جامعة باتنة 1
كلية الحقوق والعلوم السياسية
قسم العلوم السياسية

التنافس الروسي-الأمريكي على الهيمنة السيبرانية وتأثيره على الأمن العالمي 2016-2024

مذكرة معدة ضمن متطلبات نيل شهادة الماستر في العلوم السياسية
تخصص: العلاقات الدولية

إعداد الطالبة:
زعتر أسماء.

إشراف الأستاذة:
أ.د. بحري دلال.

لجنة المناقشة

الاسم واللقب	الرتبة العلمية	المؤسسة الجامعية	الصفة
أ.د طروب بحري	أستاذة التعليم العالي	جامعة باتنة 1	رئيسا
أ.د دلال بحري	أستاذة التعليم العالي	جامعة باتنة 1	مشرفا ومقررا
د. سامي بخوش	أستاذ محاضر (أ)	جامعة باتنة 1	مناقشا

السنة الجامعية: 2023 / 2024

بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

﴿ وَقَالَ رَبِّ أَوْزِعْنِي أَنْ أَشْكُرَ نِعْمَتَكَ الَّتِي أَنْعَمْتَ عَلَيَّ وَعَلَىٰ وَالِدَيَّ وَأَنْ أَعْمَلَ صَالِحًا تَرْضَاهُ وَأَدْخِلْنِي بِرَحْمَتِكَ فِي عِبَادِكَ الصَّالِحِينَ ﴾

سورة النمل الآية:[19]. صدق الله العظيم

الإهداء

أهدي بكل حب وإعتزاز بحث تخرجي إلى نفسي التي تحملت كل العثرات والصعاب بتوفيق من الله.

وإلى سكان قلبي...

إلى عزيزي والوطن الذي أنتمي إليه، الذي جعل مني فتاة ما إن تُرى يقال لوالدٍ ما أكرمه وما أطيبه، وإني لأشكر الله على ما أنعم علي بأب تضج المجالس بذكره الطيب ويكفيني أنني إبنتك. دمت لي سندًا وفخرًا أسمو وأعلو به **أبي**.

إلى حبيبتي وبهجة روحي، التي تبصر في داخلي وترى عثراتي وبكائي وفرحتي والداعم الأول لتحقيق طموحي إلى صاحبة القلب الحنون التي رافقني دعاؤها طوال هذه السنين **أمي.**

حفظكما الله وأعانني على رد جزء من فضلكما علي.

إلى **أمي الثانية** وفقيدة قلبي رحمها الله وأسكنها فسيح جناته.

إلى كل **أفراد أسرتي الصغيرة** فخرًا وإعتزازًا كل بإسمه من كانوا سندًا ودعمًا، الذين أحسنوا الظن بي ولم ينسوني بدعائهم.

وإهداء من القلب إلى القلب لرفاق الخطوة الاولى والخطوة ماقبل الأخيرة إلى عائلتي الثانية: **خولة**، **حنين** كنتما سحابًا ممطرًا طوال الخمس سنين. إلى من يسعدهم نجاحي وأرادوا بي خيرًا أهدي عملي المتواضع وأسأل الله أن يجعله عملاً ينفعني وينتفع به.

﴿ وَإِذْ تَأَذَّنَ رَبُّكُمْ لَئِن شَكَرْتُمْ لَأَزِيدَنَّكُمْ ﴾ سورة إبراهيم، الآية: [07].

فالحمد لله الذي ما إنتهى درب ولا ختم جهد ولا تم سعي إلا بفضله الحمد لله الذي بارك لي وأعانني وأعطاني القوة والصبر لإتمام هذا البحث، اللهم إجعلها بداية خير وتوفيق لي.

كما أتقدم بجزيل الشكر لمشرفتي الفاضلة الأستاذة الدكتورة **بحري دلال**، على إشرافها على هذا العمل بما تفضلت علي بتوجيهاتها ونصائحها طيلة فترة إنجازه، ولم أجد منها إلا الصدر الرحب والخلق الطيب جزاك الله خيرًا و أدام عليك العلم والفضل والنعم وأسأل الله أن يزيدك من فضله.

وأتقدم بالشكر والتقدير للسادة الأفاضل أعضاء لجنة المناقشة، رئيسة اللجنة الأستاذة الدكتورة **بحري طروب،** والعضو المناقش الدكتور **بخوش سامي**، لقبولهم مناقشة مذكرة تخرجي.

وأشكر كل أساتذة قسم العلوم السياسة جامعة باتنة 1 الذين كان لهم الفضل في تكويني طوال السنوات الخمس، وأخص بالذكر الأستاذة الدكتورة **بحري طروب** لحسن معاملتها وطيبتها ودعمها الدائم لي وتقديم نصائح أكاديمية وحياتية. لم أنسى ولن أنسى كلماتك التي كانت بلسما في فترات صعبة مررت بها، شكرا من القلب أستاذتي الفاضلة بارك الله فيك على كرمك وعطائك ودمت خيرًا وقلبًا عطوفًا لي ولجميع الطلبة. كما أشكر أستاذتي **العايب سرية** على مساعدتها ونصائحها التي قدمتها لي في إنجاز هذا العمل أسأل الله أن يرزقك من فضله الواسع لكرمك وحسن معاملتك. وأتقدم بجزيل الشكر لكل الأسرة الجامعية لكلية الحقوق والعلوم السياسية لجامعة باتنة 1. كما أتقدم بجزيل الشكر للأستاذ الدكتور **حمادي جمال** بجامعة بسكرة كلية العلوم والتكنولوجيا قسم الهندسة المدنية والري لمساعدته في تنقيح الملخص باللغة الإنجليزية.

ويسعدني أن أتقدم بجزيل الشكر لكل من ساعدني ومد يد العون وشجعني لإتمام هذا العامل ليرقى إلى المستوى المطلوب إن شاء الله.

ملخص الدراسة:

اهتمت هذه الدراسة بالتنافس الروسي–الأمريكي على الهيمنة السيبرانية وتأثيره على الأمن العالمي في الفترة من 2016 إلى 2024، بهدف البحث في إستراتيجية سعي روسيا والولايات المتحدة الأمريكية للتنافس على تحقيق الهيمنة السيبرانية وتأثير هذا التنافس على الامن العالمي.

بعد الحرب الباردة والتغيير الجذري الذي حدث في جميع المجالات نتيجة للتطور التكنولوجي الرقمي، دخل العالم مرحلة جديدة وبداية ثورة صناعية رابعة بإدماج الذكاء الإصطناعي وأنترنت الأشياء، فقد برز الفضاء السيبراني كمجال خامس مع المجالات الأربعة الأخرى وظهرت ساحة معركة جديدة للتنافس بين القوى الكبرى على هذا الفضاء، حيث زادت حدة التنافس بين روسيا والولايات المتحدة لسعي كل منهما فَرْضَ هيمنتها كشكل جديد للحرب الباردة من خلال تعظيم قوتها وقدراتها السيبرانية بغرض زيادة القدرات الإستراتيجية عبر تبني إستراتيجية دفاعية وهجومية خاصة وأن هذا الفضاء سيصبح مسرحا للصراعات والحروب المستقبلية، وإدراكهما أهمية التحكم في المعلومة واستخدام التكنولوجيا بالأخص في ظل الطبيعة المتسارعة التي يتطور بها هذا الفضاء يصبح أي نظام سيبراني قابل للإختراق. فالتنافس السيبراني المتزايد بينهما يلقي بظلاله على الأمن العالمي ويشكل خطرًا ويهدد بعواقب وخيمة وبعيدة المدى على مختلف الأبعاد العسكرية، الإقتصادية، السياسية والإجتماعية. وقد اقتضت طبيعة الموضوع الإعتماد على كل من المنهج الوصفي، التحليلي.

الكلمات المفتاحية: التنافس السيبراني، الهيمنة السيبرانية، روسيا، الولايات المتحدة الأمريكية، الأمن العالمي.

Abstract:

This study focused on the Russian-American competition for cyber dominance and its impact on global security in the period extending from 2016 to 2024, with the aim of researching the strategies of Russia and the United States of America in their competition for cyber hegemony and its impact on global security.

After the Cold War and the radical change that occurred in all fields as a result of digital technological development, the world entered a new phase and the beginning of the Fourth Industrial Revolution with the integration of Artificial Intelligence and the Internet of Things. Cyberspace has emerged as a fifth field with the other four fields and a new battlefield has emerged for competition between the major powers over this space. As the intensity of competition between Russia and the United States increased as each of them sought to impose its domination as a new form of the Cold War by maximizing its cyber power and capabilities with the aim of increasing strategic capabilities by adopting a defensive and offensive strategy, especially, since this space will become a theatre for future conflicts and wars, their awareness of the importance of controlling information and using technology, especially, in with the acceleration nature in which this space is developing, and any cyber system becomes hackable. The increasing cyber competition between them emphasize a shade over

the global security, poses a threat, and threatens with terrible and long-term consequences on various military, economic, political and social dimensions. The nature of the topic necessitated reliance on the descriptive, analytical approaches.

Keywords: Cyber competition, Cyber hegemony, Russia, USA, global security.

خطة الدراسة

مقدمة:

الفصل الأول: مدخل مفاهيمي نظري للهيمنة السيبرانية.

المبحث الأول: المفاهيم الأساسية للهيمنة السيبرانية.

المطلب الأول: مفهوم الهيمنة السيبرانية.

المطلب الثاني: المفاهيم ذات الصلة بالهيمنة السيبرانية.

المطلب الثالث: الأبعاد الدولية للهمينة السيبرانية.

المبحث الثاني: النظريات المفسرة للهيمنة السيبرانية.

المطلب الأول: النظرية الواقعية.

المطلب الثاني: نظرية الأمننة.

الفصل الثاني: التنافس الروسي-الأمريكي على الهيمنة السيبرانية.

المبحث الأول: التطور الكرونولوجي للتنافس الروسي-الأمريكي على الهيمنة السيبرانية.

المطلب الأول: التنافس السيبراني الروسي-الأمريكي منذ 2016-2020.

المطلب الثاني : التنافس السيبراني الروسي-الأمريكي منذ 2020-2024.

المبحث الثاني: الإستراتيجية الروسية-الأمريكية للتنافس على الهيمنة السيبرانية.

المطلب الأول: الإستراتيجية الروسية التنافسية على الهيمنة السيبرانية.

المطلب الثاني: الإستراتيجية الأمريكية التنافسية على الهيمنة السيبرانية.

الفصل الثالث: تأثير التنافس السيبراني الروسي-الأمريكي على الأمن العالمي ومستقبله.

المبحث الأول: واقع تأثير التنافس السيبراني الروسي- الأمريكي على الأمن العالمي.

المطلب الأول: واقع تأثير التنافس السيبراني الروسي-الأمريكي على البعد الإقتصادي والعسكري.

المطلب الثاني: واقع تأثير التنافس السيبراني الروسي-الأمريكي على البعد السياسي والإجتماعي.

المبحث الثاني: مستقبل التنافس السيبراني الروسي- الأمريكي.

المطلب الأول: السيناريو التصاعدي.

المطلب الثاني: السيناريو التنازلي.

المطلب الثالث: سيناريو استمرار الوضع القائم.

الخـــاتـــمة.

قائـــمة الـمـراجـع.

فهرس المـحـتويـــات.

مـقـــدمـــة

تطـورت العـلاقـات الـدولـية بعد الحرب الباردة من حيث الفواعل والقضايا والأساليب المتباينة، وخلال ذلك تطورت التكـنولـوجيا الرقمية محدثة تغييرًا جذريًا في جميع المجالات، بل وقد أصبحنا على أعـتاب ثورة صنـاعية رابعة يقودها الذكاء الإصطناعي وأنـترنـت الأشياء، فبروز الفضاء السيبراني بإعتباره مـجـالًا خامسًا بالإضافة للمجالات الأربعة السابقة (البر، البحر، الجو و الفضاء) وزيادة تأثير العامل التكنولوجي في السيـاسات الـدولـية خلق نوعًا جديدًا من التنافس غير التقليدي بين الـدول الكبرى في السياق الدولي ولغياب الحدود المادية في هذا الفضاء، أصبح ما يعرف بالسيـادة مفهوما يـؤرق كـاهل الدول بإعتباره تـهـديدًا يسَهِّل إلحاق الـضرر بـأمنها فقد أصبح الفضاء السيبراني بديـلًا عن الحـروب التقليـدية والمواجهة المباشرة بين الدول تسعـى من خـلاله كل مـن روسـيا والـولايات المـتحدة لتحقيق أهدافها من خلال تعظيم قوتها والسعي للـهيمنة على هذا المـجال لـحمايـة أمنها القومي والتأثير على سيـاساتها الخارجية والإستراتيجية في الساحة الدولية.

الإشـكـالـية:

تسعى الدراسة للإجابة على الإشكالية التالية:

- كيف يؤثر سـعـي روسيا والولايات المتـحـدة الامريكية لتحقيـق الهيـمنة السيبرانية على الأمـن العـالـمي؟

الأسئلة الـفرعية:

تـتـفرع عن الإشكالـية الأسـئلـة الفرعية التـالية:

1. ماهي الهيمنة السيبرانية والمفاهيم ذات الصلة؟ وماهي أبعادها الدولية ؟
2. ماهو تاريخ التنافس الروسي– الأمريكي في المجال السيبراني وماهي إستراتيجية لكل منهما ؟
3. ماهو تأثير التنافس السيبراني الروسي–الأمريكي على الأمن العالمي ومستقبله؟

الفرضيات:

هذا الموضوع يحاول الإجابة على الإشكالية المطروحة والأسئلة الفرعية من خلال إقتراح فرضيتين كإجابة مبدئية وهما كالتالي:

- تنتهج كل من روسيا والولايات المتحدة إستراتيجية دفاعية وهجومية في إطار سعيها لتعزيز الامن السيبراني وتحقيق الهيمنة في هذا الفضاء.
- كلما زاد التنافس الروسي–الأمريكي على الهيمنة السيبرانية، كلما تزايد تأثيره على الأمن العالمي.

حدود الدراسة:

الزمانية: لقد حددت فترة الدراسة منذ الإتهامات الموجهة لروسيا من قبل الولايات المتحدة وزعم تدخلها في إنتخاباتها الرئاسية في سنة 2016 إلى غاية 2024 سنة الدراسة، وعليه سيتم تسليط الضوء على الإتهامات السيبرانية المتبادلة بين كلتا الدولتين في هذه الفترة وإدراج إستراتيجيتهما السيبرانية التنافسية لتحقيق الهيمنة في هذا الفضاء.

المكانية: يمكن تحديد الحدود المكانية للدراسة في الفضاء السيبراني، رغم غياب الحدود المادية في هذا الفضاء إلا أن أهميته الكبيرة بسبب التغييرات التي يشهدها الواقع الدولي تجعل كل من روسيا والولايات المتحدة تسعى للهيمنة عليه.

أهمية الدراسة:

الأهمية العلمية: تتجلى الأهمية العلمية للدراسة في ضرورة تحديد مفهوم الهيمنة السيبرانية، ومعرفة الإستراتيجية السيبرانية التنافسية لكل من روسيا والولايات المتحدة الأمريكية لتحقيقها، كونها أصبحت مهمة لما يشهده العالم من تطور معلوماتي تكنولوجي هائل، وكيف أصبح يعتمد على التكنولوجيا بشكل كبير من قبل جميع الفواعل في المجتمع الدولي.

الأهمية العملية: تظهر الأهمية العملية للدراسة في تقديم تحليل لتأثير التنافس السيبراني الروسي–الأمريكي على الأمن العالمي على مختلف الأبعاد: الاقتصادية والعسكرية، السياسية والإجتماعية، وإستشراف مستقبل التنافس بينهما في هذا الفضاء.

أهداف الدراسة:

تهدف الدراسة إلى تقديم إطار علمي منظم من خلال:

- البحث في مفهوم الهيمنة السيبرانية وتوضيح المفاهيم الأخرى ذات الصلة .
- البحث في تاريخ التنافس الروسي–الأمريكي على الهيمنة السيبرانية من انتخابات 2016 وتأثير كوفيد 19 على إستخدام التكنولوجيا، باعتبار مرحلة كورونا نقطة انعطاف في العلاقات الدولية.
- البحث في إستراتيجية التنافس السيبراني بين كل من روسيا والولايات المتحدة الامريكية.
- البحث في تأثير هذا التنافس السيبراني الروسي–الأمريكي على الأمن العالمي.

المناهج المعتمدة:

تعتمد هذه الدراسة على عدد من المناهج المتبعة للبحث في العلوم السياسية وهي:

المنهج الوصفي : بهدف تقديم فهم دقيق للهيمنة السيبرانية ومحاولة توضيح المفاهيم الأخرى ذات الصلة، وفي وصف الأبعاد الدولية للهيمنة السيبرانية من خلال تحديد أهميتها في الواقع الدولي. كما أستخدم هذا المنهج بهدف تفسير ظاهرة التنافس السيبراني بين كل من روسيا والولايات المتحدة الأمريكية وتحديد إستراتيجيتهما لذلك، تم إستخدام هذا المنهج في وصف علاقة التأثير بين التنافس السيبراني والأمن العالمي.

المنهج التاريخي: تم اعتماد هذا المنهج في ذكر السياق التاريخي للمنافسة الروسية–الامريكية في المجال السيبراني.

المنهج التحليلي: أُستخدم المنهج التحليلي بهدف محاولة تقديم إطار تحليلي لتأثير التنافس الروسي الأمريكي في المجال السيبراني على الأمن العالمي.

الدراسات السابقة: أتاحت مراجعة الأدبيات العديدة ذات الصلة بالبحث، والصادرة عن مراكز أنجلوسكسونية وعربية، الاطلاع على الدراسات التي تناولت الفضاء السيبراني وكيفية سعي الدول الكبرى للهيمنة عليه ومن بين هذه الدراسات نجد:

1. دراسة Marie Beazner وPatrice Robin، بعنوان: " Hot Spot Analysis : cyber conflict between US and Russia"، الصادرة عن: **Center for Security Studies**، 2017، والتي تم التركيز فيها على الخلفية والتطور الكرونولوجي للصراع السيبراني بين الولايات المتحدة الأمريكية وروسيا منذ سنة 2008 إلى 2016 مع الانتخابات الامريكية والاتهامات الموجهة لروسيا آنذاك، وكيفية تأثير الحوادث السيبرانية على المستوى المحلي والدولي وتحليل تأثير الهجمات السيبرانية على العلاقات بين البلدين. وفي الأخير تناولت الدراسة عدة إجراءات لتفادي حوادث سيبرانية مماثلة لما حدث في الولايات المتحدة الأمريكية، من خلال التركيز على تحسين الدول لأمنها السيبراني وزيادة الوعي بالبروباجندا والمعلومات المضللة والخاطئة، وتعزيز الدول لتدابير بناء الثقة من أجل تطوير المعايير الدولية للفضاء السيبراني في المستقبل، وموافقة الدول على إمكانية تطبيق القانون الدولي على أنشطة الدول في الفضاء السيبراني دون وجود معايير منظمة لهذه الأنشطة، وسيتم التركيز في هذه الدراسة على التطور الكرونولوجي للتنافس السيبراني بينهما في الفترة من 2016 إلى 2024.

2. دراسة علي عبد الرحيم العبودي، بعنوان: "هاجس الحروب السيبرانية وتداعياتها على الأمن و السلم العالميين"، الصادرة عن **مجلة قضايا سياسية**، 2019، تناولت هذه الدراسة نشأة السيبرانية كمفهوم والمفاهيم الأخرى، وكيفية تحول الصراع بين الدول من شكله التقليدي إلى السيبراني، ثم تطرقت إلى خصائص الفضاء السيبراني والحروب السيبرانية، فضلا عن تداعيات هذه الأخيرة على الأمن والسلم

الدوليين. خُتمت الدراسة بتوصيات من شأنها الحد من مخاطر الفضاء السيبراني والمعززة لحفظ حالة الأمن والسلم الدوليين، وسيتم التركيز في هذه الدراسة على تأثير التنافس السيبراني الروسي الأمريكي على الأمن العالمي على الأبعاد الاقتصادية، العسكرية، السياسية والإجتماعية.

3. دراسة من تحرير Simon Saradzhyan، المعنونة ب: "US-Russian Contention in Cyberspace"، الصادرة عن **Belfer Center for Science and International Affairs**،2021، قام الباحثون بتقديم وجهتي نظر حول آفاق الخلاف السيبراني بين الولايات المتحدة الأمريكية وروسيا. تناولت الموضوع من منظورين: الروسي و الأمريكي. وقد توصلت إلى عدة نتائج مفادها أن المخاطر المتعلقة بالسيبرانية في العلاقات الأمريكية–الروسية تشكل تهديدًا حقيقيًا للحياة والممتلكات. كما يتفقون أن العلاقات بين البلدين في المجال السيبراني يسودها الشعور بعدم الثقة وسوء الفهم، مع تركيزها على وجهة النظر الأمريكية أكثر منها في الجانب الروسي، بينما في هذه الدراسة سيتم التركيز على وجهة نظر كلتا الدولتين.

4. دراسة شريفة كلاع، بعنوان: "الصراع الروسي–الصيني–الأمريكي للإستحواذ على الهيمنة في الفضاء السيبراني"، الصادرة عن **مجلة السياسة العالمية**، 2022، تناولت هذه الدراسة موضوع الصراع بين هذه الدول الثلاث للإستحواذ على الهيمنة في المجال السيبراني، حيث قدمت تعريفا للحروب السيبرانية وأهدافها في الفضاء السيبراني كما تطرقت إلى إتجاهات الخلاف بين الدول الثلاث فيه وذكر مختلف الأساليب الدفاعية الواجب إتخاذها لتأمينه. وتشير الدراسة إلى صعوبة اللجوء إلى الحروب التقليدية في الوقت الحالي يجعل الدول تلجأ إلى الفضاء السيبراني لتحقيق الهيمنة بما يخدم مصالحها للمحافظة على أمنها وبالتالي سيادتها. إلا أن في هذه الدراسة سيتم تقديم مفهوم للهيمنة السيرانية.

مبررات إختيار الموضوع:

الأسباب الموضوعية:

- حداثة الموضوع في الساحة الدولية، مع تزايد الاهتمام بالتكنولوجيا والتحول الرقمي في الوقت الراهن.
- دراسة التنافس الروسي–الأمريكي في الفضاء السيبراني نظرًا لتصاعد أهمية هذا الأخير في عصرنا الحالي فقد أصبح من يملك المعلومة يملك القوة وإعتبار هذا التنافس إمتدادا للحرب الباردة.

الأسباب الذاتية:

- الموضوع يندرج ضمن تخصص العلاقات الدولية، ومن المواضيع الجديدة في هذا الحقل.
- الرغبة في الإطلاع ومعرفة أعمق بالدراسات الإستراتيجية والأمنية عموما والأمن والفضاء السيبراني خصوصا.

الصعوبات التي واجهها الباحث:

- موضوع حديث نسبيا لم يتم التطرق إليه في أغلب الدراسات الجامعية والأكاديمية و بالتالي قلة نوعية المراجع التي تجمع متغيرات الموضوع وتخص بالذكر تأثير التنافس السيبراني الروسي–الأمريكي على الأمن العالمي.
- إتساع نطاق الموضوع وسرعة التطورات المرتبطة به تجعل من الصعب الإلمام بكل تفاصيله.

تبرير الخطة:

للإجابة على الإشكالية والأسئلة الفرعية المطروحة ولإختبار صحة الفرضيات المقترحة تم الإعتماد في هذه الدراسة على خطة مقسمة إلى 3 فصول رئيسية :

الفصل الأول بعنوان: **مدخل مفاهيمي نظري للهيمنة السيبرانية،** وتم تقسيمه إلى مبحثين، **المبحث الأول** معنون ب: **المفاهيم الأساسية للهيمنة السيبرانية،** تم التطرق فيه إلى مفهوم الهيمنة السيبرانية والمفاهيم الأخرى ذات الصلة، والأبعاد الدولية للهيمنة السيبرانية وذلك بتحديد أهميتها في الواقع الدولي. و**المبحث الثاني** بعنوان: **النظريات المفسرة للهيمنة السيبرانية** لإبراز الإطار النظري للدراسة، بذكر النظرية الواقعية القائمة على أساس القوة، لما لهذه النظرية من أهمية في العلاقات الدولية وقدرتها التفسيرية للعديد من الظواهر في الساحة الدولية. والتطرق إلى نظرية الأمننة التي برزت في فترة الحرب الباردة في ظل التوتر بين روسيا والولايات المتحدة الأمريكية ومواكبتها التطورات وقدرتها التفسيرية للتهديدات الأمنية الدولية الجديدة في ما يسمى بالفضاء السيبراني.

بينما، **الفصل الثاني:** بعنوان: **التنافس الروسي– الأمريكي على الهيمنة السيبرانية،** الذي يندرج تحته مبحثين، **المبحث الأول:** معنون ب: **التطور الكرونولوجي للتنافس الروسي–الأمريكي على الهيمنة السيبرانية،** لفهم واقع التنافس السيبراني بينهما لابد من فهم وسردٍ للتطور التنافسي بينهما منذ 2016 إلى ماقبل كوفيد 19 كنقطة إنعطاف في العلاقات الدولية، ثم ما بعد كوفيد 19 إلى يومنا هذا (2024) فالعالم بعد كورونا لم يكن مماثلًا لما قبل ذلك. و**المبحث الثاني** كان بعنوان: **الإستراتيجية الروسية–الأمريكية للتنافس على الهيمنة السيبرانية.** تم إدراج مختلف الإستراتيجيات لكلا البلدين في سعيهما لتحقيق الهيمنة قي الفضاء السيبراني.

في حين، **الفصل الثالث:** معنون ب: **تأثير التنافس السيبراني الروسي–الأمريكي على الأمن العالمي ومستقبله،** و قسم هو الآخر إلى مبحثين، **المبحث الأول:** بعنوان: **واقع تأثير التنافس السيبراني الروسي–الأمريكي على الأمن العالمي،** والقيام بدراسة تأثير هذا التنافس بين البلدين على الأبعاد الأربعة (حسب **Barry Buzan)** للأمن العالمي. و**المبحث الثاني:** بعنوان: **مستقبل التنافس السيبراني الروسي–الأمريكي،**

حيث تم القيام بدراسة إستشرافية لهذا التنافس. وفي الأخير، **الخاتمة** التي كانت إثباتا للفرضيات المطروحة وتم عرض فيها مجموعة من الإستنتاجات.

الفصل الأول: مدخل مفاهيمي نظري للهيمنة السيبرانية.

التهديدات الأمنية الجديدة (اللاتماثلية) التي يشهدها النظام الدولي بعد الحرب الباردة التي أصبحت لا تعترف بالسيادة والحدود الجغرافية للدول، أحدثت تغييرًا جذريًا في مجال العلاقات الدولية عموما والدراسات الأمنية والإستراتيجية بصفة خاصة.

بعد أن كان الاهتمام منصبًا على القوة الصلبة "Hard Power"، برزت القوة الناعمة" Soft Power " التي تعتمد على قدرات الجذب و الاقناع، لكن مع التقدم الهائل في تكنولوجيا المعلومات برز ما يسمى بالمجال السيبراني"Cyber Domain" وما يحتويه من مفاهيم مختلفة كالقوة السيبرانية"Cyber Power"، الحرب السيبرانية "Cyber War" والهيمنة السيبرانية "Cyber Dominance" . هذه الأخيرة أصبحت ذات شأن وأهمية لدى الدول الكبرى، لتأثيرها في السياسات العالمية وتغيير موازين القوى. حيث أصبح من يكسب هذه التكنولوجيا ويحسن استخدامها تمكنه من تحقيق أهدافه الإستراتيجية والتأثير في سلوك مختلف فواعل المجتمع الدولي.

سيتم في هذا الفصل التركيز على مفهوم الهيمنة السيبرانية ،المفاهيم ذات الصلة بها، وتحديد الأبعاد الدولية للهيمنة السيبرانية. كما سيتم التطرق إلى مختلف النظريات المفسرة للهيمنة السيبرانية.

المبحث الأول: المفاهيم الأساسية للهيمنة السيبرانية.

المطلب الأول: مفهوم الهيمنة السيبرانية.

الهيمنة تعني سيطرة مجموعة على أخرى والتي غالبا ما تدعمها معايير وأفكار شرعية، وكثيرا ما يستخدم مصطلح الهيمنة لوصف الموقف المهيمن نسبيا لمجموعة معينة من الأفكار إلى أن تصبح شائعة، وبديهية، ومتداولة هذا ما يحول دون نشر الأفكار البديلة. [1] أما الفضاء السيبراني (Cyberspace) الذي يعود أصل مصطلح Cyber فيه إلى تطور أعمال **نوربرت وينر Norbert Wiener**، الذي قدم تعريف السيبرانية في كتابه بأنها:" التحكم و التواصل في الحيوان والآلة"، وأشار إلى فكرة أن البشر يمكنهم التفاعل مع الآلات، وأن النظام الناتج يمكن أن يوفر بيئة بديلة للتفاعل تشكل أساسا لمفهوم الفضاء السيبراني. في بداية الثمانينات من القرن العشرين صاغ كاتب الخيال العلمي William Gibson (مصطلح Cyberspace) الفضاء السيبراني في أحد كتبه بجمع كلمة السيبرنطيقا "Cybernetics" (علم التحكم الآلي) مع كلمة الفضاء "Space"، وعلى الرغم من حدوث الأمر في إطار خيالي إلا أن الكلمة أصبحت مستخدمة في الأوساط المهنية والأكاديمية مع إنتشار شبكة الأنترنت على نطاق واسع. [2]

[1] Ben Rosamond, Hegemony Encyclopedia Britannica, 11 April 2024, seen the 30th April 2024.
[2] Rain Ottis, Peter Lorents, "Cyberspace: Definition and Implications", Cooperative Cyber Defence Center of Excellence, Tallin, Estonia, 2010, p. 01.

فالفضاء السيبراني هو مجال إفتراضي من صنع الإنسان لا حدود له يعتمد على نظم الكمبيوتر وشبكات الأنترنت وكم هائل من البيانات والمعلومات والأجهزة[1]، يعتبر مجالا حيويا وجيوستراتيجيا يخاض فيه العديد من الحروب والهجمات الرقمية.[2]

كما أن هناك من عرف الفضاء السيبراني بوصفه الذراع الرابعة للجيوش الحديثة إلى جوار القوات البرية والبحرية والجوية[3]، خاصة وأن الأنترنت تشهد معارك حقيقية تدور في هذا العالم الإفتراضي، وهناك من يرى أنه يمثل البعد الخامس للحرب. [4]

وتعرف وزارة الدفاع الأمريكية الفضاء السيبراني، بأنه مجال يتسم باستخدام الإلكترونيات (أي تكنولوجيا المعلومات)، والطيف الكهرومغناطيسي في تخزين البيانات وتعديلها وتبادلها عن طريق أنظمة شبكات الإتصال والبنية التحتية المادية المرتبطة بها. [5]

وعند قول الهيمنة يعني استخدام القوة لنشر الأفكار لمجموعة معينة وسيطرتها على أخرى وفي الفضاء السيبراني نجد القوة السيبرانية (Cyber power) التي يعتبر **جوزيف ناي Joseph Ney** من أبرز المهتمين بها ويرى بأنها ليست أول مرة يتأثر مفهوم القوة فيها بالتطور التكنولوجي، ففي القرن الخامس عشر قد تأثر المفهوم بإختراع الطابعة وما أحدثه من تطور في الإصلاح داخل أوروبا.[6] يرى أن القوة السيبرانية مرتبطة بإمتلاك المعرفة التكنولوجية والقدرة على إستخدامها.[7]

يعرفها **جوزيف ناي Joseph Ney** بأنها:" القدرة على تحقيق النتائج المرجوة من خلال استخدام الموارد المعلوماتية المتصلة إلكترونيا في الفضاء السيبراني، وفي تعريف يُستخدم على نطاق واسع:

---

[1] إسماعيل زروقة، " الفضاء السيبراني والتحول في مفاهيم القوة و الصراع"، مجلة العلوم القانونية و السياسية، م. 10، ع.01 (أفريل 2019): ص.1017.

[2] علاء الدين فرحات، "الفضاء السيبراني: تشكيل ساحة المركة في القرن الحداي و العشرين"، مجلة العلوم القانونية و السياسية، م.10، ع.03 (ديسمبر2019): ص.90.

[3] زروقة، المرجع السابق، ص. 1017.

[4] شريفة كلاع، "الصراع الروسي– الصيني– الأمريكي للإستحواذ على الهيمنة في الفضاء السيبراني"، مجلة السياسة العالمية، م.06، ع.01 (2022): ص.1011.

[5] شريفة كلاع، "الأمن السيبراني و تحديات الجوسسة و الإختراقات الإلكترونية للدول عبر الفضاء السيبراني"، مجلة الحقوق و العلوم الإنسانية، م.15، ع.01 (2022): ص.294.

[6] إيهاب خليفة، القوة الإلكترونية كيف يمكن أن تدير الدول شؤونها في عصر الأنترنت؟ "الولايات المتحدة نموذجا"، ط.1.(القاهرة: العربي للنشر والتوزيع، 2017)، ص.24.

[7] المرجع نفسه، ص.56.

القوة السيبرانية هي القدرة على استخدام الفضاء السيبراني لخلق مزايا والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك بأدوات القوة. [1]

يتبع **جوزيف ناي Joseph Ney** في تعريفه أن القوة السيبرانية يمكن إستخدامها لتحقيق النتائج المرغوبة في الفضاء السيبراني، أو يمكن إستخدام أدوات سيبرانية لتحقيق النتائج المرجوة في مجالات أخرى غير المجال السيبراني. [2]

تعرف القوة السيبرانية Cyber power، بأنها الموارد البشرية والمادية في بيئة اِستراتيجية التي يمكن أن تستخدم لخلق تأثيرات في الفضاء السيبراني. [3]

إذا مفهوم الهمينة السيبرانية المكون من المفهومين السابقين، يشير إلى قدرة دولة، أو مجموعة من الدول على فرض السيطرة على الفضاء السيبراني بما في ذلك الأنترنت، المراقبة السيبرانية والحروب السيبرانية. ويشير هذا المفهوم إلى القدرة على التفوق والسيطرة في الفضاء السيبراني، ويمثل القوة السيبرانية التي يمكن أن تمتلكها دولة أو جهة معينة في العالم الرقمي. تتعلق الهيمنة السيبرانية بالقدرة على حماية البنية التحتية السيبرانية والبيانات والأنظمة من الهجمات السيبرانية، فتحقيق الأمن السيبراني يعزز من الهيمنة السيبرانية.

"....و يبدو الثابت اليوم في العلاقات الدولية وتوازنات القوى، أن الحرب الباردة والصراع بين الأقطاب في العالم تحول إلى حرب سيبرانية صامتة وقد تكون مدمرة في الأعوام المقبلة، من هنا بدأت دول العالم، الواحدة تلو الأخرى تستكشف الخيارات المتاحة لتعزيز قدراتها الهجومية في الفضاء السيبراني..". [4]

"عودٌ على بدء، فإنها ظاهرة متعددة الجوانب تعمل على تغيير العالم، في حين أن التكنولوجيا قد تفتح طرقا جديدة للإكتشاف والتواصل، فإنها تشكل أيضا تحديات وتهديدات كبيرة للمجتمعات في جميع أنحاء المعمورة...". [5]

---

[1] Joseph Ney,"Cyber Power", Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2010, p04.

[2] Ibid., p04

[3] Robert Jake Bebber, "Cyber Power and Cyber Effectiveness: An analytic Framework", Comparative Strategy, November 2017, p04.

[4] خالد وليد، "الفضاء السيبراني... نحو إمتلاك "ناصية القوة""، قناة الجزيرة، 10 سبتمبر،2021، قسم المقالات. متاحة على الرابط:

https://bit.ly/4adeCDs

[5] خالد وليد محمود، "عن "الهيمنة" و"التحكم" الرقمي"، القدس العربي، 18 أوت، 2023، قسم المقالات. تم الصفح يوم 2024/02/10 متاحة على الرابط

https://bit.ly/3JTHiX5

المطلب الثاني: المفاهيم ذات الصلة بالهيمنة السيبرانية.

هناك العديد من المفاهيم المشابهة والتي تتعلق بالهيمنة السيبرانية، ولذلك لابد من تقديم تعريف لهذه المفاهيم للفهم الجيد والقدرة على التمييز بين المصطلحات:

1. **التنافس السيبراني: (Cyber Rivalry):**

التنافس ظاهرة حتمية في العلاقات الدولية، فمنذ ظهور مفهوم الدولة القومية بعد معاهدة وستفاليا والدول تتنافس في مختلف المجالات، عسكريا، إقتصاديا،... . ومع التطور التكنولوجي والثورة المعلوماتية وبروز الفضاء السيبراني، تسعى الدول إلى فرض هيمنتها وتعظيم قوتها. يمكن القول أن التنافس السيبراني، هو مجموعة من التفاعلات في بيئة تكنولوجية عالمية معقدة (الفضاء السيبراني) ويتم التركيز فيه على القوة السيبرانية، بسعي كل طرف لزيادة قوته وتعظيمها داخل هذا الفضاء عن طريق زيادة الدفاع السيبراني من خلال إستراتيجيات سيبرانية وزيادة الأمن السيبراني.[1]

2. **الصراع السيبراني: (Cyber Conflict):**

الصراع في الفضاء السيبراني يشير إلى الأفعال المتخذة من قبل أطراف نزاع ما لتحقيق ميزة على خصومهم، بإستخدام أدوات تقنية مختلفة[2]. بمعنى هو إستخدام تكنولوجيا الحاسوب لأغراض التدمير من أجل التغيير،التأثير أو التعديل. كما يعرف بأنه: نموذج للحرب غير المتكافئة تسعى من خلاله كل أطراف الصراع المختلفة إلى تعظيم الإستفادة من الفضاء السيبراني، بسط النفوذ، الهيمنة وحماية أمنها القومي. فضلا عن تحقيق مكاسب غستراتيجية، إقتصادية، سياسية ومالية لم تكن لتحققها عبر الوسائل العسكرية التقليدية[3].

3. **الجريمة السيبرانية: (Cyber Crime):**

تعبر الجريمة السيبرانية من بين الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها والتي إرتبطت بتقنية المعلومات. فقد أصطلح على تسميتها بداية: إساءة إستخدام الكومبيوتر، ثم إحتيال الكومبيوتر، فالجريمة المعلوماتية بعدها جرائم الكومبيوتر والجريمة المرتبطة بالكومبيوتر ثم جرائم التقنية العالية، إلى جرائم الهاكرز وأخيرا الجريمة السيبرانية.[4] وقد إتجه العديد من الفقهاء إلى إعتماد

---

[1] رؤى عبدالله محمد، الطاهر محمد الفادني، "أثر التنافس السيبراني الأمريكي–الروسي على الأمن العالمي في الفترة 2015–2022م "(رسالة ماجستير غير منشورة، جامعة النيلين، الخرطوم، 2022)، ص. 26.

[2] Herbert Lin," Cyber Conflict and International Law", International Review of The Red Cross, Vol. 94, N°.886 (Summer 2012): p.515.

[3] جاسم محمد طه، "التهديدات السيبرانية و انعكاساتها على الأمن القومي الأمريكي"، مجلة تيكريت للعلوم السياسية، م. 02، ع. 32(2023): ص.193.

[4] ياسمينة بونعلرة،"الجريمة الإلكترونية"، مجلة المعيار، م. 20، ع. 39(2015): ص. 276 .

تعريف منظمة التعاون الاقتصادي والتنمية للجريمة الإلكترونية التي تعرف بأنها كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها.[1]

تتسم هذه الجريمة السيبرانية، بالسرعة، والتطور المستمر في وسائل إرتكابها، وإنعدام العنف المادي ضد الإنسان فيها مقارنة مع الجرائم التقليدية، عابرة للحدود كما تتسم بصعوبة تحديد مصدرها. [2]

4. **التجسس السيبراني: (Cyber Espionage):**

يشير لعملية مستمرة لجمع المعلومات السرية حول الخصوم ومعرفة نواياهم وقدراتهم، يهدف هذا النشاط للوصول إلى البيانات السرية للشركات والحصول على بيانات الملكية الفكرية، والمعلومات الخاصة وبراءات الإختراع والقيام بالتلاعب السري بالبيانات والبنية التحتية الحيوية للتحضير للحرب السيبرانية. [3]

5. **الحرب السيبرانية: (Cyber Warfare):**

لا يوجد إجماع على تعريف محدد ودقيق لمفهوم الحرب السيبرانية، حيث عرفها كل من ريتشارد كلارك وروبرت كناك "Richard Clarke & Robert Knake" بأنها الأعمال التي تقوم بها دولة ما، تحاول من خلالها إختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى، بهدف تحقيق أضرار بالغة أو تعطيلها. ويعرفها آخرون بأنها: مفهوم يشير إلى أي نزاع يحدث في الفضاء الإلكتروني ويكون له طابع دولي.[4]

كون الحرب مفهوما يرتكز بالأساس على إستخدام الجيوش النظامية وكان يسبقها إعلان واضح لحالة الحرب وميدان قتال محدد إلا أن في الفضاء السيبراني، فإنها غير محددة المجال أو الأهداف، كونها تتحرك عبر شبكات المعلومات والإتصال المتعدية للحدود الدولية، أو اعتمادها على أسلحة إلكترونية جديدة تلائم السياق الإلكتروني لعصر المعلومات. [5]

---

[1] المرجع نفسه، ص ص. 277، 278.

[2] سعيد بن سالم البادي وآخرون، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، د.ط. (عمان: مجمع البحوث والدراسات، 2016)، ص.20.

[3] Fred Schreier, "On Cyberwarfare", Dcaf Horizon Working Paper, N°.7 (2015): p. 09.

[4] كريم أنصر سفاح، "الحروب الإلكترونية وأثرها على الأمن القومي"، قسم الدراسات التكنولوجية والأمن السيبراني، مركز النهرين للدراسات الاستراتيجية، تم التصفح يوم: 02 مارس 2024. متاحة على الرابط:
https://www.alnahrain.iq/post/1031

[5] أميرة عبد العظيم محمد عبد الجواد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، مجلة الشريعة والقانون، ع.35، ج. 03، (2020): ص.390.

فالحرب السيبرانية هي إستخدام التكنولوجيا الحديثة والأنترنت للقيام بالهجمات على الأهداف الحيوية الحكومية، التجارية، الصناعية والعسكرية وتتطلب مهارات تقنية عالية وخبرة في الأمن السيبراني والحماية من الهجمات الإلكترونية. [1]

6. **الهجوم السيبراني: (Cyber Attack):**

يطلق على الشلل المتعمد أو تدمير قدرات شبكة العدو مثل سرقة المعلومات من أجهزة التخزين، والهجوم على نظم المعلومات والإتصالات.[2]

7. **الإرهاب السيبراني: (Cyber Terrorism):**

يعتبر التعريف الذي قدمه "Dorthy Dayang" من أشمل التعاريف للإرهاب السيبراني، حيث قال إنه إلتقاء الإرهاب مع الفضاء السيبراني، وهو يشير إلى التهديدات غير القانونية المستهدفة للشبكات الإلكترونية والمعلومات المخزنة بهدف إخافة الحكومات أو إجبارها، أو حتى إخافة عامة الناس وإجبارهم على إتخاذ مواقف معينة لتعزيز أهداف سياسية أو إجتماعية.[3] يمكن أن يتسبب في خسائر مادية أو إقتصادية وحتى بشرية إذا ما أُستهدفت العمليات الإرهابية شبكات الصناعة النووية و المصانع الكيميائية.[4]

8. **الردع السيبراني: (Cyber Deterrence):**

يعني محاولة الدول لردع المنافسين من إلحاق الضرر بالبنى التحتية الحيوية الخاصة بها، بالعمل على تطوير أساليب الردع للمساعدة في منع حدوث الهجمات السيبرانية من خلال جعل تكلفة الهجوم باهظة وذلك بتأمين أنظمة الحاسوب بحيث يصعب الأمر على المهاجمين لإيجاد ثغرات في هذه الأنظمة وأيضا محاولة فرض عقوبات، والتهديد بالرد على الهجمات.[5] ولا زالت الدول تسعى لحماية أنظمتها وسد الثغرات إلا أن التطور الهائل الذي يحدث في هذا المجال يصعب ذلك ويجعلها دائما عرضة للمخاطر والتهديدات.

---

[1] عز الدين قطوش، "الحرب الباردة الأمريكية–الروسية في الفضاء السيبراني"، مجلة مدارات سياسية، م.07، ع.02 (2023): ص.289.

[2] زينب شنوف، "الحرب السيبرانية في العصر الرقمي حروب ما بعد كلاوزفيتش"، المجلة الجزائرية للأمن والتنمية، م. 09، ع. 02 (جويلية 2022): ص. 92.

[3] حنان دريسي، " الحروب السيبرانية: تحول في أساليب القتال وثبات في المبادئ والأهداف"، مجلة الفكر القانوني والسياسي، م. 06، ع. 01(2022): ص.915.

[4] المرجع نفسه، ص. 915.

[5] بشار خليل، "الحرب السيبرانية، الأهداف، الردع، الدفاع"، المجلة العلمية السورية للمعلوماتية، ع. 155 (أكتوبر2022).

9. **الإستراتيجية السيبرانية: (Cyber Strategy):**

تعني تطوير وتوظيف القدرات اللازمة للعمل في الفضاء السيبراني، تعتمد الإستراتيجية السيبرانية على القدرات السيبرانية لتحقيق مختلف أهداف الأمن العسكري، السياسي، الإقتصادي،... . وتوفير الموارد والتكاليف الواجب إتخاذها لمواجهة التهديدات في هذا الفضاء.[1]

10. **الأمن السيبراني:(Cyber Security) :**

شأنه في ذلك شأن العديد من المفاهيم فهو الآخر لا يوجد تعريف واحد ومحدد له، فهناك من يرى أنه يعني مجموع الإجراءات الواجب إتخاذها من قبل الأجهزة الأمنية للمحافظة على سرية المعلومات الإلكترونية ومنع الإختراقات الفيروسية. هناك من يَعُدُّهُ متداخلا مع أمن المعلومات مدعيا أن الأمن السيبراني هو فرع من فروع أمن المعلومات. [2]

هناك من عرفه بأنه الأسلوب والإجراءات المرتبطة بعمليات إدارة المخاطر الأمنية التي تتبعها المنظمات والدول لحماية سرية وسلامة وتوافر البيانات والأصول المستخدمة في الفضاء السيبراني.[3]

وعليه فالأمن السيبراني هو: مزيج من العمليات والتقنيات والممارسات والهدف منه حماية البرامج والتطبيقات والشبكات وأجهزة الكمبيوتر والبيانات من الهجوم، ويشمل الأمن السيبراني: أمن مادي للبرامج والتطبيقات والشبكات وأجهزة الكمبيوتر، أمن غير مادي (معنوي) متعلق بالبيانات والمعلومات من أي هجوم وأضرار وسرقة للمعلومات والتحكم في الوصول الصحيح للأجهزة والتطبيقات لحمايتها من الضرر. [4]

المطلب الثالث: الأبعاد الدولية للهيمنة السيبرانية.

للهيمنة السيبرانية أهمية كبيرة في الواقع الدولي، حيث تعتبر جزءًا مهما من العلاقات الدولية في عصرنا الحالي، ويتضح ذلك من خلال تأثيرها على أمن الدول والعلاقات بين فواعل المجتمع الدولي. توضح الدراسات أن التفوق في المجال السيبراني أصبح جزءًا أساسيا لأمن الدول الأمر الذي يفضي إلى تحول في مفهوم القوة والعديد من المفاهيم الأخرى كالحروب، الصراع ....الخ.

---

[1] شنوف، المرجع السابق، ص. 92.

[2] كلاع، (الأمن السيبراني..)، المرجع السابق، ص.298.

[3] مصطفى إبراهيم سلمات الشمري، "الأمن السيبراني و أثره في الأمن الوطني العراقي"، مجلة العلوم القانونية و السياسية، م.10، ع.01 (2021): ص.155.

[4] كلاع، المرجع السابق، ص. 298.

حيث أصبح للحروب السيبرانية والأمن السيبراني تأثير مهم في تشكيل السياسات الخارجية وإستراتيجيات الدول في الساحة الدولية تجاه باقي الفواعل الأخرى. يعتبر المجال السيبراني من أهم المجالات في القرن 21 وذلك بسبب التطور الهائل في التكنولوجيا والإتصالات وتوسع إستخدام الأنترنت والأجهزة الذكية، حيث يبرز كعنصر حاسم في تشكيل مستقبل الواقع الدولي لما له من تأثير كبير على جميع جوانب المجتمع الدولي هذا ما يدفع القوى الكبرى وروسيا وأمريكا كنموذجين للدراسة للتنافس والرغبة في التفوق في هذا المجال. وهذا ما يعطي للهيمنة السيبرانية أهمية متزايدة في الواقع الدولي لأنها تؤثر على الأمن، السيادة والإقتصاد.

- إمكانية إستخدامها كوسيلة للقوة أو الردع في العلاقات الدولية من خلال شن الهجمات السيبرانية أو التجسس الإلكتروني، أضحت مجالا لتنافس الفاعلين من الدول ومن غير الدول، إذ زاحمت الكيانات المختلفة من غير الدول الدولة القومية للتسابق على مقدرات القوة السيبرانية لتحقيق الأهداف المختلفة[1]، وأضحى الأمن السيبراني على رأس أولوية الأمن القومي للدول بمفهومه الواسع الذي لا يقتصر على الجوانب العسكرية وأمن الحدود فقط ولكن يشمل أمن الاقتصاد الرقمي وأمن المعلومات. [2]
- إعادة تعريف للسيادة، مع بروز الفضاء السيبراني العابر للحدود الجعرافية ومع تزايد الشبكات الرقمية والأنترنت أدى ذلك لتغير مفهوم السيادة ولم يعد يقتصر على الحدود الجغرافية بل أصبحت الدول تسعى لتحقيق السيادة السيبرانية من خلال سعيها لحماية مصالحها الوطنية والخارجية وحماية أمنها القومي.

أضحت الدولة التي لا تملك التكنولوجيا السيبرانية المحصنة أمنيا يصبح فضاؤها السيبراني المتضمن للأصول، الموارد، المعلومات، الخدمات والبنية التحتية التابعة لجميع القطاعات الحيوية (التجارية، الأمنية والعسكرية....الخ) عرضة للهجمات والتهديدات السيبرانية. وبالتالي أصبح هذا الفضاء من أولويات السياسات الخارجية للعديد من الدول وخاصة القوى الكبرى، وضمن إستراتيجيات الأمن القومي لها.[3]

- من أبعاد الهيمنة السيبرانية في الواقع الدولي تأثيرها على الاقتصاد، فتطور الهجمات السيبرانية يهدد بتجمد الاقتصاد العالمي، سواء لجهة الأضرار التي تتكبدها الشركات والمؤسسات المختلفة (الحكومية والخاصة)، علاوة على خسائر الأفراد. لأن كلما زاد الإعتماد على التقنيات الرقمية والتكنولوجية زادت

[1] سماح عبد الصبور عبد الحي، "القوة السيبرانية في العلاقات الدولية: دراسة في الحروب السيبرانية بالتطبيق على عام 2020"، مركز الحضارة للدراسات و البحوث، قضايا و نظرات، ع.21 (أفريل 2021): ص.94.

[2] المرجع نفسه، ص.96.

[3] حياة حسين، "الفضاء الإلكتروني وتحديات الأمن العالمي"، مجلة العلوم القانونية و السياسية، م.12، ع.01 (أفريل 2021): ص.1067.

إحتمالات التعرض للهجمات الإلكترونية والسيبرانية والتي أدت وتؤدي إلى تعطيل العمليات التجارية وسرية البيانات، علاوة على مخاطر الأمن القومي.[1] هذا ما يجعل القوى الكبرى تسعى لتحقيق التفوق في الفضاء السيبراني لحماية بنياتها التحتية وإقتصاداتها من التهديد والإختراق.

المبحث الثاني: النظريات المفسرة للهيمنة السيبرانية.

اختلفت النظريات التي شهدها حقل العلاقات الدولية، بغرض فهم وتفسير الواقع الدولي بشكل أوضح، وبروز العديد من المفاهيم المختلفة والجديدة كالهيمنة السيبرانية، التي تسعى الدول الكبرى لتحقيقها والناتجة عن التطور والتقدم المعلوماتي الحاصل في الساحة الدولية، وكنتيجة لذلك تنوعت نظريات العلاقات الدولية المفسرة للتغييرات الحادثة من جهة وإبراز أهم أطروحاتها وتعزيزها من جهة أخرى.

المطلب الأول: النظرية الواقعية.

الواقعية هي التي يتم وفقها النظر إلى العلاقات الدولية كعلاقات قوة[2]، وبإعتبار الفضاء السيبراني مجالًا جديدًا وحيويًا للعلاقات بين الدول سواء كانت تعاونية أو صراعية أدى ذلك إلى تغير في طبيعة ومفهوم القوة من خلال تهديد أمن الفضاء السيبراني.[3] حيث أصبحت الدول تسعى لتعظيم قوتها السيبرانية لرغبتها في تحقيق الهيمنة على هذا الفضاء.

نجد أن التصور الواقعي في العلاقات الدولية قد تأثر بتصور الفيلسوف السياسي البريطاني " Thomas Hobbes"، بإعتباره أن الحالة الفطرية للإنسان الشريرة تجعل العلاقات الدولية تصارعية، وأن هذا الصراع حتما موجود، وشيء لا يمكن تجنبه[4]. و غياب السلطة العليا المنظمة للعلاقات بين الدول، تجعل النظام العالمي الذي تتفاعل فيه هذه الأخيرة فوضويًا تتصارع فيه من أجل القوة وفق منطق "الكل ضد بعضهم البعض"[5]، أي أنه لاتوجد قيود على سلوك الفرد، يمكن لأي شخص في أي وقت إستخدام القوة، ويجب على

---

[1] كيف يهدد تطور الهجمات السيبرانية الإقتصاد العالمي؟ ، سكاي نيوز عربية، 15 نوفمبر 2023، تم تصفح الموقع يوم 2024/03/12. متاحة على الرابط:

https://bit.ly/3yaet69

[2] عادل زقاغ، مترجما، "مفهوم الأمن في نظرية العلاقات الدولية"، الموسوعة الجزائرية للدراسات السياسية الإستراتيجية، 16 جانفي 2021، تم تصفح الموقع يوم 2024/03/22. متاحة على الرابط:

https://bit.ly/3WywWDC

[3] عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، ط.2. (القاهرة: المركز العربي لأبحاث الفضاء الإلكتروني،2016)، ص. 21.

[4] زقاغ، مترجما، المرجع السابق.

[5] زقاغ، المرجع نفسه.

الجميع أن يكونوا دائمًا على إستعداد لمواجهة مثل هذه القوة بالقوة.[1] كما تأثر "Hans Morgenthau" بوجهة نظر "Hobbes" حول طبيعة الإنسان، على غرار "Morgenthau" نجد "Kenneth Waltz" يتبع خطى " Hobbes" فيما يتعلق بالفوضوية الدولية كعنصر أساسي من عناصر العلاقات الدولية. [2]

وبتطبيق إفتراضات النظرية الواقعية على الهيمنة السيبرانية نجد أنها تتوافق في تفسير العديد من الأمور المتمثلة في خلفيات مسببات الصراع السيبراني بين الوحدات ورغبتها في التفوق السيبراني، بإعتبار العلاقات بينها في الساحة الدولية تصارعية، تسعى كل وحدة لتعظيم قوتها في هذا الفضاء من أجل المحافظة على أمنها ومواجهة التهديدات. كما أن الطبيعة الفوضوية للفضاء السيبراني، فهو الآخر لا وجود فيه لسلطة مركزية لتنظيم العلاقات والتفاعلات الحادثة بين الوحدات في الواقع الدولي. هذا ما يغرس شعورًا بعدم الثقة بين الدول في هذا الفضاء الإفتراضي.[3] هذا ما يجعل هذه الأخيرة تطمح للهيمنة على الفضاء السيبراني لحماية أمنها من خلال تحقيق زيادة وتعظيم في قوتها، والتي هي مفهوم رئيسي في التفكير الواقعي، وحسب "Kenneth Waltz": "القوة هي الملاذ الأخير في السياسة الداخلية أما في السياسة الدولية فإن القوة ليست الملاذ الأخير بل إنها الملاذ الأول والدائم". [4]

المطلب الثاني: نظرية الأمننة.

تعتبر نظرية الأمننة من بين إسهامات مدرسة كوبنهاجن التي هي من بين أبرز المدارس التي عمدت توسيع وتعميق مفهوم الأمن[5] خاصة بعد الحرب الباردة، مستمدة أصولها التنظيرية في العلاقات الدولية من كتاب المنظر باري بوزان "Barry Buzan" الذي يعتبر من أبرز مفكريها بعنوان: **الناس، الدول والخوف، إشكالية الأمن القومي في العلاقات الدولية (People, States and Fear : The National Security Problem in International Relations)** الصادر عام 1991. [6]

مع ظهور التهديدات اللاتماثلية بين الفواعل في الساحة الدولية نتيجة التغيير الحاصل في الواقع الدولي وزيادة إكتساح الأنترنت والتكنولوجيا والإعتماد الكلي عليها من قبل العديد من الدول خاصة في الوقت الراهن،

---

[1] W. Julian Korab-Karpowicz, "Political Realism in International Relations", The Stanford Encyclopedia of Philosophy, Center for The Study of Language and Information (Summer 2017): p.11, 12.

[2] Ibid., p.12.

[3] Anthony Craig & Valeriano Brandon, "Realism and Cyber Conflict: Security in The Digital Age", E-International Relations (February 2018): p.2.

[4] عبد الصادق، المرجع السابق. ص.16.

[5] توفيق بوستي، "مدرسة كوبنهاغن نحو توسيع وتعميق مفهوم الأمن"، مركز المعهد المصري للدراسات، دراسات إستراتيجية (22 مارس 2019): ص.01.

[6] المرجع نفسه. ص. 01.

بما يسمى أنترنت الأشياء (Internet of Things) والذكـاء الإصطناعي (Aartificial Intelligence)، أصبحت هذه الفضاءات أكثر عرضة للإختراق والقرصنة. فأصبحت كل دولة تهدف لتعزيز أمنها السيبراني للتصدي للتهديد في هذا الفضاء، هذا ما نجده في الإسهامات التي طورها Ole Weaver التي تشير إلى متى يمكن إعتبار شيء ما مشكلة أمنية،[1] هذا مايعرف بعملية الأمننة فهي التي يتم فيها تحويل المشاكل إلى قضايا أمنية من خلال إضفاء الطابع الأمني عليها،[2] وهي المسار الذي يمكن من خلاله لفاعل ما أن يعلن مسألة محددة أو فاعل آخر على أنه يشكل تهديدًا فعليا.[3] إذا فالجوهر الأساسي لنظرية الأمننة Securitization Theory هو إعتبار الأمن كفعل خطابي وأن السياسات المؤطرة لأمن الدول ليست أمرًا مسلمًا به بل مصممة من قبل صناع القرار أو ما يعرف بالفاعل المؤمنِن A securitizing actor، بإستغلال الظروف الدولية وإظهارها كما لو أنها تهديد بالغ الخطورة والضخامة.[4] كما أطلق المفكر Buzan فكرة مستندة إلى نظرية الأمننة وهي فكرة الأمننة الكلية Macro-Securitization في دراسته لعام 2006 الموسومة بـ: " The War on Terrorism as The New Macro-Securitization"، والتي تشير إلى نفس فكرة الأمننة لكن بممارسة أكثر إتساعا، بالإعتماد على بناءات عالمية للتهديدات وحسب Buzan فإن هناك على الأقل سببين محتملين لهذه الظاهرة يتمثل الأول في العولمة والثاني يعود إلى الإعتقاد بإيديولوجية عالمية.[5] وعليه يتبين أن التهديد السيبراني للدول في ظل الإعتماد المتزايد على التكنولوجيا والتنافس على فرض الهيمنة في هذا الفضاء يوسع نطاق التهديدات وتأثيره على باقي المجالات وفق منطق الأمننة الكلية. وعلى قول" Barry Buzan" في تعريفه للأمن بأنه: " **العمل على التحرر من التهديد**" وقدرة الدول والمجتمعات على الحفاظ على هويتها المستقلة وسلامة وظائفها ضد القوى التي يعتبرونها معادية.[6] وعند قول "Buzan" التحرر لا يقصد الإنفلات من التهديد، فالأمن المطلق حسبه في ظل فوضوية النظام الدولي غير موجود ويبقى الأمن نسبيًا[7] والنقطة

---

[1] المرجع نفسه، ص. 18.

[2] صباح بالة، "مدرسة كوبنهاغن في تفسير الدراسات الأمنية"، الموسوعة السياسية، 9 ديسمبر 2020. تم التصفح يوم: 10 أفريل 2024، متاحة على الرابط:

https://bit.ly/3WzJYkv

[3] سليم قسوم، الإتجاهات الجديدة في الدراسات الامنية دراسة في تطور مفهوم الأمن في العلاقات الدولية، ط. 4. (أبوظبي: مركز الإمارات للدراسات والبحوث الإستراتيجية،2021)، ص. 120.

[4] المرجع نفسه، ص. 121.

[5] المرجع نفسه، ص. 123.

[6] Barry Buzan," New Patterns of Global Security in The Twenty-First Century", Royal Institute of International Affairs, Vol. 67, N°. 3 (July1991) : p. 432.

[7] بوستي، المرجع السابق، ص.2.

الأساسية للأمن هي البقاء.[1] ويظل الهاجس الأكبر لدى رجال الدولة وصناع القرار الذين اعتبروا أن ضمان ظروف البقاء والإستمرار هي من أولويات السياسة العليا للدولة.[2]

[1] Buzan, op cit., p. 432.

[2] بالة، المرجع السابق.

https://bit.ly/3WzJYkv

الفصل الثاني: التنافس الروسي- الأمريكي على الهيمنة السيبرانية.

نتيجةً للتوجه المتزايد للمجتمع الدولي نحو التكنولوجيا الرقمية ولضعف أنظمته أمام التهديدات السيبرانية، تحفزت قضية الأمن السيبراني، فتحول الفضاء السيبراني إلى ساحة جديدة للصراع الدولي بين القوى الكبرى من أجل فرض الهيمنة والنفوذ على هذا الفضاء[1]. إذ أُعتبر هذا الأخير عنصرًا أساسيًا من عناصر القوة الشاملة للدولة فأصبحت الدول تركز على التفوق في هذا المجال لغرض زيادة قدراتها الإستراتيجية،[2] وتأمين المعلومات والأنظمة ضد التهديدات التي عادة ما تستهدف الوصول لمعلومات حساسة، تغييرها أو إتلافها،[3] ومنعها عن الخصوم. فنجد كل من روسيا والولايات المتحدة الأمريكية من أكبر القوى فضلا عن وجود الصين، بريطانيا.... أيضا بالإضافة إلى قوى إقليمية أخرى كإيران، إسرائيل وتركيا.... وتم التركيز على روسيا والولايات المتحدة الأمريكية بإعتبار ما يحدث بينهم نوعا جديدا من الحرب الباردة. وذلك بسعيهما نحو تحقيق الهيمنة في هذا المجال من خلال إتخاذ إجراءات حماية عبر تبني سياسات دفاعية ضد التهديدات المحتملة ومنع تعرضها لعمليات هجومية وتعزيز أمنها وتبني سياسات هجومية عبر إتخاذ إجراءات لمهاجمة مصادر التهديد.[4]

ولفهم طبيعة التنافس السيبراني بين هاذين البلدين بإختلاف استراتيجياتهما لابد من الحديث عن التطور التاريخي للمنافسة السيبرانية بينهما.

المبحث الأول: التطور الكرونولوجي للتنافس الروسي-الأمريكي على الهيمنة السيبرانية.

في سنة 1982 حاولت المخابرات الروسية التسلل إلى مقر اللجان الوطنية الجمهورية والديمقراطية بتنفيذ تجسس يختلف عن التجسس التقليدي ضد حملة إعادة إنتخاب الرئيس رونالد ريغن Ronald Reagen في سعيهم لتشويه صورته بتعزيز شعار « **REAGEN Means War** »، رغم تلك الجهود إلا أنه فاز بـ 49 من أصل 50 ولاية،[5] ولايخفى أن الولايات المتحدة في عهده كانت تستخدم الحروب السيبرانية، حيث

[1] محمد طه، المرجع السابق، ص.179.

[2] المرجع نفسه، ص. 179.

[3] هبة جمال الدين، "الأمن السيبراني والتحول في النظام الدولي"، مجلة كلية الإقتصاد والعلوم السياسية، م.24، ع. 01، (جانفي 2023): ص.190.

[4] نصيرة صالحي، "القوة الذكية: التنافس العالمي على قوة الفضاء الإلكتروني والقدرات السيبرانية"، دفاتر السياسة والقانون، م. 13، ع. 1 (2021): ص. 380.

[5] Evan Osnos, and others," Tump, Putin and the New Cold War", The New Yoker, Published in the Print Edition of the March 6 2017, issue, with the headline “Active Measures”. The site has been seen 1/04/2024. Available at the link
https://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war

أعتبر أول من أنشأ وحدات أمريكية متخصصة في العمليات السيبرانية،[1] أما بعد نهاية الحرب الباردة، وإنهيار الإتحاد السوفياتي، وتحول العالم من الثنائية القطبية إلى الأحادية القطبية، حيث فقدت روسيا قوتها بينما أصبحت الولايات المتحدة الأمريكية قوة متـفدرة، إلا أنه بمجرد إستلام الرئيس فلاديمير بوتين" Vladimir Putin"مقاليد الحكم في روسيا عمل على إستعادتها لمجدها السابق. حيث كان هنا تقارب روسي-غربي خاصة بعد أحداث الحادي عشر من سبتمبر 2001، لكن هذا التقارب لم يدم طويلاً، فقد بدأت التوترات والصراعات تتطور والتي من أبرزها:[2]

- الغزو الأمريكي على العراق سنة 2003.
- الصراع في القوقاز سنة 2008 والذي تخللته هجمات سيبرانية بين روسيا وجورجيا.
- وآخر ما فصل روسيا عن الولايات المتحدة الأمريكية بشكل نهائي كان التدخل العسكري المتعدد الدول في ليبيا سنة 2011، الذي كان الرئيس الروسي فلاديمير بوتين "Vladimir Putin"معارضا عليه في حين وافق عليه الرئيس الروسي السابق دميتري ميدفيديف "Dmitry Medvedev" .

إذا هذه الخلافات جعلت كل طرف يضع الآخر تحت المراقبة المكثفة وإعتبار كل ماحدث وسيلة للإستفزاز.[3] وبما أن أي دولة تتعرض لهجوم سيبراني تلقي الإتهامات على دولة منافسة لها، أو عند قيامها هي الأخرى بهجوم سيبراني يكون ضد الدولة المهددة لمكانتها في الساحة الدولية، وذلك لصعوبة تحديدٍ للجهة المسؤولة عن صدور الهجمات السيبرانية؛ مثل ما حدث في الصراع الروسي -الأوكراني في سنة 2014 لضم شبه جزيرة القرم بالرغم من أنه كان تدخلا عسكريا إلا أنه لا يخلو من الهجمات السيبرانية بين الطرفين، ما جعل الصراع السيبراني اليوم بمثابة حاضنة لمختلف الصراعات سواء كانت هذه جوية، بحرية، برية أو فضائية فإنها حتما تتضمن هجومًا سيبرانيًا. وفي هذه الدراسة تم التطرق إلى التنافس السيبراني بين روسيا والولايات المتحدة في الفترة من 2016-2020 ثم من 2020- 2024.

المطلب الأول: التنافس السيبراني الروسي-الأمريكي منذ 2016-2020.

تعتبر الإتهامات الموجهة لروسيا في تدخلها بالإنتخابات الرئاسية الأمريكية في سنة 2016 عند فوز الرئيس الأمريكي السابق **دونالد ترامب** "Donald Trump" على نظيرته وزيرة الخارجية الأمريكية السابقة **هيلاري كلينتون** "Hillary Clinton"، النقطة المفصلية للدراسة كبداية لتصاعد الهجمات السيبرانية بين البلدين،

[1] أحمد عثمان محمد، "الحروب السيبرانية وأثرها في العلاقات الدولية روسيا والولايات المتحدة الأمريكية نموذجا"، مجلة الجامعة العراقية،ع. 59، ج. 02 (2023): ص. 468.

[2] Marie Beanzer & Patrice Robin, "Hotspot Analysis: Cyber-Conflict between the United States of America and Russia", Center for Security Studies (June 2017): p. 06.

[3] Ibid., p. 06.

واعتبرها البعض حربا باردة ثانية " Cold War 2". كان الرد من الإدارة الأمريكية آنذاك بطرد 35 دبلوماسيا روسيا وإغلاق منشأتين وفرض عقوبات إقتصادية على روسيا.[1] وقد خفت ملامح شدة الخلاف حول هذه الإعتداءات إلا أن إتهام روسيا بشن هجمات سيبرانية على حلفاء الولايات المتحدة في أوروبا عام 2018 وخاصة عند إتهام بريطانيا لها بشن هجمات سيبرانية ضدها[2]، ما دفع بحلف الناتو على إثر ذلك إلى تأسيس مركز للدفاع الإلكتروني، والبحث في موقف تجاه الرد على الهجوم الإلكتروني، بوصفه هجوما مسلحا وفق القانون الدولي، والبحث في مدى إمكانية تطبيق المادة 05 من ميثاق حلف الناتو، والتي تنص على: دخول الهجوم المشترك حيز التنفيذ ضد أي هجوم على أي دولة عضو في الحلف، بإعتباره إعتداءً على جميع أعضائه. [3]

تجدر الإشارة إلى أنه في هذه الفترة وإلى غاية سنة 2019 تزايدت حدة الهجمات السيبرانية بين الولايات المتحدة الأمريكية وروسيا، عند قيام مهاجمين سيبرانيين روس بإستهداف 19 دولة في 75 هجومًا سيبرانيًا، إلا أن الهدف الرئيسي لروسيا كان المساس بالبنية التحتية المعلوماتية للولايات المتحدة الأمريكية والوصول لمعلومات حساسة[4]. وقدرت الهجمات السيبرانية التي تعرضت لها الولايات المتحدة الأمريكية بأكثر من 50% من مصدر روسي أو صيني، و27.8% مصدر مجهول.[5]

في المقابل سلط مقال بصحيفة **ذ نيويورك تايمز** " The New York Times" الأمريكية في الـ 15 من يونيو سنة 2019 الضوء على إستمرار الإتهامات بينهما، فقد تضمن هذا المقال تقاريرًا تفيد بتنشيط وكالة الإستخبارات المركزية الأمريكية CIA لعمليات قرصنة إلكترونية ضد مؤسسات حكومية روسية، وأن جنودًا في قيادة الحرب السيبرانية الأمريكية زرعوا شيفرة في أنظمة الطاقة الروسية لضربها في حال تدهور العلاقات بين البلدين. رغم نفي الجانب الأمريكي لهذه الإتهامات إلا أن الجانب الروسي لم يستبعدها ومؤكدًا بشأن تعرض المجالات

---

[1] Muhammed Riaz Shad, "Cyber Threat in Interstate Relations: Case of US-Russia Cyber Tensions", Policy Perspective, Vol. 15, N°. 2 (2018): p. 41.

[2] عادل عبد الصادق، "صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية"، المركز العربي لأبحاث الفضاء الإلكتروني، تم التصفح يوم: 2023/03/28. متاحة على الرابط:

https://accronline.com/print_article.aspx?id=29415

[3] هديل حربي ذاري، "قوة الفضاء السيبراني في ساحة صراع جديدة بين القوى الدولية و الإقليمية في القرن 21"، قضايا سياسية، ع. 72 (2023): ص. 357.

[4] كلاع، (الصراع الروسي ...)، المرجع السابق، ص. 1018.

[5] Joe Robinson, "Cyberwarfare Statistics : A Decade of Geopolitical Attacks", Privacy Affairs, 10 December 2022. Available at the Link :
https://www.privacyaffairs.com/geopolitical-attacks/

الإستراتيجية الحيوية للإقتصاد الروسي لهجمات إلكترونية من الخارج و تعرض موسكو هي الأخرى لهجمات متكررة.

المطلب الـثـاني: التنافس السيبراني الروسي-الأمريكي منذ 2020-2024.

أُعتبرت سنة 2020 بيئة محفزة لزيادة الهجمات السيبرانية، فقد تعرض العالم لجائحة كورونا التي ساهمت في زيادة سرعة تحديث كثير من المجتمعات تكنولوجيًا وزيادة الإعتماد على الأنترنت والتكنولوجيا. في ظل ذلك زادت الهجمات السيبرانية بسبب زيادة العمل عن بعد، إضافة لضعف ثقافة الأمن السيبراني لدى المجتمعات ووجود ثغرات أمنية في العديد من الأنظمة لصعوبة تأمينها بصورة كاملة من الهجمات السيبرانية.[1]

خلال هذه الفترة، تعرضت الولايات المتحدة الامريكية لأكبر هجوم سيبراني، حسب وزير الخارجية الأمريكي السابق "Mike Pompeo" متهما روسيا بذلك. حسب مانشرته وكالة **Reuters**، المهاجمون السيبرانييون زعم أنهم مجموعة «APT29 » * تمكنوا من الوصول إلى البريد الإلكتروني لوزارتي التجارة والطاقة في الولايات المتحدة الأمريكية، بإختراقهم لشركة **FireEye** الأمريكية للأمن السيبراني التي تعمل على صد الهجمات السيبرانية، وتمكن هؤلاء المخترقون من تثبيت برنامج خبيث على تحديث **Solarwinds** أصاب نحو 18 ألف نظام لدى عملاء الشركة. قوبلت هذه الإتهامات بنفي شديد من روسيا مصرحة بأنها رهاب أعمى منها يلوح به عند وقوع أي حادثة. [2]

في حين وزير الخارجية الأمريكية آنذاك وجه أصابع الإتهام لروسيا، إلا أن الرئيس الأمريكي " Donald Trump" الذي كانت ولايته على وشك الإنتهاء كان قد برأ روسيا من هذا الهجوم مضيفا أنها قد تكون الصين

---

* [1] PT 29 المعروفة أيضا بـ : Cozy Bear وThe Dukes مجموعة قرصنة مرتبطة بالحكومة الروسية، يعتقد انها تنشط منذ 2008، تقوم بسرقة المعلومات الحساسة والبيانات المالية والشخصية، وتعطيل الأنظمة والتجسس وجمع المعلومات الإستخباراتية. إستغلت ثغرة في برنامج Solarwinds للوصول إلى أنظمة FireEye الداخلية.
* FireEye: شركة متخصصة في الأمن السيبراني تأسست عام 2004، يقع مقرها الرئيسي في كاليفورنيا، الولايات المتحدة.
* Solarwinds : شركة أمريكية، تطور برمجيات تساعد الشركات على إدارة البنية التحتية لتكنولوجيا المعلومات الخاصة بها.

[1] جمال الدين، المرجع السابق، ص. 212.

[2] "من يقف وراء أكبر هجوم سيبراني في تاريخ أمريكا ؟"، TRTعربي،21 ديسمبر 2020. تم تصفح الموقع يوم: 2024/03/30 متاحة على الرابط.

https://bit.ly/44z6Sds

وراءه. وفي خضم ذلك تعهد الرئيس المنتخب "Joe Biden" في تلك الفترة بجعل الرد على الهجوم السيبراني بشكل عام أولوية قصوى بمجرد توليه منصب الرئاسة. [1]

أما في سنة 2021، تعرضت شركة Microsoft لهجمات سيبرانية استهدفت *Exchange Server، من خلال استغلال ثغرات أمنية في النظام وتم ربط الهجوم بمجموعة Nobelium التابعة للإستخبارات الروسية، حيث قاموا بسرقة بيانات من خلال تقنية *Zero-day، حيث سمحت لهم هذه الثغرات بالوصول إلى مختلف حسابات البريد الإلكتروني لكبار المسؤولين التنفيذيين في الشركة. مما إعتبرته الولايات المتحدة تهديدًا للخدمات الأساسية التي تعتمد عليها الدولة. إلا أن هذه الهجمات هي الأخرى نفتها روسيا مرارًا وتكرارًا رافضة وضع أي هجوم سيبراني على عاتق مسؤوليتها.[2] وجاء ذلك بعد القمة الأمريكية-الروسية في جنيف صيف 2021، التي تناولت قضية القرصنة السيبرانية بين البلدين، حيث قام آنذالك الرئيس الأمريكي "Biden Joe" بإعطاء "Putin Vladimir" قائمة تضم 16 قطاعًا مهمًا وعرفهم على أنهم بنية تحتية للولايات المتحدة الأمريكية لاينبغي إختراقها. [3]

تزامنًا مع التدخل العسكري الروسي في أوكرانيا وفي سنة 2022، تم إستهدافها سيبرانيا من خلال تعطيل العديد من المواقع الإلكترونية الحكومية، وجاء ذلك بعد إبداء الرئيس الأوكراني "Volodymyr Zelensky" رغبته في إنضمام دولته لحلف الناتو، ما إعتبرته روسيا تهديدًا لأمنها القومي خاصة بتوسع حلف الشمال الأطلسي شرقا. وذلك حسب ما قاله المرشح للإنتخابات الرئاسية الامريكية القادمة Robert Kennedy Jr وإعرابه عن أن هذه الحرب هي حرب بالوكالة بين روسيا والولايات المتحدة.[4] وقامت هذه الأخيرة، بفرض عقوبات إقتصادية على روسيا، ماجعلها متخوفة من شن هذه الأخيرة هجمات سيبرانية كرد فعل على تلك

---

[1] المرجع نفسه.

[2] "مايكروسوفت: قراصنة روس يستهدفون سلسلة إمداد التكنولوجيا"، موقع العربيـة، 25 أكتوبر 2021، تم التصفح يوم 2024/04/01، متاحة على الرابط :

https://bit.ly/3yf88ql

* Exchange Server: هو خادم بريد إلكتروني في مايكروسوفت يتيح الإجتماعات للمستخدمين ويسمح بإرسال وإستقبال رسائل البريد الإلكتروني وتتبع المواعيد وإنشاء قوائم المهام.

* Zero-Day : تعني وجود ثغرة أمنية في نظام معين، تعطي القراصنة والمهاجمين فرصة لإستغلالها قبل أن يتم إكتشافها من قبل مطوري البرنامج وإصلاحها.

[3] "على أرض محايدة.. بايدن وبوتين يعقدان أول قمة رئاسية بينهما"، موقع CNN العربية، 16 جوان 2021، تم التصفح يوم 2024/04/01، متاحة على الرابط:

https://arabic.cnn.com/world/article/2021/06/16/biden-putin-first-presidential-summit

[4] "الحرب الأوكرانية هي حرب بالوكالة بين روسيا وأمريكا"، قناة العربية، 07 مارس 2024، متاحة على الرابط:

https://www.youtube.com/watch?v=-59_NDo661U

العقوبات. في المقابل أعلنت الخارجية الروسية أن الولايات المتحدة شنت هجمات سيبرانية على روسيا بأيدي الجيش الإلكتروني الأوكراني الذي أسسته، فقد أشار مدير دائرة أمن المعلومات الدولي في الخارجية الروسية إلى زيادة عدد الهجمات على المواقع الروسية مقارنة بنفس الفترة عام 2021، مشيرًا إلى أن معظم الهجمات الصادرة كانت من أراضي الولايات المتحدة وحلفائها.[1] رغم نفي الولايات المتحدة هي الأخرى قيامها بهجمات ضد روسيا إلا أنها ظلت إحتمالية، هذا مايمكن إعتباره حربا سيبرانية بالوكالة* بين روسيا والولايات المتحدة.

في سنة 2023، كان هناك تبادل للإتهامات بين روسيا والولايات المتحدة، حيث إتهمت وزارة الخارجية الروسية حلف NATO بالتحضير لشن هجمات سيبرانية ضدها مستهدفة مواقع الطاقة ومرافق حيوية. وإتهمت روسيا حلفاء الولايات المتحدة بشن هجمات ضدها ودعمهم لنشاط قراصنة أوكرانيين.[2] أما في بداية سنة 2024، تعرضت Microsoft أيضا لهجوم من قراصنة زعم أنهم مرتبطين بالحكومة الروسية، وإتهامهم بالسعي إلى جمع معلومات استخبارية عبر التجسس على المصالح الخارجية على المدى البعيد[3]. وكانت هناك مخاوف روسية بشأن تدخلات سيبرانية أمريكية في الانتخابات في ظل التوترات والإتهامات المتبادلة بين روسيا والولايات المتحدة الأمريكية، أصدرت المخابرات الروسية بيانًا متهمتة الإدارة الأمريكية بالتحريض لخفض نسبة المشاركين في الإنتخابات، عبر الأنترنت بدعوات لتجاهلها. [4]

---

[1] "روسيا: واشنطن تشن هجمات سيبرانية علينا بأيدي الأوكرانيين"، الشرق الأوسط، 25 أكتوبر 2022، تم تصفح الموقع: 2024/04/01، متاحة على الرابط:

https://bit.ly/3Uy3ISJ

* حرب سيبرانية بالوكالة: شكل حديث من الصراعات الدولية، تعني إستخدام الدول وكلاء لتنفيذ هجماتها السيبرانية، وهذا يحقق للدولة الأصل مصالحها بتكلفة زهيدة، كما يجعل تتبعها ومعرفة مصدرها الأصلي صعبًا، هذا النوع من الحروب يعكس التحديات الجديدة في السياسة الدولية والأمن القومي، تساهم في تحقيق أهداف الدول دون اللجوء للصراع المباشر ما يتيح التهرب من المسؤولية الدولية.

[2] " تبادل الإتهامات... الهجمات السيبرانية تشتعل بين الغرب وموسكو"، موقع skynews عربية، 28 جويلية 2023، تم التصفح يوم 2024/04/01، متاحة على الرابط:

https://bit.ly/4dA15Zl

[3] "مايكروسوفت تتعرض لهجوم من قراصنة مرتبطين بروسيا"، موقع الجزيرة نت، 2 جانفي 2024، تم التصفح يوم 2024/04/1، متاحة على الرابط:

https://bit.ly/3QDNZ3j

[4] فهيم الصوراني، "روسيا تحشد لإنتخاباتها الرئاسية وسط مخاوف من هجمات سيبرانية"، موقع الجزيرة نت، 14 مارس 2024، تم التصفح يوم: 2024/04/01، متاحة على الرابط:

https://bit.ly/4agx0LE

وبالنظر في الإنتخابات الرئاسية الأمريكية المزعم إجراؤها في 05 من نوفمبر 2024، هناك تزايد للمخاوف من تعرضها لهجمات سيبرانية ومحاولة للتأثير من جانب روسيا[1] وإستخدام وسائل التواصل الاجتماعي للتأثير في الرأي العام وزرع الإنقسامات، خاصة في ظل التطور التكنولوجي والإعتماد على الذكاء الإصطناعي المتزايد، لإمكانية إستغلاله في التمويه والتضليل بمحاكاة المعلومات المضللة في شكل نص أو صوت، صورة أو فيديو لجعل الأمر يبدو وكأنه صادر عن سلطة رسمية.[2] وجاء هذا بعد المكالمة المزيفة في محاولة لإنتحال شخصية الرئيس الحالي "Joe Biden" لتحريض الناخبين على عدم التصويت في الإنتخابات التمهيدية في ولاية New Hampshire، فالهجمات السيبرانية على البنية التحتية للإنتخابات الرئاسية تسعى لتقويض سريتها ونزاهتها. كما قدم Dmitry Bridzhe، رؤية تحليلة للوضع بين روسيا والولايات المتحدة في ظل هذه الإنتخابات مبينًا التوجه الروسي لدعم الرئيس الأمريكي السابق دونالد ترامب"Donald Trump"على حساب الرئيس الحالي جو بايدن" Joe Biden" رغم كونه هو الآخر تحديًا لتعارض سياسته أحيانًا مع مصالح روسيا إلا أنه يظل خيارًا أفضل في نظر الرئيس الروسي "Vladimir Putin".[3]

وفي ظل التنافس السيبراني بين روسيا والولايات المتحدة الأمريكية وتبني سياسات هجومية من خلال تبادل الإتهامات وشن الهجمات، لجمع المعلومات والبيانات السرية لكلا الطرفين، واستخدامها في خدمة المصالح الوطنية لكل طرف وتعطيل البنى التحتية وضرب المؤسسات الحكومية والدفاعية لكل دولة. تسعى في المقابل كل منهما لتعزيز سياساتها الدفاعية فضلا عن الهجومية من خلال تعزيز أمنها السيبراني، ومعالجة الثغرات الأمنية في أنظمتها. وعليه كل من روسيا والولايات المتحدة تنتهج إستراتيجية سيبرانية لتحقيق ذلك.

المبحث الثاني: الإستراتيجية الروسية-الأمريكية للتنافس على الهيمنة السيبرانية.

في خضم التوتر المتصاعد بين الولايات المتحدة وروسيا وزيادة حدة المواجهة السيبرانية بينهما في ضوء الإتهامات المتبادلة بتوجيه هجمات إلكترونية على أهداف حيوية مختلفة. يتزامن ذلك مع سعي كلا البلدين

[1] "عاصفة سيبرانية تتجمع فوق الإنتخابات الأمريكية"، أندبندنت عربية، 28 نوفمبر 2024، تم الصفح يوم 2024/04/03، متاحة على الرابط:

https://bit.ly/44x2U5n

[2] "الذكاء الإصطناعي يهدد الإنتخابات الأمريكية .. ماعلاقة روسيا؟"، سكاي نيوز عربية، 09 مارس 2024، تم التصفح يوم: 2024/04/03، متاحة على الرابط:

https://bit.ly/3wuPTws

[3] أندبندنت عربية، المرجع السابق.

لتعزيز أمنهما[1] للمحافظة على بنياتهم التحتية والمعلوماتية ومواجهة أي هجمات محتملة من الطرف الآخر. وذلك بسعي كل من روسيا والولايات المتحدة لإنتهاج إستراتيجيات معينة. وقد شهدت إستراتيجية العمليات السيبرانية الروسية-الامريكية تطورًا ملحوظًا على مدى السنوات القليلة الماضية،[2] حيث لكل منهما دوافع إستراتيجية للخوض في هذه المنافسات السيبرانية، التي تختلف بحسب رؤية ودور صانع القرار. إلا أن الهدف الأسمى والوحيد للتنافس في هذا الفضاء هو تحقيق وتعظيم القوة بما تستدعيه ضرورة أحداث الواقع الدولي الراهنة وحماية الأمن السيبراني، وفرض رؤية كليهما لكيفية تشكيل القواعد والمبادئ الدولية لتنظيم التهديدات المحتملة في الفضاء السيبراني.[3]

المطلب الأول: الإستراتيجية الروسية التنافسية على الهمينة السيبرانية .

تقدم روسيا الإتحادية تحت قيادة الرئيس Vladimir Putin، نموذجا واضحا كأحد الدول التي سعت لتنمية قدراتها في المجال السيبراني خلال السنوات القليلة الماضية وتطويرها كسلاح فعال لمواجهة خصومها في مقدمتهم الولايات المتحدة وحلفائها، وفي إدارة تفاعلاتها الدولية والإقليمية وسعيها لإستعادة مجدها والهيمنة على هذا الفضاء. وجعل الأمن السيبراني على قائمة الأولويات في إستراتيجيتها، لإقرارها أن التهديدات المستقبيلة ستكون سيبرانية.[4] في ماي 2018، تم تأسيس وزارة التنمية الرقمية والإتصالات ووسائل الإعلام في الإتحاد الروسي، لتنظيم وتنفيذ سياسة الدولة في هذا الشأن، وتم تخصيص قسم الأمن السيبراني كقسم تابع للوزارة يتحمل مهام إدارة المشاريع في مجال الأمن السيبراني وإدارة الإجراءات التي تحجب التهديدات السيبرانية وذلك في إطار تحقيق الإستقرار وضمان أمن وسلامة البنية التحتية المعلوماتية.[5]

---

[1] أماني عصام محمد، "إستخدام روسيا للقوة السيبرانية في إدارة تفاعلاتها الدولية"، مجلة كلية الإقتصاد والعلوم السياسية، م. 22، ع. 04 (أكتوبر 2021): ص ص. 168، 169.

[2] ديميتري بريجع، "تصاعد الصراع السيبراني... روسيا والغرب في مواجهة إلكترونية متصاعدة"، مركز الدراسات العربية والأوراسية، 15 مارس 2024، تم تصفح الموقع يوم 2024/03/26، متاحة على الرابط:

https://bit.ly/3QC4DjO

[3] كلاع، (الصراع ...)، المرجع السابق، ص. 1019.

[4] نهى علي أمير، "الأمن السيبراني في إستراتيجية الأمن القومي الروسي"، آفاق آسيوية، م. 07، ع. 11 (مارس 2023): ص. 171.

[5] ميار عادل فتحي عبد الحميد وآخرون، "دور القيادة الروسية في تعزيز الأمن السيبراني 2012-2023"، المركز الديمقراطي العربي، 22 جوان 2023.

https://democraticac.de/?p=90695#google_vignette

كما أنشأت وكالة أبحاث الأنترنت أو ما يعرف بجيش المتصيدين "ARMY Troll " تابع لوكالة الأمن الإتحادي الروسي، يضم آلاف الموظفين ويتم التخصيص له حوالي 300 مليون دولار سنويا من ميزانية الدفاع الروسي.[1]

وفي 2018/09/10، أنشأ جهاز الأمن الفيدرالي الروسي مركزًا وطنيًا لتنسيق مكافحة الهجمات السيبرانية على البنية التحتية الحيوية في روسيا، لتولي مهام الكشف والوقاية والقضاء على تداعيات الهجمات السيبرانية وتبادل المعلومات بين الهيئات المختصة في الداخل والخارج، وتحليل الهجمات الماضية وتطوير أساليب مكافحتها، وجار العمل على فصل روسيا كلها على الأنترنت بهدف زيادة فاعلية دفاعاتها ضد الهجمات الإلكترونية والقرصنة، حيث أن تداول البيانات بين المواطنين والمؤسسات في هذه الحالة سيكون داخل البلاد لا عن طريق مراكز توجيه دولية. [2]

ويتجلى ذلك في إعتزامها من خلال منظمة البريكس وضع أنترنت مستقلة وموازية لشبكة الأنترنت الحالية، ببناء البرازيل منظومة كابلات بإمكانها ربط روسيا، والصين، والهند وجنوب إفريقيا بطول 34 ألف كيلومتر، بربط عدة مدن من هذه الدول فضلا عن قدرة توفير خدمات الأنترنت في 21 دولة إفريقية. [3]

وكان البرلمان الروسي قد وافق في 12 فيفري 2019 على قانون عزل البلاد عن شبكة الأنترنت العالمية، بهدف جعل البلاد في موقع أفضل لصد أي هجمات إلكترونية محتملة من الخارج خاصة من الولايات المتحدة الأمريكية. وكان ذلك مماثلا للنظام الرقابي الصيني على الأنترنت Great firewall لتعزيز السيادة الوطنية.[4]

حيث ترتكز الرؤية الإستراتيجية الروسية على استخدام مصطلح "أمن المعلومات" كبديل عن الأمن السيبراني بإعتباره مصطلحا شاملا وهذا الأخير جزء تابع له، وتأكيدها على أهميته بإعتباره أحد الجوانب الأكثر استخداما للدول الأخرى لإختراق القاعدة الأمنية والمعلوماتية لروسيا.[5] حيث تسعى روسيا لبناء معايير دولية لتعزيز القدرات في مجال مواجهة التهديدات الداخلية لأمن المعلومات أو مواجهة التهديدات الخارجية، تعتمد عقيدتها الأمنية السيبرانية على تطبيق السيادة الوطنية على الفضاء السيبراني، لذا فإن السيادة السيبرانية ودور الدولة

[1] قطوش، المرجع السابق، ص. 294.

[2] عصام محمد، المرجع السابق، ص. 169.

[3] المرجع نفسه، ص. 174.

[4] "موسكو : البرلمان يوافق على عزل روسيا عن شبكة الأنترنت العالمية"، 12 فيفري 2019، تم التصفح يوم 2024/03/29، متاحة على الرابط،

https://alnqabialjanubi.com/archives/768

[5] عادل فتحي عبد الحميد وآخرون، المرجع السابق.

https://democraticac.de/?p=90695#google_vignette

في مجال المعلومات والتنظيم والسيطرة هي مرتكزات أساسية لإستراتيجية الأمن السيبراني.[1] ووفقا للعقيدة الروسية للإستراتيجية السيبرانية فهي تعمد إستخدام الأسلحة السيبرانية الهجومية بإعتبارها قوة مضاعفة (Multiplied Strength) في الحروب لزيادة القدرات القتالية للدولة إلى جانب القدرات العسكرية. [2]

فعند تحليل البنود الخاصة بالأمن السيبراني في إطار إستراتيجية الأمن الروسي يتبين أن في الإستراتيجية الصادرة في 2021، زاد الإهتمام بالأمن السيبراني ومع تجديد كل إستراتيجية يتزايد الاهتمام به وتزداد البنود الخاصة به. ولذلك يتزايد الإهتمام بتعظيم القوة السيبرانية، فالغاية الروسية في وجهة نظر الرئيس الروسي Putin هي إزاحة الأحادية القطبية ونزع الهيمنة الأمريكية من الفضاء السيبراني وصعود روسيا كقوة عظمى في هذا المجال. [3]

فالإستراتيجية الروسية تهدف لجعل الدولة الروسية قادرة على مواجهة التهديدات المتزايدة وذلك بتحقيق مستوى من الإنتاج التكنولوجي يحاكي التطور الحادث في الواقع الدولي، وإدراكها لمخاطر وأسباب التهديدات والهجمات السيبرانية المستمرة من قبل الدول الخصوم ومن قبل الشركات التكنولوجية العالمية.[4] في إطار ذلك قدمت روسيا إلى اللجنة الخاصة في الأمم المتحدة مشروع إتفاقية بشأن مكافحة الجرائم السيبرانية ومحاولة الإقتراح الروسي لوضع قواعد السلوك المتبعة في الفضاء السيبراني ولإستبدال إتفاقية بودابست لعام 2001 والتي ترفضها روسيا وتعتبرها تهديدًا مباشرًا لسيادتها، لسماح هذه الإتفاقية لأجهزة الإستخبارات الغربية بالوصول اللامتناهي إلى قواعد البيانات الإلكترونية لسائر الدول وخاصة مايتعلق بالمادة 32 والتي تسمح لأصحاب البيانات بالسيطرة على إستخدامها بدلا من الحكومات. [5]

وقد أدلى Dmitry Polyanskiy نائب رئيس الوفد الروسي في الأمم المتحدة بتصريح حيال رفض الولايات المتحدة منح تأشيرات لممثلي روسيا في منتدى الأمم المتحدة لأمن المعلومات، دليل على رغبتها في الهيمنة على هذا المجال ما يؤثر على وضع إتفاقية مكافحة الجريمة السيبرانية، مؤكدًا على تأييد روسيا وضع معاهدة شاملة ذات نطاق واسع تتوافق مع مشروع إتفاقيتها.[6] لذلك تسعى روسيا تحت قيادة الرئيس Vladimir Putin

---

[1] كلاع،(الصراع ...)، المرجع السابق، ص. 1022.

[2] قطوش، المرجع السابق، ص. 295.

[3] عادل فتحي عبد الحميد وآخرون، المرجع السابق.

[4] المرجع نفسه.

[5] عادل عبد الصادق،" صراع السيادة السيبرانية بين التوجهات الروسية و الأمريكية"، المركز العربي لأبحاث الفضاء الإلكتروني، تم التصفح يوم: 2023/03/29. متاحة على الرابط:

https://accronline.com/print_article.aspx?id=29415

[6] "موسكو: رغبة الولايات المتحدة في الهيمنة تتعارض مع مشروع مكافحة الجرائم الإلكترونية"، 21 أوت 2023، تم التصفح يوم: 01 أفريل 2024، متاحة على الرابط:

نحو مواجهة مشروع الأحادية الأمريكية بدعوتها لإقامة نظام عالمي متعدد الأقطاب ورغم دعوتها للتعددية القطبية إلا أنها تتحرك في الوقت نفسه في إطار بناء قوتها الذاتية دون الدخول في مواجهة مباشرة مع الولايات المتحدة. [1] ووفقا لتقييم التهديدات السنوي لمجتمع الإستخبارات الأمريكي فإن روسيا ستشكل تهديدا سيبرانيا عالميا مستمرا بإعتبارها أن التشويشات السيبرانية سياسة خارجية لتشكيل قرارات الدول الأخرى واستخدام قدراتها في التجسس والتأثير والهجوم بشكل مستمر ضد مجموعة متنوعة من الأطراف. فهي تحافظ على قدرتها لإستهداف البنية التحتية الحيوية بما في ذلك الكابلات تحت الماء وأنظمة التحكم الصناعي في الولايات المتحدة وحلفائها.[2]

المطلب الثاني: الإستراتيجية الأمريكية التنافسية على الهيمنة السيبرانية.

في المجال الزمني للدراسة تقدم الولايات المتحدة تحت قيادة كل من الرئيس السابق الأمريكي دونالد ترامب Donald Trump والرئيس الحالي جو بايدن Joe Biden نموذجا واضحا كأحد الدول التي سعت ولاتزال تسعى لتعظيم قدراتها في المجال السيبراني والحفاظ على دورها المهين في هذا الفضاء وتشكيله وحمايته إنطلاقا من قناعة مفادها أن الولايات المتحدة هي المنشئة للأنترنت ولابد من أن تحافظ على هيمنتها عليها. [3]

وتعد الإستراتيجية السيبرانية لإدارة دونالد ترامب Donald Trump أول إستراتيجية مفصلة للولايات المتحدة منذ 2003 (فترة إدارة الرئيس الأسبق جورج بوش الإبن)، وفقا لبيان مجلس الأمن القومي لتحديدها الأولويات الحاسمة للحفاظ على المصالح الأمريكية في الفضاء السيبراني وإتاحتها القيام بالعمليات السيبرانية الهجومية ضد خصومها وتخفيف قواعد إستخدام الأسلحة السيبرانية لحماية البلاد من هجمات سيبرانية لا تهدد فقط الديمقراطية الأمريكية، لكن المؤسسات الإقتصادية والأمنية الأمريكية والتي تؤثر حتما على قيادتها للنظام الدولي الذي أسسته وهيمنتها عليه.[4]

ففي إطار سعي الولايات المتحدة لفرض هيمنتها وفرض قواعد السلوك في الفضاء السيبراني ترى أن الإقتراح الروسي بشأن مشروع إتفاقية الأمم المتحدة لمكافحة الجرائم السيبرانية كمحاولة لإستبدال إتفاقية بودابست

---

https://bit.ly/4aeIcbD

[1] عادل فتحي عبد الحميد وآخرون، المرجع السابق.

[2] Office of the Director of National Intelligence, Annual Threat Assessment of the U.S Intelligence Community (5 February 2024): p. 16.

[3] عمرو عبد العاطي، "إستراتيجية أمريكية هجومية ضد التهديدات السيبرانية"، المركز المصري للفكر والدراسات الإستراتيجية، 31 أكتوبر 2018، تم التصفح يوم 14 فيفري 2024، متاحة على الرابط:

https://ecss.com.eg/2077/

[4] المرجع نفسه.

2001 التي وقعت عليها الولايات المتحدة إلى جانب 55 دولة أخرى بأنها ستعزز من قدرات روسيا وغيرها من البلدان السلطوية في الإتصالات في الداخل وفي بلدان أخرى، فالولايات المتحدة ترى أنه لا حاجة لتدخل الحكومات في هذا الفضاء السيبراني وأن للقطاع الخاص دور مركزي في ذلك. [1]

تعتبر الإستراتيجية السيبرانية الأمريكية أن الفضاء السيبراني يجب أن يعزز من التفوق العسكري بمعنى التركيز على تعزيز وتعظيم القدرات العسكرية إلى جانب تعزيز القدرات السيبرانية وممارسة الأنشطة الإستخباراتية وحماية الأمن القومي والعمل على ردع القوى الدولية المنافسة ومواجهة سرقة الأسرار الصناعية وتهديد البنية التحتية المعلوماتية والنظام الديمقراطي ....، والعمل على ذلك من خلال:

- تعزيز وضمان القدرة السيبرانية للجيش الأمريكي لكسب الحروب والإستجابة السريعة للهجمات السيبرانية المؤثرة على مصالح الولايات المتحدة.
- السعي لشن هجمات إستباقية لحماية البنية التحتية المعلوماتية وإعتماد أسلوب الدفاع إلى الأمام من خلال ضرب مصادر الخطر خارج الحدود قبل أن تصل إلى الداخل. [2]

كما جاءت الإستراتيجية الأمريكية في عهد ترامب في إطار السعي لإنشاء فرع سادس للجيش الأمريكي والتركيز على الفضاء السيبراني لتحقيق الهيمنة في هذا الفضاء بإعتباره ساحة جديدة للحروب المستقبلية، بتبادل المعلومات وزيادة صلاحيات وزارة الدفاع لرقابة جهود الأمن السيبراني ومكافحة الجرائم السيبرانية بالتعاون مع حلفائها لمحاولة تحديد مصدرها. [3] وقد صدرت هذه الإستراتيجية بعد تقرير صادم لمكتب المحاسبة الحكومي الأمريكي في سبتمبر 2018 عن حالة الأمن السيبراني داخل الولايات المتحدة منتقدًا غياب إستراتيجية أمريكية شاملة للأمن السيبراني، مايجعل الوكالات الفيدرالية والبنية التحتية الحيوية للبلاد عرضة للخطر مع تنامي التهديدات الأمنية وتعقدها.[4]

فقد عززت واشنطن من دفاعاتها السيبرانية حيث أنشأت القيادة السيبرانية الأمريكية United States Cyber Command وتعرف إختصارا بـ USCYBERCOM مجموعة عمل خاصة لمواجهة أنشطة روسيا في الفضاء السيبراني،[5] تخضع هذه القيادة للإشراف المباشر من قبل مساعد وزير الدفاع الأمريكي وتتولى

[1] عبد الصادق، (صراع السيادة...)، المرجع السابق.

[2] المرجع نفسه.

[3] قطوش، المرجع السابق، ص. 292.

[4] عبد العاطي، المرجع السابق.

[5] عصام محمد، المرجع السابق، ص. 169.

هذه القيادة مسؤولية إدارة شبكات الحاسوب في كل أصناف الجيش الأمريكي ويتمثل دورها المحوري في مجال تأمين الحماية الإلكترونية لها والقيام بهجمات سيبرانية إستباقية ضد الخصوم.[1]

حيث وقع الرئيس الأمريكي السابق Donald Trump مرسوما في 2018/08/16 ألغى بموجبه التوجيه الرئاسي لسلفه Barack Obama لتنظيم إستخدام الأسلحة السيبرانية ضد معارضي الولايات المتحدة الأمريكية المعروفة باسم الأمر التنفيذي20 (PPD 20) * التي أصدرها Barack Obama في أكتوبر 2012 وظل مضمونها سريا إلى أن تم الكشف عن تسريبات إدوارد سنودن Edward Snowden الموظف السابق في وكالة الامن القومي الأمريكي في 2013[2] و التي نشرت بواسطة صحيفة الغارديان البريطانية The Guardian والتي تتيح للحكومة الأمريكية القدرة على المراقبة والتنصت من خلال مراقبة الشبكات والأنظمة الإلكترونية التي أعتبرت إنتهاكا للخصوصية، ألغاها الرئيس السابق **دونالد ترامب** Trump Donaldعلى النحو الذي يعطي الوكالات الأمريكية مزيدًا من الحرية لشن هجمات سيبرانية دفاعية وهجومية دون الحاجة للحصول على موافقة مسبقة.[3]عند قيام أي دولة بنشاط سيبراني ضدها يكون الرد بطريقة هجومية ودفاعية ولن يتم بالضرورة في الفضاء السيبراني وتتبنى إستراتيجية قائمة على الهجوم الدفاعي والتحرك إلى الأمام خارج الحدود وإختراق شبكات الخصم وتعزيز القدرات لجمع المعلومات الإستخباراتية والإستعداد للصراعات المستقبلية. [4]

وانعكست شخصية الرئيس الأمريكي السابق **دونالد ترامب** Trump Donald على إستراتيجيته،[5] كونه رجل إقتصادي عمدت إستراتيجيته إلى تعزيز الاقتصاد الأمريكي الرقمي، بتشجيع الإبتكار في قطاع التكنولوجيا والذكاء الإصطناعي بالإضافة إلى بناء قوة عاملة حكومية في مجال الأمن السيبراني من خلال توظيف المتخصصين في هذا المجال في المؤسسات الحكومية، والدعوة إلى حرية الأنترنت في جميع أنحاء العالم وتزويد حلفائها بقدرات سيبرانية للتعامل مع التهديدات السيبرانية المستهدفة لمصالحهم المشتركة. [6]

---

[1] عبدالله محمد، الفادني، المرجع السابق، ص. 67.

* PPD 20 : Presidential Policy Directive 20 تم التوقيع عليه من قبل الرئيس باراك أوباما يوفر إطارا للأمن السيبراني الأمريكي يركز على إدخال الأدوات السيبرانية في الجهود الأمنية الوطنية.

[2] قطوش، المرجع السابق، ص. 291.

[3] كلاع، (الصراع الصيني....)، المرجع السابق، ص. 1020.

[4] عبد الصادق، (صراع السيادة.....)، المرجع السابق.

[5] يحيى سعيد قاعود، علا عامر الجعب، وثيقة الأمن القومي الأمريكي 2017، قراءة تحليلية في إستراتيجية دونالد ترامب، في مجلة قراءات إستراتيجية، تحرير. بسيسو. مطيع، والطيبي. أحمد. (غزة: مركز التخطيط الفلسطيني، 2018)، ص. 35.

[6] قطوش، المرجع السابق، ص. 292.

أما الإستراتيجية في عهد الرئيس الحالي **جو بايدن** Biden Joeجاءت منتقدة لإستراتيجية الرئيس السابق **دونالد ترامب** Trump Donald يإعتبار أنها فشلت في إعطاء الأولوية للأمن السيبراني لإلغائه العديد من المناصب السيبرانية رفيعة المستوى فقد أعاد وظيفة مجلس الأمن القومي السيبراني التي ألغاها الرئيس السابق **دونالد ترامب** Donald Trump، وقام بملء ذلك الفراغ الذي خلفته إدارة سلفه.[1] كما تم إنشاء كتيبة هجومية جديدة للعمليات السيبرانية في 2021 تقدم الدعم للقوات الإلكترونية للجيش الأمريكي للحماية والدفاع عن البلاد من الهجمات الإلكترونية. [2]

فأصدر أمرًا تنفيذيًا يؤكد ضرورة تبادل المعلومات حول التهديدات السيبرانية وتحديث الأمن السيبراني عبر وحدات الحكومة الفيدرالية، كما وقع في عام 2022 قانون الإبلاغ عن الحوادث السيبرانية للبنية التحتية الحرجة (Cyber Incident Reporting For Critical Infrastructure Act of 2022) CIRCIA والذي يتطلب من وكالة الأمن السيبراني وأمن البنية التحتية CISA * تطوير وتنفيذ اللوائح التي تتطلب من الكيانات المعنية الإبلاغ عن الحوادث السيبرانية[3] في غضون 72 ساعة، ومدفوعات برامج الفدية في غضون 24 ساعة.[4]

على الرغم من الأن الإدارات السابقة أولت إهتماما بالتأثير الهائل للتهديدات السيبرانية والعمل على سبل مواجهتها إلا أن إدارة بايدن قد تكون أول إدارة أمريكية مدركة لأهمية الأمن السيبراني وتشجع على أكبر قدر من الإنسجام والتنسيق بين سياسات الأمن السيبراني وإستراتيجية الأمن القومي بإشراك القطاع الخاص في سياسات الدفاع السيبراني وقامت بإجراءات لإعادة هيكلة المؤسسات لمواجهة التهديدات السيبرانية من خلال الكشف عنها وتبادل المعلومات، إلى جانب فرض عواقب صارمة على الجهات المتورطة في شن الهجمات بأي شكل من الأشكال.[5]

---

[1] "الإختراق والحرب الإلكترونية كيف تتصدى إدارة بايدن للخطر؟"،19 قناة الحرة، أفريل 2022، تم التصفح يوم 2024/04/14، متاحة على الرابط

https://arbne.ws/3wEOFP8

[2] قطوش، المرجع السابق، ص. 292.

[3]* ISA: Cybersecurity and Infrastructure Security Agency، وكالة الأمن السيبراني وأمن البنية التحتية هي وكالة حكومية أمريكية تعمل تحت إشراف وزارة الامن الداخلي مهمتها تعزيز الامن السيبراني في الولايات المتحدة وتقديم الممارسات السيبرانية لمساعدة الأفراد وإعطاء تدابير وقائية لإدارة المخاطر السيبرانية.

سارة عبد العزيز،" كيف تتعامل إدارة بايدن مع تهديدات الأمن السيبراني؟"، مركز المستقبل للأبحاث والدراسات المتقدمة، 20 مارس 2024، تم التصفح يوم 16 أفريل 2024.

https://bit.ly/3UZNRxV

[4] Vivek Mishra, Sameer Patil, "Decoding the Biden Administration's Cyber Security Policy", ORF Issue Brief, N°686 (January 2024): p. 20.

[5] عبد العزيز، المرجع السابق.

في مارس 2023، إقترحت إدارة Joe Biden إستراتيجية وطنية لتعزيز الأمن السيبراني ومواجهة التهديدات في هذا الفضاء، فقد حددت مجموعة التهديدات التي تتطلب إهتماما فوريا وشملت هجمات الفدية المستهدفة للبنية التحتية الوطنية الحيوية والتجسس السيبراني، وأقرت هذه الإستراتيجية أن التهديدات يمكن أن تعطل الأمن القومي والإستقرار الإقتصادي والسلامة العامة.[1] وخاصة مع الطبيعة المتصلة للبنية التحتية الوطنية الحيوية وإنتشار أجهزة الأنترنت الذكية وتزايد المهاجمين السيبرانيين المستغلين للثغرات التي خلقها المنهج التقليدي الردعي للأمن السيبراني، أدى إلى ضرورة وجود إستجابة سريعة وشاملة. [2]

وقد شكلت هذه الإستراتيجية لحظة محورية في نهج الولايات المتحدة في التعامل مع التهديدات السيبرانية، حيث إعترفت بنقائص السياسات السابقة وشدة التهديدات المتصاعدة، وأنه لابد من نهج إستباقي وشامل وأن يكون تعاوني بين القطاعين العام والخاص لتحقيق الأمن السيبراني.[3] بمعنى أنه لا يعزز الدفاع ضد التهديدات الحالية فقط بل يجعل الولايات المتحدة في موضع يسمح لها بمعالجة/ مواجهة المخاطر الناشئة بشكل إستباقي.[4]

كما تتبع إستراتيجية الرئيس الحالي جو بايدن Joe Biden نهج الثقة المعدومة Zero Trust Approach وهو نهج يشير إلى نموذج أمن سيبراني يقر بأن التهديدات موجودة في كل مكان وعلى كل مستوى وأن كل شخص وكل شيء داخل النظام المتصل مشتبه به، لذلك فالطريقة الوحيدة هي التحقق المستمر والتوكيل لكل عنصر في نظام الأمن السيبراني فهي تقوم على التجزئة بمعنى تقسيم الشبكات إلى أجزاء للحد من إنتشار التهديدات. في هذا النهج يتحول التركيز من تأمين نقاط الدخول في النظام المتصل بالشبكة إلى حماية البيانات. [5]

ويضع نهج الثقة المعدومة دورة مستمرة من التحقق والتفويض، وأثناء الإنتقال نحو نهج الثقة المعدومة أنشأت إدارة الرئيس **جو بايدن** Joe Biden نموذج نضج الثقة المعدومة Zero Trust Maturity Model (ZTMM) لتوجيه الوكالات الحكومية في جعل أنظمة الحواسيب الخاصة بها أكثر أمنا ومعرفة مدى تقدمها في نهج الثقة المعدومة. [6]

[1] Mishra, Patil, ibid., p. 16.
[2] Mishra, Patil, ibid., p. 17.
[3] Ibid.
[4] عبد العزيز، المرجع السابق.
[5] Mishra, Patil, ibid., p. 17.
[6] Ibid., p. 18.

من أجل إنجاح هذه الإستراتيجية قدر الإنفاق في سنة 2023 على القدرات السيبرانية وتكنولوجيا المعلومات للجيش الأمريكي بـ 16.6 مليار دولار،[1] ومن المتوقع أن ينمو إلى 26.75 مليار دولار في عام 2028،[2] كما يبلغ إجمالي الإنفاق على ميزانية الدفاع الأمريكي لسنة 2024، 886 مليار دولار بتخصيص 842 مليار دولار لوزارة الدفاع الأمريكية البنتاغون و44 مليار دولار للبرامج المتعلقة بالدفاع في مكتب التحقيقات وميزانية سنة 2024 تزيد 28 مليار دولار عن 858 مليار دولار ميزانية العام الماضي.

في إطار التأكيد على أهمية هذا الفضاء وسعي كل من روسيا والولايات المتحدة الأمريكية لفرض هيمنتهما عليه قدمت **الباحثة إبتسام عبد الزهرة العقبي**، مفادها أن الصراع سيكون حسب التطور التكنولوجي من خلال علاقته بالمجالات الجغرافية الأخرى التي يغطيها (البر، البحر، الجو، والفضاء) وعليه فإن نتيجة التوجه التكنولوجي يتجه نحو عولمة العالم إقتصاديا، وثقافيا، وسياسيا وجعل مركز القلب له، ليصبح نقطة التحكم والتوجيه في المستقبل، ما سيدفع إلى وضع نظرية أخرى للتطبيق مستقبلا:

- أن من يحكم المعرفة، ويمتلكها، ويحسن استخدامها، سيهيمن على الفضاء السيبراني.
- وأن من يتحكم بالفضاء السيبراني سيتحكم بالمجالات الأربعة الأخرى.
- ومن يحكم هذه المجالات سيحكم وسيهيمن على العالم. [3]

وهذه النظرية تبين الدور والأهمية التي يحظى بها الفضاء السيبراني في الوقت الحالي حيث أصبح بمثابة قاعدة كبرى تضم جميع الميادين الأربعة.

وعليه لابد من الإشارة إلى أن أي نظام سيبراني لأي دولة مهما بلغت قوتها ومكانتها ومهما طورت إستراتيجية أمنها السيبراني يمكن إختراقه وتعرضه لمختلف التهديدات السيبرانية مع الأخذ بعين الإعتبار إختلاف القدرة الدفاعية للدول تجاه هذه التهديدات، إلا أن إمكانية إختراقه تبقى مطروحة لسرعة وإستمرارية تطور البرامج والأسلحة السيبرانية. [4]

---

[1] عزالدين قطوش ، المرجع السابق، ص. 291.

[2] "سوق الأمن السيبراني العسكري- النمو والإتجاهات وتأثير Covid-19 والتوقعات 2024-2029"، تم التصفح يوم 2024/04/16، متاحة على الرابط

https://www.mordorintelligence.com/ar/industry-reports/military-cybersecurity-market

[3] كلاع، (الصراع الصيني....)، المرجع السابق، ص ص . 1013، 1014.

[4] فاتح حارك ورياض حمدوش، "الدولة بين الهمينة وتحقيق الامن في الفضاء السيبراني"، المجلة الجزائرية للأمن الإنساني، م. 07، ع. 01 (جانفي 2022): ص. 137.

الفصل الثالث: تأثير التنافس السيبراني الروسي–الأمريكي على الأمن العالمي ومستقبله:

طغت التهديدات العسكرية التقليدية على القرن العشرين، بينما شهد القرن الواحد والعشرين سيادة التهديدات الأمنية غير التقليدية بما في ذلك الإرهاب والجريمة العابرة للحدود والحروب الأهلية وتدهور البيئة وعدم الأمان المعلوماتي/السيبراني. من بين هذه التهديدات يعتبر التهديد السيبراني الأكثر تطورا وتعقيدا، بسبب نقص القواعد الدولية التي تحكم وتنظم العلاقات بين الدول في هذا الفضاء الفوضوي، ولإنتشار التطور التكنولوجي والمعلوماتي عبر المجتمعات وبروز الأنترنت كظاهرة عالمية الأمر الذي استلزم زيادة في إعتماد المجتمع على هذه التكنولوجيا، ما أدى في نهاية المطاف إلى أن يشكل هذا المجال السيبراني عنصرًا أساسيًا في الأنشطة التشغيلية للدول في المجالات الاجتماعية، الاقتصادية، السياسية والعسكرية، ونظرًا للإستخدام الإيجابي والسلبي للتكنولوجيا يوفر هذا الفضاء فرصا لتحسين وتسهيل الحياة وفي الوقت نفسه يشكل تهديدات خطيرة للأمن الفردي والوطني والعالمي. [1]

المبحث الأول: واقع تأثير التنافس السيبراني الروسي– الأمريكي على الأمن العالمي.

في إطار سعي كل من روسيا والولايات المتحدة الأمريكية لفرض هيمنتهما على الفضاء السيبراني، ولأهميته الكبيرة في الوقت الحالي، من خلال إنتهاج كل منهما إستراتيجيات هجومية ودفاعية لمواجهة التغييرات والتحديثات في مجال القرصنة تنشأ دورة تنافسية. مع ترابط العالم بشكل مروع بسبب التفشي الهائل للأنترنت. حيث كشفت أحدث دراسة لموقع Statista، أنه من أفريل 2024 قدر عدد مستخدمي الأنترنت بـ: 5.44 مليار مستخدم مما يمثل % 67.1 من سكان العالم، ومن هذا المجموع قدر عدد مستخدمي مواقع التواصل الاجتماعي بـ: 5.07 مليار مستخدم أي ما يعادل 62.6% من سكان العالم.[2]

هذا مايتيح إمكانية وسرعة الوصول للعديد من البيانات السرية، والقدرة على إختراق العديد من المراكز والوكالات الحكومية والدفاعية لجمع المعلومات الحساسة والتأثير على النتائج السياسية وبالتالي التأثير فيما هو إجتماعي. كما أن إرتباط الإقتصاد العالمي بالفضاء الإلكتروني حيث تتم الملايين من العمليات المالية والتجارية اليومية من خلاله، فالفضاء السيبراني أصبح جزءً لا يتجزأ من عمل مختلف المرافق الحيوية هذا ما يزيد من مكانته وخطورته في الوقت نفسه وتأثيره على الأمن العالمي.

[1] Muhammad Riaz Shad, " Cyber Threat in Interstate Relations: Case of US-Russia Cyber Tensions", Policy Perspectives, Vol. 15, N°. 2, (2018): p. 41.
[2] Ani Petrosyan, "Number of Internet and Social Media Users World Wide as of April 2024", Statista, seen 08 May 2024, available at the link:
https://www.statista.com/statistics/617136/digital-population-worldwide/

المطلب الأول: واقع تأثير التنافس السيبراني الروسي–الأمريكي على البعد الإقتصادي والعسكري.

تستخدم روسيا والولايات المتحدة القوة السيبرانية لتحقيق الأهداف العسكرية سواء من خلال تحقيق الردع السيبراني والسعي لتحقيق أقصى درجات الأمان لشبكة الأنترنت الداخلية لهما وتعزيز الأمن القومي مما يتيح الكشف السريع لأماكن الإختراق والتعرف على مصادرها، أو من خلال الهجمات السيبرانية الخارجية التي تُشَّنُ لتحقيق الأهداف العسكرية.[1] مثال ذلك الحرب الروسية على أوكرانيا ونجاحها في توظيف إستراتيجيتها السيبرانية إلى جانب قواتها العسكرية وضم العديد من الأقاليم (دونيتسك ولوغانسك، خيرسون...)، باعتبارها قد أصبحت حرب سيبرانية بالوكالة بين روسيا والولايات المتحدة بسبب الدعم السيبراني الذي تقدمه الولايات المتحدة لأوكرانيا من خلال مشاركتها معلومات استخباراتية حول عمليات القرصنة السيبرانية التي تقوم بها الخدمات الاستخباراتية الروسية، لمساعدتها في تحسين دفاعاتها السيبرانية وتقديم الدعم التقني.[2]

وتتمثل ميزة هذا الأمر في أنه يربط الوحدات العسكرية بالأنظمة العسكرية الإلكترونية، والسماح بسهولة تبادل المعلومات وتدفقها والقدرة على إصابة الأهداف عن بعد، إلا أن هذا الأمر يجعل من خطر تعرض هذه الوحدات أو الأنظمة العسكرية لإختراق خارجي من خلال ثغرات في النظام العسكري والتعرض للتجسس أو التلاعب بالبيانات والأنظمة العسكرية، وإمكانية إعادة توجيه الأسلحة وذلك بالسيطرة على الطائرات المسيرة أو إسقاطها قبل الوصول لهدفها ضد أهداف وهمية أو ضد حليف [3] أمرًا حتميًا.

كما تعد التكنولوجيا أساس المعاملات المالية والإقتصادية، نظرًا لزيادة إعتماد الشركات على المنصات الرقمية. ورغم محاولة روسيا والولايات المتحدة استخدام القوة السيبرانية بما يخدم مصالحها الإقتصادية وحتى العسكرية للحفاظ على أمنها السيبراني والحفاظ على البنى التحتية والمؤسسات التي تتحمل مسؤولية الحفاظ على الأمن الداخلي والإقتصاد.[4] إلا أن استمرارية التطور التكنولوجي يؤدي إلى وجود عدد كبير من الثغرات في الأنظمة السيبرانية وإمكانية استغلال هذه الفجوات لتنفيذ أضرار على منظمة معينة بطرق مختلفة. هذا قد يؤثر على الناحية المالية من جهة أو من حيث توقف العمل من جهة أخرى.[5] ونظرا لإرتباط البنى التحتية لشبكات الطاقة والمؤسسات المالية وأنظمة النقل.... الخ بالتكنولوجيا يجعلها عرضة للإختراق.

---

[1] خليفة، المرجع السابق، ص.197.

[2] Office of the SPOKESPERSON, "U. S Support for Connectivity and Cybersecurity in Ukraine", U.S Department of State, 10 May 2022, seen 25 April 2024, available at the link: https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/

[3] خليفة، المرجع السابق، ص. 197.

[4] Emile S Mbung Kala," Critical Role of Cyber Security in Global Economy", Open Journal of Safety Science and Technology (25 December 2023): p. 231.

[5] Kala, op cit., p. 232.

وأحد الأسباب الرئيسية لأهمية الأمن السيبراني في الإقتصاد العالمي هو تأثيره المحتمل على الإستقرار المالي. الزيادة في الهجمات السيبرانية المستهدفة للمؤسسات المالية وأنظمة الدفع لا تتسبب في تعطيل عمليات المؤسسات فقط بل تجعل البيانات الحساسة للعملاء ومعلومات بطاقات الإئتمان عرضة للخطر. كما تؤدي الهجمات السيبرانية إلى عواقب إقتصادية خطيرة، وتصبح سرقة الملكية الفكرية عائقا أمام الإبتكار والقدرة التنافسية بين الدول وتجعل تصاميمَ المنتجات الجديدة وعمليات الإنتاج والإستراتيجيات التسويقية والصناعات الدوائية عرضة للسرقة من قبل دول منافسة. [1]

الطبيعة المترابطة للإقتصاد العالمي الحديث تجعل تأثير هجوم سيبراني واحد ذو تداعيات إقتصادية بعيدة المدى، فالهجوم السيبراني على نظام بنية تحتية حيوية مثل شبكات الكهرباء أو شبكات النقل يؤدي إلى تعطيل وإيقاف الأنظمة الإقتصادية عبر عدة دول. مثال ذلك إدعاء الولايات المتحدة تعرضها لهجوم سيبراني صادر عن مجموعة Killnet في 10 من أكتوبر 2022 وإتهام روسيا بذلك وإعتباره كرد فعل على العقوبات المفروضة عليها بسبب حربها على أوكرانيا، استهدف هذا الهجوم مطارات أمريكية ورغم أن الأنظمة التي أُستهدفت كانت غير مسؤولة عن مراقبة الحركة الجوية ولم تتعطل الرحلات [2] إلا أن إحتمالية حدوث هجمات سيبرانية من هذا القبيل ما قد يسبب تأخيرًا في الرحلات الجوية وخسائر مالية لشركات الطيران والمسافرين تبقى مطروحة.

كما نجد أن التكلفة السنوية للهجمات السيبرانية في سنة 2024 تقدر بـ: 9,5 تريليون دولار والتي تزيد بنسبة % 19 عن سنة 2023، كما أنه من المتوقع أن يبلغ إجمالي الضرر الناتج عن الهجمات السيبرانية حوالي 12,4 تريليون دولار في سنة 2027. [3]

المطلب الثاني: واقع تأثير التنافس السيبراني الروسي–الأمريكي على البعد السياسي والإجتماعي.

تُسَخِّر كل من روسيا والولايات المتحدة القوة السيبرانية للتجسس وجمع المعلومات الحساسة لتحقيق أمنها القومي ومصالحها الإستراتيجية، وهو نشاط موجود منذ القدم وقد أُستخدم في زمن السلم والحرب، إلا أن

[1] Mohammed B. E. Saaida, "The Use of Cyber Warfare and its Impact on International Security", Science for All Publications, Vol. 01, N°. 01 (July 2023): p. 2.

[2] " تقارير عن تعرض مطارات كبرى لهجوم سيبراني روسي"، قناة Euronews بالعربية، 10 أكتوبر 2022، تم التصفح يوم: 30 مارس 2024، متاحة على الرابط:

https://arabic.euronews.com/2022/10/10/cyberattacks-reported-at-us-airports-killnet-russia-pro-russian-hacker-group

[3] Atika Lim,"The True Cost of Cyber Attacks in 2024 and Beyond", 05 February 2024, available at the link:
https://www.expressvpn.com/blog/the-true-cost-of-cyber-attacks-in-2024-and-beyond/

التكنولوجيا قد طورت من أساليبه وطرقه، أصبح بفضل التطور التكنولوجي التجسس على ملايين الأفراد والعديد من الدول أمرا سهلا، وما كشفته قضية Snowden خير دليل على ذلك.

لا يمكن إنكار أن كلا البلدين يقومان بجمع المعلومات من خلال وسائل سيبرانية، لكنهما يختلفان حول معايير استخدام هذه المعلومات، بينما تلتزم الولايات المتحدة الأمريكية في الحفاظ على سرية المعلومات إلا أن روسيا تستغلها لتحقيق حرب المعلومات وتستخدمها في سياق الهجمات السيبرانية كجزء من الحرب الهجينة ضد الغرب [1]وتشمل 3 أهداف:

- جمع المعلومت الحساسة من خلال العمليات السيبرانية.
- نشر الدعاية للتلاعب في الرأي العام.
- استغلال المعلومات لزعزعة السلطات الحكومية.

لأن النشاط السيبراني الذي يهدف إلى حرب المعلومات يكون مدفوعا سياسيًا.[2] وقد تستخدم هذه المعلومات للتأثير على النتائج السياسية في الغرب، مثل التدخل الروسي المزعوم في الإنتخابات الأمريكية لسنة 2016، فالهدف من هذه الهجمات السيبرانية هو التأثير على قرارات وتصورات الدول الأخرى بما يخدم المصالح، أو يمكن أن يكون الهدف نشر الدعاية ونشر المعلومات لغرض تقويض وهدم مصداقية المؤسسات السياسية وتعزيز الإنقسامات داخل الدول المستهدفة .[3]

هذا ما له تأثير على البعد الاجتماعي، من خلال مايعرف باسم العمليات النفسية، وهي جانب من الهجمات السيبرانية تهدف للتركيز على التلاعب بالرأي العام، كون الطبيعة المترابطة للأنترنت وإنتشار وسائل التواصل الإجتماعي، خلقت بيئة محفزة ومساعدة على سرعة إنتقال المعلومة وإنتشارها. وتشكيل الرأي العام على نطاق عالمي والتأثير على العقول، وتدرك كل من روسيا والولايات المتحدة أهمية هذه المنصات وقوتها في الدعاية وتوجيه الرأي العام، واستخدامها لتحقيق أهدافها ومصالحها دون مواجهة عسكرية مباشرة وذلك من خلال:

- حملات التضليل: نشر المعلومات الزائفة أو المضللة عن طريق بث الأخبار الوهمية والكاذبة على وسائل التواصل الاجتماعي لخلق نوع من الإرتباك وزرع الإنقسامات.
- البروباجندا السيبرانية: سواء كانت على شكل مقالات أو فيديوهات ومنشور على مواقع التواصل الاجتماعي لتعزيز حيثيات معينة وأيديولوجيات تتماشى مع أهداف الدولة التي تشن الهجمات

[1] Shad, op cit., p. 52
[2] Ibid., p.47.
[3] Ibid., p.52.

السيبرانية. كما حدث في ثورات الربيع العربي فقد لعبت هذه المنصات دورًا مهمًا وتعتبر نموذجا لنقل الحشد الإفتراضي على أرض الواقع.[1]

وبالحديث على مواقع التواصل الاجتماعي يعني الحديث على أكبر خمس شركات أمريكية الـ *GAFAM والتي أصبحت تعرف بالـ *GAMAM، فقد تبين في العقد الأخير أن لها تأثيرًا واسعًا بإعتبار أنها الوسيلة الأولى للتواصل وتبادل المعلومات.[2] كما أن قواعد البيانات الكبيرة التي جمعتها الـ GAFAM، تثير مخاوف بشأن خصوصية المستخدمين وأمان بياناتهم في ظل التنافس السيبراني وإمكانية الإختراق والحصول على البيانات، ولعل فضيحة Cambridge Analytica في 2018 خير دليل على ذلك بتسليطها الضوء على إمكانية استغلال المعلومات الشخصية والتأثير على السلوك العام والإنتخابات. خاصة أن هناك إدعاءات بشأن استخدام البيانات المأخوذة في إنشاء إعلانات سياسية والتأثير في الانتخابات الأمريكية في 2016.[3]

مع التطور الحادث في الواقع الدولي والإعتماد المتزايد على التكنولوجيا من قبل الدول والمؤسسات الحكومية والسياسية الأمر الذي يسهل المشاركات الإنتخابية من خلال الإنتخاب والقيام بالإستفتاءات الشعبية عن بعد. فالترابط التكنولوجي في المؤسسات السياسية رغم تسهيله لعدة أمور إلا أن الثغرات الناتجة عن التطور الرهيب في الفضاء السيبراني تخلق فرصا للخصوم للتلاعب بالرأي العام ونشر المعلومات المضللة، ما يؤدي إلى تقويض شرعية العمليات والمؤسسات السياسية، ويؤثر كل هذا على البعد الإجتماعي بفقدان المجتمع ثقته في النظام السياسي ومسؤوليه والتخوف بشأن بياناتهم ومعلوماتهم الشخصية لإمكانية استغلالها.

على الرغم من قلة الوقائع السيبرانية الفعلية بين روسيا والولايات المتحدة بالتحديد خلال فترة الدراسة، إلا أن التطورات السريعة التي تحدث في هذا الفضاء وسعي كل منهما لحماية أمنهما وفرض رؤيتهما على القواعد المنظمة لسلوك الدول في الفضاء السيبراني واستخدام قدراتهم السيبرانية للمساس بالبنى التحتية للدول الخصوم، فضلا عن ترابط العالم بسبب الأنترنت يجعل من إحتمالية حدوث العديد من الهجمات والإختراقات السيبرانية

---

[1] Giovanni Cadioli,"The Evolution of Cyber Conflicts and its Impact on International Security: A Comprehensive Analysis" (Thesis paper, School of Economics and Political Science, University of Padua, Italy, Academic year 2023/2024), p. 58.

*GAFAM: Google, Amazon, Facebook, Apple, Microsoft.

*GAMAM: Google, Amazon, Meta, Apple, Microsoft.

[2] عبد الرحمان عادل، " التقنيات السيبرانية والسيطرة على السوق من ينتج ومن يستهلك؟"، قضايا ونظرات، ع. 23 (أكتوبر، 2021): ص. 39.

[3] "The Rise of GAFAM: Investing in The Future of Technology", Faster Capital, 21 April 2024, seen 06 May 2024, Available at the link: https://fastercapital.com/content/The-Rise-of-GAFAM--Investing-in-the-Future-of-Technology.html

المماثلة والتي تشكل تهديدًا للأمن العالمي أمرًا حتميًا. وظهور تكنولوجيا المعلومات، خاصة مع إنتشار الأنترنت الذي قام بتغيير ديناميكيات الأمن العالمي بطرق لم يسبق لها مثيل. فما بدأ كميزة تكنولوجية تربط الناس والأفكار عبر الحدود تطور وأصبح سلاحا ذو حدين يقدم فرصًا وضعفًا على نطاق عالمي،[1] وما بدأ كتجربة فضولية من طالب دراسات عليا مع دودة موريس في 1988 تحول إلى مجال معقد ومتعدد الجوانب الدولية ومتعدد الأدوات من تجسس وتنافس... إلخ.[2]

المبحث الثاني: مستقبل التنافس السيبراني الروسي– الأمريكي.

في إطار دراسة وتوقع مستقبل التنافس السيبراني الروسي–الأمريكي تم إقتراح 3 سيناريوهات:

السيناريو التصاعدي والذي يشير إلى زيادة حِدَّة التنافس السيبراني بينهما.

السيناريو التنازلي والذي يشير إلى إنحسار حِدة المنافسة بينهما في المجال السيبراني.

سيناريو استمرار الوضع القائم الذي يدل على استمرار الأوضاع الحالية.

المطلب الأول: السيناريو التصاعدي.

بالنظر للتوترات السيبرانية بين الولايات المتحدة وروسيا نجد أنها ركزت على الإختراقات والتجسس للحصول على المعلومات وعلى الرغم من عدم إمكانية معرفة مصادرها بصورة قطعية، إلا أن القضية السيبرانية العميقة وطويلة الأمد بين البلدين تتعلق بالهجمات السيبرانية التي يمكن أن تحدث في حالة نشوب نزاع مسلح بشكل صريح، وعليه من المتوقع أن يشهد التنافس السيبراني الروسي–الأمريكي تصاعدًا في ظل توفير أنترنت الأشياء البيئة المناسبة لذلك. حيث قال مايكل روجرز Michael Rogers ، المدير السابق لوكالة الأمن القومي (2014–2018)، أن الدول الأجنبية بما في ذلك روسيا تسعى للوصول إلى البنية التحتية للولايات المتحدة والحصول على المعلومات لاستخدامها في حالة ما إذا قرروا بشكل محتمل فعل شيء ما.[3] وفي ظل تزايد حدة التنافس بينهما ليس من المرجح أن تتراجع حرب المعلومات بينهما، في ظل إصرار روسيا على نفوذها التقليدي على دول إرثها السوفييتي، وأي تقدم للغرب تجاه هذه المناطق واستقطابها يدفع بها لتبني أسلوب الحرب الهجينة (Hybrid warfare) وهي مزيج من الأدوات التقليدية وغير التقليدية في تعاملها مع الغرب وخاصة مع إمكانية اللجوء إلى الخيار العسكري التقليدي في التعامل مع الولايات المتحدة وحلفائها.[4]

---

[1] Cadioli, op cit., p. 4.
[2] Ibid., p. 29.
[3] Shad, op cit., p. 53.
[4] محمد بسيوني،" عقيدة جيراسيموف: دوافع الإستراتيجية الروسية لحرب المعلومات ضد الدول الغربية"، مركز المستقبل، 23 أكتوبر 2017، تم الصفح يوم 10 مارس 2024، متاحة على الرابط:

https://bit.ly/4dwyjsC

كما أن الإستعمال المتزايد للقدرات السيبرانية يثير مخاوف بشأن إمكانية بروز سباق الأسلحة السيبرانية كما كان عليه الحال إبان الحرب الباردة، بإستثمار الدول بشكل كبير في الحصول على هذه القدرات للتفوق على منافسيها، والتخوف بشأن إمكانية أن يتجاوز هذا الإعتماد المتسارع وتطوير القدرات السيبرانية، تطوير التدابير الأمنية في المقابل.[1]

المطلب الثاني: السيناريو التنازلي.

أما في ما يخص السيناريو التنازلي، يمكن القول أنه بإعتبار الهجمات السيبرانية التي تشنها دولة على أخرى هي سمة متكررة في السياسة العالمية في القرن 21، واستخدام الدول الفضاء السيبراني لأغراض التجسس وغيرها من الوظائف منذ بزوغ عصر الأنترنت. فكل من روسيا والولايات المتحدة الأمريكية تستخدمان الهجمات السيبرانية لتحقيق أهداف سياسية وإقتصادية وعسكرية بشكل أسرع وأكثر فعالية مما يمكن تحقيقه من خلال العقوبات الإقتصادية أو العمليات العسكرية وبأقل قدر من العواقب. [2] وعليه يتوقع هذا السيناريو أن يشهد التنافس السيبراني الروسي–الأمريكي تراجعا، خاصة بعد تعليق وزير الخارجية الروسي سيرغي لافروف **Serguei Lavrov** في أفريل 2022 حول الهجمات السيبرانية قائلا:" فيما يتعلق بحوكمة الأنترنت والأمن السيبراني أعتقد أنه أصبح واضحا للجميع سواء كانوا مسؤولين سياسيين أو خبراء مهنيين، أنه دون إتفاقية عالمية تنظم عمليات الفضاء الرقمي، فإن العالم سيقبل على فوضى سيبرانية، ستكون كارثية العواقب على الإقتصاد والأمن الدولي".[3] يؤكد ضرورة عقد إتفاقية لتنظيم سلوك الدول المتبع في هذا الفضاء وأن غيابها له عواقب وخيمة.

كون فعالية إستراتيجية مبدأ الردع ضعيفة في الفضاء السيبراني، والدور البارز الذي تلعبه التهديدات السيبرانية في العلاقات الدولية تجعل من الفضاء السيبراني مسرحا محتملا للصراع أو على الأقل مصدرًا للتوترات بسبب غياب قواعد لضبط سلوكها فيه مقارنة بوجود القواعد والقوانين المحددة لضبط علاقات الدول في الفضاء المادي.[4] ووجود دليل تالين الذي يعتبر غير ملزم إلا أنه يعتبر دليلا موثوقا على تطبيق القانون الدولي على العمليات السيبرانية ووجود العديد من المحاولات لضبط سلوك الدول في هذا الفضاء[5] يسلط الضوء على ضرورة إدراج إتفاقية لتنظيم فوضوية الفضاء السيبراني رغم التحديات الكبيرة التي تواجهها بشأن التفسيرات المختلفة

---

[1] Cadioli, op cit., p. 90.

[2] "Cyber Conflict Around the Globe", Johns Hopkins University, seen 27/04/2024, Available at the link:
https://cyberheatmap.isi.jhu.edu/

[3] فيروز زياني،" للقصة بقية، الحرب السيبرانية... حرب صامتة ميادينها الحواسيب وشبكة الأنترنت"، قناة الجزيرة، 17 أكتوبر 2022، متاحة على الرابط:
https://www.youtube.com/watch?v=bZkqS6R7_xw

[4] Shad, op cit., p.46.

[5] Cadioli, op cit., p. 7.

للدولتين لما يسمح به وما يشكل سلوكًا غير شرعي في الفضاء السيبراني ما يجعل وضع قانون لتنظيم هذه السلوكات وتطوير معايير وقواعد واضحة في هذا الفضاء أمرًا صعبًا وتحديًا يؤرق كاهل المجتمع الدولي.[1]

فالتعاون بين الدول في هذا المجال يعزز إمكانية وضع إتفاقية دولية منظمة للفضاء السيبراني، ومحاولة الإتفاق بين روسيا والولايات المتحدة بشأن تحديد ما يعتبر سلوكًا مقبولاً وما يعد تهديدًا، كذلك العمل على تجنب اِستخدام الأسلحة السيبرانية الهجومية والإكتفاء بتقوية تقنيات الدفاع السيبرانية لكلا الدولتين يؤدي إلى التخفيف من حدة التوتر بينهما.

المطلب الثالث: سيناريو استمرار الوضع القائم.

يتوقع هذا السيناريو أن يشهد التنافس السيبراني الروسي–الأمريكي إستمرارًا على وضعه الحالي، وما يعزز هذا الطرح هو إدراك كل منهما خطورة تزايد حدة التنافس في ظل حدوث التطورات السريعة في الفضاء السيبراني، والتحديات التي تفرضها المنافسة على الهيمنة عليه وعواقبها على الأمن العالمي. كما أن إشكالية عدم وجود ثقة إستراتيجية بينهما تثير شكوك كل دولة تجاه الأخرى وجعلها محط أنظارها. إذ أن العقيدة السيبرانية المختلفة لكل منهما لتحقيق مصالحهما تحول دون وجود معاهدة دولية أو إتفاقية دولية لتنظيم السلوك الدولي في هذا الفضاء بسبب المصالح المتضاربة لكليهما.[2]

في ضوء ما تم عرضه من معلومات حول التنافس السيبراني بين روسيا والولايات المتحدة الامريكية، وبالنظر إلى العوامل التي تم طرحها سابقًا تم ترجيح أن السيناريو التصاعدي هو الأكثر واقعية وإحتمالية للحدوث، وذلك لعدة أسباب تم ذكرها في مايلي:

- التطور السريع الذي يحدث في هذا الفضاء السيبراني والذي يتسبب في إضعاف القدرات الدفاعية للدولتين وبالتالي يخلق ثغرات لإختراق البنى التحتية الحيوية لكليهما، يجعل من فكرة تطوير تقنيات دفاعية قوية وعدم استخدام الهجمات السيبرانية مستحيلة الحدوث حاليا. فكل دولة تتحرك وفق مصالحها وبما أن الفضاء السيبراني هو فضاء الحروب المستقبلية يؤدي ذلك إلى سعي كل منهما لتعزيز أمنهما السيبراني وزيادة شن الهجمات السيبرانية والتجسس على بعضهما البعض. حيث نجد تفسير نظرية توازن الدفاع والهجوم لذلك، والتي تقوم فكرتها على تكاليف الدفاع والهجوم، فالدول تلجأ للهجوم إذا كانت تكاليفه أقل من الدفاع وتلجأ للدفاع إذا كانت تكاليف الهجوم أعلى من الدفاع. وعليه تلجأ الدول لشن هجمات سيبرانية على بعضها البعض كونها تعد ذات تكلفة منخفضة نسبيًا في هذا الفضاء بغرض تحقيق مكاسب مختلفة.[3]

---

[1] Ibid., p. 19.

[2] Shad, op cit., p. 53.

[3] حارك وحمدوش، المرجع السابق، ص. 137.

- خلق مسألة الخوف والشعور بعدم الثقة واللذان هما مكونان من صميم المعضلة الأمنية، حيث يرى Waltz وMearsheimer إمكانية وجود تعاون في ظل الفوضى إلا أن تحقيقه والمحافظة عليه أكثر صعوبة، ففكرة وجود إتفاقية لتنظيم سلوك الدول في هذا الفضاء وتحديد ما الذي يسمح به وما يشكل تهديدًا يمكن حدوثها لكن يبقى من الصعب تحقيقها والمحافظة عليها وتواجهها تحديات كبيرة، أولها تخوف الدولتين من قيام الأخرى بالإخلال بتعهدها في تلك الإتفاقية وأن تحرز إحداهما تقدمًا على الأخرى. [1] إضافة إلى صعوبة وضع أدلة نهائية لمصدر الهجمات السيبرانية.[2]

[1] قسوم، المرجع السابق، ص. 71.

[2] Shad, op cit., p. 54.

الخـاتـمـة

إن الإعتماد المتزايد للدول على الفضاء السيبراني وبإعتباره مجالا خامسا فضلا عن المجالات الأربعة السابقة (البر، البحر، الجو والفضاء) ونظرًا لتحول الكل نحو التكنولوجيا الرقمية خاصة مع الذكاء الإصطناعي (AI) وأنترنت الأشياء (IoT) أدى هذا إلى زيادة أهميته في الوقت الراهن، وفي خضم ذلك تسعى كل من روسيا والولايات المتحدة الأمريكية لفرض الهيمنة عليه وحماية أمنها من خلال تعظيم قدراتها وقوتها السيبرانية.

تم إثبات فرضية أن كل من روسيا والولايات المتحدة تنتهجان إستراتيجيات دفاعية وهجومية في إطار سعيهما لتعزيز أمنهما السيبراني وتحقيق الهيمنة على هذا الفضاء من خلال التطرق إلى الإستراتيجيات المُنْتَهَجة والتي تختلف حسب رؤية ودور صانع القرار، فرغبة روسيا لإزاحة الغرب عن هيمنته على التكنولوجيا والأنترنت عائد إلى رؤية الرئيس الروسي فلاديمير بوتينPutin Vladimir بضرورة إستعادة مجد روسيا الإتحادية ومواكبة التغييرات العالمية، من خلال تبني إستراتيجية دفاعية والعمل على عزل روسيا عن الأنترنت العالمي وفرض سيادتها الوطنية عليها؛ وإنشائها لعدة مراكز ووكالات أبحاث للتصدي للهجمات السيبرانية وإنتهاج إستراتيجية هجومية من خلال شن هجمات سيبرانية خارجية. وفي المقابل تسعى الولايات المتحدة لفرض هيمنتها على هذا الفضاء إنطلاقا من فكرة مفادها أنها هي من أنشأت الأنترنت ولابد من المحافظة على هيمنتها عليها وذلك من خلال إنتهاجها هي الأخرى سياسات دفاعية بإنشائها للفرع السادس للجيش الأمريكي في عهد الرئيس السابق دونالد ترامب Donald Trump، والعمل على الرد على الأنشطة السيبرانية بطرق هجومية ودفاعية وليس بالضرورة في الفضاء السيبراني، أما إستراتيجية الرئيس الحالي جو بايدن Joe Biden سعت لتعزيز سياسات الدفاع السيبراني من خلال إنشاء قوات دعم إلكترونية وإصدار قوانين الإبلاغ عن الهجمات السيبرانية والعمل على ربط الوحدات الحكومية والدفاعية لزيادة سرعة تبادل المعلومات حول التهديدات السيبرانية للإستجابة والتصدي لها في أسرع وقت ممكن وإنتهجت إستراتيجيته نهج الثقة المعدومة بمعنى التشكيك في كل ماهو متصل بالنظام والتحقق المستمر. وبينما ترى روسيا أنه من الضروري تدخل الحكومات في الفضاء السيبراني وأن للدولة دور مركزي، تعتبر الولايات المتحدة أنه لا حاجة للتدخل الحكومي وأن للقطاع الخاص دور في هذا الفضاء؛ وعلى غرار وجود إستراتيجية دفاعية إلا أن هناك أفضلية للهجوم على الدفاع خاصة أن تكاليف الهجوم في الفضاء السيبراني منخفضة؛ مع ميزة عدم القدرة على معرفة المصادر الأصلية للهجمات.

فإدراك كل من روسيا والولايات المتحدة أهمية الهيمنة والسيطرة على هذا الفضاء السيبراني الذي سيصبح مجالا للتنافس والصراعات والحروب المستقبلية فيصبح من يتحكم في المعلومة والمعرفة التكنولوجية يتحكم في هذا الفضاء ومن خلاله يحكم المجالات الأربعة وبالتالي سيهيمن على العالم، هذا ينشأ دورة تنافسية بين الدولتين لفرض هيمنتهما عليه خاصة وأنه في ظل التطور السريع يستحيل وجود نظام سيبراني لدولة ما غير قابل للإختراق مهما بلغت قوتها.

وفي ظل الطبيعة المترابطة للفضاء السيبراني وميزة سرعة الوصول للمعلومات وتسهيل المعاملات على كافة الأصعدة إلا أن الدورة التنافسية بينهما على الهيمنة السيبرانية تلقي بظلالها على الأمن العالمي وكلما زاد التنافس بينهما كلما تزايد تأثيره على الأمن العالمي وتسببه بعواقب وخيمة على مختلف الأبعاد: العسكرية من خلال فكرة السيطرة على الطائرات المسيرة وتوجيهها ضد أهداف وهمية أو حليفة. الإقتصادية بإختراق للبنى التحتية لمختلف شبكات النقل وتعطيلها أو التلاعب بالمؤسسات المالية وتأثير ذلك على عدة دول أخرى نظرًا للطبيعة المترابطة للفضاء السيبراني. السياسية عن طريق التجسس على بعضهما البعض وجمع المعلومات الحساسة وإستخدامها للتأثير على قرارات وتصورات الدول وللتأثير على الانتخابات. الاجتماعية بالقيام بما يعرف بالعمليات النفسية خاصة في ظل إنتشار مواقع التواصل الاجتماعي وسهولة التأثير على العقول والتخوف بشأن المعلومات والبيانات الخاصة بالمستخدمين. مع صعوبة وجود إتفاقية دولية في الوقت الحالي لتنظيم قواعد السلوك في الفضاء السيبراني لغياب الثقة بين كلا الدولتين وصعوبة تطوير دفاعات قوية وتأمينها بصورة كلية حاليا؛ يصبح من المرجح زيادة التنافس السيبراني بينهما في السنوات القليلة القادمة مع عدم القدرة على الجزم بالوضع الذي سيكون بينهما في هذا الفضاء نظرا لتطوره الهائل بصورة مستمرة وسريعة.

تم التوصل في هذه الدراسة إلى النتائج التالية:

1. الهيمنة السيبرانية مكونة من مفهومين؛ الهيمنة والفضاء السيبراني، وتعني الهيمنة سيطرة مجموعة على أخرى وغالبا ما تكون هذه المجموعة مدعومة بمعايير وأفكار شرعية لتصبح شائعة وبديهية. كما تعرف وزارة الدفاع الأمريكي الفضاء السيبراني بأنه مجال تستخدم فيه الإلكترونيات وتخزين وحفظ البيانات وتعديلها وتبادلها عن طريق أنظمة شبكات الإتصال والبنى التحتية المرتبطة بها ويعتبر مجالًا حيويا وجيوستراتيجيا يخاض فيه العديد من الهجمات والحروب الرقمية. فالهيمنة السيبرانية تعني قدرة دولة أو مجموعة من الدول على فرض السيطرة على الفضاء السيبراني بإعتباره مجال الصراعات والحروب المستقبلية وتتمثل في القوة السيبرانية التي تمتلكها الدولة في هذا الفضاء وتسعى لتعظيمها لتحقيق الأمن السيبراني وبالتالي تعزيز الهيمنة السيبرانية.
2. الأبعاد الدولية للهيمنة السيبرانية تتمثل في أهميتها في الواقع الدولي فالتفوق في الفضاء السيبراني في الوقت الحالي أصبح جزءًا أساسيًا لأمن الدول لتوسع إستخدام الأنترنت والأجهزة الذكية وزيادة الإعتماد على التكنولوجيا.
3. إدراك روسيا والولايات المتحدة الأمريكية أهمية هذا الفضاء ورغبتهما في الهيمنة عليه خلق نوعا جديدًا من الحرب الباردة بينهما من خلال إنتهاجهما إستراتيجيات دفاعية وهجومية مرتبطة بالعقيدة الإستراتيجية ووجهة نظر ورؤية صناع القرار لكلتا الدولتين.
4. رغم مزايا هذا الفضاء لتوفيره فرصًا لتحسين الحياة وتسهيلها إلا أن سرعة وإستمرارية تطوره وطبيعته المترابطة تنشأ دورة تنافسية بين كل من روسيا والولايات المتحدة وتأثيرها على الأمن العالمي على

مختلف الأبعاد العسكرية، الاقتصادية، السياسية والإجتماعية، لإمكانية إختراق الوحدات العسكرية والبنى التحتية الحيوية وشبكات الطاقة وأنظمة النقل وصعوبة تأمينها بصورة كلية. وفي ظل إنتشار مواقع التواصل الاجتماعي يصبح من السهل التلاعب بالرأي العام وزرع الإنقسامات وتقويض المؤسسات السياسية في الدول من خلال حملات التضليل والبروباجندا السيبرانية وسرعة إنتشارها في هذه البيئة. كما أن القدرة على التجسس وجمع المعلومات الحساسة وإستغلالها لحقيق مصالحهما الإستراتيجية دون مواجهة مباشرة يضعف ثقة المجتمع بنظامه السياسي والتخوف بشأن إمكانية إستغلال بياناتهم ومعلوماتهم.

5. في الوقت الراهن يصعب التعاون بين الدولتين لوضع إتفاقية لتنظيم سلوك الدول في هذا الفضاء وتبقى فكرة وضعها ممكنة لكن يصعب تحقيقها والمحافظة عليها في ظل فوضوية الفضاء السيبراني والشعور بالشك وعدم الثقة بين الدول فضلا عن طبيعته المتسارعة التي تجعل من فكرة تطوير تقنيات دفاعية غير قابلة للإختراق غير ممكنة التحقيق حاليا.

قـــائـمـــة المـــصـــادر والمـــراجـــع

المراجع باللغة العربية:

❖ الكتب:

1. بن سالم البادي، سعيد وآخرون. الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها. د.ط. عمان: مجمع البحوث والدراسات، 2016.
2. سعيد قاعود، يحيى وعامر الجعب، علا. وثيقة الأمن القومي الأمريكي 2017، قراءة تحليلية في إستراتيجية دونالد ترامب. في مجلة قراءات إستراتيجية، تحرير. بسيسو، مطيع والطيبي، أحمد. غزة: مركز التخطيط الفلسطيني، 2018.
3. عبد الصادق، عادل. أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني. ط. 2. القاهرة: المركز العربي لأبحاث الفضاء الإلكتروني، 2016.
4. قسوم، سليم. الإتجاهات الجديدة في الدراسات الأمنية دراسة في تطور مفهوم الأمن في العلاقات الدولية. ط. 4. أبوظبي: مركز الإمارات للدراسات والبحوث الإستراتيجية، 2021.
5. خليفة، إيهاب. القوة الإلكترونية كيف يمكن أن تدير الدول شؤونها في عصر الأنترنت؟ الولايات المتحدة نموذجا. ط. 1. القاهرة: العربي للنشر والتوزيع، 2017.

❖ المجلات العلمية:

1. إبراهيم سلمات الشمري، مصطفى. " الأمن السيبراني وأثره في الأمن الوطني العراقي". مجلة العلوم القانونية والسياسية، م. 10، ع. 01 (2021): ص ص . 149- 190.
2. بونعلرة، ياسمين. " الجريمة الإلكترونية". مجلة المعيار، م. 20، ع. 39 (2015): ص ص. 273- 314.
3. بوستي، توفيق." مدرسة كوبنهاغن نحو توسيع وتعميق مفهوم الأمن". مركز المعهد المصري للدراسات، دراسات إستراتيجية،(22 مارس 2019): ص ص. 1-23.
4. جمال الدين، هبة. " الأمن السيبراني والتحول في النظام الدولي". مجلة كلية الاقتصاد والعلوم السياسية، م. 24، ع. 01 (يناير 2023): ص ص. 189- 230.
5. دريسي، حنان. " الحروب السيبرانية: تحول في أساليب القتال وثبات في المبادئ والأهداف". مجلة الفكر القانوني والسياسي، م. 06، ع. 01 (2022): ص ص. 909- 922.
6. زروقة، إسماعيل. " الفضاء السيبراني والتحول في مفاهيم القوة والصراع". مجلة العلوم القانونية والسياسية، م. 10، ع. 01 (أفريل 2019): ص ص. 1016- 1031.
7. حارك، فاتح و حمدوش، رياض. " الدولة بين الهيمنة وتحقيق الأمن في الفضاء السيبراني". المجلة الجزائرية للأمن الإنساني، م. 07، ع. 01 (جانفي 2022): ص ص. 130- 151.

8. حسين، حياة. " الفضاء الإلكتروني وتحديات الأمن العالمي". مجلة العلوم القانونية والسياسية، م. 12، ع. 01 (أفريل 2021): ص ص. 1066- 1089.
9. حربي ذاري، هديل. " قوة الفضاء السيبراني في ساحة صراع جديدة بين القوى الدولية والإقليمية في القرن 21". قضايا سياسية، ع. 72 (2023): ص ص. 338- 367.
10. طه محمد، جاسم. " التهديدات السيبرانية وإنعكاساتها على الأمن القومي الأمريكي". مجلة تيكريت للعلوم السياسية، م. 02، ع. 32 (2023): ص ص. 178- 229.
11. كلاع، شريفة. " الأمن السيبراني وتحديات الجوسسة والإختراقات الإلكترونية للدول عبر الفضاء السيبراني". مجلة الحقوق والعلوم الإنسانية، م. 15، ع. 01 (2022): ص ص. 292- 314.
12. كلاع، شريفة. " الصراع الروسي- الصيني- الأمريكي للإستحواذ على الهيمنة في الفضاء السيبراني". مجلة السياسة العالمية، م. 06، ع. 01 (2022): ص ص. 1009- 1028.
13. عادل، عبد الرحمان. " التقنيات السيبرانية والسيطرة على السوق من ينتج ومن يستهلك؟". قضايا ونظرات، ع. 23 (أكتوبر 2021): ص ص . 39- 46.
14. عبد العظيم محمد عبد الجواد، أميرة. " المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام". مجلة الشريعة والقانون، ع. 35، ج. 03 (2020): ص ص. 363- 541.
15. عبد الصبور عبد الحي، سماح. " القوة السيبرانية في العلاقات الدولية: دراسة في الحروب السيبرانية بالتطبيق على عام 2020". مركز الحضارة للدراسات والبحوث، قضايا ونظرات، ع. 21 (أبريل 2021): ص ص. 93- 105.
16. علي أمير، نهى. " الأمن السيبراني إستراتيجية الأمن القومي الروسي". آفاق آسيوية، م. 07، ع. 11 (مارس 2023): ص ص. 168- 196.
17. عصام محمد، أماني. " إستخدام روسيا للقوة السيبرانية في إدارة تفاعلاتها الدولية". مجلة كلية الاقتصاد والعلوم السياسية، م. 22، ع. 04 (أكتوبر 2021): ص ص. 167- 190.
18. عثمان، أحمد. " الحروب السيبرانية وأثرها في العلاقات الدولية روسيا والولايات المتحدة الأمريكية نموذجا". مجلة الجامعة العراقية، ع. 59، ج. 02 (2023): ص ص. 460- 474.
19. فرحات، علاء الدين. " الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين". مجلة العلوم القانونية والسياسية، م. 10، ع. 03 (ديسمبر 2019): ص ص. 88- 107.
20. صالحي، نصيرة. " القوة الذكية: التنافس العالمي على قوة الفضاء الإلكتروني والقدرات السيبرانية". دفاتر السياسة والقانون، م. 13، ع. 01 (2021): ص ص. 374- 385.

21.قطوش، عز الدين." الحرب الباردة الأمريكية– الروسية في الفضاء السيبراني". مجلة مدارات سياسية، م. 07، ع. 02 (2023): ص ص. 287– 300.

22.شنوف، زينب، " الحرب السيبرانية في العصر الرقمي حروب مابعد كلاوزفيتش". المجلة الجزائرية للأمن التنمية، م. 09، ع. 02 (جويلية 2022): ص ص. 89– 103.

23.خليل، بشار. " الحرب السيبرانية، الأهداف، الردع، الدفاع". المجلة العلمية السورية للمعلوماتية، ع. 155 (أكتوبر 2022).

❖ الرسائل الجامعية:

1. عبد الله محمد، رؤى والفادني، الطاهر محمد. " أثر التنافس السيبراني الأمريكي–الروسي على الأمن العالمي في الفترة 2015– 2022م (رسالة ماجستير غير منشورة، جامعة النيلين، الخرطوم، 2022).

❖ المواقع الإلكترونية:

1. الصوراني. فهيم، " روسيا تحشد لإنتخاباتها الرئاسية وسط مخاوف من هجمات سيبرانية". موقع الجزيرة، 14 مارس 2024.

https://bit.ly/4agx0LE

2. أنصر سفاح. كريم." الحروب الإلكترونية وأثرها على الامن القومي".قسم الدراسات التكنولوجية والامن السيبراني، مركز النهرين للدراسات الإستراتيجية.

https://www.alnahrain.iq/post/1031

3. بالة، صباح." مدرسة كوبنهاغن في تفسير الدراسات الأمنية". الموسوعة السياسية. 9 ديسمبر 2020.

https://bit.ly/3WzJYkv

4. بسيوني، محمد. "عقيدة جيراسيموف: دوافع الإستراتيجية الروسية لحرب المعلومات ضد الدول الغربية". مركز المستقبل، 23 أكتوبر 2017.

https://bit.ly/4dwyjsC

5. بريجع، ديميتري،" تصاعد الصراع السيبراني... روسيا والغرب في مواجهة إلكترونية متصاعدة". مركز الدراسات العربية والأوراسية، 15 مارس 2024.

https://bit.ly/3QC4DjO

6. زياني، فيروز." للقصة بقية، الحرب السيبرانية... حرب صامتة ميادينها الحواسيب وشبكة الأنترنت". قناة الجزيرة، 17 أكتوبر 2022.

https://www.youtube.com/watch?v=bZkqS6R7_xw

7. زقاغ، عادل، مترجما. " مفهوم الأمن في نظرية العلاقات الدولية". الموسوعة الجزائرية للدراسات السياسية والإستراتيجية، 16 جانفي 2021.

https://bit.ly/3WywWDC

8. عادل فتحي عبد الحميد، ميار وآخرون. "دور القايدة السياسية الروسية في تعزيز الأمن السيبراني 2012– 2023". المركز الديمقراطي العربي، 22 جوان 2023.

https://democraticac.de/?p=90695#google_vignette

9. عبد العاطي، عمرو." إستراتيجية أمريكية هجومية ضد التهديدات السيبرانية". المركز المصري للفكر والدراسات الإستراتيجية، 31 أكتوبر 2018،

/https://ecss.com.eg/2077

10. عبد العزيز، سارة." كيف تتعامل إدارة بايدن مع تهديدات الأمن السيبراني؟". مركز المستقبل للأبحاث والدراسات المتقدمة، 20 مارس 2024.

https://bit.ly/3UZNRxV

11. عبد الصادق، عادل." صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية". المركز العربي لأبحاث الفضاء الإلكتروني.

https://accronline.com/print_article.aspx?id=29415

12. خالد، وليد. " الفضاء السيبراني... نحو إمتلاك ناصية القوة". قناة الجزيرة، 10 سبتمبر 2021، قسم المقالات.

https://bit.ly/4adeCDs

13. خالد، وليد محمود. "عن "الهيمنة" و" التحكم الرقمي""، القدس العربي، 18 أغسطس 2023، قسم المقالات.

https://bit.ly/3JTHiX5

14. " الإختراق والحرب الإلكترونية كيف تتصدى أدارة بايد للخطر؟". قناة الحرة، 19 أبريل 2022.

https://arbne.ws/3wEOFP8

15. " الحرب الأوكرانية هي حرب بالوكالة بين روسيا وأمريكا". قناة العربية، 07 مارس 2024.

https://www.youtube.com/watch?v=-59_NDo661U

16. "الذكاء الإصطناعي يهدد الإنتخابات الأمريكية... ما علاقة روسيا؟". سكاي نيوز عربية،09 مارس 2024.

https://bit.ly/3wuPTws

17. " كيف يهدد تطور الهجمات السيبرانية الإقتصاد العالمي؟". سكاي نيوز عربية، 15 نوفمبر 2023.

https://bit.ly/3wuPTws

18. " مايكروسوف: قراصنة روس يستهدفون سلسلة إمداد التكنولوجيا". موقع العربية، 25 أكتوبر 2021.

https://bit.ly/3yf88ql

19. " مايكروسوف تتعرض لهجوم من قراصنة مرتبطين بروسيا". موقع الجزيرة، 20 يناير 2024.

https://bit.ly/3QDNZ3j

20. "موسكو: البرلمان يوافق على عزل روسيا عن شبكة الأنترنت العالمية". 12 فيفري 2019.

https://alnqabialjanubi.com/archives/768

21. " موسكو: رغبة الولايات المتحدة في الهيمنة تتعارض مع مشروع مكافحة الجرائم الإلكترونية".

https://bit.ly/4aeIcbD

22. " سوق الأمن السيبراني العسكري –النمو والإتجاهات وتأثير 19 –Covid والتوقعات 2024– 2029.

https://www.mordorintelligence.com/ar/industry-reports/military-cybersecurity-market

23. " عاصفة سيبرانية تتجمع فوق الإنتخابات الأمريكية". أندبندنت عربية، 28 نوفمبر 2024.

https://bit.ly/44x2U5n

24. " على أرض محايدة... بايدن وبوتين يعقدان أول قمة رئاسية بينهما". CNN العربية، 16 يونيو 2021.

https://arabic.cnn.com/world/article/2021/06/16/biden-putin-first-presidential-summit

25. " روسيا: واشنطن تشن هجمات سيبرانية علينا بأيدي الأوكرانيين". الشرق الأوسط، 25 أكتوبر 2022.

https://bit.ly/3Uy3ISJ

26. " تبادل الإتهامات... الهجمات السيبرانية تشتعل بين الغرب وموسكو". Skynews بالعربية، 28 يناير 2023.

https://bit.ly/4dA15Zl

27. " تقارير عن تعرض مطارات كبرى لهجوم سيبراني روسي". Euronews بالعربية، 10 أكتوبر 2022.

https://arabic.euronews.com/2022/10/10/cyberattacks-reported-at-us-airports-killnet-russia-pro-russian-hacker-group

المـراجـع باللغة الإنـجـليزيـة:

- Articles:
  1. Beanzer, Marie, & Robin, Patrice."Hotspot Analysis: Cyber-Conflict Between the United States of America and Russia". Center for Security Studies, (June 2017): p p. 1-27.
  2. Bebber, Robert Jake." Cyber Power and Cyber Effectiveness: An analytic Framework". Comparative Strategy, (November 2017): p p. 426- 436.
  3. Buzan, Barry. "New Patterns of Global Security in The Twenty- First Century". Royal Institute of International Affairs, Vol. 67, N°. 03 (July 1991): p p. 431- 451.
  4. Craig, Anthony, & Brandon, Valeriano. " Realism and Cyber Conflict: Security in The Digital Age". E- International Relations, (February 2018): p p. 1- 11.
  5. Herbert, Lin. "Cyber Conflict and International Humanitarian Law". International Review of The Red Cross, Vol. 94, N°. 886 (Summer 2012): p p. 515- 531.
  6. Kala. E. S. Mbung, " Critical Role of Cyber Security in Global Economy". Open Journal of Safety Science and Technology, (25 December 2023). p p. 231- 248.
  7. Korab- Karpowicz, W. Julian. "Political Realism in International Relations", The Stanford Encyclopedia of Philosophy, Center for the Study of Languages and Information (Summer 2017): p p. 1-11.
  8. Mishra, Vivek, & Patil, Sameer. "Decoding the Biden Administration's Cyber Security Policy".ORF Issue Brief, N° 686 (January 2024) p p. 1-30.
  9. Ney, Joseph. " Cyber Power". Belfer Center For Science and International Affairs, Harvard Kennedy School (May 2010): p p. 1- 26.
  10. Office of The Director of National Intelligence. "Annual Threat Assessment of U. S Intelligence Community" (5 February 2024): p p. 1-40.
  11. Ottis, Rain, & Lorents, Peter." Cyberspace : Definition and Implications". Cooperative Cyber Defense Center of Excellence, Tallin, Estonia (2010): p p. 267- 270.
  12. Saaida, B. E. Mohammed." The Use of Cyber Warfare and its Impact on International Security",Science for All Publications, Vol. 01, N°. 01(July 2023): p p. 1- 5.
  13. Schreier, Fred. " On Cyber warfare". Dcaf Horizon Working Paper, N°. 07 (2015): p p. 1- 133.
  14. Shad, Muhammed Riaz. "Cyber Threat in Interstate Relations: Case of US-Russia Cyber Tensions".Policy Perspective, Vol. 15, N°. 02 (2018): p p. 41- 55.

❖ University Dissertations:

1. Cadioli, Giovanni. " The Evolution of Cyber Conflicts and its Impact on International Security: A Comprehensive Analysis" (Thesis paper, School of Economics and Political Science, University of Padua, Italy, Academic year 2023/2024).

❖ Websites:

1. Ben, Rosamond. " Hegemony ".Encyclopedia Britannica, 11 April 2024. https://www.britannica.com/topic/hegemony

2. "Cyber Conflict Around the Globe". Johns Hopkins University. https://cyberheatmap.isi.jhu.edu/

3. Lim, Atika. "The True Cost of Cyber Attack in 2024 and Beyond".05 February 2024. https://www.expressvpn.com/blog/the-true-cost-of-cyber-attacks-in-2024-and-beyond/

4. Office of the SPOKERPERSON. " U.S Support for Connectivity and Cybersecurity in Ukraine". U.S Department of State, 10 May 2022 https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/

5. Osnos, Evan and Others. "Trump, Putin and the New Cold War". The New Yoker, Published in the Print Edition of The March 6th 2017, issue with the headline "Active Measures". https://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war

6. Petrosyan, Ani. "Number of Internet and Social Media Users World Wide as of April 2024". Statista. https://www.statista.com/statistics/617136/digital-population-worldwide/

7. Robinson, Joe."Cyber Warfare Statistics: A Decade of Geopolitical Attacks". Privacy Affairs, 10 December 2022. https://www.privacyaffairs.com/geopolitical-attacks/

8. "The Rise of GAFAM : Investing in The Future of Technology". Faster Capital, 21 April 2024. https://fastercapital.com/content/The-Rise-of-GAFAM--Investing-in-the-Future-of-Technology.html

فـــهرس الـمحـتويـات

فهرس المحتويات

الإهداء .....

شكر وتقـدير.....

ملخص الدراسة: .....

مـقـــدمـــة 1

الفصل الأول: مدخل مفاهيمي نظري للهيمنة السيبرانية..... 8

المبحث الأول: المفاهيم الأساسية للهيمنة السيبرانية..... **9**

المطلب الأول: مفهوم الهيمنة السيبرانية..... 9

المطلب الثاني: المفاهيم ذات الصلة بالهيمنة السيبرانية. 11

المطلب الثالث: الأبعاد الدولية للهيمنة السيبرانية..... 15

المبحث الثاني: النظريات المفسرة للهيمنة السيبرانية. **17**

المطلب الأول: النظرية الواقعية..... 17

المطلب الثاني: نظرية الأمننة. 18

الفصل الثاني: التنافس الروسي–الأمريكي على الهيمنة السيبرانية...... 21

المبحث الأول: التطور الكرونولوجي للتنافس الروسي–الأمريكي على الهيمنة السيبرانية. **22**

المطلب الأول: التنافس السيبراني الروسي–الأمريكي منذ 2016–2020. 23

المطلب الـثـاني: التنافس السيبراني الروسي–الأمريكي منذ 2020–2024..... 25

المبحث الثاني: الاستراتيجية الروسية–الأمريكية للتنافس على الهيمنة السيبرانية. **28**

المطلب الأول: الإستراتيجية الروسية التنافسية على الهمينة السيبرانية 29

المطلب الثاني: الإستراتيجية الأمريكية التنافسية على الهيمنة السيبرانية. 32

الفصل الثالث: تأثير التنافس السيبراني الروسي–الأمريكي على الأمن العالمي ومستقبله: 38

المبحث الأول: واقع تأثير التنافس السيبراني الروسي– الأمريكي على الأمن العالمي..... **39**

المطلب الأول: واقع تأثير التنافس السيبراني الروسي–الأمريكي على البعد الإقتصادي والعسكري. 40

المطلب الثاني: واقع تأثير التنافس السيبراني الروسي–الأمريكي على البعد السياسي والإجتماعي. 41

المبحث الثاني: مستقبل التنافس السيبراني الروسي– الأمريكي..... 44

المطلب الأول: السيناريو التصاعدي..... 44

المطلب الثاني: السيناريو التنازلي..... 45

المطلب الثالث: سيناريو استمرار الوضع القائم..... 46

الخـاتـمـة 48

قـــائـمـــة المـــصـادر والمـــراجـــع 52

فـــهرس الـــمحـــتويـــات..... 61