الحرب الإلكترونية بين *الولايات* المتحدة الأمريكية وروسيا

Electronic warfare between the United States of America and Russia

رقولي كريم[1]

جامعة محمد لمين دباغين –سطيف 02

وغليسي أحلام[2]

جامعة محمد لمين دباغين –سطيف 02

تاريخ الإرسال: 2020/04/05 تاريخ القبول: 2020/05/07 تاريخ النشر: 2020/06/30

****

ملخص:

تسعى هذه الدراسة إلى معالجة أحد المواضيع المهمة في حقل العلاقات الدولية والمتعلقة بالحرب الإلكترونية بين الولايات المتحدة الأمريكية وروسيا، فبعد التطور التكنولوجي الهائل الذي مس جميع جوانب الحياة والتفاعلات الدولية، ظهر الفضاء الإلكتروني كمجال جديد للصراع بين الفواعل على مستوى النظام الدولي.

ونتيجة لذلك تبلورت الحرب السيبرانية Cyber War بخصائص مغايرة للحروب التقليدية من حيث الأنشطة والفواعل، وقد سعت كل من الولايات المتحدة الأمريكية وروسيا إلى الاستفادة من الميزات التي يوفرها الفضاء الإلكتروني، ونقل الصراع الدائر بينهما إلى العالم الرقمي، ولقد مثل التدخل الروسي في الانتخابات الرئاسية الأمريكية عام 2016 تجسيدا واقعيا لهذا النوع من الحروب.

الكلمات المفتاحية: الفضاء الإلكتروني، الحرب الإلكترونية، الصراع، الولايات المتحدة الأمريكية، روسيا.

Abstract:

This study seeks to address one of the important issues in the field of international relation and electronic warfare between the United States of America and Russia. After the enormous technological development that affected all aspects of international life and interactions, cyberspace emerged as a new area of conflict between actors at the level of the international system.

As a result, cyber warfare has crystallized in characteristics other than conventional was in terms of activities and actions, and the United States of America and Russia have sought to take advantage of the advantages offered by cyberspace and to bring the conflict between them into the digital world. Russia's intervention in the recent American presidencies of 2016 represented a realistic embodiment of this type of war.

Keywords: Electronic space, Electronic Warfare, Conflict, United States of America, Russia.

[1] **رقولي كريم جامعة محمد لمين دباغين –سطيف02**، karimchO53@hotmail.com

[2] وغليسي أحلام **جامعة محمد لمين دباغين –سطيف 02**، ahlemouaghlici@gmail.com.

مقدمة:

عرفت العلاقات الدولية مع نهاية الحرب الباردة تطورا كبيرا، من حيث الفواعل والمواضيع والأدوات المستخدمة في إدارة مختلف التفاعلات، وفي ظل هذه القفزة النوعية التي تزامنت مع ثورة التكنولوجيا الرقمية والتي اقتحمت شتى مجالات الحياة الإنسانية والتفاعلات الدولية، ظهر نوع جديد من التهديدات والمتمثل في الصراع الإلكتروني، الذي وجب على الدولة القومية التعامل معه ومواجهته، لأن أي هجوم على قطاع من القطاعات من شأنه إحداث أضرار كبيرة من شأنها التأثير على أمن الدولة، وبالتالي أصبحت الدولة مضطرة للاهتمام بفضائها الإلكتروني كونه أضحى ساحة جديدة للتفاعلات الدولية. فتبلورت الحرب الإلكترونية بوصفها شكلا جديدا من أشكال التفاعلات الدولية.

_ إشكالية البحث:

تتمحور الدراسة حول الحرب الإلكترونية بين الولايات المتحدة الأمريكية وروسيا، ومن ثم توجب على هذه الدراسة طرح الإشكالية التالية: **كيف أثرت الحرب الإلكترونية على طبيعة العلاقة بين الولايات المتحدة الأمريكية وروسيا؟**

_ المقاربة المنهجية:

_ **المنهج الوصفي التحليلي:** تم الاعتماد على هذا المنهج للإحاطة بأبعاد الظاهرة المدروسة، وذلك من خلال وصف وتحليل مفهوم الحرب الإلكترونية.

_ **منهج دراسة حالة:** قمنا باستخدام هذا المنهج لتسليط الضوء على طبيعة الصراع الأمريكي الروسي في الفضاء الإلكتروني.

_ فرضية الدراسة:

_ أدى التطور التكنولوجي وبروز عصر المعلومات إلى ظهور الفضاء الإلكتروني كمجال جديد تدور فيه الصراعات الدولية.

_ هدف الدراسة:

تسعى هذه الدراسة إلى محاولة فهم الحروب الإلكترونية كشكل جديد من أشكال التفاعلات الدولية، وإعطائها بعد نظري من شأنه أن يقدم تفسير علمي لها، وبعد ذلك سنحاول إسقاط هذا المفهوم على طبيعة العلاقة بين الولايات المتحدة الأمريكية وروسيا، من خلال التطرق إلى التدخل الروسي في الانتخابات الأمريكية كمظهر للحرب الإلكترونية بين الجانبين.

2-المبحث الأول: مقاربة معرفية نظرية للحروب الإلكترونية

فرض العالم الافتراضي نفسه كساحة جديدة للصراع الدولي، بعد أن اقتحمت التكنولوجيا جميع مجالات الحياة الإنسانية والتفاعلات الدولية، فظهرت مفاهيم جديدة في العلاقات الدولية أهمها الحروب الإلكترونية كنوع جديد للحروب.

2-1-المطلب الأول: تعريف الحرب الإلكترونية

لا يوجد إجماع بين الدارسين والباحثين حول تعريف موحد للحرب الإلكترونية، إلا أنهم اتفقوا بأنها صراع مسلح أو عنيف منظم، تشنه الدولة لتحقيق مصلحتها ضد دولة أخرى، مع اقتران الحرب بالتقنيات الإلكترونية التي أفضت إليها ثورة المعلومات.(Anthony E. Spezio, 2002, p 633.)

_ ويعرف **ريتشارد كلارك وروبرت كينك** بأنها "أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكومبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها". (ريتشارد أي كلارك وروبرت كي كنيك، 2012، ص 21.)

_ ويعرفها **سميت** بأنها "مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظام المعلومات المعادية بهدف التأثير والإضرار بها في الوقت نفسه للدفاع عن نظم المعلومات الخاصة بالدولة". (أحمد اوبيس الفتلاوي، 2016، ص 216,)

_ أما **كينيث جريس** فعرفها بأنها " القدرة على الدفاع والهجوم على المعلومات من خلال شبكات الحاسب الآلي عبر الفضاء الإلكتروني، بالإضافة إلى شل قدرة الخصم على القيام بنفس هذه الهجمات"

وتشمل الحرب السيبرانية عند جريس خمسة عناصر رئيسية هي التجسس، الدعاية، الحرمان من خدمة الأنترنت وتعديل البيانات والتلاعب بها. (إيهاب خليفة، 2017، ص 47.)

2-2-المطلب الثاني: أنماط الحرب الإلكترونية:

_ نمط الحرب الباردة الإلكترونية والصراع منخفض الشدة:

تستخدم الأطراف المتنازعة في هذا النمط من الحروب الفضاء الإلكتروني كساحة للصراع منخفض الشدة، ويتميز الصراع بين الأطراف في هذا النمط من الحروب، بأنه طويل الأمد ويمس العديد من الجوانب الثقافية، الاقتصادية والاجتماعية.

لها وسائل عدة منها شن الحروب النفسية، اختراقات متعددة، التجسس وسرقة المعلومات، شن حرب الأفكار والتنافس بين الشركات التكنولوجية العالمية وأجهزة الاستخبارات الدولية.

_ نمط الحرب الإلكترونية متوسطة الشدة:

يستخدم الفضاء الإلكتروني في هذا النمط من الحروب كساحة للصراع بين الأطراف، وتكون الحرب فيها مشابهة للحرب على الواقع، وبإمكانها أن تتطور لحرب عسكرية. وتكون الحرب الإلكترونية عن طريق اختراق المواقع الإلكترونية وتخريبها وشن حرب نفسية ضد الخصوم.

_ نمط الحرب الإلكترونية الساخنة والصراع مرتفع الشدة:

هذا النمط من الحروب يقوم على فرضية نشوء حروب في الفضاء الإلكتروني، وتكون غير متوازية مع الأعمال العسكرية التقليدية.

لم يشهد العالم هذا النوع من الحروب ولكن يبقى احتمال حدوثها وارد في المستقبل، نتيجة لتطور القدرات التكنولوجية واتساع الاعتماد المتبادل بين الدول والفواعل من غير الدول على الفضاء الإلكتروني، وينطوي هذا النمط على سيطرة البعد التكنولوجي على إدارة العمليات الحربية، أين يتم استخدام الأسلحة الإلكترونية فقط ضد منشآت العدو، وكذا اللجوء إلى الروبوتات الآلية في الحروب والطائرات دون طيار، في إدارتها عن بعد، بخلاف تطوير القدرات في مجال الدفاع والهجوم الإلكتروني والاستحواذ على القوة الإلكترونية، وفي هذا السياق يتم أيضا استخدام الفضاء الإلكتروني للاستعداد لحرب المستقبل عبر قيام الدول بتدريبات على توجيه ضربة أولى لحواسيب العدو واختراق العمليات العسكرية عالية التقنية، أو حتى استهداف الحياة المدنية والبنية التحتية المعلوماتية والهدف من ذلك تحقيق

الهيمنة الإلكترونية الواسعة بشكل اسرع في حالة نشوب صراع. (الحرب السيبرانية وتداعياتها على الأمن العالمي، 27-06-2019. https://www.politics-dz.com.)

2-3-المطلب الثالث: نموذج جوزيف ناي في توظيف القوة الإلكترونية

عمل جوزيف ناي على تطوير نموذج يتم الاستخدام فيه آليات معلوماتية لتوفير قوة صلبة وقوة ناعمة، حيث ترتكز عناصر القوة على وجود نظام متماسك يعظم القوم المتحصل عليها من خلال الترابط بين القدرات التكنولوجية، السكانية، الاقتصادية، الصناعية، العسكرية، وإرادة الدولة وغيرها بما يسهم في دعم إمكانيات الدول على ممارسة الإكراه، أو الإقناع أو ممارسة التأثير السياسي في أعمال الدول الأخرى بغرض الوصول للأهداف الوطنية من خلال قدرات التحكم والسيطرة على الفضاء.

وقد أعطت القوة السيبرانية دفعا في تدعيم القوة الناعمة للدول، حيث بات الفضاء الإلكتروني مسرحا لشن هجمات تخريبية ترتبط بنشر المعلومات المظللة، والحرب النفسية، والتأثير في توجهات الراي العام والنشاط السري الاستخباراتي، من جهة أخرى أعطت دعم للدول فيما يتعلق بزيادة الإنفاق في سياسات الدفاع الإلكتروني، وحماية شبكاتها الوطنية من خطر التهديدات وبناء مؤسسات وطنية للحماية الإلكترونية. (الحرب السيبرانية وتداعياتها على الأمن العالمي، 27-06-2019، https://www.politics-dz.com.)

ويستند هذا النموذج إلى ثلاث مفاهيم مركزية لفهمه تتمثل في:

1/ القوة الإلكترونية: يعرف ناي القوم الإلكترونية بأنها "القدرة على الحصول على النتائج المرجوة من خلال استخدام المعلومات المرتبطة بالفضاء الإلكتروني، لخلق مزايا والتأثير في الأحداث المتعلقة بالبيئات الواقعية الأخرى وذلك عبر أدوات إلكترونية".

يجادل ناي بأن مفهوم القوة الإلكترونية يشير إلى مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الإلكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل. (خليفة إيهاب، 2014، ص ص 24-25.)

وتتعدد أدوات ممارسة القوة في العلاقات الدولية وفقا لقدرات وإمكانيات ورغبات القوى المشاركة فيه، فقد تكون القوة العسكرية من اهم هذه الأدوات، وقد تكون القوة الاقتصادية والحصار الاقتصادي والمالي هما العامل الرئيسي للسيطرة على الخصم وممارسة القوة عليه، وقد تكون الأداة المعلوماتية من خلال وسائل الاتصال والتكنولوجيا الحديثة والأنترنت هي العامل الرئيسي لحل الصراع بين دولتين.

ويجادل ناي بأن هناك صعوبة في السيطرة على الفضاء الإلكتروني، فرغم سيطرة الدول عليه إلا أن هناك العديد من الفواعل التي تشاركها، ما يجعل الحكومات قلقة في حالة تسريب المعلومات، وذلك نظرا لصعوبة السيطرة عليه (الفضاء الإلكتروني). (إيهاب خليفة، 2017، ص 25.)

2/ القوة الإلكترونية وانتشار القوة: هناك العديد من الخصائص التي ساعدت على انتشار الفضاء الإلكتروني والاعتماد عليه بشكل متزايد، منها قلة التكلفة الاقتصادية، السرعة في التباد المعلومات، سهولة استخدامه فضلا عن إمكانية تخفي الفاعلين الذين يستخدمونه وعدم الكشف عن هوياتهم الحقيقية، وهو ما جعل الفضاء الإلكتروني بيئة جاذبة لمستخدميها، ودفعتهم إلى توظيفه في مختلف المجالات السياسية، الاقتصادية، الاجتماعية والعسكرية.

وكان نتيجة لذلك، تنوع وزيادة عدد الفاعلين المستخدمين للفضاء الإلكتروني، وتعدد مجالات استخدامه ووظائفه، فلم يعد يقتصر على تبادل المعلومات فحسب، بل أصبح بإمكان أحد مستخدمي الفضاء الإلكتروني أن يوقع خسائر فادحة بالطرف الآخر، وأن يتسبب في شلل البنية المعلوماتية والاتصالية الخاصة به، وهو ما يسبب خسائر عسكرية واقتصادية، من خلال قطع أنظمة الاتصال بين الوحدات العسكرية بعضها ببعض، أو تضليل معلومات أو سرقة معلومات سرية عنها أو من خلال التلاعب بالبيانات الاقتصادية والمالية وتزييفها أو مسحها من أجهزة الحواسيب، وعلى الرغم من فداحة الخسائر إلا أن الأسلحة تتمثل في فيروسات إلكترونية تخترق شبكة الحاسب الآلي، وتنتشر بسرعة بين الأجهزة وتبدأ عملها في سرية تامة وبكفاءة عالية، وهي بذلك لا تفرق بين المقاتل والمدني، وبين العام والخاص، وبين السري والمعلوم.

3/ الفواعل الدولية وتوظيف القوة الإلكترونية: يحدد جوزيف ناي ثلاثة أنواع من الفاعلين الذين يمتلكون القوة الإلكترونية.

أ_ الدول: التي لديها قدرة كبيرة على تنفيذ هجمات إلكترونية وتطوير البنية التحتية ومماسة السلطات داخل حدودها.

ب_ الأفراد (القراصنة): الذين يمتلكون معرفة تكنولوجية عالية والقدرة على توظيفها وعادة ما تكون هناك صعوبة في الكشف عن هوياتهم، ومن الصعب ملاحقتهم.

ج_ الفاعلون من غير الدول: يستخدم هؤلاء الفاعلون القوة الإلكترونية لأغراض هجومية بالأساس، إلا أن قدرتهم على تنفيذ أي هجوم سيبراني مؤثر يتطلب مشاركة ومساعدة أجهزة استخباراتية متطورة، ولكن يمكنهم اختراق المواقع الإلكترونية واستهداف الأنظمة الدفاعية، ويمكن حصر الفواعل من غير الدول في (الشركات متعددة الجنسيات-المنظمات الإجرامية-الجماعات الإرهابية). (إيهاب خليفة، 2017، ص

3-المبحث الثاني: الصراع الإلكتروني الأمريكي – الروسي

أدى التطور التكنولوجي الذي شهده العالم إلى تغيير طبيعة الصراع الدولي، وبذلك عملت الولايات المتحدة وروسيا إلى نقل صراعهما إلى الفضاء الإلكتروني لتحقيق مصالحهما بعيدا عن المواجهة المباشرة.

3-1-المطلب الأول: الاستراتيجية الأمريكية في الأمن الإلكتروني:

يعتبر التهديد الإلكتروني من بين التهديدات الجديدة التي أصبحت تهدد الأمن القومي الأمريكي، حيث توقعت العديد من التقارير والدراسات الأمريكية وقوع حروب إلكترونية في السنوات القادمة، وبذلك أصبح الأمن الإلكتروني على قمة أولويات الأمن القومي الأمريكي.

ومن أجل حماية معلوماتها الرقمية، خاصة المتعلقة بالأمن القومي عمدت الولايات المتحدة إلى تطبيق جملة من الإجراءات القانونية، التقنية والرقابية، التي تتناسب مع مكانتها الدولية وتطلعاتها السياسية، الاقتصادية، الاجتماعية والثقافية، مما يجعلها الدولة الأكثر أمننا في العالم.

_ **المنظومة القانونية:** تضم سلسلة من القوانين الفدرالية التي تنظم التعامل مع المعلومات الإلكترونية من منظور الأمن القومي الأمريكي، وقانون إصلاح وإدارة قطاع تكنولوجيا المعلومات، وقانون الحية الإلكترونية وغيرها من القوانين. (وليد غسان سعيد جعلود، 2013، ص 64.)

_ **المنظومة الفنية:** وهي التي تقوم بوضع المعايير الفنية والتقنية الموحدة للتعامل مع الأمن الإلكتروني، تتشكل هذه المنظومة من عدة جهات مختصة كالمعهد القومي للتكنولوجيا، ولجنة السياسة القومية لتشفير المعلومات، والتي تعمل على تشفير وترميز المعلومات والبيانات المتداولة إلكترونيا وحفظها، وكذا حمايتها من التداول اللاسلمي.

_ **المنظومة التنفيذية والتطبيقية والرقابية:** هي عبارة عن مجموعة من الهيئات والوكالات الفدرالية المسؤولة عن تطبيق وتنفيذ سياسات الأمن الإلكتروني، وتكون على اتصال مباشر مع المؤسسات والوزارات القومية الأمريكية، حيث تقدم لها هذه الخيرة الاستشارات والتطبيقات المعلوماتية والأمنية الإلكترونية، تقوم هذه المنظومة بالتنسيق مع العشرات من الوكالات على رأسها وكالة المخابرات ووكالة الأمن القومي، وزارة الدفاع، المكاتب المعنية بالشؤون الاجتماعية والاقتصادية، بهدف إبقاء الأمن المعلوماتي متزن مع جميع الجهات والحصول على قدر كاف من المعلومات المتعلقة بالأمن المعلوماتي الأمريكي. (وليد غسان سعيد جعلود، 2013، ص 65.)

ولقد أشارت الولايات المتحدة الأمريكية في استراتيجيتها الخاصة بأمنها القومي والصادرة عام 2010، إلى التهديد الذي يمكن أن تشكله الدول على المصالح الأمريكية في الفضاء الإلكتروني، حيث ركزت بشكل كبير على تداعيات أي هجوم محتمل على الاقتصاد القومي الأمريكي، حيث أصبحت ترى في الفضاء الإلكتروني بأنه يشكل المجال الخامس الذي تمارس فيه العمليات العسكرية. (نوران شفيق، 2018، ص 72.)

وبالتالي عليها أن تعمل على حفظ أمنها، وذلك عبر استراتيجية أمنية تقوم على أربع ركائز:

- ✓ تعزيز الأمن القومي الأمريكي من خلال تبادل المعلومات عبر الوكالات المتخصصة من أجل حماية شبكات الكومبيوتر وتأمين البنية التحتية الحيوية للبلاد.
- ✓ تعزيز الاقتصاد الرقمي، بتشجيع الابتكار في مجال التكنولوجيا، وذلك من خلال العمل مع شركات التكنولوجيا لتعزيز اختبارات الأمن الإلكتروني في المنتجات الجديدة، بالإضافة إلى بناء قوة عاملة حكومية في مجال الأمن الإلكتروني، من خلال توظيف المختصين من ذوي الكفاءات في مجال الأمن الإلكتروني في المؤسسات والوكالات الأمريكية.
- ✓ مكافحة التهديدات الإلكترونية، من خلال استخدام كافة أدوات القوة الأمريكية لردع أي هجومات وتعزيز المعايير الدولية في الفضاء الإلكتروني.
- ✓ الدعوى إلى حرية الأنترنت في جميع أنحاء العالم، وتزيد حلفائها بالقدرات الإلكترونية لمواجهة التهديدات المشتركة. (عمرو عبد العاطي، استراتيجية أمريكية هجومية ضد التهديدات السيبرانية، 31-10-2018، https://www.ecsstudies.com.

3-2-المطلب الثاني: الاستراتيجية الروسية في الأمن الإلكتروني:

اهتمت روسيا بأمنها المرتبط بالشق الإلكتروني بعد تأسيس مجلس الأمن الروسي عام 1992 ومؤسساتها الأمنية، حيث عملت على إنشاء مؤسسات متخصصة بالقضايا الإلكترونية لما يشكله هذا المجال من تهديد، ومن بين هذه المؤسسات نجد مجلس الأمن، جهاز الأمن الفدرالي للتحكم التقني، ووزارة الاتصالات وتكنولوجيا المعلومات.

وتتركز المهام بين الإدارات المختلفة في الأنشطة المتعلقة بالأمن الإلكتروني كالآتي:

_ وزارة الداخلية تهتم بمواجهة الجرائم الإلكترونية.

_ وزارة الدفاع تهتم بكل ما يتعلق بأخطار الحروب الإلكترونية وتطوير القدرات الإلكترونية الهجومية للجيش الروسي.

_ جهاز الأمن الفدرالي يهتم بالإرهاب الإلكتروني. (نوران شفيق، 2018، ص ص 66-69.)

وقد بدأ الأمن الإلكتروني يشكل محور اهتمام القيادات الروسية عام 2000، حيث أدركت روسيا الدور الذي أصبح يلعبه الأمن الإلكتروني في تحقيق المصالح القومية وتعزيز الاستقرار الاجتماعي والسياسي، وبناءا على ذلك قامت بتطوير استراتيجيتها الأمنية، وذلك نظرا لتزايد التنافس التكنولوجي بين الفواعل على مستوى النظام الدولي، وقد سعت روسيا إلى تطوير اتفاقية دولية لمواجهة المخاطر الإلكترونية الناتجة عن هذا التنافس.

وقد أنشأت روسيا ما يعرف بجيش المتصدين تابع لوكالة الأمن الاتحادي الروسي يضم الآلاف من الموظفين، يخصص له سنويا حوالي 300 مليون دولار من ميزانية الدفاع الروسية. (أحمد يوسف الجميلي، القدرات السيبرانية سلاح روسيا ضد الخصوم، 19-06-2018، https://www.making policies.org.) ويعد خامس أقوى جيوش العالم الإلكترونية بعد كل من الولايات المتحدة الأمريكية، الصين، بريطانيا وكوريا الشمالية على التوالي، ويعتمد على عنصر المباغتة لإرباك الخصم، وتتلخص مهامه فيما يلي:

- ✓ القيام بعمليات التجسس على الخصوم
- ✓ شن الهجمات الإلكترونية التي تسبب الضرر بالبنى التحتية والاقتصادية والمواقع الحكومية في الدول المعادية
- ✓ شن حروب معلوماتية في وسائل الإعلام والشبكات الاجتماعية عن طريق القيام بعمليات اختراق الحسابات والبريد الإلكتروني، وإنشاء حسابات وهمية على شبكة المعلومات الدولية، وفتح الآلاف من الحسابات المزيفة على مواقع التواصل الاجتماعي للرد على الآلاف من التعليقات والمقالات ونشر الشائعات وتضليل الحقائق في محاولة لدعم الموقف الروسي وتوجيه الرأي العام ضد الخصوم.

_ الأدوات التي تعتمد عليها روسيا في الحرب الإلكترونية:

حسب دراسة قام بها ديفيد سميث David J. Smith فإن روسيا تستخدم في الحرب المعلوماتية الاستخبارات، التجسس المضاد، الخداع، التضليل، تدمير الاتصالات وأنظمة دعم الملاحة، الضغوط النفسية، الدعاية الحاق الضرر بنظم المعلومات.

ومن خلال ذلك فالحرب المعلوماتية الروسية تستند إلى أداتين رئيسيتين:

- ✓ **التضليل المعلوماتي:** حيث تعتمد روسيا على توظيف الأدوات الإعلامية والدعائية المختلفة بهدف إعادة إنتاج روايات مضللة للآخرين ومشوهة للحقائق، وذلك لخدمة المصالح الروسية على حساب الأطراف الغربية، ويظهر هذا النمط في تعامل وسائل الإعلام الروسية مع الأحداث السياسية التي شهدتها الدول الغربية.
- ✓ **القرصنة الإلكترونية:** يشكل الهجوم على البنية المعلوماتية للدول الأخرى جزءا هاما من استراتيجية حرب المعلومات الروسية، باعتباره وسيلة للحد من فعاليات الخصم، وإرباكه وتضليله، ناهيك عن فعالية عمليات القرصنة في تجزئة نظام القيادة لدى الدول المعادية لروسيا، والسيطرة عليها ولو لفترة زمنية محدودة.

وفي الوقت الذي كانت فيه الدول الغربية تتهم روسيا بالتورط في عمليات القرصنة الإلكترونية، كانت روسيا تعمل على صياغة نموذج جديد من العلاقات، يطلق عليه "تيم مور Tim Maurer" توظف فيه وكلاء سيبرانيين Cyber Proxy Actors، من منظمات ومجموعات خاصة بالقرصنة أهمها APT29/APT28، وهو ما يسمح لها بتحقيق مصالحها، وكذا التنصل من الاتهامات الغربية الموجهة لها.

وتسعى روسيا من خلال مقاربة حرب المعلومات إلى ما يلي:

_ تقويض قدرة الخصم وإضعافه على المواجهة من خلال عمليات القرصنة.

_ تشويه القوى المناهضة من خلال نشر معلومات والحقائق زائفة حول العدو، وتشييد صورة إيجابية حول حلفائها.

_ العمل على إثارة مشاكل داخلية في الدول المناوئة لروسيا.

_ مواجهة العقوبات الغربية التي فرضتها الدول الأوروبية على روسيا عام 2014 والمتمثلة في حظر التأشيرات، تجميد الأصول وفرض قيود تجارية واقتصادية، وذلك كرد فعل على تدخل روسيا في أوكرانيا في 2014، وضم شبه جزيرة القرم بعد استفتاء مارس من نفس العالم. (محمد بسيوني، عقيدة جيراسيموف: دوافع الاستراتيجية الروسية لحرب المعلومات ضد الدول الغربية، 23-10-2017، .https://futureuae.com)

3-3-المطلب الثالث: التدخل الروسي في الانتخابات الأمريكية كمظهر للحرب الإلكترونية بين أمريكا وروسيا

تعود حيثيات هذه الحادثة إلى عام 2012 أين ادعت روسيا بأن **هيلاري كلينتون** -عندما كانت تشغل منصب وزيرة الخارجية الأمريكية- شجعت الاحتجاجات التي انطلقت بعد انتهاء الانتخابات الروسية في مارس 2012، و التي أتت ب**فلاديمير بوتين** رئيسا لروسيا الاتحادية، الأمر الذي دفع المعارضة الروسية و المنافسين الأربعة ل**بوتين** من التشكيك في نزاهة الانتخابات فانطلقت المظاهرات و الاحتجاجات، و في المقابل قامت حملة اعتقالات طالت قادة المعارضة في روسيا من قبل السلطات، فأعربت الخارجية الأمريكية عن قلقها من حركات القمع و المعارضة أكثر من مرة، و هو ما اعتبرته القيادة الروسية محاولة من **كلينتون** لخلق حالة من الفوضى السياسية في البلاد. (عمرو صبحي، تكتيك الدرع والسيف في استخدام القوة السيبرانية، 26-04-2018، .http://www.qcrrseg.org)

أصبحت الدول في الوقت الراهن تعمل جاهدة من اجل حماية الحسابات الإلكترونية والبريدية التابعة للدولة، من اجل تجنيب أمنها القومي خطر الحروب الإلكترونية، لذلك فقد أصبحت تمنح المسئولين حسابات بريدية رسمية ولكن في بداية سنة 2015، وقبل أن تعلن **كلينتون** عن نيتها في الترشح للانتخابات الرئاسية الأمريكية، كشفت تقارير صحفية عن استخدام **هيلاري** بريدا إلكترونيا خاصا تستخدمه بدلا من البريد الرسمي وهو ما أثار المخاوف الأمريكية حول تعرضه لعمليات قرصنة مما يهدد الأمن القومي.

اتهمت الولايات المتحدة الأمريكية روسيا بالقيام بهجمات إلكترونية و ذلك باختراق البريد الإلكتروني للحزب الديمقراطي الأمريكي و مدير حملة المترشحة **هيلاري كلينتون، جون بوديشا** و قامت بتسريب رسائل البريد الإلكتروني إلى موقع ويكيليكس لنشرها كما استخدمت حسابات روسية شبه معلنة و أخرى خفية على مواقع التواصل الاجتماعي هاشتاغات و عبارات منتشرة لإظهار ما يبدو أنهم مؤيدو المرشح الجمهوري **دونالد ترامب** المحافظون أو المشجعون يمينيون متطرفون على وسائل التواصل الاجتماعي و التي تمتلئ تعريفاتهم الشخصية بكلمات مثل الدولة المسيحية، أمريكا، الجيش ثم يدفعون بهاشتاغات مؤيدة ل**ترامب** مع أخبار كاذبة و مضللة إلى الجمهور الأمريكي الأمر الذي ساعد على إحداث حالة التأييد ل**ترامب** و التشكيك في الحكومة الأمريكية. (أحمد يوسف الجميلي، القدرات السيبرانية سلاح روسيا ضد الخصوم، 19-06-2018، https://www.making policies.org)

الاستنتاجات:

لقد توصلت هذه الدراسة إلى مجموع من النتائج تتمثل في:

_ صعوبة تحديد تعريف موحد وشامل للحرب الإلكترونية وذلك راجع لتعدد استخداماته والتطورات المعرفية التي مازالت تلحق بهذا المصطلح.

_ أصبح الفضاء الإلكتروني ساحة جديدة للصراع الدولي، وذلك من خلال استخدامه في أعمال تدميرية وتخريبية كتخريب الأنظمة المعلوماتية والشبكات ما يهدد أمن الدول.

_ وجدت الدول نفسها أمام نوع جديد من التهديدات، وهو ما فرض عليها تبني استراتيجيات دفاعية بهدف تقويض خطر الحروب الإلكترونية، خاصة في ظل امتلاك بعض الفواعل الدولية القدرة الهجومية في المجال الإلكتروني.

_ عملت الولايات المتحدة الأمريكية وروسيا على نقل مجريات الحرب الباردة إلى الفضاء الإلكتروني، وقد مثل التدخل الروسي والانتخابات الرئاسية الأمريكية الأخيرة في 2016 بمثابة إعلان عن حرب باردة جديدة انتقلت ساحتها إلى الفضاء الإلكتروني.

وبناءا على ذلك فإن الفضاء الإلكتروني أصبح اليوم الساحة التي ترى فيه الدول المجال الذي يساعدها لتحقيق مصالحها القومية في مختلف المجالات، وبالتالي فإن أي تهديد محتمل أو هجوم على أي قطاع يؤدي لحدوث عدم توازن استراتيجي، وهو ما يعبر عن نمط جديد من التهديدات للأمن القومي للدول، وإمكانية حدوث حروب سيبرانية، حيث أصبحت هذه الأخيرة إحدى أدوات التأثير في المعلومة المستخدمة في مختلف مستويات ومراحل الصراع، بهدف التأثير بشكل سلبي عليها وعلى نظم عملها. لذلك يتوجب على الدول العمل على إنشاء منظمات وهيئات تعنى بمسؤولية تنظيم الفضاء الإلكتروني وتكون ملزمة.

قائمة المراجع:

_ Spezio, Anthony E. (2002**). Member leee Electronic Warfar Systems, Transactions on microwave theory and techniques** (3).

_ أي كلارك، ريتشارد. وكي كنيك روبرت. (2012)، **حرب الفضاء الإلكتروني التهديد التالي للأمن القومي وكيفية التعامل معه**، (ط. 1). الإمارات: مركز الإمارات للبحوث والدراسات الاستراتيجية.

_ الفتلاوي، أحمد اوبيس. (2016)، **الهجمات السيبرانية: مفهومها المسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر ، مجلة المحقق الحلي للعلوم القانونية والسياسية (04)**،

_ خليفة، إيهاب. (2017)، **مجتمع ما بعد المعلومات: تأثير الثورة الصناعية على الأمن القومي.** مصر: العربي للنشر والتوزيع.

_ الحرب السيبرانية وتداعياتها على الأمن العالمي، 27-06-2019. .https://www.politics-dz.com

_ المرجع نفسه.

_خليفة، إيهاب، (2014)، **القوة الإلكترونية وأبعاد التحول في خصائص القوة**، مصر: مكتبة الإسكندرية، ووحدة الدراسات المستقبلية.

_ إيهاب خليفة، (2017)، **مجتمع ما بعد المعلومات: تأثير الثورة الصناعية على الأمن القومي.** مصر: العربي للنشر والتوزيع.

_ المرجع نفسه.

_ غسان، وليد سعيد جعلود، (2013)، **دور الحرب الإلكترونية في الصراع العربي الإسرائيلي**، مذكرة مقدمة لنيل شهادة الماجستير، كلية الدراسات العلي نابلس، فلسطين.

_ المرجع نفسه.

_ شفيق، نوران. (2018)، **أثر التهديدات الإلكترونية على العلاقات الدولية دراسة في أبعاد الأمن الإلكتروني.** القاهرة: المكتب العربي للمعارف.

_عمرو، عبد العاطي. 31-10-2018، استراتيجية أمريكية هجومية ضد التهديدات السيبرانية، https://www.ecsstudies.com.

_ شفيق، نوران. المرجع سبق ذكره.

_ الجميلي، أحمد يوسف. 19-06-2018، القدرات السيبرانية سلاح روسيا ضد الخصوم، https://www.making policies.org

_ بسيوني، محمد. 23-10-2017، عقيدة جيراسيموف: دوافع الاستراتيجية الروسية لحرب المعلومات ضد الدول الغربية. https://futureuae.com

_صبحي، عمرو. 26-04-2018، تكتيك الدرع والسيف في استخدام القوة السيبرانية، .http://www.qcrrseg.org

_ الجميلي، أحمد يوسف. المرجع سبق ذكره.