفضاء الإلكترونى وأنماط التفاعلات الدولية: دراسة فى أبعاد الأمن الإلكترونى"، مرجع سابق، ص ١٠٤.

[8] فى فبراير ٢٠٠٧ أصدر البرلمان فى استونيا قراراً يقضى بازالة كل الأبنية او الرموز المرتبطة بالعقود الخمسة التى كانت فيها استونيا تحت الاحتلال السوفيتى بعد الحرب العالمية الثانية. ومن ضمن ما قضى القانون بازالته هو تمثال برونزى لضابط من الجيش الأحمر (الجيش الوطنى للاتحاد السوفيتى) فى تالين، فى العاصمة الإستونية، كان قد وضع فى استونيا عام ١٩٤٧ كرمز لفوز الجيش السوفيتى على الجيش النازى. وقد أدى قرار نقل التمثال الى موجات رفض عارمة، وتظاهرات من قبل الروس الموجودين فى استونيا، والذين اتهموا الحكومة الاستونية بأنها بهذا القرار تعيد كتابة التاريخ وتحرف الذاكرة. انظر فى ذلك: نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية دراسة في أبعاد الأمن الألكتروني، (القاهرة: المكتب العربى للمعارف، ٢٠١٨)، ص ١٣٩.

[9] رغدة الهيبي، "الردع السيبرانى: المفهوم والإشكاليات والمتطلبات"، مفاهيم استراتيجية، القاهرة: المركز العربى لابحاث الفضاء الالكترونى، ٢٠١٧، ص ٦.

[10] **Ryan T, Kaminski. (2010). "Escaping the Cyber State of Nature: Cyber Deterrence and International Institutions". In: C. Czosseck & K. Podins (eds.),*Conference on Cyber Conflict Proceedings*, Tallinn, Estonia, pp. 80- 82.**

[11] إيهاب خليفة، "الحرب السيبرانية.. مراجعة العقيدة العسكرية استعدادا للمعركة القادمة"، السياسة الدولية، يناير ٢٠١٨، العدد ٢١١، ص ٢٠.

[12] نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية دراسة في أبعاد الأمن الألكتروني، (القاهرة: المكتب العربى للمعارف، ٢٠١٨)، ص ١٤١.

[13] شبكة بوتنتس تتكون على شكل شبكة من الروبوتات الصغيرة تحوم برامج ضارة حيث أنها لديها القدرة على التحكم في أي جهاز مع عنوان IP بما في ذلك مسجلات الفيديو والكاميرات بالاضافة الى الأجهزة الاستهلاكية الأخرى مما قد تسبب انقطاع الانترنت على نطاق أوسع، وسرقة المعلومات والتجسس، حيث أن بوتنتس تشكل خطراً أمنياً كبيراً على مناطق ذات نطاق واسع في الإنترنت اليوم.
http://alwatannewspaper.ae/?p=224185

[14] انظر فى ذلك ايضاً: أليس لوماس، "توتر محتدم: التشاحن الأمريكى– الروسى تحت مظلة حلف الناتو"، اتجاهات الأحداث، يوليو ٢٠١٥، العدد ١٢، ص ص ٧٧–٧٩.

[15] نورا نور شفيق، أثر التهديدات الالكترونية على العلاقات الدولية دراسة في أبعاد الأمن الألكتروني، مرجع سابق، ص ١٤٣.

[16] ولم تتوقف فقط العديد من المواقع الالكترونية فى جورجيا عن العمل، وإنما توقفت معظم شبكات الانترنت لأنها تعتمد بدرجة كبيرة على كابلات الألياف الضوئية التى تمر عبر روسيا، والتى أنفقت عليها كل من روسيا والهند والصين عشرات البلايين من الدولارات لمد شبكة الانترنت فى معظم انحاء اسيا وافريقيا، ليس فقط لتقديم خدمة يمكن أن تدر على تلك الدول دخلا ماليا مرتفعا كما يظن البعض، وهو الأهم أن تصبح تلك الدول هى المتحكمة فى حركة تشغيل الانترنت التى تعتمد بشكل رئيسى على تلك الكابلات، والتى أصبح من يمتلكها أو تمر من خلال أرضة يملك قوة استراتيجية لا يمكن الاستهانه بها، ولم تكن معظم هذه الهجمات تدار من قبل القيادة العسكرية الروسية كما قد يتبادر الى الذهن، ولكن الكثير منها تم الإعداد لها علنا بين المتعاطفين مع روسيا من قراصنة الانترنت الروس "الهاكرز" قد تنادوا منذ فترة تحت شعارات مثل "قف مع بلدك ياأخى" أو "من أجل حماية روسيا والدفاع عنها"، أو ما شابه من شعارات، واندلعت الحرب قد أن تندلع العمليات العسكرية عبر الفضاء الالكترونى. انظر: عادل عبد الصادق الجخة، "أثر الإرهاب الإلكترونى على مبدأ إستخدام القوة فى العلاقات الدولية ٢٠٠١-٢٠٠٧"، رسالة ماجستير، منشورة، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، ٢٠٠٩، ص ص ٢١٦

[17] بدأت روسيا يوم 8 أغسطس 2008 بهجوم عسكري من جورجيا على مقاطعتى جنوب أوسيتيا وأبخازيا، وبعدها قامت القوات الروسية بهجوم مضاد سريع على جورجيا. حيث تقع أوسيتيا الجنوبية وسط جورجيا من ناحية الشمال، وحدودها محاذية لجمهورية أوسيتيا الشمالية .غالبية الأوسيت فى جمهورية الجنوب هم من المسيحيين .استولت روسيا على أوسيتيا كاملة عام 1878 قسمتها بعد الثورة البلشفية إلى كيانين، ألحق الشمالى بالاتحاد الروسى والجنوبى بجورجيا.
حيث تحول جورجيا دون توحد أوسيتيا الجنوبية والشمالية .وقد بدأ التوتر فى العلاقة بين أوسيتيا الجنوبية وجورجيا مع إتجاه الأخيرة إلى الاستقلال عن الاتحاد السوفيتى .ومع بداية التسعينيات أعلنت أوسيتيا الجنوبية نيتها إعلان المنطقة تابعه للنفوذ الروسى، وهو ما اعترض عليه البرلمان الجورجى، لتبدأ المواجهات بين الانفصاليين فى أوسيتيا والشرطة الجورجية ما أسفر عن مقتل أكثر من عشرة.

[18] انظر:
Jonas Kjellén, "Russian Electronic Warfare: The role of Electronic Warfare in the Russian Armed Forces", FOI, September 2018.

[19] نوران شفيق، "الفضاء الالكتروني وأنماط التفاعلات الدولية"، رسالة ماجستير، غير منشورة، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، ٢٠١٤، ص ١٧٠

[20] نورا نور شفيق، أثر التهديدات الالكترونية على العلاقات الدولية دراسة في أبعاد الأمن الألكتروني، مرجع سابق، ص ص ١٤٦-١٤٧.

[21] كانت القرم جزءًا من روسيا منذ القرن ١٨، مع أن الروس الإثنيين لم يصبحوا المجموعة السكانية الأكبر فى القرم حتى القرن ٢٠. تمتعت القرم بحكم ذاتى تحت اسم جمهورية القرم السوفيتية الاشتراكية ذاتية الحكم منضوية تحت جمهورية روسيا السوفيتية الاتحادية الاشتراكية من ١٩٢١ حتى ١٩٤٥، إذ قام ستالين بتهجير الأكثرية التترية القرمية وألغى الحكم الذاتى. فى ١٩٥٤، قامت القيادة السوفيتية التي ترأسها نيكيتا خروتشوف بنقل أوبلاست القرم من جمهورية روسيا السوفيتية الاتحادية الاشتراكية إلى جمهورية أوكرانيا السوفيتية الاشتراكية. لم يُسمح للتتاريين القرميين بالعودة إلى ديارهم، أعيد الحكم الذاتى إلى القرم فى السنة الأخيرة من وجود الاتحاد السوفيتى، ١٩٩١. ومع وجود توترات انفصالية خلال عقد التسعينات، ظلت القرم جمهورية ذاتية الحكم ضمن أوكرانيا.
وأصبح إقليم القرم ذاتى الحكم جزءًا من أوكرانيا المستقلة منذ ١٩٩١. وحالة القرم القانونية كجزء من أوكرانيا اعترفت بها روسيا، التى تعهدت بالحفاظ على وحدة أوكرانيا فى مذكرة بودابست للضمانات الأمنية التى وُقعت فى ١٩٩٤. الاتفاقية وقعتها أيضًا الولايات المتحدة والمملكة المتحدة إلى جانب أوكرانيا التى تخلت بموجب هذه الاتفاقية عن أسلحتها النووية. التطورات اللاحقة فى القرم ووضع قواعد أسطول البحر الأسود الروسي أضحت مثارًا للتوتر في العلاقات الروسية الأوكرانية.

[22] مايكل كوفمان، كاتيا ميجاشيفا، عبر من عمليات روسيا فى شبه جزيرة القرم وشرق أوكرانيا، (كاليفورنيا: مؤسسة راند، ٢٠١٧)، ص ١٢.

[23] **Ennis, Stephen, "Putin's RIA Novosti Revamp Prompts Propaganda Fears," BBC Monitoring, December 9, 2013. As of July 15, 2016: http://www.bbc.com/news/world-europe-25309139**

[24] مايكل كوفمان، كاتيا ميجاشيفا، عبر من عمليات روسيا فى شبه جزيرة القرم وشرق أوكرانيا، مرجع سابق، ص ١٤.

[٢٥]انظر فى ذلك:
Darczewska, Jolanta, The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study, Warsaw, Poland: Centre for Eastern Studies, Point of View Number 42, May 2014. As of November 6, 2015: http://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf

[٢٦]انظر فى ذلك:
O'Loughlin, John, and Gerard Toal, "Mistrust About Political Motives in Contested Ukraine," Washington Post, February 13, 2015a. As of November 6, 2015:
https://www.washingtonpost.com/blogs/monkey-cage/wp/2015/02/13/ mistrust-about-political-motives-in-contested-ukraine/

[٢٧] لمزيد من التفصيل حول تلك الاستطلاعات:
O'Loughlin, John, and Gerard Toal, "The Crimean Conundrum," open Democracy.net, March 3, 2015b. As of July 28, 2016:
https://www.opendemocracy.net/od-russia/john-o%E2%80%99loughlin-gerard-toal/crimean-conundrum

[٢٨] لمزيد من التفصيل انظر:
Toal, Gerard, and John O'Loughlin, "Russian and Ukrainian Viewers Live on Different Planets," Washington Post, February 26, 2015. As of August 31, 2016:
https://www.washingtonpost.com/blogs/monkey-cage/wp/2015/02/26/ Russian-and-Ukrainian-tv-viewers-live-on-different-planets/

[٢٩]مايكل كوفمان، كاتيا ميجاشيفا، عبر من عمليات روسيا فى شبه جزيرة القرم وشرق أوكرانيا، مرجع سابق، ص ص ٢٩-٣٠.

[٣٠]المرجع السابق، ص ص ٥٠-٥١.

[٣١] لمزيد من التفصيل:
Hakim, Danny, "Once Celebrated in Russia, the Programmer Pavel Durov Chooses Exile," New York Times, December 2, 2014. As of November 6, 2015:
http://www.nytimes.com/2014/12/03/technology/once-celebrated-in-russiaprogrammer-pavel-durov-chooses-exile.html

[٣٢]مايكل كوفمان، كاتيا ميجاشيفا. عبر من عمليات روسيا فى شبه جزيرة القرم وشرق أوكرانيا، مرجع سابق، ص ص 53-52.

[٣٣] بسمة الإتربى، "أساليب غير تقليدية لحروب الإعلام بين موسكو وواشنطن"، اتجاهات الأحداث، يوليو ٢٠١٧، العدد ٢٢، ص ص ٥١-٥٢.

[٣٤]انظر فى ذلك:
Emerson T, Brooking. P. W. Singer. (November 2016). "War Goes Viral: How Social Media Got Weaponized", The Atlantic, pp. 70-80.

[٣٥]أليكسى كلينيكوف، "متلازمة أفغانستان: اتجاهات الرأى العام الروسى تجاه التدخل العسكرى فى سوريا"، اتجاهات الاحداث، فبراير ٢٠١٦، العدد ١٥، ص ٧٧.

[٣٦] لمزيد من التفصيل انظر: يورى بارمان، "الاعتماد المتبادل: المحددات الاقتصادية لسياسة روسيا الشرق أوسطية"، اتجاهات الأحداث، يونيو ٢٠١٧، العدد ٢١، ص ٧٣.

[٣٧] أليكسى كلينيكوف، "متلازمة أفغانستان: اتجاهات الرأى العام الروسى تجاه التدخل العسكرى فى سوريا"، مرجع سابق، ص ٧٨.

[38] **Russian participation in the Syrian military conflict, Levada Center, November 6, 2015, accessible at; http://www.levada.ru/en/**