الصراع الروسي- الصيني- الأمريكي للاستحواذ على الهيمنة في الفضاء السيبر اني

The Russian-Chinese-American struggle for hegemony in cyberspace

د/ شريفة كلاع

جامعة الجزائر 3، (الجزائر)

cherifaklaa@gmail.com

تاريخ الاستلام: 2022/02/25 تاريخ القبول للنشر: 2022/06/02 تاريخ النشر: 2022/06/05

ملخص: تركز هذه الدراسة على موضوع الصراع الروسي، الصيني، الأمريكي للاستحواذ على الهيمنة في الفضاء السيبراني، حيث تهدف إلى تبيان طبيعة وأهداف الحروب السيبرانية الواقعة في الفضاء السيبراني، واتجاهات الخلاف الأمريكية، الروسية، والصينية فيه، ومختلف الأساليب الدفاعية المتخذة لتأمينه، وتشير نتائج هذه الدراسة إلى أنه في ظل صعوبة اللجوء إلى حروب تقليدية في صراعات هذه الدول في الوقت الراهن، فإنها تلجأ إلى الفضاء السيبراني باعتباره مجالا خامسا للحروب في إدارة صراعاتها، والسعي لامتلاك التكنولوجيا المتقدمة لخدمة الأساليب الدفاعية لتأمين الفضاء السيبراني الذي أصبح يمس بسيادة الدول في النظام الدولي

الكلمات المفتاحية: الصراع؛ الولايات المتحدة الأمريكية؛ روسيا؛ الصين؛ الهيمنة؛ الفضاء السيبراني.

Abstract: *This study focuses on the subject of the Russian, Chinese, and American competition to gain prominence in the cyberspace. It aims to clarify the nature and objectives of cyber wars waged in the cyberspace, the trends of the American, Russian, and Chinese dispute in it, as well as the various defensive measures taken to secure it. This conclusion of this study indicates that given the complexities of resorting to conventional wars currently, these powers resort to cyberspace as the fifth field of wars in managing their conflicts. Hence, striving to possess advanced technology to secure the cyberspace became an imperative as a result of the latter's increasing impact on the sovereignty of states in the international system.*

key words: *Conflict; United States of America; Russia; China; Hegemony; cyberspace.*

1.مقدّمة:

ببروز الفضاء السيبراني كساحة للصراع الدولي بين القوى الكبرى ولغياب الحدود المادية فيه، أصبح مفهوم السيادة أمرا مؤرقا للدول على اعتبار أنه يهدد أمنها الوطني، وله تأثيراته في على طبيعة الصراعات الدولية، إذ أصبح الفضاء السيبراني كبديل عن الحروب المباشرة بين الدول، وذلك عبر استخدام شبكات الاتصال والمعلومات، وأحدث التقنيات التكنولوجية والتي تتجاوز كل الحدود التقليدية المعروفة للدول، كما يعتبر مجالا يسهل من خلاله إلحاق التهديد والضرر بأمنها، لذلك تسعى الدول إلى استراتيجيات وأدوات لردع الهجومات الإلكتروني، من أجل تحقيق أمنها السيبراني الذي يكمل سيادتها الوطنية .

أهداف البحث:

يهدف هذا البحث إلى تقديم دراسة تحليلية تحاول الإلمام بمدى أهمية موضوع الصراع الروسي، الصيني، والأمريكي للاستحواذ على الهيمنة في الفضاء السيبراني، وذلك من خلال التطرق إلى مفهوم الحرب السيبرانية وتداخلاتها مع المفاهيم ذات العلاقة بالصراع السيبراني، وكذا طبيعة وأهداف الصراعات والحروب السيبرانية الواقعة في الفضاء السيبراني، كما تستعرض اتجاهات الخلاف الأمريكي، روسي، الصيني حول الفضاء السيبراني، ومن ثم التطرق إلى ما اتخذته تلك القوى من أساليب دفاعية لتأمين الفضاء السيبراني.

إشكالية البحث: وتتمثل فيما يلي: إلى أي مدر يمكن أن يمثل الفضاء السيبراني مجالا للخلاف وبعدا خامسا للصراع الروسي، الصيني، الأمريكي؟

فرضية البحث: وتكمن فيما يلي:

*كلما تزايد استخدام الفضاء السيبراني بشكل واسع واتخاذه ساحة للحرب، كلما أدى ذلك إلى نقل الحروب والصراعات بين الولايات المتحدة الأمريكية وروسيا والصين إليه بما يتم التأثير به على السيادة والأمن السيبراني وهو ما يستوجب ضرورة وضع أساليب دفاعية لتأمين الفضاء السيبراني .

منهج البحث: تم الاعتماد في هذا البحث على المنهج التاريخي وكذا الإحصائي، والتي تخدم موضوع البحث وتساعد على الإجابة على إشكالية الموضوع المطروحة .

عناصر البحث: سيتم معالجة موضوع: "الصراع الروسي – الصيني – الأمريكي للاستحواذ على الهيمنة في الفضاء السيبراني"، وذلك من خلال تناول النقاط التالية:

1 - الحرب السيبرانية وتداخلاتها مع المفاهيم ذات العلاقة بالصراع السيبراني.

2 - طبيعة وأهداف الصراعات والحروب السيبرانية الواقعة في الفضاء السيبراني.

3 - اتجاهات الخلاف الأمريكي، روسي، الصيني حول الفضاء السيبراني.

4 - الأساليب الدفاعية المتخذة لتأمين الفضاء السيبراني.

2. الحرب السيبرانية وتداخلاتها مع المفاهيم ذات العلاقة بالصراع السيبراني:

1.2 الفضاء السيبراني (Cyber Space):

يعرف الفضاء السيبراني أو ما يطلق عليه أيضا "الحيز" أو "الفضاء الافتراضي" بأنه؛ المجال الرقمي الإلكتروني (Digital Medium) الممتد عبر مختلف خطوط الاتصالات المعدنية والضوئية والهوائية وقنواتها في شبكة الأنترنت، وهو بهذا المعنى، طريق المعلومات الفائقة السرعة بتعبيره التكنولوجي (البابلي، 2021، ص: 21).

وهناك من يعرفه بأنه عبارة عن بيئة إلكترونية غير ملموسة معقدة التفاعل يتم فيها بناء نماذج لظواهر أو صور إلكترونية لظواهر شبه حقيقية في التفاعلات والتعاملات البعيدة، فالسَّيْبَرة عملية انعكاسية نشطة يعكس فيها مدخلات التفاعلات الإلكترونية في بيئة لا يستطيع الإنسان إدراكها، وبصورة أخرى هي عبارة عن شبكة إلكترونية لمجموعة من الخوادم الإلكترونية حيث تتفاعل هذه الشبكات التي تتوفر فيها قاعدة بيانات، فيما بينها باستخدام وسيلة تواصل افتراضية متجاوزة كل الحواجز الجغرافية والسياسية، سعيا وراء تحسين قدرة الاتصال والتعامل الإلكتروني، كما أنها محاكاة حاسوبية عادة ما تكون في صورة بيئة افتراضية لمستخدمي العالم الافتراضي (علي، 2020، ص ص: 53 - 54).

وقد عرِّف الفضاء السيبراني أيضا بأنه عالم افتراضي يتشابك مع عالمنا المادي، يتأثر به ويؤثر فيه بشكل معقد، حيث تقوم العلاقة بين العالمين على نظرة تكاملية تحمل بين طياتها مزايا ومخاطر لا تتوقف، وهناك من وصفه بالذراع الرابعة للجيوش الحديثة إلى جوار القوات البرية والبحرية والجوية، خاصة وأن الأنترنت تشهد معارك حقيقية تدور في هذا العالم الافتراضي، وهناك من يرى أنه يمثل البعد الخامس للحرب، كما يعرف على أنه المجال المادي وغير المادي الذي يتكون من عناصر تتمثل في أجهزة الكمبيوتر والشبكات والبرمجيات وحوسبة المعلومات والمحتوى ومعطيات النقل والتحكم ومستخدمو كل هذه العناصر، حيث تعد هذه العناصر العامل المشترك في جميع محاور استخدام الفضاء السيبراني، سواء أكانت الجهات المستخدمة قادرة على تعظيم قيمها وقدراتها بما في ذلك رفع كفاءة العنصر البشري أم كانت في مرحلة متأخرة (شلوش، 2018، ص: 190).

2.2 الأمن السيبراني (Cyber Security):

يعرف الأمن السيبراني بأنه حزمة العمليات والإجراءات التي تتوخى تأمين وحماية الشبكات وأجهزة الكمبيوتر والبرامج من الهجوم، أو التلف أو السرقة والوصول غير المصرح به، للحد من الهجمات الإلكترونية بغير وجه حق، كما أنه عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال، واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها، وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية، واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من مخاطر الفضاء السيبراني (بلعسل بنت نبي، عمروش، 2021، ص: 165).

كما يعني الأمن السيبراني: مجموع الإجراءات الواجب اتخاذها من قبل الأجهزة الأمنية أو الأخرى غيرها ذات العلاقة، للمحافظة على سرية المعلومات الإلكترونية، ومنع الاختراقات الفيروسية من أجل ضمان وصول المعلومات الحاسوبية إلى الجهات المختصة في الوقت المناسب، وضمان عدم وقوعها في أيدي الأعداء أو الأصدقاء على حد سواء خصوصا بعد الثورة الهائلة في عالم الاتصالات والتداولات الإلكترونية، حيث شكل هذا النوع من الأمن هاجسا استراتيجيا للقوى العالمية والمتمثلة في الولايات المتحدة الأمريكية والصين وروسيا، إذ تدور في وقتنا الحالي حرب إلكترونية بين هذه القوى من أجل اختراق المعلومات والتأثير على أسعار البورصة والعملات وغيرها من المنشآت (علي، 2020، ص: 56).

3.2 الحرب السيبرانية (Cyber Warfare):

يعد مفهوم الحرب السيبرانية مفهوما جديدا على صعيد النزاعات الدولية، وهي تشير إلى: أساليب للحرب تعتمد على تكنولوجيا المعلومات وتستهدف الحواسيب والمواقع الإلكترونية، وتشمل عمليات تسلل إلى أنظمة الحاسب الآلي، ودمع بيانات أو تصديرها أو إتلافها أو تغييرها أو تشفيرها، كما تشمل عمليات زرع برمجيات ضارة للتجسس، وغير ذلك من العمليات السيبرانية أو الإلكترونية، أو ما يطلق عليه عمليات اختراق أو قرصنة إلكترونية (البابلي، 2021، ص: 27).

كما أنها تعني؛ استخدام تكنولوجيا الكمبيوتر لتعطيل أنشطة دولة أو مؤسسة، وخاصة الهجوم المعتمد على أنظمة المعلومات لأغراض استراتيجية أو عسكرية (بريوش، 2019، ص: 9)، حيث تحدث تلك الحرب في الفضاء السيبراني (الإلكتروني) ويكون لها طابع دولي، بواسطة حكومة ما أو نيابة عنها من فواعل من غير الدول والحكومات، من خلال اختراق شبكة ما اختراقا غير مصرح به بغرض إضافة أو تغيير أو تزييف البيانات أو التسبب في تعطيل جهاز الكمبيوتر أو إتلافه أو تعطيل وإتلاف جهاز متصل بشبكة أو منصات أخرى أو بمعدات يتحكم فيها نظام الكمبيوتر، ويبرز في هذا التعريف السمات العسكرية والسياسية والاقتصادية للفضاء السيبراني المرتكز على عالم الاتصالات والمعلومات، وتطور وسائل التشبيك والتواصل، وعلى خلق أدوات تهديد مختلفة وخطيرة تقوم بإحداث أضرار ملموسة كبيرة ومدمرة (بريوش، 2019، ص: 11 – 12)، وبذلك تعد الحرب السيبرانية جزءً من عمليات المعلومات التي يمكن أن يتم استخدامها في مستويات ومراحل الصراع المختلفة سواء كان ذلك على الجانب التكتيكي أو العملياتي أو الاستراتيجي، ويتم استخدام تلك الهجمات في أي وقت سواء أكان وقت سلم أم حرب أم أزمة (إيهاب خليفة، القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الأنترنت، الولايات المتحدة نموذجا، 2017، ص: 27).

3. طبيعة وأهداف الصراعات والحروب السيبرانية الواقعة في الفضاء السيبراني:

1.3 أهداف الصراعات والحروب السيبرانية الواقعة في الفضاء السيبراني:

لقد برز الفضاء السيبراني كمجال تنشأ فيه نزاعات بين الفاعلين المختلفين، خاصة مع الاعتماد الكبير على تكنولوجيا الاتصال والمعلومات، وعلى إثر ذلك برز الصراع السيبراني كحالة من التعارض في المصالح والقيم بين الفاعلين الدوليين في الفضاء السيبراني، وفي هذا الإطار يمكن القول بأن أهداف

الحروب السيبرانية الواقعة بين الدول تختلف وفقا لطبيعة أهداف الصراعات السيبرانية، والتي يمكن تبيانها على النحو التالي (عادل عبد الصادق، أنماط الحروب السيبرانية وتداعياتها على الأمن العالمي، 2017، ص: 33 – 34):

1 – صراع سيبراني ذو طبيعة سياسية: حيث تحركه دوافع سياسية، وقد يأخذ شكلا عسكريا يتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء السيبراني، بهدف إفساد النظم المعلوماتية، والشبكات والبنية التحتية، ويتضمن هذا النوع من الصراعات توظيف أسلحة إلكترونية من قبل فاعلين داخل المجتمع المعلوماتي، أو من خلال التعاون مع قوى أخرى لتحقيق أهداف سياسية.

2 – صراع ذو طبيعة مرنة: أي الصراع حول الحصول على المعلومات والتأثير في المشاعر والأفكار، وشن حرب نفسية وإعلامية، ويتم ذلك من خلال تسريب المعلومات، واستخدامها عبر منصات إعلامية، بما يؤثر في طبيعة العلاقات الدولية، كالدور الذي أداه موقع "ويكيليكس" في الدبلوماسية الدولية.

3 – صراع سيبراني على التقدم التكنولوجي: حيث يأخذ هذا النمط من الصراعات السيبرانية طابعا تنافسيا حول الاستحواذ على سباق التقدم، وسرقة الأسرار الاقتصادية والعلمية، وقد يمتد إلى محاولة للسيطرة على الأنترنت وأسماء النطاقات وعناوين المواقع، والتحكم بالمعلومات، والعمل على اختراق الأمن الوطني للدول بدون استخدام طائرات أو متفجرات أو حتى انتهاك حدود الدول، كهجمات قراصنة الكمبيوتر، وتدمير المواقع والتجسس، بما قد يكون له تأثيرات مدمرة على الاقتصاد، والبنية التحتية بذات قوة التفجير التقليدي.

4 – صراع سيبراني على المعلومات والاستخبارات: فمع صعوبة الفصل بين أنشطة الاستخبارات، وجمع المعلومات، وحروب الفضاء السيبراني، أو التمييز بين الاستخدام السياسي والإجرامي، يبدو الفضاء السيبراني بيئة مناسبة للصراعات المعلوماتية، إذ يسهم في دعم قدرة الأجهزة الأمنية للدول، أو حتى الجماعات المختلفة على تشكيل شبكة عالمية من العملاء بدون تورط مباشر، بالإضافة إلى رخص التكلفة، وسهولة الاتصال وصعوبة الرقابة التقليدية على التفاعلات السيبراني، وقد مثل ذلك عنصر جذب لاستخدام الأسلحة السيبرانية، وتوظيفها لتحقيق أهداف سياسية وعسكرية.

وفي إطار التأكيد على أهمية فضاء القوة السيبرانية والذي يعتبر البعد الخامس من فضاءات القوة الاستراتيجية، يؤكد "جوزيف ناي" (Josef S. Nye) من خلال كتابه "مستقبل القوة" (The Future of Power) الصادر عام 2011، على أن: القوى الكبرى في العالم ستتعرض لضغوط شديدة لممارسة سيطرتها على المجال السيبراني في الطريقة التي اكتسبت بها التفوق على الجو والبحر والبر (Nye, 2011, p : 150)، وفي هذا الإطار فإنه حسب رؤية الباحثة "ابتسام عبد الزهرة العقبي" وفقا لدراسة قدمتها عام 2018 بعنوان: "الصراع الجيوستراتيجي الأمريكي – الروسي في الفضاء الإلكتروني"، فإن الصراع سيكون حسب التطور التكنولوجي، من خلال علاقته بالمجالات الجغرافية التي يغطيها وهي (الأرض، الجو، البحر، والفضاء)، وعليه فإن نتيجة التوجه التكنولوجي تتجه نحو عولمة العالم اقتصاديا وثقافيا وسياسيا وخلق

مركز القلب له، ليكون نقطة التحكم والتوجيه في المستقبل، حيث سيدفع إلى وضع نظرية أخرى ستكون قيد التطبيق مستقبلا، وهي تقوم على (العقبي، 2022):

1 - أنه من يسيطر على المعرفة ويمتلكها ويتحكم بها، سيسيطر على المجال الخامس (الفضاء السيبراني).

2 - وأن من يسيطر على الفضاء السيبراني، سيسيطر ويتحكم في المجالات الجغرافية الأربعة (البر، البحر، الجو، و الفضاء).

3 - ومن يسيطر على المجالات الجغرافية الأربعة، سيسيطر على العالم.

ومن ثم فالفكرة الأساسية انطلاقا مما ذكر أعلاه يكمن دور الفضاء السيبراني في ربط مختلف ميادين الحرب الأربعة (البر، البحر، الجو، والفضاء الخارجي) مع بعضها البعض، وبعبارة أخرى أصبح الفضاء السيبراني بمثابة قاعدة كبرى تربط ميادين الحرب كلها، بل أن الأمر يتعدى ذلك ليشمل مجالات أخرى كالطاقة والشبكات ومختلف المواقع الحكومية ، وبالتالي فإن أي جهة أخرى سواء كانت دولة صغيرة بقدرات سيبرانية كبيرة، أو حتى مجموعة أفراد متخصصين في الأمن السيبراني، سيكونون قادرين على إيجاد أي ثغرة أو نقطة ضعف محتملة في النظام السيبراني للدولة واستغلالها واستهداف قطاعات عسكرية واقتصادية معينة، كما يمكن الإشارة إلى أن أي نظام سيبراني لأي دولة قابل للتعرض لمختلف التهديدات السيبرانية سواء بالنسبة للأنظمة المتطورة أو الأكثر تطورا، في حين تتفاوت درجة الصعوبة في اختراق تلك الأنظمة، لكنها تبقى قابلة للاختراق، وحتى لو وجد هناك نظام سيبراني حصين ضد الهجمات السيبرانية، فإن حصانته لن تدوم طويلا، وذلك بسبب السرعة الكبيرة التي يتطور بها عالم التكنولوجيا ومجال الذماء الاصطناعي في الوقت الراهن (حارك، حمدوش، 2022، ص: 137).

2.3 طبيعة الصراعات والحروب السيبرانية:

في ظل تحول الفضاء السيبراني إلى مجال متزايد لتنافس السياسات للدول وغيرها من الفاعلين، أصبح الصراع في الفضاء السيبراني يعرف باستخدام تكنولوجيا الحاسوب في الفضاء السيبراني لأغراض التدمير من أجل التأثير، أو التغيير أو التعديل في التفاعلات الدبلوماسية والعسكرية بين الكيانات المختلفة، وذلك بعيدا عن ساحة المعارك، إذ يأخذ ذلك الصراع نمطين هما (عبد الصبور، 2017، ص: 6):

1 – الحوادث الفردية (Cyber Incidents): ويقصد بها العمليات والحوادث الفردية التي تتم على فترات مختلفة، وليست مستمرة لفترة معينة.

2 – النزاعات السيبرانية (Cyber Disputes): والتي تدار بأدوات افتراضية بين دولتين في فترة زمنية معينة، ويحتوي على واحد أو أكثر من الحوادث الفردية.

حيث تجدر الإشارة هنا إلى الصراعات السيبرانية تختلف عن نظيراتها التقليدية وبالأخص العسكرية، والتي تعد حكرا على الدولة والجماعات المسلحة، وهي صراعات تدور في مساحة جغرافية معينة، وتستمر لفترة معينة، وتكون محددة الأطراف والأهداف، وإن كانت الصراعات المسلحة على أرض الواقع قد دخلت فيها أدوات تكنولوجيا لإدارة الصراعات بين الدول، فعندما تنشب حروب تقليدية بين الدول؛ تصبح قطاعات الاتصالات، والمعلومات، والبنى التحتية والمعلوماتية ضمن الأهداف العسكرية، خاصة مع ارتباط

تلك القطاعات بالأمن الوطني للدول، ومن ثم أصبحت هناك أسلحة ذات طبيعة إلكترونية ضمن الحروب، مثل وسائل التواصل الاجتماعي، والأقمار الصناعية، وأسلحة النانو التكنولوجية، الطائرات من دون طيار، والأسلحة الروبوتية (عبد الصبور، 2017، ص: 6).

لقد غيرت العمليات الواقعة في الفضاء السيبراني طبيعة حرب المعلومات، وبدأ على إثرها تغيير طبيعة الحروب كلها (باسيت، 2014، ص: 57)، ولذلك تلجأ الدول إلى إدارة صراعاتها مع خصومها من خلال توظيف الحروب السيبرانية كأدوات إضافية في حروبها، الأمر الذي مختلف دول العالم تتعرض إلى عمليات اختراق إلكترونية وجوسسة في الفضاء السيبراني للحصول على معلومات عسكرية كانت أو مدنية، وحتى القيام بالتعرض لعمليات إتلاف للبيانات وتدمير المنشآت، ونظرا لأن الدول تختلف فيما بينها من حيث أنظمة الحماية والدفاع الإلكتروني، وتبيان قدرات الدول الكبرى في مجال التحكم في الفضاء السيبراني ومحاولات الهيمنة والسيطرة عليه، ما خلق تحديات أمنية تتعرض لها الدول دونما استثناء، وفيما يلي يمكن تبيان مختلف تلك التحديات:

1 – استهداف البنية التحتية الحرجة للدولة: تستهدف الهجمات السيبرانية إعاقة الخدمات الحيوية، وكذا نشر برمجيات خبيثة وفيروسات لتخريب أو تعطيل البنية التحتية لاتصالات وتكنولوجيا المعلومات ونظم التحكم الصناعية الحيوية، خاصة المرافق المهمة منها وقواعد البيانات والمعلومات القومية والخدمات الحكومية والرعاية الصحية والاسعاف العاجل وغيرها، وذلك عبر عدة قنوات تشكل الشبكات اللاسلكية والذاكرة النقالة، بالإضافة إلى القنوات الأخرى الشائعة (البريد الإلكتروني ومواقع الأنترنت والشبكات الاجتماعية وشبكات الاتصالات السلكية)، مما يؤثر تأثيرا ملموسا على البنية التحتية لتلك المنشآت والمرافق وعلى الخدمات والأعمال المرتبطة بها (البابلي، 2021، ص: 35).

ويتم استهداف البنية التحتية للدولة سواء كانت مدنية أو عسكرية بهجمات إلكترونية، مثل استهداف محطات الطاقة والوقود والخدمات المالية والمصرفية ونظم الاتصالات والمواصلات، ومن أبرز الأمثلة على ذلك تعرض أوكرانيا خلال شهر جوان 2017 لهجمة إلكترونية شملت محطات الطاقة، بالإضافة إلى المؤسسات المالية وأحد أكبر مطاراتها، وقد شهدت السنوات القليلة الماضية العديد من الهجمات الإلكترونية على بعض البنى التحتية الحرجة والمؤسسات العسكرية، مثل محطات الطاقة النووية كقيام فيروس "ستاكسنت" (Struxnet) بتعطيل حوالي ألف من أجهزة الطرد المركزي في منشأة تخصيب اليورانيوم في "ناتانز" في وسط إيران في عام 2010، فضلا عن تعرض أنظمة الكمبيوتر لشركة كوريا الجنوبية للطاقة المائية والنووية التي تديرها الدولة لهجمات إلكترونية في شهر ديسمبر 2014، واتهمت الولايات المتحدة الأمريكية روسيا بالتورط في شن هجمات إلكترونية على شبكات الكمبيوتر في عدة محطات للطاقة النووية (إيهاب خليفة، القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الأنترنت، الولايات المتحدة نموذجا، 2017، ص: 56 – 57).

2 – السيطرة على الأنظمة العسكرية: ويقصد بها قيام قراصنة محترفين أو جيوش نظامية إلكترونية بشن هجمات إلكترونية بغرض السيطرة على نظم القيادة والسيطرة عن بعد، الأمر الذي يؤدي إلى إخراج بعض

منظومات الأسلحة عن سيطرة القيادة المركزية، وإعادة توجيهها نحو أهداف داخلية أو ضد دولة صديقة، ما يمكن أيضا السيطرة على الطائرات دون طيار أو الغواصات النووية في أعماق البحار، أو السيطرة على الأقمار العسكرية في الفضاء الخارجي وإخراجها عن سيطرة الدولة التابعة لها هذه الأسلحة والمعدات، حيث تزداد خطورة مثل هذه الهجمات في ضوء التطور التكنولوجي واعتماد اللوجستيات ونظم القيادة والتحكم وتحديد الأهداف وإصابتها على برامج الكمبيوتر وشبكات الاتصالات (إيهاب خليفة، القوة الإلكترونية: كيف يمكن أن تدير شؤونها في عصر الأنترنت، الولايات المتحدة نموذجا، 2017، ص: 57).

ومن أجل الحصول على معلومات أمنية من خدمات الأنترنت، يستغل أيضا الأفراد، الجماعات الإرهابية، الدول ومختلف الفواعل؛ برامج وتطبيقات تقنية حديثة من خلال خرائط "جوجل" (Google) وخدمات "جوجل إيرث" (Google Earth) للحصول على صور لمواقع أمنية، والتي تتيح لهم الحصول على تحديد مواقع فورية للمناطق الحساسة بكل سهولة، كما يقوم بعض العسكريين بوضع بياناتهم الشخصية على صفحات الأنترنت ومواقع التواصل الاجتماعي، وهي التي من خلال تحليلها يمكن الوصول إلى معلومات أمنية مهمة عن العسكريين وأمور تتعلق بالعمل وأماكن الإقامة والتحركات وأدق الأسرار الخاصة بهم (البابلي، 2021، ص: 42 – 43).

3 – سرقة المعلومات والبيانات العسكرية أو التلاعب بها: تعتبر من أخطر الجرائم التي تهدد مستخدمي شبكة الأنترنت والخدمات الإلكترونية، حيث قد تتعرض البيانات للسرقة بهدف انتحال الشخصية والاستيلاء على الممتلكات، وهو ما يحدث خاصة مع مواقع شبكات التواصل الاجتماعي، ومواقع التجارة الإلكترونية، مما يشكل خطرا كبيرا على مصالح المستخدمين والخدمات الإلكترونية والمؤسسات والحكومات ومختلف الجهات المدنية والعسكرية (البابلي، 2021، ص: 35 – 36).

وتتم سرقة المعلومات والبيانات أو التلاعب بها من خلال اختراق قواعد البيانات العسكرية وسرقتها أو تزييفها أو تدميرها إلكترونيا، حيث تسعى الهجمات الإلكترونية في هذه الحالة إلى اختراق الشبكات الخاصة بالمؤسسات العسكرية، بهدف سرقة خرائط نشر أنظمة التسليح أو التصميمات الخاصة بالمعدات العسكرية، وقد انطلقت واحدة من أخطر الهجمات ضد أنظمة حواسيب الجيش الأمريكي في عام 2008 من خلال وصلة "يو إس بي USB" متصلة بكمبيوتر محمول تابع للجيش في قاعدة عسكرية موجودة في الشرق الأوسط، ولم يتم اكتشاف انتشار برامج التجسس في كل من الأنظمة السرية وغير السرية في الوقت المناسب، مما شكل ما يشبه جسرا رقميا تم من خلاله نقل آلاف الملفات من البيانات إلى "خوادم خارجية" (Servers)، وبالمثل تم استهداف أكثر من 72 شركة من بينها 22 مكتبا حكوميا و13 من مقاولي قوات الدفاع بهدف سرقة معلومات حول الخطط والمباني العسكرية (إيهاب خليفة، القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الأنترنت، الولايات المتحدة نموذجا، 2017، ص: 57).

4 – جمع معلومات اقتصادية استخباراتية: وهو ما يتحقق عن طريق اختراق قواعد البيانات المالية والمصرفية وقواعد بيانات الشركات والبنوك وجمع المعلومات التي قد تؤثر على الأمن القومي للدولة، وكذلك من خلال التجسس على المسؤولين الماليين ووزراء المالية ورؤساء الشركات الكبرى، حيث أصدر

الرئيس الأمريكي السابق "باراك أوباما" أثناء فترة عهدته الثانية أوامره بوقف التنصت على مقري صندوق النقد الدولي والبنك الدولي، وذلك في إطار مراجعة أنشطة جمع المعلومات الاستخباراتية، وذلك في أعقاب التسريبات التي كشف عنها المتعاقد السابق مع وكالة الأمن القومي الأمريكية "إدوارد سنودن" بشأن برامج لجمع كميات من البيانات عن حلفاء وأعداء الولايات المتحدة الأمريكية (إيهاب خليفة، القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الأنترنت، الولايات المتحدة نموذجا، 2017، ص: 57).

وفي ظل التنافس الاستراتيجي الأمريكي – الصيني حول احتكار التكنولوجيا والتقنية، وحقوق الملكية الفكرية ونقل التكنولوجيا وتطوير تقنية الجيل الخامس والذي ترى فيه الولايات المتحدة الأمريكية أنه مجالا يمكن توظيفه في مجال الأنشطة الاستخباراتية، سعت الصين بشكل دؤوب لفض ذلك الاحتكار وتحسبا في أن تتخلص من تبعيتها التكنولوجية للغرب، أنشأت الصين من خلال "الأكاديمية الصينية للهندسة" سنة 2013 فريقا ضم أكثر من 100 أكاديمي وعالم باحث اتجاه تطوير القطاع الصناعي الصيني، واستعراض إجراءات واستراتيجيات الدول الصناعية المتقدمة، وقضايا القطاع الصناعي الصيني وآثار التقدم الرئيسية، وبعد سنتين من الجهود قدم الفريق بحثا حول القطاع الصناعي الصيني استندت إليه الحكومة الصينية في صياغة استراتيجيتها "صنع في الصين 2025"، حيث تهدف إلى الارتقاء بالقطاع الصيني وتحويله إلى قطاع متقدم يسهم في تعزيز القدرة التنافسية الصناعية الصينية، لتنضم الصين إلى صفوف دول العالم المتقدم في القطاع الصناعي، من حيث تخفيض استهلاك الموارد ورفع إنتاجية العمل، وتعزيز القدرة على الابتكار وتحسين الهيكل الصناعي، والإسراع في تكامل المعلومات والتصنيع وزيادة عدد براءة الاختراع، والاستثمار في البحث والتطوير والعنصر البشري، ونسبة الربح من المبيعات على نحو يساعد في رفع القطاع الصناعي للصين على نحو شامل، ويجعلها في مقدمة الدول المنتجة لتكنولوجيا الثورة الصناعية الرابعة (إيهاب خليفة، الصراع الأمريكي – الصيني على التكنولوجيا الفائقة الذكاء، 2019، ص: 91) ، حيث تسعى الصين إلى السيطرة الرقمية، والاستثمار في تقنية الجيل الخامس.

4. اتجاهات الخلاف الأمريكي، روسي، الصيني حول الفضاء السيبراني:

يعد المجال السيبراني كحالة جديدة من أنماط الصراع، في ظل بروز اتجاهات جديدة للتنافس الروسي - الصيني - الأمريكي حول السيادة السيبرانية، وهو ما انعكس على القضايا والاستراتيجيات والتي ستؤثر حتما على مستقبل الصراع السيبراني بين الدول الكبرى من جهة وتأثير ذلك على الأمن الجماعي الدولي من جهة أخرى، وفيما يلي نبين اتجاهات التفكير حول رؤية كل من روسيا والولايات المتحدة الأمريكية والصين حول المجال السيبراني:

1.4 اتجاهات الخلاف الروسي – الأمريكي حول المجال السيبراني:

لقد استحوذت قضية الفضاء السيبراني على اهتمام متصاعد لدى كل من روسيا والولايات المتحدة الأمريكية، خاصة على إثر تداعيات التحقيقات بشأن التدخل الروسي في الانتخابات الأمريكية بفوز الرئيس السابق "دونالد ترامب"، وباتت ملامح الخلاف حول الاعتداءات تخف وطأتها، إلا أن اتجاهات الخلاف أخذت في التصاعد بعد اتهام روسيا بشن هجمات سيبرانية على حلفاء الولايات المتحدة الأمريكية في أوروبا

عام 2018، خاصة بعد اتهام بريطانيا لروسيا بشن هجمات سيبرانية ضدها، وقد ساعد التوتر التجاري بين الصين والولايات المتحدة الأمريكية إلى تصاعد الاتهامات بقيام الصين بالتجسس على الرئيس الأمريكي السابق "ترامب"، ومن جهة أخرى عززت العقوبات الأمريكية على روسيا والصين من التقارب في الرؤى حول المجال السيبراني، وتصاعدت المخاوف من استيراد البرمجيات من الخارج لاستخدامها لاستهداف البنية التحتية المعلوماتية، واستخدام القوانين والتشريعات للحماية والرقابة على استيراد التكنولوجيا، والحذر من احتمال ارتباط الشركات التكنولوجية الأجنبية بأهداف دولة معادية، إذ تصاعد الخوف من التعرض للتجسس الاقتصادي والصناعي وتوظيف أجهزة الاستخبارات الأجنبية للمجال السيبراني (عادل عبد الصادق، صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية، 2021).

وتجدر الإشارة إلى أنه في الفترة ما بين 2009 – 2019 تزايدت حدة الهجمات السيبرانية بين الولايات المتحدة الأمريكية، الصين وروسيا ضد بعضهم البعض ، فخلال تلك الفترة تم تنفيذ 79 هجوما سيبرانيا من قبل مهاجمين ترعاهم الصين استهدفت 20 دولة، وقد كانت نسبة 32% من تلك الهجمات موجهة ضد الولايات المتحدة الأمريكية، الأمر الذي جعل هذه الأخيرة الهدف الأول للقراصنة السيبرانيون الصينيين، وخلال نفس الفترة استهدف المهاجمون السيبرانيون الروس 19 دولة في 75 حادثا هجوميا، وقد كان الهدف الرئيسي لروسيا هو الولايات المتحدة الأمريكية، كما هاجمت أيضا 8 دول في الاتحاد الأوربي، وخلال نفس الفترة أيضا كانت الولايات المتحدة الأمريكية مصدرا لما يقل عن 12 هجوما إلكترونيا عالميا نصفها وقع في عام 2019، وقد استهدفت ثلاثة من الهجمات التي انطلقت من الولايات المتحدة الأمريكية: كوريا الشمالية، حيث تعرضت الصين وإيران للهجوم مرتين لكل منهما (Robinson, 2022).

جدول رقم (01): الهجمات السيبرانية لكل من الصين، روسيا، الولايات المتحدة الأمريكية ضد بعضهم خلال فترة (2009 – 2019)

الدولة	نسبة/ عدد الهجمات السيبرانية (2009 – 2019)
الصين	* تم تنفيذ 79 هجوما إلكترونيا موثقا من قبل مهاجمين ترعاهم الدولة الصينية، استهدفت 20 دولة. * 32% من هجمات الصين كانت موجهة ضد الولايات المتحدة الأمريكية، مما جعل الولايات المتحدة الأمريكية أكبر هدف للقراصنة الصينيين.
روسيا	* استهدف المهاجمون الروس 19 دولة في 75 حادثا بين عامي 2009 و2019. * الهدف الرئيسي لروسيا هو الولايات المتحدة الأمريكية، إلا أنها هاجمت أيضا 8 دول في الاتحاد الأوروبي، بما في ذلك سلسلة من الهجمات على البرلمان الألماني وأوكرانيا.
الولايات المتحدة الأمريكية	* كانت الولايات المتحدة الأمريكية مصدر ما لا يقل عن 12 هجوما إلكترونيا عالميا على مدى السنوات العشر الماضية، نصفها وقع في عام 2019. * استهدفت ثلاثة من الهجمات المعروفة التي انطلقت من الولايات المتحدة الأمريكية: كوريا الشمالية، وتعرضت الصين وإيران للهجوم مرتين لكل منهما.

المصدر: * Joe Robinson. (2022). "Cyberwarfare statistics: A decade of geopolitical attacks", 21 November 2021, privacy affairs, (28/01/2022), see the link: https://bit.ly/3v17Nno

وفي محاولة للاستجابة لتلك التهديدات أصبح الغرب بقيادة الولايات المتحدة الأمريكية والشرق بقيادة روسيا والصين اللذان يتصارعان على فرض رؤية كليهما لكيفية تشكيل القواعد والمبادئ الدولية، التي من شأنها تنظيم التعامل مع التهديدات المحتملة في الفضاء السيبراني، ومما أربك المشهد الدولي هو تحول الصين وروسيا من العزلة عن السياسات العالمية إلى الانخراط وبشدة بها، بل والسعي إلى وجود تكتل قوي في مواجهة تكتل آخر بقيادة الولايات المتحدة الأمريكية، وقد أدى هذا الخلاف بين كلا الجانبين إلى عدم التوصل إلى اتفاق حول الأمن السيبراني والاختلاف في الرؤية للاستراتيجيات والمبادئ والأهداف والتعريفات التي تعبر عن تضارب في المصالح، والتي تكشف عن تمسك الولايات المتحدة الأمريكية بهيمنتها السيبرانية وبخاصة بعد تدشين قيادة عسكرية للفضاء الإلكتروني عام 2009، كما عملت أيضا الولايات المتحدة الأمريكية في 7 أوت 2018 بتدشين قيادة عسكرية للفضاء الخارجي لتصبح الفرع السادس للجيش، وهو الأمر الذي يكشف انتقال الصراع حول عسكرة "المجالات الدولية" إلى الفضاء الخارجي بهدف السيطرة والهيمنة ومنع خصومها من الاستفادة من المزايا الاستراتيجية، ومواجهة تطوير روسيا أسلحة فضائية قادرة على استهداف الأقمار الصناعية الأمريكية (عادل عبد الصادق، صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية، 2021).

وعلى المستوى الدبلوماسي قدمت روسيا مشروع اتفاقية الأمم المتحدة للتعاون في مكافحة الجرائم المعلوماتية، وذلك في محاولة لاستبدال "اتفاقية بودابست" لعام 2001، والتي وقعت عليها الولايات المتحدة الأميركية إلى جانب 55 دولة أخرى، والتي ترفضها روسيا، حيث تراها تهديدا مباشرا لسيادتها، خاصة فيما يتعلق بالمادة 32 (ب) والتي تسمح لأصحاب البيانات بالسيطرة على استخدامها، بدلا من الحكومات، إذ يحاول الاقتراح الروسي وضع قواعد السلوك المتبعة في الفضاء السيبراني، والتحقيق المشترك في الأنشطة الخبيثة، وفي المقابل رأت الولايات المتحدة الأمريكية أن الاتفاقية المقترحة ستعزز من قدرات روسيا وغيرها من الدول السلطوية في السيطرة على الاتصالات في الداخل وفي بقية الدول الأخرى، خاصة بعد تأييد تجمع "البريكس" للمبادرة الروسية، من أجل ضرورة تبني صياغة آلية تنظيمية ملزمة بشأن مكافحة الاستخدام الإجرامي لتقنيات المعلومات والاتصالات تحت رعاية الأمم المتحدة، حيث شمل الخلاف بين القوتين نمطين رئيسيين للصراع، هما (عادل عبد الصادق، صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية، 2021):

1. **النمط الاول:** يتمحور حول توظيف القوة "الناعمة" في التدخل الخارجي، وذلك من خلال محاولة روسيا والولايات المتحدة توظيف الفضاء السيبراني في شن الحرب النفسية أو نشر المعلومات المضللة أو دعم المعارضة الداخلية عبر الأنترنت.
2. **النمط الثاني**: يتمحور حول توظيف القوة "الصلبة" في التدخل الخارجي عبر الفضاء السيبراني من خلال تهديد أمن البنية التحتية المعلوماتية عبر شن هجمات سيبرانية وفيروسات تخريبية، وتطوير استخدام "الأسلحة السيبرانية".

جدول رقم (02): اختلاف الرؤى حول الفضاء السيبراني

اختلاف الرؤي حول الفضاء السيبراني		
القضية	الولايات المتحدة الأمريكية والمملكة المتحدة	روسيا والصين
الفضاء السيبراني	فوضوي	فضاء سيادي
التنظيم	دور مركزي للقطاع الخاص ولا حاجة ضرورية لتدخل الحكومات	دور مركزي للدولة وضرورة التدخل الحكومي
حوكمة الأنترنت (من يصنع السياسات)	مشاركة كافة أصحاب المصلحة (حكومة، قطاع خاص، أكاديمي، مجتمع مدني)	دور أساسي للدول ووضع قواعد ومنظمات جديدة للتعامل مع الظاهرة المستحدثة

المصدر: *عادل عبد الصادق. (2021). "صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية"، تاريخ النشر: 26 جويلية 2019، المركز العربي للفضاء الإلكتروني، تاريخ الاطلاع: (2021/12/26)، نقلا عن الرابط التالي: https://bit.ly/3ltdEwX

وفي إطار تسابق الولايات المتحدة الأمريكية وروسيا لتعزيز أمنها السيبراني في مواجهة أي هجمات محتملة من الطرف الآخر، أنشأ جهاز الأمن الفدرالي الروسي في 10 سبتمبر 2018 مركزا لتنسيق مكافحة الهجمات السيبرانية على البنية التحتية الحيوية في روسيا، يتولى مهام الكشف والوقاية والقضاء على تداعيات الهجمات السيبرانية، وتبادل المعلومات بين الهيئات المتخصصة في الداخل والخارج، وتحليل الهجمات السيبرانية الماضية وتطوير أساليب مكافحتها، وجار العمل على فصل روسيا كلها عن الأنترنت بهدف زيادة فاعلية دفاعاتها ضد الهجمات السيبرانية والقرصنة، حيث أن تداول البيانات بين المواطنين والمؤسسات في هذه الحالة سيكون داخل روسيا لا عن طريق مراكز توجيه دولية، وتجدر الإشارة هنا إلى أن البرلمان الروسي قد وافق في 12 فيفري 2018 على قانون عزل الدولة عن شبكة الأنترنت العالمية، لجعل روسيا في موقع أفضل لصد أي هجمات سيبرانية محتملة من الخارج وبخاصة من الولايات المتحدة الأمريكية، وذلك على غرار نظام "جريت فايروول" الصيني الذي ينظم الأنترنت لتعزيز السيادة الوطنية، ومن ناحية أخرى عملت الولايات المتحدة الأمريكية على تعزيز دفاعاتها السيبرانية أيضا، حيث أنشأت القيادة الإلكترونية الأمريكية مجموعة عمل خاصة لمواجهة أنشطة روسيا في الفضاء السيبراني، إذ وقع الرئيس الأمريكي السابق "دونالد ترامب" مرسوما في 16 أوت 2018 يلغي بموجبه التوجيه الرئاسي لسلفه "باراك أوباما" لتنظيم استخدام الأسلحة السيبرانية ضد معارضي الولايات المتحدة الأمريكية رقم (20) لسنة 2012، على النحو الذي يخفف القيود المفروضة على شن هجمات سيبرانية ضد معارضيها، وقد ظل مضمون هذه الوثيقة سريا حتى عام 2013 عندما كشف الموظف السابق في وكالة الأمن القومي الأمريكية

"إدوارد سنودن" عن عدد من الوثائق السرية المتعلقة بعمل أجهزة الاستخبارات الأمريكية والبريطانية، كما أصدر البنتاغون الأمريكي مطلع سنة 2018 قائمة "لا تشتر" متضمنة أسماء عدد من الموردين الذين ربما تكون قد استهدفتهم مجموعات القراصنة المعادية الذين تدعمهم روسيا والصين، وجرى تعميمها على مسؤولي الشراء الذين يعملون مع الجيش الأمريكي لتزويده بالخدمات المرتبطة بالتكنولوجيا وغيرهم من الفرق المسؤولة عن توفير البرمجيات للقوات المساحة الأمريكية، وعلى الرغم من كل الجهود من يظل سباق الهجمات السيبرانية قائمة، ويتزايد من حين لآخر في ظل التوتر المتزايد بين روسيا والولايات المتحدة الأمريكية، وإعلان الرئيس الأمريكي السابق "دونالد ترامب" تخليه عن حيادية شبكة الأنترنت، وهو الأمر الذي يثير مخاوف القوى الكبرى في النظام الدولي وخصوصا الصين وروسيا اللتين تطالبان بانفتاح أمريكي في التعامل مع فرص السيطرة الدولية على أمن الفضاء السيبراني (محمد، 2021، ص: 169 – 170).

2.4 ملامح التغير في الاستراتيجية الأمريكية تجاه المجال السيبراني:

لقد أقرت الولايات المتحدة استراتيجية جديدة للأمن السيبراني في عام 2018، واتخذت موقفا أكثر حدة في القتال السيبراني والحرب السيبرانية عن ذي قبل، وذلك في مقابل تهديدات كل من الصين وروسيا وآخرين، حيث دخلت حيز التنفيذ بعد قرار الرئيس الأمريكي السابق "ترامب" بإلغاء قواعد حددها سلفه "باراك أوباما" للعمليات السيبرانية، والاتجاه للاستعداد للحرب السيبرانية من خلال بناء قوة أكثر فتكا، وتوسيع التحالفات والشراكات، حيث أن قيام أي دولة بنشاط سيبراني ضدها سيكون الرد بطريقة هجومية ودفاعية ولن يتم بالضرورة في الفضاء السيبراني، وأن فشل عملية ردع الأنشطة السيبرانية التي تشكل استخدام للقوة ضد الولايات المتحدة الأمريكية أو حلفائها ستدفع إلى استخدام القوة المشتركة من القدرات العسكرية ردا على ذلك في المجال المادي، والاتجاه كذلك إلى تبني استراتيجية قائمة على "الهجوم الدفاعي"، والتحرك إلى الإمام خارج الحدود واختراق شبكات الخصم، وتعزيز القدرات لجمع المعلومات الاستخباراتية والاستعداد للصراعات المستقبلية، فمن وجهة نظر الولايات المتحدة الأمريكية؛ أن الفضاء السيبراني يجب أن يعزز من التفوق العسكري وممارسة الأنشطة الاستخباراتية، وحماية الأمن القومي الأمريكي، والعمل على ردع القوى الدولية المنافسة، ومواجهة سرقة الأسرار الصناعية وتهديد البنية التحتية المعلوماتية والنظام الديموقراطي، وذلك من خلال العمل على (عادل عبد الصادق، صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية، 2021):

1 - **ضمان قدرة الجيش الأمريكي**: على القتال وكسب الحروب في أي مجال، بما في ذلك الفضاء السيبراني، وحماية الأمن القومي وردع العدوان الذي قد يشنه الأعداء، والاستجابة السريعة للهجمات السيبرانية التي تمثل استخداما للقوة ضد مصالح الولايات المتحدة الأمريكية وحلفائها وشركائها الاستراتيجيين.

2 - **السعي لشن هجمات استباقية:** هزيمة أو ردع الأنشطة السيئة عبر الأنترنت، والتي تستهدف البنية التحية الحرجة، والتي قد تؤثر في قدرة وزارة الدفاع الأمريكية في القتال والدفاع عن المصالح الوطنية، واعتماد أسلوب الدفاع من خلال ضرب مصادر الخطر خارج حدود الولايات المتحدة الأمريكية قبل أن تصل إلى الداخل.

3 - **تعزيز التعاون مع الهيئات المعنية:** الدفاع مع القطاعين العام والخاص لتنسيق أنماط الاستجابة ونقل الخبرات والتعاون في تنفيذ الاستراتيجية القومية للأمن السيبراني.

4 - **التعاون مع الحلفاء:** من أجل تعزيز القدرة على مواجهة الهجمات السيبرانية، وتعزيز جاهزيتها في مجال الدفاع السيبراني والردع ومواجهة الهجمات وتَشارُك المعلومات للعمل على فاعلية مواجهة التهديدات السيبرانية وتعزيز وضع الأمن السيبراني.

5 - **تعزيز قواعد السلوك الرسمي للدولة:** في الفضاء السيبراني من أجل العمل على تبني المبادئ الطوعية وغير الملزمة لسلوك الدولة في الفضاء السيبراني، وتأييد عمل لجنة فريق الخبراء الحكوميين التابع للأمم المتحدة المعني بالتطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي (UNGGE).

3.4 التغير والاستمرار في الاستراتيجية الروسية في المجال السيبراني:

لم تدشن روسيا قيادة عسكرية للفضاء السيبراني كما فعلت الولايات المتحدة الأمريكية، إلا أنها تعتمد على استراتيجيات جديدة لتعزيز قدراتها في مجال القوة السيبرانية، حيث ترتكز الرؤية الاستراتيجية الروسية على استخدام مصطلح "أمن المعلومات" كمفهوم بديل عن "الأمن السيبراني"، وذلك لأنها ترى أنه مصطلح شامل يغطي الأمن السيبراني باعتباره جزء تابع له، إذ ترى أنه من الصعوبة ممارسة الدولة الرقابة والتنظيم الكامل للأمن السيبراني، حيث تسعى روسيا لبناء معايير دولية من خلال التعاون في الفضاء السيبراني، إما لتعزيز القدرات في مجال مواجهة التهديدات الداخلية لأمن المعلومات أو مواجهة التهديدات الخارجية، ومن ثم فإن أبرز سمات الأمن السيبراني الروسي؛ هو تطبيق السيادة الوطنية على الفضاء السيبراني (Cyber Sovereignty)، لذا فإن "السيادة السيبرانية" ودور الدولة في مجال المعلومات والتنظيم والسيطرة، هي مرتكزات أساسية لاستراتيجية الأمن السيبراني الروسي، وهو ما يجعلها عامل معوق في بناء المعايير الدولية المتعلقة بالأمن السيبراني من وجهة نظر الدول الغربية (عادل عبد الصادق، صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية، 2021).

يذكر المنظور الروسي في العديد من الوثائق المعنية بالعقيدة الروسية في "ضمان أمن المعلومات"، والذي يُظهر نية الحكومة الروسية لقيادة الجهود الدولية لتحقيق درجات عالية من الأمن، وذلك من خلال العديد من الطرق القانونية والمؤسسية والتكنولوجية وغيرها، وهو الأمر الذي يلاقي انتقادات كبيرة من قبل القوى الغربية مثل الولايات المتحدة الأمريكية، والتي ترى أنها تمارس سياسات استبدادية لقمع الحريات للمعارضة الروسية، وأن ذلك يعبر عن تحكم مفرط في الفضاء السيبراني، وذلك على الرغم من أن المبدأ الأول في استراتيجية الأمن السيبراني الروسي قد تضمن حرية المواطنين وحقوقهم الدستورية، وهو ما يعني عن عدم ممارسة سيادتها على الفضاء السيبراني إلى مستوى "السيطرة الكاملة"، ولكن يمكن أن يكون أقرب إلى مستوى "الرقابة"، إذ تحتفظ روسيا بعلاقات تعاونية مع الصين في مجال الفضاء السيبراني عبر اتفاقهما عام 2015، وانضمامها لمنظمة شنغهاي للتعاون، بينما لا توجد علاقات متقاربة مع الولايات المتحدة الأمريكية بشأن التفاوض حول الفضاء السيبراني، ورغم ذلك تصر روسيا على سعيها لإرساء قواعد دولية من خلال التوافق الجماعي الدولي، حيث أن تناقض روسي مع القوى الغربية حول إنشاء معايير الأنترنت

الدولية، خاصة فيما يتعلق بالاختلاف بين تناول ومعالجه مفهومي "الفضاء السيبراني" و"السيادة السيبرانية"، وذلك إلى جانب الخلاف بشأن استخدام السلطة السيادية في الفضاء السيبراني و"لتهديدات السيبرانية"، والتي تُعرِّفها روسيا تحت مصطلح "التهديدات الأمنية المعلوماتية"، حيث تفصل بين تهديدات أمن المعلومات الخارجية والأخرى الداخلية، إذ ترى أنها أكثر حساسية ضد التهديدات السيبرانية الموجة إلى الداخل الروسي (عادل عبد الصادق، صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية، 2021).

ولأجل تحقيق الأمن السيبراني، ذلك تعتمد الاستراتيجية الروسية الخاصة بالحروب السيبرانية مثل الصين على استخدام الأسلحة الإلكترونية الهجومية باعتبار أنها "قوة مضاعفة" (Fore Multiplier) في الحروب، بمعنى أنها تزيد من القدرات القتالية للدولة إذا ما تم استخدامها إلى جانب قدرات عسكرية أخرى، كما تعتد الاستراتيجية الروسية على محاولة تعطيل البنية التحتية المعلوماتية للخصم، والاتصالات المدنية والعسكرية له قبل البدء في العمليات العسكرية التقليدية، فوفقا للعقيدة العسكرية الروسية لا بد وأن يسبق الهجوم العسكري الناجح عمليات أخرى تهدف إلى منع الخصم من حصول على معلومات من مصادر خارجية، وتعطيل عمليات التداول المالية والائتمانية، ومحاولة التأثير على الرأي العام في الدولة الخصم عن طريق المعلومات الخاطئة والدعاية التي تخدم المصالح الروسية، ومن ثم يساعد التخطيط في مرحلة ما قبل الهجوم للقيام بعملية الاختراق السري لأنظمة الخصم في تحقيق هذه الأهداف، وأبرز مثال على تلك الهجمات التي اتهمت روسيا بشنها سنة 2008 ضد جورجيا قبل توجيه ضربة عسكرية ضدها (محمد، 2021، ص: 174 – 175).

4.4 اتجاهات مستقبل الصراع السيبراني بين روسيا والصين والولايات المتحدة الأمريكية:

وتتمثل في (عادل عبد الصادق، صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية، 2021):

1 - الاتجاه الأول: يتمثل من خلال الانتقال من الصراع على السيادة في الفضاء السيبراني إلى الفضاء الخارجي، وخاصة مع حالة التداخل بين كلا المجالين ولمواجهة التهديدات الروسية في مجال القوة الفضائية.

2 - الاتجاه الثاني: من خلال التحول من الصراع "الناعم" على المعلومات والاستخبارات إلى صراع "صلب" على الاستحواذ على القوة السيبرانية ذات الطابع التدميري، والاستثمار في تطوير واستخدام الأسلحة السيبرانية من أجل تعزيز القيادة والسيطرة.

3 - الاتجاه الثالث: وذلك بالانتقال من الطابع العالمي المفتوح للفضاء السيبراني إلى الحمائية الدولية والدفع نحو "البلقنة" وفرض سيادة الدولة الوطنية في مقابل نظرية الفوضى.

4 - الاتجاه الرابع: وذلك من خلال تصاعد بناء القدرات في مجال شن الهجمات السيبرانية المنظمة، والتحول من تبني السياسات الدفاعية إلى أخرى هجومية ذات طابع استباقي وهو ما يهدد بعسكرة الفضاء السيبراني.

5 - **الاتجاه الخامس**: من خلال تأثير تزايد حالة الاحتقان خاصة بين روسيا والولايات المتحدة الأمريكية بسعي كل طرف إلى إيجاد تكتل دولي داعم له وضاغط على الطرف الآخر، خاصة وأن العقوبات الأمريكية على روسيا قد ساعدت في التقارب مع الصين.

6 - **الاتجاه السادس**: من خلال توظيف الفضاء السيبراني لتحقيق أهداف خارجية، والتدخل في الشئون الداخلية من خلال دعم حركات معارضة سياسية أو مسلحة سواء عبر تقديم الدعم التقني أو السياسي أو الإعلامي.

7 - **الاتجاه السابع**: وذلك عبر التوجه لتوظيف الفضاء السيبراني لفرض العقوبات الدولية على السلوك بمنع تصدير تكنولوجيا عسكرية أو تجسسية أو قطع كابلات الأنترنت الموصلة للدولة أو حجب مواقع مساندة للدولة في الداخل.

8 - **الاتجاه الثامن:** عن طريق تصاعد الأنشطة السرية والاستخباراتية وتوظيف برمجيات التجسس والرصد، والتحول من توجيه هجمات سيبرانية من الخارج إلى الداخل إلى توظيف عملاء الاستخبارات أو الدبلوماسيين المقيمين بشن هجمات من الداخل إلى داخل الدولة.

وما يمكن قوله في هذا الصدد أن تصاعد التوتر بين القوتين الأمريكية والروسية إلى جانب الصين ودول أخرى سيعمل على تهديد الأمن الجماعي الدولي، وهو ما يعزز اتجاه إعادة الاعتبار للقانون الدولي والمنظمات الدولية في حفظ الأمن والسلم الدوليين، خاصة وأنه من المرجح أن تنتقل الحرب الباردة الجديدة عبر الفضاء السيبراني إلى داخل المعسكر الغربي من قبل روسيا والصين إلى حين تحقيق التوازن الاستراتيجي في النظام الدولي (عادل عبد الصادق، صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية، 2021)، ولمعالجة تلك الهواجس يشير الأمريكي "روبرت كنيك" في كتابه "حوكمة الأنترنت في عصر انعدام الأمن الإلكتروني"؛ على الولايات المتحدة الأمريكية أن تعمل على وضع قواعد جديدة لسلوك الدول في الفضاء السيبراني، فطوال العقد الأول من القرن الواحد والعشرين كانت الولايات المتحدة الأمريكية تتخذ موقفا معارضا لأي مناقشات حول التجسس والحرب في الفضاء السيبراني، وكانت تسعى لحصر تركيز المجتمع الدولي على معالجة الجريمة الإلكترونية، والاعتراض الأمريكي حسب "روبرت كنيك" نابع من رؤية مفادها: أن الدول أن تحترم التزاماتها بتقييد أنشطتها في الفضاء السيبراني، وأن التحقق من وفاء الدول بالتزاماتها سيكون أمر شبه مستحيل، بيد أن هذا الموقف نابع من تطبيق تجربة الحد من التسلح إبان الحرب الباردة، وهو أمر لا يسهل تطبيقه على مشكلة أمن الفضاء السيبراني الحالية، فالاتفاقات الدولية المحدودة والمركزة يمكن أن تفيد الولايات المتحدة في بعض الحالات، وعلاوة على ذلك فإن عدم رغبة الولايات المتحدة الأمريكية حسبه في خوض مفاوضات حول هذا الموضوع يزيد مصداقية الرأي الذي مفاده: أن الولايات المتحدة الأمريكية تسعى للسيطرة على الفضاء السيبراني (كنيك، 2011، ص: 33).

5. الأساليب الدفاعية المتخذة لتأمين الفضاء السيبراني:

في ظل تنامي التوتر والصراعات في العلاقات بين الولايات المتحدة الأمريكية، روسيا، والصين، لجأت هذه القوى إلى اتخاذ إجراءات للحد من التهديدات الواقعة في الفضاء السيبراني، واتخاذ إجراءات لضبط الهجومات السيبرانية عليها، وكذا تطوير قدراتها الدفاعية من خلال اعتماد الدفاع السيبراني الدفاعي، وذلك عبر ثلاثة أساليب رئيسية وهي:

1.5 الكشف المبكر للهجمات السيبرانية في وقتها الحقيقي: عن طريق:

1 – الاكتشاف (Detect): وذلك باستخدام "الحساسات" (Sensors) الذكية المدعومة بخصائص الذكاء الاصطناعي (البابلي، 2021، ص: 69)، على الشبكات والبرامج والتطبيقات، بالإضافة إلى توظيف المعلومات الاستخباراتية لرصد أي نشاط غير طبيعي قد يصنف على أنه هجمات سيبرانية، وبداية مواجهتها واحتواءها قبل أن تبدأ نشاطها في الشبكة أو النظم المستهدفة (إيهاب خليفة، القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الأنترنت، الولايات المتحدة نموذجا، 2017، ص: 55)، حيث توفر تقنية المعلومات وسائل متنوعة لحماية الشبكات والتي من أهمها: "جدران الحماية" (Firewalls) التي عرفت في جدران الحماية التقليدية بالمصافي، وقد تطورت أخيرا لتصبح أجهزة حماية متعددة الخصائص، "الإدارة الموحدة للتهديدات" (UTM) وهي جدران حماية لديها خصائص متعددة في صندوق واحد، وتتضمن تصفية البريد الإلكتروني الدعائي (Spam)، وإمكانات الحماية من الفيروسات، وكشف ومنع التجسس (IDS/IPS) وتصفية محتوى صفحات الويب، وتوظيف التطبيقات الأمنية للذكاء الاصطناعي من حيث الرصد والتحليل (البابلي، 2021، ص: 70).

2 – الحماية (Protect): وذلك عبر وضع أنظمة للحماية من المخاطر الإلكترونية المحتملة، فبمجرد تحديد المخاطر الإلكترونية المحتملة، فإنه يجب العمل على الحماية منها من خلال وضع الضمانات المناسبة وتنفيذها، وذلك للعمل على استمرارية تقديم خدمات البنية التحتية الحيوية وعدم تأثرها بالهجمات السيبرانية (البابلي، 2021، ص: 70).

2.5 الهجوم السيبراني الإستباقي:

وذلك من خلال استخدام ونشر "الديدان البيضاء" (White Worms)، وهي برامج قادرة على اكتشاف التطبيقات الضارة وتدميرها قبل توظيفها في إطلاق هجمات سيبرانية محتملة، كما تقوم أيضا بتدمير أدوات وبرمجيات القراصنة، وهو ما يساعد في إحباط مخطط الهجمات نفسها، وتحديد هوية ومصدر الهجمة، بما يمكن من إطلاق هجمة إلكترونية مضادة فيما تعرف بـ "الاختراق العكسي" (Hack-back).

3.5 التضليل والإخفاء (الخداع):

وهو ما يتحقق عن طريق إخفاء هويات الأهداف الاستراتيجية للدولة على الأنترنت وتضليل الخصم أثناء محاولة الوصول إليها أو اختراقها، من خلال أدوات التمويه والخداع وتغيير ملامح الأهداف الاستراتيجية للدولة، بما يساعد على تضليل الخصم وتشتيت الانتباه عن الهدف الرئيسي (إيهاب خليفة،

القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الأنترنت، الولايات المتحدة نموذجا، 2017، ص: 55).

وتجدر الإشارة إلى هناك العديد من العوامل التي تعقِّد من مهمة الدفاع في الفضاء السيبراني وقد حدد "لوكاس كيلو" (Lukas Kello) أهمها فيما يلي (فاتح حارك ورياض حمدوش، 2022)، ص: 139 - 140):

1 – صعوبة التنبؤ بالهجوم السيبراني.

2 – احتمال بقاء الهجوم غير مكتشف.

3 – التعقيد الكبير الذي يتميز به الفضاء السيبراني وصعوبة اكتشاف كل الثغرات الموجودة في النظام.

4 – المخاطر المتعلقة باسترداد الأجهزة والقطع التكنولوجية، حيث أن أنظمة الكمبيوتر تعتمد بشكل كبير على القطع التكنولوجية مثل المعالجات وبطاقات الرسومات وغيرها التي تصنعها شركات مختلفة، وبالتالي يتزايد الشك حول إمكانية تحميل تلك القطع ببرامج ضارة بغرض استخدامها فيما بعد.

وعلى إثر ذلك قامت كل من روسيا، الصين، الولايات المتحدة الأمريكية، بتطوير عقيدتها الأمنية، وأصبحت تعتبر الفضاء السيبراني مسرحا للعمليات العسكرية، كما أوجدت قيادات خاصة ومستقلة لقيادة العمليات السيبرانية (زروقة، 2019، ص: 1026)، والتي لديها وحدات قتالية خاصة بالحرب السيبرانية، حيث تتميز بقدراتها الهجومية والدفاعية المتقدمة، ولعل أبرز تلك الوحدات القتالية: القيادة السيبرانية الأمريكية (US Cyber Command) والتي استحدثها البنتاغون في شهر جوان 2009، ومهمتها الرد على هجمات قراصنة المعلومات وتنفيذ عمليات في الفضاء السيبراني؛ الوحدة 61398 في الصين والتي تتسم بأنشطتها السرية داخل جيش التحرير الشعبي الصيني، حيث تقوم بعمليات التجسس الإلكتروني وقرصنة المعلومات والبيانات، وقد بدأت في شن أول هجماتها منذ عام 2006؛ قراصنة الظل التابعين للحكومة الروسية وهم من الطلبة المتميزين في استخدام الحاسب الآلي والذين أدمجتهم وزارة الدفاع الروسية في وحدات علمية خاصة، وتجدر الإشارة إلى أن روسيا تمتلك عدد كبير من القراصنة سواء المتطوعين أو الذين تم توظيفهم لخدمة أغراض عسكرية، وقد وظفتهم روسيا عان 2007 بشن هجمات سيبرانية سريعة ومدروسة شاملة على إستونيا أدت إلى دمار لوجستي كبير (خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي، 2019، ص: 151 – 155).

6.الخاتمة:

لقد تزايد استخدام الفضاء السيبراني بشكل واسع في ظل التقدم والتطور التكنولوجي واعتبارها بعدا خامسا للحروب، الأمر الذي أدى إلى نقل الحروب والصراعات بين الولايات المتحدة الأمريكية وروسيا والصين إليه، في ظل صعوبة اللجوء إلى حروب تقليدية بينها في الوقت الراهن، إذ لجأت إلى الفضاء السيبراني في إدارة صراعاتها، والسعي لامتلاك التكنولوجيا المتقدمة لخدمة الأساليب الدفاعية لتأمين الفضاء السيبراني الذي أصبح يمس بسيادة الدول في النظام الدولي، واعتبارا لما تم ذكره أعلاه فقد خلص هذا البحث إلى النتائج التالية:

1 – أصبح الفضاء السيبراني مجالا خامسا للحرب بين القوى الكبرى (روسيا، الصين، الولايات المتحدة الأمريكية) من أجل بسط السيطرة والهيمنة، وهو ما خلق تنافسا بينها.

2 – أصبح هناك سعي روسي – صيني لإقامة نظام أمن سيبراني عالمي لمنع الولايات المتحدة الأمريكية من محاولاتها للسيطرة على الفضاء السيبراني وفرض رؤاها بخصوصه.

3 – لقد فرضت الهجمات السيبرانية والحروب السيبرانية فكرة النظر في السيادة الكاملة، التي أصبحت في حالة انكشاف أمني وهو ما كان الخلاف حوله من طرف الصين، روسيا، الولايات المتحدة الأمريكية.

4 – تعمد كل من الولايات المتحدة الأمريكية، روسيا والصين إلى اللجوء إلى الحروب السيبرانية لإدارة صراعاتها البينية، نظرا لصعوبة تحديد هوية المهاجمين عبر الفضاء السيبراني، ولصعوبة حدوث حروب تقليدية مباشرة على أرض الواقع، وقد ازدادت تلك الحروب في السنوات الأخيرة نظير حالة التنافس على التكنولوجيا الفائقة التطور، وكذا التنافس الاقتصادي، والظروف التي خلقتها مختلف الصراعات الراهنة في النظام الدولي.

7.المراجع:

1 – باللغة العربية:

[1]- البابلي، عمار ياسر زهير البابلي. (2021). "التحديات الأمنية المعاصرة للهجمات السيبرانية"، *مجلة الفكر الشرطي*، م. 30، ع. 118، ص ص: 27 – 70.

2 – العقبي، ابتسام عبد الزهرة. (2022). "نظرية قلب الارض بين الجغرافيا والفضاء الالكتروني (رؤية مستقبلية)"، (2022/02/10)، نقلا عن الرابط التالي: https://bit.ly/3zJqhZH

3 - باسيت، جون. (2014). "حرب الفضاء الإلكتروني: التسلح وأساليب الفاع الجديدة"، في: *الحروب المستقبلية في القرن الحادي والعشرين*، أبو ظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية.

4 - بلعسل بنت نبي، ياسمين وعمروش، الحسين. (2021). "التهديدات الإلكترونية والأمن السيبراني في الوطن العربي"، مجلة نوميروس الأكاديمية، م. 2، ع. 2، ص: 165.

5 - بريوش، نضال ناجي بدوي. (2019). "الصراع السيبراني مع العدو الصهيوني"، دراسة منشورة مقدمة للحصول على دبلوم الدراسات الفلسطينية من أكاديمية دراسات اللاجئين، ص ص: 9 – 12.

6 - حارك، فاتح وحمدوش، رياض. (2022). "الدولة بين الهيمنة وتحقيق الأمن في الفضاء السيبراني"، *المجلة الجزائرية للأمن الإنساني*، م. 7، ع. 1، ص ص: 137 – 140.

7 - خليفة، إيهاب. (2017). *القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الأنترنت؟، الولايات المتحدة نموذجا*، القاهرة: العربي للنشر والتوزيع.

8 - خليفة، إيهاب. (2019). "الصراع الأمريكي – الصيني على التكنولوجيا الفائقة الذكاء"، *مجلة السياسة الدولية*، م. 54، ع. 218، ص: 91.

9 - خليفة، إيهاب. (2019). *مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي*، القاهرة: العربي للنشر والتوزيع.

10 - زروقة، إسماعيل. (2019). "الفضاء السيبراني والتحول في مفاهيم القوة والصراع"، *مجلة العلوم القانونية والسياسية*، م. 10، ع. 01، ص: 1026.

11 - شلوش، نورة. (2019). "القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول"، *مجلة مركز بابل للدراسات الإنسانية*، م.8، ع.2، ص: 190.

12 – عبد الصادق، عادل. (2021). "صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية"، تاريخ الاطلاع: 26 جويلية 2019، المركز العربي للفضاء الإلكتروني، تاريخ الاسترجاع: (2021/12/26)، نقلا عن الرابط التالي: https://bit.ly/3ltdEwX

13 - عبد الصادق، عادل. (2017). "أنماط الحروب السيبرانية وتداعياتها على الأمن العالمي"، *مجلة السياسة الدولية*، ملحق اتجاهات نظرية، م. 52، ع. 208، ص: 33.

14 - عبد الصبور، سماح. (2017). "الصراع السيبراني .. طبيعة المفهوم وملامح الفاعلين"، *مجلة السياسة الدولية*، ملحق اتجاهات نظرية، م. 52، ع. 208، ص: 6.

15 – علي، زياد علي. (2020). *الصراع والأمن الجيوسيبراني في الساحة الدولية: دراسة في استراتيجيات الاشتباك الرقمي*، عمان: دار أمجد للنشر والتوزيع.

16 – كنيك، روبرت. (2011). *حوكمة الأنترنت في عصر انعدام الأمن الإلكتروني*، أبو ظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية، سلسلة دراسات عالمية، ع. 95.

17 - محمد، أماني عصام. (2021). "استخدام روسيا القوة السيبرانية في إدارة تفاعلاتها الدولية"، *مجلة دراسات*، مركز الأهرام للدراسات الاستراتيجية، القاهرة، م. 22، ع. 4، ص ص: 169 – 175.

2 – باللغة الأجنبية:

18 – Robinson, Joe. (2022). "Cyberwarfare statistics: A decade of geopolitical attacks", 21 November 2021, privacy affairs, (28/01/2022), see the link: https://bit.ly/3v17Nno

19 – S. Nye, Josef. (2011). *The Future of Oower*, New York: Public Affairs.