الحروب السيبرانية وأثرها في العلاقات الدولية

روسيا والولايات المتحدة الأمريكية نموذجاً

م. احمد عثمان محمد

جامعة التقنية الوسطى معهد الإدارة / الرصافة قسم تقنيات إدارة المواد

Cyber Wars and Its Influence in International Relations: Russia and USA Model

By: Ahmed O. Mohammed

Institute, Management / Rissafa

pfkvmxc@gmail.com

ملخص

أصبحت الحروب السيبرانية جزءاً لا يتجزأ من استراتيجيات إدارة الصراع الدولي وفرض الإرادة في العلاقات الدولية، مما دفع العديد من الدول والقوى الدولية لتبني استراتيجيات سيبرانية واضحة ومعلنة، وكذلك إجراء تعديلات دستورية وتشريعية تسمح باتخاذ خطوات جدية في إطار توفير الأمن السيبراني للدولة ببعدية الإيجابي والسلبي، إذ يشمل البعد السلبي للأمن السيبراني قدرة الدولة على تأمين نفسها ضد الهجمات السيبرانية من دول أخرى، بينما يشمل البعد الإيجابي توافر القدرة لدى الدولة على شن الهجمات السيبرانية عند الحاجة، وذلك بهدف الحصول على معلومات، أو شل قدرة الخصوم في مجال محدد، أو تدمير قدرات الدولة الخصم دون الحاجة إلى إعلان الحرب رسمياً أو تحريك قوات عسكرية على الأرض.ولما كان للحروب السيبرانية تأثيراً كبيراً ومتزايداً في العلاقات الدولية في عالم ما بعد العولمة، وفي إطار التطور التكنولوجي الكبير في تكنولوجيا الاتصالات، كان من الطبيعي أن تنتهج اثنتين من القوى الدولية الكبرى (روسيا، الولايات المتحدة) نهجاً استراتيجياً يتماشى مع دخول البعد السيبراني إلى أبعاد إدارة صراعاتهما الدولية المختلفة.وفي إطار كل ما سبق، نرصد في هذه الورقة البحثية مفهوم الحرب السيبرانية، وأهميته وأبعاده المختلفة، وكذلك تأثيراته المتزايدة في مجال العلاقات الدولية، مع نموذج تطبيقي يتمثل في اثنتين من القوى الدولية الكبرى (روسيا والولايات المتحدة الأمريكية) وكيف قامت كل منهما بتوظيف الحروب السيبرانية توظيفاً استراتيجياً يخدم أهدافهما الاستراتيجية في إدارة صراعتهما الدولية.

الكلمات المفتاحية:الحروب السيبرانية– الهجمات السيبرانية– العلاقات الدولية– روسيا– الولايات المتحدة الأمريكية

Abstract

Cyberwars have become an integral part of strategies for managing international conflict and imposing will In international relations, which prompted many countries and international powers to adopt clear and declared cyber strategies, as well as to make constitutional and legislative amendments that allow taking serious steps in the framework of providing cyber security for the state in both positive and negative dimensions, as the negative dimension of cyber security includes the state's ability to secure itself Against cyber-attacks from other countries, while the positive dimension includes the availability of the ability of the state to launch cyber-attacks when needed, with the aim of obtaining information, or paralyzing the ability of opponents In a specific field, or destroying the capabilities of the adversary country without the need to officially declare war Or move military forces on the ground.And since cyber warfare has a significant and increasing impact on international relations in the post-globalization world, In the context of the great technological development in communications technology, it was natural for two of the major international powers (Russia, the United States) to adopt a strategic approach in line with the entry of the cyber dimension to the dimensions of managing their various international conflicts.Within the framework of all of the above, we monitor in this research paper the concept of cyber warfare, its importance and various dimensions, as well as its increasing effects in the field of international relations, with an applied model represented in two of the major international powers (Russia and the United States of America) and how each of them strategically utilized cyber warfare to serve their strategic goals in managing their international conflict.

key words: Cyber wars - Cyber-attacks - International Relations - Russia - USA

مقدمة:

تعتبر الحروب السيبرانية أحد أشكال الجيل الخامس من الحروب، وهي الحروب التي يتعاظم استخدامها على نطاق واسع مع التطور التكنولوجي في وسائل الاتصالات، وأنظمة التشغيل الإلكترونية، واتجاه الدول للرقمنة. وتتجه العديد من الدول – التي تمتلك الأدوات التكنولوجية اللازمة – لشن الحروب السيبرانية عند اللزوم بدلاً من الحروب العسكرية التقليدية نظراً لانخفاض تكلفتها المادية والمعنوية، مع عظم تأثيرها.ويزخر التاريخ المعاصر بالعديد من الحروب السيبرانية بين الدول وبعضها البعض، إلى الحد الذي جعل قوى دولية كبرى تنشأ وحدات عسكرية قتالية متخصصة في الحروب السيبرانية، أبرزها على الإطلاق (القيادة السيبرانية الأمريكية US Cyber Command، الوحدة ٦١٣٩٨ الصينية، الوحدة ٨٢٠٠ الإسرائيلية، قراصنة الظل التابعة للحكومة الروسية)، كما أصدرت العديد من الدول استراتيجياتها الخاصة بمواجهة الحروب السيبرانية، وكذلك تم إجراء التعديلات الدستورية اللازمة بما يتيح إصدار تشريعات وقوانين لمجابهة الحروب السيبرانية بأنواعها.[1]لقد أدت نهاية الحرب الباردة إلى بروز العديد من التحديات والتهديدات التي لم يشهدها المجتمع الدولي من قبل، والتي تُعرف بالتهديدات اللاتماثلية أو اللاتناظرية العابرة للحدود التي لا تعترف لا بالحدود أو السيادة الوطنية أو فكرة الدولة القومية، ومن أبرزها الحروب السيبرانية، مما أفضى إلى اعتبار الفضاء السيبراني بمثابة المجال الخامس في

الحروب بعد البر والبحر والجو والفضاء، الأمر الذي أدى إلى حدوث تحولات في حقل الدراسات الأمنية والاستراتيجية وكذلك على مستوى الممارسة السياسية.ومع التغيرات المتلاحقة التي يشهدها النسق الدولي في عالم ما بعد العولمة – التي أفرزت الاعتماد على تكنولوجيا الاتصالات لتحقيق الربط بين الدول وبعضها البعض– وما يصاحبها من أنماط سلوكية وتفاعلية جديدة بين الدول، برزت الحاجة إلى إضافة بعد جديد لأبعاد الدراسات الأمنية في العلاقات الدولية وهو مفهوم الأمن السيبراني كمتغير جديد في العلاقات الدولية، بما يشمله من دراسة أساليب وطرق وآثار الهجمات السيبرانية، ومن هنا، تأتي هذه الدراسة في ذلك الإطار لتحليل أبعاد وطرق الحروب السيبرانية وتأثيرها في العلاقات الدولية، مع دراسة حالة للحروب السيبرانية التي تشنها كل من روسيا والولايات المتحدة الأمريكية.[٢]

أهمية البحث:تنبع أهمية البحث من كونه محاولة علمية لقياس مفهوم وأبعاد الحرب السيبرانية ومدى تأثيرها على العلاقات الدولية بين دول العالم المختلفة، وكذلك دورها في تشكيل ترتيب سلم القوى بين القوى الدولية المختلفة في إطار استخدامها للتأثير وفرض الإرادة كأحد أدوات إدارة الصراع الدولي.

هدف البحث:يهدف البحث للإجابة عن التساؤل البحثي الرئيسي والتساؤلات البحثية الفرعية من خلال تحليل أبعاد الحروب السيبرانية وأثرها في العلاقات الدولية بين القوى الدولية المختلفة.

مشكلة البحث:تكمن المشكلة البحثية في قياس مدي تأثير استخدام القوى الدولية المختلفة للهجمات السيبرانية على علاقاتها الدولية المختلفة، وذلك في ضوء الصراع على القوة وفرض الإرادة، وبناء على ذلك، يمكن طرح التساؤل البحثي الرئيسي للورقة البحثية على النحو التالي:**إلى أي مدى يمكن أن يكون للحروب السيبرانية تأثير في صياغة شكل وطبيعة العلاقات الدولية بين القوى الدولية المختلفة؟**وينبثق عن التساؤل البحثي الرئيسي عدد من التساؤلات البحثية الفرعية كالتالي:

- ما مفهوم وأبعاد الحروب السيبرانية؟
- ما تأثير استخدام الحروب السيبرانية في صياغة وتشكيل العلاقات الدولية المختلفة؟
- ما أبرز الهجمات السيبرانية التي استخدمتها كل من روسيا والولايات المتحدة والتي أسهمت بشكل كبير في لعب دور مؤثر في الصراعات الدولية؟
- كيف تستخدم كل من روسيا والولايات المتحدة الهجمات السيبرانية كأحد أدوات إدارتها لعلاقاتها الدولية؟

فرضية البحث:ينطلق البحث من فرضية رئيسية تعتبر عماد هذه الدراسة تقوم على وجود علاقة ارتباطية هامة بين استخدام الحروب السيبرانية (كمتغير مستقل)، والتأثير في شكل وطبيعة العلاقات الدولية (كمتغير تابع).

منهج البحث:يستخدم البحث كل من المنهج الوصفي التحليلي ومنهج دراسة الحالة، وذلك كالتالي:

- المنهج الوصفي التحليلي:تم اعتماده من منظور الوصف والتحليل لمفهوم الحروب السيبرانية وأبعادها ودراسة تأثير استخدام الحروب السيبرانية في العلاقات الدولية.
- منهج دراسة الحالة:تم استخدامه للتركيز على استخدام كل من (روسيا، الولايات المتحدة الأمريكية) للحروب السيبرانية للتأثير في صياغة وتشكيل علاقاتهما الدولية وفرض إرادتهما في المشكلات الدولية المختلفة في إطار إدارة الصراع الدولي.

هيكلية البحث: تم تقسيم الدراسة إلى مبحثين وخاتمة، كالتالي:

- المبحث الأول: مفهوم الحروب السيبرانية ودورها في صياغة وتشكيل العلاقات الدولية.
- المبحث الثاني: دور استخدام كل من روسيا والولايات المتحدة للحروب السيبرانية في العلاقات الدولية لكل منهما.

– خاتمة.

المبحث الأول مفهوم الحروب السيبرانية ودورها في صياغة وتشكيل العلاقات الدولية

أولاً: مفهوم الحروب السيبرانية: يعتبر مصطلح السيبرانية واحد من أكثر المصطلحات تردداً في مجال العلاقات الدولية،وتشير المقاربة اللغوية لكلمة"cyber" إلى أنها لفظة يونانية الأصل مشتقة من كلمة "kybernetes" بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجاز اً للمتحكم"governor" ،وتجدر الإشارة إلى أن العديد من المؤرخين يرجعون أصلها إلى عالم الرياضيات الأمريكي Norbert Wieners 1894– 1964 وذلك للتعبير عن التحكم الآلي، فهو الأب الروحي المؤسس للسيبرانية من خلال مؤلفه الشهير Cybernetics or Control and Communication in the Animal and Machine وأشار في كتابه إلى أن السيبرانية هي التحكم والتواصل عند الحيوان والآلة، والإنسان والآلة، ليستبدل مصطلح الآلة بعد الحرب العالمية الثانية بأجهزة الكمبيوتر.[٣]وبالنظر إلى أن مصادر

قوة الدولة وأشكالها تتغير، فإلى جانب القوة الصلبة ممثلة في القدرات العسكرية والاقتصادية، تزايد الاهتمام بالأبعاد غير المادية للقوة، ومن ثم بروز القوة الناعمة التي تعتمد على جاذبية النموذج والإقناع، ومع ثورة المعلومات ظهر شكل جديد من أشكال القوة هو القوة السيبرانية التي لها تأثير كبير على المستوى الدولي والمحلي، فمن ناحية، أدت إلى توزيع وانتشار القوة(Cyber Power) بين عدد أكبر من الفاعلين، ما جعل قدرة الدولة على السيطرة موضع شك،ومن ناحية أخرى منحت الفاعلين الأصغر قدرةً أكبر على ممارسة كل من القوة الصلبة والقوة الناعمة عبر الفضاء السيبراني، وهو ما يعني تغيرات في علاقات القوى في السياسة الدولية[4].من هذا المنطلق أصبح الباحثون في حقل العلاقات الدولية وبقية الحقول الفرعية في الدراسات الأمنية والدراسات الاستراتيجية بشكل متزايد حول أثر التكنولوجيا على الأمن القومي والدولي،ويشمل ذلك تأثيرها على المفاهيم ذات الصلة كالقوةpower والسيادةsovereignty والحوكمة العالميةglobal governance والأمننةsecuritization ، وكذلك اهتم الباحثون كيف يعمل توسع الإنترنت على إعادة بلورة الأشكال التقليدية وقواعد القوة الدولية التي تعمل على نطاق واسع للدخول في عصر جديد للجيوبوليتيك[5].وعلى مستوى الممارسة للدول، فقد ارتبط ظهور الهجمات السيبرانية بعاملين أساسين، كالتالي:

١- استحداث أجهزة الكمبيوتر في منتصف الخمسينيات من القرن المنصرم كأداة لمعالجة وحفظ المعلومات رافقه تضافر جهود عدد من الشركات الخاصة والعامة، توج بتطوير وحدة المعالجة المركزية رقمياً، وذلك لتسهيل المهام الموكلة لها، وقد تطور ذلك بصورة جذرية في العقود اللاحقة، حتى أصبح جهاز الكمبيوتر أساساً في عمل الكثير من المؤسسات الخاصة والعامة، فضلاً عن الحياة اليومية.

٢- ظهور الشبكة العنكبوتية (الإنترنت) ، الذي أحدث انقلاباً مثير اً في حياة البشرية من خلال التواصل ونقل المعلومات بسرعة فائقة، وقد سارعت الدول في وتيرة استخدام الكمبيوتر لتحقيق قفزات نوعية في المجال الأمني والعسكري في مطلع التسعينيات من القرن العشرين، وذلك حتى أطلق البعض عليها مصطلح الحرب السيبرانية الباردة Cyber Cold War أو سباق التسلح السيبراني Cyber Arms Race.[٦]ويحدد جوزيف ناي نوعين من الفواعل الذين يمتلكون القدرة على شن هجمات سيبرانية،[٧] كالتالي:

١- **الدول** :والتي لديها قدرة كبيرة على تنفيذ هجمات سيبرانية وتطوير البنية التحتية وممارسة السلطات داخل حدودها، فالدولة هي الفاعل المحوري بامتياز في هذا العالم الافتراضي، لما لها من مكانة على أساس التفوق التكنولوجي والمؤهلات التي ترشحها لتبني هذه المكانة.

٢- **الفواعل من غير الدول**: ويستخدم هؤلاء الفاعلون القوة السيبرانية لأغراض هجومية بالأساس،إلا أن قدرتهم على تنفيذ أي هجوم سيبراني مؤثر تتطلب مشاركة ومساعدة أجهزة استخباراتية متطورة، ولكن يمكنهم اختراق المواقع الإلكترونية واستهداف الأنظمة الدفاعية،وتشمل هذه الفواعل ما يلي[٨]:

أ- الشركات متعددة الجنسيات :تمتلك بعض شركات التكنولوجيا موارد للقوة تفوق قدرة بعض الدول، ولا تنقصها سوى شرعية ممارسة القوة التي ما زالت حكراً على الدول، فخوادم شركات (جوجل، فيسبوك، مايكروسوفت) على سبيل المثال، تسمح لها بامتلاك قواعد البيانات العملاقة التي من خلالها تستكشف، وتستغل الأسواق، وتؤثر في اقتصاديات الدول وفي ثقافة المجتمعات وتوجهاتها.

ب- المنظمات الإجرامية :تقوم هذه المنظمات الإجرامية بعمليات القرصنة السيبرانية، وسرقة المعلومات واختراق الحسابات البنكية وتحويل الأموال، كما توجد سوق سوداء على الإنترنت المظلم لتجارة المخدرات والأسلحة والبشر.

ج- الجماعات الإرهابية :تعد من أبرز الفواعل الدولية، خاصة بعد أحداث 11 سبتمبر، حيث تستغل الفضاء السيبراني في عمليات التجنيد والتعبئة والدعاية وجمع الأموال والمتطوعين، كما تحاول جمع المعلومات حول الأهداف العسكرية، وكيفية التعامل مع الأسلحة وتدريب المجندين عن بعد.

د- الأفراد :أصبح الفرد بفضل الفضاء السيبراني فاعلاً مؤثراً في العلاقات الدولية،ومن أبرز النماذج (جوليان أسانج) مؤسس WikiLeaks الذي نجح في نشر ملايين الوثائق السرية ومنها وثائق للإدارة الأمريكية على سبيل المثال، ما خلق مشاكل دبلوماسية بين الولايات المتحدة الأمريكية وحلفائها.وبناء على كل ما سبق، يمكن تعريف الحروب السيبرانية على أنها (الأفعال الصادرة من أجهزة كمبيوتر وشبكات المعلومات التابعة لدولة ما بشكل منظّم ومدروس على أجهزة كمبيوتر وشبكات معلومات لدولة أخرى، بغرض التجسّسEspionage ، أو التخريبSabotage ، أو التوجيه)، وتعتمد الهجمات السيبرانية أساساً على الوحدات السيبرانية التي تضمّ الجنود السيبرانيين، وهم في الأصل قراصنة رقميّون يتمّ استخدامهم على شكل فرق متخصّصة، وإعطاءهم إمكانات لوجستيّة وخوادم على شبكات المعلومات، وتوجيههم لأغراض محدّدة، مثل مراقبة كلّ شبكات المعلومات الحسّاسة (شبكات الطاقة، المياه، الكهرباء، الاتصالات، الأمور الماليّة في البنوك)،

أو الردّ على أي هجمات، أو التجسّس، أو توجيه الرأي العام لدول معادية،[9] وكانت معظم الهجمات السيبرانية سابقًا تُشنّ بواسطة أشخاص أو مبرمجين لأهداف شخصيّة؛ أمّا في العقدين الأخيرين،فقد دخلت المنظّمات الأمنيّة والحكومات إلى هذه الساحة، وأخذت تُنفق الملايين لتطوير قدراتها وبناء جيوش سيبرانية، وبرزت إسرائيل والولايات المتحدة والصين وروسيا وإيران والمملكة المتّحدة وكوريا الشماليّة وفرنسا في مقدّمة الدول المتقدّمة في تقنيّات الحروب السيبرانية[10]، ومن جانب آخر، تنقسم الهجمات السيبرانية الى أنماط رئيسية، كالتالي[11]:

١- **البرمجيات الخبيثة Malware**:البرمجيات الخبيثة هو مصطلحٌ يُستخدم لوصف البرمجيات التي تخترق الشبكة أو الأنظمة دون علم ملّاكها من خلال ثغرةٍ أمنية، ويحدث تنشيطها عادةً من قِبل المستخدم عند النقر على رابط مشبوه، أو تنزيل مرفق بريد إلكتروني مجهول المصدر، ومن أمثلتها:

أ- برمجيات التجسس Spyware: وهي برمجياتٌ تعمل على نقل المعلومات من الأجهزة المُصابة دون علم مالكيها بهدف التجسس.

ب-برمجيات الفدية Ransomware: هي نوعٌ يُصمَّم بهدف ابتزاز المال، وذلك من خلال منع المستخدم من الوصول إلى الملفات أو نظام الحاسوب حتى تُدفع الفدية. ومع ذلك، لا يُعد دفعها ضماناً حتمياً لاسترداد الملفات أو النظام.

٢- **هجمات يوم الصفر Zero-Day Attack**:يُطلق هذا الاسم على الهجمات التي تستغل الثغرات الأمنية قبل اكتشافها من قِبل الجهة نفسها، وقبل أن تشرع في إصلاحها وإيجاد الحلول لها.

٣- **الهجمات المستهدفة**:يتم فيه استخدام عدد من أساليب القرصنة لمهاجمة مستخدمٍ أو منظمةٍ محددةٍ مسبقاً.

٤- **حقن تعليمات الاستعلام "SQL"**:يتضمن هذا النوع من الهجمات إدراج التعليمات البرمجية الخبيثة في خادم باستخدام حقن تعليمات الاستعلام الهيكلية (إس كيو إل)، وذلك يجبر الملقم على كشف المعلومات التي لا تُكشف غالباً. ويمكن للمهاجم تبنّي هذه الهجمة عبر إرسال شفرةٍ خبيثة إلى مربع بحث في أحد مواقع الويب الضعيفة.

٥- **الهندسة الاجتماعية Social Engineering**:وهو تهديدٌ يلجأ إلى استخدام أساليب مختلفةٍ للتأثير على الضحية ودفعه لكشف معلوماتٍ شخصية أو سرية حساسة دون أن يشعر، ومن ثم استخدامها بغرض الاحتيال.

٦- **التصيّد الاحتيالي Phishing**:يتضمن إرسال رسائل بريد إلكتروني احتيالية، تشبه رسائل المصادر الموثوقة، وتهدف إلى سرقة بيانات حساسة مثل أرقام بطاقات الائتمان، ومعلومات تسجيل الدخول، وهو من أكثر أنواع الهجمات السيبرانية شيوعاً.

٧- **هجوم الوسيط (Man-in-the-Middle)**:نوعٌ من أنواع الهجمات التي تُعرف أيضاً باسم هجمات التنصت، ويحدث أن يعترض المهاجم خط التواصل بين طرفين بغرض التنصت، أو التلاعب بالمعلومات المتبادلة بينهما أو سرقتها.

٨- **حجب الخدمة DDos**:يستهدف هجوم حجب الخدمة الخدمات السيبرانية أو الشبكة بهدف منع المستخدمين من الوصول إليها عبر إغراقها بطلبات وهمية تتسبب في عجز النظام عن تلبية الطلبات الحقيقية. وتتوافر للحروب السيبرانية العديد من المزايا والخصائص[12]، كالتالي:

١- تستطيع الحروب السيبرانية إلحاق الأضرار بالخصم، مهما كانت طبيعتها، من دون أن تتجاوز الحدّ الفاصل بين الحرب والسلام بشكل رسميّ.

٢- صعوبة تحديد مصدرها وكلفته، إذ لا تعلن عنها الدولة المنفّذة غالبًا أو حتى الدولة المستهدفة، فتبقى مجهولة المصدر لأوقات طويلة، حيث إنّ تحديد مصدرها يحتاج إلى تتبع وعمل من فرق متخصّصة[13].

٣- يزول العامل الجغرافي في الحروب السيبرانية، بحيث يصبح أيّ مركز أو منشأة عُرضة للاستهداف، ولا يقتصر على الأرض بل يصل التهديد إلى الفضاء، عبر إرسال الفيروسات إلى الأقمار الصناعية لتعطيلها أو سرقة البيانات منها[14].

٤- الحروب السيبرانية أقلّ كلفة من الحروب التقليديّة، وهي عامل مساعد فاعل بها،وتُعدّ أكثر أنواع المواجهة التي تعبّر عن حروب الجيل الخامس، لأنّها تشمل عمليّة التحكم عن بعد وتقنيّات الاتصال الجديدة[15].

٥- إنّها تهديد وفرصة على نحو تبادليّ؛ فهي أداة للتجسّس، وسلاح للحرب، يستطيع الخصوم استخدامها لإلحاق الأذى بالخصم، ويستطيع الخصم أيضًا استخدامها لإلحاق الأذى بخصومه.

٦- مؤثرة في السياسة والاقتصاد على الصعيد الدوليّ، نتيجة انتقال جزء كبير من الصراعات بين القوى العظمى في العالم إلى شبكة الإنترنت والوسط الرقمي مع تزايد ارتباط العالم بالفضاء السيبراني، تزامناً مع تراجع دور الدولة في ظلّ العولمة وانسحابها من بعض القطاعات الاستراتيجية لمصلحة القطاع الخاصّ، وفي الوقت ذاته، تصاعدت أدوار الشركات متعدّدة الجنسيّات، خاصّة العاملة في مجال التكنولوجيا.

٧- تسبّب الحروب السيبرانية خسائر ماليّة ضخمة، وقد تُفضي إلى خسائر في الأرواح إذا تجاوزت قطاعات حسّاسة جداً، مثل أنظمة المستشفيات، وأنظمة التبريد في المفاعلات النوويّة.

٨- لا يسبقها أيّ مؤشرات، بمعنى أنّها من الممكن أن تحدث في أيّ وقت وفي أيّ مكان، وبتأثير سريع جداً.

ثانياً: دور الحروب السيبرانية في صياغة وتشكيل العلاقات الدولية: أدى اتساع علاقة الدول بالفضاء السيبراني، وما خلفته من حروب سيبرانية إلى جملة من المخاطر والتداعيات على تفاعلات السياسة الدولية، يمكن طرح أبرزها على النحو التالي[١٦]:

١- تصاعد المخاطر السيبرانية، خاصة مع قابلية المنشآت الحيوية (مدنية وعسكرية) في الدول للهجوم السيبراني عليها عبر وسيط وحامل للخدمات، أو شل عمل أنظمتها المعلوماتية، الأمر الذي يؤثر في وظائف تلك المنشآت، وبالتالي، فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة استراتيجية بالغة الأهمية، سواء في زمن السلم أو الحرب.

٢- تعزيز القوة وانتشارها، فمن جهة، عزز الفضاء السيبراني ما يسمي بـ "القوة المؤسسية" في السياسة الدولية، وهي تعني أن يكون لها دور في قوة الفاعلين، وتحقيق أهدافهم وقيمهم في ظل التنافس مع الآخرين، والإسهام في تشكل الفعل الاجتماعي في ظل المعرفة والمحددات المتاحة، والتي تؤثر في تشكيل السياسة العالمية.

٣- عمل الفضاء السيبراني على إعادة تشكيل قدرة الأطراف المؤثرة، مثل الولايات المتحدة، فبعدما كانت الأخيرة تملك ما يشبه الاحتكار لمصادر القوة، بعد انتهاء الحرب الباردة، برزت عملية انتشار القوة بين أطراف متعددة، سواء أكانت دولاً، أم من غير الدول.

٤- عسكرة الفضاء السيبراني، وذلك سعيا لدرء تهديداته على أمن الفضاء السيبراني، وبرز في هذا الإطار اتجاهات، مثل التطور في مجال سياسات الدفاع والأمن السيبراني، وتصاعد القدرات في سباق التسلح السيبراني، وتبني سياسات دفاعية سيبرانية لدي الأجهزة المعنية بالدفاع والأمن في الدول، وتزايد الاستثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة.[١٧]

٥- بناء الجيوش السيبرانية ورصد ميزانيات للتطوير في مجال الهجوم والدفاع والحماية، وتتصدر الولايات المتحدة الأمريكية المشهد في بناء الجيوش السيبرانية وكذلك الميزانية الضخمة التي تُخصصها له؛ حيث تنفق سنوياً نحو ٧ مليارات دولار على الأمن السيبراني وكذلك كوريا الشمالية، إذ تُخصص نحو ٢٠٪ من الميزانية العسكرية للأمن السيبراني.[١٨]

٦- إدماج الفضاء السيبراني ضمن الأمن القومي للدول، وذلك عبر تحديث الجيوش، وتدشين وحدات متخصصة في الحروب الإلكترونية، وإقامة هيئات وطنية للأمن والدفاع السيبراني، والقيام بالتدريب، وإجراء المناورات لتعزيز الدفاعات السيبرانية، والعمل على تعزيز التعاون الدولي في مجالات تأمين الفضاء السيبراني، والقيام بمشروعات وطنية للأمن السيبراني.

٧- الاستعداد لحروب المستقبل، حيث تتبني العديد من الدول استراتيجية حرب المعلومات باعتبارها حرباً للمستقبل، والتي يتم خوضها بهدف التشتيت، وإثارة الاضطرابات في عملية صناعة القرار لدي الخصوم، عبر اختراق أنظمتهم، واستخدام ونقل معلوماتهم، وهنا، ترى الدول الكبرى أن من يحدد مصير تلك المعركة المستقبلية ليس من يملك القوة فقط، وإنما القادر على شل القوة، والتشويش على المعلومة.[١٩]

٨- تحديث القدرات الدفاعية والهجومية، حيث سعت الدول إلى تحديث النشاط الدفاعي لمواجهة مخاطر الحرب السيبرانية، والاستثمار في البنية التحتية المعلوماتية، وتأمينها، وتحديث القدرات العسكرية، ورفع كفاءة الجاهزية لمثل هذه الحرب عن طريق التدريب، والمشاركة الدولية في حماية البنية المعلوماتية، والاستثمار في رفع القدرات البشرية داخل الأجهزة الوطنية المعنية، وهنا يتعلق التوجه الأخطر بنقل تلك القدرات من الدفاع إلى الهجوم عن طريق استخدام تلك الهجمات في إطار إدارة الصراع والتوتر مع دول أخرى.[٢٠]

٩- تطور شكل سباق التسلح التقليدي بين القوى الدولية المختلفة في إطار الردع وإدارة الصراع الدولي من سباق تسلح في مجال الأسلحة التقليدية أو النووية إلى سباق تسلح سيبراني.[٢١]

١٠- تشكيل هيئات وطنية للأمن السيبراني، حيث أن الحرب السيبرانية لا تُفرق بين مدني وعسكري وبالتالي هذه الهيئات تكون مهمتها رفع مستوى الوعي بالأمن السيبراني وإعداد الاستراتيجية الوطنية للأمن السيبراني والإرشادات المتعلقة به ووضع السياسات والمعايير الوطنية للتشفير، هذا بالإضافة لسن التشريعات الوطنية للأمن السيبراني مثل قانون مكافحة الجرائم السيبرانية.

١١- على المستوى الاقتصادي، قد تستهدف الهجمات السيبرانية توقف الإنترنت كلياً في الدولة المُستهدفة، مما يؤدي لتوقف المعاملات البنكية ومعاملات الحكومة الإلكترونية وسرقة أرقام وتفاصيل بطاقات الائتمان التي يتم التسوق بها عبر الإنترنت، مما ينتج عن ذلك تعطل تدفق الأموال في الدولة وبالتالي توقف أهم القطاعات في الدولة مثل الصناعة وغيرها من قطاعات الدولة.[٢٢]

١٢- على المستوى النفسي؛ قد تستهدف الهجمات السيبرانية إحداث حالة من الهلع في الدولة مثل اختراق المواقع الإلكترونية وإعلان حالة الطوارئ مما يثير القلق لدى المواطنين ويتسبب في إحداث حرب نفسية.

١٣- على المستوى الثقافي، قد تستهدف الحرب السيبرانية مسخ هوية الدولة من خلال الترويج لأفكار الدولة المُهاجمة بأساليب تستهدف شباب الدولة وتُأثر على أفكاره ومعتقداته وهذا ما يُعرف بالغزو الثقافي الذي يستهدف اختراق البنية الفكرية للمجتمعات من خلال اختراق العقول عبر زرع أفكار تُدمر الإبداع وتُعرقل التنمية الشاملة في الدولة، وهذا ما تستخدمه العديد من الفواعل غير الدولية مثل التنظيمات الإرهابية التي تستهدف الشباب وتجعله يتخذ مسلكاً وطريقاً ضد دولته وغمسه في الأفكار المُتطرفة، وكل هذا يتم عن طريق مواقع التواصل الاجتماعي والقنوات الفضائية[23].

١٤- على المستوى السياسي، قد تستهدف الحرب السيبرانية إثارة الفتن في الدولة وشحن الشعب ضد السلطة الحاكمة وخطابات بث الكراهية من خلال مُخاطبة الشعب بأن هناك العديد من المخاطر التي تُحيط بالدولة وأن السلطة الحاكمة لا توفر الاحتياجات الأساسية للشعب وكذلك مُطالبة شعب الدولة المُستهدفة بالحصول على حقوقه المنهوبة، مما يؤدي إلى خروج الشعب إلى مظاهرات وقد تتطور لثورات غير سلمية هدفها التخريب وتدمير الدولة المُستهدفة.[٢٤]وتبقي مشكلة دخول العالم سباق التسلح السيبراني A Cyber Arms Race في تحديد ماهية تلك الأسلحة التي يمتلكها الآخرون، حيث لا يملك المجتمع الدولي قدرة سريعة على التدخل لاحتوائها، ولا يوجد مجال لتفعيل التفتيش كآلية مراقبة، مثل حالة الأسلحة النووية، كما تنطوي عملية بناء القدرات العسكرية في مجال الحروب السيبرانية على عناصر أساسية، كالتالي[٢٥]:

١- السعي إلى امتلاك التكنولوجيا، وأنظمة الحماية، وتطوير قدرات هجومية تعمل على تحقيق التفوق التقني.

٢- تطوير القدرات الهجومية، إما عبر بناء القدرات الذاتية، أو بالاستعانة بالأفراد والشركات المتخصصة، وتطوير القدرة على اختبار مدي الجاهزية لمواجهة الهجمات السيبرانية.

٣- العمل على توفير الميزانيات المخصصة لتطوير القدرات الهجومية والدفاعية، وخاصة مع قلة تكلفتها، مقارنة بحجم ما ينفق على الجيوش التقليدية.وتتلخص متطلبات توافر الأمن السيبراني الدولي كالتالي[٢٦]:

١- التأكد من سلامة الدفاعات السيبرانية.

٢- عدم تعرض الدفاعات السيبرانية لأي خلل فني طارئ.

٣- ألا تعالج مسألة الدفاعات السيبرانية بشكل منفصل عن غيرها، وإنما ضمن ترسانة شاملة للدفاع تشكل إطارا رادعا لأي حرب استباقية.

المبحث الثاني دور استخدام كل من روسيا والولايات المتحدة للحروب السيبرانية في العلاقات الدولية لكل منهما

بالرغم من أنه من النادر الجزم بمصدر الهجمات السيبرانية، كما أن الدولة المهاجمة لا تعلن مطلقاً مسئوليتها عن الهجمات، إلا أنه وفي سياق الصراعات الدولية، تستطيع الدول حصر الاتهامات فيمن يتحمل مسئولية مهاجمتها، ونستعرض فيما يلي أبرز الهجمات السيبرانية الروسية والأمريكية، وكيف استخدمتها كلتا الدولتين في إطار إدارة صراعاتهما الدولية المختلفة، وذلك كالتالي:

أولاً: الحروب السيبرانية الروسية:تستخدم روسيا سلاح الحروب السيبرانية بكفاءة وبكثافة في صراعاتها الدولية المختلفة، حيث قامت بشن هجمات سيبرانية قوية على كل من (إستونيا، جورجيا، أوكرانيا) وغيرهم من الدول، وفي إطار التزامن مع دخول الحرب الروسية الأوكرانية عامها الثاني في عام ٢٠٢٣، ستركز الورقة البحثية على الحروب السيبرانية الروسية الأوكرانية، كونها أحد مُكوِّنَات المواجهة بين روسيا وأوكرانيا منذ انهيار الاتحاد السوفيتي في عام ١٩٩١، حيث بدأت روسيا في تطويرِ برمجيّاتها الخبيثة بالتزامن مع تقلد الرئيس الروسي فيلاديمير بوتين مقاليد السلطة في روسيا، وسُجِّلَت الهجمات الأولى على أنظمة المعلومات للمؤسسات الخاصة ومؤسسات الدولة في أوكرانيا خلال الاحتجاجات الجماهيرية في عام ٢٠١٣، فيما عُرف إعلاميًا باسمِ (عمليّة هرمجدون) وهي حملة روسية للتجسّس السيبراني المنهجي على أنظمة المعلومات للوكالات الحكوميّة ووكالات إنفاذ القانون ووكالات الدفاع الأوكرانيّة. [٢٧]كما تزامن استيلاء القوات الروسية على شبة جزيرة القرم مع هجمات سيبرانية روسية قوية تأثَّرت بها أنظمة المعلومات للوكالات الحكومية الأوكرانية بين عامي ٢٠١٣ و٢٠١٤ عن طريق فيروس

كمبيوتر عُرف بعددٍ من الأسماء بينها سنايك (Snake) ويوروبورس(Uroborus) ، إذ تعرَّضت مكاتب ومراكز الاتصالات الأوكرانيّة في الجزيرة للهجوم وتمَّ العبث بكابلات الألياف البصريّة، مما أدى إلى قطع الاتصال بين شبه الجزيرة والبر الرئيسي لأوكرانيا، كما أُغلقت مواقع الحكومة الأوكرانية ومواقع وقنوات وسائل الإعلام التابعة لها في الجزيرة كما عُطِّل الوصول لبعضِ مواقع التواصل الاجتماعي بعدما جرى استهدافها من خلالِ هجمات الحرمان من الخدمة، في حين تم اختراق أو التشويش على الهواتف المحمولة للعديد من البرلمانيين الأوكرانيين.[٢٨]وتعتبر عمليات القرصنة والتشويش التي زامنت احتلال روسيا للقرم البداية الحقيقية للحرب السيبرانيّة بين كييف وموسكو، حيث بدأت شركات الأمن السيبراني الأوكرانية في تسجيلِ زيادة في عدد الهجمات السيبرانية على أنظمة المعلومات في أوكرانيا، وسمَّى الباحثون الأمنيون الأوكرانيون مجموعَتين من المتسللين الروس الذين نشطوا في الحرب السيبرانيّة الروسية الأوكرانية، تُعرَف المجموعة الأولى باسمِAPT29 ، في حين تُعرَف المجموعة الثانيّة باسمِAPT28 .[29] ومنذ ذلك الحين، توالت الهجمات السيبرانية الروسية في إطار حرب سيبرانية شنتها روسيا على أوكرانيا كأحد أدوات فرض الإرادة الروسية على أوكرانيا على خلفية الخلافات السياسية بينهما، وذلك كالتالي[٣٠]:

١- عملية هرمجدون عام ٢٠١٣.

٢- عملية سنايك في فبراير عام ٢٠١٤.

٣- الهجمات على النظام الآلي الانتخابي الأوكراني في يونيو ٢٠١٤.

٤- اختراق شبكة الكهرباء في أوكرانيا في ديسمبر ٢٠١٥، وحدثت تلك الهجمات باستخدام فيروس حصان طروادة بلاك إنيرجي(BlackEnergy) على شركات الطاقة في أوكرانيا التي تُوفّر الطاقة لمناطق كييف وإيفانو فرانكيفسك وتشرنيفتسي، ويكتسب هذا الهجوم أهميته من كونه أول هجوم سيبراني ناجح على شبكة الكهرباء الأوكرانية.

٥- الاختراق الثاني لشبكة الكهرباء في أوكرانيا في ديسمبر ٢٠١٦.

٦- الهجمات السيبرانيّة على مواقع حكوميّة في أوكرانيا في ديسمبر ٢٠١٦.

٧- هجمات روسية سيبرانية قويّة استهدفت عشرات المواقع الإلكترونيّة في أوكرانيا، تلاها هجوم آخر مرتبطٌ بها في يونيو ٢٠١٧ باستخدامِ فيروس بيتيا.

٨- استهداف مواقع الحكومة الأوكرانية في يناير ٢٠٢٢ وذلك بعد يوم واحد من فشل المفاوضات الأمريكية الروسية بشأن مستقبل أوكرانيا في الناتو.

٩- أدَّت الهجمات السيبرانيّة الروسية في فبراير ٢٠٢٢، بعد بدء الغزو الروسي لأوكرانيا إلى إسقاطِ العديد من المواقع الحكومية والمصرفية الأوكرانية الرئيسية، وبدأت الهجمات السيبرانية قبل ساعات من هجوم موسكو على أوكرانيا في ٢٣ فبراير ٢٠٢٢، إذ استخدمت برنامج FoxBladeعشية الغزو الروسي، وتمكنت موسكو بموجب هذا الهجوم من محو البيانات الموجودة على الشبكات الحكومية الأوكرانية بالكامل والسيطرة على البيانات الموجودة في كافة الشبكات[31].وفي المقابل، شنت أوكرانيا العديد من الهجمات السيبرانية الأوكرانية على روسيا في إطار الرد على الهجمات السيبرانية الروسية القوية على أوكرانيا، وذلك كالتالي:

١- هجوم التاسع من مايو ٢٠١٦، وهو هجومٌ ناجحٌ اخترقت فيهِ مجموعات سيبرانيّة أوكرانيّة عددًا من مواقع الجماعات الانفصاليّة فيما يُعرف باسمِ جمهورية دونيتسك الشعبية، وكذلك مواقع روسية للدعاية المناهضة لأوكرانيا وموارد شركات عسكرية روسية خاصّة.

٢- الاختراق الأوكراني للقناة الأولى في التليفزيون الروسي في يونيو ٢٠١٦، حيثُ نجحت مجموعات قرصنة أوكرانيّة هم (Falcon Flame)، و (Trinity)، و(Rukh8) في اختراق خادم الشركة الخاص بالقناة الأولى الروسيّة.

٣- تسريبات سوركوف (The Surkov Leaks) التي تم الإعلان عنها في أكتوبر ٢٠١٦ حينما سرَّبت مجموعة قرصنة أوكرانيّة ما مجموعهُ ٢٣٣٧ رسالة بريدٍ إلكتروني ومئات المرفقات الروسيّة، والتي تكشفُ عن خطط للاستيلاءِ على شبه جزيرة القرم بالكامل من أوكرانيا وإثارة الاضطرابات الانفصالية في دونباس (التسريبات تمت عام ٢٠١٦ لكنَّ تاريخ الوثائق يعود للفترة ما بين سبتمبر ٢٠١٣ وديسمبر ٢٠١٤).[٣٢]

٤- إنشاء الجيش السيبراني الأوكراني على يدِ ميخايلو فيدروف، النائب الأول لرئيس الوزراء الأوكراني ووزير التحوّل الرقمي، في ٢٥ فبراير ٢٠٢٢ وذلك تزامنًا مع الغزو الروسي لأوكرانيا،الهدف الأساسي لهذا الجيش السيبراني بحسبِ فيدروف هو المساهمة وبقوّة في الحرب السيبرانية

ضد روسيا، حيث طلب فيدوروف المساعدة من خبراء التقنيّة من مختلف بقاعِ العالم، ونشرَ على حسابٍ رسمي في تليجرام قائمةً ضمَّت ٣١ موقعًا إلكترونيًا لمنظمات الأعمال والدولة الروسية من أجلِ استهدافها.

ثانياً: الحروب السيبرانية الأمريكية:تستخدم الولايات المتحدة الأمريكية الحروب السيبرانية منذ عهد الرئيس الأمريكي الراحل رونالد ريجان، الذي كان أول من أنشأ وحدات أمريكية متخصصة في العمليات السيبرانية، وشنت الولايات المتحدة الأمريكية منذ ذلك الحين الملايين من الهجمات السيبرانية ضد خصوم الولايات المتحدة في النزاعات الدولية المختلفة، وشملت قائمة ضحايا الحروب السيبرانية الأمريكية كل من (كوريا الشمالية، العراق، روسيا، الصين، إيران) وغيرها من الدول، وستقوم الورقة البحثية بالتركيز على الحرب السيبرانية التي شنتها الولايات المتحدة على إيران، وذلك في إطار إدارة الولايات المتحدة للصراع الدولي مع إيران.[٣٣]قامت الولايات المتحدة بالعديد من الهجمات السيبرانية ذات الأهداف المختلفة على إيران،وسنلقى الضوء على الهجمات السيبرانية الأمريكية التي استخدمتها الولايات المتحدة ضمن الاستراتيجية الأمريكية لفرض الإرادة وإدارة الصراع الدولي فيما يخص الملف النووي الإيراني، ففي إطار المحاولات الأمريكية لمنع إيران من امتلاك سلاح نووي، وبالإضافة للعقوبات الاقتصادية والتوترات الدبلوماسية بين الطرفين، استخدمت الولايات المتحدة الحروب السيبرانية ضد إيران من خلال شن العديد من الهجمات السيبرانية بهدف تدمير البنية التكنولوجية للمفاعلات النووية الإيرانية ومنع إيران من امتلاك السلاح النووي[٣٤]، وكذلك إجبار إيران على القبول بالشروط الأمريكية للتفاوض حول البرنامج النووي الإيراني، وذلك كالتالي:

١- عام ٢٠٠٦، استهداف منشأة نطنز النووية الإيرانية من خلال هجمات سيبرانية سميت باسم (Flame)، قامت بالتأثير على أنشطة تخصيب اليورانيوم وتدمير أجهزة الطرد المركزي وذلك عن طريق السيطرة على الدوائر الإلكترونية الخاصة بها وزيادة سرعتها للحد الذي أدى لتدميرها.

٢- عام ٢٠١٠، استهداف منشأة نطنز النووية الإيرانية للمرة الثانية عن طريق هجمات (Stuxnet) السيبرانية والتي استهدفت أجهزة تخصيب اليورانيوم، وكانت نتيجة الهجمات أن أغلقت إيران البرنامج النووي الإيراني بشكل مؤقت وذلك بعد تعطيل أكثر من ٣٠ ألف جهاز كمبيوتر داخل المنشأة وخارجها مرتبطة بالبرنامج النووي الإيراني، هذا بالإضافة إلى تدمير ١٠٠ جهاز طرد مركزي.[٣٥]

٣- في فبراير ٢٠١٢، استهداف المفاعل النووي الإيراني في بوشهر وتعطيل ١٦ ألف جهاز كمبيوتر داخل المفاعل وخارجه مرتبطة بالبرنامج النووي الإيراني، هذا بالإضافة إلى سرقة آلاف الملفات ورسائل البريد الإلكتروني بالغة السرية.

٤- في ديسمبر ٢٠١٢، الاستهداف الثاني لمفاعل بوشهر النووي في هجمات سيبرانية عرفت باسم (Flamer) وسرقة آلاف الملفات والمعلومات السرية والمرتبطة بالبرنامج النووي الإيراني، بالإضافة إلى تدمير ١٢٠ جهاز طرد مركزي.[٣٦]وفي المقابل، أصبحت ايران ذات هجمات سيبرانية فعالة خاصة بعد الهجوم السيبراني عليها من قبل الولايات المتحدة بفيروس stuxnet في عام ٢٠١٠ اذ تحسنت تلك القدرات السيبرانية بشكل مطرد واعتبرت إيران قوة سيبرانية من الدرجة الثالثة كونها قادرة على شن هجمات أكثر تعقيداً وتدميراً خاصة ضد الولايات المتحدة الامريكية، وفي الاستراتيجية الأمنية الإيرانية تعمل القدرات السيبرانية كركيزة فعالة خاصة بما تسمى(عقدة الردع) اذ تهدف القدرات السيبرانية الإيرانية إلى معاقبة السلوك غير المرغوب فيه للخصوم وردع الجهات التي تنوي القيام بتلك الهجمات، وقد زادت ايران من مخصصات الميزانية للأنشطة السيبرانية بحوالي ١٢ ضعفاً للفترة (٢٠١٣ – ٢٠٢١) بنسبة ١٢٠٠٪ من أجل الارتقاء بالقدرات السيبرانية وتعزيزها، بما يمنح إيران الجاهزية الكاملة لتعطيل الخدمة ضد آلاف الشبكات الكهربائية ومحطات المياه وشركات الرعاية الصحية والتكنولوجية وخطوط الغاز والبترول في الولايات المتحدة الامريكية واختراق البريد الالكتروني والاتصالات ايضاً، لذا شنت إيران العديد من الهجمات السيبرانية على الولايات المتحدة الأمريكية، وذلك كالتالي[٣٧]:

١-في عام ٢٠١٢، شنت إيران هجمات سيبرانية استهدفت المؤسسات المالية والبنوك الرئيسية في الولايات المتحدة مثل (JP Morgan، Bank of America، Wells Fargo) من خلال مهاجمة شبكات مراكز المعلومات الرئيسية مما أدى إلى انهيار وتدمير المواقع الإلكترونية لتلك المؤسسات والبنوك مما عطل الخدمات المصرفية وتحقيق خسائر مالية تقدر بـ ٢ مليار دولار.

٢-في عام ٢٠١٢، هاجمت إيران الشبكة الداخلية لسلاح مشاة البحرية الأمريكية (المارينز)، مما أدى إلى سرقة آلاف الملفات بالغة السرية وأجبر الولايات المتحدة على تغيير الشبكة بأكملها.

٣-في عام ٢٠١٣، شنت إيران هجمات سيبرانية استهدفت السيطرة على شبكات الكهرباء وخطوط الغاز والبترول الأمريكية، مما أسفر عن تعطيل تلك الخدمات لمدة ٩ ساعات قبل أن تتمكن الولايات المتحدة من إعادة تشغيلها مرة أخرى، وحققت الهجمات خسائر مالية تقدر بـ ٤ مليار دولار.

٤-في عام ٢٠١٤، استخدمت إيران نوعاً من البرمجيات الخبيثة (Wiper Malware) ضد شبكات الخدمات العامة في لاس فيجاس، وحققت الهجمات خسائر تقدر بـ ١٤ مليار دولار.

٥-في عام ٢٠١٥، أطلقت إيران عدداً من الهجمات السيبرانية ضد عدد ٤٦ بنكاً ووكالة حكومية ومؤسسة مالية أمريكية، محققة خسائر وصلت لـ ٨ مليار دولار.

٦-في فبراير ٢٠١٨، شنت إيران سلسلة متتالية من الهجمات السيبرانية على الولايات المتحدة استهدفت ١٤٤ جامعة أمريكية، ومنظمتين غير حكوميتين، و٥ وكالات فيدرالية، و١١ شركة أجنبية خاصة، وأسفرت الهجمات عن سرقة الآلاف من الأبحاث العلمية، والمعلومات السرية التي تخص الأمن الداخلي للولايات المتحدة.

٧-في أكتوبر ٢٠١٩، قامت إيران بهجمات سيبرانية تستهدف الحسابات المتعلقة بحملة إعادة انتخاب الرئيس الأمريكي (دونالد ترامب) بهدف التأثير على فرص إعادة انتخاب ترامب لولاية جديدة.

٨-في نوفمبر ٢٠٢٠، أطلقت إيران حملة هجمات سيبرانية الهدف منها التأثير على الناخبين الأمريكيين بغرض تقويض احتمالات إعادة انتخاب دونالد ترامب.

ثالثاً: رؤية تحليلية: صاغت كل من الولايات المتحدة الأمريكية وروسيا استراتيجية متكاملة لعلاقاتهما الدولية وأسلوب إدارتهما للصراعات الدولية المختلفة، وكانت الحروب السيبرانية دائماً ما تحتل ركناً رئيسياً في تلك الاستراتيجية، وفي إطار الصراع (الروسي/ الأوكراني) و (الأمريكي/ الإيراني) كانت الحرب السيبرانية حاضرة وبقوة في المشهد السياسي والاستراتيجي، وذلك كالتالي:

١- استخدمت روسيا الحرب السيبرانية على مدار الصراع الروسي الأوكراني منذ عام ٢٠١٣ وحتي الغزو الروسي لأوكرانيا عام ٢٠٢٢، حيث تدرك روسيا أن الصراع الروسي مع الغرب بقيادة الولايات المتحدة هو الصراع الحقيقي، وأن أوكرانيا ما هي إلا واجهه لهذا الصراع، لذا كانت الحرب السيبرانية هي الوسيلة المثلى التي تحقق الأهداف الاستراتيجية الروسية دون الانزلاق في مواجهة عسكرية مباشرة أو صدام سياسي مع الغرب، واستمر ذلك حتي تطورت الأوضاع السياسية بالشكل الذي أجبر روسيا على تطوير استراتيجية إدارة الصراع من الحروب غير المباشرة (الحروب السيبرانية) إلى مواجهة سياسية وعسكرية مباشرة.

٢- على المستوى التكتيكي، استخدمت روسيا الحروب السيبرانية لشل وإرباك مراكز القيادة والسيطرة ومراكز العمليات الأوكرانية، وذلك بهدف تمهيد الجبهة عشية الغزو الروسي لأوكرانيا في فبراير ٢٠٢٢، مما منح القوات الروسية الأريحية التكتيكية أثناء عبور الحدود الروسية الأوكرانية والتوغل في المناطق الشرقية لأوكرانيا.

٣- على المستوى السياسي والدبلوماسي، شنت روسيا العديد من الحروب السيبرانية بالتزامن مع الانتخابات الرئاسية في أوكرانيا بغرض توجيه الناخبين الأوكرانيين لانتخاب المرشح الرئاسي الذي تفضله روسيا ويخدم مصالحها في أوكرانيا، وهو ما نجحت روسيا فيه بالفعل بنجاح المرشح الرئاسي المدعوم من روسيا فيكتور يانكوفيتش برئاسة أوكرانيا عام ٢٠١٠.

٤- ومن جهة أخرى، كانت الحرب السيبرانية هي أنسب البدائل المتاحة أمام متخذ القرار الأوكراني خلال مراحل إدارة الصراع الروسي/ الأوكراني، فعسكرياً، فإن مقارنة القوات والقدرات العسكرية الروسية والأوكرانية ليست في صالح أوكرانيا، لذا فإن قرار المواجهة العسكرية المباشرة مع روسيا لم يكن من الخيارات المطروحة للتنفيذ، وشكلت الحرب السيبرانية الاختيار الأكثر واقعية.

٥- على المستوى الاقتصادي، شكلت الحرب السيبرانية الاختيار الأفضل بالنسبة لأوكرانيا في مواجهة روسيا نظراً لانخفاض تكلفتها بالمقارنة مع تكلفة المواجهة العسكرية المباشرة، وهو ما يتناسب مع القدرات الاقتصادية الأوكرانية في مواجهة روسيا.

٦- على المستوى السياسي، كان للوزن السياسي والاستراتيجي الكبير لروسيا دوراً حاسماً في رغبة أوكرانيا في عدم الدخول في صدامات سياسية مباشرة مع دولة كبرى بحجم روسيا، وأن أي مواجهة سياسية مع روسيا لن تكون في صالح أوكرانيا، لذا كانت الحروب السيبرانية هي الاختيار الأفضل من وجهة النظر السياسية في أوكرانيا.

٧- أما الولايات المتحدة الأمريكية، فكانت منغمسة تماماً في العراق وأفغانستان عام ٢٠٠٦، ولم تكن مستعدة عسكرياً أو اقتصادياً للدخول في مواجهات عسكرية جديدة، بالإضافة إلى أن المشاعر العدائية حول العالم لكل ما هو أمريكي نتيجة الغطرسة الأمريكية في التعامل ما بعد أحداث ١١ سبتمبر وما تبعها من الغزو الأمريكي لكل من العراق وأفغانستان، لذا كانت الحرب السيبرانية هي البديل الأفضل من

وجهة نظر الإدارة الأمريكية في ذلك الوقت للتعامل مع الملف النووي الإيراني، كبديل منخفض التكلفة وغير معلن ولا يقود لمواجهات سياسية أو عسكرية مباشرة.

٨- وبالنسبة لإيران، مثلت الحروب السيبرانية اختياراً مثالياً للنظام الإيراني، لأنها نموذج للحرب غير المتكافئة، فهي شبيهه لحد كبير بحرب العصابات والعمليات الإرهابية، لذا فهي حرب مثالية للنظام الإيراني لأنه يستخدمها كأداة فعالة للهجوم على خصمة دون اللجوء إلى مواجهة عسكرية مباشرة، وذلك في ظل التفاوت الكبير في القدرات العسكرية بينها وبين الولايات المتحدة والذي لن يكون في صالح إيران على أي حال في حالة اندلاع صدام مسلح بين الطرفين.

٩- وعلى المستوى الاقتصادي، وكما هو الحال بالنسبة لأوكرانيا، فإن القدرات الاقتصادية الإيرانية يناسبها أسلوب الحروب السيبرانية نظراً لانخفاض تكلفتها، بالإضافة إلى العقوبات الاقتصادية الأمريكية الكبيرة على الاقتصاد الإيراني والتي تجعل إيران من الناحية الاقتصادية ليست في أفضل حالاتها.

١٠- وعلى المستوى السياسي، يعاني النظام الإيراني من عزلة سياسية كبيرة فرضتها عليه العقوبات الأمريكية بالإضافة للسياسيات الإيرانية المختلفة، لذا فإن إيران بمنأى عن مزيد من العزلة السياسية في حالة الدخول في صدام معلن مع الولايات المتحدة الأمريكية، لذا كانت الحروب السيبرانية هو الاختيار الأفضل في هذا الإطار، وذلك في ظل تميز الهجمات السيبرانية بصعوبة تحديد مصدرها.

خاتمة:

أبرز استخدام كل من روسيا والولايات المتحدة الأمريكية للحروب السيبرانية ضمن استراتيجية متكاملة لإدارة الصراعات الدولية التي يخوضها كل منهما الأهمية المتزايدة لمفهوم الحروب السيبرانية ودورها المتعاظم في التأثير على العلاقات الدولية لكل من الدولتين، وكذلك مشاركتها الأساسية في صياغة وتشكيل العلاقات الدولية كأحد أهم الأدوات الحديثة لإدارة الصراع الدولي وفرض الإرادة في الصراعات الدولية.فمع نهاية القرن العشرين وبداية القرن الحادي والعشرين أصبحت الحروب السيبرانية ركناً أساسياً في إدارة الصراعات الدولية مما فرض على معظم دول العالم اتخاذ تدابير وإجراءات تعزز الأمن السيبراني وتنمي قدراتها السيبرانية وتعمل على تقوية وتدعيم دفاعاتها السيبرانية، بالإضافة إلى التعديلات الدستورية والتشريعية التي تتيح مظلة قانونية للعمل السيبراني، فضلاً عن تخصيص نسب مضطردة من ميزانيات الدفاع لإنشاء وتطوير وتدعيم وحدات قتالية سيبرانية متخصصة، مستغلة في ذلك التكلفة المنخفضة للحروب السيبرانية بالمقارنة بالحروب التقليدية، وكذلك الميزة الأبرز والتي تتمثل في أنها حرب عابرة للحدود والقوميات دون الحاجة لتحريك قوات عسكرية نظامية على الأرض، وكذلك عدم المسئولية الدولية نظراً إلى أنه يصعب تحديد مرتكب الهجمات السيبرانية بدقة.وفي سياق الصراع الدولي بين كل من (روسيا وأوكرانيا)، (الولايات المتحدة وإيران) استخدمت الدول الأربعة الحروب السيبرانية كوسيلة استراتيجية لتحقيق أهدافهم السياسية، ظهر ذلك على مدار سنوات امتدت من عام ٢٠١٣ إلى عام ٢٠٢٢ في الصراع الروسي الأوكراني، وكذلك على مدار سنوات امتدت من عام ٢٠٠٦ إلى عام ٢٠٢٢ في إطار الصراع الأمريكي الإيراني على خلفية الملف النووي الإيراني، وأظهرت الحروب السيبرانية (الروسية/ الأوكرانية)، (الأمريكية/ الإيرانية) مدى تأثير الحروب السيبرانية في العلاقات الدولية بشكل كبير، وذلك بالدرجة التي أضحى فيها البعد السيبراني بعداً لا يمكن إغفاله أو تجاوزه في إدارة أي دولة لعلاقاتها الدولية في إطار استراتيجيات إدارة الصراع الدولي.

قائمة المصادر

أولاً: المراجع باللغة العربية:

أ- الكتب:

١- إيهاب خليفة، الحرب السيبرانية: الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، مركز المستقبل للأبحاث والدراسات المتقدمة، القاهرة، ٢٠٢٠.

٢- مرعي علي، الحرب السيبرانية ومتطلبات الأمن القومي الجديدة، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، ٢٠٢٢.

٣- محمد القحطاني، قدرات القرصنة السيبرانية الإيرانية، مركز الملك فيصل للبحوث والدراسات الإسلامية، الرياض، ٢٠٢٠.

٤-نبيل عودة، العمليات السيبرانية في الحرب الروسية الأوكرانية: طبيعتها وأنماطها، مركز الشرق للأبحاث الاستراتيجية، إسطنبول، سبتمبر ٢٠٢٢.

ب- الرسائل العلمية:

١- حارك فاتح، الفضاء السيبراني والتحول في شكل الحروب: دراسة حالة روسيا، رسالة ماجستير، كلية العلوم السياسية، جامعة القسطنطينية، الجزائر، ٢٠٢٢.

ج- الدوريات:

١- أحمد الميموني، الجبهة النشطة: تداعيات المواجهة السيبرانية بين إيران وإسرائيل، مجلة الدراسات الإيرانية، السنة الرابعة، العدد ١٢، المعهد الدولي للدراسات الإيرانية، الرياض، أكتوبر ٢٠٢٠.

٢- إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، المجلد ١٠، العدد الأول، جامعة محمد بوضياف، الجزائر، ٢٠١٨.

٣- أماني عصام محمد، استخدام روسيا للقوة السيبرانية في إدارة تفاعلاتها الدولية، مجلة كلية الاقتصاد والعلوم السياسية، المجلد ٢٢، العدد ٤، جامعة القاهرة، أكتوبر ٢٠٢٢.

٢-إيهاب خليفة، الحالة السيبرانية في نظريات العلاقات الدولية: الحاجة إلى مراجعة جديدة، بقلم خبير، العدد ٢٣، مركز المعلومات ودعم اتخاذ القرار، القاهرة، ديسمبر ٢٠٢١.

٥-حازم محمد خليل، استغلال الفضاء السيبراني في الحروب غير التقليدية: دراسة في الوكالة السيبرانية والإرهاب السيبراني، مجلة كلية الدراسات الاقتصادية والعلوم السياسية، المجلد الثامن، العدد ١٥، جامعة الإسكندرية، يناير ٢٠٢٣.

٦-دلالي جيلالي، رهانات الأمن السيبراني الوطني في ظل التحول الرقمي: قراءة في التأصيل المعرفي واستراتيجية المواجهة التشريعية، مجلة كلية القانون الكويتية العالمية، السنة العاشرة، العدد الأول، الكويت، ديسمبر ٢٠٢١.

٧-سهيلة هادي، الحروب الإلكترونية في ظل عصر المعلومات، رؤى استراتيجية، المجلد الرابع، العدد ١٤، مركز الإمارات للدراسات والبحوث الاستراتيجية، يونيو ٢٠١٧.

٨-لبنى خميس، أثر السيبرانية في تطور القوة، مجلة حمورابي، العدد ٣٣، كلية العلوم السياسية، جامعة النهرين، بغداد، ٢٠٢٠.

٩-محمد ماجد، الأبعاد التنموية والاستراتيجية للأمن السيبراني ودوره في دعم الاقتصادات الرقمية والمشفرة، سلسلة قضايا التخطيط والتنمية، العدد ٣٢٦، معهد التخطيط القومي، القاهرة، أغسطس ٢٠٢١.

١٠- هبه جمال الدين، الأمن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد والعلوم السياسية، المجلد ٢٤، العدد الأول، جامعة القاهرة، يناير ٢٠٢٣.

ثانياً: المراجع الأجنبية:

B- Books:

1- Andreas Wenger, Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation, Center for Security Studies, Swiss Federal Institute of Technology, Zurich, 2022.

2- Barry Buzan, The Evolution of International Security Studies, Cambridge University Press, New York, 2009.

3- Benedikt Muller, Cyberspace and International Relations: Theory, Prospect and Challenges, Springer, Berlin, 2014.

4- David Clark, At The Nexus of Cyber Security and Public Policy, The National Academies Press, Washington DC, 2014.

5- Kenneth Geers, Cyber War in Perspective: Russian Aggression Against Ukraine, NATO Publications, Tallinn, Estonia, 2015.

6- Lukman Adewale, Cyber Theater a Fifth Domain of International Politics: Africa and The Rest of the World in The Cyberspace, National Institute for Policy and Strategic Studies, Nigeria, 2020.

7- Marie Baezner, Cyber and Information Warfare in The Ukrainian Conflict, Center for Security Studies, Zurich, October 2018.

8- Marco De Falco, Stuxnet Facts Report: A Technical and Strategic Analysis, NATO Publications, Tallinn, Estonia, 2012.
9- Matthias Schulze, Cyber Escalation: The Conflict Dyad USA/ Iran as a Test Case, German Institute for International and Security Affairs Publications, Berlin, December 2020.
10- Simona Tarpova, Russia's War on Ukraine: Timeline of Cyber-Attacks, European Parliament Research Service, European Parliament, Brussel, June 2022.

C- Periodicals:

1- Adam Segal, Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet, Vol.80, Council on Foreign Relations, Washington DC, 2022.
2- Alexander Gamero, Cyber Conflicts in International Relations: Framework and Case Studies, Explorations in Cyber International Relations, Vol. 73, Massachusetts Institute of Technology, Harvard University, 2022.
3- David Graham, Cyber Threats and The Law of War, Journal of National Security Law and Policy, Vol.87, Center on National Security, Georgetown University, Washington DC, 2019.
4- Kathleen Curlee, Cyber Warfare: A Weapon of Mass Destruction, Journal of International Relations, Vol. 23, Sigma Iota Rho National Honor Society for International Studies, Philadelphia, USA, April 2021.
5- Rika Isnarti, A Comparison of Neorealism, Liberalism, and Constructivism in Analyzing Cyber War, Andalas Journal of International Studies, Vol.5, Andalas University, Indonesia, November, 2016.
6- Samantha Bradshaw, Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity, Global Commission on Internet Governance, Vol. 23, Chatham House, December 2015.
7- Sharon Cardash, Cyber Domain Conflict in the 21st Century, The Whitehead Journal of Diplomacy and International Relations, Vol.82, Seton Hall University, New Jersey, USA, 2021.
8- William Banks, Cyber Attribution and State Responsibility, International Law Studies, Vol.97, Stockton Center for International Law, Naval War College, Rhode Island, USA, 2021.

D- Thesis and dissertations:

1- David Edelman, Cyber Attacks in International Relations, PhD Thesis, The University of Oxford, 2013.
2- Friday Ikechukwu Eze, Cyber as an Instrument of Foreign Policy, Master's Thesis, University of Manitoba, Canada, 2019.
3- Marcelo Gomes, Cyber Security: A Case Study of Brazil, Master's Thesis, National Defense College, Pakistan,2019.
4- T. Ivanjko, International Cyber Security Challenges, Master Thesis, Faculty of Humanities and Social Sciences, University of Applied Sciences, Zagreb, Croatia, 2017.

---

[1] T. Ivanjko, International Cyber Security Challenges, Master Thesis, Faculty of Humanities and Social Sciences, University of Applied Sciences, Zagreb, Croatia, 2017, pp. 12-19.

[2] إيهاب خليفة، الحالة السـيبرانية في نظريات العلاقات الدولية: الحاجة إلى مراجعة جديدة، بقلم خبير، العدد ٢٣، مركز المعلومات ودعم اتخاذ القرار، القاهرة، ديسمبر ٢٠٢١، ص ٤-١٣.

[3] Rika Isnarti, A Comparison of Neorealism, Liberalism, and Constructivism in Analyzing Cyber War, Andalas Journal of International Studies, Vol.5, Andalas University, Indonesia, November, 2016, pp. 13-24.

[4] إسـماعيل زروقة، الفضـاء السـيبراني والتحول في مفاهيم القوة والصـراع، مجلة العلوم القانونية والسـياسـية، المجلد ١٠، العدد الأول، جامعة محمد بوضياف، الجزائر، ٢٠١٨، ص١٠٦-١١٣.

[5] David Clark, At The Nexus of Cyber Security and Public Policy, The National Academies Press, Washington DC, 2014, pp. 54-67.

[6] Barry Buzan, The Evolution of International Security Studies, Cambridge University Press, New York, 2009,
pp. 121-134.

[7] Samantha Bradshaw, Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity, Global Commission on Internet Governance, Vol. 23, Chatham House, December 2015, pp. 13-21.

[٨] لبنى خميس، أثر السيبرانية في تطور القوة، مجلة حمورابي، العدد ٣٣، كلية العلوم السياسية، جامعة النهرين، بغداد، ٢٠٢٠، ص ١٤٥- ١٥٢.

[٩] هبه جمال الدين، الأمن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد والعلوم السياسية، المجلد ٢٤، العدد الأول، جامعة القاهرة، يناير ٢٠٢٣، ص ١٩٠ – ٢٠١.

[10] Adam Segal, Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet, Vol.80, Council on Foreign Relations, Washington DC, 2022, pp.98-112.

[11] Friday Ikechukwu Eze, Cyber as an Instrument of Foreign Policy, Master's Thesis, University of Manitoba,
Canada, 2019, pp. 84-91.

[12] William Banks, Cyber Attribution and State Responsibility, International Law Studies, Vol.97, Stockton Center for International Law, Naval War College, Rhode Island, USA, 2021, pp. 15-21.

[13] حازم محمد خليل، استغلال الفضاء السيبراني في الحروب غير التقليدية: دراسة في الوكالة السيبرانية والإرهاب السيبراني، مجلة كلية الدراسات الاقتصادية والعلوم السياسية، المجلد الثامن، العدد ١٥، جامعة الإسكندرية، يناير ٢٠٢٣، ص ٢٣-٥٤.

[14] مرعي علي، الحرب السيبرانية ومتطلبات الأمن القومي الجديدة، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، ٢٠٢٢، ص ٣٢-٥٥.

[15] سهيلة هادي، الحروب الإلكترونية في ظل عصر المعلومات، رؤى استراتيجية، المجلد الرابع، العدد ١٤، مركز الإمارات للدراسات والبحوث الاستراتيجية، يونيو ٢٠١٧، ص ١٢-١٩.

[16] Alexander Gamero, Cyber Conflicts in International Relations: Framework and Case Studies, Explorations in Cyber International Relations, Vol. 73, Massachusetts Institute of Technology, Harvard University, 2022, pp. 73-89.

[17] Sharon Cardash, Cyber Domain Conflict in the 21st Century, The Whitehead Journal of Diplomacy and International Relations, Vol.82, Seton Hall University, New Jersey, USA, 2021, pp. 42-61.

[18] Andreas Wenger, Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation, Center for Security Studies, Swiss Federal Institute of Technology, Zurich, 2022, pp. 211-267.

[19] Marcelo Gomes, Cyber Security: A Case Study of Brazil, Master's Thesis, National Defense College, Pakistan, 2019, pp. 43-62.

[20] إيهاب خليفة، الحرب السيبرانية: الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، مركز المستقبل للأبحاث والدراسات المتقدمة، القاهرة، ٢٠٢٠، ص ٤٦-٧٨.

[21] Benedikt Muller, Cyberspace and International Relations: Theory, Prospect and Challenges, Springer, Berlin, 2014, pp. 33-67.

[٢٢] محمد ماجد، الأبعاد التنموية والاستراتيجية للأمن السيبراني ودوره في دعم الاقتصادات الرقمية والمشفرة، سلسلة قضايا التخطيط والتنمية، العدد ٣٢٦، معهد التخطيط القومي، القاهرة، أغسطس ٢٠٢١، ص ١٥٤- ١٦٧.

[23] Lukman Adewale, Cyber Theater a Fifth Domain of International Politics: Africa and The Rest of The World in The Cyberspace, National Institute for Policy and Strategic Studies, Nigeria, 2020, pp. 23-45.

[24] David Graham, Cyber Threats and The Law of War, Journal of National Security Law and Policy, Vol.87, Center on National Security, Georgetown University, Washington DC, 2019, pp.43-56.

[25] Kathleen Curlee, Cyber Warfare: A Weapon of Mass Destruction, Journal of International Relations, Vol. 23, Sigma Iota Rho National Honor Society for International Studies, Philadelphia, USA, April 2021, pp. 56-78.

[٢٦] دلالي جيلالي، رهانات الأمن السيبراني الوطني في ظل التحول الرقمي: قراءة في التأصيل المعرفي واستراتيجية المواجهة التشريعية، مجلة كلية القانون الكويتية العالمية، السنة العاشرة، العدد الأول، الكويت، ديسمبر ٢٠٢١، ص ١٨-٣٢.

[٢٧] أماني عصام محمد، استخدام روسيا للقوة السيبرانية في إدارة تفاعلاتها الدولية، مجلة كلية الاقتصاد والعلوم السياسية، المجلد ٢٢، العدد ٤، جامعة القاهرة، أكتوبر ٢٠٢٢، ص ١٦٨- ١٨٠.

[28] Marie Baezner, Cyber and Information Warfare in The Ukrainian Conflict, Center for Security Studies, Zurich, October 2018, pp. 34-52.

[29] Kenneth Geers, Cyber War in Perspective: Russian Aggression Against Ukraine, NATO Publications, Tallinn,
Estonia, 2015, pp. 67- 88.

[30] Simona Tarpova, Russia's War on Ukraine: Timeline of Cyber-Attacks, European Parliament Research Service, European Parliament, Brussel, June 2022, pp. 3-8.

[31] حارك فاتح، الفضاء السيبراني والتحول في شكل الحروب: دراسة حالة روسيا، رسالة ماجستير، كلية العلوم السياسية، جامعة القسطنطينية، الجزائر، ٢٠٢٢، ص ٧٨- ٩٩.

[٣٢] نبيل عودة، العمليات السيبرانية في الحرب الروسية الأوكرانية: طبيعتها وأنماطها، مركز الشرق للأبحاث الاستراتيجية، إسطنبول، سبتمبر ٢٠٢٢، ص ١٨-٣١.

[33] Matthias Schulze, Cyber Escalation: The Conflict Dyad USA/ Iran as a Test Case, German Institute for International and Security Affairs Publications, Berlin, December 2020, pp. 48-66.

[34] David Edelman, Cyber Attacks in International Relations, PhD Thesis, The University of Oxford, 2013, pp. 201-255.

[35] Marco De Falco, Stuxnet Facts Report: a Technical and Strategic Analysis, NATO Publications, Tallinn, Estonia, 2012, pp. 51-69.

[٣٦] أحمد الميموني، الجبهة النشطة: تداعيات المواجهة السيبرانية بين إيران وإسرائيل، مجلة الدراسات الإيرانية، السنة الرابعة، العدد ١٢، المعهد الدولي للدراسات الإيرانية، الرياض، أكتوبر ٢٠٢٠، ص ١٣- ١٩.

[٣٧] محمد القحطاني، قدرات القرصنة السيبرانية الإيرانية، مركز الملك فيصل للبحوث والدراسات الإسلامية، الرياض، ٢٠٢٠، ص ٢٣-٥٩.