جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة الأنبار
كلية القانون والعلوم السياسية
قسم العلوم السياسية

التنافس المعلوماتي بين الولايات المتحدة الأمريكية والصين:

دراسة في الأمن السيبراني

رسالة تقدم بها الطالب

محمد جسام على الله

إلى مجلس كلية القانون والعلوم السياسية- جامعة الأنبار وهي جزء من متطلبات الحصول على شهادة الماجستير في العلوم السياسية / الدراسات الدولية.

بإشراف

أ. م. د. رسول حسين علي

١٤٤٣هـ ٢٠٢١م

﴿يَا مَعْشَرَ الْجِنِّ وَالْإِنسِ إِنِ اسْتَطَعْتُمْ أَن تَنفُذُوا مِنْ أَقْطَارِ السَّمَاوَاتِ وَالْأَرْضِ فَانفُذُوا لَا تَنفُذُونَ إِلَّا بِسُلْطَانٍ﴾

سورة الرحمن: (٣٣)

الإهداء

الى الأحبة..

والدتي ووالدي... براً وأمتناناً

زوجتي وأولادي... حباً واعتزازاً

محمد

الشكر والأمتنان

الحمد لله الذي وسع علمه كل شيء، والصلاة والسلام على نبي الرحمة محمد صلى الله عليه وسلم، وبعد.

أشكر الله وأحمده (سبحانه وتعالى) على إتمام هذا الجهد المتواضع ثم من كان له الفضل في قبول الإشراف على رسالتي الأستاذ المساعد الدكتور رسول حسين علي، والشكر موصول إلى أستاذي في السنة التحضيرية الأستاذ المساعد الدكتور أحمد علي محمد الذي كان له الفضل في اختيار موضوع الدراسة، وإلى أساتذتي في كلية القانون والعلوم السياسية، وعلى رأسهم السيد العميد الأستاذ المساعد الدكتور هادي مشعان ربيع المحترم والسيد رئيس القسم الاستاذ المساعد الدكتور عماد رزيك عمر، والأساتذة الكرام في المرحلة التحضيرية قداوتنا الاجتماعية والأكاديمية، ولن أنسى حرصهم على تقديم كل معلومة مفيدة في مجال البحث العلمي الأكاديمي الرصين، كما أتقدم بالشكر إلى المقوم اللغوي والمقوم العلمي على جهودهم في تقويم الرسالة، ولجنة المناقشة الموقرة لتجشمها عناء قراءة الرسالة وتقويمها، وموظفي الكلية ومكتبة الكلية، كما أشكر جميع من ساعدني ولو بكلمة طيبة.

وشكري الخاص إلى البروفيسور جيمس اندريو لويس – معاون مدير المركز الاستراتيجي للدراسات الدولية في واشنطن (CSIS)، والشكر موصول إلى المعنيين في وزارة الخارجية الامريكية قسم شؤون شرق آسيا والمحيط الهندي، وذلك لقبولي كعضو متابع لكل نشاطات المركز (CSIS) ونشاطات قسم شرق آسيا والمحيط الهندي في الوزارة من خلال البريد الالكتروني.

الباحث

الملخص

خلّف التنافس السيبراني اثاراً متباينة على صعيد العلاقات الدولية والنظام الدولي، ولعل واحداً من أهم اثارهِ يتجلى اليوم في التنافس السيبراني المُحتدم بين الولايات المتحدة الأمريكية والصين فعلاقات الصين الجديدة ونُقاط القوة التي أصبَحت تتمتع بها في كثير من الأصعدة ومنها الأمن السيبراني، تَعني أن لديها مكانة ومسؤوليات جديدة في العالم، تُنافس فيها الولايات المتحدة كقائد للنظام العالمي، أذ يُمكن للتنافس السيبراني أن يصبح عاملاً مُهماً وربما حاسماً في عملية إعادة تعريف العلاقة الثنائية بين القوتين العظميين، بل قد يؤدي إلى تفاقم المنافسة الاقتصادية والعسكرية، إلى حد الصراع بينهما في المستقبل.

إنِّ التطور الهائل الذي أدخله العالم على البنية التحتية العالمية للمعلومات خلال العقدين الماضيين، جعل من الفضاء السيبراني ساحة جديدة ومهمة للتنافس الدولي، وعليه فقد غدا الأمن السيبراني يحتل مركز الأولوية في الاستراتيجيات الأمنية للقوى الدولية العظمى والكبرى التي تتنافس على الصدارة، في ظل نظام دولي جديد متعدد الأقطاب آخذ في الظهور ولكن لم يتضح بعد مخططه أو شكله النهائي، والواقع إن التنافس بين الولايات المتحدة والصين ليس جديداً، ولكنه أخذ أشكالاً ووسائل جديدة فرضها التطور التقني والتكنولوجي الذي يشهده العالم، ويبدو أن العناصر الأكثر تأثيرًا في التفكير الصيني اليوم، هي الرغبة في تطوير قدرات عسكرية غير تقليدية ومتكافئة مع الولايات المتحدة، واستعادة مكانة الصين التي تستحقها في العالم، هذه العوامل مجتمعة مع شعور وأضح بصعود الصين كقوة منافسة للهيمنة الامريكية، جعلت الولايات المتحدة تنظر للصين بأنها أخطر منافس لمكانتها العالمية، من وجهة نَظر الولايات المُتحدة ثمةَ قضايا رئيسة، تُشكل مصدر خطر على الأمن السيبراني هي: الشكُوى من الاختراقات الصينية المتكررة لشبكات المعلُومات، واحتمال أن تكون الصين على أهُبة الاستعداد لشن هجوم الكتروني بهدف تدمُّير البنية التحتية الاساسية الأمريكية، أما الجانب الصيني فانهُ يشجُب هذه الاتهامات ويدّعي بأنه هو الذي يتعّرض للهجُوم الإلكتروني كما ينتَقد الجانب الصيني تموّيل الولايات المتحدة لتكنُولوجيا التحايل على رقابة الانترنيت، وُيؤيد حق الدول في الرقابة على المعلومات داخل حدودَها، أو ما يعرف (بالسيادة الالكترونية)، كما ترفض الصين الهيمنة الأمريكية على الانترنيت.

قائمة المحتويات

قائمة الجداول

الاختصارات

الاختصار	الاسم باللغة العربية	الاسم باللغة الانكليزية
IMF	صندوق النقد الدولي	International Monetary Fund
GDP	الناتج المحلي الاجمالي	Gross domestic product
CSIS	مركز الدراسات الاستراتيجية والدولية	Center for Strategic & International Studies
SIPRI	معهد ستوكهولم الدولي لأبحاث السلام	Stockholm International Peace Research Institute
IW	حرب المعلومات	Information warfare
AI	الذكاء الاصطناعي	Artificial intelligence
COVID-19	مرض فيروس كورونا	Coronavirus diseas 2019
NSA	وكالة الأمن القومي	National Security Agency
RCEP	اتفاقية الشراكة الاقتصادية الشاملة	Regional Comprehensive Economic Partnership Agreement
G5	تقنيات الجيل الخامس للأنظمة الالكترونية	Fifth generation technologies for electronic systems
HGV	المركبات الانزلاقية بسرعة فوق صوتية	glide Vehicles High speed
OECD	منظمة التعاون الاقتصادي والتنمية	Organization for Economic Cooperation and Development
GCS	المجتمع المدني العالمي	Global Civil Society
Belt	الحزام الاقتصادي لطريق الحرير	Silk Road Economic Belt

Chinese Communist Party	الحزب الشيوعي الصيني	CCP
United States Space Command	قيادة الفضاء الأمريكية	USSC
North Atlantic Treaty Organization	منظمة حلف شمال الأطلسي	NATO
Rare earth elements	العناصر الأرضية النادرة	REE

المقدمة

سابقا كانت المنافسة التقليدية والقُوة العسكرية تُحددان طبيّعة الخطابات السياسية وشكل النظام العالمي ومراكز القُوى الكبرى في هذا النظام، إلا أن بروّز العامل السيبراني واتساع تأثيرهُ في السياسات الدولية وخاصةً بداية القرن الحادي والعشرين، أضاف أبعاداً أخرى للقُوة العسكرية، ولم يعد هناك حُدود بين ما هو مدني وعسكري، ومن ثَم أخذت المنافسة –ومنها المنافسة بين الولايات الامريكية والصين – سِمات غير تقليدية من حيث الفاعلين والقضايا أو طرق التفاعُل في عالمِنا الراهن.

ومع بروز الفضاء الالكتروني (cyberspace) كساحة للتنافس العالمي، واجهّت المفاهيم التقليدية في العلاقات الدولية: الصراع، الأمن، القوة والسيادة، تحديات واضحة من حيث مدى تكيفُها مع طبيعة التفاعلات في الواقع الافتراضّي، حيث برزت الحاجة الى مَداخل ورؤى نظرية أكثر قُدرة على تفسير طبيعة التغيُرات التي أحدثتها الحقائق التكنُولوجية بهذه المفاهيم.

ومن بين أبّرز نَماذج التنافس المعلوماتي في عصرنا الراهن، التنافس الأمريكي –الصيني، فمُنذ تأسيس جمهورية الصين الشعبية سنة ١٩٤٩، أتسمت العلاقة بين الولايات المُتحدة والصين بقدر كبير من التنافس والتحّدي، وقد ازدادت حدة المنافسة التي تُفرق بين البلدين في الفترة الأخيرة والتي تنعَكس على الفضاء الالكتروني بقدر ما تنعكِس على العلاقات في العالم الفعلي. وفي الواقع من بين جميّع المجالات التي اضطَربت بها العلاقة بين الطرفّين كان مجال الفضاء الإلكتروني أكثرُها أثارةً للخلاف.

لذلك تسعى كل من الولايات المتحدة الأمريكية كونها الدولة المهُيمنة على النظام الدولي، والصين التي تُحاول الحد من هذه الهيمَنة، وفرض نفسها كلاعّب أساسِ في النظام الدولي بما يتناسب مع الإمكانيات والقُدرات التي أصبحت تتمتع بها، إلى العمل باستمرار من أجل الحد من التهديّدات والاختراقات الإلكترونية في مجال الفَضاء الالكتروني لكلا الدولتيّن، ومنع أو التخفيف من هذه المخاطر نظراً لارتباطِها الشديد بالأمن القومي لكلا القوتين وتأثيرها على الأمن العالمي.

أهمية الدراسة:

تكمن أهمية الدراسة في إطار الاهتمام الدولي المتصاعد في الأمن السيبراني، وما فرضهُ من تحُولات طالت أغلب مجالات الحياة اليومية ، بدءاً من الممارسات الحكومية مروراً بالعلاقات بين الدول، وصولاً الى جهود المنظمات الإقليمية والدولية لا سيما جهود الأمم المتحدة ، كما أن أهميتها تَتركز، في الكشف عن أهمية البُعد السيبراني في العلاقات الأمريكية – الصينية لاسيما وأن العلاقة بينهُما ستُحدد الصورة المستقبلية للنظام العالمي، وأن الفضاء التجاري والسيبراني هما الفضاءان الأكثر سُخونة في العلاقة بين هاتين القوتين العظيمين.

هدف الدراسة:

تهدف الدراسة الى ما يلي:

١- بيان تأثير التنافس السيبراني في العلاقة ما بين الولايات المتحدة الأمريكية والصين في الحقل العلاقات الدولية وأبعادهُ في التَنافس الامريكي الصيني، بغية استِشراف مُستقبل النظام العالمي، والتنافس المحموم على القيادة فيه.

٢- تقديم رؤية لصانع القرار حول أهمية وخطُورة الأمن السيبراني على الأمن القومي، واستِدراك المخاطر المستقبلية التي ربُما يُسببها التنافس بين الصين والولايات المتحدة في العلاقات الدولية، كونهُما أهم قوتين تَتصدران النظام الدولي.

إشكالية الدراسة:

إنِّ المتغير السيبراني دخل الى حقل العلاقات الدولية بشكل كبير، وأصبح أحد المتغيرات الأساسية التي باتت تؤثر في طبيعة العلاقات الأمريكية – الصينية، وذلك نتيجة التطورات والتغيُرات في الأحداث والظروف التي تشهدُها البيئة الدولية، والسؤال المركزي للدراسة هو: هل من الممكن أن يصل التنافس الصيني – الأمريكي في مجال المعلومات الى حد الصراع والمواجهة في الفضاء الالكتروني؟ كما يتفرع عن هذا السؤال أسئلة فرعية أخرى أهمها.

- ماهي طبيعة التنافس المعلوماتي بين الولايات المتحدة الأمريكية والصين

- وكيف يؤثر هذا التنافس على العلاقة بين البلدين
- ما طبيعة تأثيره على العلاقات الصينية الأمريكية؟
- هل أن الفضاء الالكتروني والتفاعلات التي تحصل فيه معززة للسلم والأمن الدوليين ؛ ام أنه عامل عدم استقرار للنظام العالمي؟

فرضية الدراسة:

تنطلق الدراسة من فرضية مفادها: أن التنافس الأمريكي – الصيني في مجال المعلومات أصبح عاملاً أساسياً في العلاقة التنافسية بينهما، هذه العلاقة التي تتجه الى التصعيد والمواجهة أكثر منها الى التعاون والاندماج، في ضوء العلاقة التي يشوبها الغموض والتعقيد بين القوتين اللتين تتصدران المشهد الدولي.

منهج الدراسة:

إنّ طبيعة موضوع الدراسة فرضت على الباحث، تحديد المناهج المعتمدة فيها، إذ اعتمدت الدراسة على المنهج التحليلي فضلا عن المنهج المقارن بغية المقارنة بين معالجة كل من الطرفين للتهديدات النابعة من الفضاء الالكتروني، أضافة الى المنهج القانوني حيث تسعى المنظمات الدولية والدول المتقدمة خاصة الى محاولة إيجاد تكييف قانوني للفضاء الالكتروني، والهجمات الالكترونية التي تقوم بها الفواعل من الدول وغير الدول، في محاولة لأنفاذ القانون على هذه الجرائم للحد منها.

نطاق الدراسة:

يتحدد نطاق الدراسة، مكانياً ضمن الفضاء الإلكتروني للولايات المتحدة والصين وما يتضمنه ذلك التنافس من تدابير واستراتيجيات دفاعية وتوظيف للقوة الالكترونية، وزمانيا ركزت الدراسة على حقبة تكنولوجيا المعلومات نهاية القرن العشرين و بداية القرن الحادي والعشرين (١٩٩٠– ٢٠٢٠) وانطلاقا الى دراسة الآفاق المستقبلية للتنافس المعلوماتي بين الصين والولايات المتحدة.

الدراسات السابقة:

إن موضوع الأمن السيبراني بصورة عامة – والاستراتيجية السيبرانية للولايات المتحدة والصين خاصة – هي موضوع جديد في حقل دراسة العلاقات الدولية، لذلك تطرقت بعض الدراسات السابقة الى موضوع التحول الاستراتيجي، من الاستراتيجيات التقليدية وتباينها وصولاً الى الاستراتيجية المراد دراستها (السيبرانية)، ويمكن اعتبار العلاقات الامريكية – الصينية أكثرها تأثرا في مجال توظيف القوة الالكترونية في التفاعلات الدولية –الأمن السيبراني– مقارنة مع بقية الدول، ومن هذه الدراسات.

١– عبد الكريم زهير عطيه الشمري، الاستراتيجية الأمريكية للهيمنة على الفضاء السيبراني، رسالة ماجستير، جامعة الموصل، كلية العلوم السياسية، ٢٠٢١. حيث ركزت الدراسة على محاولة الولايات المُتحدة الهيمنة على الفضاء الالكتروني، أذ تطرقت الدراسة الى الاستراتيجية السيبرانية لكل من، روسيا ، الصين ، كوريا الشمالية ، ألمانيا ، إيران ، اليابان والهند والتصارع بين هذه الاستراتيجيات الحليفة منها وغير الحليفة للولايات المتحدة، وسعي الولايات المتحدة الأمريكية لفرض نفوذها الفضاء الالكتروني الدولي. إلا إن الدراسة لم تركز على التنافس المعلوماتي الأمريكي– الصيني في مجال الأمن السيبراني، وتأثيره على السلم والأمن الدوليين.

٢– دراسة فريدة طاجين، تأثير القوة السيبرانية على الاستراتيجيات الأمنية للدول الكبرى – دراسة حالة الصين – ، رسالة ماجستير، جامعة قاصدي مرباح ورقلة، ٢٠١٨ . تركز هذه الدراسة على تزايد تأثير القُوة السيبرانية على الاستراتيجية الصينية في مجال الفضاء السيبراني او ما يطلق عليه الحرب الباردة الجديدة وسعي الصين لتبني استراتيجية أمنية لحماية الأمن القومي ضد التهديدات والهجمات الإلكترونية المعادية ، دون الإشارة الى الاستراتيجية الأمريكية في هذا المجال ومحاولة الولايات المتحدة فرض هيمنتها السيبرانية لتُشكل امتداد للهيمنة العسكرية والسياسية على الصعيد الدولي. وتفيد هذه الدراسة عند تناولنا الاستراتيجية السيبرانية الصينية .

٣– دراسة: إيهاب خليفة، القوة الالكترونية: كيف يمكن أن تُدير الدول شؤونها في عصر الانترنت، الصادرة عن دار العربي للنشر، القاهرة ٢٠١٧. وقد تناول فيها الباحث التغيرات التي طرأت على القوة بفعل الانترنت، وعناصر القوة الالكترونية الأمريكية من حيث العناصر والتهديدات

وكيفية توظيف القوة الالكترونية في المجال السياسي، الاقتصادي والعسكري أضافة الى انواع الأسلحة السيبرانية حيث ركزت على القوة الالكترونية الامريكية ولم تتطرق الى القوة الصينية.

٤- جيمس أندرو لويس، الحرب الإلكترونية والمنافسة في العلاقة بين الصين والولايات المتحدة (Electronic warfare and competition in the relationship between China and the United States)، مركز الدراسات الاستراتيجية والدولية (CSIS)، واشنطن، تموز ٢٠١٠. وكانت باللغة الانكليزية أذ تمت ترجمة الدراسة من قبل الباحث، وتشير الدراسة إن الولايات المتحدة والصين تعملان على إعادة تحديد علاقتهما الثنائية، حيث تعني نقاط القوة الجديدة للصين أن لديها موقعًا جديدًا ومسؤوليات جديدة في العالم، ويمكن أن يصبح الصراع السيبراني عاملاً مهماً وضاراً في عملية إعادة التعريف الثنائي هذه، لأنه يشمل ويؤدي إلى تفاقم المنافسة الاقتصادية والعسكرية، وقد غطت الفترة لغاية ٢٠١٠.

٥- دراسة بعنوان التوصل إلى اتفاق مع الصين بشأن الفضاء الالكتروني، وقد جاءت على شكل تقرير أعده كل من (سكوت وارين، ومارتن سي ليبيكي وأستريد ستوث سيفالوس، مؤسسة راند للنشر، كاليفورنيا ،٢٠١٦) ويناقش التقرير مسألتين أساسيتين: المجموعة المعنية بعلاقات الولايات المتحدة مع الصين، وتلك المعنية بوضع قواعد السلوك في الفضاءِّ الإلكتروني، ولاسيما القواعد التي تعزز الأمن والحرية، كما ناقش التقرير كذلك مشكلة الفضاء الإلكتروني في العلاقات بين الولايات المتحدة والصين دون الإشارة الى مستقبل التنافس بين الدولتين

٦- دراسة: (كينيث ليبرثال وبيتر دبليو سينجر)، الأمن السيبراني والعلاقات بين الولايات المتحدة والصين، معهد بروكينغز، واشنطن فبراير ٢٠١٢، توضح الدراسة أن عالم الإنترنت لديه عدد من الخصائص الخاصة التي تشكل تحدي للعلاقات الأمريكية الصينية الحالية وآفاق الوصول إلى إجماع على القواعد أو آليات التنفيذ التعاونية. وتشير الدراسة بأن قضية الأمن السيبراني تُهدد بأن تصبح مصدر رئيسي للخلاف بين الولايات المتحدة والصين، ويكمن الخطر في أن التكنولوجيا التي تربط العالم ستفرق بين هاتين الدولتين وبدلاً من ذلك ؛ على واشنطن وبكين أن تبدأ في بناء أُسس لمزيد من التفاهم والتعاون المتبادل، وجاءت الدراسة هنا لتشكل امتداد زماني لموضوع التنافس بين الولايات المتحد والصين في مجال التنافس السيبراني .

وهذه الدراسة المتواضعة جاءت مكملة ومعززة للدراسات السابقة، ولتشكل أضافة نوعية الى موضوع الأمن السيبراني – الذي يمتاز بالتطور السريع – ومدى تأثيرهُ على السلم والأمن العالمي، وهل أصبح العالم في وضع أفضل مما كان عليه قبل دخول التكنولوجيا الرقمية الى الحياة على مستوى الافراد والدول، ومدى تأثير الأمن السيبراني على استقرار السلم والأمن الدوليين، في ظل الاستخدام الواسع للأنترنت.

هيكلية الدراسة

اقتضت طبيعة الدراسة تقسيمها الى مقدمة و ثلاثة فصول والخاتمة التي ذكرتُ فيها أهم الاستنتاجات، درس الفصل الأول: الفضاء الالكتروني والأمن السيبراني: مدخل مفاهيمي من خلال مباحث ثلاثة هي: ماهية الأمن السيبراني ، والمبحث الثاني تناول الفضاء الإلكتروني والعلاقات الدولية وتضمن المبحث الثالث اهمية القانون الدولي لتنظيم الفضاء الإلكتروني اما الفصل الثاني: أختص بالبعد السيبراني في العلاقات الأمريكية – الصينية من خلال ثلاثة مباحث اختص الأول بطبيعة العلاقات بين البلدين وعرض المبحث الثاني والثالث الاستراتيجية السيبرانية لكل من الولايات المتحدة الأمريكية والصين، وفي الفصل الثالث: حاولت الدراسة استشراف التنافس السيبراني الأمريكي– الصيني (في الفضاء الإلكتروني) وأفاقه المستقبلية، حيث تناول المبحث الأول، مستقبل الأمن السيبراني وتضمن المبحث الثاني تجارة الأسلحة السيبراني نظرة مستقبلية وقد جاء المبحث الثالث لبيان مستقبل التنافس السيبراني بين الولايات المتحدة الأمريكية والصين للسيطرة واستثمار موارد الفضاء الخارجي التي تشكل مصدر الثروات المستقبلية بعد شحتها أو نفادها على سطح الأرض.

الفصل الأول

الفضاء الإلكتروني والأمن السيبراني (مدخل مفاهيمي)

يشهد الفضاء الإلكتروني تنامياً مستمراً في استخداماتهِ وتطبيقاتهِ، التي أصبح لها دور جوهري في تحسين الحياة البشرية، في المجالات الاقتصادية والاجتماعية وتحقيّق أهداف التنمية المُستدامة، وفضلاً عن أهميتهِ في مجالات الاتصالات والملاحة والبث الإعلامي؛ حيث أصبح الفضاء الخارجي عاملاً مهماً، لرصد تغُير المناخ ومكافحة التصحُر وإدارة الكوارث وتحسين إدارة الموارد الطبيعية للأرض لذلك، فمن الضروري الاسَتمرار في استكشاف الفضاء وتطوير وتعزيز البحث العلمي، وتوفير المُوارد التي من شانها ان تُتيح لنا استخدامهِ بطُرق سلمية تعود بالنفع على العالم أجمع.

بالرغم من اختلاف تسمية مُصطلح الفضاء الإلكتروني، من قبل المختصين في هذا المجال ما بين مصطلح الأمن السيبراني تارة والفضاء الالكتروني تارة أخرى، إلا أن الدراسة سوف تذهب لاستعمال كلمة الإلكتروني عندما يكون الحديث عن الفضاء الإلكتروني والفضاء بشكل عام، ونشير الى مصطلح "السيبراني" عند الحديث عن التنافس السيبراني والأمن والاختراق والتجسس والهجمات، أي كل ما يخص الأمن تحديداً؛ لكون الأمن السيبراني جزء من الفضاء الالكتروني، وسيتم تقسيم الفصل الى ثلاثة مباحث:

المبحث الأول: يتناول الأمن السيبراني والحروب السيبرانية

المبحث الثاني: يتضمن الفضاء الإلكتروني والعلاقات الدولية

المبحث الثالث: فقد بيِّن الاجراءات الدولية لتنظيم الفضاء الالكتروني.

المبحث الأول: ماهية الأمن السيبراني

انتقل جزءاً كبيرا من الصراعات بين القِوى الكبُرى في العالم، من ميادّين القتال التقليدية إلى ميادّين الفضاء الالكتروني وشبكات الإنترنت والعالم الرقمي، وتُعد حماية مصالح الدولة من أهم أولويات واضعّي سياسات الامن القومي الدفاعية، وأصبح الأمن السيبراني من أولويات الأمن القومي وضمن البيئَة الاستراتيجية للدولة، التي عرفتها كلية الحرب الأمريكية هو [1] " نظام عالمي حافل بتهديدات واسعة ومُثيرة للشكوك والصراع متأصل فيها وغير قابلة للتنبؤ، وتكون القُدرات الوطنية للدفاع عن المصالح القومية العُليا للدولة، مقيّدة بقيود مرتبطة بحجم الموارد البشرية والمادية وتغُلب عليها سمات التّقلب والتوجس والتعقّيد والغموض".

المطلب الأول: مفهوم الأمن السيبراني والمفاهيم المقاربة له

لقد أصبح الأمن السيبراني من أولويات الأمن في السياسة الامنية للدول، وخاصة في الدول الكبرى حيث يُصَنّف صُناع القرار مسائل الدفاع السيبراني، من أولويات القضايا الدفاعية الوطنية، كون الحروب السيبرانية أصبحت أخطر ما يُهدد سيادة الدول والشركات وحتى الأفراد، وكون الأمن السيبراني جزء من الفضاء الإلكتروني سوف نعرفه في هذا المطلب مع تعريف مفهوم الأمن السيبراني وأمن المعلومات وكذلك توضيح المفاهيم المقاربة له.

أولاً: تعريّف الفضاء الالكتروني. (Cyberspace)

أشتهر مُصطلح الفضاء الإلكتروني في التسعينيات، بعد تُوسع استخدامات الإنترنت والشبكات والاتصال الرقمي وقد ظهرت عدة تعريفات، فقد عرفتهُ جامعة الدفاع الوطني الأمريكية بانه " مجال تشغيلي تجري فيه مجموعة من العمليات ذات طابع الكتروني، مُحكم بمجموعة من الاستخدامات التي تعتمد على الالكترونيات والاطياف الكهرومغناطيسية لإنشاء وتخزين وتبادل المعلومات من خلال مجموعة من نُظم المعلومات المتصلة عبر الانترنيت والبنى التحتية الخاصة

(١) نقلا عن هاري آر .يارغر، الاستراتيجية ومحترفو الأمن القومي: التفكير الاستراتيجي وصياغة الاستراتيجية في القرن الحادي والعشرين، ترجمة راجح محرز علي، مركز الامارات للدراسات والبحوث الاستراتيجية، ابو ظبي، ٢٠١١، ص٥٦.

به" [١].ويعرَف (de Rosnay Joel) في هذا الاطار الفضاء الرقمي او الفضاء الالكتروني (cyberspace) بوصفه " فضاء يجمع بين مكونين هما الفضاء والزمان الالكترونيين، فضاء تم تشكيلهُ بواسطة شبكات التواصل التي اقيمت بين الحواسّيب" [٢].

ثانياً: مفهوم الأمن السيبراني.

الأمن السيبراني يقصد بهِ الأمن الإلكتروني من حيث اللغة ويهتم بمسألة الحماية والدفاع ضد الهجمات الإلكترونية، من خلال توفير البرامج لمنع الاختراقات، اذاً هو" إتخاذ اجراءات ووضع معايير لمنع وصول المعلومات الخاصة أو لحماية تلك المعلومات، بأن تكون في أيدي جهة معادية أشخاص غير مخولين بها عبر الشبكة المعلوماتية" [٣].

ومصطلح "السيبرانية– (cybernetic) مُشتق من المصطلح الأغريقي (kybernetes)، ويعني قائد الدفة او الحاكم، وأصل الكلمة الإنجليزية (cyber) متأصل في المصطلحات التي يَكثُر استخدامها في مجال تكنُولوجيا المعلومات مثل الفضاء الإلكتروني – (Cyberspace) أي العالم الرقمي و"الخيال العلمي السيبراني (Cyberpunk) [٤] وفي اللغة الإنكليزية تعني السيبرانية أنها" تتعلق او تتضمن أجهزة الكمبيوتر او شبكات كمبيوتر مثل الأنترنيت" [٥] ولا ينبغي فهِم السيبرانية على أنها تنطبق فقط على النُظُم القائمة على الآلات؛ فالبشر كافة يعتمدّون على حلقات تعقيب سيبرانية في أجسامُنا من أجل إدارة العمليات الحيوية مثل التَنفس والدورة الدموية، ولاسيما التُواصل

---

(1) Daniel T.Kuehl, "From Cyber Space to Cyber power: Defining the problems "in Franklin D. Krammer,Stuart, and Larry K.Wentz. eds, cyber power and national security (Washington, D.C: National defense up,2009,p.2 .

(2) de Rosnay Joel L Homme Symbiotique, Reqard sur la troisieme millenaire, paris, LeSeuil,15 March 1995..Available: https://www.seuil.com/ouvrage/l-homme-symbiotique-regards-sur-le-troisieme-millenaire-joel-de-rosnay/9782020217149 the date visit 15 February.

(٣) فريدة طاجين، تأثير القوة السيبرانية على الاستراتيجيات الأمنية للدول الكبرى – دراسة حالة الصين – ، رسالة ماجستير، جامعة قاصدي مرباح ورقلة،الجزائر، ٢٠١٨، ص ١٩ .

(٤) وهو اسلوب ادبي يشير الى ما بعد الحداثة، للتفصيل ينظر: بيتر بي سيل، الكون الرقمي– الثورة العالمية في الاتصالات، ترجمة ضياء وزّاد، مؤسسة هنداوي للنشر، لندن، ٢٠١٧، ص٢٢.

(٥) قاموس ميريام ويبستر متاح على الرابط : Merriam-webster.com.

مع الآخرين [١]. لكن الترجمة العربية تحديدا لكلمة (cyber) تعني الإلكتروني، إلا أن الشائع عند الباحثيّن هو استعمال كلمة سيبراني وكُثرة الاستعمال هذه أعطت تصور لدى الكثير عن هذا المصطلح وأن كان البعض يَستعمل كلمة (افتراضي، معلوماتي، الكتروني ورقمي)، كما أشارت إلى ذلك الباحثة (رغدة البهي) هناك عدد من الترجمات العربية لمصطلح (cyber) منها المعلُوماتي والافتراضي والسيبراني والرقمي إلا أن الباحثة تميل الى استخدام لفظ سيبراني بوصفهِ الأقرب الى الترجمة الانكليزية " [٢].

كانت القضايا المتعلقة بالأمن حتى أواخر القرن العشرين هي القضايا التقليدية، (الأبعاد العسكرية والاقتصادية) في حين ظهرت على الساحة العالمية قضايا جديدة لم تكون مألوفة من قبل " مثل الأمن الشخصِي، والأمن البيّئي والصحي والامن الثقافي، والأمن السيبراني، وهي قضايا حديثة لا تنَدرج ضمن الأمن التقليدي، فقد أشار الكاتب(Richard H. Ullman) إلى إعادة تعريف الأمن في مقالة له عام ١٩٨٣بعنوان (Redefining Security)، باعتبار المنظُور الضّيق للأمن القومي الذي يتلخص بحماية حدود الدولة من الهجمات العسكرية مفهُوم خاطئ وخطر" [٣]. أذ اعُتبر الفضاء الإلكتروني منذ بداية القرن الحادي والعشرين أحد مجالات الأمن القومي وعَدهٌ المختصين بأنه "المجال الخامس غير التقليدي للحرب (المجال البري ، البحري ، الجوي، والفضاء) من حيث تشابكية العالم الافتراضي مع العالم المادي، وهو الذراع الرابع لقوات الدولة الاستراتيجية البرية والجوبة والبحرية" [٤]. وفي حال تعرض الدولة للهجمات السيبرانية فأن هذه الهجمات لا تفرق بين ما هو مدني وعسكري. ومع بروّز الفضاء الالكتروني (Cyberspace) كساحة جديدة للصراع العالمي، بدأت المفاهيم التقليدية مثل الصراع، الأمن، القُوة، والسيادة تواجه تحديات تتعلق بمدى مُلائمتها أو تكيفِها مع نوع التحديات في الواقع الافتراضي.

---

(١) المصدر نفسه، ص ص٢١-٢٢.

(٢) رغدة البهي، الردع السيبراني: المفهوم والاشكاليات والمتطلبات، مجلة العلوم السياسية والقانون العدد الاول، المركز الديمقراطي العربي للدراسات الاستراتيجية والاقتصادية، برلين، كانون الثاني ٢٠١٧، ص ٤٩.

(٣) نقلا عن إيهاب خليفة، الأمن السيبراني الماهية والاشكاليات، مجلة رؤى مصرية ،العدد٥٧،مركز الأهرام للدراسات الاجتماعية والتاريخية، القاهرة، ٢٠١٩، ص٤-٥.

(٤) يونس مؤيد يونس مصطفى ، استراتيجية الولايات المتحدة الامريكية للأمن السيبراني ،مجلة كلية العلوم السياسية جامعة الموصل ، العدد ٥٥، ٢٠١٨ ،ص ١٢٦.

وقد حددت الولايات المتحدة قائمة طويلة من الصناعات التي يجب حمايتها من الهجمات الإلكترونية، وبالتالي تقع ضمن مسؤولية الأمن السيبراني القومي، وتشمل البنية التحتية وأنظمة الغذاء والمياه والزراعة والأنظمة الصحية والطاقة أضافة الى أنظمة الدفاع [١]. وقد أشار مجلس الاتحاد الأوربي في لائحتهِ الفقرة (١) تلعب أنظمة الشبكات والمعلومات وشبكات وخدمات الاتصالات الإلكترونية دورًا حيويًا في المجتمع وأصبحت العمود الفقري للنمو الاقتصادي" [٢].ومن أجل الاحاطة بكل جواني الأمن السيبراني والوقوف على أشكاله ومكوناتهِ ومنظومة العمل التي ينشط خلالها هذا المتغير الجديد والمهم لا بد من الإشارة أهم ثلاث أشكال رئيسية للأمن السيبراني وهي [٣]:

١- القُوة السيبرانية: التي تعني القدرة على استخدام الفضاء الإلكتروني لخلق مزايا والتأثير على الأحداث في بيئات تشغيلية أُخرى وعبر الأدوات "من القوة "

٢- الِدفاع السيبراني ويُقصد به الدفاع الالكتروني: "مجموعة القُدرات النظامية التي تمتلكُها القوات المسلحة للحماية من تأثيرات الهجمات السيبرانية والتخفيّف من حدتِها والتعافي منها بسرعة".

٣- الردّع السيبراني: نتيجةً للطبيعة الخاصة بالفضاء الالكتروني فأنهُ من الصعوبة منع الهجمات الإلكترونية بصورة كُلية من الأساس؛ نتيجة للهجمات الصفرية والثغرات التي يتم اكتشافُها وصعوبة تعقب مصدر الهجمات ومعرفة الفاعل من الناحية الفنية.

ونظراُ لطبيعة الفاعلين في هذا المجال من حيث سهولة شن الهجمات الإلكترونية وصعوبة منعها او ايجاد تكييف قانوني لها يمكن بيان أهم اشكاليات الأمن السيبراني فيمكُن أجمالها بالآتي [٤]:

١- صعوبة معرِفة مصدر الهجمات (صعوبة تحديد هوية المعتدي).

---

(1) Lewis, J. A. Cybersecurity and Critical Infrastructure Protection. Washington, (CSIS) Center for Strategic and International Studies,, January 2006,p.4.

(2) REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of, 17 April 2019,p.2.

(٣) ايهاب خليفة، مصدر سبق ذكره، ص ٥

(٤) المصدر نفسه، ص ص٦-٧.

٢- صعُوبة وضع الخصُم في تهديد حقيقي. أي إن الدول التي تتعرض لهجمات سيبرانية هي التي تُقدر مدى الخسائر التي تلّحق بها، لذلك قد تشن دولة هجُوماً على دولة أخرى لكن هذا الهجُوم في تقدير الدولة المُعتدى عليها غير مُؤثر وفي هذه الحالة يفشل الردّع .

٣- صعُوبة منع الهجمات الصفرية* نتيجة التحديث المستمر بنُظم المعلومات.

مقابل هذه الإشكاليات التي تحدد طبيعة هذا المتغير يمكن القول ان أهم ميّزات الأمن السيبراني، إنها ذات طابع اجتماعي وتقني متعدد التخصصات، وكونها شبكة خالِية من النطاق، حيث من المُحتمل أن تكون قُدرات الجهات الفاعلة في الشبكة متشابهة الى حد كبير، مع درجات عالية من التغيّير والترابُط وسُرعة التفاعل [١].

ويعكس الأمن السيبراني من جهة الى "وصف الحد الأدنى من المتطلبات اللازمة لنظام المعلومات الحفاظ على مستوى مقبول من المخاطر" [٢]. بمعنى تقليل المخاطر الى الحد الأدنى او لمنع وصول المعلومات إلى جهات معادية وبذلك يَتداخل مع مصطلح أمن المعلومات وهذا ما سيتم تفصيله في الفقرة اللاحقة.

ثالثاً: أمنّ المعلُومات.

يهتم أمن المعلومات بحماية كل ما يتعلق بالمعلومات ضِمن الحاسَب أو خارجهِ وليس حماية الحاسب فقط ، حيث إن كل ما يُحفظ ضمن أي نظام حاسُوبي يُدعى بيانات ولكنها لا تُسمى معلومات إلا حين تتم مُعالجتها لتأخذ معنى، أي تصبح صورة يمكن رؤيتها أو نَص يمكن قراءتهُ أو ملف ما يمكن تشغيلهُ، وهذا المصطلح يتداخل مع مُصطلح الأمن السيبراني لكن المختصين في مجال الأمن وتقنية المعلومات أوضحوا إن المُصطلحين ليسا متطابقين، كُون الأمن السيبراني

---

* "الهجمات الصفرية" (Zero-Day Attack): وهي الثغرات الحديثة غير المكتشفة الموجودة في البرامج ونظم التشغيل مثل "ويندوز"، ويستغلها قراصنة المعلومات في إحكام السيطرة على الأجهزة، وزرع البرمجيات الخبيثة فيها، وتفعيلها لسرقة البيانات او تدميرها، للتفصيل ينظر: إيهاب خليفة، الهجمات الصفرية، كيف يمكن الاستعداد لليوم الأسود في الأنترنيت مركز المستقبل للأبحاث والدراسات المتقدمة،١٧ايار ٢٠١٧ متاح على الرابط: https://futureuae.com/ar/Mainpage/Item/2802/ تأريخ الزيارة ١شباط ٢٠٢١.

(١) نفس المصدر ، ص٨ .

(2) Committee on National Security Systems (CNSS) Glossary, CNSSI No. 4009 April 6, 2015,p.112.

يتجاوز حدُود الأمن المعلوماتي التقليدي –حماية مصادر المعلومات فقط – بل يتجاوزُها إلى حماية الاشخاص، في الأمن السيبراني هذا العامل له بُعد إضافي، وهو إن البشر كأهداف مُحتملة للهجمات السِيبرانية أو حتى المُشاركة عن غير قصد في هجُوم إلكتروني. هذا البُعد الإضافي له آثار أخلاقية على المُجتمّع ككُل، حيث يمكن اعتبار حماية بعَض الفئات الضعيفة، مثل الأطفال، مسؤولية مجتمعّية [١].ويعتبر جيش التحرير الشعبي الصيني أمن المعلومات بأنهُ: "حماية جميع المعلومات من التعطّيل والدّمار أو السرِقة حماية طبيعية ومعالجُتها ونقلها" [٢]. وأمن المعلومات يتَضمن أمن مُحتوى المعلومات، وأمن أنظمة المعلومات، أمن البنُية التحتية للمعلومات، أمن تبادُل المعلومات والوعي بأمن المعلومات.

بالتالي تَتلخص مُهمة هذا النوع من الأمن، إلى حماية الأنظمة الحاسُوبية من الوصول غير الشرعّي لها، أو العَبث بالمعلومات أثناء التخّزين أو المُعالجة أو النقل، أيضًا يهدُف إلى الحماية ضد تعطيل خدمة المُستخدمين الشرعيّين.

رابعاً: أمن الانترنيت: (Internet Security)

وهو المجال الذي يتضَمن إجراءات ومقاييس ومعايير الحماية المفروض أتخاذُها، او الالتزام بها لمُواجهة التهديدات ومنع التعدّيات او الحد من إثارها. ويرتبط أمن الشبكات والانترنيت ارتباطاً وثيقاً بأمن المعلومات، والوصُول إلى هذه الأخيرة او بثُها أو الاطلاع عليها والمتاجرة فيها أو تشويهّها، هو ما يقف عادةً وراء عمليات الاعتداء على الشبكات والانترنيت، وأمن الانترنيِت هو فرع من أمن الكمبيوتر، والغاية من أمن الانترنيت هو وضع قواعد وتدابّير لاستخدامها ضد الهجمات على الانترنيت [٣].

---

(١) فريدة طاجين، سياسات الدفاع الماليزية في ظل التهديدات الأمنية للبيئة الرقمية: الواقع والتحديات." الملتقى الدولي الثاني حول سياسات الدفاع، كلية الحقوق والعلوم السياسية: قسم العلوم السياسية، جامعة قاصدي مرباح، ورقلة،2017 ، ص343.

(2) Amy Chang, Warring State: China's Cybersecurity Strategy, Center for a New American Security ,Washington, December 2014, p.14.

(٣) منى الأشقر جبور، وعزيز ملحم بربر، أمن الشبكات والانترنيت، جامعة نايف العربية للعلوم الامنية، كلية التدريب قسم البرامج التدريبية، القاهرة، ٢٠٠٨،ص ص ١، ٩.

أنّ أمن الشبكات والانترنيت لا يُمكن تأمُينها بشكل كامل وتام، مالم يكُن للسُلطات المختصة إمكانات رصد وضبط ومُتابعة وملاحقة بشكل شامل، ولكُل أنواع العمليات في الوقت المناسب، فاختراق الأنظمة وسرِقة المعلومات ليس الهّم الوحيد، فهناك أيضا ضرورة لمنع استخدام الجريمة المنظمة لإمكانات تكنُولوجيا المعلومات والاتصالات، في تسهّيل أعمُالها ومنع ملاحقتها وتطوير اساليب وإمكانات عملُها، أن أمن الفضاء الالكتروني يتوقف بِشكل كبير على الحد من اسِتخدام تكنولوجيا المعلومات والاتصالات لأغراض جنائية، او لأغراض تتنافى والمصلحة العامة لمُختلف المعلومات [١].

خامساً: الأمن السحابي: (Cloud Security)

ويُعد الأمن السحابي تقنية إلكترونية تَعتمد على حفِظ المعلومات والملفات ضمن المنُظومة الخاصة بالحماية الالكترونية، وهو جُزء من الأمن السيبراني، أن زيادة الاعتماد على الخدمات السحابية يمكن أن يولد نقاط ضعف في أنظمة البُنية التحتية للدول، بسبب الهجمات المتكررة التي يشنها القراصنة في اليوم الواحد من أجل تدمير او سرقة المعلومات [٢]. والحوسبة السحابية تتمتع بسمات رئيسية هي [٣]:

أ- تعددية الوظائف (الموارد المشتركة): بخلاف نماذج الحوسبة السابقة (المخصصة لشخص واحد) تعتمد الحوسبة السحابية على نموذج عمل يتم فيه يتم تقاسم الموارد في الشبكة .

ب- قابلية التوسع الهائلة: إذ يوفر القدرة على القياس إلى عشرات آلاف الأنظمة.

ت- المرونة: يمكن للمستخدمين زيادة و تقليل موارد الحوسبة الخاصة بهم.

ث- الدفع حيث مكان البحث : يدفع المستخدمون فقط مقابل الموارد التي يستخدمونها بالفعل .

ج- التوفير الذاتي للموارد: مثل إضافية الأنظمة (القدرة على المعالجة والبرمجيات والتخزين) .

---

(١) المصدر نفسه ، ص ١٠ .

(٢) دلال العودة، الصراعات الدولية الحديثة، الطبعة الاولى، دار الطلائع للنشر والطباعة، القاهرة ٢٠١٥،ص٧٨ .

(3) Sean Carlin, Kevin Curran, University of Ulster, UK, Cloud Computing Security, International Journal of Ambient Computing and Intelligence, 3(1), 14-19, January-March 2011,p.14-15.

سادسا: أمن البيانات: (Data security)

وتَعني حماية البيانات من أي قوة مُدمرة، أو من أي فعل غير مرغوب بهِ من قبل مُستخدمين غير مخولين، وهو فرع من فرُوع الأمن السيبراني، ألا أنهُ يخص بعض جُوانب قطاعات الاقتصاد والمصارف العالمية، والتي تُعاني من هجمات افتراضية كبيرة بهَدف الحصول على معلومات، تخُص الحسابات المصرفية والمعلومات للمنظمات الدولية، وكذلك اختراق المضاربة في الاسواق المالية [١].

المطلب الثاني: الصراعات السيبرانية

في السابق كانت المُؤتمرات تُعقد من أجل تقليل خطر الحرب النووية، أما اليوم فقد أصبح عقد المؤتمرات وخاصةً بين كل من الولايات المُتحدة والصين، والتي تهدُف معظمها إلى تقليل مخاطر المواجهة والصراع في الفضاء الالكتروني، أو الشبكة العنكبوتية [٢]، فالعالم يشهد التحولات التاريخية التي تكون فيها التكنُولوجيا الهجُومية أرخص من الدِفاعية وأكثر قوةً. سنحاول في هذا المطلب بيان الموضوعات التي ترتبط بالصراع السيبراني، وهي الصراع السيبراني والحروب الافتراضية أضافة الى انواع الهجمات الكترونية.

اولا: الحروب السيبراني:

لقد مَرّت الحروب بين الدول بعِدة بمراحل – أُطلق عليها أجيال الحروب – تطور عبرها الحرب نتيجة المُعدات المستخدمة فيها والخُطط والنظريات من الحروب التقليدية وصولاً الى الحروب السيبرانية، ويمكن اجمال تلك المراحل بالاتي:

١-حُروب الجيل الأول:(Canvential war) يمكن اعتبار حروب الجِيل الأول شاملة للحُروب التي سبَقت عام ١٦٤٨م [٣].

---

(١) علي زياد العلي، الصراع والأمن الجيوسيبراني في السياسة الدولية "دراسة في استراتيجيات الاشتباك الرقمي "، دار امجد للنشر والتوزيع، عمان، ٢٠١٩ ، ص ص ٦٤، ٦٥.

(٢) جريدة العرب، مستقبل الفضاء السيبراني مجال الصراع بين الدول، ٨تشرين الاول ٢٠١٥. متاح على الرابط: https://alarab.co.uk تأريخ الزيارة ٥ كانون الثاني ٢٠٢١.

(٣) أيمل خوري، صراعات الجيل الخامس، ط١، شركة المطبوعات للتوزيع والنشر، بيروت، ٢٠١٦، ص٣٢.

٢- حُروب الجيل الثاني: (querilla war١٨٦٠-١٩١٨) شهِدت هذه المرحلة حرب العصابات او الحرب الثورية، والتي تكون بين جَيش نظامي تقليدي، وبين مَجموعات مقاتلة ذات هدف واحد صغيرة العَدد مُقارنة بالجيش النظامي [١].

٣ - حُروب الجيل الثالث:(preventive war)الحرب الوقائية والتي تُشكل الضربة الاستباقية فيها أساس مُهم في مواجهة الخطر قبل وقوعهِ [٢]، ويعتقد بعض المختصين إن فترة هذه الحرب هي (١٩٢٠-١٩٥٤).

٤ - حُروب الجيل الرابع: يُعتبر البعض أن حروب هذا الجيل، هي حرب المنظمات الارهابية حسب الوصف الأمريكي لها، ويُطلق عليه الحرب اللا متماثلة. ويُعتبر هذا النوع من الحروب "من أخطر أنواع الحرب؛ فهي تعتمد على التفرقة السياسية والفكِرية والايديولوجية، وتَستخدم الطائرات بدون طيار في المُراقبة والتجسس وتنفذ الأهداف بالأسلحة الذكية [٣]. مثال ذلك عمليات الاغتيال عن بُعد*.

٥- الجيّل الخامس: أو ما يُسمى الجيل الرابع المُتقدم والذي يستخدم العنف المسلح عبر مجموعات عقائدية مُسلحة أذ يستخدم من تم تجنيدهم "بالتكنولوجيا المتقدمة"**، والسُبل الحديثة لحشد الدعم المعنوي والشعبي. أن صِراعات الجيل الخامس لا تعكس فقط نشاط المتمردين؛ بل تَفتح الباب على مصراعيهِ للدول التي تُنافس الولايات المتحدة الأمريكية كقُوة مُهيمنة، فهي تتأثر

---

(١) علي زياد العلي ، مصدر سبق ذكره ، ص٦٩

(٢) جليل خلف شويل، صراعات الجيل الرابع المستقبل للشعوب وليس للحكام، جريدة البينة الجديدة، في ٨ ايلول ٢٠٢٠. متاح على الموقع: https://albayyna-new.net/content.php?id=21358 تأريخ الزيارة ٦ كانون الثاني ٢٠٢١

(٣) ستيفان هالبر وجوناثان كلارك، التفرد الأمريكي المحافظون الجدد والنظام العالمي، ترجمة عمر الايوبي، دار الكتاب العربي، بيروت ٢٠٠٥، ص٢٦٠.

* مثل العملية التي قامت بها الولايات المتحدة في العراق عام ٢٠٢٠ باغتيال قائد الحرس الثوري الايراني قاسم سليماني والقيادي في الحشد الشعبي ابو مهدي المهندس. وهذه العمليات تعزز الرؤية التي ترجح بأن تطور الفضاء الالكتروني يشكل عامل اختراق للسيادة الوطنية وزعزعة الاستقرار.

** يقصد بالتكنولوجيا المتقدمة الأسلحة المتطورة التي تستخدمها العصابات المنظمة مثل الصواريخ المضادة للدروع والطائرات بدون طيار والعمليات الانتحارية ومهاجمة المدنيين (حيث استخدمت في مصر والعراق واليمن وأفغانستان منذ سنة ١٩٩١) للتفصيل ينظر: سيد عبد النبي محمد، صراع الأمم وحروب الجيل الخامس، وكالة الصحافة العربية ناشرون، الجيزة، ٢٠١٩، ص٦.

بالعوامل السياسية والاقتصادية والعامل الاجتماعي حيث العلاقات مع الدول وارتباط الاقتصاد بالجيش من حيث الانفاق أما اجتماعيا، فقد ساهم الانفتاح وانتشار التواصل مع الاخرين على التأثر في حركات التمرد المسلحة [١] .

٦- حُروب الجيل السادس والسَابع: أصبح الخبراء والاستراتيجيون يتَحدثون اليوم عن الجيل السادس من الحُروب وهي الأخطر على البشرية، خاصةً أن العالم أصبح شُبه مفتوح على بعضهِ أنها حرب الفايُروسات والأمراض المُعدية والخطرة [٢]. والجيّل السابع من الحرب يشبهَ الجيل السادِس من حيث الأهداف والتقنيات حيث يُحاول كُل طرف أنهاء الطرف الأخر من خِلال استخدام الأسلحة الذكية وَشبكات الانترنيت لأغراض التجسُس [٣].

٧- الحُروب الافتراضية.

يُعد مصطلح (الحرب الافتراضية) او(الحرب التخيُلية) (Virtual war) واحداً من المصطلحات المُتفرعة من مصطلح (الواقع التخيلي) أو (الافتراضي"، ويقصد به البيئة الاصطناعية التي تنشأ عبر الكومبُيوتر وأجهزة تكنُولوجيا المعلومات الأخرى وأدواتها" [٤]، بمعنى الحرب غير تقليدية مجالها الفضاء الإلكتروني .

إنِّ حُروب المُستقبل يجب أن تُواكب التحولات الاجتماعية العميقة في بُنى المجتمعات، وعليه فإن إدارتُها الرئيسية ستكون مُتمثلة بالقوة الناعمة (المعلومات) و "القوة الصلبة" التقليدية أصبحا متشابكين بشكل متزايد، عبر العديد من المجالات السياسية والاقتصادية والعسكرية، بحيث تكون للقوة الناعمة (المعلوماتية) الأسبقية على القوة التقليدية المادية، وظهر مجال جديد معروف

---

(١) محمد عبد ربه المغير، تحصين الجبهة الداخلية من حروب الجيل الخامس، مجلة الدراسات الاستراتيجية والعسكرية – المركز الديمقراطي العربي، المجلد الاول، العدد الثاني، كانون الاول ٢٠١٨، ص٥٠-٥١.

(٢) بدرة قعلول، الجيل السادس للحروب – حرب الفيروسات، المركز الدولي للدراسات الاستراتيجية الأمنية والعسكرية، الجزائر، ٢٠٢٠.متاح على الموقع: https://strategianews.net/ تأريخ الزيارة ٧ كانون الثاني ٢٠٢١.

(٣) عادل عبد الجواد محمد، دور مراكز المعلومات في التعامل مع الازمات، مجلة الأمن والحياة، العدد ٣٥٨، الرياض، ٢٠١٦، ص٤٣.

(٤) يونس مؤيد يونس مصطفى، استراتيجية الولايات المتحدة الأمريكية للأمن السيبراني، مجلة قضايا سياسية كلية العلوم السياسية جامعة النهرين، العدد ٥٥، ٢٠١٨، ص ١٢٣.

باسم "استراتيجية المعلومات" وأصبح هناك قطبين يحددان الاهتمامات الأمنية، أحدهما هو في الأساس قطب تكنولوجي ، وهو الفضاء السيبراني والقطب الأخر هو في الأساس سياسي وفكري يمثل القوة الناعمة [١].

والفرق بينَ الحرب السيبرانية والحرب التقليدية: إنَّ الحروب التقلّيدية وخاصةً العسكرية تُعد حكراً على الدولة والجماعات المُسلحة، حيث تدور الحرب التقليدية في مَساحات جُغرافية مُحددة وزمن مُحدد وهي محددة الأهداف والأطراف، بينما الحرب السيبرانية لا تقتصر على الفاعليّن من الدول فقط، وثمةَ فارق بين الصراعات السيبرانية والهَجمات المادية أو الهجمات غِير المُبرمجة (Non Software – based Attacks) وتَشمل الهجمات المادية والمغناطّيسية ضد الشبكات الالكترونية عبر أسلحة تقليدية (صواريخ وقنابل) وهي بذلك لا تُعد هجمات إلكترونية، والفَرق الأخر إن الصراعات التقليدية تُفرق بين مستويّي الجرائم والحروب، فَالجريمة مُشكلة قانونية تُعالج وفق القانون بينما الحرب تَتعلق بالعسكريّين وبالأسلحة، أما في مجال الصراعات السيبرانية فأن الجرائَم والحُروب الالكترونية تنفذ بنفس الأدوات والبنى التحتية التقنية، ويمكن أن يُسهم فيها فاعلون من غير الدول، ولا يُوجد حدُود فاصلة بين جرائم الانترنيت والحرب الإلكترونية، وذلك إن كليهُما يأتي ضمن الصراع الإلكتروني [٢]. وتكمن خُطورة الصراعات السيبرانية بأنها واطئة الكُلفة بالنسبةِ للمُهاجم وقد يقوم بها فرد، مِثال على ذلك " في تشرين الاول ٢٠١٥ خدع مُخترق مراهق خدمة عُملاء (Verizon و AOL) للوصول إلى حساب بريد إلكتروني خاص لمُدير وكالة المُخابرات المركزية جون برينان" [٣].

---

(1) John Arquilla, David F Ronfeldt,The emergence of Noopoli-tik Toward of Americam Strateay, Rand Monograph Report Rand, Sanga Monica,California, 1999, pp.ix,x.

(٢) نوران شفيق علي، الفضاء الالكتروني وانماط التفاعلات الدولية: دراسة في أبعاد الامن الإلكتروني، رسالة ماجستير، جامعة القاهرة، كلية الاقتصاد والعلوم السياسية، ٢٠١٤، ص٥٩.

(3) Center of Strategic and International Studies, Significant Cyber Incidents Since 2006, Washington,p.30.

ثانياً: الهُجوم السيبراني. (Cyber attack)

الهجوم السيبراني (الإلكتروني) هو "اختراق الشبكات لحقن الحاسِبات بكم هائل من البيانات لتعطّيلها أو ارباك مُستخدميها، ونشر الفايروسات (Viruses)"، كما يشمل الهُجوم الإلكتروني قطع خدمة الانترنيت (Denial Of Service Attacks) عَن الخصم وتدمّير البيانات، فضلا عن ذلك مُهاجمة الشبكات ويمكن التميّيز بين الدفاع عن الشبكات (Defending networks) واستطلاع الشبكات (Network Exploition) وتَشمل الأولى حماية الشبكات وأجهزة الكومبُيوتر من أي اختراق خارجي، إما الاستطلاع فيعني القُدرة على الدخول غير المشُروع والتجسس على شبكات الخَصم، دون أن يُصاحب ذلك تدمّير او تَخريب البيانات [١].

ويمكن اعتبار الحرب بين استونيا ورُوسيا عام ٢٠٠٧، وحرب روسيا على جورجيا عام ٢٠٠٨، هي حروب استُخدمت فيها الادوات السيبرانية وهي امتّداد للحرب التقليدية [٢].

١- أنواع الهجمات السيبرانية

تختلف الهجمات الإلكترونية وتتعدد انواعها ومنفذيها والهدف منها ، كذلك من حيث خطورة المعلومات التي تسعى لها الجهة المنفذة ، لذا لابد من التمييز بين نوعين من الهجمات السيبرانية:

أ - **هجمات سيبرانية ذات طبيعة عَسكرية:** وهي هجمات لها نفس التداعيّات الناجمة عن الاستَخدام المادي للقُوة العسكرية، والتي تتمثل في أتساع نِطاق التدمير، ووقُوع وفيات بين العسكريّين والمدنيين، وانهيار البُنية التحتية للدولة، ومنها:

- استهداف البُنية التحتية للدولة: وتشمل جميع المؤسسات المُهمة في الدولة.

- سرقة المعلومات والبيانات العسكرية أو التلاعُب بها.

---

(١) إيهاب خليفة، القوة الالكترونية: كيف يُمكن أن تُدير الدول شؤونها في عصر الانترنيت، ط ١، العربي للنشر والتوزيع، القاهرة، ٢٠١٧، ص،ص٨٧ -٨٨.

(٢) عبد الغفار عفيفي الدويك، استراتيجية الردع السيبراني.. التجربة الأمريكية، مجلة السياسة الدولية، المجلد ٥٣، العدد ٢١٣، مؤسسة الأهرام، القاهرة، حزيران ٢٠١٨، ص ١٩٦.

– السيطرة على الأنظَمة العسكرية: ويُقصد بها السيطرة على نُظم القيادة والسيطرة عن بُعد بما يُخرج الأسلِحة والوحدات والكتائب العسكرية عن القِيادة المركزية [١].

ب– الهَجمات السيبرانية غِير العسكرية:

حيث يُمكن أن تكون آثارها ذات طبيعة اقتصادِية أو اجتماعية، على الدولة التي تَتعرض للهُجوم، وتُعتبر الهجمات محظُورة إذا استهدفت المدنيّين أو كانَت عشوائية حسب ما جاء (بدليل تالين)* القسم الثالث القاعدة (٣٢) [٢]، وتشمل عدة انواع أهُمها:

– الدعاية الاعَلامية (الحرب النفسية السيبرانية) [٣].

– الإرهاب السِيبراني: ظهر الإرهاب السيّبراني؛ نتيجة لِاستخدام تكنُولوجيا المعلومات والاتصالات للقيّام بأعمال إرهابية، حيث عرفهُ (James Andrew Lewis) بأنه "استخدام أدوات شبكة الكمبُيوتر لإغلاق البُنى التحتّية الوطنية الحيوية (مثل الطّاقة والنقل والعمليات الحكومية) أو لإكراه أو تخوِيف الحكومة أو السُكان المدنيين" [٤].

– تأليب الرأيَ العام ضد الحُكومة وتشويه الرموز السياسية ونشر الفَكر المتطّرف وتجنّيد الأفراد من قِبل المنُظمات والجماعات المتطرفة [٥]

---

(١) إيهاب خليفة، ما هو موقف ميثاق الأُمم المتحدة من استخدام القوة السيبرانية في التفاعلات الدولية؟، مركز المستقبل للأبحاث والدراسات المتقدمة، ٢٤/تشرين الاول ٢٠١٩. متاح على الموقع: https://futureuae.com/ar/Mainpage/Item/ تأريخ الزيارة ٧ كانون الثاني ٢٠٢١.

* دليل تالين للقانون الدولي المنطبق على الحرب الإلكترونية.، قام بإعداده مجموعة من أبرز فقهاء القانون الدولي، نشر الإصدار الأول منه عام ٢٠١٣، ويحتوى على ٩٥ قاعدة قانونية إرشادية لعمل أو سلوك الدول في سياق الحرب الإلكترونية. وصدر الإصدار الثاني منه في العام ٢٠١٧، ويحتوى على ١٥٤ قاعدة، ليشكل مستوى أكثر اتساعاً لمعالجة العمليات الإلكترونية. للتفصيل ينظر: دليل تالين بشأن القانون الدولي المطبق على الحروب السيبرانية ، ترجمة علي كاظم الموسوي٢٠١٧ ،شركة المؤسسة الحديثة للكتاب٢٠١٩.

(٢) المصدر نفسه ، ص٧.

(٣) علم الدين بانقا، مخاطر الهجمات الالكترونية (السيبرانية) واثارها الاقتصادية –دراسة حالة دول مجلس التعاون الخليجي، سلسلة دراسات تنموية، المعهد العربي للتخطيط، العدد ٦٣، الكويت، نيسان ٢١٠٩، ص٤٨.

(٤) رسالة من السيد جيمس لويس، ويمكن الاطلاع على نص الرسالة الملحق رقم (١).

(٥) إيهاب خليفة، ما هو موقف ميثاق الأُمم المتحدة من استخدام القوة السيبرانية في التفاعلات الدولية، مصدر سبق ذكره، ص٢.

ويُمكن اعتبار الولايات المُتحدة الامريكية أكثر الدول عُرضة للهجمات السيبرانية والتي تشكل ٣٥% من مجموع الهجمات حول العالم موجهَة ضدها حسب احصائية لعام ٢٠١٧ وذلك نتيجة الأستخدام الواسع للرقمنة في كافة المؤسسات والبنى التحتية فيها [١].

٢- مصدر الهَجمات السيبرانية

قد يُكون مطلقو الهجمات السيبرانية من داخل اقليم الدولة المستَهدفة، او من خارج حدُودها السياسية. حيث تَخضع الجهة المنفذة للهُجوم للقانون الوطني في الحالة الأولى، واذا كان المنُفِذ من خارج حدُود الدولة فيخضع للقانون الدولي، ولكن في حالة أن مصدر تلك الهجمات هو جهة رَسمية تابعة لدولة اخُرى وتقع في نفس اقليم تلك الدولة، مثل السفارات فيكُون الحكم ان مصدر تلك الهجمات هو اقلّيم تلك الدولة التي تمثلها السَفارة، حيث يَنص القانون الدولي إن السفارات والبِعثات الدبلوماسية تتمتع بحصانات خاصة وتُعامل كما لو كانت على اقليم دولتَها المُبعوثة منها [٢].

ولكن عندما تكُون الدولة عاجِزة عن ردع الجماعات والأفراد الذين يطلقون الهجمات من داخل اراضّيها، باتجاه دولة اخرى يكون لِلدولة حق الدفاع عن نفِسها ، وقدر تعلق الامر بالهجمات السيِبرانية فقد أجاز الخبراء المشاركين في اعداد (دليل تالين للحرب الالكترونية) للدولة حق الدفاع الشَرعي ضد الهجمات الالكترونية التي تنطلق من دولة اخرى غير قادرة على منع تلك الهجمات [٣].

وقَد يكون مصدر الهجَمات رُوبوتات تستأجُرها العديد من منظمات الجريّمة الإلكترونية، بشكل مَنفصل مثل شبكة (EMOTET)*، التي تُديرها عصبات الجريمة الالكترونية [١].

---

(١) فريدة طاجين، تأثير القوة السيبرانية على الاستراتيجيات الأمنية للدول الكبرى ، مصدر سبق ذكره ،ص٣٣.

(٢) للتفصيل ينظر : اتفاقية فيينا للعلاقات الدبلوماسية ١٩٦١ .

(3) Dinstein, Computer, Network Attacks and Self-Defence, 2002, p.108.Available at Link:https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1397&context=ils. the visit at 9 January.

* وهي عبارة عن روبوتات غالبًا ما تستأجرها العديد من منظمات الجريمة الإلكترونية، وتستخدم في عمليات الفدية او التجسس. للتفصيل ينظر: الملحق رقم (٢)(Global Cyber News – February 2021).

المطلب الثالث: الردع والدفاع السيبراني

للوصول إلى استراتيجية شاملة للردع السيبراني لا بد من مراعاة مجموعة من الخطوات على المستويين المحلي والدولي، عبر من خِلال دخول الدول في حوار استراتيجي ما بين الدول وشركائهم لضمان استعدادهم للحُروب السيبرانية، والتعاون الدولي من خلال خلق بيئة قانونية وتشريعية مناسبة لمواجهة الحروب السيبرانية، للحد من شن مزيد من الهجمات السيبرانية، كما يجب تحديد قواعد عالمية مقبولة وواضحة لتحقيق الأهداف في الفضاء الالكتروني، عن طريق الدفاع والردع السيبِراني.

أولاً: مفهُوم الردع السيبراني

يُعّرف الردع السيبراني بأنه "منع الاعمال الضارة ضد الأصُول الوطنية في الفضاء الإلكتروني والأصول التي تدعم العمليات الإلكترونية" [٢]. والهدف من الردع هو خلق مثبطات لبدء أو تنفيذ المزيد من الأعمال العدائية، و بمعاقبة السلوك السيئ ولكنه يُعد ضمنيًا بحجب العقوبة إذا لم تحدث أفعال سيئة ويتطلب القدرة على التمييز بين السلوك الجيد والسيئ. الإيجابيات الكاذبة والسلبيات الكاذبة على حد سواء [٣]."خلق مجموعة من المحفزات المانعة لقيام احد اطراف الصراع باعتداء أو هُجوم مستقبلا" وغيرها، ويقُوم الردع السيبراني على ثلاثة أُسس تُعتبر ركائز استراتيجية الردع السيبراني وتشمل: [٤]

أ-مصداقية الدفاع، ب- القُدرة على الانتقام، ج- الرغبة في الانتقام.

ويَتطلب الردع لحماية أنظمة المعلومات وردع المحاولات لاختراقِها، توافر أنظمة نسخ احتياطية لتلافي فقدان المعلومات في حالة أي هُجوم الِكتروني على أنظمة وبيانات المعلومات

---

(١) رسالة عبر البريد الالكتروني للباحث من مؤسسة كارنيغي للسلام الدولي (Carnegie Cyber Policy Initiative)من فريق المؤسسة تيم مورير وإيفان بيرك وفريق مبادرة السياسة الإلكترونية: cyberpolicy@ceip.org توجد نسخه من الرسالة في الملحق رقم (٢).

(٢) رغدة البهي، مصدر سبق ذكره، ص ٥٢ .

(3) Martin C. Libicki, Cyberdeterrence and Cyberwar,Santa Monica,Rand, 2009, p. 28.

(٤) رغدة البهي، مصدر سبق ذكره، ص٤٨.

المحفُوظة في الحواسِيب، وهذه الحالة يُعبر عنها بمصداقية الدفاع وتُعد الحل العملي الأكثر فاعلية.

أما الأساس الثاني: هو القُدرة على الانتقام، لابد أن يتوقع المهاجم أنه سوف يتكبد خسائر تفُوق ما يَتعرض لهُ المُدافع من اضرار، وهذا يتطلب القُدرة على الانتقام والقيام بَهجمات سيبرانية ضد المُهاجم بعد التعرف عليه وهذا صعب التحقق.

أما ما يتعلق بالرغبة في الانتقام، وعندما يتعرض المدافع لهُجوم سيبراني يجب أن يُعلن عن رغبتهِ في الانتقام من المُهاجم، أذ ان امتلاك القُدرة على الانتقام لا تكفي بدُون وجود رَغبة لتنفيذ الانتقام لردع المُهاجم، كما أنه ليس من السُهولة تحقيق الردع الالكتروني بسبب خاصية التخفي التي تعيق امكانية التعرف على مصدر الهجُوم، وهنا قد يتساءل البعض حول امكانية أن تقوم الهجمات الالكترونية بتهديد السلم والأمن العالميين؟. في ظل نظام دولي مُتعدد القطبية وتعدد الفاعلين من الدول وغير الدول الذين يَستخدمون القوة الالكترونية في التفاعلات الدولية وخاصّية التخفّي لمنفذيّ الهُجوم الإلكتروني فاحتمالات الصراع تتزايد [١].

ورغم تشابهُ أركان نظرية الردع التقليدي – المصداقية والقُدرة والرغبة في تنفيذ العقُوبة مع نظرية الردع السيبراني، الا أنهُ من الصعوبة منع الهجمات السيبرانية بشكل تام بسبب الطبيعة الخاصة بالفضاء الإلكتروني والثغرات التي توجد فيه والفيروسات والأسِلحة السيِبرانية التي يتم تطويرها باستمرار. فالردع بالطُرق التقليدية لا يتحقق غالبا في الفضاء الالكتروني، مما دَفع البعض الى أعادة تعريف الردع بما يتناسب مع الطبيعة السيبرانية للعلاقات الدولية [٢].

ثانياً: الدِفاع السيبراني:

يُقصد بالدفاع السيبراني من الناحية الفنية هو: حماية الشبكات وأجهزة الكمبيوتر من أي عملية اختراق خارجي، فيَجب أن يكون التأمّين على مُستوى البرمجيات(Software) والمُكون المادي للشبكات (Hardware)، وذلك للحفاظ على الشبكة من اي هجوم او اختراق خارجي

(١) إيهاب خليفة، القوة الالكترونية، مصدر سبق ذكره، ص١٠٠.

(٢) إيهاب خليفة، الأمن السيبراني الماهية والاشكاليات، مصدر سبق ذكره ، ص ٥.

"بالأسلحة الالكترونية"*، وكذلك تأمين المكون المادي للشبكات من قبل مصممي انظمة الحماية للعمل في ظروف غير عادية. و"يشير الجيش الأمريكي إلى تطبيقات القوة السيبرانية على أنها عمليات شبكة كمبيوتر(CNO)وتقسمها إلى ثلاث فئات: الدفاع عن شبكة الكمبيوتر (CND) ، هجوم على شبكة الكمبيوتر(CNA)، واستغلال شبكة الكمبيوتر (CNE)، يركز CND بشكل عام على الوقاية من اي تسلل أو هجوم خارجي" [١] بمعنى الدفاع عن المؤسسات الحيوية وأنشاء أنظمة حماية سيبرانية للحيلولة دون اختراقها من قبل الجهات المعادية، و ةهجاوم عمليات التسلل الخبيثة .ولا يمكن تحقيق الأمن عن طريق استخدام مهندسي برمجيات بارعين يصممون شبكات منيعة عمليا فقط، بل يتطلب الأمر تضافر جهود قادة السياسة ومبتكري الصناعة والباحثين 28الأكاديميين، والحرفيين والمسؤولين العسكريين والموظفين العاديين من كل دوائر الحكومة والأعمال التجارية للدفاع ضد التهديدات المتقدمة والمستمرة من قبل القراصنة والجهات الحكومية

وأهم وسيلة لنجاح الدفاع في مجال الفضاء الالكتروني هو التعاون بين الدول وتبادل المعلومات والخبرات التقنية ولهذا السبب اعتُبر المؤتمر السنوي التاسع للأمن السيبراني للمنطقة الوسطى– الذي استضافته القيادة المركزية الأمريكية – منبراً بالغ الأهمية للمساعدة في بناء العلاقات وتبادل المعلومات بين أصحاب المصلحة .وفي هذا الصدد صرّح الفريق (Thomas W Bergeson) 2020، نائب قائد القيادة المركزية الأمريكية، قائلاً "لا يمكن لأي منا أن يواجه تحديات الأمن السيبراني بمفرده" [٢]، وهذه إشاره الى ضرورة التعاون والعمل الجماعي لضمان

ثالثا: مشروعية الدفاع ضد الهجمات السيبرانية.

---

* وهي عبارة عن برامج يتم تصميمها مثل "فايروسات الحاسوب، الديدان، أحصنة طروادة (برامج صغيرة داخل برامج كبيرة، وسيتم التطرق لها بالتفصيل في الفصل الثالث المبحث الثاني من الرسالة.

(1) Colonel Jayson M. Spade, Chinas Cyber Power and Americas National Security, Jeffrey L. Caton Editor, U.S Army War College, M ay 2012, p.7,8,9.

(٢) مجلة يونيبات، المؤتمر السنوي التاسع للأمن السيبراني للمنطقة الوسطى نيسان ٢٠١٩، الدفاع السيبراني https://unipatmagazine.com/ar / تأريخ الزيارة ١١شباط ٢٠٢١.

للرد على الهجمات السيبرانية لابد من وجود مبررات وحجج كما هو الحال مع الرد على الهجمات التقليدية، والتي يمكن اجمالها بالآتي:

١- حق الدفاع ضد الهُجوم الإلكتروني حسب الأداة والأثر والمسؤولية.

كل دولة تَتعرض الى هجوم سيكون لها رد فعل او دفاع عن النفس وقد نَصت على ذلك المادة (٥١)* من ميثاق الامم المتحدة، التي بيّنت حق الدول في الدفاع عن نفسِها في حالة تعرضُها لهجوم مُسلح وقع فعلاً، وعند تطبيق هذه الشُروط على حالة الدفاع ضد الهُجوم الالكتروني يجب تقدير الهجوم السيبراني كونهُ اعتداء مسلح ام لا، وحسب قرار الجمعية العامة الخاص بتعرّيف العُدوان الذي ينص على " اعتماد القُوة المسلحة من قبل دولة ما ضد سيادة دولة اخرى او سلامتُها الاقليمية او استقلالها السياسي، او بأي صورة اخرى تنافي ميثاق الامم المتحدة.." [١]، وحيث ذكر التعريف استخدام القُوة المسلحة، فهل الهجوم السيبراني ينطوي على استخدام القوة المسلحة؟ توجد ثلاثة مذاهبّ بهذا الخُصوص [٢].

المذهب الاول: بحسب الاَداة المُستخدمة، مثلاً اذا حصل هجوم اِلكتروني على مولدات الطاقة لدولة ما وادى إلى تدميرها، فبِحسب هذا المذهب يتم النظر الى مدى امكانية تدمّير هذه المولدات في السياق عن طريق تفجيرها بأسلحة يدوية مثلاً، أما المذهب الثاني: يكون على اساس الأثر الذي يُخلفهُ الهجوم، اي يُصنف كهجوم مسلح عن طريق قياس الأثر جراء الهُجوم السيبراني بحيث أن الاثار المترتبة على هذا الهجوم لا يمكن ترتيبها الا عن طريق استخدام القوة المادية (الحركية) كالتلاعُب بالأنظمة المالية والبنكية لدولة ما، ويتحدد المذهب الثالث: على اساس المسؤولية المُطلقة وحسب هذا المذهب يُعتبر اي هجوم على البنية التحتية لدولة ما – وخاصة المرتبطة بالصحة والأمن – من قبيل هجوم مسلح [٣].

---

* تنص المادة ٥١ من ميثاق الأمم المتحدة على أنه "ليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول، فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء (الأمم المتحدة) وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي". للتفصيل ينظر: ميثاق الامم المتحدة.

(١) الفصل السابع من ميثاق الامم المتحدة.

(٢) يحيى مفرح الزهراني، الابعاد الاستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، جامعة الوادي ،الجزائر العدد ٢٣، السنة ١٤، شتاء ٢٠١٧،ص ص ٢٣٧.

(٣) المصدر نفسه، ٢٣٨.

ويعتبر المذهب الثالث هو الأكثر منطقية وسهولة في القياس، والاستنتاج المهم هو مدى قدرة الدولة على استخدام القوة بشكل مشروع، رداً على هجوم إلكتروني ومسؤولية الدولة المُعتدية [١]. ويُعد ابلاغ مجلس الأمن فورا عن الهجوم، من ضمن الشروط التي تَمنح حق الرد ليتَمكن من أتخاذ التدابير اللازمة للمحافظة على السلم والأمن الدوليين. بالاستناد أيضا إلى حُكم محكمة العدل الدولية عام ٢٠٠٥ في القضية بين الكونغو وأوغندا*.

٢- ضوابط مشُروعية حق الدفاع.

من الضوابط المهمة لمنح حق الدفاع هو (التناسُب) [٢]، بين الهجوم وطريقة الرد عليه، ومن الصعُوبة تحقيق ذلك عند الرد على الهجمات الإلكترونية بسبب اتساع الفضاء الإلكتروني، كما حصل عندما استَهدفت الولايات المُتحدة البرنامج النووي الإيراني بفِايروس (Stuxnet)حيث امتدَ اثرهُ الى دول اخرى، كما تُعتبر الهجمات السيبرانية العشوائية محظُورة وهذا ما نصت عليه القاعدة (٤٩) في (دليل تالين) [٣].

وقد تبّنت الولايات المتحدة ما يُسمى بحق الدفاع الاستباقي كحق مشروع للدفاع بعد أحداث ١١ ايلول عام ٢٠٠١ وقامت باتخاذ اجراءات احترازية ضد أي خطر حتى قبل وقوعهِ، بمعنى اتخاذ كافة التدابير الضرورية لمواجهة اي عمليات اولية لم يتم اكتمالها بعد ولا تُشكل خطراً في وضعها الحالي، ولكنها سُوف تُشكل خطراً في حالة لاحقة عند الانتهاء من تجهيزها . كما اعترفت إيران وكوريا الشمالية بهذا النوع من الدفاعات، وإذا طُبق حق الدفاع الأستباقي على الهجمات السيبرانية، لنّ يكون هناك سَند قانوني دولي يَسمح بالهجمات الدفاعية ضد اي أعمال بدائية لم تُكتمل بعد.

---

(1) David E. Graham."Cyber Threats and the Law of War "JOURNAL OF NATIONAL SECURITY LAW,POLICY, Vol, 4:87, 13 Aug 2010, p. 91-92.

* فقد قضت المحكمة الدولية إن عدم ابلاغ اوغندا لمجلس الأمن بالهجمات وبعملية الدفاع التي قامت بها، يعد دفاعا غير قانوني ويعد انتهاك لمبدأ حظر استعمال القوة. للتفاصيل ينظر: تقرير محكمة العدل الدولية في ١ آب/ ٢٠٠٤ – ٣١ تموز ٢٠٠٥ الدورة (٦٠) الملحق رقم 4 (A/60/4) الأنشطة المسلحة في أراضي الكونغو (جمهورية الكونغو الديمقراطية ضد أوغندا) ص٤٠-٤٧.

(٢) الدين جيلاني ابو زيد وماجد الحموي، الوسيط في القانون الدولي العام، دار الشواف، الرياض،٢٠٠٣، ص ص ١٤٤، ١٤٨.

(٢) دليل تالين ، مصدر سبق ذكره، ص١١.

بناء على ما تقدم تبين أن مفهوم الأمن السيبراني يتداخل مع مفاهيم اخرى، هي الحُروب السيبرانية والهجُوم السيبراني، وكذلك يتَميز هذا المفهوم بالتطور والتغّير المُستمر ؛ كُونه يتأثر بالتكنولوجيا وتقنية المعلومات التي تشهد تسارع مستمر في تطّورها، أضافة إلى أنه يتجاوز حدود الدولة التقليدية ويكون في فضاء مفتوح وغير مُسيطر عليهِ من قِبل الدولة او النظام الدولي، ويُشكل خطورة كبيرة على الأمن القومي للدول، وذلك لصعُوبة معرفة مصدر الهجمات من جهة، وامكانية شن مثل هذهِ الهجمات من قبل الفاعلّين من غير الدول وحتى الأفراد؛ بسبب قلة تكلُفة الهجمات مقابل الآثار المدمرة التي تُسبُبها، وعدم وجود تكييف قانوني دولي متفق عليه للحَد من هذه الهجمات، مما يستوجِب التعاون وتبادل المعلومات بين الدول لتحقيق أكبر قدر من الأمن.

المبحث الثاني: الفضاء الالكتروني والعلاقات الدولية

أصبح الفضاء الالكتروني أحد مجالات العلاقات الدولية ولهُ تأثير كبير على تشكيل هذهِ العلاقات وتفاعُلاتها، عِبر أدوات تكنولوجيا المعلومات والاتصالات المُتطورة، واصبح لها تأثير في محتويات السياق الدولي وخصائص وأطراف العلاقات الدولية، وهو ماُ يسمى بصُعود السياسة السيبِرانية (Cyber politics) في العلاقات الدولية، حيث كانَ للتحولات التي حدثتّ في بداية القرن الحادي والعشرين انعكاسٍ على نظرية العلاقات الدولية والاطر النظرية المُفسرة لها. إذ اغفلت المناهج التقليدية في دراسة العلاقات الدولية، دَور التكنُولوجيا وتطور الاتصالات وركزّت سابقاً على فهم التكنُولوجيا كأحد هياكل القوة الحتمي، والذي يؤدي الى تجاهل دور سياسة التنمية التكنُولوجية، أما الآن ومن أجل فهم السياسة العالمية، بدأ التركيز على تحليل وفِهم الثورة المعلوماتية. ويتضمن هذا المبحث ثلاثة مطالب.

المطلب الأول: الفضاء الالكتروني

لقد أصبح الفضاء الإلكتروني –الذي يُعتبر على غرار مفاهيم القرن التاسع عشر–، فضاء واسع يُمارس فيهِ الجميع نشاطهُ الفكري ويّعبر عن أفكارهِ، ويناقش اهتماماتهِ مع الجميع عبر هذا الفضاء الواسع، الذي يشمل كُل الاطياف دون قيّود تُحدد ذلك النشاط، وفي هذا المطلب ستُبين الدراسة تعريف والانترنت أضافة إلى توضيح خصائص الفضاء الالكتروني.

أولاً : أهمية الفضاء الإلكتروني

اعتبر جوزيف ناي " إن الفضاء الإلكتروني يوضح نقطة مفادها، إن انتشار القوة لا يعني المساواة في السلطة أو استبدال الحكومات باعتبارها أقوى الجهات الفاعلة في السياسة العالمية، و قد يخلق بعض تحولات القوة بين الدول من خلال فتح فرص محدودة للقفز من قبل الدول الصغيرة التي تستخدم حرب غير متكافئة ، فمن المرجح أن يزيد المجال السيبراني من انتشار القوة إلى الجهات الفاعلة غير الحكومية ، ويوضح أهمية الشبكات كأحد الأبعاد الرئيسية للسلطة في القرن الحادي والعشرين" [1]، ويُعبر عن صورة لشبكة عالمية تربط بين الادمغة الفردية على المُستوى العالمي والتي تشكل ما يسمى (cerveau planetaire) كما يدعوهُ (de Rosnay

(1) Joseph S. Nye, Jr., Cyber power, op. cit,p.19.

Joel)، (دماغ هجين) – بيولوجي وإلكتروني–"، انهُ فضاء للشبكات الآلية والعضوية المترابطة فيما بينها بشكل لا متناهي [١].

اذاً الفضاء الإلكتروني هو بمثابة المستودع الذي تجتّمع بهِ كُل أنظمة الحاسوب، وتجري فيه كافة عمليات التواصل الإلكتروني التي تحدُث بصورة مستمرة، داخل الفضاء الإلكتروني حيث تجتمع فيه عناصر متعددة، فهذه المساحة تشمل مجموعة البيانات والمعلومات الخاصة بكل شبكة من شبكات الحاسوب، كما يحتوي هذا الفضاء كذلك على أجهزة الحاسوب والأنظمة البرمجية المعقدة، بالإضافة إلى المستخدمين.

إضافة الى ذلك هناك كلمة أخرى تُشير إلى الفضاء الالكتروني، وهي العالم الافتراضي (VIRTUALWORLD) والذي يُشير إلى التمثيل الرمزيّ والمجازي للمعلومات كما تنتقل فيهِ البيانات الالكترونية، ونظراً لارتباط المُجتمعات العالمية فيما بينها بنُظم معلومات تقنية، عن طريق الاقمار الصناعية وشبكات الاتصال الدولية فقد زادت الخطورة الإجرامية للجماعات والمنظمات الارهابية، و قامت بتوظيّف طاقتها للاستفادة من تلك التقنية، واستغلالها في عملياتها الاجرامية واعمالها غير المشروعة [٢].

ثانياً: الانترنيت

أصبح من الضروري أنَّ يتم التمّييز بين الانترنيت والفضاء الالكتروني، الإنترنت هو نظام اتصال عالميّ لنقل البيانات عبر أنواع مختلفة من الوسائط، ويُمكن وصفهُ بأنه شبكة عالميّة تربَط شبكات مختلفة سواء كانت شبكات خاصّة أو عامّة، تجاريّة، أو أكاديميّة، بواسطة تقنيّات لاسلكية أو ألياف ضوئية [٣]. لكن الفضاء الإلكتروني أوسع من الانترنيت، فعلى الرغم من أن الفضاء الالكتروني ينبني على الأنترنيت كأساس لهُ، فأنهُ يمثل تجربة أكثر ثراءً، بمعنى إن الانترنيت جزء من الفضاء الإلكتروني الواسع الذي يتحرك ويقوم بوظائفه ضمن هذا الحيز (الفضاء الإلكتروني) ، وهناك من يقول بعدم وجود فاصِل بين الفضاء الإلكتروني والانترنيت، لكن هناك اختلافا مهماً في

---

(١) نقلا عن حجيبة قاقو، الفضاء العمومي الالكتروني والتعبئة السياسية الذكية، مجلة العلوم السياسية والقانون، المركز الديمقراطي العربي للدراسات الاستراتيجية والاقتصادية، برلين، العدد الثاني، أذار ٢٠١٧، ص١٧٠.

(٢) موسى محمد مصطفى، الارهاب الإلكتروني، القاهرة، مطابع الشرطة، ٢٠٠٩، ص٥٦.

(3) Dictionary, Merriam–Webster, the definition of Internet .

المجال ،السعة و الخبرة بين الأثنين، فالذين لا يرُون الانترنيت ألا عبارة عن بيانات ضخمة، لا يُمكن ان يدركوا ما الذي يتحدث بهِ مواطنو الفضاء الالكتروني حيث يعتقد هؤلاء (مُستخدِمي الانترنيت) إن الفضاء الالكتروني مجرد شيء غامض [١]. ورغم الفوائد التي يمكن أن يقدمها الانترنيت بأنه مصدر للمعلومات، وسيلة اتصال سريعة في إدارة الاعمال التجارية، مصدر لتلقي العلم – ظهرت أهمية ذلك في جائحة كورونا حيث التعلم أصبح عن بُعد– ويُعد وسيلة للترفيه، ولكنهُ لا يخلوا من نقاط ضعف او سلبيات في الانترنيت منها [٢]:

١– طريقة كتابة العناوين للدخُول إلى موقع معين على الانترنيت، وهذا يُعد بحد ذاتهِ كشف للموقع او البيانات التي سُوف يتم الاتصال بها او التعامل معها.

٢– الموصِلات او المسارات بين مقدمّي الخدمة، والتي تشكل ما يعرف بنظام او بروتوكول البوابات الحديدية، وهنا يجد قراصنة الفضاء الإلكتروني فُرصة أخرى لمحاولة اختراق البيانات التي تخص الفرد او المؤسسة.

٣– إنِّ كل ما يُحرك او يُحدد البيانات تعد مفتوحة وغير مشفرة إلى حد ما، والأمر هنا يشبه الموجات التي تبثها الاذاعة المحلية فان أي شخص من الممكن أن يفتح هذه المحطة ويستقبل الاشارة التي تطلقها أذن فمجال الانترنيت والتنقل بين مواقعه يعد شبهُ مفُتوح للتجسُس على البيانات والمعلومات المهمة.

٤– القُدرة على نشر التحركات المقصُود منها الاضِرار بمصالح الاخرين، ومهاجمة أجهزة الحاسُوب عن طريق البرامج التي تحمل فايروسات، أو رسائل تؤدي الى أتلاف او إيقاف جهاز الحاسوب وهذه تُسمى البرامج الخبيثة، على سبيل المثال الدخُول على المواقع المُصابة بالفايروسات أو فتح مرفقات الرسائل البريدية.

---

(١) لورنس لسيج، الكود المنظم للفضاء الالكتروني، ترجمة محمد سعد طنطاوي، الطبعة الثانية، مؤسسة هنداوي، القاهرة، ٢٠١٤، ص٣١.

(٢) ريتشارد كلارك وروبرت نيك، حرب الفضاء الالكتروني، مركز الأمارات للدراسات والبحوث الاستراتيجية، ط١، ابو ظبي، ٢٠١٢، ص ص٩٨–١٠٧.

٥- إنّ شبكة الانترنيت، شبكة ضخمة لا مركزية التصميم، لأن مصمميها أرادوها أن لا تخضع للتحّكم من جانب الحُكومات وهذه تُعد نقطة ضعَف إضافية في تصميم الانترنيت حيث عمد مصممو البرامج أن يعطوا أولوية كُبرى للامركزية على حساب الامن.

ويعتقد المختصُون في مجال الانترنيت والبرمجيات إن أهم الاسباب التي تجعل عمليات الاختراق امراً ممكنا هي [١]:

١- وجود عيّوب في تصمّيم الانترنيت.
٢- وجود عيّوب في المُعدات والبرمجيات.
٣- الاتجاه لتوصيل المَزيد من الاجهزة على الخط المباشر.

ثالثاً: خَصائص الفضاء الإلكتروني:

للفضاء الإلكتروني العديد من الخصائص والمزايا ، اتسم بها نتيجة التطور السريع الذي يشهده هذا الحيز فهو يتيح حرية التعبير عن الرأي والتخفي لذا يمكن ذكر اهم المَزايا للفضاء الإلكتروني منها [٢]:

١- (الحُرية النسبية) وضُعف السيطرة الحكُومية .
٢- سُهولة التُواصل مع الأخرين وبناء روابط افتراضية .
٣- الطَبيعة الطُوعية غير الجبرية وهذا يُفسر الأقبال الشديد على استخدامه.

إضافة الى الميزات التي يتصف بها الفضاء الإلكتروني الذي يشهد العديد من النشاطات وتنفيذ الأعمال عن بعد فأن له سلبيات كثيرة منها [٣]:

١- يمكن أن يؤدي قضاء الكثير مِن الوقت في الفضاء الإلكتروني إلى مَشاكل في العالم الحقيقي مثل الشعور بالعُزلة والمشاكل الصحية.

---

(١) المصدر نفسه، ص٩٨.
(٢) محمد عبد ربه المغير، مصدر سبق ذكره، ص ٩٧.
(٣) المصدر نفسه ، ص ٩٨.

٢- التنزيلات غير القانونية عبر مواقع الشبكة الإلكترونية رغم إنها ميّزة كبيرة للمعجبين إلا أنها تمثل عيباً كبيراً لشركات الانتاج وحقوق الملكية الفكرية.

والواقع إن هناك تخّوفاً حقيقياً من أن يتحول الفضاء الإلكتروني إلى وسيلة مُحتملة لأصحاب النزعات الرأسمالية والتجارية، الأمر الذي يُعزز من اتجاهات السيطرة والتحكم والاحتكار العالمي، وهو ما يُبشر رُبما بعصر الإمبريالية الرقمية* (Digital Imperialism) ونتحول عندها من الحديث عن ثورة في التحرر إلى ثورة في التَحكم، إن الفضاء الإلكتروني ومن خلال تغلغلهُ الكبير في تعاملاُتنا الحياتية والاجتماعية أصبح يفرِض تأثيراً متزايداً على الشؤون العالمية والنظام الدولي، فإذا كان تعريف السياسة في آخر المطاف هو إدارة المُمكن من أجل تحديد من يَحصل على ماذا ومَتى وَكيف؟ فإن الفضاء الإلكتروني سُوف يكون ساحة هامة ورُبما رئيسية للتفاعلات السياسية في المستقبل القريب، حيث تتزِايد أهمية الفضاء الإلكتروني في الشؤون الأمنية العالمية [١].

فقد عُدَ الفضاء الالكتروني بأنه يمثل البُعد الخامس للحرب بعد – البُعد الدبلوماسي، البُعد العسكري، البُعد الاقتصادي والبُعد المعلوماتي– من حيث تشابُكية العالم الافتراضي مع العالم المادي في ظل علاقة تأثرية متبادلة، وقد وُصف بأنه الذراع الرابع لقوات الدولة الاستراتيجية البرية والجوية والبحرية[[٢]. لقد أختصر الفضاء الالكتروني حاجز الزمان والمكان، وخلق مساحات للتفاعلات الداخلية والخارجية في الواقع الافتراضي، بين الفاعلين الدوليين من الدول وغير الدول نتيجة امتلاكهِ سمات عدة منها:

---

* يستعمل مصطلح الامبريالية الرقمية في وصف الحالات التي تقوم فيها المنتجات الرقمية بتغيير العادات الاجتماعية، او الاحتكار والسيطرة على الوصول الى منتجات رقمية تنتمي اصلا إلى المجال العام. للتفصيل ينظر: آدم مستيان، العالم العربي وامبريالية المصادر الرقمية. ٢ كانون الثاني ٢٠١٧ متاح على الرابط: https://www.academia.edu/31613485/%D8%A7%D9%84%D8%B9%D8%A7%D9%84%D9%85_%D8%. تأريخ الزيارة ٢٠ كانون الثاني ٢٠٢١.

(١) نبيل عودة، الفضاء الالكتروني والشؤون الدولية، ١٥ أيلول ٢٠١٨. متاح على الرابط: https://arabicpost.net/opinions/2020/09/03 تأريخ الزيارة ٢٣كانون الثاني ٢٠٢١.

(٢) نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول، ، المجلد الثامن، العدد الثاني، مجلة مركز بابل للدراسات الانسانية، الحلة ، ٢٠١٨. ص١٩٠.

١- أنهُ ساحة صراع افتراضية بين أطراف مختلفة من حيث المستوى والتصنيف ويشمل المدنيين والعسكريين وهو اقل تكلفة.

٢- أصبحت الدول أكثر اعتماداً على الشبكات الالكترونية في إدارة البنية التحتية.

٣- لم تعد هناك حدود بالمعنى التقليدي لها، من حيث التأثير المتزايد لاستخدام التكنولوجيا والشبكات [١].

٤- صعوبة الردع الإلكتروني كون الفضاء الالكتروني ساحة هُلامية افتراضية يصعب على الدول وضع الحدود على سيادتها وهي بذلك – الدولة – فاقدة لركن من أركانها.

٥- غياب الشفافية الدولية لِصعوبة تحديد هوية المُعتدي [٢].

عليهِ يمكن القول أن الفضاء الإلكتروني، بقدر ما اصبح مجالاً واسعاً للتفاعلات وتبادل الخدمات، فهو كذلك مجال للمُنافسة والصراع مع صعوبة السيطرة على النشاطات المعادية التي تحدث فيه، حيث يتضمن نشاطات فردية على المستوى العلمي إضافة الى النشاطات بين الفواعل من الدول.

المطلب الثاني: تأثير الفضاء الالكتروني في حقل العلاقات الدولية

لقد احدَث الفضاء الالكتروني ثورةً معرفية وعملية في علم العلاقات الدولية ضمن النظام الدولي، كُل ذلك فرض تغييرات جذرية اقتضت البحث عن تصورات وطُرق جديدة لتدريس مادة العلاقات الدولية، تختلف عن الطُرق التقليدية الجامدة التي كانت تتناول مادة العلاقات الدولية، وستتناول الدراسة في هذا المطلب، اولاً الفضاء الالكتروني وظاهرة تفسير العلاقات الدولية مقارنة بالنظرية التقليدية وادارة الفضاء الالكتروني.

اولاً: الفضاء الإلكتروني وظاهرة تفسير العلاقات الدولية مقارنة بالنظرية التقليدية

---

(١) سماح عبد الصبور، الصراع السيبراني: طبيعة المفهوم وملامح الفاعلين – اتجاهات نظرية في تحليل السياسة الدولية، ملحق مجلة السياسة الدولية، العدد ٢٠٨، القاهرة، مركز الاهرام للدراسات السياسية والاستراتيجية، ٢٠١٧، ص٦.

(٢) ريتشارد كلارك وروبرت نيك، مصدر سبق ذكره، ص ص٢٥١-٢٥٢.

نتيجة الأهمية التي شكلها الفضاء الإلكتروني، والذي يمثل الأمن السيبراني جزء منه وانعكاس ذلك على العلاقات الدولية، مما دَفع الباحثّين في مجال العلاقات الدولية إلى إعادة النظر في المفاهيّم والمنطلقات النظرية لتفِسير ظاهرة العلاقات الدولية، وقد فرضت ظاهرة الفضاء الإلكتروني نوع من التداخل بين مستويات ثلاثة لتحلّيل ظاهرة العلاقات الدولية هي: مُستوى الافراد، ومُستوى البِناء السياسي الداخلي للدولة والمُستوى الدولي ليُصبح هناك ما يُطلق عليهِ بالمجتمع العالمي، الذي يَتعدد فيهِ الفاعلون وتتوحد فيهِ القضايا والاهتمامات. وقدر تعلق الأمر بالمستوى الدولي فهو اختبار مدى صلاحيتهِ وامكانية تطبيقهُ في معالجة ثلاث اشكاليات، تخُص (Cyber International Relation) أي درجة الاندماج بين الفضاء الإلكتروني والعلاقات الدولية، حيث ركزّت النظرية التقليدية للعلاقات الدولية على قضية، السلام، الحرب، التعاون والمنافسة بين الفاعلين من الدول، التي صيّغت في منتصف القرن السابعَ عَشر والقرن العشرين وبالتالي أصبحت لا تَتنَاسب مع التطُورات في النظام الدولي وانعكاس ذلكَ على العلاقات الدولية [1].

لقد أصبح من الضروري أن تأخذ النظريات في دِارسة العلاقات الدولية في حسابِها، المُتغير التكنُولوجي في تفسير حركة العلاقات الدولية وتفاعُلاتها، مقارنة بالنظريات التقليدية التي تَعتمد على احترام الحدُود التقليّدية وسيادة الدولة، لذا بَرز دور الفَضاء الإلكتروني كظاهرة دولية جديدة لهُ تأثير في نظرية العلاقات الدولية والمفاهّيم المرتبطة بها، من حيث التَداخل بين التفاعلات الرسمية وغير الرسمية، وبين مستويات التحليل الداخلي والاقليمي وعبر القومية والدولية والعالمية، اضافة الى تَجاوز الفضاء الإلكتروني سيادة الدولة على أراضيها متجاوزا معوقات المكان والزمان. لذا قَسم (جيس روزناو) النظام الى مكونين:

الأول:- النظام الدولي ،عالم الدولة وهو محدد لهُ تقاليده وانظمتهُ وله عدد محدُود من اللاعبين الذين يمكن التكُهن بهم وبأفعالهِم بدرجة معينة.

(١) عادل عبد الصادق، الفضاء الالكتروني واشكاليات نظرية العلاقات الدولية، مجلة السياسة الدولية، المجلد ٥٠، العدد ٢٠٠، القاهرة، نيسان ٢٠١٥، ص ١٢٤.

الثاني:- هو النظام العالمي، عالم مُتعدد المراكز فيه عدد شُبه مطلق من الفاعلين والمشاركين لديهم القدرة على العمل المستقل عن الدولة التي يعيشون على أرضها، وهو ما يعرف بالتنظيمات الدولية العابرة للحدود [١].

وظيفة النظام العالمي التقليدي بدأت بالتغير نظراً لازدياد أهمية العلاقة بين ظاهرة الفضاء الإلكتروني والعلاقات الدولية وهذه الأهمية تعود لعدةَ عوامل منها [٢]:

١- إعادة النظر في تأثير الحتمية التكنُولوجية في ظل قُدرة نظريات العلاقات الدولية في تفسيرها، رغم أن الكثير من الافتراضات الحتمية اكدتّ على حتمّية العامل التكنُولوجي في التفاعلات والتغُيرات الاساسية في النظام الدولي.
٢- تأثير الفضاء الإلكتروني في كافة المجالات – مدنية، عسكرية، اقتصادية واجتماعية – مما اعَطى الحُجة في نقد النظريات التقليدية في العلاقات الدولية.
٣- هناك علاقة تَأثير مُتبادل بين السياسة والفضاء الإلكتروني "السيبراني"، حيث تُركز معظم دراسات العلاقات الدولية على الأسئلة المُتعلقة بإدارة الإنترنت أو الحرب الإلكترونية، أو الدِفاع الإلكتروني، ونتيجة لذلك، تعمل الدول على توسيّع قُدراتها الدفاعية السيبرانية. وفي المُقابل، يُؤثر الفضاء الإلكتروني على السياسة فيما يَتعلق بالديمقراطية أو التَعبئة أو المُشاركة السياسية، فضلًا عن قضايا الأمن القومي.
٤- نتيجة توَسع وتَعدد الفاعلّين في النظام الدولي التي فَرضها الفضاء الإلكتروني، لم تُعد دراسة العلاقات الدولية تقتصر على الدول والحكومات، بل امتّدت دارستُها الى مستويات فرعية عِبر القومية وفوق القومية.

ثانياً: إدارة الفضاء الإلكتروني

يُعد الخلاف بين الفاعلين الدوليّين – بما في ذلك الدول، والمؤسسات الدولية وغير الحكومية والشركات الخاصة–، على المعايير الفنية واللوائح والمؤسسات التي تحدد هيكل الفضاء الإلكتروني هو القضية المركزية في إدارة هذا المجال. و يمكن وصف الفضاء الإلكتروني بحسب نظريات

(١) نقلا عن عادل عبد الصادق، ص ١٢٥.
(٢) المصدر نفسه، ص ١٢٧.

العلاقات الدولية ، بأنه اختبار صعب للحالة الساكنة ، واختبار سهل للمجتمع المدني العالمي، إذا وُجد أن الدول هي الجهات الفاعلة الرئيسية في مجال الإنترنت ، سوف تحتاج أدبيات العولمة إلى إعادة النظر في العلاقة بين الدول والجهات الفاعلة غير الحكومية، لكل من المنظمات الحكومية الدولية والمنظمات غير الحكومية حيث لها أدوار تلعبها في الحوكمة العالمية [١].

و ترى إدارة الإنترنت أنَّ الدول في موقعها الجهات الفاعلة الأكثر ضعفاً وغير الدول في أقوى حالاتها. هذا بالتأكيد استنتاج معظم علماء العلاقات الدولية الذين يدرسون الفضاء الالكتروني ، تلاحظ (ديبورا سبار) أن "المنظمات الدولية والحكومات الوطنية تفتقر إلى سلطة الشرطة في الفضاء السيبراني ويوافق (هوفلر) على ذلك ، مشيرًا إلى "الطابع اللامركزي والمفتوح والعالمي للإنترنت يجعل من الصعب تصميم وتنفيذ لوائح فعالة" [٢].

ويُجادل (Farrell)[ ][٣]، أيضًا بأن سُلطة الدولة على الفضاء الإلكتروني لم تتراجع إلى حد كبير، حيث ينظر في اتفاقية "الملاذ الآمن"* بين الولايات المتحدة والاتحاد الأوروبي بشأن خصُوصية البيانات، ويرى أنهُ في حين أن الاتفاقية هي في الواقع نهج هجين جديد من التنظيم الدولي على أساس تنفيذ القواعد الخاصة، وهي نفسها القواعد الأساسية التي أنشأتها سلطة الدولة، وأن اتفاقية الملاذ الآمن توفر دورًا مهمًا لتنص على كل من التصميم والتنفيذ.

---

(1) Daniel W. Drezner, The Global Governance of the Internet: Bringing the State Back In, Political Science Quarterly, Vol. 119, No. 3, The Academy of Political Science (Fall, 2004),pp.479 .

(2) Ibid,p.481.

(3) Henry Farrell, "Constructing the International Foundations of E-Commerce – The EU-US Safe Agreement," International Organization 57.2 2003,pp. 278-279.

* وهي الاتفاقية الموقعة عام ٢٠٠٠ لغرض نقل وتبادل البيانات والمعلومات الشخصية عن المواطنين الأوروبيين الى الولايات المتحدة، وقد ألغيت هذه الاتفاقية من قبل محكمة العدل الاوربية عام ٢٠١٥أثر شكوى مقدمة من قبل الناشط النمساوي ماكس ضد شبكة فيسبوك، وتم ابدالها بأتفاقية جديدة هي " درع الخصوصية " للتفصيل ينظر:

The Decision of the European Court of Justice

The date visit at 28 February 2021,Available at Link https://www.researchgate.net/publication/320473454_Safe_Harbor_The_Decision_of_the_European_Court_of_Justice

يُحدد (Newman)، المستوى القومي عبر هيئات البيانات الخاصة بين الدول الأعضاء في الاتحاد الأوروبي باعتبارها المُحركات الرئيسية الدولية لوضع القواعد الخاصة باللوائح على مستوى الاتحاد الأوروبي لإدارة الفضاء، تمثل حُجة (Newman) تحديًا قويًا لمزاعم (Drezner) وآخرين الذين يُشككون في تآكل سلطة الدولة، ومع ذلك هناك حاجة لمزيد من العمل التجريبي، لمعرِفة ما إذا كانت هذهِ النتائج يمكن تعمّيمها وتطبيّقها خارج الاتحاد الأوروبي وعِبر الوطنية، ليس من الواضح إلى أي درجة تعكس أطُروحة (Newman) الخَصائص الفريدة للفضاء الإلكتروني أو العولمة بشكل عام أو الاتحاد الأوروبي خاصه [١].

في كتابتهُما لمجتمع السياسات، يقترح كل من (Baird and Cukier) الشراكة بين القطاعين العام والخاص، للحُكم تعتمد على سُلطة الدول للشرعية والفعالية، يقول (Cukier) أن الحكومات تقدم فرصًا أكبر للمُشاركة الديمقراطية من المنظمات الدولية والمنظمات غير الحكومية، ويمكن أن توفر شرعية أكبر. ويُجادل بذلك ؛ يمكن للمؤسسات الهجينة للحُكم أن تجمع بنجاح بين الشرعية الديمقراطية للحكومات وسلطاتها العليا في الإنفاذ بشمولية وتفُوق خبرة في أنظمة التعددية [٢].

يُكرس كل من (Cukier، Baird، Lessig) جميعًا اهتمامًا بالبنية الأساسية للإنترنت، وكيفية معالجة الخلاف السياسي للمعايير واللوائح الفنية – ولا سيما تنظيم الملكية الفكرية – وتحديد الدرجة التي يمكن للفضاء الالكتروني أن يَعمل بها بشكل مَفتوح ومع ذلك، يؤكد (Baird) أن الولايات المتحدة لديها التزام بالقيم الليبرالية أكبر من مُعظم الدول، ومن المرجح أن تضمن أن تلك القيم تنعكس في حُكم الإنترنت، أكثر مما هو عليه الحال مع أي ترتيب يوفر قدرًا أكبر من السُلطة في اتخاذ القرار لأصحاب المصلحة الدوليّين الآخرين، الذين غالبًا ما يكون لديهم مصالح تتعارض مع هذه القيم. يفضل كل من (Baird and Cukier) بشكل عام، مجمّوعة أكثر شمولاً من المؤسسات الحاكمة التي تَمزج بين الدول والجهات الفاعلة الخاصةَ وغير الحكومية، مع

---

(1) Abraham L. Newman, “Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive,” International Organization 62.1 2008,pp.109, 120. نقلا عن Robert Reardon and Nazli Choucri1, The Role of Cyberspace in International Relations:, Paper Prepared for the 2012 ISA Annual Convention San Diego, CA April 1, 2012, p.12

(2) Robert Reardon and Nazli Choucri1,op.cit,p.13.

الاعِتراف بِصعوبة إنشاء مثل هذه المؤسسات بطريقة تَسمح لِمن هُم أقل قوة من أصحاب المصلحة في النظام الدولي ليكون لهم صوت، ولا سيما الدول الصغيرة والفقيرة التي كان لها تأثير ضئيل على اللوائح والقوانين والمعايير الفنية التي تحدد الفضاء الالكتروني [١].

إن أحد الجوانِب الأكثر إثارةً للاهتمام في الأدبيات المُتعلقة بالحُكم هو تَحديدها المفاضلة في حُوكمة الفضاء الإلكتروني بين الشُمولية والانفتاح. يفضل المُختصين جميعهم تقريبا ترتيبًا أكثر شُمولية وديمقراطية لحوكمة الفضاء الإلكتروني، بَشكل أفضل لتمثيل تنوع أصحاب المصلحة. في الواقع، كما يشير (ليسيج)، وكما جادل العديد من المُختصون في أقسام أخُرى من هذا الاستطلاع، بأن انفتاح الفضاء الإلكتروني بدأت بالفعل في التغيّير، وبدأت المشاعات الإلكترونية منذ فترة طويلة في التفتت على أساس الحدود السياسية. لا أحد في هذه المجموعة يقدم طريقاً واضحاً للمضي قدما، أو حلاً لهذه الأمور الأساسية. حيث يرى (Farrell)، أن الإقناع يمكن ان يكون آلية فعالة للحُكم المشترك، وأداة لتسوية الاختلافات الجوهرية في القيم إذا كان الفضاء الإلكتروني يعُد بالفعل بأن يكون له تأثير تحولي تقدمي على السياسة الدولية وأفضل إدارة له تكون عن طريق الأمم المتحدة، كونها المنظمة التي تضم أكبر عدد من الدول الفاعلة والعظمى [٢].

وترى الدراسة أن هؤلاء المؤلفيّن رغم اختلافهم حول القُوة التي يمكن أن تتَمتع بها الدول المختلفة عبر الإنترنت ومدى التأثير الذي يَجب أن يتمتعوا به – إنهم يرفضُون بشكل مُوحد أن يكون الانترنيت مفتُوح وغير مركزي – يَتمتع بالحُكم والتنظيم الذاتي–، او أن يَعمل بشكل مُستقل تمامًا عن أي سلطة حكومية، ويتم تَحديد هياكل هذه المؤسسات – التي تقوم على أدارة الفضاء والانترنيت – من خلال المَكسب الجماعي الذي تُقدمة للدول الأقوى، بينما الدول الأضعَف تَنزل إلى دور هامشي غير حكومي.

---

(1) Lawrence Lessig, The Internet Under Siege, Foreign Policy 127 2001. Available at Link: https://foreignpolicy.com/2009/11/16/the-internet-under-siege.the date at January 2021. the date visit 20 January 2021.

(2) Henry Farrell, OP. Cit, p. 280.

المطلب الثالث: الفضاء الالكتروني والمجتمع المدني العالمي

يمكن أن نلُاحظ تأثير الفضاء الإلكتروني على أهم القضايا التي تَخُص المُجتمع المدني العالمي وتَتأثر بالتقَدم التكنُولوجي بشكل مباشر. وهي الحكم والتأثيرات على الانظمة الاستبدادية والتنمية والأمن، والتي سوف تبينُها الدراسة في هذا المطلب، وعلى مدار عقدين من الزمن أعتبر العُلماء أن تكنولوجيا المعلومات والاتصالات يمكن أن تُعزز إنشاء (المجتمع المدني العالمي) وتعمل على خلق فرص اكبر للاتصال بين المجتمعات بشرط ضبط هذه التكنولوجيا بما يخدم المصالح للدول من التعاون.

اولاً: تأثير الفضاء الالكتروني على المجتمع المدني العالمي

تتناول أدبيات المجتمع المدني العالمي (Global Civil Society) تأثير الفضاء الإلكتروني التحوليّ على النظام العالمي، من خلال فَحص قدرتهُ على تعزيز المجتمع المدني العالمي (GCS) بشكل مباشر مسألة ما إذا كانت التكنولوجيا الإلكترونية لديها القدرة على تطوير جهات فاعلة جديدة عِبر الوطنية، تتجاوز سُلطة الدول وسيادتها، أنه ليس من المستغرب أن يأخذ البنائِيون زمام المُبادرة في هذا المَجال، كما هو الحال في كثير من الطُرق البنائية الأنسَب لمُعالجة التغييرات في الهوية من خلال العمل التواصلّي، حيث يُجمع الباحثون على قوة الدور الذي تلعبهُ التكنولوجيا الإلكترونية في تعزيز تنمية مثل هذا المجتمع وتعزيز دور الفاعلين والجماعات والهويات المشتركة عبر الوطنية. وأغلب المختصين في مجال العلوم السياسية يَرون الفضاء الإلكتروني على أنهُ احتمال أداة التمكين. تصف (Mernissi) [1].- كاتبة في مجال التكنولوجيا – على سبيل المثال، كيف مكنت التكنولوجيا الإلكترونية المرأة في العالم العربي، من خلال توفير منتدى يُسهل الوصول إليه للتعبير السياسي، لقد منح انفتاح الفضاء الإلكتروني وعدم الكشف عن هويته هؤلاء النساء صوتًا لم يكن ليُعبر عنه بخلاف ذلك، وقد بدأ هذا يؤثر بشكل إيجابي على وضع المرأة في

---

(1) Fatema Mernissi, “Digital Scheherazades in the Arab World,” journal Current History, University of California Press,,Volume 105, issue 689, March 2006, p. 121-126.

نقلا عن Robert Reardon and Nazli Choucri1, The Role of Cyberspace in International Relations:, Paper Prepared for the 2012 ISA Annual Convention San Diego, CA April 1, 2012, p.9.

المنطقة العربية على، بمعنى تمكين المرأة في الممارسة السياسية، فالمرأة العربية وغيرها من النساء في مناطق اخرى لها تقاليد واعراف تحد من مشاركة المرأة في المجال السياسي [١].

ويجادل العديد من المختصين ، بأن احتمالات نظام المجتمع المدني العالمي ستكون دائمًا مقيدة بحقيقة، إن العلاقات الاجتماعية التي يتم إنشاؤها عبر الإنترنت أضعف بكثير وأكثر عابرة من العلاقات الشخصية في الواقع الفعلي، والبعض متشكك حول قدرة الفضاء الإلكتروني على التغلب على الثقافة المحلية والهويات الإقليمية واستبدالها مع تلك العالمية، تذهب (Mernissi) إلى أبعد من ذلك من خلال وصفها للفضاء الإلكتروني، بأنه تهديد للهوية المحلية وتشير إلى التأثير المدمر للفضاء الإلكتروني على أنه "الحد"، الفاصل بين الحياة الخاصة والعامة، بينما يثير هؤلاء الباحثون نقاطًا منطقية وتحديات مهمة للافتراضات السابقة في الأدبيات، فأنهم فشلوا في دعم هذه الادعاءات بالتحليل التجريبي، كما أنهم فشلوا في النظر بشكل كامل في الحالات التي توجد فيها بالفعل روابط اجتماعية مهمة عبر الوطنية، وكيف يمكن أن تتأثر هذه الروابط بالفضاء الالكتروني، يصف العديد من الباحثين الخلاف السياسي ليس فقط داخل الفضاء الإلكتروني، ولكن أيضًا إدارة الفضاء الإلكتروني نفسه. يجادل (Schmidt) و (Cohen)، على سبيل المثال، بوجود منافسة عبر الفضاء الإلكتروني بين الفائزين والخاسرين المحتملين، في هذه الحالة، فأن الدول الديمقراطية –دول الغرب– ستستفيد أكثر من نشر التكنولوجيا السيبرانية في الوقت الحاضر، في حين أن الأنظمة الصغيرة والاستبدادية ستسعى إلى التخفيف من التهديد الذي تشكله عليها نتيجة استقرار النظام. ويجادل (Deibert) بأن الدول قد تُغير بنية الفضاء الإلكتروني لتناسب أغراضُهم ومصالحهم [٢].

ثانياً: الفضاء الالكتروني والأنظمة الاستبدادية.

تشير أغلب الدراسات أن الحكام يرغبون بأن يكون تأثيرهم واضح في ادارة الدولة، وقدر تعلق الامر بالأنترنيت فأنهم يرفضون بشكل موحد إنترنت مفتوح ولامركزي يتمتع بالحكم الذاتي، أي إن السلطة الحاكمة دائما تحاول أن يكون الانترنيت تحت سيطرتها؛ لكي توجه افكار وعقول المواطنين بما يتناسب وسياستها او العقيدة التي تحاول نشرها، وترى مثل تلك الأنظمة، أنه لا يمكن أن يعمل

(1) Robert Reardon and Nazli Choucri Op. cit. p. 9.
(2) Ibid,Op. cit. p.10.

هذا بشكل مستقل تمامًا عن أي سلطة حكومية، ويمكن ملاحظة ذلك بشكل واضح في كل من الصين وكوريا الشمالية وايران وغيرها من الدول، التي تعتبر الانترنيت والنفاذ إلى الشبكة يجب أن يكون تحت سيطرتها وإدارتها المركزية.

مجال آخر مميز في الأدبيات هو تأثير انتشار شبكة الانترنيت على الأنظمة الاستبدادية، التي قد تواجه معارضة من نوع جديد بوسائل جديدة لا يمكن قمعها ومن خارج الحدود السياسية. وكان العديد من المختصين ومحللي السياسات متفائلين بشأن آثار التحول الديمقراطي والتحرير الذي سوف يحدثه الفضاء الإلكتروني على المجتمعات التي تحكمها أنظمة استبدادية، بينما، يرى باحثون آخرون أن التكنولوجيا الإلكترونية "محددة القيمة" وأنظمة التحكم الدقيقة والمعقدة كما يصفها كل من (Boas, Hachigian, and Kalathil) يمكن أن تستخدمها الأنظمة الاستبدادية للتغلب على الآثار المزعزعة للاستقرار السياسي للفضاء الإلكتروني ويعتبر وصف (Hachigian) للإنترنت الصيني هو الأكثر تفصيلاً في هذا المجال، حيث تقوم الصين بفرض رقابة على عدد كبير من مواقع الويب التي يمكن الوصول إليها [١]. بالمقابل، يدافع المفكِّرون الصينيون عن أسلوبهم في تحديد حرية الانترنيت؛ لتعزيز سيادة الدولة ويتحدثون عن مفهومٍ جديد هو "مجتمع المستقبل المشترك" والذي سيجعل النظام الدولي أكثر ودًّا مع الأنظمة غير الديمقراطية [٢].

أخيرًا يمكن القول إن النظام الاستبدادي يستخدم الفضاء الإلكتروني لمصلحته الخاصة، من خلال استخدامه كمنصة خاصة به للدعاية وعن طريق تشجيع المواطنين على الإنترنت، من اجل بث الروح القومية داخل البلد وخارجه لتعزيزها لدى المواطنين المغتربين.

ثالثاً: الفضاء الالكتروني والنمو الاقتصاد (التنمية)

---

(1) Nina Hachigian, "China's Cyber-Strategy,", Journal Foreign Affairs, Volume 80,issue 2, Washington Quarterly, March-April 2001, pp. 118,133. And, Nina Hachigian, "The Internet and Power in One-Party East Asian States," Washington Quarterly,Center for International Strategic Studies,Volume 25,issue 3, summer 2002, pp. 41,58. نقلا عن Robert Reardon and Nazli Choucri Op. cit. p.18.

(2) Charles Edel, Mira Rapp-Hooper, The 5 Ways U.S.-China Competition Is Hardening, Foreign Policy Journal, May 18,2020,, p6. Available at Link: https://foreignpolicy.com/2020/05/18/united-states-competition-coronavirus-pandemic-tensions. The date at visit is March 26, 2021.

يرى (ألفين توفلر) في كتابة "تحول السلطة" ان الاقتصاد تحول نحو " اقتصاد المعرفة " والسلطة اصبحت هي المعرفة والثروة والقوة مع التأكيد على المعرفة "ان السلطة في الحياة الاقتصادية ستذهب غدا الى الذين يعرفون بشكل افضل حدود المعلومات..." [١]، والتي يمكن تحقيقها من خلال زيادة القدرة على الإرسال والوصول بسرعة وتخزين المعلومات على نطاق عالمي.

ويُعد (Persaud)، أن الفضاء الالكتروني آلية لتحسين تدفق المعرفة التي يتم التعامل معها باعتبارها سلعة اقتصادية، بمعنى انتشار تكنولوجيا المعلومات –جنبًا إلى جنب مع التحرر الاقتصادي الدولي– وذلك من خلال السماح بتدفق رأس المال عبر الحدود للاستثمار في "الأفكار الجيدة". وتأثير تكنولوجيا المعلومات على النمو الاقتصادي، كما أنهم يقرون بأن هذه الفائدة لا يتم توزيعها بشكل منصف ومتساو عبر المجتمعات المختلفة. بمعنى إن انتشار التكنولوجيا السيبرانية من المرجح أن تخلق – او تعمق – "فجوة رقمية" بين المجتمعات المتقدمة والمجتمعات الاقل تطورا لصالح الاولى، يدعي (Hammond) على سبيل المثال، أن هذه الفجوة المتزايدة يمكن أن تخلق تهديدا للأمن، حيث تلجأ الدول الاقل تطورا الى الوسائل العنيفة كوسيلة للحصول على بعض هذه المكاسب [٢].

ومع ذلك، لا يتفق المختصون على الأسباب المحددة للفجوة الرقمية أو السياسات المناسبة للتصدي لها، ويجادل البعض بأن البلدان المتخلفة يمكنها الاستفادة من تكنولوجيا المعلومات و"القفزات" السابقة للدول المتقدمة، أي يمكن للدول الانتقال مباشرة إلى أحدث التقنيات مثل الأقمار الصناعية وأنظمة الاتصالات، أو أنظمة الإنترنت المتقدمة، بينما يرى البعض الاخر بأن مثل هذه القفزات غير ممكنة؛ مادامت الدول تفتقر إلى رأس المال البشري والتنظيمي والمؤسسات القانونية والسياسية والاقتصادية المستقرة اللازمة للاستفادة من التكنولوجيا للتنمية الاقتصادية، ويشير (Aiden) إلى إن نشر تكنولوجيا المعلومات المقترن بسياسات التحرر الاقتصادي، دليل على أن العامل الدافع وراء هذه المبادرات ليس التنمية بل توسع الرأسمالية العالمية ويعتبر انتشار تكنولوجيا

---

(١) ألفين توفلر، تحول السلطة، ترجمة لبنى الريدي، ج١، الهيئة المصرية العامة للكتاب، القاهرة،١٩٩٥، ص١٨٨.

(2) Robert Reardon and Nazli Choucri Op. cit. p.15-16.

المعلومات هو ببساطة شكل جديد من أشكال الإمبريالية. ويعتقد آخرون، مثل (Kudaisya) و(Bletha)، أن الحكومة نفسها هي التي يجب أن تقوم بتطوير التقنيات السيبرانية، وقد مارست مثل هذا الدور الولايات المتحدة ودول شرق اسيا بفاعلية، في بناء البنية التحتية لتكنولوجيا المعلومات بسبب خيارات السياسة المفتوحة على الخارج [1].

جدول رقم (١) الترتيب العالمي لمؤشر الحياة الرقمية للدول الخمس الاولى من مجموع (٣٤) دولة عام ٢٠١٦

ت	الدولة	الدرجة من ١٠٠
١	**الولايات المتحدة الامريكية**	**٩٦,٣**
٢	**كندا**	**٩٢,٤**
٣	**أستراليا**	**٩٠,١**
٤	**المملكة المتحدة**	٨٨,٧
٥	**ألمانيا**	٨١,٠

الجدول من اعداد الباحث بالاعتماد على المصدر: تقرير شركة تليفونيكا* لعام ٢٠١٦

وفقا لمؤشر تليفونيكا للحياة الرقمية (TIDL)* في الجدول رقم (١) المعني باستخدام التكنولوجيا في كافة مناحي الحياة الاقتصادية والاجتماعية، حلت الولايات المتحدة في المركز الأول، وكان تسلسل الصين (٢٤) من مجموع (٣٤) دولة وهذا يشير غلى إن الصين لازالت تفرض الكثير من القيود على استخدام الانترنت في أغلب مجالات الحياة –خاصة على للمواطنين في الوصول لخدمة الانترنت. ويشير التقرير إلى أن التحول إلى الحياة الرقمية مكن الشعوب من تحقيق تقدم اجتماعي، مع خلق فرص أكبر للثروة وقد شكلت صناعة التكنولوجيا الرقمية ما يقرب من خُمس النمو العالمي في العقدين الماضيين، وتُقدر التقارير أن كل ١٠% زيادة في رقمنة الاقتصاد يمكن أن يزيد نمو

(1) Ibid,p.16.

* تليفونيكا هي شركة متعددة الجنسيات مقرها في مدريد، رائدة عالميا في مجال الاتصالات، تأسست عام ١٩٢٤. للتفصيل ينظر شركة تليفونيكا للحياة الرقمية Telefonica Index Digital Life (TIDL) متاح على الرابط: https://thegedi.org/telefonica-index-on-digital-life/ تأريخ الزيارة: ٥ ايار ٢٠٢١.

متوسط الناتج المحلي الإجمالي للفرد بنسبة تصل إلى ٤٠%. ويعتمد مؤشر تليفونيكا للحياة الرقمية، على ثلاثة مؤشرات فرعية لقياس قدرات الدولة في مجال الحياة الرقمية وهي: [١]

١ – درجة الانفتاح الرقمي، وتعني مدى جودة البنية التحتية الرقمية، وحرية استخدام الإنترنت والانفتاح، والخدمات العامة الرقمية.

٢ – الثقة الرقمية، وتقيس مدى ارتباط وثقة الأفراد والمنظمات في البنية التحتية الرقمية للبلاد، (درجة الاعتماد الرقمي، والخصوصية والأمن).

٣– ريادة الأعمال الرقمية، وتقيس جاهزية المواطنين والمنظمات للاستفادة من البنية التحتية الرقمية، ويرتبط هذا المؤشر بمدى (محو الأمية الرقمية، وانتشار الأعمال التجارية الرقمية، والابتكار، والتمويل).

رغم أن الأمن السيبراني أصبح " بُعداً جديداً من ضمن أبعاد الأمن القومي، والذي أحدث تغييرا جوهريا في مفاهيم العلاقات الدولية (الصراع، القوة والتهديد) وفرض على الفواعل الدولية الانتقال من عالم مادي الى عالم افتراضي في غاية التعقيد والتشابك، خاصة بعد الاعتماد المتزايد على التقنية الرقمية وتأثيرها في كافة التفاعلات الدولية، مما حتم على الدول ضرورة ايجاد وسائل فعالة لمواجهة التهديدات السيبرانية التي تمتاز بالتغيير والغموض، والعمل على تحقيق الأمن السيبراني للحفاظ على امنها القومي" [٢].

وتذهب الدراسة مع هذا الرأي إذا توفرت القدرة على تنظيم سلوك الفاعلين – من الدول وغير الدول – في مجال الفضاء الالكتروني، وأنفاذ القانون الخاص بالجرائم الالكترونية، لأن التطور التكنولوجي وخاصة في مجال الفضاء، أعطى مساحة اكبر وأسهل للتدخل في شؤون الدول عبر اختراق الحدود الوطنية الالكترونية، التي تكون السيطرة عليها اكثر صعوبة من السيطرة على الحدود التقليدية، ومن أجل ضبط كل ذلك سيكون التعاون الدولي مهم جدا.

---

(1) Erkko Autio (university College London),Laszlo (University of Pécs), Telefonica Index Report, Digital Life, June 2016,pp. 17,30.

(٢) عبد الكريم زهير عطيه الشمري، الاستراتيجية الأمريكية للهيمنة على الفضاء السيبراني، رسالة ماجستير، جامعة الموصل، كلية العلوم السياسية، ٢٠٢١، ص ص٥٦–٥٧.

المبحث الثالث: القانون الدولي والفضاء الالكتروني

يُمثل تطوير القانون الدولي وألياته تدريجيا أحدى مسؤوليات الامم المتحدة الرئيسية في الميدان القانوني، حيث أصبحت بيئة الفضاء الخارجي الجديدة مَجالاً هاماً لممارسة تلك المسؤوليات، ولقد تحققّت العديّد من الاسهامات الهامة في قانون الفضاء الخارجي، بِفضل جهُود لجنة الامم المتحدة لاستخدام الفضاء الإلكتروني في الأغراض السلمية ولجنتها الفرعية القانونية. وأصبح من الضروري أن تكُون الامُم المتحدة في الواقع محوراً للتعاون الدولي في ميدان الفضاء الإلكتروني من أجل صياغة القواعد الدولية اللازمة لذلك.

ثمةَ اعتقاد سائد بأن الفضاء الإلكتروني يستحّيل إخضاعهُ للتنظيم الحكومي؛ أي إنهُ بحكم جوهرهُ مُحصن ضد سيطرة الحكومة أو غيرها من الجهات؛ فالأمر ليس في طبيِعة الفضاء الإلكتروني التي تجعله مستعصيًا عن التنظيم، بل أن الفضاء الإلكتروني ليس له "طبيعة" خاصة به من الأساس، هناك فقط "كود منظِّم" ؛ وهو مجموعة البرمجيّات والأجهزة التي تَجعل الفضاء الإلكتروني على ما هو عليه، وكما قال ويليام ميتشل: هذا الكُود هو قانون الفضاء الالكتروني [١]، في هذا المبحث سوف نتناول ثلاثة مطالب، الأول يتطرق إلى القانون الدولي والجرائم السيبرانية، وفي المطلب الثاني تذهب الدراسة لتوضيح أهم الاتفاقيات التي تنظم مكافحة الجرائم السيبرانية، إضافة إلى المطلب الثالث الذي يبين دور الأُمم المتحدة في تنظيم الفضاء الالكتروني.

المطلب الأول: وسائل تنظيم الفضاء الإلكتروني بموجب القانون الدولي

على غِرار السوابق التاريخية بما فيها تطُور النُظم القانونية لانتشار الأسلحة النووية، فإن وضع قوانين ومعايير قابلة للتطبيق على الفضاء الإلكتروني، سيكون بدون شك عمليةً لا تخلو من بُطء وتعثُّر من الناحية التنظيمية [٢]، ومن أجل توضيح أهمية القانون في تنظيم الفضاء الإلكتروني سوف نتطرق هنا إلى القانون الدولي للفضاء الالكتروني ووسائل تنظيم الفضاء وتعريف الجريمة السيبرانية وأهم خصائصها مع بيان طرق مكافحتها.

---

(١) لورنس لسيج، مصدر سبق ذكره، ص ص٢٠،٢٦.

(٢) احمد عبد الرحمن المحمود، البعثة الدائمة لدولة الأمارات لدى الأُمم المتحدة، استخدام الفضاء الخارجي في الاغراض السلمية. الكلمة التي ألقها ممثل دولة الأمارات أمام رئاسة لجنة المسائل السياسية الخاصة وأنهاء الاستعمار، والسيد ديفيد كندل رئيس لجنة الاستخدامات السلمية للفضاء الخارجي، في ١٣تشرين الاول ٢٠١٦ في الامم المتحدة.

اولاً: القانون الدولي للفضاء الإلكتروني.

رغم تزايُد الوعي بأهمية الأمن السيبراني، فإن إمكانيات تطبيق القانون الدولي لتنظيم سُلوك الدول في الفضاء الالكتروني تظل محدودة، ولقد دارت عدة نقاشات بشأن قُدرة القانون الدولي على ضَبط أنشطة الدول في الفضاء الالكتروني، إذ جاءت التغيرات التكنولوجية بأنشطة جديدة، لا يوجد تكيّيف قانوني واضح يُلائمها في الاطر القانونية الحالية، أو أنها كشفت عن التعارض ما بين القوانين الدولية القائمة، بحيث أصبح هناك تأثير مُتبادل بين التقدم التكنولوجي وما ينتج عنهُ من مسائل وتحديات وقدرة القانون الدولي على التكيف معها [١].

ومن بين التحديات التي تواجهُها الدول ووكالات إنفاذ القانون، هو إيجاد أساس قانوني لتحديد عتبة السلوك القانوني في الفضاء الالكتروني، وقد تم مؤخراً بذل محاولات لتطوير معايير سلوك دولية، إلى جانب نقاشات حول ما يُمكن اعتبارهُ سلوكاً مقبولاً في الفضاء الالكتروني وما لا يُمكن اعتباره كذلك [٢]. وقد أدت التداعيات التي نتجت عن الهجمات التي استهدفت البُنية التحتية الرقمية لإستونيا إلى إنشاء مركز التميّز للدفاع السيبراني التعاوني*، وقد تم إنشاء المركز في خضم الهجمات السيبرانية ضد جورجيا في ٢٠٠٨. وفي الفترة ما بين ٢٠٠٩ –٢٠١٢، وبِطلب من مركز التميز للدفاع، قامت مجموعة من الخُبراء والباحثين القانونيين بتقييم إمكانية تطبيق المبادئ القانونية على الهجمات السيبرانية، وتم تتويج هذه الجهُود بنشر (دليل تالين) الذي يبحث إمكانية تطبيق القانون الدولي على الفضاء الإلكتروني [٣].

وبالرغم من كونه (دليل تالين) عبارة عن وثيقة غير مُلزمة قانونياً، إلا أنه يتناول عدداً من المفاهيم، مثل الحصار السيبراني والهجمات المرفقة باستخدام القوة ويُقدم تعريفات لـ"الخسارة" و"الضَرر" في سياق الفضاء الالكتروني، كما أنه يعد مبادرة رائدة. ورغم التحديات التي تواجه

---

(١) بهاء عدنان السعيري وعماد عبد خضير الزرفي، انتقال التهديدات من الواقع الى العالم الافتراضي، مجلة كلية العلوم السياسية، جامعة الكوفة، المجلد ٢٧، العد ٤، ٢٠١٩، ص٤٨٣.

(٢) الياس الصديقي، الفضاء الافتراضي والقانون الدولي، المركز العربي لأبحاث الفضاء الالكتروني،٢٥ تشرين الثاني ٢٠١٧. متاح على الموقع:

http://accronline.com/article_detail.aspx?id=28959 تأريخ الزيارة ٥ ايار ٢٠٢١.

* وهو عبارة عن مُبادرة أطلقها حلف الناتو لإجراء بحُوث في مجال الأمن السيبراني

(٣) بهاء عدنان السعيري، مصدر سبق ذكره، ص٤٨٤.

وضع إطارات قانونية للعمليات المُسلحة وعدم ضمان امتثال الدول دائماً، فإن هذه المفاهيم تَخضع للقانون الدولي سواء تم تطبيقُها في البر أو الجو أو البحر، فمثلاً، يُحدد مجلس الأمن التابع للأُمم المتحدة، الإجراءات المتخذة إذا تم شَن هُجوم عدواني على احد أعضائها وحسب المواد (المادة ٣٩) والإجراءات المؤقتة التي سيتم اتخاذها (المادة ٤٠) والنهج المتبع لإعادة إحلال السلام (المادتان ٤١و٤٢)[1] .

وخلال لقاء المجموعة الأممية للخُبراء الحكوميين حول التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي، قامت الجهات الحكومية خاصة الأمريكية والروسية والصينية بالاتفاق حول أهمية تطوير معايير في مجال الفضاء الالكتروني، بغض النظر عن التعاريف المتضاربة للقواعد وعدم الاتفاق حول كيفية النهوض بها، وفي هذا السياق يجب أن تعمل الدول على تنفيذ أنشطتُها في الفضاء الخارجي بروح من المسؤولية والشفافية، الكفيلة بتعزيّز تدابير الثقة والأمن للفضاء، كما يجب تعزيز القانون الدولي المُتعلق بالفضاء الخارجي بما يساهم في كبح سباق التسلح في الفضاء" [2].

ثانياً: وسائل تنظيم الفضاء الالكتروني

هل هناك طريقة لتنظيم الفضاء الالكتروني بما فيها الرسائل الاعلانية والمُواد الاباحية وصولاً إلى المُستوى التنظيمي الذي يخضعان لهُ في الفضاء الواقعي؟

تُعتبر الانماط التنظيمية الاربعة – القانون، الأعراف الاجتماعية، السوق، المعمار – هي أهم الوسائل المستخدمة في تنظيم الفضاء الالكتروني أو القيود التي يمكن أن تفرض على مستخدمي الفضاء الإلكتروني، من عدة جوانب، ويُمكن أن نلاحظ ذلك من خلال الانماط او القيود الاربعة وهي [3]:

١- القانون: تقّيد الوسائل التنظيمية ضد عمليات الاحتيال والخِداع التي يقوم بها من يُرسلون الرسائل البريدية الاعلانية في الفضاء الواقعي والتي تخضع لتنظيم مكثف.

---

(١) الأُمم المتحدة – مجلس الأمن، التدابير المتخذة في حالات تهديد السلم والإخلال به ووقوع العدوان (الفصل السابع)، المادة (٣٩) – المادة (٥١).

(٢) احمد عبد الرحمن المحمود، مصدر سبق ذكره.

(٣) لورنس لسيج، مصدر سبق ذكره، ص ص ٣٤٧، ٣٥٢.

٢- تنظيم الأعراف الاجتماعية، رسائل البريد الاعلانية في الفضاء الواقعي حيث ثمةَ شُعور بما هو مناسب للإعلان عنهُ بأن يكون مسموح به اجتماعياً.

٣- تُنظم الاسواق رسائل البريد الاعلانية في الفضاء الواقعي حيث تكُون كُلفة الرسائل في الفضاء الواقعي مرتفعة جداً، أي إن العائد منها يجب أن يكون مناسباً قبل ارسالُها، مما يؤدي الى تقليص حجم رسائل البريد الاعلانية التي يَجري ارسالِها في الفضاء الالكتروني.

٤- المعمار، يعتبر معمار الفضاء الإلكتروني هو وسيلة الحماية الحقيقية لحرية التعبير فيه، بل هو "التعديل الأول" الحقيقي في الفضاء الإلكتروني، ولا يُعد هذا التعديل الأول قانونًا محليًّا.

وقسم من المختصين يعتبرون إن (الكود)*، هو القانون المُنظم للفضاء الالكتروني، ويُقصد بهِ التحول من فضاء الكتروني فوضَوي إلى فضاء إلكتروني خاضع للسيطرة، أن كثير من الحرية التي كانت موجودة في الفضاء الإلكتروني عند نشأتهُ، لن تكون موجودة في مستقبلِه، وكما قال (ويليام ميتشل): هذا الكود هو قانون الفضاء الإلكتروني، أو بعبارة (جول ريد نيبرج) "قانون عالم المعلوماتية " اذاً الكود هو القانون [١].

ثالثاً: الجرائم السيبرانية.

مع تزايد انتشار تقنيات المعلومات والاتصالات ونمو فرص تبادل المعلومات آنياً في عالم واسع، أصبح أمن الفضاء الإلكتروني مسألة مُعقدة تتعدى أمكانية الدول وتتطلب تعاونا عالميا لضمان أمن الأنترنت، وبحسب دراسة (نورتون) التي أعُدتّ عام ٢٠١١، فإن " تهديدات الفضاء الإلكتروني تزايدت بشكل كبير في العام الماضي حيث بلغ عَدد الضحايا (٤٣١) مليون شخص بالغ من مختلف بقاع العالم" [٢].مقارنة بعدد مستخدمي الأنترنيت الذي وصل الى (٤،٨٠مليار)

---

* ويقصد به الرمز السري لدخول الشخص الى موقعه او بريده الإلكتروني ويكون عبارة عن مجموعة ارقام او حروف او الاثنين معا. للتفصيل ينظر: لورنس لسيج، الكود المنظم للفضاء الالكتروني، ص٢٤٨.

(١) لورنس لسيج، مصدر سبق ذكره ص٢٦.

(٢) لازاروس كابامبي، الأُمم المتحدة، اجتماع المجلس الاقتصادي والاجتماعي حول اهمية أمن الفضاء الالكتروني، نيويورك، ١٢ كانون الثاني ٢٠١١، ادارة الشؤون الاقتصادية والاجتماعية: متاح على الموقع الرسمي للأُمم المتحدة: تأريخ الزيارة ٢٢شباط ٢٠٢١.

https://www.un.org/development/desa/ar/news/intergovernmental-coordination/cybersecurity-demands-global-approach.html

شخص حول العالم [١].ومع تزايد الاعتماد على الانترنيت وتقنية المعلومات يتزايد عدد الخروقات والانشطة الاجرامية، وتتراوح هذه الخروقات والاعمال غير المصرح بها من النشاط السياسي والاحتيال وتعطيل الخدمة...الخ، كل هذه تقع ضمن الجرائم السيبرانية. وتشير الجريمة السيبرانية، إلى أي جريمة تتضمن استهداف الشبكات الحاسوبية. وقد يستخدم الحاسوب في ارتكاب الجريمة وقد يكون هو الهدف، وإلحاق الضرر بالممتلكات التي تكون عادة على شكل سرقة أو تخريب أو تعطيل البيانات الخاصة بتلك الجهة التي تعرضت للهجوم، والجرائم الالكترونية على مستوى الدول عادة تشكل تهديد على أمنها القومي، والقانون الدولي يحاول أن يصنف تلك الافعال من ضمن الجرائم التي تحاسب عليها المحكمة الجنائية الدولية .

وقد عرفت اتفاقية كومنولث الدول المستقلة (الجريمة الإلكترونية) بأنها " الجريمة المتعلقة بمعلومات الكمبيوتر على أنها فعل إجرامي الهدف منه هو معلومات الكمبيوتر" [٢] ، سواء بالاختراق والتجسس والتخريب .

وتصّنف الجرائم الالكترونية إلى مجموعات مختلفة من الطوائف واعتماداً على عدة معاييرمنها: [٣]

١- جرائم وفقا لمعيار المستهدفين، جرائم ضد الاشخاص وجرائم ضد الدول.

٢-جرائم الكترونية وفقا لمعيار المصلحة او الحق المعتدى عليه، وهنا تصنف الجرائم الالكترونية إلى جرائم الاعتداء الالكتروني على النفس (الابتزاز)، جرائم الاعتداء الالكتروني على الاموال مثل: (جرائم القرصنة والغش والاحتيال الالكتروني) اضافة الى جرائم الارهاب

(1) Digital 2021 July Global Statshot Report , 6 November Available at link:

https://datareportal.com/reports/digital-2021-july-global-statshot.Date vist 6 November 2021.

(٢) مكتب الأُمم المتحدة المعني بالمخدرات والجريمة، دراسة شاملة عن الجريمة السيبرانية، الأُمم المتحدة، نيويورك، ٢٠١٣، ص ص١١، ١٦.

(٣) هالة احمد الرشيدي، الجهود الدولية في مجال مكافحة الجرائم الإلكترونية، مجلة الديمقراطية، العدد ٥٧، مؤسسة الأهرام، القاهرة، تموز ٢٠١٩، ص٣٠.

الالكتروني الذي يجمع بين جرائم الاعتداء على الانفس والاموال [١]. وقسم آخر يُصنّف الهجمات الالكترونية كما يأتي: [٢]

١- استهداف البنية التحتية للدولة: سواء كانت محطات الطاقة والنقل والخدمات المالية والمصرفية، من قبل جماعات أو حتى فرد وبكلفة قليلة جداً مقارنة بالأضرار التي تسببها للدولة*.

٢- هجمات القراصنة (الهاكر) وهي محاولة اتلاف البيانات أو استهداف جهاز الحاسوب نفسه.

٣- سرقة الاموال: من خلال تصيد بعض عملاء البنوك عبر البريد الالكتروني.

٤- البرامج الخبيثة التي تستهدف انظمة المعلومات للدول والشركات وتعمل على تدميرها أو العبث بالبيانات.

٥- استغلال الاطفال والأحداث والنساء في الإباحيات.

٦- سرقة الملكية الفكرية: وتعني سرقة المعلومات الموثقة إلكترونيا ونشرها بطرق غير شرعية (بدون ترخيص).

رابعاً: خصائص الجرائم السيبرانية وطرق مُكافحتها

---

(١) عبد الله بن عبد العزيز بن فهد العجلان، الارهاب الإلكتروني في عصر المعلومات، بحث مقدم الى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الانترنيت "، والمنعقد بالقاهرة في ٤-٢ حزيران ٢٠٠٨، ص ١٤.

(٢) إسراء جبريل رشيد مرعي، الجرائم الالكترونية الاسباب الاهداف طرق الجريمة ومعالجتها، المركز الديمقراطي العربي للدراسات الاستراتيجية الاقتصادية والسياسية، القاهرة، ٩أب ٢٠١٦، ص ص١٣-١٤.

* في تموز سنة ٢٠٢١ تم اختراق نظام السكك الحديدية الإيرانية ، من قبل مجموعة (إندرا) الايرانية المعارضة وهذا الهجوم يشكل تحذيرا لإيران حيث ألحق ضرراً كبيراً بوسائل النقل ؛ لا سيما انه نُفذَ من قبل مجموعة صغيرة بلا ميزانية او كوادر او امكانيات حكومية ، وربما تم التنفيذ من خارج البلاد. للتفصيل ينظر: Ronen Bergman, Mysterious Hacker Group Suspected in July Cyberattack on Iranian Trains ,The New York Times, Aug 14 2021. https://www.nytimes.com/2021/08/14/world/middleeast/iran-trains-cyberattack.html تأريخ الزيارة ١٥آب ٢٠٢١ .

نظراً لأتساع الجريمة السيبرانية وانتشارها على مجال واسع، بحيث اصبحت تفوق من حيث العدد والأضرار التي تسببها، الجرائم الواقعية التقليدية ، وهي تميزت بالكثير من الميزات التي فرقتها عن الجرائم العادية ، فهي تتميز بعِدة صفات منها:

١- صعوبة معرفة مرتكب الجريمة بسبب تعدد المواقع الإلكترونية وسهولة تخفي الفاعل.
٢- سهولة طمس معالم الجريمة والدلائل التي تدل على الفاعل.
٣- تعتبر قليلة الجهد وأقل عنفا جسديا مقارنة بالجرائم التقليدية.
٤- ليس لها زمان ومكان محدد فهي تحدث في كل العالم وفي أي وقت [١].
٥- الفعل الجرمي بواسطة استخدام أنظمة تقنية حديثة لا يقتصر على المجني عليه فقط وانما يشمل متضررين اخرين داخل وخارج الدولة المستهدفة، وهو بذلك اكثر ضرراً من الهجمات التقليدية [٢]. وتحاول الدول الحد من هذه الجرائم ومكافحتها بعدة طرق منها [٣]:

١- نشر الوعي بين المواطنين والمجتمع بخطورة الهجمات الإلكترونية وكيفية حدوثها.
٢- فرض سياسات وعقوبات دولية ومحلية على مرتكبي الجرائم الالكترونية.
٣- تفعيل أحدث الوسائل والتقنيات للكشف عن هوية الفاعل.
٤- تحديث التشريعات والقوانين بما يتلاءم والتطورات السريعة التي تحدث في مجال الفضاء الإلكتروني.

المطلب الثاني: الاتفاقيات المنظمة للفضاء الإلكتروني ومكافحة الجرائم الالكترونية

هناك العديد من الاتفاقيات التي عقدت للحد من الجرائم الالكترونية، منها اتفاقية كومنولث الدول المستقلة٢٠٠١ واتفاقية منظمة شنغهاي للتعاون١٩٩١، وسيتم التركيز هنا على اتفاقية بودابست لعام ٢٠٠١، والاتفاقية العربية لعام ٢٠١٠لكونها الأكثر تفصيلا والأقرب للموضوع .

اولاً: الاتفاقية الاوربية للجرائم الالكترونية

---

(١) علي زياد العلي، مصدر سبق ذكره، ص ص٨٩-٩٠.

(٢) كركوري مباركة حنان، خصوصية ارتكاب الجريمة في النظام المعلوماتي –دراسة تحليلية في ضوء القانون الجزائري –، مجلة الدراسات الاستراتيجية والعسكرية، المجلد الثاني، العدد الثامن، المركز الديمقراطي العربي، برلين، ، ايلول ٢٠٢٠، ص ١٤.

(٣) إسراء جبريل راشد مرعي، مصدر سبق ذكره، ص ١٧.

تعد اتفاقية جرائم الإنترنت، والمعروفة أيضًا باسم اتفاقية (بودابست) سنة ٢٠٠١بشأن جرائم الإنترنت، أول معاهدة دولية تسعى إلى معالجة جرائم الإنترنت وجرائم الكمبيوتر، من خلال مواءمة القوانين الوطنية وتحسين تقنيات التحقيق وزيادة التعاون بين الدول، وقد صاغها مجلس أوروبا في ستراسبورغ بفرنسا بمشاركة نشطة من الدول المراقبة في مجلس أوروبا (كندا واليابان والفلبين وجنوب إفريقيا والولايات المتحدة)، ودخلت حيز النفاذ في ١ تموز ٢٠٠٤. لقد جاء في الديباجة أن هدف مجلس أوروبا هو تحقيق وحدة أكبر بين أفراده، والاعتراف بقيمة تعزيز التعاون مع الدول الأطراف الأخرى، مقتنعين بالحاجة إلى اتباع سياسة جنائية مشتركة، على سبيل الأولوية، حيث تهدف الاتفاقية إلى حماية المجتمع من الجرائم الإلكترونية، من خلال اعتماد التشريعات المناسبة وتعزيز التعاون الدولي؛ مدركًا للتغييرات العميقة التي أحدثتها الرقمنة والتقارب والعولمة المستمرة لشبكات الكمبيوتر، فهي تشعر بالقلق من مخاطر استخدام شبكات الكمبيوتر والمعلومات الإلكترونية أيضًا لارتكاب جرائم جنائية، وإذ تدرك الحاجة إلى التعاون بين الدول والصناعات الخاصة في مجال مكافحة الجرائم الإلكترونية والحاجة إلى حماية المصالح المشروعة في استخدام وتطوير تقنيات المعلومات؛ إيمانًا بأن المكافحة الفعالة للجريمة الإلكترونية تتطلب تعاونًا دوليًا متزايدًا وسريعًا وفعالًا في المسائل الجنائية ؛ من خلال تسهيل اكتشافها والتحقيق فيها والملاحقة القضائية على المستويين المحلي والدولي، ومن خلال توفير الترتيبات اللازمة لتعاون دولي سريع وموثوق [1]. وقد جاء في الفصل الثاني – التدابير الواجب اتخاذها على المستوى الوطني – من الاتفاقية المادة الثانية باعتبار الوصول غير المشروع الى انظمة الكمبيوتر او اي بيانات ومعلومات رقمية وبدون حق، جرائم جنائية عندما ترتكب عمدا، ويتبنى كل طرف أتخاذ تدابير تشريعية وفق قانونها المحلي.

المادة (٦):- إساءة استخدام الأجهزة، يتخذ كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لوضعه كجرائم جنائية بموجب قانونها المحلي، عندما تُرتكب عمداً وبدون حق:

(1) European Treaty Series–N0.2,185,Convention on Cybercrime, Budapest,23.xI.2001,pp. 1,4 .

الإنتاج، البيع، الشراء للاستخدام، الاستيراد، التوزيع أو صنعه بأي طريقة أخرى متاح من جهاز، بما في ذلك برنامج كمبيوتر، تم تصميمه أو تكييفه بشكل أساسي من نظام الكمبيوتر يمكن الوصول إليه، بقصد استخدامها لغرض ارتكاب أي من الجرائم المنصوص عليها سابقا [١].

ثانياً: الاتفاقية العربية لمكافحة تقنية المعلومات.

نتيجة لارتفاع معدلات الجرائم الالكترونية في الشرق؛ بسبب مكاسبها الكبيرة، وانخفاض المخاطر وسهولة الوصول لها واستجابة لهذا الواقع، برزت الحاجة الماسة إلى عقد اتفاقية في هذا المجال [٢]. وتم توقيع الاتفاقية من قبل مجلس وزراء الداخلية العرب في ٢١كانون الاول ٢٠١٠ أذ وقعت أحدى وعشرون دولة عربية من ضمنها جمهورية العراق التي صدقت على الاتفاقية في ايلول ٢٠١٣، ودخلت الاتفاقية حيز النفاذ في ٧ شباط ٢٠١٤، وتهدف الاتفاقية – كما جاء في الديباجة – "إنَّ الدول العربية الموقعة، رغبة منها في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، واقتناعاً منها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات، وأخذاً بالمبادئ الدينية والأخلاقية السامية ولا سيما أحكام الشريعة الإسلامية، وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الجرائم، ومع مراعاة النظام العام لكل دولة، والتزاما بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الإنسان ذات الصلة من حيث ضمانها واحترامها وحمايتها" [٣]. كما جاء في المادة الأولى من الاتفاقية التي نصت على: "تهدف هذه الاتفاقية الى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرىء أخطار هذه الجرائم، حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها" [٤]. وبما إنَّ الجرائم الالكترونية مرتبطة دائما بالتطورات المستمرة في مجال تقنية وتكنولوجيا المعلومات، فقد نصت الفقرة الختامية السابعة بأنه:" يجوز للدولة الطرف أن تقترح تعديل أي نص من نصوص

---

(1) Ibid, p.5 .

(2) ECONOMIC AND SOCIAL COMMISSION FOR WESTERN ASIA (ESCWA), United nations, Policy Recommendations on Cyber safety and Combating Cybercrime in the Arab Region 14 April 2015, p.1.

(٣) الأمانة العامة لجامعة الدول العربية الدول العربية – إدارة الشؤون القانونية – الشبكة القانونية العربية، نص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الفصل الختامي احكام ختامية، ٢٠١٠، ص ١٣.

(٤) المصدر نفسه ، ص١٤

هذه الاتفاقية وتحيله إلى الأمين العام لجامعة الدول العربية الذي يقوم بإبلاغه إلى الدول الأطراف في الاتفاقية لاتخاذ قرار باعتماده بأغلبية ثلثي الدول الأطراف..." [1]. والغاية من هذه الفقرة هو لمواكبة التطورات التكنولوجية التي قد تحدث في مجال مكافحة الجرائم الالكترونية، وامكانية أجراء التعديلات اللازمة.

بناء على ما تقدم ترى الدراسة إن تأثير الفضاء الالكتروني على العلاقات الدولية قد تزايد في السنوات الأخيرة، وهذا ما تؤكده الاستراتيجيات الأمنية السيبرانية المتجددة التي تقوم على أساس أن الفضاء الالكتروني أحد المجالات المهمة التي باتت تشكل خطرا على الأمن القومي للدول، وأبرز دليل على هذا هو إعلان أجهزة الأمن القومي أن الفضاء الإلكتروني هو "المجال الخامس للحرب" (بعد الأرض، والبحر، والجو، والفضاء). ونتيجة لذلك، وسعت العديد من الدول قدراتها الدفاعية السيبرانية. ولا بد من الاهتمام به للحفاظ على أمنها، وتشير النقاشات المؤسسية إلى صعوبة الاتفاق حول حوكمة الإنترنت بسبب تضارب المصالح بين الدول الديمقراطية والسلطوية، فيما يتعلق بقيمة حرية الإنترنت مما جعل ضرورة العمل على وضع الاتفاقيات والقواعد لتنظيم الفضاء الالكتروني.

اذاً هناك علاقة تأثير متبادل بين السياسة والفضاء الإلكتروني "السيبراني"، حيث تركز معظم دراسات العلاقات الدولية على الأسئلة المتعلقة بإدارة الإنترنت أو الحرب الإلكترونية، أو الدفاع الإلكتروني والهجوم السيبراني، وكلها تتداخل مع مفهوم الأمن السيبراني، ومع ذلك، تظل سيادة الدولة من أهم الآثار المترتبة على علاقة السياسة بالفضاء الإلكتروني، وضرورة البحث عن الطرق والوسائل التي تمارِس من خلالها الجهات الفاعلة (الدول أو غير الدول) السيطرة على الفضاء السيبراني، وتواجه الدول صعوبة في تكييف الهجمات السيبرانية ضمن القانون الدولي،

ولمعرفة أهم القضايا التي تُعد مصدر تنافس أو حتى مصدر خلاف يصل إلى حد الصراع، بين الدولتين أضافة إلى الاستراتيجية الأمريكية والصينية في مجال الأمن السيبراني، كل ذلك نُحاول التركيز عليه في الفصل الثاني والذي يتضمن بيان أهم الاستراتيجيات الأمريكية التي جعلت من الأمن السيبراني مجال جديد ومهم في الأمن القومي. لكُل من أمريكا والصين.

---

(١) نفس المصدر ص ١٤.

الفصل الثاني

البعد السيبراني في العلاقات الامريكية– الصينية

من المعلوم أن كلا من الولايات المتحدة الأمريكية والصين تملكان موارد كبرى وتفاعلات دولية واسعة، ما يجعل النظام الدولي ككل محط اهتمام سياسات كلا الدولتين. وأحيانا توصف علاقتهما بالعلاقة بين الاثنين الكبار (G–2) كونها العامل الرئيس الاكثر تأثيرا في النظام الدولي .وتعود العلاقة بين الدولتين في "مرحلة خروج الولايات المتحدة من عزلتها وانفتاحها على قارة اسيا نهاية القرن التاسع عشر، واتخاذ سياسة الباب المفتوح ، وكانت الحرب اليابانية أفضل حدث لدخول الولايات المتحدة الى الصين لأنهاء الاحتلال الياباني، لأجزاء من شرق الصين" [1]، ويعتقد الباحث إن دعم الصين من قبل الولايات المتحدة لتولي مقعد دائم في مجلس الأمن سنة ١٩٤٥ ،كان في صالح تلك العلاقة بين البلدين، التي ما لبثت أن تأزمت عندما تولى الشيوعيين السلطة سنة ١٩٤٩ ،و تعمل الولايات المتحدة والصين على إعادة تحديد علاقتهما الثنائية، حيث تعني نقاط القوة الجديدة للصين – الناتج المحلي الكبير والنمو الاقتصادي الذي انعكس على زيادة الأنفاق العسكري والتطور العسكري– أن لديها موقعًا جديدًا ومسؤوليات جديدة في العالم، لذا يمكن أن يصبح الصراع السيبراني عاملاً مهماً في عملية إعادة التعريف بالعلاقة الثنائية هذه، لأنه يؤدي إلى تفاقم المنافسة الاقتصادية والعسكرية. وسوف نتناول في هذا الفصل الموضوع في ثلاثة مباحث.

المبحث الأول: يبين طبيعة العلاقات الأمريكية–الصينية.

المبحث الثاني: يركز على الاستراتيجية الأمريكية للأمن السيبراني.

المبحث الثالث: طبيعة الاستراتيجية الصينية للأمن السيبراني التي تبين التنافس السيبراني بينهما في.

---

(١) لبنى خميس مهدي وخضر عباس عطوان، الأبعاد الاستراتيجية للعلاقات الصينية الأمريكية وآفاقها المستقبلية، مجلة، العدد ٧٤، دراسات دولية مركز الدراسات الاستراتيجية والدولية، جامعة بغداد، ، ٢٠١٨، ص٣.

المبحث الأول: طبيعة العلاقات الامريكية الصينية

تعود العلاقات بين الولايات المتحدة الأمريكية والصين الحديثة إلى عام١٩٤٩م في عهد ماوتسي تونغ مؤسس الصين الحديثة، ونظراً للمكانة التي تتميز بها كل من الدولتين، تتحمل كل منهما المسؤولية والمهام المشتركة للحفاظ على السلام العالمي وتعزيز التنمية المشتركة، وذلك يتطلب من الجانبين النظر الى العلاقات بينهما والتعامل بشكل صحيح وملائم، وايجاد طريق التعايش السلمي بينهما رغم الخلافات، وعلى هذا الاساس يحاول الطرفان اقامة نوع جديد من العلاقة، القائمة على أساس عدم التصادم والاحترام المتبادل والتعاون والكسب المشترك.

ومن أجل ايضاح وافً للعلاقة بين الولايات المتحدة والصين، سيتم تقسم المبحث إلى ثلاثة مطالب تتناول إبعاد العلاقات الأمريكية الصينية، والاستراتيجية الأمريكية تجاه الصين، ثم بيان أبرز القضايا التي توثر على هذه العلاقة بين البلدين.

المطلب الأول: أبعاد العلاقات الامريكية الصينية

مما لاشك فيه إن العلاقات الأمريكية–الصينية من أهم العلاقات بين قوتين لهما وزنهما في النظام الدولي في القرن الحادي والعشرين، "وإن السيطرة العالمية للولايات المتحدة الأمريكية تعتمد بشكل مباشر على المدى الزمني والمدى الفعال لاستمرار هذه السيطرة (التفوق على الصين) الأميركية على القارة الأورآسية، مع بقاء اليابان محمية أميركية بصورة رئيسة، والمحافظة على الشراكة الاقتصادية مع الحلفاء في جنوب شرق آسيا لمحاصرة الصين" [(١)]. ويمكن التعرف أكثر على هذه العلاقة من خلال بيان الابعاد السياسية والاقتصادية أضافة الى العلاقات العسكرية.

أولا: العلاقات السياسية والدبلوماسية

على المستوى الدبلوماسي يمكن اعتبار نقطة الانطلاق في هذه العلاقة، هو البيان المشترك الذي صدر في كانون الأول ١٩٧٨، ويُعد ١ كانون الثاني سنة ١٩٧٩ التأريخ الرسمي لبداية العلاقة بين الولايات المتحدة والصين، حيث شهد تبادل التمثيل الدبلوماسي، والاتفاق على تسوية قضية تايوان، التي تعد المساءلة الحاسمة في تطبيع العلاقات بين البلدين.

---

(١) زيغنيو بيرجنسكي، رقعة الشطرنج الكبرى السيطرة الأمريكية وما يترتب عليها جيواستراتيجياً، ترجمة: وزارة الدفاع مركز الدراسات العسكرية، واشنطن، ط٢، ١٩٩٩، ص ص ٢٨، ٣٢.

وعلى الرغم من عدم الثقة في العلاقة بين الدولتين، كونها معقد ومليئة بالتناقضات إلا أنهما بحاجة الى استمرارية هذه العلاقة نتيجة المصالح التجارية المتبادلة، ويعتقد الباحث أن أهم مُحدد في منع المواجهة العسكرية بين الطرفين هو العامل الاقتصادي، حيث الحجم الكبير للتبادل التجاري بينهما أذ أصبحت الصين الدولة الثانية بعد الولايات المتحدة من حيث الناتج المحلي وكمية السلع المصدرة على المستوى العالمي، ونسبة احتياطي عالية جداً من العُملة تفوق الولايات المتحدة، وما يُلاحظ على العلاقات الصينية الأمريكية أنها" تشكل نمطاً فريداً، فلا هي منافسة صريحة ولا هي عداء مستتر، ولكنها مع ذلك تظل تعمل في إطار توازن دقيق من المصالح المتبادلة والتهديدات المتوقعة" [١].

إنِّ طبيعة التنافس بين الطرفين وضخامة المصالح الاقتصادية الثنائية، والمكانة التي بدأت تتمتع بها الصين من حيث حجم الاقتصاد ومعدل النمو ومقدار الرصيد من العملة الاجنبية، لا يسمح بتراجع او تقلص العلاقة بينهما، أضافة الى حاجة الصين الماسة للتقنيات الحديثة وأسرار التكنولوجيا المتقدمة، كما إن الصين تهتم كثيراً بأستقرار وتطور العلاقات الصينية الأمريكية، ولكنها لا تعترف بما يُدعى "بالدول القائدة والدول التابعة" [٢]. وبالتالي تقوم الاستراتيجية الأمريكية الشاملة على مبدأ تحقيق الزعامة العالمية ؛ من خلال منع ظهور منافس عالمي آخر يكون معاديا لها، والحيلولة دون العودة الى نظام متعدد الاقطاب معتمدة في ذلك على قدرتها للتوسع في قوتها العالمية ، من خلال السيطرة البرية والجوية أضافة الى سعيها للهيمنة على الفضاء حديثا [٣].

عليه يمكن القول ان العلاقات الامريكية –الصينية ذات طبيعة مركبة من عدة عناصر [٤]:

١- الحرص الأمريكي على علاقة شراكة مع قوة كبرى صاعدة.

٢-محاولة الولايات المتحدة أن تبقي التطور والنفوذ الصيني تحت المراقبة الأمريكية الدائمة.

---

(١) صفاء حسين علي الجبوري. العلاقات الأمريكية الصينية في مرحلة ما بعد الحرب الباردة. مجلة جامعة تكريت كلية العلوم القانونية والسياسية، المجلد ٣، السنة ٣، العدد ١٢، ٢٠١١، ص١٥٠-١٥١

(٢) عبد الكريم زهير عطية الشمري، مصدر سبق ذكره، ص٨٥.

(٣) صفاء حسين علي الجبوري، مصدر سبق ذكره، ص ١٨٩ .

(٤) باهر مردان، العلاقات الصينية-الامريكية، بكين، ٢٠١٤، ص٣. متاح على الرابط التالي: https://www.academia.edu/6003157 تأريخ الزيارة ١شباط ٢٠٢١.

٣-حرص الولايات المتحدة على منع التقارب أو التعاون بين اليابان وبلدان آسيا المجاورة مع الصين.

ألا أن ما يُعكر جو العلاقة السياسية عادة، هو انتقاد الولايات المتحدة للصين، على سبيل المثال "انتقدت الولايات المتحدة الصين لقمعها حرية التعبير على الانترنيت، وربما تصبح أنماط السلوك هي موضوع المفاوضات بين الولايات المتحدة الأمريكية والصين في المستقبل"، وغالبا ما تُوجّه الولايات المتحدة انتقادات غير مباشرة للصين [١]. تتمثل برصد انتهاك حقوق الانسان وتقييد حرية الانترنت من خلال فرض رقابة على اغلب المواقع الإلكترونية من الحكومة .

وعند تولى الرئيس (جون بايدن) منصبه في كانون الثاني ٢٠٢١، كان شعار حملته المفضلة: (أمريكا عادت)، والتي لخص من خلالها سياسية حكومته الخارجية، وفي خطابه الأول للسياسة الخارجية، أعلن الرئيس (بايدن) أن الصين هي "المنافس الأكثر جدية لأمريكا" وتعهد بمواجهة بكين في مجموعة من القضايا، من حقوق الإنسان إلى الملكية الفكرية، وسيكون رده على حملة الصين المستمرة ضد المتظاهرين المؤيدين للديمقراطية والسياسيين في هونغ كونغ مؤشرًا مبكرًا على السياسة الخارجية تجاه بكين [٢].

ثانيا: العلاقات الاقتصادية والتجارية

العلاقة بين البلدين قديمة ولكنها توسعت في العقود الثلاثة الماضية، حيث وصل حجم التبادل التجاري بينهم الى (٦٤٨،٢) مليار دولار لعام ٢٠٢٠ حسب تقرير نشره موقع (Economic Times online) [٣]، واضاف ان قيمة صادرات الصين تبلغ حوالي (٤٧٨،٩)مليار دولار بينما تبلغ

---

(١) سكوت وارين، مارتن سي ليبيكي، وأستريد ستوث سيفالوس، التوصل الى أتفاق مع الصين بشأن الفضاء الالكتروني، مؤسسة راند للنشر، كاليفورنيا، ٢٠١٦، ص٨-١٠ .

(2) President Joe Biden delivers a speech on foreign policy at the State Department, in Washington, Feb. 4, 2021, World Politics Review, U.S. Foreign Policy Under Biden,, Available at the link: https://www.worldpoliticsreview.com/insights/29534/with-biden-s-foreign-policy-us-seeks-to-reclaim-its-global-standing. The date is March 31, 2021.

(3) The volume of trade exchange is $648.2 billion between China and the United States, The Economic Times online. The date is May 5, 2021.p. 3.

الصادرات الامريكية إلى الصين نحو (١٦٩،٣) مليار دولار. بعد أن كان خمسة مليارات سنة ١٩٨٠، وبذلك تكون الصين ثاني أكبر شريك تجاري للولايات المتحدة الامريكية–وقد تصبح الشريك رقم واحد –وثالث أكبر سوق لصادراتُها، ويمكن رسم صورة عن العلاقات الاقتصادية الأمريكية –الصينية من خلال الحقائق والأرقام التالية [١]:

١– تُعد الصين ثاني أكبر شريك تجاري مع الولايات المتحدة بعد كندا، حيث شكلت صادراتها الى الولايات المتحدة (٤٧٨،٩) مليار دولار، مقابل (١٦٩،٣) مليار دولار للواردات الصينية من أمريكا.

٢– تملك الصين أكبر احتياطي للعملة الأجنبية في العالم وصل الى أكثر من (٣) ترليون* دولار

٣– بلغت صادرات الولايات المتحدة من فول الصويا إلى الصين نسبة (٦٠%) من أجمالي الصادرات واشترت الصين (٣٠%) من أجمالي صادرات القطن الامريكي.

ونظرًا لحجم الصين، فإن الحوادث المؤسفة التي لا مفر منها والتي قد تصاحب عملية الإصلاح، قد يكون لها تداعيات دولية، ويُعد ذلك السبب وراء أدخال الصين إلى منظمة التجارة العالمية.

ورغم ذلك تحدث الكثير من التوترات في العلاقات التجارية بين البلدين؛ عقب فرض رسوم او تصريحات لمسؤولين، وقد شهدت فترة إدارة الرئيس الأمريكي(ترامب) الكثير من هذه التوترات، مثلا في تغريده له على تويتر أن "الصين استفادت من الولايات المتحدة لسنوات طويلة حتى تقدموا علينا لأن رؤساءُنا لم يقوموا بعملهم، لذلك يجب على الصين إلا ترد لأن ذلك سيزيد الأمور سوءا" [٢]. كان ذلك بعد فرض رسوم من قبل الحكومة الامريكية على السلع الصينية.

ثالثا: العلاقات العسكرية

تميزت العلاقات الأمريكية–الصينية في المجال العسكري، بالتذبذب مقارنة بنظيرتها الاقتصادية وذلك بسبب موقف كلا البلدين من القضايا الخلافية وخاصة قضية تايوان، حيث قامت

---

https://economictimes.indiatimes.com/topic/official-website.

(١) قائمة البلدان حسب احتياطيات العملات الأجنبية، متاح على الموقع https://www.marefa.org/% : تأريخ الزيارة ٣شباط ٢٠٢١ .

* واحد ترليون يساوي ألف مليار (١ ترليون = ١٠٠٠ مليار)

(2) Donald J. Trump (@real Donald Trump) May 13, 2019

الولايات المتحدة ببيع أسلحة الى تايوان*، عدة مرات منها بيع معدات للاتصالات العسكرية في نهاية سنة ٢٠٢٠ [١]. من جانبها ترى الحكومة الصينية إن تعزيز العلاقات العسكرية مع واشنطن، يعني بأنها ستحصل على العديد من المكاسب الاستراتيجية فضلا عن أرسال رسائل سياسية وأهمها: إنّ عملية التحديث للمؤسسة العسكرية الصينية تتطلب خبرات متراكمة كالتي تمتلكها نظيرتها الامريكية، من حيث حجم القدرات والامكانيات والانتشار العالمي والكفاءة القتالية، لذلك اتفقت الصين والولايات المتحدة على توسيع دائرة التبادلات العسكرية، كجزء من الجهود الرامية لبناء علاقات أكثر استقراراً، إذ كان لقاء وزير الدفاع الصيني (Zhang Wanquan) بنظيرهُ الامريكي (Chuck Hagel) بالعاصمة الأمريكية في اب ٢٠١٣ كخطوة باتجاه تعزيز العلاقات العسكرية، ويرى (هنري كيسنجر) أن صلب العقيدة العسكرية الأمريكية يكمن في مبدأ عدم سيطرة أية قوة معادية على الشواطئ المقابلة للولايات المتحدة الأمريكية، سواء في المحيط الأطلسي أو المحيط الهادئ، أي أن غرب أُوروبا وشرق آسيا، يجب أن تكون من المناطق الحليفة للولايات المتحدة الأمريكية، إذ تَرافق تراجع الخطر الروسي على غرب أُوربا**، مع تعاظم الخطر الصيني على شرق أسيا [٢]. وقد رافق ذلك زيادة في الانفاق العسكري لكل من الولايات المتحدة والصين في عام ٢٠٢٠ مقارنة بالسنوات السابقة، والجدول أدناه يبين مستوى الإنفاق العسكري للدول الخمس الأعلى حول العالم عام ٢٠٢٠.

---

* قررت الولايات المتحدة في ٢٩كانون الثاني ٢٠١٠ بيع أسلحة الى تايوان بقيمة ٦،٤ مليار دولار ونتيجة لهذا السلوك الامريكي علقت الحكومة الصينية علاقاتها مع الولايات المتحدة ليَستمر الحال إلى نهاية عام ٢٠١٠ حيث تم استئناف العلاقات العسكرية لكن ليس بالمستوى المطلوب. للتفصيل ينظر: بكين تجمد علاقتها العسكرية مع واشنطن بسبب صفقة أسلحة أمريكية لتايوان. متاح على الموقع التالي:

https://www.france24.com/ar/20100130-china-usa-taiwan-weapons-saling-diplmocy-crisi-relation-pekin-washington تأريخ الزيارة ٢شباط ٢٠٢١.

(1) Editor Chen Zhuo, Source China Military Onlin, Chinese defense ministry denounces $280 million US arms sales to Taiwan,9-12-2020. Available at the link: http://eng.chinamil.com.cn/view/2020-12/09/content_9949608.htm تأريخ الزيارة ٢شباط ٢٠٢١

** دول غرب أُوربا (النمسا بلجيكا فرنسا ألمانيا لوكسمبورج هولندا سويسرا، ودول شرق آسيا (الصين اليابان كوريا تايوان منغوليا.

(٢) هنري كيسنجر، هل تحتاج الولايات المتحدة إلى سياسة خارجية نحو دبلوماسية للقرن الحادي والعشرين، ترجمة عمر الأيوبي، ط ٢، بيروت، دار الكتاب العربي، ٢٠٠٣،ص ص ١٠٦، ١٠٨.

جدول رقم (٢) بالإنفاق العسكري للدول الخمس الأعلى حول العالم عام ٢٠٢٠ [١].

الدولة	مليار دولار	النسبة المئوية من الانفاق العالمي
الولايات المتحدة	٧٧٨	**% ٣٩**
الصين	**٢٥٢**	**%١٣**
الهند	٧٢،٩	**% ٣,٧**
روسيا	٦١،٧	**% ٣,١**
المملكة المتحدة	**٥٩,٢**	**% ٣,٠**

الجدول من اعداد الباحث. المصدر: معهد ستوكهولم الدولي لأبحاث السلام.

بينما بلغت ميزانية الدفاع الامريكية لعام ٢٠٢١ (٧٢٢) مليار دولار، مقارنة بالميزانية لعام ٢٠٢٢ (FY)*التي تسعى أدارة الرئيس (بايدن ٢٠٢١) لاعتمادها من الكونغرس، والبالغة (٧١٥) مليار دولار، والتي تضع خمسة أشياء يجب مراقبتها في طلب الميزانية السنة المالية ٢٠٢٢وهي [٢] :

١- ما هو مقدار خفض قوة الجيش المقترحة.

٢ - كم عدد السفن الحربية وأنواعها من أجل التوسع البحري.

٣- ،خفض البرامج الاستراتيجية القديمة دون تسميتها بشكل واضح .

٤- برنامج الطائرة F-35 المكلف ومحاولة تخفيضه.

٥- تبرير عدد القوات اللازمة لردع وصد الهجمات الإرهابية.

---

(1) Nan Tian, Alexandra Kuimova, Diego Lopes da silva, and others, Trends In World Military Expenditure 2019, Stockholm International Peace Research Institute (SIPRI), April 2020,p.2.

* (FY)العام المالي fiscal year للتفصل عن العام المالي٢٠٢٢ لنفقات وزارة الدفاع الأمريكية وطلب الرئيس بايدن لهذه الميزانية ينظر: (ملخص طلب التمويل التقديري للرئيس بايدن للسنة المالية ٢٠٢٢)

Summary of the President's Discretionary Funding Request

(2) Todd Harrison, What to Look for in the FY 2022 Defense Budget Request, Center for Strategic International Studies (CSIS), Washington, April 29 2021,p.2-4.

بالمقابل بلغت ميزانية الدفاع الصينية لسنة ٢٠٢١ (٢٠٩) مليار دولار، وهذا المعدل من الأنفاق العسكري الصيني يثير قلق الولايات المتحدة [١]. حيث يذكر (بيتر وايزمان)، كبير الباحثين في معهد ((سيبري): "إن النمو في الإنفاق العسكري الأميركي يعتمد الى حد كبير على العودة المتوقعة إلى المنافسة بين القوى العظمى" [٢]، وهذه أشاره واضحة للصين كمنافس جديد بدلاً من الاتحاد السوفيتي السابق والتي احتلت المركز الثاني في الانفاق العسكري العالمي لسنة ٢٠٢١، ويلاحظ من الجدول أعلاه إن هذه هي المرة الأولى التي ظهرت فيها دولتان آسيويتان بين أكثر ثلاث دول من حيث الانفاق العسكري، هما الصين والهند. بناء على ما تقدم يمكن القول إن الصين تسعى لعلاقة متكافئة مع الولايات المتحدة، بعيداً عن سياسة الهيمنة التي تحاول الولايات المتحدة ممارستها تجاه الصين، ويعتبر العامل الاقتصادي هو المحدد الاساسي لضبط هذه العلاقة لحاجة الطرفين المتبادلة في ميدان التجارة، كما تحرص الصين على الاستفادة من القدرات العسكرية الامريكية المتراكمة لتطوير قدراتها العسكرية أضافة الى زيادة انفاقها العسكري في السنوات الاخيرة.

المطلب الثاني: الاستراتيجية الأمريكية تجاه الصين

بعد نهاية الحرب الباردة أصبح الحديث يدور حول النظام أحادي القطبية، الذي تهيمن عليه الولايات المتحدة، لكن هذا الوضع لم يستمر طويلاً، ونتيجة للنمو الاقتصادي للصين وسعيها الحثيث لمواجهة التفرد الأمريكي، بدأت الولايات المتحدة تضع استراتيجيتها للحد من الصعود الصيني. عليه سوف نتطرق هنا إلى الاستراتيجية الأمريكية تجاه الصين بعد الحرب الباردة بالإضافة إلى الاستراتيجية الأمريكية تجاه الصين في عهد الرئيس الامريكي دونالد ترامب.

اولاً: الاستراتيجية الأمريكية تجاه الصين بعد الحرب الباردة

شكلت العلاقة بين الولايات المتحدة والصين دوراً مهما في مجمل العلاقات الدولية وخاصة بعد الحرب الباردة وانكفاء الاتحاد السوفيتي السابق كقوة مكافئة للولايات المتحدة، التي اصبحت

(1) Wu Qian: China's defense budget growth in 2021 is stable and moderate, Xinhua News Agency,8/3/2021. Available at the link:
http://www.gov.cn/xinwen/2021-03/08/content_5591373.htm the date visit: 4 May

(2) Nan Tian, Alexandra Kuimova,Op.cit,p.3.

قطباً مهيمنا في النظام الدولي، رغم إن الكثير من المختصين في مجال السياسة الدولية لم يقروا بهذا الوضع –احادي القطبية– إذ تملك الولايات المتحدة عناصر القوة الاقتصادية والعسكرية والسياسية أضافة إلى النفوذ السياسي والتواجد العسكري في مناطق حيوية كثيرة ، ومن المنظور الصيني فأن البيئة الدولية شهدت في مرحلة ما بعد الحرب الباردة خمسة ملامح اساسية :هي إن الولايات المتحدة تشكل تهديدا للصين نتيجة الخلاف المستمر معها، تعتبر اليابان قوة اقتصادية أكثر استقلالية ولديها صلات تجارية مع الصين ومع أمريكا أيضا ويجب الحفاظ على تلك العلاقة (الصينية مع اليابان) ، ظهور دول آسيوية مناهضة للصين وحليفة للولايات المتحدة الأمريكية كوريا الجنوبية ودول جنوب شرق اسيا(كمبوديا إندونيسيا الفلبين ميانمار تايلاند ماليزيا ...الخ) أضافةً إلى التقدم العسكري والاقتصادي للهند، واخيراً بروز خطر دول إسلامية غير مستقرة نسبيا على حدود الصين في اسيا الوسطى*، قد تشكل خطرا على الاقليات الاسلامية في الصين نتيجة انهيار الاتحاد السوفيتي السابق. ورغم إن السياسة الأمريكية تسعى لعلاقة تعاونية مع الصين، إلا أنَّ بعض الجهات الحكومية الامريكية تدعو إلى إتباع سياسة أكثر حزما تجاه الصين (١).

ولكن منتصف التسعينيات تقريبًا أدرك صنّاع القرار الصينيون أن الموقع الريادي للولايات المتحدة لن يتزعزع، وأن قوتها الوطنية الشاملة لن تضاهيها أي دولة بمفردها في المستقبل المنظور، لذا يمكن اعتبار بداية التسعينات فترة ظهور نظرية التهديد الصيني للولايات المتحدة (التي تقوم على العداء للغرب) في ظل النمو الاقتصادي المتصاعد، إذ تسعى الدولة الأكثر ثراءً وقوة إلى مد نفوذها الاقليمي والدولي، الذي ينعكس على ترتيب القوة على المستوى الدولي، وظهرت مدرستان حول التهديد الصيني للولايات المتحدة الاولى: متأثرة بالتوجه الواقعي حيث يرى مؤيدو هذا التوجه إن الصين تهدف إلى الهيمنة من وراء صعودها، كما فعلت الولايات المتحدة لذا ستسعى الصين لاحتواء اليابان وكوريا الجنوبية، من خلال تطوير قوة عسكرية لن تستطيع باقي

* الدول الإسلامية التي استقلت بعد انهيار الاتحاد السوفييتي ست جمهوريات، واحدة منها هي أذربيجان التي تقع في القوقاز، والخمس الباقية تقع في منطقة آسيا الوسطى، وهي أوزبكستان، كازاخستان، تركمانستان، ومنها قيرغيزستان، طاجيكستان مجاورة للصين

(١) صفاء حسين علي الجبوري، مصدر سبق ذكره، ١٥٤–١٥٥ .

الدول التصدي لها، بينما ترى المدرسة الليبرالية: إن سلوك الصين السياسي والعسكري يمكن تقييده من خلال المؤسسات الدولية [١].

لقد أدت التغيرات في بنية النظام الدولي، إلى وضع العلاقة الصينية- الأمريكية في مستوى جديد، حيث تحاول الولايات المتحدة الحفاظ على مكانتها الدولية لأطول فترة ممكنة، لتأتي أحداث ١١ ايلول التي اثارت التساؤلات والشكوك حول قدرة الولايات المتحدة للحفاظ على مكانتها في قمة الهرم الدولي، مقابل صعود بعض الدول على رأسها الصين، كل ذلك أثار جدلاً داخل الولايات المتحدة حول أسلوب التعامل مع الصين، ما بين الحذر من تنامي قوتها العسكرية، ورغبة الصين في قيادة آسيا، وبين الانفتاح على الصين وتوسيع العلاقات الاقتصادية والحوارات الدبلوماسية [٢]. وترى الدراسة أن مرحلة ما بعد الحرب الباردة تُعد بداية مرحلة جديدة للصين لأخذ دور يناسب إمكاناتها السكانية ،الاقتصادية والعسكرية بعد أن ترك الاتحاد السوفيتي السابق فراغاً على الساحة الدولية، لذا وجدَت الصين نفسها في صدارة الدول للحد من الهيمنة الأمريكية عن طرق التنافس التجاري، بمعنى أن هذه المرحلة شكلت بداية الصعود الصيني، الذي طالما تسعى الصين ليكون سلمياً، والذي تقابلهُ الاستراتيجية الامريكية التي تراوح بين احتواء الصين عن طريق التعاون أو ممارسة الضغط وعزل الصين عن دول المنطقة احياناً اخرى .

ثانيا: الاستراتيجية الأمريكية تجاه الصين خلال أدارة الرئيسين دونالد ترامب (٢٠١٦-٢٠٢٠) وجون بايدن

يمكن وصف الاستراتيجية الامريكية تجاه الصين في عهد أدارة الرئيس السابق (دونالد ترامب) بالتشدد وخاصة في مجال الاقتصادي وحقوق الانسان، حيث جاء في البيان الصحفي نهاية عام ٢٠٢٠ (لمايكل بومبيو) سكرتير الرئيس الامريكي للشؤون الخارجية، الخاص بفرض عقوبات من قبل وزارة الخارجية الامريكية، على دخول مسؤولين من الحزب الشيوعي وعائلاتهم إلى الولايات المتحدة، "لن تقف الولايات المتحدة مكتوفة الأيدي بينما ينفذ الحزب الشيوعي الصيني

(١) سالي نبيل شعراوي، العلاقات الصينية الأمريكية وأثر التحول في النظام الدولي، القاهرة، العربي للنشر والتوزيع، ٢٠١٧، ص٩١.

(٢) السيد امين شلبي، هل الصعود الصيني تهديد للولايات المتحدة.، مجلة السياسة الدولية، القاهرة، مركز الاهرام للدراسات الاستراتيجية. العدد ١٦٥، ٢٠٠٦، ص٢٩.

انتهاكات حقوق الإنسان التي تستهدف (الأويغور) والعرقيين (الكازاخيين) وأفراد الأقليات الأخرى في (شينجيانغ)..." [١]. بالمقابل أعلنت الصين عقوبات على كبار الجمهوريين ومن بين المستهدفين السناتور (تيد كروز) و(ماركو روبيو) وكلاهما منتقد صريح لسياسة الصين [٢]. وفي عهد أدارة الرئيس (جون بايدن) الذي تسلم الرئاسة في ٢٠٢١ يقول: (**Max Baucus**)* "إن العلاقة بين الولايات المتحدة والصين لن تتغير كثيرًا على المدى القصير في عهد الرئيس (بايدن) الذي تركز أدارته على الاقتصاد المحلي... هناك العديد من الاسباب المتسببة بين الصين والولايات المتحدة ؛ بما في ذلك عدد قليل من الأمريكيين الذين زاروا الصين، وهم لا يعرفون الصين حقا..." [٣]. وهذه أشاره الى ان الإدارة الأمريكية لا تعرف الكثير من التفاصيل عن حياة الصين عن كثب، ويحث السفير (Baucus Max) المسؤولين والسياسيين الأمريكان الى التعرف جيد على طبيعة وثقافة الصين لصنع سياسة واضحة ومدركة لمكانة الصين الدولية في الوقت الحاضر.

من خلال ما تقدم يمكن القول أنه توجد العديد من النظريات التي تفسر العلاقة الصينية-الامريكية في اطار الامن الاقليمي، ومنها "نظرية تحول القوى"، فعلى سبيل المثال يقول: (Aaron Friedber)* في تحليله للعلاقة الثنائية بين البلدين "إن تاريخ العالم مليء بأمثلة من العلاقات

---

(١) للتفصيل ينظر: البيان الصحفي لسكرتير الرئيس الأمريكي دونالد ترامب للشؤون الخارجية مايكل ريتشارد بومبيو بشأن الفظائع في شينجيانغ، ١٩كانون الثاني ٢٠٢١. متاح على الموقع: تأريخ الزيارة ٣شباط ٢٠٢١.
https://2017-2021.state.gov/determination-of-the-secretary-of-state-on-atrocities-in-xinjiang/index.html

(2) BBC News, China sanctions 11 U.S. officials on Hong Kong issue, the parties dismissed it, August 11, 2020.

متاح على الموقع الزيارة https://www.bbc.com/zhongwen/trad/chinese-news-53738020
٥ شباط ٢٠٢١

* (Max Baucus) السفير الامريكي لدى الصين (٢٠١٤- ٢٠١٧). للتفصيل ينظر: تصريح السفير الامريكي لدى الصين، الموقع الرسمي لوزارة الخارجية الأمريكية، متاح على الموقع: تأريخ الزيارة ٥شباط ٢٠٢١
https://2009-2017.state.gov/r/pa/ei/biog/221450.htm

(٣) العربية CRL online مقابلة خاصة مع ماكس بوكس سفير الولايات المتحدة السابق لدى الصين، متاح على الموقع:

تأريخ 17:54:14 2020-07-18 http://arabic.cri.cn/video/3189/20200718/508525.html
الزيارة ٦شباط ٢٠٢١

* هارون فرايدبيرغ، مواليد ١٩٥٦ أستاذ السياسة والشؤون الدولية ، جامعة برينستون ، الولايات المتحدة الأمريكية .

المضطربة بين القوى الصاعدة والمهيمنة" [١]. حيث أن القوى الصاعدة تسعى لتغيير الحدود الاقليمية والتراتبية السائدة في النظام الدولي بينما تركز القوى المهيمنة على الحفاظ على الوضع القائم بكافة السبل، آخذاً في الاعتبار تزايد التدخل الأمريكي في الدول المجاورة للصين بشكل غير مسبوق [٢].

وبذلك تشكل العلاقات الصينية – الامريكية نمطاً فريداً من العلاقات الثنائية، بما تتضمنهُ من عناصر متناقضة مثل الصراع والتعاون والاستقلالية والاعتماد المتبادل، وتسعى كل منهم للعمل في اطار توازن دقيق من المصالح المتبادلة يحكمها العامل الاقتصادي.

المطلب الثالث: اهم القضايا المؤثرة على العلاقات الصينية الامريكية

تتنافس الولايات المتحدة والصين في الفضاء الالكتروني، لتأمين قدراتها في مجالات مهمة ومنها التكنولوجيا، أنهم يتنافسون في مجالات عدة ومنها التجارة الالكترونية، سنحاول في هذا المطلب أن نوضح أبرز القضايا الاقتصادية والسياسية المؤثر على العلاقة الصينية – الامريكية.

أولاً: **التنافس التجاري بين الصين والولايات المتحدة.**

العديد من القضايا أصبحت مجال للتنافس والخلاف بين البلدين ؛ نتيجة التحول في نوع وادوات القوة وليس مجرد التحول من محور الى آخر [٣]، بناءً على هذه المفاهيم النظرية يعتبر التنافس التجاري، أهم القضايا الخلافية بين الصين والولايات المتحدة ويخضع لقانون الدولة الأولى بالرعاية منذ عام ١٩٨٠ الذي منحته الولايات المتحدة للصين، وهذا التبادل يعد تفاعل تعاوني ألا أنه أتخذ نمط التنافس بدل التعاون، عندما أتهمت الولايات المتحدة الصين بالعمل على إغراق السوق الامريكية بالسلع الصينية مما أدى الى تدهور العلاقة بينهم، خاصة بعد أن وصل العجز

(1) Miles Kahler, the rise of emerging Asia: regional peace and global security, by the Peterson Institute for International Economics and the Asian Development Bank Institute, working paper series, May 2013,p.4.

(٢) سالي نبيل شعراوي، مصدر سبق ذكره،ص١٨٥.

(3) Sangbae Kim, US-China Competition in Cyberspace A Perspective of Emerging Power Politics and Platform Competition,The East Asia Institute (EAI), January 2019,p.2

التجاري للولايات المتحدة بحدود (٦١٢) مليار عام ٢٠١٨ [١]. وفيما يلي جدول يبين حجم التبادل التجاري بين البلدين.

جدول رقم (٣) يبين حجم التبادل التجاري بين الصين والولايات بين (١٩٨٠- ٢٠٢٠) الارقام بالمليارات

السنة	الصادرات الامريكية (مليار دولار)	الواردات الامريكية (مليار دولار)
١٩٨٠	٣،٨	١،١
١٩٩٠	٤،٨	١٥،٢
٢٠٠٠	١٦،٣	١٠٠،١
٢٠١٠	٩١،٩	٣٦٤،٩
٢٠٢٠	٦٧٣	٧١١

المصدر: الجدول من اعداد الباحث The Economic Times News, China overtakes US as EU's biggest trading partner, February 15, 2021. Available at the link: https://economictimes.indiatimes.com/news/international/business date of the visit March 13, 2021.

والجدول أعلاه يبين إن حجم التجارة مع الصين بلغ (٧١١) مليار دولار في نهاية ٢٠٢٠ مقارنة مع (٦٧٣) مليار دولار للولايات المتحدة.

ويُظهر تقرير صندوق النقد الدولي أن اقتصاد الصين أصبح أكبر من الاقتصاد الأمريكي بما يعادل (٢٤,٢ تريليون دولار للصين مقابل ٢٠,٨ تريليون دولار لأمريكا) نهاية عام ٢٠٢٠ [٢]. وبسبب النمو السريع للصين والذي تعتبره الولايات المتحدة يشكل تنافس وتهديداً كبير لاقتصادها ومكانتها، لذا بدأت أول مظاهر الحرب التجارية بين البلدين، في الحملة الانتخابية للرئيس(دونالد

(١) باهر مردان، مصدر سبق ذكره، ص٧.

(2) Graham Allison, China Is Now the World's Largest Economy. We Shouldn't Be Shocked, Harvard Kennedy School, Belfer Center for science International Affairs, Cambridge, October 15, 2020,Available at the link: https://nationalinterest.org/feature/china-now-world%E2%80%99s-largest-economy-we-shouldn%E2%80%99t-be-shocked-170719t.Date the visit February 6 2021

ترامب) سنة ٢٠١٦ حيث وعد برفع قيمة الضرائب الجمركية على البضائع الصينية، وذلك لمعالجة العجز التجاري الامريكي [١].

جدول رقم (٤) يبين اكبر اقتصاديات الدول لعام ٢٠١٨

ت	الدولة	القيمة بالترليون
١-	الولايات المتحدة	٢٠,٤
٢-	الصين	١٤
٣-	اليابان	٥,١
٤-	المانيا	٤,٢
٥-	المملكة المتحدة	٢,٩٤
٦-	فرنسا	٢,٩٣
٧-	الهند	٢,٨٥
٨-	ايطاليا	٢,١٨
٩-	البرازيل	٢,١٤
١٠	كندا	١,٨

Source: International monetary Fund,2018 (IMF).

من جانب آخر يُعد مشروع الحزام والطريق (طريق الحرير) وهو البُعد الاكثر خطورة في الصراع الامريكي- الصيني، بما يشكلهُ من تهديد للمصالح الأمريكية في آسيا والشرق الاوسط وأفريقيا وأُوروبا، والذي يُعد بديل عالمي عن منظومة الطرق التي تربط أوروبا بالشرق واليابان، حيث تُسيطر عليه الولايات المتحدة، أضافة الى تركيز الصين جهودها في مجال البحث العلمي

(1) Lucia Mutikani Reporting, The U.S. trade deficit surged to a 10-year high in 2018, Fox Business, March 6, 2019. Available at Link: https://www.foxbusiness.com/economy/us-trade-deficit-jumps-to-10-year-high-in-2018 تأريخ الزيارة ٢٢شباط ٢٠٢١

والابتكار من خلال زيادة الأنفاق على العلوم والتكنولوجيا حيث بلغ ما يقارب (2.09%) من أجمالي الناتج المحلي عام ٢٠١٤ حسب تقرير اليونسكو [١].

كل هذه المؤشرات تجعل الولايات المتحدة تخشى صعود الصين وتنامي دورها في منطقة الشرق الأوسط، وتطور قوة الصين الاقتصادية التي تنعكس على القوة العسكرية – من خلال زيادة الأنفاق العسكري* – وبالتالي مكانتها الدولية، ولغرض الحد من المنافسة الصينية روج مستشار الأمن القومي (Herbert Raymond McMaster)** للرئيس (دونالد لترامب) لمبدأ "النهج التنافسي تجاه الصين" باعتباره أكبر تحول في السياسة الخارجية للولايات المتحدة مُنذ الحرب الباردة، ومن أجل المنافسة الفعلية يتعين على واشنطن أن تتفوق على المنافسة الصينية، وليس التقليل من شأنها فقط [٢].

وفي إطار تحسين العلاقات التجارية ومحاولة الحد من تصاعد التنافس التجاري، تم توقيع الاتفاقية الاقتصادية والتجارية بين البلدين في ١٥ كانون الثاني عام ٢٠٢٠، حيث وصف الرئيس الامريكي (دونالد ترامب) الاتفاق قائلا: "أن ما جرى أكبر من مجرد اتفاق، نحن أدخلنا تغييرات واسعة على التجارة الدولية... حيث أصبح لدى الأميركيين حكومة تضمن مصالحهم في المقدمة"

---

(١) كونج كاو، تقرير اليونسكو للعلوم، ٢٠١٥، ص ٥٩٦. متاح على الموقع:
https://ar.unesco.org/sites/default/files/usr15_china_ar.pdf
تأريخ الزيارة ٢٥شباط ٢٠٢١.

* بلغ الأنفاق العسكري الصيني لعام ٢٠١٩ (٢٦١مليار دولار) للتفصيل ينظر: Nan Tian, Alexandra – Kuimova, Diego lopes da silva, and others, Trends In World Military Expenditure 2019, Stockholm International Peace Research Institute (SIPRI), April 2020, p.3.

** Herbert Raymond McMaster لذي شغل منصب مستشار الأمن القومي رقم ٢٦ للولايات المتحدة من ٢٠كانون الثاني ٢٠١٧ إلى ٩ نيسان ٢٠١٨. للتفصيل ينظر: Peter Baker and Michael R .Gordon, Trump Chooses H.R. McMaster as National Security Adviser, The New York Times, Feb. 20, 2017,- Available at the lin: https://www.nytimes.com/2017/02/20/us/politics/mcmaster-national-security-adviser-trump.html Visit date April. 12, 2012.

(2) Evan A. Feigenbaum, Meeting the Challenge in Asia, journal National Interest Newsletter, December 22, 2020,,pp.1-5. Available at:Date visit at 26 February: https://nationalinterest.org/feature/meeting-challenge-asia-174917

[١].وقد تضمن الاتفاق موضوعات الملكية الفكرية، ونقل التكنولوجيا وتجارة المواد الغذائية والمنتجات الزراعية، والخدمات المالية والسياسات الاقتصادية والعملات وآلية فض المنازعات التجارية، حيث وافقت الصين بموجب هذا الاتفاق على زيادة وارداتها من المنتجات والخدمات الأميركية بما لا يقل عن (٢٠٠) مليار دولار خلال العامين المقبلين عما كانت عليه حجم الواردات عام ٢٠١٧، كما ستعيد الولايات المتحدة النظر في الكثير من الرسوم المفروضة على الواردات الصينية [٢]. وقال الرئيس الامريكي(دونالد ترامب) بهذا الخصوص "سنُبقي الرسوم الجمركية، لكنني سأوافق على إلغائها إذا توصلنا إلى إبرام المرحلة الثانية سأبقيها وإلا فلن يكون لدينا أي ورقة للتفاوض" [٣].

وتُعد تصريحات وزير الخارجية الصيني (Wang Bi) في المؤتمر الصحفي عن سياسة الصين التجارية تجاه الولايات المتحدة، عن" الحرب التجارية مع الولايات المتحدة " تأكيداً على سياسة الصين السلمية وتجنب المواجهة مع الولايات المتحدة ،حيث أكد على نقاط مهمة [٤]:

١- سيعمل الجانبان على توسيع التعاون في مجالات واسعة على أساس المنفعة المتبادلة والكسب المشترك وحسن أدارة الخلافات.

٢- ستلتزم الصين بطريق التنمية الذي اختارتهُ بنفسها، وتكون تنمية الصين ونهضتها أمراً لا يمكن التراجع عنه.

٣- يعتقد البعض أن الصين ستحل محل الولايات المتحدة على المسرح الدولي، وهذا الحُكم غير دقيق، إذ أن الصين تسير في طريق الاشتراكية ذات الخصائص الصينية.

---

(١) تصريحات الرئيس الأمريكي دونالد ترامب وتصريح وزير الخزانة الامريكي ستيفن منوتشين، حول اتفاق التجارة الأميركي- الصيني متاح على الموقع:.https://www.aljazeera.net/ebusiness/2020/1/16 تأريخ الزيارة ٢٣شباط ٢٠٢١.

(2) ECONOMIC AND TRADE AGREEMENT BETWEEN THE GOVERNMENT OF THE UNITED STATES OF AMERICA AND THE GOVERNMENT OF THE PEOPLE'S REPUBLIC OF CHINA, On January 15, 2020,p.3.

(٣) تصريحات الرئيس الامريكي دونالد ترامب، مصدر سبق ذكره.

(٤) المؤتمر الصحفي الذي عقدته الدورة الأولى للمجلس الوطني الثالث عشر لنواب الشعب بتأريخ ٨ أذار ٢٠١٨ في المركز الاعلامي الخاص بالمجلس، حيث دعت وزير الخارجية الصيني (Wang Bi) للإجابة على أسئلة الصحفيين الصينين والاجانب. حول سياسة الصين الخارجية وعلاقاتها الدولية.

ثانياً: قضية تايوان:

كانت ولا تزال قضية تايوان إحدى أهم القضايا التي تؤرق العلاقة الأمريكية-الصينية، ويمكن اعتبارها كذلك ورقة ضغط أمريكية على الصين، لا تختلف كثيراً عن قضايا حقوق الإنسان، والتي تحاول الولايات المتحدة إبرازها من حين لآخر من أجل تحقيق مصالحها، مخالفة بذلك الموقف الصيني الذي يعتبر تايوان جزءاً لا يتجزأ من الأُمة الصينية، وقد أوضح الرئيس الصيني (شي جين بينغ ٢٠١٣- ٠٠٠) للرئيس (دونالد ترامب) عند زيارة الأخير للصين في تشرين الثاني ٢٠١٧ "تأمل الصين أن يواصل الجانب الأمريكي الالتزام الصارم بمبدأ "الصين الواحدة"، ويمنع حدوث اضطرابات للصورة الأوسع للصين والولايات المتحدة" [١]. مقابل ذلك أبلغ الرئيس الامريكي (ترامب) الرئيس الصيني شي جين بينغ بأن حكومة الولايات المتحدة أيدت وتمسكت بسياسة "صين واحدة"، وكانت وزارة الدفاع الصينية قد حذرت الولايات المتحدة "بتوخي الحذر في خطابها وتصرفاتها"، مثلا صفقة بيع الولايات المتحدة إلى تايوان في ٩كانون الاول ٢٠٢٠ مُعدات الاتصالات العسكرية بقيمة (٢٨٠) مليون دولار، وقد عارضتها الصين بشدة [٢]. وهذه الصفقة تنتهك مبدأ "صين واحدة" و"البيانات المشتركة الثلاثة"* بين الصين والولايات المتحدة، وخاصة بيان ١٧ آب، حسب تصريح (هوا تشون وانغ) المتحدثة باسم الخارجية الصينية [٣]. ورغم كل ما تبذلهُ

---

(1) Reporting by Ben Blanchard, Taiwan the most important issue in Sino-U.S. ties, China's Xi tells Trump, Reuters, NOVEMBER 9, 2017.Available at Link: https://www.reuters.com/article/us-trump-asia-china-taiwan/taiwan-the-most-=important-issue-in-sino-u-s-ties-chinas-xi-tells-trump-idUKKBN1D90YI Date visit at 25 January 2021.

(2) Chen Zhuo, China Military On lin, Op. cit ,p. 2.

* البيانات المشتركة الثلاثة:هي عبارة عن مجموعة من ثلاثة بيانات مشتركة أصدرتها حكومتا الولايات المتحدة وجمهورية الصين الشعبية (P.R.C.) عام ١٩٧٢، ١٩٧٩، ١٩٨٢ وقد لعبت هذه البيانات الرسمية دورًا مهمًا في إقامة العلاقات بين الولايات المتحدة وجمهورية الصين الشعبية. وتكون عنصرا أساسيا في الحوار بين الدولتين). للتفصيل ينظر: Three Communiqué.

The Date visit at 29Fubrury 2021:

https://en.wikipedia.org/wiki/Three_Communiqu%C3%A9s Available at link:

(3) Li Jiayao,US blasted for military gear sales to Taiwan, China Daily,9-12-2020. Available at link: http://eng.chinamil.com.cn/view/2020-12/09/content_9949984.ht

الولايات المتحدة من دعم لحكومة تايوان، فأنها ليست مستعدة لخوض حرب مع الصين من أجلها، ويعتبر حادث السفينة (USS John P. Murtha)** افضل دليل على ذلك [١].

ثالثاً: حقوق الإنسان:

تعد قضية حقوق الإنسان من أكثر القضايا إثارة للجدل في العلاقة بين الولايات المتحدة والصين، وينتقد ممثّلي المنظمات غير الحكومية الأمريكية ووسائل الإعلام والحكومة المعاملة السيئة من قبل الحكومة الصينية للمنشّقين والجماعات الدينية والسجناء في الداخل، أما على المستوى الخارجي فقد عبّر عن ذلك سكرتير الرئيس الامريكي للشؤون الخارجية (بلينكن) عام ٢٠٢١،بقوله "تستخدم الصين الإكراه والعدوان لتقويض الحكم الذاتي بشكل منهجي في هونغ كونغ، وتقويض الديمقراطية في تايوان، وانتهاك حقوق الإنسان في شينجيانغ والتبت*..." [٢].

وتزعم الولايات المتحدة أن هذه السياسة تقوم على انتهاك حقوق الإنسان المعترف بها دوليًا، وتتمثّل انتقادات الولايات المتحدة لحقوق الانسان في الصين، من خلال التقييد على حريات النشطاء السياسيين، فرض قيود على الانترنيت، استغلال الدولة للقانون والنظام القضائي لتجريم حرية التعبير، وسيطرة الدولة ورقابتها على الممارسات الدينية [٣]. ويمكن اعتبار القمع العنيف ضد

** وهي سفينة نقل برمائية امريكية تعمل برفقة السفن التجارية في مضيق تايوان تم اغراقها بالخطأ (حسب ادعاء الصين) بواسطة صاروخ صيني مضاد للسفن اثناء تدريبات تجريها الصين تسبب بمقتل ٨٠٠ من البحرية الأمريكان دون الرد على الصين. للتفصيل ينظر: غراهام أليسن، مصدر سبق ذكره.

(١) غراهام أليسون، مصدر سبق ذكره، ص ص٣٣٨-٣٤٠.

* نص التصريح باللغة الإنكليزية (And China uses coercion and aggression to systematically erode autonomy in Hong Kong, undercut democracy in Taiwan, abuse human rights in (Xinjiang and Tibet

(2) A message from the US State Department/East Asia and Pacific Division on the researcher's mail is listed in the appendix., Secretary Antony J. Blinken, Secretary of Defense Lloyd Austin, Japanese Foreign Minister Toshimitsu Motegi, and Japanese Defense Minister Nobua Kishi at a Joint Press Availability, March 16, 2021 للتفصيل ينظر: نص الرسالة ضمن الملحق رقم (٤)

(3) Andrew J. Nathan, professor of Chinese politics at Columbia University, U.S.-China Relations Since 1949, New York: W.W. Norton, 1997, p.1. Available at link: http://afe.easia.columbia.edu/special/china_1950_us_china.htm.Date visit 15 March 2021

الطلاب المتظاهرين في بكين في ٤ تموز ١٩٨٩- ما يسمى بحادث " تيانانمين"** الحدث الأبرز الذي جعل حقوق الإنسان كقضية خلاف بين الولايات المتحدة والصين، وترى الصين إن هدف الولايات المتحدة هو الهيمنة وليس دعم مبادئ حقوق الانسان، ومتجاهلة بذلك نصوص القانون الدولي الخاصة بعدم التدخل في الشؤون الداخلية للدول [١].

رابعاً: تغير المناخ:

تشير الاحصاءات الخاصة بالتلوث، إن كل من الولايات المتحدة والصين يتسببان بنسبة (٤١%) من انبعاثات غاز ثاني أوكسيد الكاربون عالمياً، وهي السبب الرئيسي للاحتباس الحراري، وقد تعهد كلا الطرفين بتقليل نسبة الانبعاثات إلى اقل مستوى ممكن، رغم إن الرئيس الامريكي (دونالد ترامب) لم يكن ملتزما كثيراً باتفاقيات المناخ والتلوث، ويتجلّى ذلك في تصريح الرئيس الفرنسي (ماكرون) عند تنصيب الرئيس الامريكي (جون بايدن) في٢٠ كانون الثاني ٢٠٢١ أذ أعرب عن تفاؤله بعودة واشنطن الى أتفاق باريس حول المناخ [٢].

وفي هذا السياق قال: (جينغدون يوان)، كبير الباحثين في معهد ستوكهولم الدولي لأبحاث السلام "سيبري" "إن إدارة الرئيس (بايدن) ستكون منفتحة مع الصين بشأن مسألة تغير المناخ، بينما لا تزال "حازمة في مجالات التجارة والتكنولوجيا والأمن الإقليمي" [٣]، وهناك أسباب متنوعة لهذه المخاوف، حيث يشعر بعض الخبراء المهتمين بالأمن بالقلق، من أن إدارة الرئيس الأمريكي

** مظاهرات ساحة تيانانمن أو تُعرف باسم حادثة الرابع من يونيو هي مجموعة من المظاهرات الوطنية التي وقعت في جمهورية الصين الشعبية، بين ١٥ أبريل، ١٩٨٩ و٤ يونيو، ١٩٨٩، وتمركزت في ساحة تيانانمن في بكين التي كانت محتلة من قبل طلاب جامعيين صينيين طالبوا بالديمقراطية والإصلاح، وقد استعملت الحكومة القوة المفرطة في انهاء المظاهرات مما نتج عنه الكثير من الضحايا والمعتقلين. للتفصيل ينظر: Tanks roll into Tiananmen Square (4 June 1989) - BBC Newsnight.Available at link: https://www.youtube.com/watch?v=KrYGiwhOuBo The date at 28 April 28, 2021

(١) سالي نبيل شعراوي، مصدر سبق ذكره، ص١٣٣.

(2) White House Direct Publication, Joseph R. Biden Jr. officially announces. acceptance of the Pars Accord, concluded on December 12, 2015,January 20,2021. ملحق (٧)

(٣) رياض الخالق، اجتماع "ألاسكا" فرصة لإنعاش العلاقات الأمريكية الصينية، وكالة الاناضول. ١٨ أذار ٢٠٢١.متاح على الموقع:https://www.aa.com.tr/ar تأريخ الزيارة ٢٨نيسان ٢٠٢١.

(بايدن) ستعطي الأولوية للتعاون مع الصين بشأن قضايا المناخ فوق الاهتمامات الاستراتيجية الأخرى، رغم تأكيد الرئيس (بايدن) – في خاطب دليل الأمن القومي الأمريكي المؤقت سنة ٢٠٢١ – على أزمة المناخ واعتبارها من أولويات الاستراتيجية الأمريكية [١]. إذ يخشى مؤيدو النظر إلى العلاقة بين الولايات المتحدة والصين على أنها صراع أيديولوجي راسخ، من أن التعاون يمكن أن يُضعف التركيز على ما يصفونه بطموحات كل جانب التي لا يمكن التوفيق بينها، وأعرب البعض عن مخاوفهم من أن بكين ستمنع التعاون في قضايا المناخ ما لم تحصل على تنازلات أمريكية في مجالات أخرى من العلاقة بينهما، على سبيل المثال، في هونغ كونغ أو شينجيانغ، وهذا يتناقض مع وجهة نظر المبعوث الرئاسي الأمريكي الخاص لشؤون المناخ، (جون كيري) والمبعوث الصيني الخاص لتغير المناخ (شيه جينهوا) في اجتماع شنغهاي يومي ١٥ و ١٦ نيسان ٢٠٢١ لمناقشة جوانب أزمة المناخ واكد المبعوثان على التزام الولايات المتحدة والصين بالتعاون مع بعضهما البعض ومع الدول الأخرى لمعالجة أزمة المناخ ، التي يجب معالجتها بالجدية والإلحاح اللذين تطلبهما، والعمل معًا ومع الأطراف الأخرى لتعزيز تنفيذ اتفاقية باريس [٢].

وترى الدراسة أن الخطورة التي يشكلها تغير المناخ وأثاره على البيئة، تكمن في تعامل الولايات المتحدة والصين في هذه المسألة من زاوية المصالح والتنازلات المتبادلة، وليس من زاوية الاثار السلبية الحقيقية المترتبة على الانبعاثات وأثرها على المناخ، بمعنى ان الطرفين يتخذ من قضية المناخ ورقة للتفاوض لتحقيق المصالح، وليس لإيجاد حل حقيقي لانبعاثات الحرارة المؤثرة على المناخ.

خامساً: مبادرة الحزام والطريق:

منذ بدأ التخطيط لمبادرة الحزام والطريق في عام ٢٠١٣، كان تطوير البنية التحتية للسكك الحديدية الصينية أمرًا حاسمًا في نهج بكين للاستثمار في جنوب شرق آسيا، وفي كتابهم الأخير

(1) President Joseph R. Biden, Jr. Interim National Security Strategic Guidance, The White House, Washington March 2021,p.7.

(2) US Department of State, OFFICE OF THE SPOKESPERSON, U.S. –China Joint Statement Addressing the Climate Crisis, April 17, 2021.Available at link: https://www.state.gov/u-s-china-joint-statement-addressing-the-climate-crisis . The date visit 5 July 2021, 01:20 .

(أنهار الحديد: السكك الحديدية والقوة الصينية في جنوب شرق آسيا) يبين كل من (لامبتون وكويك) الدوافع والآثار المترتبة على هذا التطور، الذي تشكله البنية التحتية الصينية، فضلاً عن ردود الفعل المتنوعة المتمثلة بموقف الولايات المتحدة الامريكية من مشروع السكك الذي يمر عبر جنوب شرق آسيا، وقد اصبحت مبادرة الحزام والطريق محور السياسة الخارجية (لشي جين بينغ)، فهي إذ تمتد من بحر الصين الجنوبي في الكتلة الأرضية الاوراسية (أوروبا وآسيا) [١] ،لتشمل أغلب مناطق آسيا، لذا يمكن القول إنها خطة التنمية الأكثر طموحاً من أي وقت مضى، وتصف بكين إن هذه المبادرة ستفكك حواجز الاستثمار، وتنشئ مسارات تجارية جديدة، وتحسن الخدمات اللوجستية الدولية، وتعزز التكامل المالي الإقليمي، أضافة إلى تعزيز "السلام العالمي"[٢].

ولا تزعم الصين أي ملكية لهذه المبادرة، على الرغم من إن المبادرة هي في الواقع مشروع صيني إلى حد كبير، من جانب اخر تُعتبر هذه المبادرة قناة استثمار بِديلة لاحتياطات الصين من العُملات الاجنبية التي بلغت اكثر من (٣٢١٦) مليار دولار نهاية عام ٢٠٢٠ في سندات الخزانة الامريكية [٣].

سادساً: فايروس كورونا (COVID-19)

انتشر فيروس كورونا (COVID-19) الذي بدأ في مدينة ووهان الصينية منتصف تشرين الثاني ٢٠١٩، وفي الولايات المتحدة ظهرت الاصابة الأولى في ولاية واشنطن في ١٥ كانون الثاني سنة ٢٠٢٠، وقد تبادل الطرفين ألقاء اللوم على بعضهما البعض لانتشاره السريع والمدمّر، ومن خلال الاتهامات المتبادلة، يسعى كل طرف لإضعاف الآخر وتحقيق مكاسب سياسية، حيث تسعى الولايات المتحدة القيام بإجراءات تضعف او تهزم الصين في منطقة شرق اسيا وعزلها عن العالم، وذلك في خطوة للحد من الطموح الصيني للهيمنة على المنطقة اقليمياً [٤].

---

(١) توم ميلر، الحلم الآسيوي للصين "بناء إمبراطورية على طول طريق الحرير الجديد"، ترجمة عبد الرحمن الياس، ط١، قنديل للطباعة والنشر، دبي، ٢٠١٩، ص ص٥٥-٥٦.

(2) David M. Lampton And others, Chinese Infrastructure Development in Southeast Asia, The lecture was given by the Stimson Center, November 16, 2020 .

(٣) توم ميلر، مصدر سبق ذكره، ص٥٧.

(٤) سالي نبيل شعراوي، مصدر سبق ذكره ص، ص١٧٩-١٨٠.

لقد حاول الرئيس الامريكي (دونالد ترامب) تشتيت الانتباه، حول عدم قدرة الحكومة الأمريكية على السيطرة على الفايروس، من خلال أطلاق الاتهامات على الصين، فتارة اطلق تسمية (الفايروس التاجي) على فايروس كورونا، وفي أحيان أخرى أطلق اسم فايروس (ووهان) [١]. ويرى البعض أن فايروس كورونا ما هو إلا جزء من نظرية المؤامرة ،وآخرون يروجون على أنه سلاح بيولوجي تم تصنيعه في المختبرات،- والدراسة تؤيد الرأي الأخير- وهذا أن صح ينذر بحرب جرثومية بدل الحرب التقليدية) الأسلحة والقوة العسكرية [٢]. لقد أظهرت أزمة فايروس كورونا ضعف الادارة الأمريكية في التعامل مع الأزمة، مما يضعف مكانة الولايات المتحدة عالميا، وقد برز دور الدبلوماسية الصينية وقوتها الناعمة من خلال المساعدات التي قدمتها للدول الاخرى، فالصين ذات النظام السياسي الشمولي كانت أكثر فاعلية من الدول الغربية في التعامل مع أزمة فايروس كورونا، مما عزز مكانتها العالمية. وتُعد المساعدات أداة "هجومية" مهمة في فن الحكم الاقتصادي الأمريكي، هكذا تنظر الولايات المتحدة إلى المساعدات الصينية لدول ضمن الفلك الأمريكي، هي أداة اقتصادية من ضمن أدوات القوة الناعمة [٣].

وكان للفايروس أثاره الاقتصادية على العالم، أكثر مما سببته الأزمة المالية سنة ٢٠٠٨ وتسبب فايروس كورونا بوفاة ما يقارب من (٥،١٠٤،٨٩٩) مليون شخص لغاية يوم ١٦ تشرين الثاني ٢٠٢١ [٤]، حيث أدى الى تباطؤ النمو الاقتصادي الصيني لعام ٢٠٢٠ كما توقعت وكالة

---

(1) Carla A. Hills, The Impact of the Coronavirus on US-China Relations, China US Focus, Apr 10,2020. Available at link: https://www.statista.com/statistics/278206/foreign-exchange-reserves-of-china/. The date of visit is 13 March 2021.

(٢) هالة محمود طه دودين، العلاقات الصينية الأمريكية ما بين الحرب التجارية وفايروس كورونا، المركز الديمقراطي العربي، مجلة قضايا آسيوية، العدد الرابع، برلين، نيسان ٢٠٢٠، ص٢٥.

(3) Giovanna Cinelli, Kristen Cordell, Wendy Cutler, and others,, Course Economics in National Security Tools of Coercion and Inducement,Center for Strategic & International Studies,(csis) executive education, Washington, May 17, 2021.p.5.

(4) Official website of the World Health Organization. Available at Link: Globally, as of 5:23pm CEST, 16 November 2021, there have been 253,640,693 confirmed cases of COVID-19, including 5,104,899 deaths, reported to WHO. As of 14 November 2021, a total of 7,307,892,664 vaccine doses have been administered..
. https://covid19.who.int/

(بلومبيرج إيكونوميكس)* انخفاضًا في الناتج المحلي الإجمالي الصيني بنسبة ٢٠٪، حتى إن أسعار النفط أصبحت تتأثر بشكل مباشر بمستوى الاصابات في الفايروس. ورغم تخصيص الولايات المتحدة والصين مبالغ مالية كبيرة لخطط الطوارئ الاقتصادية، كان لفايروس كورونا الأثر الكبير في أرباك الخطط الاقتصادية للمستثمرين [١].

وتذهب الدراسة الى أن أزمة فايروس كورونا تضاف الى القضايا التي تؤثر في توتر العلاقة بين الصين والولايات المتحدة، حيث الاتهامات المتبادلة بين الطرفين، وبذلك يُعد فايروس كورونا أحد القضايا المستجدة التي ربما تزيد من حدة التوتر والصراع الذي يغلب عليه الطابع الاقتصادي اكثر منه العسكري بين البلدين، وكان تعامل الصين مع أزمة كورونا على المستوى العالمي أفضل من الولايات المتحدة، بالسيطرة على الفايروس وتقديم المساعدات والدعم للدول الاخرى، وهذا يحسب للصين على المستوى الدولي، مقارنة بالموقف الضعيف والخجول للولايات المتحدة والاتحاد الاوربي في تقديم الدعم الدولي. وترى الدراسة ان على الدول ان تتحد من اجل التصدي للوباء حيث المسؤولية تقع على الجميع وان يكون ذلك في سقف اولوياتها بدلاً من تبادل الاتهامات.

من خلال القراءة لأهم العوامل المؤثرة في العلاقات الصينية – الأمريكية تؤشر الدراسة أن أهم نقاط الضعف التي تعاني منها الصين هي علاقاتها مع دول المنطقة الاقليمية المجاورة لها – اليابان، فيتنام، الهند، كوريا الجنوبية، واكثر قضية تؤرق الصين هي قضية تايوان – التي تعتبر من الاوراق الرابحة التي تستعملها الولايات المتحدة للضغط على الصين، ويرى البعض إن مسار العلاقة الأمريكية الصينية، آخذاً بالاتجاه التعاوني التنافسي أكثر من الاتجاه التصادمي، إذ إن

---

* بلومبيرغ نيوز (بالانجليزية: Bloomberg News) هي وكالة انباء دولية تأسست في عام ١٩٩٠. في نيويورك وكان اسمها بلومبيرغ بيزنس نيوز لتقديم تقارير وأخبار ماليه. للتفصيل ينظر: الصفحة الرئيسية للوكالة متاح على الرابط: https://www.bloomberg.com/middleeast تأريخ الزيارة ٢٨شباط ٢٠١٢.

(1) Rosamond Hutt, The Economic Effects of the COVID-19 Coronavirus Around The World (world economic forum), published date 17-2-2020 date of view 30-11-2020.Available at Link:
https://www.weforum.org/agenda/2020/02/coronavirus-economic-effects-global-economy-trade-travel.the date visit 28 January2021./

هناك علاقات تبادل تجاري واستثمارات ثنائية بين الصين والولايات المتحدة الامريكية التي تجاوزت المئة مليار دولار امريكي حتى عام ٢٠١٦.

ولكن الدراسة لا تؤيد وجهة النظر هذه حيث تشير الدلائل الاقتصادية والعسكرية – من حيث معدل الانفاق العسكري في الصين وسعيها للحصول على التكنلوجيا العسكرية الحديثة– ان العلاقة الامريكية– الصينية تتجه نحو التنافس والصراع اكثر من التعاون، رغم محاولة الطرفين الابتعاد عن التصعيد باتجاه المواجهة وفي هذا السياق يذكر (غراهام اليسون) ان مجرد وجود قوة صاعدة فهذا يعني تهديد للقوة المهيمنة "[1] في اشارة الى أثر النمو الصيني على هيكلية النظام الدولي ومكانة الولايات المتحدة الأمريكية، التي تشعر بخطورة الصعود الصيني وسعيهُ لقيادة منطقة آسيا كمرحلة أولى من مراحل توسيع النفوذ الصيني للعالم.

(١) محاضرة ألقاها غراهام أليسون حول كتابه الجديد، حتمية الحرب، على قناة (TED) في شباط ٢٠٢١.متاحة على الموقع: تأريخ الزيارة ١٧أذار ٢٠٢١.
https://www.ted.com/talks/graham_allison_is_war_between_china_and_the_us_inevitable#t-6261.

المبحث الثاني: الاستراتيجية الأمريكية للأمن السيبراني

في إطار مواجهة التهديدات الإلكترونية المختلفة، والتدفقات الضخمة والسريعة عبر شبكات الانترنيت في ظل النظام العالمي الجديد، وبروز العامل الرقمي كعنصر اساسي من عناصر قوة الوحدات الدولية – بما فيها الفواعل من غير الدول – كل ذلك أدى إلى تصاعد سرعة التفاعلات بين الفاعلين على المستوى الاقليمي والدولي، وبالتالي أنعكس ذلك على مفاهيم الأمن القومي للدول، التي لم تعُد بعضها قادرة على السيطرة على حركة التهديدات السيبرانية التي تتعرض لها، لذلك تسعى الولايات المتحدة كونها الدولة المهيمنة على النظام الدولي الى حد ما، وفي ظل وجود قوى دولية تعمل على تهديد مصالحها، إلى تبني استراتيجية قومية لمحاولة منع أو التخفيف من هذه التهديدات التي تمس أمنها القومي، وأتخاذ اجراءات وقائية للحد من المخاطر المترتبة على الفضاء الالكتروني.

المطلب الأول: الركائز الاساسية للاستراتيجية الامريكية للفضاء الالكتروني ٢٠١٨

أكد الرئيس الامريكي (دونالد ترامب) على أهمية الفضاء في الاستراتيجية الأمريكية وقال: " يُعد الفضاء الإلكتروني جزءًا لا يتجزأ من جميع جوانب الحياة الأمريكية، بما في ذلك الاقتصاد والامن والدفاع...، وقد زاد الخصوم من وتيرة وتعقيد أنشطتهم الإلكترونية المعادية". لقد اتخذت ادارة الرئيس (ترامب) العديد من الاجراءات لمواجهة التهديدات الالكترونية، حيث وقَّع الرئيس على (الأمر التنفيذي) (١٣٨٠٠)*. الخاص بالأمن السيبراني، ومع الاستراتيجية الإلكترونية الوطنية لعام ٢٠١٨، أصبحت الولايات المتحدة تمتلك أول استراتيجية إلكترونية مفصلة بالكامل منذ ١٥ عامًا" [1]. وتقوم الاستراتيجية الوطنية الأمريكية للفضاء الالكتروني لعام ٢٠١٨ على اربعة ركائز:

الركيزة الأولى:

* وهو الامر الذي ينص على تعزيز الأمن السيبراني للشبكات الفيدرالية والبنية التحتية الحيوية ويعتبر خطوة باتجاه انفاذ القانون الخاص بالهجمات السيبرانية وردع المهاجمين، للتفصيل ينظر: وزارة الدفاع الأمريكية ، الاستراتيجية الأمريكية للأمن السيبراني لعام ٢٠١٨ ،

(1) President Donald J Trump, National Cyber Strategy To the United States of America, September 2018, PP.6-11.

تقوم على حماية الشعب الأمريكي، الوطن، طريقة الحياة الأمريكية، تأمين الشبكات الفيدرالية، المعلومات، وتتضمن مزيد من المركزية للإدارة والرقابة على الأمن السيبراني الفيدرالي، حيث ستعمل الإدارة على زيادة تمكين وزارة الأمن الداخلي(DHS) Department Homeland) Security) لتأمين الإدارات الفيدرالية وشبكات الوكالات، وهذا يشمل ضمان أن تتمتع وزارة الأمن الوطني بإمكانية الوصول المناسب إلى أنظمة معلومات الوكالة لأغراض الأمن السيبراني، ويُعد تأمين البنية التحتية الحيوية وإدارة مخاطر الأمن السيبراني مسؤولية يتم تقاسمها من قبل القطاع الخاص والحكومة الفيدرالية من خلال:

١-تحفيز الاستثمار في مجال الأمن السيبراني: الاستثمار في الأفراد والتكنولوجيا لتحقيق هذا الهدف، حيث تعمل الحكومة والقطاع الخاص معاً لتصميم تقنية أكثر أمانًا تمنحنا القدرة على حماية ولتحسين مرونة الأنظمة والشبكات الحكومية والصناعية المهمة [١].

٢- إعطاء الأولوية لاستثمارات البحث وتطوير البنية التحتية الوطنية لمعالجة مخاطر الأمن السيبراني على البنية التحتية الحيوية.

٣-تحسين النقل والأمن البحري: فالاقتصاد والتجارة مبنية على تأمين خطوط النقل البحرية العالمية امام حركة السلع.

٤- مكافحة جرائم الإنترنت وتحسين الإبلاغ عن الحوادث والهجمات الالكترونية:

مثلا، الهجوم الإلكتروني الذي شنه القراصنة الروس في كانون الاول ٢٠٢٠ – الذي يعدهُ المختصين هو الأسواء منذ سنوات، – حيث تمكنوا من اختراق الاهداف التي لا تملك منصة (Orion) المخترقة من شركة سولار ويندز (Solar Winds) [٢].

(1) United States. White House Office, National Security Strategy, May 2010, p.14.

(٢) عادل درويش، القراصنة الروس يستهدفون شركة Crowd Strike، مجلة التطوير الرقمي، العدد الرابع، ٢٨، كانون الاول ٢٠٢٠. متاح على الموقع: https://www.ddc.iq/articles/3758 تأريخ الزيارة ٣١ كانون الاول ٢٠٢١.

٥-تحديث المراقبة الإلكترونية وقوانين جرائم الكمبيوتر: وذلك بالتنسيق مع الكونجرس، لتعزيز قدرات تطبيق القانون من أجل جمع الأدلة اللازمة بشكل قانوني عن الجرائم والنشاطات الخبيثة، وفرض العقوبات المناسبة على الجهات السيبرانية المعادية.

٦- الحد من التهديدات العابرة للحدود والقرصنة الحاسوبية التي تقوم بها عبر الوطنية الجماعات الإجرامية، والتي تشكل تهديدًا كبيرًا للأمن القومي، عن طريق المنظمات الجنائية في الفضاء السيبراني من خلال تفعيل القانون لمحاكمة المجرمين خارج الدولة .

الركيزة الثانية: تعزيز الرخاء الأمريكي

تُعد شبكة الإنترنت التي توفرها الحكومة الأمريكية – محليا وخارجيا – أحد عوامل تعزيز القيم الأمريكية في الحرية والأمن والازدهار، في ظل العالم الرقمي الحديث، والسعي للحفاظ على نفوذ الولايات المتحدة في النظام التكنولوجي، وهذا يتم من خلال [1]:

١- تعزيز حيوية السوق واقتصاد رقمي مرن يرتبط بطبيعته بالأمن القومي حيث أصبح الاقتصاد متجذرًا بشكل متزايد في التقنيات الرقمية، ودعم ومكافأة مرونة الفضاء السيبراني.

٢- تعزيز التدفق المجاني للبيانات عبر الحدود: تسعى الولايات المتحدة لرفع الحواجز غير المبررة أمام التدفق الحر للبيانات والتجارة الرقمية، التي تؤثر على القدرة التنافسية للشركات الامريكية مقابل الصينية.

٣- رعاية وحماية الاختراع الأمريكي: يعتبر الابتكار أمر بالغ الأهمية للحفاظ على الميزة الاستراتيجية للدول في الفضاء السيبراني، والسعي لتحفيز الريادة في مجال "الذكاء الاصطناعي" *. علم المعلومات، والبنية التحتية للاتصالات من الجيل المتقدم.

٤- نظام حماية الملكية: يتضمن الحماية القوية للملكية الفكرية من السرقة.

---

(1) Kendall Scherr, Cybersecurity Strategy2018, Department of Homeland Security (DHS), homeland security Digital Library · Published May 15 2018, p.1.

* الذكاء الاصطناعي (Artificial Intelligence) سيتم تناول الموضع بتفصيل أكثر في الفصل الثالث من هذه الدراسة، المبحث الاول، المطلب الثاني.

٥- تطوير القوى العاملة في الأمن السيبراني، من خلال التعاون بين القطاعين العام والخاص، لتدريب القوى العاملة في مجال الأمن السيبراني [١].

الركيزة الثالثة: الحفظ على السلام باستخدام القوة السيبرانية

إنَّ المشاركة في الفضاء الإلكتروني تعمل بالفعل على تغيير توازن القوى الاستراتيجي، وتعمل الولايات المتحدة على توظيف الانترنيت في كل عناصر القوة الوطنية، وردع السلوك المزعزع للاستقرار في الفضاء الإلكتروني الذي يتعارض مع المصالح الوطنية للولايات المتحدة الأمريكية من خلال النقاط الآتية [٢]:

١- تعزيز الاستقرار السيبراني من خلال قواعد المسؤولية وسلوك الدولة، بمعنى يجب أنفاذ وتطبيق القانون ضد اي سلوك او نشاط الكتروني معادي، بفرض العقوبات الصارمة على كل من ينتهك الفضاء السيبراني وفقا لتشريعات محلية ودولية تخص الجرائم الإلكترونية.
٢- مكافحة التأثير السيبراني وعمليات المعلومات: ستستخدم الولايات المتحدة جميع الأدوات المناسبة للقوة الوطنية لفضح ومواجهة تدفق التأثير الضار بالبيانات ونظم.
٣- القيادة بذكاء موضوعي وتعاوني، عن طريق استخدام كافة الوسائل السيبرانية وتحديد اي نشاط سيبراني معادي لمواجهتهُ بالتعاون مع شركائها الدوليين.
٤- تفعيل مبادرة الردع السيبراني لمكافحة التأثيرات السيبرانية المعادية، حيث ستستخدم الولايات المتحدة الأمريكية جميع الادوات المناسبة للقوة الوطنية، لمواجهة تدفق التأثير المعادي عبر الانترنت، والحملات الأعلامية التي تستخدم المنصات الإلكترونية المظللة.

الركيزة الرابعة: تحسين التأثير السيبراني للولايات المتحدة الأمريكية

تسعى الولايات المتحدة للحفاظ على دور قيادي دولي نشط ومؤثر؛ لمعالجة مجموعة واسعة من التهديدات والتحديات لمصالحها في الفضاء السيبراني، والسعي للحفاظ على الانفتاح طويل المدى وذلك من خلال.

(1) National Cyber Strategy To the United States of America, September 2018,p.16.
(2) Ibid, p.20.

١- تعزيز انترنيت آمن ومفتوح وموثوق به قابل للتشغيل المتبادل، والعمل على النهوض بحقوق الإنسان ومواجهة الجهود الاستبدادية للرقابة والتأثير على الإنترنت، والدعوة للمشاركة السياسية والابحاث العلمية [١].

٢- تعزيز الأسواق والمحافظة عليها من أجل تميز الولايات المتحدة في جميع أنحاء العالم، والمساهمة في بناء قدرات الشركاء في مجال الأمن السيبراني، للحفاظ على النفوذ الأمريكي ضد المنافسين العالميين [٢]. حيث أدى دخول المجال السيبراني إلى انكشاف استراتيجي للدول التي تحاول بشتى الوسائل الحد من هذا الانكشاف لحماية أمنها القومي، والانكشاف الاستراتيجي للقوى الفاعلة وغير الفاعلة في النظام الدولي هو مبتغى امريكي [٣]. من خلال الركائز الاساسية لاستراتيجية الأمن السيبراني لسنة ٢٠١٨ ، وتستنتج الدراسة إن الولايات المتحدة بدأت بشكل فعلي التركيز على الأمن السيبراني، كأحد مجالات الأمن القومي المهمة إذ أصبح الفضاء الإلكتروني متغير مهم في التأثير على العلاقات الدولية، والأمن السيبراني -كونهُ جزء من هذا الفضاء-وبما لهُ من دور في حماية أنظمة البنية التحتية الإلكترونية، أصبح من أولويات الاستراتيجية الأمنية.

المطلب الثاني: استراتيجية المثلث الدفاعي الإلكتروني الأمريكي

تسعى الولايات المتحدة إلى تطوير استراتيجيتها بما يتناسب مع التطور التكنولوجي، الذي بدأ يشكل أهم عوامل القوة للدولة، حيث أصبح الدفاع الالكتروني أحد وسائل الدفاع المهمة للحفاظ على الأمن القومي، وفي هذا المطلب سيتم التركيز على ركائز المثلث الدفاعي، وماهي مجالات القوة في المواجهة الالكترونية، وأهم التهديدات التي تواجه الأمن السيبراني للولايات المتحدة.

اولاً: ركائز المثلث الدفاعي

---

(١) عبد الكريم زهير عطية الشمري، مصدر سبق ذكره، ص ص١٣٤-١٣٥.

(2) National Cyber Strategy, To the United Stated of America,2018. Op. cit, p. 20-26.

(٣) عادل عبد الصادق، القوة الإلكترونية: أسلحة الدمار الشامل في عصر الفضاء الإلكتروني، مجلة السياسة الدولية، مؤسسة الأهرام، القاهرة، العدد ١٨٨، نيسان ٢٠١٢، ص٣٠.

تقوم استراتيجية المثلث الدفاعي على أعادة الهيكلة الفدرالية كأداة رئيسية لتأمين الشبكات ونظم المعلومات من خلال التركيز على الجهود الدفاعية في ثلاثة محاور هي [١]:

١- شركات المستوى الاول (العمود الفقري)، والذي تمثلهُ الشركات الاساسية التي توفر خدمة الانترنيت ومن بينها خمس شركات* ضخمة، وتعتبر حماية شركات المستوى الأول بمثابة حماية البنية التحتية الأمريكية الخاصة بالأنترنيت[[٢].

ولابد للمهاجم أن يمر اولاً بشركات المستوى الأول، لذا فأن حماية هذه الشركات وتوفير برامج الدفاع ضد الهجمات الإلكترونية، يمكن أن تساعد في ضبط المهاجم لحظة دخولهُ العصب أو العمود الفقري لشركات المستوى الأول.

٢- تأمين شركة الكهرباء: قد يتساءل البعض لماذا تتصل شبكة الكهرباء بالفضاء الالكتروني؟ ؛ فبدون الكهرباء سوُف يتوقف عمل معظم الأشياء التي تُعد مهمة جداً للحياة وفي كافة المجالات (الاقتصادية، الصحية، الصناعية، والامنية) وأسهل طريقة هو أن يقوم مهاجم تابع لدولة اخرى، بأحداث ضرر واسع بالولايات المتحدة من خلال ايقاف شبكة الكهرباء بشكل كلي او جزئي.

٣- وزارة الدفاع : ويقصد به أن الاعتداء الالكتروني الذي تقوم به دولة ما على الولايات المتحدة، ويكون تركيز الهجوم الالكتروني اولاً، على شبكات وزارة الدفاع الامريكية التي تقوم بتنفيذ الرد. وقد كان تصريح الرئيس (اوباما)، بمثابة عامل ردع للدول التي تحاول شن مثل هذه الهجمات: "اريد ان اعلنها واضحة لأي دولة قد تفكر في استخدام الاسلحة الالكترونية ضدنا... سأستخدم كافة الصلاحيات المنوطة بي بصفتي القائد الاعلى للقوات المسلحة الامريكية..." بمعنى ان الرد قد

---

(١) ريتشارد كلارك وروبرت نيك، مصدر سبق ذكره، ص ١٩٣- ٢٠٥ .

* هي شركة " إيه تي آند تي AT&T وفيريزون Verizon وليفيل ثري 3 Level وكويست Qwest وسبرينت Sprint " وهي شركات تعمل في مجال الاتصالات وشبكات الانترنيت في الولايات المتحدة الأمريكية وقسم منها يتنافس مع شركة T-Mobile في مجال الاتصال اللاسلكي وتمكين الولايات المتحدة لقيادة العالم في خدمة 5G حيث تحاول شركة هواوي الصينية المبادرة في تنفيذها عالميا. للتفصيل ينظر:

(2) AT&T and =Verizon Are Feeling the Heat of Real Competition, T-Mobile, September 22, 2020, The official website of T-Mobile.Available at Link: https://www.t-mobile.com/news/un-carrier/real_competition_blog

يكون بطرق دبلوماسية، اقتصادية، الكترونية، او بطرق فعلية حسب ما يقتضي الظرف والهدف الذي سيكون الرد من اجله، وتسمى هذه الفكرة في استراتيجية الحرب النووية "هيمنة التصعيد"* [1].

ثانيا: قياس القوة في مجال حرب الفضاء الإلكتروني

لا تتحدد عملية قياس القوة في مجال حرب الفضاء الإلكتروني، بالاعتماد على قدرة الدولة في مهاجمة الاخرين، وإنما هناك عاملين مهمين وهما الدفاع والاعتماد، أضافة الى عامل الهجوم، فالدفاع هو قياس قدرة الدولة على إتخاذ إجراءات للصد، عند تعرضها للهجوم وتخفيف أثاره، بينما يشير الاعتماد الى مدى اتصال الدولة بالأنترنيت، ويمكن توضيح درجة التفاعل بين هذه العوامل الثلاثة من خلال الجدول أدناه:

جدول رقم (٦) كيفية قياس محصلة القوة في مجال حرب الفضاء الإلكتروني

الدولة	هجوم الكتروني	اعتماد الكتروني	دفاع الكتروني	أجمالي القوة
الولايات المتحدة	٨	٢	١	١١
روسيا	٧	٥	٤	١٦
الصين	٥	٤	٦	١٥
ايران	٤	٥	٣	١٢
كوريا الشمالية	٢	٩	٧	١٨

الجدول من اعداد الباحث بالاعتماد على المصدر: ريتشارد كلارك وروبرت نيك، حرب الفضاء الالكتروني، مركز الأمارات للدراسات والبحوث الاستراتيجية، ط١، ابو ظبي، ٢٠١٢، **ص**١٨٠

من خلال الجدول اعلاه، نلاحظ أن الدولة كلما قل اعتمادها على الشبكات الالكترونية، زادت درجتها على مقياس الاعتماد، وتفسير ذلك انهُ كلما انتشرت الشبكات الالكترونية في البلاد يُعد مؤشراً جيداً، ولكن هذا الانتشار عندما يكون مقياس لقدرة الدولة على الصمود أمام الهجمات الالكترونية يعتبر عامل ضعف في الدولة، فالصين مثلا لديها درجة عالية في مجال الدفاع وذلك

* بمعنى ان الرد يأخذ منحى تصاعدي وقد يصل الى مستوى الرد العسكري التقليدي العنيف.

(١) ريتشارد كلارك وروبرت نيك، مصدر سبق ذكره، ص ٢١٢.

لقدرتها على عزل الشبكات بأكملها عن بقية عالم الفضاء الالكتروني [١]. وكذلك الحال مع كوريا الشمالية التي تسيطر على خدمات الانترنيت، لذلك فإن الدول الاقل تقدما من الولايات المتحدة في مجال الفضاء الالكتروني، ربما تكون أقل ضررا في حالة حدوث حرب في الفضاء، وفي هذا السياق يقول الأدميرال الامريكي السابق(Mike McConnell)* "لأننا الاكثر تقدما من الناحية التقنية – فلدينا أعلى سرعة للبث – فإننا الاكثر تعرضا للمخاطر" وذلك لأن الولايات المتحدة ربطت اقتصادها بالأنترنيت فقطاعات البنية التحتية المدنية الثمانية عشر** الحساسة، كلها تعتمد على الانترنيت لتنفيذ مهامها الاساسية الالكترونية [٢]. وترى الدراسة إن هذه المعادلات ليست بالضرورة تنطبق على جميع الدول نتيجة اختلاف ظروف الدول والتطور المستمر في مجال التقنيات والتكنولوجيا العسكرية منها خاصة. و"تنظر الصين إلى التفوق الفضائي على أنه جزء من القدرة على التحكم في مجال المعلومات، وهذا عنصر أساسي في الحرب الحديثة" [٣]. بحيث تشكل النجاحات التي تحققها الصين في مجال الفضاء الالكتروني تهديد للولايات المتحدة.

ثالثا: التهديدات التي تواجه الولايات المتحدة في الفضاء الإلكتروني

بعد أحداث ١١ ايلول عام ٢٠٠١، والتي أظهرت كيف يمكن أن يكون استغلال المعلومات من قبل الإرهابيين لهُ وقعٍ كبير في تحقيق نتائج كبيرة ضمن مستويات الضرر الجسدي والمادي بتكاليف قليلة مقارنة بالخسائر التي تترتب على الدولة التي تتعرض للهجوم الارهابي

---

(١) ريتشارد كلارك وروبرت نيك، مصدر سبق ذكره، ص١٨٠.

* سياسي امريكي وسناتور عن ولاية كنتاكي الأمريكية منذ عام ١٩٨٥، انتخب زعيما للجمهوريين بمجلس الشيوخ عام ٢٠١٤.

** تشمل قطاعات البنية التحتية: الاتصالات السلكية واللاسلكية، محطات الطاقة والكهرباء، البنية التحتية الخاصة بصناعة نظم الدفاع والاسلحة...الخ للتفصيل ينظر: ريتشارد كلارك وروبرت نيك، ص١٨١.

(٢) ريتشارد كلارك وروبرت نيك، مصدر سبق ذكره، ص ص١٧٧، ١٧٨، ١٧٩.

(3) Jim Garamone, Department of Defense.GOV, DIA Report Details Threats to America's Space-Based World, FEB. 11, 2019. Available at Link:Date visit 18 March 2021 https://www.defense.gov/Explore/News/Article/Article/1754509

الإلكتروني [١]. لذا بدأ التركيز على الفضاء الالكتروني كتهديد للأمن القومي؛ نتيجة استخدامه من قبل الدول والفواعل من غير الدول بسبب قلة الجهد والتكلفة عند تنفيذ هذا النوع من الهجمات [٢].

ومن أبرز التهديدات التي تواجهها الولايات المتحدة الأمريكية في الأمن السيبراني والتي تشكل خطورة على امنها القومي هي:

١- التجسس الالكتروني (السيبراني): ويتم ذلك عن طريق الدخول غير المشروع الى أنظمة وبيانات الحواسيب الخاصة بالولايات المتحدة، من أجل اضعافها أو تخريب و سرقة المعلومات [٣]. وهذه الاعمال تقوم بها الدول المنافسة للولايات المتحدة الأمريكية، ومن أجل حماية (الحدود الوطنية الالكترونية)*، والتي أصبحت عملية اختراقُها أسهل من الحدود الجغرافية ويتم ذلك "بعمليتي اختراق هما: التخطي التجاري للحدود القومية، وعملية التخطي المعلوماتي للحدود القومية" [٤]. لذا انشأت وزارة الدفاع الأمريكية (البنتاغون) قوة دفاع شبكات الكمبيوتر المشتركة-JTF (CND) لتولي مهمة الهجوم والدفاع الإلكتروني والتي أطلق عليها عام ٢٠٠٩ (القيادة الالكترونية الأمريكية) [٥]. ولم ينظر القانون الدولي لحالة التجسس- بشكل عام- اثناء النزاعات كجريمة دولية

---

(١) رنا علي خلف ، المقوم التكنولوجي وأثره في السياسة الأمريكية ، مجلة السياسة الدولية كلية العلوم السياسية جامعة بغداد، العدد ٤٩، السنة ٢٠١٥ ، ص ٢٣٩ .

(٢) نورة شلوش، مصدر سبق ذكره ، ص ١٩٠.

(٣) عبد الهادي محمود الزيدي، التجسس الاسرائيلي الالكتروني على الدول العربية، مجلة دراسات دولية، مركز الدراسات الدولية، جامعة بغداد، العدد ٥٨، تموز ٢٠١٤، ص١٤١.

* يقصد بالحدود الوطنية الإلكترونية: حماية انظمة وبيانات المؤسسات الحكومية والشركات داخل حدود الدولة او خارجها كما هو الحال في الحفاظ على الحدود الجغرافية التقليدية إلا ان حماية الحدود الوطنية الإلكترونية لها مدى اوسع لأنها لا تعبر عن الدفاع بالشكل المادي وأنما هو دفاع معنوي إلكتروني غير ملموس يتضمن اجراءات دفاعية مكلفة مقابل هجمات الكترونية قليلة التكلفة، للتفصيل ينظر: عادل عبد الصادق، الفضاء الإلكتروني وتهديدات جديدة للأمن القومي.

(٤) رنا علي خلف، مصدر سبق ذكره ، ص ٢٣٥.

(٥) عادل عبد الصادق، الفضاء الإلكتروني وتهديدات جديدة للأمن القومي، مجلة السياسة الدولية، العدد ١٨٠، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، ٢٠١٠، ص٤٨.

بحد ذاتها ولم يتم تصنيفها كجرائم حرب، ولكن هذا لم يُضفي المشروعية على أعمال التجسس من وجهة نظر القانون الدولي [١].

٢- الارهاب الالكتروني: ويشمل الاعتداء على شبكة الانترنيت لتعطيل خدماتها واشاعة عدم الثقة في خدمة الانترنيت بين المستخدمين، وعرفه (James A. Lewis) بأنه: "استخدام ادوات شبكات الحاسوب في تدمير او تعطيل البنى التحتية الوطنية المهمة مثل الطاقة والنقل، او بهدف ترهيب الحكومة والمدنيين" [٢].

٣- الحروب الإلكترونية: ويقصد بها قيام الفواعل من الدول وغير الدول، بشن هجمات إلكترونية ضد أهداف مختلفة ويستهدف كل المؤسسات والشركات المدنية والعسكرية [٣]. ويرى (**Kenneth Gears**) أن العناصر الرئيسية للحرب الإلكترونية هي: التجسس، الدعاية، الحرمان من خدمة الانترنيت، مهاجمة البنية التحتية والتلاعب بالبيانات [٤].

٤- التحريض على الكراهية والعنف: وذلك من خلال نشر أفكار العنصرية والطائفية والابتزاز عبر شبكات الانترنيت، من أجل الإساءة الى سمعة الولايات المتحدة امام الرأي العالمي [٥].

٥- الاستخبارات الخارجية: وخاصةً التابعة لروسيا الاتحادية والصين، التي تشكل التهديد الرئيس في أختراق أجهزة صنع القرار الوطني والاجهزة السرية الاستخبارية للولايات المتحدة [٦].

---

(١) ليث صلاح الدين حبيب، التجسس وأحكامه ابان النزاعات المسلحة الدولية، مجلة جامعة الأنبار للعلوم القانونية والسياسية، العدد الاول، كلية القانون والعلوم السياسية، جامعة الأنبار، ، ٢٠٠٩، ص٤٢٩.

(٢) رؤى خليل سعيد، الإرهاب الالكتروني وأثره في أمن الدول – السعودية نموذجا –، مجلة حمورابي، العدد ٢٥-٢٦، مركز حمورابي للبحوث والدراسات الاستراتيجية، شتاء – ربيع ٢٠١٨، ص٥٢.

(٣) عادل عبد الصادق، مصدر سبق ذكره، ص ٣١.

(4) Kenneth Gears, Cyberspace and the Changing Nature of Warfare, U.S. Representative Cooperative Cyber Defense Centre of Excellence Tallinn, Estonia,2008,p.3.

(٥) يونس مؤيد يونس مصطفى، مصدر سبق ذكره، ص١٣٦.

(٦) اللجنة الاقتصادية والاجتماعية لغرب آسيا الاسكوا، الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية، الأُمم المتحدة، ٩ شباط ٢٠١٥، ص٧٢.

٦- الفضاء والفضاء المضاد: مع تزايد الخصوم المحتملين وتطوير قدرات الفضاء المضاد، تزداد التهديدات لأنظمة الفضاء الامريكية، فالصين تملك قدرات التشويش على الاقمار الصناعية وتسعى لبناء أنظمة مضادة للأقمار الصناعية الأمريكية خاصة؛ حيث تعتبر الولايات المتحدة السيادة على الفضاء الخارجي جزءا مهم من العقيدة العسكرية الامريكية [١].

ومن اجل مواجهة الهجمات الالكترونية، تقوم وزارة الدفاع الأمريكية بصفة دورية بإجراء محاكاة للتعرض لحرب إلكترونية فيما يطلق عليه (Cyber Storm)* عاصفة الحواسيب، كما عملت على تطوير أسلحة إلكترونية تشمل فيروسات قادرة على تخريب شبكات العدو [٢].

المطلب الثالث: توظيف القوة الإلكترونية الأمريكية في التفاعلات الدولية

سعت الولايات المتحدة إلى توظيف واستخدام القوة الإلكترونية في أدارة علاقاتها (السياسية والعسكرية والاقتصادية) مع الدول، حيث أصبحت التكنولوجيا ونظم المعلومات من أهم أدوات قياس قوة وفاعلية الدولة وتحقيق أهداف سياستها الخارجية، وقد عرّف (جوزيف ناي) القوة الإلكترونية بأنها: "القدرة على استخدام الفضاء الإلكتروني لخلق مزايا والتأثير على الأحداث في بيئات تشغيلية أخرى وعبر أدوات القوة الالكترونية" [٣] ويتضمن هذا المطلب توظيف القوة الإلكترونية الأمريكية في ثلاثة أبعاد هي: السياسية والعسكرية والاقتصادية.

أولاً: توظيف القوة الإلكترونية الأمريكية في التفاعلات السياسية الدولية

يُعد اللجوء إلى القوة الالكترونية لإدارة التفاعلات السياسية أحدى الطرق غير التقليدية التي تستطيع الدول وخاصةً الولايات المتحدة، من خلالها تحقيق أهدافها ويتم ذلك بعدة وسائل:

---

(١) يونس مؤيد يونس مصطفى، مصدر سبق ذكره، ص١٣٨.

* يتمثل الهدف الأساسي لـ Cyber Storm 2020 في تعزيز الاستعداد للأمن السيبراني وقدرات الاستجابة من خلال التمرين، للتفصيل ينظر:

Cybersecurity and Infrastructure Security Agency's (CISA) DEFEND TODAY, CYBER STORM 2020: NATIONAL CYBER EXERCISE, JULY 2020,p1.

(2) United States. White House Office, National Security Strategy,May-2010,p.27.

(3) Joseph S. Nye, Jr., Cyber power,Op.cit,p.3.

١-**الدبلوماسية الرقمية (Digital Diplomacy):** يعرف (Lewis) الدبلوماسية الالكترونية بأنها: "استخدام أدوات الاتصال الرقمية (وسائل التواصل الاجتماعي) من قبل الدُبلوماسيين للتواصل مع بعضهم البعض ومع الجمهور في الدول التي يعملون فيها" [١].

وقد شهدت الدبلوماسية الإلكترونية تزايداً كبيراً في شعبيتها خلال السنوات الأخيرة، إذ أصبحت الدول–الغربية منها خاصة– تستخدم الانترنيت في نشر المعلومات الدبلوماسية لتحسين صورة الدولة، من خلال التفاعل مع المواطنين عبر شبكات التواصل الاجتماعي، وخلق عملية ربط بين الدبلوماسيين مع بعضهم البعض، في كل مكان وفي أي وقت والتنسيق مع الشركاء الخارجيين لإدارة الازمات بطريقة آمنة وفعالة [٢].

٢- الاستخبارات الإلكترونية: (Cyber Intelligence)

تُحاول أغلب الدول التجسس على بعضها البعض وهو أمر تقليدي، لكن تطور طرق التجسس بسبب الثورة التكنولوجية، التي سهلت القيام بالتجسس على الأفراد والشركات والدول، مما حول الصعوبة من كيفية التجسس إلى كيفية ادارة الكم الهائل من المعلومات الناجمة عن عمليات التجسس، أذ كشفت تسريبات(سنودن)* عن الكثير من عمليات التجسس، مثال ذلك الازمة الدبلوماسية بين المانيا والولايات المتحدة الأمريكية بسبب قيام الاخيرة، بالتجسس على هاتف المستشارة الالمانية (انجيلا ميركل)عام ٢٠٠٢.

٣- الرسائل عبر شبكات التواصل الاجتماعي: (Messages via social media)

---

(1) Olubukola S. Adesina, Foreign policy in an era of digital diplomacy, The Cogent Social Sciences Journals,1 March 2017, P.3.

(2) Digital Diplomacy Series: Foreign Policy and Digital Engagement - Embassy of Italy, the Embassy of Italy in Washington DC and Young Professionals in Foreign Policy, (YPFP) hosts the panel discussion: FOREIGN POLICY AND THE FUTURE OF ENGAGEMENT, May 29, 2014. Discussion seminar, Available at Link: https://www.youtube.com/watch?v=_TMki-bKldg date visit 19March2021

* إدوارد جوزيف سنودن أمريكي ومتعاقد تقني وعميل موظف لدى وكالة المخابرات المركزية، عمل كمتعاقد مع وكالة الأمن القومي قبل أن يسرب تفاصيل برنامج التجسس بريسم إلى الصحافة. في يونيو ٢٠١٣ سرب سنودن مواد مصنفة على أنها سرية للغاية من وكالة الأمن القومي، منها برنامج بريسم إلى صحيفة الغارديان وصحيفة الواشنطن بوست للتفصيل ينظر: https://en.wikipedia.org/wiki/Edward_Snowden

ويتم ذلك باستخدام القادة السياسيين لهذه القنوات من الاتصالات لكسب الدعم والتأييد، حيث يستخدم أغلب رؤساء الدول موقع تويتر للتواصل مع الجماهير، وكان على رأس تلك القائمة الرئيس (باراك اوباما) من حيث عدد أعضاء تويتر الذّين يتابعون نشاطهُ على الموقع [١].

٤- دعم المعارضة السياسية الإلكترونية (Supporting the electronic political opposition):

يُعد الفضاء الالكتروني وخاصة في النظم السياسية الدكتاتورية، مجال واسع لأنشاء المدونات واستخدام مواقع التواصل الاجتماعي، للتعبير عن الراي مما يسبب قلق وامتعاض لهذه الأنظمة السياسية التي تقوم باعتقال المدونين الإلكترونيين أو حجب بعض المواقع الاجتماعية [٢].

٥- مواجهة فكر الحركات الإرهابية (Confronting the ideology of terrorist movements):

عملت الولايات المتحدة على متابعة ومكافحة هذه الحركات التي تنشط في الفضاء الالكتروني، من خلال تعقب المواقع التي تبُث أفكار متطرفة وأختراق البريد الإلكتروني والحسابات الالكترونية للشخصيات التي تتبنى هذا الفكر.

ثانياً: توظيف القوة الإلكترونية الأمريكية في التفاعلات العسكرية الدولية

تعمل الولايات المتحدة على استخدام قوتها الإلكترونية لتحقيق اهداف عسكرية، من خلال الردع الإلكتروني عبر تعظيم معايير الأمان للشبكات، أو عن طريق الهجمات الإلكترونية الخارجية التي تشنها لتحقيق أهدافها العسكرية، وقد مثّلت القوة الالكترونية أحد الاسلحة العسكرية التي يمكن أن تحقق بها الولايات المتحدة الأمريكية اهدافها بفعالية، من خلال سرقة المعلومات العسكرية

---

(١)- ايهاب خليفة، القوة الإلكترونية، مصدر سبق ذكره، ص١٨٥.

(٢) عادل عبد الصادق، الانترنيت والدبلوماسية ومعركة القوة الناعمة بين الولايات المتحدة وايران، المركز العربي لأبحاث الفضاء الالكتروني (ACCR)، ٢٠١٨.متاح على الموقع: http://www.accronline.com/article_detail.aspx?id=29022 تأريخ الزيارة ٢ أذار.

والتلاعب بها، ومن الأمثلة على توظيف القوة الإلكترونية المجال العسكري هو نجاح قوات الدفاع الجوي الايرانية في السيطرة الكترونيا على طائرة بدون طيار وانزالها على الأراضي الايرانية [١].

كذلك تتعرض شبكات الاتصال اللاسلكية للخصوم، أو ممارسة نوع من الحرب النفسية (Psychological Warfare) عبر النفاذ الى موجات البث اللاسلكية للجيش، حيث مارست مثل هذا النوع من الحرب، القوات الامريكية سنة ٢٠٠٣ أبان الحرب على العراق، بأرسال رسائل إلى الضباط والجنود عبر موجات البث والاتصال للقوات المسلحة، او ألقاء المنشورات جواً على الجيش، لغرض ممارسة الضغط النفسي على الجيش العراقي [٢].

ثالثا: توظيف القوة الإلكترونية الأمريكية في التفاعلات الاقتصادية الدولية

أصبحت التكنولوجيا أساس التعاملات المالية والاقتصادية في القرن الحادي والعشرين، بحيث أصبحت الدولة التي تملك هذه التكنولوجيا تستطيع إلى حد كبير التأثير في الاقتصاد العالمي [٣]. وقد عملت الولايات المتحدة على استخدام القوة الإلكترونية في ادارة العلاقات الدولية الاقتصادية من خلال.

١- تعزيز مكانة الاقتصاد الامريكي: حيث ساهمت شركات المعلومات وتكنلوجيا الاتصالات بنسبة (٧,١%) من الناتج القومي الامريكي عام ٢٠١١، وتُعد الولايات المتحدة أكبر مصدر لصناعة تكنلوجيا المعلومات، وهذا يؤكد ما جاء في كتاب (الفين توفلر) بعنوان (تحول السلطة) حيث اشار: "إن راس المال والنقود في طريقها للتحول الى المعرفة ". وبذلك أصبح من يملك وسائل الاعلام وشبكات الاتصال، هم أصحاب الثروة وليس أصحاب المصانع والانتاج

---

(١) ايران تسقط طائرة استطلاع أمريكية بدون طيار، وكالة رويترز للأنباء ١٧- تشرين الاول ٢٠١١.متاح على الموقع: http//Arabic.rt.com/news/573311/ تأريخ الزيارة ٥أذار ٢٠٢١.

(٢) اولاف تايلر، التهديدات الجديدة: الابعاد الإلكترونية، مجلة حلف الناتو. في ١١ ايلول ٢٠١١. متاح على الموقع:تاريخ الزيارة ١٨أذار ٢٠ http://www.nato.int./docu/reviw/2011/11-september/Cyber-Threads/AR/index.htm

(٣) إيهاب خليفة، القوة الإلكترونية، مصدر سبق ذكره، ص٢١٦.

الصناعي(مصانع السيارات والاثاث...الخ)، وهذا يجسد بشكل جيد ما يطلق عليه اليابانيون تعبير (الاقتصاد اللين) الجديد [١].

٢- جمع المعلومات الاقتصادية (Economic intelligence):

تُعد كل من روسيا والصين أبرز القراصنة الإلكترونيين لجمع المعلومات الاقتصادية والاستخباراتية الأمريكية، حسب تقرير مكتب مكافحة التجسس الذي صنف الصين بانها الأكثر نشاطاً في عملية القرصنة الإلكترونية، وبما أن الولايات المتحدة لاعب أساس في النظام الاقتصادي الدولي، فان اقتصادها دائماً معرض لخطر الاختراق والقرصنة بهدف الحصول على المعلومات الاقتصادية والصناعية التي تتحكم في الاسواق العالمية، ومن الأمثلة على ذلك قيام قراصنة صينيون بأختراق البيانات لشركة كوكاكولا الأمريكية، التي حاولت شراء شركة صينية للعصائر، وذلك لغرض الحصول على الوثائق الخاصة باستراتيجية التفاوض لشراء الشركة الصينية بأفضل الاسعار [٢].

٣- التجسس على مسؤولي الشركات والمؤسسات.

تُعد العاصمة واشنطن مقرٌ للكثير من المؤسسات المالية (البنك الدولي، صندوق النقد الدولي) التي تعرضت لمحاولات تجسس من قبل الحُكومة الأمريكية، وذلك بعد تسرب أخبار عن تجسس وكالة الأمن القومي على هذه المؤسسات، مما دفع الرئيس الامريكي (اوباما) بإصدار أوامر بوفق التنصت على مقر المؤسسات المالية المذكورة [٣].

---

(١) ألفين توفلر، مصدر سبق ذكره، ص ص٤٤،١١٧.

(2) DAVID E.SANGER,Chinse Army Unit Is Seen as Tied to Hacking Against U.S, newspaper The New York t Times, February 18, 2013, Accessed on July 10th,2014,on.Available at Link: https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html The date at 19 March 2021.

(3) Act for Fiscal year 2021. Authorization Congressional Intelligence Committee, Intelligence.

٤- تحويل الأموال بطرق غير شرعية ومساندة الشركات الأمريكية العملاقة في مجال التكنلوجيا، الكثير من الدول ومنها الولايات المتحدة تعاني من القرصنة الإلكترونية على المصارف والمؤسسات المالية من خلال اختراق بياناتها وأنظمة حماية المعلومات [١].

لقد تغيرت الأشكال التقليدية للقوة بفعل التقدم التكنولوجي، وأصبحت القوة غير ثابتة من حيث المصدر والجهة التي تملكها، وكان للفضاء الإلكتروني الأثر الكبير في تغير موازين القوى اقتصاديا وعسكريا، بحيث أصبح الفاعل الذي يملك هذه التكنولوجيا والقادر على تصنيعها وتطويرها، له الدور البارز في التأثير على الأحداث السياسية ،الاقتصادية والعسكرية، ورغم تقدم الولايات المتحدة في مجال القوة الإلكترونية، فان قدرتها على توظيفها في المجالات الاقتصادية أضعف من سابقيها؛ كون الاقتصاد الأمريكي يعتمد على الأصول غير المادية (المعلوماتية)، وتعرضها بشكل مستمر لعمليات قرصنة الكترونية مما يشكل نقطة ضعف تهدد الاقتصاد [٢].

بناءاً على ما تقدم يمكن القول ان الولايات المتحدة تمكنت من توظيف قوتها الالكترونية، لتغيير بعض المفاهيم الاستراتيجية التي تتعلق بالتهديدات غير التقليدية للأمن، وأنتقلت من مرحلة التجسس على الأفراد إلى التجسس على الشعوب وقادة الدول، كما نجحت الولايات المتحدة في التواصل مع الشعوب، من خلال بث رسائل سياسية تدّعم الرؤية الأمريكية والسياسة الخارجية عبر مواقع التواصل الاجتماعي.

وقد أهتمت الولايات المتحدة باستخدام القوة الألكترونية، لما تتمتع به من قدرات متقدمة فمعظم الشركات المصدرة للتكنولوجيا (كوكل، آبل، مايكروسوفت وتويتر)، هي شركات أمريكية فضلا عن الدور الذي تلعبه وكالة الامن القومي الامريكي في تطوير القدرات الإلكترونية الأمريكية، كما عمدت الإدارات المتعاقبة سوآء خلال فترتي إدارة الرئيس (بوش ٢٠٠١-٢٠٠٩) او الرئيس (اوباما٢٠٠٩-٢٠١٧)، على إنشاء العديد من الخطط الاستراتيجية (الهجومية والدفاعية) وتعظيم التعامل الدولي في مجال مكافحة الهجمات الإلكترونية.

---

(١) إيهاب خليفة، القوة الالكترونية، مصدر سبق ذكره، ص ص٢٢٦، ٢٣٠.

(2) Joseph S. Nye. Jr, Op.cit., p.3.

المبحث الثالث: الاستراتيجية الصينية للأمن السيبراني

تتضمن الاستراتيجية الصينية لأمن الشبكات استخدام المعلومات للتأثير أو السيطرة على عملية صنع القرار لدى الأعداء، وما يترتب عليها من أنشطة، وذلك لخدمة الأهداف الصينية الهجومية والدفاعية، وهذه التفسيرات ربما تُعد أوسع نطاقاً من الرؤية الأمريكية في مجال الأمن الإلكتروني، حيث تعتبر المبادرة الأمريكية الوطنية الشاملة للأمن الإلكتروني، والتي انطلقت في كانون الثاني سنة ٢٠٠٨، أكثر محدودية في نطاقها، إذ تُركز على تعزيز القدرات الدفاعية التكنولوجية والبشرية، مما حث الصين- منذ بداية القرن الحادي والعشرين خاصة- إلى زيادة الاهتمام بالفضاء الإلكتروني، وتطوير القدرات العسكرية الخاصة بالفضاء الإلكتروني، ونتيجة لمخاوف الصين حيال البيئة الأمنية الخارجية، فإنه ليس من المستغرب أن يعرب المخططون الصينيون عن رأيهم القائل "أن نسيان التحضير للحرب سيؤدي إلى أزمة لا محالة" [١].

وهذا يفسر الاهتمام المتنامي للصين في مجال الأمن السيبراني وتكنولوجيا المعلومات، التي أصبحت من العوامل المهمة في تشكيل قوة الدولة حاليا، وقد تضمن هذا المبحث ثلاثة مطالب الأول يوضح عناصر الاستراتيجية الصينية للأمن السيبراني. والثاني يبحث في الاستراتيجية الصينية على المستوى الخارجي، أضافة الى المطلب الثالث الذي يبين التوجه الصيني نحو الردع الاستراتيجي في الفضاء الالكتروني.

المطلب الأول: عناصر الاستراتيجية الصينية للأمن الإلكتروني

تُعد حماية الأمن السيبراني للصين من ضمن أولويات الاستراتيجية الصينية، للمضي قدمًا في بناء مجتمع متطور وآمن لكل جوانب الحياة، وهو ضمانة مهمة لتحقيق هدف نضال "المئوية الثانية" وتحقيق الحلم الصيني بالتجديد العظيم للأمة الصينية [٢]. والعلاقة الإلكترونية بين الولايات المتحدة والصين كانت أقل خطورة مما هي عليه اليوم، على الرغم من المستويات عالية الاهتمام

---

(1) Michael S. Chase, Arthur Chan, China's Evolving Approach to "Integrated Strategic Deterrence, RAND Corporation, 2016,p.1.

(2) Paul Rosenzweig,China's National Cybersecurity Strategy, December 27, 2016.Available at Link:
https://www.lawfareblog.com/chinas-national-cybersecurity-strategy The date visit at 20 March 2021.

بقضايا الأمن السيبراني في كلا البلدين، ومن أجل تفسير السياسة الصينية بما في ذلك نشاطها الإلكتروني الداخلي، يتناول هذا المطلب قانون الأمن السيبراني لجمهورية الصين الشعبية والمحفزات الصينية في مجال الفضاء الإلكتروني.

أولاً: قانون الأمن السيبراني لجمهورية الصين الشعبية

في تشرين الثاني سنة ٢٠١٦ قدمت مجموعة قيادة الأمن السيبراني والمعلوماتية (CILG)، مشروع " قانون الأمن السيبراني الصيني" والذي اقرته الهيئة التشريعية العليا لجمهورية الصين الشعبية، ودخل حيز النفاذ في الاول من حزيران سنة ٢٠١٧ بموجب المادة (٧٩) منه، وتمت صياغة هذا القانون بهدف: حماية الحقوق والمصالح المشروعة للمواطنين والاشخاص الاعتبارين والمنظمات الأخرى، وتعزيز التنمية المعلوماتية السليمة في مجال الاقتصاد والتطوير العلمي، إذ نصت المادة (٣) في الفصل الاول من القانون على" تستمر الدولة في التأكيد بشكل متساو على الأمن السيبراني وتطوير المعلوماتية وتلتزم بمبادئ الاستخدام الفعال،... وضمان الأمن وتقوم الدولة في بناء البنية التحتية للشبكة والتوصيل البيني، وتشجيع الابتكار... وتدعم تنمية موظفي الأمن السيبراني المؤهلين، وتنشئ نظاما كاملاً لحماية الأمن السيراني" وجاء في نص المادة (٧) "تقوم الدولة بنشاط التبادل والتعاون الدولي في مجالات حوكمة الفضاء الالكتروني،... ومكافحة الجرائم الالكترونية غير القانونية..." وقد تضمنت المادة (٣١) من القسم الأول في الفصل الثالث من القانون، سلطة الدولة في تنفيذ الحماية الرئيسية على أساس نظام الحماية متعدد المستويات للأمن السيبراني لقطاعات البنية التحتية الاساسية [1].

لقد أدى النمو السريع في التجارة الإلكترونية، والتقدم التكنولوجي في الحوسبة وتحليل البيانات الضخمة، لاسيما في الصين إلى ظهور قضايا جديدة تتعلق بالأمن السيبراني، كما إن زيادة الاستثمار في تكنولوجيا التصنيع "الذكية" وتقنية "إنترنت الأشياء" تقود أيضا نحو خطوات لضمان استخدام واسع لما يسمى (بالآلات الذكية)، وتطوير الصناعات الداعمة للبنية التحتية

(1) Cybersecurity Law of the People's Republic of China June 1, 2017, Translate by Rogier Creemers, Paul Triolo and Graham Webste, June 29 2018,pp.3.9.

والمهمة لضمان بيئة آمنة للأمن القومي ومحصنة ضد الهجمات الالكترونية [١]. وتركز مواد هذا القانون، على طبيعة وتدفق المعلومات الرقمية التي تم تنظيمها في الصين، وتوحيدها جمعها واستخدامها، ويجب على مُشغلي الشبكات الذين يُعرفون باسم أصحاب الشبكات ومزودي خدمات الشبكة حسب ما جاء في المادة (٥٤) الفقرة رقم (١) من الفصل الخامس من القانون) ، أن يقوموا بتوضيح مسؤوليات الأمن السيبراني داخل مؤسساتهم، وأتخاذ تدابير تقنية لحماية عمليات الشبكة، ومنع تسريب البيانات وسرقتها، وتبليغ الجهات المختصة عن حوادث الأمن السيبراني التي تتعرض لها مؤسساتهم [٢].

وعَكس هذا القانون جهود واسعة النطاق من قبل الحكومة الصينية لإدارة أنشطة الفضاء الإلكتروني بشكل مباشر، ومكافحة التهديدات الإلكترونية التي يمكن أن تقوض الأمن على المستوى العالمي، كما وجدت الدراسة أن أغلب مواد القانون جاءت لتأكد سيطرت الدولة، على أغلب النشاطات الالكترونية وشبكات التواصل الرقمية، على مستوى الأفراد والمؤسسات والشركات الخاصة، في خطوة لتعزيز سيادة الدولة على الفضاء الالكتروني.

ثانياً: المحفزات الصينية في مجال الفضاء الإلكتروني

تعتبر الصين المجال الإلكتروني مجال حيوي بالنسبة لها ، وخاصة في الجانب الاقتصادي الذي عكس قوة الصين الصاعدة ، وكذلك انعكس هذا العامل على قدرة الصين في تقليل الفجوة الرقمية مع الولايات المتحدة المريكية ،وتتمثل هذه المحفزات في الأبعاد الآتية:

١- البُعد الاقتصادي: (القرصنة والجرائم الإلكترونية)، وأمن الشبكات الاستراتيجية الصينية لها محركان رئيسيان:

---

(١) احمد يوسف كيطان، استراتيجية الأمن الوطني السيبراني للصين: قراءة في قانون الأمن السيبراني الصيني، الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، ٢٧ تشرين الثاني ٢٠١٩، دراسة صادرة عن مركز النهرين للدراسات الاستراتيجية ، ، ص٣.

(2) Cybersecurity Law of the People's Republic of China, OP. Cit,p.15 .

أ- ضمان استمرار النمو الاقتصادي، فعدد السكان الذي تجاوز (١،٤ مليار) نسمة نهاية سنة ٢٠١٩، يعتبر مصدر قلق كبير للصين والخوف من انخفاض معدل النمو الاقتصادي وارتفاع معدلات سن الشيخوخة [١].

ب- ردع أي نشاط غير مرغوم عبر الإنترنت المحلي، حيث تحاول الجهات الفاعلة غير الحكومية في الصين الحصول على المعلومات الاقتصادية الصناعية من الولايات المتحدة بطرق عدة.

رغم إن الجانب الصيني يدحض هذه الاتهامات، مصراً على أن الدولة لا تدعم "أي نشاط تجسسي إلكتروني" [٢]. كما تبرُز الاستراتيجية السيبرانية للصين بشكل فعال في أنتاج وتصدير تكنولوجيا المعلومات والاتصالات الذي من المتوقع أن يصل الى (١,٨) ترليون دولار نهاية سنة ٢٠٢١ [٣]. مقارنة بالصادرات الامريكية البالغة (١٨٨،٧٨٦)مليار دولار لسنة ٢٠١٩من تكنولوجيا المعلومات حسب التقارير الرسمية للبنك الدولي [٤].

٢- البُعد السياسي: (السيادة في إدارة المعلومات والنشر)

تقوم الصين بتقييد استخدام الانترنيت وتفرض عقوبات على النشاط السيبراني الضار بالأمن القومي، أذ جاء في المادة (٥٩) من قانون الأمن السيبراني الصيني " في حالة عدم قيام مشغلي الشبكات بأداء واجبات حماية الأمن السيبراني... يتم فرض غرامة تتراوح بين (الف ومئة الف يوان صيني)..." [٥] وتقييد الوصول إلى المعلومات على الإنترنت أو وسائل التواصل الاجتماعي ومواقع التواصل، لحماية الاستقرار السياسي الداخلي، وتشعر الحكومة الصينية بالقلق

---

(١) صحيفة الشعب اليومية الصينية، عدد سكان الصين يتجاوز ١,٤ مليار نسمة في ٢٠١٩، الموقع الرسمي للصحيفة ١٧كانون الثاني ٢٠٢٠. متاح على الموقع: تأريخ الزيارة ٢١أذار ٢٠٢١ =
h ttp://arabic.people.com.cn/n3/2020/0117/c31664-9649819.html =

(2) Amy Chang, Op.cit, pp. 21,23.

(٣) عبد الكريم زهير عطية الشمري، مصدر سبق ذكره، ص ٩٢.

(٤) صادرات التكنولوجيا المتقدمة (بالأسعار الجارية للدولار الأمريكي، الموقع الرسمي للبنك الدولي، متاح على الموقع:
https://data.albankaldawli.org/indicator/TX.VAL.TECH.CD.٢٠٢١ تأريخ الزيارة ٢٢أذار.

(4) Amy Chang, Op .cit, p,24.

(5) Ibid,pp25-26.

من الوصول غير المقيد إلى الإنترنت أو المعلومات غير المنضبطة، وللتخفيف من أثار ذلك، نفذت الصين تدابير تتطلب "تسجيل الأسم الحقيقي" للمستخدم للشبكات الاجتماعية ". وتستخدم الحكومة الصينية أيضا جهات فاعلة غير حكومية، للقيام بأعمال تُوصف من قبل الولايات المتحدة كونها تجسسيه، بينما ترى الصين أنها من أجل المصلحة الوطنية، لذلك تقترح الصين طريقة مميزة للفضاء السيبراني، تسمح للصين بالتحكم في حركة الانترنيت داخل حدودها، بينما يشمل المفهوم الغربي للفضاء السيبراني مفهومًا مفتوحًا، من حيث التدفق الحر للمعلومات عبر الحدود.

٣- البُعد العسكري: (التطبيقات الإلكترونية في مجال الدفاع الوطني)

تشير الدراسة التي أجرتها الباحثة (Am Chang)، إن الصين قامت باستخدام شبكة الإنترنت وتكنولوجيا المعلومات في المجال العسكري منذ عدة سنوات، ألا إن الحدث المهم والذي أحدث نقطة التحول الرئيسية في النهج الصيني، هو استخدام الولايات المتحدة للتكنولوجيا العسكرية المتقدمة في حرب الخليج، فمنذ ذلك الحين بدأت بكين بالاهتمام بالأبحاث العلمية وزيادة الأنفاق عليها؛ لتطوير تكنولوجيا المعلومات والاتصالات من أجل توظيفها في الحروب المستقبلية وظهور ما يسمى بنظرية (تهديد الصعود الصيني) [١].

لقد عملت الصين على ترسيخ أُسس استراتيجية الأمن الإلكتروني في العلوم والأدبيات العسكرية الصينية، مثل: المبادئ التوجيهية للاستراتيجية العسكرية (The Military Strategic Guidelines)، وعلم الاستراتيجية العسكرية (The Science of Military Strategy) واستغلال المجال الالكتروني في اساليب الدفاع والهجوم [٢].

وبسبب اختلاف الثقافات الاستراتيجية فإن ما قد تعتبره الصين آليات دفاعية، قد يفسر من قبل الولايات المتحدة وغيرها من الدول الغربية على أنهُ آليات هجومية. ولن تكون قضية تايوان والنزاعات الاقليمية والبحرية بعيدة عن تلك النشاطات العسكرية الإلكترونية بين الصين والولايات المتحدة.

(1) Michael S. Chase, Arthur, Op.cit, p. 2.

(2) Amy Chang, Op.,cit, pp. 27-28.

المطلب الثاني: الاستراتيجية الصينية للأمن الإلكتروني على المستوى الخارجي

الاستراتيجية الصينية في مجال الأمن الالكتروني، تسعى إلى تعزيز أنظمة الحماية والدفاع الإلكترونية نتيجة التطور المستمر في التقنية الرقمية، وهنا تحاول الدراسة فهم استراتيجية الأمن الإلكتروني الصينية، وبيان الموقف الصيني من النشاط الامريكي في هذا المجال، ونظرة الصين للمؤسسات الدولية ودورها في مجال الأمن السيبراني.

اولاً: اهداف استراتيجية الأمن الإلكتروني الصينية

لفهم هذه الاستراتيجية لابد من معرفة الاهداف الاستراتيجية للصين وسلوكيات السياسة الخارجية لتقليل احتمالية سوء الفهم وسوء التقدير، من خلال تعزيز الحوار بين الجهات الفاعلة الإقليمية والدولية، وتعمل الصين على توسيع التفاعل بين مجتمع السياسة الخارجية الصينية ونظرائهم في البلدان الأخرى، وكان لتوقيع اتفاقية "عدم الاختراق" التاريخية سنة ٢٠١٥ مع الولايات المتحدة لتحقيق ميزة تجارية، تأثير في صياغة الاستراتيجية الصينية وتمرير التشريعات لتعزيز وضعها الأمني في مجال الفضاء، مع حماية مصالحها الاقتصادية، وتعمل الصين على تعزيز جبهتها المحلية بإطار قانوني، على سبيل المثال: (قواعد السلوك السيبراني، العقوبات الإلكترونية) وما إلى ذلك، من خلال القدرة على ممارسة الإجراءات القانونية ضد الأجانب الذين لهم مصالح في الدولة، وبالتالي الحفاظ على سيادتها السيبرانية [1].

وتوضح الدراسة التي نشرتها الباحثة (Amy Chang)، وجود اختلاف بين الولايات المتحدة والصين في تعريف بعض المصطلحات المعنية بموضوع الفضاء والأمن الإلكتروني، الأمر الذي يتسبب في وجود فجوة إدراكية، في فهم المصطلحات الالكترونية، وتضيف الدراسة إن الاستراتيجية الصينية لأمن الشبكات تتضمن استخدام المعلومات للتأثير أو السيطرة على عملية صنع القرار لدى الأعداء، وذلك لخدمة الأهداف الصينية الهجومية والدفاعية، وهذه التفسيرات –

(1) Emilio Iasiello, China's Cyber Initiatives Counter International Pressure, Journal of Strategic Security, Volume 10,issue 1,January 2016, p.6.

من وجهة نظر الكاتبة – تُعد أوسع نطاقاً من الرؤية الأمريكية في مجال الأمن الإلكتروني، التي تركز على تعزيز قدرات السيادة السيبرانية [١].

ثانيا: موقف الصين من النشاط الأمريكي في مجال الفضاء الإلكتروني

ترى الصين أن استراتيجية الأمن السيبراني الأمريكية مصدر تهديد للمصالح الصينية، حيث يركز العديد من المحللين الصينيين، على كيفية استخدام الولايات المتحدة لتكنولوجيا الشبكات والمعلومات للتدخل في الشؤون الداخلية للدول الأخرى، وكيف تهدد الهيمنة الأمريكية الإلكترونية الأمن الصيني في المجالات المختلفة، ومن أكثر القضايا التي أثارت مخاوف وقلق الصين في هذا المجال هو، إعلان الولايات المتحدة في تموز ٢٠١١ أن الفضاء الإلكتروني أصبح مجالاً جديداً للحرب، فضلاً عن تسريبات "سنودن" الاستخباراتية في ايار وتموز ٢٠١٣ [٢]. واتهام وزارة العدل الأمريكية خمسة من ضباط (جيش التحرير الشعبي الصيني)، بتهمة التجسس الاقتصادي في إيار ٢٠١٤، كل من الحالات الموضحة أعلاه تُشير إلى أنه بغض النظر عن السبل المتبعة لتغيير سلوك الصين (العسكري والدبلوماسي والاختراق الالكتروني) في هذه الحالات، فأن جهود تعديل السلوك الأمريكي الذي يهدد الأمن القومي الصيني أو تخترق سيادتها، من المحتمل أن تثير ردود فعل غير مرغوب فيها من قبل الحزب الحاكم (CCP)، لذا وضعت الصين في مقابل هذه التحديات أهدافاً رئيسية لتعبئة الحرب الإلكترونية في بكين، من أبرزها تدريب الموظفين العسكريين والمدنيين على الحروب الإلكترونية، وتشكيل وحدات حربية ووحدات احتياط متخصصة في مجال الفضاء والأمن السيبراني [٣].

إنّ تأثير إعلان الولايات المتحدة للفضاء السيبراني كمجال جديد للحرب وإنشاء الولايات المتحدة الأمريكية لما يُسمى: (CYBERCOM) * في حزيران ٢٠٠٩ قد غيرت من ملامح ساحة

---

(١) إسراء احمد اسماعيل، عناصر الاستراتيجية الصينية للأمن الإلكتروني، ٥ شباط ٢٠١٥.متاح على الموقع: https://futureuae.com/ar-/MainPage/Item/684.٢٠٢١ تأريخ الزيارة ٢٢أذار

(2) Edward Snowden: Leaks that exposed US spy programme, BBC NEWS, 17 January 2014 .

(3) Amy Chang Op,.cit,. p, 27.,

* هي تمثل القيادة الإلكترونية الأمريكية(USCYBERCOM) تأسست في منتصف عام ٢٠٠٩ في مقر وكالة الأمن القومي (NSA) ويرأسها بشكل مدير جهاز الأمن القومي منذ إنشائها. جزء من وزارة الدفاع الأمريكية ولها

المعركة العالمية، لذا تُفضل الحكومة الصينية تجنُب التعاون مع واشنطن، وذلك يعود لثلاثة أسباب رئيسية وهي: [١]

١- عدم الثقة بإقامة علاقات تتمتع بالشفافية مع واشنطن.

٢- لاحظت الصين عدم التزام الولايات المتحدة بالمعاملة بالمثل في تبادل المعلومات.

٣- خسارة الولايات المتحدة لمكانتها القيمية، بعد تسريبات "سنودن" الاستخباراتية، الأمر الذي أعطى الصين المُبرر لتأخير أو رفض أي طلبات متعلقة بتعديل توجهاتها في مجال الفضاء الإلكتروني.

ثالثاً: موقف الصين من الأمن السيبراني في المؤسسات الدولية

بما إن قواعد القانون الدولي لم تحدد بعد بشكل دقيق تقنين عمليات شبكة الكمبيوتر، قامت الصين بتعديل قانونها السابق، الذي يعتبر أن قوانين النزاع المسلح لا تنطبق على النشاطات السيبرانية، وكعضو في مجموعة الخبراء الحكوميين التابعة للأمم المتحدة، وافقت الصين في تقرير تموز ٢٠١٣ الصادر عن (GGE)* أنه يجب أن يُوجه القانون الدولي للأمم المتحدة سلوك الدول – في المجال السيبراني –، حيث يذكُر التقرير أن "القانون الدولي، وبناء على ما جاء في ميثاق الأُمم المتحدة، هو قابل للتطبيق وضروري للحفاظ على السلام والاستقرار وتعزيز الانفتاح والأمن، وأن تكون بيئة تكنولوجيا المعلومات والاتصالات سلمية ويسهل الوصول إليها". كما وافقت على القاعدة التي تنص على: "يجب على الدول الوفاء بالتزاماتها الدولية فيما يتعلق بالأفعال غير المشروعة دوليًا المنسوبة إليها، وعدم السماح للجهات الفاعلة باستخدام أراضيها بشكل غير قانوني"

دور أساسي في الحرب السيبرانية وتعمل على توحيد أتجاه عمليات الفضاء الإلكتروني، وتعزيز قدرات الفضاء الإلكتروني لوزارة الدفاع، للتفصيل ينظر: الموقع الرسمي للقيادة الأمريكية السيبرانية، متاح على الموقع: تأريخ الزيارة ٢٢أذار ٢٠٢١.

Official website of the United States' Cyber Command. https://www.cybercom.mil

(١) علي زياد العلي، مصدر سبق ذكره، ص ص١٦٩-١٧١.

* (GGE) (Group of Governmental Experts) وهي هيئة مكونة من ١٥ عضوًا ضمن مؤسسات الأُمم المتحدة مهمتها الدراسة وبناء المعايير في مجال المعلومات وتقديم التقارير حسب اختصاصها. للتفصيل ينظر: Available at Link: The United Nations Group of Governmental Experts https://dig.watch/processes/un-gge.Date visit 1 May 2021

[١]. يشير قبول الصين لقابلية تطبيق القانون الدولي على الفضاء الإلكتروني إلى حالة واحدة وهي الامتثال للمعايير الغربية، على سبيل المثال يؤيد "ليانغ يابين"**، بسياق كتاباته في Times (Study Schools Party Central) فكرة إضفاء الديمقراطية على حوكمة الإنترنت من خلال الأُمم المتحدة وتحدي هيمنة الولايات المتحدة على هذا المجال [٢].

المطلب الثالث: تطوير الردع الاستراتيجي الصيني في الفضاء الإلكتروني

تعتمد عوامل الردع الاستراتيجي في الصين على تحليل التهديدات الأمنية المستجدة، نتيجة التطورات السريعة في مجال الفضاء الالكتروني، ويعتقد الباحثون والمختصون في الاستراتيجية الصينية،(Liang Yabin Amy Chang) إن الجيش الصيني يجب أن يكون قادراً على حماية المصالح الصينية في الفضاء والفضاء الإلكتروني والتي سوف نوضحها في محورين الأول: هو الردع من خلال الفضاء الالكتروني، والثاني قدرات حرب المعلومات.

اولاً: الردع من خلال الفضاء الإلكتروني

تنظر الصين إلى الفضاء الإلكتروني كمجالات هامة للردع الاستراتيجي، إذ أصبح الفضاء الإلكتروني ركيزة اساسية للتنمية الاقتصادية والاجتماعية ومجالًا جديدًا للأمن القومي، و أصبحت المنافسة الاستراتيجية الدولية في الفضاء الإلكتروني شرسة بشكل متزايد، وتدعي الصين بانها واحدة من أكثر الدول التي تعرضت لهجمات القراصنة ، حيث تُواجه أنظمة البنية التحتية للشبكات تهديدات خطيرة ، كما يتزايد تأثير الفضاء الإلكتروني على الأمن العسكري بشكل تدريجي، وتسعى لتسريع بناء قوات الفضاء السيبراني [٣].

---

(1) Amy Chang, Warring State, Op. cit,pp.27,30.

** ليانج يابين، أستاذ مشارك، في معهد الدراسات الاستراتيجية الدولية مدرسة الحزب التابعة للجنة المركزية للحزب الشيوعي الصيني. للتفصيل ينظر: ThinkINchina متاح على الموقع:

https://thinkinchina.asia/liang-yabin/ تأريخ الزيارة ١ ايار ٢٠٢١

(2) Michael S. Chase, Arthur Chan, Op. cit, pp.3,14.

(3) Xinhua News Agency, China's military strategy (May 2015), Information Office of the State Council of the People's Republic of China,p.8.

ومع توسع مصالح الصين – ونقاط ضعفها المحتملة– في هذه المجالات، مع رغبتها في إنشاء عالم متعدد الاقطاب على حساب الولايات المتحدة الأمريكية، وحسب محللين وخبراء استراتيجيين في جيش التحرير الشعبي، فإن مجالات الفضاء الإلكتروني لم تعد تمتلك أهمية متزايدة فحسب؛ وإنما باتت محل نزاع، حيث جاء في التقرير الحكومي بعنوان "الاستراتيجية العسكرية" سنة ٢٠١٥ أن "مجالات الفضاء الإلكتروني أصبحت مجالات للمنافسة بين الدول" ما بين دول عدة، بما فيها الولايات المتحدة الأمريكية وروسيا واليابان وألمانيا والمملكة المتحدة وكندا [١].

وذلك عن طريق التطور السريع والتطبيق الواسع للعلوم وتكنولوجيا المعلومات، حيث تتحول شبكة الانترنيت إلى مجالات استراتيجية جديدة، يسمح للردع الاستراتيجي باستخدام أنواع عديدة من وسائل الردع ويُعرِّف خبراء الاستراتيجية في جيش التحرير الشعبي الصيني ردع الشبكات، أنه: "واحد من ثلاثة أنماط رئيسية للنزاع العسكري في مجال الشبكات"، إلى جانب "استطلاع الشبكات" و"هجمات الشبكات والعمليات الدفاعية"، إلا أن الردع في الفضاء الإلكتروني يختلف عن الردع الاستراتيجي التقليدي بجوانب عدة، منها صعوبة تحديد هوية المعتدي، أماكن تواجده، ونوع الأسلحة المستخدمة في الهجمات الإلكترونية أضافةً الى قلة التكاليف التي ربما يفقدها المُعتدي في حالة عدم امتثالهُ للردع في مجال الفضاء الإلكتروني [٢].وعلى الدولة تحصين مؤسساتها بأدوات الردع لمنع الهجمات الإلكترونية ضد البنى والموؤسسات الحيوية ومن هذه الأدوات هي [٣] .

١- انشاء نظم انذار مسبق.

٢- تعدد مصادر الطاقة داخل البلاد ، مثلا ايجاد بديل تقليدي لتشغيل الطاقة الكهربائية عندما تتعرض لهجوم الإلكتروني.

٣- تشفير البيانات الرئيسية، مثل البيانات العسكرية والمالية المهمة .

---

(١) مايكل إس تشايس، آرثر تشان، نهج الصين المتطور "إزاء الردع الاستراتيجي المتكامل، مؤسسة راند في سانتا مونيكا، كاليفورنيا، ٢٠١٦، ص ١٤.

(٢) المصدر السابق، ص١٦-١٧.

(٣) ايهاب خليفة ، إمكانية تحقيق الردع في صراعات الفضاء الإلكتروني ، مجلة اتجاهات الأحداث ، العدد ١٣، آب ٢٠١٥ ، ص ٥١.

ثانياً: قدرات حرب المعلومات (information warfarecapabilities)

إنّ مفهوم حرب المعلومات(IW)* يبقى في حالة تجدد مستمر بسبب التطور السريع في هذا المجال، وحسب العقيدة المشتركة للصين والولايات المتحدة بخصوص الحرب المعلوماتية، فأنها تعني "الإجراءات المتخذة للتأثير على نظم المعلومات ومعلومات الخصم أثناء دفاع المرء عن نظم المعلومات الخاصة بها " [١]. وتصف وزارة الدفاع الصينية في تقريرها السنوي لسنة ٢٠١١ الخاص بقدراتها العسكرية "المعلوماتية" على أنها "الظروف التي تستخدم فيها القوات العسكرية الحديثة أنظمة الكمبيوتر وتكنولوجيا المعلومات وشبكات الاتصالات المتقدمة للحصول على ميزة عملية على أي خصم"، وقد عَدّ المحللون الصينيون الحرب المعلوماتية نوع من "الحرب غير التصادمية" حيث لم تُعد المسافة تمثل عائقا في ساحة المعركة، ويلبي ذلك المتطلبات المتأصلة لهجمات القوة النارية القتالية المشتركة غير التصادمية في الحرب المعلوماتية، وهذا هو جوهر ساحة أي معركة معلوماتية، ويعتبر توجه الصين لحرب المعلومات (IW) كأسلوب لخوض الحرب غير المتكافئة ضد الولايات المتحدة [٢].

والغرض من حرب المعلومات، هو التأثير على قرارات الخصم او تعطيل القرار او أحداث أرباك في معلومات الخصم، وبالتالي يكون القرار خطأ أو غامضاً. لقد حققت الصين إنجازات مثيرة للإعجاب في مجال قدرات حرب المعلومات بما في ذلك التطورات المتعلقة بعمليات الشبكات الحاسوبية، التي تساعد الجيش الصيني على جمع المعلومات لتنفيذ هجمات الكترونية فعالة،

---

* information warfare. ظهر هذا المفهوم في منتصف التسعينات بعد ان أصبحت تكنولوجيا المعلومات والرقمنة وشبكات الانترنيت تشكل عامل أساسي في كافة المجالات وخاصة العسكرية والسياسية لأغلب الدول المتقدمة منها خاصة. للتفصيل ينظر:

Dean Cheng, "Prospects for China's Military Space Efforts," in Roy Kamphausen, David Lai, and Andrew Scobell, eds., 34.Beyond the Strait: PLA Missions Other Than Taiwan, Carlisle, Pa.: Strategic Studies Institute, April 2009, p.224.

(١) تيموثي آر هيث، كريستين غانيس، كورتيز إي كوبر، إعادة تطوير الصين وجيش التحرير الشعبي: الاستراتيجية العسكرية واستراتيجية الأمن القومي–ومفاهيم الردع والقدرات القتالية–، مؤسسةRAND ،سانتا مونيكا، كاليفورنيا.، ٢٠١٦،ص ص٣٥-٣٦.

(2) Toshi Yoshihara, CHINESE INFORMATION WARFARE: A Phantom Menace Or Emerging ONDAN Threat?, The Strategic Studies Institute (SSI) is part of the U. S. Army War College, Washington,2001,p.3.

وبحسب وزارة الدفاع الأمريكية، فإن مثل هذه الهجمات "يمكن تنفيذها لتقييد أفعال الخصم وتأخير زمن الاستجابة من خلال استهداف الجوانب اللوجستية المتعلقة بالشبكة والاتصالات والأنشطة التجارية" [1].

من خلال ما تقدم يمكن القول أن العلاقات الصينية – الأمريكية تتراوح بين الهدوء والتوتر من حين لآخر ويبدو إن السمة الاساسية ستكون مبنية على المنافسة الاستراتيجية، وتبقى المصالح المشتركة بينهُما الأساس الذي يضبط سلوك كل بلد تجاه الآخر، ويخفف من حدة التوترات التي تحدث لأسباب عدة، حيث طغت الأسباب الاقتصادية على علاقة التنافس بين الصين والولايات المتحدة، وتتميز استراتيجية الصين بالانتشار الهادئ – الصعود السلمي– وتسعى دائما لدعم اقتصادها وتقويته، أذ ينمو بمعدلات تعتبر الاعلى عالميا، وهي أكبر دائن للولايات المتحدة الامريكية، وتذهب الدراسة، بأن النقاشات حول تأثير جيش التحرير الشعبي الصيني وخطورة الهجمات التي تدعي واشنطن انها من فعله، مبالغ فيها ويراد منها في أحيان كثيرة الضغط على الصين وتهيئة الرأي العام الدولي لتقبل الصورة التي ترسمها الولايات المتحدة عن الصين، وهذا فيه جانب من الصحة بسبب الكثير من عمليات التجسس التي تقوم بها الولايات المتحدة، على مستوى الافراد والمؤسسات وقادة الدول، التي أجاز بعضها القانون الامريكي؛ لحماية الأمن القومي للولايات المتحدة.

تضمن الفصل الثاني العلاقات الامريكية – الصينية في مجال الفضاء الالكتروني، واستراتيجيتهما السيبرانية وتوظيف القوة الالكترونية في التفاعلات السياسية، وبقي أن نوضح في الفصل الثالث، التنافس السيبراني الأمريكي– الصيني (في الفضاء الإلكتروني) وأفاقه المستقبلية، من خلال بيان سعي الولايات المتحدة والصين لتطوير الأسلحة فائقة السرعة (الفرط صوتية)، والسباق لاستثمار موارد الفضاء الخارجي التي سوف تشكل ميداناً جديداً للتنافس.

(1) Michael S. Chase, Arthur Chan, OP. cit, pp. 26-27.

الفصل الثالث

التنافس السيبراني الأمريكي- الصيني وأفاقهُ المستقبلية

لقد كان من نتائج التطور التقني والمعلوماتي هو استخدام القوة الذكية والرقمية لتحقيق المصالح القومية للدول، وعدم الزج بالقوة التقليدية في أماكن النزاعات التي تتواجد فيها مصالح الدول، وخاصة – الولايات المتحدة والصين – مما دفع إلى التركيز على الفضاء الالكتروني لتحقيق الأمن السيبراني، والتوجه لمقاربات دولية تتوافق مع معالجة المخاطر السيبرانية، فمن أولويات الاستراتيجية الامريكية هو الهيمنة على الفضاء الالكتروني، بالمقارنة مع الصين التي تحاول إخفاء رغبتها نحو الصدارة، وطرح مبدأ الصعود السلمي في تولي مركز القيادة العالمية، انطلاقا من مكانتها الاقتصادية التي تُعبر عنها في مبادرة الحزام والطريق، ليصبح الفضاء الإلكتروني في المستقبل أهم مجالات التنافس والصراع بين القوتين، الذي يمثل امتداد للتنافس التجاري وتكنولوجيا المعلومات والاتصالات.

وقد أصبحت العديد من القطاعات الحيوية مثل النقل والطاقة والصحة والتمويل والأهم من كل ذلك هو انتاج الأسلحة ذات التقنية المتطورة، ميداناً للتنافس والتي تعتمد بشكل متزايد على التقنيات الرقمية لتنفيذ مهامها الأساسية، حيث توفر الرقمنة فرصًا وحلولًا للعديد من التحديات التي تواجه العالم، ولكنها في الوقت نفسه تعرض الاقتصاد والمجتمع للتهديدات السيبرانية، وأمام التطوير المستقبلي للأمن السيبراني العالمي طريق طويل لكي تقطعه الدول، وذلك لأن هذا المجال من الأمن في معظم الدول مجال حديث ضمن الأمن القومي، رغم أن الجميع يتطلع إلى اتجاه التطوير المستقبلي للأمن السيبراني، في هذا الفصل سوف نتناول أبرز الافاق المستقبلية للتنافس المعلوماتي وتجارة الأسلحة بين الولايات المتحدة والصين. من خلال ثلاثة مباحث.

المبحث الأول: التنافس التكنولوجي لتجارة الاسلحة السيبرانية

المبحث الثاني: التنافس المعلوماتي بين الولايات المتحدة والصين

المبحث الثالث: مستقبل الأمن السيبراني (للولايات المتحدة الأمريكية والصين)

المبحث الأول: التنافس التكنولوجي لتجارة الاسلحة السيبرانية

يواجه المجتمع الدولي في الوقت الحالي، عددًا كبيرًا من التهديدات الأمنية التي تَتسم بتغُيرها وتطورها المستمر، وأتساع نطاق تأثيرها الذي يمتَد ليؤثر في الأمن العالمي بشكل عام، ولعل أبرز هذه التَهديدات الأمنية المعاصرة وأكثرُها حداثة وأوسعُها انتشاراً، هي الأسلحة السيبرانية التي أصبحت من التعقيد بمكان، حيثُ بات من الصعب حصرُها أو تطوير استراتيجيات مُحكمة لمواجهتها بشكل كامل، خاصةً مع تعدد أشكَالها وصعوبة معرفة مصادرها وتَطورها المُتسارع والمستمر، أضافة إلى سعة تأثيرها مقارنةٌ بُكلفة استخدامها المنخفضة وإمكانية استعمالها من قبل الفواعل من غَير الدول (الافراد والجماعات المسلحة والشركات)، ومن أجل معرفة التطورات في ميدان الأسلحة الالكترونية، سيتم تقسيم هذا المبحث الى مطلبين : المطلب الأول أنواع الأسلحة السيبرانية والمطلب الثاني: التنافس الصيني – الأمريكي في مجال التكنولوجيا العسكرية.

المطلب الأول: أنواع الأسلحة السيبرانية

تُعرّف الأسلحة السيبرانية بأنها: "تلك الأدوات التي يتم استخدامها أو التهديد بها لأحداث الضرر المادي أو الوظيفي للأجهزة والنظم والهياكل الإلكترونية وتختلف الأسلحة السيبرانية من حيث درجة خطورتُها وتعقيدها، وتتراوح ما بين أسلحة بسيطة قادرة فقط على إحداث ضَرر خارجي بالنظام الإلكتروني دون اختراقه، وأخرى مُعقدة يمكن من خِلالها اختراق النظام وإحداث أضرار بالّغة به قد تؤدي إلى تدميره كلياً أو توقفه عن العمل بشكل كامل" [١]. اذاً هي نوع من البرامج التي يتم تصميمُها للقيام بوظائف مختلفة (الدفاع والهجوم) وفى النقاط التالية، نُوضح أبرز أنواع الأسلحة السيبرانية وأكثُرها استخدامًا على الساحة الدولية وهي [٢]:

١- فيروسات الحاسُوب (Viruses): وهي برامج صُممت لتعديل أو تخريب خصائص الملفات أي إن الغرض منها هو الحاق الضَرر بحاسوب آخر او السيطرة عليهِ.

---

(١) نوران شفيق، أشكال التهديدات الإلكترونية ومصادرها، المركز الاوربي لدراسات مكافحة الارهاب، المانيا – هولندا، ٢٩ كانون الثاني ٢٠٢٠،ص ٤.

(٢) إيهاب خليفة، القوة الالكترونية، مصدر سبق ذكره، ص ص٨٣- ٨٧.

٢- الديدان (worms):هي برامج صغيرة تَتكاثر بنسخ نفسَها عن طريق الشبكات وصممت للقيام بأعمال تخريبية وسِرقة البيانات الخاصة بالمستخدمِين أثناء تصفحُهم الانترنيت وتكون سريعة الانتشار ويصعُب التخلص منها.

٣- أحصنة طروادة (Trojan Horses): هي عبارة عن شيفرة أو برنامج صَغير مَخفي ضمن برنامج أكبر، يكون ذو شعِبية عالية ويقوم بنشر دُودة أو فايروس ومن الصعب اكتشافه؛ حيث يعمل على مسح اثارهُ التي لا تحمل صفة تخريبية، ويعمل على أضعاف أنظمة الدفاع لدى الضحية؛ ليُسهل اختراق جهازه وسرقة البيانات.

٤- القنابُل المنطقية (Logic bombs): وهي من أنواع أحصنة طروادة التي سبق ذكُرها وتوضع داخل النظام الذي يُطوره المبرمج وتصمم للعمل عند أحداث معينة او تنفيذ أمر ما وتُسبب تخريب او مسح بيانات النظام للطرف المُستهدف.

٥- الابواب الخلفية (backdoors)*: يتركها مُصمم النظام عمداً للدخول الى النظام عند حاجتهِ لذلك، إذ تقوم الدول الكبرى المصدِرة للبرمجيات بترك مثل هذه الثغرات لاستخدامها عند الحاجة، وخاصة اثناء حرب المعلومات ضد نظام أي دولة اجنبية اخرى. وقد يستغُلها القراصنة في استهداف البيانات أو شن هجمات من قبل مجموعات القرصنة غير الحكومية، التي تقوم بهجمات برامج الفدية باستخدام الأبواب الخلفية على الخوادم (Exchange) التي تركها مصمّمو الدول القومية وراءهم [١].

٦- الرَقائق (Chipping): قد تتضمن الرقائق الإلكترونية وظائف لا تَعمل في الظروف العادية أو عندما يتم الاتصال بها عن بعد، حيث يمكن أن تستجيب لتردد معين لبعض موجات الراديو، فتشل الحياة في مجتمع او دولة ما.

---

* قامت الشركة اليابانية المعروفة (Sony) في عام ٢٠٠٥ بشحن ملايين الأقراص المدمجة الموسيقية للعملاء في جميع أنحاء العالم، وكانت هناك مشكلة كبيرة مع هذه المنتجات، حيث اختارت الشركة تثبيت الجذور الخفية (rootkit) على كل قرص مضغوط، مما يعني أنه كلما تم وضع القرص المضغوط في جهاز كمبيوتر، يقوم (rootkit) بتثبيت نفسه على نظام التشغيل، عندما يتم ذلك، ستستطيع الشركة الاستماع للمستخدم وترسل البيانات مرة أخرى إلى خوادم الشركة. للتفصيل ينظر: إيهاب خليفة، القوة الإلكترونية مصدر سبق ذكره ص٨٤.

(1) Global Cyber News ,April 7 2021, A message from the Carnegie Carnegie Cyber Policy Initiative, Endowment via the e-mail to the researcher's e-mail للتفصيل حول الابواب الخلفية والثغرات الالكترونية يمكن الاطلاع على نص الرسالة في الملحق رقم (٥).

٧- المدافع (HERF): وهي عبارة عن مَدافع تطلُق موجات راديو مركزه وعالية الطاقة والتردد، والتي يُمكنها تعطيل وأتلاف أي هدف إلِكتروني، مثل أغلاق شبكة حاسُوب أو إعادة تشغيلهُ بشكل دوري مما يُسبب ضرر بالغ في الشبكة.

٨- القنابل (EMP): هي تشبهَ المدافع غير أنها تستّخدم نبضات الكترومغناطِيسية، من خلال التَسلل الى مُواقع العدو الإلكترونية الحساسة، والتي سوف تُسبب تلف كل الحواسيب والشبكات في دائرة انفجارها غير المُدوي او المشتعل، وضررها أوسع وأبعد من المدافع كونَها؛ لا تنتقي الهدف بل تُصيب عدة أهداف بدون تَحديد.

وقد استُخدمت أغلب أنواع هذه الأسلحة السيبرانية، على مدى السنوات العَشرين الماضية في كثير من الهَجمات الإلكترونية، سوآء على مستوى الدول، الشركات او الأفراد وقد أصدر مركز الدراسات الاستراتيجية والدولية (CSIS) في واشنطن دراسة لأهم الاحداث والهجمات السيبرانية مُنذ ٢٠٠٦ ولغاية ٢٠٢٠ [١].

ويمكن اعتبار الصراع بين استونيا ورُوسيا عام ٢٠٠٧، وحرب رُوسيا على جُورجيا سنة ٢٠٠٨، أمثله واضحة أُستُخدم فيها السلاح السيبراني "كما قامت الاستخبارات الروسية بتنفيذ هجمات إلكترونية واسعة التأثير في ٢٨ تشرين الاول ٢٠١٩ ضد قواعد البيانات بجورجيا، مستهدفة مواقع حكومية ووسائل إعلام ومؤسسات غير حكومية وهيئة المحاكم، وتسببت بتعطيل برامج قنوات التليفزيون بالبلاد" [٢]، فضلا عن اختراق البريد الالكتروني الخاص ب(**John Podesta**) رئيس الحملة الانتخابية للمُرشحة للرئاسة الامريكية (هيلاري كلينتون) في تموز ٢٠١٦، والهُجوم الايراني على عدد كبير من الحُواسيب لشركة ارامكو السعودية في ١٤أيلول ٢٠١٩، جميعها تُعتبر هجمات إلكترونية [٣]. وتأتي الولايات المتحدة الأمريكية في المرتبة الاولى

---

(1) Significant Cyber Incidents Since 2006, Washington, Op. cit, pp.4-47.

للتفصيل ينظر: اهم الاحداث والهجمات السيبرانية منذ عام ٢٠٠٦ -٢٠٢٠.

(٢) نهى العبادي، الاتحاد الأوروبي، تداعيات الحرب الإلكترونية مع روسيا، المركز الاوربي لدراسات مكافحة الارهاب والاستخبارات، المانيا، ١٣ نيسان ٢٠٢١، ص٣.

(٣) عبد الغفار عفيفي الدويك، استراتيجية الردع السيبراني.. التجربة الأمريكية، مجلة السياسة الدولية، المجلد ٥٣، العدد ٢١٣، مركز الأهرام ،القاهرة، حزيران ٢٠١٨، ص١٩٦.

عالميًا من حيث التعرُض لهجمات سيبرانية، تليها المملكة المتحدة في المرتبة الثانية، وذلك وفقًا للموقع السويدي المُهتم بتكنولوجيا المعلومات والأمن الإلكتروني (SPECOPS) [١].

المطلب الثاني: التنافس الأمريكي الصيني في مجال التكنولوجيا العسكرية (فائقة السرعة)

يختص هذا المطلب ببيان أهمية (العناصر الارضية النادرة)* في صناعة تكنولوجيا الأسلحة المتطورة، والتي تُشكل عامل ضغط من قبل الصين تجاه الولايات المتحدة الأمريكية، في مجال التكنولوجيا المتطورة لصناعة الأسلحة فائقة السرعة.

تعتبر العناصر الأرضية النادرة أحد أهم نقاط التنافس التجاري بين الولايات المتحدة والصين، إذ تزود الصين العالمَ بأغلب احتياجاته منها، وتسعى الصين غالباً لاستخدامها كوسيلة للضغط السياسي في المفاوضات التجارية مع الإدارة الأمريكية، رغم أن الخبراء يرجحون أمكانية ايجاد بديل عنها ولو على المدى الطويل في حال أوقفت الصين تصديرها تمامًا[٢] . ويوضح (يوجين جولز)، أستاذ العلوم السياسية أنه في حالة قطع الإمدادات الصينية، فمنجم العناصر الأرضية النادرة الموجود في كاليفورنيا قد يكون البديل عنها كمرحلة أولى رغم المنافسة الصينية له، أضافة إلى محاولة إيجاد بدائل عن هذه المواد، وفي ضوء تهديد الصين باستخدام ميزة العناصر الأرضية النادرة كسلاح، قد تستثمر شركات أكثر في اختراعات تستعيض عن هذه المواد بشيء آخر،

---

(١) نهى العبادي، مصدر سبق ذكره، ص٤.

* العناصر الأرضية النادرة :(REE) هي مجموعة من سبعة عشر عنصرًا معدنيًا وتشمل هذه الأنواع الخمسة عشر اللانثانيدات في الجدول الدوري بالإضافة إلى سكانديوم والإيتريوم، وتعد العناصر الأرضية النادرة جزءًا أساسيًا من العديد من الأجهزة عالية التقنية. وخاصة الصناعات العسكرية والأسلحة الذكية، أطلق اسم "نادرة" على هذه العناصر بسبب قلة الأماكن التي كانت تستخرج منها سابقا: للتفصيل ينظر:

(2) Reuters staff, China ready to hit back at U.S. with rare earths, Reuters newspapers, May 29 2019. =Available at Link:

https://www.reuters.com/article/us-usa-trade-china-rareearth-idUSKCN1SZ07V Date at 8 May 2021.

وخاصة خلال أزمة الأمداد التي حدثت سنة ٢٠١٠، على الرغم من أن الصناعات الخاصة بالأمن القومي قد تكون غير متهيئة للاستغناء عن العناصر الأرضية النادرة بشكل تام [١].

وتبرز أهمية تلك الموارد النادرة في انتاج الأسلحة المتقدمة في ترسانة الولايات المتحدة – من صَواريخ (Tomahawk) إلى الطائرة المقاتلة (F-35) والطرادات المُجهزة بنظام (Aegis)، التي تعتمد تمامًا على المكونات المُصنوعة باستَخدام (عناصر أرضية نادرة)، حيث تلّوح الصين بقطع الإمدادات الأمريكية مِن العناصر الأرضية النادرة، التي تَدخل في الصناعات الحربية الآنفة الذكر، والتي يمكن إدراجُها في قيود تَصدير التكنولوجيا الصينية إلى الولايات المُتحدة، وهي نفسَها استجابة للضُغوط الأمريكية على شركة الاتصالات العملاقة (Huawei)، وفي هذا السياق قال (جيمس كينيدي)*: لقد غيّرت الصين بِشكل فعال الطريقة التي تدير بها الحرب، ورُبما النتيجة ايضا، وقال (كينيدي): "الأرض النادرة هي في الواقع مُحفز للهيمنة، فأن دُخول الولايات المتحدة في صراع مع الصين، وحيث إن الأخيرة تُزود المواد المهمة لغالبِية الأسلحة عالية الجودة في الولايات المتحدة ؛ يمكُنها تحديد نتيجة الصراع الى حداً ما، ويمكن أن يؤدي ذلك إلى تحول في الهيمنة" [٢]، بمعنى تحول في الهيمنة إلى حداً ما لصالح الصين .

وفي هذا السياق خلُص مكتب المساءلة الحُكومية في عام ٢٠١٦ إلى أن "وزارة الدفاع الأمريكية، (البنتاغون) ليس لديها نهج شامل على مستوى الإدارة لتحديد العناصر الأرضية النادرة، التي تُعتبر بالغة الأهمية للأمن القومي، وكيفية التعامل مع اضطرابات الإمداد المحتملة لضمان الوصول المستمر والموثوق". أذ تخشى من عدم تُوفر هذه المواد في الظروف الحرِجة، كما أوضح

---

(1) Jeremy Hsu, Don't Panic about Rare Earth Elements, Scientific American, a division of Springer Nature America, INC.,May 31,2019,p.4-5.

* هو مؤسس الشركة الخاصة لاستشارات موراد الأرض النادرة تركز على التداعيات الأمنية كونها تدخل في صناعة الأسلحة الذكية. للتفصيل عن المواد النادرة ينظر:

Jamil Hijazi and James Kennedy, Caught between rare earths and Chinese dominance Part 2: A walk down memory lane,News China Rare Earth, April 23 2021.Available at Link: https://www.mining.com/caught-between-rare-earths-and-chinese-dominance-the-story-behind-everything-no-one-is-telling-you-part-two/. the Date visit 28-March 2012.

(2) Andrew Wagner, op. cit. television interview.

البنتاغون بِشكل واضح مخاوفهُ في مراجعة عام ٢٠١٨، والتي أتهمت الصين بتعمد الاستفادة من احتكارها لهذه المَعادن للضَغط على القاعدة الصناعية الدفاعية الأمريكية، على سبيل المثال، اعِتادت الولايات المتحدة على صُنع مغناطيس دائم من أيونات النيوديميوم والبُورون، وهي الأداة التي تُساعد في تُوجيه الصواريخ الموجهة إلى أهدافها؛ وهذه أغلبها تقريبًا مصُنوعة في الصين، ولا يتم تَصنيع أي منها في الولايات المتحدة، ووجدَ التقرير أنه في كثير من الحالات لا يوجد بديل لهذه المواد، وفي حالات أخرى يكون الوقت والتكلفة لاختبار وتأهيل البدائل "باهظةً" (١).

لذا فأن الصين تُمثل خطرًا كبيرًا ومتزايدًا على توريد المواد والتقنيات التي تُعتبر استراتيجية وحاسمة للأمن القومي للولايات المُتحدة، وهي تشكل نقاط الضَعف المُحتملة للأمن القومي مع اشتداد الحرب التجارية بيّن واشنطن وبكين، ويأتي ذلك في ظِل الصراع من أجل الهيمنة على التكنولوجيا الفائقة بين الصين التي تَسعى لتقود العالم في هذا المَجال، وبينَ الولايات المتحدة الأمريكية التي تُحاول الحفاظ على مكانتها في مواجهة الصين.

وقد أصبحت تِلك الهيمنة الصَناعية مُكملة لسِباق الصين السريع لمُواكبة الهيمنة التكنولوجية للجيش الأمريكي، والتي ظَهرت بشكل واضح خِلال حرب الخليج سنة ١٩٩١، عندما أحدثّت القنابُل الذكية والطائِرات بدون طيار (Drone) ثُورة في الحرب الحديثة، وتحاول الصين تقليل الفجوة في هذهِ الصناعة المُتطورة رغم إنها تمتلك عدة أنواع من هذه الطائرات، حيث تعمل حاليا على تصِنيع طائرة بدون طَيار من طراز (CH-7)* بمُواصفات عالية (٢).

أقنعَ هذا التطور القادة الصينِيين بضرورة اللحاق بالرَكب التكنولوجي؛ لتقليل الفجوة العسكرية مع الولايات المتحدة الأمريكية، وقد أمضت بكين السُنوات الثلاثّين الماضية في فعل ذلك، كما

---

(١) إيهاب خليفة، مصدر سبق ذكره، ص٣.

* من المقرر انتاج هذا النوع عام ٢٠٢٢ بمواصفات تجعلها قادرة على التحليق بارتفاع ١٣ ألف متر وسرعة ٥٧١ ميل/ ساعة. للتفصيل ينظر: مصطفى كمال، الطائرات بدون طيار النشأة والتطور.

(٢) مصطفى كمال، الطائرات بدون طيار النشأة والتطور، مجلة السياسة الدولية، مركز الأهرام للدراسات السياسية والاستراتيجية، المجلد ٥٥، العدد٢٢٠، القاهرة، نيسان ٢٠٢٠، ص٢٣٤.

أشار الى ذلك نائب سكرتير الرئيس الامريكي لشؤون الدفاع الأسبق(Robert Work) (٢٠١٤-٢٠١٧) وزميلهُ السابق في البنتاغون (Greg Grant) [١].

وفي سياق سَعي الصين لتطويّر أسلحة فائقة السُرعة كما نَصت على ذلك الورقة البيضاء للدفاع الصيني؛ لتقليل الفجوة في التُفوق التكنولوجي الأمريكي وخاصةً في ميدان الاسلحة [٢].إذ ذكَرت الباحثة (كانيا) في (مركز الأمن الأمريكي الجديد)*، "إن الولايات المتحدة لم تُعد تمتلك هيمنة عسكرية وتقنية واضحة، وأن الصين تَظهر بسُرعة كقوة عظمى مُحتملة في مجال العلوم والتكنولوجيا." وإن الصناعة العسكرية الصينية رُبما تكون المنافس الأول للولايات المتحدة في استخدام الذكاء الاصطّناعي؛ لمُساعدتها على أتخاذ قرارات أفضل في ميدان المعركة، وفي سنة ٢٠١٧، أطلقت الصين، مجموعة من الأسلحة التكنولوجية الفائقةَ التي رُبما تُهدد التفوق العالمي للولايات المُتحدة، وتَشمل الابتكارات الصينية خمسة أنواع من الاسلحة [٣]:

١- المدفَع الكهرومغناطيسي

يُستخدم هذا المدفع طاقة كهرومغناطيسية قوية لإطلاق القذائِف على بعد (١٠٠ ميل بحري) (١١٥ ميلا)، أسَرع ٧ مرات من سُرعة الصوت وبخلاف المتفجرات، وهذا يقلل نطاق وسُرعة البنادِق التقليدية، التي تصِل مسافة ذخيرتُها فقط إلى (١٠ إلى ٢٠ ميلا بحريا) واختبرت الولايات المتحدة تكنولوجيا مماثلة الا أنها ليِست في البَحر.

---

(1) Andrew Wagner, Op.cit, p. 3

(2) Anthony H. Cordesman, China's New 2019 Defense White Paper: An Open Strategic Challenge to the United States Center for Strategic International Studies (CSIS), July 24 2019,P.1-3.

* وهو مؤسسة بحثية مقرها واشنطن. للتفصيل ينظر: موقع الأمن الأمريكي الجديد. متاح على الموقع: https://www.cnas.org/publications/reports/imbalance-of-power تأريخ الزيارة ١٢ نيسان ٢٠٢١

(3) Eric Baculinao, Chinese military innovations threaten American supremacy, NBC News Digital, Feb 17 2018., Available at: the Date visi. April 21-2021. https://www.nbcnews.com/news/world/these-chinese-military-innovations-threaten-u-s-superiority-experts-say-n848596#anchor-2Hightechwarships

٢- السُفن الحربية فائقة التكنولوجيا. أطلقت الصين هذا النوع من السُفن سنة ٢٠١٧ وهي مُصممة لتكُون مُضادة للطائرات والصوَاريخ والسُفن والغواصات، ويكون لها دورٍ مهماً ضمن تشكيلات حاملة الطائرات الصينية المُستقبلية.

٣- الطائِرات المُقاتلة: طائرة (تشنجدو جى ٢٠)، وهي أول طائرة شبح محلِية الصُنع يطلق عليها أسم (النسر الأسود)، ومن المتوقع أن تتصدى لنظِيراتُها الأمريكية طراز (أف٢٢) و(إف-٣٥)، وهي مُقاتلة من الجِيل الخامس تتَمتع بقُدرة إصابة الهدف وتوجيه ضَربات دقيقة على بُعد (٢٠٠ كيلومتر) [١].

٤- المَركبات المُنزلقة فائقة السُرعة (أسرع من الصوت).

في تَشرين الثاني ٢٠١٧ أجرت الصين أول اختبار للمركبة المُنزلقة فائقة السرعة (DF-17) وهي ذات مدى متوسط، وتمتاز بقدرتِها على الانزلاق إلى الارض بِمسار بطيءٍ ومُتعرج لتلافي أنظمة الدفاع الصاروخية الامريكية المُجهزة، ويُعتقد ان الولايات لم تجرِ اختباراً من هذا النوع بل تسعى الى تطويرهِ [٢].

٥- الذكاء الاصطّناعي: تسعى الصين لِخُطط طموحة لرفع مُستوى الغواصات النووية باستِخدام الذكاء الاصطّناعي وخُطط " لقيادة العالم" في هذا المجال، وتحقيق صناعةَ الذكاء الاصطناعي بقيمة (١٥٠ مليار دولار) أمريكي بِحلول عام ٢٠٣٠ [٣].

---

(1) Alexander Smith, China Offers First Glimpse of Chengdu J-20 Stealth Fighter, NBC News Digital, Nov. 1, 2016. Available at: https://www.nbcnews.com/news/china/china-offers-first-glimpse-chengdu-j-20-stealth-fighter-n676156. Date visit. April 24-2021

(2) Ankit Panda, Introducing the DF-17: China's Newly Tested Ballistic Missile Armed With a Hypersonic Glide Vehicle, The Journal December, December 28, 2017.= =Available at the link: https://thediplomat.com/2017/12/introducing-the-df-17-chinas-newly-tested-ballistic-missile-armed-with-a-hypersonic-glide-vehicle/. the visit at April 24 2021.

(3) Eric Baculinao, Op. cit. net.

وفي دِراسة جديدة لمركز الأمن الأمريكي الجَديد بشأن "التعويّض التقني العسكري" للصين قال (كينيدي) إن أسلحة الجيل القادَم من المُرجح أن تعتمد بشكل أكبر على المواد الأرضِية النادرة عاليةَ المُعالجة، بما في ذلك الصواريخ التي تفُوق سُرعتها سُرعة الصوت وأسلحة الطاقة الموجهة. لكن في الوقت الحالي، لا تزال الولايات المُتحدة بدُون إجابة لمعضِلة موارد الأرض النادِرة، بمعنى إنها لم تتّمكن من إيِجاد البديل المُناسب لهذه المواد لتقليل استيرَادها من الصين [1].

إنِّ أسلحة الفضَاء الإلكتروني ليست مُجرد المرحلة التالية في التطّور، الذي يجعل الحرب أقل فتكاً كما يَعتقد البعض، فاذا لم يتم التحُكم فيها بالطريقة السليّمة فقد تُؤدي الخلافات البسيطة إلى تفاقُم الاوضاع بصورةٍ تخرُج عن نطاق السِيطرة مما يُسبب اندلاع الحرب على نطاق واسع، بغض النظر أذا كان الامر مُتعمد ام عَفوي، كَما حدث مع الصين عندما فقدّت السيطرة على الصاروخ (Long March 5B) الذي سقطَ في المُحيط الهندي- بحر العرب –، كُل تلك الاحداث تُشكل مخاطر كبيرة على السّلم والاستَقرار العالمي.

(1) Keith Johnson, Lara Seligman, Op. cit.p.4.

المبحث الثاني: التنافس المعلوماتي بين الولايات المتحدة والصين

وفقاً للمعهد الدولي للدراسات الاستراتيجية في لندن، سيُشكل الفضاء الإلكتروني أحد أهم مَيادين التنَافس المعلوماتي والصراعات والحروب المُستقبلية، "فلا توجد دولة مهما عظُمت قدراتها العسكرية، ولا مؤسسة مهما عظمت قوتُها الاقتصادية في مأمن من خطر الهجمات الإلكترونية" [١]. وستكون الولايات المتحدة الأمريكية والصين من أكثر الدول مُنافسةً وتوتُر في هذا الحِيز الواسع من الفضاء، وقد تحولّت نظرة الولايات المتحدة إلى الصين، من كونِها شريكاً استراتيجياً إلى مُنافس استراتيجي. أذ تحدّت الصين الإدارة الامريكية في خمسة مجالات رئيسية: السِيطرة على حافة المُحيطين الهندي والهادي، والتِجارة والاقتصاد، بحث الصين عن معايِير تقنية بديلة، والسَعي وراء الهيمنة التكنولوجية والتقدُم العسكري الصيني. ومع ذلك، فهذا الخلاف مُعقد بسبب العلاقة الاقتصادية الوثيقة بينهما التي تتمثل بحجم التبادل التجاري الكبير بين البلدين .

المطلب الأول: التنافس الأمريكي – الصيني للسيطرة على موارد الفضاء

دَفع شُح الموارد في كوكب الارض إلى البحث في الفَضاء عن مُوارد أخُرى، وخاصة مع بداية القرن الحادي والعشرين؛ وذلك بِسبب وجوّد موارد نادِرة (البلاتين والذهب) في أجرام سماوية، بكميات تختلف عما هو مُوجود في كوكُبنا الارض، وقد بدَأت حديثاً قسم من شركات القطاع الخاص مثل (Google) في دعِم الاستثّمار في مجال المعادَن الفضائية، وذلك بسبب شحَة او بِداية نفاد قسم منها على كوكَب الارض؛ إن الماء ومكوناتهِ الاساسية (الاوكسجين والهيدروجين H2O) وهو أكثر مكونات وقُود الصواريخ، يمكن استخراجه من الاجرام السماوية الغنية بالكاربون، أذ تّم في سنة ٢٠١٦ تطوير نظام (Comet) وهو نِظام دفع فضائّي يعمل بالماء، وبالتالي يَمكن الاستفادة من الأجرام السماوية لاستِخراج هذا الوقود كونَها غنية بالكاربون [٢].

---

(1) Ashley J. Tellis, Alison Szalwinski, and Michael Wills, Strategic Asia 2020 U.S.– china competition for global influence, The National Bureau of Asian Research, January 21, 2020,p.2.

(٢) وثائقية دي دبليو: الأجرام السماوية – مناجم جديدة في الفضاء؟ متاح على الموقع: https://www.youtube.com/watch?v=3e9t24bIBUQ تأريخ الزيارة: ٤ نيسان ٢٠٢١

كُل هذا يدفع إلى التَنافس في الفضاء الإلكتروني وخاصة بين الولايات المتحدة والصين، لذا بدأ الفضاء الإلكتروني يشهد تغيُرات كبيرة، بسبب تَصاعد الخطاب في الدول المُتقدمة حول الموارد الطبَيعية في الفضاء الخارجي، والتي تُقدر قيمتُها بتريليونات الدولارات، (مثل البلاتين والتيتانيوم والطاقة الشمسية) [١]. ويُعد تطوير برنَامج الفضاء الصيني أولّوية بالنسبةِ لبكين، حيث دعا الرئيس (شي جين بينغ) البلاد إلى ترسيخ نفسها كقُوة فضائية، وتُصر الصين على أن برنامجها مُخصص للأغراض السلمية، لكن وزارة الدفاع الأمريكية تدّعي بأن أنشطة الصين، تهدُف إلى منع الخصُوم من استخدام الأصُول الموجودة في الفضاء في أي أزمة [٢].

وتُعد طمُوحات الصين الفضائية مدفوعةً باستراتيجية طويلة الأجل للحُصول على الموارد، إذ امَتلكت في سنة ٢٠٢٠ محطة فضائية خاصة بِها ؛ وبحلول عام ٢٠٥٠ تَطمح الصين إلى نظام طاقة شمسية تجارِي فضائي في مَدار جُغرافي متزامن، وأخيراً مستوطنة بشرية على سطح القمر، وتعمل الدولة على تطوير القُدرة على تعدين الكويكبات والقمر، لذا فإن إنشاء وجود مكانّي خارجي أطول، أو رُبما حتى دائم أمراً مطلوب إلى حدٍ كبير، وتتَجاوز أهداف الصين للفضاء في القرن الحادي والعشرين، الهدَف قصير المدى المتمثل في "أن تكُون الأولى" في الفضاء، إلى استثمارات طويلةِ الأجل ستفُيد الاقتصاد الصيني بشكل مُباشر، والسؤال الذي يطرح نفسهُ هنا هو: هل أن سعيّ الصين إلى الفضاء يُؤدي إلى صِراع مع الولايات المتحدة في هذا المجال، سيوفر فهم طبيعة طُموحات الفضاء الصينية الرئيّسية الثلاثة التالية:

١- الطاقة الشمسِية الفضائية: يَسعى النظام المُقترح إلى تسخير الطاقة الشمسية باستَخدام الأقمار الصناعية ثُم إعادة إرسال الطاقة إلى محطّات الاستقبال على الأرض بِاستخدام تقنية الميكروويف.

٢- التعدّين القمري والكويكبات، طُموح الفضاء الكبير القادِم للصين، هو استخراج موارد مثل التيتانيوم والهيليوم والمياه من سطحَ القمر.

---

(١) نامراتا جوسوامي، صراع مستقبلي: نشاط دولي واسع لاستغلال موارد الفضاء الخارجي، معهد الولايات المتحددة للسلام، العدد ٢٨، واشنطن، ٢٠١٨، ص ٥٨.

(2) Michael Martina, China aims for manned moon landing year 2036,Reuters, April 29, 2016.Available at Link: the Date visit on March 30- 2021.
https://www.reuters.com/article/us-china-space-moon-idUSKCN0XQ0JT

٣- محطة فضاء: استثمرت الصين بِكثافة في تَطوير محطتُها الفضائية الخاصة منذ سنة ٢٠١١ والتي أكمَلتها عام٢٠٢٠ وأطلقت عليها اسم (تيانجونج) (قَصر السماوية) [١].

في الخمسّين عامًا القادمة رُبما ستظهر مُنافسة أيضًا، حول أي نظام قيِم يصبح مهيمنًا على الموارد القائمة على الفضاء: "الاشتراكِية ذات الخصائِص الصينية" أو "النموذج الأمريكي لريادة الأعَمال الحُرة". هناك على الأقل سيناريوهان محتملان للنِزاع يمكن أن يُجهدا العلاقة الدبلوماسية.

الأول: هو إذا أقرّت الصين نسختُها الخاصة من قانون الكويكبات، الذي يُقنن منطقة عدم التدخل للقمر والكويكبات، ويُؤسس أساس الادعاء لمبدأ "من يأتي أولاً يخدم أولاً"*.

والثاني: هو أنهُ بحلول سنة ٢٠٢٢، من المُرجح ان تكتسِب الشركات الصينية الممّولة من الدولة والشركات الخاصة الُقدرة على تعدين الكويكبات، وفي سنة ٢٠٢٤ يُخطط لإِطلاق الكويكب (الطويل) الغني بالبلاتين بقيمة (٥) تريليون دولار أمريكي بالقُرب من سطح القمر.

مثل هذهِ السيناريوهات يَجب وضعها في الاعتِبار عند تدوين القانون الدولي بشأن المُوارد الفضائية، إن نهِج "من يأتي أولاً يخدم أولاً" غير المُنسق يخلق إمكانية توتر العلاقة الدبلوماسية، لا سيما عندما تصبَح الموارد الأرضية أكثر نُدرة، وقد يؤدي نهج الصين الفريّد، الذي يتجه نحو المكانة والأكثر استَغلالًا للموارد، إلى إجهاد العلاقات أكثر من غيرها، مثل هذا المُستقبل هو أقرب أكثر مِما نعتقد.

ونتيجة لهذه الضغُوط، أصدر الكونغرس "القانون الأمريكي للتنافس التِجاري في الفضاء (S.U Commercial Space Launch Competitiveness Act) سنة ٢٠١٥، والذي بدورهِ يَمنح المواطنين الامريكان حق ملكية "المُوارد الفضائية " في الفضاء وفقا لمبدأ "الأولوية لمن

---

(1) Namrata Goswami, Star Wars From Space-Based Solar Power to Mining Asteroids for Resources: China's Plans for the Final Frontier, Policy Forum, 7 September 2016,pp.1-2. Available at Link:
https://www.policyforum.net/star-wars. the Date visit at March 30,2021

* هذا المبدأ نص عليه القانون الأمريكي للتنافس التجاري في الفضاء لعام ٢٠١٥ والذي ربما يدفع الصين لإصدار قانون مماثل. للتفصيل ينظر: القانون الأمريكي للتنافس التجاري لعام ٢٠١٥.

يسبق "[1]. وفي سنة ٢٠١٧ مررّت لوكسمبورغ قانونا مشابِها للقانون الامريكي، خاص بالشركات التي تقع مقراتَها على اراضِيها [2]. كما أهتمت دول أخرى مثل الصين عِبر تبني تشريع مُماثل للاستثمار في مجال الفضاء، حيث وَضعت خُططا طموحة لتنمية مواردَها الفضائية بحلول سنة ٢٠٤٥ [3]. وبذلك بدَأت الشركات المَرحلة الثانية من التحضير للتعديّن وهي الاستكشاف في الفضاء.

ومع تنامي المصالَح التجارية والأصُول العسكرية، برز سِباق تسلح في الفضاء الخارجي، حيث وجه الرئيس الصيني (شي جينغ بينغ) "قُوة الدعم الاستراتيجي الصينية" (Strategic Support Force) التي أنُشئت في سنة ٢٠١٥، والمُكلفة بشؤون "الفضاء والإنترنت"، لدعم الوجود الصيني في الفضاء الخارجي، ورداً على تطوير كُل من الصين ورُوسيا قدراتهُما الفضائية المدنية والعسكرية على حدٍ سواء، أعلن الرئيس الأمريكي (دونالد ترامب) في حزيران ٢٠١٨ عن تأسّيس "القوة الفضائية الامريكية" [4].

ونتيجة لغياب الأُطر التنظيمية الواضحة، التي ترسي قواعِد واضحة لتنظيم الاستغلال العادل لثروات الفضاء الخارجي، نَشأت الحاجة إلى إضافة تعديلات لمُعاهدة الفضاء الخارجي لعام ١٩٦٧، وتُعد لوكسمبورج من أولى الدول التي وضَعت تشريعات لتنظيم التعدّين الفضائي، وأنشأت صندوقاً سيادياً يجذب استثمارات شَركات الفضاء الخاصة، ويمكن أن يُمثل تصاعد التنَافس الاقتصادي في الفضاء الخارجي، عاملاً إضافياً يساعد على عسكرتهِ، والتي بدأت مع

---

(1) U.S Commercial Space Launch Competitiveness Act, Congress.Gov, PUBLIC LAW 114-90—NOV. 25, 2015 ''CHAPTER 513—SPACE RESOURCE COMMERCIAL EXPLORATION AND UTILIZATION,p.19.

للتفصيل ينظر: القانون الأمريكي للتنافس التجاري في الفضاء سنة ٢٠١٥، توجد نسخه من نص القانون باللغتين العربية والانكليزية في جامعة الانبار\ مكتبة كلية القانون والعلوم السياسية تم ترجمتها وايداعها من قبل الباحث.

(٢) وثائقية دي دبليو: الأجرام السماوية – مناجم جديدة في الفضاء؟، مصدر سبق ذكره.

(٣) نامراتا جوسوامي، مصدر سبق ذكره، ص ٦٠

(4) Zhang Tao,Strive to build a strong, modern strategic support force: Xi, China Military Xinhua Aguste 29 2016. Last accessed. Available at Link: http://eng.chinamil.com.cn/view/2016-08/29/content_7231309.htm. the visit at March 20, 2021.

مطلع العقد الأول مِن القرن الحادي والعشرين، وذلك من خلال نَشر الأقمار الصناعية العسكرية، بالإضافة إلى تطويّر الأسلحة المُضادة للأقمار الصناعية [١]. ويُعد غياب الاطر القانونية وعدم كِفاية القائمة منها حالياً لتنظّيم مسألة اِستغلال الفضاء، أحد العوامل التي ساعدّت على تصاعُد حدة التنافس في الفضاء الخارجي، فبينما تنُص "معاهدة الفضاء الخارجي" على إن "الفضاء الخارجي، بما فيه القمر والأجرام السماوية الأخرى، لا يَخضع للحيازة القومية من خلال ادعاء السيادة، عن طريق الاستغلال أو الاحَتلال، أو بأي وسيلة أخرى، حسب ما نصت عليه المادة الأولى من المعاهدة على أن: "الفضاء الخارجي، بما في ذلك القمر والأجرام السماوية الأخُرى، يجب أن يكون مفتوحاً لجميع الدول لاستِكشافه واستغلالهِ" [٢].

يبدو إن اِستخراج الثروات المعدنية من الأجرام السماوّية وكأنه خيال علمي، لكنهُ قد يَصبح حقيقةٍ واقعة قريبا، فالشركات والدول القوية لديها بالفعل مُخططات لمثل هذه المشاريع، التي أصبح مُستقبل استثمارها قريب جدا [٣]، وتعمل بجهد لتأمين الثروة من الفضاء، وبذلك يتم تفسير الحق في استَغلال مُوارد الفضاء من قبل كُل دولة بما يخدُم مصالحها، مما يُعزز التنافس والتصعيد وخاصةٍ بين الولايات المتحدة والصين، وذلك لعدم وجود أطُر قانونية دولية واضحة في هذا المَجال، وعلى العراق كدولة ضمن المجتمع الدولي أن يعمل من أجل الاستفادة من ذلك المجال الحيوي والمستقبلي ولو بالحد الادنى.

المطلب الثاني: التحديث المستقبلي العسكري للجيش الصيني في مجال الفضاء

تُعد الصين أكبر مُنافس استراتيجي للولايات المُتحدة، وعلى عكس معظم مُنافسي الولايات المتحدة في فترة ما بعد الحرب الباردة، فأن الصين أن تقَترب من القُدرات الأمريكية في مجال الأنظمة الفضائية والاختَراق الإلكتروني، قد تحتاج الدول أيضًا إلى قدرات حرب إلكترونية متقدمة ومزيد من المعلومات من أجل التمكن من مهاجمة الخصم وشل قدرتهِ العسكرية أو قدرة الخصم

---

(١) نامراتا جوسوامي، مصدر سبق ذكره، ص ٦١.

(2) Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, September 14, 2018.Available at Link: https://bit.ly/2oghNq3. the date visit at 29 March 2021.

(٣) وثائقية دي دبليو، مصدر سبق ذكره.

على السيطرة على قواتهِ وهذا يتضح اكثر في أوقات الصراع و الحرب الفعلية، والتطور الفعلي لقدرات الصين السيبرانية يمكن أن يردع الولايات المتحدة ودول أخرى، بينما لا تحتاج الولايات المتحدة إلى ردع الدول الأخرى عبر الفضاء الإلكتروني كونها تحقق الردع فعليا من خلال القوة العسكرية [١].

وتَسعى الصين والدول غِير الصديقة للولايات المتحدة، إلى الاعتِماد على شبكات الكمبِيوتر والاتصالات لتعطّيل القُوات الأمريكية والقوات الحليفة في مَسرح الحرب، وهذا يعني تقويّض حُرية العمل الأمريكية في السُواحل وربما المُحيطات التي تتواجد فيها، وسيواجه الحلفاء مجموعة واسعة من العملّيات السيبرانية التي تهدُف إلى تعطيل أنظمة القِيادة والتحكُم، في الوقت نفسه، تظّل الولايات المتحدة في وضع غير مُؤات بالنسبة للصين من حيث أساسيات الصِراع العسكري في الساحِل الآسيوي [٢].

ويُحذر (Martinag) من أن الولايات المتحدة ستُواجه "الهجمات الإلكترونية والسيبرانية العُدوانية التي تركز على تعطيل شبكات (C4ISR)* الأمريكية" [٣]، في النزاعات المستقبلية، والصين تطمح

---

(1) Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." Journal of Strategic Security, Volume 4, No. 2, Washington, Summer 2011, pp.3,4.

(2) Peter Dombrowski, America third offset strategy new milirary technologies and implications for the asin pacific, S. Rajaratnam School of International Studies (RSIS), June 2015,p.7.

* C4ISRNET: هي انظمة شبكية مكرسة لتقنيات الاتصالات والدفاع وتكنولوجيا المعلومات الاستخباراتية والأنظمة غير المأهولة وأجهزة الاستشعار، GEOINT والإنترنت. إن القدرات الشبكية لهذه التقنيات هي التي غيرت مشروع الحرب.وتعني C4ISRNET (وسائل الإعلام لعصر المخابرات العسكرية) للتفصيل ينظر:
Robert Martinage, Toward a New Offset Strategy Exploting U.S. Long-Term Advantages To Restore U.S. Global Power Projection Capability, Press Meeting, In the Center for Strategic and Budgetary Analysis, October 27, 2014, Available at: =https://csbaonline.org/research/publications/toward-a-new-offset-strategy-exploiting-u-s-long-term-advantages-to-restore

(3) Robert Martinage, Toward a New Offset Strategy Exploting U.S. Long-Term Advantages To Restore U.S. Global Power Projection Capability (Center for Strategic and Budgetary Analysis 2014), p. 32. Available at Link:

إلى الوصّول للصناعة والتقنيات الاستراتيجية المُوازية (Offset) للولايات المتحدة، الافتراض الوحيد الأساسّي الذي تقوم عليهِ استراتيجية الموازية الثالث (America's Third OFFSET Strategy) أن العامل الاقتصادي والصناعي والتكنولوجي يُعتبر أساس قوة الولايات المتحدة، التي يُمكن تسخِيرها للتغلُّب على مزايا الخصُوم المحتملّين والصعوبات الملازمة المرتبطة بالجيش [١].

يدعوا بعض المُختصين ومنهم توم (Tom Mahnken)، وبناءً على التحلِيلات التي طورها مكتب التقيّيم الصافي التابع لوزارة الدفاع الأمريكية ، إلى أن تَتبنى الولايات المتحدة الاستراتيجيات التنافُسية، التي تفرض تكاليف على الخصُوم، والخصوم المحتملّين ومن خلال تحديد المُشكلة فأن الولايات المتحدة قد لا تكون كذلك قادرة على الحفاظ على استراتيجية السُرعة على المدى الطويل، وربما يكون هناك مُنافس واحد محتمل على الأقل، وهو الصين في وضع أفضل للفُوز بالمنافسة التكنولوجية، حيث لا يِزال النمو الاقتصادي في الصين مُرتفعاً، بين (٧-٩%) في السنوات الأخيرة، واستعدادَها للاستثمار في التحدِيث العسكري نما بِشكل هائل على مدى العقد الماضي، وتبذل الصين الكثير من الجُهود للازدهار التكنُولوجي من خلال إنجازات الآخرين على مدى عُقود، وقد وظفت الصين نظامًا متطورًا لاكتشاف التقنيات الأجنبية، والحُصول عليها بُكل الوسائل الممكنة، وتحوِيلها إلى أسلحة وسلِع تنافسية دون تعويض أصحابِها. لقد أدى النشاط في مجال الأمن السيبراني، إلى زيادة هذه المشكلات المُستعصية على الحل، بالرغم من الاهتمام من قبل إدارة الرئيس (أوباما) بهذا النشاط والنمو النسبّي لـ "للأمن السيبراني" الذي مثل أحد مُكونات ميزانيات الدفاع الأخيرة [٢].

إذ شكّل الانفاق العسكري الامريكي (٧٣٢ مليار دولار) أي ما يُعادل (٣٨%) من الإنفاق العسكري العالمي لسنة ٢٠١٩، بينما بلغَ الانفاق العسكري الصيني (٢٦١ مليار دولار) ما يُعادل ١٤% من الانفاق العالمي لنفس العام [٣]. ورغم الفارِق في الانفاق مُقارنة بالولايات المتحدة إلا أنهُ

---

file:///C:/Users/pdombrow/Downloads/Offset-StrategyWeb%20(2).pdf. The date visit at 1 April 2021.

(1) Peter Dombrowski, Op. cit, p. 8.

(2) Ibid,p.8.

(3) Nan Tian, Alexandra Kuimova, Diego lopes da silva, Op. cit,p.2.

لمزيد من التفاصيل حول الانفاق العسكري العالمي ينظر في الملحق رقم (٤).

أصبح مبلغ كبير مقارنةً بالسنوات الماضية* بالنسبة للصين ؛وهي تُحاول تقليل الفجوة في التسلّح مع الولايات المتحدة، التي تعتبر أن الصين المُنافس البديل للاِتحاد السوفيتي السابق [١].و تُعد صناعة الأسلحة الصينية من بين أكبر صناعات الأسلحة الوطنية في العالم. بناءً على مبيعات الأسلحة، للشركات الصينية حيث بلغ إجمالي مبيعات الأسلحة لشركة (AVIC) للطائرات بحدود (٢٠مليار دولار) سنة ٢٠١٧ وتشير مبيعات الشركات من الاسلحة، إلى إن الصين هي ثاني أكبر منتج للأسلحة في الشرق الأوسط بعد الولايات المتحدة وقبل روسيا. ومن الصعب الحصول على جدول دقيق بالمبيعات او أنتاج الاسلحة؛ إذ تحد الحكومة الصينية من الوصول للحصول على معلومات حول جميع شركات الأسلحة لصالح الأمن القومي [٢].

وتنفق الصين مبالغ طائلة على البحث والتطوير من جل زيادة الابتكار، وقد شهد الإنفاق الوطني على البحث والتطويّر في الصين زيادة بأكثر من (٣٥ ضعفًا) بين عامي ١٩٩١ و٢٠١٨، من (١٣,١) مليار دولار إلى (٤٦٢,٦) مليار دولار بما يعادل (٢،١٩%) من إجمالي الناتج المحلي. بينما كان الإنفاق على البحث والتطوّير في الصين في المرتبة الثانية بعد الولايات المتحدة (٥٥١،٥) مليار في عام ٢٠١٨، فقد كان أكثر مِن الدُول الأربعَ التالية – اليابان وألمانيا وكُوريا الجنوبية وفرنسا – مجتمعةً وحسب الجدوَل أدناه الذي يوضح إجمالي الإنفاق المحلي على البحث والتطوير في الصين مُقارنة مع بعض الدول [٣].

---

* ويقدر معهد (sipri) أن إنفاق الصين العسكري بلغ عام ٢٠٠٨ (٨٤،٩ مليار دولار) غير أن سياسيين وخبراء عسكريين أميركيين وغربيين يشكّكون بالأرقام التي تعلنها بكين، ويؤكدون بأن هذه الأرقام لا تعكس الموازنة العسكرية الفعلية للصين، التي تتراوح حسب تأكيد وزارة الدفاع الأميركية، بين ٩٧ و١٣٩ مليار دولار للعام ٢٠٠٧ (في حين كانت الميزانية الرسمية المعلنة تشير إلى ٤٦ مليار دولار للعام نفسه. للتفصيل ينظر: الانفاق العسكري العالمي لعام ٢٠٢٠، معهد أستوكهولم للسلام والابحاث الدولية (sipri) الملحق رقم (٤).

(1) Annual Report to Congress Military Power of the People's Republic of China, Washington, 2008,p.14 .

(2) Nan Tian and FEI US, ESTIMATING THE ARMS SALES OF CHINESE COMPANIES Stockholm International Peace Research Institute (SIPIR), January 2020,P.7,15.

(3) Center for Strategic International Studies, China's Power, How Developed Is China's Arms Industry?, p.12. Available at the link: https://chinapower.csis.org/arms-companies/ the Date visit April 15 2021,

جدول رقم (٨) يوضح الانفاق في مجال البحث والتطوير لأعلى ست دول

ت	الدولة	السنة	المبلغ بالمليار (دولار امريكي)
١	الولايات المتحدة الامريكية	٢٠١٨	٥٥١,٥ مليار دولار
٢	الصين	٢٠١٨	٤٦٢,٦ مليار دولار
٣	اليابان	٢٠١٨	١٧٣,٣ مليار
٤	المانيا	٢٠١٨	١٢٩,٦ مليار
٥	كوريا الجنوبية	٢٠١٨	٩٥,٥ مليار دولار
٦	فرنسا	٢٠١٥	٥٨,٥ مليار دولار

الجدول من اعداد الباحث. المصدر: منظمة التعاون الاقتصادي والتنمية (OECD)* متاح على الموقع:

https://data.albankaldawli.org/indicator/GB.XPD.RSDV.GD.ZS

وذلك سَعياً منها إلى تجهيز قواتِها المُسلحة بوسائل الحرب الحديثة التي "تقوم على المعلومات"، أي الحرب التي تقوم على الاستخدام الكثّيف لتكنُولوجيا المعلومات العالية المُستوى، وعلى الأسلحة الدقيقة وتكنُولوجيا الاتصالات، ونسب الإنفاق هذه غِير مدرجة في الميزانية العسكرية الرسمية؛ بحيث لا يمكن معرفة المستوى الحقيقي للأنفاق العسكري الصيني بشكل دقيق [١].

لقد امتلكّت الصين برامج فضائية مُتطورة تشتمل، على "أقمار صناعية للاستشعار عن بُعد، وقُدرات خاصة بالبنية التحتِية للنشاط الفضائي وتكنُولوجيا الفضاء وتصنيع الأقمار الصناعية والصواريّخ والملاحة الفضائية، بما يجعُلها قادرة على تفسير واستقبال المعلومات من الأقمار الصناعية الأوروبية والأمريكية. فللفضاء الإلكتروني أهمِية استراتيجية، حيث أصبح

* منظمة التعاون الاقتصادي والتنمية (OECD) Development Organization for Economic Cooperation

(١) محمد دياب، جدلية العلاقة بين الأنفاق العسكري والتنمية الاقتصادية، مجلة الدفاع الوطني اللبناني، العدد ٢٥، بيروت، كانون الثاني ٢٠١١، ص٢.

ساحة مهمة للتَنافس ولتعظّيم القوة الاقتصادية والعلمية، والحفاظ على أمن الدولة وطمُوحها في احتلال مَكانة لها في النظام العالمي في عَصر الثورة العلمية والتكنولوجية [1].

لقد تعددت مجالات التَنافس بين الولايات المُتحدة والصين، حيث ظهر مجال آخر هو الهيمنة على الفضاء الإلكتروني، إنّ المؤشرات التي تّم تناولاها في هذا الفصل أشرت أن أبرز مجالات التنافس، هي تكنولوجيا المعلومات وأنظمة الحماية الخاصة بالبُنى التحتية وانظمة الدفاع ضد الهجمات السيبرانية، وهو ما يؤكد إن المجال السيبراني سيكون هو المجال الأهم للتَنافس الدولي بين القوتين العالميتين، لكسِب مُوقع الصدارة في النظام العالمي خلال العقود القادمة.

(١) عادل عبد الصادق، الفضاء ساحة جديدة للتنافس الاسيوي، مجلة السياسة الدولية، المجلد ٤٦، العدد ١٨٣، مركز الأهرام للدراسات الدولية السياسية والاستراتيجية، كانون الثاني ٢٠١١، ص ص٦٤-٦٥.

المبحث الثالث: مستقبل الأمن السيبراني (للولايات المتحدة الأمريكية والصين)

لعل من الصعوبة بمكان توقع مستقبل الأمن السيبراني وأبعاده بدقة؛ لا سيما وأن المخترقين يطورون أدوات جديدة باستمرار، لكن هناك بعض التوقعات الخاصة بمستقبل أمن المعلومات، وقد أحدثت تقنيات الذكاء الاصطناعي ثورةً في عالم التكنولوجيا، وأصبحت الكثير من الصناعات والأعمال تعتمد عليه، ومع توسع رقعة الشركات والمؤسسات التي تعتمد تقنيات الذكاء الاصطناعي، ازدادت مخاطر اختراق هذه التقنيات، وأصبحت هدفًا رئيسًا للمخترقين، حيث يُعد الذكاء الاصطناعي حجر الأساس لجميع أنظمة حماية المعلومات.

إذ لا يمكن لأحد أن يخبرنا بالضبط عن التهديد السيبراني الرئيسي التالي أو من أين سيأتي، ولكن لايزال الخبراء لديهم فكرة جيدة عن الاتجاه العام الذي تسلكه الدول في هذا المجال، هذا التحدي سيدفع المبرمجين إلى استخدام التقنية ذاتها للكشف عن الثغرات الأمنية وإصلاح الأخطاء قبل أن يكتشفها المخترقون، ويجب الانتباه إلى تنبؤات الأمن السيبراني المستقبلية، من خلال المحاور التالية: سنحاول التعرض لأهم التطورات والتحديات التي تواجه الأمن السيبراني عبر الفضاء الإلكتروني في المستقبل من خلال ثلاثة مطالب: الأول يبين الأفاق المستقبلية للتنافس الامريكي الصيني السيبراني على المستوى الدولي، والثاني يتناول مستقبل الأمن السيبراني في ظل الذكاء الاصطناعي (Intelligence Artificial) أضافة الى المطلب الثالث الذي بيّن ماهية التنافس الأمريكي–الصيني في مجال الذكاء الاصطناعي.

المطلب الأول: الافاق المستقبلية للتنافس الأمريكي– الصيني السيبراني على المستوى الدولي

يُعد التنافس الصيني الأمريكي من أهم العوامل المؤثرة في طبيعة النظام العالمي؛ وذلك لما تمتلكهُ الدولتان من عوامل وعناصر القوة في مجال الفضاء الالكتروني، حيث ترغب الولايات المتحدة الاحتفاظ بالهيمنة على النظام الدولي وبالتالي الفضاء الإلكتروني، وترى في الصعود الصيني قوة مناهضة لدورها الاقليمي والعالمي، وتهديد لمصالحها الحيوية وأمنها القومي، مقابل السياسة الصينية التي تسعى لتحقيق هدفين [1].

(1) China's Great Firewall, Washington Post, November 6, 2018.Available at the link: https://bit.ly/2maTv2c. Date visit at 1 April.

الأول: أزاحه الولايات المتحدة كقوة بارزة في غرب المحيط الهادي.

والثاني: توحيد آسيا في كتلة تخضع لمصالح الصين الاقتصادية والسياسية، ولو على المدى البعيد، كما أنها يمكن أن تلعب دوراً مهما من خلال عالم متعدد الاقطاب، لا تكون فيه الهيمنة لقوة واحدة، ولغرض الوقوف على مستقبل النظام العالمي وتأثير التنافس الأمريكي- الصيني في مجال الفضاء، على طبيعة النظام العالمي يمكن التطرق إلى أهم السيناريوهات المستقبلية والعوامل المحركة لهذا الصراع [١].

وقدر تعلق الأمر بالتنافس الأمريكي الصيني في المجال السيبراني، ورغبة الطرفين بالسيطرة على الفضاء الالكتروني والتقنية الرقمية من خلال شركات تكنولوجيا المعلومات، لذا من المتوقع أن تشهد العلاقة بين الدولتين تنافساً من خلال تطوير تقنيات الذكاء الاصطناعي، التي يمكن استخدامها من قبل الحكومات لرصد وفهم سلوكيات المواطنين والسيطرة عليهم، حيث ابتكرت الصين نظام المراقبة (نظام جدار الحماية العظيم)* [٢]، والذي أنتشر على الانترنيت بين الدول ذات التوجه الواحد(تايلند، سيريلانكا، فيتنام، اثيوبيا، ايران، العراق، زانبيا، زنبابوي وماليزيا) وهذا النظام سيكرس الاستبداد(الفكري والثقافي) وتقييد الحريات الفردية من وجهة نظر الدول الغربية، ويُقابل بالرفض من قبل الولايات المتحدة التي تدعوا للديمقراطية الليبرالية، حيث سيكون التنافس القادم بين السيطرة الرقمية والديمقراطية الليبرالية، بمعنى ستكون هناك مقابلة أيديولوجية بين الانظمة الغربية والأنظمة الشرقية التي تقودها الصين، من خلال تقديم مشاريع ضخمة لتكنولوجيا

---

(1) Henry A. Kissinger, The Future of U.S.-Chinese Relations Conflict Is Choice, Not a Necessity, journal Foreign Affairs, Vol.91, No. 2 March 2012, p.4.

* جدار الصين الناري العظيم، Great Firewall of China، هو مزيج من التدابير التشريعية والتكنولوجية التي تفرضها جمهورية الصين الشعبية لتنظيم الإنترنت محلياً. ودور الجدار في الرقابة على الإنترنت في الصين هو منع الوصول إلى مواقع إلكترونية أجنبية مختارة وتبطيء حركة الإنترنت العابر للحدود.للتفصيل ينظر:

Matthew Bey, The Age of Splinternet: The Inevitable Fracturing of the Internet, Stratfor, 25 April, 2019.

(2) Matthew Bey, The Age of Splinternet: The Inevitable Fracturing of the Internet, Stratfor, 25 April, 2019. Available at Link: date of the visit April 1, 2021.
https://worldview.stratfor.com/article/age-splinternet-inevitable-fracturing-internet-data-privacy-tech

المعلومات تشمل المجتمع مثل مشروع (جدار الحماية العظيم) الذي يمّكن الحكومات من مراقبة البيانات والسلوكيات بشكل انتقائي [١].

وقدر تعلق الأمر بمستقبل الصراع في الفضاء الالكتروني فقد حدد (Jason Healey) خمسة سيناريوهات، في ضوء تطور الاحداث على المستوى الدولي وعلى النحو الآتي [٢]:

السيناريو الأول: أن ساحة الفضاء الالكتروني تبقى آمنه للتواصل مع الاخرين، مع توظيف الصراعات الإلكترونية في سرقة البيانات الشخصية او العامة، ومع استمرار استخدام الجيوش للأسلحة الإلكترونية ومحاولة الدول تعزيز أنظمة دفاعاتها ضد الهجمات الإلكترونية التي يسعى لها الإرهابيون من خلال تطوير التقنيات في هذا المجال.

السيناريو الثاني: ويشير إلى الأمان الجزئي حيث يصبح الفضاء الالكتروني مجال صراع، في الجو والبحر والفضاء مقابل استمرار الاتصالات بين الأفراد والجماعات والدول بشكل آمن، مع وجود مناطق اخرى غير آمنة ودول لا تقوى على مواجهة مخاطر الصراع السيبراني؛ بسبب تأخرها تقنينا في هذا المجال مثل الصومال والعراق.

السيناريو الثالث: يتحدث فيه جاسون (Jason) عن مساحة واسعة من الأمان في الفضاء الإلكتروني، بحيث يكون وضع الدفاع بالنسبة للفاعلين أكثر من الهجوم، وبالتالي استحداث انظمة وبرامج إلكترونية متقدمة في مجال الدفاع مع نفقات عالية للاستثمار في هذا المجال.

السيناريو الرابع: يشير إلى بناء السيادة والحدود داخل الفضاء الالكتروني، وهو ما يطلق عليه وضع البلقنة الالكترونية* (Electronic Balkanization) وبالتالي لن تكون هناك شبكة دولية

---

(1) Yuan Yang,The Great Firewall of China web of control.Financial Times, March12,2019.Available at Link: the date visit at 2 April 2021.
https://www.ft.com/conent/e19b3022- 40eb-11e9-9bee-efab61506f44

(2) Jason Healey, The Five Futures of Cyber Conflict and Cooperation, The Georgetown Journal of International Affairs, Georgetown University Press, Washington,2011,pp.110,113.

* "ويقصد بها الشبكة المقسمة splinternet " أو "بلقنة الإنترنت" – تجزئته – الذي يصف وضعاً تكون فيه شبكة المعلومات الرقمية العالمية مجزأة إلى شبكات أصغر بفعل سلسلة متنامية من القواعد واللوائح والضوابط– وهذا

واحدة للمعلومات، أذ تسعى عدة قوى (الصين، روسيا) لتامين مجالها الإلكتروني في مواجهة الصراعات مع قوى أخرى مثل الولايات المتحدة [١].

اما السيناريو الأخير: فهو الوضع الأخطر مقارنة بالأوضاع السابقة في حالة عدم السيطرة على الفضاء الإلكتروني، مما يتيح الفرصة للقراصنة والجماعات الإرهابية في أحداث تأثير على نطاق واسع، مما يجعل الفضاء مجالاً غير آمن، بالنسبة للاتصالات والتجارة والخدمات مع تصاعد حدة الصراع بين الفواعل للسيطرة عليه.

وعليه يمكن القول إن مستقبل النظام الدولي في مجال الفضاء الإلكتروني أصبح مرتبطاً – إلى حد كبير – بالتنافس بين الصين وأمريكا، وهذا التنافس مرشح للتهدئة أو التصعيد في العلاقة بينهم، على أن جميع المؤشرات ترجح التصعيد أكثر من التهدئة؛ لأن الولايات المتحدة والصين، تحكمها بذلك مصالح تلك الدولتين وخاصة من جانب الصين مما يترتب عليه نظام ثنائي القطبية، كأن يسيطر على الأمن السيبراني أمريكيا وروسيا، أو أن يسيطر على الذكاء الاصطناعي أمريكا والصين، وربما يكون نظام متعدد الاقطاب، بحيث تستطيع عدة دول الصعود إلى قمة الهرم في النظام العالمي وهو الاحتمال الأرجح.

وتعمل الحكومة الصينية على تطوير تكتيكات تقنية عالية الدقة؛ لمحاربة تلك الخاصة بالولايات المتحدة وفي هذا السياق يقول (Robert Work): "إن مواجهة هذه التكتيكات تتطلب تغييرًا في النهج التكنولوجي للجيش"، ومن هذه الأساليب الصينية هو ما يسمونهُ حرب تدمير النظام والذخائر الموجهة، وفي مقابل ذلك حسب قول (Robert): "فأن هامش تفوقنا يتضاءل بشدة في المجالات الرئيسية، ومنها مجال تكنولوجيا الأمن السيبراني، وهي تحديات يجب مواجهتها إذا كانت الولايات المتحدة ترغب في تجنب إلحاق ضرر دائم بأمنها القومي" [٢].

المفهوم موجوداً منذ سنوات طويلة –، لكنه يتجه الآن نحو النقطة التي يصبح فيها هذا المفهوم حقيقة واقعة، بمعنى أدق تقييد حرية الانترنيت. للتفصيل ينظر: Mattew Bey, op. cit

(1) Ibid,p.114.

(2) Andrew Wagner, One-on-one with former Deputy Secretary of Defense Robert Work,Government Matters, June 23, 2019 Available at Link: https://govmatters.tv/one-on-= one-with-former-deputy-secretary-of-defense-robert-work.Date vest 15-3-2021. the date visit 3 April 2021/.

ومن المتوقع أن تشتد المنافسة التكنولوجية بين الولايات المتحدة والصين في "الأسواق الثالثة"* حيث تُقرر الدول النامية أنظمة الاتصالات التي ستتبناها، وتعمل الصين بالفعل على تطوير رؤيتها الخاصة – طريق الحرير الرقمي– وتُهيئ نفسها للاستفادة تجاريًا واستراتيجيًا مع نمو السكان وازدياد عدد سكان العالم عبر الإنترنت [١].

المطلب الثاني: الأمن السيبراني في ظل الذكاء الاصطناعي (Artificial Intelligence)

سوف نتناول في هذا المطلب تعريف الذكاء الاصطناعي(AI)(Artificial Intelligence)، وتأثير الذكاء الاصطناعي على الأمن السيبراني وما هو مجال التنافس الامريكي – الصيني في ميدان الذكاء الاصطناعي.

ليس هناك تعريّف واضح لوصف الذكاء الاصطناعي، إذ تحاول معظم التعريفات الحالية التعبير عن الذكاء الاصطناعي كعملية حاسوبية، تُحاكي الذكاء والسلوك البشري وتتصرف بذكاء، لكن بصورة عامة يتم تعريّف الذكاء الاصطناعي، على أنه "مجال علمي مسؤول عن إنتاج حلول قائمة على الكمبيوتر للمشاكل المعقدة التي يواجه البشر صعوبة في إيجاد حلول لها" [٢]. بمعنى الدقة والسرعة في ايجاد الحلول والنتائج للمسائل التي تُحل عبر الكمبيوتر.

---

* السوق الثالث: هو قطاع من السوق غير المنظم، ويمارس السوق الثالث دور المنافس للمتخصصين (أعضاء السوق المنظم) والعملاء في هذه السوق هم: المؤسسات الاستثمارية الكبيرة. للتفصيل ينظر:
Ken Watanabe, Diane Rinaldo, Jonathan E. Hillman, Global Networks 2030 Developing Economies and Emerging Technologies, CSIS, Washington, March 2021. p.14.

(1) Ken Watanabe, Diane Rinaldo, Jonathan E. Hillman, Global Networks 2030 Developing Economies and Emerging Technologies, A webinar organized by the Center for Strategic International Studies, Washington, March 29, 2021, p.13.

(2) Chowdhary K.R, "Fundamentals of Artificial Intelligence," First edition, Springer India, New Delhi, 2020,p.95.

وقد برز أتجاهان في مجال تطبيق الذكاء الاصطناعي هما [١]:

الاتجاه الأول: "الأنظمة الخبيرة"، وهو محاولة تَعليم الكمبيوتر القواعد التي أتقنها العقل البشري، بينما أتخذ الاتجاه الثاني: "الشبكات العصبية" نهجًا مختلفًا، حيث حاول هؤلاء الممارسون إعادة بناء الدماغ البشري نفسهُ، وقد أكتشف هؤلاء الباحثون أنهم سيذهَبون مباشرة إلى مصدر الذكاء وهو العقل البشري، هذا النهج يحاكي البنية الأساسية للدماغ وبناء طبقات من الخلايا العصبية الاصطناعية التي يمكنها استقبال المعلومات ونقلها في نطاق هيكل شبيه بشبكاتنا من الخلايا العصبية البيولوجية.

ولبيان تأثير الذكاء الاصطناعي على الأمن السيبراني، هناك العديد من الصفات التي يمكن ملاحظتها على الذكاء الاصطناعي والذي بدورهِ يؤثر على الأمن السيبراني منها:

١ – يُعد استخدام الذكاء الاصطناعي في الأمن السيبراني جديدًا نسبيًا، بينما يجادل بعض خبراء الأمن السيبراني بأن الإجابة على الأمن السيبراني، هي التعلم الآلي لاكتشاف الخروقات المعقدة، وفي سياق الأمن السيبراني، يحاول الذكاء الاصطناعي الدفاع عن النظام من خلال تقييم أنماط السلوك التي تشير إلى وجود تهديد للأنظمة، وقد تم تحديد ثلاثةَ تحديات رئيسة تواجهُ صناعة أمن المعلومات، وذلك باعتبار أن العالم يتجه بشكل متسارع نحو الاستخدام الواسع لوسائل الاتصال الرقمية الحديثة، لذا يمكن معالجة كل منها من خلال حلول التعلم الآلي على النحو التالي [٢]:

أ– سيكون الذكاء الاصطناعي مكونًا أساسيًا لجميع أنظمة الأمن السيبراني؛ أذ يمكن استخدام الذكاء الاصطناعي والتعلّم الآلي لأتمته المهام ومعالجة البيانات واتخاذ القرارات، بشكل أسرع بكثير مما يمكن لأي إنسان، ورغَم التقنيات الجديدة بما في ذلك الذكاء الاصطناعي، فهي تخلقُ بطبيعتها مخاطر للأمن السيبراني، هذا يعني أنه مع اعتماد المزيد من المؤسسات على التعلم الآلي للعمليات ذات المهام الحرجة، فمن المؤكد أن أنظمة الذكاء الاصطناعي ستصبح هدفًا رئيسيًا للقراصنة.

---

(1) Kai-Fu Lee, AI superpowers: China, Silicon Valley, and the new world order, Boston: Houghton Mifflin Harcourt, New York, 2018, p.15.

(2) Chowdhary K.R,Op.cit, p.96.

ب- لن يُغير الذكاء الاصطناعي عالم الأمن السيبراني فقط، من خلال مَنح المتسلّلين طريقة جديدة للوصول إلى المؤسسات المستهدفة، بل سيستخدم مطورو الأمن السيبراني الذكاء الاصطناعي بأنفسهم لمعالجة الثغَرات الأمنية، واكتشاف المشكلات الأمنية قبل الاستفادة منها، وصد الهجمات حال وقوعها [١].

ج- محدودية الوقت والميزانية للبَحث أو التحقّيق: إن تقديم طلب إلى المحللين للتحقّيق في الهجمات أمر مكلف ويستغرق وقتًا طويلاً ، والذكاء الاصطناعي ليس جاهزًا ليَحل محل البشَر، ولكن من خلال أتمتة عملية التعرف على الأنماط، يمكنهُ تعزيز الجهود البشرية.

٢ - ويمكن تقييم استخدام الذَكاء الاصطناعي في الفضَاء الإلكتروني في فئتين؛ استخدام الذكاء الاصطناعي للدفاع السيبراني واستخدَام الذكاء الاصطناعي في الجرائم الإلكترونية [٢].

أ- استخدام الذكاء الاصطّناعي للدفاع السيبراني، ويكون ذلك من خلال ثلاثة مستويات [٣].

المستوى الأول: آليات الدفاع الإلكتروني الثابتةَ التقليدية مثل الهوية والمصادَقة والتحكم في الوصول للبيانات.

المستوى الثاني: آليات الدفاع السيبراني الاستبَاقي، مثل جَمع المعلومات وتقييم الأمان ومراقبة حالة الشبكة والهجُوم.

المستوى الثالث: إدارة الدفاع الإلكتروني، والتي تقوم بإجراء تقييم شَامل لحالة الشبكة واختيار آليات الدفاع المناسبة أو المُثلى وتكيّيفها.

---

(1) Jacob Parker, Cybersecurity is a key issue of our time, Techrader Newsletter, May 19, 2020, P.3. Available at Link: https://global.techradar.com/en-za/news/what-is-the-future-of-cybersecurity the date visit 4 April 2021.

(2) Ensar Seker, Is the Future of Cyber Security in the Hands of Artificial Intelligence (A3)?, Center for a New American Security (CNAS), Washington, Jun 10, 2020, P.4.

(3) I. Kotenko, "Multi-agent Modelling and Simulation of Cyber-Attacks and Cyber-Defense for Homeland Security", IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 2007.

ب- استخدام الذكاء الاصطناعي في الجَرائم الإلكترونية:

يتوقع المختصون أن تستخدم تقنيات الذكاء الاصطناعي في الهجمات الإلكترونية؛ لما تتمتع به من ميزات تُشجع المجرميّن الإلكترونيين على استخدامها، ما يتطلب حُوكمة الذكاء الاصطناعي والحَد من المخاطر والأثار السلبية له، مع ضرورة تعزيز وعي المُستخدِم، وتعاون الباحثين مع صّناع القرار، ما يُحتِّم على الحُكومات فرض حد أدنى من المعايير على الشركات لتصنّيع أنظمة مقاومة للهجمات السيبرانية، للأستفادة من القفَزات الهائلة للذكَاء الاصطّناعي على نحو أمثل، وتجنُب المخاطر والسلبيات الناتج عنهُ [١].

ويمكن أن يؤدي إساءة استخدام الذكاء الاصطناعي إلى تهديد الأمن بعدة طرق [٢]:

- التهديدات للأمن الرَقمي (الاختراقات والقرصنة).
- التهديّدات للأمن الجسدي (عمليات الابتزاز والعنف).
- التهَديدات للأمن الاجَتماعي، الاقتصادي والسياسي.(التأثير على سلُوك وتقاليد المجتمع، سرقة الحسابات، الدعاية والتضليل السياسي)

وقدر تعلق الأمر بالتنافس بين واشنطن وبكين في مجال الذكاء الاصطناعي في القرن الحادي والعشرين الأبرز على مستوى العالمي، مما يمهد الطريق لنوع جديد من العالم ثنائي القطبية، ويوضح (Kai-Fu Lee) - أحد أكثر الخبراء المرمُوقين في العالم في مجال الذكاء الاصطناعي- على الرغم من أهمية هذا التنافس بين القوتين العظميين في العالم، إلا أنه يتضاءل مقارنة بمشاكل فقدان الوظائف وتزايد عدم المساواة - محليًا وفيما بين البلدان - التي سيستحضرها الذكاء الاصطناعي، في غضون خمسة عشر عامًا سيتمكن الذكاء الاصطناعي من الناحية الفنية من استبدال حوالي ٤٠ إلى ٥٠ بالمائة من الوظائف في الولايات المتحدة الأمريكية، وسوف يقضي بالفعل على ملايين الوظائف صعودًا وهبوطًا في السلم الاقتصادي، في الوقت نفسه ،

---

(١) أبرز التوقعات عن الأمن السيبراني في العالم العربي وأوروبا وإفريقيا في ٢٠٢١، الحاجة إلى اتخاذ إجراءات مجدية لرفع سوية الأمن الإلكتروني، مرصد المستقبل، دبي، ٢كانون الثاني ٢٠٢٠. متاح على الموقع:
https://mostaqbal.ae/most-prominent-predictions-of-cybersecurity-in-the-arab-world-europe-and-africa-in-2021 /. تأريخ الزيارة ٢٢-٣- ٢٠٢١.

(2) Ensar Seker, Op.cit,p.6.

ستؤدي الأتمتة القائمة على الذكاء الاصطناعي في المصانع إلى تقويض الميزة الاقتصادية (العمالة الرخيصة) لتطور الدول التي تمتلكها تاريخيا، وسهولة نقل التقنية الى دول اخرى، حيث يمتاز الذكاء الاصطناعي بسمات منها "الانفتاح والسرعة"، الذي يجعل من الصعوبة على الدول المتقدمة احتكار التطور التقني. ورغم أن الرئيس (ترامب) في زيارتهُ للصين سنة ٢٠١٧ بدأ حديثه في اللغة الإنجليزية ثم تحولت اللغات فجأة الى الصينية –نتيجة تقنيات الترجمة وقال: "الذكاء الاصطناعي يغير العالم" [١] ، متحدثًا بلغة صينية خالية من العيوب ولكن بصوت ترامب المعتاد.

ومقابل تخفيض النفقات المخصصة للذكاء الاصطناعي، في عهد أدارة الرئيس ترامب فقد عززت الصين من جهودها في القطاعين العام والخاص بالعمل على تطوير الذكاء الاصطناعي، وربما يضمن الدعم الحكومي الصيني لأبحاث الذكاء الاصطناعي إلى قيادة العالم ، والسعي للتحول الى قوة عظمى في ذلك المجال بحلول عام ٢٠٣٠. رغم ذلك يعتقد(Kai–Fu Lee) ، أنه ورغم تَخلف الصين لسنوات عديدة، عن الولايات المتحدة في مجال الذكاء الاصطَناعي، لكن على مدار السُنوات الثلاث الماضية(٢٠١٥، ٢٠١٦ ، ٢٠١٧)، بدَأت الصين تشهد موجة كبيرة من التوجه الكبير نحو الذكاء الاصطّناعي.

لقد مَنحت الشركات الأمريكية العملاقة في مجال الإنترنت وتقنيات المعلومات، الولايات المتحدة هيمنة على العالم الرقمّي تُضاهي قوتَها العسكرية والاقتصادية في العالم الحقيقي، وهنا يكشفُ) (Lee) أنَّ الصين قلّصت الفجوة مع الولايات المتحدة بوتيرة سريعة وَغير متوقعة، في تقنيات الذكاء الاصطناعي، ويُجادل المؤلف في كتابه (القوى العُظمى للذكاء الاصطناعي) أنه وبسبب هذه التطورات غير المسُبوقة في الذكاء الاصطناعي، ستحدث تغييرات جذرية في وقت أقرب بكَثير مما نَتوقع، مع بدءَ احتدام المنافسة بين الولايات المُتحدة والصين في الذكاء الاصطناعي، وَيحث (Lee) البلدين على قبول المسؤوليات الكبيرة التي تأتي مع القوة التكنولوجية الهائلة، وإن الذكاء الاصطَناعي سيكون له تأثير كبير على وظائف أصحاب الياقات الزرقاء، في إشارة إلى العُمال، لكنه يتوقع أن يَكون هناك تأثير للذكاء الاصطناعي الصيني والأمريكي على وظائف ذوي الياقات البيضاءَ أيضًا، وهم العاملون في القطاع الصحي [٢].

(1) Kai-Fu Lee, op, cit. P.16.

(2) Ibid, op, cit. P.17-55

ويُدحض **(Lee)** وجهة النظر التي ترى ببساطة أن رجال الأعمال الصينيّين ليسوا سوى "مقلدّين" يفتقرون إلى القُدرة على الابتكار. حيث ذكر(فوكاياما) " فالصينيون لم يبتكرون شيئا جديداً فيما يتعلق بالتكنولوجيا والعلوم الاساسية، هم يلحقون ويقتربون من المرحلة التي سيحتاجون فيها لفعل ذلك" [١]. ولكن الدراسة لا تؤيد ما ذهب اليه (فوكاياما)، لأن من يصل (الصين) الى هذا المستوى من المنافسة والنمو الاقتصادي المرتفع ؛ لا يمكن أن يكون كل اعتماده أو كل إنجازاته على ابتكارات وتقنيات الغير، وفي هذا السياق دعا (James Norman Mattis) ٢٠١٧-٢٠١٩ سكرتير الرئيس الأمريكي السابق (دونالد ترامب) لشؤون الدفاع، إلى مزيدٍ من الإنفاق في مجال الذكاء الاصطناعي خشية الطموح الصيني، بما في ذلك المشروعات التي تعمل عليها وحدة الابتكار التجريبية التابعة لوزارة الدفاع، وطالب الحكومة بتدعّيم عَلاقاتها مع الشركات التكنولوجية، خاصة تلك التي تعمل في مجال الذكاء الاصطناعي، بل تصاعدت بعض المقترحات بمنع إستيراد أي أجهزة من شركة(Huawei)and(ZTE) ومنع التعامل مع أي متعاقد خارجي لهُ تعاملات مع هذه الشَركات خشية التعّرض للاختراق الصيني وتهديد الأمن القومي الأمريكي [٢].إنّ الحَجم الهائل للابتكار الصيني ووتيرتهُ قد يؤديان إلى سباق تَسلح للذكاء الاصطّناعي تتنافس فيه الصين والولايات المتحدة بقوة على القيادة [٣]. ومع ذلك، فإنَّ القضية لا تتعلق فقط بمنافسة الولايات المتحدة للصين، فثمةَ قضية أكبر تتمثل في مُعادلة: البشر مقابل الذكاء الاصطناعي، ومن وجهة نَظر **(Lee)**، تتفُوق الولايات المتحدة والصين بقوة على بَقية العالم، الأمر الذي سيؤدي إلى تفاقم عَدم المساواة العالمية من خلال وضع قُوة غير متكافئة في أيدّي هاتين الدولتين [٤].

---

(١) اللقاء التلفزيوني قناة WarCQC مع الكاتب فوكاياما. بعنوان: هل ستهيمن الصين على العالم، ترجمة سعيد القحطاني ٢٩ بتأريخ حزيران ٢٠٢٠. متاح على الموقع:
https://www.facebook.com/watch/?ref=saved&v=312549466435499 تأريخ الزيارة ٢٤نيسان ٢٠٢١.

(٢) إيهاب خليفة، أبعاد الصراع الصيني-الأمريكي على الهيمنة التكنولوجية، مركز المستقبل للأبحاث والدراسات المتقدمة ابو ظبي، ٦ كانون الاول ٢٠١٨، ص٣.

(3) Winston Ma, The Digital War: How China's Tech Power Shapes the Future of AI, Blockchain and Cyberspace, Wiley Publishing Corporation, New York, January, 2021, p.45.

(4) Kai-Fu Lee, Op.cit, p.14.

المطلب الثالث: البعد الثالث للفضاء السيبراني

يعد مُكعب الأمن السيبراني (Cybersecurity cube) أداة تم تطويرها من قبل (McCumber)- أحد خُبراء الأمن السيبراني الأوائل- من أجل المُساعدة في إدارة حماية الشبكات والمجالات والإنترنت، ويتضمن ثَلاثة أبعاد [1]:

يُحدد البُعد الأول: أهداف حماية الفضاء السيبراني، وهي المبادئ الأساسية الثلاثة: (السرية والنزاهة والتوافر) ، والتي يشار إليها عادة باسم (CIA Triad)*، ويحدد البُعد الثاني: الحالات الثَلاث للمعلومات أو البيانات.

أما البُعد الثالث: للمُكعب فيشمل الخبرة المطلوبة لتوفير الحماية، وغالبًا ما تُسمى هذه الفئات الثلاث ضمانات الأمن السيبراني.

فالبُعد الثالث للفضَاء السيبراني يُركز على المهارات والانضباط لحماية الأمن في الفضاء السيبراني، حيث يَستخدم محترفو الأمن السيبراني مجموعة من المَهارات التي تركز على تنمية قدرات وعقول مُستخدمي شبكة الانترنيت، مع الحرص على البقاء دائمًا على "الجانب الصَحيح" من القانون، وقد كان التدخل الرُوسي في الانتخابات الرئاسية الأمريكية عام ٢٠١٦ والمعلومات المُتصلة بالانتخابات، قد تم عبر الأبعاد الثلاثة للفضاء السيبراني هي: المادية، الإعَلامية، والمعرفية، ويتشكل البُعد الأول والثاني: عندما يَستغل المتسللون عيوب الأجهزة والبرامج للوصول غير المُصرح به إلى أجهزة الكمبيوتر، والشبكات، والمعلومات المسروقة التي عثروا عليها، أما البعد الثالث: فهو هدف جَديد وأكثر أهميةً؛ **إنه عُقول المستَخدمين** تأتي هذه النظرة ثُلاثية الأبعاد للفضاء السيبراني، من البروفيسور (دان كويل) من جامعة الدفاع الوطني، الذي أعَرب عن قلقه بشأن أنشطة القرصنة التقليدية وما تَعنيه للأمن القومي، لكنَ الخطورة الجديدة تكمُن في استخدام هذه الادوات لاستهداف تصورات الناس وعمليات تفكيّرهم أيضًا، ومن أبرز الامثلة على ذلك،

---

(1) Illya Golovatenko, The Three Dimensions of the Cybersecurity Cube, Dec 13,2018,p.1. Available at Link:
https://swansoftwaresolutions.com/the-three-dimensions-of-the-cybersecurity-cube/#cerber-recaptcha-msg Date of visit,29- March 2021.

* السرية والنزاهة والتوافر، (Confidentiality, integrity and availability)

التدخل الرُوسي في الانتخابات الامريكية سنة ٢٠١٦ عندما استخدموا أدوات على شَبكة الإنترنت للتَأثير على وجهات نَظر الأمريكيين السياسية، وعلى أصواتهُم [١].

إنّ استعمال بعض أدوات الإنترنت لأغراض التجسس ووقود لحَملات التضَليل هو نوع جديد من الغزو الثقافي، وتكمن فكرتهُم في أن الخطوط تتلاشى بين الحرب التقليدية التي تَستخدم القنابل والصواريخ والبَنادق، والحرب غير التقليدية المُتخفية التي تُمارس منذ فترة طويلة ضد قلوب وعُقول الأجانب، من خلال قُدرات المُخابرات وقدرات القوات الخاصة، بعبارة أخرى إنهم يَخترقون نظامًا مختلفًا من خلال الهندسة الاجّتماعية على نطاق واسع، حيث ذَكر المحلل العسكري والفيلسوف الصيني (سون تزو) منذ أكثر من ٢٤٠٠عام، من بديهيات الحرب أنه من الأفضل: "إخضاع العدو دون قتال" وهذا ينطبق تماما على مقولة " أهداف قديمة وتقنيات جديدة ".

إن استخدام المعلومات أو التَضليل، أو الدعاية المنظمة (Propaganda)، كسلاح يمكن أن يكون أحد السُبل لزعزعة استقرار السكان وشل قدرات البلد المستهدف،وإنّ مُكافحة التضليل الرقمي وتحليل هذا النوع من السلوك الاستَفزازي، فيه الكثير من الصعُوبة ناهيك عن التصدي له، فالولايات المتحدة تُحاول التأثير على الجماهير الأجنبية والآراء العالمية، عَبر خدمات إذاعة صوت أمريكا من خلال الإنترنت والخدمات الإذاعّية ونشاطات الاستخبارات، وليست الحُكومات فقط هي التي تتدّخل في حملات التضليل، بل يمكن للشركات ومجموعات المناصرة وغَيرهم أيضًا إجراء هكذا حملات، بسبب القوانين والأنظمة التي تُمثل وسائل غير فعالة، علاوةً على ذلك، كانت شركات الإعلام الاجتماعي بطيئةً إلى حد ما في الاستَجابة لهذه الظاهرة، وقد ذكرت منصة تويتر أنها علّقت أكثر من (٧٠) مليون حساب مُزيف في اقل من سنة [٢].

---

(1) Richard Forno, Hackers Target 3rd Dimension of Cyberspace: Users' Minds,18 October 2018. Available at Link: https://www.livescience.com/63214-hackers-target-your-mind.html. Date visit at 25 March 2021.

(2) Craig Timberg, Elizabeth Duskin, Twitter is sweeping out fake accounts like never before, putting user growth at risk, The Washington Post, July 7 2018. Available at Link :The date of the visit is March 29, 2021.

وفي الصين نُلاحظ الكثير من التشّدد تجاه خدمة الانترنيت، من حيث تَدفُق المعلومات وحُرية الاستخدام والتواصل مع المؤسسات الحُكومية او القطاع الخاص بالإضافة الى الأفراد، وللأمانة العلمية وجد الباحث ذلك، من خلال مراسلة وزارة الخارجية الصينية والسفارة الصينية في واشنطن، إذ تم حجب الرسائل مباشرة من قبل الدوائر والمؤسسات الصينية، مقارنة بوزارة الخارجية الامريكية التي استجابت لكل الرسائل بصورة مباشرة، مما يدل على سيطرة الحكومة الصينية على خدمة الانترنيت وفرض قيود مبالغ فيها [١].

ولكن الدفاع الحقيقي تجاه وَسائل التأثير الالكترونية، يحدث في الدماغ، حيث تَعتمد أفضل حماية ضد التهديدات **للبُعد المعرفي** بالنسبة للفضاء السيبراني، على أعمال المُستخدمين ومعرفتهُم، يذكُر (Mc Cumber) بأن الأدوات التكنولوجية ليسَت كافية لهزيمة مجرميّ الإنترنت؛ وإنما يجب على مُحترفي الأمن السيبراني أيضًا بناء دفاع قوي من خلال وضع السياسات والإجراءات والمبادئ التوجيهية التي تُمكن مستخدمي الفضاء السيبراني من البقاء بأمان واتباع الممارسات الجيدة [٢].

إنّ العلاقة والتفاعل في مجال الأمن السيبراني والفَضاء الالكتروني، بين الولايات المُتحدة والصين، ربما تزيد من المنافسة التكنولوجية بينهُما في الأسواق غير المُنتظمة حيث تُقرر الدول النامية أنظمتها الالكترونية التي ستتّبناها، وتعمل الصين بالفعل على تطوير رؤيتها الخاصة – طريق الحرير الرقمي– وتُهيئ نفسها للاستفادة تجاريًا واستراتيجيًا من زيادة مستخدميّ الانترنيت، ومحاولة الولايات المتحدة الحفاظ على تفوقها في مجال تكنولوجيا الفضاء، مما يُؤثر على مستقبل النظام الدولي في مجال الفضاء الالكتروني –الى حداً كبير– وهذا التنافس رُبما يتجه نحو مزيد من التصعيد، المحكوم بمصالح تلك الدولتين وخاصة من جانب الصين، مما يترتب عليه نظام ثُنائي

---

https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/

(١) نسخة من الرسالة التي تم حظرها بتأريخ ٢ نيسان ٢٠٢١ والمرسلة الى البريد الالكتروني الخاص بالسفارة الصينية في واشنطن. (CHINAEMBASSY_US@fmprc.gov.cn) يمكن الاطلاع على الرسالة في الملحق رقم (٣) وكذلك يمكن الاطلاع على نص رسالة الخارجية الأمريكية التي جاء في مضمونها الموافقة على اشتراك الباحث كعضو للحصول على نشاطات الوزارة في قسم شؤون شرق آسيا والمحيط الهادئ في الخارجية الامريكية عبر البريد الالكتروني للباحث، في الملحق رقم (٤).

(2) Illya Golovatenko, Op. cit.p.2.

القُطبية عندما تُسيطر على الذكاء الاصطناعي الولايات المتحدة والصين، او مُتعدد الاقطاب وهو النظام الذي تسعى الصين للوصول اليه [1].

وقدر تعلُق الأمر بُمستقبل التنافس في الفضاء الالكتروني، فأن الأمان في الفضاء الالكتروني سيكون محدُود بشكل عام، مع وجود صراع في الجو والبحر والفضاء أي أمان جُزئي لوجود فواعل غير قادرة على التصّدي لمخاطر الصراع السيبراني، والسيناريو الاقَرب للواقع يتمثل بنظام مُتعدد الاقطاب، من خلال السياسة التي تتبعها الصين لتفاديّ الصراع واحتواء القَلق الأمريكي من هذا الصُعود، أذ يقوم الفكر الصيني على مبدأ الابتعاد عن تحدي الولايات المتحدة، إنِّ الحَجم الهائل للابتكار الصيني ووتيرتهُ المتصاعدة، قد يؤديان إلى سباق تسلّح للذكاء الاصطناعي تَتنافس فيه الصين والولايات المتحدة بقوة على القيادة، لكن من المُرجح أن تظهر فَجوة كبيرة داخل المُجتمعات الواحدة او مع المجتمعات الخارجية، ويُعد فقدان الكثيّر من الوظائف احتمالًا حقيقيًا؛ حيث من المرجح أن تَطغى وتيرة وحجم الاضطرابات على قُدرة أسواق العمل على التأقلم والتكيف مع الوضع المستجد الذي يطغي عليه طابع التكنولوجيا الرقمية.

وقدر تعلق الامر بأبعاد المثلث للفضاء السيبراني، يُعد البُعد المعرفي هو أهم أبعاد هذا المثلث، لذا يجب أن يسعى مُستخدمو الانترنيت في الفضاء الإلكتروني، ليصبحوا أكثر دراية بتهديدات الفضاء السيبراني وإنشاء ثقافة للتعّلم والوعي؛ من أجل تحصين بياناتهُم الشخصية وأنظمة المؤسسات العاملين فيها.

(1) Andrew Wagner,Op.cit.

الخاتمة

إنِّ التنافس السيبراني هي تَعبير عن التطّورات التي يعيشها العالم، ولذلك فهي مُستمرة على الأرجح ولها تأثِير عميق، وما قد يُؤثر على تراجُعها هو ظهور مسار آخر للهجمات الدولية، إذا توقف العالم عن استخدام التكنُولوجيا الحالية مُستبدلا إياها بأنماط أحدث في عالم لا يتوقف عن التطّور، ورُبما تصبح الهجمات الإلكترونية في المُستقبل هي الوسائل الأكثر استخداماً في التنافس المعلوماتي بدلاً عن الحروب التقليديّة، وتستَخدم الصين هذا النوع من التنافس ضد الولايات المتحدة، التي تعتبُرها القُوة المهيمنة والتي تُحاول عزل الصين عن محيطها، والحد من الصعود الصيني، وبالتالي فأن استمرار تأثير هذه التحديات على قوة الدول يعني استمرار الصين في استهداف الولايات المُتحدة عِبر الهجَمات السيبرانية، كنُوع من إجراءات الدفاع عن حُقوقها او من أجل الضغط على الولايات المتحدة

والواقع إن المنافسة الإلكترونية يمكن ان تحتل في الوقت الحالي الحرب التقليدية، لكنها ربما تكون مقدِمة تحضيرية، لأنها تستّهدف إفشال مُنظومة تبادل المعلومات تمهيداً للحرب وليست هي الحرب ذاتها ، ولكِنها مفتاح الدخول للحرب، وربما تمثل مفاتيح الانتصار في المستقبل القريب. لذلك أصبح الأمن الإلكتروني من أهم هواجِس الدولة الأمنية لضمان أمن وسلامة منشآتها الإلكترونية. لذلك ينبغي توظّيف استراتيجية قوية خاصة بالأمن السيبراني، ببذِل المزيد من الجُهد للانتباه لهجمات طلب الفِدية، تأمين عمليات تسجّيل الدخول للتطبيقات التي يتم الوصول إليها من خارج الشبكة، باستخدام أساليب محمية قوية، فَحص وتصفية حركة مُرور البيانات على الإنترنت، الاحتفاظ بُنسخ احتياطية لجميّع الأنظمة والبيانات الشخصية الهامة، تحسّين تبادُل المعلومات وتخطيط المهام وقيادتُها فيما يتعلق بالشؤون السيبرانية.

إنِّ علاقة التَنافس المتجذِرة بين الولايات المتحدة الأمريكية والصين في المَزايا النسبية التي تمتلِكها الولايات المتحدة بالفعل، وعلى الرغم من أن المنافسة ستّظل السِمة المُحدِدة للعلاقة، فإن كلا البلدين سيستمران في التأثر – سواء كان ذلك إيجابا أو سلبا– بقدرتهُما على التنسيق بشأن التحديات المُشتركة التي لا يستطيع أي منهُما حلها بمفردهِ، مثل الأمراض الوبائية والرُكود في الاقتصاد العالمي وتغّير المناخ ومنع انتشار الأسلِحة النووية، إن الولايات المتحدة رُبما تُحقق

نجاحًا أكبر في التفوق على الصين اقتصاديًا وتفوقُها في مسائل الحُوكمة، إذا ركزّت على تحسين وضعها في الداخل أكثر من محاولة إعاقة المبادرات الصينية، والمُهمة المطرُوحة لِبست الوقُوف في طريق الصين وتحويل قوة صاعدة إلى عدو في هذه العملية، ولكن بتجدّيد مزايا الولايات المتحدة الأمريكية في مُنافستها مع الصين.

الاستنتاجات:

١- يمكن اعِتبار سيادة الدولة من أكثر العناصر التي تأثرت بالثورة المعلُوماتية، أذ ألقت بظلاِلها على الواقع السياسي، وذلك بسبب أتِساع القُدرة لدى الفواعل من غير الدول على اختراق سيادة وحدود الدولة، التي أصبحت مُجرد خطُوط تمثل شكل وحجم الدولة، دون القدرة على منع الاختراقات الإلكترونية لسيادة الدولة، بحيث أصبح هناك تحول في مفهوم القومية " إلى مفهوم سيادة الشعب أو المواطن".

٢- ظهور مفهوم جديد للحُدود غير الحدود التقليدية وهي الحدود الوطنية الإلكترونية، التي أصبحت مُهمة حمايتها أصعب على الدولة مقارنة بالحدود السياسية للدولة، وإمكانية اختراقها أسهل من الحدُود التقليدية للدولة، إلا أن هذا لا يُبرر ممارسة القيُود المفرطة على حرية المواطن في الصين، مقابل الحرية الأوسُع بالنسبة للمواطن الامريكي، وهذا يُحسب للولايات المتحدة في مجال حقوق الانسان على المستوى العالمي.

٣- أصبح الأمن السيبراني أحد مجالات الأمن القومي، التي تَستدعي الاهتمام الكبير من قبل الدولة والاكثر أهمية بالقياس إلى المجالات الاخرى- الأمنية منها خاصة - ؛ وذلك لتطور وتغّير الطُرق ووسائل التهّديد الإلكتروني للأمن القومي للدول كما أصبحت الهجمات الإلكترونية والجرائم الإلكترونية عابرة للحدُود القومية، وفي ازدياد مستمر مع التوقعات بازدياد أعداد الأجهزة التي سيتم توصيلها(بإنترنت الأشياء)* بحلول عام ٢٠٢٤.

* ويقصد به شبكة الأجهزة القادرة على جمع البيانات ومشاركتها مع الأجهزة الأخرى الموجودة على الشبكة نفسها، والتحكم فيها عن بعد من خلال البنية التحتية للشبكة الحالية، (بمعنى ربط اجهزة المنزل مثلا بالأنترنت).

٤- من خلال أحصاء العدد الكُلي لحوادث الأمن السيبراني، نلاحظ ارتفاع مُستوى الهجمات السيبرانية، حيث يكون ذلك واضحاً من خلال المقارنة بين سنة ٢٠١٤ حيث بلغ (٤٢,٠٨) مليون اختراق بينما وصل في سنة ٢٠١٥ الى (٥٩,٠٦)مليون اختراق، وتم أحصاء (١٤٥ مليون) برنامج ضار سنة ٢٠١٩، وهذا يجعل من النشاط السيبراني الدولي عامل عدم استقرار للسلم والأمن الدوليين، ويضاف إلى ذلك إن المجتمع الدولي يفتقر إلى القواعد والخبرة والاتفاقيات التي تواكب التطور المستمر في مجال الأمن السيبراني، بالإضافة إلى رغبة الصين ورُوسيا في تغيّير الوضع الراهن في العلاقات الدولية.

٥- تَعمل الولايات المُتحدة والصين على إعادة تَحديد علاقتهُما الثنائية، حيث تعني نُقاط القوة الجديدة للصين أن لديها مُوقعًا جديدًا ومسؤوليات جديدة في العالم، بحيث أصبحت المنافسة التكنولوجية عنصراً محددٍ للعلاقة الثنائية، لأنها يمكن أن يؤدي إلى تفاقم المنافسة الاقتصادية والعسكرية.

٦- الصعّود السلمي للصين سيكُون مقبول لدى أغلب الدول؛ حيث أرتبط بثلاث أفكار رئيسة هي: "التنمية الاقتصادية السياسية "، و"السيادة السياسية" و"قانون الدولة" مقابل تمسُك الولايات المتحدة بخطاب القُوة وتغيير النظام الدولي لمصلحِتها، إذ يتحدث الصينيون عن احترام السيادة وتنوع الحضارات، كما أن الدُبلوماسية الصينية تقدم المساعدات والقروض غِير المشرُوطة، وخاصةً في أزمة جائحة كورونا في خطوة لتفعيل القُوة الناعمة.

التوصيات:

١- يفضل أن يتمسك الجانبين الصيني والأمريكي باتجاه تطور العلاقة الثنائية من المنظور الاستراتيجي، والبعيد المدى وبالمُوقف المسؤول تجاه التاريخ والشعب، وتعزيز الاتصال والحوار والتواصُل انطلاقاً من المصالح الأساسية للشَعبين وشعُوب العالم، بما يُعيد العلاقة الثُنائية إلى مسارها الصحيح، وعلى صانعّي القرار في الولايات المتحدة، تغيير النَهج المُتبع في التعامل مع الصين، وبذل جهُود مشتركة مع الجانب الصيني لإدارة الخلافات والسيطرة عليها على أساس مبدأ الاحترام المُتبادل، وعلى الصين التخفّيف من القيُود التي تفرُضها على حرية

المواطنّين في اِستخدام الانترنت، والعمل على تغيّير النظر للصين من قِبل العالم الخارجي، على أنها دولة تنتَهك حقوق الملكية الفكرية في كثير من المجالات، لتعزيز مكانتُها الدولية.

٢- من الأفضل ان تقوم الولايات المتحدة الأمريكية باتِخاذ نَهج مُتعدد الأبعاد بشكل مُتزايد، لتُأكد لحلفائِها أن الولايات المتحدة ستستمر في الحِفاظ على القُدرة والعزم على دعمهِم في أي أزمة، حتى مع تعزيز الصين لقُدراتها على "الردع الاستراتيجي المتكامل".

٣- توصي الدراسة بضرورة تضمين موضوع الأمن السيبراني، كمادة ضمن المناهج الدراسية للكليات ذات العلاقة بهذا الموضوع – وخاصة في العراق –على مستوى الدراسات الأولية والعليا؛ باعتباره موضوع حديث ومهم، حيث أخذ بعداً مهما ضمن مجال الأمن القومي للدول، أضافة إلى الاستخدام الواسع له في أغلب مجالات الحياة على مستوى الأفراد والدول، والتطور المستمر في تقنية وتكنولوجيا المعلومات، حيث أصبحت المعرفة تشكل " الثروة والسلطة والنفوذ " كما توصي الدراسة الجهات المختصة في العراق بدعم مراكز الأبحاث المتخصصة في مجال الفضاء الخارجي للاستفادة من منها في رفد صنّاع القرار بمصادر المعلومات والرؤى والتوصيات في هذا المجال الحيوي والمهم.

قائمة المصادر والمراجع

القرآن الكريم

أولاً: الوثائق

١- الأمانة العامة لجامعة الدول العربية الدول العربية – إدارة الشؤون القانونية – الشبكة القانونية العربية، نص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الفصل الختامي أحكام ختامية، ٢٠١٠.

٢- الأُمم المتحدة مكتب شؤون الفضاء الخارجي، معاهدات الأُمم المتحدة ومبادئها المتعلقة بالفضاء الخارجي وقرارات الجمعية العامة والوثائق الأخرى ذات الصلة.

٣- ميثاق الأُمم المتحدة الفصل السابع .

٤- اللجنة الاقتصادية والاجتماعية لغرب آسيا الاسكوا، الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية، الأُمم المتحدة، ٩ شباط ٢٠١٥.

٥- المؤتمر الصحفي الذي عقدته الدورة الأولى للمجلس الوطني الثالث عشر لنواب الشعب الصيني بتأريخ ٨ أذار ٢٠١٨ في المركز الاعلامي الخاص بالمجلس، حيث دعت وزير الخارجية الصيني (Wang Bi) للإجابة على أسئلة الصحفيين الصينين والأجانب. حول سياسة الصين الخارجية وعلاقاتها الدولية.

ثانياً:القواميس

١- قاموس ميريام ويبستر(Merriam Webster) متاح على الرابط
https://www.merriam-webster.com

ثالثاً: الكُتب العربية والمُترجمة:

١- : توم ميلر، الحلم الآسيوي للصين "بناء إمبراطورية على طول طريق الحرير الجديد"، ترجمة عبد الرحمن الياس، ط١، قنديل للطباعة والنشر، دبي، ٢٠١٩.

٢- ألفين توفلر، تحول السلطة، ترجمة لبنى الريدي، ج١، الهيئة المصرية العامة للكتاب، القاهرة،١٩٩٥.

٣- أيمل خوري، صراعات الجيل الخامس، ط١، شركة المطبوعات للتوزيع والنشر، بيروت، ٢٠١٦.

٤- إيهاب خليفة، القوة الإلكترونية كيف يمكن أن تدير الدول شؤونها في عصر الانترنيت، ط١، العربي للنشر والتوزيع، القاهرة، ٢٠١٧.

٥- بيتر بي سيل، الكون الرقمي – الثورة العالمية في الاتصالات، ترجمة ضياء وزاد، مؤسسة هنداوي للنشر، لندن، ٢٠١٧.

٦- الدين جيلاني أبو زيد وماجد الحموي، الوسيط في القانون الدولي العام، دار الشواف، الرياض،٢٠٠٣.

٧- ريتشارد كلارك وروبرت نيك، حرب الفضاء الالكتروني، مركز الأمارات للدراسات والبحوث الاستراتيجية، ط١، ابو ظبي، ٢٠١٢.

٨- زيغنيو بيرجنسكي، رقعة الشطرنج الكبرى السيطرة الإمريكية وما يترتب عليها جيواستراتيجياً، ترجمة: وزارة الدفاع مركز الدراسات العسكرية،واشنطن، ط٢، ١٩٩٩.

٩- سالي نبيل شعراوي، العلاقات الصينية الأمريكية وأثر التحول في النظام الدولي، القاهرة، العربي للنشر والتوزيع، ٢٠١٧.

١٠- ستيفان هالبر وجوناثان كلارك، التفرد الأمريكي المحافظون الجدد والنظام العالمي، ترجمة عمر الايوبي، دار الكتاب العربي، بيروت ٢٠٠٥.

١١- سكوت وارين، مارتن سي ليبيكي، وأستريد ستوث سيفالوس، التوصل الى أتفاق مع الصين بشأن الفضاء الإلكتروني، مؤسسة راند للنشر، كاليفورنيا، ٢٠١٦.

١٢- علي زياد العلي، الصراع والأمن الجيوسيبراني في السياسة الدولية "دراسة في استراتيجيات الاشتباك الرقمي "، دار امجد للنشر والتوزيع، عمان، ٢٠١٩.

١٣- غراهام أليسون، حتمية الحرب بين القوة الصاعدة والقوة المهيمنة –هل تنجح الصين وأمريكا في الافلات من فخ ثيوسيديديس؟، ترجمة أسماعيل بهاء الدين سليمان، دار الكتاب العربي، بيروت، ٢٠١٨.

١٤- لورنس لسيج، الكود المنظم للفضاء الإلكتروني، ترجمة محمد سعد طنطاوي، الطبعة الثانية، مؤسسة هنداوي، القاهرة، ٢٠١٤.

١٥- موسى محمد مصطفى، الارهاب الإلكتروني، القاهرة، مطابع الشرطة، ٢٠٠٩.

١٦- هاري آر. يارغر، الاستراتيجية ومحترفو الأمن القومي: التفكير الاستراتيجي وصياغة الاستراتيجية في القرن الحادي والعشرين، ترجمة راجح محرز علي، مركز الامارات للدراسات والبحوث الاستراتيجية، ابو ظبي، ٢٠١١.

رابعاً: الرسائل والاطاريح:

١- عبد الكريم زهير عطيه الشمري، الاستراتيجية الأمريكية للهيمنة على الفضاء السيبراني، رسالة ماجستير، جامعة الموصل، كلية العلوم السياسية، ٢٠٢١.

٢- فريدة طاجين، تأثير القوة السيبرانية على الاستراتيجيات الأمنية للدول الكبرى – دراسة حالة الصين –، رسالة ماجستير، جامعة قاصدي مرباح ورقلة، ٢٠١٨.

٣- نوران شفيق علي، الفضاء الإلكتروني وانماط التفاعلات الدولية: دراسة في أبعاد الأمن الإلكتروني، رسالة ماجستير، جامعة القاهرة، كلية الاقتصاد والعلوم السياسية، ٢٠١٤.

خامساً: الدوريات

١- أحمد يوسف كيطان، استراتيجية الأمن الوطني السيبراني للصين: قراءة في قانون الأمن السيبراني الصيني، مركز النهرين للدراسات الاستراتيجية، الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، ٢٧ تشرين الثاني ٢٠١٩.

٢- إسراء جبريل رشيد مرعي، الجرائم الإلكترونية الأسباب الأهداف طرق الجريمة ومعالجتها، المركز الديمقراطي العربي للدراسات الاستراتيجية الاقتصادية والسياسية، القاهرة، ٩أب ٢٠١٦.

٣- إيهاب خليفة، أبعاد الصراع الصيني–الأمريكي على الهيمنة التكنولوجية، مركز المستقبل للأبحاث والدراسات المتقدمة ابو ظبي، ٦ كانون الاول ٢٠١٨.

٤- _____، الأمن السيبراني الماهية والاشكاليات، مجلة رؤى مصرية ،العدد٥٧،مركز الأهرام للدراسات الاجتماعية والتاريخية، القاهرة، ٢٠١٩ .

٥- بهاء عدنان السعيري وعماد عبد خضير الزرفي، انتقال التهديدات من الواقع الى العالم الافتراضي، مجلة كلية العلوم السياسية، جامعة الكوفة، المجلد ٢٧، العد ٤، ٢٠١٩.

٦- تيموثي آر هيث، كريستين غانيس، كورتيز إي كوبر، إعادة تطوير الصين وجيش التحرير الشعبي: الاستراتيجية العسكرية واستراتيجية الأمن القومي-ومفاهيم الردع والقدرات القتالية-، مؤسسة راند،سانتا مونيكا، كاليفورنيا، ٢٠١٦.

٧- جريدة العرب، مستقبل الفضاء السيبراني مجال الصراع بين الدول، ٨تشرين الاول ٢٠١٥. متاح على الموقع: https://alarab.co.uk تأريخ الزيارة ٥ كانون الثاني ٢٠٢١.

٨- جهاد عمر محمد الخطيب، دراسة بحثية العلاقات الأمريكية الصينية "آفاق الصراع والتعاون" ٢٠٠٨م – ٢٠١٥ م، المركز الديمقراطي العربي للدراسات الاستراتيجية الاقتصادية والسياسية، القاهرة،١٧ حزيران ٢٠١٦.

٩- حجيبة قاقو، الفضاء العمومي الألكتروني والتعبئة السياسية الذكية، مجلة العلوم السياسية والقانون، المركز الديمقراطي العربي للدراسات الاستراتيجية والاقتصادية، برلين، العدد الثاني، اذار ٢٠١٧.

١٠- حمد سعد أبو عامود، العلاقات الأمريكية الصينية، مجلة السياسة الدولية، العدد ١٤٥، مؤسسة الأهرام ،القاهرة، يوليو٢٠٠٨.

١١- خالد حنفي إشكالية تداخل الصراعات السيبرانية والتقليدية، ملحق مجلة السياسة الدولية، العدد ٢٠٨، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، ٢٠١٧.

١٢- دلال العودة ، الصراعات الدولية الحديثة ،الطبعة الأُولى ، دار الطلائع للنشر والطباعة ،القاهرة ٢٠١٥.

١٣- رغدة البهي، الردع السيبراني: المفهوم والاشكاليات والمتطلبات، مجلة العلوم السياسية والقانون العدد الاول، المركز الديمقراطي العربي للدراسات الاستراتيجية والاقتصادية، برلين، كانون الثاني ٢٠١٧.

١٤- رؤى خليل سعيد، الإرهاب الإلكتروني وأثره في أمن الدول – السعودية نموذجا –، مجلة حمورابي، العدد ٢٥-٢٦، مركز حمورابي للبحوث والدراسات الاستراتيجية، شتاء – ربيع ٢٠١٨.

١٥- رنا علي خلف، المقوم التكنولوجي وأثره في السياسة الأمريكية ، مجلة السياسة الدولية ،العدد٤٩، كلية العلوم السياسية جامعة بغداد، ٤٩، السنة ٢٠١٥.

١٦- سماح عبد الصبور، الصراع السيبراني: طبيعة المفهوم وملامح الفاعلين – اتجاهات نظرية في تحليل السياسة الدولية، ملحق مجلة السياسة الدولية،، العدد ٢٠٨،مؤسسة الأهرام القاهرة، مركز الأهرام للدراسات السياسية والاستراتيجية، ٢٠١٧.

١٧- السيد امين شلبي، هل الصعود الصيني تهديد للولايات المتحدة.، مجلة السياسة الدولية، القاهرة، مركز الاهرام للدراسات الاستراتيجية. العدد ١٦٥، ٢٠٠٦.

١٨- سيد عبد النبي محمد، صراع الأمم وحروب الجيل الخامس، وكالة الصحافة العربية ناشرون، الجيزة، ٢٠١٩.

١٩- صفاء حسين علي الجبوري. العلاقات الأمريكية الصينية في مرحلة ما بعد الحرب الباردة، مجلة جامعة تكريت كلية العلوم القانونية والسياسية، المجلد ٣، السنة ٣، العدد ١٢، ٢٠١١.

٢٠- عادل عبد الجواد محمد، دور مراكز المعلومات في التعامل مع الازمات، مجلة الأمن والحياة، العدد ٣٥٨، الرياض، ٢٠١٦.

٢١- عادل عبد الصادق، الفضاء الإلكتروني واشكاليات نظرية العلاقات الدولية، مجلة السياسة الدولية، المجلد ٥٠، العدد ٢٠٠،مؤسسة الأهرام القاهرة، نيسان ٢٠١٥.

٢٢- _____، الفضاء الإلكتروني وتهديدات جديدة للأمن القومي، مجلة السياسة الدولية، العدد ١٨٠، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، ٢٠١٠.

٢٣- _____، الفضاء ساحة جديدة للتنافس الآسيوي، مجلة السياسة الدولية، المجلد ٤٦، العدد ١٨٣، مؤسسة الاهرام، كانون الثاني ٢٠١١.

٢٤- _____، القوة الإلكترونية: أسلحة الدمار الشامل في عصر الفضاء الإلكتروني، مجلة السياسة الدولية، مؤسسة الاهرام، القاهرة، العدد ١٨٨، نيسان ٢٠١٢.

٢٥- عبد الغفار عفيفي الدويك، استراتيجية الردع السيبراني. التجربة الأمريكية، مجلة السياسة الدولية، المجلد ٥٣، العدد ٢١٣، مؤسسة الأهرام القاهرة، حزيران ٢٠١٨.

٢٦- عبد الله بن عبد العزيز بن فهد العجلان، الارهاب الإلكتروني في عصر المعلومات، بحث مقدم الى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الانترنيت"، والمنعقد بالقاهرة في ٤-٢ حزيران ٢٠٠٨.

٢٧- عبد الهادي محمود الزيدي، التجسس الاسرائيلي الإلكتروني على الدول العربية، مجلة دراسات دولية، مركز الدراسات الدولية، جامعة بغداد، العدد ٥٨، تموز ٢٠١٤.

٢٨- علم الدين بانقا، مخاطر الهجمات الإلكترونية (السيبرانية) واثارها الاقتصادية –دراسة حالة دول مجلس التعاون الخليجي، سلسلة دراسات تنموية، المعهد العربي للتخطيط، العدد ٦٣، الكويت، نيسان ٢١٠٩.

٢٩- كركوري مباركة حنان، خصوصية ارتكاب الجريمة في النظام المعلوماتي –دراسة تحليلية في ضوء القانون الجزائري –، مجلة الدراسات الاستراتيجية والعسكرية، المجلد الثاني، العدد الثامن، المركز الديمقراطي العربي، برلين، ، ايلول ٢٠٢٠.

٣٠- لبنى خميس مهدي وخضير عباس عطوان، الابعاد الاستراتيجية للعلاقات الصينية الأمريكية وآفاقها المستقبلية، مجلة دراسات دولية مركز الدراسات الاستراتيجية والدولية، جامعة بغداد، العدد ٧٤، ٢٠١٨.

٣١- ليث صلاح الدين حبيب، التجسس وأحكامه أبان النزاعات المسلحة الدولية، مجلة جامعة الأنبار للعلوم القانونية والسياسية، العدد الأول، كلية القانون والعلوم السياسية، جامعة الأنبار، ٢٠٠٩.

٣٢- مايكل إس تشايس، آرثر تشان، نهج الصين المتطور "إزاء الردع الاستراتيجي المتكامل، مؤسسة راند في سانتا مونيكا، كاليفورنيا، ٢٠١٦.

٣٣- محمد دياب، جدلية العلاقة بين الأنفاق العسكري والتنمية الاقتصادية، مجلة الدفاع الوطني اللبناني، العدد ٢٥، بيروت، كانون الثاني ٢٠١١.

٣٤- محمد عبد ربه المغير، تحصين الجبهة الداخلية من حروب الجيل الخامس، مجلة الدراسات الاستراتيجية والعسكرية – المركز الديمقراطي العربي، المجلد الأول، العدد الثاني، كانون الاول ٢٠١٨.

٣٥- مصطفى كمال، الطائرات بدون طيار النشأة والتطور، مجلة السياسة الدولية، مركز الأهرام للدراسات السياسية والاستراتيجية، المجلد ٥٥، العدد٢٢٠، القاهرة، نيسان ٢٠٢٠.

٣٦- مكب الأُمم المتحدة المعني بالمخدرات والجريمة، دراسة شاملة عن الجريمة السيبرانية، الامم المتحدة، نيويورك، ٢٠١٣.

٣٧- منى الأشقر جبور، وعزيز ملحم بربر، أمن الشبكات والانترنيت، جامعة نايف العربية للعلوم الامنية، كلية التدريب قسم البرامج التدريبية، القاهرة، ٢٠٠٨.

٣٨- نامراتا جوسوامي، صراع مستقبلي: نشاط دولي واسع لاستغلال موارد الفضاء الخارجي، معهد الولايات المتحددة للسلام، العدد ٢٨، واشنطن، ٢٠١٨.
٣٩- نهى العبادي، الأتحاد الأوروبي . تداعيات الحرب الإلكترونية مع روسيا، المركز الاوربي لدراسات مكافحة الارهاب والاستخبارات، المانيا، ١٣ نيسان ٢٠٢١.
٤٠- نوران شفيق، أشكال التهديدات الألكترونية ومصادرها، المركز الاوربي لدراسات مكافحة الارهاب، المانيا – هولندا، ٢٩ كانون الثاني ٢٠٢٠
٤١- نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول، المجلد الثامن، العدد الثاني، مجلة مركز بابل للدراسات الانسانية، الحلة، ٢٠١٨
٤٢- هالة احمد الرشيدي، الجهود الدولية في مجال مكافحة الجرائم الالكترونية، مجلة الديمقراطية، مؤسسة الاهرام، العدد ٧٥، القاهرة، تموز ٢٠١٩.
٤٣- هالة محمود طه دودين، العلاقات الصينية الأمريكية ما بين الحرب التجارية وفايروس كورونا، المركز الديمقراطي العربي، مجلة قضايا اسيوية، العدد الرابع، برلين، نيسان ٢٠٢٠.
٤٤- يحيى مفرح الزهراني، الابعاد الاستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، العدد ٢٣، السنة ١٤، شتاء ٢٠١٧.
٤٥- يونس مؤيد يونس مصطفى، استراتيجية الولايات المتحدة الأمريكية للأمن السيبراني، مجلة قضايا سياسية كلية العلوم السياسية جامعة النهرين، العدد ٥٥، ٢٠١٨.

سادساً: التقارير

١- أحمد عبد الرحمن المحمود، البعثة الدائمة لدولة الأمارات لدى الأُمم المتحدة، استخدام الفضاء الخارجي في الاغراض السلمية. الكلمة التي ألقها ممثل دولة الأمارات أمام رئاسة لجنة المسائل السياسية الخاصة وأنهاء الاستعمار، والسيد ديفيد كندل رئيس لجنة الاستخدامات السلمية للفضاء الخارجي، في ١٣تشرين الاول ٢٠١٦ في الأُمم المتحدة.
٢- الأُمم المتحدة – مجلس الأمن، التدابير المتخذة في حالات تهديد السلم والإخلال به ووقوع العدوان (الفصل السابع)، المادة (٣٩)- المادة (٥١).

٣- تقرير محكمة العدل الدولية في ١ آب/ ٢٠٠٤ – ٣١ تموز ٢٠٠٥ الدورة (٦٠) الملحق رقم ٤ (A/60/4) الأنشطة المسلحة في أراضي الكونغو (جمهورية الكونغو الديمقراطية ضد أوغندا).

٤- الأُمم المتحدة، الجمعية العامة، مجلس حقوق الإنسان الدورة الثالثة والعشرون البند ٣ من جدول الأعمال، ٩ نيسان ٢٠١٣.

٥- دليل تالين بشأن القانون الدولي المطبق على الحروب السيبرانية ، ترجمة علي كاظم الموسوي٢٠١٧ ،شركة المؤسسة الحديثة للكتاب٢٠١٩.

سابعاً: المحاضرات والبيانات

١- البيان الصحفي لسكرتير الرئيس الأمريكي دونالد ترامب للشؤون الخارجية مايكل ريتشارد. بومبيو بشأن الفظائع في شينجيانغ، ١٩كانون الثاني ٢٠٢١. متاح على الموقع: تأريخ الزيارة ٣شباط ٢٠٢١. https://2017-2021.state.gov/determination-of-the-secretary-of-state-on-atrocities-in-xinjiang/index.html

٢- تصريح السفير الأمريكي لدى الصين، الموقع الرسمي لوزارة الخارجية الامريكية، متاح على الموقع: تأريخ الزيارة ٥شباط ٢٠٢١ ٢٠١٧. state.gov/r/pa/ei/biog/221450.htm- https://2009

٣- فريدة طاجين، سياسات الدفاع الماليزية في ظل التهديدات الأمنية للبيئة الرقمية :الواقع والتحديات، الملتقى الدولي الثاني حول سياسات الدفاع، كلية الحقوق والعلوم السياسية:قسم العلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2017.

٤- محاضرة ألقاها غراهام أليسون حول كتابه الجديد، حتمية الحرب، على قناة (TED) في شباط ٢٠٢١.

ثامناً: اللقاءات التلفزيونية

١- اللقاء التلفزيوني قناة WarCQC مع الكاتب فوكاياما. بعنوان: هل ستهيمن الصين على العالم، ترجمة سعيد القحطاني ٢٩ بتأريخ حزيران ٢٠٢٠.

تاسعاً: الانترنت

١- أبرز التوقعات عن الأمن السيبراني في العالم العربي وأوروبا وإفريقيا في ٢٠٢١، الحاجة إلى اتخاذ إجراءات مجدية لرفع سوية الأمن الإلكتروني، مرصد المستقبل، دبي، ٢كانون الثاني ٢٠٢٠. متاح على الموقع: https://mostaqbal.ae/most-prominent-predictions-of- cybersecurity-in-the-arab-world-europe-and-africa-in-2021/

٢- آدم مستيان، العالم العربي وامبريالية المصادر الرقمية. ١٢ كانون الثاني ٢٠١٧ متاح على الموقع:/https://www.academia.edu/31613485 تأريخ الزيارة ٢٠ كانون الثاني ٢٠٢١.

٣- إسراء أحمد اسماعيل، عناصر الاستراتيجية الصينية للأمن الإلكتروني، ٥ شباط ٢٠١٥.متاح على الموقع: https://futureuae.com/ar-/MainPage/Item/684 تأريخ الزيارة ٢٢أذار ٢٠٢١.

٤- اولاف تايلر، التهديدات الجديدة: الأبعاد الإلكترونية، مجلة حلف الناتو. في ١١ ايلول ٢٠١١. متاح على الموقع: تاريخ الزيارة ١٨أذار ٢٠ http://www.nato.int./docu/reviw/2011/11-september/Cyber-Threads/AR/index.htm

٥- إيهاب خليفة، الهجمات الصفرية، مركز المستقبل للابحاث والدراسات المتقدمة، متاح على الموقع: https://futureuae.com/ar/Mainpage/Item/2802/ تأريخ الزيارة ١شباط ٢٠٢١.

٦- إيهاب خليفة، ما هو موقف ميثاق الأُمم المتحدة من استخدام القوة السيبرانية في التفاعلات الدولية؟، مركز المستقبل للابحاث والدراسات المتقدمة. ٢٤/تشرين الاول ٢٠١٩. متاح على الموقع: https://futureuae.com/ar/Mainpage/Item/ تأريخ الزيارة ٧ كانون الثاني ٢٠٢١.

٧- باهر مردان، العلاقات الصينية – الأمريكية، بكين،٢٠١٤، ص٣. متاح على الرابط التالي: https://www.academia.edu/6003157 تأريخ الزيارة ١شباط ٢٠٢١

٨- بدرة قعلول، الجيل السادس للحروب – حرب الفيروسات. المركز الدولي للدراسات الاستراتيجية الامنية والعسكرية. الجزائر، ٢٠٢٠. متاح على الموقع: https://strategianews.net/ تأريخ الزيارة ٧ كانون الثاني ٢٠٢١.

٩- تصريحات الرئيس الامريكي دونالد ترامب وتصريح وزير الخزانة الأمريكي ستيفن منوتشين، حول أتفاق التجارة الأميركي- الصيني متاح على الموقع:.https://www.aljazeera.net/ebusiness/2020/1/16

١٠- جليل خلف شويل، صراعات الجيل الرابع المستقبل للشعوب وليس للحكام، جريدة البينة الجديدة، في ٨/٩/ ٢٠٢٠. متاح على الموقع: تأريخ الزيارة ٦ كانون الثاني ٢٠٢١ https://albayyna- new.net/content.php?id=21358

١١- رسالة من السيد جيمس لويس (JALewis@csis.org) عبر البريد الإلكتروني الخاص للباحث (moh09l2006@uoanbar.edu.iq) في ١٢ أذار ٢٠٢١ الساعة ٥:٢٢ مساء ويمكن الاطلاع على نص الرسالة بالملحق.

١٢- رياض الخالق، اجتماع "ألاسكا" فرصة لإنعاش العلاقات الأمريكية الصينية، وكالة الاناضول. ١٨ أذار ٢٠٢١.متاح على الموقع:https://www.aa.com.tr/ar تأريخ الزيارة ٢٨نيسان ٢٠٢١.

١٣- صادرات التكنولوجيا المتقدمة (بالأسعار الجارية للدولار الأمريكي، الموقع الرسمي للبنك الدولي، متاح على الموقع:
https://data.albankaldawli.org/indicator/TX.VAL.TECH.CD.تأريخ الزيارة ٢٢أذار ٢٠٢١.

١٤- صحيفة الشعب اليومية الصينية، عدد سكان الصين يتجاوز ١,٤ مليار نسمة في ٢٠١٩، الموقع الرسمي للصحيفة ١٧كانون الثاني ٢٠٢٠. متاح على الموقع: تأريخ الزيارة ٢١أذار ٢٠٢١ : http://arabic.people.com.cn/n3/2020/0117/c31664- 9649819.html

١٥- عادل درويش، القراصنة الروس يستهدفون شركة Crowd Strike، مجلة التطوير الرقمي، العدد الرابع،٢٨، كانون الأول ٢٠٢٠.متاح على الموقع: https://www.ddc.iq/articles/3758

١٦- عادل عبد الصادق، الانترنيت والدبلوماسية ومعركة القوة الناعمة بين الولايات المتحدة وايران، المركز العربي لأبحاث الفضاء الالكتروني (ACCR)، ٢٠١٨.متاح على الموقع: http://www.accronline.com/article_detail.aspx?id=29022 تأريخ الزيارة ٢ أذار ٢٠٢١

١٧- العربية CRL online مقابلة خاصة مع ماكس بوكس سفير الولايات المتحدة السابق لدى الصين، متاح على الموقع: http://arabic.cri.cn/video/3189/20200718/508525.html 2020-07-18 17:54:14 تأريخ الزيارة ٦شباط ٢٠٢١.

١٨- قائمة البلدان حسب احتياطيات العملات الأجنبية، متاح على الموقع : https://www.marefa.org/% تأريخ الزيارة ٣شباط ٢٠٢١ .

١٩- كونج كاو، تقرير اليونسكو للعلوم، ٢٠١٥، متاح على الموقع: https://books.google.iq/books تأريخ الزيارة ٢٥شباط ٢٠٢١.

٢٠- لازاروس كابامبي، الأُمم المتحدة، اجتماع المجلس الاقتصادي والاجتماعي حول اهمية أمن الفضاء الالكتروني، نيويورك، ١٢ كانون الثاني ٢٠١١، ادارة الشؤون الاقتصادية والاجتماعية: متاح على الموقع الرسمي للأُمم المتحدة: تأريخ الزيارة ٢٢شباط ٢٠٢١. https://www.un.org/development/desa/ar/news/intergovernmental-coordination/cybersecurity-demands-global-approach.html

٢١- مجلة يونيباث، المؤتمر السنوي التاسع للأمن السيبراني للمنطقة الوسطى نيسان ٢٠١٩،

٢٢- مكتب الأُمم المتحدة لشؤون الفضاء الخارجي، اللقاء التلفزيوني مع مديرة المكتب سيمونيتا دي بيبو، ١٢ كانون الثاني ٢٠١٧. متاح على الموقع: https://news.un.org/ar/audio/2017/01/359542 تأريخ الزيارة ١٢ شباط ٢٠٢١.

٢٣- ميليسا هاثاواي، أدارة الخطر السيبراني الوطني، منشورات موقع المدى، ٢٠١٨. متاح على الموقع:- https://potomacinstitute.org/images/CRI/Managing-National-Cyber-Risks_FINAL-Arabic.pdf

٢٤- نبيل عودة، الفضاء الإلكتروني والشؤون الدولية، ١٥/ ٩/ ٢٠١٨. متاح على الموقع: https://arabicpost.net/opinions/2020/09/03 تأريخ الزيارة ٢٣كانون الثاني ٢٠٢١.

٢٥- الياس الصديقي، الفضاء الافتراضي والقانون الدولي، المركز العربي لأبحاث الفضاء الإلكتروني،٢٥ تشرين الثاني ٢٠١٧. متاح على الموقع: http://accronline.com/article_detail.aspx?id=28959 تأريخ الزيارة ٥ ايار ٢٠٢١.

English Sources:

First the documents:

1- A message from the US State Department/East Asia and Pacific Division on the researcher's mail is listed in the appendix., Secretary Antony J. Blinken, Secretary of Defense Lloyd Austin, Japanese Foreign Minister Toshimitsu Motegi, and Japanese Defense Minister Nobua Kishi at a Joint Press Availability, March 16, 2021.Available on link: https://www.state.gov/secretary-antony-j-blinken-secretary-of-defense-lloyd-austin-japanese-foreign-minister-toshimitsu-motegi-and-japanese-defense-minister-nobuo-kishi-at-a-joint-press-availability
2- China’s New 2019 Defense White Paper.
3- Cybersecurity Law of the People’s Republic of China June 1, 2017, Translate by Rogier Creemers, Paul Triolo and Graham Webste, June 29 2018,
4- ECONOMIC AND SOCIAL COMMISSION FOR WESTERN ASIA (ESCWA), United nations, Policy Recommendations on Cybersafety and Combating Cybercrime in the Arab Region 14 April 2015.
5- European Treaty Series –N0.185, Convention on Cybercrime, Budapest, 23.XI.2001 .
6- REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of, 17 April 2019 .
7- Economic and Trade Agreement signed on January 15, 2020, between the Governments of the United States of America and the People's Republic of China.

8- President Donald J Trump, National Cyber Strategy To the United States of America, September 2018.
9- President Joe Biden delivers a speech on foreign policy at the State Department, in Washington, Feb. 4, 2021, World Politics Review, U.S. Foreign Policy Under Biden,, Available at the link: https://www.worldpoliticsreview.com/insights/29534/with-biden-s-foreign-policy-us-seeks-to-reclaim-its-global-standing. The date is March
10- President Joseph R. Biden, Jr. Interim National Security Strategic Guidance, The White House, Washington, March 2021.
11- Summary of President Biden's estimated funding request for fiscal year (FY) 2022.
12- The United States. White House Office, National Security Strategy, May 2010.
13- U.S Commercial Space Launch Competitiveness Act, Congress.Gov, PUBLIC LAW 114–90—NOV. 25, 2015 ‘‘CHAPTER 513—SPACE RESOURCE COMMERCIAL EXPLORATION AND UTILIZATION.
14- U.S. Department of State BUREAU OF EAST ASIAN AND PACIFIC AFFAIRS U.S. Relations With China, AUGUST 22, 2018.Available at Link: https://www.state.gov/countries-areas/china/.
15- White House Direct Publication, Joseph R. Biden Jr. officially announces acceptance of the Pars Accord, concluded on December 12, 2015,January 20,2021.
16- World Bank Global Economic Prospects 2018.Available at link: 10 https://www.worldbank.org/en/news/press-release/2018/06/05/global-economy-to-expand-by-3-1-percent-in-2018-slower-growth-seen-ahead.
17- Xinhua News Agency, China's military strategy (May 2015), Information Office of the State Council of the People’s Republic of China .

Second: Encyclopedias, Dictionaries

1- Dictionary, Merriam-Webster, the definition of Internet.

Third: books

1- Amy Chang, Warring State: China’s Cybersecurity Strategy, Center for a New American Security, ,Washington, December 2014 .

2- Abraham L. Newman, “Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive,” International Organization 62.1 2008 .

3- Chowdhary K.R, "Fundamentals of Artificial Intelligence," First edition, Springer India, New Delhi, 2020 .

4- Henry Farrell, “Constructing the International Foundations of E-Commerce – The EU-US Safe Agreement,” International Organization 57.2 2003.

6- Joseph S. Nye, Jr., Cyber power , Belfer Center for Science and International Affairs, Harvard Kennedy School , Cambridge, May2010 .

7 - Kai-Fu Lee , AI superpowers : China, Silicon Valley, and the new world order, Boston : Houghton Mifflin Harcourt, New York, 2018 .

8- Kenneth Gears , Cyberspace and the Changing Nature of Warfare, U.S. Representative Cooperative Cyber Defense Centre of Excellence Tallinn, Estonia ,2008 .

9- Lawrence Lessig, Code and Other Laws of Cyberspace, New York: Basic Book 1999.

10 - Martin C. Libicki , Cyberdeterrence and Cyberwar ,Santa Monica , Rand , 2009 .

11- Winston Ma, The Digital War: How China's Tech Power Shapes the Future of AI, Blockchain and Cyberspace, Wiley Publishing Corporation, New York, January , 2021.

Forth: periodicals

1- A group of international experts, (The NATO Cooperative Cyber Defence Center of Excellence), Tallinn's Handbook on International Law Applicable to Cyber Wars, Michael N. Schmitt, Cambridge University Press, March 2013.
2- Allen L. Hammond, “Digitally Empowered Development,” Journal Foreign Affairs,Volume 80,issue 2, Council on Foreign Affairs, March-April 2001.
3- Amy Chang, Warring State: China’s Cybersecurity Strategy, Center for a New American Security,,Washington, December 2014.

4- Annual Report to Congress Military Power of the People's Republic of China, Washington, 2008.
5- Anthony H. Cordesman, China's New 2019 Defense White Paper: An Open Strategic Challenge to the United States Center for Strategic International Studies (CSIS), July 24 2019.
6- Center of Strategic and International Studies, Significant Cyber Incidents Since 2006, Washington.
7- Colonel Jayson M. Spade, Chinas Cyber Power and Americas National Security, Jeffrey L. Caton Editor, U.S Army War College, May 2012.
8- Committee on National Security Systems (CNSS) Glossary, CNSSI No. 4009 April 6, 2015.
9- Cybersecurity and Infrastructure Security Agency's(CISA) DEFEND TODAY, CYBER STORM 2020: NATIONAL CYBER EXERCISE, JULY 2020.
10- Daniel T.Kuehl, "From Cyber Space to Cyber power: Defining the problems "in Franklin D. Krammer,Stuart, and Larry K.Wentz. eds, cyber power and national security (Washington, D.C: National defense up,2009
11- Daniel W. Drezner, The Global Governance of the Internet: Bringing the State Back In, Political Science Quarterly, Vol. 119, No. 3, The Academy of Political Science (Fall, 2004),pp,479-481.
12- David E. Graham."Cyber Threats and the Law of War "JOURNAL OF NATIONAL SECURITY LAW,POLICY, Vol, 4:87, 13 Aug 2010.
13- Emilio Iasiello,China's Cyber Initiatives Counter International Pressure,Journal of Strategic Security, Volume 10,issue1,January 2016.
14- Ensar Seker, Is the Future of Cyber Security in the Hands of Artificial Intelligence (A3)?, Center for a New American Security (CNAS), Washington, Jun 10, 2020.
15- Erkko Autio (university College London),Laszlo (University of Pécs), Telefonica Index Report, Digital Life, June 2016.
16- Fatema Mernissi, "Digital Scheherazades in the Arab World," journal Current History University of California Press,,Volume 105, issue689, March 2006.
17- Giovanna Cinelli, Kristen Cordell, Wendy Cutler, and others,, Course Economics in National Security Tools of Coercion and Inducement, Center for Strategic & International Studies, (csis) executive education, Washington, May 17, 2021.

18- Henry A. Kissinger, The Future of U.S.-Chinese Relations Conflict Is Choice, Not a Necessity, journal Foreign Affairs, Vol.91, No. 2 March 2012.
19- Jason Healey, The Five Futures of Cyber Conflict and Cooperation, The Georgetown Journal of International Affairs, Georgetown University Press, Washington,2011.
20- Jeremy Hsu, Don't Panic about Rare Earth Elements, Scientific American, a division of Springer Nature America, INC.,May 31,2019.
21- John Arquilla, David F Ronfeldt, The emergence of Noopoli-tik Toward of Americam Strateay, Rand Monograph Report Rand, Sanga Monica,California, 1999.
22- Ken Watanabe, Diane Rinaldo, Jonathan E. Hillman, Global Networks 2030 Developing Economies and Emerging Technologies, A webinar organized by the Center for Strategic International Studies, Washington, March 29, 2021.
23- KENDALL SCHERR, Cybersecurity Strategy2018, Department of Homeland Security (DHS), homeland security Digital Library · PUBLISHED MAY 15 2018 ·
24- Lewis, J. A. Cybersecurity and Critical Infrastructure Protection. Washington,(CSIS) Center for Strategic and International Studies, January 2006.
25- Lora Saalman, Balancing Chinese Interests in North Korea and Iran, Carnegie Endowment for International Peace, APRIL 01, 2013.
26- Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." Journal of Strategic Security, Volume 4, No. 2, Washington, Summer 2011.
27- Michael Krepon, Space and Nuclear Deterrence, In: Michael Krepon & Julia Thompson (Eds.), Anti-Satellite Weapons, Deterrence and Sino-American Space Relations, United States: Stimson Center, September 2013.
28- Michael S. Chase, Arthur Chan, China's Evolving Approach to "Integrated Strategic Deterrence, RAND Corporation, 2016.
29- Miles Kahler, the rise of emerging Asia: regional peace and global security, by the Peterson Institute for International Economics and the Asian Development Bank Institute, working paper series, May 2013.

30- Nan Tian and FEI US, ESTIMATING THE ARMS SALES OF CHINESE COMPANIES Stockholm International Peace Research Institute (SIPIR), January 2020
31- Nan Tian, Alexandra Kuimova, Diego Lopes da silva, and others, Trends In World Military Expenditure 2019, Stockholm International Peace Research Institute (SIPRI), April 2020
32- Nan Tian, Alexandra Kuimova, Diego lopes da silva, and others, Trends In World Military Expenditure 2019, Stockholm International Peace Research Institute (SIPRI), April 2020.
33- Nina Hachigian, "China's Cyber-Strategy,", Journal Foreign Affairs, Volume 80,issue 2, Washington Quarterly, March-April 2001.
34- Nina Hachigian, "The Internet and Power in One-Party East Asian States," Washington Quarterly,Center for International Strategic Studies,Volume 25,issue 3, summer 2002.
35- Olubukola S. Adesina, Foreign policy in an era of digital diplomacy, The Cogent Social Sciences Journals,1 March 2017.
36- Peter Dombrowski, AMERICA'S THIRD OFFSET STRATEGY NEW MILITARY TECHNOLOGIES AND IMPLICATIONS FOR THE ASIA PACIFIC, S. Rajaratnam School of International Studies (RSIS), June 2015.
37- Robert L. Gallucci is Dean of the Edmund A. Walsh School of Foreign Service at Georgetown University, North Korea, Iran, and the Proliferation of Nuclear Weapons: The Threat, U.S. Policy, and the Prescription... and the India Deal,2006.
38- Robert Reardon and Nazli Choucri1, The Role of Cyberspace in International Relations:, Paper Prepared for the 2012 ISA Annual Convention San Diego, CA April 1, 2012.
39- Ronnie D. Lipschutz, "Reconstructing World Politics – the Emergence of Global Civil Society," Journal of International Studies, Washington,Volume:21, issue 3, December 1, 1992.
40- Sean Carlin, Kevin Curran, University of Ulster, UK, Cloud Computing Security, International Journal of Ambient Computing and Intelligence, 3(1), 14-19, January-March 2011.
41- Sangbae Kim, US-China Competition in Cyberspace A Perspective of Emerging Power Politics and Platform Competition, The East Asia Institute (EAI), January 2019.

42- Todd Harrison, What to Look for in the FY 2022 Defense Budget Request, Center for Strategic International Studies (CSIS), Washington, April 29 2021.
43- Torkunov A. Strategy of the Trump Administration on Asia-Pacific, Mirovaya ekonomika i mezhdunarodnye otnosheniya, 2019, vol. 63, No 6,p 29,32.
44- Toshi Yoshihara, CHINESE INFORMATION WARFARE: A Phantom Menace Or Emerging ONDAN Threat?, The Strategic Studies Institute (SSI) is part of the U. S. Army War College, Washington,2001.
45- United States. White House Office, National Security Strategy,May-2010.

Fifth: Lectures and seminars:

1- David M. Lampton And others, Chinese Infrastructure Development in Southeast Asia, The lecture was given by the Stimson Center, November 16, 2020.
2- Digital Diplomacy Series: Foreign Policy and Digital Engagement - Embassy of Italy, the Embassy of Italy in Washington DC and Young Professionals in Foreign Policy, (YPFP) hosts the panel discussion: FOREIGN POLICY AND THE FUTURE OF ENGAGEMENT, May 29, 2014. Discussion seminar.
3- I. Kotenko, "Multi-agent Modelling and Simulation of Cyber-Attacks and Cyber-Defense for Homeland Security", IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 2007.

Sixthly: Channels:

1- Edward Snowden: Leaks that exposed US spy programme, BBC NEWS, 17 January 2014.

Seventh: Internet Sources.

1- Alexander Smith, China Offers First Glimpse of Chengdu J-20 Stealth Fighter, NBC News Digital, Nov. 1, 2016. Available at: 7https://www.nbcnews.com/news/china/china-offers-first-glimpse-chengdu-j-20-stealth-fighter-n676156.. Date visit. April 24-2021.

2- Andrew J. Nathan, professor of Chinese politics at Columbia University, U.S.-China Relations Since 1949, New York: W.W. Norton, 1997, p 1. Available at link: http://afe.easia.columbia.edu/special/china_1950_us_china.htm.Date visit 15 March 2021
3- Andrew Wagner, One-on-one with former Deputy Secretary of Defense Robert Work,Government Matters, June 23, 2019 Available at Link: https://govmatters.tv/one-on-one-with-former-deputy-secretary-of-defense-robert-work.Date vest 15-3-2021. the date visit 3 April 2021/.
4- Ankit Panda, Introducing the DF-17: China's Newly Tested Ballistic Missile Armed With a Hypersonic Glide Vehicle, The Journal December, December 28, 2017. Available at the link: https://thediplomat.com/2017/12/introducing-the-df-17-chinas-newly-tested-ballistic-missile-armed-with-a-hypersonic-glide-vehicle/. the visit at April 24 2021.
5- BBC News, China sanctions 11 U.S. officials on Hong Kong issue, the parties dismissed it, August 11, 2020.
6- Carla A. Hills, The Impact of the Coronavirus on US-China Relations, China US Focus, Apr 10,2020. Available at link: https://www.statista.com/statistics/278206/foreign-exchange-reserves-of-china/. The date of visit is 13 March 2021.
7- Center for Strategic International Studies, China's Power, How Developed Is China's Arms Industry?, p 12. Available at the link: https://chinapower.csis.org/arms-companies/ the Date visit April 15 2021.
8- China's Great Firewall, Washington Post, November 6, 2018.Available at the link: https://bit.ly/2maTv2c. Date visit at 1 April.
9- Craig Timberg، Elizabeth Duskin, Twitter is sweeping out fake accounts like never before, putting user growth at risk, The Washington Post, July 7 2018. Available at Link:The date of the visit is March 29, 2021. https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/

10- DAVID E.SANGER,Chinse Army Unit Is Seen as Tied to Hacking Against U.S, newspaper The New York t Times, February 18, 2013, Accessed on July 10th,2014,on Available at Link: https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html The date at 19 March 2021.

11- de Rosnay Joel L Homme Symbiotique, Reqard sur la troisieme millenaire, paris, LeSeuil,15 March 1995..Available: https://www.seuil.com/ouvrage/l-homme-symbiotique-regards-sur-le-troisieme-millenaire-joel-de-rosnay/9782020217149 the date visit 15 February.

12- Dinstein, Computer, Network Attacks and Self-Defence, 2002, page 108.Available at Link: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1397&context=ils.the visit at 9 January.

13- Donald J. Trump (@realDonaldTrump) May 13, 2019. 9

14- EditorChen Zhuo, Source China Military Onlin, Chinese defense ministry denounces $280 million US arms sales to Taiwan,9-12-2020. Available at the link: http://eng.chinamil.com.cn/view/2020-12/09/content_9949608.htm تأريخ الزيارة ٤شباط ٢٠٢١

15- Eric Baculinao, Chinese military innovations threaten American supremacy,NBC News Digital, Feb 17 2018., Available at: the Date visi. April 21-2021. https://www.nbcnews.com/news/world/these-chinese-military-innovations-threaten-u-s-superiority-experts-say-n848596#anchor-2Hightechwarships.

16- Evan A. Feigenbaum, Meeting the Challenge in Asia, journal National Interest Newsletter, December 22, 2020, P 1-5.Available at:Date visit at 26February https://nationalinterest.org/feature/meeting-challenge-asia-174917.

17- Graham Allison, China Is Now the World's Largest Economy. We Shouldn't Be Shocked, Harvard Kennedy School, Belfer Center for science International Affairs, Cambridge, October 15, 2020,Available at the link:

https://nationalinterest.org/feature/china-now-world%E2%80%99s-largest-economy-we-shouldn%E2%80%99t-be-shocked-170719t.Date the visit February 6 2021.

18- Illya Golovatenko, The Three Dimensions of the Cybersecurity Cube, Dec 13,2018 Available at Link: https://swansoftwaresolutions.com/the-three-dimensions-of-the-cybersecurity-cube/# cerber-recaptcha-msg Date of visit,29-March 2021.

19- Jacob Parker, Cybersecurity is a key issue of our time, Techrader Newsletter, May 19, 2020, P,3. Available at Link: https://global.techradar.com/en-za/news/what-is-the-future-of-cybersecurity the date visit 4 April 2021.

20- JIM GARAMONE, Department of Defense.GOV, DIA Report Details Threats to America's Space-Based World, FEB. 11, 2019. Available at Link: https://www.defense.gov/Explore/News/Article/Article/1754509 Date visit 18 March2021.

21- Lawrence Lessig, The Internet Under Siege, Foreign Policy 127, 2001 Available at Link: https://foreignpolicy.com/2009/11/16/the-internet-under-siege.the date at January 2021. the date visit 20 January 2021.

22- Li Jiayao,US blasted for military gear sales to Taiwan, China Daily,9-12-2020. Available at link: http://eng.chinamil.com.cn/view/2020-12/09/content_9949984.ht

23- Lucia Mutikani Reporting, The U.S. trade deficit surged to a 10-year high in 2018, Fox Business, March 6, 2019. Available at Link: https://www.foxbusiness.com/economy/us-trade-deficit-jumps-to-10-year-high-in- 2018.

24- Matthew Bey, The Age of Splinternet: The Inevitable Fracturing of the Internet, Stratfor, 25 April, 2019. Available at Link: date of the visit April 1, 2021. https://worldview.stratfor.com/article/age-splinternet-inevitable-fracturing-internet-data-privacy-tech

25- Michael Martina, China aims for manned moon landing year 2036,Reuters, April 29, 2016.Available at Link: the Date visit on March 30- 2021. https://www.reuters.com/article/us-china-space-moon-idUSKCN0XQ0JT

26- Namrata Goswami, Star Wars From Space-Based Solar Power to Mining Asteroids for Resources: China's Plans for the Final Frontier, Policy Forum, September 7, 2016,pp1-2. Available at Link: https://www.policyforum.net/star-wars. the Date visit at March 30,2021

27- Official website of the United States' Cyber Command. https://www.cybercom.mil

17- Official website of the World Health Organization. Available at Link: https://covid19.who.int.

28- Paul Rosenzweig,China's National Cybersecurity Strategy, December 27, 2016.Available at Link: https://www.lawfareblog.com/chinas-national-cybersecurity-strategy The date visit at 20 March 2021.

29- Reporting by Ben Blanchard, Taiwan the most important issue in Sino-U.S. ties, China's Xi tells Trump, Reuters, NOVEMBER 9, 2017.Available at Link: https://www.reuters.com/article/us-trump-asia-china-taiwan/taiwan-the-most-important-issue-in-sino-u-s-ties-chinas-xi-tells-trump-idUKKBN1D90YI.

30- Richard Forno, Hackers Target 3rd Dimension of Cyberspace: Users' Minds,18 October 2018. Available at Link: https://www.livescience.com/63214-hackers-target-your-mind.html. Date visit at 25 March 2021.

31- RISKS IN CYBERSPACE, 2011, Available at Link: https://www.localweb.com/risks-in-cyberspace.The date visit at 26 February 2021.

32- Robert Martinage, Toward a New Offset Strategy Exploting U.S. Long-Term Advantages To Restore U.S. Global Power Projection Capability (Center for Strategic and Budgetary Analysis 2014), p. 32. Available at Link: file:///C:/Users/pdombrow/Downloads/Offset-StrategyWeb%20(2).pdf. The date visit at 1 April 2021.

33- Ronen Bergman, Mysterious Hacker Group Suspected in July Cyberattack on Iranian Trains ,The New York Times, Aug 14 2021. https://www.nytimes.com/2021/08/14/world/middleeast/iran-trains-cyberattack.html

34- Peter Baker and Michael R .Gordon, Trump Chooses H.R. McMaster as National Security Adviser, The New York Times, Feb. 20, 2017,- Available at the lin: https://www.nytimes.com/2017/02/20/us/politics/mcmaster-national-security-adviser-trump.html

35- The Economic Times News, China overtakes US as EU's biggest trading partner, Feb 15, 2021. Available at the

link: https://economictimes.indiatimes.com/news/international/business/china-overtakes-us-as-eus-biggest-trading-partner/articleshow/80926110.cms?from=mdr. date of the visit March 13, 2021.

36- The Stimson Center, a Chinese foreign policy project, October 28, 2020. Available at Link: https://www.stimson.org/project/chinese-foreign-policy Date visit at 22March 2021..

37- Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, September 14, 2018 Available at Link: https://bit.ly/2oghNq3. the date visit at 29 March 2021.

38- US Department of State, OFFICE OF THE SPOKESPERSON, U.S China Joint Statement Addressing the Climate Crisis, April 17, 2021.Available at link:

https://www.state.gov/u-s-china-joint-statement-addressing-the- climate-crisis . The date visit 5 July 2021, 01:20 .

39- Wu Qian: China's defense budget growth in 2021 is stable and moderate, Xinhua News Agency,8/3/2021. Available at the link http://www.gov.cn/xinwen/2021-03/08/content_5591373.htm the date visit: 4 May

40- Yuan Yang,The Great Firewall of China web of control.Financial Times, March12,2019.Available at Link: the date visit at 2 April 2021. https://www.ft.com/conent/e19b3022- 40eb-11e9-9bee-efab61506f44

41- Digital 2021July Global Statshhot,6 November,Available at Link: http://datareportal.com/reports/digital-july-global-statshot.

42- Zhang Tao,Strive to build a strong, modern strategic support force: Xi, China Military Xinhua Aguste 29 2016. Last accessed. Available at Link: http://eng.chinamil.com.cn/view/2016-08/29/content_7231309.htm. the visit at March 20, 2021.

الملاحق

رقم الملحق	عنوان الملحق
١	نص الرسالة من السيد جيمس اندرسن نائب مدير معهد CSIS
٢	نص رسالة مؤسسة كارنيغي للسلام الدولي في ٧نيسان
٣	نص الرسالة التي تم حذفها من قبل السفارة الصين في واشنطن
٤	نص رسالة الخارجية الأمريكية بالموافقة على اشتراك الباحث لتلقي نشاطات شؤون شرق آسيا والمحيط الهادئ
٥	نص رسالة مؤسسة كارنيغي للسلام الدولي حول الثغرات الإلكترونية
٦	تقرير معهد أستوكهولم للسلام حول الأنفاق العسكري العالمي لعام ٢٠٢٠
٧	موافقة الرئيس الأمريكي جوزيف بايدن على أتفاقية باريس
٨	دليل الأمن القومي الاستراتيجي المؤقت ٢٠٢١
٩	الاتفاقية الاقتصادية التجارية بين حكومة الولايات المتحدة والصين ٢٠٢٠

Abstract

The cyber factor has had mixed effects on the level of international relations and the international system, and perhaps one of its most important effects is reflected today in the fierce cyber competition between the United States of America and China. China’s new relations and the strengths that it has become in many areas, especially cyberspace, means that it has a position New responsibilities in the world, in which the United States competes as a leader of the global system, as cyber conflict can become an important and perhaps decisive factor in the process of redefining the bilateral relationship between the two great powers, and may even lead to an exacerbation of economic and military competition, to the extent of conflict between them in the future.

The tremendous development that the world has brought into the global information infrastructure during the past two decades has made cyberspace a new and important arena for international competition and conflict. Accordingly, cybersecurity has become a priority in the security strategies of the great and major international powers that compete for the lead, under an international system. A new multipolar is emerging, but its outline or final form is not yet clear. In fact, the conflict between the United States and China is not new, but it has taken new forms and means imposed by the technical and technological development that the world is witnessing. It seems that the most influential elements in Chinese thinking today, is the desire to develop unconventional military capabilities on par with the United States, and to restore China's deserved place in the world after the "century of humiliation." These factors, combined with a clear feeling of China’s rise as a rival force for American hegemony, made the United States view China as the most dangerous competitor to its global position. Conflict and confrontation in cyberspace? What is the impact of this on international peace and security? The study found that this relationship tends to conflict and confrontation rather than cooperation and integration, between the two forces that are at the fore in the international scene.

The study was divided into three chapters, the first describing cyberspace and cybersecurity as a concept, and the second: the cyber dimension in US-Chinese relations, and the third chapter dealing with anticipating the future of US-Chinese cyber competition in outer space.

Ministry of Higher Education and Scientific Research

AL-Anbar University

College of Law and Political Sciences

The informationa competitics between the United States of America and China

(A study in cybersecurity)

Master Thesis submitted by submitted by

Mohammed j. Alaallah Al-Janabi

To the Council of the College of Low and Political Science As partial fulfillment for Master Degree in International studies

Under the Supervision of

Assistant Professor

Rasoul Hussain Ali

1443A.H. *2021A.D.*