Journal of Al-Farabi for Humanity Sciences (3) Issue (1) May(2024)

ISSN: 2957-3874 (Print)
Journal of Al-Farabi for Humanity Sciences (JFHS)
https://www.iasj.net/iasj/journal/419/issues
مجلة الفارابي للعلوم الإنسانية تصدرها كلية الفارابي الجامعة

الاستراتيجيات والسياسات المتبعة لمواجهة التهديدات السيبرانية

أ.م .د. عمر عبدالله عفتان

جامعة كلكامش كلية العلوم السياسية

Strategies and policies to confront cyberspace Threats

AssistantProfessor Doctor. Omar Abdullah Aftan
Gilgamesh University- Colleg of Political Science
Dromarabdullah0@gmail.com

الملخص

أصبح الفضاء السيبراني يمثل ساحة جديدة للحرب ومصدراً لتهديدات خطيرة تواجه الأمن القومي للدول، حيث كلما تزايد ارتباط الدول بالفضاء السيبراني لإدارة شؤونها كلما تزايدت التهديدات السيبرانية لأمنها القومي مما يجعلها عرضة لهجمات متعددة وخطيرة، خاصة في ضوء التقدم التكنولوجي السريع وتطور العمليات السيبرانية الهجومية وتنامي قدراتها التدميرية وتهديداتها للأمن القومي، حيث برزت مصادر جديدة للمخاوف والتهديدات المتعلقة بالأمن القومي مع ظهور الفضاء السيبراني ودور الفاعلين من غير الدول في النظام الدولي، وقد ظهرت انماط جديدة من الصراعات السيبرانية القائمة على الانترنت والتكنولوجيا الحديثة، بدءاً من الجريمة الالكترونية العابرة للحدود الوطنية، والتجسس بالاعتماد على أدوات الفضاء السيبراني، والإرهاب السيبراني إلى الهجمات والحروب السيبرانية التي يمكن أن تعطل النظم العسكرية أو تغلق خوادم الحكومات او تدمر البنى التحتية . لقد صار الفضاء السيبراني عالماً افتراضياً يعكس الواقع المادي الحقيقي بكل تعقيداته. لقد شهدت السنوات الأخيرة تزايداً كبيراً في الهجمات السيبرانية المدفوعة بأهداف سياسية وتوظيفها في إطار تحقيق أهداف السياسة الخارجية، أو التلاعب بالعمليات الانتخابية في الدول المعادية فضلاً عن توظيفها في إطار ما يسمى بـ "الاستخبارات السيبرانية" وبذلك أضحت قضية الأمن السيبراني تتصدر بشكل متزايد أجندة الأمن القومي للعديد من دول العالم .**الكلمات المفتاحية: الاستراتيجيات – السياسات – التهديدات السيبرانية – الأمن القومي.**

Abstract

Cyberspace has became a new dimension of wars and a source of serious of countries. The expansion by various countries and institutions in employing cyberspace to manage their affair in the political, economic, military, ect fields means, as a result, an increase in the possibilities of being exposed to multiple and dangerous cyber attacks, especially in light of the rapid and noticeable technological progress and software with highly advanced capabilities, and the resulting challenges and threats related to the national security of countries.Cross – border electronic attacks, electronic espionage operations, and cyber terrorism have become a new type of war and conflict between countries in our current era.These electronic attacks and operations through cyberspace can be used militarily to target an disrupt various military systems, politically by manipulating election results, and economically and socially when, for example, targeting and destroying infrastructure.Achieving cyber security has become one of the most important pillars of national security strategies and policies for many countries in the world, as a result of the increase in cyber attacks in recent years as a means of achieving political, economic, military, and social goals that threaten national security and stability of the countries.

المقدمة

أصبح الفضاء السيبراني مجالاً متزايداً لتنافس الدول والفاعلين من غير الدول، وأحياناً يصل هذا التنافس الى مستوى الصراع بين هؤلاء الفاعلين، وقد يأخذ هذا الصراع نمطين، النمط الأول الحوادث الفردية وهي الحوادث والعمليات التي تتم على فترات متباينة وليست مستمرة لفترة معينة، أما النمط الثاني فهو النزاعات السيبرانية والتي تدار عبر أدوات سيبرانية بين دولتين خلال فترة زمنية معينة وربما يشتمل على حادثة أو أكثر من الحوادث

الفردية، وقد أحدثت تكنولوجيا المعلومات تغييراً وتأثيراً على استخدام القوة العسكرية، وعلى نوعية الاسلحة سواء الدفاعية أو الهجومية، أن تكنولوجيا المعلومات اضافت ابعاداً أخرى للقوة العسكرية مثل استخدامها في شن هجمات سيبرانية ضد الأعداء؟ وتسعى العديد من الدول إلى تحديث قدراتها السيبرانية سواء الدفاعية أو الهجومية وكذلك الاستثمار في البنية السيبرانية التحتية المعلوماتية وتأمينها، وان هناك دول سيبرانية عظمى تمتلك قدرات سيبرانية هجومية، في مقدمتها الولايات المتحدة وروسيا والصين فضلاً عن شركات البرمجيات العالمية الأكبر انتاجاً لبرامج وتطبيقات القوة السيبرانية الفاعلة، وتنوعت مواقف الدول من تهديدات الفضاء السيبراني، ما بين اتخاذ سياسات وتبني استراتيجيات للأمن السيبراني، وإصدار القوانين والتشريعات الخاصة بالأمن السيبراني، وكذلك استحداث وحدات عسكرية خاصة لتنفيذ عمليات الدفاع والهجوم السيبراني.

هدف البحث: يتجلى في قلة الدراسات العلمية التي تناولت قضية التوظيف السياسي للهجمات السيبرانية حيث يحتاج إلى المزيد من الدراسة والبحث العلمي، كونه من الموضوعات الحديثة في علم السياسة بشكل عام وحقل العلاقات الدولية بشكل خاص مما يستدعي مزيداً من البحث والدراسة، حيث يحتاج صانع القرار إلى دراسات توضح كيف يتم توظيف الهجمات السيبرانية وأدوات الفضاء السيبراني لتحقيق أهداف سياسية والوقوف على الأسباب التي أدت إلى تزايد هذه النوعية من الهجمات خلال السنوات الأخيرة، فضلاً عن معرفة ردود أفعال الدول للتعامل مع هذه الهجمات.

إشكالية البحث: تتمثل المشكلة البحثية في رصد وتحليل الأسباب التي أدت إلى تزايد الهجمات السيبرانية المدفوعة بأهداف سياسية خلال السنين الأخيرة مع الوقوف على أهم انماط التوظيف السياسي لهذه الهجمات، والسؤال الرئيس هو:

لماذا تزايدت الهجمات السيبرانية المدفوعة بأهداف سياسية خلال السنين الأخيرة؟ وما هي أنماط التوظيف السياسي لهذه الهجمات؟

منهجية البحث: يعتمد على منهج قياس وتحليل القوة بالتطبيق على القوة السيبرانية، وذلك في ضوء استخدام الدول والفاعلين من غير الدول للقوة السيبرانية لشن هجمات سيبرانية ضد أطراف أخرى لتحقيق أهداف أهمها الأهداف السياسية.

هيكلية البحث: تم تقسيم البحث إلى ثلاثة مباحث تناول المبحث الأول الاستراتيجية السيبرانية لروسيا الاتحادية، وتطرق المبحث الثاني إلى الاستراتيجية السيبرانية للصين، فيما ركز المبحث الثالث على الاستراتيجية السيبرانية للولايات المتحدة الأمريكية.

المبحث الأول الاستراتيجية السيبرانية لروسيا الاتحادية

تسعى الاستراتيجية السيبرانية الروسية إلى الحد من الاختراق السيبراني الخارجي لروسيا ومقاومة التأثير الأجنبي المحتمل من خلال أدوات الفضاء السيبراني؛ حيث راقبت روسيا كيف تم استخدام أداة نشر المعلومات في إطار حرب المعلومات لتحقيق التغيير السياسي والإطاحة بنظم الحكم القائمة خلال العقد المنصرم في دول الاتحاد السوفيتي السابق بواسطة الثورات الملونة، وبالتالي تخشى روسيا من استخدام الخصوم سلاح المعلومات ضدها كما تشارك روسيا الصين في الاعتقاد بأهمية السيادة الوطنية على الفضاء السيبراني[١]. فقد لعبت أدوات الفضاء السيبراني دورا خطيرًا في الحركات الاحتجاجية والثورات الملونة في الدول المجاورة لروسيا مثل جورجيا في ٢٠٠٣، واوكرانيا في ٢٠٠٤، وقيرغيزستان ٢٠٠٥، ولذلك عملت روسيا على تعزيز الدفاعات السيبرانية والتفكير في كيفية مواجهة مثل هذه المخاطر[٢].وفي نهاية عام ٢٠١١ صدر أول بيان رسمي حول دور الجيش الروسي في الفضاء السيبراني، وأصبح من أهم مهام القوة السيبرانية الروسية أن تعمل على الوقاية من حروب المعلومات؛ حيث تعتبر روسيا الحرب السيبرانية جزءًا من حرب المعلومات[٣]. وتنتظر روسيا إلى الجانب المعلوماتي للقضايا السيبرانية باهتمام شديد ويشعر بعض صناع السياسة الروس أن تفكك الاتحاد السوفيتي السابق كان بسبب هجوم إدراكي أو معلوماتي بواسطة عملية إعلامية متعمدة؛ كما تناقش العديد من الدراسات الروسية "الحرب العالمية الثالثة" على أنها حرب معلومات بالأساس. وبشكل عام لا تفضل روسيا على المستوى الرسمي استخدام مصطلح "سايبر "Cyber، ولكنها تفضل استخدام مصطلح "حرب المعلومات" للحديث عن الأضرار أو التهديدات التي تواجه أمن المعلومات. ويعطي العسكريون الروس أهمية خاصة للمعلومات في إطار العمليات النفسية؛ معتبرين أن التهديد النفسي للدولة هو تهديد رئيسي لأمنها في القرن الواحد والعشرين. لذلك فإن المفهوم الاستراتيجي الروسي يركز على حماية الدولة من المعلومات الضارة؛ مع التركيز في الوقت نفسه على القوانين الدولية التي يمكن أن تقيد استخدام وتطوير الدول لـ "أسلحة المعلومات" Information Weapons صمت ممصمل وهو مصطلح يستخدم غالبًا في روسيا[٤]وقد أنشأ جهاز الأمن الفيدرالي الروسي مركزًا وطنيًا لتنسيق مكافحة الهجمات السيبرانية على البنية التحتية الحيوية الروسية في سبتمبر عام ٢٠١٨ ووفقًا ل ألكسندر بورتنيكوف رئيس الجهاز فإنه أمر بإنشاء مركز للتنسيق الوطني بشأن حوادث الكمبيوتر بهدف الكشف والوقاية والقضاء على العواقب الناجمة عن الهجمات المرتبطة بالحواسب الآلية؛ وتبادل المعلومات مع الهيئات المتخصصة ومع الشركاء الأجانب؛ وأيضًا بهدف تحليل الهجمات السيبرانية الماضية وتطوير الأساليب المناسبة لمكافحتها[٥].ولقد دعت روسيا مرارًا إلى عقد معاهدة دولية تمنع أو على الأقل تقيد من التهديدات

السيبرانية وتحول دون حدوث سباق تسلح سيبراني؛ على أن تشتمل المعاهدة على تعريف للعدوان في الفضاء السيبراني يكون متفقًا عليه من جانب المجتمع الدولي؛ وكذلك تعريف الأسلحة السيبرانية؛ وذلك في ضوء نظر روسيا بقلق إلى تطور القدرات السيبرانية لدى بعض الفواعل من الدول وغير الدول والتي من شأنها مساعدة أجهزة الأستخبارات الأجنبية على اختراق روسيا من خلال وسائل تقنية[٦]وقد أيدت مجموعة دول لبريكس BRICS اقتراحاً روسياً لإنشاء اتفاقية الأمم المتحدة للتعاون في مكافحة الجرائم المعلوماتية على أساس أنها آلية تنظيمية ملزمة من شأنها مكافحة الاستخدام الإجرامي لتقنيات المعلومات والاتصالات تحت إشراف ورعاية الأمم المتحدة. وقد هدفت روسيا من الاتفاقية إلى وضع قواعد لسلوك الدول في الفضاء السيبراني وتعزيز التعاون الدولي فيما يتعلق بالتحقيق المشترك في الأنشطة السيبرانية الخبيثة؛ ولكن الولايات المتحدة رفضت الاقتراح الروسي مُدّعية أن هذه الاتفاقية من شأنها تعزيز القدرات الروسية وقدرات عدد من الدول التي وصفتها بأنها سلطوية' في السيطرة على الفضاء السيبراني داخلها وذلك على حد زعمها[٧].وفي إطار تحدي روسيا للهيمنة الأمريكية على الفضاء السيبراني؛ وقع الرئيس بوتين في الأول من مايو لعام ٢٠٠٩ على مشروع قانون يهدف إلى ضمان التشغيل المستدام لـ "رونت" Runet وهو الجزءِ الروسي من الإنترنت العالمي. ونص التشريع الجديد – الذي قد يكلف روسيا نحو ٤٦٦؛ مليون دولار أمريكي – على مجموعة من التدابير والاجراءات اللازمة لضمان تشغيل الإنترنت الروسي ومكافحة التهديدات السيبرانية؛ وهي تشمل إنشاء نظام أسماء نطاقات وطني Domain Name System لتخزين جميع عناوين بروتوكول الإنترنت IP Address وجميع أسماء النطاقات بعيدًا عن منظمة الأيكان ICANN وهي هيئة الإنترنت للأسماء والأرقام المخصصة والتي تتخذ من الولايات المتحدة مقراً لها وتعمل وفق عقد موقع مع الحكومة الأمريكية. حيث تعد أيكان المنظمة أو الجهة المعنية بتشغيل شبكة الإنترنت حول العالم. كما يقيد القانون نقل بيانات مستخدمي الإنترنت الروس إلى خوادم Servers خارج البلاد. وبالتالي إذا قررت الولايات المتحدة قطع خدمة الإنترنت عن روسيا سيكون لدى هذه الأخيرة قطاع مستقل من الإنترنت يعمل بسلاسة ويضمن التواصل ونقل البيانات بين المستخدمين الروس. ورغم عدم وجود سوابق لحجب الإنترنت عن عمد لبلدان بأكملها، إلا أن الخبراء في هذا المجال يؤكدون أن ذلك ممكن تقنياً[٨].وقد اندفعت وسائل إعلام غربية وبعض المعارضون الروس إلى اتهام روسيا ببناء "إنترنت سيادي"؛ على غرار ما شيدته الصين على مر السنين. ولكن الحكومة الروسية نفت ذلك؛ وأوضح خبراء روس أن التشريع يتم تحريفه في وسائل الإعلام؛ وأنه يحتوي على مكونان، الأول هو التأكد من استمرار عمل الإنترنت إذا تم إغلاقه من الخارج؛ وهو احتمال وارد وروسيا ليست مستعدة تمامًا لذلك. أما الجزءِ الثاني فيتعلق بتزويد السلطات الروسية بالأدوات التقنية اللازمة لمواجهة التحديات الناشئة عن الهجمات السيبرانية المحتملة على الشبكات الوطنية[٩].ومن جهة أخرى؛ وفي مارس عام ٢٠١٩ وقع الرئيس الروسي فلاديمير بوتين قانوناً المواجهة الأخبار الكاذبة والمشوهة للحقائق (المزيفة)؛ وفرض القانون حظرًا على "نشر معلومات عامة غير موثوقة في شبكات المعلومات والاتصالات؛ تحت ستار الأخبار الموثوقة؛ والتي تخلق تهديدًا يلحق الضرر بحياة أو صحة المواطنين؛ أو الممتلكات أو تشكل تهديدًا بحدوث اضطرابات عامة بالنظام العام والأمن العام أو التي تخلق إعاقة في عمل المرافق الحيوية الهامة من مواصلات أو بنية تحتية اجتماعية أو عمل المنظمات الائتمانية المالية أو مواقع الطاقة أو الصناعة أو الاتصالات". وفي حال العثور على مثل هذه المعلومات في مواردٍ الإنترنت المسجلة وفقاً للقانون الروسي الخاص بوسائل الإعلام العامة؛ فسيتقدم المدعي العام الروسي أو ممثلوه، بطلب إلى هيئة مراقبة الاتصالات الروسية "روسكومنادزور" Roskomnadzor لاتخاذ تدابير لحجب الوصول إلى المواقع الإلكترونية ذات الصلة[١٠].وكثيرًا ما تؤكد الكتابات الأمريكية والغربية أن روسيا لديها مخاوف عميقة من حرية تبادل المعلومات عبر الفضاء السيبراني والتي قد تشكل تهديدًا محتملاً للمجتمع أو الدولة؛ وأنها بذلك تتناقض مع الإجماع الغربي حول حرية تداول المعلومات؛ وأن هذه الاختلافات تقوض محاولات التوصل إلى اتفاق على مبادئ أو قواعد الفضاء السيبرائي العالمي[١١]فبينما ترى الدول الغربية – خاصة الولايات المتحدة الأمريكية وبعض حلفائها الأوروبيين الفضاء السيبراني مفتوحًا ومشتركًا بين كافة الدول Open and Shared تعمل روسيا في المقابل – من وجهة نظرهم – على إنشاء شبكة إنترنت وطنية مستقلة ومُخطط لها أن تكون غير متصلة بشبكة الإنترنت العالمية خلال عام ٢٠٢٠[١٢]. إلا أن الرئيس الروسي فلاديمير بوتين – في اجتماع له مع ممثلي وكالات الأنباء الروسية في ٢٠ فبراير ٢٠١٩ – أكد أن روسيا لا تعتزم قطع ذاتها عن شبكة الإنترنت؛ لكنه أشار إلى أهمية تعزيز "السيادة الرقمية' بالنسبة إلى روسيا وأوضح أن قطع الإنترنت عن روسيا أمر ممكن» ولذلك من الضروري إنشاء قطاعات مستقلة مرتبطة بالإنترنت.وعلى خلفية تصاعد الاتهامات الموجهة ضد روسيا من قبل الولايات المتحدة الأمريكية وبعض الدول الغربية بشأن شنها هجمات سيبرانية ضد الولايات المتحدة وعدد من الدول الأوروبية؛ أكد الرئيس فلاديمير بوتين – على هامش مؤتمر للأمن السيبراني عُقد في موسكو يوليو ٢٠١٨ – أن عدد الهجمات السيبرانية ضد بلاده في الربع الأول من عام ٢٠١٧ قد ارتفع بمقدار الثلث مقارنة بالفترةٍ ذاتها من عام 2017 داعيًا إلى توحيد جهود جهات إنفاذ القانون ومجتمعات الأعمال والمنظمات العامة والمواطنين لمواجهة خطر هذه الهجمات. وفي أكتوبر من من عام ٢٠١٨ أشار رئيس الوزراء الروسي ديمتري ميدفيديف

في منتدى موسكو الدولي "الابتكار المفتوح – ٢٠١٨" أن الخبراء أكدوا أن خسائر دول العالم المترتبة على الهجمات السيبرانية في الفضاء السيبراني بلغت في عام ٢٠١٧ فقط نحو تريليون دولار أمريكي؛ وفي روسيا وحدها بلغت الأضرار الناجمة عن الهجمات السيبرانية في عام ٢٠١٧ نحو ٦٠٠ مليار رويل أي ما يقارب ٩ مليار دولار(١٣).وفي سياق متصلء تجدر الإشارة إلى أن روسيا قد طورت قدرات فائقة ومتميزة في مجال الحرب الإلكتر ونية' Electronic Warfare ومن الواضح أنها تتفوق على الولايات المتحدة في هذا السياق؛ وذلك وفقًا لشهادة كبار العسكريين في الجيش الأمريكي. ففي يوليو من عام ٢٠١٨ أشار براين سوليفان Brian Sullivan وهو عقيد في الجيش الأمريكي – إلى أن قواته واجهت بيئة حرب الكترونية مزدحمة" أثناء قتالهم في شمال شرق سوريا خلال فترة انتشارهم التي استمرت تسعة أشهر وامتدت من سبتمبر ٢٠١٧ إلى مايو ٢٠١٨. وأوضح الجنرال ريموند توماس Raymond Thomas قائد قيادة العمليات الخاصة الأمريكية Head of U.S. special Operations Command في مؤتمر عُقد في فلوريدا أبريل عام ٢٠١٨ أن بيئة الحرب الإلكترونية الروسية في سوريا أصبحت أكثر بيئة عدوانية على هذا الكوكب". مؤكدًا أن الروس "يختبروننا كل يوم" مشيرًا إلى الروس يقومون بإيقاف الاتصالات وحتى تعطيل الطائرات المصممة للحرب الإلكترونية. ويتهم المحللون الغربيون روسيا بأنها تستخدم سوريا بشكل متزايد لاختبار الأسلحة الإلكترونية الروسية الجديدة والتي طورتها موسكو على مدى السنوات العشر إلى الخمس عشرة سنة الماضية؛ في تحدي لهيمنة حلف الناتو على الأسلحة التقليدية؛ معتبرين أن العمليات العسكرية في أوكرائيا قد منحت موسكو فرصة مماثلة لاستخدام هذه الأنظمة الجديدة في القتال، كما أتاح الصراع في سوريا الفرصة لروسيا لمعرفة كيفية استجابة الأنظمة الأمريكية المتطورة لهجمات الحرب الإلكترونية(١٤).وقد دفع هذا التفوق الروسي المسئولين العسكريين الأمريكيين إلى الاعتراف بأن الولايات المتحدة يجب عليها تطوير قدرات الحرب الإلكترونية للحاق بالركب؛ لأنهم تأخروا عن الروس في هذا المجال. ففي أكتوبر من عام ٢٠١٥ صرح رونالد بونتيوس Ronald Pontius نائب قائد القوات السيبرانية الامريكية Deputy to Army Cyber Command's Chief أن الولايات المتحدة لا تحرز تقدمًا بالسرعة التي يتطلبها التهديد"؛ أما الكولونيل جيفري تشيرش Jeffrey Church قائد وحدة الحرب الالكترونية بالجيش الأمريكي The Army's Chief Electronic Warfare فقد أشار إلى صعوبة تحقيق قوات الحرب الإلكترونية الأمريكية تقدمًا ملموسًا لأن ذلك يتطلب تجاوز النقص في كلا من معدات الحرب الإلكترونية» والقوة العسكرية التي تقلصت 'بعشرات الآلاف من الجنود في ظل وجود ميزانية عسكرية ضعيفة(١٥).ومن جهة أخرى؛ يبدو من الواضح أن روسيا ترفض هيمنة الولايات المتحدة على الفضاء السيبراني من خلال امتلاك الأخيرة وإدارتها منفردة لنظام تحديد المواقع العالمي جي بي إس The Global Positioning System (GPS)، حيث أنه مملوك ومدار من قبل وزارةٍ الدفاع الأمريكية. ولذلك رفضت استخدام النظام الأمريكي وطورت نظام تحديد مواقع وطني روسي خاص بها وهو جلوناس GLONASS. غير أن الولايات المتحدة كثيرا ما اتهمت روسيا بمحاولة التشويش على النظام الأمريكي. فقد اتهم المجلس الاستشاري الوطني لتحديد المواقع والملاحة والتوقيت Positioning, Navigation, and Timing Advisory Board أو ما يُعرف اختصاراً بـ (PNT Advisory Board) – وهو هيئة مستقلة تقدم المشورة للحكومة الأمريكية بشأن نظام تحديد المواقع العالمي (GPS) – اتهم روسيا في مايس ٢٠١٨ بأنها قامت بالتشويش على نظام تحديد المواقع العالمي في بحر البلطيق في عام ٢٠١٧ خلال مناورات 'زاباد" Zapad العسكرية الروسية في مناطقها الغربية في سبتمبر ٢٠١٧ بالقرب من دول البلطيق، مشيراً أنها فعلت ذلك مراراً في شرق البحر المتوسط وأيضًا في أكتوبر ٢٠١٧ خلال مناورات حلف شمال الأطلسي (الناتو)؛ والتي عقدت في النرويج. حيث فشلت إشارات جي بي إس عبر أقصى شمال الترويج وفنلندا، وأجبرت الطائرات المدنية على التنقل يدويّا، كما لم يعد بإمكان المواطنين العاديين الوثوق بهواتفهم الذكية. ولذلك يرى المجلس الاستشاري PNT أن هدف روسيا من التشويش على النظام الأمريكي هو تشجيع اعتماد واستخدام نظام تحديد المواقع الروسي "جلوناس" بدلاً من النظام الأمريكي العالمي وتخويف جيرانها بشكل عام من الاعتماد على التكنولوجيا الأمريكية.ويُعد نظام تحديد المواقع العالمي الذي تملكه وتديره وزارةٍ الدفاع –الأمريكية هو الأكثر استخدامًا حول العالم؛ حيث أنه يوفر لأي شخص مدني حرية الوصول إليه باستخدام جهاز استقبال جي بي أس، ولذلك فأغلب الهواتف الذكية في مختلف دول العالم والتي يتم تصنيعها في الوقت الحاضر يكون مُثبتًا بها نظام تحديد المواقع العالمي GPS–enabled كما يستخدم تسعة من كل عشرة من مالكي الهواتف الذكية التطبيقات المدعومة من نظام جي بي إس؛ ولكن الصين – على العكس من ذلك – تدير نظام الملاحة عبر الأقمار الصناعية المملوك لها "بايدو" BeiDou؛ كما يدير الاتحاد الأوروبي بدوره نظام الملاحة "غاليليو" Galileo وهو مستقل عن جي بي إس(١٦).ومن جهتها أصدرت منظمة الأمن والتعاون في أوروبا OSCE – وهي مجموعة دولية لمراقبة النزاعات – تقارير بشكل مستمر عام ٢٠١٤ أكدت فيها أن الطائرات بدون طيار Drones التابعة لها تعرضت للتشويش الروسي على نظام تحديد المواقع الأمريكي على المستوى العسكري؛ مشيرة إلى أن هذه الطائرات كانت تمشِط سماء جنوب شرق أوكرانيا على مدار عام ٢٠١٤ بهدف مراقبة الصراع هناك مما أجبر المراقبين على إنهاء مهامهم في هذه المناطق(١٧)وفي

إطار حرب نظم الملاحة عبر الأقمار الصناعية؛ فإن تخريب نظام الملاحة عبر الأقمار الصناعية للخصم Satellite Navigation System سيوجه ضربة هائلة لقواته المسلحة، والتي ربما تجد ذاتها مضطرة إلى الاعتماد على أدوات أدنى في إدارة العمليات العسكرية؛ وفي هذا السياق تصبح السفن الحربية قادرة على عبور المحيطات بدقة أقل؛ وستجد الطائرات الحربية صعوبة في تحديد موقع قوات برية صديقة. وبالنظر إلى الهيمنة العالمية لنظام تحديد المواقع العالمي الأمريكي (GPS)؛ فإن الحروب الموجهة إلى نظم الملاحة عبر الأقمار الصناعية ربما تتجاوز بكثير الإضرار بجيش معين؛ فمن الممكن أن تجد سفن الشحن التي تحمل ٨٠٪ من التجارة العالمية ذاتها تسير في الاتجاه الخاطئ بشكل تلقائي؛ ويمكن أن تصطدم بالضخور أو السفن الأخرى، وقد يلجأ الطيارون إلى الهبوط اليدوي[١٨].

المبحث الثاني الإستراتيجية السيبرانية للصين

رغم أن الصين تأخرت عن كثير من الدول الغربية في الاهتمام بالإنترنت واستخدامه، إلا أنها لحقت بالركب بسرعة شديدة؛ ووفقًا لمركز معلومات شبكة الإنترنت الصيني China Internet Network Information، بلغ عدد مستخدمي الإنترنت في الصين في عام 1997 أقل من مليون نسمة[١٩]؛ ووفقًا للمركز ذاته بلغ هذا العدد في حزيران ٢٠١٩ نحو ٨٥٤ مليون مستخدم بزيادة قدرها نحو ٢٦ مليون عن نهاية عام ٢٠١٨ وهو ما يوضح سرعة انتشار الإنترنت والزيادة المطردة في المستخدمين[٢٠]لقد شاهدت الصين تأثير الإنترنت على الاقتصاد الأمريكي والأوروبي وبعض الاقتصادات الآسيوية وأدركت أنه لا يوجد خيار غير الإنترنت ليدفع نحو مستقبل اقتصادي واعد. ومع زيادة ارتباطها بالاقتصاد العالمي وعضويتها في منظمة التجارةٍ العالمية وجدت الصين أنه لابد من تقنيات جديدة تتبعها الشركات الصينية حتى تظل – على الأقل – قادرة على المنافسة[٢١]وتأتي استراتيجية الصين تجاه الفضاء السيبراني ضمن رؤية استراتيجية أوسع تجاه النظام الدولي؛ حيث تتحفظ الصين على النظام الدولي القائم والذي تهيمن عليه الولايات المتحدة وحلفائها الغربيين وتدفع في اتجاه نظام دولي متوازن متعدد الأقطاب؛ وترى الصين أن الدولار الأمريكي المهيمن على النظام المالي العالمي القائم هو دليل على قوة الولايات المتحدة وهيمنتها على النظام الدولي» وترى أن الولايات المتحدة وحلفائها يريدون ضمان الهيمنة والنفوذ على النظام الدولي وبالتبعية الهيمنة على إدارة الفضاء السيبراني. وترفض الصين محاولات الولايات المتحدة وحلفائها فرض الرؤية الأمريكية والغربية حول حرية الإنترنت على الدول الأخرى؛ وكذلك التفسير الأمريكي والغربي للقانون الدولي وكيف أنه يؤيد هذه الرؤية. ولكن تحفّظ الصين على النظام الدولي والمالي القائم لم يعن أبدًا انعزالها دوليًا ولكن على العكس من ذلك يعتمد الاستقرار الاجتماعي والاقتصادي للصين على استمرار تدفق التجارة العالمية وتدفق المعلومات كما لم تمنعها رؤيتها الخاصة للفضاء السيبراني من ابرام بعض الاتفاقيات الثنائية التي تخص التفاعل السيبراني مع الدول الأخرى ومثال لذلك إبرامها اتفاقية ثنائية مع الولايات المتحدة عام ٢٠١٥ لوقف الهجمات السيبرانية التي يتم شنها بهدف التجسس الصناعي وسرقة الأسرار الصناعية؛ وذلك باعتبار أن مثل هذه الاتفاقيات يمكن أن تنزع فتيل التوترات مع البلدان الأخرى؛ كما تتماشى هذه الاتفاقية مع توجه الصين نحو تطوير تكنولوجيات تسعى إلى حمايتها من التجسس الصناعي[٢٢]وترتبط استزاتيجية الصين للفضاء السيبراني بأمنها 'القومي ارتباطًا وثيقا حيث ترى الصين أن التهديدات السيبرانية حافزًا على الاضطرابات الداخلية سواء جاءت من قوى خارجية كالولايات المتحدة أو من جماعة معارضة محلية. وخير مثال على ذلك الاضطرابات والثورات التي شهدتها أوكرانيا ودول آسيا الوسطى والدول العربية في عصر المعلومات. ولذلك تشعر الصين بالقلق من أن القوى المعادية يمكن أن تستخدم الإنترنت لتقويض سلطة الحزب الشيوعي الصيني وزعزعة استقرار البلاد من خلال شن هجوم سيبراني أو مجردٍ نشر معلومات. وتتوافق استراتيجية الصين السيبرانية مع سياستها الصناعية. وعلى الرغم من أن قدرات الصين فبالتقنيات الناشئة مثل الذكاء الاصطناعي أصبحت أكثر تطوراً إلا أنها لا تزال تعتمد إلى حد كبير على التكنولوجيا الغربية؛ وتأمل بكين في كسر هذه التبعية من خلال خطة "صنع في الصين" بحلول عام ٢٠٢٥ ومثلما تشعر الولايات المتحدة بالقلق من أن منتجات شركات التكنولوجيا الصينية هاواوي و'زد تي إي" ZTA قد تشتملان على ثغرات أو أبواب خلفية Backdoors يمكن أن تستغلها بكين في التجسس، كذلك فإن الصين قلقة من أن التكنولوجيا الغربية يمكن أن تكون وسيلة أجهزة الاستخبارات الغربية للتجسس على الصين. ولقد اتخذت إدارة الرئيس شي جين بينج Xi Jinping عدة خطوات للتخفيف من المخاطر السيبرانية من خلال تشديد الرقابة على الإنترنت؛ وإصدار التشريعات المنظمة للفضاء السيبراني[٢٣].وبهدف تمزيز القدرة الدفاعية والهجومية السيبرانية الصينية أعاد جيش التحرير الشعبي الصيني PLA تنظيم ذاته عام ٢٠١٥ وذلك بإنشاء قوة الدعم الاستراتيجي SSF والتي تختص بالتعامل مع العمليات العسكرية الدفاعية والهجومية والعمليات الاستخباراتية في القضاء السيبراني؛ كما تختص بالعمليات العسكرية في الفضاء فضلاً عن مسئوليتها عن الحرب السيبرانية الدفاعية والهجومية. وكان جيش التحرير الشعبي الصيني قد أولى اهتمامًا كبيرًا بحرب المعلومات والحرب الإلكترونية وقدرات الحرب السيبرانية منذ مطلع القرن الواحد والعشرين[٢٤]ورغم أن بداية الإنترنت كانت عبارة عن برنامج صغير لدى وزارة الدفاع الأمريكية (البنتاغون) وحولته الولايات المتحدة إلى منصة عالمية تربط بين أكثر من نصف مكان العالم

وعشرات المليارات من الأجهزة وظل منذ فترة طويلة مشروعًا أمريكيًا خالصا تهيمن عليه الولايات المتحدة إلا أن الصين بدأت خطوات فعلية لإزاحتها عن قيادة الفضاء السيبراني لتحاول هي امتلاك زمام القيادة. ويتضح ذلك من إعلان الرئيس الصيني "شي جين بينج" عن خططه لتحويل الصين إلى 'قوة سيبرانية عظمى"؛ وقد أوضح منذ تولية السلطة في ٢٠١٢ مدى الذور الذي يلعبه الإنترنت في رؤيته للصين؛ وذلك بعد سنوات من تجزأ السياسة السيبرانية الصينية بين مجموعة واسعة من الإدارات الحكومية.فقد أعلن شي جين بينج عن أنه سيرأس ما يُسمى القيادة المركزية لأمن الإنترنت والمعلوماتية؛ كما أنشأ وكالة جديدة هي قيادة الفضاء السيبراني للصين The Cyberspace Administration of China، ومنحها مسؤولية تحقيق الأمن السيبراني الصيني وتطوير الاقتصاد الرقمي Digital Economu وتأمل الصين أن تقود العالم في نهاية المطاف في التقنيات المتقدمة مثل الذكاء الاصطناعي والروبوتات والحوسبة الكمية Quantum Computing (وتعني القدرة على إجراء عمليات حسابية متعددة ومعقدة في الوقت ذاته لحل بعض المشكلات والتي لا تستطيع أجهزة الحاسب الآلي العادية حلها). وفي عام ٢٠١٧ حددت الحكومة الصينية خارطة الطريق لكي تتحول إلى "مركز ابتكار الذكاء الاصطناعي الأول في العالم" بحلول عام ٢٠٣٠. وقد أصبح للصين صوتًا مسنْموعًا في إدارة الفضاء السيبراني عالميًا خاصة في ضوء امتلاكها أكبر عدد من المواطنين المتصلين بالإنترنت أكثر من أي دولة في العالم. ونظرًا لحجم الصين وتطورها التكنولوجي؛ فإن بكين لديها فرصة جيدة للنجاح في إعادة تشكيل الفضاء السيبراني من وجهة نظرها الخاصة[٢٥]ونتيجة تخوف الصين من مخاطر الهجمات السيبرانية على الشبكات الحكومية والخاصة والتي قد تؤدي إلى تعطيل الخدمات الحيوية وتضر بالنمو الاقتصادي بل وقد تسبب التدمير المادي؛ أعلن جيش التحرير الشعبي عن خطط للإسراع بتطوير قواته السيبرانية وتعزيز دفاعات الشبكة الصينية؛ واستطاعت الصين من خلال اللوائح والتشريعات المحلية والابتكار التكنولوجي والسياسة الخارجية أن تبني نظام حصين الدفاع السيبراني من الصعب اختراقه؛ كما تهدف الصين إلى تقليل اعتمادها على شركات التكنولوجيا الأمريكية لحماية أمنها القومي؛ وهو الاعتقاد الذي تم تعزيزه في عام ٢٠١٣ عندما كشف إدوارد سنودن عن أن أجهزةٍ المخابرات الأمريكية وصلت إلى بيانات ملايين الأشخاص التي تديرها وتنقلها الشركات التكنولوجية الأمريكية. وقد اتخذت الصين من مبدأ "السيادة السيبرانية Cyber – Sovereignty أساساً لإدارة الإنترنت في معارضة واضحة للرؤية الأمريكية التي تهدف إلى ضمان إنترنت عالمي ومفتوح. ووفقًا لشي جين بينج تمثل السيادة السيبرانية حق كل دولة على حدة في اختيار طريقتها الخاصة لتطوير الإنترنت؛ ونموذجها للتنظيم السيبراني والسياسات العامة للإنترنت؛ ومشاركتها في إدارة الفضاء السيبراني العالمي على قدم المساواة[٢٦]وتتمثل رؤية الصين للفضاء السيبراني العالمي في وجود عدد من شبكات الإنترنت الوطنية في كل دولة على حدة؛ بحيث يكون لكل دولة سيادة سيبرانية على شبكة الإنترنت لديها. وبالتالي فهي تريد أن تُضعف من نموذج إدارة الفضاء السيبراني العالمي بواسطة شركات القطاع الخاص الأمريكية والغربية وهو النموذج المدعوم من قبل الولايات المتحدة وحلفائها. ففي الوقت الذي تدعو فيه الصين إلى مبدأ سيادة الدولة على الإنترنت لديها تدعو واشنطن وحلفائها إلى نموذج موزع Distributed Model لإدارة الإنترنت يشمل الهيئات الفنية والقطاع الخاص والمجتمع المدني والحكومات. ويعتقد صناع السياسة الصينيون بأن الصين سيكون لها تأثير أكبر فيما يخص تنظيم تكنولوجيا المعلومات وتحديد القواعد العالمية لإدارة الفضاء السيبراني.حال أن تمكنت الأمم المتحدة من القيام بدور أكبر في إدارة الإنترنت. وقد تركزت جهود الصين المُشاهدة لكتابة قواعد إدارة الفضاء السيبراني من خلال الأمم المتحدة؛ ففي عام ٢٠١٧ دعت الصين إلى 'نهج متعدد الأطراف لإدارة الفضاء السيبراني مع قيام الأمم المتحدة بدور قيادي في بناء توافق دولي في الآراء بشأن قواعد إدارةٍ الفضاء السيبراني؛ وهذا من شأنه أن يعطي أولوية لمصالح الحكومات على مصالح شركات التكنولوجيا ومنظمات المجتمع المدني؛ وسيسمح ذلك للصين بتعبئة أصوات الدول النامية والتي يرغب الكثير منها أيضًا في التحكم في الإنترنت والحد من التدفق الحر للمعلومات. وبالإضافة إلى العمل من خلال الأمم المتحدة؛ تنظم الصين سنوي المؤتمر العالئي للإنترنت في وتشين Wuzhen تعرض فيه رؤيتها للإنترنت[٢٧].وفضلاً عن ذلك من المحتمل أن يكون لبكين تأثير كبير على إدارة الفضاء السيبراني عالميًا من خلال سياستها التجارية والاستثمارية» خاصة من خلال مبادرة "الحزام والطريق، وهي جهد ضخم لبناء البنية التحتية التي تربط الصين بالمحيط الهندي والخليج الفارسي وأوروبا. حيث أنه بالإضافة إلى إنشاء السكك .الحديدية والطرق وخطوط الأنابيب والموانئ والمناجم والمرافق على طول طريق الحرير العملاق؛ أكد المسؤولون الصينيون على ضرورة قيام الشركات الصينية ببناء 'طريق حرير رقمي" Digital Silk Road بما يشتمل من كابلات الألياف الضوئية؛ وشبكات الهاتف المحمول ومحطات الأقمار الصناعية ومراكز البيانات والمدن الذكية: والمشاهد أن الرؤية الصينية للإنترنت ومفهوم السيادة السيبرانية يتصاعد دوليًا. ووفقًا لتقرير مؤسسة فريدوم هاوس الأمريكية Freedom House فإن هناك مزيد من الدول التي تجبر شركات التكنولوجيا على تخزين بيانات مواطنيها داخل حدود أراضيهاء فضلاً عن إجبار هذه الشركات على السماح للحكومة بإجراء مراجعات أمنية لمعدات الشبكات الخاصة بها كما أن قدرةٍ الأفراد على الوصول إلى الإنترنت وإستخدامه بسهولة في التعبير عن الرأي انخفضت خلال السبع سنوات الأخيرة[٢٨].ولا تربط الصين تمددها التكنولوجي بأية

تدخلات سياسية أو مساعي للهيمنة؛ وإنما الاحتفاظ بكونها شريك تجاري لعدد كبير من دول العالم والعديد من كبرى الشركات التكنولوجية، ورغم أن الصين منتج عملاق ومساهم في التطور التكنولوجي والعلمي في العالم إلا أنها اتخذت خطوات متحفظة من الانفتاح العالمي والعولمة والهيمنة الثقافية الغربية للحفاظ على الخصوصية الصينية، ومن خلال التشريعات السيبرانية وضعت الصين خطوط حمراء لا ينبغي تجاوزها عند التعامل مع الإنترنت؛ أهمها عدم تعريض النظام السياسي الصيني أو مصالحه للخطر أو تجاوز القانون الوطني في الصين؛ أو الإضرار بحقوق الآخرين أو الأنظمة الأخلاقية أو صحة المعلومات المتداولة[٢٩]. ويقوم مزودو خدمات الإنترنت في الصين Internet Service أو ما يطلق عليه اختصارًا ١٥٨٨ – دوزا مهمًا في تنظيم الإنترنت في الصين بما يحقق أهداف الحكومة. حيث. يتحملون مسئولية حظر المحترى Online Content Blocking وتصفيته على الإنترنت؛ وبناءً على طلب الحكومة يقوم مزودو خدمات الإنترنت بتطبيق تقنيات الحظر والتصفية بمنع المستخدمين المحليين من زيارة بعض المواقع الأجنبية مثل مواقع التواصل الاجتماعي الغربية أو منع المستخدمين الأجانب من زيارة مواقع محلية معينة. وتعرف أجهزة وبرامج الحظر والتصفية باسم "جدران الحماية" The Great Firewall (GFW) [٣٠].من جهة أخرى استطاعت الصين بناء مواقع وتطبيقات وطنية على الإنترنت بديلة للتطبيقات التي تنتجها الشركات الغربية. حيث قامت ببناء شبكة إنترنت محلية؛ وتدشين محركات بحث وطنية Search Engines ومن أشهرها محرك البحث بايدو Baidu وهو بديل لمحرك البحث الأمريكي جوجل. كما أنشأت منصات للتجارة الإلكترونية؛ ومواقع تواصل اجتماعي (شبكات اجتماعية) صينية؛ وتقوم الصين بحجب المواقع الإلكترونية التي تبث الشائعات أو تدعو لإسقاط الدولة أو تدعو للفرقة الطائفية. وهناك موقعان صينيان لتبادل الصور وهما "إيكاشا" و"إيكسون" وهما بديلان لموقع فليكر ؛ ويعتبر موقع "هودونج" بديل موقع ويكيبيديا الموسوعي. وهناك منصتي أيوكو" Youku واتودو" Tudou في مقابل موقع/ تطبيق_يوتيوب. وتوجد منصات "كايشين" و"تنسنت" و"سينا" و"ويبو مقابل موقع تطبيق تويتر. ولم تسمح الحكومة الصينية حتى الوقت الحاضر لشركة. جوجل الأمريكية بالعمل في الصين رغم الضغوط الشديدة والانتقادات الغربية المستمرة للصين بأنها تقف ضد حرية الإنترنت؛ كما تحجب الصين عمل الشبكات الاجتماعية الأمريكية والغربية[٣١].وفي المقابل أحسنت الصين استغلال الشبكات الاجتماعية الصينية الوطنية؛ حيث تتميز هذه الشبكات باحتوائها على نسبة كبيرة جدًا من الحسابات النشطة وأسماء حقيقية للمستخدمين ويرجع ذلك إلى الرقابة الحكومية[٣٢]، وذلك بعكس الشبكات الاجتماعية الأمريكية مثل موقع تطبيق فيسبوك والذي يحتوى على آلاف الحسابات المزيفة أو الخاملة أو المكررة؛ والتي قد تتسبب في حجم تفاعل غير حقيقي وانتاج محتوى مزيف تجاه القضايا العامة. وبذلك تساعد الشبكات الاجتماعية الحكومة الصينية في النهاية على اتخاذ القرار السليم والتنبؤ بالأزمات؛ هذا فضلاً عن منع محاولات التدخل الخارجي في الشئون الداخلية الصينية والتي قد تتم بواسطة اللجان الإلكترونية الخبيثة التي تعمل على إنشاء رأي عام مزيف على الشبكات الاجتماعية أو تحاول تعزيز الفرقة والإنشقاق الداخلي أو تعمل على افتعال أزمات أو تضخيم أزمات قائمة من آ خلال نشر وتداول أخبار كاذبة أو شائعات.وبالتالي لا تعد الشبكات الاجتماعية في الصين أداة لإثارة الاحتجاجات الاجتماعية في ظل وجود رقابة حكومية؛ بل على العكس تُعد أداة لاحتواء التهديدات قبل انتشارها ووسيلة جيدة لقياس الرأي العام تجاه القضايا العامة من خلال تقنيات تحليل المحتوى من البيانات الضخمة وتطبيقات الذكاء الاصطناعي فضلاً عن كونها منصة للدعاية الحكومية. كما تساعد هذه الشبكات المحلية المواطنين على الوصول إلى المعلومات والمشاركة في النقاش العام وبالتالي محاربة الفساد والاستجابة الحكومية للمشكلات القائمة[٣٣].ورغم أن الصين تعمل على تطوير قدراتها السيبرانية الهجومية إلا أنها تركز أيضًا على الدفاع السيبراني؛ فالشبكات في الصين تنقسم إلى قطاعات للاستخدامات الحكومية والجامعية والتجارية وتتولى الحكومة الصينية حمايتها. حيث تتولى الدفاع عن شبكات الدولة ككل وليس الشبكات العسكرية فحسب. والإنترنت في الصين يشبه شبكة داخلية Interanet لشركة خاصة؛ وتقوم الحكومة الصينية بدور مقدم خدمة الإنترنت؛ وهي المسؤوله عن الدفاع عن الشبكات. ورغم وجود رقابة على الإنترنت في الصين بما في ذلك "الجدار الناري العظيم" إلا أن ذلك له ميزات تأمينية لحجب البرامج الخبيثة.وقد استثمرت الصين في تطوير نظم التشغيل المملوكة لها والحصينة ضد الهجمات السيبرانية وهي مثبّته على الشبكات. كما أن البُنى التحتية في الصين لا تعتمد بشكل كبير على الحاسب الآلي مثل الولايات المتحدة. وعلى سبيل المثال فإن نظام الطاقة الكهربائية في الصين يركز على تلق تبث اركللب قن كيزا بن الاععل اليدري ورف أن ذلك ربما بعد تأخراً تكنولوجياً إلا أنه ميزة في إطار حروب الفضاء السيبراني[٣٤]، وتمتع الحكومة بالسلطة والأدوات اللازمة لفصل الإنترنت في الصين عن العالم قد يدفعها لأن تفعل ذلك في حال نشوب صراع سيبراني مع الولايات المتحدة. وذلك على عكس هذه الأخيرةِ والتي لا تستطيع فصل ذاتها عن الإنترنت في ضوء ارتباط الاقتصاد الأمريكي بالإنترنت أكثر من أي دولة أخرى؛ كما أن قطاعات البنية التحتية المدنية والتي صنفتها وزارة الأمن الداخلي الأمريكية بأنها قطاعات حساسة تعتمد جميعها على الانترنت لتنفيذ مهامها وبالتالي فهي عرضة للهجمات السيبرانية من جانب دول أخرى[٣٥]وبذلك عززت الاستراتيجية السيبرانية للصين من دفاعها السيبراني ضد أي هجمات سيبرانية أجنبية محتملة في إطار الصراعات والحروب القائمة عبر

الفضاء السيبراني. وكذلك منع أي محاولات للتدخل الأجنبي في الشؤون الداخلية للصين بواسطة مواقع التواصل الاجتماعي. وقدرة الصين على أن تفصل ذاتها عن شبكة الإنترنت الدولية بشكل تام في حال تعرضها لهجوم سيبراني دفع شركة مايكروسوفت العالمية لأن تشهد للصين – عبر موقعها الإلكتروني – بأن لديها أدنى معدل إصابة بالبرمجيات الخبيثة مقارنة بباقي دول العالم(٣٦).

المبحث الثالث الاستراتيجية السيبرانية للولايات المتحدة الأمريكية

تعتبر الولايات المتحدة الأمريكية أن الفضاء السيبراني هو بمثابة منصة هامة للتجارة العالمية والاقتصاد العالمي؛ لذلك تحاول دائمًا الحفاظ على دورها التاريخي المهيمن والقائد لدول العالم فيما يخص الأمن السيبراني العالمي؛ وذلك لضمان فضاء سيبراني مستقر والحفاظ على استمرار تدفق المعلومات دوليًا والتبادل التجاري العالمي. وكثيرًا ما تحاول الولايات المُتحدة قيادة باقي حلفائها لوضع القواعد والمعايير التي يجب أن تتبعها المؤسسات الدولية المنوط بها إدارة أمن الفضاء السيبراني العالمي؛ تلك المؤسسات التي تقوم بدورها بقيادة مختلف دول العالم فيما يخص الالتزام بالقواعد والمعايير الضرورية للحفاظ على أمن الفضاء السيبراني محلياً(٣٧).وتاريخياً يُعد البنتاغون الأمريكي هو صاحب أول شبكة حاسبات في العالم والتي تُعرف باسم "اربانت" ARPANET وهي النواة الأولى لشبكة الإنترنت الدولية. ويشغل البنتاغون في الوقت الحالي أكثر من ١٥ ألف شبكة حاسوبية عبر ٤ آلاف منشأة في ٨٨ دولة. ونسبة كبيرة من هذه الشبكات تخضع لما يُعرف ب "الجدران النارية" Firewalls كما يقتصر البنتاغون على نسخته السرية من الفضاء السيبراني والتي تُعرف باسم "سيبرنت" SIPRNet؛ ولكن مع ذلك تدخل أجهزة البنتاغون على الشبكة العامة للإنترنت أكثر من مليار مرة يوميًا. وكان الأدميرال مايكل ماكونيل Michael McConnell رئيس الاستخبارات الأمريكية الوطنية سابقًا قد قدّر أنٍ نحو ٩٨٪ من اتصالات الحكومة الأمريكية بما فيها الاتصالات السرية تتم عبر شبكات يملكها ويديرها مدنيون(٣٨).ولا تزال الولايات المتحدة – حتى اليوم – هي من تخترع أغلب التكنولوجيات على مستوى العالم؛ وهي من تقوم بتوفير أكثر المحتويات على الإنترنت؛ مثل التطبيقات والمعلومات، والترفيه؛ والنقاش، والأخبار/ وشبكات التواصل الاجتماعي. ورغم أن أغلب القدرات السيبرانية الأمريكية تقع خارج الحكومة وسيطرتها؛ إلا أنّ وكالة الأمن القومي الأمريكي تمتلك قدرات تقنية وتشغيلية هامة؛ وتتضمن هذه القدرات وسائل متطورة في مجال الأمن السيبراني، وكذلك القدرة على المراقبة وتنفيذ تحركات هجومية. وقد اعتبرت الولايات المتحدة الأمريكية أن الحرب السيبرانية لا تقل عن الحرب المادية التقليدية؛ وذلك نظرًا لخطورة الحرب السيبرانية والتي يمَكنها :نَل من قدرة أنظمة الكمبيوتر التي يملكها العدو، سواء كان ذلك في سياق صراع مسلح أو غير مسلح؛ وأحيانًا تختار الولايات المتحدة اللجوء إلى استخدام القوة السيبرانية لإرغام أعدائها أو عقابهم عندما ترى أن اللجوء إلى القوة العسكرية المادية غير مناسباً(٣٩)ورغم سعي العديد من دول العالم إلى الحد من الاعتماد على الخوادم الأمريكية ومحاولة بناء شبكات إنترنت وطنية لحماية أمنها القومي إلا أنه في الوقت الحالي لا تزال الشركات الأمريكية تتمتع بالهيمنة في مجالات متعددة ترتبط بالإنترنت؛ فلا يزال محرك البحث على الإنترنت "جوجل" هو المهيمن في العالم وتمتلكه شركة جوجل الأمريكية؛ كما تهيمن: شركتا مايكروسوفت وأبل على قطاع أنظمة التشغيل Operating Systems كما تهيمن هاتان الشركتان بالإضافة إلى شركة جوجل على قطاع أنظمة تشغيل الهواتف الذكية؛ كما تعتبر شركة سيسكو سيستمز الأمريكية Cisco Systems الأولى عالمياً في مجال المعدات الشبكية؛ كما تسيطر الشركات الأمريكية مثل فيسبوك وجوجل وتويتر وغيرها على سوق شبكات التواصل الاجتماعي في العالم؛ كما أن معظم الشركات التي تعمل في الإنترنت مُسجّلة في الولايات المتحدة(٤٠). ولذلك نجد أن الولايات المتحدة قد حققت فوائد اقتصادية وعسكرية واستخباراتية كبيرة بواسطة قيادتها للفضاء السيبراني العالمي خلال فترة طويلة وهي تحاول حاليًا الحفاظ على هذه القيادة.ولقد اعترفت لأول مرة هيئة الأركان المشتركة الأمريكية Joint Chiefs of Staff بالآثار المدمرة للتأثيرات الناتجة عن استخدام الأسلحة السيبرانية في عام ٢٠٠٤ وفي يونيو من عام ٢٠٠٩، استحدث البنتاجون "القيادة السيبرانية الأمريكية" U.S. Cyber Command، وهي قيادة عسكرية تتمثل مهامها الأساسية في صد هجمات القراصنة المعلوماتية وتنفيذ عمليات في الفضاء السيبراني، وذلك في ضوء أن الأخطار المرتبطة بالفضاء السيبراني هي من أهم التحديات التي تواجه الاقتصاد العالمي والأمن القومي في القرن الواحد والعشرين(٤١)، وتم تعيين أول جنرال عسكري مهمته إدارةٍ حروب الفضاء السيبراني وهو إلكسندر كيث؛ وهدفت وزارة الدفاع الأمريكية من إنشاء هذه القيادة أن تقوم بالإشراف على كافة الجهود المتعلقة بحروب الإنترنت في كافة أفرع القوات المسلحة الأمريكية؛ والدفاع عن شبكات وزارة الدفاع والدولة الأمريكية ككل والاستعداد لخوض الحروب؛ وضمان حماية حرية عمل الولايات المتحدة وَخرية عمل حلفائها في الفضاء السيبراني؛ وحرمان أعداء الولايات المتحدة من حرية العمل في هذا الفضاء إذا تطلب الأمر ذلك، وفي عام ٢٠١١، أعلن نائب وزير الدفاع الأمريكي وليام ج. لين William J. Lynn يا أنه سيتم التعامل – كعقيدة عسكرية جديدة – مع الفضاء السيبراني كمجال تشغيلي Operational Domain مماثل للأرهد ض والجو والبحر والفضاء الخارجي(٤٢).وقد اعتبرت إدارةٍ الرئيس الأمريٍ يكي السابق باراك أوباما أن الولايات المتحدة تمتلك الحق في شن ضربات سيبرانية استباقية إذا رأت الولايات المتحدة أن هناك هجوم

عسكري على وشك الوقوع ضدهاء فضلاً عن أن الاستراتيجية السيبرانية لوزارة الدفاع الأمريكية لعام ٢٠١٥ قد تركت الباب مفتوحًا أمام شن الولايات المتحدة هجمات سيبرانية استباقية Pre-emptive Cyberattacks[٤٣] ورغم أن الولايات المتحدة قد طورت العديد من الأسلحة السيبرانية الهجومية واستخدمتها، إلا أنها بذلك كشفت لغيرها من الدول عن هذه الأسلحة وربما لا تكون الولايات المتحدة هي المنتصرة إذا تم استخدام هذه الأسلحة ضدها. فهي تتعرض لأخطار سيبرانية أكبر مما يمكن أن تتعرض له دولة أخرى وذلك نتيجة اعتمادها بشكل كبير على الفضاء السيبراني[٤٤].وقد اتخذ البنتاجون الأمريكي عدة قرارات مهمة في الفترة من ٢٠١٧ إلى ٢٠١٨ للعمل على سد الفجوة في القدرات السيبرانية وقدرات الحرب الإلكترونية مع بعض الدول التي تعتبرهما الولايات المتحدة أعداء لها خاصةٌ روسيا والصين. ففي أغسطس ٢٠١٧ أعلن الرئيس دونالد ترامب رفع مستوى قيادة الفضاء السيبراني إلى مستوى "قيادة قتالية موحدة" مسئولة عن عمليات الفضاء السيبراني بعد أن كانت تعمل تحت قيادة فرعية في الجيش. وجاء ذلك – وفقاً لتصريحات ترامب – بهدف بهدف تحسين الدفاع عن الولايات المتحدة وزيادة التعبئة ضد مخاطر الفضاء السيبراني والمساعدة في طمأنة حلفاء وشركاء الولايات المتحدة وردع الخصوم. ومن شأن هذه القيادة الموحدة الجديدة أن تعزز من فعالية الرد السريع وتطوير وسائل جديدة في الحرب السيبرانية والمعلوماتية. ويعكس هذا القرار أهمية المجال السيبرائي كتهديد رئيس للأمن القومي في الولايات المتحدة والعديد من الدول الكبرى الأخرى؛ حيث تضع هذه الخطوة العمليات البِنتاغون التي تتم عبر الفضاء السيبراني على مستوى مماثل لقيادات البنتاجون التسعة المقاتلة الأخرى التي يقودها جنرالات أو أدميرالات؛ وهو ما يعد توسعًا تاريخيًا فى استراتيجية الحرب الأمريكية.كما صنّف البنتاغون "الإنترنت" على أنه يعد الميدان الرابع من ميادين الحروب بعد الجو والبحر والبرء كما تقوم الحكومة الأمريكية بمناورة سنوية تسمى "سايبر ستورم" Cyber Strom وذلك بهدف اختبار مدى جاهزيتها للتصدي لأية هجمات سيبرانية محتملة من جهات أجنبية؛ ويشارك بهذه المناورة ما يقرب من ١١٢ جهازا أمنيًا أمريكياً[٤٥]وفي ٢٠ سبتمبر ٢٠١٨ أصدرت الولايات المتحدة استراتيجية لحماية "الأمن القومي السيبراني" الأمريكي؛ أطلقت عليها "الاستراتيجية السيبرانية القومية" National Cyber Strategy، ولأول مرة يتم استخدام مصطلح أمن قومي سيبراني؛ وتم تشكيل جيش أمريكي قوامه ٢٠٠٠ من القراصنة (الهاكرز) مهمته الأساسية القيام بما يلزم لحماية الأمن القومي الأمريكي من الهجمات السيبرانية؛ والقيام بشن أعمال سيبرانية هجومية إذا تطلب الأمر ذلك[٤٦].وتُعد هذه الاستراتيجية السيبرانية القومية أول استراتيجية سيبرانية مُفصّلة للولايات المتحدة منذ نحو ١٥ عاماً. وجاء فيها أن أمن الفضاء السيبراني هو ضرورة لحماية الأمن القومي الأمريكي وتعزيز الرخاء للشعب الأمريكي، وأن الأنشطة السيبرانية الخبيثة لأعداء الولايات المتحدة قد زادت في شدتها وتعقيدها. وأشارت إلى أن هناك دولاً تتمسك بمفاهيم مثل "السيادة" ولكنها لا تتوقف عن انتهاك قوانين الدول الأخرى وتنخرط في أنشطة التجسس الاقتصادي وغير ذلك من الأنشطة السيبرانية الخبيثة مما يتسبب في خسارة للشركات والحكومات والأفراد حول العالم. كما أن هذه الدول تنظر إلى الفضاء السيبراني على أنه ميداناً مهمًا يمكن استغلاله لتحييد القوة العسكرية والاقتصادية والسياسية الأمريكية وبالتاليم تصبح أمريكا وشركاؤها وحلفاؤها في خطر. وحددت الاستراتيجية دول معينة تشن مثل هذه الهجمات السيبرانية على الولايات المتحدة وتسبب لها أضرارًا بالغة وهي روسيا وإيران وكوريا الشمالية والصين. مشيرة إلى أن هذه الدول تستخدم أدوات سيبرانية لتقويض الاقتصاد والديمقراطية الأمريكية وتسرق الملكية الفكرية الأمريكية وتحاول زرع الشقاق والخلافات في العملية الديمقراطية وتطور أسلحة سيبرانية جديدة وأكثر فعالية[٤٧].وتُعد الاستراتيجية السيبرانية القومية لعام ٢٠١٨ استزاتيجية أكثر تفصيلاً من: الاستراتيجية القومية لحماية الفضاء السيبراني التي أصدرتها إدارة الرئيس الأسبق جورج دبليو بوش عام ٢٠٠٣ حيث تحدد كيفية حماية المصالح الأمريكية في الفضاء السيبراني انطلاقًا من أن الولايات المتحدة هي من أنشأت الإنترنت وعليها الحفاظ على دورها المهيمن في هذا الفضاء وحمايته. كما تجيز للولايات المتحدة القيام بعمليات سيبرانية هجومية؛ وخففت القيود التي أقرتها إدارة الرئيس السابق باراك أوباما للقيام بهجمات سيبرانية على خصوم الولايات المتحدة[٤٨].ووفقًا لاستراتيجية عام ٢٠١٨ فإن قيام أي دولة بنشاط سيبراني هجومي ضد الولايات المتحدة سيدفع الأخيرة إلى الرد دفاعيًا وهجوميًا وليس بالضرورة أن يكون ذلك في الفضاء السيبراني؛ وفي حالة فشل ردع الأنشطة السيبرانية والتي تعتبر استخدامًا للقوة ضد الولايات المتحدة وحلفائها سيدفع ذلك الولايات المتحدة نحو استخدام القدرات العسكرية ردًا على ذلك في المجال المادي. فضلاً عن ذلك تجيز الاستراتيجية التحرك خارج الحدود واختراق شبكات الخصوم وتعزيز القدرات لجمع المعلومات الاستخباراتية[٤٩]وفي سياق متصل؛ وبهدف حماية الأمن القومي الأمريكي ومنع أنشطة التجسس السيبراني من الجهات الأجنبية أصدر الرئيس دونالد ترامب في ١٥ مايو لعام ٢٠١٩ قرارًا يمنح الحكومة الفيدرالية الحق في منع الشركات الأمريكية من شراء معدات الاتصالات المُصنعة في شركات أجنبية والتي تغتبر مصدر خطر أمني. وبرر البيت الأبيض هذا الإجراء بوجود خصوم أجانب يستغلون بصورة متزايدة مكامن ضعف في الخدمات والبُنى التحتية التكنولوجية في مجالي الإعلام والاتصالات في الولايات المتحدة؛ وبالتالي يهدف القرار إلى التصدي للأعمال الخبيثة التي يتسبب فيها الإنترنت مثل التجسس الاقتصادي والصناعي على حساب الولايات المتحدة وشعبها[٥٠].ثم تلى هذا القرار قيام الحكومة الأمريكية فعليًا بإدراج

شركة هواوي الصينية العملاقة في قائمة سوداء تمنع عمليًا الشركات التكنولوجية الأمريكية من العمل معهاء وقد اتخذت واشنطن هذا القرار متعللة بأن الشركة قد تستخدم التكنؤلوجيا التي تطورها في التجسس لصالح بكين[٥١]، ولكن وبرغم هذه الأزمة استطاعت عملاق التكنولوجيا الصيني إبرام عقود لبناء شبكات اتصالات الجيل الخامس في عشرات الدول حول العالم؛ من بينها الاتفاق مع شركة الاتصالات الروسية "إم تي إس" لتطوير شبكة "الجيل الخامس" في روسيا خلال عام ٢٠٢٠. وربما يؤدي قرار ترامب إلى تخلف الولايات المتحدة عن الصين وروسيا في مجال الإنترنت فائق السرعة من الجيل الخامس, وقد أشار جيمس جون مستشار الأمن القومي الأمريكي الشابق في فبراير من عام ٢٠١٩ إلى تخلف الولايات المتحدة عن الصين في شبكات الجيل الخامس؛ مؤكدًا أن الإنترنت فائق السرعة من الجيل الخامس سيحدث ثورة في الاقتصاد الرقمي؛ وسوف يصبح التكنولوجيا الأكثر تطورًا في هذا القرن؛ والصين لديها كل الفرص للفوز في هذه المنافسة[٥٢].

الخاتمة

يمثل تزايد التوظيف السياسي غير السلمي لأدوات الفضاء السيبراني من جانب الدول والفاعلون من غير الدول تهديداً للأمن القومي للدول، مثل توظيفها في إطار الحملات الخبيثة والعمليات النفسية السيبرانية لزرع وتعميق الشقاق الداخلي والانقسامات المجتمعية، وخلق الفتن والازمات أو تعميق ازمات قائمة والعمل على تفاقمها، ونشر الشائعات والاخبار المغلوطة لإشاعة الفوضى وعدم الاستقرار السياسي إلى حد قلب نظم الحكم، أو إضعاف الدول وتحويلها إلى دول مفككة وضعيفة وقاشلة Failed states، كما يتم توظيف هذه الأدوات في إطار الاستخبارات السيبرانية من خلال توظيف المواقع الإلكترونية والتطبيقات على الهواتف المحمولة وبعض البرمجيات المتطورة والخبيثة لسرقة بيانات المستخدمين والمؤسسات الحكومية والخاصة واستغلالها، ويمكن تحديد أهم أسباب تزايد الهجمات السيبرانية المدفوعة بأهداف سياسية خلال السنوات الأخيرة:

أولاً: اسباب تزايد الهجمات السيبرانية المدفوعة بأهداف سياسية خلال السنوات الأخيرة:

١) الفوضى التي تتسم بها التفاعلات في الفضاء السيبراني بشكل عام، فهناك غياب شبه كامل لقواعد القانون الدولي المنظمة للتفاعلات غير السلمية والعمليات السيبرانية الهجومية في الفضاء السيبراني، مما يدفع لجوء بعض الدول والفاعلين من غير الدول إلى شن هجمات سيبرانية لتحقيق أهداف سياسية.

٢) غياب المؤسسات الدولية وآليات مراقبة سلوك الدول في الفضاء السيبراني.

٣) طبيعة الفضاء السيبراني ذاته وخصائصه: حيث تشجع هذه الخصائص الدول والفواعل من غير الدول على توظيف الهجمات السيبرانية لتحقيق أهدافهم بطرق غير شرعية ويتيح الفضاء السيبراني للمهاجمين إمكانية التنكر والاعتماد على المرتزقة السيبرانية.

٤) وجود ثغرات قد تكون تقنية أو غير معلومة ويتم استغلالها لشن الهجمات السيبرانية.

التوصيات والمقترحات لمواجهة التهديدات السيبرانية:

أولاً: إنشاء هيئة وطنية عليا لمراجعة متطلبات الأمن السيراني.ثانياً: صياغة استراتيجية متكاملة للأمن السيبراني.ثالثاً: إنشاء مركز عمليات أمن المعلومات isoc على مستوى الوزارات والهيئات الحكومية المختلفة (مركز عمليات الأمن السيبراني).رابعاً: زيادة الاعتماد على تقنيات الذكاء الاصطناعي في مواجهة التهديدات السيبرانية.خامساً: على المستوى الاكاديمي: إنشاء جامعات وطنية متخصصة في قضايا الأمن السيبراني.سادساً: التعاون الدولي لإنشاء قواعد قانونية دولية فعالة لمواجهة التهديدات السيبرانية.

هوامش البحث

(1) Matthew Bey. "Great Powers in Cyberspace: The Strategic Drivers behind US, Chinese and Russian Competition". The Cyber Defense Review. Vol. 3, No. 3 (Fall 2018), P: 33.

(2) Matthew J. Flynn. “Cyber Rebellions: The Online Struggle for Openness”. T Journal of International Affairs , Vol. 71, No. 1.5, (Special Issue: Contentious Narratives: Digital Technology and the Attack on Liberal Democratic Norms) (2018), P: 108.

(٣) د. عبد الغفار الدويك، تقرير التوازن العسكري ٢٠١٩: قراءة تحليلية لـ القدرات السيبرانية في العالم، السياسة الدولية، عدد ١٦، ابريل ٢٠١٦، ص٢٧٦.

(٤) مصطفى عصام نعوس، حق الدولة في استخدام القوة في القضاء الإلكتروني للدفاع عن النفس، مجلة الحقوق، الكويت، مجلد ٣٨، عدد ١، ص٥٧٣.

(5) Timothy L. Thomas ."Nation-State Cyber Strategies: Examples from China and Russia". In "Cyber Power and National Security", Edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. (United States , National Defense University Press, 2009) .PP: 673 - 679

(6) Franz-Stefan Gady and Greg Austin. "Russia, the United States, and Cyber Diplomacy: Opening the Doors". EastWest Institute. 2010.P: 6.

(٧) د. عادل عبد الصادق، الصراع على الفضاء السيبراني بين التوجيهات الروسية والامريكية، التقرير الاستراتيجي العربي ٢٠١٨، القاهرة، مركز الدراسات السياسية والاستراتيجية بالاهرام، ص٢٧.

(٨) عادل عبد الصادق، اسلحة الفضاء الالكتروني في ضوء القانون الدولي الإنساني، سلسلة أوراق عدد ٢٣، الاسكندرية، ٢٠١٦، ص٨.

(٩) عصام فاعور ملكاوي، الفضاء الإلكتروني ساحة حرب دولية مفترضة. أربد للبحوث والدراسات، الأردن، مجلد ١٨، عدد ٢، ٢٠١٥، ص١٠٩.

(١٠) سماح عبد الصبور، الصراع السيبراني، طبيعة المفهوم وملامح الفاعلين، مجلة السياسة الدولية، عدد ٢٠٨، ٢٠١٧، ص٥.

(١١) ايهاب خليفة، امكانيات تحقيق الردع في صراعات الفضاء الإلكتروني، دورية اتجاهات الاحداث، عدد ١٣، ٢٠١٥، ص٤٨.

(12) Mari Ristolainen. "Should RuNet 2020 Be Taken Seriously? Contradictory Views about Cybersecurity between Russia and the West". In Juha Kukkola, Mari Ristolainen and Juha-Pekka Nikkarila (Eds.), "Game Changer: Structural Transformation of Cyberspace". (Finland, Finnish Defence Research Agency Publications, 2017), P: 7

(١٣) ربيع محمد يحيى، اسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط، دورية رؤى استراتيجية، مركز الامارات للدراسات والبحوث الاستراتيجية، عدد ٣، ٢٠١٣، ص٦٧.

(١٤) سارة عبد العزيز، الحرب السيبرانية، التداعيات المحتملة لتصاعد الهجمات الالكترونية على الساحة الدولية، دورية اتجاهات الأحداث، عدد ٢٠، ٢٠١٧، ص٩.

(١٥) عادل عبد الصاحب، انماط الحرب السيبرانية وتداعياتها على الأمن العالمي، السياسة الدولية، عدد ٥٣، ٢٠١٧، ص٣٢.

(١٦) Elisabeth Braw. "The GPS Wars Are Here". Foreign Policy. Published on December 17, 2018. Accessed on 15/6/2019, Available at: https:/foreignpolicy.com/2018/12/17/the-gps-wars-are-here/

(17) paul McLeary. "Russia's winning the Electronic War". Op.cit, Accessed on 15/6/2019, Available at: https:/foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/

(18) Elisabeth Braw. "The GPS Wars Are Here". Op.cit. Accessed on 15/6/2019, Available at: https://foreignpolicy.com/2018/12/17/the-gps-wars-are-here/

(19) Nina Hachigian. "China's Cyber-Strategy". Foreign Affairs, Vol. 80, No. 2 (March — April, 2001). P. 119.

(20) Xinhua News Agency. Published on 30 August 2019, Available at: http://www.xinhuanet.com/english/2019-08/30/c_138351278 htm.

(21) Nina Hachigian. "China's Cyber-Strategy". Op.cit. P: 120.

(22) Matthew Bey. "Great Powers in Cyberspace: The Strategic Drivers behind US, Chinese and Russian Competition". Op.cit, P: 31.

(23) Ibid, P.32.

(٢٤) د. عبد الغفار الدويك، تقرير التوازن العسكري ٢٠١٩، قراءة تحليلية لـ القدرات السيبرانية في العالم، مصدر سابق، ص٢٧٦ – ٢٧٧.

(25) Adam Segal. "When China Rules the Web: Technology in Service of the State". Foreign Affairs. Vol. 97, No. 5 (September/October 2018). P: 10.

(26) Ibid, P: 11.

(٢٧) مها محمد محمد علام، ثورة المعلومات والأمن القومي، دراسة حالة الولايات المتحدة الامريكية، رسالة ماجستير، كلية الاقتصاد والعلوم السياسية، القاهرة، ٢٠١٤، ص٣٦.

(٢٨) سعاد محمد أبو ليله، دور القوة: ديناميكيات الانتقال من الصلبة إلى الناعمة إلى الافتراضية، مجلة السياسة الدولية، عدد ١٨٨، ابريل ٢٠١٢.

(٢٩) د. عادل عبد الصادق، كيف وظفت الصين الشبكات الاجتماعية في خدمة التنمية، مجلة الدبلوماسي، القاهرة، يناير ٢٠١٩، ص٦٠.

(30) Henry L. Hu, "The Political Economy of Govering ISPs in China: Perspectives of Net Neutrality and Vertical Integration." The China Quarterly (Cambridge University Press on behalf of the School of Oriental and African Studies), No. 207. September 2011, PP: 523 - 524

(٣١) د. عادل عبد الصادق، كيف وظفت الصين الشبكات الاجتماعية في خدمة التنمية، مصدر سابق، ص٦٢.

(٣٢) المصدر السابق، ص٦٤.

(٣٣) سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي، رؤية مستقبلية، مجلة رسالة الحقوق، جامعة كربلاء، العراق، عدد ٢، ٢٠١٥، ص٧٨.

(٣٤) جون باسيت، حرب الفضاء الالكتروني، مركز الدراسات للبحوث والدراسات، الامارات، ٢٠١٤، ص٥٨.

(٣٥) ريتشارد إيه كلارك، روبرت كيه كنيك، حرب الفضاء الالكتروني: الخطر القادم على الأمن القومي وسبل مواجهته – دراسة مترجمة، مركز الامارات للدراسات والبحوث الاستراتيجية، الامارات، ٢٠١٢، ص١٧٧.

(36) Tim Rains. "The Threat Landscape in China: A Paradox". Microsoft Corporation. Published on March 11, 2013. Accessed on 18/8/2019. Available at: http://www.microso.com/secuity/blog/2013/03/11/the-threat-landscape-in-china-a-paradox/

(37) Ryan David Kiggins. "US Leadership in Cyberspace: Transnational Cyber Security and Global Governance". In Jan-Frederik Kremer and Benedikt Miiller (eds.) "Cyber Space and International Relations." (Berlin: Springer-Verlag, 2014). P: 1.

(٣٨) بيتر سينجر، دروس الحروب الماضية والاتجاهات التكنولوجية المستقبلية في القرن الواحد والعشرون، مركز الامارات للدراسات والبحوث الاستراتيجية، الامارات العربية المتحدة، ٢٠١٤، ص٨٣.

(39) David C. Gompert, Hans Binnendijk. "The Power to Coerce: Countering Adversaries without Going to War. Op.cit, P: 29.

(٤٠) عبد الله مسعود، دراسات في الأمن القومي، كلية الإدارة والاقتصاد، جامعة بنغازي، ٢٠٠٢، ص٤٢.

(٤١) د. عبد المنعم المشاط، الأمن القومي العربي، مكتبة الشروق، القاهرة، ٢٠٠٦، ص٤٧.

(٤٢) د. سماح عبد الصبور عبد الحي، القوة الذكية في السياسة الخارجية، دار البشير، القاهرة، ٢٠١٤، ص١٦.

(43) Ryan J. Hayward. "Evaluating the Imminence of a Cyber Attack for Purposes of 'Anticipatory Self-Defense". Columbia Law Review, Vol. 117, No. 2. (March 2017). PP: 401 - 402.

(٤٤) أحمد أبو زيد محمد، بداية الحرب الالكترونية، مجلة الدبلوماسي، السعودية، ٢٠١٠، ص٢٦.

(٤٥) نادية مصطفى، القوة الذكية في السياسات الخارجية للدول، مركز الحضارة للدراسات السياسية، ٢٠١٦، ص٢٧٦.

(٤٦) م. عادل عبد المنعم، الهجمات السيبرانية وتأثيرها على الأمن القومي، السياسة الدولية، عدد ٢١٣، يوليو ٢٠١٨، ص٢٠٣.

(47) National Cyber Strategy of the United States of America. (Document). Issued by the White House. Washington, DC. September 2018. PP: 1 - 40.

(٤٨) عمرو عبد العاطي، استراتيجية امريكية هجومية ضد التهديدات السيبرانية، المركز المصري للفكر والدراسات الاستراتيجية ECSS، بتاريخ ٣١ اكتوبر ٢٠١٨، تاريخ الدخول ٢٠١٩/٥/١٢ متارح على https://bit.ly/2VZDU5M

(٤٩) عادل عبد الصادق، الصراع على الفضاء السيبراني بين التوجهات الروسية والامريكية، مصدر سابق، ص٢٧ – ٢٨.

(٥٠) رغدة البهبي، الوكالة السيبرانية، عوامل النشأة وانماط الفواعل، مجلة السياسة الدولية، عدد ٢١٨، ٢٠١٩، ص١٥.

(٥١) بوخنوس أمال، مصطلح الجريمة في قانون العقوبات الجزائري بين الصيغة والمفهوم، مجلة الحكمة، الجزائر، العدد ١، ٢٠٢١، ص٣٤.

(٥٢) عمار ياسر زهير، التحديات الأمنية المعاصرة للهجمات السيبرانية، مركز بحوث الشرطة.

قائمة المصادر

أولاً: الكتب:

١) بيتر سينجر، دروس الحروب الماضية والاتجاهات التكنولوجية المستقبلية في القرن الواحد والعشرون، مركز الامارات للدراسات والبحوث الاستراتيجية، الامارات العربية المتحدة، ٢٠١٤.

٢) جون باسيت، حرب الفضاء الالكتروني، مركز الدراسات للبحوث والدراسات، الامارات، ٢٠١٤.

٣) د. سماح عبد الصبور عبد الحي، القوة الذكية في السياسة الخارجية، دار البشير، القاهرة، ٢٠١٤.

٤) د. عبد المنعم المشاط، الأمن القومي العربي، مكتبة الشروق، القاهرة، ٢٠٠٦.

٥) ريتشارد إيه كلارك، روبرت كيه كنيك، حرب الفضاء الالكتروني: الخطر القادم على الأمن القومي وسبل مواجهته – دراسة مترجمة، مركز الامارات للدراسات والبحوث الاستراتيجية، الامارات، ٢٠١٢.

٦) عبد الله مسعود، دراسات في الأمن القومي، كلية الإدارة والاقتصاد، جامعة بنغازي، ٢٠٠٢.

٧) نادية مصطفى، القوة الذكية في السياسات الخارجية للدول، مركز الحضارة للدراسات السياسية، ٢٠١٦.

ثانياً: البحوث:

١) أحمد أبو زيد محمد، بداية الحرب الالكترونية، مجلة الدبلوماسي، السعودية، ٢٠١٠.

٢) ايهاب خليفة، امكانيات تحقيق الردع في صراعات الفضاء الإلكتروني، دورية اتجاهات الاحداث، عدد ١٣، ٢٠١٥.

٣) بوخنوس أمال، مصطلح الجريمة في قانون العقوبات الجزائري بين الصيغة والمفهوم، مجلة الحكمة، الجزائر، العدد ١، ٢٠٢١.

٤) ربيع محمد يحيى، اسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط، دورية رؤى استراتيجية، مركز الامارات للدراسات والبحوث الاستراتيجية، عدد ٣، ٢٠١٣.

٥) رغدة البهبي، الوكالة السيبرانية، عوامل النشأة وانماط الفواعل، مجلة السياسة الدولية، عدد ٢١٨، ٢٠١٩.

٦) سارة عبد العزيز، الحرب السيبرانية، التداعيات المحتملة لتصاعد الهجمات الالكترونية على الساحة الدولية، دورية اتجاهات الأحداث، عدد ٢٠، ٢٠١٧.

٧) سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي، رؤية مستقبلية، مجلة رسالة الحقوق، جامعة كربلاء، العراق، عدد ٢، ٢٠١٥.

٨) سعاد محمد أبو ليله، دور القوة: ديناميكيات الانتقال من الصلبة إلى الناعمة إلى الافتراضية، مجلة السياسة الدولية، عدد ١٨٨، ابريل ٢٠١٢.

٩) سماح عبد الصبور، الصراع السيبراني، طبيعة المفهوم وملامح الفاعلين، مجلة السياسة الدولية، عدد ٢٠٨، ٢٠١٧.

١٠) عادل عبد الصاحب، انماط الحرب السيبرانية وتداعياتها على الأمن العالمي، السياسة الدولية، عدد ٥٣، ٢٠١٧.

١١) عادل عبد الصادق، اسلحة الفضاء الالكتروني في ضوء القانون الدولي الإنساني، سلسلة أوراق عدد ٢٣، الاسكندرية، ٢٠١٦.

١٢) د. عادل عبد الصادق، الصراع على الفضاء السيبراني بين التوجيهات الروسية والامريكية، التقرير الاستراتيجي العربي ٢٠١٨، القاهرة، مركز الدراسات السياسية والاستراتيجية بالاهرام.

١٣) د. عادل عبد الصادق، كيف وظفت الصين الشبكات الاجتماعية في خدمة التنمية، مجلة الدبلوماسي، القاهرة، يناير ٢٠١٩.

١٤) م. عادل عبد المنعم، الهجمات السيبرانية وتأثيرها على الأمن القومي، السياسة الدولية، عدد ٢١٣، يوليو ٢٠١٨.

١٥) د. عبد الغفار الدويك، تقرير التوازن العسكري ٢٠١٩: قراءة تحليلية لـ القدرات السيبرانية في العالم، السياسة الدولية، عدد ١٦، ابريل ٢٠١٦.

١٦) عصام فاعور ملكاوي، الفضاء الإلكتروني ساحة حرب دولية مفترضة، أربد للبحوث والدراسات، الأردن، مجلد ١٨، عدد ٢، ٢٠١٥.

١٧)مصطفى عصام نعوس، حق الدولة في استخدام القوة في القضاء الإلكتروني للدفاع عن النفس، مجلة الحقوق، الكويت، مجلد ٣٨، عدد ١.

ثالثاً: الرسائل الجامعية:

١) مها محمد محمد علام، ثورة المعلومات والأمن القومي، دراسة حالة الولايات المتحدة الامريكية، رسالة ماجستير، كلية الاقتصاد والعلوم السياسية، القاهرة، ٢٠١٤.

رابعاً: المواقع الإلكترونية:

١) عمرو عبد العاطي، استراتيجية امريكية هجومية ضد التهديدات السيبرانية، المركز المصري للفكر والدراسات الاستراتيجية ECSS، بتاريخ ٣١ اكتوبر ٢٠١٨، تاريخ الدخول ٢٠١٩/٥/١٢ متارح على https://bit.ly/2VZDU5M.

خامساً: المصادر الاجنبية:

1) Adam Segal. "When China Rules the Web: Technology in Service of the State". Foreign Affairs. Vol. 97, No. 5 (September/October 2018)
2) Elisabeth Braw. "The GPS Wars Are Here". Foreign Policy. Published on December 17, 2018. Accessed on 15/6/2019, Available at: https:/foreignpolicy.com/2018/12/17/the-gps-wars-are-here
3) Elisabeth Braw. "The GPS Wars Are Here". Op.cit. Accessed on 15/6/2019, Available at: https://foreignpolicy.com/2018/12/17/the-gps-wars-are-here
4) Franz-Stefan Gady and Greg Austin. "Russia, the United States, and Cyber Diplomacy: Opening the Doors". EastWest Institute. 2010
5) Henry L. Hu, "The Political Economy of Govering ISPs in China: Perspectives of Net Neutrality and Vertical Integration." The China Quarterly (Cambridge University Press on behalf of the School of Oriental and African Studies), No. 207. September 2011
6) Mari Ristolainen. "Should RuNet 2020 Be Taken Seriously? Contradictory Views about Cybersecurity between Russia and the West". In Juha Kukkola, Mari Ristolainen and Juha-Pekka Nikkarila (Eds.), "Game Changer: Structural Transformation of Cyberspace". (Finland, Finnish Defence Research Agency Publications, 2017)
7) Matthew Bey. "Great Powers in Cyberspace: The Strategic Drivers behind US, Chinese and Russian Competition". The Cyber Defense Review. Vol. 3, No. 3 (Fall 2018)
8) Matthew J. Flynn. "Cyber Rebellions: The Online Struggle for Openness". T Journal of International Affairs , Vol. 71, No. 1.5, (Special Issue: Contentious Narratives: Digital Technology and the Attack on Liberal Democratic Norms) (2018)
9) National Cyber Strategy of the United States of America. (Document). Issued by the White House. Washington, DC. September 2018
10) Nina Hachigian. "China's Cyber-Strategy". Foreign Affairs, Vol. 80, No. 2 (March — April, 2001)
11) paul McLeary. "Russia's winning the Electronic War". Op.cit, Accessed on 15/6/2019, Available at: https:/foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war
12) Ryan David Kiggins. "US Leadership in Cyberspace: Transnational Cyber Security and Global Governance". In Jan-Frederik Kremer and Benedikt Miiller (eds.) "Cyber Space and International Relations." (Berlin: Springer-Verlag, 2014)
13) Ryan J. Hayward. "Evaluating the Imminence of a Cyber Attack for Purposes of 'Anticipatory Self- Defense". Columbia Law Review, Vol. 117, No. 2. (March 2017)
14) Tim Rains. "The Threat Landscape in China: A Paradox". Microsoft Corporation. Published on March 11, 2013. Accessed on 18/8/2019. Available at: http://www.microso.com/secuity/blog/2013/03/11/the-threat-landscape-in-china-a-paradox
15) Timothy L. Thomas ."Nation-State Cyber Strategies: Examples from China and Russia". In "Cyber Power and National Security", Edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. (United States , National Defense University Press, 2009)
16) Xinhua News Agency. Published on 30 August 2019, Available at: http://www.xinhuanet.com/english/2019-08/30/c_138351278 htm