



الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة الوادي



كلية الحقوق والعلوم السياسية

مخبر السياسات العامة وتحسين الخدمة العمومية في الجزائر

أطروحة دكتوراه

مقدمة لاستكمال متطلبات نيل شهادة الدكتوراه في الطور الثالث (LMD)

الشعبة: العلوم السياسية

التخصص: استراتيجية وعلاقات دولية

صراع الهيمنة بين الولايات المتحدة الأمريكية والصين في الفضاء السيبراني - دراسة جيوبوليتيكية في الاستراتيجيات والمآلات -

إعداد الطالب: سليم دحماني

نوقشت بتاريخ [2024/12/26] أمام لجنة المناقشة:

الاسم واللقب	الرتبة	الجامعة	الصفة
المكي الدراجي	أستاذ	جامعة الوادي	رئيساً
الصادق جرایة	أستاذ	جامعة الوادي	مشرفاً
الهادي دوش	أستاذ	جامعة الوادي	مناقشاً
خالد بقاص	أستاذ	جامعة الوادي	مناقشاً
فوزي نور الدين	أستاذ	جامعة بسكرة	مناقشاً
فريدة طاجين	أستاذ	جامعة ورقلة	مناقشاً

السنة الجامعية: 2024-2025 م / 1446-1447 هـ

الإهداء

إلى أمي ... رحمها الله

إلى والدي

إلى زوجتي

إلى إسراء، أسماء وأسيل

أهدي هذا العمل

شكر

خالص الشكر والتقدير للأستاذ المشرف: البروفيسور **الصادق جرایة** الذي لم ييخل
علينا بالدعم والنصح والتوجيه.

والشكر موصول لأساتذة كلية الحقوق والعلوم السياسية بجامعة الوادي على دعمهم
ومرافقتهم.

وجميل العرفان لكافة أساتذة وإطارات وموظفي جامعة الوادي على مساعدتهم
وخدماتهم.

وأتّم العرفان لمدينة الوادي، لأرضها المباركة وشعبها الطيب وأخص بالذكر صديقي
"العبيدي محمد الأزهر".

شكراً جزيلاً لكل من ساهم في إتمام هذا العمل

مقدمة

تطور الفضاء السيبراني مع بداية الألفية الثالثة ليُصبح مجالاً استراتيجياً في العلاقات الدولية، حيث عزز التشبيك المكثف نقل الكثير من الأنشطة البشرية إلى الفضاء السيبراني، وأحدث ثورة في نمط حياة الأفراد والمجتمعات، ونقل وسائل التواصل إلى مستوى غير معهود، كما فتح آفاقاً للتنمية الاقتصادية بالكاد، بدأ العالم يستكشف ماهيتها. لقد قدم النمو الهائل للفضاء السيبراني بتخطيه حاجزي الزمان والمكان وُعوداً بالسلام والرفاهية للعالم، لكنه في نفس الوقت خلق تحديات كبرى للدول والجيش، فالتهديدات التي رافقت نمو الفضاء السيبراني نتيجة التفاعلات السياسية والصراعات والعنف فرضت على الدول رفع القضايا المتعلقة به إلى مستوى "السياسة العليا"، كما أن التفاعلات العالمية التي يوفرها الفضاء السيبراني غيرت من مفاهيم الحدود، النفوذ والتأثير، سياسات القوة والعلاقات الدولية وغيرها من المفاهيم التقليدية. ذلك أن الفضاء السيبراني بميزاته الفريدة يعمل على تحويل السياسة العالمية، ويمنح الفرصة للدول التي تحتل موقعاً في طليعة التكنولوجيا الرقمية لزيادة قوتها ونفوذها، وإلا فهي تخاطر بفقد الكثير من قوتها ومكانتها.

في نفس السياق، قادت الولايات المتحدة الأمريكية تطور الفضاء السيبراني منذ البداية، وكانت الصين من المتأخرين نسبياً في هذا المجال، لكنها لم تدخر جهداً للالتحاق بالركب، وهذا كان نتيجة لاستراتيجية صينية واعية، حيث بذلت القيادة الصينية جهوداً كبيرة للانتقال من مرحلة التقليد ونسخ التكنولوجيا إلى مرحلة ابتكارها كانعكاس لمسيرة طويلة بدأت في تسعينيات القرن المنصرم، كان محركها التحول الدراماتيكي نحو اقتصاد السوق. كما كان لدروس الحرب الباردة والحرب الأمريكية على العراق بالغ الأثر في إدراك القيادة الصينية أن الفضاء السيبراني فرصة تاريخية لبناء قوة البلاد وتحقيق التنمية وفق النموذج الصيني والتجديد العظيم للأمة الصينية، كذلك استغلت الصين جاذبيتها للاستثمارات في إلزام المستثمرين بنقل التكنولوجيا إلى داخل الصين وهذا ما ظهرت نتائجه من خلال بروز شركات التكنولوجيا الصينية العملاقة التي تنافس الشركات التكنولوجية الأمريكية مهد الفضاء السيبراني وتتفوق عليها في بعض المجالات، هذا الصعود التقني الصيني كان سبباً مباشراً في ظهور مخاوف وقلق متزايد على الجانب الأمريكي من أن الصين تسعى للهيمنة على الفضاء السيبراني وإزاحة الولايات المتحدة عن قيادتها العالمية، يؤكد ذلك دعوات الرئيس الصيني "شي جين بينغ" في العديد من المناسبات بأن "الابتكار التكنولوجي

أصبح ساحة المعركة الرئيسية في الساحة العالمية، وسوف تزداد المنافسة ضراوة على الهيمنة التكنولوجية بصورة غير مسبقة"، وعليه، فالصين عازمة على عدم التخلف عن الركب في الفضاء السيبراني.

في المقابل، تُظهر الولايات المتحدة عزمًا -لا يقل عن نظيره عند الصين- على الاحتفاظ بتفوقها وريادتها في الفضاء السيبراني والاستفادة منه في المجالات الحيوية (سياسياً، أمنياً، اقتصادياً وصناعياً). هذه الرغبة في الحفاظ على الهيمنة جاءت على خلفية فشل الولايات المتحدة في جذب الصين للانخراط في النظام الدولي الليبرالي تحت قيادتها من خلال سياسات الشراكة والتعاون خلال الأربعين سنة الماضية، بل على العكس مما هو متوقع، امتلك النظام الصيني الشيوعي قدرات هائلة حوله إلى قوة تعديلية تعارض علناً قيادة الولايات المتحدة للعالم، كما أن إدراك صانع القرار في الولايات المتحدة بأن الفضاء السيبراني (التكنولوجيا) هو المحدد الرئيس للرفاهية والقوة الوطنية الأمريكية زاد من إيمان واشنطن أن الصين هي أهم تهديد جيوبوليتيكي تواجهه الولايات المتحدة في القرن الواحد والعشرين، وأن الساحة المركزية للمنافسة الاستراتيجية ستكون التكنولوجيات المتقدمة.

على صعيد آخر، الجيوبوليتيكا رغم استبعادها الأكاديمي لعقود من الزمن فإنها كممارسة لم تغب أبداً عن المشهد العالمي، حيث تستمر الصراعات السياسية والاستراتيجية والمحللون والإعلام في إحيائها وتأكيد حصافة التفسيرات والرؤى التي يقدمها منهج التحليل الجيوبوليتيكي. كما أن مرونتها كنظام علمي مفتوح وسع آفاقها البحثية لتشمل الظاهرة الصراعية في فضاءات تخيلية مثل الفضاء السيبراني.

وبناءً على ما تقدم، تقع هذه الدراسة ضمن مجال الدراسات الجيوبوليتيكية والاستراتيجية، حيث تسعى للاستفادة من منهج التحليل الجيوبوليتيكي كنظام علمي مفتوح للتحقق من ملاءمته لفك شفرة الصراع الأمريكي الصيني المحتدم منذ بداية القرن الحالي في/على الفضاء السيبراني، من خلال تحليل العوامل الجيوبوليتيكية التي تتحكم في تطوير واشنطن لاستراتيجيات في الفضاء السيبراني ترمي لكبح وتقييد طموحات الصين العالمية، واستراتيجيات بकिन للصمود وتحدي الهيمنة الأمريكية، مع تقديم رؤى وسيناريوهات مستقبلية لما سيؤول إليه هذا الصراع.

1. أسباب اختيار الموضوع:

إن لكل موضوع أسباباً تدفع الباحث لدراسته، وجاء موضوع "صراع الهيمنة بين الولايات المتحدة الأمريكية والصين في الفضاء السيبراني: دراسة جيوبوليتيكية في الاستراتيجيات والمآلات" كحلقة كبرى تضاف إلى ما بدأه الباحث في طور الماجستير من دراسات حول التهديدات في الفضاء السيبراني، كما أن الملاحظة الفاحصة لانحسار بعض شركات التكنولوجيا الصينية واختفائها عن المشهد التكنولوجي العالمي تُثير في نفس الباحث عاصفة من الأسئلة التي تحتاج إلى إجابة.

أولاً، الدوافع الذاتية.

- الباحث مهندس كمبيوتر له شغف كبير لمتابعة المستجدات في الفضاء السيبراني (تقنية كانت أو سياسية).
- ميول ذاتية للدراسات الجيوبوليتيكية التي تقدم فهماً للحاضر واستشرافاً مميّزاً للمستقبل والذي يعين الباحث للتأقلم مع التقنيات المستقبلية (هل سيكون عالم الغد الرقمي صينياً أو أمريكياً أو مجزأً).
- رغبة الباحث في تنوير وتثقيف القارئ العادي، والباحث، وصانع القرار حول خطورة الصراع الذي يحدث في الفضاء السيبراني.
- رغبة الباحث في تقديم مساهمة أكاديمية علمية باللغة العربية في موضوع قد يكون المحرك الرئيس لتحولات جذرية في النظام الدولي.

ثانياً، الدوافع الموضوعية.

- كون الموضوع جديداً، وشحّ الدراسات باللغة العربية، وأن ما كُتب بهذه اللغة في معظمه ترجمات لدراسات أجنبية على ما بين هذه الدراسات من التفاوت في جديتها وقيمتها وذيوها وتأثيرها، وتوزع متغيرات الدراسة بين العديد من الدراسات الأجنبية، فضلاً عن احتدام الصراع بين الولايات المتحدة والصين الذي يشهد تحولات وتغييرات سريعة وعميقة، كل ذلك جعل الموضوع محل اهتمام الباحث.
- عودة الجيوبوليتيكا للمجتمع الأكاديمي والاستعمال المكثف لمفرداتها (الهيمنة، الحرب الباردة، الصراع، الاحتواء ...) لدى النخب السياسية والأكاديمية.

- تقهقر شركة هواوي مفخرة التكنولوجيا الرقمية الصينية في مجال الهواتف الذكية بعد أن كانت رائدة بسبب العقوبات الأمريكية، يدفعنا للتساؤل والبحث عن الأسباب الموضوعية والتي لا يمكن أن تكون مجرد إخفاقات تجارية أو اقتصادية.

2. أهمية الدراسة:

تبرز أهمية الدراسة من الجوانب العلمية (النظرية) والعملية (التطبيقية) التي تتناولها كما سيأتي:

أولاً، الأهمية العلمية.

تأتي أهمية الدراسة في الجانب العلمي من خلال تطرقها لمجموعة من النقاشات الأكاديمية المحتمدة حول الجيوبوليتيكا، والتساؤلات حول قدرتها التفسيرية للظواهر في المجالات الافتراضية والتخيلية غير المرتبطة بـ"الأرض"، لذلك جاءت هذه الدراسة للتأكيد على عودة الجيوبوليتيكا لتصبح مركز اهتمام الباحثين والسياسيين. كما أنها أثبتت أنها مقارنة لا غنى عنها في دراسة مواضيع الصراع، حيث تُبرز الدراسة ملائمة منهج التحليل الجيوبوليتيكي لدراسة ظواهر الفضاء السيبراني حتى وإن كان يُصنف على أنه فضاء افتراضي أو متخيل.

كذلك، تقدم الدراسة فهماً عميقاً بخلفية جيوبوليتيكية للكيفية التي تُبنى بها استراتيجيات القوى العظمى في الفضاء السيبراني، وتستفيد من الاستبصارات التي تقدمها الجيوبوليتيكا لرسم السيناريوهات المستقبلية لصراع الهيمنة في الفضاء السيبراني.

ثانياً، الأهمية العملية.

تسعى الدراسة إلى فهم عملية بناء وتطوير الاستراتيجيات المتعلقة بالفضاء السيبراني وفق المبادئ الجيوبوليتيكية لكل من الولايات المتحدة الأمريكية والصين، ومن ثم فهم تأثير المبادئ الجيوبوليتيكية لكل دولة على تحديد الأهداف النهائية لاستراتيجياتها.

من جهة أخرى، تقدم الدراسة رؤية مستقبلية للصراع بين القوى العظمى في الفضاء السيبراني وهذا ما يساعد الدول، الشركات وحتى الأفراد في تطوير استراتيجياتهم الخاصة، تكييف أهدافهم وتقنياتهم المستقبلية على ضوء ما سيؤول إليه الصراع الراهن.

3. أهداف الدراسة:

رغم قلة المهتمين والباحثين في موضوع الصراع الأمريكي الصيني في الفضاء السيبراني -خاصة في عالمنا العربي- حيث يصنف الكثير منهم الصراع كصراع تقني-تجاري إلا أن هذه الدراسة تكشف أن الموضوع أوسع وأعمق وبحاجة إلى:

- استكشاف قوة المقاربات الجيوبولتيكية وقدرتها على فهم وتفسير واستشراف الظواهر في الفضاء السيبراني، ومنه إظهار الدور المركزي للعامل الجيوبولتيكي في بناء وتطوير الاستراتيجيات في الفضاء السيبراني.
- فهم أسباب وجذور ومظاهر الصراع بين الولايات المتحدة والصين في/على الفضاء السيبراني، وتحليل استراتيجيات كل طرف بالاعتماد على المنهج الجيوبولتيكي واستقراء الأهداف النهائية لكل منها.
- محاولة تقديم رؤية استشرافية وفق سيناريوهات تنبؤية لما سيؤول إليه الصراع التكنولوجي الأمريكي الصيني لتكون معيناً للتقنيين وصناع القرار في تطوير الاستراتيجيات المناسبة المتعلقة بالفضاء السيبراني.

4. الدراسات السابقة:

من خلال الاطلاع على الأدبيات التي عالجت مواضيع قريبة من موضوع الدراسة نجد أنها؛ إما محاولات لتطبيق المنهج الجيوبولتيكي في الفضاء السيبراني بشكل عام، أو عالجت المنافسة التكنولوجية بين الولايات المتحدة والصين وفق مقاربات ومداخل للصراع غير المنهج الجيوبولتيكي، أو أنها طبقت المنهج الجيوبولتيكي على تقنية واحدة أو جزء من الصراع الأمريكي الصيني في الفضاء السيبراني، لذلك، جاءت هذه الدراسة لتخصيص ما عمّ وجمع ما افترق وإكمال ما نُقص، ومن بين الدراسات المهمة نذكر:

- دراسة (مقال) صادرة في 2015 في مجلة "Hérodote" الشهيرة التي أسسها "إيف لاکوست" بعنوان "La Geopolitique pour comprendre le Cyberspace" للبروفيسور "Frédéric Douzet"، والتي ناقشت فيها إمكانيات المقاربات الجيوبولتيكية في معالجة قضايا الفضاء السيبراني مثل: الأمن، السيادة، الديمقراطية والحريات، كما لمحت إلى ضرورة تطوير النقاشات الجيوبولتيكية في الفضاء السيبراني جنباً إلى جنب مع النقاشات التقنية لأن ذلك يتعلق بمستقبل العالم الذي نعيش فيه.

- دراسة (مقال) صدرت في 2019 في مجلة "China Quarterly of International Strategic Studies" بعنوان "US.-China Tech War Impacts and Prospects" للباحث الصيني "Haiyong Sun" والتي حل فيها أسباب الحرب التكنولوجية التي تشنها إدارة "ترمب" على الصين وأثرها في تدهور العلاقات الثنائية بين البلدين، كما أكد على ضرورة بذل الطرفين المزيد من الجهود لإدارة المنافسة بينهما وتعزيز التعاون المفيد لكلا البلدين.
- دراستين لـ "غراهام أليسون" صادرتين عن "مركز بلوفر" بجامعة "هارفارد"، الأولى (كتاب) بعنوان "Destined for War: Can America and China Escape Thucydides's Trap?" صدر سنة 2017 وحل فيه الكاتب خطورة المنافسة بين الولايات المتحدة والصين والتي قد تؤدي إلى الحرب بسبب الشك وعدم اليقين المتبادل، والثانية (ورقة عمل) بالاشتراك مع باحثين آخرين صدرت سنة 2021 بعنوان "The Great Tech Rivalry: China vs the U.S" حول التقدم التكنولوجي الذي أحرزته كل من الولايات المتحدة والصين في العشرين سنة الأخيرة، كما عرض فيها المحركات الكبرى للمنافسة التكنولوجية بين البلدين.
- دراسة (مقال) لـ "آدم سيغال" صادر في مجلة "Foreign Affairs" سنة 2018 يحمل عنوان "عندما تحكم الصين الواب" قدم فيه رؤية استشرافية لطموحات الصين للهيمنة على الفضاء السيبراني وشرح خطط الصين للتفوق وكيف سيكون عليه الفضاء السيبراني في ظل الهيمنة الصينية وما يُمكن للولايات المتحدة أن تفعله في مواجهة الصعود الصيني.
- دراسة (تقرير) لمحللين من "مجموعة أوراسيا" حمل عنوان "جيوبوليتيكا أشباه النواقل" صدر سنة 2020 وقدم فيه الباحثون شرحاً لكيفية تأثير الجيوبوليتيكا في صناعة أشباه النواقل ووضعها الجيوبوليتيكي كنقطة اختناق في المنافسة التكنولوجية الأمريكية الصينية، كما يرى الباحثون أن مستقبل صناعة أشباه النواقل مرهون بالتوازنات المستقبلية للمثلث؛ الولايات المتحدة، الصين وتايوان، كما قدم التقرير مثلاً جيداً للتحليل الجيوبوليتيكي لتقنيات الفضاء السيبراني تم تطبيقه وتوسعته في دراستنا ليشمل مختلف التقنيات الأخرى.

5. إشكالية الدراسة:

نجحت الولايات المتحدة في منافسة خصم جيوبوليتيكي هو الاتحاد السوفياتي، ومنافس تكنولوجي حديث هي اليابان، لكن الصين اليوم تلعب هاذين الدورين ولديها قدرات هائلة اقتصادياً وتكنولوجياً كما تُطور بشكل لافت قدراتها العسكرية، ومن ناحية أخرى، يدرك صانع

القرار في كل من الولايات المتحدة والصين بأن الفضاء السيبراني أصبح المصدر الرئيس للقوة الجيوبوليتيكية والسيطرة عليه تعني التفوق اقتصادياً وعسكرياً، لذلك يسعى الطرفان إلى تطوير الاستراتيجيات الملائمة لضمان الفوز بالمستقبل.

وعليه، وبناءً على هذه المعطيات يتبلور السؤال البحثي المركزي التالي:

ما حدود تحكم العامل الجيوبوليتيكي في بناء ونجاح استراتيجيات كلٍّ من الولايات المتحدة الأمريكية والصين في صراعهما للهيمنة في/على الفضاء السيبراني؟

الأسئلة الفرعية:

1. مامدى ملائمة منهج التحليل الجيوبوليتيكي لتفسير ظاهرة الصراع في الفضاء السيبراني؟
2. ماهي مضامين وتجليات الصراع الأمريكي-الصيني في الفضاء السيبراني؟ وماهي تداعياته على العلاقات والتوازنات الدولية؟
3. كيف تؤثر العوامل الجيوبوليتيكية على بناء الاستراتيجيات المتعلقة بالفضاء السيبراني لكل من الولايات المتحدة والصين؟
4. ما مآلات الصراع في الفضاء السيبراني بين الولايات المتحدة والصين؟

6. الفرضيات:

1. تسمح المقاربات الجيوبوليتيكية المتعددة النطاقات والعابرة للمجالات البحثية من معالجة وتفسير قضايا الصراع في الفضاء السيبراني بكل تعقيداتها.
2. يتمظهر الصراع الأمريكي الصيني في سعي البلدين لتضخيم قدرتهما السيبرانية وتوظيفها للمنافسة في/على كل طبقة من طبقات الفضاء السيبراني.
3. ترسم المبادئ الجيوبوليتيكية لكل من الولايات الأمريكية والصين الأهداف النهائية لاستراتيجيات البلدين في الفضاء السيبراني.
4. تنتهي استراتيجيات الولايات المتحدة الأمريكية في الفضاء السيبراني عند هدف واحد؛ كبح الصعود الصيني ودمج الصين في نظام دولي جديد تهيمن عليه الولايات المتحدة.

5. تهدف الاستراتيجيات الصينية في الفضاء السيبراني للحاق تكنولوجياً بركب الدول المتقدمة، تجاوزها، الهيمنة على الفضاء السيبراني ومن ثم بسط النموذج الصيني عالمياً.

6. مستقبل الصراع الأمريكي الصيني في الفضاء السيبراني يرتبط بقدرة الطرفين أو أحدهما على تحقيق الاستدامة في الابتكار وتحقيق الاختراقات في تقنيات الفضاء السيبراني.

7. المناهج والأدوات البحثية للدراسة:

تعتمد الدراسة كما هو موضح في عنوانها منهج التحليل الجيوبوليتيكي كمنهج رئيس في تحليل ظاهرة الصراع الأمريكي الصيني في الفضاء السيبراني، وتحليل استراتيجيات الطرفين وفق المبادئ الجيوبوليتيكية لكل دولة، وقد خصص مطلب كامل من الفصل الأول للتطرق للمقاربة الجيوبوليتيكية ومستويات التحليل وأهم القضايا التي يمكن معالجتها، كما خصص المبحث الثالث من الفصل الأول لمناقشة مدى ملائمة منهج التحليل الجيوبوليتيكي لتفسير ظواهر الفضاء السيبراني وتخطي التحدي المنهجي حول اعتبار الفضاء السيبراني إقليمياً.

كما اعتمدت الدراسة تقنية السيناريوهات التي تعتبر من الأدوات المنهجية الأكثر استعمالاً في الدراسات الاستشرافية وتقدم وصفاً لوضع مستقبلي ممكن أو محتوم أو مرغوب فيه، مع توضيح المسارات التي تؤدي إلى هذا الوضع المستقبلي انطلاقاً من الوضع الراهن أو من وضع ابتدائي مفترض، وفي دراستنا خصصنا الفصل الأخير لتتبع المآلات المحتملة للصراع الأمريكي الصيني من خلال المتغيرات المتحركة في كل سيناريو من السيناريوهات الثلاثة المعتمدة.

8. صعوبات الدراسة:

صادفتنا صعوبة فيما تعلق بالمصادر والمراجع باللغة الصينية، فقلة المراجع المتوفرة على الأنترنت وصعوبة الوصول إلى بعضها بسبب تعقيدات الولوج إلى المكتبات الإلكترونية الصينية من الممكن أن يكون قد فوت علينا الاطلاع على بعض الأفكار والرؤى الصينية المهمة.

إضافة إلى أن الجمع بين حاجز اللغة والمصطلحات المبتكرة (في المجال السيبراني) التي ينتجها النظام والمفكرون في الصين تستهلك الكثير من الوقت والجهد لفهم المراد منها، وفي بعض الأحيان تختلف المصطلحات في الترجمة الإنجليزية -على قلتها- عن معانيها الأصلية باللغة الصينية، وهذه نقطة (أي اللغة) أثّرت في الصراع الأمريكي الصيني حيث تقتخر الولايات المتحدة بقوة جذب أكبر بكثير للمواهب في المجال التقني وأحد الأسباب هي اللغة.

9. التصميم الهيكلي للدراسة:

لمعالجة الإشكالية المطروحة والإلمام بالموضوع من مختلف الزوايا تبيننا خطة تكونت من أربعة فصول توالى كما يلي:

الفصل الأول: ورد بعنوان "جيوبوليتكا الفضاء السيبراني" ويُعنى بالتأصيل النظري والمفاهيمي للجيوبوليتكا كعلم ومنهج تحليل، الفضاء السيبراني كمحل لظاهرة الصراع، ومن ثم تطبيق منهج التحليل الجيوبولتيكي على ظواهر الفضاء السيبراني، حيث جاء **المبحث الأول** ليسلط الضوء على الجيوبولتيكا، تطورها وتتبع مراحل أفولها وازدهارها منذ الآباء المؤسسين وتأصيلاتهم، ووصولاً إلى المدارس المعاصرة للجيوبولتيكا وتوسعاتها في مستويات التحليل والقضايا، مع توضيح لمنهج التحليل الجيوبولتيكي، وقدم **المبحث الثاني** مفاهيم للفضاء السيبراني وما تعلق به من ظواهر كالقوة والصراع وشرح علاقة التأثير والتأثير مع العلاقات الدولية، أما **المبحث الثالث** فقد ناقش التأصيل المنهجي للدراسة أي إمكانية وكيفية القيام بالتحليل الجيوبولتيكي للفضاء السيبراني من خلال تقديم هندسة الطبقات والنوموس والنقاش حول ظاهرتي الحدود والسيادة في هذا الفضاء.

الفصل الثاني: ورد بعنوان "مضامين الصراع الأمريكي الصيني في الفضاء السيبراني" ويُعنى برصد وتفسير وتحليل -وفق المنهج الجيوبولتيكي- كيفية استخدام كل من الولايات المتحدة والصين لقدراتهما ضد بعضهما البعض في كل طبقة من طبقات الفضاء السيبراني ما يؤثر على علاقتهما الثنائية والتوازنات الدولية، جاء **المبحث الأول** ليستعرض القدرات السيبرانية لكل من الولايات المتحدة الأمريكية والصين، و**المبحث الثاني** ليكشف عن تطبيق تلك القدرات في كل طبقة والصراع الدائر حول النفوذ والسيطرة بين البلدين، أما **المبحث الثالث** فقد رصد تداعيات الصراع الأمريكي-الصيني على العلاقات الثنائية والتحالفات والتوازنات الدولية والنظام الدولي بشكل عام.

الفصل الثالث: الموسوم بـ "استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني" يقدم الفصل بداية قراءة في أهم المقاربات والمنطلقات الفكرية الجديدة لإدارة الصراع في الفضاء السيبراني -التي لها علاقة بمجال التحليل الجيوبولتيكي- والتي تعمق فهمنا لكيفية تطوير وبناء استراتيجيات كل دولة للهيمنة في/على الفضاء السيبراني انطلاقاً من مبادئها

الجيوبوليتيكية ومدرکها الاستراتيجي لهذا الفضاء، لذلك، قدم **المبحث الأول** مجموعة من المقاربات النظرية والأفكار الجديدة لإدارة الصراع في الفضاء السيبراني مثل: الهيمنة الرقمية، اللعبة الجيوبوليتيكية الرقمية ونظرية الردع ...، وحل **المبحث الثاني** الاستراتيجيات السيبرانية والاستراتيجيات الكبرى الأمريكية المتعلقة بالفضاء السيبراني وأبرز العلاقة بين أهدافها النهائية والمبادئ الجيوبوليتيكية للولايات المتحدة والإدراك الاستراتيجي لصانع القرار الأمريكي، أما **المبحث الثالث** فقد تتبع مراحل تطور المبادئ الجيوبوليتيكية الصينية ومن ثم وضع الأهمية الاستراتيجية للفضاء السيبراني عند صانع القرار الصيني وصولاً إلى تحليل أهم استراتيجيات سيبرانية كبرى طورها القادة الصينيون "الصين الرقمية" وما سبقها واندماج معها من مشاريع ومبادرات تسعى للتفوق في الفضاء السيبراني ومدى انسجام أهدافها مع المبادئ الجيوبوليتيكية والأهمية الاستراتيجية للفضاء السيبراني لدى القادة في الصين.

الفصل الرابع: جاء تحت عنوان " مآلات الصراع الأمريكي الصيني في الفضاء السيبراني " ليضعنا أمام مسارات متعددة لما سيؤول إليه صراع الهيمنة بين القوتين العظميين، وبما أن تقنية السيناريوهات كانت الأكثر ملاءمة للدراسة جاء كل مبحث من المباحث الثلاثة للفصل ليقدّم شروحاً مستفيضة حول مسار من مسارات الصراع، **فالمبحث الأول** رسم لنا سيناريو ضبط الصراع من خلال المعايير والاتفاقيات وصولاً إلى إدارة المنافسة والتعايش السلمي بين البلدين، أما **المبحث الثاني** فقد برر الأسباب وحلّل المؤشرات التي تُفضي إلى استمرار الصراع في شكل حرب باردة جديدة محورها التكنولوجيا وفي مركزها صناعة الرقائق، أما **المبحث الثالث** فقد عرض لنا صورة المستقبل القاتمة لصراع الهيمنة، فبين تفكك الفضاء السيبراني أو هيمنة أحد الطرفين وفرض نموده ورؤيته للفضاء السيبراني بالقوة، يبقى تفجر حرب سيبرانية شاملة قد تدمر الفضاء السيبراني هو أسوأ السيناريوهات.

الفصل الأول

جيوبوليتيكا الفضاء السيبراني

يسعى هذا الفصل لتقديم مفهوم واضح لعلم الجيوبوليتيكا وتتبع مراحل توهجها، أفولها وإعادة إحيائها من جديد، عبر تبسيط أفكار ورؤى الآباء المؤسسين لهذا العلم، مروراً بمرحلة الأفول والعزل في الأوساط العلمية، وانتهاءً بعمليات الإحياء والتجديد التي لحقت بها، لتصبح الجيوبوليتيكا علماً يتتبع نشاطات الإنسان أينما كانت، ويُعطي فهوماً وتفسيرات مميزة للصراع حول القوة والنفوذ.

ثم يعالج الفصل "الفضاء السيبراني" والمفاهيم المتعلقة به، حيث يناقش التفاعلات التي تحدث فيه كأحد النشاطات البشرية المعاصرة، ويُبيّن العلاقة (تأثير/تأثر) بينه وبين العلاقات الدولية، وكيف أن مفاهيم مثل القوة قد تحولت وانتشرت بين الفاعلين، والصراع الذي تبدل مضمونه وتغيرت أدواته وانعكاسته.

وللتعمق في فهم الصراع في الفضاء السيبراني باستخدام منهج التحليل الجيوبوليتيكي كان لزاماً علينا تجاوز التحدي المنهجي الذي يتمثل في السؤال حول ما إذا كان الفضاء السيبراني إقليماً، حتى يكون صالحاً للتحليل الجيوبوليتيكي، حيث يقدم الفصل مفهوم الطبقات لفهم مكونات الفضاء السيبراني، ومفهوم النوموس لمعرفة كيف تتطور القوانين داخل هذا الفضاء، ويختم بنقاش ينقل فيه أهم ميزتين للأقليم إلى الفضاء السيبراني وهما الحدود السيبرانية والسيادة السيبرانية.

المبحث الأول: الجيوبوليتيكا... تطور النظرية ومنهج التحليل

مرت الجيوبوليتيكا كعلم بفترات متباينة من الازدهار، الأفول وإعادة الإحياء خلال مسيرتها المستمرة على مدى أكثر من قرن من الزمان، فاختلاف وجهات النظر حول علاقة الجغرافيا بالسياسة وارتباطها بالقوة والتوسع جعل الجيوبوليتيك تتوزع عبر العديد من المدارس والممارسين، وفي المقابل، خلق لها الكثير من الأعداء والرافضين، ولكن ماتقدمه من رؤى واستبصارات حول العالم والصراع والمستقبل جعل منها منهج التحليل الأكثر اعتماداً لدى السياسيين والاستراتيجيين والباحثين لفهم واستشراف النزاعات والصراعات بين القوى المختلفة حول النفوذ والسيطرة والزعامة على المستويات الكونية، الإقليمية والداخلية.

المطلب الأول: الجيوبوليتيكا رؤية للعالم

الفرع الأول: الجيوبوليتيكا بين الأفول وإعادة الإحياء

بعد ظهور الطروحات الأولى للجيوبوليتيكا (الدولة كائن حي، المجال الحيوي) على يد فريديريك راتزل في نهاية القرن التاسع عشر، والتي شكلت المبادئ الأساسية لظهور وتطور الأفكار والفروض الجيوبوليتيكية، أعطى رودولف كيلين التعريف الأول للمصطلح الجديد "الجيوبوليتيكا" على أنها "علم الدولة كجسم جغرافي متجسد في المكان".

وكان للسير هيلفورد.ج ماكندر الفضل في صياغة القانون الأساسي للجيوبوليتيكا، عبر رؤيته الكونية للعالم وتقسيماته المَدوية (قلب الأرض، الهلال، جزيرة العالم)¹، والتي لا تزال تستعمل حتى اليوم في فهم وتفسير واستشراف الأحداث الكونية، كما وضع ألفرد ماهان أسس القوة البحرية التي مكنت الولايات المتحدة الأمريكية من الهيمنة على العالم لاحقاً، إلا ان اندلاع الحرب العالمية الثانية وما سببته ألمانيا النازية من دمار للعالم، جعل الأكاديميين يوجهون أصابع الاتهام للجيوبوليتيكا عبر تجريم كارل هاوسهوفر ومساهمة طروحاته المؤكدة لثنائية قوى البر في مواجهة قوى البحر في تبرير الغزو النازي وشرعنة سياسات هتلر التوسعية، وهذا ما دعا الجغرافيين إلى اعتبار الجيوبوليتيكا "الابن العاق" لأسرة الجغرافيا، أو كما سماها الجغرافي الأمريكي ريتشارد هرتشهون "سماً فكرياً".

¹ هالفورد جورج ماكندر، المحور الجغرافي للتاريخ، انظر في: ألكسندر دوغين، أسس الجيوبوليتيكا، مستقبل روسيا الجيوبوليتيكي. تر: عماد حاتم، بيروت: دار الكتاب الجديد المتحدة، 2004، ص 551.

بقيت الجيوبوليتيكا منبوذة في الأوساط العلمية - خاصة الغربية منها¹ - ومستبعدة كخطاب أكاديمي لفترة ما بعد الحرب العالمية الثانية وحتى سبعينيات القرن الماضي، حيث بدأت تلوح بوادر إحياء هذا العلم، كما أكد ذلك أستاذ الجيوبوليتيكا الأمريكي **سول كوهين** بقوله "إن قضايا الجيوبوليتيكا من الأهمية بمكان، بحيث يستحيل على الجغرافيين إزاحتها جانبا".

اتخذ هذا الإحياء للجيوبوليتيكا ثلاث صيغ حسب **بيتر تايلور وكولن فلنت**²، إذ أصبح المصطلح أكثر شعبية ورواجاً في وسائل الإعلام وبين الساسة، ويرجع الفضل في ذلك لكتابات **هنري كيسنجر** واستعماله المكثف لمصطلح الجيوبوليتيكا في مذكراته، حيث كشفت المناقشات المكثفة والواسعة لتلك المذكرات عما يقدمه هذا الفكر من استبصارات وفهوم للسياسات العالمية ولاستراتيجيات إدارة التنافس الكوني بين القوى المتصارعة.

أما الصيغة الثانية فكانت إحياء الجيوبوليتيكا كخطاب أكاديمي، بدءاً بمراجعة الماضي المخجل للجيوبوليتيكا (أو الذي أريد تشويهه) من أجل المضي للمستقبل وتطوير هذا العلم، كما بدأ المفكرون في إعادة دراسة القضايا التقليدية للجيوبوليتيكا دون الشعور بالخزي بل إن دمج مواضيع الجيو-ايكونوميك والهيمنة أعطى دفعا قويا للدراسات الجيوبوليتيكية، كما حاول بعض المفكرين مثل **جيروا أوتواثيلا** إعادة صياغة وإصلاح الجيوبوليتيكا لتتلائم مع مستجدات السياسة العالمية وتحولاتها باستعمال تفسيرات مابعد-بنوية للممارسات الجيوبوليتيكية بغية تطوير جيوبوليتيكا نقدية متحررة من سرديات الماضي المخزي.

وتتضمن الصيغة الثالثة المدافعين على فكرة "الضرورة الجغرافية"، أو الحتمية الجغرافية باعتبارها العنصر الثابت في أي فكر استراتيجي، ويسميهما الكاتبان **بيتر تايلور وكولن فلنت** مجموعات الضغط من المحافظين ودعاة الحرب، لكن الفكرة في الحقيقة هي أساس الجيوبوليتيكا

¹ يقول **كلاوس دودز** أن الجيوبوليتيك أثناء فترة الركود في الغرب قد انتعشت في دول أمريكا الجنوبية (البرازيل، الأرجنتين، تشيلي) انظر: **كلاوس دودز، ديفيد أتكينسون، الجغرافيا السياسية في مائة عام (التطور الجيوبوليتيكي العالمي)**، ج1، تر: عاطف معتمد، عزت زيان، المركز القومي للترجمة، العدد 1592، 2010، ص19.

ويؤكد **ليسلي هابل** أن البحث وممارسة الجيوبوليتيكا لم تتوقف ابدا، حيث قدمت عدة دراسات جيوبوليتيكية في فترة الضعف تحت مسميات الدراسات الإستراتيجية أو الجغرافية، انظر:

Leslie W Hepple, "The revival of geopolitics", **Political Geography Quarterly**, Vol 5, N° 4, 1986, pp S22-S23.

² **بيتر تايلور وكولن فلنت، الجغرافيا السياسية لعالمنا المعاصر (الاقتصاد العالمي، الدولة القومية، المحليات)**، تر: عبد السلام رضوان واسحق عبيد، الكويت: مطابع السياسة، 2002، ص 93-95.

التقليدية أو الأرثوذكسية وهذا مانجده عند أبرز الجيوبوليتيكيين المعاصرين مثل "ألكسندر دوغين" الذي يعتنق مذهب "الجغرافيا مصيراً" و"الإنسان المدوي".

الفرع الثاني: الجيوبوليتيكا ... نظام علمي مفتوح

لطالما قدمت الجيوبوليتيكا للمفكرين والممارسين رؤية كونية للعالم، فبعد أن وضع راتسيل مبادئ هذا العلم معتبرا الدولة كائناً حياً ينمو ويتوسع عبر **المدى الأرضي**، وبيّن قيمة الجغرافيا في دراسة تطور الدول حين وضع قوانين التوسع السبعة للدولة¹، جاء بعده **كيلين** ليعطي هذا العلم اسماً جديداً هو "الجيوبوليتيكا"، وتعتبر كتابات الجغرافي الانجليزي السير **هالفورد ماكندر** عملاً تأسيسياً لعلم الجيوبوليتيكا، حيث اعتبر أن المنظومة الكونية دخلت في "العصر مابعد الكولومبي"² وسعى لفهم القضايا والعلاقات بين الدول على الصعيد الكوني، وتفسيرها بشكل كلي في مختلف تجلياتها المكانية، ونتج عن تقسيماته للعالم عبر دوائر كونية المفاتيح اللازمة لفهم اللوحة الجيوبوليتيكية العالمية (قلب الارض **Heartland**، الهلال الداخلي، الهلال الجزيري)، وبرّر بذلك مقولته الأشهر: "من يحكم قلب العالم يحكم الجزيرة العالمية، ومن يحكم الجزيرة العالمية يحكم العالم".

وبناءً على ما سبق، وبالجمع بين أفكار **ماكندر** وخوفه من توحيد قوى البر، و**ماهان** المدافع عن قوى البحر، يتجلى لنا القانون الأبدي للجيوبوليتيكا الكلاسيكية: **التيلوركراتيا ضد التالاسوكراتيا** أو قوى البر ضد قوى البحر، هذا القانون شرحه الفيلسوف والحقوقي الألماني **كارل شميت** في كتابه "الأرض والبحر" معللاً التوتر الكوني بين الشرق والغرب³، وهو ما عرف فيما بعد بـ **جيوبوليتيكا الحرب الباردة**، حيث سخّرت الولايات المتحدة الأمريكية (باعتبارها ممثلاً للتالاسوكراتيا) كل استراتيجياتها لمواجهة الاتحاد السوفياتي (ممثلاً للتيلوركراتيا) انطلاقاً من رؤى

¹ وضع فريديريك راتسيل في كتابه "حول قوانين تطور الدولة في المجال" سنة 1907، سبعة قوانين تحكم توسع الدولة التي اعتبرها كائناً حياً يولد وينمو ويموت، وعليه فإن التوسع على حساب الدول الضعيفة أو فقدان الأراضي لصالح الدول الأقوى عمليتان طبيعيتان في دورة الحياة الداخلية للدولة، انظر في: ألكسندر دوغين، مرجع سابق، ص.ص 78-79.

² يعتبر ماكندر حسب تقسيماته للتاريخ الجيوبوليتيكي للأرض أن المنظومة الأرضية دخلت عصر مابعد كولومبس، حيث لم يعد هناك مكان للغزو، وعليه فإن أي صراع أو انفجار اجتماعي يرتد إلى البر من جديد، وديناميكية الحضارات محكوم عليها بالتصادم. انظر في: ألكسندر دوغين، مرجع سابق، ص 93 و ص 551-553.

³ كارل شميت، التوتر الكوني بين الشرق والغرب والمواجهة بين الأرض والبحر، انظر في: ألكسندر دوغين، مرجع سابق، ص 595.

ومبادئ جيوبوليتيكية لماهان وسبيكمان، هذا الأخير الذي طور ونقح مفهوم الهلال الداخلي Rimland ويبن أنه مفتاح السيطرة على العالم، محققاً بذلك المعادلة الجيوبوليتيكية الأشد تأثيراً والأسرع تمكيناً للولايات المتحدة الأمريكية في الهيمنة العالمية.

إضافة إلى ذلك، مارس السياسيون والعسكريون في الولايات المتحدة الأمريكية الجيوبوليتيكا طيلة فترة نبذها في المجتمعات العلمية، لأنهم ادركوا قدراتها المتميزة وآلياتها الفعالة في تفسير الممارسات الاستراتيجية في العلاقات الدولية، فهي بحق تعطي رؤية للعالم وتجب على الأسئلة "الكبرى" و"الأبدية" و"العتيقة"¹ حول تركيبة العالم وطبيعة الصراع فيه والذي تغزوه إلى التناقض بين حضارة الأرض وحضارة البحر والصدام الأبدي بينهما، كما تعطي فهوماً عن عالم اليوم وتشكيلاته السياسية والعسكرية، كما تستشرف المستقبل، وتتنبأ بمصير التفاعلات الدولية.

بعد نهاية الحرب الباردة كثر الحديث عن نهاية الدولة ونهاية الجغرافيا تحت وطأة العولمة والتطور التكنولوجي، وهذا ما يستوجب نهاية الجيوبوليتيكا، لكن ما حدث هو العكس، وبشكل لافت أصبحت الجيوبوليتيكا "موضة"، تستعمل بإفراط في وسائل الإعلام وعند السياسيين (أحيانا بغير المعنى الذي وجد من أجله المصطلح) وكذا في الأوساط العلمية، حيث يصف "دوغين" الجيوبوليتيكا بأنها "الدليل الذي لا بديل عنه لجميع من يتخذون القرارات في الميادين الأعظم أهمية في الحياة السياسية الروسية من السياسيين وأصحاب المشاريع، والاقتصاديين والمصرفيين والدبلوماسيين والمحليين وعلماء السياسة ومن في حكمهم"².

هذا الزخم الجيوبوليتيكي وسع ميادين البحث لهذا العلم، فظهرت: جيوبوليتيكا العواطف، جيوبوليتيكا الأديان، جيوبوليتيكا الانتخابات، جيوبوليتيكا المياه... إلخ، مما دعا كارل جين لوصف الجيوبوليتيكا بأنها: "فوضى رهيب"³، لكن في المقابل أصبحت أكثر شعبية كما أشار إلى

¹ يقدم كليمنت فيدال مصطلح "رؤية للعالم" عبر الإجابة عن ستة 6 أسئلة جوهرية حول العالم كما يلي: ماهو؟ من أين أتى؟ إلى أين؟ ماهو الجيد وماهو السيئ؟ ماذا نفعل؟ ماهو صح وماهو خطأ؟ وهاته الأسئلة تغطي الجوانب: الأنطولوجي، التكويني، التنبؤ، القيم، الباراكسيولوجي والابستمولوجي، وبعد الإجابة عليها تتشكل لدينا رؤية للعالم، انظر:

Clément Vidal, "What is a worldview?.", *De wetenschappen en het creatieve aspect van de werkelijkheid*, 2008.

² ألكسندر دوغين، مرجع سابق، ص 5.

³ أغنيشكا لغوتسكا، الجيوبوليتيك الجديدة: ما الجديد فعليا في هذا الحقل؟، ترجمة: جلال خشيب، مركز ادراك للدراسات والاستشارات، 2018.

ذلك جيرارد اوتاتويل في تقسيماته للنسخة المابعد-حادثة للجيوبوليتيكا أو ما يسمى الجيوبوليتيكا النقدية، حيث نقلت الجيوبوليتيكا المعاصرة مجال البحث من المجال الجغرافي المرتبط بالأرض إلى المكان/الفضاء الذي ينشط فيه الإنسان، فالجيوبوليتيكا تُعنى بتتبع النشاط البشري. كما توسعت مستويات التحليل إلى المستوى الإقليمي والمحلي وتعدد الفاعلون بعد أن كانت الدولة محور التحليل، فالجيوبوليتيك اليوم تدرس صراع وتفاعل مختلف الفاعلين في فضاءات جديدة كلياً بما فيها الفضاء السيبراني، حيث يرى البعض أن الجيوبوليتيكا تعكس الحقائق الدولية وتشكيلة القوة العالمية المتجلية عن التفاعل بين الجغرافيا من جهة وبين التكنولوجيا والتنمية الاقتصادية من جهة أخرى.

في هذا السياق، يوصي فيل كيلي بعد أن أجرى مقارنة بين الجيوبوليتيكا التقليدية والنقدية، بمواصلة البحث في الجيوبوليتيكا التقليدية جنبا إلى جنب مع الاستعانة بطروحات ومفاهيم الجيوبوليتيكا النقدية، فالمزوجة بين الرؤيتين تعطي فهماً أكثر عمقا وأكثر إنتاجية، حيث يقول: "يجب قبول وجهات النظر الفريدة لكلا النوعين باعتبارها مشروعة ومنتجة، وكل منهما في حد ذاتها تخبرنا في مكان ما عن نصف الحقيقة"¹.*

لذلك يحق لنا اعتبار الجيوبوليتيكا بتشكيلاتها النظرية المتعددة ومفاهيمها المتنوعة منظومة تفسيرية رائدة تفرض ثبوتيتها في تفسير الماضي وفعاليتها في تنظيم الحاضر وتصميم آفاق المستقبل.

المطلب الثاني: الجيوبوليتيكا التقليدية: الآباء المؤسسون

اتسم التنظير الجيوبوليتيكي التقليدي بتعدد المدارس والمفكرين، والاختلافات الكبيرة بينها التي تصل إلى حد التناقض، فمرحلة البدايات أو ما يطلق عليها الجيوبوليتيكا التقليدية تميزت بالتحليل الكوني للعالم، والاهتمام بالإجابة عن السؤال المحوري: من سيحكم العالم؟ حيث برزت مدرستان كبيرتان هي المدرسة الألمانية و المدرسة الانجلوساكسونية.

¹ Kelly Phil, Kelly, "A critique of critical geopolitics", **Geopolitics**, vol 11, N° 1, 2006.

*جميع النصوص المترجمة إلى اللغة العربية الواردة في متن هذه الدراسة قام بها الباحث.

الفرع الأول: المدرسة الألمانية

نشطت الدراسات الجيوبوليتيكية في ألمانيا بعد الحرب العالمية الأولى، فبعد الهزيمة في الحرب والتوقيع على معاهدة فرساي المهينة، بحث كل من المفكرين والعسكريين في أسباب الهزيمة وعوامل النهوض واستعادة أمجاد الماضي.

أولاً، فريدريك راتزل (1844-1904): الدول كائنات حية

الجغرافي الألماني الذي يُعتبر "أب الجيوبوليتيكا"¹، عمل أستاذاً للجغرافيا في كل من معهدي ميونيخ ولايبزيغ، تأثرت الرؤية الفكرية لراتزل بالهيجيلية (التطورية) والداروينية ونمت لديه فكرة اعتبار الفضاء (المكان) المحرك الأساسي للتاريخ، صدر كتابه الأكثر أهمية "الجغرافيا السياسية Politische Geographie" سنة 1897، والذي قدم فيه رؤيته حول الدولة منطلقاً من مقارنة عضوية، فالدولة عند "راتزل" كائن حي ينمو ويكبر ثم يتحلل ويتلاشى، وهذه النظرة "العضوية" توضح فهم راتزل للتطور الممتد للدولة على أنه ظاهرة طبيعية حية، كما تنعكس هذه النظرة العضوية على فهم راتزل للمدى حيث تنتقل طبيعته المادية إلى طبيعة حيوية ويصبح وسطاً حيويًا أو مجالاً حيويًا Lebensraum².

كما ربط راتزل بين نمو الدولة والقوة، حيث يعتبر أن القوة عامل أساسي في تأمين عملية النمو، فالدولة العظمى -عند راتزل- خلال مراحل نموها الطبيعي تتوسع باستمرار حتى تحقق متطلبات وجودها³، يحدد راتزل ديناميكيات عملية التوسع ويقدم مبرراتها ومسوغاتها من منظور قوانين القوة والصراع والبقاء للأقوى، حيث يقدم في كتابه "قوانين تطور الدول في المجال" الصادر سنة 1901، سبعة قوانين تشكل في نظره الأساس التي تقوم عليه عملية التوسع⁴.

تعرضت هذه القوانين إلى انتقاد شديد كونها أعتبرت شرعنة لعمليات الاستعمار والغزو وحطمت فكرة "حصانة الحدود"، وفُهمت ك دليل مرشد للإمبرياليين، إلا أن جيرار ديسوا يعطي

¹ ألكسندر دوغين، مرجع سابق، ص 75.

² ألكسندر دوغين، مرجع سابق، ص 77.

³ عبد القادر محمد فهمي، المدخل إلى دراسة الاستراتيجية، ط2، عمان: دار المجدلوي للنشر والتوزيع، 2013، ص 62.

⁴ محمد رياض، الأصول العامة في الجغرافيا السياسية والجيوبوليتيكا، القاهرة: مؤسسة هنداي للتعليم والثقافة، 2014، ص 46-45.

قراءة مغايرة وأكثر عمقا لأفكار راتزل حول المجال الحيوي وقوانين التوسع السبعة¹، حيث يُظهر أن هذه الأفكار ما هي إلا محاولة من راتزل لإيقاظ الإحساس بالمدى لدى قادة ألمانيا الذين كانوا لا يعطون قيمة حقيقية للمعطيات الجغرافية.

ثانياً، رودولف كيلين (1864-1922) : ألمانيا القوة القارية

كانت ميولات السويدي كيلين لألمانيا واضحة، وعلى خطى أستاذه راتزل كانت المقاربة العضوية في دراسته للدولة طاغية على أفكاره وفروضة، حيث قام بتطوير طروحات راتزل حول العلاقة بين المكان (المدى) والتنظيم السياسي للدولة، وقام بإضافة اللاحقة Geo إلى مصطلح السياسة Poltik، ليقدم مصطلحا جديدا هو الجيوبوليتيك Geopolitik معرفا إياها بأنها: "العلم الذي يتصور الدولة كجسم جغرافي، أو كظاهرة متحركة في المكان"².

يؤكد كيلين على طرح راتزل في كتابه " الدولة مظهر من مظاهر الحياة " Staten som livsform الصادر سنة 1917، حيث ماثل بين البناء العضوي للدولة ونظيره لدى الكائن الحي، وشبه عاصمة الدولة بالقلب وطرق المواصلات بالشرابين، كما ناقش إشكالية التناقض بين عمليات التوسع والقانون الدولي متسائلاً: أيهما أجدد بالمراعاة، قوانين الطبيعة أم قوانين البشر؟ ويُرجح في مناقشته القانون الطبيعي، الذي يسمو -حسب كيلين- على كل قوانين البشر، مؤكداً على حتمية نمو الدولة³.

ظهرت قوة أفكار كيلين من خلال تطبيقه لها على الوضع في أوروبا، حيث اعتبر ألمانيا هي "الدولة القارية"، حيث تتميز بعوامل البناء الثقافية والفكرية والاقتصادية والروح العسكرية، وحدد مساراً للهيمنة العالمية عبر ثلاث مراحل⁴، تبدأ بأن تصبح ألمانيا قوة برية كبرى، ثم تهزم بريطانيا في البحر، وأخيراً تحقق السيادة العالمية.

¹ انظر: جبرار ديسوا، دراسة في العلاقات الدولية، الجزء الأول: النظريات الجيوسياسية، تر: قاسم المقداد، دمشق: دار نينوى للدراسات والنشر والتوزيع، 2014، ص.ص 97-102.

² نفس المرجع، ص 81.

³ عبد القادر محمد فهمي، مرجع سابق، ص 67.

⁴ نفس المرجع، ص 68.

لقد كانت أفكار كيلين تمثل الأساس النظري الجيواستراتيجي لسياسة ألمانيا التوسعية في الحربين العالميتين، إذ فسرت الحرب العالمية الأولى بأنها صراع جيوبوليتيكي بين قوى النمو التصاعدي الألمانية (دول المحور) وقوى النمو التنازلي الفرنسية والإنجليزية (الأطراف).

ثالثاً، كارل هاوسهوفر (1869-1946): المجال الحيوي وانفتاح ألمانيا نحو الشرق

أسس الجنرال الألماني هاوسهوفر معهد ميونيخ للجيوپوليتيكا، كما أصدر المجلة المشهورة "Zeitschrift für Geopolitik" ابتداءً من سنة 1923 والتي قدم فيها معظم آرائه وأفكاره حول الجيوبوليتيكا.

لم تخرج أفكار هاوسهوفر عن مبادئ المدرسة العضوية الألمانية، حيث يرى أن الدولة كائن حي يحتاج للنمو والتوسع، وأن تكوين الدولة العظمى مبني على أساس النمو والتوسع في المجال الحيوي، وهذا راجع لاعتقاده بأن "المجال الحيوي" هو العامل الأهم الذي يتحكم في تاريخ البشرية.

دفع هاوسهوفر بالجيوبوليتيكا -كما يقول جيرار ديسوا- إلى التفكير الدائم بالعلاقات الدولية ذات الطابع الاستراتيجي، حيث أكد على حتمية المواجهة مع القوة البحرية الأنجلوساكسونية إذا لم ترد ألمانيا أن تموت مخنوقة¹ (من منظور العقدة الأزلية لدى المفكرين الألمان حول العزلة والخنق الذي تعاني منه ألمانيا)، هذا ما دفعه لتقديم تقسيم ثلاثي للعالم وفق مفهوم المجال الحيوي؛ حيث تسيطر ألمانيا على أوروبا وأفريقيا، واليابان على شرق آسيا، والولايات المتحدة على الأمريكيتين، غير أن كتاباته لم تُخف رغبته في تحقيق ألمانيا السيطرة على العالم في نهاية الأمر.

قدم هاوسهوفر عقيدته حول ألمانيا القومية العظمى مُنظراً بذلك لعملية النمو والتوسع الألماني من خلال طرحه لفكرة الانفتاح نحو الشرق، ومحور هذه العقيدة هو إقامة "حلف قاري" أو محور "برلين-موسكو-طوكيو"، ويؤكد على رؤيته بالاستشهاد بمقولة الأمريكي هوميرلي: "ستدق الساعة الأخيرة للسياسة الأنجلوساكسونية عندما يتحد الألمان والروس واليابانيون"².

لقد كانت مساهمة هاوسهوفر فاعلة في تطبيق الجيوبوليتيكا كمنهج، وكان دفاعه كبيراً حول الحتمية الجغرافية كمفسر أساسي لمسيرة التاريخ، إلا أن علاقته بـ"هتلر" والحزب النازي أثارت

¹ جيرار ديسوا، مرجع سابق، ص 128.

² ألكسندر دوغين، مرجع سابق، ص 114-115.

الكثير من النقد وردود الفعل السلبية حول الجيوبوليتيكا، مما جعلها علماً منبوذاً وتم تغييرها أكاديمياً مدة طويلة من الزمن.

رابعاً، كارل شميدت (1888-1985): التضاد بين البر والبحر

لم تَحِد أفكار الفيلسوف الألماني شميدت عن المدرسة العضوية، وجاء إنتاجه الفكري مليئاً بالاستعارات من المورث الديني والأساطير لتفسير العوامل الجيوبوليتيكية وتأثيرها على الحضارة والتاريخ السياسي، أبرز شميدت العلاقة بين الثقافة السياسية والمدى المكاني، حيث يوضح في كتابه "نوموس الأرض"¹ كيف يؤثر المكان على الحضارات والدول التي تتشكل فيه، ويقارن بين "نوموسات" تاريخية مختلفة²، ليكشف التناقض النوعي والتاريخي بين "نوموس الأرض" و"نوموس البحر"، ويصوغ بذلك منهجية جيوبوليتيكية خاصة لتفسير التاريخ السياسي للعالم.

هذا التناقض بين البر والبحر الذي يعتبره "ديسوا" التضاد المؤسس للجيوبوليتيكا، يشرحه شميدت في عملين يُعتبران من الأعمال الأساسية في الجيوبوليتيكا هما: "الأرض والبحر" الذي صدر سنة 1942، وبعده "التوتر الكوني بين الشرق والغرب والمواجهة بين البر والبحر" والذي صدر في خضم الحرب الباردة، حيث أعطى شميدت صورة عن حضارتين مختلفتين، متعاديتين، وأعطى لعناصر اللوحة الجيوبوليتيكية الكونية التالاسوكراتيا (القوة البحرية) والتيلوركراتيا (القوة البرية) تفسيرات فلسفية عميقة، ووصف المواجهة بينهما بالمواجهة بين "لويثان"³ و "البهيموث"⁴، وخلص إلى أن المواجهة الجيوبوليتيكية للعالم الأنجلوساكسوني تتخذ معنى اجتماعياً سياسياً، وللدول البرية معنى تاريخياً إيدولوجياً وفلسفياً⁵.

يقدم شميدت نظرة مستقبلية حول التطورات التقنية والتكنولوجية، حيث يعتبر أن تطور سلاح الجو وغزو الفضاء الخارجي والاتصالات (يسميها دوغين الإيروكراتيا وتعني "سلطة الجو" والاثيروكراتيا وتعني "سلطة الأثير" أو المدى الكوني) لا تشكل أنظمة جيوبوليتيكية مستقلة بقدر

¹ النوموس كلمة يونانية تعني المقياس الأول لجميع التدابير اللاحقة، ويقصد بها شميدت القوانين والأفعال والتدابير والمراسيم من جميع الأنواع. انظر المطلب الثاني من المبحث الثالث لهذا الفصل.

² Carl schmitt, *The nomos of the earth*, Trans: GL Ulmen, Telos Press, New York, 2003.

³ لويثان وحش بحري مذكور في الأساطير القديمة والتوراة.

⁴ البهيموث وحش أرضي يشبه الفيل أو فرس النهر مذكور في الأساطير القديمة والتوراة.

⁵ كارل شميدت، *التوتر الكوني بين الشرق والغرب والمواجهة بين البر والبحر*، في: ألكسندر دوغين، مرجع سابق، ص

ماهي تطور لـ"نوموس البحر"، وأنها الحقبة المتقدمة من "التالاسوكراتيا"، ذلك أن شميدت يرى أن كل التطورات التقنية والتكنولوجية لغزو الفضاءات الجديدة تدفع إلى "تميع الوسط" حيث تترافق مع عمليات ثقافية وحضارية تشمل كل المستويات بداية على المستوى الاستراتيجي، ووصولاً إلى المستويات الأخلاقية، الروحية، الاجتماعية والسياسية¹.

الفرع الثاني: المدرسة الانجلوساكسونية

أولاً، ألفريد تايلر ماهان (1840-1914): القوة البحرية

يعد الأميرال ألفريد ماهان من أوائل المؤرخين والاستراتيجيين الذين درسوا أهمية الموقع الجغرافي البحري للدولة، حيث أبرز أهميته في بناء قوة الدولة وإعطائها ميزة التفوق والسيطرة العالمية، كرس ماهان العديد من مؤلفاته للحديث حول "القوة البحرية"، حيث ربطها بالتوجه البحري والتجاري للدولة، كما أضاف لها شروطاً أخرى²، وعند إسقاطه لهذه الشروط على الولايات المتحدة وجد أن تطور التجارة الخارجية الأمريكية نتيجة حتمية لنموها الاقتصادي، وهذا ما يستدعي حمايتها بتواجد أسطول بحري قوي، وهو ما انتهى بالهيمنة الأمريكية على العالم، كما أنه تنبأ في كتابه "مشكلات آسيا" الذي صدر سنة 1900 ببلوغ السيادة العالمية عبر استخدام (احتلال) قواعد عسكرية تحيط بأوراسيا³.

رسخت لدى ماهان من خلال دراساته ثلاث قناعات⁴، أولاً، تفوق القوة البحرية في صراعها مع القوة القارية، ثانياً، وجوب السيطرة على البحار للسيطرة على العالم، ثالثاً، وجوب الدفاع عن الخطوط البحرية. لقد كان ماهان من أكثر القادة الذين أصغت قيادة بلاده لآرائه وطبقته، حيث أثبت كيف يمكن للآراء الجيوبوليتيكية أن تعمل لخدمة مصالح الدولة.

ثانياً، هالفورد ج ماكندر (1861-1947): قلب العالم Heartland

يُعد الجغرافي وعالم السياسة والدبلوماسي البريطاني السير هالفورد ماكندر من الآباء المؤسسين للجيوبوليتيكا، وتعتبر مداخلته "المحور الجغرافي للتاريخ" التي قدمها للجمعية الملكية

¹ ألكسندر دوغين، مرجع سابق، ص 155.

² للاطلاع حول العوامل التي يتطلبها بناء وتطوير القوة البحرية عند ماهان انظر في: عبد القادر محمد فهمي، مرجع سابق، ص 78-80.

³ محمد رياض، مرجع سابق، ص 77.

⁴ جيرار ديسوا، مرجع سابق، ص 106-107.

للجغرافيا سنة 1904، والكتيب الذي أصدره في 1919 بعنوان "المثل الديمقراطية والواقع" والتي ضمّتهما رؤيته للتاريخ والجغرافيا، من النصوص الأساسية في الجيوبوليتيكا ويعتبرهما "دوغين" النص الجيوبوليتيكي الأساس لهذا العلم.

ينطلق ماكندر في أطروحته من اهتمامه وقلقه العميق حول مصير بريطانيا العظمى وإمبراطوريتها، ليعطي تحذيراً للرأي العام الإنجليزي حول الأخطار الكونية التي تتربص به، فمن خلال تقسيماته للتاريخ الجيوبوليتيكي للعالم إلى ثلاث مراحل تسبق، ترافق وتتلو اكتشافات الرحالة "كولومبس"، ادرك ماكندر أن العالم دخل في مرحلة مابعد كولومبس حيث أصبح مكاناً مغلقاً، ولا توجد أرض جديدة لاكتشافها وغزوها¹، وعليه فلا بد من ادراك العالم بوصفه منظومة تؤثر عناصرها بعضها ببعض، مما يعطي الامكانية لسيطرة إمبراطورية (دولة كبرى) على العالم.

يقدم ماكندر ترسيمة للعالم تتشكل من المساحة القارية الأكبر (أوروبا وآسيا وإفريقيا) والتي ترتبط مع بعضها مشكلة "جزيرة العالم World Island"، داخل هذه الجزيرة يحدد ماكندر المنطقة الأكثر أهمية وحساسية وهي المناطق غير الصالحة للملاحة وتمتد عبر أوروبا وآسيا، ويعتبرها محصنة من الغزو والاعتداء، ويسمّيها "قلب العالم Heartland"، يحيط بالقلب "الهلال الداخلي Rimland" والذي يشمل معظم المناطق الساحلية لجزيرة العالم والذي يعتبره ماكندر منطقة الحضارة الأكثر كثافة، وأخيراً يأتي الهلال الخارجي أو المحيطي وهو المناطق الأبعد عن قلب العالم.

يرى ماكندر أن حركة التاريخ محكومة بعمليات الصدام التي تسير في اتجاهين، من داخل القلب إلى الخارج (الهلال الخارجي) والعكس عبر ما يسمّيه "قراصنة البر" و"قراصنة البحر"، لتكون منطقة الوسط (الهلال الداخلي) بؤرة التطوير الأفضل للحضارة²، ليقدم في الأخير مقولته الأشهر "من يسيطر على أوروبا الشرقية يحكم قلب الأرض، ومن يسيطر على قلب الأرض يحكم الجزيرة العالمية، ومن يسيطر على الجزيرة العالمية يحكم العالم"³.

إن مساهمة ماكندر الكبرى في الجيوبوليتيك هي إعطاء تصور مبسط للعلاقات الدولية، ونقل الأهمية الجيوبوليتيكية من مجرد الموقع الجغرافي إلى تفاعلات البشر والعمران

¹ الكسندر دوغين، مرجع سابق، ص 93.

² الكسندر دوغين، مرجع سابق، ص 87-88.

³ جيرار ديسوا، مرجع سابق، ص 114-115.

والموارد والاتصالات، هذا إضافة إلى أنه أثبت أن للجيوبوليتيكا القدرة على استيعاب السياق العالمي لحركة التاريخ.

ثالثاً، نيكولاس سبيكمان (1893-1943) : منطقة الحافة

يرى أستاذ العلاقات الدولية الأمريكي سبيكمان أن أمن وسلامة الدولة له ارتباط وثيق بالعوامل الجغرافية، حيث يُرجع فهم السياسة الخارجية للدولة إلى دراسة وفهم موقعها الجغرافي، كما يرى أنه من الناحية الجيوبوليتيكية فإن طبيعة تفاعلات السياسة الدولية وتغير مراكز القوى الدولية يؤثر على القيمة السياسية للموقع الجغرافي¹، حيث يتأثر الأداء السياسي للدولة بتغير علاقاتها بالقوى الدولية وبتغير هذه الأخيرة.

يعالج سبيكمان في كتابه "الاستراتيجية الأمريكية في عالم السياسة الدولية" السلوك الثنائي للولايات المتحدة (السلوك الانعزالي، السلوك التدخل) حيث يرفض بشدة سياسة العزلة، ويقدم مقارنة مؤسسة على الفضاء المادي والموقع الجغرافي مع سيطرة الجغرافيا العسكرية والقوة على أطروحته حتى لقب بـ "هاوسهوفر أمريكي".

يرى سبيكمان أن الجيوبوليتيكا هي الأداة الأكثر أهمية في السياسة الدولية كمنهج تحليل وكنظام للمعادلات تسمح باستنباط الاستراتيجية الأقوى تأثيراً، لذلك سعى لتقديم المعادلة الجيوبوليتيكية الأشد تأثيراً لتمكين الولايات المتحدة من تحقيق السيطرة العالمية بأسرع الطرق².

بنى سبيكمان أطروحته من خلال الطعن في مصداقية القيمة الاستراتيجية لأطروحة "ماكندر" ومنطلقاتها النظرية، حيث يرى أن منطقة "القلب" عند ماكندر تفتقد إلى مؤهلات القيادة³، لذلك فهو يركز على منطقة الريميلاند، فهي حسب سبيكمان منطقة الثقل الرئيسية في صياغة التوجهات نحو السيطرة العالمية، ليخلص إلى القول بأنه: "من يتحكم في حافة الأرض يتحكم في أوراسيا، ومن يتحكم في أوراسيا يتحكم بمصير العالم"⁴.

¹ عبد القادر محمد فهمي، مرجع سابق، ص 94.

² الكسندر دوغين، مرجع سابق، 105.

³ جبرار ديسوا، مرجع سابق، ص 156.

⁴ عبد القادر محمد فهمي، مرجع سابق، ص 96-97.

يؤكد "دوغين" أن سبيكمان هو مهندس النصر الأمريكي، وأن معظم النظريات الجيوبوليتيكية الأطلسية الجديدة إما تطوير لأفكاره أو شرح لها.

المطلب الثالث: الجيوبوليتيكا المعاصرة: إعادة الإحياء

جاءت المرحلة الثانية للجيوبوليتيكا كنتاج لعملية الإحياء التي شهدت عودة هذا العلم إلى الأوساط الأكاديمية، وتميزت بتغييرات مست مستويات التحليل ومجالات البحث الجيوبوليتيكي، إضافة إلى ارتباط الأفكار الجيوبوليتيكية بالدول الكبرى ورؤية كل دولة لمكانتها على الرقعة الجغرافية العالمية، كما ساهم المفكرون كل حسب موقعه على اللوحة الجيوبوليتيكية العالمية في تحديد رؤيته للعالم.

الفرع الأول: جيوبوليتيكا الحرب الباردة

أولاً، هنري ألفريد كيسنجر (1923-...) : سياسي ودبلوماسي أمريكي، شغل منصب وزير الخارجية ومستشار الأمن القومي خلال فترتي الرئيسين نيكسون وفورد، كان له الفضل في إعادة إحياء مصطلح "الجيوبوليتيكا"، حيث عرّفها في المجلد الأول من مذكراته المعنونة بـ "سنوات البيت الأبيض" الصادرة سنة 1979 بقوله: "أعني بالجيوبوليتيكا النهج الذي يهتم بمتطلبات التوازن"¹، وكما يوضح كل جيوفري سلاون و كولين غراي أن كيسنجر استخدم مصطلح الجيوبوليتيك لسببين هما²، أولاً، بوصفها طريقة تحليل لمواجهة السياسات الليبرالية للمثالية الأمريكية، ثانياً، كبديل لسياسات المحافظين وإيديولوجيتهم المناهضة للشيوعية.

قدم كيسنجر في مذكراته دراسة معمقة للعلاقات الدولية والتاريخ المعاصر، حيث برز كرائد في سياسة الانفراج الدولي والعلاقة مع الاتحاد السوفياتي في خضم الحرب الباردة، كما وضح منظوره الجيوبوليتيكي للخروج من فيتنام، وسياسة التقارب مع الصين، غير أن التطبيق الأعلى للجيوبوليتيك كان في ما يسمى "الدبلوماسية الثلاثية" والتي سعت إلى ربط علاقات أوثق مع الصين والاتحاد السوفياتي أقوى من علاقتهما ببعضهما البعض، وهذا ما عزز موقع الولايات المتحدة الاستراتيجي في المنطقة³.

¹ Henri Kissinger, *The White House Years*, Boston: Little Brown, 1979, P 914.

² Geoffrey Sloan & Colin S. Gray, "Why geopolitics?", *Journal of Strategic Studies*, Vol 22, N°2-3, 1999, pp 1-11.

³ Hedley Bull, "Kissinger: The Primacy of Geopolitics", *International Affairs (Royal Institute of International Affairs 1944-)*, Vol 56, N° 3, 1980, pp 484-487.

كما يؤكد كيسنجر ذلك في كتابه "الدبلوماسية" بقوله: "إن تفوق قوة عظمى واحدة على أحد المجالين الأوراسيين -أوروبا وآسيا- يستمر في تقديم تعريف جيد للخطر الاستراتيجي الذي تتعرض له أمريكا سواء بوجود حرب باردة أو بدونها"¹.

ثانياً، زبيغنيو بريجنسكي (1928-2017): مفكر استراتيجي أمريكي ومستشار الأمن القومي لدى الرئيس جيمي كارتر، قام بإحياء أفكار ماكندر حول قلب العالم (الماكندرية الجديدة)، شرح في كتابه "رقعة الشطرنج الكبرى" كيف أن أوراسيا هي محور الحركة الجيوبوليتيكية ومركز الاهتمام الجيوستراتيجي العالمي، إلا أنها تعاني من فراغ استراتيجي، لذلك اعتبر أن السيطرة عليها هي المفتاح لإكمال السيطرة العالمية، حيث يقول: "أوراسيا هي رقعة الشطرنج التي يستمر فيها الصراع من أجل السيادة العالمية"².

دفع خوف بريجنسكي من اجتماع مقومات القوة في أوراسيا للسعي لتجنب أي تقارب بين روسيا وأوروبا (فيما يعرف بإشكالية قلب العالم)، ومن أجل اتقاء انبثاق قوة أوراسية مهيمنة قد تقف في وجه الولايات المتحدة جعل محور الاستراتيجية الأمريكية الاستمرار في الحضور الدائم فوق جزيرة العالم ومراقبة -أو التدخل في- مختلف الصراعات الدائرة فيها، بغرض الحفاظ على توازن أوراسي أو ما دعاه "التعددية الجيوبوليتيكية"³.

يرى بريجنسكي أن الهيمنة الأمريكية ضرورية لاستقرار العالم، لذلك صاغ قاعدتين أساسيتين للاستراتيجية الأمريكية مبنية على تحليل جيوبوليتيكي دقيق لأوراسيا هما⁴، أولاً، تحديد ومعرفة الدول التي تتمتع بديناميكية جيواستراتيجية حقيقية، والتي تكون قادرة على إحداث انقلاب كبير في التوزيع الدولي للسلطة، ثانياً، صياغة سياسات نوعية لموازنة الآثار المترتبة على السياسات المرفوضة التي تتبعها تلك الدول، وهذا في سبيل ضمان أطول مدة للهيمنة الأمريكية.

ثالثاً، الأطلسية الجديدة: بعد نهاية الحرب الباردة والانتصار الباهر للأطلسية وقوى البحر على قلب العالم، برز في الولايات المتحدة الأمريكية توجهان جيوبوليتيكيان يعكسان رؤى الحزبين الكبيرين (الديمقراطيين والجمهوريين)، ممثلين بأبرز مفكرهم؛ فوكوياما وهنتغتون.

¹ جيرار ديسوا، مرجع سابق، ص 166.

² زبيغنيو بريجنسكي، رقعة الشطرنج الكبرى: الأولوية الأمريكية و متطلباتها الجيوستراتيجية، ترجمة: أمل الشرقي، عمان: الاهلية للنشر والتوزيع، 1999، ص 5.

³ جيرار ديسوا، مرجع سابق، ص 154.

⁴ نفس المرجع، ص 163.

أ. يوشيهيرو فرانسيس فوكوياما (1952-...) ونهاية التاريخ : مثل فوكوياما الأستاذ الجامعي وعالم السياسة والاقتصاد الاتجاه التقائي، حيث يرى فوكوياما أن الانتصار الذي حققته الولايات المتحدة والغرب في الحرب الباردة وتشكل عالم أحادي القطب يدل على نهاية الانقسام الإيديولوجي والجيوبوليتيكي للعالم، فالعالم يسير نحو عالم واحد موحد جيوبوليتيكياً، حيث يؤمن الجميع بإيديولوجيا صائبة وصالحة وحتمية، فالديمقراطية الليبرالية قد تشكل نقطة النهاية في التطور الإيديولوجي للإنسانية، والصورة النهائية للحكم البشري، وبالتالي فهي تمثل نهاية التاريخ¹، فنظام مابعد الحرب الباردة هو المرحلة العليا من تطور البشرية.

ب. صامويل فيليبس هنتغتون (1927-2008) وصدام الحضارات: يقدم العالم والسياسي الأمريكي البروفيسور هنتغتون رداً على أطروحة فوكوياما - نظرة تشاؤمية لعالم مابعد الحرب الباردة، فهو يرى أن الانتصار الجيوبوليتيكي الظاهري للأطلسية (الولايات المتحدة والغرب) ليس انتصاراً حضارياً، فسرعان ما ستطفو خصائص حضارية وجيوبوليتيكية لدى الشعوب غير الغربية، نظراً لتحررها من القوالب الإيديولوجية السابقة، وسيكون الصراع بين جماعات من حضارات مختلفة هو البعد الأخطر في السياسة الكونية الجديدة².

فالنصر في الحرب الباردة لم يُلغِ أبداً الخطر على الغرب، هذا الخطر ينبثق من تشكيلات جيوبوليتيكية أخرى موجودة أو في طريقها للظهور، فحضارات العالم تطورت في خط مواز لتطور الأطلسية والحضارة الغربية، ما يؤهلها لاتخاذ وضعية المواجهة من جديد، لذلك فإن الصيغة الجيوبوليتيكية التي يتبناها هنتغتون هي صيغة "الغرب والآخرين"³.

ومن أجل المواجهة القادمة يضع هنتغتون خطة عمل تعتمد على تدعيم الجبهة الأطلسية (أوروبا وأمريكا) ومحاولة إضعاف الحضارات الأخرى وتقويتها خاصة الحضارة الكنفوشيوسية (الصين) والحضارة الإسلامية واللتين يعتبرهما أخطر الأعداء المحتملين للأطلسية⁴.

الفرع الثاني: الجيوبوليتيكا الداخلية (المدرسة الفرنسية)

بدأت المدرسة الجيوبوليتيكية الفرنسية مع أفكار فيدال دي لابانش Vidal de la blanche التي جاء بها كرد على حتمية المكان عند راتسيل، حيث يرى لابانش أن الإنسان (الحرية

¹ فرانسيس فوكوياما، نهاية التاريخ وخاتم البشر، تر: حسين احمد امين، القاهرة: مركز الاهرام للترجمة والنشر، 1993، ص 8.

² صمويل هنتغتون، صدام الحضارات إعادة صنع النظام العالمي، تر: طلعت الشايب، ط2،، 1999، ص 29.

³ ألكسندر دو غين، مرجع سابق، ص 159.

⁴ نفس المرجع، ص 161-162.

(الإنسانية) هو صاحب المبادرة في تفعيل إمكانية إعطاء الدور المهم للمساحة الجغرافية في التاريخ السياسي، وهذا ما يعتبره دوغين تصحيحاً للحتمية الجغرافية الألمانية¹.

وكانت الإضافة الأهم للمدرسة الفرنسية تلك التي جاء بها "إيف لاکوست Ives lacoste" المفكر اليساري المهتم بقضايا التنمية والعالم الثالث، والذي يُعد "أب الجيوبوليتيكا الفرنسية"، حيث قدم من خلال مجلته "هيرودوت Herodote" تعريفاً جديداً للجيوبوليتيكا يُظهر من خلاله عدم اتفاهه مع منظري المدرسة العضوانية الألمانية ومنظري البراغماتية الأنجلوساكسونية في آن واحد، حيث يحدد "لاکوست" بدقة أن مصطلح الجيوبوليتيكا يشير إلى: "جميع ما يتعلق بتنازع السلطات أو النفوذ على الأقاليم وعلى الشعوب التي تقطن فيها، تنازع بين القوى السياسية من مختلف الأشكال"، فـ"لاکوست" نقل مستوى التحليل الجيوبوليتيكي من العالمي إلى المحلي، وكان الاهتمام الرئيس لمجلة "هيرودوت" على قضايا "جيوبوليتيك الأمة" وضمن السياق الفرنسي الخالص، ويضيف "ديسوا"² أن التحليل الجيوبوليتيكي لاکوست-هيرودوت قدم الوقائع على الأفكار، وكان التركيز ليس فقط على فهم الصراعات (النزاع على السلطة والنفوذ) بين الدول فحسب، بل داخل الدولة نفسها، هذا ما جعل "دوغين"³ يعتبر أن هذه الجيوبوليتيكا الداخلية لاعولمة للجيوبوليتيكا، ودعا إلى استبعادها من حقل الجيوبوليتيكا لأنها مجرد منهجية تحليلية سياسية وسوسيولوجية.

الفرع الثالث: الجيوبوليتيكا النقدية

ظهرت مدرسة الجيوبوليتيكا النقدية كتيار جديد لإعادة تأهيل وتطوير الجيوبوليتيكا التقليدية وتخليصها من السرديات الأرثوذكسية معتمدة على تفكيكية جاك دريدا وميشال فوكو، حيث عملت على التقليل من أهمية الحتمية الجغرافية نحو تعزيز دور العوامل السيوسولوجية في العلاقات الدولية، حيث يشير الأستاذ جيراو أوتوايلا Gearóid Ó Tuathail إلى أن الجغرافيا لاتعد نتاجاً للطبيعة وإنما نتاجاً لتاريخ من الصراع بين سلطات متنافسة حول القوة/السلطة لتنظيم العالم، احتلاله وإدارته⁴، كما يقسم أوتوايلا الجيوبوليتيكا النقدية إلى أربع مناهج بحثية (الجيوبوليتيكا الرسمية، العملية، الهيكلية، الشعبية)⁵، كما يضيف كولن فلنت أن الجيوبوليتيك النقدي يسعى

¹ نفس المرجع، ص 102.

² جيرارديسوا، مرجع سابق، ص 205.

³ ألكسندر دوغين، مرجع سابق، ص 174.

⁴ أغنيشكا لغوتسكا، مرجع سابق، ص 10.

⁵ Tuathail Gearóid Ó, "Understanding critical geopolitics: Geopolitics and risk society", **Journal of Strategic Studies**, Vol 22, N° 2, 1999, p 111.

لفهم الآليات والقوانين الجيوبوليتيكية للدول (من هم الأعداء؟ من هم الحلفاء؟ كيف نبرر ذلك للجمهور وللمجتمع الدولي؟) من خلال منظور "التحالف"، والجزء الأهم هو تبرير ذلك للناخبين وللمجتمع الدولي من خلال دراسة الجيوبوليتيكا الشعبية، إذ أنه في زمن العولمة والفضاء السيبراني صارت النزاعات في الأماكن البعيدة جغرافياً أمراً يهم الجمهور ويتأثر به، ويرتبط هذا بظاهرة تخیل المكان أو ما يسمى "الجغرافيا الماورائية Meta-geography".

المطلب الرابع : التحليل الجيوبوليتيكي والمدرک الاستراتيجي

الفرع الأول: منهج التحليل الجيوبوليتيكي

يعد التحليل الجيوبوليتيكي أحد المقاربات النظرية الأكثر شهرة في تحليل السلوك الصراعي للدول، والصراع الدولي بشكل عام، واعتمدت المقاربة الجيوبوليتيكية في نسختها التقليدية "الدولة" كمستوى أساسي للتحليل، ثم توسعت إلى مستويات تحت وعبر وفوق وطنية في نسختها المعاصرة (خاصة النقدية)، ويقدم التحليل الجيوبوليتيكي استبصارات وفهوما متميزة لكل من السياسيين والعسكريين ويسمح لهم بوضع الاستراتيجيات والسياسات المناسبة من خلال تقدير الأمكنة/الأقاليم التي تحدث/أو يمكن أن تحدث فيها الصراعات والصدامات حول المصالح والنفوذ.

يستفيد الباحثون من المقاربة الجيوبوليتيكية في تحليل القضايا الأمنية المتعلقة بقضايا النزاع، التنافس، الصراع، الهيمنة، النفوذ والمصالح، الإرهاب وتوازن القوى، حيث تنقل أغنيشكا لغوتسكا في جدالها حول فائدة المنظور الجيوبوليتيكي عن كارل جين أن الجيوبوليتيكا أداة جيدة للبحث في السياسة العالمية، لأنها تمنحنا منهجية أولية لمتابعة المشكلات المحددة المتعلقة بالمكان، الإقليم الأرضي، الجغرافيا ومجالات النفوذ¹، كما تجدر الإشارة إلى أن الجيوبوليتيكا النقدية فتحت آفاقاً ومجالات جديدة للبحث فكتاب دومينيك مواسييه "جيوبوليتك العواطف" وسع اهتمام الجيوبوليتيك من الجغرافيا والسياسة إلى العاطفة والشعور، إضافة إلى أن كولن فلنت عند حاجته عن الجيوبوليتيكا كان يقصد التحالفات والإجابة عن الأسئلة من قبيل: من أنا؟ من أقاتله؟ لماذا؟² وليس المساحة الأرضية في حد ذاتها.

¹ أغنيشكا لغوتسكا، مرجع سابق، ص 16.

² Flint Colin, *Introduction to geopolitics*, Routledge, 2006, p 190.

في نفس السياق، وبتتبع مسار تطور منهج التحليل الجيوبوليتيكي نجد أنه بدأ على أساس جغرافي بحث أو ما عُرف بالحنمية الجغرافية، حيث تحدد الجغرافيا مصير الدول والعالم، ثم تطور لاحقاً مع عمليات الإحياء والنقد إلى مستويات تحليل متباينة (محلي، إقليمي، عالمي) وانتقل من التركيز على المساحة الأرضية إلى التركيز على علاقات القوة بشتى تمثلاتها، صلبة كانت أو ناعمة، ومختلف جوانبها العسكرية والسياسية والاقتصادية والحضارية والتكنولوجية، وتقصي الكيفية التي يساهم بها المجال أو الفضاء (سواء كان رقعة جغرافية أو إقليمياً أو وطنياً متخيلاً) في تحديد وتوجيه تفاعلات القوة بين مختلف الفاعلين.

من جهة أخرى، يدور محور التحليل الجيوبوليتيكي حول قضية ما أو مشكلة ما أو ما يسميها لأكوست "الوضعية الجيوبوليتيكية"، حيث تنشأ المشكلة الجيوبوليتيكية وتتطور في إطار التفاعلات الجغرافية السياسية للمجال، كما تتأثر بالعوامل الإقليمية والدولية حسب أهمية هذا المجال ومدى تداخل مصالح القوى الفاعلة فيه، وبناءً على ذلك يشترط لأكوست لاعتبار قضية ما وضعيةً جيوبوليتيكية وجود إقليم تتصارع فيه قوى فاعلين أو أكثر، إضافة إلى مسار تاريخي يرصد علاقات القوة بين الفاعلين.

وإضافة إلى ما سبق، يشمل التحليل الجيوبوليتيكي ثلاثة (03) أبعاد أو مرتكزات رئيسية هي: جوهر الحدث، عامل الحدث، بيئة الحدث¹.

1. تحليل جوهر الحدث ويقصد به معرفة مسببات المشكلة الداخلية (جغرافية، بشرية، اقتصادية، حضارية) داخل مجالها سواء كان دولة أو إقليمياً أو فضاءً متخيلاً، ومن ثم ربط المشكلة بسياسة الدولة / أو الدول ذات الصلة المباشرة بها، وأخيراً انعكاسات المشكلة على المستويين الإقليمي والدولي.

2. تحليل عامل الحدث بفهم طبيعة ومدى تأثير القوى والعوامل (إقليمية أو دولية) التي تتدخل في الحدث (التدخلات الخارجية) بمختلف الوسائل والتقنيات وتدفع به باتجاه التصعيد أو التهدئة.

3. تحليل بيئة الحدث داخل مجالها الجغرافي الجيوبوليتيكي الإقليمي والعالمي، بتحديد الفاعلين الخارجيين ومصالحهم (خاصة القوى الكبرى)، وانعكاس ذلك على الأمن المحلي والدولي، وأثر المشكلة على العلاقة بين الدول والتحالفات بينها وتوازن القوى، وتأثيرها على إعادة تشكيل الأقاليم الجيوبوليتيكية القائمة.

¹ فؤاد حمه خورشيد، الجيوبوليتيك المعاصر تحليل، منهج، سلوك، مؤسسة هنداوي للتعليم والثقافة، 2013، ص 26.

وخلاصة لذلك، فعملية الربط في التحليل بين جوهر وعامل وبيئة الحدث تعد جوهرية في التحليل الجيوبوليتيكي المعاصر، ناهيك عن الإلمام بالبيانات الجغرافية والبشرية والاقتصادية والتكنولوجية، مع القدرة على رسم السيناريوهات وتحديد الاتجاهات المستقبلية للمشكلة، حيث يتم التحليل في إطار النظام الدولي وتوجهاته والدور الذي تلعبه القوى الكبرى، دون إغفال تكنولوجيا المعلومات والاتصال كما يؤكد ذلك ماكندر بمقولته "لكل قرن منظوره الجيوبوليتيكي الخاص"¹.

الفرع الثاني: المبادئ الجيوبوليتيكية والمدرک الاستراتيجي

تماشياً مع ما تم ذكره سابقاً، فالجيوبوليتيكا رؤية للعالم، حيث يعتمد بناء ونجاح الاستراتيجيات العامة للدول على قدرتها في وضع المبادئ الجيوبوليتيكية الملائمة لوضعها في النظام الدولي، فاستراتيجية الأمن القومي للدولة هي نتاج فهم ودقة الثلاثية (الدور، الإدراك الاستراتيجي، المبادئ الجيوبوليتيكية)، فالمبادئ الجيوبوليتيكية كما يعرفها بيتر تايلور وكولن فلنت هي مجموعة الفرضيات الاستراتيجية التي تضعها حكومة ما فيما يتعلق بالدول الأخرى في صياغتها لسياستها الخارجية²، أو هي الكيفية التي يُوجه بها بلد ما نفسه تجاه العالم³، حيث تنطوي هذه الفروض الاستراتيجية الإجرائية على تحديد وتقييم للمجالات والمناطق الجغرافية خارج حدود الدولة وإدراك أهميتها الاستراتيجية الحالية والمستقبلية (هل هي تهديد يجب مواجهته أم هي فرصة لبسط النفوذ والسيطرة)، لذلك توصف المبادئ الجيوبوليتيكية للدول على أنها وحدات البناء الأساسية للنظم الجيوبوليتيكية العالمية.

يقدم فلنت انطلاقاً من رؤيته للجيوبوليتيكا القائمة على التحالفات خمسة محاور رئيسية لعملية تقييم المجالات والمناطق الجغرافية هي⁴:

1. من هم حلفاؤنا الحاليون والمحتملون.
2. من هم أعداؤنا الحاليون والمحتملون.
3. كيف نحافظ على حلفائنا الحاليين ونستقطب الحلفاء المحتملين.

¹ Donald W. Meinig, "Heartland and rimland in Eurasian history", **Western Political Quarterly**, Vol 9, N° 3, 1956, p 553-569.

² بيتر تايلور وكولن فلنت، مرجع سابق، ص 164.

³ Collin, **Op.cit**, p 55.

⁴ **Ibid**, p 56.

4. كيف نواجه أعداءنا الحاليين والتهديدات المستجدة.

5. كيف نبرر نتائج تقييماتنا الأربعة السابقة لجمهورنا وللمجتمع الدولي.

ويولي فلنت أهمية كبرى للعنصر الأخير، حيث إن فشل الحكومة في تبرير تعريفها للعدو خاصة إذا كانت هناك دعوات للحرب قد يُفشل استراتيجيتها العامة ويعصف باستقرارها، ويقدم أمثلة على ذلك بالحكومتين الإسبانية والبريطانية في تحالفهما في الحرب على العراق في 2003.

من جهة أخرى، يحدد فلنت ثلاث مستويات للمبادئ الجيوبوليتيكية: المحلي والإقليمي والعالم، فكل الدول لها رؤية محددة لجيرانها المباشرين، والعديد من الدول لها مطامع للنفوذ داخل إقليمها، أما قادة العالم (القوى الكبرى) فلها مبادئ جيوبوليتيكية عالمية تتناسق مع إدراك صانع القرار فيها للدور¹ الذي تلعبه في النظام الدولي، هذا الأخير (أي الدور) يعتبر علامة بارزة للمبادئ الجيوبوليتيكية للدول الكبرى حيث يشتمل على ثلاثة (03) أبعاد رئيسية هي:

1. إدراك صانع القرار وتصوره لمجالات نفوذ دولته، ودرجة هذا النفوذ.

2. تصور صانع القرار للدوافع الرئيسية للوحدة الدولية، وتفاوتها بين التعاون والصراع.

3. توقعات صانع القرار لحجم التغيير المحتمل في النظام الدولي نتيجة أداء دور معين (قوة مهيمنة، قوة صاعدة، قوة تعديلية)².

¹ وضح هولستي كيف أن الأدوار عبارة عن متغيرات سببية في تفسير كيفية عمل النظام الدولي، مع تركيزه على أدوار الدول الصغيرة، كما بين أن الدور وحده غير كاف لمعرفة كل المهام التي تقوم بها الدولة في النظام الدولي للمزيد يرجى الاطلاع على المقال: Kalevi J. Holsti, "National role conceptions in the study of foreign policy", **International studies quarterly**, Vol 14, N°3, 1970, pp 233-309.

² للمزيد حول إدراك الوحدة الدولية لدورها كقوة صاعدة أو مهيمنة أو تعديلية يرجى الاطلاع على كتاب: النضال من أجل الاعتراف في العلاقات الدولية: القوى الراهنة والتعديلية والصاعدة، ميشيل موراي، 2019، والتي بحثت إشكالية كيف يمكن أن تدير قوة الوضع الزاهن الصعود السلمي لقوى جديدة؟ حيث تخلص إلى أن استمرارية حالة عدم اليقين تعرقل التعاون الدولي، حيث تسعى فيه القوى التعديلية للحصول على الاعتراف بدورها كقوى كبرى.

وعليه، فإن صياغة المبادئ الجيوبوليتيكية تتطلب إدراكاً وفهماً للعلاقة بين الدولة والبيئة الدولية أو السياق الدولي، حيث يلعب الإدراك الاستراتيجي دوراً رئيساً في توفير جملة من العوامل لتحليل البيئة الدولية منها¹:

1. تحديد طبيعة وخصائص النظام الدولي، من حيث نوعية الفرص والتهديدات المنبثقة.
 2. الطرق المتاحة للاستفادة من الفرص ومواجهة التهديدات خدمة لمصالح الدولة.
 3. مدى تأثير البيئة الدولية على سلوك الدول حسب قدراتها وإمكانياتها المتباينة، وقدرتها على المناورة بالوسائل المتاحة لها.
- وبناءً على ما تقدم، فإن المبادئ الجيوبوليتيكية تحدد وتوجه صانع القرار لبناء الاستراتيجيات العامة للدولة -خاصة استراتيجيات الأمن القومي- من أجل بلوغ الأهداف وتحقيق المصالح ذات الأهمية الحيوية.

¹ عادل البديوي، الإدراك الاستراتيجي للولايات المتحدة الأمريكية: دراسة في المبادئ الجيوبوليتيكية، عمان: دار الجنان للنشر والتوزيع، 2015، ص 85.

المبحث الثاني: الفضاء السيبراني بُعد جديد في العلاقات الدولية

بدأت الأنترنت كمشروع عسكري داخل وكالة مشاريع البحث المتقدمة الأمريكية (ARPA) وحين نجح العلماء في ربط كمبيوتر جامعة كاليفورنيا في لوس أنجلوس بكمبيوتر شركة BBN للتكنولوجيا في جامعة كامبريدج، لم يخطر على بالهم أنه بعد خمسين 50 سنة سيتحول هذا الإنجاز إلى أكبر شبكة عبر العالم وما أصبح يعرف بـ "الفضاء السيبراني" والذي سيربط ما يقارب خمسة 5 ملايين من سكان العالم، أي أكثر من 60% من البشر¹، وأكثر من أربعين 40 مليار جهاز²، لقد أصبح الفضاء السيبراني حقيقة يومية للأفراد والمجتمعات، كما أضحت يُحدد ويُشكل السياسة العليا للدول من خلال التحديات التي يفرضها على الأمن القومي والأثر الذي يتركه على أنظمة صنع القرار، ذلك أنه خلق نوعاً جديداً من القوة التي تتوزع وتنتشر بين العديد من الفاعلين الجدد على الساحة الدولية، مما سرع بظهور أنواع جديدة من الصراع حول النفوذ والهيمنة.

المطلب الأول : مفهوم الفضاء السيبراني، خصائصه وفواعله

يعد الفضاء السيبراني فضاءً (عالمًا، مجالاً) جديداً من صنع البشر، حيث تشكل في خضم التطور السريع الذي عرفته تكنولوجيا المعلومات والاتصال ICT في العقود الثلاثة الماضية، وتشكل من التشبيك المكثف والتفاعل الديناميكي لكل من الآلات والبشر والبيانات.

من الناحية الإيتومولوجية، ورد مصطلح الفضاء السيبراني "Cyberspace" بداية في روايتي الخيال العلمي "Burning Chrome" سنة 1981 و "Neuromancer" سنة 1984، للكاتب وليام جيبسون، حيث وصف عالماً يتكون من مزيج من البشر والآلات يعيش فيه المشغلون الشرعيون هلوسة توافقية يومية³، ثم استخدم المصطلح لاحقاً لوصف كل ما يتعلق بالشبكات.

وتجدر الإشارة إلى أن أصل كلمة سايبير "Cyber" تعود إلى الفعل $\kappa\upsilon\beta\epsilon\rho\epsilon\omega$ (kybereo) والذي يعني في اللغة اليونانية القديمة يوجه، يرشد، يتحكم...، وقد ورد مصطلح Cybernetics

¹ الإحصائيات مأخوذة من تقارير موقع wearesocial المتخصص في إعداد الإحصائيات والتقارير حول كل ما يتعلق بالانترنت والهاتف المحمول حول العالم (تاريخ زيارة الموقع 2021-11-29).

² حسب إحصائيات شهر مارس 2021 لموقع Statista فإن عدد أجهزة انترنت الأشياء سيفوق 30 مليار جهاز إضافة إلى أجهزة الكمبيوتر والهواتف المحمولة والشبكات الذي يفوق 10 ملايين جهاز.

³ Binxing Fang, Fang Zhang, **Cyberspace sovereignty**, Springer Singapore, 2018, p 13.

في أعمال نوربارت فاينر حول علم التحكم الآلي والاتصال بين الحيوان والآلة¹، حيث يقدم فكرة إمكانية التحام الإنسان بالآلة لتشكيل بيئة بديلة للتفاعل.

أما كلمة فضاء "Space" فالمفهوم يختلف باختلاف مجال البحث، فالرياضيات تعتبره مجاًلاً ثلاثي الأبعاد، والفيزياء تضيف له الحركة والزمن ليذل على الزمكان، وفي دراستنا هذه نركز على المفهوم الذي تطرحه الفلسفة الاجتماعية من خلال أفكار هنري لوفيفر² و ديفيد هيني³ حيث ركزا على البعد الاجتماعي للفضاء ليصبح منتجاً اجتماعياً ومجاًلاً لتفاعل الإنسان مع المكان، أي أن مفهوم الفضاء يستند إلى واقع السلوك البشري وممارسات الإنسان فيه.

أما من الناحية الاصطلاحية، فلا يوجد اتفاق بين الباحثين أو الهيئات الوطنية وحتى الدولية على مفهوم موحد للفضاء السيبراني، وذلك راجع لتباين فهم وإدراك كل طرف لهذا الفضاء الجديد، إضافة إلى اختلاف الاستراتيجيات المتبعة للاستفادة من مزاياه المتاحة ومواجهة التحديات والمخاطر التي يفرضها⁴، فمن منظور تقني هناك من يعرفه على أنه فضاء التواصل المشكل من خلال الربط البيئي العالمي لمعدات المعالجة الآلية للمعطيات الرقمية⁵، ومن منظور التنافس والصراع هناك من يعرفه على أنه مجال الحرب الخامس بعد الأرض، البحر، الجو والفضاء الخارجي أو هو الذراع الرابعة للجيش⁶. لذلك، ولأغراض هذه الدراسة نستعرض تعريفات للاتحاد الدولي للاتصالات ITU كهيئة دولية متخصصة، إضافة إلى تعريفات لهيئات رسمية في كل من الولايات المتحدة الأمريكية والصين.

¹ Norbert Wiener, **Cybernetics or Control and Communication in the Animal and the Machine**, MIT press, 2019, p14.

² Lefebvre Henri, **La production de l'espace**, Éditions Anthropos, 1986, p 15.

³ David Harvey, **Time-space compression and the postmodern**, Modernity: After Modernity, 1999, 98-118.

⁴ صنف كل من Zhang و Binxing ما يقارب 40 تعريفاً مختلفاً للفضاء السيبراني من طرف الدول والهيئات حسب درجة تركيز كل مفهوم حول: البنية التحتية، البيانات، المستخدمين و العمليات، للمزيد يرجى الاطلاع على:

Binxing Fang, Fang Zhang, **Op.cit**, p 17-27.

⁵ Olivier KEMPF, **Introduction à la Cyberstratégie**, Paris, Economica, 2012, P 9.

⁶ عباس بدران، **الحروب الالكترونية: الاشتباك في عالم متغير**، بيروت: مركز دراسات الحكومة الالكترونية، 2010، ص4.

يعرف الاتحاد الدولي للاتصالات ITU الفضاء السيبراني بأنه " المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي: أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكم، ومستخدمو كل هذه العناصر"¹.

وفي الولايات المتحدة الأمريكية، تقوم لجنة أنظمة الأمن القومي CNSS بإعداد مرجع موحد للمصطلحات الواجب استعمالها في الوثائق والتقارير الخاصة بالأمن القومي، وهو ملزم لجميع الإدارات والهيئات الأمريكية تجنباً للتعارض في استعمال المصطلحات، وقد جاء تعريف الفضاء السيبراني في آخر تحديث لها في التعليمات رقم CNSSI No. 4009 الصادرة بتاريخ 06 افريل 2015 على أنه " الشبكة المترابطة للبنى التحتية لتكنولوجيا المعلومات، وتشمل الأنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعالجات ووحدات التحكم المدمجة في الصناعات الحيوية"².

أما في الصين، لا يستعمل الأكاديميون ولا الحكومة ولا الجيش الصيني مصطلح Cyber بالمفهوم الغربي، وبدلاً منه يستعمل جيش التحرير الشعبي PLA الصيني في وثائقه وتقاريره مصطلحي "المعلومات Information" و "الشبكات Network"، فمثلاً مصطلح الأمن السيبراني Cybersecurity في الغرب يقابله مصطلح أمن المعلومات Information security أو أمن الشبكات Network Security عند الصينيين³، لذلك يمكن الاستئناس بما ورد في الاستراتيجية الصينية لأمن الفضاء السيبراني الصادرة في 2016 حيث وصفت الفضاء السيبراني بالتالي: " في أعقاب التطور السريع لثورة المعلومات، يعمل الفضاء السيبراني المكون من الأنترنت وشبكات الاتصالات السلكية واللاسلكية وأنظمة الكمبيوتر وأنظمة التحكم المؤتمتة والمعدات الرقمية والتطبيقات والخدمات والبيانات التي تحملها، حالياً على تغيير حياة الناس وطرق إنتاجهم بشكل شامل، ويؤثر تأثيراً عميقاً على عملية تطوير تاريخ المجتمع البشري"⁴.

¹ The International Télécommunication Union, ITU Toolkit for Cybercrime Legislation, Geneva, 2010, P 12.

² لجنة أنظمة الأمن القومي، تعليمات رقم CNSSI N°4009، بتاريخ 06 افريل 2015، ص40، على الرابط: <https://bit.ly/3KTV3e2> تاريخ الاطلاع: 2021-12-01.

³ Chang Amy, Warring State China's Cybersecurity Strategy, December 2014, p 13-14.

⁴ جمهورية الصين الشعبية، المكتب الوطني لمعلومات الإنترنت الاستراتيجية الوطنية لأمن الفضاء الإلكتروني، الاستراتيجية الوطنية لأمن الفضاء الإلكتروني، على الرابط: <https://bit.ly/45EbcYl>. تاريخ الإطلاع: 2021-12-01

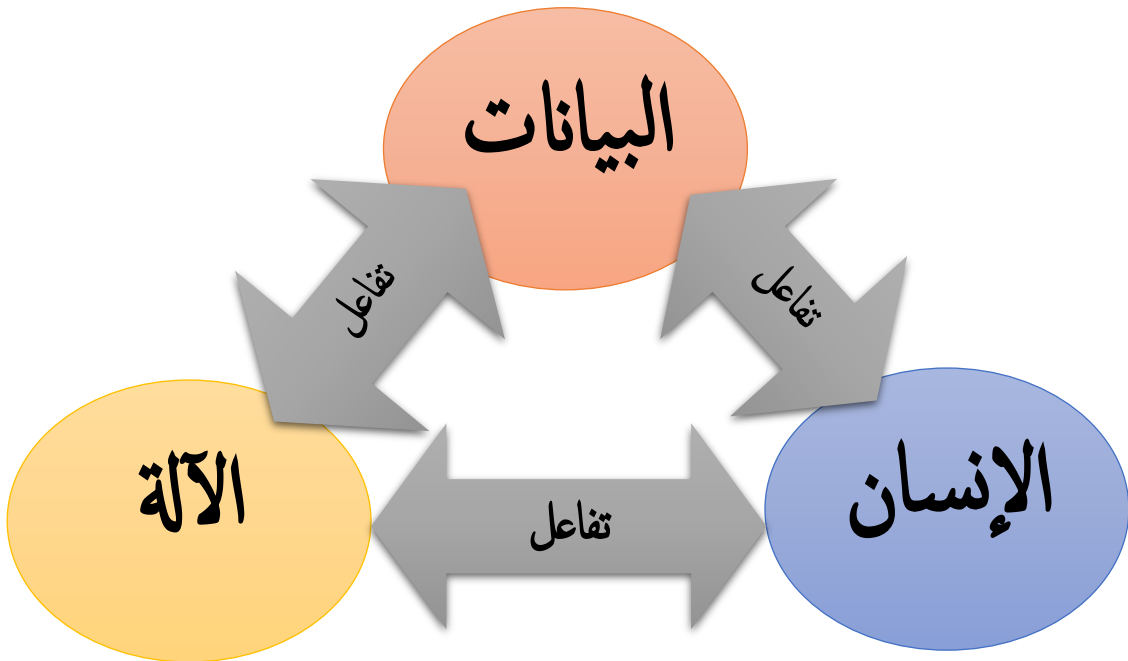
من خلال التعريفات السابقة وتقصي التعريفات المختلفة للدول والهيئات يمكن أن نحصر أربعة (04) أبعاد أو مكونات رئيسية للفضاء السيبراني وهي:

1. البنية التحتية (Infrastructure): وتشمل جميع أنظمة الكمبيوتر، الهواتف النقالة، شبكات الاتصال السلكية واللاسلكية، شبكات التلفزيون والراديو، أنترنت الأشياء، شبكات المراقبة والحساسات، الشبكات الصناعية... إلخ.
2. البيانات (Data): كل الإشارات الرقمية بكل أنواعها، التي ينتجها الإنسان أو الآلة، ويمكن تخزينها، نقلها، تعديلها أو حذفها.
3. المستخدمون (Users): سواء كانوا من البشر (مطورون، مشغلون، مستعملون) أو من الآلات (روبوتات أو غيرها).
4. التفاعل أو العمليات (Interaction/Operations): وتشمل جميع النشاطات والسلوكيات في الفضاء السيبراني.

وخلاصة لما سبق، يُمكن تعريف الفضاء السيبراني تعريفاً مختصراً شاملاً لكل الأبعاد السابقة فنقول أنه " فضاء تتفاعل فيه الآلات والبشر والبيانات".

شكل رقم 01 - نموذج تمثيلي للفضاء السيبراني.

المصدر: من تصور وإعداد الباحث.



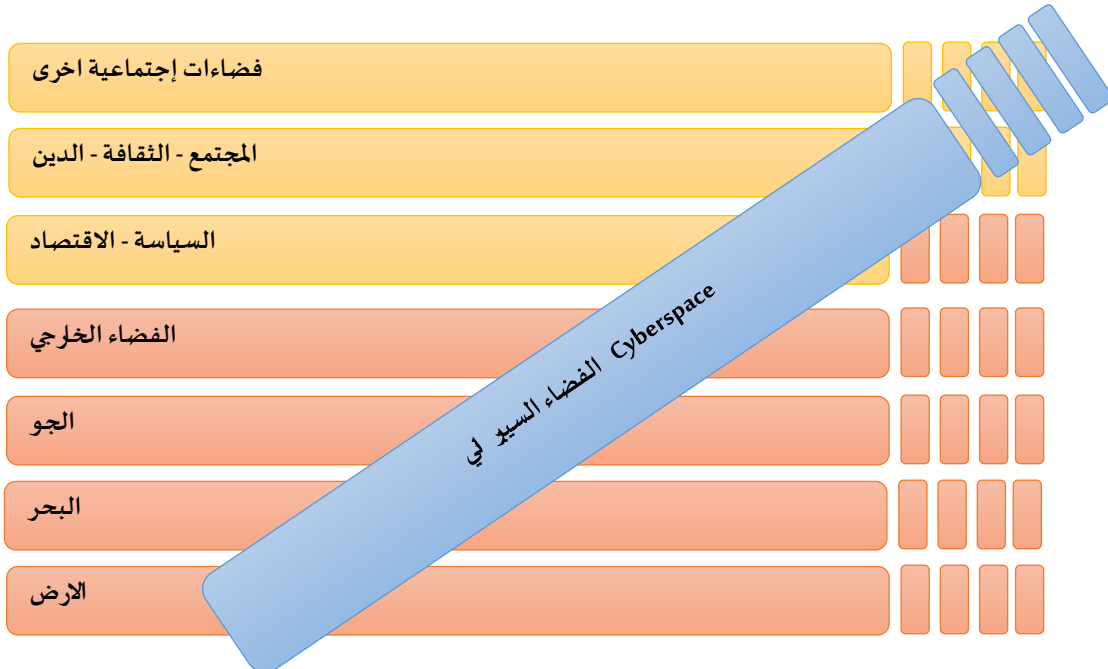
هذا التفاعل الديناميكي بين هذه الأبعاد يعطي للفضاء السيبراني خصائص فريدة ومميزة، فهو في الوقت ذاته يمثل للأفراد والمجموعات والحكومات منجماً للفرص لخدمة مصالحهم، ومصدراً للتهديدات والمخاطر.

لذلك يمكن أن نجمل خصائص الفضاء السيبراني في النقاط التالية:

- ✓ **اللامركزية**، حيث إن الفلسفة التي بنيت عليها الأنترنت في البداية تقوم على لامركزية التسيير والقيادة، حتى أن البعض دعا إلى استقلال الفضاء السيبراني¹.
- ✓ **اللحظية أو الوقتية**، وعدم الوثوقية فالفضاء السيبراني دائم التغير والتبدل، فعمليات التغير في أبعاده تتم بسرعة الضوء.
- ✓ **الاختراق والتغلغل**، يتجاوز الفضاء السيبراني قيود الجغرافيا والحدود، ويتعدى الفوارق الاجتماعية والاختلافات السياسية والدينية والثقافية، فهو يتخلل ويشمل جميع الفضاءات المادية والاجتماعية.

شكل رقم 02: تغلغل الفضاء السيبراني عبر الفضاءات المادية والقيمية.

المصدر: من تصور وإعداد الباحث.



¹ John Perry Barlow, **A Declaration of the Independence of Cyberspace**, Switzerland, 1996, URL: <https://bit.ly/3OL7W6O>, seen at: 02-12-2021.

✓تجاوز المساءلة والمسؤولية، إن إثبات الأفعال (الإسناد) في الفضاء السيبراني عملية صعبة ومعقدة، وذلك بسبب المجهولية كصفة أساسية للفاعلين، فحجب هويات الفاعلين تجعل من إسناد العمليات عملية صعبة التحقيق.

المطلب الثاني: علاقة التأثير والتأثر بين الفضاء السيبراني والعلاقات الدولية

جعلت ميزة الانتشار والتغلغل من الفضاء السيبراني حقيقة واقعية يومية في حياة الأفراد والمنظمات والدول، فالملاحظ أن عمليات التحول الرقمي في المجالات السياسية والاقتصادية والاجتماعية تتزايد بسرعة كبيرة، كما أن اعتماد الجهات الفاعلة في العلاقات الدولية على البنية التحتية ووسائل وأدوات الفضاء السيبراني جعل آثاره جلية في السياسة الدولية، الاقتصاد العالمي والعلاقات الاجتماعية، وعليه فقد انتقل الاهتمام بالفضاء السيبراني من مجال "السياسة الدنيا" إلى دائرة "السياسة العليا"¹ وتكثفت الأبحاث حول فهم وتشخيص علاقته وتأثيره على قضايا الحرب والسلام، الأمن القومي، التعاون والصراع، مصالح الدولة وقيمها، وذلك من خلال محاولة تطويع (تعظيم الفرص وتقليل التهديدات) الفضاء السيبراني لخدمة مصالح الدولة.

وتفسيراً لما سبق، فإن علاقة التأثير المتبادلة بين الفضاء السيبراني والعلاقات الدولية يمكن فهمها من خلال التطرق إلى بُعدين رئيسيين، أولاً على مستوى **التنظير**، وذلك بالتساؤل عن مدى جدوى النظريات والمقاربات الكلاسيكية في فهم وتفسير والتنبؤ بسلوكات وتفاعلات الجهات الفاعلة الدولية في العصر الرقمي، أم نحن بحاجة لمقاربات جديدة ، ثانياً على مستوى **السياسات والممارسات**، وذلك برصد التطورات والتحولات في قضايا السياسة الدولية، سواء من ناحية نوع القضايا والمستجد منها، أو طريقة التعامل معها من طرف الفاعلين الدوليين.

الفرع الأول: على مستوى التنظير

يتساءل بعض الباحثين، هل مازالت النظريات الكلاسيكية مهمة في عالم الفضاء السيبراني؟ وهل مازال لآراء الاستراتيجيين الأوائل أمثال "كلاروفيتش" و"صن أتزو" مكان في توفير خيارات

¹ Nazli Choucri, *Cyberpolitics in international relations*, MIT press, 2012, p 03.

لصانعي السياسات، وتقديم نظرة ثاقبة لطبيعة الحرب والصراع والتعاون والسياسة في العالم الرقمي؟¹

تستدعي الإجابة على هذا السؤال فحص الكيفية التي ساهمت بها التطورات التكنولوجية في ظهور سلوكيات وتفاعلات جديدة بين المجتمعات والدول، فمنذ بداية تشكل الفضاء السيبراني برزت روايتان متباينتان² رغم اتفاقهما على أن **الفوضى** هي السمة المميزة لهذا الفضاء الجديد.

يُشير **الليبراليون بقيادة التقنيين والاكاديميين** بفضاء الحرية وتشارك المنفعة، ويرون أن إضفاء الطابع الديمقراطي على الفضاء السيبراني يتم عبر التعاون الدولي المُركّز، من خلال التنظيم المشترك -أو ما تسميه الليبرالية الأمن الجماعي- ضد السلوكيات المعادية للفواعل المختلفة تحت شعار "دعو التكنولوجيا تعمل"، فالفضاء السيبراني عند الليبراليين "مشاع" يتجاوز الحدود الإقليمية وهو ملك للجميع بما يوفره من "حرية الوصول للمعلومات"، كما يرون أن أمن المعلومات أو الأمن السيبراني كبعد جديد من أبعاد الأمن الدولي "سلعة جماعية" يجب أن يدعمها الجميع من خلال تطوير معايير وقواعد الأنترنت، ويدّعي **جوزيف ناي** أن الفضاء السيبراني يقع في المنطقة الرمادية بين الحرب والسلم³، ويُرجع ذلك إلى غياب معايير دولية مشتركة للأنترنت، لذلك فغالبا ما يدعو إلى التعاون لوضع معايير وقواعد سلوك دولية لتنظيم هذا الفضاء⁴.

لكن يبدو أن إطار التعاون الدولي والأمن الجماعي الذي يطرحه الليبراليون ضبابي إلى حد ما، خاصة أن المجهولية وصعوبة الإسناد سمتان رئيستان للفضاء السيبراني، مما يخلق حالة عدم الثقة بين الفاعلين، إضافة إلى الضعف الشديد التي تعاني منه المنظمات الدولية (وأحيانا

¹ Craig B. Greathouse, "Cyber war and strategic thought: Do the classic theorists still matter?", **Cyberspace and International Relations**, Springer, Berlin, Heidelberg, 2014, pp 21-40.

² Mary McEvoy Manjikian, "From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik", **International Studies Quarterly**, Vol 54, Issue 2, 2010, pp 381-401.

³ Richard Harknett J & Joseph S Nye Jr, "Is Deterrence Possible in Cyberspace?", **International Security**, Vol 42, N° 2, 2017, pp196-199.

⁴ يقترح **جوزيف ناي** ثمانية قواعد تشمل جميع أصحاب المصلحة في الفضاء السيبراني إلى جانب مبادئ وتدابير بناء الثقة بغية

تحقيق الحد الأدنى من الاستقرار في الفضاء السيبراني، للاطلاع على المزيد على الرابط: <https://bit.ly/3y9Nzaq>

تُتهم بخدمة فاعل معين على حساب الآخرين) يجعل من التعويل عليها في تخفيف حدة الفوضى وتنظيم الفضاء السيبراني مجرد أفكار طوباوية.

لذلك نجد أن **العسكريين والاستراتيجيين** يقودون الرواية **الواقعية**، حيث إن الكثير من افتراضات التيار المهيمن على التنظير في العلاقات الدولية تنطبق على التفاعلات في الفضاء السيبراني، فقد ظهر مصطلح "الحرب السيبرانية" مبكراً¹، إذ أُعتبر الفضاء السيبراني امتداداً لميدان المعركة وهو البعد الخامس للحرب بعد الأرض، البحر، الجو والفضاء الخارجي، ويجدر بالجيش التكيف الاستراتيجي معه؛ كما يرى الواقعيون أن لامركزية الفضاء السيبراني منحت سمة الفوضى، ورغم أنه يتجاوز الجغرافيا ولا يعترف بالحدود إلا أن له طابعاً وإيديولوجياً رأسمالية (خاصة الاقتصاد الرقمي) ميزته الرئيسية هي التنافس والصراع، والسيطرة على المعلومات تجعل منها سلاحاً يقرر الفوز والهزيمة²، فالواقعية أعطت تفسيرات مميزة للتهديدات السيبرانية وسباق التسلح السيبراني بين الدول، كما بينت أن الصراع السيبراني مجرد استنساخ لمعضلة الأمن Security dilemma في العالم المادي³.

في المقابل، نجد أن تقدير القوة السيبرانية للدول ومعرفة ميزان القوى السيبراني يحتاج إلى المزيد من الدراسة والتوضيح والضبط عند الواقعيين، إضافة إلى صعوبة تطبيق نظرية الردع في الفضاء السيبراني نظراً لخصائص الأسلحة السيبرانية⁴، كما أن مركزية الدولة في التحليل الواقعي لا يمكن الإبقاء عليها خاصة مع بروز فواعل أخرى تمتلك من القوة أكثر من الدول (شركات التكنولوجيا مثلاً).

¹ John Arquilla & David Ronfeldt, "Cyberwar is coming!", **Comparative Strategy**, Vol 12, N°2, 1993, pages 141-165.

² يعتمد الاستراتيجيون على أفكار صن أتزو التي ضمنها كتابه "فن الحرب"، حيث إن الهدف من الحرب ليس تدمير العدو ولكن جعله غير قادر على القتال أو غير راغب فيه، وهذا ما يسعى إليه مفهوم السيطرة أو الهيمنة على المعلومات.

³ يقدم جون ميرشايمر في كتابه "مأساة سياسة القوى العظمى" خمسة افتراضات لبناء نظريته الواقعية هي: فوضوية النظام الدولي، قدرة الدول على الحاق الضرر بغيرها، حالة عدم اليقين في السياسة الدولية، الأمن والبقاء على رأس أولويات الدول، الدول فاعل عقلائي، ثم يخلص الى ثلاث سلوكيات رئيسة في العلاقات الدولية هي: الخوف وعدم الثقة بين الدول، الاعتماد على النفس، تعظيم القوة، وهو بهذا يقدم نظريته الهجومية لتفسير السلوك الخارجي للدول.

⁴ Richard J Harknett and Joseph S Nye Jr, **Op.cit.**

وتعقياً على ما سبق، فإن السرديات الكبرى في العلاقات الدولية غالباً ما تفشل في إعطاء صورة كاملة عن السلوكيات والتفاعلات داخل الفضاء السيبراني، حتى النقاد الذين يعتمدون على الهويات والفرد كأساس للتحليل فشلوا في تفسير بعض سلوكيات الدول في الفضاء السيبراني (مثل تجسس الو.م.أ على حلفائها)، كما تجدر الإشارة إلى سعي بعض الباحثين لتقديم مقاربات جديدة للعلاقات الدولية في العصر الرقمي، فمثلاً تقدم نازلي شكري مقارنة تعتمد على نظرية الضغوط الجانبية لتفسير دوافع سلوكيات الفواعل، مع توسيع مستوى التحليل إلى "النظام العالمي" والذي يشمل مستويات التحليل التقليدية (الفرد، الدولة، النظام الدولي) بُغية تفسير ديناميات التفاعل بين الفواعل الجديدة التي برزت في الفضاء السيبراني¹.

الفرع الثاني: على مستوى السياسات والممارسات

لقد شهدت العلاقات الدولية تطوراً في طبيعة القضايا المطروحة، جنباً إلى جنب مع تغيير واضح في ديناميات التفاعل بين الدول وظهور فواعل جديدة على الساحة الدولية.

فالأمن الذي يُعتبر جوهر العلاقات الدولية، عرف تطوراً كبيراً على مختلف مستوياته (الدولي، القومي، الإنساني) متأثراً بالتحديات الجديدة التي فرضها الفضاء السيبراني، وظهور فواعل جديدة من غير الدول جعلت من الأمن السيبراني أولوية قصوى على أجندات السياسيين والعسكريين، كما أصبحت القضايا المستجدة مثل حماية البنية التحتية الحرجة وتوطين التكنولوجيا تقود استراتيجيات وسياسات الدول وتحدد سلوكها الخارجي، لذلك تعمل الدول على تشكيل جيوش سيبرانية لحماية الأمن القومي في إطار صراع سيبراني غير معلن، وهذا ما أثار الجدل حول حدوث حروب سيبرانية بين مؤيد² ومعارض³، كما تعالت الأصوات حول قضايا خصوصية الأفراد في الفضاء السيبراني وحماية بياناتهم الشخصية المهددة حتى من الدول نفسها، مما يجعل من الفرد الحلقة الأضعف في سلسلة الأمن السيبراني.

¹ Nazli Choucri, Op.cit.

² Richard Clarke, & Knake Robert, **Cyber war: The next threat to national security and what to do about it**, Haper Collins, 2010.

³ Thomas Rid, **Cyber war will not take place**, Oxford University Press, USA, 2013.

وفي نفس الصدد، عرف **الاقتصاد العالمي** ترابطاً وتشكيباً كثيفاً بفعل تطور تكنولوجيات المعلومات والاتصال، كما ظهر مفهوم جديد عرف بالاقتصاد الرقمي، وازداد التنافس الدولي حول الأسواق بسبب سرعة الوصول إلى المستهلكين وتوسع عمليات التسويق عبر الأنترنت، كما برزت شركات التكنولوجيا كفاعل قوي ومؤثر في السياسة العالمية، هذا في مقابل مخاطر التجسس السيبراني الاقتصادي وما يسببه من خسائر كبيرة وتوتر في العلاقات بين الدول، إضافة إلى دور العملات الرقمية والمخاوف من انفلات السلطة المالية من يد الدول لصالح كيانات جديدة.

أما ما يتعلق بقضايا **المجتمع المدني الدولي**، فقد عزز الفضاء السيبراني تشكيل وتقوية الرأي العام الدولي، حيث ساهم في تطوير جهات فاعلة وطنية وإقليمية وعالمية تتجاوز سلطة الدولة وتتحداه في بعض الأحيان (مثال الربيع العربي)، فمهما كان نوع وحجم القضية سرعان ما تجد من يتبناها ويدافع عنها ويوصلها إلى أعلى مستويات السلطة في مختلف أنحاء العالم، لذلك فإن إنشاء شبكات اجتماعية عالمية قد ساهم بشكل فعال في نشر قيم السلام والحرية والازدهار، في المقابل يساهم التواصل الاجتماعي أيضاً في تشكيل كيانات قومية أو إثنية أو عنصرية (مثال النازيون الجدد) ما قد يكون سبباً في حدوث الصراعات.

بالنسبة **للتعاون الدولي**، سهلت عمليات التشبيك المكثف تبادل المعلومات والخبرات بين الدول، وأضفت نوعاً من الشفافية والثقة في التعاملات، كما سعى العديد من أصحاب المصلحة في الفضاء السيبراني إلى تعزيز الثقة والتعاون الدولي، وجعله فضاءً للسلام والحرية والازدهار، من خلال الدعوة إلى **حوكمة الأنترنت** وضبط سلوك الفاعلين وتحييد النشاطات الخبيثة والإجرامية، كما ظهر نوع جديد من الدبلوماسية سُمي **بالدبلوماسية الرقمية** ساهمت في تقريب وجهات النظر بين الفاعلين.

المطلب الثالث: القوة السيبرانية

تُعد القوة من المفاهيم المركزية في العلاقات الدولية، فالدولة الواسطالية تقوم على مبدأ احتكار الاستخدام الشرعي للقوة، والقوة مفهوم نسبي وديناميكي يرتبط بالسياق، فمنظرو الواقعية يجادلون بأنه في عالم تحكمه الفوضى تسعى الدول للحفاظ على بقائها من خلال امتلاك، تعظيم واستعمال القوة، والقوة العسكرية على وجه الخصوص كما يراه **مورغانشو**، ورغم أن عناصر القوة

توسعت عند كل من كينيث والتز¹ وجون ميرشايمر² لتشمل عناصر غير عسكرية مثل السكان والجغرافيا والاقتصاد والتكنولوجيا والاستقرار السياسي، إلا أنها بقيت محصورة في صبغتها المادية الصلبة، إذ أن القوة (الصلبة أو الخشنة) هي قدرة الدولة على التأثير في سلوك الدول الأخرى³؛ في المقابل قلل أصحاب المداخل النظرية الأخرى من أهمية قوة الدولة المادية بالتركيز على فواعل أخرى كالمنظمات عند الليبراليين والتركيز على القيم والمعايير عند البنائيين، كذلك فرّق كل من جوزيف ناي وروبرت كيوهين⁴ بين القوة الصلبة والقوة الناعمة، فالأولى هي قدرة الكيان على استخدام التهديدات أو المكافآت لجعل الكيانات الأخرى تفعل ما لم تكن لتفعله لولا ذلك، أما القوة الناعمة فهي قدرة الكيان على تحقيق الأهداف من خلال الجاذبية بدلاً من الإكراه.

بناءً على ما سبق، فإن قوة الدولة تعتمد على ركيزتين أساسيتين هما توفر الموارد و القدرة على التأثير، وتتبلور في أربعة مستويات هي: الدبلوماسية (القوة السياسية)، التكنولوجيا المتقدمة (قوة المعلومات)، النظام الاقتصادي (القوة الاقتصادية)، نظام الجيش (القوة العسكرية)، أو ما يعرف بنموذج DIME لقوة الدولة والذي اعتمده الرئيس الأمريكي جيمي كاتر 1977⁵، تعمل هذه المستويات الأربعة بشكل متناسق ومتكامل في مختلف الفضاءات أو المجالات، الأرض والبحر والجو والفضاء الخارجي وحالياً تعمل كذلك في الفضاء السيبراني.

بطبيعة الحال، فتطور تكنولوجيا المعلومات والاتصال قدم أدوات ووسائل جديدة ساهمت في تطور وتعدد انماط التفاعلات على الساحة الدولية، كما أثرت في شكل وطبيعة القوة بنوعيتها الصلبة والناعمة، كما أن سِمَتَي المجهولية وسهولة الدخول إلى الفضاء السيبراني شجعت الجهات الفاعلة الدولية الأصغر على امتلاك وممارسة القوة الصلبة والناعمة في السياسة الدولية، مما أدى إلى انتشار القوة بين الفاعلين وبالضرورة تآكل وانتشار السلطة حيث أصبحت الشبكات أقوى أبعاد السلطة، ما دفع الدول الكبرى لوضع الفضاء السيبراني على رأس أولوياتها

¹ Kenneth Waltz, **Man, the state, and war**, Columbia University Press, 2018, pp 159 – 160.

² جون ميرشايمر، مرجع سابق، ص 55.

³ Abramo Fimo Kenneth Organski, **World Politics**, Knopf, New York, 1968, p103.

⁴ Robert O Keohane & Joseph S Nye Jr, “Power and interdependence in the information age”, **Foreign Affairs**, Vol 77, N° 5, 1998, pp 81-94.

⁵ **National Security Council**, Presidential Directive/NSC-18, U.S. National Strategy, The White House, Washington, DC, 1977.

الاستراتيجية، الأمنية، الاقتصادية والسياسية، بغية تحقيق مصالحها الأمنية وتكريس تفوقها الاقتصادي وتعزيز سيطرتها السياسية، وهذا ما خلق مفهوماً جديداً للقوة هو القوة السيبرانية.

فالقوة السيبرانية Cyberpower كما يعرفها **جوزيف ناي** هي "القدرة على الحصول على النتائج المرجوة من خلال استخدام موارد شبكة المعلومات الإلكترونية في المجال السيبراني"¹، وهو يربطها بمجموعة من الموارد تعتمد على عمليات إنشاء والتحكم والاتصال مع البيانات، البنية التحتية، الشبكات والبرمجيات، والمهارات البشرية، إذن فالقوة السيبرانية تعتمد على مدى تطور المعرفة التكنولوجية والقدرة على استعمال هذه المعرفة، كما يؤكد جوزيف ناي أن استخدام الأدوات السيبرانية لخلق مزايا والتأثير على الأحداث يكون داخل الفضاء السيبراني نفسه أو في البيئات الواقعية الأخرى.

وبناءً على ماسبق، فالقوة السيبرانية هي امتلاك القدرة على السيطرة على البيانات والأجهزة والبشر (سواء كانوا مشغلين أو مستخدمين) بغية التأثير في التفاعلات التي تحدث بينهم.

كما تجدر الإشارة إلى أن خصائص الفضاء السيبراني الفريدة منحت القوة السيبرانية خاصيتين جديدتين هما: **الانتشار** و **تعدد الفاعلين**، فالقوة السيبرانية توزعت وانتشرت بين فاعلين جدد خاصة أن القطاع الخاص هو المساهم الأكبر في الفضاء السيبراني، وهذا ما منح القدرة للفاعلين الصغار في السياسة الدولية على امتلاك واستخدام القوة وتحدي سلطة الدولة، مما يجعل سيطرة الدولة على هذا الفضاء موضع شك.

كذلك، يشير جوزيف ناي إلى **ظاهرة انتشار القوة** بأن المزيد من القضايا ومجالات التأثير والتفاعل تقع خارج نطاق السيطرة الكلية للدولة²، فالكثير من المخاطر والتهديدات والتحديات الجديدة لمواطني دولة ما غالباً ما تأتي من الخارج، بما فيها قضايا الهجرة والمناخ والأزمات المالية والأوبئة، مع عجز الدول عن السيطرة عليها بسبب أن القوة تحت تأثير التكنولوجيا انتشرت عمودياً وأفقياً ونحن نتجه إلى عالم تختفي فيه التعددية القطبية نحو عالم بلا أقطاب³.

¹ Joseph S Nye Jr, **Cyber power**, Harvard Univ Cambridge MA Belfer Center for Science and International Affairs, 2010, p 04.

² **Ibid**, p 01.

³ Joseph S Nye Jr, **The future of power**, Public Affairs, 2011, p113.

ومن زاوية أخرى، فإن مشاركة فواعل تحت/فوق دولية في مصادر القوة التي كانت حكرًا على الدولة، جعل عملية انتشار القوة تأخذ بعدين، أولاً، داخل الدولة ذاتها، حيث مكن الفضاء السيبراني الفواعل التقليدية والجديدة من امتلاك قوة أكبر في المشاركة السياسية والتأثير على عملية صنع القرار، إضافة إلى تأثير الفواعل الخارجية على الرأي العام الداخلي وتوجيهه، وهذا ما أضعف قوة الدولة (السلطة)، ثانياً، خارج الدولة، حيث أصبح الفاعلين في داخل الدولة يشاركون في القضايا الدولية ويؤثرون في تفاعلات السياسة العالمية، وهذا ما ينهي احتكار الدولة لدور الفاعل الوحيد في العلاقات الدولية.

وإضافة لما سبق، يُقدم جوزيف ناي ثلاثة أوجه لاستخدام القوة السيبرانية في صورتها الصلبة والناعمة وهي: أولاً، تأثير الفاعل (أ) على الفاعل (ب)، ثانياً، تحكم الفاعل (أ) في أجندة الفاعل (ب) وجعله يستبعد بعض الاستراتيجيات، ثالثاً، قدرة الفاعل (أ) على ترتيب أوليات الفاعل (ب)¹، كما يرى أن الحكومات و الدول الكبرى لازالت تمتلك الكثير من الموارد والقدرة على التأثير مما يُبقيها فاعلاً قوياً في الفضاء السيبراني.

وفي خضم سعي الدول لامتلاك، تعظيم واستخدام للقوة السيبرانية يجب أن تتوفر على مجموعة من الخصائص الضرورية المادية والمعارية، نلخصها في أربعة عناصر رئيسية:

1. البنية التحتية التكنولوجية: في العصر الرقمي وتحت وطأة العولمة لابد للدولة أن تكون لها بنية تحتية تكنولوجية قوية، تتمثل في شبكات الاتصال المتطورة، وأجهزة الكمبيوتر الفائقة السرعة والبرمجيات وغيرها، لأن هذا ما تحتاجه الدولة لإدارة شؤونها خاصة في القطاع المالي والمصرفي الذي يتطلب السرعة والدقة في التنفيذ، إضافة إلى تسيير الموارد الكبرى كالغاز والكهرباء والماء، وتقديم الخدمات العامة للمواطنين (الحكومة الالكترونية) والذي يُعتبر مؤشراً لمدى قوة الدولة وتطورها.

2. التطور التقني: ويُقصد به مدى قدرة الدولة في على التطوير والابتكار وتشكيل وإعادة تشكيل الفضاء السيبراني، حيث توجد مجموعة من المجالات التقنية التي تتنافس عليها الدول مثل: تكنولوجيا الجيل الخامس، الذكاء الاصطناعي، الحوسبة الكمومية، البيانات الضخمة، تعليم

¹ Ibid, p 130-131.

الآلة... إلخ، ففوة الدولة تزيد كلما زاد عدد براءات الاختراع في هذه المجالات، لذلك من واجب الدولة الاستثمار في العنصر البشري بالتعليم والتدريب والاستغلال.

3. **البنية المؤسسية والتشريعية:** وتقوم على مجموعة المؤسسات والهيئات المكلفة باستخدام القوة السيبرانية لخدمة مصالح الدولة، من خلال وضع الاستراتيجيات والسياسات اللازمة عبر ضبط العمليات السيبرانية (مهاجمة الشبكات، الدفاع عن الشبكات، استطلاع الشبكات) وهذا لدرء التعارض وتضارب المصالح بين أصحاب المصلحة في الفضاء السيبراني (خاصة القطاع العام والقطاع الخاص)، ومن جهة أخرى، وجود قوانين ومعايير تضبط التفاعل داخل الفضاء السيبراني الداخلي للإبقاء على سلطة وسيادة الدولة على الأقل داخل حدودها الإقليمية.

4. **خطة استراتيجية للفضاء السيبراني:** أو الإيديولوجيا¹ السيبرانية للدولة، أي كيف ترى الدولة هذا الفضاء، فالعناصر السابقة عاجزة في حد ذاتها على تحقيق أهداف ومصالح الدولة في غياب خطة استراتيجية ورؤية واضحة تجاه الفضاء السيبراني، فعلى الدولة أن تُقدم إجابات واضحة للأسئلة من قبيل: هل تعتمد على الهجوم أم تكتفي بالدفاع، هل تسعى لتعزيز التفاهم والتعاون أم أن الصراع هو الخيار المحتوم.

المطلب الرابع: الصراع السيبراني

تعكس القراءة الأولية لأدبيات الصراع ثراءً فيما تقدمه من مفاهيم للمصطلح، من حيث طبيعته المعقدة ومسبباته ومصادره المتداخلة ومستوياته المختلفة (الفرد، الجماعة، الدولة) وأبعاده المتباينة (النفسية، الاجتماعية، الاقتصادية، السياسية... إلخ)، فالصراع يشير إلى عملية تفاعل ديناميكية، كما يعبر عن موقف تنافسي أو تعارض وإع بين طرفين أو أكثر الهدف منه إلحاق الأذى والضرر المادي أو المعنوي بالطرف الآخر، فالصراع كما يراه اسماعيل صبري مقلد هو عبارة عن تنازع الإرادات الوطنية²، كما يقدم بيتر فالنستين مفهوماً للصراع يركز على ثلاث عناصر هي: التحرك (Action) والاختلافات (Incompatibility) والأطراف أو المحركين (Actors)، فالصراع عند فالنستين هو "وضع اجتماعي يكافح فيه ما لا يقل عن طرفين للحصول

¹ Jill Rowland, Mason Rice, and Sujeet Shenoi, "The anatomy of a cyber power", **International Journal of Critical Infrastructure Protection**, Vol 7, N°1, 2014, pp 3-11.

² إسماعيل صبري مقلد، العلاقات السياسية الدولية: دراسة في الأصول والنظريات، الجيزة: المكتبة الأكاديمية، 1991، ص 223.

على مجموعة من الموارد المحدودة في اللحظة نفسها في فترة زمنية معينة¹، والكفاح حسب فالنستين يغطي العديد من النشاطات بما فيها الحرب، في حين أن أغلب الآراء تقول بفكرة أن الصراع هو المرحلة السابقة للحرب.

علاوة على ذلك، فبروز الفضاء السيبراني وتغلغله في جميع المستويات والأبعاد السابقة الذكر، ساهم في ظهور سياقات وأنماط جديدة للصراع نتيجة ما يقدمه من أدوات حديثة في متناول الفاعلين الدوليين، وما يخلقه من مساحات وفضاءات مختلفة للتفاعلات الداخلية والدولية على حد سواء، فالفضاء السيبراني حيّد عاملي الزمان والجغرافيا، فالتفاعلات تحدث بسرعة الضوء، وتتلاشى فيها الحدود الجغرافية، والفواصل بين المدني والعسكري، والعام والخاص، فالكل مترابط ومتشابك، فالصراع السيبراني يكشف حالة التعارض والتنافس بين مصالح وقيم وحاجيات الفاعلين وتتازع الإرادات في الفضاء السيبراني كما في الصراعات التقليدية، وعلى الفضاء السيبراني من أجل التفوق والهيمنة التكنولوجية وامتلاك القوة السيبرانية.

من جهة أخرى، فإن إضافة اللاحقة "سيبراني-Cyber" لمفاهيم مثل الصراع، الحرب، الهجوم، الدفاع... إلخ، خلق تداخلاً كبيراً بين التعريفات، فغالباً ما نجد مفهوم الصراع السيبراني والحرب السيبرانية يدلان على معنى واحد. يختار العديد من الباحثين تعريف ريتشارد كلارك للحرب السيبرانية على أنها "العمليات التي تقوم بها دولة ما لاختراق أجهزة الكمبيوتر والشبكات الخاصة بدولة أخرى بغرض إلحاق الضرر أو التشويش"² للدلالة على مصطلح الصراع السيبراني، في حين يميز باحثون آخرون بين المصطلحين، فاللجنة الدولية للصليب الأحمر تشير إلى الصراع السيبراني بأنه "سعي طرف ما لتحقيق ميزة على حساب الأطراف الأخرى باستعمال الأدوات والتقنيات التي يوفرها الفضاء السيبراني في إطار أوسع للصراع حول المصالح الاقتصادية والثقافية والدبلوماسية والمسائل العسكرية"³، كما يعتبر براندون فاليريانو بأن حدوث حرب سيبرانية أمر مستبعد وما يحدث في الواقع يبقى عند عتبة الصراع والذي يُعرفه بأنه "استخدام المعالجات

¹ Peter Wallensteen, **Understanding conflict resolution**. Sage, 2018, p18.

² Richard Clarke, & Knake Robert, **Op.cit**, p 14.

³ Herbert Lin, "Cyber conflict and international humanitarian law", **International Review of the Red Cross**, Vol 94, N° 886 ,2012, pp 515-531.

الدقيقة والتقنيات الأخرى المرتبطة بها في الفضاء السيبراني، لأغراض خبيثة و/أو مدمرة من أجل التأثير أو التغيير أو التعديل على التفاعلات الدبلوماسية والعسكرية بين الكيانات¹.

وبناءً على ماسبق، وبالاكتفاء على تعريف فالنستين للصراع فإن الصراع السيبراني هو تلك العمليات السيبرانية التي يقوم بها فاعل أو أكثر للحصول على موارد أو ميزات في الفضاء السيبراني على حساب الطرف أو الأطراف الأخرى.

وتفسيراً لذلك، فيُقصد بالموارد البيانات الضخمة (Big Data) والشبكات (Networks) والبرامج (Software)، أما الميزات فهي نسبة السيطرة والقدرة على التحكم في بُعد أو أكثر من أبعاد الفضاء السيبراني الأربعة (المستخدمون والمشغلون، الأجهزة، البيانات، التفاعلات).

العمليات السيبرانية: عادة ما يشير المصطلح إلى استعمال القدرات السيبرانية (أو إظهار القوة) بُغية تحقيق الأهداف في ومن خلال الفضاء السيبراني، فحسب وزارة الدفاع الأمريكية (DoD) فالعمليات السيبرانية في المجال العسكري تعني استعمال القدرات السيبرانية لخلق التأثير الذي يدعم العمليات في الواقع المادي والفضاء السيبراني²، غير أن الصين وروسيا تستعملان مصطلح "معلومات" بدل مصطلح "سايبير" ليصبح مفهوم "عمليات المعلومات" يشمل "الإجراءات المتخذة لتحقيق التفوق من خلال التأثير على معلومات الأعداء وأنظمتهم في مقابل تقوية وحماية معلوماتنا وأنظمتنا وبنيتنا التحتية"³، ويمكن تقسيم العمليات السيبرانية إلى ثلاث أنواع رئيسية:

1. **الهجوم السيبراني:** وهو عملية إظهار القوة في وعبر الفضاء السيبراني، ويتم ذلك عبر استخدام البرمجيات الخبيثة (Malwares) والمكونات المادية للأجهزة بغرض إضافة، تعديل، حذف البيانات على الأنظمة والشبكات لإحداث تأثير مادي أو معنوي أو معرفي.

¹ Brandon Valeriano, Ryan C. Maness, **Cyber war versus cyber realities: Cyber conflict in the international system**, Oxford University Press, 2015, pp 31-33.

² Catherine A Theohary, **Defense primer: Cyberspace Operations**, Congressional Research SVC, 2021, URL: <https://sgp.fas.org/crs/natsec/IF10537.pdf>

³ Dennis Granåsen, Margarita Jaitner, "The Offensive Cyber Operations Playbook", **18th European Conference on Cyber Warfare and Security (ECCWA 2019)**, University of Coimbra, Portugal, 2019, p 197.

2. **الدفاع السيبراني:** والهدف منه تحييد جميع التهديدات والمخاطر السيبرانية التي تهدد الشبكات والأنظمة والبنية التحتية، والحفاظ على استمرارية العمل داخل الفضاء السيبراني، وينقسم إلى نوعين: أولاً، **الدفاع السيبراني السلبي** والذي يهتم بتعزيز الأمن السيبراني وحماية الأنظمة والشبكات الداخلية، ويرتكز على مفهوم المرونة السيبرانية (Cyber Resilience) والتي تعني إمكانية مواصلة تقديم الخدمات في الفضاء السيبراني رغم التعرض إلى الهجمات، ثانياً، **الدفاع السيبراني النشط** ويتم فيه تتبع الهجمات السيبرانية والرد عليها.

3. **عمليات الاستطلاع، المراقبة والجوسسة:** والهدف منها جمع أكبر كم من البيانات وذلك عبر اختراق الأنظمة والشبكات، والبقاء على اطلاع على أحدث التقنيات والأحداث في الفضاء السيبراني، وهذا لتقديم المعلومات المهمة لصانع القرار والعاملين في مجالي الدفاع والهجوم السيبراني.

كما تجدر الإشارة إلى أن تطور مفهوم الأمن خاصة بعد أحداث 11 سبتمبر، وزيادة اعتماد الدولة على الفضاء السيبراني في مختلف المجالات جعل من العمليات السيبرانية تتدرج تحت العديد من الأطر¹ أو المجالات نلخصها فيما يلي:

1. **حوكمة الفضاء السيبراني:** بما أن القطاع الخاص هو المساهم الأكبر في الفضاء السيبراني، فإن نشاطات الدولة السيبرانية وسعيها لحوكمة هذا الفضاء في مجملها عمليات استباقية وقائية، وتشكل جزءاً لا يتجزأ من استراتيجيات الأمن السيبراني.

2. **الحماية:** حيث أصبحت حماية البنية التحتية الحرجة (سواءً السيبرانية أو المادية) على رأس أوليات المهام التي تقوم بها الدولة.

3. **تعزيز وتطبيق القانون:** ذلك أن الفضاء السيبراني خلق تحدياً جديداً للقوانين التقليدية وهيئات إنفاذ القانون، لذلك تسعى الدول إلى سن قوانين تتلاءم والتحديات الجديدة، إضافة إلى تشكيل هيئات مكلفة بالبحث في الكيفيات المثلى لتقنين الأحداث السيبرانية (مثلاً: الجريمة السيبرانية) وإنفاذ القانون.

4. **الاستخبارات ومكافحة التجسس:** رغم أنها من المهام الأمنية التقليدية للدولة إلا أنها عرفت تطوراً كبيراً في المجال السيبراني، فكما مكنت الدولة من جمع المزيد من البيانات والمعلومات

¹ Paul AL Ducheine, Peter BMJ Pijpers, "The notion of cyber operations", **Research Handbook on International Law and Cyberspace**, Edward Elgar Publishing, 2021, pages 218-229.

الاستخباراتية بأقل جهد، فإنها وضعت الدول في حالة انكشاف معلوماتي خطيرة صعبت معها مهمة حماية الأسرار والمعلومات الاستخباراتية.

5. **العمليات العسكرية:** ويشار إليها عموماً بالحرب السيبرانية، فهي تلك العمليات التي تحدث في الفضاء السيبراني في إطار صراع مسلح، أو لدعم عمليات السلام، كما يعرف المجلس الاستشاري الهولندي العمليات السيبرانية العسكرية على أنها "سلوك عسكري يشتمل على عمليات لتعطيل أنظمة كمبيوتر الخصم أو تضليلها أو تعديلها أو تدميرها من خلال القدرات السيبرانية"¹، لذلك فالعديد من دول العالم حرصت على تشكيل وحدات للحروب السيبرانية (مثل: US cyber command الأمريكية، الوحدة 61398 الصينية وغيرهما)

الفواعل الدولية للفضاء السيبراني: يشير مفهوم "الفاعل الدولي" إلى كل سلطة أو جهاز أو مجموعة أو حتى فرد يمارس نشاطات تؤثر بشكل أو بآخر على حركة التفاعلات الدولية، كما يتحمل المسؤولية عن القرارات والآليات التي يتبعها لتنفيذ سياساته واستراتيجياته الخارجية في الساحة الدولية.

ولكي يمتلك الفاعل صفة "فاعل دولي" يشترط إسماعيل صبري مقلد توفر أربعة معايير أساسية هي²:

1. قابلية التحديد، أي أن يكون الفاعل معروفاً بصفاته التي تميز دوره في العلاقات الدولية.
2. امتلاك حد معين من القدرة على التأثير والقدرة على حماية مصالحه.
3. القدرة على التفاعل مع الفاعلين الآخرين.
4. القدرة على البقاء والاستمرار على الساحة الدولية لفترة معقولة من الزمن.

وبما أن الفاعل في الفضاء السيبراني (هناك من يسميه الفاعل الرقمي) هو ذلك الكيان الذي يمارس تأثيره في وعبر الفضاء السيبراني والذي من أهم خصائصه سرعة التغير والتبدل في الطبيعة والشكل، فالفاعلون بدورهم يتغيرون من حيث العدد وقوة التأثير، في المقابل، إذا حقق

¹ Ibid.

² إسماعيل صبري مقلد، العلاقات السياسية الدولية: النظرية و الواقع. الجيزة: المكتبة الأكاديمية، 2011، ص ص 93-94.

أي من الفاعلين المعايير السابقة الذكر، فإنه يتم تصنيفه ضمن قائمة الفاعلين الدوليين في الفضاء السيبراني.

وبناءً على ماسبق، واعتماداً على ما قدمه جوزيف ناي في كتابه "مستقبل القوة" من تصنيفات للفاعلات الدولية في الفضاء السيبراني¹، تقترح الدراسة تصنيفاً يعتمد على معيارين أساسيين هما؛ **المعيار القيمي**، ونعني به ما يمتلكه الفاعل من قدرات قيمة كالسيادة والقدرة على وضع القوانين وتطبيقها، **المعيار المادي**، ونعني به امتلاك الفاعل للقدرات المادية (تقنية، مالية، لوجيستية...) في الفضاءين المادي والسيبراني على حد سواء، وعليه فإن تصنيفات الفاعلين في الفضاء السيبراني تكون كالتالي:

1. **الدول القومية/التحالفات**: تقليدياً الدول هي الفاعل الرئيس في العلاقات الدولية، ومن المرجح أن تبقى كذلك في المستقبل القريب، وهو ما ينطبق كذلك على التحالفات بين الدول، وهذا يعود لامتلاكها السيادة والحق في الإكراه وسن القوانين وإنفاذها داخل حدودها، هذا إضافة لتحكمها ولو بنسب متفاوتة في تسيير اقتصادها ومواطنيها، مع ميزة السيطرة على قطاعي الاستخبارات والجيش وهذا ما يمنحها القدرة على اتخاذ قرارات الحرب والسلام، لهذا فالدولة فاعل رئيس في الفضاء السيبراني سواء تعلق الأمر بالتنظيم (القوانين والسياسات والاستراتيجيات السيبرانية) أو بالاستعمال (القدرة على التحكم في أبعاد الفضاء السيبراني أو حتى قطع الاتصال المادي الكلي أو الجزئي به).

2. **المنظمات**: تعتبر المنظمات بأنواعها (الحكومية/غيرالحكومية، الدولية/الإقليمية) من الفاعلين البارزين في الفضاء السيبراني خاصة في مجال التشريع والتنظيم، ففضايا تطبيق القانون في الفضاء السيبراني، الحوكمة، تقنين الحرب السيبرانية وحماية الخصوصية وغيرها من المواضيع تدخل في صلب النقاشات الدولية.

3. **شركات التكنولوجيا**: الفضاء السيبراني من صنع شركات التكنولوجيا، فهي من تتحكم في تكوينه، تسييره ورسم مستقبله، وسواء كانت شركات لصناعة التقنية (ميكروسوفت، آبل، سيسكو، هواوي...) أو لتقديم الخدمات في الفضاء السيبراني (فايسبوك، علي بابا، أمازون، قوقل...) فهي تمتلك قدرات (مادية) تفوق قدرات الكثير من الدول، والصراعات بينها وبين الدول غير خافية

¹ Joseph S Nye Jr, *The future of power*, Op.cit, pp 132-139.

(الصين ضد قوقل، الو.م.أ ضد هواوي، الاتحاد الأوروبي ضد فايسبوك...)، لذلك فهي من أكبر الفاعلين المؤثرين في الفضاء السيبراني.

4. الكيانات الأقل تنظيماً والأفراد: يشمل هذا الصنف العديد من التنظيمات الشرعية وغير الشرعية، حيث يضم مجموعات الهاكرز، تنظيمات الإرهاب والجريمة المنظمة، الحركات السياسية والدينية والعرقية، إضافة إلى الأفراد كمؤثرين على المستوى الدولي أو كمبلغين¹، ويتميز هذا الصنف من الفاعلين بالمناسباتية، أي أن ظهورهم وتأثيرهم - رغم أنه في بعض الأحيان يكون تأثيراً بالغاً مثل ما قام إدوارد سنودن - على الساحة الدولية يحدث في أوقات متباعدة ولفترة وجيزة، إضافة إلى أن قدراتهم التقنية ضعيفة نسبياً إذا ما قُورنت بالقدرات التي تمتلكها الدول.

¹ المبلغ هو الذي يقوم بالافصاح والكشف عن معلومات متعلقة بأنشطة فاسدة، أو غير قانونية، أو منطوية على مخاطر يتم ارتكابها في/ أو بواسطة منظمات في القطاع العام أو القطاع الخاص، وتثير مخاوف أو تمثل تهديداً للأفراد أو المؤسسات (منظمة الشفافية الدولية).

المبحث الثالث : التحليل الجيوبوليتيكي للفضاء السيبراني

يتعقب التفكير الجيوبوليتيكي النشاطات البشرية¹، يقول سبيكمان: إن طبيعة المشكلة هي من يحدد ليس فقط طبيعة التحليل الجغرافي، بل كذلك حجم المنطقة الواجب تحليلها²، ومن البديهي أن يتبادر إلى ذهن السؤال التالي: لماذا البحث في جيوبوليتيكا الفضاء السيبراني؟ والإجابة عن السؤال تنطلق من فرضيتين أساسيتين، أولاً، لأن الجيوبوليتيكا تقدم رؤية للعالم، فهي تُعطي فهوماً حول تركيبة العالم، طبيعة الصراع، من يحكم وإلى ما ستؤول إليه الأمور، ثانياً، الجيوبوليتيكا كما يعرفها **لاكوست** هي تنازع السلطة والنفوذ على الإقليم والشعوب التي تسكنه، فهي تهتم بدناميكيات الصراع حول إقليم معين، والتصورات المتباينة والاستراتيجيات المتضاربة للفاعلين للسيطرة والهيمنة، لذلك فهي تعطينا فهوماً حول طبيعة الفضاء السيبراني، والصراعات داخله، وتجيئنا عمّن يسيطر ويتحكم فيه، وكما يؤكد **جون شيلدون** على أن فهم جيوبوليتيكا القوة السيبرانية يمكن أن تساعد صانعي القرار والمحللين في فهم دوافع ومحفزات مختلف الفاعلين في الفضاء السيبراني³.

لكن يبقى التساؤل مطروحاً حول إمكانية أن يكون الفضاء السيبراني شكلاً جديداً من الإقليم؟ لتجاوز هذا التحدي المنهجي نستعين بـ"الجغرافيا الماورائية Metageography" أو ظاهرة تخيل المكان، والتي يعرفها **مارتن لويس** بأنها الأطر المكانية التي من خلالها ينظم البشر معرفتهم حول العالم⁴، والتي تنطلق من مبدأ أن المكان يتشكل عن تصور البشر ووعيهم به، فالتصور الأولي للفضاء السيبراني كان ذلك المكان أو الفضاء الحر، والذي ليس من حق الدول والحكومات التدخل فيه⁵، ولكن بعد العام 2000 أصبحت الدول تعتبره المجال الخامس للحرب، وبالتالي يجب تعيين حدوده وحماية سيادته وتطبيق القانون داخله مثل أي إقليم تقليدي.

¹ أغنيشكا لغوتسكا، مرجع سابق، ص 08.

² فؤاد حمه خورشيد، مرجع سابق، ص 19.

³ John B Sheldon, "Geopolitics and cyber power: Why geography still matters", **American Foreign Policy Interests**, Vol 36,N°5, 2014, pp 286-293.

⁴ Martin W Lewis, Kären Wigen, **The myth of continents**, University of California Press, 1997, p ix.

⁵ كتب John Perry Barlow العضو في مؤسسة الحدود الإلكترونية EFF سنة 1996 إعلان لاستقلال الفضاء السيبراني ورفض تدخل الحكومات في تسييره أو السيطرة عليه على الرابط: <https://bit.ly/3OL7W6O>.

من جهة أخرى، فالفضاء السيبراني وفقاً للأنطولوجيا الإقليمية التي يتبناها "دانيال لامباش" هو مجموعة من الأقاليم غير الحصرية المتداخلة والمتقاطعة، يتم إعادة التفاوض باستمرار على أشكالها (حدودها) وخصائصها (محاولة السيطرة عليها)¹، لذلك غالباً ما تُثار الأسئلة حول حدود هذه الأقاليم والقوانين التي تحكمها وكذلك حول القوة والصراع داخلها.

المطلب الأول : الطبقات لفهم جيوبوليتيكا الفضاء السيبراني

عند استحضار بنية الفضاء السيبراني وتفكيكها نحصل على مجموعة من الطبقات تحدث التفاعلات فيها وعبرها، وتحتوي كل طبقة على مجموعة متباينة من الفاعلين والقضايا والتفاعلات، كما تحدث فيها صراعات جيوبوليتيكية حول السيطرة والتحكم والهيمنة.

يختلف عدد الطبقات وتسمياتها، **فالتقنيون** اعتمدوا منذ نهاية السبعينيات وبداية الثمانينيات على نموذج **OSI** "ربط الأنظمة المفتوحة - Open Systems Interconnection" والذي يستخدم لضمان تشبيك الأجهزة والأنظمة المتباينة وفق بروتوكولات موحدة والتي تشكل الفضاء السيبراني اليوم، ويتشكل من سبع 07 طبقات هي: الطبقة الفيزيائية، ربط البيانات، الشبكة، النقل، الدورة، التمثيل، التطبيقات²، وهذه الطبقات خاصة فقط بالشبكات ولا تشمل المستخدمين والمشغلين، ومن ثم قام **الباحثون** المتخصصون في العلوم الأخرى (غير علم الكمبيوتر والشبكات) بدمج بعض الطبقات وإعادة تسميتها أو إضافة طبقات أخرى حسب ضرورات البحث ولغرض التبسيط والفهم والتوضيح³، لذلك، تستخدم هذه الدراسة نموذج الطبقات الأربع (**The Four-layer Model**)⁴ وهي على التوالي: طبقة البنية التحتية المادية (الفيزيائية)، طبقة البروتوكولات (المنطقية)، طبقة التطبيقات والبرامج وطبقة المحتوى (البيانات والتفاعل البشري) .

¹ Daniel Lambach, "The territorialization of cyberspace", **International Studies Review**, Vol 22, N°3, 2020, pp 482-506.

² Hubert Zimmermann, "OSI reference model-the ISO model of architecture for open systems interconnection", **IEEE Transactions on communications**, Vol 28, N° 4, 1980, pp 425-432.

³ Robert J Domanski, **Who Governs the Internet? The Emerging Policies, Institutions, and Governance of Cyberspace**, CUNY Academic Works, 2013, pp 61-65.

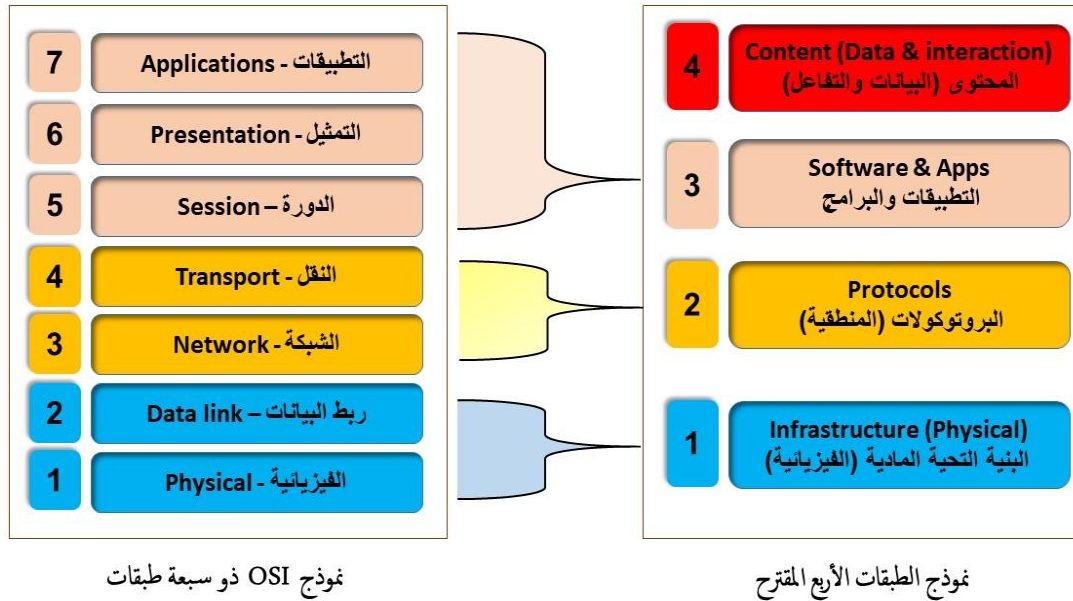
⁴ يستعمل العديد من الباحثين نموذج الطبقات الأربع لكن أحياناً بتسميات متباينة، مثل ما تقدمه البروفيسور "فريدريك دوزيت" والباحث "دومنسكي روبرت"، انظر:

Frédéric Douzet, « La géopolitique pour comprendre le cyberspace », **Hérodote**, vol. 152-153, no. 1-2, 2014, pp 3-21.

Robert J Domanski, **Op.cit**, p 66.

شكل رقم 03: تحويل نموذج OSI إلى نموذج الطبقات الأربع.

المصدر: من إعداد الباحث.



ويمنحنا هذا النموذج (الشكل 03) القدرة على فهم وتحليل الصراعات التي تحدث داخل وعبر كل طبقات الفضاء السيبراني، من خلال معرفة طبيعة كل طبقة، وتحديد الفاعلين الرئيسيين فيها، ورصد أهم القضايا التي تؤثر على بناء وتنفيذ استراتيجيات الفاعلين وديناميكيات التفاعل بينهم.

1. طبقة البنية التحتية المادية (الفيزيائية): والتي تمثل الجزء المادي للفضاء السيبراني، وتتشكل من مجموعة الأجهزة الرقمية كأجهزة الكمبيوتر والهواتف النقالة وأجهزة الشبكات وخوادم تخزين البيانات وغيرها، ويتم ربط هذه الأجهزة بواسطة وسائط التشبيك كشبكات الاتصال السلكية واللاسلكية وكوابل الألياف البصرية وشبكات الأقمار الصناعية.

تخضع البنية التحتية للقيود الجغرافية والسياسية، حيث يمكن إنشاء بنية جديدة، ربطها أو فصلها عن الشبكة العالمية أو حتى تدميرها، يسيطر على صناعة الأجهزة الرقمية شركات القطاع الخاص، حيث تصدر الشركات الصينية صناعة الهواتف المحمولة، في حين أن الولايات المتحدة الأمريكية تسيطر على صناعة أجهزة الكمبيوتر، وتتوزع كبرى خوادم تخزين البيانات بين الولايات المتحدة وأوروبا، أما بالنسبة لوسائط التشبيك فشبكات الاتصال السلكية واللاسلكية وكوابل الألياف البصرية العابرة للمحيطات والتي يمر عبرها أكثر من 80% من البيانات العالمية فتتوزع ملكيتها

وتسييرها بين الشركات القطاع الخاص (خاصة في الولايات المتحدة) وشركات الاتصالات المملوكة للدولة، وهذا مايفسر قدرة الحكومات على التحكم في تدفق البيانات ومراقبتها والقيام بعمليات الفلترة والحجب، كما أن صناعة الأجهزة الخاصة بالشبكات خاصة الشبكات اللاسلكية (الجيل الخامس 5G) ومد كوابل الألياف البصرية تشهد صراعاً كبيراً بين شركات التكنولوجيا الصينية من جهة، والأمريكية والأوروبية من جهة أخرى.

وتجدر الإشارة إلى أن الاتحاد الدولي للاتصالات ITU يقوم بوضع المعايير التقنية على المستوى الدولي لضمان سلاسة الاتصالات والشبكات¹، إلا أن هذا لم يمنع من بروز قضايا الأمن السيبراني وحماية البيانات، إضافة إلى أن حماية وتأمين البنية الرقمية التحتية أصبحت تعتبر من التحديات الاستراتيجية للدول، حيث توجد دعوات لحماية الكوابل البحرية من التهديدات المادية (الكوارث الطبيعية، التدمير من طرف دول أو مجموعات) وكذلك من التجسس والقرصنة.

2. طبقة البروتوكولات (المنطقية): هي مجموعة الخدمات التي تُمكن من ربط جهاز ما بالشبكة، كما تضمن نقل البيانات بموثوقية عالية بين نقطتين عبر الشبكة، فهندسة الشبكة المبنية على النموذج OSI تركز على وجود لغة مشتركة بين جميع مكونات الشبكة (بروتوكول TCP/IP)، ومن ثم تأتي الخدمات الرئيسية للشبكة وهي:

- **التوجيه (Routing):** وهو عملية اختيار مسار البيانات عبر الشبكة أو بين الشبكات.
- **التسمية والعنونة (DNS):** وهو نظام التسمية الهرمي المستخدم لتحديد الأجهزة والموارد الأخرى التي يمكن الوصول إليها عبر الشبكة، حيث يتم ربط كل اسم (لغة الإنسان مثلاً: google.com) بعنوان IP خاص (لغة الآلة مثلاً: 8.8.8.8 @IP).

والجدير بالذكر أن بروتوكولات التوجيه ومجموعة كبيرة من الخدمات التي تضمن التفاعل عبر الشبكات تقوم بتطويرها ومراقبتها مجموعة من التقنيين والمطورين والمنظمات غير الربحية (مثل: W3C, IETF, ISOC...) ²، أما خدمة التسمية والعنونة DNS ففي البدء كان يسيورها شخص واحد هو "جون بوستل" الملقب بـ"إله الأنترنت" حيث كانت مهمته اختيار أسماء سهلة للمواقع وربطها بعناوينها المكونة من الأرقام المعقدة، ثم أنشأت هيئة IANA لتولي المهمة، وفي 1998 تولت ICAAN مهمة التسمية والعنونة وكانت جزءاً من وزارة التجارة الأمريكية، وفي

¹ نبذة عن الاتحاد الدولي للاتصالات ITU على الموقع الرسمي: <https://bit.ly/3skQ8b8>.

² Robert J. Domanski, Op.cit, pp 98-103.

أكتوبر 2016 أصبحت ICAAN منظمة دولية مستقلة مع بقاء مركزها الرئيس في لوس أنجلوس بالولايات المتحدة الأمريكية.

واستناداً إلى ما سبق، تشهد هذه الطبقة تحديات وصراعات كبيرة، فالبنية الأولية للشبكة (الأنترنت) لم تولي أهمية كبرى للاعتبارات الأمنية، ذلك أن مطوري بروتوكول الربط TCP/IP كان هدفهم الأول هو إيصال البيانات بفاعلية دون الاهتمام بمحتوى البيانات أو تحديد المرسل والمستقبل جغرافياً، فخاصية المجهولية التي يتميز بها الفضاء السيبراني كانت أساس الشيفرة البرمجية للأنترنت، فالاختيارات التقنية سببت تحديات سياسية وأمنية للحكومات والدول، حيث برزت قضايا مثل: صعوبة مراقبة محتوى الأنترنت، حماية الخصوصية، صعوبة معرفة وتتبع المجرمين وغيرها من قضايا الأمن السيبراني.

من جهة أخرى، برزت قضية حوكمة الأنترنت واتهام الصين وروسيا للولايات المتحدة الأمريكية بالسيطرة على منظمة ICAAN مما يجعل الأنترنت فضاءً أمريكياً وليس فضاءً عالمياً حراً.

3. طبقة التطبيقات والبرامج: وتتكون هذه الطبقة من مجموعة كبيرة من البرامج الحاسوبية وتطبيقات الهاتف المحمول والتي تمكن المستخدمين من استعمال الشبكة (الأنترنت) دون الحاجة إلى معرفة البرمجة والأكواد المعقدة، أي أنها الطبقة التي تربط بين ما يفهمه الإنسان وما تفهمه الآلات، تُقسم هذه الطبقة إلى ثلاث 03 مجموعات رئيسية هي:

- أنظمة التشغيل (Operating systems): وهي البرامج الضرورية لتشغيل الأجهزة.
- برامج المستخدم ومواقع الأنترنت وتطبيقات الهاتف المحمول.
- البرامج الخبيثة (Malwares): مثل الفيروسات وبرامج التجسس وغيرها.

تشير الإحصائيات إلى أن ما يقارب 90% من الأجهزة الرقمية في العالم تستخدم أنظمة التشغيل التي طورها شركات أمريكية (Android المملوكة لـ Google، Windows لشركة Microsoft، iOS لشركة Apple)¹، بالنسبة لمحركات البحث يسيطر Google على أكثر من 80% من عمليات البحث في الأنترنت، كما يتصدر Facebook قائمة تطبيقات التواصل الاجتماعي بما يقارب ثلاثة 3 ملايين مستخدم، يليه على التوالي برامج Youtube وInstagram،

¹ المزيد من الإحصائيات والتفاصيل حول استخدام أنظمة التشغيل على الرابط: <https://bit.ly/3OL7ZiW>.

ثم البرنامجين الصينيين Wechat و TikTok بعدد مستعملين يفوق مليار شخص¹، كما لا توجد إحصائيات دقيقة حول البرامج الخبيثة، إلا أنه ما يُعرف بالتهديدات السيبرانية المتقدمة والمستمرة (APT) تقوم بها دول مثل الولايات المتحدة، الصين، روسيا، إسرائيل، كوريا الشمالية أو مجموعات تدعمها هذه الدول.

ومما سبق، فالبرامج والتطبيقات تفرض تحديات اقتصادية واجتماعية وسياسية وأمنية، حيث إن طبيعة البرنامج أو التطبيق تحدد وتوجه سلوك المستخدم، فهي تعمل على فرض سياسات معينة قد تتعارض مع سياسات الدول، هذا إضافة إلى قضايا انتهاك الخصوصية الفردية وجمع البيانات الشخصية واستعمالها لأغراض تجارية وأمنية، وقضايا التجسس بشقيه الاقتصادي والسياسي.

4. طبقة المحتوى (البيانات والتفاعل): وتعتبر من الطبقات المهمة ويرجع ذلك إلى أنها الطبقة المرئية للجميع، فهي الطبقة التي تتم فيها التفاعلات الاجتماعية والاقتصادية والسياسية بين المستخدمين، فالمحتوى (المعلومات) أصبح ذا أهمية بالغة في الشؤون العالمية، ف قوة المعلومات تُستعمل للتأثير على البيئة السياسية والاجتماعية، ولخلق النمو الاقتصادي والثروة، وكذلك لتعزيز ميزة صنع القرار على المنافسين²، إن القدرة على التحكم في المحتوى تلعب دوراً حاسماً في توجيه سلوك المجتمعات سواءً لأغراض اقتصادية أو سياسية أو أمنية.

كما أن عمليات السيطرة على البيانات بأنواعها: البيانات المتاحة للجمهور (Open Data) والبيانات الضخمة (Big Data) والبيانات الوصفية (Meta Data) تتم عبر جميع طبقات الفضاء السيبراني السابقة الذكر، حيث يوجد تنافس شديد حول البيانات بين شركات التكنولوجيا الكبرى ومن ورائها الدول ووكالات الاستخبارات، لكن ما يجعلها قوة حقيقة هي القدرة على تحويلها إلى معلومات مفيدة والذي يتم عبر تكنولوجيات معقدة ومتطورة، هذه التكنولوجيات تشمل عدة مجالات منها: تقنيات الجيل الخامس، الحوسبة الكمومية، التنقيب عن البيانات، تعلم الآلة، الذكاء الاصطناعي وغيرها³، ومن المهم التنويه إلى أن هذه المجالات هي محور الصراع الصيني الأمريكي حول التكنولوجيا المتقدمة.

¹ يقدم موقع Wearesocial إحصائيات وتقارير سنوية حول استعمال التكنولوجيا في العالم: <https://bit.ly/3sgqnse>.

² Eric Rosenbach, Katherine Mansted, **The geopolitics of information**, Belfer Center for Science and International Affairs, 2019, p 2.

³ Ibid, pp 3-4.

المطلب الثاني : نوموس الفضاء السيبراني

يعتبر كارل شميدت من المفكرين الأوائل الذين استعملوا المصطلح اليوناني "نوموس" والذي يُقصد به التقسيم والتوزيع الأول للأراضي¹، أو كما يُعبر عنه **دوغين** بالعلاقة بين المكان والمجموعة الإنسانية والنظم السياسية والحقوقية²، فالنوموس هو الشكل المباشر الذي يجعل النظام السياسي والاجتماعي للشعب مرئياً مكانياً، كما أن هناك من يستعمل مصطلح "النوموس" للدلالة على "القانون" أو "التنظيم".

وعليه فإن دراسة نوموس الفضاء السيبراني تتعلق بفهم كيفية تشكل وتطور التنظيم داخل الفضاء السيبراني، وما هو تأثيره على الحدود والتقسيمات الجغرافية الموجودة مسبقاً، ومن ثم معرفة طريقة توزيع الحقوق والقوانين النازمة للسيطرة والسيادة في هذا الفضاء الجديد.

الفرع الأول: تطور نوموس الفضاء السيبراني

يجادل "شميدت" أن سيرورة التاريخ تفرض ظهور نوموس جديد يرافق الأحداث العالمية كعملية أساسية لتقسيم الأراضي والذي يعتبر ضرورياً لكل عصر جديد أو حقبة تاريخية لتعايش الشعوب والدول والحكام والقوة³، وبناءً عليه فإن نوموس الفضاء السيبراني والذي هو من صنع الإنسان كان في صيغته البدائية فكرةً عسكرية، واضحة الحدود والمعالم، تسيطر عليه وزارة الدفاع الأمريكية ويخضع لقوانينها.

لكن لم يمر وقت طويل حتى حدث التقسيم الأول لهذا الفضاء، حيث أصبحت شبكة وزارة الدفاع شبكة مستقلة، وبدأ التقنيون والعلماء ببناء أكبر شبكة عالمية، كان الكود الناظم لهذه الشبكة هي الشيفرة في حد ذاتها، وكانت الاختيارات التقنية هي الموجه لتطور الشبكة مرتكزة على مبدأ **اللامركزية** أي غياب أي نوع من التحكم أو السيطرة المركزية، ومبدأ **الحرية** أي غياب أي تنظيم أو رقابة على المحتوى، حتى أن "جون بيرلي بارلو" في إعلانه الشهير "استقلال الفضاء السيبراني"⁴ أكد على أن الفضاء السيبراني هو الموطن الجديد للعقل، وأن الحكومات التقليدية ليس لها الحق في السيطرة عليه، كما جادل بأن مواطني هذا الفضاء يسعون لعقد اجتماعي جديد

¹ Carl Schmitt, **Op.cit**, p 67.

² ألكسندر دوغين، مرجع سابق، ص 120.

³ Carl Schmitt, **Op.cit**, p 78.

⁴ John Perry Barlow, **Op.cit**.

خاص بهم، لقد بُني الفضاء السيبراني على أسس الإنفتاح، الإدارة الذاتية، حرية التبادل والتعبير، والقاعدة الأسمى هي السعي لانتشار المعلومة دائما ومهما كانت الصعاب، لقد أصبح الفضاء السيبراني في هذه الحقبة أقرب إلى المشاعات العالمية.

لكن مع بداية الألفية الجديدة عرف الفضاء الرقمي تحولات جذرية، حيث حدث التقسيم الثاني لهذا الفضاء، فمع تزايد عدد الفاعلين وأصحاب المصلحة، تنامت محاولات الحكومات والجيوش -التي اعتبرته البعد الخامس للحرب- للسيطرة على الفضاء السيبراني، فقد أُعتبر كإقليم للغزو، للسيطرة، للمراقبة، للامتلاك، إقليم يجب احترام حدوده، سيادته وقوانينه¹، جرت محاولات لفرض السيادة على الشبكات داخل إقليم الدولة، وأصبحت قضايا الأمن السيبراني على رأس أولويات الدول والحكومات، واشتد الجدل والصراع بين الحكومات والعسكريين حول قضايا الأمن القومي والحدود والسيادة، وبين شركات التكنولوجيا والأفراد حول قضايا الحرية والخصوصية، وعليه فإن نوموس الفضاء السيبراني في هذا العصر لا يزال يتطور ويتحول بسرعة ولم يستقر بعد على طبيعة ثابتة.

الفرع الثاني: حدود جديدة أم فضاء بلا حدود

الحد السياسي هو ذلك الخط الفاصل بين الدول الذي يظهر على الخرائط، والحد يعني المنع والفصل بين الدولة والدول المجاورة لها، وداخل هذه الحدود تمارس الدولة سلطاتها، ويكون لها حق الانتفاع بها واستغلالها²، وللحدود وظيفة تنظيمية للإقليم الجغرافي وفرض القانون والسياسة، وتشمل أهميتها الأبعاد السياسية والأمنية، الاقتصادية، الاجتماعية والثقافية.

من جهة أخرى، قامت أغلب الحروب والصراعات حول الحدود، فهي تُعتبر مشكلة معقدة لم تعد ترتبط فقط بالأرض ولكن امتدت إلى البحر والجو والفضاء الخارجي³ والفضاء السيبراني كما في دراستنا هاته، إن فكرة الحدود المتغيرة رافقت تطور الجماعة البشرية، فالمدرسة العضوانية الألمانية (انظر المبحث الأول من هذا الفصل) كانت تقوم على مبدأ التوسع والنمو على حساب

¹ Frédérick Douzet, Op.cit.

² هارون علي أحمد ، أسس الجغرافيا السياسية، القاهرة: دار الفكر العربي، 1998، ص 171.

³ محمد رياض، مرجع سابق، ص ص 147-148.

الدول المجاورة، فرائزل كان يرى أن الحد هو العضو الطرفي للدولة، وتغيراته ماهي إلا دلالة على توسع الدولة وقوتها أو انكماشها وضعفها¹.

واستناداً إلى ما سبق، وبما أن ما يُميز الفضاء السيبراني هو سرعة نقل المعلومات دون التقيد بالزمن أو الجغرافيا، كما أنه يخلق مجالاً جديداً للنشاط والتفاعل البشري أطلق عليه وصف "فضاء بلا حدود" كسرد مضاد للجغرافيا المكانية والقانونية والسياسية، فالفضاء السيبراني يخترق الحدود السياسية للدولة ويُقوض -يحد من جدوى وشرعية- القوانين والقواعد الداخلية²، ويرسم حدوداً جديدة هي الشاشات والمستخدمون، ذلك لأن الفضاء السيبراني يُضعف بشكل جذري العلاقة بين الظواهر والتفاعلات ذات الأهمية القانونية والموقع الجغرافي، لقد أدى ظهور الشبكات إلى تدمير الرابط بين الموقع الجغرافي و: أولاً، قوة سيطرة الحكومات على سلوك الأفراد والكيانات التي تعيش على الرقعة الجغرافية، ثانياً، آثار السلوك والتفاعل السيبراني على الأفراد أو الأشياء، ثالثاً، شرعية الجهود السيادية المحلية لتنظيم الظواهر الداخلية والعالمية، رابعاً، القدرة على وضع وتطبيق القواعد.

وبالتالي، فالفضاء السيبراني يغير الطريقة التي ينظر بها البشر إلى الحدود، فهو يدمر مفاهيم الحدود التقليدية ونظام وضع القواعد على أساس الحدود بين المساحات المادية، ويعيد بناء مفهوم جديد للحدود، فالتحديات والمخاطر التي رافقت انتشار الفضاء السيبراني عبر حدود الدول جعل منه ظاهرة أمنية متعددة للحدود القومية تحت ضغط العولمة، كما حفز الانكشاف الحدودي الحكومات ومحاولة إعادة ضبط الحدود وبسط السيادة، ويظهر ذلك جلياً في تكثيف إجراءات المراقبة وفلترة تدفق المعلومات والتحكم في البنية الفيزيائية للشبكة، فالصين عبر "جدار الحماية العظيم" تسطير على تدفق الأنترنت من وإلى البلاد، وكوريا الشمالية تفرض قيوداً متشددة للوصول إلى المحتوى خارج البلاد، إيران وروسيا تسعى لتشغيل أنترنت داخلية (وطنية) غير مرتبطة بالشبكة العالمية³، وهو ما يؤكد سعي الدول لفرض سيادتها وتحقيق مصالحها في الفضاء السيبراني داخل الرقعة الجغرافية التي تشغلها.

¹ جيرار ديسوا، مرجع سابق، ص 99.

² David R. Johnson, David Post, "Law and borders: The rise of law in cyberspace", *stanford law review*, Vol 48, N° 5 ,1996, pp 1367-1402.

³ Percy Judkins Blount, *Reprogramming the world: cyberspace and the geography of global order*, E-International Relations publishing, Bristol, England, 2016, p 82.

المطلب الثالث: أمانة الفضاء السيبراني

يعتبر مفهوم الأمانة Securitization من المفاهيم الأساسية في حقل الدراسات الأمنية والاستراتيجية والعلاقات الدولية، ويعود الفضل إلى مدرسة كوبنهاغن في بناء مفهوم ونظرية الأمانة حيث يرى كل من "أولي ويفر" و"باري بوزان" أن الأمانة هي ذلك الخطاب -الذي هدفه الإقناع- الذي يضفي طابع التهديد على موضوع معين¹، ويعمل الخطاب على الاستدلال بوجود تهديد وجودي (مادي أو معنوي) من أجل إقناع الجمهور المستهدف، حيث يكون فعل الأمانة أكثر نجاحاً كلما كان أكثر إقناعاً للجمهور، والغاية منه هو الوصول إلى شرعنة اللجوء إلى ترتيبات استثنائية في التعامل مع القضية، ونقلها من مجال السياسات العامة العادية إلى مجال السياسات الطارئة.

الفرع الأول: أمانة الفضاء السيبراني بين الحكومات ومنظمات حقوق الإنسان

تقننت مبكراً دول قليلة مثل الولايات المتحدة الأمريكية، روسيا والصين، إلى تهديدات ومخاطر الفضاء السيبراني، ففي تسعينيات القرن المنصرم اقتضت جهود مواجهة التهديدات السيبرانية على الجانب التقني، وحُصرت في تطوير البرامج والأجهزة من قبل التقنيين والعسكريين، لكن مع بداية الألفية الجديدة وخصوصاً بعد أحداث 11 سبتمبر حدث تحول في الاستراتيجية الأمنية في الولايات المتحدة الأمريكية (خاصة محاربة الإرهاب)، وحدثت نقلة نوعية في خطاب الأمانة رافقه اتخاذ الكثير من التدابير والإجراءات أبرزها المراقبة الشاملة في وعبر الفضاء السيبراني، ومن ثم انتشر خطاب الأمانة إلى مختلف دول العالم، والذي يُعرّف بأنه تحويل (قضايا) الفضاء السيبراني إلى دائرة اهتمام الأمن القومي².

وعطفاً على ما سبق، فإن مزيجاً من الابتكارات التكنولوجية المتسارعة والظروف الجيوبوليتيكية المتقلبة جعل من الحكومات ومن ورائها وكالات الأمن والاستخبارات تدرك أن التهديدات الناشئة عن هذه التطور الرقمي ستكون لها آثار أمنية وسياسية واقتصادية ومجتمعية مدمرة³، فالتشبيك الكثيف والاستعمال الواسع للتكنولوجيا الرقمية في مختلف القطاعات الصناعية

¹ Barry Buzan, et al, **Security: A new framework for analysis**, Lynne Rienner Publishers, 1998, p 25.

² Ronald Deibert, "Cybersecurity: the new frontier", **Foreign Policy**, 2012, pp 45-58.

³ Lene Hansen, and Helen Nissenbaum, "Digital disaster, cyber security, and the Copenhagen School", **International studies quarterly**, Vol 53, N°4, 2009, pp1155-1175.

والمالية والخدماتية جعل الخبراء الأمنيين يدقون ناقوس الخطر حول مدى سلامة وتأمين البنية التحتية الرقمية من الهجمات السيبرانية التي قد تشنها دول معادية أو مجموعات إرهابية، خاصة وأن المجموعات الإرهابية تستغل الفضاء السيبراني للدعاية والتجنيد، ومن جهة أخرى، مع تسارع وانتشار عمليات المراقبة الشاملة تعالت الأصوات حول قضايا انتهاك الخصوصية وحماية البيانات الشخصية للأفراد.

عناصر الأمنة: يمكن تحديد أربعة عناصر أساسية لعملية الأمنة هي: الفاعل (المؤمنن)، التهديد، الموضوع (المُهدّد) والجمهور، وبتطبيق ذلك على الفضاء السيبراني نجد مجموعة متنوعة من الجهات الفاعلة التي تسعى لإقناع الجماهير بأنها تواجه تهديداً وجودياً، أهمها: الحكومات ووكالات الأمن والاستخبارات، ومنظمات حقوق الإنسان وحماية الخصوصية.

أولاً، **الحكومات ووكالات الأمن والاستخبارات** التي لها القدرة على الوصول إلى جمهور أوسع، كما يدعمها متحدّثون أمنيون موثوقون، ف خبراء وكالات الأمن والاستخبارات يملكون قدراً عالياً من المصداقية والسلطة والخبرة الفنية، ففي تسعينيات القرن الماضي في الولايات المتحدة الأمريكية مهد الأنترنت تزايد الاهتمام بتهديدات الفضاء السيبراني من قبل السياسيين والشركات والإعلام، فكان الحديث حول "بيرل هاربور سيبرانية" و"أسلحة الدمار الشامل السيبرانية"، وبعد أحداث الحادي عشر من سبتمبر طغت خطابات السياسيين والأمنيين حول قضايا الأمن السيبراني، حماية البنية التحتية الرقمية، المراقبة الشاملة واستخدام الإرهاب للقرصنة¹، بداية من الرئيس كلينتون والأمر التنفيذي رقم 13010 المتعلق بحماية البنية التحتية الحرجة من التهديدات السيبرانية، ومروراً بالأمر التنفيذي 13231 المتعلق بحماية البنية التحتية الحرجة في عصر المعلومات في عهد جورج بوش، ووصولاً إلى مذكرة حول تحسين الأمن السيبراني للأمن القومي ووزارة الدفاع وأنظمة مجتمع الاستخبارات في عهد الرئيس الأمريكي الحالي جوزيف بايدن²، كانت كلها مليئة بالتحذير من التهديدات السيبرانية ومحاولة إقناع الجمهور والسلطة التشريعية وشركات التكنولوجيا بمدى التهديد والعمل على انتزاع رضاهم تجاه التدابير والإجراءات المتخذة لمواجهة، الصين من جهتها سعت إلى منع وصول مواطنيها إلى بعض مواقع الأنترنت التي اعتبرتها تهديداً للاستقرار السياسي والمجتمعي، وغالباً ما يتم التركيز على الأمن السيبراني وحوكمة

¹ Ibid.

² المعلومات مستقاة من موقع The American Presidency Project والذي يحتوي على جميع التصريحات والخطب والوثائق الخاصة بفرق العمل للرؤساء الأمريكيين.

الأنترنت في خطاب المسؤولين الصينيين حتى أن الرئيس "تشى" يرأس شخصياً المجموعة الرائدة لأمن الأنترنت والمعلوماتية المركزية في الصين، روسيا، من جهتها أدرجت أمن المعلومات في استراتيجية أمنها القومي، وكانت قضايا الفضاء السيبراني حاضرة في المفاوضات بينها وبين الولايات المتحدة حول السلام والأمن العالميين، حلف الناتو بدوره عدّل من استراتيجيته واعتبر الفضاء السيبراني مجالاً لنشاطاته خاصة بعد الهجمات السيبرانية على إستونيا في 2007.

ثانياً، **منظمات حقوق الإنسان وحماية الخصوصية الرقمية**، حيث لعبت التسريبات التي قدمها المبلغون دوراً مركزياً في فضح عمليات الجمع غير المبررة والكثيفة للبيانات الشخصية للأفراد، وكذا الاستعمال السيء وغير القانوني لها، ولعل أبرز الحالات ما قام به إدوارد سنودن الذي كشف عن برنامج المراقبة الشاملة والمكثفة التي تقوم به وكالة الأمن القومي الأمريكية NSA، وكذلك **كريستوفر ويلي** الذي كشف تلاعبات شركة "كامبريدج اناليتيكا" ببيانات النخبين الأمريكيين¹، هذه التسريبات وصلت إلى جمهور واسع من مستخدمي الأنترنت، كما جعلت المنظمات الحقوقية ومنظمات حماية الخصوصية تدق ناقوس الخطر حول مدى احترام الحكومات والشركات على حد سواء لخصوصية الأفراد ومدى الحماية التي يقدمونها لبياناتهم، وهذا ما حفز الأفراد والشركات على تغيير سلوكياتهم تجاه الخصوصية وحماية البيانات، حيث أفتتح الكثيرون بأهمية اتخاذ احتياطات أكبر فيما يتعلق بأمن بياناتهم، وشراء المنتجات ذات العروض الأمنية الجيدة، ومعارضة التشريعات الجديدة بشأن مراقبة الحكومات ووكالات الأمن للنشاطات في الفضاء السيبراني، كما حفز شركات التكنولوجيا على السعي إلى تنفيذ "حلول تقنية" للمراقبة كزيادة مستوى التشفير²، والتي تحد من قدرة الحكومات على الوصول إلى بيانات المستخدمين.

الفرع الثاني: المعضلة الأمنية السيبرانية - من الأمنة إلى العسكرة -

صاغ عالم السياسة الأمريكي **جون هارتز** مصطلح "المعضلة الأمنية" لأول مرة في مقاله "Idealist internationalism and security dilemma"³، ثم توسع استخدام المصطلح خاصة عند مفكري التيار الواقعي في العلاقات الدولية، فالمعضلة الأمنية أو المأزق الأمني هي تلك

¹ Dominika Popielec, "From Edward Snowden to Christopher Wylie: The Face of the Second Generation Whistleblowing", *Zeszyty-Prasoznawcze*, t. 62, nr 3(239), s. 39-51, Kraków 2019, pp 46-47.

² Steven Hersee, *The Cyber Security Dilemma and the Securitisation of Cyberspace*, Dissertation, Royal Holloway, University of London, 2019, p 93.

³ John H Herz, "Idealist internationalism and the security dilemma", *World politics*, Vol 2, N° 2, 1950, pp 157-180.

الحالة من الخوف الهوبزي كما يسميها هيربرت بيتر فيلد والتي تنشأ في حالة الفوضى ويغذيها الخوف وعدم اليقين المتبادل بين فاعلين مدفوعين باحتياجاتهم الأمنية الخاصة، فيسعى كل طرف لتجميع القوة وهو ما يؤدي في النهاية إلى تفاقم انعدام الأمن.

وبناءً على ماسبق، فالفضاء السيبراني تتوافر فيه ظروف الفوضى، الخوف وعدم اليقين، إضافة إلى خصائص المجهولية (العدو مجهول) والسرعة والانتشار (سرعة انتشار التهديد) وهذا ما يجعل المعضلة الأمنية تتفاقم أكثر، فبعد التحذيرات وخطاب الأمانة وتحت تأثير ضغوطات الأمن القومي توجهت الحكومات مباشرة نحو تعديل استراتيجيات الأمن القومي ووضع استراتيجيات خاصة بالأمن السيبراني، ففي الولايات المتحدة الأمريكية كانت أول مسودة لاستراتيجية الأمن السيبراني في 2001 وتم اعتمادها في 2003، وفي الصين كان التحول الاستراتيجي في العقيدة العسكرية للجيش الصيني قد بدأ منذ حرب الخليج الثانية 1990 ولكن التأكيد جاء في الكتاب الأبيض للجيش الصيني في 2009، حيث أقر أن الهدف الاستراتيجي هو بناء جيش معلومات قادر على الانتصار في حرب المعلومات¹، كما تم تشكيل الجيوش والوحدات الخاصة بالحروب السيبرانية، حيث أقر الرئيس الأمريكي "ترمب" في 2018 تشكيل قيادة عسكرية مستقلة خاصة بالفضاء السيبراني²، كما توجد وحدات وهيئات تختلف مسمياتها في الكثير من دول العالم، وهو ما جعل من عملية عسكرة الفضاء السيبراني تتزايد وتنتشر بشدة.

لقد كانت الهجمات السيبرانية على استونيا 2007 والتي أتهمت روسيا بالوقوف وراءها إيذاناً ببدء عصر جديد من الحروب، وجعلت من الدول تأخذ تهديدات الفضاء السيبراني على محمل الجد، لكن أبرز الهجمات السيبرانية كان فيروس "ستاكسنت Stuxnet" الذي هاجم المفاعلات النووية الإيرانية، وقد أتهمت الولايات المتحدة وإسرائيل بتطوير هذا الفيروس، والذي جعل النقاش يحتدم حول ما إذا كان يُعتبر من أعمال الحرب أو هو دون ذلك، ومدى إمكانية تطبيق القانون الدولي على الهجمات السيبرانية، إضافة إلى قضايا الحد من انتشار الأسلحة السيبرانية (مثل: برنامج بيغاسوس) واعتبارها أسلحة دمار شامل³.

¹ Information Office of the State Council of the People's Republic of China, **China's National Defense in 2008**, January 2009, Beijing, URL: <https://bit.ly/3E6pWmX>.

² تاريخ القيادة السيبرانية الأمريكية على موقعها على الإنترنت: <https://bit.ly/3YKJ1EQ>.

³ Cristian Barbieri, Jean-Pierre Darnisand Carolina Polito, **Non-proliferation Regime for Cyber Weapons. A Tentative Study**, Istituto Affari Internazionali, March 2018, p 6.

المطلب الرابع: السيادة السيبرانية

الفرع الأول: تطور مفهوم السيادة السيبرانية

تتطور فكرة السيادة مع تطور المجتمعات البشرية، والسيادة بمفهومها الحديث وليدة معاهدة واستغاليا 1648، كما تُعد من الركائز الأساسية التي يقوم عليها القانون الدولي وتُدار على ضوءها العلاقات الدولية المعاصرة، ولا يوجد اتفاق بين الباحثين حول مفهوم المصطلح، فالسيادة مفهوم ديناميكي ومتطور ومرن إلا أنه في العموم يُشير إلى السلطة العليا التي تتمتع بالاستقلالية والإرادة وعدم الخضوع لأي سلطة خارجية والتي لها الحق في تنظيم وإدارة الإقليم¹، السكان والموارد، ويترتب على السيادة أربعة حقوق أساسية هي الاستقلال، المساواة، الحق في الدفاع عن النفس والحق في التشريع، كما تلتزم الدول ذات السيادة باحترام سيادة الدول الأخرى، عدم الاعتداء، عدم التدخل في الشؤون الداخلية للدول.

إلا أنه في عصرنا الرقمي، لطالما أُعتبر الفضاء السيبراني (أو الأنترنت) فضاءً عاماً حراً وغير مركزي، يتجاوز الحدود والسلطات القضائية المحلية، لذلك فإن طبيعة الفضاء السيبراني وخصائصه الفريدة تُقوضان الركائز الأساسية لمفهوم السيادة، فهندسة الفضاء السيبراني مبنية على ضمان انتقال المعلومات بحرية عبر التشبيك المكثف، وهذا ما يُصعب على الدول عملية ضبط الحدود في هذا الفضاء كما يُميع مفهوم الإقليم الوطني، أما بالنسبة للمواطنين فقد ظهر مفهوم المواطن الرقمي، والذي يملك هوية أو هويات متعددة في فضاءات إفتراضية متباينة كما يخضع لقوانين وقواعد مُشغلي تلك المنصات والتطبيقات، كما أن ظهور اقتصاد جديد مبني على المعرفة والتكنولوجيا جعل من هذه الموارد الجديدة تحت سيطرة ونفوذ شركات التكنولوجيا الكبرى، وهو ما جعل من سيادة الدولة في هذا المجال أمراً مشكوكاً فيه.

وبناءً على ماسبق، ظهرت دعوات إلى تطوير مفاهيم مثل "سيادة البيانات" و"السيادة الرقمية" و"السيادة السيبرانية"² كإمتداد طبيعي لسيادة الدولة في الواقع المادي، حيث تمتلك الدول القدرة

¹ أيمن أحمد الورداني، حق الشعب في استرداد السيادة، القاهرة: مكتبة مدبولي، 2008، ص 43.

² ظهرت مصطلحات عديدة تربط بين السيادة والمجال السيبراني مثل: السيادة التكنولوجية، السيادة الرقمية، سيادة البيانات، سيادة الشبكات، سيادة الأنترنت ... وغيرها، انظر:

Stéphane Couture, Sophie Toupin, What Does the Concept of 'Sovereignty' Mean in Digital, Network and Technological Sovereignty?, **GigaNet: Global Internet Governance Academic Network, Annual Symposium**, 2017.

على التحكم في البنية التحتية السيبرانية الموجودة على إقليمها والسيطرة على بياناتها وبيانات مواطنيها، فالسيادة السيبرانية يجب أن تترث السمات الأساسية للسيادة الوطنية، ويقدم "بيكسين فانغ" تعريفاً شاملاً للسيادة السيبرانية ينقل فيه ركائز السيادة الأساسية إلى الفضاء السيبراني، حيث يعتبر أن "سيادة الدولة على الفضاء السيبراني تستند إلى أنظمة تكنولوجيا المعلومات والاتصالات الخاضعة لتشريعات الدولة، تتكون حدودها من مجموعة من منافذ الشبكة الداخلية للدولة المتصلة بشبكات الدول الأخرى، تخضع المنشآت المكونة للفضاء السيبراني والبيانات المنقولة وتشغيل البيانات لتشريعات وإدارة الدولة التي تنتمي إليها، تمارس سيادة الفضاء الإلكتروني لحماية العمليات المختلفة للبيانات من خلال الأدوار السيبرانية"¹، كما يجادل "فانغ" أن الحقوق والمبادئ المترتبة عن السيادة في الواقع المادي تنتقل آلياً إلى الفضاء السيبراني؛ فلا يجوز التدخل أو السيطرة على عمليات البنية التحتية الرقمية لدولة أجنبية، فمن حق الدولة حماية الفضاء السيبراني الخاص بها من العدوان، كما يجب على الدول إظهار الاحترام المتبادل لسيادة الفضاء السيبراني لبعضها البعض، ولا يجوز بحال من الأحوال لدولة ما غزو الفضاء السيبراني لدولة أخرى، كما لا يجوز لدولة أن تتدخل في شؤون إدارة الفضاء السيبراني لدولة أخرى، لأن الدول تتمتع بوضع متساو كمبدأ من مبادئ سيادة الفضاء السيبراني².

الفرع الثاني: جدلية تبني مفهوم السيادة السيبرانية

يقول "كراسنر" يستدعي الحكام مبادئ السيادة -الواستقالية- حين تحقق مصالحهم ويستبعدونها حين تتعارض وتلك المصالح³، وهذه المقولة تنطبق أيضاً على السيادة السيبرانية، فإذا كانت السيادة الواستقالية جاءت من أجل منع الصراع بين الدول فإن السيادة السيبرانية خلقت نزاعاً وصراعاً بين الدول حيث تشكل معسكرين متباينين؛ المعسكر الأول، يؤيد إقرار مبدأ السيادة في الفضاء السيبراني بقيادة الصين وروسيا، والمعسكر الثاني، مناوئ لها ويطالب بجعل الفضاء السيبراني فضاءً حراً لامركزياً، بقيادة الولايات المتحدة الأمريكية وحلفائها وشركات التكنولوجيا الكبرى.

إلا أن مصطلح "السيادة السيبرانية" سيطر على الكتابات الأكاديمية والتصريحات السياسية خاصة بعد خطاب الرئيس الصيني "شي جي بينغ" في المؤتمر العالمي الأول للإنترنت في عام 2014 والذي دعا فيه إلى "احترام السيادة السيبرانية".

¹ Binxing Fang, Fang Zhang, *Op.cit*, p 85.

² *Ibid*, p 85-86.

³ Stephen D Krasner, *Sovereignty*, Princeton University Press, 1999, p 69.

وبطبيعة الحال فإن المعسكر المطالب بتطبيق السيادة في الفضاء السيبراني له مبرراته، حيث إن طبيعة وجدة التهديدات والمخاطر السيبرانية جعلت من الفضاء الرقمي من أكبر المهددات للأمن القومي للدول، كما أن هذه التهديدات تطال مصالح الدولة في مختلف المجالات أو الأبعاد السيادية نذكر منها¹:

البعد السياسي: وفقاً للسيادة الواسطالية فإن للدولة الحق في الهيمنة على الإقليم والمواطنين والتشريع والإدارة، لذلك فإن التفاعلات السياسية التي تتم عبر الفضاء السيبراني داخل الدولة أو مع الدول الأخرى يجب أن تخضع للقوانين الداخلية والمبادئ والأعراف الدولية، لذلك فإن عمليات التأثير على المواطنين في دولة أجنبية عبر نشر الأخبار الكاذبة والبروباغندا تُعتبر محاولة لزعزعة النظام السياسي من الداخل وتشكل تهديداً فعلياً للنظام السياسي، وبالتالي فإن السيادة السيبرانية تصبح حقيقة لا مفر منها ولا يمكن إنكارها على المستوى السياسي.

البعد العسكري: تُشكل الكثير من الدول وحدات أو جيوشاً سيبرانية، والعديد من الجيوش في العالم تعتبر الفضاء السيبراني مجالاً للحرب، وبما أن مهمتها الأساسية هي الدفاع وحماية مصالح الدولة وأمنها القومي في الفضاء السيبراني، أو بعبارة أخرى، حماية السيادة الوطنية، فإن السيادة السيبرانية موجودة في الواقع كما توفر أيضاً أساساً قانونياً للجيش للتواجد في الفضاء السيبراني.

البعد الاقتصادي: تواجه الدول عقبات في ممارسة سلطتها الاقتصادية في الفضاء السيبراني، ذلك أن التجارة عبر الأنترنت عابرة للحدود مما يصعب عمليات تحصيل الضرائب وإدارتها، وحماية حقوق المستهلكين ومصالحهم، وتنظيم مختلف العلاقات التجارية، وخاصة إدارة المعلومات والبيانات التي أصبحت مورداً له قيمة اقتصادية، وهذا ما يستوجب إنشاء آلية لإدارة اقتصاد الشبكة، ويثبت حاجة الدولة للسيادة السيبرانية على المستوى الاقتصادي.

البعد الثقافي: رغم التنوع الثقافي في العالم إلا أنه غالباً ما توجد صراعات وعدم توافق بين الثقافات المختلفة، لذلك تتخبط الدول في عمليات الدفاع عن ثقافتها وترسم "الخطوط الحمراء" التي ينبغي لمواطنيها عدم تخطيها، لكن تحت وطأة العولمة والتشبيك بين الأفراد في الفضاء السيبراني تضحل هذه الخطوط الحمراء، لذلك فالدول تسعى لفرض سيادتها في هذا الفضاء حفاظاً على ثقافتها من الزوال.

¹ Binxing Fang, Fang Zhang, Op.cit, p114-117 .

الاستقرار الاجتماعي: غالباً ما يتقاطع الفضاء المادي والسيبراني، وعليه فإن ما يحدث من جرائم أو تحريض في الفضاء السيبراني يؤثر بشكل كبير على الاستقرار الاجتماعي، لذلك لا يجب تجاهل النشاطات السيبرانية الخبيثة بل يجب أن تخضع للعقوبات القانونية التي تفرضها الدولة كأحد تطبيقات مبدأ السيادة.

في المقابل، يجادل الرافضون لمبدأ السيادة السيبرانية بأن مبدأ السيادة الواسطالية القائم على حق الدولة في الهيمنة على إقليمها الجغرافي يتعارض مع فلسفة الفضاء السيبراني والتي تقوم على الربط المكثف للشبكات وحرية انتقال المعلومة عبر الحدود متحدية الجغرافيا والمسافات، لذلك فإن أي فرض للسيادة في الفضاء السيبراني ستكون نتيجته تقسيم (أو بلقنة¹) هذا الفضاء ويفقده سمته الأساسية والغاية من صنعه وهي التواصل وتبادل المعلومات.

بالإضافة إلى أن تطبيق السيادة السيبرانية خاصة في دول استبدادية قد تمنح الحكام المستبدين أداة جديدة - المراقبة الشاملة، فرض قوانين خاصة، التحكم في المحتوى - لزيادة سيطرتهم واضطهادهم لشعوبهم² وهذا ما يتعارض مع مبادئ حقوق الإنسان العالمية التي تسعى لتعزيز حرية التعبير.

وأخيراً، يتعارض مفهوم السيادة السيبرانية بصيغته الصينية-الروسية مع نموذج حوكمة الأنترنت الذي تقدمه الولايات المتحدة الأمريكية وحلفاؤها والذي يتمحور حول إسناد مهمة تنظيم ورسم السياسات في الفضاء السيبراني إلى مجموعة متعددة من أصحاب المصلحة³ والتي تشمل شركات التكنولوجيا، القطاع العام، القطاع الخاص، المنظمات والمجتمع المدني.

الفرع الثالث: قيود تطبيق السيادة السيبرانية

بغض النظر عن الداعين لتطبيق مبدأ السيادة السيبرانية أو المعارضين له يواجه تطبيق هذا المبدأ وما يترتب عليه من حقوق إشكاليات وتحديات كبيرة في الفضاء السيبراني.

¹ Oxford Analytica, **Balkanisation of the internet will rise**, Emerald Expert Briefings oxan-db, 2021.

² Oxford Analytica, **Digital authoritarianism in Africa is evolving**, Emerald Expert Briefings oxan-db, 2022.

³ Wolfgang Kleinwächter, "Cybersecurity, Internet Governance, and the Multistakeholder Approach", **New Conditions and Constellations in Cyber**, 2021, pp 41-58.

أولاً، في الواقع المادي تعاني السيادة من تآكل وضبابية في التطبيق، حيث إن الدول تتباين في تفسيراتها لعمل ما أنه انتهاك للسيادة يستوجب رداً أو أنه يبقى دون عتبة التصعيد، وتزداد الضبابية في الفضاء السيبراني، فإذا كانت الدولة تعتق مبدأ السيادة الشاملة أو الجامعة فإن التفاعلات السيبرانية بحد ذاتها انتهاك للسيادة، كما يجادل "إيغان" بأن تصميم الأنترنت في حد ذاته قد يؤدي إلى بعض التعدي على الولايات القضائية السيادية الأخرى¹، فالسيادة بالمفهوم الواسع دائماً منتهكة، لذلك فمن غير الواضح كيف يمكن للدولة استعمال سلطاتها التقديرية فيما إذا كانت توظّر هذه الأنشطة السيبرانية ضمن انتهاكات السيادة التي تتطلب اتخاذ تدابير مضادة، أم تفضل التعامل معها بلغة الدبلوماسية والقانون الجنائي المحلي².

ثانياً، حتى بمراعاة طبيعة الفضاء السيبراني العابرة للحدود وبتطبيق منهج السيادة النسبية أو المرنة فإنه تواجهنا مشكلة تحديد المعايير التي على ضوءها يُعتبر نشاط ما انتهاكاً للسيادة، وما هي عتبة الحد الأدنى المسموح به، وفي أغلب الأحيان تعتمد الدول (الاتحاد الأوروبي، حلف شمال الأطلسي، فرنسا...) معايير تقييم للآثار الكمية/النوعية على الدولة والمجتمع مثل حجم الضرر المادي (السياسي، الاقتصادي والمجتمعي)، تعطيل البنية التحتية، حساسية البيانات المتضررة وغيرها³، إلا أن دولاً أخرى لا تتبنى أية معايير أو عتبة واضحة، ولا يوجد اتفاق لحد الآن حول المعايير المحددة لانتهاك السيادة، لذلك فانتهاك السيادة السيبرانية يبقى ممارسات ذاتية تحكمها السلطة التقديرية للحكومات.

ثالثاً، تبقى إشكالية أخرى هي اثبات انتهاك السيادة السيبرانية، فصفة المجهولية في الفضاء السيبراني تُعطي الفاعل خيارات كثيرة لإخفاء الهوية والمجال الجغرافي الذي ينشط فيه⁴، فيمكن لهجوم سيبراني ينتهك السيادة أن يتم انطلاقاً من عدة دول مروراً بدول مختلفة، وهذا ما يجعل إسناد تهمة انتهاك السيادة لدولة أو فاعل معين عملية غاية في الصعوبة.

¹ Brian J Egan, "International Law and Stability in Cyberspace", **Berkeley Journal of International Law**, Vol 35, Issue 1, 2017, pp 169-180.

² Harriet Moyihan, "The application of international law to state cyberattacks: Sovereignty and non-intervention", **Royal Institute of International Affairs**, 2019.

³ **Ibid.**

⁴ Mohamed Chawki, "Anonymity in cyberspace: Finding the balance between privacy and security", **International Journal of Technology Transfer and Commercialisation** Vol 9 Iss 3, 2010, pp 183-199.

الفرع الرابع: السيادة السيبرانية والصراع الجيوبوليتيكي العالمي

لا يُعد الجدل حول السيادة السيبرانية جدلاً أكاديمياً وتقنياً فحسب بل هو انعكاس للصراع الجيوبوليتيكي العالمي بين القوى الكبرى المتنافسة خاصة الولايات المتحدة الأمريكية من جهة والصين وروسيا من جهة أخرى حول قضايا حوكمة الأنترنت¹، فالصين وروسيا تتهمان الولايات المتحدة بالهيمنة على الفضاء السيبراني وإحتكار الميزات الاستراتيجية التي يوفرها، كما ترفضان مساعي حلف شمال الأطلسي - دليل تالين - لتطبيق القانون الدولي للحرب في الفضاء السيبراني وتعتبران أن هذه السياسات في جوهرها عسكرة لهذا الفضاء تحت غطاء الأمن السيبراني، ومن جهتها الولايات المتحدة وحلف شمال الأطلسي يضعان الصين وروسيا على رأس قائمة الدول التي تقوم بالهجمات الخبيثة في الفضاء السيبراني، وتعتبران الدعوة إلى تطبيق السيادة السيبرانية ما هي إلا محاولة من الدول الشمولية للسيطرة على الأنترنت وانتهاك حرية التعبير وحقوق الإنسان.

هذا الصراع الجيوبوليتيكي الذي أحدث شرخاً في الرؤى تجاه مبدأ السيادة السيبرانية، انعكس بدوره على أعمال فريق الخبراء الحكوميين التابع للأمم المتحدة حول "التحديات الحالية والمحتملة في مجال أمن المعلومات" وتطوير مبادئ وقواعد السلوك المسؤول للدول في الفضاء السيبراني، والذي لم يصل لحد الآن إلى معايير واضحة حول السيادة السيبرانية، كما أن الصين تنظم سنوياً المؤتمر العالمي للأنترنت في "ووتشن Wūzhèn" للدفاع عن مفهوم سيادة الحكومات كرد فعل على منتدى حوكمة الأنترنت (IGF) التابع للأمم المتحدة يسعى لمعالجة قضايا حوكمة الأنترنت بالاعتماد على أصحاب المصلحة المتعددين.

¹ Milton L. Mueller, "Against sovereignty in cyberspace", *International Studies Review*, vol 22, issue 4, 2020, pp 779-801.

انطلقت الجيوبوليتيكا من أطروحات وأفكار العضوانية الألمانية والتي اعتبرت الدولة كائناً حياً ينمو ويتطور وقدم الفصل في بدايته رؤية الآباء المؤسسين راتزل، هاوسهوفر، ماهان وماكندر، ومفاهيم قلب الأرض و صراع التالاسوكراتيا والتيلوركراتيا وغيرها، ثم تطرق إلى رؤية وأفكار الجيوبوليتيكيين المعاصرين وكيف حدث تحول الجيوبوليتيكا من التركيز على الحتمية الجغرافية الضيقة إلى تتبع النشاط البشري عبر فضاءات أوسع والتي من بينها الفضاء السيبراني.

وفي القسم الثاني للفصل قدمنا مفهوماً للفضاء السيبراني الذي يتكون من خلال تفاعل البيانات والآلات والبشر، ووضحنا أن التفاعلات الدولية أصبحت في مجملها تحدث في وعبر هذا الفضاء، حيث برز نوع جديد من القوة انتقلت وانتشرت بين العديد من الفاعلين في النظام الدولي، وهذا ما خلق صراعات جديدة بأدوات سيبرانية للهيمنة والنفوذ على الساحة الدولية.

واستفدنا من الأفكار التي طرحها الجيوبوليتيكيون المعاصرون حول الجغرافيا الماورائية لجعل الجزء الافتراضي من الفضاء السيبراني صالحاً للتحليل الجيوبوليتيكي، كذلك يسمح تقسيم الفضاء السيبراني إلى طبقات بتحديد الصراعات الجيوبوليتيكية في كل طبقة، فإن كانت قضايا السيطرة والحدود والسيادة واضحة إلى حد ما في البنية التحتية الفيزيائية للفضاء السيبراني فإن بقية الطبقات يسودها الغموض وعدم اليقين وتتنشأ فيها صراعات جيوبوليتيكية خاصة بين الولايات المتحدة الأمريكية والصين للهيمنة في وعلى هذه الطبقات.

الفصل الثاني

مضامين الصراع الأمريكي الصيني

في الفضاء السيبراني

يسعى هذا الفصل في بدايته إلى التعرف على القدرات السيبرانية لكل من الولايات المتحدة والصين وذلك باختيار أداة القياس المناسبة من بين مؤشرات القدرات السيبرانية المتوفرة، ذلك لأن معرفة قدرات البلدين يسمح لنا بالتعمق وتحليل وفهم الصراعات الدائرة بينهما في كل طبقة من طبقات الفضاء السيبراني، وبتطبيق منهج التحليل الجيوبوليتيكي (جوهر الحدث، عامل الحدث، بيئة الحدث) يستكشف المبحث الثاني الصراعات الجيوبوليتيكية حول تقنيات وطرق إدارة الفضاء السيبراني كل حسب تواجهه في الطبقة الخاصة به، ومن ثم يتطرق المبحث الثالث إلى تداعيات الصراع التكنولوجي الأمريكي الصيني على العلاقات الثنائية بين البلدين وأثره على إحياء وتشكيل تحالفات استراتيجية جديدة وعلاقة ذلك بتوازن القوى ومستقبل النظام الدولي.

المبحث الأول: القدرات السيبرانية للولايات المتحدة الأمريكية والصين

من الواضح أن الدول على اختلاف حجمها في الساحة الدولية تسعى لزيادة تأثيرها وقوتها في الفضاء السيبراني، كما أنه يوجد وعي متزايد لدى النخب السياسية والعسكرية والأكاديمية بأن امتلاك القوة السيبرانية وزيادة وتضخيم القدرات في الفضاء السيبراني مع تطبيقها في المنطقة الرمادية للعمليات (Gray zone operations) يمكن أن يحدث تأثيراً بالغاً بالتوازنات الثنائية والإقليمية والدولية بين الولايات المتحدة الأمريكية وحلفائها من جهة، والصين وروسيا من جهة أخرى¹، لذلك تسعى الدول القوى العظمى للهيمنة على تكنولوجيا المعلومات والاتصال، ورغم أن المتغيرات الأساسية التي تساهم في القوة السيبرانية غير واضحة تماماً مما يصعب عملية قياسها إلا أن السعي لتحديدها وفهمها يساعد الباحثين وصانعي القرار في فهم وتحسين الاستراتيجيات والسياسات السيبرانية للدولة.

المطلب الأول: مؤشر القدرات السيبرانية للدولة

إن الإجابة على السؤال: من هي أقوى دولة في الفضاء السيبراني؟ يتطلب بداية تحديد وضبط لمفهوم القدرات (القوة) السيبرانية للدولة والمفاهيم المشابهة لها، فإذا كانت القوة السيبرانية للدولة هي شكل من أشكال التأثير أو مقاومة التأثير التي تقوم به الدولة في الفضاء السيبراني فإن هذه القوة تعتمد على توافر مجموعة من الموارد والأصول والمهارات البشرية، يُقدم "أنطوني كراغ" مفهوماً للقدرات السيبرانية للدولة على أنها: "مجموعة الموارد والأصول التي يمكن للدولة الاعتماد عليها واستعمالها لممارسة أو مقاومة التأثير في الفضاء السيبراني"²، لذلك فإن "كراغ" يفرق بين "القوة السيبرانية" و"القدرات السيبرانية" فالأولى تظهر من خلال النتائج والثانية عبارة عن الموارد والأصول المتوفرة³، بعبارة أخرى، فإن دولة ما تُعتبر قوة سيبرانية إذا استعملت قدراتها السيبرانية لتحقيق أهدافها في الفضاء السيبراني، في حين أنه يمكن أن تمتلك دولة أخرى قدرات سيبرانية كبيرة غير أنها لا تستعملها (لعدم وجود أهداف واضحة في الفضاء السيبراني) أو لأنها

¹ The International Institute for Strategic Studies, **CYBER CAPABILITIES AND NATIONAL POWER: A Net Assessment**, June 2021, p 175, URL: <https://bit.ly/45CKorA>.

² Anthonym Craig, **Capabilities and conflict in the cyber domain: an empirical study**, Dissertation, Cardiff University, 2020, p 58.

³ Ibid.

لا تُحسن استعمالها (لوجود ضعف في تكتيكات استخدام القدرات السيبرانية) وهذا ما يُعبر عنه بأن الدولة تملك قدرات سيبرانية كامنة أو محتملة.

وعلى خلاف ما سبق، هناك من يُركز على القدرات السيبرانية الهجومية (OCCs) للدولة، ففوة الدولة في الفضاء السيبراني مرهونة بحجم قدراتها السيبرانية الهجومية، حيث يُعرف "قاموس وزارة الدفاع الأمريكية DoD للمصطلحات العسكرية والمرتبطة" العمليات السيبرانية (COs) بأنها "توظيف القدرات السيبرانية حيث يكون الغرض الأساسي هو تحقيق الأهداف في/من خلال الفضاء السيبراني"¹، في المقابل، يشير المعهد الأسترالي للسياسات الاستراتيجية (ASPI) للقدرات السيبرانية الهجومية في سياق العمليات السيبرانية بأنها "امتلاك الموارد والمهارات والمعرفة والمفاهيم والإجراءات التشغيلية التي تمنح القدرة على التأثير في الفضاء السيبراني"².

وتماشياً مع ما تم ذكره سابقاً، فالقوة السيبرانية تشير إلى تلك القابلية للسيطرة والهيمنة على الفضاء السيبراني من خلال توظيف قدرات الدولة السيبرانية، لكن يبقى التساؤل حول مدى مصداقية وصحة مؤشرات القدرات السيبرانية، فعلى خلاف القوة العسكرية التقليدية التي تمتلك مؤشرات أكثر واقعية كعدد الجنود، نوع الأسلحة، عدد الدبابات والطائرات والرؤوس النووية التي تمتلكها الدولة، من الصعوبة بمكان تحديد حتى ما يمكن اعتباره "سلاحاً سيبرانياً" وهذا ما يطرح عدة إشكالات ويضع حدوداً لدقة مؤشرات القوة السيبرانية يمكن أن نلخصها في ما يلي:

- الطبيعة غير المادية والمؤقتة لعناصر الفضاء السيبراني (خاصة البرمجيات) مما يجعل الدول تُبقي أسلحتها السيبرانية في درجة قصوى من السرية.
- صعوبة جمع بيانات موثوقة حول الفواعل من غير الدول خاصة القطاع الخاص - والذي يُعتبر من أكبر الفاعلين المؤثرين في الفضاء السيبراني - مما يجعل التقييم الكلي لقدرات الدولة السيبرانية محل شك.
- غياب (عدم توفر) بيانات عامة حول القدرات السيبرانية للكثير من الدول (عدم وجود سياسة سيبرانية أو استراتيجية منشورة أو إحصائيات موثوقة).

¹ US. Department of Defense, Dictionary of military and associated terms, Joint Publication 1-02, 2010 (As Amended Through 15 February 2016, p 58, URL: <https://bit.ly/47GExTP>.

² Tom Uren, Bart Hogeveen, and Fergus Hanson, "Defining offensive cyber capabilities", **Briefing and Memos from the Research Advisory Group, The Hague Centre for Strategic Studies**, 2018, pp 73-90.

- ميزة المجهولية وصعوبة إسناد العمليات السيبرانية لفاعل محدد، إضافة إلى نفي الدول استخدام مجموعات سيبرانية (هاكرز) تُصعب من تقييم القدرات السيبرانية للدولة.
- البيانات المتوفرة حول العمليات (الحوادث) السيبرانية تقتصر على الحوادث المعلنة -التي تم كشفها للعامة- وهذا ما يُعزز الشكوك حول العمليات السيبرانية المتقدمة والأكثر تطوراً والتي تبقى سرية وهذا ما يقدر في مصداقية مؤشرات القدرات السيبرانية للدولة.

على الرغم من الإشكالات السابقة الذكر فقد حاول الباحثون التقليل من أثرها على جودة المؤشرات من خلال دراسة وتحليل العديد من المتغيرات المختلفة والتطرق إلى الجوانب المتعددة التي تبني عبرها الدول قوتها السيبرانية، ولعل من أبرز المؤشرات العالمية لقياس قوة الدولة في الفضاء السيبراني نذكر ما يلي:

الفرع الأول: مؤشر القوة السيبرانية CPI Booz Allen Hamilton

طورت وحدة التحقيقات التابعة لمجلة "الإيكونوميست The Economist" برعاية شركة Booz Allen Hamilton سنة 2011 نموذجاً لقياس القوة السيبرانية لدول مجموعة العشرين G20 يستخدم هذا النموذج منهج البحث الكمي والنوعي، ويتكون من 39 متغيراً ومتغيراً فرعياً، مقسمة على أربع فئات تتمحور حولها القوة السيبرانية هي¹:

1. الإطار القانوني والتنظيمي: ويشمل مدى التزام الحكومة بتطوير القوانين والتنظيمات السيبرانية، الحماية السيبرانية، الرقابة السيبرانية، حماية الملكية الفكرية.
2. السياق الاقتصادي والاجتماعي: ويشتمل مستوى التعليم، المهارات التقنية، التجارة وبيئة الابتكار.
3. البنية التحتية التكنولوجية: وتشمل ثلاث عناصر مهمة متعلقة بتكنولوجيا المعلومات والاتصال وهي : النفاذ، الجودة، الانفاق، إضافة إلى مدى تأمين خوادم الأنترنت.
4. التطبيقات الصناعية للفضاء السيبراني: وتدرس مدى توفر وفعالية الشبكات الذكية، التجارة الإلكترونية، التطبيقات الإلكترونية في مجالات الصحة والنقل، والحكومة الإلكترونية.

¹ Unit, Economist Intelligence, Cyber power index: findings and methodology, Booz Allen Hamilton, 2011, p 24.

يشير المؤشر في نسخته الوحيدة (2011) إلى تصدر المملكة المتحدة القائمة كأقوى دولة في الفضاء السيبراني متبوعة بالولايات المتحدة الأمريكية، استراليا، ألمانيا وكندا على التوالي، فيما احتلت الصين المركز الثالث عشر (انظر الجدول رقم 01)، ويعزو أصحاب المؤشر هذا الترتيب إلى الانتشار المكثف للإنترنت والإمكانية الكبيرة لشعوب الدول الغربية في النفاذ للخدمات السيبرانية.

يُعد مؤشر **CPI Booz Allen Hamilton** من بين المحاولات الأولى لقياس القوة السيبرانية للدول، لكن لم يتم تحديثه على الإطلاق ولا توجد إلا النسخة الأولى لسنة 2011 مما يجعله غير فعال في بيئة سريعة التغير، هذا إضافة إلى عدم تطرقه للقدرات السيبرانية الهجومية للدول وهو ما يجعل نتائجه نسبية إلى حد بعيد.

الفرع الثاني: المؤشر العالمي للأمن السيبراني GCI للاتحاد العالمي للاتصالات ITU

يقوم الاتحاد الدولي للاتصالات ITU وهو هيئة تابعة للأمم المتحدة بإصدار تحديثات لهذا المؤشر (03 إصدارات) لغرض قياس مدى التزام الدول بالأمن السيبراني، من أجل زيادة الوعي بقضايا الفضاء السيبراني وأبعاده المختلفة، كما تستخدم الدول المؤشر العالمي للأمن السيبراني في¹:

- ✓ المناقشات في المنتديات الرسمية والتي تتيح التقييم الذاتي وزيادة التنسيق العالمي.
- ✓ توحيد الرؤى حول المبادرات الوطنية والموارد المستخدمة لإدارة الأمن السيبراني.
- ✓ المقارنة بين الدول للاستفادة من الممارسات الجيدة في الفضاء السيبراني.
- ✓ رفع مستوى الوعي بين مختلف أصحاب المصلحة بشأن احتياجات التنسيق على المستوى الوطني والإقليمي والدولي.

يقوم هذا المؤشر على توزيع استبيان على البلدان الأعضاء في الاتحاد الدولي، تحتوي استمارة الاستبيان على مجموعة أسئلة (82 سؤال في اصدار 2020) موزعة على خمس (05) ركائز أساسية لرصد أكثر من 20 متغير، وجاء توزيع المتغيرات على الركائز الخمس في الاصدار 2020 كالتالي²:

¹ International Telecommunication Union, Global Cybersecurity Index 2020, ITUPublications, 2020, p VI, URL: <https://bit.ly/3svomsc>.

² Ibid, p VII.

1. **الجانب القانوني:** ويتعلق بمدى توافر القوانين والتنظيمات الخاصة بالجريمة السيبرانية والأمن السيبراني ويضم تشريعات الأمن السيبراني، حماية البيانات، حماية البنية التحتية السيبرانية الحرجة.
2. **الجانب التقني:** ويتعلق بقياس مدى تطبيق القدرات السيبرانية من خلال الوكالات والهيئات الوطنية والخاصة للأمن السيبراني، ويشمل عدد الهيئات ومدى انخراطها في عمليات حماية الفضاء السيبراني الوطني.
3. **الجانب التنظيمي:** يتعلق بقياس الاستراتيجيات الوطنية والهيئات التنظيمية للأمن السيبراني الوطني، ويضم استراتيجيات الأمن السيبراني الوطني، استراتيجيات حماية الطفولة في الفضاء السيبراني، منظمات الأمن السيبراني.
4. **جانب تنمية القدرات:** ويتعلق بقياس حملات التوعية والتدريب والتعليم والحوافز المقدمة لتنمية قدرات الأمن السيبراني، ويشمل مبادرات التوعية وبرامج البحث والتطوير في مجال الأمن السيبراني.
5. **جانب التعاون:** ويتعلق بقياس مدى التعاون بين الوكالات والشركات والدول في مجال الأمن السيبراني، ويتم ذلك برصد الشراكات الثنائية والمتعددة الأطراف بين الفواعل المختلفة.

وجاءت نتائج الاصدار الأخير (مؤشر سنة 2020) لتضع الولايات المتحدة الأمريكية في المرتبة الأولى والصين في المرتبة الثالثة والثلاثين ضمن قائمة 182 دولة في العالم، لكن مع ملاحظة أن الولايات المتحدة لم تُقدم إجابة على الاستبيان¹ وهذا ما يطرح عدة تساؤلات عن سبب جعلها في المقدمة في غياب بيانات رسمية، كما أن عملية التقييم التي تتم ذاتياً أي من طرف الدولة نفسها قد يجعل بعض البيانات والمعلومات محل شك، إضافة إلى أن المؤشر يختص بالأمن السيبراني فقط ولا يتطرق إلى بقية مكونات القوة السيبرانية كالقدرات الهجومية مثلاً لذلك فهو لا يُقدم نظرة شاملة عن قوة الدول السيبرانية.

¹ Ibid, pp 25-27.

الفرع الثالث: المؤشر الوطني للقوة السيبرانية NCPI لمركز بلفر للعلوم والشؤون الدولية التابع لجامعة هارفارد.

قدم باحثو مركز بلفر سنة 2020 نموذجاً لقياس القدرات السيبرانية، وتم تطبيقه على 30 دولة، يتشكل النموذج المقترح من 32 متغيراً خاصاً بالنوايا (ويحدد الباحثون سبعة نوايا رئيسية للدولة في الفضاء السيبراني هي: المراقبة، التحكم، الدفاع، الهجوم، المخابرات، التجارة، المعايير) و 27 متغيراً خاصاً بالقدرات السيبرانية تتوزع عبر 07 أهداف للدولة، وتم جمع البيانات من خلال المعلومات العامة المتاحة للجمهور.

ويتبع النموذج نهجاً شاملاً في قياس القوة السيبرانية للدولة بجمع ما أمكن من بيانات حول مكونات القوة السيبرانية في سياق الأهداف الوطنية، حيث يُقيم كل من استراتيجيات الحكومة في المجال السيبراني، قدرات الدفاع والهجوم السيبراني، الموارد المخصصة، دور القطاع الخاص، المهارات البشرية و الابتكار.

يُحدد فريق مركز بلفر أهداف القوة السيبرانية كأهداف مشتركة تسعى معظم الدول لتحقيقها في وعبر الفضاء السيبراني على النحو التالي¹:

1. **رصد ومراقبة المجموعات المحلية:** حيث تمنح الدولة لنفسها الأدوات القانونية وقدرات المراقبة السيبرانية لرصد واكتشاف وجمع المعلومات الاستخبارية عن التهديدات والجهات الفاعلة داخل حدودها، ويتم ذلك من خلال عمليات المراقبة الشاملة للمواطنين، مراقبة حركة الأنترنت، كسر التشفير، مكافحة أجهزة الاستخبارات الأجنبية ومنظمات الجريمة والجماعات الإرهابية.

2. **تقوية وتعزيز الدفاعات السيبرانية الوطنية:** تُعطي الدولة الأولوية لتعزيز الدفاع عن الأنظمة الوطنية في الفضاء السيبراني، وتحسن القدرة على الصمود في حال تعرضها للهجوم، وهذا يشمل الدفاع السيبراني النشط وتعزيز الأمن السيبراني خاصة للصناعات الحساسة، والمواطنين بشكل عام، والعمل على زيادة الوعي الوطني بالتهديدات السيبرانية.

3. **التحكم في بيئة المعلومات ومعالجتها:** وهو ما يعكس مدى قدرة الدولة على استخدام الوسائل والأدوات السيبرانية للتحكم في المعلومات والأخبار في الداخل والخارج، ويتم عبر محاولة حماية

¹ Julia Voo, et al, **National Cyber Power Index 2020: Methodology and Analytical Considerations**, China Cyber Policy Initiative, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2020, p 21.

الخصوصية على الأنترنت وحرية التعبير للمواطنين، كما يتضمن عمليات نشر الدعاية محلياً، بث وتضخيم المعلومات المضللة خارجياً، إضافة إلى استخدام القدرات السيبرانية لاستهداف وتعطيل عمل المجموعات المضادة في الفضاء السيبراني عبر إزالة المواد المتطرفة من وسائل التواصل الاجتماعي ودحض الدعاية الأجنبية.

4. جمع المعلومات الاستخبارية في دول أخرى لحماية الأمن القومي: يعكس قدرة الدولة على جمع الأسرار حول الدول الأخرى، حيث يشمل جمع المعلومات حول الأنشطة الدبلوماسية والتخطيط العسكري ومراقبة المعاهدات وغيرها، ويتم من خلال عمليات الاختراق وانتهاك المواد السرية.

5. تنمية الكفاءة السيبرانية والتكنولوجيا الوطنية: ويعكس محاولة الدول تنمية صناعة التكنولوجيا المحلية سواء بطرق مشروعة كالاستثمار في البحث والتطوير وتنمية المهارات البشرية في مجال الأمن السيبراني، أو بطرق غير مشروعة كالتجسس الصناعي ضد الشركات الأجنبية.

6. تدمير أو تعطيل البنية التحتية للخصم وقدراته: ويعكس استخدام دولة ما تقنيات وتكتيكات سيبرانية لردع أو إضعاف قدرة الخصم على القتال في الفضاء السيبراني أو التقليدي، ويشمل الهجمات السيبرانية على البنية التحتية الحيوية، وهجمات DDOS على الشبكات الحكومية، ويشمل كذلك هجمات لإثبات النية والقدرة على ردع الخصم.

7. تحديد القواعد والمعايير التقنية السيبرانية الدولية: ويعكس مدى مشاركة بلد ما في المناقشات القانونية والسياسية والفنية الدولية حول معايير الأنترنت، المعاهدات الثنائية والمتعددة في المجال السيبراني، الانضمام إلى الشراكات والتحالفات السيبرانية لمكافحة الجريمة السيبرانية ومشاركة الخبرة والقدرات التقنية.

كما يُقدم فريق مركز بلفر ثلاث مؤشرات مختلفة، مؤشر قياس النية السيبراني (Cyber Intent Index)، مؤشر قياس القدرة السيبراني (Cyber Capability Index) CCI، ثم يتم جمع المؤشرين في المؤشر الرئيس وهو المؤشر الوطني للقوة السيبرانية (National Cyber Power Index) NCPI من خلال المعادلة التالية:

$$National\ Cyber\ Power\ Index\ (NCPI) = \frac{1}{7} \sum_{x=1}^7 Capability_x * Intent_x$$

وخلص تقرير مركز بلفر لسنة 2020 إلى أنه باعتماد مؤشر من 100 درجة فإن الولايات المتحدة الأمريكية جاءت في المقدمة تليها الصين في المركز الثاني، ورغم أن فريق البحث يُقر بصعوبة جمع البيانات في بعض الدول خاصة ماتعلق بسريّتها، إلا أن مؤشر بلفر NCPI يبقى من المؤشرات الجيدة والفعّالة في قياس القوة السيبرانية للدولة.

الفرع الرابع: مشروع قياس القوة السيبرانية للمعهد الدولي للدراسات الاستراتيجية INSS

يُقدم مشروع INSS منهجية جديدة لتقييم القوة السيبرانية للدولة، وتم تطبيقه على 15 دولة مقسمة تقسيماً جيوبوليتيكياً محضاً إلى أربع كتل جيوبوليتيكية هي:

1. دول تحالف العيون الخمس (الو.م.أ، المملكة المتحدة، كندا، أستراليا)
2. حلفاء سيبرانيون لتحالف العيون الخمس (فرنسا، إسرائيل، اليابان).
3. دول يعتبرها التحالف تهديداً سيبرانياً (الصين، روسيا، إيران، كوريا الشمالية)
4. دول في مراحل مبكرة من تطور قوتها السيبرانية (الهند، اندونيسيا، ماليزيا، فيتنام).

اعتمد المشروع منهجية البحث النوعي، حيث تم تقييم القدرات السيبرانية لكل دولة في سبع فئات مختلفة (1- الاستراتيجية والعقيدة. 2- الحوكمة والقيادة والسيطرة. 3- قدرات الاستخبارات السيبرانية الأساسية. 4- التمكين والاعتماد على الأنترنت. 5- الأمن السيبراني والمرونة. 6- الريادة العالمية في شؤون الفضاء السيبراني. 7- القدرة الهجومية السيبرانية) وكيفية تقاطعها مع الأمن والاقتصاد الدولي، المنافسة والشؤون العسكرية.

وكانت نتائج البحث موزعة إلى ثلاثة مستويات:

المستوى الأول، مخصص للدول ذات نقاط القوة الرائدة عالمياً عبر جميع الفئات، واستحقت الولايات المتحدة الأمريكية التواجد منفردة في هذا المستوى.

المستوى الثاني، مخصص للدول التي تتمتع بنقاط قوة رائدة عالمياً في بعض الفئات، وضم العديد من الدول الغربية إضافة إلى الصين.

المستوى الثالث، مخصص للدول التي لديها نقاط قوة أو نقاط قوة محتملة في بعض الفئات ولكنها ضعيفة في فئات أخرى.

كخلاصة لما سبق، يوضح الجدول الموالي (جدول رقم 01) مقارنة بين مختلف مؤشرات قياس القوة السيبرانية، ويرصد أوجه التشبه والاختلاف في منهجية البحث.

جدول رقم 01: مقارنة بين مؤشرات القوة السيبرانية.

المصدر: من إعداد الباحث¹.

المؤشر	CPI Booz Allen Hamilton	GCI الاتحاد الدولي للاتصالات	NCPI مركز بلفر	CPP المعهد الدولي للدراسات الاستراتيجية
سنة آخر إصدار	2011	2020	2020	2021
عدد الإصدارات	01	03	01	01
الهدف	قياس القوة السيبرانية للدولة	قياس التزام البلدان بزيادة الأمن السيبراني	قياس القوة السيبرانية للدولة مقارنة مع أهدافها	قياس القدرات السيبرانية وعلاقتها بقوة الدولة
عدد الدول المدرجة	19	182(2020)	30	15
عدد المتغيرات	39	25	59	
الترتيب	X	X	X	X
المواضيع				
القوانين والتنظيمات	X	X	X	X
الاقتصاد والمجتمع	X	X	X	X
التطبيقات الالكترونية في الحياة العامة	X		X	X
الاستراتيجيات			X	X
التطور التقني		X	X	X
الهجوم السيبراني			X	X
المخابرات			X	X
التعاون		X	X	X

¹ تم إعداد الجدول بالاعتماد على جدول مقارنة بين المؤشرات في تقرير مركز بلفر صفحة رقم 09 مع تعديل في المؤشرات والمواضيع، للمزيد يرجى الاطلاع على تقرير مؤشر القوة السيبرانية لمركز بلفر على الرابط : <https://bit.ly/3qITVyl>

من خلال الجدول أعلاه، يلاحظ تفوق مؤشري NCPI و CPP من حيث المواضيع التي يغطيها في حساب القوة السيبرانية للدولة مع تفوق لمؤشر NCPI من حيث عدد المؤشرات واستعمال منهج البحث المزدوج الكمي والنوعي، وكذلك عدد الدول المدرجة في التقرير النهائي.

من ناحية أخرى، وفي ما يخص النتائج المتحصل عليها وترتيب الدول حسب قوتها السيبرانية يقارن الجدول الموالي (جدول رقم 02) بين نتائج (الدول العشر الأولى) لمختلف المؤشرات.

جدول رقم 02: مقارنة ترتيب 10 دول الأوائل في مختلف مؤشرات القوة السيبرانية.

المصدر: من إعداد الباحث بالاعتماد على ترتيب مختلف المؤشرات.

المؤشر الترتيب	CPI Booz Allen Hamilton 2011	GCI الاتحاد الدولي للاتصالات 2020	NCPI مركز بلفر 2020	CPP المعهد الدولي للدراسات الاستراتيجية 2021
01	المملكة المتحدة	الولايات المتحدة	الولايات المتحدة	الولايات المتحدة
02	الولايات المتحدة	المملكة المتحدة	الصين	الصين (متوقع)
03	استراليا	السعودية	المملكة المتحدة	المملكة المتحدة، كندا، استراليا، فرنسا، اسرائيل، اليابان
04	المانيا	استونيا	روسيا	
05	كندا	كوريا الجنوبية	هولندا	
06	فرنسا	سنغفورة	فرنسا	
07	كوريا الجنوبية	اسبانيا	المانيا	
08	اليابان	روسيا	كندا	
09	ايطاليا	الإمارات العربية	اليابان	روسيا، ايران
10	البرازيل	ماليزيا	استراليا	

من خلال الجدول أعلاه، يلاحظ تصدر الولايات المتحدة الأمريكية للترتيب في مختلف مؤشرات القوة السيبرانية الحديثة، كما يوضح كل من مؤشري NCPI و CPP أن الصين تأتي في المرتبة الثانية مباشرة في دلالة على وجود صراع بين الدولتين.

المطلب الثاني: الولايات المتحدة الأمريكية القوة السيبرانية الرائدة (مهد الأنترنت)

ليس خافياً قيادة الولايات المتحدة الأمريكية في الفضاء السيبراني ويُعزى ذلك إلى أن هذا الفضاء هو صناعة أمريكية، فجهاز الكمبيوتر الأول صنع في الولايات المتحدة كما تم أول ربط لكمبيوترين في جامعات ومخابر وزارة الدفاع الأمريكية، لذلك ليس من المفاجئ أن تصدر

الولايات المتحدة الترتيب في مؤشرات القوة السيبرانية المختلفة، وعليه، فلرصد وتقييم القدرات السيبرانية للولايات المتحدة (والصين في المطلب الموالي) تعتمد الدراسة على تصنيفات مركز بلفر لأهداف الدولة السبعة في الفضاء السيبراني، مع تدعيم متغيرات مركز بلفر لقياس القدرات السيبرانية بمتغيرات من مؤشرات أخرى عند الحاجة.

1. **الرصد والمراقبة السيبرانية:** من أجل تنظيم وتقنين عمليات المراقبة لغرض التحكم الأفضل في بيانات المواطنين وضبط التعاملات مع الجهات الخارجية وتعزيز الدفاع كانت الولايات المتحدة سباقة في سن التشريعات والقوانين الخاصة بالجرائم السيبرانية، الشفافية و حماية البيانات، حيث سن المشرع الأمريكي قانون الاحتيال وإساءة استخدام الكمبيوتر سنة 1986 لمكافحة جرائم الكمبيوتر، قانون الخصوصية سنة 1974 و قانون لجنة التجارة الفيدرالية رقم 15 لحماية البيانات وحماية الخصوصية للمواطنين، غير أن أحداث 11 سبتمبر عجلت بصور قانون باتريوت "Patriot Act" في أكتوبر 2001 والذي يعطي صلاحيات واسعة للحكومة بمراقبة الاتصالات والتجسس¹، ورغم الانتقادات الشديدة للقانون ومحاولات التعديل عليه إلا أن تسريبات "سنودن" سنة 2013 أظهرت بشكل لافت أن الولايات المتحدة تملك ترسانة قوية لرصد ومراقبة مواطنيها وكل ما يمر عبر شبكات الأنترنت.

لعل ما يسهل عمليات المراقبة في الولايات المتحدة هو أن نسبة النفاذ للأنترنت للأفراد ارتفعت من 43% سنة 2000 إلى 91% سنة 2020 أي ما يفوق 300 مليون مستخدم حسب إحصائيات البنك الدولي²، في حين أن 82% من المواطنين الأمريكيين يستخدمون برامج وتطبيقات التواصل الاجتماعي حسب موقع Statista³.

من جهة أخرى، فإن عمليات المراقبة لا تقوم بها الوكالات الحكومية فحسب بل إن جزءاً كبيراً منها يقوم يتولاه القطاع الخاص، يقول "جاي ستانلي" في تقرير حول خصوصية قطاع المراقبة السيبرانية في الولايات المتحدة في بدايات الاهتمام بالفضاء السيبراني سنة 2004 أن "خصوصية مهام الحكومة كانت دائماً الطريقة الأكثر شعبية للقيام بالأعمال، والمراقبة ليست

¹ Orin S Kerr, "Internet surveillance law after the USA Patriot Act: The big brother that isn't", SSRN Electronic Journal, Vol 97 No 2, 2002, pp 607-674.

² إحصائيات البنك الدولي على الرابط: <https://bit.ly/3KR97jS>.

³ إحصائيات موقع Statista على الرابط: <https://bit.ly/3tizo1Q>.

استثناء¹، فشرركات القطاع الخاص تزود الحكومة ببيانات المواطنين طوعية أو وفقاً لاتفاقيات مبرمة بين الطرفين أو خضوعاً لقوانين مكافحة الإرهاب وحماية الأمن القومي، وفي المحصلة فالحكومة الأمريكية لها كامل الصلاحيات والقدرات لمراقبة شاملة لمواطنيها، لكن رغم ذلك فإن مؤشر منظمة بيت الحرية **Freedom house** لحرية الإنترنت تصنف الولايات المتحدة في المركز 12 مع الدول التي تضمن حرية الإنترنت بمجموع 75 نقطة (معوقات النفاذ: 21 نقطة، حجب محتوى الإنترنت: 29 نقطة، انتهاك حقوق المستخدم: 26 نقطة)².

2. **السيطرة والتحكم:** تقنياً تمتلك الولايات المتحدة قدرات ضخمة للتحكم في تدفق البيانات والأنترنت عبر العالم، حيث يمكنها ربط/قطع الأنترنت عن أجزاء كبيرة في العالم، ذلك أنها تمتلك تقنيات الأنترنت عبر الأقمار الصناعية وتستحوذ على الجزء الأكبر من كابلات الألياف البصرية، أما من ناحية المحتوى وخدمات البحث فالمواقع الثلاث الأولى في ترتيب المواقع الأكثر زيارة في العالم محجوزة لمواقع أمريكية (قوقل، يوتيوب، فايسبوك)، كما يتواجد 14 موقعاً أمريكياً في قائمة المواقع الـ 20 الأكثر زيارة³، ويسيطر محرك البحث قوقل على 91,42% من عمليات البحث على الأنترنت⁴، وفي خضم انتشار الهواتف الذكية وتطبيقات التواصل الاجتماعي فمن بين التطبيقات السبعة التي يفوق عدد المستخدمين النشطين فيها المليار مستخدم نجد خمسة تطبيقات أمريكية مسيطرة هي فايسبوك، يوتيوب، واتساب، انستغرام وماسنجر⁵، وهذا كله يمنح حكومة الولايات المتحدة قدرات كبيرة للتحكم في المحتوى وتوجيهه والسيطرة على المعلومات بالحذف أو الحجب أو النشر.

3. **الدفاع السيبراني:** تضطلع القيادة السيبرانية للولايات المتحدة **USCyberCom** بمهمة الدفاع السيبراني، أنشأت القيادة السيبرانية في 2009 حيث كانت تابعة لوكالة الأمن القومي **NSA** ثم رُقيت إلى قيادة مقاتلة مستقلة (واحدة من بين عشر قيادات تابعة للبننتاغون) في عهد الرئيس دونالد ترمب سنة 2018⁶.

¹ Jay Stanley, *The surveillance-industrial complex: How the American government is enlisting private parties in the construction of a surveillance society*, National Headquarters, 2004, p 2.

² إحصائيات منظمة **Freedom house** على الرابط: <https://bit.ly/3mhJhsI>

³ حسب إحصائيات موقع **Similairweb** لشهر أبريل 2022 على الرابط: <https://bit.ly/3zoMAGh>

⁴ حسب إحصائيات موقع **Wearesocial** لشهر جانفي 2022 على الرابط: <https://bit.ly/3P7SR0t>

⁵ حسب إحصائيات موقع **Wearesocial** لشهر أكتوبر 2021 على الرابط: <https://bit.ly/399x868>

⁶ موقع القيادة السيبرانية للولايات المتحدة على الأنترنت على الرابط: <https://bit.ly/3YKJ1EQ>

تتمثل مهمتها في قيادة ومزامنة وتنسيق التخطيط والعمليات في الفضاء السيبراني - للدفاع عن المصالح الوطنية وتعزيزها - بالتعاون مع الشركاء المحليين والدوليين، كما أن رؤيتها تتمثل في بلوغ والإبقاء على تفوق الولايات المتحدة في الفضاء السيبراني، كما أنها تعتمد في عملها على القوانين والتنظيمات الواردة في الاستراتيجية السيبرانية الوطنية 2018 والاستراتيجية السيبرانية لوزارة الدفاع 2018 (سيتم التطرق للاستراتيجيتين في الفصل الموالي)، يُقدر عدد فرقها العاملة في مختلف المجالات العسكرية بـ 133 فريق.

أما بالنسبة للمجال المدني الداخلي تقود وكالة الأمن السيبراني وأمن البنية التحتية CISA (تعرف كذلك بفريق الطوارئ السيبراني للولايات المتحدة USCERT) الجهود الوطنية لفهم وإدارة وتقليل المخاطر على البنية التحتية السيبرانية والمادية من أجل ضمان بنية تحتية حيوية وآمنة ومرنة للشعب الأمريكي¹، كما وجب التنويه على أن معظم شركات الأمن السيبراني الكبرى في العالم هي شركات أمريكية فهي تحتل المراتب الأولى من حيث القوة والفاعلية وتمثل أكثر من 3/4 عدد الشركات العالمية².

كما تزخر الولايات المتحدة بالطاقات البشرية المؤهلة (المركز الثاني في عدد براءات الاختراع³)، ويتواجد بها عدد كبير من شركات التكنولوجيا الرائدة (توطين التكنولوجيا)، إلا أن عدد مستخدمي الأنترنت الكبير نسبياً وسرعة تدفق الأنترنت العالية والمجالات الكثيرة التي تعتمد على تكنولوجيا المعلومات والاتصال جعل ترتيب الولايات المتحدة دون الوسط من بين الدول الآمنة سيبرانياً⁴ حيث تتزايد قابلية بنيتها التحتية (خوادم الأنترنت) للاختراق والعطب⁵.

4. **الهجوم السيبراني:** رغم أن القدرات السيبرانية الهجومية تُعد من أسرار الدول وهذا راجع لطبيعة الحروب السيبرانية والأسلحة المستخدمة فيها، إلا أنه بشكل عام تُعد القدرات السيبرانية الهجومية للولايات المتحدة الأكثر تطوراً من أي دولة أخرى، ذلك أنها تمتلك جميع الأسس اللازمة: قدرة استخباراتية سيبرانية متطورة تشغلها مهارات بشرية عالية التكوين؛ قيادة تحالف العيون الخمس

¹ موقع وكالة الأمن السيبراني وأمن البنية التحتية على الأنترنت على الرابط: <https://www.cisa.gov/about-cisa>

² انظر ترتيب شركات الأمن السيبراني على مواقع: companiesmarketcap.com، cybersecurityventures.com، softwaretestinghelp.com، esecurityplanet.com، clutch.co، netify.com

³ إحصائيات المنظمة الدولية للملكية الفكرية لسنة 2020 على الرابط: <https://bit.ly/3Hu0Xv0>

⁴ حسب ترتيب موقع **Comparetech** على الرابط: <https://bit.ly/3mLNx3X>، على الرغم من أن الاتحاد الدولي للاتصالات يصنفها الدولة الأولى في مجال الأمن السيبراني لكن مع ملاحظة غياب البيانات التي اعتمد عليها.

⁵ تقرير موقع **Shodan** حول عدد الخوادم القابلة للاختراق والتي تعتبر نقاط ضعف، على الرابط:

<https://bit.ly/3MU37Vy>

المتقدم تقنياً؛ قاعدة أكاديمية عريقة¹ ومجمع صناعي سيبراني قوي (المركز السادس عالمياً في تصدير التكنولوجيا الفائقة)²؛ عقيدة سيبرانية واضحة من خلال استراتيجية سيبرانية محدثة باستمرار (آخر تحديث هو الاستراتيجية السيبرانية الوطنية 2018)؛ سلطات قانونية تنظم الاستخدام المسؤول لقدرات الولايات المتحدة في الهجمات السيبرانية.

من جهة أخرى، يعكس عدد موظفي القيادة السيبرانية الأمريكية البالغ 6200 موظف يُضاف إليهم عدد غير معروف في وكالتي NSA و CIA حجم القدرات الهجومية للولايات المتحدة في الفضاء السيبراني، ورغم العدد القليل من الحالات المعلنة لهجمات سيبرانية أمريكية (من الممكن أن الأمر يعود للقوانين الصارمة أو لأنها عمليات شديدة التعقيد يصعب كشفها) إلا أنها تتميز بقدرة كبيرة على الإضرار بالخصوم، مثل ما حدث مع فيروس Stuxnet ضد إيران و الهجمات ضد تنظيم الدولة، الصين، روسيا و كوريا الشمالية.

5. **المخابرات:** ليس خافياً التطور الكبير واتساع وعمق القدرات الاستخباراتية السيبرانية الأمريكية، تتركز هذه القدرات في القيادة العسكرية لوكالة الأمن القومي NSA، القيادة المدنية لوكالة الاستخبارات المركزية CIA مع صلاحيات خارجية سرية موسعة ومكتب التحقيقات الفيدرالي FBI المكلف بالأمن الداخلي، يزيد من قوة التنسيق والتآزر بين أطراف هذا المجمع الاستخباراتي ترؤس مدير وكالة الأمن القومي للقيادة السيبرانية للولايات المتحدة USCyberCom، كما تُعزز الولايات المتحدة قدراتها الاستخبارية بالتحالفات والشراكات الدولية لعل أبرزها تحالف العيون الخمس والذي يُعد الأقوى في التاريخ البشري، ومن أجل البقاء في الريادة تتعاون الوكالات الاستخبارية الأمريكية مع العديد من الشركات والجامعات لتطوير وتقييم التقنيات الحديثة³، لذلك فالميزانية السنوية الأمريكية المخصصة للوكالات هي الأعلى عالمياً حيث تتعدى سنوياً بأكثر من 80 مليار دولار في السنوات الخمس الأخيرة (2018-2022)⁴.

¹ تُصنف 38 جامعة أمريكية من بين أفضل الجامعات في العالم حسب تصنيف موقع timeshighereducation على الرابط: <https://bit.ly/3b1qtvj>

² حسب إحصائيات البنك الدولي لصادرات التكنولوجيا الفائقة لسنة 2021 على الرابط: <https://bit.ly/3xWxMgU>

³ حسب موقع مكتب مدير الإستخبارات الوطنية على الرابط: <https://bit.ly/47G4Vxd>.

⁴ نفس المرجع.

6. التجارة الإلكترونية والاقتصاد الرقمي: تُشير إحصائيات موقع Statista¹، تقارير بنك جي بي مورغان حول اتجاهات التجارة الإلكترونية العالمية² و تقارير مؤتمر الأمم المتحدة للتجارة والتنمية UNCTAD حول الاقتصاد الرقمي³ أن التجارة الإلكترونية تمثل 14% من تجارة التجزئة في الولايات المتحدة، حيث ينفق 77% من المواطنين على التسوق من الأنترنت ما يعادل 770 مليار دولار سنة 2021 وتنمو السوق بمعدل 11% سنوياً لتبلغ 1,32 تريليون دولار في 2025، تتصدر كل من Amazon و Ebay قائمة أكبر منصات التجارة الرقمية الأمريكية، كما تقود شركات التكنولوجيا الكبرى الاقتصاد الرقمي ثلاثة منها تفوق قيمتها السوقية التريليون دولار (آبل، ألفابت، ميكروسوفت) كما تتواجد 72 شركة من بين أكبر 100 شركة تكنولوجية في الولايات المتحدة⁴.

7. القواعد والمعايير: بما أن الفضاء السيبراني قد تم ابتكاره في الولايات المتحدة فلا عجب أن تضع شركات التكنولوجيا الأمريكية الرائدة معايير وقواعد الاتصال (بروتوكولات الاتصال ونقل البيانات)، كما أن منظمة ICANN المكلفة بإدارة عناوين الأنترنت هي منظمة أمريكية في الأصل رغم وصفها بالاستقلالية، يُضاف إلى ذلك العدد الكبير من القوانين والتشريعات الوطنية والمحلية (الخاصة بكل ولاية) حول الخصوصية حماية البيانات والأمن السيبراني، من جهة أخرى سعت الولايات المتحدة لعقد العديد من الاتفاقيات الثنائية والجماعية مع حلفائها (تحالف العيون الخمس، الهند، فرنسا...) ومنافسيها (الصين وروسيا) ومع المنظمات والهيئات الإقليمية والدولية (الاتحاد الأوروبي، مجموعة 7، مجموعة 20، حلف الناتو...)،⁵ مع حرصها على المشاركة في الاجتماعات والملتقيات الخاصة بوضع القواعد والمعايير في الفضاء السيبراني (منتدى حوكمة الأنترنت) وممارسة قوتها الناعمة لأجل خدمة توجهاتها ورؤيتها لمستقبل هذا الفضاء.

¹ إيرادات التجارة الإلكترونية بالتجزئة في الولايات المتحدة من 2017 إلى 2025، موقع Statista على الرابط :

<https://bit.ly/3QNPAC6>

² على الرابط : <https://bit.ly/3njKIHy>

³ على الرابط: <https://bit.ly/47K7Y7n>

⁴ Jonathan Ponciano, The World's Largest Tech Companies In 2022: Apple Still Dominates As Brutal Market Selloff Wipes Trillions In Market Value, The Global 2000, Forbes website, May 2022, URL: <https://bit.ly/3HTEOX2>.

⁵ فهرس حول معايير وقواعد الفضاء السيبراني، الاتفاقيات الثنائية والجماعية على موقع carnegieendowment.org على الرابط : <https://bit.ly/3E6NqbB>.

خلاصة لما تقدم، تمتلك الولايات المتحدة العديد من نقاط القوة الرائدة خاصة في: التحكم، الدفاع، الهجوم والمخابرات، مما يؤهلها لإعتلاء الهرم كأقوى دولة سيبرانية في العالم.

المطلب الثالث: الصين ... قوة سيبرانية متنامية بسرعة

بدأ القادة الصينيون في احتضان تكنولوجيا المعلومات والاتصال منذ تسعينيات القرن المنصرم، مدفوعين بعامل الضعف النسبي في مجال الالكترونيات من جهة، ومزايا التحول الاقتصادي الضخم والنمو السريع وعمليات نقل التكنولوجيا المتقدمة من الشركات العالمية إلى داخل الصين من جهة أخرى، حيث إنشأت الصين أكبر نظام للمراقبة الشاملة في العالم داخل البلاد، كما تظهر رغبتها الجدية في أن تصبح قوة سيبرانية من خلال إصدار استراتيجيتها العسكرية سنة 2015 و الاستراتيجية الرسمية للأمن السيبراني سنة 2016.

ومن أجل رصد وتقييم القوة السيبرانية الصينية نستخدم نفس المؤشر (مركز بلفر) مع الاستعانة بمتغيرات من المؤشرات الأخرى من أجل التوضيح والتعليل.

1.الرصد والمراقبة السيبرانية: جاء التعديل على القانون الجنائي لجمهورية الصين الشعبية لسنة 1997 لمكافحة الجرائم المتعلقة بالكمبيوتر وحماية المواطن الصيني (المواد 217، 285، 286 و 287)، كما أكد "قرار اللجنة الدائمة للمجلس الوطني لنواب الشعب الصيني بشأن تعزيز حماية المعلومات على الأنترنت" الصادر في 2012 على حماية البيانات والخصوصية الرقمية ويُعزز هذه الحقوق قانون التجارة الإلكترونية لجمهورية الصين الشعبية الذي صدر في 2018¹، لكن وجود أكثر من مليار مستخدم للأنترنت² وما يقارب المليار مستخدم نشط على شبكات التواصل الاجتماعي³ يضع الحكومة الصينية أمام تحد كبير في تسيير هذه الحشود الكبيرة وفرض النظام حسب توجهات الحزب الحاكم الصيني، لذلك سعت السلطات الصينية إلى إنشاء نظام للمراقبة منذ 2003 والذي عُرف باسم "الجدار الناري العظيم - Great FireWall" والذي يعمل على مراقبة وفلترة محتوى الأنترنت داخل الصين⁴، وهذا ما جعل الصين تحتل

¹ يقدم موقع مجلس الأمم المتحدة للتجارة والتنمية قائمة بالتشريعات والقوانين الخاصة بالفضاء السيبراني ومكافحة الجريمة السيبرانية لأغلب دول العالم، وما يتعلق بالتشريعات والقوانين الصينية توجد على الرابط : <https://bit.ly/3YJl8O1>.

² إحصائيات موقع Statista على الرابط: <https://bit.ly/3sfWvfC>.

³ إحصائيات موقع Statista على الرابط: <https://bit.ly/47KW2m8>.

⁴ Roya Ensafi, et al, "Analyzing the Great Firewall of China Over Space and Time", **Proceedings on Privacy Enhancing Technologies**, Vol 1, 2015, pp 61-76.

المرتبة الأخيرة في مجال حرية الأنترنت وحصولها على 10 نقاط فقط (معوقات النفاذ: 8 نقاط، حجب محتوى الأنترنت: 2 نقاط، انتهاك حقوق المستخدم: 0 نقطة)¹ حسب منظمة Freedom house.

2. السيطرة والتحكم: تتحكم الصين في عمليات نقل البيانات من وإلى داخل البلاد وتحدد قائمة بالمواقع الآمنة التي يمكن للصينيين تصفحها بفضل الجدار الناري العظيم، كما أنها تمارس سيطرة كلية على المحتوى في الداخل حيث تفرض سلطة إدارة الأنترنت الصينية قيوداً صارمة على مواقع وتطبيقات الأنترنت ولها كامل الصلاحيات في حذف أي منشور لا يتوافق مع الرؤية العامة للحزب الحاكم مع إمكانية المتابعة القضائية ومعاقبة أصحاب الموقع أو التطبيق²، وتجدر الإشارة إلى أن السلطات الصينية كانت قد حظرت المواقع والتطبيقات الأميركية المشهورة (قوقل، فايسبوك، تويتر... وغيرها) وبدلاً منها يستعمل أكثر من مليار مستخدم صيني للأنترنت مواقع وتطبيقات صينية كمحرك البحث بايدو Baidu وتطبيق التواصل الاجتماعي ويشات Wechat³ وهذا ما يمنح الحكومة في الصين قدرة كبيرة على السيطرة والتحكم في الفضاء السيبراني الصيني، أما على المستوى العالمي فالصين تستخدم المساومة لإخضاع شركات التكنولوجيا العالمية للسماح لها بالعمل في الصين (المفاوضات مع قوقل) ولعل تطبيق تيك توك Tik Tok هو التطبيق الصيني الوحيد (النسخة الصينية تسمى Douyin) الذي يُستعمل على نطاق عالمي واسع حيث يقرب عدد مستخدميه المليار مستخدم⁴.

3. الدفاع السيبراني: كشفت كل من تسريبات سنودن 2013 وتقرير شركة الأمن السيبراني Mandiant الأميركية حول وحدة التجسس السيبراني (61398) التابعة لجيش التحرير الصيني PLA⁵ ضعف الدفاعات السيبرانية الصينية على المستويين المدني والعسكري، وهو ما دفع القادة الصينيين وعلى رأسهم الرئيس تشي جين إلى إعادة هيكلة للهيئات المسؤولة عن الدفاع والأمن السيبراني ووضعها تحت قيادة موحدة تخضع لسلطة الرئيس المباشرة حيث تم تشكيل مجموعة

¹ إحصائيات منظمة Freedom House على الرابط: <https://bit.ly/3mhJhsI>

² Emily Quan, "Censorship Sensing: The Capabilities and Implications of China's Great Firewall Under Xi Jinping", *Sigma: Journal of Political and International Studies*, Vol 39, Article 4, 2022, pp 19-31.

³ Ibid.

⁴ حسب إحصائيات موقع Wearesocial لشهر أبريل 2022 على الرابط: <https://bit.ly/3P7OySN>.

⁵ Center Mandiant Intelligence, *APT1: Exposing one of China's cyber espionage units*, Mandian.com, 2013. URL: <https://bit.ly/3QQxP7Y>.

القيادة المركزية للأمن السيبراني وأمن المعلومات CLSGISI رُقِيَتْ في 2018 إلى اللجنة المركزية للمعلومات والأمن السيبراني CCIC (وتعرف أيضاً باللجنة المركزية لشؤون الفضاء السيبراني CCAC)، كما أنشأ هيئة جديدة هي إدارة الفضاء السيبراني الصينية CAC مهمتها التحكم في محتوى الأنترنت، حماية الأمن السيبراني وتطوير الاقتصاد الرقمي¹ عبر إصدار القوانين والتنظيمات الملزمة التي تصدرها دورياً بغية تعزيز الدفاع والأمن السيبرانيين.

إضافة إلى ذلك تسعى الصين من خلال خطتها الواعدة "صنع في الصين 2025" إلى توطين التكنولوجيا الفائقة والتخلص من التبعية الغربية، أما ما يتعلق بالجانب العسكري، فقد تمت إعادة هيكلة الجيش الصيني في 2015 وتم إنشاء قوات الدعم الاستراتيجي SSF والتي تعتبر بيئة تشغيلية مشتركة لتنفيذ مهام الدفاع والهجوم في الفضاء والفضاء السيبراني².

لكن في المقابل تُشير الإحصائيات³ إلى أن صناعة الأمن السيبراني في الصين لاتزال في بدايتها حيث قُدرت مداخيلها سنة 2019 بـ 8 مليار دولار فقط وهذا ما يمثل 7% من إجمالي المداخيل العالمي، رغم توقعات الجمعية الصينية للأمن السيبراني CAICT بزيادة حجم سوق الأمن السيبراني وبلوغه 80 مليار يوان ما يعادل 12 مليار دولار بحلول 2023⁴، كما تُعاني الصين من ضعف أكاديمي في مجال الأمن السيبراني وعدم تواجد لجامعاتها في ترتيب أحسن الجامعات العالمية في المجال، ولذلك جاءت في المرتبة 33 حسب مؤشر الأمن السيبراني 2021 للاتحاد الدولي للاتصالات، وهذا ما يخلق تحدياً كبيراً أمام السلطات الصينية لحماية والدفاع عن الفضاء السيبراني الصيني بمستخدميه الذين يفوقون المليار وشركاته الناشئة التي تُعد بالآلاف.

4. الهجوم السيبراني: تستخدم الصين قدرات سيبرانية منخفضة المستوى في عمليات التأثير وجمع المعلومات، فهي تمتلك خبرة طويلة في تقنيات التسلل والاختراق، ورغم ان الصين لم تنتشر عقيدة للحرب السيبرانية إلا أن كتب الاستراتيجية الصينية تُشير بوضوح إلى العمليات في الفضاء

¹ Mikk Raud, "China and Cyber: Attitude, Strategies and Organization", cyber research Workshop 2015, 2015, pp 16-18.

² Kevin L. Pollpeter, Michael S. Chase, and Eric Heginbotham, The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations, CA:RAND Corporation, 2017, p 14. URL: <https://bit.ly/3xtLQgt>.

³ حسب موقع Gartner تعدى الإنفاق العالمي على الأمن السيبراني 150 مليار دولار سنة 2021 بزيادة قدرها 6.4% عن سنة 2020، للمزيد يرجى الاطلاع على الرابط: <https://gtnr.it/3N29Z3g>

⁴ Cybersecurity Association of China (CAICT), China Network Security Industry Analysis Report 2021 (中国网络安全产业分析报告 2021 年), 2021, p 10. URL: <https://bit.ly/3zDSLX2>.

السيبراني (خاصة الاستطلاع والهجوم)¹، ولا يخفى نجاح جيش التحرير الشعبي الصيني PLA ووكالات الاستخبارات الصينية في اختراق الشبكات الحكومية والصناعية الأمريكية في العديد من المرات وهذا ما يرجح الاعتقاد بإمكانية زرع فيروسات في هذه الأنظمة والشبكات قد تستعمل لاحقاً في حالة الحرب، يتمتع جيش التحرير الشعبي الصيني PLA بالقدرة (من خلال استغلال برامج وأجهزة شركات التكنولوجيا الصينية²) والإرادة (إيديولوجيا وتعليمات الحزب الحاكم) لاختراق أنظمة الخصم بغرض جمع المعلومات الاستخبارية والعمليات الهجومية.

5. المخابرات: تتكون أجهزة الاستخبارات الصينية من العديد من الوكالات المدنية والعسكرية، وأهمها وزارتي أمن الدولة MSS والأمن العام MPS، وترتكز مهمتهما في مسح التهديدات والتجسس داخلياً وخارجياً، كما تُعتبر قوات الدعم الاستراتيجي SSF الذراع الاستخباراتي لجيش التحرير الوطني الصيني PLA، تعتمد هذه الوكالات في توفير المعلومات داخلياً على ما توفره أنظمة المراقبة عبر الأنترنت، إضافة إلى شبكة هي الأضخم في العالم من كاميرات المراقبة CCTV حيث يفوق عددها 400 مليون كاميرا مراقبة³.

أما خارج الصين فعمليات الوكالات الصينية تعتمد على مجموعات الهاكرز والتطبيقات بغية جمع أكبر حجم ممكن من البيانات بغض النظر عن تعقيد العمليات أو كشفها، وقد جاء في القانون الوطني للاستخبارات لسنة 2017 في مواده 7 و14 أنه "يجب على المواطنين والمنظمات الصينية مساعدة أجهزة الاستخبارات الوطنية إذا طلبت ذلك"⁴، وهو ما يعني أن كل الصينيين أفراداً كانوا أو شركات ملزمون بالمساعدة في جمع المعلومات لفائدة الحكومة، وهذا ما جعل الدول الغربية تتهم شركات التكنولوجيا الصينية الكبرى مثل هواوي بالتجسس لصالح الحكومة.

6. التجارة الإلكترونية والاقتصاد الرقمي: تُعد الصين سوقاً كبيراً للتجارة الإلكترونية والابتكار وهو يتوسع بسرعة (خاصة بعد جائحة كورونا وقوانين الحجر الصحي)، يقوم 64% من الصينيين بالتسوق عبر الأنترنت بحجم سوقي يُقدر بـ 1,5 تريليون دولار أي ضعف السوق الأمريكية،

¹ Research Department of Military Strategy, **The Science of Military Strategy**, Military Science Press, 2013, p 148.

² تحتل الصين صدارة الدول الموردة للتكنولوجيا الفائقة حسب إحصائيات البنك الدولي لصادرات التكنولوجيا الفائقة لسنة 2021، مرجع سابق، على الرابط: <https://bit.ly/3xWxMgU>

³ Paul Bischoff, **Surveillance camera statistics: which cities have the most CCTV cameras?**, comparitech.com, May 17, 2021, URL: <https://bit.ly/3b7hYyP>

⁴ Standing Committee of the National People's Congress, **National Intelligence Law of the People's Republic of China**, Order No. 69, 2017, URL: <https://bit.ly/45CF87a>.

الفصل الثاني:

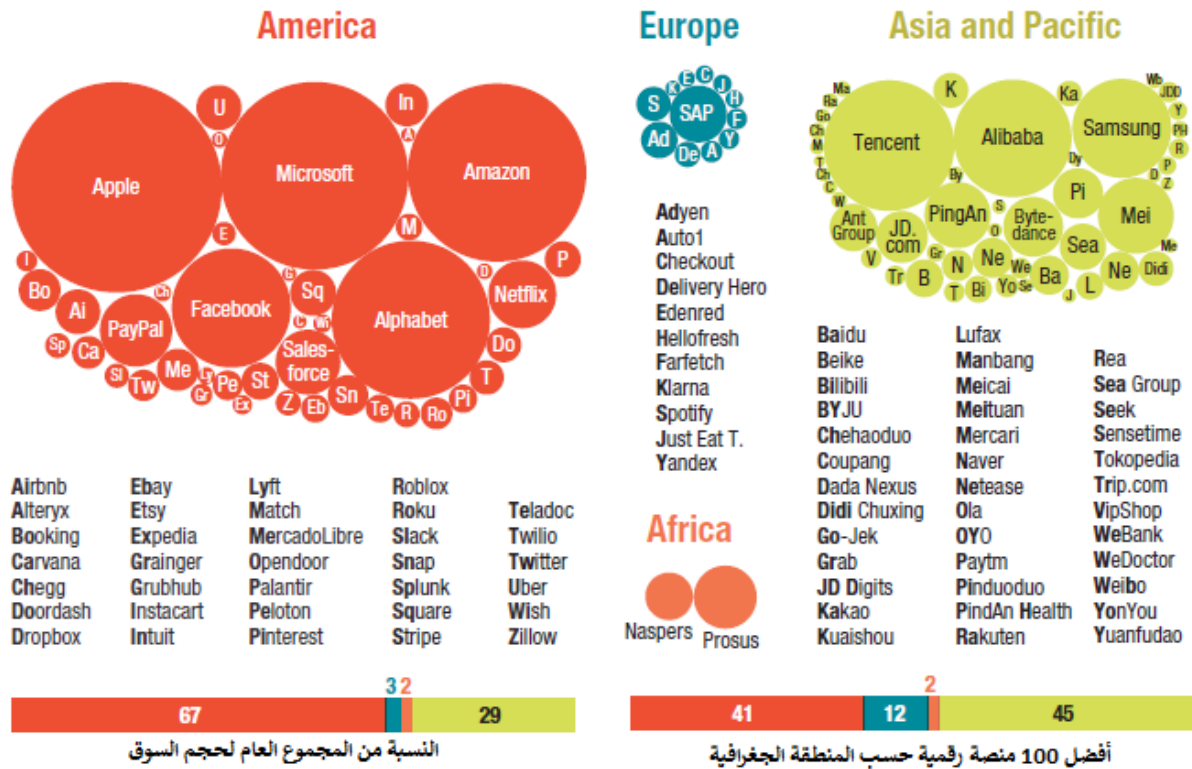
مضامين الصراع الأمريكي الصيني في الفضاء السيبراني

وتُهيمن المنصات الرقمية لـ Wechat و Alipay على عمليات التسوق والتواصل الاجتماعي والمصارف في الصين¹، كما أن شركات التكنولوجيا الصينية هي المنافس الأول والمباشر للشركات الأمريكية في خلق وإدارة الاقتصاد الرقمي العالمي، كما أن الصين تمتلك زمام المبادرة في تقنيات الجيل الخامس والسادس 5G,6G والألياف البصرية إضافة إلى محاولة إصدار أول عملة حكومية رقمية "اليوان الرقمي" وهذا كله يُعزز ويدفع بالاقتصاد الرقمي الصيني نحو الريادة.

شكل رقم 04: التوزيع الجغرافي لأفضل 100 منصة رقمية للتجارة الإلكترونية لسنة 2021

المصدر: تقرير مؤتمر الأمم المتحدة للتجارة والتنمية UNCTAD حول الاقتصاد الرقمي لسنة

2021، على الرابط: <https://bit.ly/47K7Y7n>



7. **القواعد والمعايير:** تحاول الصين تعديل وتغيير القواعد والمعايير المعمول بها في الفضاء السيبراني والمفروضة مسبقاً من طرف الشركات والحكومة الأمريكية، فعلى المستوى التقني تسعى الصين لوضع معايير وقواعد الجيل الخامس (5G) والسادس (6G) وتعديل وتطوير بروتوكولات الأنترنت، وعلى المستوى التنظيمي والتشريعي قدمت الصين للعالم مفهوم "السيادة السيبرانية" في مقابل مفهوم "الفضاء المفتوح" الذي تدعو له الولايات المتحدة، ويتم ذلك من خلال القمة العالمية

¹ حجم التجارة الإلكترونية في الصين هو الأكبر في العالم وقد تجاوزت الولايات المتحدة ابتداءً من سنة 2020، حسب إحصائيات موقع eMarketer على الرابط: <https://bit.ly/3njY7zm>

لحكومة الأنترنت التي تنظمها الصين لمناقشة والدعوة إلى سيادة الدولة على فضاءها السيبراني، إضافة إلى العديد من الاتفاقيات الثنائية والجماعية في مختلف المجالات المتعلقة بالفضاء السيبراني (التدريب، السياسات، الأمن، العمليات السيبرانية، الجريمة...) ¹، وتستغل الصين قوتها الناعمة ² لحشد الدول ودعم رؤيتها لكيفية إدارة وتنظيم الفضاء السيبراني.

خلاصة لما تقدم، لدى الصين مجموعة مهمة من نقاط القوة خاصة ما يتعلق بالتحكم، الهجوم وتطوير القواعد والمعايير، ويبدو واضحاً المجهودات الكبيرة التي تبذلها الحكومة لتطوير بقية الفئات رغم تباين النتائج، كما أن نمو قدراتها السيبرانية المتسارع يعكس نواياها للحاق بالولايات المتحدة.

¹ Theresa Hitchens, Nilsu Goren, **International Cybersecurity Information Sharing Agreements**, Center for International & Security Studies, 2017, pp 11-13.

² احتلت الصين سنة 2022 المركز الرابع في ترتيب القوة الناعمة للدول حسب مقياس **brandirectory.com** للقوة الناعمة، فيما حافظت الولايات المتحدة على الصدارة، خريطة تفاعلية على الرابط: <https://bit.ly/3Nx1wWk>

المبحث الثاني: تجليات الصراع الأمريكي الصيني في/على الفضاء السيبراني

من الواضح أن الفضاء السيبراني والابتكار التكنولوجي أصبحا على قمة السياسات العليا للكثير من الدول، فالصراعات الجيوبوليتيكية حول السلطة تتعكس مباشرة على سعي الحكومات وشركات التكنولوجيا لتحقيق التفوق التكنولوجي والهيمنة على الفضاء السيبراني العالمي، وبناءً عليه، وبالاكتفاء على هندسة الطبقات للفضاء السيبراني فإننا نرصد تنافساً حاداً بين الولايات المتحدة الأمريكية والصين، حيث تحدث في كل طبقة صراعات جيوبوليتيكية بين الدولتين حول النفوذ والهيمنة، ومن أجل فهم أعمق لهذه الصراعات نقوم بالربط بين تحليل جوهر المشكلة (أو القضية) الجيوبوليتيكية من حيث الأسباب والانعكاسات مع تحليل العوامل التي تدفع بها ومدى تأثيرها على مصالح الفواعل والقوى المؤثرة في هذه المشكلة.

المطلب الأول: الصراع على البنية التحتية المادية

سيطرت الولايات المتحدة الأمريكية من خلال شركاتها التكنولوجية على بناء وتطوير البنية التحتية المادية للإنترنت والفضاء السيبراني - التي تشمل على الأجهزة، أجهزة التشبيك ووسائط التشبيك - منذ بدايته ولم تظهر الشركات الصينية كمنافس قوي إلى في السنوات العشر الأخيرة، لذلك سنركز في هذا المطلب على ثلاث قضايا رئيسية تشكل محور الصراع بين الدولتين وهي: تقنيات الجيل الخامس 5G، كوابل الإنترنت البحرية Submarine cables، صناعة أشباه الموصلات Semiconductors .

الفرع الأول: الصراع حول تقنيات الجيل الخامس 5G

تقنية الجيل الخامس هي التقنية الأحدث للاتصالات اللاسلكية ونقل البيانات، تم تصميمها للتعامل مع أعداد كبيرة من الأجهزة وحجم بيانات ضخم، وتتميز عن الأجيال السابقة بسرعة الاتصال العالية (أكبر 100 مرة من الجيل الرابع)، حجم البيانات الضخم و الاتصال عالي الموثوقية وكذلك توفير القدرة على اتصال الآلات فيما بينها، ونتيجة لذلك فتقنيات الجيل الخامس تُقدم وعوداً كبيرة للنمو الصناعي والاقتصادي والمجتمعي، كما ترتبط تقنيات الجيل الخامس بعمليات تطوير المدن الذكية، السيارات الذكية، المنازل الذكية، إنترنت الأشياء IoTs وغيرها،

يقول "ستيفين هو" مدير الإنتاج لشركة هواوي "لقد غير الجيل الرابع الحياة، لكن الجيل الخامس سيغير المجتمع"¹.

تمتد تأثيرات تقنيات الجيل الخامس إلى الصناعة، التجارة، التمويل، التواصل الاجتماعي، التعليم والصحة وغيرها، إلا أن المخاوف الكبرى تتركز حول أثره على استقلالية صنع واتخاذ القرار لدى القادة والسياسيين والأمن القومي بصفة عامة، فسيطرة كل مناحي الحياة تزيد من مخاطر التهديد والقابلية للاختراق وتعطيل الخدمات، كما أن سيطرة طرف ثالث **Third party** على وسائل الإتصال ونقل البيانات قد يعرض الدولة بأكملها للخطر.

في جوان 2019 أصدرت وزارة الصناعة وتكنولوجيا المعلومات الصينية تراخيص تجارية لاستغلال الجيل الخامس 5G لصالح متعاملي الهاتف وشركات الاتصالات الصينية²، كان هذا الحدث إعلاناً عن بدء عصر جديد لتكنولوجيا الاتصالات والمعلومات ICT بقيادة الصين في تحدٍ واضح للريادة والهيمنة الأمريكية، تلى هذه الخطوة كم هائل من الدراسات والتصريحات والتحذيرات والمخاوف - خاصة في الولايات المتحدة وأوروبا - حول التهديدات والمخاطر التي تصاحب استخدام هذه التقنية على الأمن السيبراني والخصوصية والحريات، واللافت للانتباه أن معظم الإنتقادات والتحذيرات كانت حول جنسية الشركة المطورة للتقنية وليس للتقنية بحد ذاتها مع احتمالية أن تسيطر الصين على وضع المعايير التقنية **Standards** للتقنية الجديدة بعد أن كانت العملية إختصاصاً أمريكياً صرفاً حيث وضعت الشركات الأمريكية المعايير لكل الأجيال السابقة (1G, 2G, 3G, 4G)، لذلك فمن المفيد لدراستنا هذه فحص الشركات الكبرى والدول المتنافسة في هذا المجال.

تُهيمن الصين والولايات المتحدة على سباق تقنيات الجيل الخامس، وهذا ما جعل الفاعلين سواءً كانوا مطورين أو متعاملي الهاتف مقعدين بشدة بالصراع الجيوبوليتيكي بين الدولتين، ويمكننا رصد الصراع بين هذه الشركات في أربعة فئات أساسية هي:

¹ James Barton, "4G changed lives. 5G will change society" – Huawei's Steven Wu, developingtelecoms.com, March 2019. URL: <https://bit.ly/3nmSroi>.

² Zhengmao Li, Xiaoyun Wang, and Tongxu Zhang, **5G+: How 5G change the society**, Springer Nature, 2020, p xv.

1. الصراع حول حقوق الملكية الفكرية: تُشير تقارير حديثة¹ (جوان 2022) إلى تفوق طفيف للشركات الصينية في براءات الاختراع الخاصة بتقنيات الجيل الخامس، لكنها في المقابل لا تمثل إلا ربع ¼ الابتكارات العالمية، الجدول الموالي يقدم نسبة براءات الاختراع لكل دولة حسب ما تقدمه شركاتها التكنولوجية.

جدول رقم 03: نسب براءات الاختراع لتقنيات 5G حسب الشركات والدول.

المصدر: تقرير من Iplytics على الرابط: <https://bit.ly/3YJNTu1>

الترتيب	الدولة	الشركات	نسبة براءات الاختراع
01	الصين	Huawei, ZTE, CATT, Oppo	26.79%
02	الاتحاد الأوروبي	Nokia, Ericsson, Innovative Technology, Sisvel	15.59%
03	كوريا الجنوبية	Samsung, LG, KT	25.94%
04	الولايات المتحدة	Qualcomm, Intel, InterDigital, Apple, Optis	17.75%
05	اليابان	Sharp, Fujitsu, Sony, NEC	8.52%

2. الصراع على وضع معايير 5G: هيمنت شركة كوالكوم Qualcomm الأمريكية على هيئات وضع المعايير التقنية (3GPP، ITU) لعقود، لكن هذه الهيمنة تشهد تحدياً جدياً من طرف شركة هواوي Huawei الصينية كنتيجة لتعزيز الصين مكانتها داخل هذه الهيئات، لذلك فإن عملية وضع معايير تقنية للجيل الخامس تشهد صراعاً جيوبوليتيكياً متعدد الأطراف (الاتحاد الأوروبي بدرجة أقل) وقد يحسم هذا الصراع مدى التطور التكنولوجي لأحد الأطراف وجاذبية التسويق داخل أعضاء الهيئتين 3GPP وITU.

3. الصراع على سوق معدات 5G: تُسيطر ثلاث شركات كبرى على سوق معدات الشبكات اللاسلكية (RAN : Radio Access Network) وهي: هواوي الصينية، نوكيا الفنلندية وإيركسون السويدية، حيث تفوق مبيعاتها مجتمعة 80% من إجمالي سوق المعدات، وأعلنت هواوي على موقعها أنها تتصدر القائمة حسب تقرير موقع Globaldata في السداسي الأخير من سنة

¹ Tim Pohlmann, Magnus Buggenhagen, **Who is leading the 5G patent race?**, Iplytics, June 2022, URL: <https://bit.ly/3YJNTu1>.

¹ 2021، وجاءت الشركة الأمريكية سيسكو Cisco في المركز الخامس بعد نوكيا، إيركسون و ZTE.

وخلاصة لما سبق، فالمستقبل الواعد لتقنيات الجيل الخامس 5G سواءً تعلق الأمر بالنمو الاقتصادي الكبير أو ابتكار التقنيات الحيوية في مختلف المجالات، جعل كلاً من الصين والولايات المتحدة تنظر إلى تقنيات الـ 5G كأحد العوامل - الأدوات - الأساسية الأكثر تأثيراً في صراع القوى العظمى.

ترى الصين أن "صراع 5G" هو القفزة الكبرى لموقعها العالمي في تكنولوجيا المعلومات والاتصال ICT من خلال ادراكها بأن الصين كانت "متأخرة عن 1G، متابعة لـ 2G، اخترقت 3G، متزامنة مع 4G، ومن المتوقع أن تقود الـ 5G"²، وعليه فالصين تركز على الاستثمار الحكومي الضخم والواسع في تقنيات الجيل الخامس، في المقابل، تعتبر الولايات المتحدة أن "سباق الـ 5G هو سباق يجب على الولايات المتحدة أن تفوز به" كما صرح بذلك الرئيس الأسبق دونالد ترمب³، وحرصاً منها على كبح تقدم الشركات الصينية⁴ قامت بعمليات حظر واسعة للتكنولوجيا الصينية خاصة منتجات شركة هواوي داخل الولايات المتحدة ومارست ضغوطاً كبيرة على الدول الحليفة لاتباع نفس النهج، كما شكلت تحالفاً لشركات تكنولوجية عبر العالم لمواجهة الشركات الصينية من خلال تقديم تقنية Open-RAN والتي تسمح للمتعاملين بتثبيت منتجات متعددة المصدر بغية زيادة فرص هذه الشركات للتفوق على شركة هواوي، ولعل أبرز المقترحات هي تلك التي قدمها وزير العدل في إدارة ترمب وليام بار William Barr الذي صرح بأن "السماح للصين بالسيطرة على سوق الجيل الخامس هو تهديد للأمن القومي ومستقبل الاقتصاد الأمريكي على حد سواء"، لذلك فقد دعا الولايات المتحدة للاستثمار (شراء حصص

¹ Glen Hunt, 5G Mobile Core: Competitive Landscape Assessment, Globaldata.com, November 2021, URL: <https://bit.ly/3yC03th>.

² تقرير صادر عن المركز الصيني للتبادلات الاقتصادية الدولية والأكاديمية الصينية لتكنولوجيا المعلومات والاتصالات بتكليف من شركة Qualcomm China لتقييم أهمية تقنية 5G للاقتصاد الصيني:

China International Economic Exchange Center, 2020 China 5G Economic Report (2020 中国 5G 经济报告), 2020, URL: <https://bit.ly/3yDXo2w>.

³ Roosevelt Room, Remarks by President Trump on United States 5G Deployment, trumpwhitehouse.archives.gov, April 12, 2019, URL: <https://bit.ly/3IaEeEi>

⁴ Ellen Nakashima, Jeanne Whalen, Barr suggests U.S. consider investing in Nokia, Ericsson to counter Huawei, The Washington Post, February 6, 2020, URL: <https://wapo.st/3ydPQ4T>

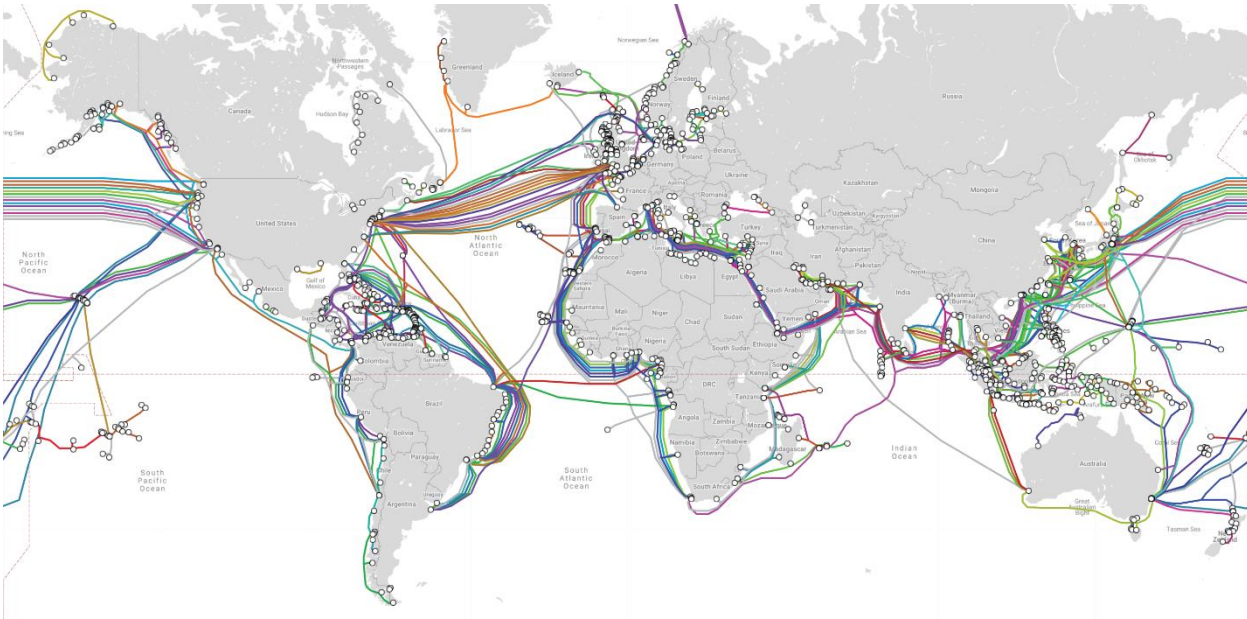
كبيرة من الأسهم) في كل من شركتي نوكيا وايركسون ودعمهما بقوة للتغلب على شركة هواوي، هذا التنافس الشديد جعل من شركات التكنولوجيا -خاصة هواوي- في قلب الصراع الجيوبوليتيكي على تقنيات وسوق الجيل الخامس وعلى الفضاء السيبراني بشكل عام.

الفرع الثاني: الصراع على كوابل الأنترنت البحرية Submarine cables

تُعد كابلات الألياف البصرية البحرية العمود الفقري للبنية التحتية الحيوية للفضاء السيبراني (الأنترنت) حيث يمر عبرها أكثر من 99% من حركة الاتصالات الدولية¹ للاستخدام الشخصي، التجاري والحكومي. يمتد عبر البحار والمحيطات حالياً 486 كابل بحري (نشط أو قيد الإنجاز) بطول إجمالي يتعدى 1,35 مليون كلم و 1306 منشأة أرضية لربط نهايات الكوابل (شكل رقم 05)².

شكل رقم 05 : خريطة كوابل الألياف البصرية البحرية.

المصدر : Telegeography.com



يتضمن استغلال الكابل البحري ثلاث (03) مراحل رئيسية هي: صناعة الكابل البحري والمعدات المرتبطة به، عمليات التثبيت، الصيانة، الإصلاح والترقية عبر قاع البحار والمحيطات، ملكية الكابل (الكيان الذي يستغل الكابل)، وكل مرحلة من هذه المراحل تشهد صراع بين مجموعة

¹ حسب إحصائيات مؤسسة تكنولوجيا المعلومات والإبتكار ITIF على الرابط: <https://bit.ly/3RdZBZu> فيما تقدرها بيانات Google بـ 98% على الرابط: <https://bit.ly/300kN74>.

² حسب إحصائيات موقع Telegeography لسنة 2022، خريطة تفاعلية على الرابط: <https://bit.ly/3R9kKEm>.

من الكيانات الخاصة، الكونسريوم (اتحاد مجموعة من الكيانات الخاصة و/أو الحكومية)، الكيانات الحكومية التابعة للدولة.

1. تتصدر صناعة الكوابل البحرية والمعدات الخاصة بها عدة شركات أبرزها: شركة Alcatel Submarine Networks وهي شركة فرنسية تابعة لشركة Nokia، شركة HMN Technologies فرع من شركة هواوي الصينية، شركة NEC اليابانية، شركة SubCom الأمريكية.

2. في مجال التركيب وتثبيت الكوابل في البحار تتصدر الشركة الأمريكية SubCom تليها الشركة الفنلندية Alcatel Submarine Networks والشركة الفرنسية Orange marine إضافة إلى الشركة البريطانية Global Marine Systems وأخيراً الشركة الصينية هواوي مارين HMN Technologies والتي تشارك في 122 مشروعاً للكوابل البحرية عبر العالم بطول 78 ألف كلم¹ كما أنها قامت بعمليات إصلاح، صيانة وترقية أكثر من 100 كابل بحري أي ما يعادل ربع الكوابل البحرية الموجودة عبر العالم².

3. تقليدياً، تمتلك شركات الاتصالات الكوابل البحرية، كما بدأت شركات الأنترنت في امتلاك حصص في الكوابل، لكن الطفرة حدثت مع بداية العقد الثاني من القرن الحالي، حيث أصبح ما يُعرف بشركات تقديم المحتوى تمتلك كوابل بحرية خاصة بها أو بمشاركة شركات أخرى، وتسيطر الشركات الأمريكية على الاستثمار في ملكية الكوابل البحرية ومنشآت الهبوط (انظر شكل رقم 05) فشركة قوقل تمتلك 20 كابل بحري، شركة ميتا -فايسبوك سابقاً- تمتلك 16 كابل، شركة ميكروسوفت تمتلك 5 كابلات وأمازون 5 كابلات³، في المقابل تمتلك ثلاث شركات اتصالات صينية هي: Telecom China و China Unicom و China Mobile حصصاً في 31 كابلاً بحرياً و تخطط لامتلاك المزيد⁴.

¹ حسب بيانات موقع الشركة على الأنترنت، خريطة تفاعلية على الرابط: <https://bit.ly/3AIksOP>.

² Jeremy Page, Kate O'Keeffe, Rob Taylor, **America's Undersea Battle with China for Control of the Global Internet Grid**, Wall Street Journal, March 12, 2019, URL: <https://on.wsj.com/3Rv6VAg>.

³ Alan Mauldin, **A Complete List of Content Providers' Submarine Cable Holdings**, blog.telegeography, Nov 9, 2017, URL: <https://bit.ly/3bOsCuF>

⁴ Matthew P. Goodman, Matthew Wayland, **Securing Asia's Subsea Network: U.S. Interests and Strategic Options**, CSIS Briefs, CSIS, April 5, 2022, URL: <https://bit.ly/3Pd9RzD>

من ناحية أخرى، تتعرض الكابلات البحرية إلى العديد من المخاطر التي تهدد الاتصالات العالمية، ومع زيادة حجم البيانات التي تمر عبر هذه الكابلات والاعتماد الكثيف عليها في مختلف القطاعات المالية، الاقتصادية، المجتمعية والعسكرية، فإن حجم الضرر يتضاعف في حالة تعطل أو قطع أي منها، فرغم أن المخاطر الطبيعية كالزلازل والبراكين تحت البحر تتسبب في تلف الكوابل وتجعل من الدول معزولة عن العالم وتحملها خسائر اقتصادية ومالية كبيرة، إلا أن المخاطر ذات الطبيعة البشرية كعمليات الصيد ورسو السفن هي الخطر الأكبر الذي يتسبب في قطع الكوابل البحرية، كما أن الصراعات الجيوبوليتيكية تجعل من الكابلات البحرية أداة استراتيجية لدى الدول، فالخوف من تعطيل أو قطع هذه الكابلات أثناء النزاعات وما يترتب عنه من قطع للاتصالات وعزل للدول عن العالم، إضافة إلى إمكانية زرع معدات تجسس على الكابلات أو في منشآت الهبوط وسرقة البيانات جعلت كلاً من الصين والولايات المتحدة تعتبر السيطرة على الكابلات البحرية (في كل مراحلها) هدفاً استراتيجياً يجب تحقيقه والفوز بالسباق فيه.

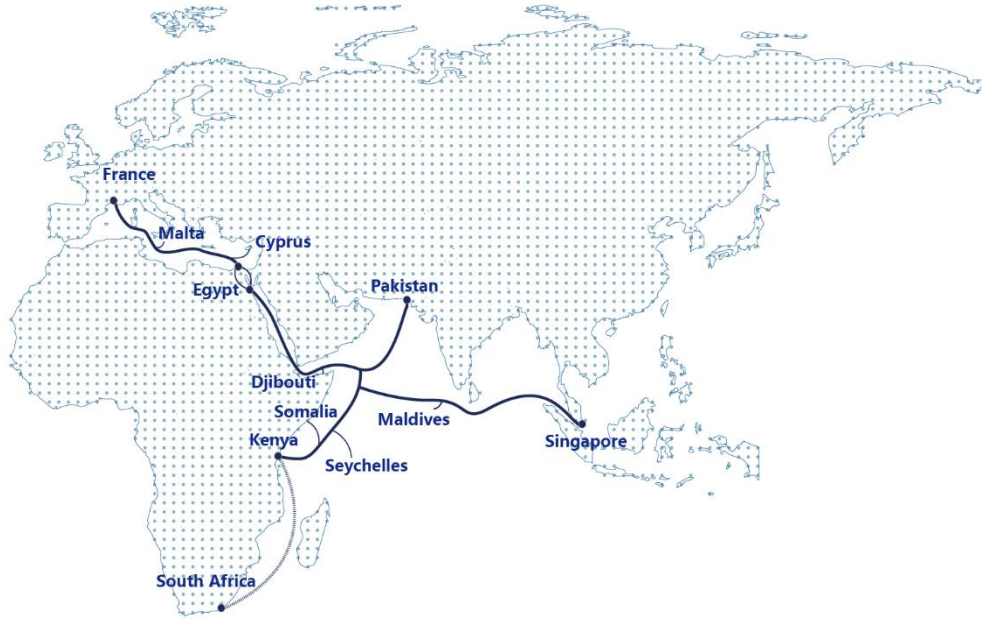
فالصين تسعى من خلال شركاتها التكنولوجية وخاصة شركة **هواوي مارين** إلى كسب المزيد من الأسواق والحصول على أكبر عدد من صفقات الكابلات البحرية سواءً تعلق الأمر بصناعتها، تثبيتها وصيانتها أو امتلاكها وتسييرها، فبعد فشل مشروع الكابل الخاص بمجموعة البريكس¹ والذي جاء كردة فعل على تسريبات سنودن 2013 وكشفه عن عمليات التجسس الكبيرة التي قامت بها الولايات المتحدة الأمريكية بفضل استحوادها على ملكية معظم الكابلات البحرية ومنشآت الهبوط، تعمل الصين على تنفيذ مشروع **طريق الحرير الرقمي Digital Silk Road** والذي يُعد جزءاً من مبادرة الحزام والطريق والذي تُعده الصين من أولويات سياستها الخارجية، ويتكون من الكوابل البحرية (عبر **Peace cable** الذي يربط الصين بإفريقيا وأوروبا) (انظر الشكل رقم 06)) والبرية (تربط بين الصين وباكستان) والأقمار الصناعية وتكنولوجيا الجيل الخامس، حيث تسعى من خلاله الصين إلى تحسين قدرات الدول التي يشملها في مجال الاتصالات السلكية واللاسلكية والكثير من مجالات التكنولوجيا الفائقة² (لعل أهمها تكنولوجيا المراقبة) وهذا ما يزيد من قدرتها على التأثير الجيوبوليتيكي والهيمنة على الفضاء السيبراني العالمي.

¹ Anna Zyw Melo, « Un câble pour les BRICS : un défi stratégique insurmontable », **Hermès, La Revue**, Vol. 79, N° 3, 2017, pp. 145-149.

² Joshua Kurlantzick, James West, **Assessing China's Digital Silk Road Initiative**, Council on Foreign Relations, 2020, URL: <https://on.cfr.org/3Pq95iU>.

شكل رقم 06: خريطة الكابل البحري "السلام".

المصدر: peacecable.net



في المقابل، ترى الولايات المتحدة ومعها الدول الغربية (يطلقون على أنفسهم اسم الديمقراطيات، في مقابل اسم الدول الشمولية: الصين وروسيا) أن تهديد الشركات الصينية هو مزيج من الجيوإيكونوميك والجيوبوليتيك، فسيطرة الولايات المتحدة على معظم الكابلات ومنشآت الهبوط يجعل منها مركزاً مالياً دولياً هاماً بعمليات تتجاوز 10 ترليون دولار يومياً، كما أن الصادرات الرقمية الأمريكية تعدت 520 مليار دولار سنة 2020، والقطاع الرقمي من المتوقع أن يوفر أكثر من 21 مليون وظيفة في الولايات المتحدة سنة 2024¹.

وعليه، فزيادة سيطرة الشركات الصينية على الكابلات البحرية يُشكل تهديداً مباشراً للقطاع الاقتصادي والمالي الأمريكي، كما يُشكل في الوقت نفسه تهديداً للأمن القومي الأمريكي، حيث تسعى الصين لتغيير طبولوجيا البنية التحتية للفضاء السيبراني مما يسمح لها بالوصول إلى أكبر حجم من البيانات الرقمية وامتلاك القدرة على قطع أو تعطيل الكابلات البحرية خلال النزاعات وهذا ما يجعل الولايات المتحدة في حالة من الانكشاف الاستراتيجي الخطير، لذلك تسعى الولايات المتحدة وحلفاؤها الغربيون إلى محاولة الحد من التمدد الصيني في قطاع الكابلات البحرية من خلال تقويض مشاريع تثبيت أو صيانة الكابلات البحرية التي تشارك فيها شركات صينية، وزيادة

¹ Matthew P. Goodman, Matthew Wayland, **op.cit.**

الاستثمار في مشاريع الكابلات التي تتجنب البر الصيني وبحر الصين الجنوبي في محاولة للتقليل من تأثير الصين عليها¹، ومؤخراً قدم الرئيس الأمريكي جون بايدن في قمة مجموعة السبع G7 لسنة 2022 المنعقدة في ألمانيا، مبادرة الشراكة من أجل البنية التحتية والاستثمار العالميين (PGII) لمواجهة مبادرة الحزام والطريق الصينية والتي تتضمن إنشاء كابل بحري لربط سنغفورة بفرنسا (آسيا بأوروبا) مروراً بمصر والقرن الإفريقي² في تحدٍ واضح لمشروع طريق الحرير الرقمي.

الفرع الثالث: الصراع على صناعة أشباه الموصلات Semiconductors

أشباه الموصلات هي تلك الرقائق المكونة من مليارات الدارات الالكترونية الدقيقة، وقد ساهم تطور أشباه الموصلات في التطور الكبير لأجهزة الحاسب الآلي في الثمانينيات، تطور الأنترنت في التسعينيات وتطور الهواتف الذكية في الألفية الجديدة، ويدخل الجيل الثالث منها (الأكثر تطوراً) اليوم في العديد من الصناعات المتقدمة أبرزها الحوسبة الكمومية الفائقة، الذكاء الاصطناعي، الجيل الخامس 5G وأنترنت الأشياء IoT، كما تُعتبر ركيزة أساسية في صناعة الأسلحة المتطورة والطائرات الحديثة والمركبات الفضائية.

تتوزع صناعة أشباه الموصلات على ثلاث (03) فئات رئيسية:

1. فئة البحث والتطوير والتصميم: حيث نجد شركات أتمتة التصميم الإلكتروني (EDA) والتي تقوم بالأبحاث العلمية وعمليات تطوير تصاميم الرقائق عبر برامج وأدوات خاصة، وتسيطر على هذه الفئة مجموعة من الشركات الأمريكية مثل: Cadence، Synopsys و Siemens.
2. فئة تصنيع أشباه الموصلات والمعدات: وفي هذه الفئة يحدث صراع كبير بين الشركات الأمريكية، التايوانية، الكورية الجنوبية، اليابانية والصينية (انظر الجدول رقم 04) وفي الوقت الحالي تحتكر شركتان هما TSMC التايوانية و Samsung الكورية الإنتاج التجاري لأحدث الرقائق من فئة 7 نانومتر (7Nm) فيما تعاني شركة Intel الأمريكية من مشاكل حالت دون تمكنها من تصنيع هذه الفئة من الرقائق، أما فيما يتعلق بمعدات صناعة أشباه الموصلات فتهيمن عليها شركة ASML الهولندية والتي تستخدم تقنيات أمريكية.

¹ Lane Burdette, **Leveraging Submarine Cables for Political Gain: US Responses to Chinese Strategy**, Journal of Public & International Affairs, 2021, URL: <https://bit.ly/3Pjfw72>.

² , **G7 summit: Leaders detail \$600bn plan to rival China's Belt and Road initiative**, BBC.com, June27,2022, URL: <https://bbc.in/3c841Bd>.

3. فئة القياس والاختبار: وتوجد العديد من الشركات التي تقوم بإنتاج أدوات الاختبار ومن ثم دمج الرقائق في الصناعات الإلكترونية المناسبة.

جدول رقم 04: شركات تصنيع الرقائق المتقدمة فئة ما دون 16Nm حسب البلدان.

المصدر: تقرير من مجموعة أوراسيا حول جيوبوليتيكا الرقائق، على الرابط: <https://bit.ly/3PtNqq4>

البلد	الشركة	دقة تصنيع الرقاقة (نانومتر)			
		3	5	7/10	14/16
تايوان	TSMC	○	○	X	X
كوريا	Samsung	○	○	X	X
و.م.أ.	Intel	○	○	°X	X
و.م.أ.	Globale F			X	X
الصين	SMIC			○	X
كوريا	SK hynix			X	X
اليابان	KIOXIA				X

من ناحية أخرى، تُعد الصين المصنع الأول في العالم للأجهزة الإلكترونية، لذلك فاحتياجاتها من رقائق أشباه الموصلات في تزايد مستمر خاصة مع انتعاش الاقتصادات وزيادة الطلب بعد أزمة كورونا، إلا أن الشركات الصينية لا توفر سوى 14% من الطلب المحلي ومن المتوقع أن تصل إلى 40% سنة 2025¹، وهو ما يؤثر على سير خطة "صنع في الصين 2025".

إضافة إلى ذلك، بعد أن كانت هواوي تستعمل في هواتفها أحدث فئة من الرقائق من فئة 7Nm والمصنعة من طرف HiSilicon الفرع الصيني لشركة TSMC التايوانية² قد جعلها العقوبات الأمريكية تتخلف عن الريادة في المستقبل وبالتالي تقف الصين زخم السباق التكنولوجي في مجالات أهمها الجيل الخامس 5G ، لذلك فالصين تنتظر إلى صناعة أشباه الموصلات على أنها ساحة معركة استراتيجية رئيسية، حيث أشار الرئيس "شي جين بينغ" في عام 2018 إلى أن

¹ Antonio Varas, Raj Varadarajan, **How Restricting Trade with China Could End US Semiconductor Leadership**, bcg.com, MARCH 2020, URL: [HTTPS://ON.BCG.COM/3YJW2GK](https://on.bcg.com/3YJW2GK).

² Eurasia Group, **The Geopolitics of Semiconductors**, eurasiaingroup.net, SEPTEMBER 2020, URL: <https://bit.ly/3PtNqq4>

"اعتماد [الصين] على التكنولوجيا الأساسية هو أكبر مشكلة خفية بالنسبة لنا"، وأضاف أنه "يجب علينا تسريع تطوير خططنا المحلية، وإنشاء أنظمة معلومات آمنة يمكن التحكم فيها"¹، تسعى الصين للإبقاء على سلاسل التوريد العالمية والحفاظ على المكاسب التي حققتها في المجال التكنولوجي، وفي نفس الوقت تقوم بتسريع تطوير صناعة الرقاقات المحلية من خلال الاستثمارات الكبرى -أكثر من 200 مليار دولار- والحوافز المقدمة للشركات بُغية تحقيق الاكتفاء الذاتي والتخلص من التبعية الخارجية خاصة الأمريكية في مجال أشباه الموصلات.

في المقابل، تُسيطر الولايات المتحدة على 45% إلى 50% من سوق أشباه الموصلات²، وتحصل على احتياجاتها من الرقاقات الدقيقة من خلال شركة TSMC التايوانية وفرعها الأمريكي WaferTech L.L.C، لكن حجم وسرعة التطور التكنولوجي الصيني عزز المخاوف لدى الولايات المتحدة من فقدان الريادة، وهذا ما فجر الحرب التجارية بين البلدين في 2018، حيث عملت الولايات المتحدة في اتجاهين متكاملين، أولاً، إبطاء وتعطيل التقدم التكنولوجي الصيني، من خلال العمل على حرمان الشركات الصينية من الرقاقات ومن تكنولوجيا صناعتها³، ثانياً، إعادة توطین صناعة أشباه الموصلات داخل الولايات المتحدة، من خلال زيادة الاستثمار والضغط على الشركات الرائدة الأجنبية (TSMC و Samsung) بإنشاء مصانع داخل الولايات المتحدة.

وملخص ما سبق، أن الحرب التجارية بين الولايات المتحدة والصين مع ما خلفته جائحة كورونا كشفت عن ضعف وعدم موثوقية سلاسل توريد أشباه الموصلات المعولمة، وهذا ما دفع البلدان باتجاه الاعتماد على النفس وتوطین تكنولوجيا الرقاقات ومحاولة تجميع كل مراحل صناعة أشباه الموصلات داخل حدود الدولة وهو ما سيعزز الهيمنة في قطاع الرقاقات.

¹ Dashveenjit Kaur, **Chip war: Is China still lagging in the semiconductor race?**, Techwire Asia, March 24, 2022, URL: <https://bit.ly/3o8qXCY>.

² Antonio Varas, Raj Varadarajan, **op.cit.**

³ سارعت الولايات المتحدة إلى فرض حظر على توريد الرقاقات للصين، ووضعت قائمة تضم العديد من الشركات والكيانات الصينية التي يُحظر التعامل معها، انظر: <https://bit.ly/3o4PwAX> و <https://bit.ly/3uRBbvz> ، كما مارست الولايات المتحدة ضغوطاً كبيرة على هولندا لإفشال صفقة بين الصين وشركة ASML لتوريد معدات لتصنيع الرقاقات الدقيقة سنة 2020.

من جهة أخرى، تعاني صناعة أشباه الموصلات من عدم توازن جغرافي، فأكثر من 75% من القدرات التصنيعية تقع في شرق آسيا، كما أن تصنيع الرقاقات الدقيقة يحتكرها بلدان في نفس المنطقة والتي تعاني من توترات ونزاعات جيوبوليتيكية مما قد يرهن مستقبل صناعة الرقاقات، ولعل مشكلة تايوان الجيوبوليتيكية أفضل عنوان للصراع حول أشباه الموصلات، فالولايات المتحدة تدفعها للاختيار بين أمريكا والصين تحت عنوان الحماية والأمن، حتى أن أحد المسؤولين الأمريكيين طالب بتدمير مصانع الرقاقات في حال غزت الصين الجزيرة، والصين ترى أن عودة تايوان للصين الأم أمر لا بد منه، وبين هذا وذاك تعمل تايوان على البقاء على مسافة واحدة من الدولتين حيث جعلت من صناعة أشباه الموصلات ركيزة استراتيجية في سياستها الخارجية.

المطلب الثاني: حوكمة الفضاء السيبراني (الأنترنت)

دفعت عمليات الرقمنة العالمية المتسارعة خاصة خلال جائحة كورونا كلاً من الولايات المتحدة والصين إلى تعزيز منهج ورؤية كل منهما لإدارة الفضاء السيبراني، ففي ظل فضاء غير متجانس ومتعدد الفاعلين والأنظمة والبروتوكولات والمعايير والأجهزة والمؤسسات أضحت قضايا حوكمة الأنترنت من بين أهم تجليات الصراع الجيوبوليتيكي بين الولايات المتحدة والصين، فكل قرار يخص إدارة الأنترنت وإن بدا في ظاهره أنه تقني بحث إلا أن انعكاساته تكون كبيرة على توازن القوى والتوترات السياسية والاقتصادية والاجتماعية.

إن سيطرة التقنيين (في الولايات المتحدة) على وضع القواعد والمعايير الناظمة في بدايات تشكل الفضاء السيبراني لم تعد كافية لضبط هذا الفضاء بعد توسعه متجاوزاً البنتاغون ليشمل القطاع المدني العام والخاص في الولايات المتحدة ثم العالم، هذا التوسع منح شركات التكنولوجيا الأمريكية ميزة حصرية في وضع القواعد والمعايير التقنية والمشاركة في وضع التشريعات والتنظيمات القانونية، لكن مع كثافة التشبيك العالمي والحاجة لاستخدام الفضاء السيبراني في مناحي الحياة المختلفة مع بروز تهديدات ومخاطر أمنية جديدة ظهرت دعوات لإعادة النظر في المسؤولية المنفردة للولايات المتحدة في إدارة الأنترنت، والمطالبة بالمزيد من نقل مسؤوليات الإشراف والإدارة لهيئات دولية أكثر شرعية، وإشراك أصحاب المصلحة المتعددين في حوكمة الأنترنت.

من جهة أخرى، كانت تسريبات سنودن في 2013 نقطة تحول رئيسية في رؤى المطالبين بالحوكمة الدولية للفضاء السيبراني، خاصة في الصين، التي قدمت مفهوم "السيادة السيبرانية" للعالم والذي يتمحور حول عودة الدولة كفاعل رئيس في تنظيم وإدارة الفضاء السيبراني ورسمت بذلك خط الصراع حول حوكمة الأنترنت.

الفرع الأول: نماذج الحوكمة المتصارعة: نموذج أصحاب المصلحة المتعددين في مقابل نموذج مجتمع المصير المشترك في الفضاء السيبراني.

تسيطر الولايات المتحدة الأمريكية على إدارة الأنترنت بحكم أنها بلد المنشأ، وظهر التلميح الأول للحوكمة في بيان السياسة العامة بشأن إدارة الأسماء وعناوين الأنترنت الصادر عن الإدارة الوطنية للاتصالات والمعلومات سنة 1998 والذي يقضي بأن حوكمة الأنترنت هي من اختصاص الشركات الخاصة مع إلزام الحكومة بإدارة الأسماء وعناوين الأنترنت DNS والمحافظة على حقوق الإنسان وحرية التعبير¹.

يُنظر إلى حوكمة الفضاء السيبراني منذ البداية على أنها نظام لامركزي قائم على الشركات الخاصة والمنظمات غير الحكومية، تستخدم الولايات المتحدة اتفاقية بودابست المتعلقة بالجريمة الإلكترونية - خاصة في جزئها الخاص بجمع البيانات دون الرجوع إلى الدولة ذات الصلة - كوثيقة استراتيجية لدعم نموذجها للحوكمة، وفرضت رؤيتها في إعلان مبادئ القمة العالمية لمجتمع الأنترنت 2003 وأجندة تونس لمجتمع المعلومات 2005 اللتين كرّستا مبدأ الأنترنت كفضاء مفتوح يخضع تطوره لقوى السوق وتتم ممارسة الحوكمة فيه بمشاركة جميع الأطراف المهمة، هذا المبدأ كان أساس الاستراتيجية الدولية للفضاء السيبراني لإدارة الرئيس أوباما 2011، والتي عكست بوضوح تعزيز نموذج أصحاب المصلحة المتعددين لحوكمة الأنترنت²، والحرص على تدفق المعلومات بعيداً عن سيطرة الحكومات والدول، وهو ما أكدته الاستراتيجية الوطنية السيبرانية 2018 حيث "تدين الولايات المتحدة محاولات السيطرة على الأنترنت المحلي"³ وتعتبره انتهاكاً لمبدأ حرية الأنترنت في إشارة للصين.

¹ انظر: <https://bit.ly/3yR42B5>

² White house, **International strategy for Cyberspace**, May 2011, URL: <https://bit.ly/3zbUMsU>

³ White house, **National Cyber strategy of the United states of America**, September 2011, URL: <https://bit.ly/3zek9u3>.

في مقابل ذلك، تنطلق الصين في بناء رؤيتها للحوكمة في الفضاء السيبراني من نقد النموذج الأمريكي، حيث ترى الصين أن نموذج أصحاب المصلحة المتعددين يكرس الهيمنة الأمريكية على عمليات وضع القواعد والمعايير والتشريعات في الفضاء السيبراني، فمعظم شركات التكنولوجيا الكبرى أمريكية، كما تسيطر الولايات المتحدة على معظم الهيئات والمنظمات ذات الصلة، فأصحاب المصلحة المتعددين ما هم إلا الوجه الآخر للحكومة الأمريكية.

لذلك، وباعتبار الفضاء السيبراني عنصراً مهماً من عناصر الأمن القومي الصيني فإن الصين تنتهج في إدارة الأنترنت المحلي مبدأ السيادة الكاملة من خلال المراقبة، إدارة المحتوى والبنية التحتية الحيوية، وتسعى لنقل هذه المبادئ للمستوى العالمي، فالأساس النظري للحكومة العالمية للأنترنت وفق الرؤية الصينية يقوم على "نظرية العالم المتناغم" للرئيس الصيني السابق "هو جينتاو" وفكرة "مجتمع المصير المشترك في الفضاء السيبراني" للرئيس الحالي "شي جين بينغ" واللتين تصبان في فكرة تطوير مجتمع دول قائم على التعاون من أجل التنمية والأمن، وقد قدمت الصين من خلال استراتيجية التعاون الدولي في الفضاء السيبراني 2017 المبادئ الأساسية لسياستها السيبرانية والتي تركز على ضمان السلام والأمن ومنع سباق التسلح والصراع، كما أشارت إلى أن مبدأ السيادة يخول للدول اختيار النهج المناسب لإدارة الأنترنت محلياً كما تلعب الأمم المتحدة دوراً رئيسياً في الحوكمة المشتركة للفضاء السيبراني¹.

وعليه، فالحوكمة العالمية للفضاء السيبراني وفق النموذج الصيني هو نظام متعدد الأطراف يعمل ضمن الأمم المتحدة، أساسه الدول يساعدها في ذلك الهيئات غير الحكومية وأصحاب المصلحة كمستشارين، ويسعى هذا النظام للاعتراف بسيادة الدول على فضاءها السيبراني، ويحمي مبدأ عدم التدخل في الشؤون الداخلية للدول، ويسعى لإنشاء مدونة قواعد ومبادئ السلوك للدول في الفضاء السيبراني² والتي ستحول الأنترنت من "منطقة رمادية" للصراع إلى فضاء واسع للتعاون الموثوق والسلام.

¹ انظر الاستراتيجية الصينية للتعاون الدولي في الفضاء السيبراني 2017 على الرابط: <https://bit.ly/3uSBfLx>

² D. A. Degterev, M. S. Ramich, D. A. Piskunov, "US—China approaches to global Internet governance: "New bipolarity" in terms of "the network society"', **International Organisations Research Journal** , Vol 16, N° 3 , 2021, pp 7-33.

الفرع الثاني: الصراع حول حوكمة الأنترنت والقضايا الخلافية

تتباين المقاربتان الأمريكية والصينية حول حوكمة الفضاء السيبراني، ففي حين تسعى الولايات المتحدة للحفاظ على/وتعزيز النموذج الحالي للحوكمة (أي نموذج أصحاب المصلحة المتعددين) الذي يخدم مصالحها ويضمن ريادتها وهيمنتها على الفضاء السيبراني، طورت الصين مجموعة من الأدوات والسياسات المتكاملة لتنفيذ نهجها الجديد للحوكمة والتصدي للهيمنة الأمريكية وذلك عبر العديد من المجالات أهمها:

1. الابتكار ووضع القواعد والمعايير التقنية: بما أن الشركات هي من تضع وتطور القواعد والمعايير التقنية تحاول الصين التصدي لهيمنة عمالقة التكنولوجيا الأمريكية أو ما يسمى **GAFAM** (Google, Apple, Facebook(Meta), Amazon, Microsoft) من خلال تشجيع الابتكار المحلي والاستثمار في شركات التكنولوجيا المحلية مع حظر الشركات الأمريكية من العمل داخل الصين، حيث إن التفوق الصيني في تقنيات الجيل الخامس والذكاء الاصطناعي يمنحها فرصة لوضع القواعد والمعايير التي تخدم مصالحها ورؤيتها للفضاء السيبراني. لكن رد الولايات المتحدة كان حاسماً من خلال فرض حظر مماثل على الشركات الصينية ومنعها من النشاط داخل الولايات المتحدة والضغط على الدول الحليفة (دول الاتحاد الأوروبي ودول تحالف العيون الخمس) لحظر التكنولوجيا الصينية من العمل داخل أراضيها تحت غطاء حماية الأمن القومي، وهذا ما يجعل الفضاء السيبراني أمام انقسام جيوبوليتيكي ويحتم على الدول الاختيار بين التكنولوجيا الأمريكية أو الصينية.

2. تعزيز سيادة الدولة في الفضاء السيبراني: ترفض الصين ودول أخرى (مثل روسيا والبرازيل وغيرهما) النموذج الحالي للحوكمة بحجة أن جعل شركات التكنولوجيا في وضع مساوٍ للدول في إدارة الأنترنت يُضعف سيادة الدول ويجعلها تتفاوض مع فواعل أقوى منها وأكثر خبرة ويمنح ميزة التفوق للشركات الأمريكية -التي أغلبها محظور في الصين- كما يرسخ هيمنة الولايات المتحدة على إدارة الفضاء السيبراني العالمي، لذلك تُروج الصين لمفهوم "السيادة السيبرانية" والذي يُعطي الدول الحق في إدارة فضاءها السيبراني المحلي وحماية أمنها القومي، كما يجعل الدول متساوية وفاعلة في المشاركة في حوكمة الأنترنت في إطار الأمم المتحدة، في المقابل تتهم الولايات المتحدة الدول الاستبدادية (في إشارة إلى الصين وروسيا) بمحاولة السيطرة على الأنترنت وما يترتب عليها من انتهاكات لحقوق الإنسان وحرية التعبير (انتهاك

مبدأ الأنترنت الحر) من خلال القيود الصارمة لاستخدام الأنترنت وعمليات المراقبة الشاملة في الفضاء السيبراني.

3. التصدي لهيمنة الولايات المتحدة على الهيئات الدولية (ICANN): من بين أهم نقاط الخلاف حول حوكمة الأنترنت هي منظمة الإيكان ICANN، وهي المنظمة المسؤولة عن إدارة عناوين الأنترنت وأسماء النطاقات على مستوى العالم، هذه المهمة التي كانت دوماً حكراً على أشخاص وكيانات أمريكية، وبعد أن تسلمت الإيكان المهمة في 1998 ظلت مسؤولة أمام السلطات الأمريكية، وهذا ما دفع الدول المعارضة للهيمنة الأمريكية وعلى رأسها الصين للمطالبة بتمكين المزيد من دول العالم من المشاركة في عملية صنع القرار داخل المنظمة، لكن رفض الولايات المتحدة التخلي عن المنظمة إستمر إلى غاية 2016 بسبب مخاوف أصحاب المصلحة والشركات وحتى بعض المشرعين الأمريكيين من سيطرة دول أخرى -استبدادية- على المنظمة وتسخير الأنترنت لخدمة مصالحهم الخاصة.

رغم تخلي الولايات المتحدة عن دور الإشراف وإعلان المنظمة نفسها منظمة غير ربحية إلا أن بقاء مقرها الرئيسي في الولايات المتحدة وتواجد 10 من مجموع 13 خادم جذر للأنترنت¹ في الولايات المتحدة يُبقي موارد الشبكة الحرجة تحت الهيمنة الأمريكية، وهو ما عزز مخاوف الصين من النفوذ الأمريكي الكبير في الإيكان، رغم هذا فالصين تشارك في عدة لجان استشارية تابعة للإيكان لكنها لم تصل بعد إلى مستوى صنع القرار داخل المنظمة لذلك فهي تعتبر الاتحاد الدولي للاتصالات ITU أكثر مصداقية للإشراف على إدارة الأنترنت، أولاً، لعلاقتها الجيدة بالاتحاد وتواجد ممثلها الكبير فيه هيئاته، فالصيني هوليان جاو انتخب مرتين لمنصب الأمين العام للاتحاد 2014 و 2018، ثانياً، الاتحاد يدعم دور الحكومات في تنظيم الأنترنت، ثالثاً، الاتحاد أكثر فعالية وموثوقية من الإيكان في اتخاذ القرارات وأكثر احتراماً للتنوع السياسي والاقتصادي والثقافي لدول العالم².

¹ خادم جذر الأنترنت هي أجهزة الكمبيوتر المسؤولة عن تخزين أسماء وعناوين الأنترنت، يوجد 13 جهاز رئيسي وأكثر من 1500 جهاز يخزن نسخ عن البيانات، يديرها 12 منظمة وهيئة 10 منها أمريكية، انظر الخريطة التفاعلية على الرابط: <https://bit.ly/3qGCUos>.

² Gianluigi Negro, "A history of Chinese global Internet governance and its relations with ITU and ICANN", *Chinese Journal of Communication*, vol 13, N°1, 2020, pp 104-121.

4. السيطرة على خطاب الحوكمة من خلال المنتديات العالمية (IGF مقابل WIC)

عالتبت القمة العالمية لمجتمع الإنترنت WSIS في جنيف 2013 لأول مرة قضايا حوكمة الإنترنت، تلتها قمة تونس 2005 والتي كان من أهم مخرجاتها الرئيسية اعتماد نموذج أصحاب المصلحة المتعددين وإنشاء منتدى حوكمة الإنترنت IGF الذي يعمل في إطار الأمم المتحدة ويُعتبر منصة متعددة الأطراف، ديمقراطية وشفافة لأصحاب المصلحة المتعددين لمناقشة قضايا حوكمة الإنترنت، يعقد المنتدى قمة سنوية في مدن مختلفة منذ 2006، لا يملك المنتدى سلطة إتخاذ القرارات أو إنشاء المعاهدات بل يكتفي بتسهيل المناقشات حول الأطر التنظيمية المقترحة، والمخاطر المحتملة، والاتجاهات العالمية لإدارة الإنترنت¹، فالمنتدى يوجه ويؤطر خطاب حوكمة الإنترنت وفق الرؤية الأمريكية لذلك نجد الحكومة وشركات التكنولوجيا الأمريكية من أبرز الممولين لمنتدى IGF مالياً وتقنياً².

يجادل نيكولا بالادينو وماورو سانتانييلو في كتابهما حول عملية انتقال IANA بأن خطاب الحوكمة وفق نموذج أصحاب المصلحة المتعددين الذي يُروج لفكرة التفاوض بين أطراف متساوية الوزن في إطار منفتح وديمقراطي، ما هو في الحقيقة إلا تعبير يرسخ الوضع المهيمن للفاعلين الأكثر سلطة في الفضاء السيبراني ويساعد على إقصاء الأطراف الأكثر عرضة للضرر³، لذلك كان الرد الصيني عبر إنشاء المؤتمر العالمي للإنترنت WIC والذي يُعقد سنوياً منذ 2014 في مدينة ووتشن Wūzhèn الصينية ويُعتبر منصة لتبادل الآراء بين الدول والباحثين حول مراجعة نموذج حوكمة الإنترنت الحالي، وقدم الرئيس الصيني "تشي" في قمتي 2019 و 2020 مبادرة "مجتمع المصير المشترك في الفضاء السيبراني" والتي ركزت على التعاون التكنولوجي والاقتصادي بين الدول بما في ذلك نشر تقنيات الجيل الخامس وإدارة الإنترنت تحت مسؤولية الأمم المتحدة⁴، إن الهدف الأساسي من المؤتمر هو توحيد الدول النامية لمعارضة نموذج الحوكمة الأمريكي والتخفيف ولما لا كسر الهيمنة الأمريكية على إدارة الإنترنت.

¹ كتيب عن "منتدى حوكمة الإنترنت"، على الرابط: <https://bit.ly/3aPtIGC>.

² الجهات المانحة للصندوق الاستئماني لمنتدى حوكمة الإنترنت، انظر: <https://bit.ly/3RQRRwT>.

³ Nicola Palladino, Mauro Santaniello, **Legitimacy, Power, and Inequalities in the Multistakeholder Internet Governance: Analyzing IANA Transition**, Springer Nature, 2020, p 01.

⁴ D. A Degterev, M. S. Ramich, D. A. Piskunov, **Op.cit.**

كخلاصة لكل ما سبق، يُطلعننا المشهد الراهن لحوكمة الأنترنت على تصارع نموذجين، نموذج مركزي يدعو لسيادة الدولة، والآخر لامركزي يوزع الحوكمة بين العديد من أصحاب المصلحة، أما بالنسبة للفاعلين فينقسمون إلى ثلاث فئات، أولاً، الحكومات مع هيمنة للحكومة الأمريكية، ثانياً، الشركات مع سيطرة لعمالقة التكنولوجيا الأمريكية والصينية بدرجة أقل، ثالثاً، المجتمع المدني والذي لا يملك نفوذاً كافياً لإسماع صوته، تُقدم الولايات المتحدة نفسها على أنها الضامن الوحيد لفضاء سيبراني آمن، مفتوح وحر، وتُخوف العالم من سيطرة الصين على الأنترنت¹ باسم مبدأ السيادة التي ما هي إلا الوجه الخفي لممارسة الاستبداد.

في المقابل، تتهم الصين الولايات المتحدة بأنها تدعو لحوكمة موزعة ظاهرياً لكن مُهيمنة عليها أمريكياً، كما تؤيد الصين حق البلدان النامية التي تُشكل الأسواق المستقبلية للتكنولوجيا إدارة فضاءها السيبراني والوقوف بوجه الشركات الكبرى، لذلك فالصين تشارك في نموذج الحوكمة الحالي للتصدي للهيمنة الأمريكية وتسعى في الوقت نفسه لخلق نظام وبيئة سيبرانية موازية قد تمنحها الهيمنة أو على الأقل القدرة على تعايش النظامين.

المطلب الثالث: التنافس على البرمجيات

تعتبر البرمجيات روح الأجهزة الرقمية، فهي ما يجعل الأجهزة قابلة للاستخدام ومن خلالها يتفاعل البشر مع الآلات، وتشهد البرمجيات بغتتها الرئيسيتين - أنظمة التشغيل والتطبيقات - صراعاً حاداً بين شركات التكنولوجيا الأمريكية والصينية، ورغم أن هيمنة الشركات الأمريكية واضحة بحكم خبرتها الطويلة في المجال، فإن الصين ومن خلال شركاتها الناشئة تسعى لتقليص الفجوة ومحاولة اللحاق بالسباق.

الفرع الأول: الهيمنة الأمريكية على أنظمة التشغيل

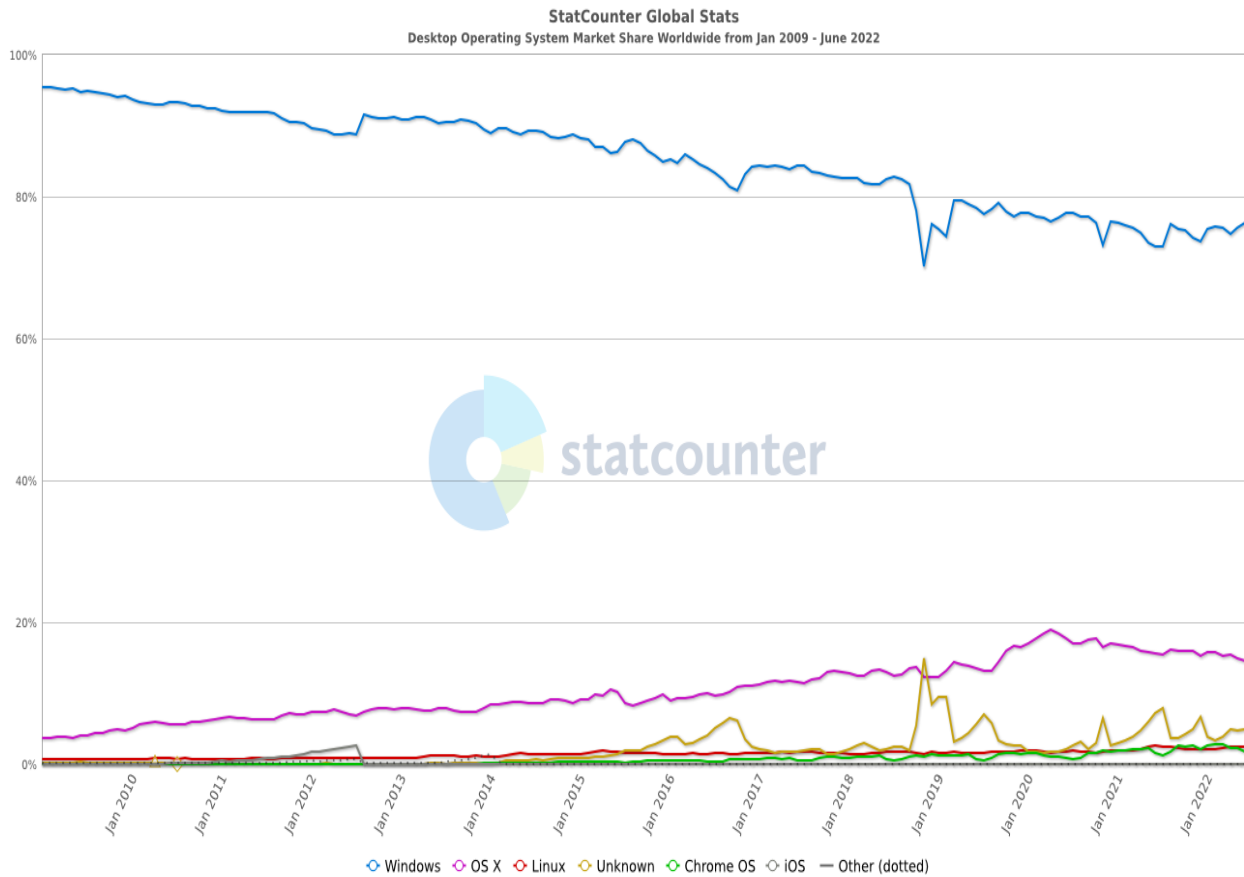
تُسيطر شركتي ميكروسوفت Microsoft و آبل Apple على سوق أنظمة التشغيل منذ بداية تطوير هذه الأنظمة في ثمانينيات القرن المنصرم وحتى يومنا هذا (شكل رقم 07)، حيث يستخدم أكثر من 76% من أجهزة الكمبيوتر في العالم نظام Microsoft Windows، يليه في المركز الثاني نظام OSx لشركة آبل والذي يعمل فقط على أجهزتها بنسبة 14,66%، وتتقاسم بقية الأنظمة المختلفة 20% من السوق حسب إحصائيات موقع statcounter لشهر جوان

¹ Adam Segal, **When China rules the web: technology in service of the state**, Foreign Affaires, september/october 2018, URL: <https://fam.ag/3PYiY7N>.

2022، أما ما يتعلق بالهواتف الذكية فتهمين شركتي (Alphabet) google و Apple على السوق (شكل رقم 08) بنسبة تفوق 99%، حيث يعمل نظام Android على أكثر من 72% من الهواتف الذكية في العالم ويستعمل أكثر من 27% هواتف الآيفون iPhone المزودة بنظام iOS¹.

شكل رقم 07: تطور سوق أنظمة التشغيل لأجهزة الكمبيوتر 2009 – 2022

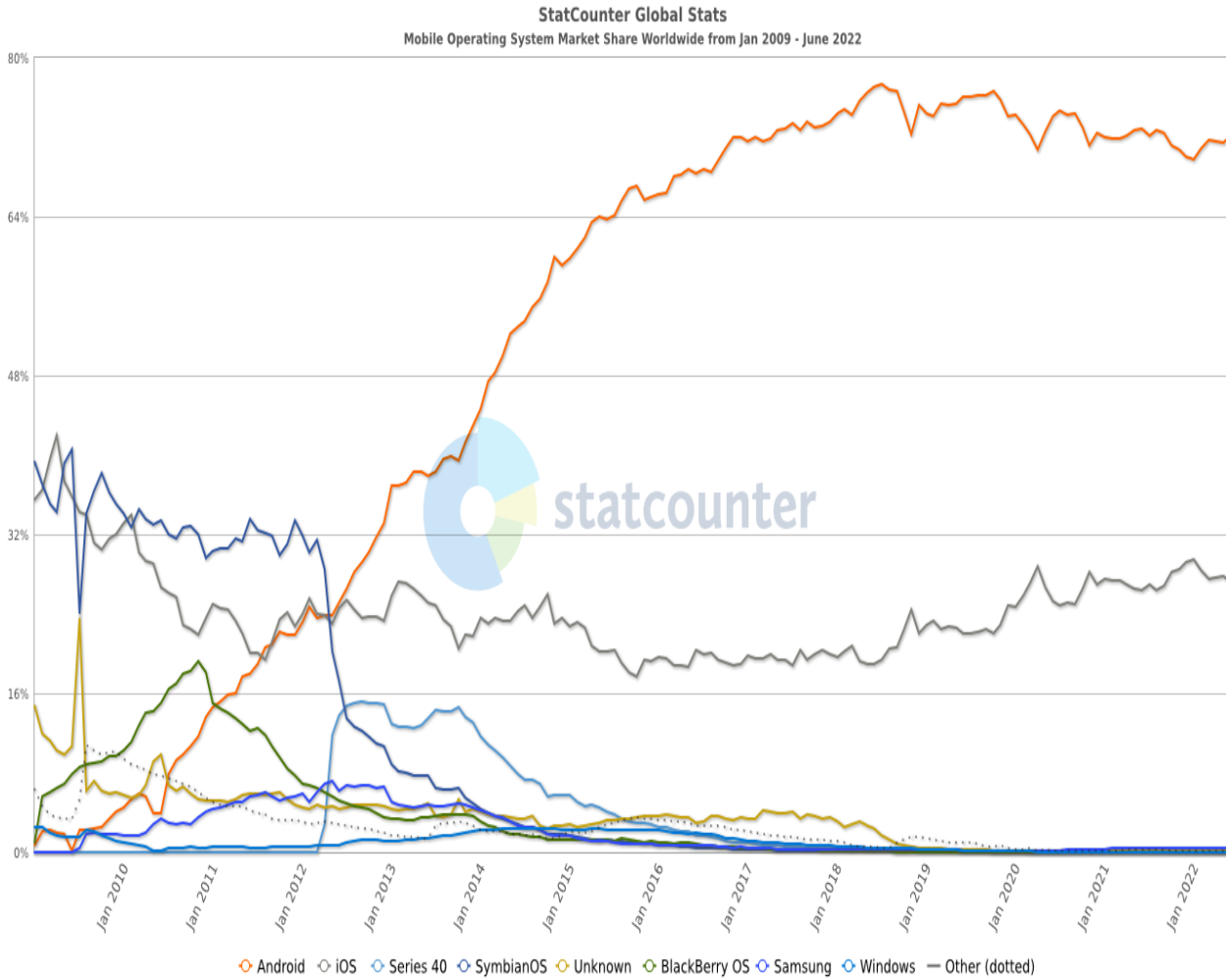
المصدر: موقع statcounter



¹ إحصائيات شهر جوان 2022 حسب موقع statcounter على الرابط: <https://bit.ly/3OwvRo5>.

شكل رقم 08: تطور سوق أنظمة التشغيل للهواتف الذكية 2009 - 2022

المصدر: موقع statcounter



وفي ظل الهيمنة الكبيرة لأنظمة التشغيل الأمريكية وعدم توافر نظام تشغيل صيني بديل ذو جودة، إذ تُشير إحصائيات موقع statcounter لشهر جويلية 2022 أن نظام Windows يُشغل أكثر من 84% من الحواسيب الصينية، تسعى الصين للتخفيف من حدة مخاطر وتهديدات استعمال البرمجيات الأجنبية على أمنها القومي وذلك من خلال؛

أولاً، الضغط على الشركات الأجنبية من أجل إشراك شركات صينية في تطوير نسخ خاصة بالصين من أنظمة التشغيل، حيث طورت شركة Microsoft بالتعاون مع شركة CETC الصينية نسخة خاصة بالحكومة الصينية من نظام Windows 10 سنة 2017¹.

¹ Terry Myerson, **Announcing Windows 10 China Government Edition and the new Surface Pro**, Windows Experience Blog, May 23, 2017, URL: <https://bit.ly/3czRJ4F>.

ثانياً، تطوير نظام تشغيل محلي، حيث بدأت عمليات التطوير منذ بداية الألفية مع نظام **Kylin OS** والذي لم يحقق أي نتائج تجارية واقتصر استعماله على الهيئات الحكومية والعسكرية خاصة بعد الأوامر الصارمة للهيئات الحكومية باستبدال الأجهزة وأنظمة التشغيل الأجنبية ببدايل محلية¹ في إطار خطة الصين الطويلة للتخلص من التبعية التكنولوجية.

أما ما يتعلق بقطاع الهواتف الذكية فيسيطر نظام **Android** لشركة **Google** على 75% من السوق الصينية وتستعمل النظام كبرى شركات صناعة الهواتف الصينية مثل: **Huawei**، **Honor**، **Xiaomi**، **Oppo** وغيرها، لكن العقوبات الأمريكية على شركة هواوي **Huawei** ابتداءً من شهر ماي 2019 سرع من إصدار الشركة لنظام تشغيل من تطوير مهندسيها **HarmonyOS** حيث كان الإطلاق الرسمي للنظام في جوان 2021² والذي من المرجح أن يكون البديل الصيني الموثوق لأنظمة تشغيل الهواتف الذكية.

الفرع الثاني: صراع تطبيقات الهواتف الذكية

وضعت الصين -لأسباب تتعلق بالأمن القومي ومخاوف حول الوصول الحر إلى بيانات مواطنيها- لائحة بتطبيقات الهواتف الذكية ومواقع الأنترنت المحظورة داخل الصين منذ 2009، يتم تحديث القائمة شهرياً ولعل أبرز التطبيقات والمواقع المحظورة تعود ملكيتها لشركات التكنولوجيا الأمريكية، فمنتجات شركة **Meta** (فايسبوك سابقاً) محظورة في الصين، كذلك الشأن بالنسبة لمعظم منتجات شركة **Google**، ويشمل الحظر كذلك الكثير من التطبيقات والمواقع مثل: **Amazon**، **Twitter**، **Youtube**، والمواقع الإخبارية مثل: نيويورك تايمز، بي بي سي، رويترز، سي أن أن وغيرها³، ومن أجل توفير الخدمات التي كانت توفرها هذه التطبيقات والمواقع الأجنبية قامت الصين بدعم شركات التكنولوجيا المحلية حيث ظهرت تطبيقات ومواقع صينية تقدم نفس خدمات التطبيقات الأجنبية وأكثر (أنظر الجدول رقم 05).

¹، **China Orders Government, State Firms to Dump Foreign PCs**, bloomberg.com, mai 6, 2022, URL: <https://bloom.bg/3cEH5tq>.

² Tom Fowdy, **New China-made operating system to offer an alternative**, china.org.cn, June 9, 2021, URL: <https://on.china.cn/3PxDFHD>.

³ Josh Summers, **List of Websites and Apps Blocked in China for 2022**, travelchinacheaper.com, July 1, 2022, URL: <https://bit.ly/3RYXB84>.

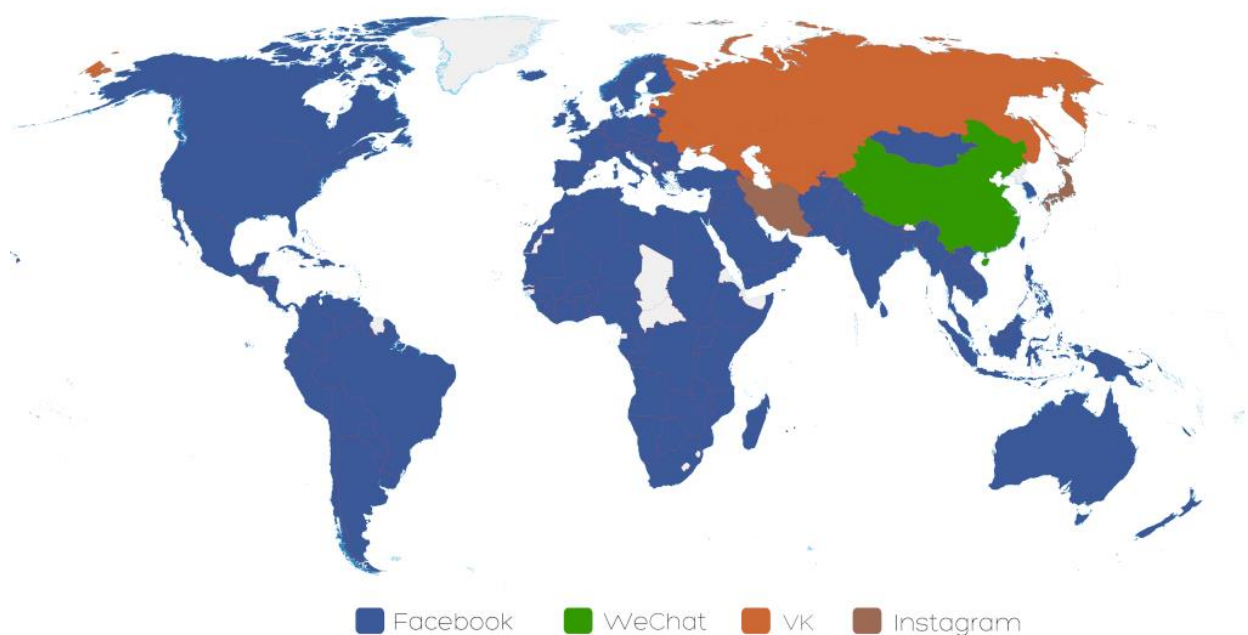
جدول رقم 05: أفضل تطبيقات الهاتف الصينية التي تقدم خدمات شبيهة بالتطبيقات الأمريكية.

المصدر: من إعداد الباحث (بالاعتماد على بيانات عدد من مواقع الإحصائيات)

الشركة	عدد المستخدمين (مليون)	التطبيق الصيني	التطبيق	الخدمة
Tecent	1300	WeChat	Facebook Twitter	التواصل الاجتماعي
Tecent	571	QQ	Messenger Whatsup	الرسائل القصيرة
Bytedance	715	Douyin	Tik Tok	الفيديو
Baidu	677	Baidu	Google	البحث في الإنترنت
Alibaba Group	639 887	AliPay TaoBao	Amazon	التجارة الإلكترونية

شكل رقم 09: خريطة استخدام شبكات التواصل عبر العالم - إحصائيات جانفي 2022.

المصدر: <https://vincos.it/world-map-of-social-networks>



من الواضح من خلال الخريطة أعلاه هيمنة تطبيقات التواصل الاجتماعي الأمريكية في العالم، ماعدا بعض الدول مثل روسيا، إيران والصين، ذلك راجع إلى أن التطبيقات الصينية تدخل في الأساس ضمن سياسة دفاعية وحرمان المنافس من دخول السوق الصينية والوصول إلى بيانات المواطنين الصينيين وليس الهدف التوسع والهيمنة، إذ أن استعمال التطبيقات الصينية موجه للمواطنين الصينيين أما الأجانب فمن الصعب الحصول على حساب في هذه التطبيقات

مما يجعلها غير مرغوب فيها، ولعل الاستثناء هو تطبيق تيك توك TikTok لشركة ByteDance الصينية الذي تعدى عدد مستخدميه مليار شخص عبر العالم.

تجدر الإشارة إلى أن إدارة الرئيس "ترمب" سعت في 2020 إلى حظر كل من تطبيق WeChat الذي يستخدمه أكثر من 19 مليون شخص (ذوي أصول صينية) في الولايات المتحدة¹ وتطبيق TikTok مع محاولة نقل ملكيته إلى شركة أمريكية والذي يستخدمه ما يقارب 85 مليون أمريكي²، كل ذلك من أجل ضمان عدم وصول الصين إلى بيانات المواطنين الأمريكيين، لكن هذه الأوامر جُمدت في عهد إدارة الرئيس الحالي بايدن³ مع مواصلة التحقق من خلو التطبيقين من أية مخاطر أمنية.

المطلب الرابع: البيانات الضخمة (Big Data) نفط القرن الواحد والعشرين

يُنتج البشر والأجهزة كمّاً هائلاً من البيانات كل يوم، ويزداد حجم البيانات مع تزايد عدد المستخدمين والأجهزة خاصة مع تطور تقنيات أنترنت الأشياء IoT، فحجم البيانات التي أُنتجت، نُسخَت واستهلكت حسب موقع Statista ارتفع من 2 زيتابايت⁴ سنة 2010 إلى 64,2 زيتابايت سنة 2020، ومن المحتمل أن يصل إلى حدود 180 زيتابايت مع نهاية سنة 2025⁵، كانت حصة الصين سنة 2018 حوالي 7,6 زيتابايت، في مقابل 6,9 زيتابايت للولايات المتحدة، ومن المتوقع أن تُنتج الصين ما يقارب 49 زيتابايت سنة 2025 في مقابل 31 زيتابايت للولايات المتحدة⁶، هذا الكم الهائل من البيانات الضخمة BigData هو المورد الذي تتصارع الدولتان حول استغلاله، ذلك أن المعلومات التي تنتج عن تحليل البيانات الضخمة هي أساس تطوير الاقتصاد،

¹ Christopher Benitez, 27 Latest WeChat Statistics: Usage, Facts, And Trend, startupbonsai, June 16, 2022, URL: <https://bit.ly/3PTm4cO>.

² L. Ceci, TikTok: number of users in the United States 2020-2023, Statista, Jan 28, 2022, URL: <https://bit.ly/3BdmIhn>.

³ الأمر التنفيذي 14034 الصادر بتاريخ 09 جوان 2021 والذي يُلغي الأمرين التنفيذي رقم 13942 ورقم 13943 الخاصين بمعالجة التهديد الذي يشكله كل من تطبيق TikTok وتطبيق WeChat، واتخاذ خطوات إضافية لمعالجة حالة الطوارئ

الوطنية فيما يتعلق بتكنولوجيا المعلومات والاتصالات وسلسلة توريد الخدمات، على الرابط: <https://bit.ly/3J3cgLt>

⁴ 1 زيتابايت = 1 180 591 620 717 411 303 424 بايت، أي 1 متبوع بـ 24 رقم .

⁵ Statista Research Department, Amount of data created, consumed, and stored 2010-2025, Statista.com, May 23, 2022, URL: <https://bit.ly/3vf9YDc>.

⁶ Saheli Roy Choudhury, As information increasingly drives economies, China is set to overtake the US in race for data, cnbc.com, 2019, URL: <https://CNB.CX/3OXTCP>.

التجارة، البحث العلمي والصحة، كما تدخل في عمليات صناعة القرار في الميادين السياسية والعسكرية، فهي بحق نفط القرن الواحد والعشرين.

لكن من أجل الاستفادة من البيانات الضخمة يجب أولاً جمعها ثم تحليلها واستخلاص المعلومات المفيدة منها، لذلك فالصراع بين الولايات المتحدة والصين حول جمع وتخزين البيانات يتم من خلال التنافس في بناء مراكز البيانات **Data centers** أما الصراع حول قدرات تحليل البيانات الضخمة فيتم من خلال تطوير تقنيات الحوسبة الفائقة والذكاء الاصطناعي.

الفرع الأول، التنافس على مراكز البيانات **Data centers**

تحتل الصين المرتبة الرابعة عالمياً من حيث عدد مراكز البيانات حيث تمتلك 447 مركزاً للبيانات أي أقل من $\frac{1}{6}$ ما تملكه الولايات المتحدة (انظر شكل رقم 10)، بل أقل مما تملكه ميكروسوفت وأمازون وقوقل مجتمعة إذ تملك الشركات الثلاث أكثر من 600 مركز بيانات و50% من مراكز البيانات الضخمة (من حيث الحجم والسعة) في العالم، وتتفق الشركات الثلاث مليارات الدولارات سنوياً لتوسيع سعة التخزين لاستيعاب الطلب المتزايد على الخدمات السحابية¹، ومن المتوقع أن يصل الانفاق على البنية التحتية السحابية والتي تعتمد أساساً على مراكز البيانات حوالي 90 مليار دولار سنة 2022²، ومن بين أبرز الشركات الرائدة نذكر **HP**، **IBM**، **Dell** الأمريكية و **Alibaba**، **Huawei** الصينية، وفي محاولة من الصين لتحسين ترتيبها العالمي في مجال مراكز البيانات واستجابة للطلب الكبير على الخدمات السحابية وضماناً لاستمرار عمليات المراقبة الحكومية الشاملة وضعت خطة لمدة ثلاث سنوات 2021-2023 تشمل استثمار 216 مليار دولار على مدى ثلاث سنوات³ للدفع بتحسين سعة تخزين البيانات وشبكة الربط بينها وتطوير الحوسبة السحابية وكفاءة استهلاك الطاقة.

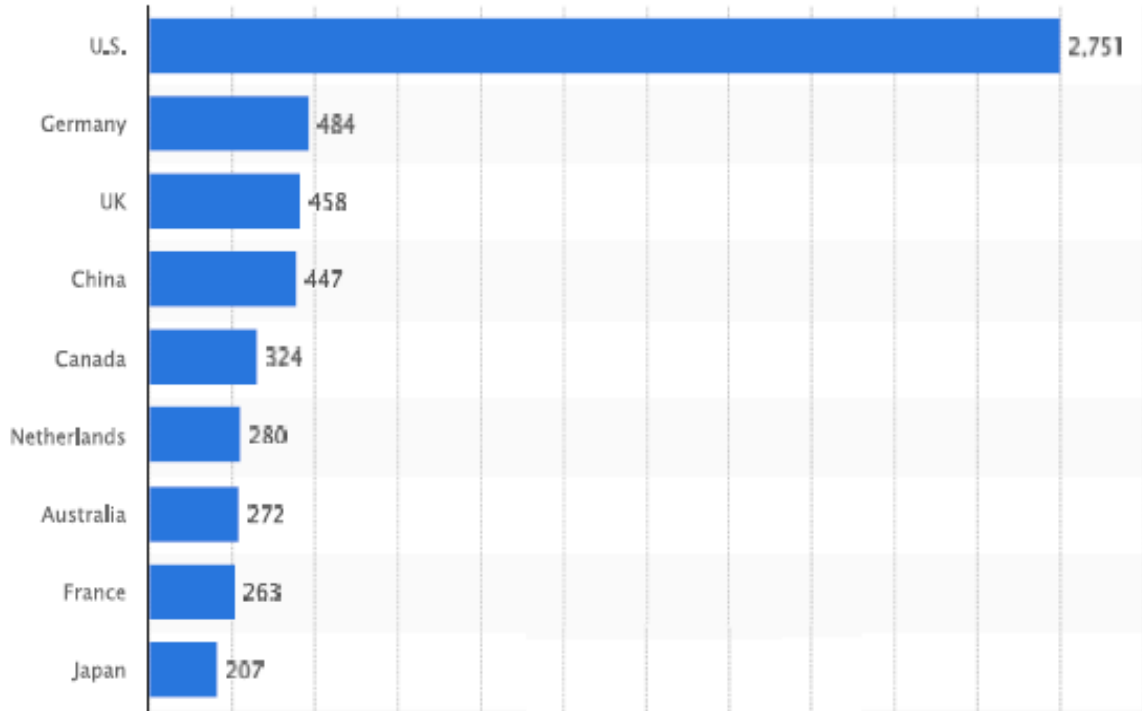
¹ السحابة **Cloud** أو الخدمات السحابية تشمل العديد من المكونات مثل الأجهزة والتخزين والمحاكاة الافتراضية، بالإضافة إلى الشبكة والموارد، ويتم دمج هذه المكونات في بنية تشكل نظام حوسبة سحابية كامل.

² Mark Haranas, **AWS, Google, Microsoft are taking over the Data Center market**, crn.com, January 27, 2021, URL: <https://bit.ly/3PUrLHJ>.

³ Arendse Huld, **“Eastern Data, Western Computing” – China’s Big Plan to Boost Data Center Computing Power Across Regions**, china-briefing.com, March 30, 2022, URL: <https://bit.ly/3zB0jJz>.

شكل رقم 10: ترتيب الدول حسب عدد مراكز البيانات لسنة 2022.

المصدر: Statista على الرابط: <https://bit.ly/3PDMXIB>



الفرع الثاني: الصراع في مجال الحوسبة الفائقة

تبقى البيانات الضخمة **Big Data** المخزنة على الأجهزة والخوادم بدون فائدة ما لم يتم تحليلها واستخلاص المعلومات للاستفادة منها، هذا الكم الهائل من البيانات لا يمكن تحليلها إلا عن طريق الأجهزة الفائقة وباستعمال التقنيات المبتكرة، لذلك فاستغلال **Big Data** يعتمد على مدى تطور التكنولوجيات المرتبطة بـ: الحوسبة الفائقة، الذكاء الاصطناعي.

يشد الصراع بين الولايات المتحدة الأمريكية والصين في مجال الحوسبة الفائقة، وهو المجال الذي تسعى من خلاله شركات البلدين إلى تصنيع كمبيوترات خارقة بسرعة معالجة عالية، ففي مجال الحوسبة الكمومية¹ **Quantum computing** وهو المجال الأحدث في عالم الكمبيوتر، تتفوق الولايات المتحدة على الصين في عدد براءات الاختراع، كما أن عدد الشركات وحجمها (Google، Microsoft، IBM) يُرجح كفة الولايات المتحدة، ففي 2019 أعلنت Google عن تحقيقها للتفوق الكمومي من خلال تصنيع جهاز كمبيوتر كمومي قادر على حل مشكلات يستغرق

¹ الحوسبة الكمومية هي مجموعة من التقنيات الحسابية تستخدم مبادئ ميكانيكا الكم مثل التشابك والتراكب والتداخل لمعالجة وتخزين ومعالجة كميات كبيرة من البيانات وإجراء الحسابات المعقدة بسرعات عالية جداً.

حلها على أقوى كمبيوتر موجود حالياً 10000 سنة، لم يتأخر الرد الصيني طويلاً، إذ أعلن الباحثون الصينيون في 2021 عن تصنيع جهازي كمبيوتر كمومي أقوى بكثير من جهاز Google.

كما تتفرد الصين في مجال الاتصالات الكمومية وتتقدم على الجميع منذ 2016 حيث استطاعت ربط قمرين صناعيين بمحطات أرضية باستعمال التشفير الكمومي، ويرجع هذا سبق إلى الدعم والتمويل الحكومي الضخم حيث تُصنف الصين الحوسبة الكمومية ضمن المجالات ذات الأولوية الاستراتيجية، فقد أنفقت الصين على تطوير الحوسبة الكمومية ما يقارب 10 مليار دولار منذ 2017 في مقابل 1,2 مليار دولار للولايات المتحدة¹، هذه الأخيرة تعتقد أن الصين قد تفوقت عليها كمومياً² مما يجعلها في حالة من الانكشاف الاستراتيجي الرقمي وتجعل من كل تقنيات التشفير المدنية والعسكرية مكشوفة للعدو، لذلك فهي تسعى من خلال أوامر الرئيس جو بايدن لتعزيز القدرات الكمومية الأمريكية³ في الدفاع والهجوم وتطوير تكنولوجيا الحوسبة الكمومية الوطنية.

بخلاف الحوسبة الكمومية التي لا تزال في مراحلها الأولى، يحتدم الصراع حول الحوسبة التقليدية من خلال إنشاء الكمبيوترات الخارقة، حسب تصنيف موقع Top500 المتخصص تمتلك الولايات المتحدة 5 من بين 10 كمبيوترات الأقوى في العالم، ويتصدر القائمة كمبيوتر Frontier والذي سيدخل الخدمة بكامل طاقته مع بداية 2023⁴، وتظهر فائدة هذه الكمبيوترات في سرعة تطوير لقاح لفيروس كورونا في المختبرات الأمريكية حيث استعملت الكمبيوترات الخارقة لإجراء محاكاة لكيفية تفاعل اللقاح مع الفيروس، من جهتها الصين تمتلك 173 كمبيوتر خارق مقابل 128 للولايات المتحدة في قائمة Top500 كما يُعتقد أنها تملك جهازين بنفس قدرة Frontier

¹ Sam Klebanov, Who's winning the quantum computing race? China and the U.S. are neck and neck, businessofbusiness.com, February 24, 2022, URL: <https://bit.ly/3S5zIB5>.

² Theresa Payton, America is Losing the Quantum Race with China, newsweek.com, May 12, 2022, URL: <https://bit.ly/3z8fLM1>.

³ من خلال الأمر التنفيذي 14073 لدعم المبادرة الكمومية الوطنية على الرابط: <https://bit.ly/3ozwiU9> بالإضافة إلى مذكرة الأمن القومي لتعزيز قيادة الولايات المتحدة في الحوسبة الكمومية وحماية أنظمة التشفير على الرابط: <https://bit.ly/3BqzCsF>.

⁴ يصنف موقع Top500 حسب ترتيب شهر جوان 2022 الكمبيوتر الخارق Frontier كأقوى كمبيوتر في العالم بقدرة حسابية تقارب 1.102 Exaflop/s، انظر: <https://bit.ly/3PUPMOQ>.

ولكنها لا تصرح بذلك بل تخطط لامتلاك 10 أجهزة خارقة بحلول 2025¹، وهذه السرية غير معتادة في هذا المجال إذ أن امتلاك كمبيوتر خارق من الأحداث التي تحتفل بها الدول وتدعو للفخر، ومن الممكن أن يكون استعمال هذه الأجهزة في مجالات عسكرية حساسة ككسر التشفير أو محاكاة التجارب النووية من الأسباب التي تدفع الصين لحجب تفوقها في مجال الكمبيوترات الخارقة.

الفرع الثالث: الصراع على الذكاء الاصطناعي AI

الذكاء الاصطناعي هو امتلاك الآلة القدرة على التفكير الذاتي وإيجاد حلول مبتكرة للمشكلات، وهو محور التطور الاقتصادي والأمن القومي حيث يصفه تقرير للجنة الأمن القومي الأمريكية للذكاء الاصطناعي NSCAI المقدم للكونغرس بأنه " حقل [علمي] الحقول [العلمية]... يحمل الأسرار التي تعيد تنظيم حياة العالم"².

قادت الولايات المتحدة أبحاث وتطبيقات الذكاء الاصطناعي إلى غاية 2015 أين برزت بوادر ثورة صينية في هذا المجال، وفي 2016 قدمت الشركة الصينية DeepMind آلة تغلبت على بطل العالم في لعبة GO والتي تعتبر أعقد من الشطرنج بآلاف المرات، تلى ذلك إعلان الرئيس الصيني شي أن الصين ستصبح رائدة في الذكاء الاصطناعي بحلول 2030 معتمداً على من سمّاهم الأبطال الوطنيين وهي شركات التكنولوجيا Alibaba للمدن الذكية، Baidu للقيادة الذاتية، iFlytek للتعرف على الصوت، SenseTime للتعرف على الوجوه، Tencent للتصوير الحاسوبي³، ساهم في إنجاح هذه الخطة العديد من الأسباب نذكر منها: الدعم الحكومي الكبير لشركات التكنولوجيا، السوق الصيني الضخم سواء تعلق الأمر بجمع وتخزين البيانات الضرورية لتطوير الذكاء الاصطناعي أو استهلاك منتجات الشركات، كما أنتجت الصين ضعف ما أنتجته الولايات المتحدة من الأوراق البحثية في مجالات الذكاء الاصطناعي وتعلم الآلة، وبلغ عدد خريجي الجامعات الصينية في علوم الكمبيوتر ثلاثة أضعاف نظيره في الولايات المتحدة، فالصين تسير بخطى ثابتة نحو التفوق في مجال الذكاء الاصطناعي.

¹ Richard Waters, **US rushes to catch up with China in supercomputer race**, Financial times.com, May 18 2022, URL: <https://on.ft.com/3vIOUuF>.

² **National Security Commission on Artificial Intelligence**, Final Report, 2021, URL: <https://bit.ly/3JctHsX>.

³ Smith Aaron , **How China surpassed the U.S. in the race for AI supremacy**, uscgpi.com, Jan 6, 2022, URL: <https://bit.ly/3cIyuWS>.

بدأت التحذيرات مبكراً في الولايات المتحدة من التطور الصيني السريع، ففي 2017 علق إيريك شميدت المدير التنفيذي السابق لـ Google على جهود الصين في الذكاء الاصطناعي بأنه: " بحلول 2020 سيلتحقون بنا، وفي 2025 سيصبحون أفضل منا، وفي 2030 سيهيمنون على الصناعة"¹، استجابت إدارة الرئيس ترمب لهذه التحذيرات من خلال زيادة التمويل لتطوير الذكاء الاصطناعي ورصدت 2 مليار دولار، كما شكلت إدارة الرئيس بايدن فرقة عمل أبحاث الذكاء الاصطناعي، لكن المشكلة على الجانب الأمريكي تتعلق بأخلاقيات تطوير الذكاء الاصطناعي والقيود المفروضة على الشركات في الوصول إلى البيانات الضخمة، وهذا ما دفع برئيس البرمجيات السابق في البنتاغون للاستقالة والتصريح بأن الصين قد تفوقت فعلاً على الولايات المتحدة وأنه " ليس لدينا فرصة لمنافسة الصين في غضون 15 إلى 20 عاماً، إنها بالفعل صفقة منتهية"².

هذه النظرة التشاؤمية برزت في تقرير لجنة الذكاء الاصطناعي NSCAI والذي أكد أن الصين عازمة على قيادة الذكاء الاصطناعي، لذلك قدم التقرير في جزئه الأول مخاطر فقدان الريادة على الاقتصاد والأمن القومي الأمريكي، وركز في جزئه الثاني على تقديم اقتراحات للفوز بسباق الذكاء الاصطناعي أبرزها زيادة الاستثمار، تهمين الرأسمال البشري والتشجيع على الابتكار، بناء التحالفات الدولية و تضمين تطوير الذكاء الاصطناعي قيم الديمقراطية وحقوق الإنسان، وهذا ما يُفسر الترويج لفكرة صراع الذكاء الاصطناعي الديمقراطي ضد الذكاء الاصطناعي الاستبدادي.

أشار الرئيس الروسي "بوتين" إلى أن "من يقود الذكاء الاصطناعي سيطر على العالم"³، لذلك فالولايات المتحدة الأمريكية تخوض معركة الذكاء الاصطناعي معتمدة على شركاتها القوية ومناخها البحثي الجاذب للخبراء في مواجهة الصين التي تملك العزيمة والموارد والدعم الحكومي اللامحدود.

1 Patrick Tucker, **China Will Surpass US in AI Around 2025, Says Google's Eric Schmidt**, defenseone.com, Nov 1, 2017, URL: <https://bit.ly/3zbtTUB>.

2 Monique Beals , **Former Pentagon official says China has won artificial intelligence battle**, theHill.com, Nov 10, 2021, URL: <https://bit.ly/3vm6BKH>.

3 , **Whoever leads in AI will rule the world': Putin to Russian children on Knowledge Day**, RT.com, Sep 1, 2017, URL: <https://bit.ly/3zCU7Rk>.

المبحث الثالث: تداعيات الصراع الأمريكي-الصيني على العلاقات والتحالفات الدولية.

يُلخص الدبلوماسي الأمريكي هنري كيسنجر تطور العلاقة بين الولايات المتحدة والصين بأنها انتقلت من الشراكة إلى التعاون، إلى عدم اليقين، إلى المواجهة القريبة أو الفعلية، كما يعتبر الفضاء السيبراني من أكبر وأشد مجالات التنافس والصراع التي أثرت على العلاقات الثنائية بين البلدين، إن فهم ديناميكية العلاقات الثنائية بين البلدين وتداعيات الصراع التكنولوجي في الفضاء السيبراني على التحالفات الأمنية والتكنولوجية الجديدة وتأثيرها على النظام الدولي وتوازنات القوى يتطلب فهم المشكلات الأساسية ورؤية كل طرف تجاه تلك القضايا.

المطلب الأول: تداعيات الصراع التكنولوجي على العلاقات الثنائية بين الو.م.أ والصين

غالباً ما تميزت العلاقة بين الولايات المتحدة والصين بالصراع والتحدي والشك الاستراتيجي، ويمكن تقسيمها إلى مرحلتين بارزتين، المرحلة الأولى منذ بداية العلاقات الرسمية لغاية 2015 وتتميز بحالة من الريبة الجيوبوليتيكية، والمرحلة الثانية بعد 2015 إلى غاية يومنا هذا وتتميز بالمنافسة الاستراتيجية الشاملة.

الفرع الأول: مرحلة 1979-2015: الريبة الجيوبوليتيكية

منذ الاعتراف الدبلوماسي الأمريكي بمبدأ الصين الواحدة في 1979 لم تتوان الولايات المتحدة عن الضغط على الصين في قضايا تعتبرها الصين حساسة كقضية تايوان وقضايا حقوق الإنسان، ومع بداية القرن الحالي، وقع الرئيس الأمريكي **كلينتون** على قانون العلاقات بين الولايات المتحدة الأمريكية والصين لعام 2000 ما مهد الطريق للصين للانضمام إلى منظمة التجارة العالمية في 2001، في 2005 بدأت الولايات المتحدة حواراً استراتيجياً مع الصين في اعتراف منها بأن الصين أصبحت قوة صاعدة، ومحاولة منها لدمجها في النظام الدولي الذي تهيمن عليه والاستفادة من نفوذها لدى الدول المعارضة (روسيا، إيران، كوريا الشمالية) للسياسات الأمريكية لجذبها ودمجها في النظام الدولي. تضاعف التبادل التجاري بين البلدين لتصبح الصين في 2006 ثاني أكبر شريك اقتصادي للولايات المتحدة بعد كندا¹، حيث تدفقت الاستثمارات

¹ الجدول الزمني للعلاقات الأمريكية-الصينية منذ تأسيس جمهورية الصين الشعبية في 1949 على موقع مجلس العلاقات الخارجية CFR على الرابط: <https://bit.ly/47GmI7o>.

الأجنبية وخاصة الأمريكية إلى الصين، وأنشأت العديد من شركات التكنولوجيا الأمريكية مصانع على التراب الصيني مستفيدة من اليد العاملة الرخيصة والسوق الكبيرة الواعدة، هذا ما شكل علاقات تكنولوجية عميقة، وسلاسل توريد معقدة للمكونات التكنولوجية تحت وطأة العولمة الاقتصادية، هذه الحركية الاقتصادية الضخمة مكنت الصين من أن تصبح ثاني أكبر اقتصاد في العالم سنة 2010¹.

وجدير بالذكر أن الخلافات بين الولايات المتحدة والصين حول قضايا الفضاء السيبراني لم تتوقف أبداً عن زعزعة الثقة بين البلدين وتدهور العلاقات بينهما، فالولايات المتحدة تضع قضايا الأمن السيبراني على رأس أولويات الحكومة، فهي تشتكي من التجسس الصيني الواسع لأغراض اقتصادية وفي بعض الأحيان التجسس على أجهزة الحكومة والجيش مما يُعرض الأمن القومي الأمريكي للخطر، هذا إضافة إلى القوانين التي تتعارض مع حرية الأنترنت والتي تطبقها الصين ضد الشركات الأمريكية لدفعها إلى مغادرة السوق الصينية، وعلى العكس من ذلك ترى الصين أن قضايا الفضاء السيبراني ما هي إلا جزء من صراعات جيوبوليتيكية أكبر، فالصين تتهم الولايات المتحدة بالهيمنة على الأنترنت والتدخل في الشؤون الداخلية للدول من خلال دعم تكنولوجيا التحايل على الرقابة التي تفرضها الصين داخل حدودها.

سعت الصين في 2009 للتخفيف من حدة الصراع بين البلدين حول الفضاء السيبراني من خلال اقتراحها لمفاوضات غير رسمية بين متخصصين من البلدين، ورغم توسع المشاركين في المفاوضات إلى مسؤولين حكوميين من البلدين إلا أنه لم يتم التوصل إلى نتائج ذات أهمية، بل على العكس من ذلك فإن اكتشاف عملية تجسس على شركة قوقل (عملية أورورا **Aurora**) دفعت الشركة إلى إقناع الحكومة الأمريكية بضرورة جعل الحادثة قضية دولية مع الصين، حيث إنتقدت وزيرة الخارجية هيلاري كلينتون رسمياً سلوك الصين في الفضاء السيبراني وطالبت بتقديم تفسيرات للحادثة.

هذه الانتقادات الأمريكية الرسمية والتي تزامنت مع الاستراتيجية الجديدة لإعادة التوازن لمنطقة آسيا والتي تراها القيادة الصينية الجديدة (الرئيس شي سنة 2012) بأنها محاولة لاحتواء الصين زادت من التوترات الجيوبوليتيكية عموماً والنزاع حول التجسس السيبراني لأغراض اقتصادية خصوصاً، إذ أن تقريراً لشركة **مانديانت Mandiant** سنة 2013 والذي ادعا وجود

¹ نفس المرجع.

أدلة على تورط جيش التحرير الشعبي الصيني PLA في عمليات قرصنة دفع بالمسؤولين الأمريكيين إلى اتهام الصين مباشرة وبشكل رسمي بالتجسس، وجعل القضية على رأس مواضيع قمة الرئيسين أوباما وشي التي عقدت في ساني لاندز 2013¹، والتي حاولت فيها الولايات المتحدة حشد تأييد عالمي للضغط على الصين لوقف عمليات التجسس، لكن تسريبات سنودن التي كشفت تجسس وكالة الأمن القومي NSA على الجميع بما فيهم الصين عرقل تلك الجهود بل جعل من الصينيين يسخرون منها حيث يعلق أحدهم بأن "الولايات المتحدة التي كانت تلعب دور الضحية البريئة للهجمات السيبرانية لفترة طويلة، تبين أنها هي الشرير الأكبر في عصرنا"²، رغم ذلك تواصلت المفاوضات المباشرة بين الطرفين مع تقدم طفيف، إلا أن إدانة 5 ضباط صينيين في قضايا تجسس سيبراني سنة 2014 دفع بالجانب الصيني إلى الانسحاب من المفاوضات والتي توقفت نهائياً حتى العام 2015.

الفرع الثاني: 2015- يومنا هذا: المنافسة الاستراتيجية الشاملة

في منتصف 2015 وصف العديد من المحللين الأمريكيين التدهور السريع للعلاقات الأمريكية-الصينية بأنها تعيش "نقطة تحول"³ لتصبح منافسة استراتيجية شاملة، كما دعا مسؤولون حكوميون بإعادة النظر في الاستراتيجية الأمريكية الشاملة تجاه الصين لموازنة صعودها السريع، وكان من نتيجة هذه الآراء تلميحات بإمكانية فرض عقوبات اقتصادية على الصين وهذا ما يراه البعض من بين أسباب عقد اتفاق بين الرئيسين "أوباما" و"شي" في سبتمبر 2015 حول منع التجسس السيبراني لأغراض اقتصادية والتعاون في مجال الجريمة السيبرانية، خفف هذا الاتفاق من حدة التوترات بين البلدين حتى إن أخبار التجسس والاختراقات السيبرانية أصبحت لصيقة بروسيا (التدخل في الانتخابات، التجسس وغيرها).

لكن مع وصول الرئيس ترمب إلى الحكم و إصدار استراتيجية الأمن القومي الجديدة لسنة 2017 تم إعادة تقييم الصين على أنها "منافس استراتيجي رئيسي" للولايات المتحدة، فبعد عقدين

¹ Scott W. Harold, Martin C. Libicki, and Astrid Stuth Cevallos, **Getting to Yes with China in Cyberspace**, Santa Monica, CA: RAND Corporation, 2016, URL : <https://bit.ly/3BwDpEF>.

² Ibid.

³ انظر مقال لـ David M. Lampton بعنوان: " نقطة التحول - هل يمكننا تضخيم ما لدينا من قواسم مشتركة؟" على الرابط: <https://bit.ly/3S8o6Ih>، ومقال لـ David Shambaugh بعنوان: " في تحول جوهري، تنخرط الصين والولايات المتحدة في منافسة شاملة" على الرابط: <https://bit.ly/3zHHmVM>.

من الريبة الجيوبوليتيكية تم التأكيد على أن الصين قوة تعديلية تسعى لتقويض هيمنة الولايات المتحدة في المحيطين الهادي والهندي وإعادة ترتيب المنطقة لصالحها¹، وبدأت حملة العقوبات والحظر فيما عُرف بـ "الحرب التجارية" ابتداءً من مارس 2018 وكان في قلب هذه الحرب "حرب تكنولوجيا" شنتها إدارة ترمب على شركات التكنولوجيا الصينية، بدأت الحملة بعمليات تضيق ثم حظر كلي لمنتجات شركة هواوي الصينية في الولايات المتحدة ثم الضغط على الدول الحليفة باتخاذ حظر مماثل خاصة ما يتعلق بتقنيات الجيل الخامس الصينية بحجة التجسس وتهديد الأمن القومي، وتحولت العلاقة بين البلدين إلى صراع حاد حول التفوق التكنولوجي.

في العام 2020 قامت وزارة التجارة الأمريكية بإضافة العديد من شركات التكنولوجيا الصينية على القائمة السوداء والتي يُحظر التعامل معها في محاولة لكبح التطور التكنولوجي الصيني السريع خاصة في مجالات تقنيات الجيل الخامس وأشباه الموصلات والذكاء الاصطناعي، ورغم الآمال الصينية في تغيير الرؤية الأمريكية مع الإدارة الجديدة في 2021 إلا أن إدارة الرئيس بايدن واصلت معظم سياسات الرئيس "ترمب" الحمائية، بل تم توسيع دائرة الحظر خاصة منع استثمارات شركات التكنولوجيا الصينية التي لها علاقة بالجيش.

وفي تطور لافت توحدت رؤى كل من الجمهوريين والديمقراطيين تجاه الصين² وتشكل لدى الأمريكيين ما يسمى "القومية التكنولوجية الأمريكية" والتي يُعد الفوز بالحرب التكنولوجية والحفاظ على ريادة الولايات المتحدة في الفضاء السيبراني من أهم مخرجاتها، كما أن النقاش في الولايات المتحدة يدور حول الطرق المثلى لتطبيق "استراتيجية فك الارتباط التكنولوجي"³ والتي تتوزع عبر مجموعة من الإجراءات الدفاعية والتي تتمثل في الأدوات التقييدية (ضوابط التصدير، قيود الاستثمار، العقوبات والحظر... إلخ) وتهدف إلى إحباط واحتواء التكنولوجيا الصينية، والإجراءات الهجومية والتي تتمثل في توسيع الاستثمار في البحث والتطوير.

أصبحت الحرب التكنولوجية هي السمة البارزة في العلاقات الثنائية بين الولايات المتحدة الأمريكية والصين، والتي تزداد تدهوراً مع زيادة حدة الإجراءات العقابية والإجراءات المضادة التي

¹ Trump, Donald J, **National security strategy of the United States of America**, Executive Office of The President Washington DC Washington United States, 2017, URL: <https://bit.ly/3Bx13kh>.

² Haiyong Sun, "US-China tech war: Impacts and prospects", **China Quarterly of International Strategic Studies**, Vol 5, N°02, 2019, pp 197-212.

³ للاطلاع على المزيد حول "استراتيجية فك الارتباط" انظر المبحث الثاني من الفصل الثالث من الدراسة.

تتخذها كلتا الدولتين، فالولايات المتحدة تُفضل الصين المقلدة على الصين المبتكرة، في حين تسعى الصين لـ"التجديد العظيم للأمة الصينية"، وبين هذا وذاك تغيب الثقة بين الطرفين ويزداد الجهل بنوايا الآخر ويُعزز من ذلك خصائص الفضاء السيبراني الفريدة ويزيد من خطره القضايا الجيوبوليتيكية الأخرى كقضية تايوان والحرب الروسية-الأوكرانية، لذلك يُحذر المفكرون وعلى رأسهم هنري كيسنجر¹ الذي يرى أن غياب الحوار بين الولايات المتحدة والصين ورؤية كل منهما للعلاقة الثنائية على أنها "منافسة استراتيجية شاملة" يزيد من خطر وقوع حوادث مدفوعة بتقنيات الذكاء الاصطناعي قد تشمل صراعاً عسكرياً على نطاق عالمي.

المطلب الثاني: تداعيات الصراع التكنولوجي على التحالفات الاستراتيجية الجديدة

طالما كانت التحالفات والشراكات ميزة جوهرية في السياسة الخارجية الأمريكية، فالولايات المتحدة تمتلك شبكة هائلة من الأطر والتحالفات والشراكات تتنوع من حيث الأهداف بين الأمني والاقتصادي، وتمتد من حيث الجغرافيا لتشمل الكرة الأرضية مياها وياستها، وحيث إن قوة وفعالية هذه التحالفات والأطر أو الحاجة لخلق تحالفات وأطر جديدة يرتبط ارتباطاً وثيقاً بالرؤية الأمريكية لمصادر التهديد فإن الصعود والتوسع الصيني العالمي في أبعاده الاقتصادية، السياسية، العسكرية وخاصة التكنولوجية جعلت منه التهديد الرئيس للهيمنة والريادة الأمريكية، لذلك فالإدارة الأمريكية تدفع بسياسة "ردع الصين" إلى تصدر قائمة الأولويات، وتسعى لاستغلال التحالفات وأطر الشراكة كأدوات لاحتواء "التهديد الصيني".

وفي خضم سعي الولايات المتحدة لتفعيل التحالفات والأطر ضد الصين تبرز مشكلتان أساسيتان، أولاً، التشابك الاقتصادي والتعقيد الكبير في العلاقات بين الصين والدول الحليفة والشريكة للولايات المتحدة، وهذا ما يجعل إختلاف وجهات النظر كبيراً ويصعب الوصول إلى اتفاق موحد حول سبل وسياسات المواجهة، فكل طرف (دولة) له حسابات الربح والخسارة الخاصة به، كما أن شعارات الديمقراطية وحقوق الإنسان لم تعد لها ذلك الوزن الكبير في علاقات الدول بالولايات المتحدة خاصة أن، ثانياً، سياسات الرئيس ترمب الحمائية "أمريكا أولاً" جعلت الكثير من دول العالم تشكك في مدى جدوى التحالفات والشراكات مع الولايات المتحدة ومدى التزامها

¹ Henry A. Kissinger, Eric Schmidt, Daniel Huttenlocher, **The Age of AI and Our Humain Future**, John Murray Press, London, 2021.

بقيادة العالم نحو الأمن والرخاء، وما رسخ هذه القناعة هو الطريقة الانعزالية والانفرادية في تعامل الولايات المتحدة الأمريكية مع "جائحة كورونا".

وعليه فإن الإدارة الأمريكية الجديدة بقيادة الرئيس بايدن تبذل جهوداً جبارة لإعادة بناء الثقة لدى الحلفاء والشركاء من خلال الانخراط في القضايا والأحداث الإقليمية سواء تعلق الأمر بالدائرة الأوراسية والدعم العسكري الكبير لأوكرانيا والتنسيق مع حلفائها الأوروبيين لفرض العقوبات على روسيا، لإثبات أن الولايات المتحدة لا تزال تقود العالم وتهتم لقضايا حلفائها وشركائها الأوروبيين، وكتمهيد نحو توسيع مهام حلف شمال الأطلسي NATO نحو دائرة المحيطين الهندي والهادي أو ما يعرف بمنطقة "الاندو-باسيفيك" حيث تُعزز الولايات المتحدة من استراتيجيتها لاحتواء الصين، والتي أسس لها الرئيس "أوباما" فيما عُرف باستراتيجية "إعادة التوازن في آسيا".

ومن أجل ضمان الفاعلية القصوى للتحالفات وتجنب الاختلافات بين الدول وتباين أو في بعض الأحيان تعارض المصالح والأولويات لكل دولة، تعمل الولايات المتحدة على إعادة إحياء وتفعيل التحالفات والأطر مع دول المنطقة مع وضع الأولويات التكنولوجية على رأس قائمة الأهداف لأسباب أمنية واقتصادية، بالإضافة إلى تشكيل تحالفات وأطر جديدة تضم عدداً محدوداً من الدول التي تتشارك نفس الرؤى في قضايا محددة، ويمكن ملاحظة هذا النمط الجديد التي تتبعه الولايات المتحدة في بناء التحالفات في النماذج التالية:

أولاً، المجموعة الرباعية QUAD: بدأت مجموعة الرباعية في 2004 كشراكة بين الولايات المتحدة، اليابان، أستراليا والهند لتقديم المساعدة الإنسانية في حالات الكوارث، أُعيد تسميتها بالحوار الأمني الرباعي في 2007 وتوسعت دائرة الاهتمامات إلى التنسيق الأمني بين الدول الأربعة، كما أخذت طابعاً رسمياً لكنها ظلت خاملة لعقد من الزمن، بسبب تكثف وتزايد العلاقات الاقتصادية بين أعضاء المجموعة خاصة أستراليا والصين، أُعيد إحياء المجموعة في 2017 واعتبرتها الولايات المتحدة مفتاح التوازن مع الصين في منطقة المحيطين الهندي والهادي، وتم رفعها إلى مستوى القمة في 2021 حيث عُقد أول لقاء رسمي لقادة الدول الأربعة والذين أكدوا على النهج الأساسي للمجموعة وهو الحفاظ على منطقة المحيطين الهندي والهادي حرة ومفتوحة ورفض أي إكراه عسكري أو اقتصادي أو تكنولوجي في إشارة للصين، وبرز التحدي التكنولوجي كأحد أهم محاور تفاهمات الرباعية في قمة ماي 2022 التي أكدت على أهمية التنسيق في

مجالات الأمن السيبراني وتكنولوجيات الجيل الخامس والذكاء الاصطناعي¹، في المقابل، ترى الصين أن تحالف الرباعية محاولة لتشكيل حلف ناتو آسيوي موجه ضدها ويسعى لاحتواء الصين في منطقة المحيطين الهادي والهندي.

ثانياً، تحالف أوكوس AUKUS: هو التحالف الأمني العسكري الأحدث الذي قدمت فيه الولايات المتحدة، بريطانيا وأستراليا نموذج التحالفات الأمنية المحدودة الجديد، وقد جاء الإعلان عن التحالف في سبتمبر 2021 على خلفية إلغاء أستراليا لصفقة غواصات مع فرنسا لصالح غواصات نووية من بريطانيا والولايات المتحدة، ذلك أن الولايات المتحدة تدفع نحو تطوير كبير لقدرات البحرية الأسترالية من خلال مشاركة للتكنولوجيا العسكرية الفائقة (خاصة النووية حيث الدولة الوحيدة التي تشارك معها هذه التقنيات هي بريطانيا) لمواجهة الصين في منطقة المحيطين الهادي والهندي، وقد تم تحديد الأولويات التكنولوجية للحلف في التفوق التكنولوجي على الصين في مجالات الذكاء الاصطناعي والحوسبة الكمومية والأمن السيبراني²، والتي تُشكل محور القدرات الاستخباراتية المستقبلية، ورغم أن تحالف العيون الخمس Five Eyes هو التحالف الأقدم في مجال الاستخبارات إلا أن الولايات المتحدة تريد تضيق مجال تشارك التقنيات الاستخباراتية الحديثة وحصره على بريطانيا وأستراليا باعتبارهما الدولتين الأكثر التزاماً بالتوجهات والرؤية الأمريكية والأكثر فعالية خاصة في حربي أفغانستان والعراق.

ثالثاً، التحالفات الاقتصادية والتكنولوجية: لمواجهة واحتواء القوة الاقتصادية الصينية وتقويض هيمنتها خاصة في آسيا سعت الولايات المتحدة إلى تشكيل أطر وشراكات ذات طبيعة اقتصادية وتجارية مع دول المنطقة، فبعد انسحاب إدارة ترمب من مبادرة الشراكة عبر المحيط الهادي TPP تحاول إدارة بايدن إعادة تأكيد أهمية منطقة المحيطين الهادي والهندي بالنسبة للولايات المتحدة وتقديم بديل قوي لقيادة الاقتصاد في المنطقة، لذلك دعا الرئيس بايدن في ماي 2022 إلى تشكيل الإطار الاقتصادي للازدهار في المحيطين الهادي والهندي IPEF والذي يضم 14 دولة كما صرح بأن هدف المبادرة هو "كتابة القواعد الجديدة لاقتصاد القرن 21"³، ورغم تنوع المجالات الاقتصادية -بما فيها المجال التكنولوجي- التي تشملها المبادرة إلا أن غياب الحوافز

¹ The White House, Quad Joint Leaders' Statement, whitehouse.gov, May 24, 2022, URL: <https://bit.ly/3Qq65U8>.

² The White House, AUKUS Leaders' Level Statement, April 05, 2022, URL: <https://bit.ly/3dc40wC>

³ The White House, Remarks by President Biden at Indo-Pacific Economic Framework For Prosperity Launch Event, May 23, 2022, URL: <https://bit.ly/3p36qQS>.

والتي من أهمها إعادة تقييم التعريفات الجمركية دعا المحليين إلى التقليل من فعاليتها في مواجهة الأطر والشركات الصينية في المنطقة، حيث إن معظم الدول لا تريد الدخول في مواجهة اقتصادية مباشرة مع الصين.

يُعلق روبرت د. أتكينسون في مجلة **Foreign Affairs** بأن الولايات المتحدة لم تعد قادرة على شراء حلفاء جيوبوليتيكيين في المنطقة¹، كما دعا آخرون إلى تطوير وتكثيف التعاون إلى مستوى **مجلس التجارة والتكنولوجيا TTC** بين الولايات المتحدة والاتحاد الأوروبي وهو إطار تعاوني يهدف إلى الحفاظ على قيادة الولايات المتحدة وحلفائها للفضاء السيبراني وجعله آمناً وموثوقاً، والتشارك في وضع معايير عالمية للتكنولوجيات الناشئة وغيرها من التكنولوجيات الحيوية التي تستند إلى القيم الديمقراطية في مواجهة الاستبداد الرقمي².

في المقابل، لا تبدو الصين مستعجلة لقيادة العالم، فهي تضع أهداف التفوق ضمن الأهداف متوسطة وبعيدة المدى، لذلك فهي تركز على التنافس في المجال الاقتصادي التكنولوجي بدل الأمني العسكري، كما أنها تنتقد بشدة التحالفات الأمنية في آسيا وتعتبر أن محصلتها الصفرية تدل على عقلية الحرب الباردة التي لا يزال يفكر بها قادة الولايات المتحدة³، فباستثناء بعض اتفاقيات التعاون العسكري مع روسيا، كوريا الشمالية، باكستان، إيران والتي تتسجم مع مبدأ "عدو عدوي صديقي" والتي تُشكل جبهة مناهضة لقيادة الولايات المتحدة وحلفائها لا تقيم الصين أية تحالفات أمنية عسكرية.

على العكس من ذلك، فالصين تنتهج سياسة "الشراكة الاستراتيجية" حيث صرح الرئيس الصيني شي في 2014 أن بلاده تحتاج إلى تكوين صداقات أكثر عبر "بناء شبكة عالمية من الشركاء"⁴، وذلك عبر التشبيك الكثيف للشراكة الاقتصادية والتكنولوجية والتي قد تتطور إلى شراكة أمنية من خلال التكنولوجيا ذات الاستخدام المزدوج، أو حتى تصدير التكنولوجيا العسكرية، فالصين من خلال هذه الشراكات تطمح لحشد الدعم الدبلوماسي أو عدم معارضة وانتقاد الموقف

¹Robert D. Atkinson, **Biden's Indo-Pacific Economic Framework Is a Paradigm Shift**, foreignpolicy.com, July 1, 2022, URL: <https://bit.ly/3vQiXuO>.

² **The White House**, FACT SHEET: U.S.-EU Trade and Technology Council Establishes Economic and Technology Policies & Initiatives, May 16, 2022, URL: <https://bit.ly/3SAIKCa>.

³ Adam PLiff, "China and the US alliance system", **The China Quarterly**, vol 233, 2018, pp137-165.

⁴ CAO DESHENG, **Xi calls for expansion of global partnerships**, Chinadaily, Sept 9, 2019, URL: <https://bit.ly/3domQRq>.

الصيني تجاه قضاياها الجوهريّة (مثل: تايوان، بحر الصين الجنوبي ... إلخ) والقضايا العالمية كالحوكمة العالمية أو حوكمة الفضاء السيبراني وغيرها.

تنشط الصين من خلال الأطر والشراكات الثنائية والإقليمية والعالمية (دول الحزام والطريق، منظمة شنغاي للتعاون SCO، منظمة دول البريكس BRICS) لتعزيز رؤيتها للقضايا الإقليمية والعالمية مستغلة ثقلها الاقتصادي والتكنولوجي، حيث تطرق خطاب الرئيس الصيني "شي" في الاجتماع 14 لقادة دول البريكس (ماي 2022) الذي حمل عنوان "إقامة علاقات الشراكة عالية الجودة وإطلاق مسيرة جديدة لتعاون البريكس" إلى أربعة محاور أهمها المحور الثالث الذي يتعلق بالتمسك بالريادة والابتكار لتعزيز التعاون، وصرح الرئيس "شي" بأنه "من يغتتم الفرص الجديدة للتنمية الاقتصادية مثل البيانات الضخمة والذكاء الاصطناعي يواكب تيار العصر، ومن يحاول التشويش.... باستغلال الوسائل في مجال التكنولوجيا بما فيها الاحتكار والحصار ووضع الحواجز من أجل الحفاظ على هيمنته سيجد طريقه مسدوداً"¹، وهذا ما يؤكد منهج الصين الاقتصادي- التكنولوجي لحشد شركائها لمواجهة هيمنة الولايات المتحدة في الفضاء السيبراني.

المطلب الثالث: تداعيات الصراع التكنولوجي على توازن القوى والنظام الدولي

يشهد العقد الثاني من القرن الحالي عودة قوية للمنافسة الاستراتيجية بين القوى العظمى خاصة بين الولايات المتحدة والصين، بعد أن عرف العالم نظاماً أحادي القطب في العقود الثلاثة التي تلت نهاية الحرب الباردة، وتزداد المنافسة حدة على خلفية التراجع المتزايد لدور ومكانة الولايات المتحدة، والصعود الصيني السريع في مختلف المجالات الاقتصادية والسياسية والعسكرية، مما جعلها التهديد الأول للهيمنة الأمريكية.

ففي عالم تحكمه الفوضى تسعى الدولتان لامتلاك ومراكمة وحتى استعمال القوة -إذا كان ذلك ممكناً- في إدارة علاقاتها الدولية، ويُعزز ذلك الاختلال في موازين القوى العالمية من جهة، والتحول في مفاهيم القوة حيث أصبحت التكنولوجيا أو المجال السيبراني المحرك الرئيس لزيادة قوة الدولة الاقتصادية والعسكرية من جهة أخرى، يُدرك قادة البلدين العلاقة الوثيقة بين الابتكار التكنولوجي وقوة الدولة الاقتصادية والعسكرية، فالتقنيات الناشئة تقع في محور ديناميكيات التفاعلات السياسية والاقتصادية العالمية، لذلك فكل من الولايات المتحدة والصين تعمل على

¹ كلمة الرئيس الصيني شي جينبينغ في الاجتماع 14 لقادة دول البريكس، ماي 2022، على الرابط:

<https://bit.ly/3PfMnJu>

مراكمة قوتيهما من خلال الابتكار التكنولوجي المستمر لاقتناع صناع القرار في البلدين أنه يمكن لأي إختراق (أو تفوق) في المجالات التكنولوجية الحيوية أن يؤدي لتغيير كبير في التوازن المستقبلي للقوة الاقتصادية والعسكرية وبالتالي التأثير على طبيعة النظام الدولي.

الفرع الأول: التكنولوجيا كمحرك لتغيير توازن القوى الاقتصادي

منذ أن تفوقت الولايات المتحدة على بريطانيا في 1870 وأصبحت أكبر اقتصاد في العالم لم تواجه تحدياً ومنافسة مثل ما تشهده اليوم أمام الصعود الاقتصادي الصيني، وليس خافياً أن الناتج المحلي الإجمالي **GDP** يعكس قوة الدولة الاقتصادية ويسمح لها بممارسة أكبر قدر من التأثير على الساحة الدولية، تُشير بعض المؤشرات إلى أن الصين قد تفوقت بالفعل على الولايات المتحدة لتصبح القائد الأول للاقتصاد منذ الأزمة المالية سنة 2008¹، كما أن إحصائيات كل من البنك الدولي وصندوق النقد الدولي تُشير إلى أن الصين قد تساوت مع الولايات المتحدة في الناتج المحلي الإجمالي في 2016 ومن المحتمل أن تتفوق عليها بفارق كبير في 2025 (انظر الشكل رقم 11).

هذا التحول الدراماتيكي في ميزان القوى الاقتصادي لصالح الصين يرجع في الأساس لسياسة الرقمنة المكثفة للاقتصاد الصيني، كما أن قطاع التكنولوجيا يُعتبر أولوية لدى القادة الصينيين حيث يظهر ذلك من خلال خطة "صنع في الصين 2025" وتصريحات المسؤولين الصينيين بأن الصين ستصبح رائدة في مجال التكنولوجيا بحلول سنة 2030، ويؤكد هذا النهج إحصائيات مكتب معلومات مجلس الدولة الصيني **SCIO** حول مساهمة قطاع التكنولوجيا في الاقتصاد الصيني، حيث بلغ حجم الاقتصاد الرقمي الصيني في 2020 أكثر من 6 ترليون دولار أي بنسبة 38,6% من الناتج المحلي الإجمالي الوطني²، ويقود هذا النمو السريع عمالة التكنولوجيا في الصين.

يقول زينون كابرون **Zennon Kapron** مؤسس شركة **Kapronasia** لأبحاث الصناعة المالية في شنغهاي: "إذا أصبحت البلاد مكتفية ذاتياً من حيث التكنولوجيا ومن ثم أصبحت قادرة على بيع وتصدير تلك المنتجات والخدمات التي تعتمد على التكنولوجيا، فسيكون ذلك بمثابة قفزة

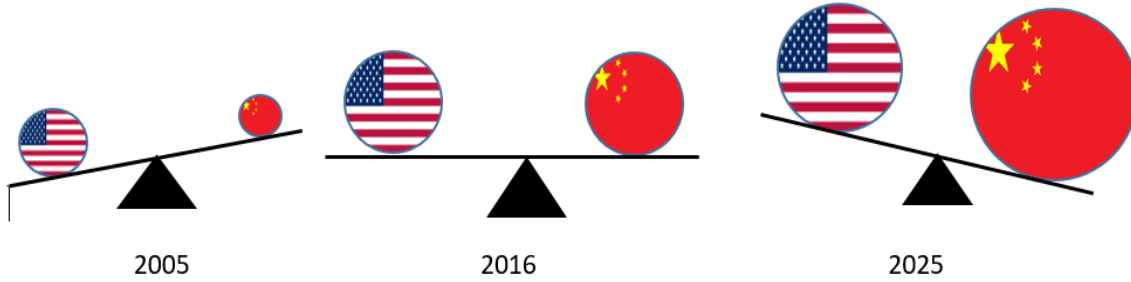
¹ Graham Allison, et al, **The Great Tech Rivalry: China vs. the US**, Belfer Center, Havard Kennedt School, March 2021, p 5. URL: <https://bit.ly/3dx0YDv>.

² Xinhua, **China forges ahead for brighter future in digital economy**, english.scio.gov.cn, April 25, 2022, URL: <https://bit.ly/3PmsIrx>.

كبيرة لاقتصادها، لأن [هذا] هو بالتأكيد المحرك الرئيسي للنتائج المحلي الإجمالي للولايات المتحدة الآن¹، وعليه فإن الصراع حول التكنولوجيا هو المحدد الرئيس لتوازن القوى في المجال الاقتصادي ومن ثم مكانة ودور الدولة في السياسة الدولية.

شكل رقم 11: تحولات ميزان القوى حسب الناتج الإجمالي الخام GDP

المصدر: من إعداد الباحث وفق إحصائيات البنك وصندوق النقد الدوليين على الرابط:
<https://bit.ly/3dwFuq3>



الناتج الخام الإجمالي GDP لتعادل القيمة الشرائية PPP (مليار دولار)

الدولة	2005	2016	2025
الولايات المتحدة	13,036.60	18,745.10	26,719.63
الصين	6,588.93	18,712.10	35,748.12

الفرع الثاني: التكنولوجيا كمحرك لتغيير توازن القوى العسكري

تُعد الولايات المتحدة الأمريكية القوة العسكرية الأولى في العالم، فمنذ نهاية الحرب العالمية الثانية راكمت الولايات المتحدة قدراتها العسكرية استجابة لمهامها ودورها الكوني في البر، البحر، الجو، الفضاء الخارجي، كما كانت لها الأسبقية في امتلاك القدرات النووية والسيبرانية، تتفق جميع المؤشرات العالمية لقياس قوة الجيوش على صدارة الولايات المتحدة كأقوى جيش في العالم بميزانية بلغت 773 مليار دولار لسنة 2023²، في المقابل احتل الجيش الصيني المركز الثالث بعد روسيا في ترتيب الجيوش السنوي على مدى العقدين الماضيين، ولكن هذه المرتبة لا تعكس التطور في العتاد والتكتيكات القتالية والجاهزية بقدر ما تشير إلى عدد الأفراد والعتاد (في أغلبه قديم ومتهالك)، إذ لم تبدأ عملية تحديث وتطوير الجيش الصيني إلا بعد 2012 حين قررت

¹ Ralph Jennings, **China's Economy Could Overtake US Economy by 2030**, voanews.com, January 04, 2022, URL: <https://bit.ly/3QG4HwG>.

² **U.S. Department of Defense**, The Department of Defense Releases the President's Fiscal Year 2023 Defense Budget, defense.gov, MARCH 28, 2022, URL: <https://bit.ly/3Aovo3u>.

القيادة الصينية تحويله إلى جيش احترافي مع زيادة سنوية في ميزانية الدفاع تقدر بـ 7 إلى 8% سنويا حيث بلغت 230 مليار دولار سنة 2022¹.

كل الأرقام السابقة تُشير إلى تفوق ساحق للجيش الأمريكي وهذا ما جعل بعض المحللين يستبعد حتى محاولة تفكير الصين في تحدي الجيش الأمريكي²، كما أن تقارير مؤسسة راند Rand ترجح كفة الولايات المتحدة بفارق كبير³، إلا أن آخرين حذروا من وقوع البلدين في "فخ ثيوسيدس"⁴، كما يجادل إيريك شميدت مؤسس Google أن الابتكار في التقنيات الناشئة (الذكاء الاصطناعي، الحوسبة الكمومية، تقنيات الجيل الخامس... وغيرها) هي حتمية اقتصادية وأمنية للمحافظة على الريادة⁵، فهي من ستحدد في السنوات القادمة توازن القوى الاقتصادي والعسكري وشكل المنافسة الدولية، وهذا ما ينعكس على استراتيجيات الدولتين في التحديث العسكري والتركيز على تطوير التقنيات الناشئة بمساعدة القطاع الخاص في الولايات المتحدة والدمج بين المدني والعسكري في الصين، وفي ظل تكتيكات القتال التي تعتمد أكثر فأكثر على العمليات المشتركة بين الوحدات العسكرية المختلفة التخصصات من خلال التشبيك الكثيف فإن تحقيق إختراقات في تطوير التقنيات الناشئة قد يمنح الدول ميزة تفوق عسكرية كبرى ويرجح توازن القوة العسكري لصالحها، ترفع ديناميكية الفائز يأخذ كل شيء من مخاطر التطوير السريع لهاته التقنيات إذ حذر الرئيس بايدن مجلس الشيوخ الأمريكي بعد محادثته مع الرئيس الصيني شي بأنه "إن لم نتحرك الآن فسوف يهزموننا"⁶ يقصد بذلك الصين.

¹ Liu Xuanzun, China boosts defense budget by 7.1% for 2022 amid complex global situation, globaltimes.cn, Mar 05, 2022 , URL: <https://bit.ly/3SMgBqR>.

² Mangesh Sawant, "Why China Cannot Challenge the US Military Primacy", Journal of Indo-Pacific Affairs, Air University Press, 2021.

³ Eric Heginbotham, Michael Nixon, et al, The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996–2017, CA: RAND Corporation, 2015. URL: <https://bit.ly/3K11Lc2>.

⁴ Graham Allison, Destined for War: Can America and China Escape Thucydides's Trap?, Harvard Kennedy School, 2017.

⁵ انظر: تقرير لجنة الأمن القومي الخاصة بالذكاء الاصطناعي على الرابط: <https://bit.ly/3JctHsX> ، شهادة إريك إي شميدت أمام لجنة القوات المسلحة بمجلس الشيوخ بعنوان: التقنيات الناشئة والدفاع: تصحيح الأساسيات على الرابط: <https://bit.ly/3bSDGri>، والكتاب الذي ألفه إيريك إي شميدت بالاشتراك مع هنري كيسنجر حول مخاطر الذكاء

الاصطناعي ومستقبل البشرية بعنوان: The Age of AI: And Our Human Future Hardcover.

⁶ رويترز، بايدن يقول الصين ستهزمنا ما لم نتحرك والرئيس الصيني يحذر من مواجهة ستكون "كارثة"، موقع رويترز، فيفري 2021، على الرابط: <https://reut.rs/3CqdYVZ>.

الفرع الثالث: أثر الصراع التكنولوجي على النظام الدولي

إن عودة الصين إلى الساحة الدولية كقوة عظمى يشير إلى أننا قد نشهد تحولاً في توازن القوة على الأقل في منطقة جنوب شرق آسيا، ذلك لأن سياسات الصين وطموحاتها تتعارض بشكل مطرد مع المصالح الأمريكية مما يجعلها في وضع غير متوافق وصراعي دائم، فالنظام العالمي الذي تسعى له الصين يتعارض بشدة مع النظام الدولي الليبرالي الذي تقوده الولايات المتحدة، وفي ظل استبعاد سيناريو الحرب المباشرة بين القوتين بسبب الترابط الاقتصادي الكثيف بين البلدين والتي تسعى الولايات المتحدة لفك الارتباط خاصة في المجال التكنولوجي، وقوة الردع النووي التي تمنع البلدين من الدخول في مواجهة عسكرية مباشرة وفق مبدأ عقلانية الدولة، وعليه يبقى الفضاء السيبراني والتقنيات الناشئة كمنطقة رمادية من أبرز مجالات الصراع بين الولايات المتحدة والصين، فالتكنولوجيا كقوة دافعة داخلية للتفوق الاقتصادي والعسكري تجعل من التنافس بين القوتين يتمحور حول السيطرة على القواعد والأعراف والمؤسسات التي ستحكم العلاقات الدولية في العقود القادمة¹.

صرحت رئيسة مجلس النواب الأمريكي نانسي بيلوسي في اختتام مؤتمر ميونخ للأمن 2020 في تعليقها حول حظر شركة هواوي الصينية أن كلا الحزبين الديمقراطي والجمهوري متفقان على أن التكنولوجيا الصينية هي التهديد الأول لأمريكا وحلفائها، وأن "الأمن القومي والاقتصاد والقيم كلها مجتمعة في قضية هواوي"²، فالولايات المتحدة ترى أن الصين تحاول تغيير النظام الدولي إلى نظام استبدادي يخدم مصالحها من خلال الابتكار والتفوق التكنولوجي، لذلك غالباً ما يستعمل المفكرون والسياسيون الأمريكيون مصطلحات التكنولوجيا النظيفة والفضاء السيبراني الحر والذكاء الاصطناعي الديمقراطي في مقابل التكنولوجيا الاستبدادية في إشارة إلى الصين.

في المقابل، تُروج الصين إلى أنها تسعى لإصلاح النظام وليس تغييره، ذلك أنها منخرطة بقوة في المؤسسات الدولية وتستفيد من العولمة الاقتصادية بشكل واضح، ولأجل عملية الإصلاح تركز الصين على التكنولوجيا لا اعتقادها بأنها السبيل الأفضل للتفوق وبفضلها يمكن تقديم النموذج

¹ X Wu, "Technology, power, and uncontrolled great power strategic competition between China and the United States", **China International Strategy Review**, Vol 2, N°1, 2020, pp 99–119.

² Nancy Pelosi, **Transcript of Pelosi, Congressional Delegation Press Conference on Conclusion of 2020 Munich Security Conference**, speaker.gov, February 16, 2020, URL: <https://bit.ly/3CfQN07>.

الصيني كنموذج ناجح عالمياً يمكن الاعتماد عليه في وضع القواعد والمعايير التي تحكم النظام الدولي في المستقبل.

وبناءً على ما سبق، فالولايات المتحدة وفي سبيل الحفاظ على هيمنتها والإبقاء على النظام الدولي الحالي فإنها تستخدم أساليب الحرب الباردة، فالنظام الدولي الحالي جاء لمواجهة الاتحاد السوفياتي الشيوعي لكن بعد أن زال الخطر الشيوعي فقد النظام سبب وجوده وبدأت التحالفات الأمريكية في الضعف والتفكك، لذلك تسعى الولايات المتحدة لإعادة إحيائه من خلال إبراز التهديد الصيني ووضعه في الواجهة لإعادة حشد الحلفاء وتخويفهم للالتفاف حول الولايات المتحدة كقائد للعالم، ويتم التركيز على المجال التكنولوجي في هذه الحرب الباردة الجديدة لأنه إذا تفوقت الصين في المجال التكنولوجي فمن الصعب كبحها في المجالين الاقتصادي والعسكري كما تزداد جاذبية نموذجها السياسي لدى بقية دول العالم.

بحث الفصل الثاني في مضامين ومضامير الصراع في/على الفضاء السيبراني بين الولايات المتحدة الأمريكية والصين، وحيث إن من المقرر في العلاقات الدولية أن القوة لازمة لخوض الصراع فقد بدأنا المبحث الأول برصد لمؤشرات القوة السيبرانية ثم طبقنا مؤشر بلفر والذي يُعتبر أحدث وأنسب أداة لقياس وتقييم القدرات السيبرانية للولايات المتحدة الرائدة في المجال السيبراني والصين التي تنمو قدراتها السيبرانية بسرعة كبيرة في المجالات السبعة الرئيسية (المراقبة، التحكم، الدفاع، الهجوم، المخابرات، الاقتصاد، القواعد والمعايير).

ومن ثم تطرقنا في المبحث الثاني لرصد وتحليل الصراع بين الدولتين في/على الفضاء السيبراني من خلال الطبقات المكونة له، فبتطبيق منهج البحث الجيوبوليتيكي قمنا بتحديد القضايا الصراعية في كل طبقة (جوهر الحدث) والفاعلين المؤثرين في القضايا سواء كانوا حكومات أو شركات (عامل الحدث) ثم تحديد مصالح كل من الولايات المتحدة والصين في القضايا وتأثير ذلك على الأمن المحلي والدولي (بيئة الحدث)، وقد عالج المبحث أهم القضايا متمثلة في: تقنيات الجيل الخامس 5G، الكوابل البحرية، أشباه الموصلات، حوكمة الأنترنت، البرامج والتطبيقات، البيانات الضخمة والذكاء الاصطناعي.

وختمنا الفصل برصد وتحليل لتداعيات الصراع التكنولوجي على علاقة البلدين الثنائية وتحولها من الشراكة إلى المنافسة الاستراتيجية الشاملة، وما تبعه من محاولات أمريكية لإعادة تنشيط تحالفاتها القديمة وبناء تحالفات جديدة محورها الصراع التكنولوجي، ثم تطرقنا إلى دور الصراع على الهيمنة التكنولوجية في بلوغ التفوق الاقتصادي والعسكري وسعي الولايات المتحدة الحفاظ على موقع الهيمنة في النظام الدولي الحالي ومواجهة محاولات الصين التعديلية.

الفصل الثالث

استراتيجيات الولايات المتحدة والصين
لإدارة الصراع في الفضاء السيبراني

يُقدم هذا الفصل في بدايته قراءة في أهم المقاربات النظرية والمنطلقات الفكرية الجديدة التي تساعدنا في فهم الكيفية التي تُطور بها كل من الولايات المتحدة والصين استراتيجياتهما لإدارة الصراع في الفضاء السيبراني، ومن ثم يقوم بفحص وتحليل استراتيجيات كل دولة للهيمنة في وعلى الفضاء السيبراني، منطلقاً من مبادئها الجيوبوليتيكية ومدرکها الاستراتيجي لهذا الفضاء.

المبحث الأول: المقاربات النظرية والمنطلقات الفكرية الحديثة لإدارة الصراع في الفضاء السيبراني

كان للبيئة الصراعية الجديدة التي يشهدها العالم المتمثلة في قطبية أحادية متراجعة وصعود متسارع لقوى دولية جديدة من جهة، وتغلغل الفضاء السيبراني في مختلف مناحي الحياة بخصائصه الفريدة من جهة أخرى، انعكاسات على عمليات إدارة الصراع في/على الفضاء السيبراني والفضاء المادي على حد سواء، ففي ظل تراجع مبدأي السيادة وعدم التدخل في الشؤون الداخلية للدول، وبروز وتنامي أدوار الفاعلين الجدد من غير الدول، يُصنف الدكتور **أحمد محمد وهبان** الاتجاهات النظرية المعاصرة لإدارة الصراع حسب الأساليب المتبعة إلى ثلاثة مستويات¹:

1. الدبلوماسية (التفاوض، المساومة، الوساطة).

2. العقوبات الاقتصادية.

3. التهديد باستخدام القوة والاستخدام الفعلي لها.

وعليه، فوفق هذه المستويات سنقوم برصد المقاربات والمنطلقات الفكرية الحديثة لإدارة الصراع في الفضاء السيبراني.

المطلب الأول: دبلوماسية الشركات

تُعد شركات التكنولوجيا اليوم من أكبر الكيانات الفاعلة على الساحة الدولية، فإيراداتها تتفوق على الناتج المحلي لكثير من الدول، كما أن عدد مستخدمي منتجاتها يفوق عدد مواطني أية دولة في العالم، لذلك فإن قراراتها التقنية والسياسية لها تداعيات وطنية وعالمية كبيرة، وهو ما يجعل تأثيرها السياسي والجيوبوليتيكي على الساحة الدولية مهماً للغاية.

وعليه، فبعد إدراك الكثير من الدول للقوة والوزن الجيوبوليتيكي الذي تملكه شركات التكنولوجيا بادرت إلى إدارة علاقاتها مع هذه الشركات من خلال موظفين حكوميين رسميين، حيث عيّنت الدنمارك سفيراً للتكنولوجيا في وادي السيلكون سنة 2017، وصرح وزير خارجيتها آنذاك أثناء حفل التنصيب بأن "شركات مثل Google و IBM و Apple و Microsoft أصبحت الآن كبيرة جداً لدرجة أن قوتها الاقتصادية وتأثيرها على حياتنا اليومية يتجاوز قوة العديد من

¹ أحمد محمد وهبان، تحليل إدارة الصراع الدولي "دراسة مسحية"، سلسلة إصدارات الجمعية السعودية للعلوم السياسية 14، جامعة الملك سعود، 2014، ص 18.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

البلدان التي لدينا فيها سفارات تقليدية"¹، حتى إنه لم يصبح غريباً أن يلتقي المدراء التنفيذيون لشركات التكنولوجيا الكبرى (خاصة الأمريكية) مع رؤساء الدول ويعقدون جلسات الحوار والمفاوضات حول المسائل التقنية بالدرجة الأولى، وقد يتعدى الأمر لمسائل الحرية وحقوق الإنسان، كما أن مشاركتهم في المحافل الدولية أصبحت لازمة، إضافة إلى ذلك، وعلى غرار الشركات الكبرى، تُنفق شركتي **Google** و **Meta** الكثير من المال على جماعات الضغط خاصة في دول الاتحاد الأوروبي من أجل الحفاظ على هيمنتها وخدمة لمصالحها.

في المقابل، بما أن الحكومات وشركات التكنولوجيا لا يتكلمون نفس اللغة، كان لازماً على شركات التكنولوجيا تعيين ممثلين دبلوماسيين لشرح مواقفهم وقراراتهم للحكومات، وتُعد شركة **Microsoft** رائدة في مجال الدبلوماسية الرقمية حيث تمتلك وحدة الدبلوماسية الرقمية الخاصة بها والتي تهتم بمشهد الأمن السيبراني العالمي وتنسق الجهود مع الفرق الحكومية الإقليمية والعالمية لتعزيز الأمن والسلام في الفضاء السيبراني، كما تتبنى الشركة برنامج الدفاع عن الديمقراطية والذي يحارب التدخلات في الانتخابات²، كذلك الحال بالنسبة لشركتي **Google** و **Meta** فكلاهما تساهمان في وضع القواعد والمعايير الدولية في الفضاء السيبراني.

لكن في بعض الحالات تصطدم طموحات الشركتين في التوسع مع التنظيمات والقوانين الداخلية للدول فتضطر إلى إجراء المفاوضات والمساومات من أجل الحصول على مزايا وفوائد تلك الأسواق، ومثال ذلك شركة **Google** حينما عانت من سياسة تفضيلية للشركات المحلية في الصين بإجبارها على احترام القوانين الصينية، وعند عجزها على التوسع داخل السوق الصينية لجأت إلى طلب الدعم من الحكومة الأمريكية لرفع دعاوى قضائية ضد الصين بحجة أن الرقابة الصينية على الإنترنت تعتبر انتهاكاً لمبدأ الحرية واعتداءً على حقوق الإنسان، ففي هذه الحالة تحولت شركة **Google** من شركة تجارية هدفها الربح وخدمة الزبائن إلى لاعب جيوبوليتيكي دولي في الصراع بين الولايات المتحدة والصين.

نظرياً، يتم تأسيس شركات التكنولوجيا كشركات تجارية تقدم الخدمات الرقمية للمستهلكين مقابل جني الأرباح والفوائد، لكن مع توسع دائرة المستهلكين وتخطي المجال الذي تعمل فيه أي

¹ Robert Gorwa, Anton peez, **Tech Hits the Diplomatic Circuit**, berlinpolicyjournal.com, June 27, 2019, URL: <https://bit.ly/3T9IsBk>.

² Patricia Gruver, **Korea-U.S International Exchange and Cooperation in Tech Diplomacy**, Pacific Council on International Policy, June 2022, URL: <https://bit.ly/3AI16cq>.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

الفضاء السيبراني حدود الدول وتآكل مبدأ السيادة جعل الحكومات تُشجع شركاتها التكنولوجية على التوسع أكثر والاستحواذ على المزيد من الأسواق والابتكار لإدراكها أن قوة الشركات التكنولوجية هي قوة للدولة، فالصين مثلاً طالما شجعت شركاتها على الحصول على المزيد من الأسواق والمواد الأولية والتكنولوجيا وقد أطلق الرئيس الصيني "شي" على عمالقة التكنولوجيا في الصين لقب "الأبطال القوميون"، وبالمثل كانت الولايات المتحدة دائماً تتباهى بريادة شركاتها التكنولوجية في الفضاء السيبراني.

غير أن هذا النمو في قوة شركات التكنولوجيا اقتصادياً وسياسياً أحدث في بعض الأحيان تصادماً بين طموحات الشركات على المستوى الدولي والسياسة الخارجية للحكومات التابعة لها، هذا ما جعل الحكومات تُراجع سياساتها تجاه الشركات الكبرى، ففي الولايات المتحدة، مع تولي الرئيس "ترمب" القيادة وتزامناً مع حربه التجارية على الصين كانت شركات التكنولوجيا الصينية أولى ضحايا هذه الحرب عبر قوانين الحظر التي أصدرتها الحكومة الأمريكية، كما مارست إدارة "ترمب" ضغوطات كبيرة بُغية التحكم وإعادة توجيه أعمال شركات التكنولوجيا الأمريكية لخدمة توجهات الحكومة، إذ لم يعد الإستثمار والربح المادي هو المحرك والدافع لأعمال الشركات بل ما تمليه مصلحة الحكومة وسياساتها الخارجية، في المقابل، كانت الشركات الصينية تحت مراقبة الحكومة منذ تأسيسها وهو ما جعل الغرب يتهمها بأنها تابعة للحزب الشيوعي الصيني الحاكم وليست شركات خاصة رغم محاولات شركات التكنولوجيا الصينية نفي هذه التهمة، لكن القوانين الصينية الصارمة أخضعها بطريقة أو بأخرى لتوجيهات ورؤية الحكومة الصينية، أو كما يصفها نوح فلدمان "الحزب في صورة شركة"¹.

وبناءً على ما تقدم، فشركات التكنولوجيا الكبرى هي حلقة الربط الرئيسية بين الاقتصاد العالمي والجيوبوليتيك، فالحكومات تدفع بالشركات إلى واجهة الصراع، وعليه، فإن كيفية تصرفها والأدوار التي تلعبها شركات التكنولوجيا الكبرى في الاقتصاد العالمي والسياسة الدولية يُحدد بدرجة كبيرة مدى إمكانية التعاون، التنافس أو الصراع بين الدول، وعندما ينهار الحاجز بين الاقتصاد والجيوبوليتيك ينهار معه الحاجز بين الأعمال والسياسة.

¹ نوح فلدمان، الحرب الهادئة مستقبل التنافس العالمي، تر: هشام سمير، الخبر: الدار العربية للطباعة والنشر، 2016، ص 188.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

المطلب الثاني: الهيمنة الرقمية ومجالات النفوذ الجديدة

ظهر مصطلح "الهيمنة الرقمية" لأول مرة في خطاب الحزب الشيوعي الصيني سنة 2015، على خلفية التحقيق الذي قامت المفوضية الأوروبية حول الإساءة المحتملة في استعمال خصوصية مستخدمي شركة Google في أوروبا، ولخص المقال المنشور في صحيفة الشعب اليومية 人民日报¹ العلاقة بين الهيمنة الرقمية والصراع على السلطة والنفوذ في الفضاء السيبراني بين دول العالم، وخُصص إلى أن قدرة الدولة على حماية "السيادة السيبرانية" تحدد موقعها المستقبلي في العالم.

تُستخدم فكرة "الهيمنة الرقمية" من قبل الصينيين لتركيز الانتقادات حول جهود الولايات المتحدة للسيطرة على سياسات الفضاء السيبراني الدولية وعمليات المراقبة السيبرانية ومحاولات احتواء وتنشيط أي تقدم تكنولوجي أو تحرك سياسي ذي صلة من قبل الصين، فهيمنة الولايات المتحدة على التقنيات والقواعد والمعايير السيبرانية تُهدد فكرة الفضاء السيبراني المتعدد الأقطاب والذي تسوده العدالة والمساواة في الحقوق والسيادة.

يُبرر مناصرو مقارنة "الهيمنة الرقمية" فكرة أن للولايات المتحدة سعت وتسعى دائماً للحفاظ على دور المهيمن في مختلف المجالات بما في ذلك المجال التكنولوجي بسرد تاريخ من قمع الولايات المتحدة للمنافسين التكنولوجيين باستعمال الوسائل المالية والتكنولوجية والقانونية، وتحت ذرائع متعددة كحماية الأمن القومي، الملكية الفكرية، قوانين التجارة الحرة والقوانين الأمريكية التي تمتد عبر العالم، ففي ثمانينيات القرن المنصرم وبعد التطور الكبير والسريع لصناعة أشباه الموصلات في اليابان التي تجاوزت الولايات المتحدة كأكبر مصدر لأشباه الموصلات في العالم، اتهمت الإدارة الأمريكية اليابان بسرقة الملكية الفكرية، واعتقلت موظفين من شركتي هيتاشي Hitachi و ميتسوبوشي Mitsubishi بتهمة التجسس الصناعي، كما استغلت "لجنة باريس التنسيقية" والتي أنشأت بعد الحرب العالمية الثانية لمنع تصدير التكنولوجيا الفائقة إلى الدول

¹ 人民日报, 捍卫“数据主权” (环球走笔) [الدفاع عن "سيادة البيانات"], opinion.cntv.cn, Jan 14, 2015, URL : <https://bit.ly/3pLFyp4>.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

الاشتراكية للتنديد بصادرات توشيبا Toshiba للاتحاد السوفياتي ثم أصدرت قانون عقوبات ضد الشركة، لتبيع الشركة أعمالها لصناعة أشباه الموصلات للشركة الأمريكية Bain capital¹.

لذلك يرى أصحاب هذا الطرح أن الولايات المتحدة اليوم تستعمل نفس الأساليب القديمة للحفاظ على هيمنتها في الفضاء السيبراني، فالحرب التجارية وقوانين الحظر التي مست الشركات الصينية خاصة شركة هواوي والتدفع بنفس الذرائع القديمة من حماية الأمن القومي وخصوصية المواطنين الأمريكيين ما هي إلا استنساخ لأساليب الماضي في محاولة لتعطيل وتقويض النهضة التكنولوجية الصينية وإبقاء الولايات المتحدة في المقدمة ولو على حساب قواعد التجارة الدولية وقوانين حقوق الإنسان.

ومن هذا المنطلق، يدعو مناصرو مقاربة "الهيمنة الرقمية" إلى أن سعي الولايات المتحدة الدائم للهيمنة يُقوض الأساس العادل للفضاء السيبراني ويعوق التعاون والابتكار ويمثل أكبر عقبة للترابط العالمي، ولتحقيق بيئة صحية لنمو الفضاء السيبراني يجب على دول العالم جميعاً أن تقول "لا" للهيمنة الرقمية الأمريكية، وأن تسعى لخلق وضع جديد من التعاون في الفضاء السيبراني، وتشكيل إطار أكثر شمولاً لإدارة الأنترنت والتحول الرقمي المستدام، وبناء مجتمع مصير مشترك في الفضاء السيبراني².

إضافة لما تقدم، تظهر دعوات للإهتمام أكثر بمجالات النفوذ الجديدة، ورغم أن مصطلح "مجال النفوذ" هو مصطلح جيوبوليتيكي ظهر منذ القرن 19م وبرزت مدلولاته بشدة أثناء الحرب الباردة إلا أن القادة الأمريكيين بعد نهاية الحرب الباردة من كليتون إلى أوباما كانوا يرفضون المصطلح ويعتبرونه قد عفا عنه الزمن ولا يمكن الحديث عن مجال للنفوذ للقوى الكبرى في عالم تتمتع فيه كل الدول بالاستقلال والسيادة، وهذا التوجه -كما يعبر عنه غراهام أليسون- لا يرجع إلى إيمان القادة الأمريكيين بالعدالة والمساواة بين الدول بقدر ما يعكس الهيمنة الأمريكية على العالم وأنه أصبح في مجمله مجالاً للنفوذ الأمريكي³.

¹ 王磊 [وانغ لي]، "清洁网络"计划的实质是数字霸权 [الهيمنة الرقمية]، [جواهر برنامج الويب النظيف هو الهيمنة الرقمية]، china.com.cn, Nov 02, 2020, URL : <https://bit.ly/3wuxZqw>.

² 新华 [شينخوا]، 美式 "数字霸权" 是全球互联互通最大障碍 [الهيمنة الرقمية الأمريكية أكبر عقبة]، [الهيمنة الرقمية الأمريكية أكبر عقبة]، chinanews.com.cn, Dec 15, 2021, URL : <https://bit.ly/3CxJPEa>.

³ Graham Allison, "The new spheres of influence: sharing the globe with other great powers", *Foreign Affairs*, 99, 2020, p 30.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

عاد المصطلح للظهور مجدداً في عهد الرئيس "ترمب" مع الشعور المتزايد لدى صناع السياسة الخارجية ومحلي الأمن القومي الأمريكيين بأن عهد الأحادية القطبية قد ولى وتم استبداله بفترة جديدة من التنافس الاستراتيجي الخطير بين القوى الكبرى، وهذا ما يظهر جلياً في استراتيجية الأمن القومي الأمريكية لسنة 2018، ومن ثم حدث انقسام بين المفكرين الأمريكيين حول قبول الولايات المتحدة بمناطق نفوذ للصين وروسيا، فالمعارضون¹ يرون أن القبول بمناطق نفوذ للصين وروسيا قد يغذي طموحات القوتين ويضعف ثقة الحلفاء ويُقيد قدرة الولايات المتحدة على تشكيل الأحداث في تلك المناطق، أما المؤيدون² فيرون أن الاعتراف بمناطق نفوذ للصين وروسيا قد يجنب العالم مخاطر الحرب المكلفة، ويحقق الاستقرار في سياسات القوى العظمى، حيث يجادل أليسون بأن على صانعي السياسة الأمريكيين التخلي عن التطلعات المثالية للعالم التي لا يمكن تحقيقها وقبول أن مناطق النفوذ ستظل سمة رئيسة للجيوبوليتيكا³.

ينسحب مفهوم "مناطق النفوذ" على الفضاء السيبراني، ففي الولايات المتحدة جاءت الدعوات الأولى منذ 2009 لاعتماد مقاربة مستوحاة من "عقيدة مونرو Monroe Doctrine" لمجابهة التهديدات والصراعات في الفضاء السيبراني أو ما أطلق عليه "عقيدة مونرو السيبرانية"⁴ والتي بموجبها تعتبر الولايات المتحدة أن الفضاء السيبراني هو مجال نفوذ أمريكي وستقوم بحماية مصالحها فيه والرد على كل الطامحين للسيطرة عليه.

في المقابل، يذهب مفكرون آخرون إلى تقسيم العالم إلى مجالات نفوذ تكنولوجية متنازع عليها، حيث يعتبرون المجال الأكثر أهمية هو **الهلال التكنولوجي** والذي يمتد من جنوب شرق آسيا مروراً بجنوب آسيا والجزيرة العربية وصولاً إلى أوروبا، هذا المجال تتصارع فيه الولايات المتحدة والصين للسيطرة والنفوذ من خلال استعمال دول الهلال الحصري للتكنولوجيا الأمريكية

¹ مثل براندز وإيدل، وروبرت كاغان من معهد بروكينغز في مقال بعنوان "العودة إلى الحرب العالمية الثالثة" في مجلة Foreign Policy، انظر: <https://bit.ly/3Cwpj6D>.

² مثل غراهام أليسون، وتيد جالين كاربنتر من معهد كاتو في مقال بعنوان "قبول مجالات النفوذ في القرن 21"، انظر: <https://bit.ly/3AjsYSw>، وبيتر بينارت من مجلة ذي أتلانتيك في مقال بعنوان "تحتاج أمريكا إلى سياسة خارجية جديدة لعصر ترمب"، انظر: <https://bit.ly/3Tmt30q>.

³ Graham Allison, "The new spheres of influence: sharing the globe with other great powers", op.cit.

⁴ جاءت في سياق التوصيات التي قدمتها ماري آن دافيدسون في شهادتها أمام اللجنة الفرعية للأمن الداخلي المعنية بالتهديدات الناشئة والأمن السيبراني والعلوم والتكنولوجيا في 2009، انظر الرابط: <https://bit.ly/3KDO4QF>.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

أو الصينية ودعمها لطرف معين في قضايا حوكمة الإنترنت العالمي¹، وعليه يمكن ملاحظة أن مجالات النفوذ التكنولوجية تمتاز بخاصيتين أساسيتين هما، أولاً، غير معترف بها من طرف القوى المتنافسة، فكل طرف يحاول السيطرة وبسط نفوذه في كل المجالات، ثانياً، لا تتوزع مجالات النفوذ التكنولوجية أفقياً فحسب بل تتراكم رأسياً كذلك، فالسيطرة على طبقة من طبقات الفضاء السيبراني في منطقة نفوذ الخصم قد يغير مجال النفوذ في الطبقات الأخرى من طرف إلى آخر.

المطلب الثالث: اللعبة الجيوبوليتيكية الرقمية

يفترض توماس شيلينغ في كتابه "استراتيجيات الصراع" أن الصراعات باعتبارها حالة طبيعية في العلاقات الدولية أشبه ما تكون بالمسابقات (المباريات أو الألعاب) والتي يسعى المنخرطون فيها للفوز، فنظرية الألعاب حسب شيلينغ هي التي تعتمد فيها أفضل حركة للاعب على ما يفعله اللاعبون الآخرون²، وباعتبار أن التنافس والصراع هو القاعدة في العلاقات الدولية فإن اللعبة بين القوى العظمى تمثل أعلى درجات هذا الصراع.

وعليه، فإن التطور السريع للتكنولوجيات الفائقة والناشئة والتسييس المتزايد للتكنولوجيا والرقمنة المتسارعة في كل دول العالم أحدثت تشابكاً بين التكنولوجيا والجيوبوليتيكا مما جعل الجيوبوليتيك السيبراني يظهر تدريجياً في ممارسات العلاقات الدولية، أي أن اللعبة الرقمية أصبحت في قلب اللعبة الجيوبوليتيكية العالمية، هذه اللعبة التي تتشكل من خلال المفاهيم التي تطرحها القوى الكبرى التقليدية لكيفية تشكيل وإدارة الفضاء السيبراني بناءً على مصالحها الخاصة، حيث يتم الدفع بقضايا الفضاء السيبراني على رأس أولويات الحكومات والجيش، ولعل أبرز المحاور التي تدور حولها اللعبة الجيوبوليتيكية الرقمية اليوم هي: أولاً، التقنيات الفائقة والناشئة كالجيل الخامس، البيانات الضخمة، الذكاء الاصطناعي والحوسبة الكمومية، ثانياً، حوكمة الإنترنت والسيادة السيبرانية، ثالثاً، سلاسل التوريد العالمية للمنتجات التكنولوجية.

¹ Valentin Weber, **Making Sense of Technological Spheres of Influence**, LSE IDEAS, Mar 31, 2020, URL: <https://bit.ly/3ANbgbI>.

² توماس شيلينغ، **استراتيجية الصراع**، تر: نزهت طيب وأكرم حمدان، بيروت: الدار العربية للعلوم ناشرون، 2010، ص 11.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

في الوقت الراهن تتشكل لنا صورة لـ "لعبة رباعية"¹ في الفضاء السيبراني في شكلها الموسع، حيث تتنافس القوى الكبرى التقليدية في الفضاء السيبراني ولكن بدرجات متفاوتة؛

أولاً، لطالما كان الفضاء السيبراني أمريكياً بامتياز، فهي التي اخترعته ثم قدمته للعالم، فكبرى شركات التكنولوجيا أمريكية فهي التي تصنع الأجهزة وتطور البرامج وتضع المعايير والقواعد التقنية، كما قدمت الولايات المتحدة مفاهيم الحوكمة كـ "حرية الإنترنت" و "الفضاء المفتوح" و "أصحاب المصلحة المتعددين"، وتعتبر أيضاً من الدول المسيطرة على سلاسل توريد المنتجات التكنولوجية، لذلك فهي تملك ميزة اللاعب المهيمن في الفضاء السيبراني.

ثانياً، تطورت الصين بسرعة وبرزت شركات تكنولوجية لها قدرات كبيرة على المنافسة، كما يُرجح أن الصين قد تفوقت بالفعل على الولايات المتحدة في بعض المجالات كالذكاء الاصطناعي، وهذا ما جعل صوتها مسموعاً في مجال حوكمة الإنترنت حيث قدمت مفهومي "السيادة السيبرانية" و "مجتمع المستقبل المشترك في الفضاء السيبراني" لمواجهة الهيمنة الأمريكية وتحويل اللعبة الرقمية من لعبة ذات محصلة صفرية كما تريدها الولايات المتحدة إلى لعبة يستفيد منها الجميع.

ثالثاً، يسعى الاتحاد الأوروبي ليكون "الطريق الثالث" في الفضاء السيبراني بعيداً عن تأثير الصين والولايات المتحدة، حيث طرح مفاهيم "سيادة البيانات" من خلال اللائحة العامة لحماية البيانات **DGPR** ويسعى لتحقيق "الاستقلال الاستراتيجي" في الفضاء السيبراني.

رابعاً، تتبنى روسيا موقفاً دفاعياً في الفضاء السيبراني، فهي تسعى لإنشاء "أنترنت سيادي" يمكن عزله عن بقية الشبكة في حال التهديد بتطبيق تدابير "قطع الاتصال النشط".

وتعقياً على ما سبق، يرى البعض أن اللعبة الجيوبوليتيكية الرقمية هي "لعبة ثلاثية الأرجل"² يلعب فيها الاتحاد الأوروبي دور القوة الموازنة، فمن جهة، يتحدى الهيمنة الأمريكية في مجال البيانات الضخمة من خلال سياسة توطين البيانات، ومن جهة أخرى، تساهم بعض دوله في الحصار التكنولوجي التي تدعو له الولايات المتحدة ضد شركات التكنولوجيا الصينية، لكن اللعبة

¹ لعبة القوى العظمى في الفضاء [数字空间的大国博弈笔谈], جمعية السرية الصينية [中国保密协会], zgblmxh.cn, Jan 21, 2022, URL : <https://bit.ly/3pN5wZh>.

²翟 崑 [تشاي كون], 数字全球化的战略博弈态势及中国应对 [الوضع الاستراتيجي للعولمة الرقمية واستجابة], rmlt.com.cn, Juin 29, 2021, URL : <https://bit.ly/3CyArQA>.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

الرقمية الكبرى العالمية اليوم محصورة بين القوتين الكبريين الولايات المتحدة الأمريكية والصين، فالاتحاد الأوروبي وروسيا لا يملكان القدرات اللازمة للصراع في أغلب مجالات اللعبة الرقمية.

إضافة إلى ما سبق، تتميز اللعبة الجيوبوليتيكية الرقمية بـ "أدلجة للتكنولوجيا" أي تحميل التكنولوجيا -والتي من المفترض أنها محايدة- القيم الإيديولوجية لأطراف اللعبة، ففي سعيها لتبرير العداء ضد الصين تعتمد الولايات المتحدة في سياسة "بناء العدو" على تمرير خطاب الفضاء السيبراني المحمل بالإيديولوجيا، حيث تستعمل مصطلحات من قبيل "الاستبداد الرقمي"، "الذكاء الاصطناعي الديمقراطي"، "الديمقراطيات العلمية والتكنولوجية" في مقابل "الدول التكنولوجية الاستبدادية"¹، هذه المصطلحات تساعد في بناء خطاب قوي موجه للحكومات لكسب تأييد الحلفاء والجمهور، وعزل المنافسين وجعلهم حالة شاذة في المجتمع الدولي.

وعليه، فإن الصراع بين القوى الكبرى في الفضاء السيبراني عبارة عن مزيج من المفاهيم الجيوبوليتيكية التقليدية والخصائص الجديدة للفضاء السيبراني، فلعبة القوى الكبرى تتجه إلى مرحلة جديدة من الجيوبوليتيكا السيبرانية، حيث يصبح التكيف مع الشكل الجديد للصراع وتجنب الخسائر الاقتصادية والأمنية من خلال الفهم الجيد لنوايا وتحركات الخصوم في قلب التخطيط الاستراتيجي للدول.

المطلب الرابع: الردع وتوازن القوى في الفضاء السيبراني

تُعتبر نظرية الردع من النظريات القديمة نسبياً والتي برزت بوضوح خلال الحرب الباردة بين الولايات المتحدة الأمريكية والاتحاد السوفياتي، وقد ارتبط مفهوم الردع إلى حد بعيد بالسلح النووي، وعُرف الردع على أنه نظرية يستخدم فيها أحد الفاعلين لتهديدات ذات مصداقية ضد فاعل آخر لإقناعه بعدم اتخاذ إجراء معين، إما من خلال زيادة التكلفة أو منع المنفعة²، إلا أنه في الكثير من الأحيان يقع الخلط بين "مفاهيم" و"نظريات" و"استراتيجيات" الردع، فالأكاديميون والاستراتيجيون العسكريون يستعملون الكثير من المصطلحات داخل المجال مثل: الردع العام، الردع الضيق، الردع بالإنكار، الردع متعدد المجالات وغيرها دون تفريق بين ما هو مفهوم، نظرية أو استراتيجية، فمثلاً إذا أخذنا مصطلح "الردع العام أو المركزي" فهو عبارة عن نظرية تُشير إلى

¹ 中国保密协会[جمعية السرية الصينية], op.cit.

² Michelle Black, and Lana Obradovic, "Multi-Actor deterrence defining the concept", *Æther: A Journal of Strategic Airpower & Spacepower*, Vol 1, N° 2, 2022, pp 69–80.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

فكرة وجود توازن ثابت للقوى بين الخصوم¹، أما الردع عبر المجالات فهو استراتيجية تُركز فيها الأهداف والغايات لمواجهة التهديدات في منطقة واحدة (الفضاء أو الفضاء السيبراني) من خلال الاعتماد على أنواع مختلفة من القدرات لتكون العمليات أكثر فعالية².

ووفقاً لـ "باتريك مورغان" فإن "استراتيجية الردع تُشير إلى المواقف والتهديدات العسكرية المحددة وطرق الربط بينها التي تتبناها الدولة للردع، أما النظرية فهي المبادئ الأساسية التي يجب أن تقوم عليها الاستراتيجية"³، كما يقدم كل من "ميشال بالاك" و "لانا أوبرادوفيتش" في مقالهما حول "الردع متعدد الفاعلين" تصنيفاً للمصطلحات المستعملة في مجال الردع من حيث كونها مفاهيم أو نظريات أو استراتيجيات⁴.

وعليه، فعند إسقاط نظرية الردع على الفضاء السيبراني تواجهنا العديد من الإشكالات، ذلك أن المجال السيبراني خلق أنواعاً جديدة من التهديدات ومجالاً جديداً للردع، حيث يمكن تقسيم مجالات التهديد ومجالات الردع حسب الجدول الموالي:

جدول رقم 06: حالات التهديد ومجالات الردع.

المصدر: من إعداد الباحث.

رقم الحالة	مجال التهديد	مجال الردع	مثال عن الحالة
01	تقليدي	تقليدي	الردع النووي
02	تقليدي	افتراضي	فيروس Staxnet
03	افتراضي	افتراضي	الهجوم السيبراني الأمريكي رداً على هجوم كوريا الشمالية على شركة Sony
04	افتراضي	تقليدي	التهديد باستعمال الأسلحة التقليدية رداً على الهجومات السيبرانية

¹ Justin V.Anderson, Jeffrey A. Larsen, and Polly M. Holdorf, **Extended Deterrence and Allied Assurance: Key Concepts and Current Challenges for US Policy**, Air force academy, Colorado springs Co Inst for national security studies, 2013, p 4.

² Erik Gartzke, Jon Lindsay, and Michael Nacht, Cross-Domain Deterrence: Strategy in an Era of Complexity, **International Studies Association Annual Meeting**, Toronto. 2014.

³ Patrick M Morgan, **Deterrence now**, Cambridge University Press, 2003, p 8.

⁴ Michelle Black, and Lana Obradovic, **op.cit.**

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

وبناءً عليه، فإذا كان العدو والتهديد معروف في الردع التقليدي أي الحالة 01 من الجدول السابق حيث إن المطلوب فقط هو وضع الاستراتيجية المناسبة أي الإجابة على السؤال: "كيف نردع؟"، فإنه عندما يتعلق الأمر بالتهديد (الهجوم) السيبراني أي الحالة 03 و04، فإن الأسئلة في الفضاء السيبراني لا تقتصر فقط على "كيف" نردع ولكن تتعدى إلى "من" و"لماذا" نردع، ذلك أن خاصية المجهولية في الفضاء السيبراني أفرزت لنا إشكالية "الإسناد" أي من الذي قام بالهجوم؟ فهندسة الفضاء السيبراني توفر خاصية التخفي للمهاجم، حتى أنه يمكن للفاعل الحقيقي أن يُورط أطرافاً أخرى ويُظهرها على أنها الفاعل، وهذا ما يجعل من الإجابة على سؤال الـ "من" عملية في غاية الصعوبة، إضافة إلى أن تعدد الفاعلين وتباين أهدافهم وغاياتهم في الفضاء السيبراني يفرض تخصيص النوع المناسب من الردع لكل نوع من الفاعلين بالإجابة على السؤال: "لماذا نردع؟"، فردع الدول القومية ليس كردع المنظمات الإرهابية ويختلف عن ردع الهاكرز، وهذا ما يُصعب وضع استراتيجية ردع شاملة لكل الفاعلين، كما أن عدم التوافق حول القوانين والتنظيمات في الفضاء السيبراني يجعل من مسألة الردع التقليدي (رد عسكري) للتهديدات السيبرانية مسألة معقدة وغير متفق عليها في غياب للخطوط الحمراء التي يجب على الفاعلين عدم تجاوزها.

من جهة أخرى، هناك من يشكك في إمكانية تطبيق الردع في الفضاء السيبراني¹ (الحالة 02 و 03) حيث إن المصادقية تكاد تكون غائبة في الردع السيبراني، إذ أن الولايات المتحدة والقدرات السيبرانية الهائلة الهجومية والدفاعية لم تُظهر إلا القليل من الفاعلية والقوة في ردع خصومها، فلو فحصنا مثال Stuxnet كأبرز هجوم سيبراني فإنه رغم تعطيله لأجهزة الطرد المركزي في المفاعلات الإيرانية فإنه لم يمنع إيران من مواصلة برنامجها النووي وبقوة أكبر، وهذا يُعزى لطبيعة الأسلحة السيبرانية (الاستعمال مرة واحدة)، وهنا نجد أنفسنا أمام مفارقة كبيرة، فإذا كانت الدولة تملك أسلحة سيبرانية لها قدرة الردع ولكن تبقيها سرية فما الفائدة منها إذ يُعلق الجنرال جيمس كارترائيت من مشاة البحرية الأمريكية على ذلك بقوله: "لا يمكن لشيء سري تملكه أن يكون رادعاً، لأنه إذ لم تعرف أنه موجود فلن يخيفك"²، في المقابل، إذا استعملت الدولة

¹ Timothy M McKenzie, *Is Cyber Deterrence Possible?*, Air University Press, 2017.

² Clorinda Trujillo, "The limits of cyberspace deterrence", *NATIONAL DEFENSE UNIV FORT MCNAIR DC*, 2014, URL: <https://bit.ly/3QbF5Hp>.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

أسلحتها السيبرانية فستكون لمرة واحدة ولن تكون رادعة بعد ذلك، إضافة إلى ذلك عدم اعتراف الدول بالعمليات السيبرانية التي تقوم بها وهو ما يجعل عملية الردع ضبابية وغير موثوقة.

تجدر الإشارة إلى أن المدافعين عن الردع في الفضاء السيبراني وعلى رأسهم "جوزيف ناي الابن"¹ يؤكدون أن الردع في الفضاء السيبراني ليس لمنع كل التهديدات ولا يمكن تشبيهه بالردع النووي الذي يمنع منعاً تاماً استعمال الأسلحة النووية، ولكن يمكن تشبيهه بردع الحكومة للجريمة، أي التقليل منها إلى أقصى حد ممكن، لذلك فإن المزج بين الآليات المتوفرة مثل التهديد بالعقاب، الإنكار والدفاع، التشابك والقوانين قد يجعل الخصوم يعيدون حسابات التكلفة والفائدة، وبما أن الهجمات السيبرانية ليست متساوية في الأهمية والكثير منها لا يتطلب الرد عليها، فلا يمكن ردع كل شيء بل يجب التركيز على ما يهدد الأمن القومي، فمفتاح الردع في العصر الرقمي هو الاعتراف بأن نهجاً واحداً للردع لا يناسب الجميع.

من ناحية أخرى، ووفق الرأي الذي يقول إن الغرض من الردع هو إيجاد توازن ثابت للقوى بين الخصوم، ينطلق "دفيد بنسون" في رؤيته للهجمات في الفضاء السيبراني من خلال مفهوم توازن القوى²، حيث يرى أن المخاوف تنشأ حول توازن القوى حينما تتاور الدول لتحسين احتمالات فوزها في الصراعات المستقبلية، ويضع جداراً نظرياً بين الإكراه والذي يكون باستعمال القوة العسكرية ويكون فورياً وسريعاً تقوم به دولة لتغيير موازين القوى لصالحها، والإعاقة والتي تعمل على تثبيط تطوير القوة بمختلف أنواعها لدى الخصم من أجل تغيير في موازين القوى وتكون طويلة الأمد وبطيئة، لذلك فهو يسمي الهجمات السيبرانية "عوائق"، فالتطور التكنولوجي جعل من المعلومات المُحرك الرئيس للنمو والتطور الاقتصادي والسياسي والعسكري، وبالتالي فهي أساس بناء القوة في مختلف المجالات ومحصلة هذه القوى هي مقدار قوة الدولة في النظام الدولي، وعليه، فإن الهجمات السيبرانية التي تسعى لجمع، تدمير أو تشويه المعلومات لدى الخصم ما هي إلا محاولة من الدول لإعاقة تطوير قوة الخصوم أو كبحها، فالهجمات في الفضاء السيبراني تعمل على إضعاف قدرات المنافسين على ضبط ميزان القوى لصالحهم.

¹ Joseph S Nye Jr, **Deterrence in Cyberspace**, Australian Strategic Policy Institute, Jun 7, 2019, URL: <https://bit.ly/3CU6UkD>.

² David Benson, "Not Cyberwar, but Cyberbalance", **Æther: A Journal of Strategic Airpower & Spacepower**, Vol 1, N° 2, 2022, pp. 81–96.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

إضافة إلى ذلك، فالبيئة الأمنية الدولية تتميز بعدم اليقين والمستقبل غير المؤكد وهو ما يجعل الدول تسعى للتحوط لاحتياجاتها المستقبلية (القوة العسكرية) من الإكراه أو مقاومة الإكراه حتى في غياب تهديد فعلي حاصر، وعلى نفس المنوال تُعبر الهجمات السيبرانية (الإعاقة) عن الحاجات الأمنية المستقبلية للدولة، فمن خلالها تعمل الحكومات على إضعاف قدرة المنافسين على تطوير القوة، وما يترتب عنه من إعادة ضبط لتوازن القوى أو الحفاظ على ميزان القوى القائم، كما أن تدهور الإنتاجية الاقتصادية والتماسك الاجتماعي والسياسي للدولة يؤدي إلى الإضرار بقدرتها على تطوير القوة ويُضعف احتمالية حل الأزمات المستقبلية لصالحها.

وعليه، فإن "بنسون" يدعو إلى استخدام لغة "توازن القوى" بدل "الحرب" للتعبير عن الهجمات والتنافس في الفضاء السيبراني، لأن ذلك يُقلل من خطورة الموقف ويُجنب الأطراف المتنافسة الانزلاق نحو القرارات المتهورة والحروب المدمرة¹، كما يساعد صانعي القرار والاستراتيجيين العسكريين في بناء الاستراتيجيات الملائمة لمستوى التهديد في الفضاء السيبراني.

¹ Ibid.

المبحث الثاني: استراتيجيات الولايات المتحدة الأمريكية في الفضاء السيبراني

ينطلق القادة الأمريكيون في تطوير الاستراتيجيات الوطنية أو الكبرى من المبادئ الجيوبوليتيكية التي توجههم في الفضاء المادي وينسحب ذلك بالضرورة على الفضاء السيبراني، كما أن تفاعلات البيئة الاستراتيجية الجديدة في الفضاء السيبراني له تأثير بالغ على الكيفية التي يدرك بها صانع القرار الأمريكي مصالحه ويحدد بها أهدافه في هذا الفضاء، لذلك فانطلاقاً من الرؤية الجيوبوليتيكية العالمية للولايات المتحدة فقد طورت استراتيجيات ذات بعد عالمي للفضاء السيبراني سواء لزيادة النفوذ أو لبسط السيطرة والحفاظ على الريادة.

المطلب الأول: المبادئ الجيوبوليتيكية الأمريكية والهيمنة العالمية

ننطلق في دراستنا للمبادئ الجيوبوليتيكية للولايات المتحدة من التعريف الذي يقدمه "كولن فلنت" والذي يرى أن المبادئ الجيوبوليتيكية هي "الكيفية التي تُوجه بها الدولة نفسها تجاه العالم" بالإجابة عن عن الأسئلة الخمسة حول تحديد/ والتعامل مع الحلفاء، الأعداء، وكيفية تبرير ذلك للجمهور في الداخل والخارج¹، فالدول مهما كان حجمها تملك مبادئ جيوبوليتيكية حيث تقوم بتقييم المجالات والمناطق الجغرافية وفقاً لمصالحها بتحديد الفرص والمخاطر والتهديدات من أجل وضع الاستراتيجيات المناسبة، إما لاقتناص الفرص أولتحييد المخاطر والتهديدات، لذلك فكل الدول تضع مبادئ جيوبوليتيكية محلية تحدد من خلالها مدى عداوة أو صداقة جيرانها المباشرين، وكثير من الدول لديها مبادئ جيوبوليتيكية إقليمية، ولكن الدول العظمى فقط هي التي تضع مبادئ جيوبوليتيكية عالمية حيث يمتد حضورها ومصالحها لتشمل جميع المناطق والمجالات في الكرة الأرضية.

وبناءً عليه، فالولايات المتحدة تُعتبر من الدول العظمى التي تمتلك مبادئ جيوبوليتيكية عالمية، ففي القرن العشرين وضعت الولايات المتحدة مبادئها الجيوبوليتيكية وفقاً لمصالحها القومية وما تتطلبه من حضور دائم وترتيب للأحداث في كل مناطق العالم، لذلك فالدول العظمى ذات الحضور العالمي والتي يسميها "مودولسكي" بـ "قادة العالم"² يُفترض أن تمتلك القدرة على التدخل في أي منطقة من العالم، وأي تحد لسلطتها في أي مكان يستوجب منها الرد، فهي تستمد شرعية قيادتها للعالم من قدرتها على الوصول إلى كل المناطق والمجالات، إضافة إلى أن محاولة أية

¹ Colin Flint, **Op.cit**, p 67.

² George Modelski, **Long cycles in world politics**, Springer, 1987, p 12.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السبراني

دولة وضع مبادئ جيوبوليتيكية عالمية يفهم على أنه تحد مباشر للدولة القائد المهيمن، وهذا ما ينطبق على حالة الصين، فمثلاً سعي الصين للتغلغل في آسيا وإفريقيا أو محاولتها التفوق في الفضاء السبراني تعتبره الولايات المتحدة الأمريكية تحدياً مباشراً لقيادتها للنظام الدولي الحالي.

تدرجت المبادئ الجيوبوليتيكية الأمريكية عبر تاريخها من المحلي إلى الإقليمي وصولاً إلى العالمي، وانتقلت سياساتها الخارجية من "الانعزالية" إلى "العولمة"، فقد قامت الولايات المتحدة كدولة على مبادئ "المصلحة الفردية"، "الملكية الخاصة" و"تقييد نطاق الحكومة" كأساس لنظامها السياسي والاجتماعي والقانوني، وهذا ما شكل طريقة الحياة الأمريكية في "العالم الجديد"¹، هذه المبادئ عززت من النزعة التوسعية لدى الأمريكيين، فمع نهاية القرن 19 كانت الولايات المتحدة قد أصبحت قوة إقليمية في النصف الشمالي للقارة الأمريكية، فبعد تحييد كل من المكسيك وكندا استولت على الكثير من الجزر في المحيط الهادي والبحر الكاريبي كما اشترت آلاسكا من روسيا وهكذا ضمنت أمنها وهيمنتها في المنطقة مستفيدة من تطبيق مبدأ مونرو 1823 على نصف الكرة الغربي، وكان المبدأ الجيوبوليتيكي الإقليمي الناظم للسياسة الأمريكية هو "السيطرة على منطقة البحر الكاريبي والمحيط الهادي"، كما كان لأفكار "ماهان" حول القوة البحرية بالغ الأثر على تحول الولايات المتحدة نحو العولمة إذ وسعت الولايات المتحدة سيطرتها ونفوذها ليشمل كوبا وهاواي وسيطرت على قناة بنما لتضمن العبور من المحيط إلى المحيط، فأصبحت التجارة والاستثمار غير المقيدتين، والتبادل الثقافي الحر هي العقل المنطقي للتوسع الأمريكي²، تنامت القوة الاقتصادية والعسكرية الأمريكية وبدأت توسعها العالمي لكن مع مراعاة تحذيرات "ماهان" حول تجنب الصدام مع بريطانيا لذلك فقد كان لكل دولة مجالات النفوذ الخاصة بها والتي تحترمها الدولة الأخرى.

كانت الحرب العالمية الأولى فرصة كبيرة للولايات المتحدة لاختبار قوتها الاقتصادية والعسكرية فكانت هي الرابح الأكبر من الحرب، إذ أفل نظام التجارة الحرة البريطاني وضعفت الامبراطورية البريطانية وتلاشى تهديدها، ولم يُعق الهيمنة العالمية المطلقة للولايات المتحدة سوى الأزمة الاقتصادية لسنة 1929 والتي أجبت التنافس الجيوبوليتيكي من جديد بين القوى الطامحة للهيمنة إقليمياً وعالمياً وخلافة بريطانيا في قيادة العالم خاصة بين الولايات المتحدة وألمانيا، لذلك

¹ Saeid Naji, Jayum A. Jawan, "US Hegemonic Leadership and its Geopolitical Codes", *International Journal of Business and Social Science*, vol 2, n° 7, 2011, pp 149-157.

² Ibid.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

فالحرب العالمية الأولى حسب نموذج "مودولسكي" لم تكن قادرة على نقل القوة العالمية من القوة المهيمنة السابقة إلى القوة الجديدة¹، ورغم ذلك احتفظت الولايات المتحدة بالمبدأ الجيوبوليتيكي القائم على "العولمة وتوسيع النفوذ".

انتهت الحرب العالمية الثانية بتدمير أهم المنافسين الجيوبوليتيكيين للولايات المتحدة، وأصبحت الولايات المتحدة ذلك "المنتصر المهيمن" وشرعت في تشكيل النظام الدولي خدمة لمصالحها كما فرضت رؤيتها للنظام العالمي على أعدائها المنهزمين وحلفائها المُدَمَرين، لكن في مقابل ذلك امتد نفوذ الاتحاد السوفياتي إلى أوروبا الشرقية وألمانيا وبدأت مرحلة جديدة من النظام الجيوبوليتيكي العالمي أو ما عُرف بـ "الحرب الباردة".

تُعتبر الحرب الباردة نظاماً جيوبوليتيكياً بقوتين عظميين، الولايات المتحدة كقوة مهيمنة والاتحاد السوفياتي كمتحدٍ، لذلك كان لزاماً على الولايات المتحدة تعديل مبادئها الجيوبوليتيكية لتناسب مع الوضع الجيوبوليتيكي الجديد، وتظهر تلك المبادئ في الوثيقة NSC-68 لمجلس الأمن القومي الأمريكي للعام 1950 في عهد الرئيس "هاري ترومان"، حيث جاء في الوثيقة أن "هزيمة المؤسسات الحرة في أي مكان، هي هزيمة في كل مكان" والتفسير الجيوبوليتيكي لهذا الكلام هو أن "جميع مناطق العالم لها أهمية استراتيجية للولايات المتحدة"، كذلك حددت الوثيقة أعداء الولايات المتحدة حيث صرحت بأنه "لا يمكن التوفيق بيننا وبين النظام السوفياتي" وأن نفوذه يعرقل إقامة النظام الدولي، لتخلص بأن الصراع مع الاتحاد السوفياتي "يفرض علينا ولمصلحتنا مسؤولية قيادة العالم"²، وعليه فقد كان المبدأ الجيوبوليتيكي الأمريكي في الحرب الباردة واضحاً وهو "قيادة العالم" مع تحديد واضح للعدو وهو "الاتحاد السوفياتي" والحلفاء وهم "كل الدول والشعوب المؤيدة للمؤسسات الحرة"، كما سعت الإدارة الأمريكية لتبرير هذا المبدأ من خلال وصفها لسياساتها بأنها تعمل على "تعزيز بيئة عالمية تمكن النظام الأمريكي من أن ينمو ويزدهر"³.

إضافة إلى ما سبق، لم يخل الفكر الجيوبوليتيكي الأمريكي على صانع القرار بالأفكار الثاقبة والحلول المبتكرة، فالبرقية الطويلة لجورج كينان **Long Telegram of George Kennan**

¹ George Modelski, *op.cit.*

² **National Security Council**, NSC 68, United States Objectives and Programs for National Security, April 14, 1950, URL: <https://bit.ly/3x9izbx>.

³ George Modelski, *op.cit.*

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

أسست لفترة طويلة من العداء والصراع بين القوتين، كما وضعت قواعد سياسة الاحتواء والتي طبقتها الولايات المتحدة في مناطق الحافة أو "الريملاند **Rimland**" كما دعا لذلك "سيكمان" وفق مقولته المشهورة "من يتحكم في حافة الأرض يتحكم في أوراسيا، ومن يتحكم في أوراسيا يتحكم بمصير العالم"، كما أن دبلوماسية "كيسنجر" ومنع التقارب الصيني-السوفياتي أحبط كل محاولة لظهور قوة مهيمنة إقليمياً في أوراسيا وحافظ على التعددية الجيوبوليتيكية كما يصفها "بريجنسكي" معللاً بذلك "ضرورة الهيمنة الأمريكية".

مكنّت المبادئ والرؤى الجيوبوليتيكية الأمريكية من تحقيق فوز ساحق للولايات المتحدة على الاتحاد السوفياتي في الحرب الباردة، أو بتعبير الجيوبوليتيكا انتصار التالاسوكراتيا على التيلوروكراتيا، هذا الانتصار الذي عبر عنه "فوكوياما" بـ "نهاية التاريخ" مُلمحاً إلى أن العالم يتجه لأن يكون ليبرالياً، ديمقراطياً وحرّاً على الطريقة الأمريكية، ولعل حرب العراق أبانت عن قوة الولايات المتحدة في حشد الدول على اختلاف توجهاتها ومصالحها حولها كقائد للعالم، لكن في المقابل خلف انهيار النظام الجيوبوليتيكي للحرب الباردة فراغاً استراتيجياً كبيراً وفوضى عالمية، وفقد المبدأ الجيوبوليتيكي القائم على "مواجهة الشيوعية" مصداقيته، كما أن الاقتصاد المحلي الأمريكي لم يكن آداؤه مناسباً لمتطلبات مكانتها العالمية، لذلك فقد ظهر تناقض بين القيم المثالية التي تدعو إليها الولايات المتحدة ومصالحها الواقعية¹، وهو ما أفقد الهيمنة الأمريكية مبررات ومصادقية قيادتها للنظام الدولي الجديد الذي دعا إليه الرئيس بوش الأب، حيث إنتهى العقد الأخير من القرن الماضي على حالة من "الارتباك الاستراتيجي" لدى القادة الأمريكيين.

بدأ القرن الواحد والعشرون على وقع الفوضى والصراعات في الكثير من الدول، كما بدأ التهديد "الإرهابي" للعلن ما منح فرصة للولايات المتحدة لإستحضار طروحات "هنتجنتون" حول "صراع الحضارات"، كما سرعت أحداث 11 سبتمبر من وضع المبدأ الجيوبوليتيكي الجديد "الحرب على الإرهاب"، هذا المبدأ منح الولايات المتحدة مشروعية التدخل في كل منطقة من العالم بحجة مكافحة الإرهاب العالمي، كما أشتق منه مصطلح "الدول المارقة" والذي يُبرر للولايات المتحدة تحييد خصومها الدوليين المفترضين، أما التطبيق الأكثر أهمية هو تبرير زيادة وتطوير القوة العسكرية الأمريكية لضمان الهيمنة المطلقة.

¹ Saeid Naji, and Jayum A. Jawan, **op.cit.**

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

تغيرت الأولويات بعد 2011، فالرئيس "أوباما" دعا "للتحول نحو آسيا" في إشارة إلى التحديات الجيوبوليتيكية الجديدة التي تفرضها الصين، وكانت استراتيجية "إعادة التوازن إلى آسيا" إيداناً بتحول المصالح الأمريكية الأكثر أهمية نحو آسيا بعيداً عن المحور الأوروبي-الشرق أوسطي، هذا ما أكدته وسارت على نهجه إدارتي "ترمب" و"بايدن" إذ أصبح المبدأ الجيوبوليتيكي "المنافسة الاستراتيجية الشاملة مع الصين وروسيا" هو الناظم لعلاقات الولايات المتحدة مع دول العالم، سواء تعلق الأمر بحشد الحلفاء وضمان ولائهم، أو مهاجمة الأعداء وتحبيدهم تحت ذريعة أن النظام الدولي الليبرالي، الديمقراطي والحر يواجه تهديداً وجودياً من طرف الأنظمة الاستبدادية.

بناءً على ماسبق، فإن المبادئ الجيوبوليتيكية للولايات المتحدة في الفضاء السيبراني ماهي إلا انعكاس للمبادئ الجيوبوليتيكية في الفضاء المادي، فالوضع الحالي يشهد صراع قوتين عظميين في الفضاء السيبراني، الولايات المتحدة كقوة مخترعة ومهيمنة على الفضاء السيبراني والصين كقوة متحدية، لذلك فتُعتبر "الهيمنة في الفضاء السيبراني" هي المبدأ الجيوبوليتيكي الذي تسيّر وفقه التفاعلات الدولية للولايات المتحدة في الفضاء السيبراني، يُعزز ذلك ويُؤكد رؤية القيادة السيبرانية للولايات المتحدة المتمثلة في "بلوغ والمحافظة على التفوق في الفضاء السيبراني"¹ كهدف أسمى يساهم في استمرار قيادة الولايات المتحدة للعالم في الفضاء المادي.

المطلب الثاني: الفضاء السيبراني في المدرك الاستراتيجي الأمريكي

يُعتبر الإدراك ترجمة عقلية على أسس معرفية وقيمية للواقع، وينتج عنه رؤى محددة للسلوك تجاه الآخر من خلال تبني استراتيجية ما²، وعندما يمارس صناع القرار والاستراتيجيون هذه العملية العقلية في إطار استراتيجي لغرض فهم وتفسير واستشراف مآلات القضايا والمواقف الدولية فإنهم يمارسون ما يُعرف بالإدراك الاستراتيجي، وهو أسلوب تفكير عالي المستوى يُجيز لصاحبه التعامل بصورة صحيحة ومنطقية مع الموقف (الحافز) والمتغيرات المحيطة بالفاعل، بما يمكنه في النهاية من الموافقة والملاءمة بين الأهداف والوسائل³، كما يرى "رايموند كوهين" في مقاله حول "إدراك التهديد في الأزمة الدولية" إن إدراك التهديد هو المتغير الحاسم في الفعل ورد الفعل

¹ US Cyber Command, Vision 2018, april 2018, URL : <https://bit.ly/3QydfdT>.

² عادل البديوي، مرجع سابق، ص 25.

³ نعمة كاظم هاشم، العلاقات الدولية، ج1، بغداد: مطبعة إباد، 1979، ص 95.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

في الأزمات الدولية وإن عدم إدراك التهديد يمنع من حشد الجهود الدفاعية للدولة¹، فالبيئة الدولية الشديدة التعقيد والمتقلبة باستمرار تفرض على صناع القرار والاستراتيجيين ممارسة عملية الإدراك بصورة مستمرة ومتواصلة لمواكبة التغيرات الحاصلة بهدف اقتناص الفرص وتحييد التهديدات وحماية الأمن القومي للدولة وتعظيم مصالحها، وذلك من خلال الموازنة بين الأهداف والمصالح والقدرات والخيارات المتوفرة لصانع القرار مسترشدين ومُشكلين في نفس الوقت لـ "المدرك الاستراتيجي" للدولة حول قضية ما، والذي يُمثل ما ينطبع في ذهن القادة من تصورات وتوقعات مستقبلية كمحصلة نهائية لعمليات الإدراك المتواصلة حول قضية ما أو موقف معين.

بناءً على ما تقدم، سيتم فحص المدرك الاستراتيجي الأمريكي للفضاء السيبراني من خلال تحليل استراتيجية الأمن القومي والاستراتيجية السيبرانية الأمريكية والتصريحات الرسمية المتعلقة بهما، وتتبع مراحل تطوره من حل تقني لمشكلة استراتيجية في الردع النووي إلى هدية تقدمها الولايات المتحدة للعالم ووصولاً إلى أكثر المجالات التي يحدث فيها الصراع الجيوبوليتيكي حول الهيمنة العالمية، وذلك وفقاً لثلاث آليات تعمل على تشكيل المدرك الاستراتيجي للدول والتي تشمل: **المصالح والأهداف**، فلطالما كانت المصلحة القومية مبرراً ومشرعناً لأهداف الدولة ومقياساً عاماً للعوامل التي تدفع بها للتعاون أو الصراع مع غيرها من الدول²، الدور في النظام الدولي، والذي يُؤثر ويتأثر بالقيم الذاتية والاجتماعية لصانع القرار، **تفاعلات البيئة الاستراتيجية**، من خلال تحليل وفهم التفاعل بين البيئتين الداخلية والخارجية للدولة.

الفرع الأول: مصالح وأهداف الولايات المتحدة الأمريكية في الفضاء السيبراني

طوّرت وزارة الدفاع الأمريكية شبكات الفضاء السيبراني في ستينيات وسبعينيات القرن المنصرم كحل تقني لتحديد استراتيجي إبان الحرب الباردة، حيث كان الهدف منها ضمان الاتصال الدائم والموثوق بين مراكز القيادة الأمريكية في حالة ضربة نووية سوفياتية، وبعد نهاية الحرب الباردة كان الفضاء السيبراني كما هو معروف اليوم قد بدأ في التشكل من خلال النمو السريع للإنترنت وبروز شركات التكنولوجيا (القطاع الخاص) التي قادت التطور الرقمي المعاصر، وأعتقد صانعو القرار في الولايات المتحدة أن تقديم الإنترنت العالمي المفتوح -كهدية للعالم-

¹ Raymond Cohen, "Threat perception in international crisis", **Political Science Quarterly**, Vol 93, N° 1, 1978, pp 93-107.

² صبري مقلد، إسماعيل، **العلاقات السياسية الدولية: دراسة في الأصول والنظريات**، مرجع سابق، ص ص 22-23.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

يخدم المصالح الاستراتيجية والاقتصادية والسياسية المتعلقة بالسياسة الخارجية الأمريكية¹، حيث تُشير الاستراتيجية الوطنية لحماية الفضاء السيبراني لسنة 2003 إلى أن أنشطة التجارة والحكومة وإدارة الأمن القومي تعتمد بشكل متزايد على البنية التحتية للفضاء السيبراني وأن حماية هذه البنية ضروري لإقتصاد الولايات المتحدة وأمنها وأسلوب الحياة الأمريكي².

كشفت حرب الخليج الثانية والتدخلات العسكرية الأمريكية في مختلف القارات عن استخدام مفرط للتكنولوجيا المتطورة وتنسيق محكم بين القيادات والوحدات القتالية وكم هائل من المعلومات الاستخباراتية مُظهرة الدور الاستراتيجي والاعتمادية الكبيرة للقوات العسكرية الأمريكية بمختلف فروعها على الفضاء السيبراني لضمان التفوق العسكري، كما أن التجارة العالمية والمعاملات المالية والاقتصادية تحولت تدريجياً نحو العالم الرقمي، وأصبح الفضاء السيبراني العمود الفقري للعولمة الاقتصادية التي تدعو إليها الولايات المتحدة، وفي نفس السياق، وتزامناً مع العولمة الاقتصادية منح الفضاء السيبراني للساسة الأمريكيين آلية سهلة وفعالة للعولمة الثقافية ونشر القيم الأمريكية مثل الديمقراطية وحقوق الإنسان، ومحاربة ما تبقى من الإرث الشيوعي في دول العالم عبر تجاوز الأنظمة ومخاطبة الشعوب مباشرة.

وبناءً على ماسبق، فقد كان الهدف الأول لإدارتي "كلينتون" و"بوش الابن" هو "ضمان فضاء سيبراني حر ومفتوح" من خلال حماية البنية التحتية لهذا الفضاء، حيث صرح الرئيس "كلينتون" في لقاء مع مدراء شركات التكنولوجيا لمناقشة أمن الشبكات والحفاظ على انفتاح الأنترنت بـ "نحن نعلم أنه يتعين علينا إبقاء الفضاء السيبراني مفتوحاً وحرّاً"³، مع التركيز على بناء الجيل القادم من الأنترنت لضمان حماية البنية التحتية للفضاء السيبراني كما أكدت عليه الاستراتيجية الوطنية لحماية الفضاء السيبراني 2003 في عهد الرئيس "بوش الابن".

شهد العقد الأول من الألفية الثالثة تحولات متسارعة في الفضاء السيبراني، حيث تزايد اهتمام الحكومات بهذا الفضاء الجديد نتج عنها عمليات عسكرية للفضاء السيبراني تزايدت باطراد في العدد والشدة، وانعكس هذا على رؤية وإدراك القادة الأمريكيين، فغلبت المصالح الأمنية خاصة

¹ Adam Segal, **A New U.S. Foreign Policy for Cyberspace**, cfr.org, July 12, 2022, URL: <https://on.cfr.org/3DAmt1a>.

² **The White House**, National Strategy to Secure Cyberspace, Washington, 2003, URL: <https://bit.ly/3s0WOaR>.

³ John Schwartz, Ariana Eun Jung Cha, **Clinton Pledges to Help Industry Fight Hackers**, washingtonpost.com, February 16, 2000, URL: <https://wapo.st/3CyOVhI>.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

بعد الصراع السيبراني بين الصين وتايوان، ثم أحداث 11 سبتمبر وإعلان الرئيس "بوش الابن" الحرب على الإرهاب، ففي افتتاحيته لاستراتيجية الأمن القومي 2006 يقول الرئيس "بوش الابن" إن "أمريكا في حرب"¹، وبناءً على هذا التقييم للوضع الدولي فقد تم توجيه كل الجهود في الفضاء السيبراني لخدمة الأمن القومي، وكان الهدف الرئيس لإدارة "بوش الابن" هو حماية الأمن القومي من خلال اعتبار الفضاء السيبراني مجالاً جديداً للحرب وأداة لتقديم الدعم العسكري للقوات الأمريكية عبر تسخير عمليات واسعة لجمع المعلومات الاستخباراتية ومكافحة الإرهاب (المنظمات الإرهابية والدول المارقة) عبر الأنترنت.

مع تسلم إدارة "أوباما" السلطة ظهر جلياً الدور الذي يلعبه الفضاء السيبراني في خدمة المصالح الأمريكية في الداخل والخارج، ولا أدل على ذلك من أفراد الفضاء السيبراني بقسم خاص في استراتيجية الأمن القومي 2010 والتشديد على الأهمية البالغة للأمن السيبراني في استراتيجية الأمن القومي 2015، كما أعاد الرئيس "أوباما" التوازن في التركيز على المصالح الأمنية والاقتصادية والسياسية الأمريكية في الفضاء السيبراني، إذ جاء في الاستراتيجية الدولية للفضاء السيبراني 2011 الذي أقرها الرئيس "أوباما" أن "البنية التحتية الرقمية أصبحت بشكل متزايد العمود الفقري للاقتصادات المزدهرة ومجتمعات البحث المرموقة والجيش القوية والحكومات الشفافة والمجتمعات الحرة"²، كما حملت استراتيجية الأمن القومي 2010 اعتراف الولايات المتحدة بوجود دول أخرى معادية (منافسة) جعل من إدارة "أوباما" توجه مصالحها نحو العمل الدولي المشترك؛ أي دعوة دول العالم للعمل على تشكيل مستقبل الفضاء السيبراني المفتوح، المزدهر، الآمن والموثوق³، لكن للمفارقة، قوضت تسريبات "إدوارد سنودن" في 2013 تلك الدعاوات وأضررت بمكانة الولايات المتحدة كمداخلة عن حرية وأمن الأنترنت، يقول "أوباما" بأن "الطريقة التي حدثت بها هذه الإفصاحات كانت ضارة بالولايات المتحدة وضارة بقدراتنا الاستخباراتية"⁴، وأصبح الهدف الأول للرئيس "أوباما" هو إعادة بناء الثقة بين الحلفاء أولاً ثم مع بقية دول العالم، تلك الثقة التي اهتزت بصورة كبيرة.

¹ The White House, The National Security Strategy of the United States of America, Washington, March 2006, URL: <https://bit.ly/3D59rry>.

² The White House, International Strategy for Cyberspace Prosperity, Security, and Openness in a Networked World, op.cit.

³ Ibid.

⁴ James S. Brady, Press Conference by the President, obamawhitehouse.archives.gov, December 20, 2013, URL: <https://bit.ly/3EWFHb>.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

وصل الرئيس "ترمب" إلى البيت الأبيض في ظل تداول أخبار عن تدخلات خارجية في الانتخابات الرئاسية عبر الفضاء السيبراني، ففي ظل البروباغندا الروسية والتجسس السيبراني الاقتصادي الصيني والهجمات السيبرانية من دول أخرى مثل كوريا الشمالية وإيران أصبحت المصالح في الداخل الأمريكي مهددة، ولعل أبرزها الديمقراطية الأمريكية متمثلة في نظامها الانتخابي، كما ورثت إدارة "ترمب" تلك الصورة السيئة عن القيادة الأمريكية للفضاء السيبراني، حيث عزز منافسو الولايات المتحدة من قوتهم وتأثيرهم ما جعل الريادة الأمريكية في خطر، إذ أصبح ضمان التفوق والحفاظ على الريادة في الفضاء السيبراني مصلحة في حد ذاتها لصانع القرار الأمريكي، يُستدل على ذلك ورود كلمة "سايبير Cyber" 46 مرة في استراتيجية الأمن القومي 2017 التي أقرها الرئيس "ترمب" إضافة إلى سنّ الاستراتيجية السيبرانية الوطنية 2018 والتي جاءت بعد 15 سنة من سابقتها لعام 2003، والتي أكدت على "إنهم [الصين، روسيا] يرون أن الفضاء السيبراني ساحة يمكن فيها تحديد القوة العسكرية والاقتصادية والسياسية للولايات المتحدة، وإمكانية تعريض أمريكا وحلفائها وشركائها للخطر"¹، لذلك جاء الهدف واضحاً في استراتيجية الأمن القومي 2017 بعنوان بارز تحت بند الركيزة الأولى والتي تتضمن حماية المواطن، الأرض وطريقة الحياة الأمريكيين وهو "الحفاظ على أمريكا آمنة في العصر السيبراني"².

مثل سلفه، استهل الرئيس "بايدن" أيامه الأولى في البيت الأبيض على وقع اختراقات سيبرانية SolarWinds و Microsoft، وتعكس خطابات "بايدن"³ ووزير خارجيته "بليكن"⁴ واستراتيجية الأمن القومي 2022⁵ الصادرة في أكتوبر، مدى التهديدات الكبرى التي يُشكلها الفضاء السيبراني والأضرار التي يلحقها بالمصالح الإيديولوجية، الجيوبولوتيكية، التكنولوجية والدبلوماسية الأمريكية، وبشكل عام فإن النظام الدولي الليبرالي الحالي التي تقوده وتدافع عنه الولايات المتحدة أصبح يُعاني من تهديد وجودي بسبب المنافسة الاستراتيجية في الفضاء السيبراني خاصة من طرف الصين، إذ يعتقد الرئيس "بايدن" أنه "إذا انتهى بنا المطاف في حرب -حرب إطلاق نار حقيقية

¹ The White House, The National Cyber Strategy of the United States of America, Washington, September 2018, URL: <https://bit.ly/3zek9u3>.

² The White House, The National Security Strategy of the United States of America, Washington, December 2017, URL: <https://bit.ly/3Bx13kh>.

³ The White House, Remarks by President Biden on America's Place in the World, Washington, FEBRUARY 04, 2021, URL: <https://bit.ly/3Tma5H4>.

⁴ Antony J. Blinken, A Foreign Policy for the American People, US department of state, state.gov, MARCH 3, 2021, URL: <https://bit.ly/3gp2GYT>.

⁵ The White House, The National Cyber Strategy of the United States of America, Washington, October 2022, URL: <https://bit.ly/3eTqx2n>.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

مع قوة كبرى- فسيكون ذلك نتيجة لاختراق سيبراني ذي عواقب وخيمة"¹، لذلك تعددت أهداف الإدارة الأمريكية الحالية بين إعادة ديمقراطية الفضاء السيبراني وتعزيز الريادة التكنولوجية وتحديث بنية التعاون الدولي لمواجهة تحديات هذا القرن.

الفرع الثاني: مرتكزات البناء الفكري الاستراتيجي الأمريكي

يُعتبر البناء الفكري للقادة والاستراتيجيين آلية هامة في تشكيل المدرك الاستراتيجي للدول، وفي حالة الولايات المتحدة، فإن مزيجاً من العقيدة الدينية بمضمونها البروتستانتية-الكالفيني، والأفكار السياسية-الاقتصادية لعصر النهضة، لعبت دوراً حاسماً في تشكيل الشخصية الأمريكية² والمجتمع الأمريكي، وحددت أنماط التفاعل والتعامل مع وحدات النظام الدولي.

أ- **العقيدة الدينية:** كان الكثير من المهاجرين الأوائل إلى أمريكا يعتقدون العقيدة البروتستانتية-الكالفينية، وكان يُطلق عليهم **الطهوريون**³، حيث كان هدفهم الأسمى تطبيق تعاليم عقيدتهم في مجتمع جديد وأرض جديدة، لذلك فالآباء المؤسسون للولايات المتحدة سعوا لتكريس مبادئ عقيدتهم الدينية في بناء القيم والأفكار وقواعد السلوك في المجتمع الأمريكي، وكان لها بالغ الأثر في تكوين العقل الأمريكي ومنهج تفكيره الاستراتيجي على المستوى الدولي.

ترتبط العقيدة الطهورية بين الإيمان والعمل، إذ يُعتبر العمل دليلاً على إيمان الفرد، فالطهورية هي دين الفعل والجهد والعمل المنتج داخل الجماعة⁴، فالمال والثروة الناتجان عن العمل والانضمام إلى زمرة الأغنياء يرمز إلى احترام المبادئ الاجتماعية والدينية، كما أن الثراء يمكن أن يكون علامة على الإصطفاء الإلهي، لذلك كما يقول "توكفيل" المال والثروة يدخلان في صلب العقيدة الدينية التي بُني عليها المجتمع الأمريكي، فالناس عندما يجمعون المال والثروة فإنهم يسعون لمرضاة الله⁵.

¹ **The White House**, Remarks by President Biden at the Office of the Director of National Intelligence, Virginia, July 27, 2021, URL: <https://bit.ly/3z18gHj>.

² فهمي عبد القادر محمد، الفكر السياسي والاستراتيجي للولايات المتحدة الأمريكية: دراسة في الأفكار والعقائد ووسائل البناء الإمبراطوري، عمان: دار الشروق، 2009، ص 33.

³ الطهورية أو البيوريتانية **Puritanism**: هي مذهب مسيحي بروتستانتي يجمع خليطاً من الأفكار الاجتماعية، السياسية، اللاهوتية، والأخلاقية. ظهر هذا المذهب في إنجلترا في عهد الملكة إليزابيث الأولى وازدهر في القرنين السادس والسابع عشر، انظر: موسوعة **Britannica** على الرابط: <https://bit.ly/3qB7S1t>.

⁴ فهمي عبد القادر محمد، مرجع سابق، ص 35.

⁵ نفس المرجع.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

كما تدعو العقيدة الطهورية كذلك إلى محاربة الشر ونشر الخير، لذلك فمن واجب المؤمنين نشر تعاليم الله وتمدين الشعوب الأخرى ليشمل الخلاص لجميع البشر، هذه الرسالة التي تتضمن العمل لصالح الخير ومحاربة الشر هي الدافع الأساس للفكر التوسعي العالمي في الولايات المتحدة الأمريكية، يقول "توماس تومس" في كتابه "الماضي الخرافي للتوارة في التاريخ" أن ثمة قناعة راسخة لدى الأمريكيين مواطنين كانوا أو رؤساء بأن الدولة الجديدة (أي الولايات المتحدة) هي من اختيار الرب، وأن الشعب الجديد هو شعب الله الذي اختاره بعناية وفق خطة إلهية مدبرة للكون¹.

وتدليلاً على ماسبق، لا تكاد تخلو تصريحات المسؤولين الأمريكيين من الاستعارات والإيحاءات الدينية، فلا يخفى استخدام الدين في الحملات الانتخابية، ولا تخلو نصوص أداء اليمين للرؤساء الأمريكيين أبداً من الإشارة إلى شكر الرب، كما يستخدم الدين تحت مسمى محاربة الشر لتبرير حروب أمريكا، فالرئيس "ترومان" أيد استخدام القنبلة النووية ضد اليابان من خلال فكرة أن الرب قد أظهر انحيازه للولايات المتحدة ويقول: "إننا نشكر الرب، إنها وصلت إلينا ولم تصل إلى أعدائنا، وإننا ندعوه إلى إرشادنا لاستخدامها في سبيله"²، وتذهب تصريحات الرئيس "جورج بوش الابن" إلى أن ما قامت به أمريكا من غزو العراق وأفغانستان هو تنفيذ لـ "مهمة من الله" أو "رسالة الله" حيث يقول: "أنا مدفوع برسالة من الله" ويضيف "سيقول لي الله: جورج اذهب وحارب هؤلاء"³، كما أن وزراء الرئيس "ترمب" لا يخفون اعتقادهم بأن "ترمب" رئيس إختاره الله، فوزير الطاقة السابق "ريك بيرري" صرح بأن "ترمب اختاره الله" ووزير الخارجية السابق "بومبيو" قال بـ "أنه من المحتمل أن الله أرسل ترمب لإنقاذ إسرائيل"⁴، وعليه، فالعقيدة البروتستانتية-الكالفينية تحدد للقادة والاستراتيجيين الأمريكيين طرق ومناهج التفكير في الذات وفي الآخر، ومن ناحية الجيوبوليتيكا، منحت لهم إجابات عن الأسئلة الخمسة حول الأعداء والحلفاء وأعطتهم تبريرات لسلوكاتهم الخارجية أمام الجمهور داخلياً ودولياً.

¹ نفس المرجع، ص 37.

² فرانك لامبرت، الدين في السياسة الأمريكية: تاريخ موجز، تر: عبد اللطيف أبو البصل، الرياض: نمور للنشر، 2015، ص ص 120-121.

³ Ewen MacAskill, **George Bush: 'God told me to end the tyranny in Iraq'**, theguardian.com, October 7, 2005, URL: <https://bit.ly/3St8Fcn>.

⁴ Alex Johnson, **Pompeo suggests God sent Trump to save Israel**, nbcnews.com, March 22, 2019, URL: <https://nbcnews.to/3DqoOeo>.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

ب- أفكار عصر النهضة السياسية والاقتصادية: تعود جذور الفكر السياسي الأمريكي إلى الطروحات الفكرية والفلسفية التي سادت أوروبا في عصر النهضة، فقد حمل الوافدون الجدد على أمريكا أفكار توماس هوبز وجون لوك وجون جاك روسو حول الحرية الفردية والعقد الاجتماعي، فكان ترسيخ حرية الفرد في التملك والفكر والمعتقد بداية لتعزيز حرية السوق والمنافسة، كما أن العمل بمبدأ المساواة شكل فيما يُعرف اليوم بقيم الديمقراطية وحقوق الإنسان، فالأفراد أحرار ومتساوون في فرص العمل والتملك وطريقة التفكير والحياة مع احترام حرية الآخرين، وهذا ما ساهم في تشكيل الهوية الأمريكية من أفراد يتباينون تاريخياً وجغرافياً، فلا التاريخ ولا العرق ولا الجغرافيا تجمع الأمريكيين بل يجمعهم التنافس مدفوعاً بالمصلحة الذاتية.

ترسخت أفكار ومبادئ الحرية الفردية في الولايات المتحدة في القرن 18، حيث تشكل فكر سياسي-اجتماعي يتوافق مع تطورات المجتمع الأمريكي، كما أنتج لنا فكراً اقتصادياً جديداً، ساهم في تطوره المذهب البراغماتي الذي طوره كل من ويليام جيمس وتشارلز ساندروز بيرس، كما كانت الحرب الأهلية بين الشمال الرأسمالي الصناعي والجنوب الرأسمالي الزراعي وانتصار الشمال في الحرب نقطة تحول محورية للمجتمع الأمريكي، حيث سادت أخلاقيات وقيم الطبقة الصناعية الصاعدة حول الربح وجني المال الواسع والمخاطرة، وانعكس هذا على القيم وقواعد السلوك في المجتمع الأمريكي، وأصبحت الحرية الفردية تعني العمل الجاد والتضحية وأحياناً المكر والخداع بغية جني المال والأرباح.

ظهر بعد هذا التحول الشركات الصناعية الكبرى والاحتكارية وانحصر مبدأ حرية المنافسة، وتحولت أمريكا إلى عالم يحكمه رجال المال والأعمال في السياسية والاقتصاد، وأصبح كبار الصناعيين هم الطبقة السياسية السائدة حيث عبروا عن الطموحات التوسعية الأمريكية داخل وخارج الولايات المتحدة وعن قيمها وأخلاقياتها، يقول السيناتور "البرت بيفريدج": "نحن الأنجلوساكسون يتعين علينا أن نلتزم بما يفرضه علينا دمننا ونحتل أسواقاً جديدة وأراض جديدة إذا لزم الأمر"، يؤكد هذه النظرة التوسعية ما يعتقده الرئيس "ثيودور روزفلت" بأن "أمركة العالم هي مصير وقدّر أمتنا"¹.

¹ فهمي عبد القادر محمد، مرجع سابق، ص 60.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

الفرع الثالث: تفاعلات البيئة الاستراتيجية للفضاء السيبراني

لم يمثل الفضاء السيبراني في بداية تشكله مشكلة أو تهديداً استراتيجياً للقادة الأمريكيين، ذلك أن نشوة النصر على الاتحاد السوفياتي والانفراد بقيادة العالم جعلهم يعتبرونه -حتى السنوات الأولى من الألفية الجديدة- أداة أو وسيلة ضمن ترسانة نشر قيم ومبادئ الولايات المتحدة في العالم، وكان التحدي الوحيد هو كيفية محاربة الجريمة السيبرانية سواء كانت من الأفراد أو المجموعات، واقتصر دور الولايات المتحدة كمخترع ومدير للفضاء السيبراني في الحفاظ عليه آمناً مع السعي نحو توسيع الشبكات وضمان وصولها لكل شعوب العالم.

بعد إعلان الرئيس "بوش الابن" الحرب على الإرهاب، أصبح الفضاء السيبراني بيئة تحمل تهديدات أمنية متزايدة، فإضافة إلى المنظمات الإرهابية التي تنشط على الأنترنت، زاد اهتمام الدول بهذا الفضاء وتحول شيئاً فشيئاً إلى ساحة للنزاعات والصراعات بين الفواعل المختلفة دولاً كانت أو غير دول، ورغم أن البيئة الاستراتيجية العالمية كانت توحى بهيمنة أمريكية واضحة وعلاقات تعاونية لكل من روسيا والصين وهو ما تُشير إليه **استراتيجية الأمن القومي 2002**¹، إلا أن هجومات روسيا السيبرانية على كل من استونيا في 2007 وجورجيا في 2008 وما كشفت عنه التحقيقات من عمليات تجسس صينية منذ بداية الألفية الجديدة² جعل من الفضاء السيبراني ساحة حرب جديدة تسعى الدول فيها لتصفية حساباتها مع خصومها دون الوصول إلى عتبة الصراع المسلح، أو ما يُطلق عليه **"المنطقة الرمادية"**، وبالنسبة للولايات المتحدة فقد سعت لحماية موقعها الريادي في الفضاء السيبراني من خلال تسخير لخدمة الأمن القومي من جهة، والدعوة لحوكمة الأنترنت وفق نموذج يضمن سيطرة الشركات التكنولوجية الأمريكية.

لكن مع تزايد القوة السيبرانية للدول وانخراطها في صراعات متباعدة في الشدة والتواتر في الفضاء السيبراني، حدث انقسام حول كيفية حوكمة الأنترنت، وبرز معسكران برؤيتين متضاربتين، فرغم دعوة **"أوباما"** لدول العالم للمشاركة في صنع مستقبل الفضاء السيبراني تطبيقاً لسياسة **"القيادة من الخلف"** إلا أن هجومات ستكاسنات **Stuxnet** على أجهزة الطرد المركزي الإيرانية

¹ **The White House**, The National Security Strategy of the United States of America, Washington, September 2002, URL: <https://bit.ly/3DbdTnw>, pp 26-28.

² كشف مخبر الأمن الإلكتروني كاسبرسكي في 2013 عن عملية واسعة للتجسس باستخدام أدوات تجسس متقدمة تستهدف المؤسسات الدبلوماسية والحكومية، وأطلق عليها اسم **"أكتوبر الأحمر Red October"** واتهم فيها مخترقون صينيون، وقدر الخبراء أن نشاطهم كان منذ سنة 2007 انظر: <https://bit.ly/3suEp6v>.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

وتسريبات سنودن حول برامج التنصت لوكالة الأمن القومي الأمريكية NSA سرع وتيرة تكوين الجيوش ووحدات الدفاع والهجوم السيبرانية في كل دول العالم، وأصبح الفضاء السيبراني ساحة حرب حقيقية، وتم إنشاء القيادة السيبرانية للولايات المتحدة USCYBERCOM في 2010 للدفاع عن المراكز والأنظمة الاستراتيجية للقوة الوطنية، وتم الاعتراف بأن الفضاء السيبراني بيئة استراتيجية يُنظر إلى سلوك الخصوم فيه على أنه ذو تأثير استراتيجي مهم¹.

بدأت ملامح البيئة الاستراتيجية للفضاء السيبراني في التجلي مع مقاربة "المنافسة الاستراتيجية الشاملة" التي جاء بها الرئيس "ترمب"، حيث عبّرت استراتيجية الأمن القومي 2018 عن عودة التنافس بين القوى العظمى وأن "الصين وروسيا بدأت في إعادة تأكيد نفوذهما الإقليمي والدولي ... إنهم ينافسوننا في ميزتنا الجيوبوليتيكية ويحاولون تغيير النظام الدولي لصالحهم"²، إضافة إلى أن "العديد من الدول اليوم ينظر إلى القدرات السيبرانية كأدوات لإظهار القوة، والبعض منهم يستعمل أدوات سيبرانية لحماية ونشر أنظمتهم الاستبدادية"³، كما تؤكد الاستراتيجية السيبرانية الوطنية للولايات المتحدة 2018 على أن عصرًا جديدًا من المنافسة الاستراتيجية قد بدأ، وأن "الإدارة [أي إدارة ترمب] انخرطت في منافسة مستمرة ضد خصوم استراتيجيين [الصين وروسيا]، دول مارقة [إيران وكوريا الشمالية]، إرهابيين ومجرمي الشبكات"⁴، وعليه فلم تصبح مهمة "ترمب" ومن بعده "بايدن" الدفاع على الولايات المتحدة فحسب، بل الدفاع على النظام الدولي الليبرالي الذي تُديره ضد تهديدات من فاعلين متباينين في بيئة استراتيجية جديدة شديدة التعقيد وسريعة النقلب هي الفضاء السيبراني.

المطلب الثالث: الاستراتيجيات الأمريكية للنموذج في الفضاء السيبراني

تتبنى الاستراتيجية السيبرانية في الغالب من الاستراتيجية الكبرى للدولة وتتداخل معها وتخدمها، وفي حالة الولايات المتحدة فقد كانت استراتيجيتها الكبرى تُركز على احتواء قوة الاتحاد السوفياتي خلال الحرب الباردة، لكن بروز الفضاء السيبراني كحقل جديد للتفاعل والصراع ترافق

¹ جاءت هذه المقاربة في وثيقة لمجموعة العمل المشتركة بين القيادة السيبرانية الأمريكية USCyberCom ووكالة الأمن القومي NSA بتاريخ 2013/02/26 وتم رفع السرية عنها في 2018/12/20 انظر الرابط: <https://bit.ly/3SBZpCP>.

² The White House, The National Security Strategy of the United States of America, Washington, December 2017, URL: <https://bit.ly/3Bx13kh>, p 27.

³ Ibid, p 31.

⁴ The White House, The National Cyber Strategy of the United States of America, Washington, September 2018, URL: <https://bit.ly/3zek9u3>, p 2.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

مع حالة من الارتباك الاستراتيجي خاصة مع انهيار المعسكر الشرقي وغياب عدو واضح، لذلك جاءت استراتيجية مكافحة الإرهاب مع بدايات القرن الحالي لتسد الفراغ، لكن عودة المنافسة بين القوى الكبرى في العقد الثاني من القرن الحادي والعشرين كما يرى "جوزيف ناي الابن"¹ منح الولايات المتحدة من جديد ميزة التركيز على التهديدات الرئيسية لأمن أمريكا واقتصادها وقيمها، لذلك فقد جاءت الاستراتيجيات السيبرانية الأمريكية لتعكس التحديات الایدولوجية، الجيوبوليتيكية، التكنولوجية والدبلوماسية لرؤية صانع القرار الأمريكي الشاملة للسياسة الخارجية والأمن القومي الأمريكي.

من جهة أخرى، ووفق منظور جيوبوليتيكي فإن القراءة الأولية للوثائق المتعلقة بالاستراتيجية الأمريكية في الفضاء السيبراني وفحص تصريحات المسؤولين والمفكرين الأمريكيين في السياق ذاته، تُقدم لنا توجيهين رئيسيين، يُركز التوجه الأول على بناء استراتيجيات للدفاع في الفضاء السيبراني والهدف الاستراتيجي منها هو تعزيز النفوذ في الفضاء السيبراني، أما التوجه الثاني فيدعو لتطبيق الاستراتيجية الكبرى للولايات المتحدة في الفضاء السيبراني في بيئة استراتيجية تشهد منافسة بين القوى العظمى والهدف الاستراتيجي هو السيطرة على الفضاء السيبراني.

بناءً على ما تقدم، يتم في هذا المطلب تحليل استراتيجيات الأمن القومي في جانبها المتعلق بالفضاء السيبراني واستراتيجيات الفضاء السيبراني الأمريكية والوثائق والتصريحات الرسمية المتعلقة بها للوقوف على مدى سعي الولايات المتحدة الأمريكية لتعزيز وتثبيت نفوذها في الفضاء الرقمي، وذلك من خلال التطرق إلى مدى وضوح رؤية صانع القرار الأمريكي حول التحديات الجيوبوليتيكية في الفضاء السيبراني، الأهداف، الوسائل و مدى الملاءمة بين الأهداف والوسائل من خلال السياسات السيبرانية المتبعة.

تتميز الولايات المتحدة الأمريكية بتعدد الجهات المسؤولة عن حماية الفضاء السيبراني والدفاع عنه، وهذا يرجع في الأساس إلى طبيعة هذا الفضاء الذي يتغلغل في جميع مناحي الحياة، لذلك فإننا نواجه تواجد العديد من الفاعلين الذين يطورون استراتيجيات للفضاء السيبراني خاصة بهم، على عكس استراتيجية الأمن القومي التي تصدر فقط عن البيت الأبيض وتعكس رؤية الإدارة الأمريكية المنتخبة، وعليه، سيتم التركيز على أهم الوثائق المتعلقة بالفضاء السيبراني

¹ Joseph S Nye Jr, **America's strategy towards the new superpower**, project-syndicate.org, Aug 3, 2021, URL: <https://bit.ly/3B6uN6R>.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

الصادرة عن الهيئات الأمريكية (البيت الأبيض، وزارة الدفاع، وزارة الأمن الداخلي، القيادة السيبرانية الأمريكية) التي تحمل في عنوانها مصطلح "استراتيجية" كآلاتي:

جدول رقم 07: وثائق الاستراتيجيات الخاصة بالفضاء السيبراني لأهم الهيئات الأمريكية.

المصدر: من إعداد الباحث.

الرقم	الهيئة	عنوان الوثيقة	سنة الاصدار
01	البيت الأبيض White House	الاستراتيجية الوطنية لتأمين الفضاء السيبراني	2003
03		الاستراتيجية الوطنية للحماية المادية للبنى التحتية الحرجة والأصول الرئيسية	2003
03		الاستراتيجية الدولية للفضاء السيبراني	2011
04		الاستراتيجية السيبرانية الوطنية	2018
05	وزارة الدفاع DoD	استراتيجية وزارة الدفاع للعمل في الفضاء السيبراني	2011
06		الاستراتيجية السيبرانية لوزارة الدفاع	2015
07		الاستراتيجية السيبرانية لوزارة الدفاع	2018
08		استراتيجية "الثقة المكدومة" لوزارة الدفاع	2022
09	وزارة الخارجية DoS	استراتيجية السياسة الدولية للفضاء السيبراني	2016
10	القيادة السيبرانية CyberCOMM	بلوغ والحفاظ على التفوق في الفضاء السيبراني	2018

من خلال قراءة ديباجة الاستراتيجيات الأربع الخاصة بالفضاء السيبراني الصادرة عن البيت الأبيض والتي يمضيها الرئيس باعتباره أعلى سلطة في البلاد -على فرض أن باقي الهيئات الرسمية لها نفس التوجهات- وتحليلات الباحثين¹ يمكن رصد ثلاثة استراتيجيات متباينة مرت بها عمليات تطوير الاستراتيجية الأمريكية للفضاء السيبراني مقسمة حسب الإدارات الرئاسية المتعاقبة، أولاً، استراتيجية الحماية والدفاع عن الفضاء السيبراني والتي ميزت فترة حكم الرئيسين "كلينتون" و"بوش الابن"، ثانياً، استراتيجية الردع التي رافقت إدارة "أوباما"، ثالثاً، استراتيجية

¹ انظر: بافال شاريكوف، تطور السياسات الأمريكية للأمن السيبراني، مجلة الاقتصاد العالمي والعلاقات الدولية، على الرابط: <https://bit.ly/3FpPE7E>. شتيفان سيونسنتو، تطور استراتيجية الدفاع الأمريكية في الفضاء السيبراني (1988-2019)، مركز دراسات الأمن زيورخ، على الرابط: <https://bit.ly/3F6nSvG>، فالنتين فيير، الترابط بين الاستراتيجية السيبرانية والاستراتيجية الكبرى: حالة الولايات المتحدة، مجلة السياسة السيبرانية، على الرابط: <https://bit.ly/3FpZpYc>.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

الدفاع إلى الأمام أو ما يُطلق عليه "المثابرة السيبرانية" والتي جاء بها "ترمب" وتسير على نهجها إدارة "بايدن".

الفرع الأول: استراتيجية تأمين والدفاع عن الفضاء السيبراني

جاءت "الاستراتيجية الوطنية لتأمين الفضاء السيبراني 2003" و "الاستراتيجية الوطنية لحماية المادية للبنى التحتية الحرجة والأصول الرئيسية" كجزء من الجهود العامة لحماية الولايات المتحدة الأمريكية، وكعنصر تنفيذي للاستراتيجية الوطنية للأمن الداخلي، إذ صدرتا في وقت شهدت فيه الولايات المتحدة تغييرات استراتيجية في عهد الرئيس "بوش الابن" حيث أصبحت التهديدات الإرهابية أولوية للأمن القومي، فهجوم الحادي عشر من سبتمبر جعل المسؤولين الأمريكيين مطالبين ببذل المزيد من الجهود لحماية الحدود والمرافق الحيوية داخل البلاد، وعليه قامت إدارة "بوش الابن" بدمج قضايا الأمن السيبراني في جدول الأعمال الخاص بسياسة الأمن القومي ومكافحة الإرهاب، وأصبحت حماية البنية التحتية الحيوية أولوية قصوى.

من جهة أخرى، صدرت الاستراتيجيتان في خضم توترات حادة وتعارض كبير بين الطبيعة الفوضوية للفضاء السيبراني والبعيدة عن كل سيطرة أو تحكم مركزي، والرغبة الملحة للحكومة الأمريكية في فرض سلطتها وتحقيق جهودها الرامية لتأمين الفضاء السيبراني، وعليه فمن خلال وثيقتي الاستراتيجيتين يمكننا استخلاص التحديات الجيوبوليتيكية، الأهداف والوسائل والسياسات التي تضمنتها والتي من خلالها يظهر التوجه العام للإدارة الأمريكية في عهد الرئيس "بوش الابن" تجاه قضايا الفضاء السيبراني.

1. التحديات الجيوبوليتيكية: أقرت "الاستراتيجية الوطنية لتأمين الفضاء السيبراني" في ديباجتها أن تأمين الفضاء السيبراني يُعد تحدياً استراتيجياً صعباً للغاية، إلا أنها لم تسمي مباشرة أي أطراف أو دول بعينها، بل جاء الوصف عاماً "الجهات الفاعلة الخبيثة" ثم يُفصل لاحقاً في متن الوثيقة بعبارة "مجرمي الأنترنت، الإرهابيين والدول القومية"، أما "استراتيجية حماية البنية التحتية" فتحصر العدو في الإرهابيين، هذا الغموض في تحديد مصادر التهديد يرجع في الأساس إلى طبيعة الفضاء السيبراني وخاصية المجهولية التي تسمح للمهاجم بالتخفي، إضافة إلى أنها تتوافق مع ما جاءت به استراتيجية الأمن القومي 2002 من تحديات جيوبوليتيكية حيث وردت مصطلحات مثل: الإرهاب والدول المارقة، إضافة إلى أن هذا الغموض المتعمد

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

يمنح الإدارة الأمريكية حرية ومرونة كبيرة في المناورة لتحديد فاعل ما أو عدة فواعل على أنهم "أعداء لأمريكا".

2. **الأهداف:** قدمت "الاستراتيجية الوطنية لتأمين الفضاء السيبراني" إطار عمل لحماية البنية التحتية الحيوية الضرورية لاقتصاد، أمن و أسلوب الحياة الأمريكي، وكان الهدف العام منها هو بناء مستقبل أكثر أماناً في الفضاء السيبراني. وجاءت الأهداف الاستراتيجية المسطرة لها منسجمة مع الاستراتيجية الوطنية للأمن الداخلي، وانقسمت إلى ثلاثة (03) أهداف استراتيجية رئيسية هي¹:

- منع الهجمات السيبرانية ضد البنى التحتية الحيوية في أمريكا.
 - تقليل تعرض الولايات المتحدة للهجمات السيبرانية.
 - تقليل الأضرار ووقت التعافي من الهجمات السيبرانية التي تحدث.
- إضافة إلى خمس (05) أولويات وطنية حاسمة في الفضاء السيبراني هي²:

- نظام وطني للاستجابة لأمن الفضاء السيبراني.
- برنامج وطني للتهديد في مجال الأمن السيبراني والحد من نقاط الضعف.
- برنامج وطني للتدريب والتوعية بأمن الفضاء السيبراني.
- تأمين الفضاء السيبراني للحكومة.
- الأمن القومي والتعاون الدولي لأمن الفضاء السيبراني.

وعليه، فإن أهداف "الاستراتيجية الوطنية لتأمين الفضاء السيبراني" ركزت على تأمين الفضاء السيبراني في الداخل الأمريكي وهو ما تفصله "استراتيجية حماية البنية التحتية الحرجة" وجاء ترتيب التعاون الدولي في آخر الأولويات.

3. **الوسائل:** يمكن اعتبار وزارة الأمن الداخلي DHS التي أنشأت في مارس 2003 في أعقاب إقرار الكونغرس الأمريكي قانون الأمن الداخلي في نوفمبر 2002 من أهم الهيئات التي أوكل إليها مهمة تأمين البنية التحتية الحيوية والفضاء السيبراني في الولايات المتحدة، حيث إنها تجمع أكثر من 22 وزارة ووكالة فيدرالية في هيئة واحدة أكثر فعالية وتكاملاً، مما يخلق بيئة

¹ The White House, National Strategy to Secure Cyberspace, op.cit, p VIII.

² Ibid, p X.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

أمنية معززة وأكثر استعداداً لمواجهة التهديدات¹ وحماية البنية التحتية الحيوية من خلال التنسيق بين القطاعين العام والخاص.

إضافة إلى ذلك، استحدثت استراتيجيتا تأمين الفضاء السيبراني وحماية البنية التحتية للعام 2003 العديد من البرامج والآليات لتطوير التعاون بين القطاعات وتعزيز وتحسين قدرتها على تأمين الفضاء السيبراني، إلا أن منتقدي هذه الاستراتيجية -خاصة خبراء الأمن- والراغبين في سيطرة كلية وقوية للحكومة على الفضاء السيبراني قللوا من جدوى هذه البرامج والآليات، إذ يُعلق "ساندي كيندال" بأن نظرة سريعة على الملخص التنفيذي للاستراتيجية والتدابير الواجب إتخاذها يخلص إلى أن أفعالاً مثل: تعزيز، تشجيع و فهم يفوق عددها بكثير الأفعال مثل: توفير، تأمين، إنشاء أو [يُضيف ساخراً] لا سمح الله تمويل².

4. السياسات السيبرانية وتأثيرها الاستراتيجي :

تظهر فعالية "الاستراتيجية الوطنية لتأمين الفضاء السيبراني 2003" و"الاستراتيجية الوطنية للحماية المادية للبنى التحتية الحرجة والأصول الرئيسية" من خلال السياسات والتكتيكات والسلوكات الأمريكية المختلفة في الفضاء السيبراني، يجادل "كولين س. غراي" في كتابيه حول الاستراتيجية "The Strategy Bridge: Theory for Practice" و "The Future of Strategy" بأن "التكتيكات تدور حول الفعل، القيام بالأشياء، بينما الاستراتيجية تدور حول عواقب السلوك التكتيكي"³ كما أن "التأثير الاستراتيجي يتجلى في التصورات والاحكام والاختيارات السلوكية للأعداء والحلفاء"⁴ وهذا ما يمنح الدولة ميزة أو عيباً استراتيجياً، وعليه فسياسات وسلوك الولايات المتحدة في الفضاء السيبراني أنتج تأثيرات استراتيجية في العديد من المجالات.

أ. في المجال العسكري:

كانت الولايات المتحدة سباقة في استعمال الفضاء السيبراني لدعم عملياتها العسكرية، يشرح "ريتشارد كلارك" في كتابه "حرب الفضاء الإلكتروني" كيفية استعمال جيش الولايات

¹ Department of Homeland Security, Creation of the Department of Homeland Security, dhs.gov, URL: <https://bit.ly/3iSmXHC>.

² Sandy Kendall, Did the National Strategy for Securing Cyberspace Wimp Out?, csoonline.com, FEB 24, 2003, URL: <https://bit.ly/3iQSOIC>.

³ Weber, Valentin, Op.cit.

⁴ Colin S Gray, The strategy bridge: theory for practice, Oxford: Oxford University Press, 2010, p 172.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

المتحدة لعمليات الاختراق الالكترونية في حروبه على العراق وكيف تعلم الاسرائيليون منهم وطبقوا ذلك في هجماتهم على المنشآت السورية¹، كما أن توجيهات إدارة الرئيس "بوش" السرية للحكومة بوضع إرشادات لتحديد متى وكيف ستشن الولايات المتحدة هجمات سيبرانية على الكمبيوترات المعادية² ومحاولات تشكيل قيادة موحدة للفضاء السيبراني أسفرت عن هجوم كبير على المنشآت النووية الإيرانية والذي عرف بـ "ستاكسنت".

هذه السياسات والتكتيكات الأمريكية غيرت من معايير سلوك الدول في الفضاء السيبراني، كما حفزت العديد من الحكومات على زيادة نفوذها وسيطرتها على هذا الفضاء بزيادة الإنفاق على القدرات السيبرانية، هذا ما أطلق موجة كبرى من الهجمات والتهديدات السيبرانية أُصطلح على تسميتها بـ "الحرب السيبرانية" لعل أبرز أمثلتها: الهجمات السيبرانية الروسية على استونيا 2007، وعلى جورجيا 2008، لقد كان لسلوك الولايات المتحدة الأمريكية في الفضاء السيبراني خلال فترة حكم الرئيس "بوش" الدور الأبرز في بداية عمليات عسكرة الفضاء السيبراني.

ب. في المجال الاقتصادي:

أنشأت الحكومة الأمريكية الأنترنت (الفضاء السيبراني) ما منحها ميزة قوية للسيطرة على البنية التحتية الحيوية وسيطرة على القواعد والمعايير التي تحكمها، ثم توسعت نحو القطاع الاقتصادي ففي عهد الرئيس "كلينتون" جرت عمليات خصخصة الأنترنت بدعم وتمويل من الحكومة نفسها، يظهر ذلك في الدعم والتمويل الذي تلقته كل من شركتي Google و Apple³، هذه البيئة الداخلية التمكينية تم تعزيزها بسياسة الأسواق المفتوحة والتجارة الحرة نحو الخارج تماشياً مع النظام الليبرالي الذي تروج له الولايات المتحدة، وكانت نتيجة هذه السياسات ظهور شركات تقنية كبرى تعدى تأثيرها الداخل الأمريكي لتصبح لاعباً جيوبوليتيكياً رئيساً على الساحة الدولية، ومنحت الولايات المتحدة تفوقاً وميزة استراتيجية اقتصادية وعسكرية عالمية.

ج. في المجال السياسي:

دعمت استراتيجيتا التأمين والحماية للعام 2003 سياستين بارزتين، أولاً، أدت الدعوة للتعاون بين القطاع العام والخاص والمواطنين لتأمين وحماية الفضاء السيبراني إلى ظهور

¹ Richard Clarke, Knake Robert, **Op.cit**, pp 23-26.

² Bradley Graham, **Bush Orders Guidelines for Cyber-Warfare**, washingtonpost.com, February 7, 2003, URL: <https://bit.ly/3PgKVZf>.

³ Valentin Weber, **Op.cit**.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

مقاربة أصحاب المصلحة المتعددين والتي دعت إليها ودافعت عنها -وتتبنها حتى اليوم- الولايات المتحدة على المستوى الدولي من أجل حوكمة الأنترنت في مؤتمر القمة العالمية لمجتمع الأنترنت WSIS جنيف 2003 وتونس 2005، في مقابل مقاربة السيادة السيبرانية التي دعت لها روسيا والصين، ثانياً، سياسة التدفق الحر للمعلومات أو حرية الأنترنت والتي تمنح الولايات المتحدة ميزة استراتيجية كبرى في سعيها لنشر الديمقراطية وتشجيع الانفتاح السياسي والاقتصادي في دول المعسكر الاشتراكي السابقة.

وتلخيصاً لما سبق، يُمكن القول أن استراتيجيتي التأمين والحماية للعام 2003 قننت وشرعن عود الدولة للسيطرة وبسط النفوذ في الفضاء السيبراني خدمة لمصالحها السياسية، العسكرية والاقتصادية، وتم ذلك من خلال تشجيع ودعم شركات التكنولوجيا الأمريكية للتوسع عبر العالم بذريعة حرية الأنترنت من جهة، ومن جهة أخرى تم بسط نفوذ الحكومة الأمريكية (سياسيين وعسكريين) على هذه الشركات ومن ثم بسط النفوذ في الفضاء السيبراني.

الفرع الثاني: استراتيجية الردع

وصل الرئيس "أوباما" إلى الحكم في خضم بيئة استراتيجية للفضاء السيبراني شديدة التعقيد، حيث إن العديد من الدول طورت قدراتها السيبرانية وشكلت وحدات خاصة للدفاع والهجوم السيبراني، ولم يعد تأمين الفضاء السيبراني الداخلي كافياً إذ أصبح الفضاء السيبراني ساحة حرب جديدة بين الدول، كما تميزت فترة حكم "أوباما" بحدثين بارزين غير الكثير من المفاهيم في الفضاء السيبراني هما: هجوم فيروس "ستاكسنت" في 2010 وتسريبات "سنودن" في 2013، لذلك أصدرت الهيئات الأمريكية على اختلاف مستوياتها استراتيجيات خاصة بالفضاء السيبراني، إذ أصدر البيت الأبيض "الاستراتيجية الدولية للفضاء السيبراني" في 2011، كما أصدرت وزارة الدفاع "استراتيجية وزارة الدفاع للعمل في الفضاء السيبراني" في 2011 و"الاستراتيجية السيبرانية لوزارة الدفاع" في 2015، إضافة إلى "استراتيجية السياسة الدولية للفضاء السيبراني" التي أصدرتها وزارة الخارجية في 2016.

1. التحديات الجيوليتيكية:

لم تحدد "استراتيجية البيت الأبيض 2011" ولا "استراتيجية وزارة الدفاع 2011" تحديات جيوليتيكية بعينها، بل جاءتا لتصف مجموعة من التحديات التقنية مثل الكوارث الطبيعية،

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

الحوادث أو التخريب¹ وأحياناً تقدم تعميماً لخصوم أمريكا مثل الحكومات الأجنبية، المجموعات الإرهابية ومجرمي الأنترنت²، إلا أن "استراتيجية وزارة الدفاع 2015" و "استراتيجية وزارة الخارجية 2016" حددت بوضوح مجموعة من الدول والكيانات كتهديد جيوبوليتيكي للولايات المتحدة، حيث صنفت "استراتيجية وزارة الدفاع 2015" الصين وروسيا كتهديد خطير إضافة إلى إيران وكوريا الشمالية اللتان تُظهران سلوكاً عدائياً للولايات المتحدة في الفضاء السيبراني مع اعتبار تنظيم داعش الجهة غير الحكومية الوحيدة التي تشكل تهديداً رئيساً بسعيها لاكتساب قدرات سيبرانية³، وأكدت على هذا "استراتيجية وزارة الخارجية 2016" حيث اعتبرت أن الصين وروسيا هما الدولتان الأكثر سعياً لتقديم رؤى بديلة لاستقرار الفضاء السيبراني كما تسعيان لحشد بقية الدول ضمن رؤيتهما التعديلية⁴.

2. الأهداف:

تُجمع الاستراتيجيات الأربع على ضرورة العمل دولياً مع الحلفاء والشركاء على ضمان بنية تحتية للمعلومات والاتصالات **منفتحة وقابلة للتشغيل المتبادل وأمنة وموثوقة** تدعم التجارة الدولية، وتعزز الأمن الدولي، وتضمن حرية التعبير والابتكار، من جهتها، فإن وزارة الدفاع DoD ومع التزامها بأنترنت مفتوح وآمن، حددت خمسة أهداف استراتيجية هي:

1. بناء قوات وقدرات سيبرانية جاهزة للعمليات في الفضاء السيبراني.
2. حماية شبكات وزارة الدفاع، والبيانات وتقليل المخاطر السيبرانية.
3. الدفاع عن الوطن الأمريكي ومصالحة الحيوية.
4. بناء خطط وخيارات للتحكم في تشكيل وتصعيد الصراعات في الفضاء السيبراني.
5. بناء وتقوية التحالفات والشراكات الدولية لردع التهديدات في الفضاء السيبراني.

جاءت هذه الأهداف كرد فعل على تسارع عمليات عسكرة الفضاء السيبراني، ومحاولة بعض الدول (خاصة الصين وروسيا) تبني ونشر مفاهيم "السيادة السيبرانية" وبناء فضاء سيبراني

¹ **The White house**, International strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World, **op.cit**, p 04.

² **Department of Defense**, Department of Defense Strategy for Operating in Cyberspace, July 2011, p 03, URL: <https://bit.ly/3HVvswb>.

³ **Department of Defense**, Department of Defense Cyber Strategy, April 2015, p 09, URL: <https://bit.ly/3FzcyZ5>.

⁴ **Department of State**, Department of State International Cyberspace Policy Startegy, March 2016, pp 16-18, URL: <https://bit.ly/3Wkbzm9>.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

خاص بها مما يؤدي إلى تفتيت "بلقنة" الأنترنت ويُفقد الولايات المتحدة الأمريكية نفوذها الكبير في الفضاء السيبراني.

3. الوسائل:

ركزت استراتيجية البيت الأبيض للفضاء السيبراني 2011 على الوسائل الدبلوماسية عموماً لتحقيق أهدافها بضمان أنترنت آمن ومفتوح أو ردع الجهات الخبيثة في الفضاء السيبراني، ثم جاءت استراتيجيتا وزارة الدفاع بالتفاصيل، حيث أكدت على الاعتماد على الحرس الوطني بشكل خاص مع التعاون مع بقية الهيئات والمنظمات ذات الصلة، كما قدمت برامج لتقييم القدرات والقوات السيبرانية، إضافة إلى برامج دائمة ومستمرة لتقييم استراتيجيات الردع، كما جاءت استراتيجية وزارة الخارجية 2016 بمجموعة من الوسائل المتنوعة أهمها:

- التأكيد على استراتيجية الردع بالحرمان والعقاب **Deterrence by denial and punishment**
- تفعيل وتعزيز القانون الدولي للتحكم في الصراعات في الفضاء السيبراني.
- مكافحة الحواجز التجارية، معارضة توطين البيانات، وفرض العقوبات الاقتصادية.
- الدفع المستمر بنهج أصحاب المصلحة المتعددين ودعم منتدى **IGF**.

من جهة أخرى، تم توحيد القوات العاملة في الفضاء السيبراني تحت قيادة موحدة هي "القيادة السيبرانية للولايات المتحدة الأمريكية **USCYBERCOM**" والتي تعمل كقيادة فرعية لـ "القيادة الاستراتيجية للولايات المتحدة **USSTRATCOM**".

4. السياسات السيبرانية وتأثيرها الاستراتيجي :

أفرزت استراتيجيات الردع في الفضاء السيبراني في عهد الرئيس "أوباما" العديد من السياسات والسلوكات الأمريكية التي كان لها آثار استراتيجية متباينة في المجالات العسكرية، الاقتصادية والسياسية.

أ. في المجال العسكري:

لقد كان للهجوم السيبراني الأمريكي على المنشآت النووية الأمريكية باستخدام "فيروس ستاكسنت" وكذا تسريبات "سنودن" حول برامج تجسس وكالة الأمن القومي **NSA** حول العالم تأثيراً استراتيجياً مزدوجاً، فمن جهة، أظهرت الولايات المتحدة قدراتها وقوتها في مجال الأسلحة

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السبراني

السبرانية والتجسس، وهو ما عزز مصداقيتها في ردع خصومها وجعل الدول الأخرى تُقبل على التحالف والشراكة معها، ومن جهة ثانية، زاد من الانقسام الجيوبوليتيكي في الفضاء السبراني، حيث حفز خصوم الولايات المتحدة (بالخصوص الصين وروسيا) إلى السعي لزيادة قدراتهم السبرانية ودمج القدرات السبرانية في التخطيط العسكري، إضافة إلى محاولة استمالة بقية الدول لتشكيل معسكر مناوئ للولايات المتحدة من خلال تبني مفاهيم السيادة السبرانية.

ب. في المجال الاقتصادي:

جعلت إدارة الرئيس "أوباما" من قضايا الأمن السبراني أولوية قصوى، حيث وضعت التهديدات السبرانية على رأس التهديدات التي تمس الأمن القومي والمصالح الاقتصادية العليا للولايات المتحدة، لذلك سعت من خلال سياسات مكافحة الحواجز التجارية ومعارضة توطين البيانات -التي تنتهجها الصين- إلى حماية ودعم شركات التكنولوجيا الأمريكية التي تعمل وتستثمر في الخارج (خاصة في الصين)، وبغرض الحفاظ على التفوق والنفوذ الأمريكي في جانبه الاقتصادي فرضت الحكومة الأمريكية مجموعة من الضوابط والعقبات على تصدير واستيراد المواد التكنولوجية¹، هذا السلوك الردعي في الفضاء السبراني مكن الولايات المتحدة من التوصل لاتفاق مع الصين حول قضايا التجسس السبراني لأغراض اقتصادية² والذي كان محور الاستراتيجيات الأمريكية، إلا أنه في المقابل، قدم حافزاً قوياً لشركات التكنولوجيا الصينية التي عرفت تطوراً سريعاً في الحجم (القيمة السوقية) والتنوع (التطوير والابتكار) لتصبح منافساً قوياً للشركات الأمريكية على مستوى العالم.

ج. في المجال السياسي:

أثبتت الوسائل الدبلوماسية التي جاءت بها إدارة الرئيس "أوباما" لمعالجة قضايا الفضاء السبراني نجاعتها، ذلك ما يتجلى في الاتفاق الذي وقع مع الصين بشأن الفضاء السبراني في سبتمبر 2015، حيث تُعتبر الصين المنافس الأكبر والذي يُشكل تهديداً مباشراً للولايات المتحدة، كما أن الجمع بين الردع والدبلوماسية منح الولايات المتحدة الأمريكية مركز الريادة في الدعوة

¹ يقدم القسم 516 من قانون الاعتمادات الموحدة والمستمرة والذي وقع عليه الرئيس "أوباما" ليصبح قانوناً في مارس 2013 مثلاً جيداً على كيفية مراقبة الصادرات، حيث يمنع بموجبه شراء أي نظام للتكنولوجيا يتم دعمه أو انتاجه أو تصنيعه أو تجميعه في الصين من قبل الإدارات الحكومية المختلفة.

² للمزيد انظر: سكوت وارين هارولد، مارتين سي لبيكي، أستريد ستوث سيفالوس، التوصل إلى اتفاق مع الصين بشأن الفضاء السبراني، على الرابط: <https://bit.ly/3BwDpEF>.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

إلى مستقبل لفضاء سيبراني مفتوح، قابل للتشغيل المتبادل، آمن وموثوق، من خلال الدعم المستمر والقوي لمقاربة حوكمة الأنترنت المبنية على أصحاب المصلحة المتعددين عبر **منتدى حوكمة الأنترنت IGF**.

وبناء على ما تقدم، فإن الاستراتيجيات المتعلقة بالفضاء السيبراني في عهد الرئيس "أوباما" عززت وبرهنت على النفوذ الكبير للولايات المتحدة الأمريكية في الفضاء السيبراني في المجالات العسكرية، الاقتصادية والسياسية، كما أنها وضعت الفضاء السيبراني في سياق أكبر للعبة الجيوبوليتكية بين القوى العظمى.

الفرع الثالث: استراتيجية الدفاع إلى الأمام (المثابرة السيبرانية)

لعب الاتفاق بين الولايات المتحدة والصين بشأن الفضاء السيبراني في 2015 دوراً مهماً في تخفيض التوتر بين الدولتين، غير أن الهجمات السيبرانية التي تلتها ازدادت حدة وخطورة عبر العالم¹، كما أنها طالت إضافة إلى الولايات المتحدة، حلفاءها وشركاءها، وفندت ما اعتقده الأمريكيون حول سيادة الولايات المتحدة للفضاء السيبراني دون منازع، وحتمية تحقيق فضاء سيبراني مفتوح وآمن، وبديهيّة جمع الثروات والمال بتوسع الفضاء السيبراني عبر التجارة والتبادل الحر للأفكار، من جهة أخرى، أثبتت بوضوح أن خصوم ومنافسي الولايات المتحدة يرون أن الفضاء السيبراني مجال يمنحهم فرصة للتغلب، تحييد وحتى هزيمة الولايات المتحدة وحلفائها.

لذلك، اتفقت استراتيجيات الهيئات الأمريكية المختلفة في إدارتي كل من "ترمب" و"بايدن" على أن عهد المنافسة الاستراتيجية قد بدأ بين الولايات المتحدة وخصومها الجيوبوليتكيين، حيث أصدر البيت الأبيض "الاستراتيجية الوطنية للفضاء السيبراني 2018"، وقدمت وزارة الدفاع DoD نسختين، الأولى في عهد "ترمب" تحت مسمى "الاستراتيجية السيبرانية لوزارة الدفاع 2018" والثانية في عهد "بايدن" تحت مسمى "استراتيجية الثقة المعدومة 2022" والتي حملت شعار "لا تثق أبداً، تحقق دوماً"، وبعد ترقية القيادة السيبرانية للولايات المتحدة الأمريكية CYBERCOM إلى قيادة مقاتلة مستقلة عبرت عن رؤيتها للصراع في الفضاء السيبراني في وثيقة بعنوان "بلوغ والحفاظ على التفوق في الفضاء السيبراني 2018".

¹ للمزيد من المعلومات انظر: قائمة بأهم الهجمات السيبرانية منذ 2006 جمعها مركز الدراسات الدولية والاستراتيجية CSIS على الرابط : <https://bit.ly/3HP1eKQ>.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

1. التحديات الجيوبوليتيكية:

تستمد الوثائق الاستراتيجية قيد الدراسة رؤيتها من التحديات الجيوبوليتيكية التي تحددها وثيقتي استراتيجيتي الأمن القومي للولايات المتحدة للعام 2017 و 2022 على التوالي، وللتين تُقران بأن عهد المنافسة الاستراتيجية بين القوى العظمى قد بدأ، وتصنفان الصين على أنها الخصم الجيوبوليتيكي الأقوى والذي يملك النية والقدرة على إعادة تشكيل النظام الدولي، إضافة إلى روسيا، كوريا الشمالية وإيران بدرجة أقل¹، لذلك فإن كل الاستراتيجيات² تُجمع على أن الولايات المتحدة دخلت في مرحلة من المنافسة الاستراتيجية طويلة الأمد مع خصومها الجيوبوليتيكيين وعلى رأسهم الصين وروسيا.

2. الأهداف:

تُقدم رؤية القيادة السيبرانية الأمريكية US CYBERCOM نظرة دقيقة للهدف الرئيس للولايات المتحدة في الفضاء السيبراني وهو "بلوغ التفوق الشامل في الفضاء السيبراني والحفاظ عليه"، هذا الهدف تُعبر عنه "الاستراتيجية الوطنية للفضاء السيبراني 2018" بتوسيع النفوذ - التأثير - الأمريكي في الخارج لفضاء سيبراني مفتوح وآمن من خلال زيادة قدرة الولايات المتحدة - وحلفائها وشركائها - على ردع وعقاب الجهات التي تستعمل الوسائل السيبرانية لأغراض خبيثة، مما يُحقق حماية للشبكات والأنظمة والوظائف والبيانات في الولايات المتحدة ويُعزز الاقتصاد الرقمي والابتكار المحلي³، من جهتها، وضعت وزارة الدفاع DoD في استراتيجيتها للعام 2018 ثلاثة أهداف كبرى⁴، أولاً، ضمان قدرة الجيش الأمريكي على القتال والفوز في أية حرب في الفضاء السيبراني، ثانياً، استباق التهديدات السيبرانية وإلحاق الضرر بالفاعلين وردعهم من خلال

¹ انظر: استراتيجية الامن القومي للولايات المتحدة الأمريكية للعام 2017، ص 2، على الرابط: <https://bit.ly/3Bx13kh>، استراتيجية الامن القومي للولايات المتحدة الأمريكية للعام 2022، ص 23، على الرابط: <https://bit.ly/3eTqx2n>.

² انظر: الاستراتيجية الوطنية للفضاء السيبراني 2018، ص 2، على الرابط: <https://bit.ly/3zek9u3>، الاستراتيجية السيبرانية لوزارة الدفاع 2018، ص 01، على الرابط: <https://bit.ly/3Yaobh6>، استراتيجية الثقة المدعومة 2022، ص iv، على الرابط: <https://bit.ly/3JJkmGE>، بلوغ والحفاظ على التفوق في الفضاء السيبراني 2018، ص 03، على الرابط: <https://bit.ly/3Qydfot>.

³ The White House, The National Cyber Strategy of the United States of America, Washington, September 2018, op.cit, p 01.

⁴ Department of Defense, Department of Defense Cyber Strategy, 2018, op.cit, p 02.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

مفهوم الدفاع إلى الأمام، ثالثاً، توسيع العمليات السيبرانية المشتركة مع الحلفاء والشركاء لوقف التهديدات السيبرانية قبل أن تصل إلى هدفها من خلال مفهوم **المثابرة السيبرانية**.

3. الوسائل:

يظهر جلياً تركيز إدارة "ترمب" على الوسائل العسكرية في سعيها لزيادة نفوذها وتأثيرها في الفضاء السيبراني، حيث تمت ترقية القيادة السيبرانية للولايات المتحدة **USCYBERCOM** إلى مستوى قيادة قتالية موحدة مستقلة، مع التركيز على الوسائل الهجومية في المجال السيبراني.

في المجال الاقتصادي، سعت إدارة "ترمب" ومن بعده "بايدن" إلى استعمال العقوبات وفرض القيود على الشركات الأجنبية -خاصة الصينية- بغرض الحفاظ على تأثير الولايات المتحدة في النظام -البيئة- التكنولوجي وتطوير الفضاء السيبراني كمحرك مفتوح للنمو الاقتصادي والابتكار والكفاءة المحليين.

كما سعت الحكومة الأمريكية من خلال الوسائل الدبلوماسية لجذب الحلفاء والشركاء أصحاب التفكير المماثل لدعم مقاربة أصحاب المصلحة المتعددين، واحتواء الخصوم الجيوبوليتيكيين الحاليين والمحتملين في الفضاء السيبراني.

4. السياسات السيبرانية وتأثيرها الاستراتيجي :

عكست السياسات السيبرانية في عهد "ترمب" صعود تيار القومية في الولايات المتحدة وبروز الحمائية الاقتصادية الوطنية للمؤسسات والشركات الأمريكية، وهذا ما حفز المنافسة الاستراتيجية الشاملة وكان له تأثيرات استراتيجية عالمية في مختلف المجالات.

أ. في المجال العسكري:

كانت ترقية القيادة السيبرانية الأمريكية إلى قيادة مقاتلة مستقلة إيذاناً ببدء مرحلة جديدة من الصراع في الفضاء السيبراني، هذا الصراع المستمر واليومي **day-a-day** يعكس تطبيقات المفهوم الاستراتيجي "**المشاركة المستمرة**" أو "**المثابرة السيبرانية**" "**Cyber persistence**" الذي قدمته رؤية القيادة السيبرانية الأمريكية، حيث خلق بيئة استراتيجية خطيرة في الفضاء السيبراني أشبه ما تكون بالحرب الباردة، زاد من حدتها تطبيق إطار العمل الذي دعت إليه "استراتيجية الثقة المدعومة" للعام 2022، وهذا ما جعل الدول الكبرى تزيد من إنفاقها على عسكرة الفضاء السيبراني،

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

كما دفع بالولايات المتحدة إلى تشكيل أحلاف سيبرانية ذات توجه عسكري ما جعل العالم يعيش مرحلة استقطاب شديدة وينقسم إلى معسكرين في الفضاء السيبراني، تقود الولايات المتحدة أحد أطرافه، والصين وروسيا الطرف الآخر.

ب. في المجال الاقتصادي:

انعكست الاستراتيجية الاقتصادية الحمائية التي انتهجتها إدارة "ترمب" على المجال السيبراني، إذ توالى إصدار القوانين واللوائح التنفيذية التي تُقيد وأحياناً تمنع عمل شركات التكنولوجيا الصينية خاصة شركتي **هواوي** و**ZTE** داخل الأراضي الأمريكية، كما وضعت قيوداً على تصدير المنتجات التكنولوجية الأمريكية، وعملت مع حلفائها لمحاصرة وإضعاف الشركات التكنولوجية الصينية.

من جهة أخرى، أدت جائحة كورونا إلى مشكلات في سلاسل التوريد للمنتجات التكنولوجية واستغلت الولايات المتحدة الفرصة للدفع بعمليات توطين التكنولوجيا في الداخل الأمريكي من جهة، ومحاولة كبح تدفق التكنولوجيا من وإلى الصين من جهة أخرى، وهذا ما يُعبر عنه بتنامي "القومية التقنية" التي طبقها الرئيس "ترمب" بشكل حاسم ضد الصين ويسير على نهجه الرئيس "بايدن" ولكن بعدائية أكبر.

ج. في المجال السياسي:

تواصل الولايات المتحدة دعم نهج أصحاب المصلحة المتعددين كمقاربة لا يمكن الاستغناء عنها في مواجهة ما تسميه "الاستبداد الرقمي" أو نهج السيادة الرقمية الذي تدعو إليه كل من الصين وروسيا، لذلك فهي تعمل على تشكيل تحالفات تكنولوجية مع الدول ذات التفكير المماثل لدعم مقاربتها بعيداً عن الأمم المتحدة التي ترى أنها تحت سيطرة كلٍ من الصين وروسيا.

إضافة لما سبق، قامت إدارة "بايدن" بإنشاء "مكتب الفضاء السيبراني والسياسة الرقمية" **CDP** في أبريل 2022 ضمن وزارة الخارجية، ويهتم المكتب بالتنسيق مع الحلفاء والشركاء لضبط قواعد السلوك والمعايير الدولية في الفضاء السيبراني، الترويج لأفكار الولايات المتحدة حول حوكمة الأنترنت وكسب شركاء جدد، كما يدعم جهودها لريادة الابتكار على مستوى العالم.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

جاءت استراتيجيات الفضاء السيبراني في عهد الرئيسين "ترمب" و"بايدن" لتُعلن بوضوح أن المنافسة الاستراتيجية بين القوى العظمى قد بدأت، وأن الصين هي الخصم الجيوبوليتيكي الأقوى، لذلك وضعت الإدارة الأمريكية "التفوق في الفضاء السيبراني" كهدف أسمى، وسخرت لبلوغ هذا الهدف مختلف الوسائل العسكرية، الاقتصادية والدبلوماسية، من أجل زيادة وتوسيع نفوذها وصولاً إلى الهيمنة في جميع مجالات الفضاء السيبراني.

المطلب الرابع: الاستراتيجيات الأمريكية للسيطرة على الفضاء السيبراني

يروج البعض (صقور الصين) في الولايات المتحدة فكرة أن صعود الصين في المجالات الاقتصادية، العسكرية، السياسية والتكنولوجية لا يمكن وقفه، وهذا ما يضع الولايات المتحدة باعتبارها المؤسس والفاعل الرئيس في النظام الدولي الحالي في مواجهتها للصين أمام خيارين استراتيجيين كبيرين، إما المشاركة أو الاحتواء.

مع توتر العلاقات بين البلدين -خاصة في الفضاء السيبراني- في العقد الثاني من القرن الحالي، وفشل سياسات الرئيس "أوباما" لجذب الصين إلى الانخراط والمشاركة في النظام الدولي -بنسخته الأمريكية- سلكت إدارة الرئيس "ترمب" خيار "الاحتواء" مدفوعة بالنجاح الذي حققته هذه الاستراتيجية في هزيمة الاتحاد السوفياتي، لكن العلاقات الاقتصادية والتجارية المعقدة والمتشابكة بين البلدين جعل من صانع القرار الأمريكي يُفكر في استراتيجية داعمة لفك هذا الارتباط الاقتصادي الكبير خاصة في شقه التكنولوجي ليتوصل إلى "استراتيجية الفصل التكنولوجي" التي يُتوقع منها المساهمة في إنجاح سياسة الاحتواء وكبح الصعود التكنولوجي الصيني السريع، وتُمكن الولايات المتحدة من السيطرة على الفضاء السيبراني.

الفرع الأول: استراتيجية الاحتواء (Containment Strategy)

يُعتبر الاحتواء الاستراتيجية التي ميّزت السياسة الخارجية الأمريكية طوال فترة الحرب الباردة، تعددت تطبيقاتها خلال الخمسة والأربعين عاماً من وجودها بتعدد الإدارات والرؤساء الأمريكيين، وكان الهدف الرئيس منها هو الاحتواء الجيوبوليتيكي للاتحاد السوفياتي بعد نهاية الحرب العالمية الثانية، ومنع زيادة نفوذ وانتشار الشيوعية في أوروبا الشرقية، آسيا، إفريقيا وأمريكا الجنوبية.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

أولاً، الإطار الفكري لاستراتيجية الاحتواء

وضع الدبلوماسي الأمريكي الشهير "جورج كينان" المبادئ الأساسية لاستراتيجية الاحتواء، حيث تضمنت برقيته المطولة "The long Telegram" التي كتبها في فيفري 1946 والتي وجهها إلى إدارة الرئيس الأمريكي "هاري ترومان" وظهرت فيما بعد في مقال لكاتب مجهول (السيد X) نُشر في مجلة الشؤون الدولية Foreign affairs أفكاره ورؤيته حول مصادر السلوك السوفيياتي¹، كما دعا إلى "أن العنصر الرئيسي لأي سياسة للولايات المتحدة تجاه الاتحاد السوفيياتي يجب أن يكون احتواءً طويل الأجل وصبوراً ولكن حازماً ويقظاً للميول التوسعية الروسية"، هذه الدعوة شكلت الطريق الثالث الذي يمكن للإدارة الأمريكية أن تسلكه بين الاسترضاء والطموح الخيالي للهيمنة الأمريكية على البيئة الأمنية العالمية، لقد شكل المشروع المركزي للاحتواء مسعى للأمن القومي لا يتطلب التفوق العسكري وصيانته بل فهماً دقيقاً وخاصاً للمصالح الأمنية الأمريكية، وهو ما يُشير إليه "لويس غاديس" بأن "المطلوب ليس إعادة تركيب العالم على صورة الولايات المتحدة، بل الحفاظ على تنوعه فحسب في مواجهة محاولات إعادة تركيبه على صورة الآخرين"²، لذلك فإن مرتكزات استراتيجية الاحتواء حسب "كينان" تشمل جميع المجالات السياسية، الاقتصادية، الأخلاقية والعسكرية، مع الاستمرار في النظر إلى الاتحاد السوفيياتي كمنافس وليس كشريك في الساحة السياسية.

ثانياً، لماذا يجب احتواء الصين؟

يتبادر إلى الذهن التساؤل حول ضرورة احتواء الصين اليوم؟ ويجب عن هذا السؤال مجموعة من المفكرين والاستراتيجيين وصناع القرار الأمريكيين (خاصة من لهم علاقة بتيار المحافظين الجدد) بأن سياسات التعاون والشاركة مع الصين والتي كانت الولايات المتحدة تأمل من خلالها دفع الصين إلى احترام النظام الدولي الليبرالي والمساهمة في تطوره قد فشلت، وهو ما عبر عنه "أنتوني بلينكن" وزير الخارجية الأمريكي في إدارتي "أوباما" و"بايدن" بقوله إن

¹ "X" (George F. Kennan), *The Sources of Soviet Conduct*, foreignaffairs.com, July 1, 1947, URL: <http://bit.ly/3Ygd1H3>.

² John Lewis Gaddis, *Strategies of containment: a critical appraisal of American national security policy during the Cold War*, Oxford University Press, 2005, p 55.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السبراني

"المقاربات المتفائلة السابقة تجاه الصين كانت معيبة"¹، كما طور فريق وزير الخارجية في إدارة "ترمب" استراتيجية تجاه الصين تستند إلى فكرة "صدام الحضارات" لـ "هنتنجتون" إذ صرحت مديرة تخطيط السياسات في وزارة الخارجية "كيرون سكينر" خلال وصفها للمنافسة بين الولايات المتحدة والصين بأنها "معركة مع حضارة وإيديولوجية مختلفة تماماً" وأضافت أنها "المرّة الأولى التي تكون فيها قوة عظمى منافسة ليست قوقازية" في تعليق لها حول الحرب الباردة بأنها كانت داخل الأسيرة الغربية، كما أضافت بأن الولايات المتحدة بحاجة إلى مفهوم للعلاقة مع الصين وفق ما سمته "الرسالة X" في إشارة لاستراتيجية الاحتواء التي قدمها "كينان"²، لذلك فإن الحاجة لاحتواء الصين تخدم هدفين؛ هدف جيوبوليتيكي يتمثل في التقليل من تأثير الصين كمركز لقوة إقليمية، وهدف جيو-استراتيجي هو ضمان استمرار الهيمنة الأمريكية، هذه الاستراتيجية تلقى دعماً لدى الكثير من المفكرين الأمريكيين إذ يجادل "ميرشايمر" بأن "الاستراتيجية المثلى للولايات المتحدة للتعامل مع الصين هي اتباع استراتيجية احتواء مماثلة لتلك التي اتبناها مع الاتحاد السوفياتي خلال الحرب الباردة"³.

بدأ تطبيق وممارسة سياسات احتواء الصين منذ 2009، حيث قدمت إدارة "أوباما" مفهوم "محور آسيا" وعُدل المصطلح فيما بعد إلى "إعادة التوازن" والهدف من هذه الاستراتيجية كان عودة الولايات المتحدة للاهتمام والالتزام بأمن منطقة المحيطين الهندي-الهادي (Indo-Pacific Region) مع التركيز أكثر على الجوانب التجارية، الاقتصادية والدبلوماسية في محاولة لكبح تنامي قوة الاقتصاد الصيني والتقليل من نفوذ وهيمنة الصين على المنطقة، لكن التحول في أولويات الخارجية الأمريكية تحت قيادة "جون كيري" نحو قضايا الشرق الأوسط من جهة، وسياسة "ترمب" الانعزالية من جهة أخرى، أفشلت عمليات الشراكة الاقتصادية مع دول آسيا خاصة مفاوضات الشراكة عبر المحيط الهادي TPP وجعلتا دول المحيط الهادي والهندي في شك من فائدة الدخول في تحالفات اقتصادية و/أو أمنية مع الولايات المتحدة، هذا ما جعل

¹ William Mauldin, Michael R. Gordon, **Blinken Backs Tough Approach to China, Says Will Work With GOP**, wsj.com, Jan. 19, 2021, URL: <http://bit.ly/3KHSjwB>.

² Paul Musgrave, **The Slip That Revealed the Real Trump Doctrine**, foreignpolicy.com, MAY 2, 2019, URL: <http://bit.ly/3xROFbM>.

³ Peter Navarro, **Mearsheimer on Strangling China & the Inevitability of War**, huffpost.com, Mar 10, 2016, URL: <http://bit.ly/3Z25RXS>.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

التقارير الصادرة¹ تُقر بأن جهود الإدارة لإعادة التوازن قد تكون غير كافية لتأمين المصالح الأمريكية في المنطقة.

حدث التحول الكبير في العلاقات الأمريكية-الصينية في عهد إدارة "ترمب"، حيث جاءت استراتيجية الأمن القومي لتؤكد على مقاربة "المنافسة الاستراتيجية الشاملة بين القوى العظمى" كما تم اعتبار الفضاء السيبراني كمجال استراتيجي حاسم في حماية الاقتصاد والأمن القومي الأمريكي، ونتج عن تطبيق استراتيجية الاحتواء في الفضاء السيبراني ما أطلق عليه "الاحتواء التكنولوجي" كأبرز عنصر في سياسات احتواء الصين.

ثالثاً، سياسات الاحتواء التكنولوجي للصين وأهم آثارها الاستراتيجية

كانت إدارة الرئيس "ترمب" سباقاً في وضع وتنفيذ سياسات لاحتواء الصعود والتمدد الصيني في الفضاء السيبراني، فمنذ 2016 برزت شركات التكنولوجيا الصينية خاصة شركتي هواوي Huawei و زاد تي اي ZTE ودخلت مجال المنافسة مع كبريات الشركات التكنولوجية الأمريكية، وهذا ما جعل الإدارة الأمريكية تُدرك مدى خطورة الصعود التكنولوجي الصيني على الاقتصاد والأمن القومي الأمريكي وعلى المكانة والدور الأمريكي في العالم، لذلك سارعت إدارة "ترمب" إلى سن قوانين وتشريعات واتخاذ إجراءات للجم تمدد نفوذ وهيمنة الشركات التكنولوجية الصينية، تابعت إدارة "بايدن" سلفها على نفس النهج في حالة من الحالات القليلة التي يتوافق فيها الحزبان الجمهوري والديمقراطي على نفس السياسات.

أ. المجالات الرئيسية للاحتواء

1. الابتكار والمعرفة، حيث تفوقت الصين على الولايات المتحدة في عدد براءات الاختراع في مجالات الذكاء الاصطناعي والجيل الخامس، لذلك كان تركيز الولايات المتحدة على الحد من تدفق الطلاب الصينيين على الجامعات الأمريكية والحد من التجسس الصيني وسرقة الملكية الفكرية، إضافة إلى دعم وتمويل مشاريع الابتكار والتطوير في الداخل الأمريكي.

¹ Michael J. Green, et al, *Asia-Pacific rebalance 2025: Capabilities, presence, and partnerships*, CSIS, 2016.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

2. **الرقاقات (Semiconductors)**، تمثل الرقاقات أو أنصاف النواقل محرك صناعة الأجهزة الرقمية كما تدخل في مختلف الصناعات التكنولوجية المدنية والعسكرية، لذلك سعت الولايات المتحدة لحرمان الصين من الحصول وتطوير الرقاقات الفائقة بالتعاون مع حلفائها وشركائها في العالم.

3. **سوق التكنولوجيا**، بما أن الابتكار يحتاج حتماً إلى التمويل، كما أن الهدف الأول للتصنيع هو الربح، سعت الولايات المتحدة لتطويق الصين في هاذين المجالين من خلال حرمان الصين من السوق الأمريكية -كأكبر سوق للمنتجات التكنولوجية الصينية- كمرحلة أولى والأسواق العالمية بالتنسيق مع الحلفاء والشركاء الغربيين والأسويين لخلق الصعود التكنولوجي الصيني.

ب. القوانين لاحتواء شركات التكنولوجيا الصينية

بدأ التطبيق الفعلي لسياسات الاحتواء التكنولوجي للصين مع الأمر التنفيذي رقم 13873 بتاريخ 15 ماي 2019 الذي وقعه الرئيس "ترمب" والذي بموجبه يحظر جميع التعاملات مع شركات التكنولوجيا الأجنبية ويمنع عملها داخل الأراضي الأمريكية¹، هذا الحظر والمنع كان موجهاً لشركة هواوي الصينية بالدرجة الأولى، تم تمديد حالة الطوارئ الوطنية الخاصة بالتهديدات التكنولوجية للشركات الصينية في فترة حكم "بايدن" من خلال إشعار² صادر عن البيت الأبيض بتاريخ 11 ماي 2021، تطورت فيما بعد القوانين والتشريعات من مختلف الهيئات الأمريكية لمحاصرة وحظر الشركات (أو الكيانات) التكنولوجية الصينية والتضييق عليها وقد تم تحديد قائمة كبيرة لهاته الكيانات المحظورة.

يُشكل مجموع هذه السياسات الهجومية ضد شركات التكنولوجيا الصينية ما يُمكن تشبيهه بـ"استراتيجية الأناكوندا" التي طُبقت من قبل ضد الاتحاد السوفياتي، والهدف منها هو التضييق

¹ Executive Order 13873 of May 15, 2019, **Securing the Information and Communications Technology and Services Supply Chain**, Federal Register, Vol 84, No 96, May 17, 2019.

² The White House, **Notice on the Continuation of the National Emergency with Respect to Securing the Information and Communications Technology and Services Supply Chain**, May 11, 2021.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

على الخصم وخنقه، ففي مجال الجيل الخامس قامت الولايات المتحدة بمجموعة من الإجراءات منها:

- حظر شركة هواوي وفروعها داخل الولايات المتحدة والضغط على الحلفاء لحظرها.
- محاولة شراء شركتي نوكيا وإيركسون ومحاولة تشكيل تحالف لتطوير الجيل الخامس.
- تطوير Open RAN للسماح للمتعاملين باستخدام أجهزة من شركات مختلفة بعيداً عن الشركات الصينية.

في مجال الرقاقات، حظرت الولايات المتحدة تصدير الرقاقات بكل أنواعها وكذلك أجهزة وبرامج تصنيعها نحو الصين، كما فرضت حصاراً على محاولات تطوير الرقاقات داخل الصين بمنع الشركات الأجنبية التي تستعمل تكنولوجيا أمريكية من التعامل مع الشركات الصينية، في المقابل، قدمت تحفيزات مالية ضخمة لتطوير الرقاقات على الأراضي الأمريكية¹ كما سعت لإنشاء فروع لشركتي TSMC التايوانية وسامسونغ الكورية الجنوبية في الولايات المتحدة في إشارة واضحة لتنامي "القومية التكنولوجية".

ب. برنامج الشبكة النظيفة (حظر التكنولوجيا والتطبيقات الصينية)

قدم "مايك بومبيو" وزير الخارجية في إدارة "ترمب" مبادرة أطلق عليها اسم "الشبكة النظيفة"، وهي محاولة لخلق فضاء سيبراني خال من التكنولوجيا الصينية سواء تعلق الأمر بالأجهزة أو بالبرامج والتطبيقات، وسعت هذه المبادرة إلى حصر التكنولوجيا الصينية في الداخل الصيني فقط، بعبارة أخرى، سيصبح الفضاء السيبراني مقسماً إلى شطرين، فضاء سيبراني أمريكي-عالمي، وفضاء سيبراني صيني، تضمن برنامج الشبكة النظيفة ستة (06) محاور أساسية هي²:

¹ The White House, **FACT SHEET: President Biden Signs Executive Order to Implement the CHIPS and Science Act of 2022**, August 25, 2022. URL: <http://bit.ly/3SIw3UY>.

² Secretary of State, **The Clean Network**, 2020, URL: <http://bit.ly/38a9t1p>.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

1. **الحامل النظيف (Clean Carrier):** حرمان شركات التكنولوجيا الصينية من تقديم خدمات نقل البيانات من وإلى الولايات المتحدة.

2. **المتجر النظيف (Clean Store):** إزالة التطبيقات غير الموثوق بها (أي التطبيقات الصينية) من متاجر التطبيقات.

3. **التطبيقات النظيفة (Clean Apps):** منع الشركات الصينية من تطوير تطبيقاتها بعدم إتاحتها للتحميل عبر الشبكة في المتاجر الرقمية الأمريكية.

4. **السحابة النظيفة (Clean Cloud):** حرمان الشركات الصينية من الوصول إلى السحابة التي تعمل فيها الولايات المتحدة وحلفاؤها وشركاؤها.

5. **الكابل النظيف (Clean Cable):** تجنب الاتصال بالكابلات الصينية وحماية الكابلات من التخريب والتدمير.

6. **المسار النظيف (Clean Path):** توفير مسار إتصال شامل لا يستخدم أي معدات إرسال أو تحكم أو حوسبة أو تخزين من بائعي تكنولوجيا المعلومات غير الموثوق بهم (أي الشركات الصينية).

إنضمت العديد من الشركات والدول إلى هذه المبادرة مكونة تحالفاً هدفه المعلن هو الوصول إلى فضاء سيبراني آمن وموثوق، ولكن نتائجه المرجوة هي ثني الدول عن شراء معدات شركتي **هواوي** و**زاد تي إي** ومن ثم حصار وخنق وإضعاف قدرات شركات التكنولوجيا الصينية لكبح الصعود التكنولوجي الصيني والإبقاء على الولايات المتحدة في المقدمة.

كان لتطبيق استراتيجية الاحتواء التكنولوجي آثار جلية على الشركات التكنولوجية الصينية وفي مقدمتها شركة **هواوي Huawei** -رمز الصعود التكنولوجي الصيني- التي قُوضت مخططاتها لتصدر قائمة الشركات التكنولوجية الأقوى في العالم، وتراجع لتخرج حتى من قائمة أفضل عشر شركات الأوائل، كما أن الرقابة على الرقاقات ثبّطت التطور والابتكار التكنولوجي في الصين وجعلت الحكومة الصينية تراجع سياساتها للتطوير والمنافسة، أما على المستوى الدولي، فقد أثرت استراتيجية احتواء الصين على مشاريع البحث العلمي، كما ستؤثر مستقبلاً

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

على مستوى التطور التكنولوجي العالمي ونمو الاقتصاد الرقمي، هذا إضافة إلى الشكوك التي طرحتها سياسات الاحتواء حول مدى فعالية وسلامة سلاسل التوريد العالمية والعولمة الاقتصادية ككل.

الفرع الثاني: استراتيجية الفصل التكنولوجي (Technological decoupling strategy)

يحدُ الترابط التكنولوجي المعقد بين الولايات المتحدة والصين من فاعلية استراتيجية الاحتواء، لذلك تسعى الولايات المتحدة لقطع أوصال هذا الترابط من خلال فصل تكنولوجيا البلدين ولو بشكل جزئي وتدرجي من أجل تحقيق التفوق.

أولاً، مفهوم الفصل التكنولوجي

لا يزال مصطلح "الفصل التكنولوجي" يكتنفه الكثير من الغموض، ويعاني تنازعا شديداً بين المفكرين والاستراتيجيين كما أنه في كثير من الأحيان مشحون سياسياً، ينتقل مفهوم الفصل التكنولوجي عبر محور طرفه الأعلى هو القطيعة التكنولوجية أو فك الارتباط التام بين الولايات المتحدة والصين، ويمثل طرفه الأدنى نوع من التخفيض البسيط أو الجزئي للاعتماد التكنولوجي المتبادل بين البلدين، وتضم "التكنولوجيا" فئة واسعة من التقنيات الرقمية التي تتضمن الأنظمة والبرمجيات والبيانات والاتصالات والشبكات، كما يشمل الفصل التكنولوجي قسمين رئيسيين، **أولاً، التكنولوجيا النهائية** وتضم المنتجات والخدمات الرقمية النهائية، **ثانياً، مدخلات التكنولوجيا** وتضم العديد من العناصر مثل المواد الخام للصناعة التكنولوجية، سلاسل التوريد، البيانات، المعرفة والمهارات البشرية، الدعم المالي والاستثمار¹.

ثانياً، لماذا تحتاج الولايات المتحدة لاستراتيجية الفصل التكنولوجي؟

بعد سنة 2010 بدأت حكومة الولايات المتحدة ترى في الترابط التكنولوجي مع الصين تهديداً جدياً للأمن القومي والازدهار الاقتصادي والقيم الأمريكية، وتزايد إدراك صانع القرار الأمريكي بأن الصين تستغل هذا الترابط التكنولوجي وتعمقه لأغراض خبيثة كالتجسس الاقتصادي والتقليدي، نشر المعلومات المضللة، التغلغل في البنية التحتية التكنولوجية الأمريكية، السعي للفوز في المنافسة الاقتصادية وقيادة العالم، لذلك سعى صانع القرار

¹ Jon Bateman, US-China technological "Decoupling": a strategy and policy framework, Carnegie Endowment for International Peace, 2022, p 123.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

الأمريكي - الديمقراطيون والجمهوريون - للحد بشكل كبير من التدفقات التكنولوجية سواء تعلق الأمر بالمنتجات أو الخدمات أو المدخلات من وإلى الصين، تُسمى هذه الاستراتيجية بـ "استراتيجية الفصل التكنولوجي".

يُمكن تقسيم الأسباب التي دفعت بالإدارة الأمريكية إلى إعتماد سياسات واسعة للفصل التكنولوجي إلى اتجاهين بارزين¹:

أ. **السلوك الخارجي الصيني**، كان المفكرون وصناع القرار الأمريكيون في تسعينيات القرن المنصرم والعقد الأول من القرن الحالي يعتقدون أن أفضل الطرق للتعامل مع الصين هي زيادة دمجها في المؤسسات الدولية وتعميق العلاقات الثنائية معها في المجالين السياسي والاقتصادي، إذ كانت المقاربة المسيطرة على الفكر الاستراتيجي الأمريكي هي أن صعود الصين متوافق مع المصالح الأمريكية بل حتى مفيد لها، لكن هذه الرؤية المتفائلة تغيرت جذرياً مع تسارع تطوير الصين لجيشها، واستمرارها في سرقة الأسرار الاقتصادية والعسكرية الأمريكية، واستغلالها لقواعد التجارة العالمية للهيمنة على الاقتصاد العالمي، إضافة إلى الرقابة المشددة على المواطنين الصينيين وقمعها للحريات والأقليات، ولذلك توصل معظم صناع القرار الأمريكيين إلى نتيجة أن الصين هي التهديد الرئيس للولايات المتحدة على المدى الطويل.

ب. **نضج التكنولوجيا الرقمية وبرز القومية التكنولوجية**، بعد 2010 شهد العالم نضجاً كبيراً للتقنيات الرقمية حيث أصبح تأثيرها واضحاً في المجتمعات، الاقتصاد والسياسة، وهو ما منح شركات التكنولوجيا قوة كبيرة لتصبح لاعباً جيوبوليتيكياً بارزاً على الساحة العالمية، ومكنها من لعب أدوار رئيسية في تشكيل السياسة العالمية حتى أكبر من كثير من الدول القومية.

شجعت الولايات المتحدة العولمة التكنولوجية في البداية، ذلك أن الفضاء السيبراني المعولم تقوده شركات التكنولوجيا الأمريكية وهذا ما يخدم مصالحها الاقتصادية والأمنية، لكن هذه الهيمنة الأمريكية ولدت غضباً لدى الصين والعديد من الدول الأخرى وحفزتهم لمحاولة استعادة بعض من السيادة الرقمية المفقودة، كما أن الموجة الموالية من التكنولوجيا خاصة الذكاء الاصطناعي والجيل الخامس وما تعد به من تحويل جذري للمجتمعات والاقتصاد زرع الخوف

¹ Ibid, p 2-3.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

لدى الولايات المتحدة من أن الصين ستتنافس على هذه التكنولوجيات وقد تتفوق فيها، ويرجع هذا الخوف في الأساس إلى أن الصين تستغل التكنولوجيا الغربية خاصة الأمريكية عبر الترابط التكنولوجي الكبير، هذا ما جعل الولايات المتحدة تفتتق بأن التكنولوجيا هي ساحة المنافسة الجديدة بين القوى الكبرى ولا يمكن ترك تنظيمها ببساطة للسوق، بل يجب على الحكومة أن تتدخل لتقديم الحماية الأفضل لها ومواءمتها مع الاستراتيجية الكبرى للدولة.

ثالثاً، سياسات الفصل التكنولوجي "الدفاعية" و"الهجومية"

تنقسم سياسات الفصل التكنولوجي التي تنتهجها الإدارة الأمريكية إلى مجموعتين، المجموعة الأولى عبارة عن تدابير "دفاعية" الغرض منها هو احتواء الصعود التكنولوجي الصيني وإحباطه وتعطيله، أما المجموعة الثانية فهي التدابير "الهجومية" والتي تهدف إلى تعزيز وتقوية القدرات التكنولوجية الأمريكية والحفاظ على ريادتها وهيمنتها.

من جهة أخرى، يتميز الفضاء السيبراني بتقنياته المتعددة كساحة مركزية للمنافسة الاستراتيجية بأنه بيئة محفوفة بالمخاطر وعدم اليقين، لذلك فإن الاعتماد المتبادل غير المنضبط مع الصين يمكن أن يترك الاقتصاد والمجتمع والأمن القومي الأمريكي عرضة للتجسس والتخريب، ويجعل أمريكا مساهمة في الانتهاكات التكنولوجية الصينية، وفي المقابل، فإن الكثير من الفصل يمكن أن يحد من تطور البيئة التكنولوجية في الولايات المتحدة، ويزيد من زعزعة استقرار العلاقات الثنائية، وينفر حلفاء الولايات المتحدة وشركاءها، وعليه يمكن تحديد ثلاثة اتجاهات فكرية لعملية الفصل التكنولوجي¹:

- **المقيدون:** يرى أنصار التقييد بأن العلاقات التكنولوجية مع الصين محصلتها صفر، فالصين تكسب مزايا إستراتيجية طويلة الأمد، بينما تجني الولايات المتحدة مكاسب هامشية، وأغلب أنصار هذا الاتجاه هم من صقور الصين في الكونغرس، المدافعين عن حقوق الإنسان ومسؤولي الأمن القومي ومجتمع الاستخبارات، كما ينادي البعض بتجاوز فكرة تثبيط الصعود التكنولوجي الصيني إلى تصميم تدابير لإلحاق الضرر بالشركات الصينية وتدميرها.

¹ Ibid, p 37-41.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

- **المتعاونون:** يجادل المتعاونون بأن الحفاظ على الترابط التكنولوجي وإمكانية الوصول إلى السوق الصينية يخدم مصالح الولايات المتحدة الاقتصادية والتكنولوجية، كما أن نظام التعاون التكنولوجي المفتوح يسمح للولايات المتحدة بأن تكون في وضع جيد للقيادة، وأغلب أنصار هذا الطرح هم شركات التكنولوجيا والزّواد المؤسسون للإنترنت، إضافة إلى بعض السياسيين مثل السيناتور **بيرني ساندرز** الذي يرى بأن الضغط المتزايد من الحزبين من أجل المواجهة مع الصين "يغذي الإنفاق، والعسكرة، والتعصب، والشعبوية في الداخل في حين يقلل من احتمال التعاون بشأن القضايا العالمية الرئيسية"¹.

- **الوسطيون:** يؤيد الوسطيون الفصل التكنولوجي الجزئي، حيث يعترفون بالتهديد الصيني طويل الأمد لكن مع مراعاة أن هناك جانباً من التكنولوجيا التي يجب الإبقاء فيه على علاقات التعاون والشراكة مع الصين خاصة ما تعلق بالقضايا العالمية، يقودهم في ذلك البيئة الغامضة وعدم اليقين حول كيفية تطور التقنيات الناشئة لذلك فهم يدعون إلى استراتيجية متحولة ووسطية تحمل شعار "ساحة صغيرة، وسياج عال"² كتعبير عن أن تدابير الفصل يجب أن تنطبق فقط على التكنولوجيا الأكثر حساسية واستراتيجية.

رابعاً، أهداف استراتيجية الفصل التكنولوجي

تسعى استراتيجية الفصل التكنولوجي لتحقيق طيف واسع من الأهداف، على رأسها تحقيق التفوق العسكري والاقتصادي على الصين عبر ضمان التفوق التكنولوجي، منعها من التجسس التقليدي والاقتصادي، وتحقيق النفوذ والهيمنة العامة عليها، لذلك شملت السياسات "الدفاعية" العديد من التدابير منها:

- **ضوابط التصدير/الاستيراد،** تقيّد ومراقبة نقل السلع والخدمات والبيانات الحساسة من وإلى الولايات المتحدة.

¹ Bernie Sanders, **Washington's Dangerous New Consensus on China**, foreignaffairs.com, June 17, 2021, URL: <http://bit.ly/3kUTjmf>.

² هي استعارة منسوبة لوزير الدفاع السابق "روبرت غيتس" ويقصد بها استراتيجية اختيار مجالات محددة بدقة وتوفير أقصى حماية لها مع عدم فقدان الفوائد من الشراكة في المجالات الأخرى.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

- قيود الاستثمار، فرض قيود على الاستثمارات الواردة والصادرة.
- تراخيص الاتصالات والمعدات، تقييد التدخل الأجنبي في الاتصالات داخل الولايات المتحدة.
- قيود التأشيرة، تتمتع حكومة الولايات المتحدة بالسلطة التقديرية لمنع الأجانب من دخول التراب الأمريكي.

كما شملت السياسات والتدابير "الهجومية" تشريعين مهمين، قانون الابتكار والمنافسة في الولايات المتحدة لعام 2021¹، والذي ركز على تمويل ودعم أبحاث تطوير صناعة الرقائق وأمن سلاسل التوريد في الولايات المتحدة، قانون المنافسة الأمريكية للعام 2022، والذي علق عليه الرئيس "بايدن" بأنه سيجعل سلاسل التوريد للولايات المتحدة أقوى وينشط الابتكار للتغلب على الصين وبقية العالم، وعليه، فالتدابير "الهجومية" تهدف إلى الدفع بالولايات المتحدة إلى المقدمة وتضمن هيمنتها على المجال التكنولوجي للعقود القادمة.

ختاماً، لا يمكن لاستراتيجية الفصل التكنولوجي في حد ذاتها أن تضمن التفوق التكنولوجي الأمريكي على المدى الطويل، لكنها يمكن أن تحبط الهيمنة الصينية على المدى القصير، لذلك فالولايات المتحدة تركز قيودها على مجموعة مختارة من مجالات التكنولوجيا حيث توشك الصين على الحصول على مزايا فريدة وذات أهمية استراتيجية طويلة الأمد.

¹ S.1260-117th Congress, **United States Innovation and Competition Act of 2021**, Congress.gov, Library of Congress, Jun 8, 2021, URL: <https://bit.ly/3JhxHdp>.

المبحث الثالث : الاستراتيجية الصينية لإدارة الصراع في الفضاء السيبراني

تزخر الصين بالموروث الفكري والحضاري الضارب في القدم، كما أنها عبر تاريخها الطويل تعرضت للعديد من حملات الغزو وتعرض الصينيون للكثير من الإذلال، وفي الخمسين سنة الأخيرة بدأ الحزب الشيوعي الحاكم مسيرة التنمية الاقتصادية التي أصبحت توصف بـ"المعجزة الصينية"، وتزامن الصعود الصيني مع بروز الفضاء السيبراني كفرصة فريدة لتحقيق "الحلم الصيني" والتي سرعان ما أدرك القادة الصينيون الفرص التي يمنحها هذا الفضاء للصين اقتصادياً، سياسياً وعسكرياً وجعلوا منه أولوية استراتيجية من خلال تطوير استراتيجيات رقمية رائدة للتجديد الشامل للأمة الصينية.

المطلب الأول: المبادئ الجيوبوليتيكية الصينية: من حلم الصين إلى حلم العالم

لم تظهر الجيوبوليتيكا بمفهومها الغربي (الكلاسيكي والنقدي) في الكتابات الصينية القديمة، لكن اليوم يستعمل أغلب الباحثين الصينيين الإطار الغربي للجيوبوليتيكا الكلاسيكية في الأجندة النفعية لخدمة مصالح الدولة الصينية، إلا أنه يمكننا اللجوء إلى مفهوم "كولن فلنت" للمبادئ الجيوبوليتيكية لاستخلاص الكيفية التي توجّه بها الصين نفسها تجاه العالم.

نجد في الموروث الفكري والحضاري والتقاليد السائدة في الصين التمييز بين الصيني وغيره من الشعوب الأخرى أو ما يُعرف في الفكر الكنفوشيوسي بـ "المركزية الصينية" هذه المركزية والتي تظهر جلية في اسم البلد "الصين" والذي ينطق في اللغة الصينية "Zhong guo" وهما كلمتان الأولى "Zhong" وتعني "الوسط" والثانية "guo" وتعني "البلد/ الأمة/ الدولة"، وعليه، فإن فكرة توسط العالم رافقت الصين منذ أيام الإمبراطورية الصينية وحتى اليوم، رغم أن الصين تعرضت في القرنين التاسع عشر والعشرين إلى حملات غزو من الدول الأجنبية ما ولد لديها الإحساس بعقدة أنها محاصرة وذليلة، كما أن تبنيها النموذج الشيوعي للحكم بعد الاستقلال جعل من الحزب الحاكم وعلى رأسه رئيس الدولة هو من يحدد الكيفية التي تنظر بها الصين إلى نفسها وإلى العالم.

وبناء على ما سبق، فإن المبادئ الجيوبوليتيكية الصينية هي مزيج من أفكار "إمبراطورية الوسط" و المبادئ والتوجهات التي يقرها قادة الحزب الشيوعي الصيني الحاكم.

الفرع الأول: المركزية الصينية

يعتقد الصينيون منذ عهد الامبراطوريات القديمة أنه إذا كان للعالم مركز، فهو الصين، لأن الصين تتوسط ذلك المركز، وتتعدى فكرة المركز لتحدد الموقع لبقية الدول والشعوب وتميز صفاتها وطريقة التعامل معها، كما أن هذه المركزية ولدت مقاربة مكانية-عرقية-حضارية للتمييز بين الصيني من عرق "الهان" وبقية الشعوب الأخرى.

بدأ التمييز بين "هوا Hua" والذي يدل على الصيني من عرق الـ"هان" و الـ"ي Yi" والتي تعني باقي الأقليات والغرباء منذ عهد أسرة "زهو" (1046 ق.م – 711 ق.م) ويحمل هذا التمييز في طياته تمييزاً مكانياً، حيث يسكن الـ"هوا" الصين، أما باقي الأجناس والشعوب فتتوزع على المناطق النائية، كما تعبر الـ"هوا" عن الحياة الأكثر تحضراً والتفوق الاجتماعي والثقافي والسياسي والمادي، أما البقية من الـ"ي" فتعكس الحياة البربرية البدائية، كما أن معيار التمايز بين الطرفين هو مدى الاحتكام للثقافة الكونفوشيوسية، وهو ما يسمح للـ"هوا" بالسيطرة على الأراضي الخصبة وسط الصين¹.

بصيغة أخرى، يتكون العالم وفق رؤية المركزية الصينية من دوائر ثلاث تُحيط بالصين التي تشكل المركز، الدائرة الأولى تتشكل من الصينيين سواء كانوا جنوداً أو فلاحين والذين غزو أراضي مجاورة للمركز وأعلنوا الولاء للصين، الدائرة الثانية تتشكل من الأتباع من غير الصينيين والذين يجب أن يعلنوا الخضوع والتبعية للصين، الدائرة الثالثة تتشكل من البرابرة وهم خارجون عن القانون كما يمكن أن يكونوا أعداء للصين².

تغير الجيوبوليتيك الكونفوشيوسي مع وصول سلالة "كينغ" من الـ"ي Yi" إلى الحكم، إذ انتقل مفهوم الـ"هوا" العرقي ليدل على "الأمة الصينية"، وأصبح الـ"ي" يدل على الأجنبي الذي يجب أن يدفع الجزية ويُظهر الإعجاب والخضوع للصين من أجل الحفاظ على التناغم والسلام حسب التقاليد الكونفوشيوسية، لكن بعد حروب الأفيون مع بريطانيا والخسارة في حرب جياوو مع اليابان في 1894 استبدل مصطلح "ي" بـ"يانغ Yang" وهو مطلق أكثر حيادية وإيجابية في وصف الأجنبي³ بعد أن استشعرت الصين أن هذا الأجنبي أكثر قوة ويمكنه التفوق عليها.

¹ An Ning, *Confucian Geopolitics*. Springer Singapore, 2020, p 37-39.

² Jean-Vincent Brisset, *La chine, une puissance encerclée*, Paris: IRIS (collection Enjeux stratégiques), 2002, p 24.

³ An Ning, *Op.cit*, p 41.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

حدث التراجع الكبير عن مبادئ المركزية الصينية والتقاليد الكونفوشوسية بعد قيام جمهورية الصين الشعبية في 1949، حيث سيطرت الإيديولوجيا الشيوعية ومفاهيم الثورة الثقافية على الصين حتى سبعينيات القرن الماضي، لكن مع بداية الثمانينيات حدثت موجة من الإصلاحات والانفتاح على العالم خاصة مع تزايد الخلافات بين الصين والاتحاد السوفياتي، وهذا ما جعل الممارسات الجيوبوليتيكية الصينية تمزج بين المقوم الشيوعي والتقاليد الكونفوشوسية التقليدية، حيث تُركز على مفاهيم التناغم والتنوع والسلام في العالم.

يقول فرانسوا جوايو¹ François joyaux في تعليقه حول "المركزية الصينية" بأن "النظرية الجيوبوليتيكية الصينية لم تكن غائبة أبداً في يوم من الأيام" ويُضيف "إن التفكير النظري في العلاقات الخارجية للصين الشعبية يربطها مباشرة بالصين التقليدية، بكل ما فيها من الفكر الكونفوشوسي".

الفرع الثاني: الرؤية الماوية للعالم (نظرية العوالم الثلاث)

لطالما اعتبرت نظرية العوالم الثلاثة لـ "ماو تسي تونغ" نظرية علمية ماركسية وسلاحاً إيديولوجياً قوياً، لكنها في المحصلة تُعبر عن مقارنة جيوبوليتيكية نمطية للعالم، وعن الطريقة التي يرى بها الحزب الشيوعي مصالحه العالمية والتي غالباً ما كانت مرتبطة ارتباطاً وثيقاً بالجغرافيا، ومحاولة الحصول على نوع من الاستقلالية الذاتية للصين بعيداً عن طرفي الحرب الباردة.

يؤكد "ماو" رؤيته للعالم في خضم الثنائية القطبية بقوله "برأيي، إن الولايات المتحدة والاتحاد السوفياتي يشكلان العالم الأول، والقوى المتوسطة مثل اليابان وأوروبا وكندا، تشكل العالم الثاني، أما نحن فننتهي إلى العالم الثالث"، هذه المقولة لخصت المبادئ الجيوبوليتيكية للصين في عهد "ماو"، إذ حددت الصين عدوياً الأساسيين (الولايات المتحدة والاتحاد السوفياتي بعد 1952)، حلفاءها، ودورها كقائد للعالم الثالث.

لم يكن إلزام الصين صارماً بالمبادئ الجيوبوليتيكية وفق الرؤية الماوية، بل على العكس من ذلك أظهر الحزب الشيوعي قدرة هائلة على التكيف مع الظروف الدولية خدمة لمصالح

¹ جيرار ديسوا، مرجع سابق، ص 226.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

الصين الاستراتيجية، لذلك وصف "ديسوا" الجيوبوليتيك الصيني بالانتهازية، ويرصد "فرانسوا جوايو" التغيرات في الرؤية الصينية للعالم كما يلي¹:

- من العام 1949 إلى 1952 لم يكن أمام الصين خيار غير التحالف مع الاتحاد السوفياتي الذي قدم الدعم اللازم لتثبيت وتعزيز النظام الجديد في الصين.
- بعد الخلاف الأيديولوجي والاستراتيجي مع موسكو عادت الصين لمبادئ الرؤية الماوية، وحددت لنفسها "المنطقة المتوسطة" لتحافظ على مسافة بينها وبين موسكو.
- منذ العام 1965 وحتى بداية السبعينيات، إستعادت الصين أفكار النظرية الثورية مع شعار **لين بياو** "حصار الأرياف للمدن" وتطبيقه على صعيد الكوكب، إذ قامت حشود العالم النامي الذي تقوده الصين بمحاصرة الدول المتطورة.
- عمل **"دينغ كسياو بينغ"** ابتداء من 1974 على إعادة إحياء مفهوم "المنطقة المتوسطة" وضبطه على إيقاع نظرية العوالم الثلاثة، ومنذ توليه الرئاسة في العام 1978 تغيرت استراتيجية الصين ورؤيتها للعالم حيث بدأت في الاقتراب أكثر من الغرب والولايات المتحدة تحديداً، واشتهر بمقولته "ليس المهم أن تكون القطعة سوداء أو بيضاء طالما كانت تصطاد الفئران".

وعليه فإن المعيار الوحيد الذي تَحَكَّم في الكيفية التي توجه بها الصين نفسها تجاه العالم في تلك الفترة كان المصالح الاستراتيجية مع قدر هائل من البراغماتية متحررة من أية قيود إيديولوجية أو جيوبوليتيكية.

الفرع الثالث: أولوية التنمية على الجيوبوليتيكا

بداية من 1989 حدث تحول في التوجهات الجيوبوليتيكية الصينية حيث تراجعت الاعتبارات الإيديولوجية أمام تنامي المصالح الاقتصادية، تم ربط السياسة الخارجية الصينية بالتنمية الاقتصادية تماشياً مع استراتيجية الانفتاح على العالم الخارجي، وبما أن العلاقات مع دول العالم (خاصة الدول الكبرى) لم تعد ذات محصلة صفرية وفق الرؤية الجديدة للقيادة الصينية، فقد انتهجت دبلوماسية براغماتية جديدة وقامت ببناء علاقات جيدة مع الولايات المتحدة خصوصاً ومع الغرب وباقي دول العالم عموماً.

¹ نفس المرجع، ص 227.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

هذا التوجه الجديد للصين تم ضبطه وفق مفهوم "المصلحة الوطنية" ما سهل انضمام الصين لمنظمة التجارة العالمية في 2001 وفتح لها الأسواق العالمية إذ لا تخلو مدينة في العالم إلا وفيها منتج كتب عليه "صنع في الصين"، وفي المقابل، تضاعف الناتج المحلي الإجمالي وارتفع مستوى دخل المواطن الصيني، هذا التطور الاقتصادي الكبير جعل من الصينيين يؤمنون بأن الصين قد أصبحت قوية ويجب أن تحظى باحترام الآخرين، لذلك سعت القيادة الصينية للبرهنة على أنها من الآن فصاعداً "قوة مسؤولة" من خلال تعاملها بحذر شديد تجاه القضايا الإقليمية¹ (خاصة ما يسمى في التقاليد الصينية الأراضي المفقودة) التي قد تتسبب في مشاكل مع جيرانها أو مع القوى الكبرى، مع التمسك الشديد بقضيتين أساسيتين للصين هما: الحد الإقليمي الشمالي والمدى البحري.

الفرع الرابع: الإندفاع نحو آسيا ونحو العالم في عهد الرئيس "شي Xi"

ميّز وصول "شي" إلى السلطة بتخلي الصين عن عقيدة "تاو جوانج يانغ هوي" المحافظة التي تقول بأنه يجب على الصين "أن تراقب ببرود، وتؤمن مواقعها، وتتعامل بهدوء، وتخفي قدراتها، وتستغل الوقت، وأن تبقى بعيدة عن الأنظار، وأن لا تأخذ أبداً زمام المبادرة"²، هذه العقيدة ميزت السياسة الخارجية الصينية لعقدين من الزمن حتى العام 2012، إلا أن السياسة الخارجية لـ "شي" بدت أكثر اندفاعاً وحزماً خاصة ما تعلق بالقضايا الإقليمية في آسيا.

بعد وصول "شي" إلى السلطة قام بتأطير "الحلم الصيني" الذي كان بدأ في الانتشار في عهد سلفه "هو جينتاو" وفق رؤية الحزب الشيوعي الصيني، يقول "شي": "إن حلم الصين هو المعنى الداخلي لدعم وتطوير الاشتراكية ذات الخصائص الصينية" والتي جوهرها أن تكون الصين "بلداً غنياً وقوياً، يُنعش الأمة ويُعزز رفاهية الشعب"³، هذه "القوة" و"الغنى" الذان ورثهما "شي" جعلاً من القادة في الصين يتكلمون علانية وبقوة حول مواضيع الأراضي الصينية (قضية تايوان مثلاً) كما تزايد الحديث عن أن مشاكل آسيا يحلها الآسيويون أنفسهم في تحد واضح للهيمنة

¹ نفس المرجع، ص 230-235.

² Zhongying Pang, "From Tao Guang Yang Hui to Xin Xing: China's Complex Foreign Policy Transformation and Southeast Asia", ISEAS-Yusof Ishak Institute, N° 7, 2020.

³ Peter Ferdinand, "Westward ho—the China dream and 'one belt, one road': Chinese foreign policy under Xi Jinping", *International Affairs*, Vol 92, Issue 4, July 2016, Pages 941–957.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

الأمريكية في المنطقة، وجاء مشروع "حزام واحد، طريق واحد" ليعلن أن الصين تسعى للتمدد نحو أوروبا مروراً بـ "الهيرتلاند".

يقول قادة الصين بأنها لا تسعى أبداً للهيمنة لا إقليمياً ولا عالمياً بل تريد تحقيق مجتمع عالمي ذي مصير مشترك، تتساوى فيه الدول وتتنوع المجتمعات والحضارات المتناغمة ويسوده التعاون والسلام، إلا أن المشككين يرون في سياسات الصين في عهد "شي" بداية خروج التتين من جحره ليهيمن على مناطق آسيا والمحيط الهادي، ثم عبر الإكراه الاقتصادي الذي يحمله مشروع "حزام واحد، طريق واحد" يهيمن على العالم.

وبناء على ماسبق، وبالنسبة للفضاء السيبراني، فإن الصين لم تظهر كقوة سيبرانية إلا مع نهاية العقد الأول من القرن الحالي، لكن القادة في الصين افترضوا أن الريادة في التكنولوجيا السيبرانية ممكنة، كما يمكن من خلالها تعزيز وتأكيد الريادة الاقتصادية ومن الممكن الدفع بالصين إلى مراتب متقدمة في المجال العسكري، لذلك فإن الصعود التكنولوجي الصيني ورغبة الصين في أن تصبح قوة عظمى في الفضاء السيبراني يعكس من جهة تقاليد المركزية الصينية، فقوة شركات التكنولوجيا الصينية تُعبر عن قوة الحضارة الصينية وريادتها العالمية ما هي إلا عودة للوضع الطبيعي الذي يجب أن تكون عليه الصين، ومن جهة أخرى، فالتكنولوجيا هي أفضل مجال لتطبيق عقيدة "تاو" للصعود السلمي الهادئ بعيداً عن الأنظار في انتظار اللحظة المناسبة لإعلان "مجتمع المصير المشترك للبشرية" وفق التقاليد الكونفوشيوسية.

المطلب الثاني: الفضاء السيبراني كخيار استراتيجي للصين

يُمكن تحديد أربع استراتيجيات كبرى¹ وضعها القادة الصينيون منذ إنشاء جمهورية الصين الشعبية في 1949، بداية مع استراتيجية الثورة (1949-1977)، استراتيجية التعافي (1978-1989)، استراتيجية بناء القوة الشاملة (1990-2003) وأخيراً استراتيجية التجديد الوطني (2004-يومنا هذا)، ورغم الاختلافات بين هذه الاستراتيجيات في الأولويات والأساليب والموارد إلا أنها تتفق حول أهداف ثابتة ومستمرة وهي ضمان سلامة الأراضي الصينية ومنع القوى الأجنبية من السيطرة على منطقة آسيا والمحيط الهادي، إضافة إلى هدفين أضيفا بعد العام 1978 هما: خلق

¹ لا توجد وثيقة رسمية تحمل عنوان "الاستراتيجية الكبرى" للدولة ولكن يمكن استنباطها من خلال الوثائق الاستراتيجية التي تصدرها الهيئات الرسمية المدنية والعسكرية في الدولة وتصريحات المسؤولين الكبار في الحكومة والجيش، تركز في الغالب على الأهداف ذات المدى الطويل وتصاغ بعبارات شاملة وواسعة.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

بيئة دولية مواتية للتنمية الاقتصادية وأن يكون للصين دور في تشكيل النظام العالمي المتغير، مع التركيز على الهدف الأسمى وهو جعل الصين أقوى¹.

إن هدف "الصين القوية" أو كما يُعبر عنه الرئيس "شي" بالحلم الصيني ماهو إلا انعكاس لمجموعة من العناصر هي: اقتصاد قوي، نظام سياسي قوي ومجتمع مستقر، يحمي كل هذا جيش متطور وقوي، لكن مع بداية القرن الحالي برز الفضاء السيبراني كمحدد جديد للقوة وكان أثره واضحاً على باقي العناصر، فالاقتصاد توجه نحو الاقتصاد الرقمي، والمجتمعات والأنظمة السياسية تأثرت بالتهديدات الجديدة عبر الأنترنت، والجيش جعلت من الفضاء السيبراني ساحة جديدة للمعارك.

لذلك، قام القادة الصينيون بإعادة تقييم الوضع الجديد واستفادوا من دروس الثورات الملونة والربيع العربي وكيف تُشن الحروب الجديدة عبر الأنترنت، كما استفاد قادة الجيش الصيني من دروس حربي العراق وكوسوفو وأدركوا ما يحمله الفضاء السيبراني من تحديات وفرص للجيش خاصة، وللمجتمع والاقتصاد والنظام السياسي في الصين عموماً، وعليه، فقد حدث تحول في كيفية بناء الاستراتيجيات الصينية في المجالات المتعددة نحو جعل الفضاء السيبراني المصلحة الأكثر أهمية والتي من خلالها يُمكن تحقيق بقية المصالح والأهداف الاستراتيجية الكبرى للصين.

إن الفهم الصحيح لمحركات السلوك الصيني والسياسات المتبعة في الفضاء السيبراني يعتمد على فهم المصالح الاستراتيجية للصين في هذا الفضاء، هذه المصالح عبر عنها الرئيس "شي" في الاجتماع الأول للمجموعة القيادية للأمن السيبراني وأمن المعلومات في 2014² حيث شدد على الأولوية القصوى للمجال السيبراني كمبادرة استراتيجية كبرى لها تأثيرات سياسية، اقتصادية وعسكرية، كما أشار إلى أن الحكومة المركزية تعتبر أمن الشبكات والمعلومات مكونين رئيسيين لكل من الأمن القومي والتنمية الوطنية، وعليه، فإن عمليات التطوير والابتكار التكنولوجي يعكس رغبة الصين في تحقيق فضاء سيبراني (على الأقل في الداخل) آمن وحديث يضمن لها الاستقرار

¹Andrew Scobell, et all, **China's Grand strategy: Trends, Trajectories, and Long-Term Competition**, Cal: RAND Corporation, 2020, p 11.

² 新华网[شين هوا نت], 习近平:把我国从网络大国建设成为网络强国 [شي جين بينغ: تحويل الصين من قوة [سيبرانية كبرى إلى قوة سيبرانية عظمى], xinhuanet.com , February 27, 2014, URL : <http://bit.ly/3JQjcNX>.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

الاجتماعي-السياسي، التنمية الاقتصادية والأمن القومي، خاصة أن جيش التحرير الصيني يُخطط لاحتمال نشوب حروب وصراعات مستقبلية في الفضاء السيبراني.

الفرع الأول: المصالح الاستراتيجية الاقتصادية

يرتبط صعود الصين على الساحة الدولية مباشرة بالاقتصاد، فخلال ثلاثة عقود الماضية حققت الصين ما أُطلق عليه المعجزة الاقتصادية، إذ حافظت على معدل نمو سنوي يعادل أو يفوق 10% ما جعلها ثاني أكبر الاقتصادات في العالم بعد الولايات المتحدة، هذا النمو الاقتصادي المطرد كان نتيجة العولمة الاقتصادية ما مكن الصين من الوصول إلى مختلف الأسواق العالمية، كما ترافق مع بروز التكنولوجيات الرقمية وظهور الاقتصاد الرقمي حيث تُشير الإحصائيات إلى أن حجم الاقتصاد الرقمي في الصين ارتفع من 1,6 تريليون دولار سنة 2012 إلى 6,7 تريليون دولار سنة 2021 وهو ما يمثل 39,8% من الناتج المحلي الخام¹.

لكن انخفاض معدلات نمو الاقتصاد الصيني في السنوات العشر الماضية وما خلفته جائحة كورونا من تباطؤ في الاقتصاد العالمي، من جهة، والتوجه العالمي السريع نحو تكثيف المعاملات الرقمية في مختلف المجالات الاقتصادية، من جهة أخرى، عزز رؤية القادة الصينيين للفضاء السيبراني كأبرز دعامة استراتيجية للاقتصاد، ووضعهم أمام تحديات كبرى يجب مواجهتها وفرص يجب استغلالها.

يبرز التحدي الأكبر للصين في المحافظة على معدل نمو اقتصادي مقبول في حدود 6%، ولتحقيق هذا المعدل تسعى الحكومة الصينية؛ أولاً، تأمين البنية التحتية السيبرانية التي تضمن تدفق المعاملات التجارية والمالية، ثانياً، ضمان مستوى عال من التحكم في الفضاء السيبراني الداخلي والمشاركة في جعل الفضاء السيبراني العالمي آمناً من أجل الاستفادة القصوى من النمو الكبير للاقتصاد الرقمي العالمي.

إضافة إلى ما سبق، يعلب أمن الأنترنت دوراً استراتيجياً في حماية وتطوير الاقتصاد الصيني، فمن جهة، تسعى الحكومة الصينية لمحاربة مجرمي الأنترنت المحليين لجعلها منصة آمنة وموثوقة للمعاملات الاقتصادية الحالية والمستقبلية، ومن جهة أخرى، لم تتوقف الصين (كما

¹ Shi Yue & Xu Zihe, **Achievements in building China's strength in cyberspace in the past decade**, globaltimes.cn, Aug 19, 2022, URL: <http://bit.ly/42t4803>.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

تتجهما الولايات المتحدة) عن التجسس السيبراني لأغراض اقتصادية، ذلك أن سرقة الأسرار الاقتصادية والملكية الفكرية تساهم في تسريع عمليات سد الفجوة التقنية بين الصين ومنافسيتها، وعليه، فإن الفضاء السيبراني يُعتبر مجالاً حيوياً للصين من أجل المحافظة على مركزها الاقتصادي المتقدم ثم الدفع بها لقيادة العالم في المجال الاقتصادي بشقيه التقليدي والرقمي.

الفرع الثاني: المصالح الاستراتيجية السياسية

تتميز الصين بنظامها السياسي شديد المركزية، حيث يُسيطر الحزب الشيوعي الصيني على مفاصل الحكم، كما أن التطور الاقتصادي والمجتمعي في الصين يعود في المقام الأول إلى الحكمة الكبيرة التي يُدير بها الحزب البلاد وفق نسخة الرئيس "شي" لـ "حلم الصين"، في المقابل، تخطى عدد مستخدمي الإنترنت في الصين عتبة المليار مستخدم، كما تطورت أساليب التدخل في الشؤون الداخلية للدول عبر الهندسة الاجتماعية وحشد الشعوب ضد حكوماتها.

من خلال المعطيات السابقة، تقطن قادة الصين في وقت مبكر للتهديدات التي يشكلها الفضاء السيبراني على استقرار النظام السياسي في الصين، إذ نجد الرئيس "شي" في خطابه العامة يشدد دائماً على أن أمن الشبكات ركيزة استراتيجية للأمن القومي كما يرأس شخصياً مجموعة القيادة المركزية لأمن الإنترنت والمعلومات ويقود السياسة السيبرانية من أعلى، إضافة إلى الدور الذي يقوم به "الجدار الناري العظيم" من مراقبة صارمة لحركة الإنترنت في الداخل الصيني، ذلك أن التحكم في إدارة ونشر المعلومات عبر شبكة الإنترنت في الداخل يخدم العديد من الأهداف:

- الحفاظ على سمعة الحزب الشيوعي كقائد للبلاد نحو التطور والريادة.
- استباق الاحتجاجات ذات الطابع السياسي (المطالبة بالديمقراطية، حقوق الإنسان، حقوق الأقليات وغيرها) وفهمها وإدارتها.
- مراقبة المعارضين السياسيين وأنصارهم.

لذلك تقترح الصين طريقة متميزة لحوكمة الإنترنت تختلف عن المفاهيم الغربية للتدابير الوقائية، فقدمت مفهوم "السيادة السيبرانية" ودافعت عنه كمقاربة عادلة وفعالة لطريقة إدارة وحوكمة الإنترنت، والذي يدعو في جوهره على أنه من حق الدول (أو الحكومات) أن تتحكم في الفضاء السيبراني الوطني الخاص بها، وهذا ما يسمح لها بشرعنة "مراقبة حركة الإنترنت" داخل حدودها.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

أما على المستوى الخارجي، تستخدم الصين الأنترنت في سياستها الخارجية كنوع من القوة الناعمة لشرح مواقفها ورؤيتها حول القضايا الإقليمية والعالمية، حيث تُتهم الصين بتوظيف جهات فاعلة - أو لا تمنعها من العمل - لأغراض تجسسية عبر الفضاء السيبراني على حكومات الدول الأخرى والمنظمات الدولية للاستفادة من ميزة سياسية في العلاقات الدولية، إضافة إلى القدرة التي تحصل عليها في توجيه الرأي العام الدولي لدعم مقارباتها أو على الأقل التعاطف معها.

وعليه، فالفضاء السيبراني هو الركيزة الاستراتيجية الأولى للحكومة الصينية في الحفاظ على الاستقرار السياسي داخلياً وإقناع المجتمع الدولي بأن الصين أصبحت قوة سياسية مسؤولة في الشؤون السياسية الدولية خارجياً.

الفرع الثالث: المصالح الاستراتيجية العسكرية

تشير منشورات أكاديمية العلوم العسكرية (AMS) التابعة لجيش التحرير الصيني والمعنونة بـ "علم الاستراتيجية العسكرية" في إصدارها الثالث (2013) إلى أن الحروب المستقبلية قد تبدأ في الفضاء الخارجي والفضاء السيبراني وأن "الوصول إلى الهيمنة الكاملة وتحقيق الانتصار على القوى المعادية يتطلب تحقيق الهيمنة في الفضاء الخارجي والفضاء السيبراني"¹، كما يؤكد الإصدار الرابع (2020) على أن التطور والانتشار السريع للأنترنت ساهم في تطور النزاعات العسكرية في الفضاء السيبراني من البسيط إلى المعقد، ومن المتسويات المنخفضة إلى المستويات العالية، وأن من يسيطر على المعلومات والشبكات سيمتلك العالم كله².

من جهة أخرى، يستمد جيش التحرير الصيني عقيدته الأمنية وتعليماته ومهامه من الحزب الشيوعي الصيني، فالجيش له ارتباط وثيق بالحزب منذ استقلال الصين في 1949 - هناك من يجادل بأن الجيش في خدمة الحزب وليس في خدمة الوطن - لذلك فـجيش التحرير الصيني له مهام تتعدى حماية الأمن القومي في المجال العسكري إلى المجالات الأخرى كالاقتصاد والمجتمع، وبما أن الفضاء السيبراني أصبح ركيزة للحفاظ على سيرورة هذه المجالات فإن مهام جيش التحرير الصيني تتكيف مع هذه التطورات كما يلي³:

¹ Shou Xiaosong & all, **Science of Military Strategy (2013)**, Traduction in English: China Aerospace Studies Institute, Academy of Military Science, Beijing: Military Science Press, 2013, p 96.

² Xiao Tianliang & all, **Science of Military Strategy (2020)**, Traduction in English: China Aerospace Studies Institute, National Defense University Press, Beijing, 2020, p 148.

³ **Ibid**, p 148-149.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

- ضمان الانتصار في الحروب، بما أن الفضاء السيبراني هو ساحة الحرب الجديدة فإن السيطرة عليه هو مفتاح النصر، لأنه أصبح يُعتبر مركزاً لساحة المعارك الحالية والمستقبلية المتعددة الأبعاد.

- حماية الأمن القومي في بعده الاقتصادي والمجتمعي، فالتشغيل الآمن للبنية التحتية السيبرانية للدولة يضمن استمرارية تشغيل بقية البنى التحتية الحيوية كالطاقة، الخدمات المصرفية والمالية، الاتصالات وغيرها، لأنه بمجرد أن تصبح البنية التحتية السيبرانية غير آمنة قد يتسبب ذلك في فشل الأجهزة الدولة بأكملها، فقدان سيطرة الحكومة وتفشي الإضطرابات المجتمعية وفي النهاية يؤدي إلى إنهاء الدولة ككل، وعليه فمصير الأنظمة الوطنية التي تقتدر إلى الوسائل الاستراتيجية للصراع العسكري في الفضاء السيبراني هو الانهيار والزوال.

وبناء على ما تقدم، فإن جيش التحرير الصيني يعتبر الفضاء السيبراني البعد الخامس للحروب، والساحة الجديدة للمعارك، والركيزة الاستراتيجية الأولى للفوز بها، كما أنه يمثل فرصة تاريخية لتحديث قدراته العسكرية والوصول بها إلى مستوى جيوش الدول العظمى بحيث يكمنه منافستها والتغلب عليها.

المطلب الثالث: الاستراتيجية السيبرانية الصينية: الصين الرقمية، من فوجيان نحو العالم

تتميز الصين بنظام حكم شديد المركزية، فالحزب الشيوعي الصيني هو من يُقرر الاستراتيجيات والتوجهات ويُصدر القوانين التي تحكم الصين في مختلف المجالات داخلياً وخارجياً، وذلك من خلال الخطط الخماسية التي تنبثق عن مؤتمرات الحزب التي تُعقد كل خمس سنوات، إضافة إلى تقارير وخطابات أمينه العام رئيس الدولة وهذه في مجملها هي المصادر الرئيسية التي يجب على الجميع في الصين حكام المقاطعات والإداريين والشركات والعمال تنفيذها واتباعها بدقة.

لا يختلف الأمر كثيراً فيما يخص الفضاء السيبراني، فإن الوثائق الرسمية -على قلتها- يتم نشرها عبر وسائل الإعلام الرسمية باللغة الصينية وهذا ما جعل تفاعل الباحثين قليلاً عبر العالم، ومن أبرز وأهم الوثائق الرسمية الصينية التي تُظهر توجهات القيادة الصينية وطريقة تعاملها مع قضايا الفضاء السيبراني هي: "قانون أمن الفضاء السيبراني" الذي أُقر في 2016 ودخل حيز التنفيذ في جوان 2017، الكتاب الأبيض الذي حمل عنوان "البناء المشترك لمجتمع المستقبل المشترك في الفضاء السيبراني" الذي صدر عن المكتب الإعلامي لمجلس الدولة الصيني في

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

نوفمبر 2022، وأخيراً "خطة التخطيط الشاملة لبناء الصين الرقمية" التي قدمها الإعلام الرسمي الصيني في فيفري 2023 والتي حددت نظرة القادة الصينيين الشاملة والمستقبلية للفضاء السيبراني، لذلك سوف يتم التركيز عليها وتحليلها بعمق في هذا المطلب.

تُعد "خطة التخطيط الشاملة لبناء الصين الرقمية" من أبرز وأحدث الوثائق الرسمية التي توضح وجهة نظر القيادة الصينية نحو التكنولوجيا والفضاء السيبراني ومستقبلهما، تم إصدارها من طرف اللجنة المركزية للحزب الشيوعي ومجلس الدولة عقب المؤتمر العشرين للحزب المنعقد في نوفمبر 2022، وظهرت في وسائل الإعلام الرسمية للحزب باللغتين الصينية والإنجليزية في فيفري 2023، وهو ما يتعبّر سابقة في تاريخ الوثائق الرسمية الصينية ويعكس رغبة القيادة الصينية في توجيه رسائل إلى العالم بأن الصين تسعى من خلال هذه "الخطة"¹ لتكون نموذجاً ناجحاً في النمو التكنولوجي وتدعو العالم للتعرف على الصين الرقمية المتطورة.

من المنظور الشامل والاستراتيجي للتنمية حسب ما يراه القادة الصينيون فإن "الخطة" هي استراتيجية شاملة لبناء الصين الرقمية، حيث تُقدم الإيديولوجية التوجيهية، الأهداف الرئيسية والمهام والإجراءات الأساسية لتنفيذ وحماية عملية البناء، لأن الصين الرقمية في نظر الرئيس "شي" والحزب عموماً هي المحرك الأهم لبلوغ التحديث ذو النمط الصيني، وتمنح الصين ميزة أساسية في المنافسة العالمية في العصر الرقمي، في حين يرى المراقبون الغربيون² أن "الخطة" هي أول استراتيجية رقمية كبرى في العالم، وأن جذورها الماركسية تُصبغ عليها طبيعة تحويلية وتنافسية شديدة، كما تسعى لخلق أول "مجتمع ذكي" في العالم كنموذج ناجح من الاشتراكية طوال صراعها التاريخي مع الرأسمالية، وإذا نجحت سيدخل العالم "عصر الابتكار الصيني" ويجلب للصين مكانة كقوة عظمى عبر مجالات إستراتيجية متعددة مدنية وعسكرية.

الفرع الأول: الأصول الفكرية لـ "الخطة"

تُعد "الخطة" نتيجةً لدمج ثلاثة عناصر (مسارات) رئيسية في مسيرة التحديث والتطوير والمنافسة مع الولايات المتحدة في الفضاء السيبراني، وهو ما عرف لاحقاً بالثالث الرقمي: الصين الرقمية، القوة السيبرانية العظمى، المجتمع الذكي.

¹ تستعمل وسائل الإعلام الصينية عند الحديث على "خطة التخطيط الشاملة لبناء الصين الرقمية" اختصار "الخطة" وتستعمل الدراسة نفس الاختصار في متن هذا المطلب.

² David Dorman & John Hemmings, "Digital China The Strategy and Its Geopolitical Implications", *Pacific Forum International, Issues & Insights*, Vol 23, Wp 2, Feb 2023.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

أولاً، مفهوم "الصين الرقمية" والتي تعود نشأته إلى الجهود التي بذلها الرئيس "شي" عندما كان حاكماً لمقاطعة "فوجيان" لرقمنة الإدارة والاقتصاد في المقاطعة في بداية الألفية الحالية، ففي العام 2000 تبنى "شي" حاكم المقاطعة آنذاك مفهوم "فوجيان الرقمي Digital Fugian" بناءً على اقتراح من نائب رئيس جامعة "فوتشو"¹، حيث أظهر "شي" بصيرة عميقة في رؤية الفرصة والقدرات الكبيرة التي تتيحها التكنولوجيا لتحسين الإدارة المحلية وزيادة الأداء الاقتصادي وكانت تلك المبادرة في إطار التجارب المبكرة للحكومة الالكترونية في الصين، وتُشير وسائل الإعلام الرسمية إلى أن الرئيس "شي" قد اتخذ القرار الاستراتيجي الرئيسي لبناء الصين الرقمية مباشرة بعد انعقاد المؤتمر الثامن عشر للحزب في 2012، إلا أن المصطلح لم يظهر للعلن إلا في خطاب "شي" في المؤتمر الثاني للأنترنت 2015 Wuzhan، وتم اعتماده رسمياً في الخطة الخمسية الثالثة عشر للحزب في 2016 ثم تم رفعه إلى استراتيجية وطنية للمعلومات في مؤتمر الحزب التاسع عشر في 2017، كما أكد الرئيس "شي" على المفهوم جنباً إلى جنب مع مفهومي "بناء قوة سيبرانية عظمى" و"المجتمع الذكي" في رسالته الموجهة إلى قمة الصين الرقمية الأولى في فوتشو (فوجيان) في 2018²، وفي نفس السياق كتبت صحيفة "قوانغمينغ ديلي" على صفحتها الأولى في 23 أبريل 2018 "من فوجيان الرقمي إلى الصين الرقمية، كان التفكير الاستراتيجي للأمين العام "شي جي بينغ" بشأن بناء الصين الرقمية متسقاً، في خط واحد مستمر، ومتصل بقوة بالفكر والنظرية"، بعد ذلك تعدد ظهور المصطلح في وسائل الإعلام والتصريحات الرسمية وتوسع ليشمل العديد من المجالات ويصبح مرادفاً لعملية التحديث وفق النمط الصيني لبلوغ تجديد الأمة العظيم في آخر وثيقة استراتيجية صادرة عن الحزب "الخطة" في 2023.

ثانياً، مفهوم "القوة السيبرانية العظمى" والذي تشكل بناءً على اقتراح من المنظر "زينج بيجيان Zheng Bigian" الذي قدمه للسلطات المركزية في بكين في 2013 والذي دعا فيه إلى أنه يجب على الصين أن تسعى لبناء نفسها كقوة سيبرانية عظمى خلال 10 سنوات مستنداً إلى تقييمه لسياسة الاحتواء التي تقوم بها الولايات المتحدة وأنها انتقلت من الفضاء المادي إلى الفضاء السيبراني وأن الصين الصين بحاجة للرد، حيث يقول بأن "الحرب السيبرانية لم تعد مسألة ما إذا كانت الصين تريد القتال، ولكن كم من الوقت قبل تُجبر على التصرف"³، تم اعتماد مقترحات

¹ David Dorman & John Hemmings, *Ibid*.

² انظر: رسالة الرئيس "شي" يهنئ فيها افتتاح أول قمة حول بناء الصين الرقمية في 2018 على الرابط:

<https://bit.ly/3MMNlyU>

³ David Dorman & John Hemmings, *Ibid*.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

ثانياً، العام 2035، وهو موعد تحقيق الريادة في التطور الرقمي، حيث تصبح الصين رائدة في التنمية الرقمية في مجالات الاقتصاد والسياسة والثقافة والمجتمع والبيئة، وبذلك يكتمل النموذج الصيني الرقمي.

الفرع الثالث: الإطار العام لتنفيذ "الخطة"

يُرمز للإطار العام لتنفيذ الـ "الخطة" بالرمز 2522 (انظر الشكل رقم: 12) وهو شعار مصمم خصيصاً لتسهيل تذكر وفهم عناصر استراتيجية بناء الصين الرقمية من طرف الكوادر والمواطنين.

شكل رقم 12: الإطار العام للبناء الرقمي في الصين (مترجم).

المصدر: تقرير التنمية الرقمية في الصين 2022 الصادر عن إدارة الفضاء السيبراني الصينية CAC.



الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

وتدل الأرقام 2-2-5-2 في الإطار العام للـ "الخطة" على:

أولاً، الأساسان (2): تضع "الخطة" أساسين ضروريين لبناء الصين الرقمية، الأساس الأول هو وجود بنية تحتية رقمية من النوع الجديد، حيث يجب تحويل البنية التحتية التقليدية إلى بنية رقمية مع تطوير بنية رقمية جديدة مكونة من مزيج من تقنيات 5G و 6G والأنترنيت الصناعي وشبكات الأقمار الصناعية وغيرها، وتعتبر الصين هذه البنية الجديدة الداعم الرئيس والضمان المادي للثورة الجديدة في التكنولوجيا والتحول الرقمي، أما الأساس الثاني فهو نظام موارد البيانات الضخمة، حيث تُعتبر صناعة البيانات الضخمة كصناعة استراتيجية ناشئة تقوم على توليد البيانات وجمعها وتخزينها ومعالجتها وتحليلها وخدمتها، وهي الدعم الرئيسي لتفعيل إمكانات عناصر البيانات ومحرك مهم لتسريع تغيرات الجودة والكفاءة والقوة للتنمية الاقتصادية والاجتماعية.

ثانياً، الخطة المتكاملة ذات المجالات الخمس (5)

تهدف الـ "الخطة" لتحقيق التجديد العظيم للأمة وجعل الصين أول وأكبر دولة رقمية في العالم، لذلك فقد وضعت إطاراً للعمل على جميع القطاعات والمستويات من أجل الدمج العميق للتكنولوجيا الرقمية مع الاقتصاد، الحكومة، المجتمع، الثقافة والبيئة، حتى يصبح الكل رقمي والكل مترابط، وتزداد فرص نجاح التحديث ذي النمط الصيني ليصبح نموذجاً عالمياً جذاباً تقتدي به دول العالم، ففي مجال؛

الاقتصاد، تُشير الـ "الخطة" إلى ضرورة التمكين الكامل للتنمية الاقتصادية، دمج الاقتصاد التقليدي بالاقتصاد الحقيقي، والسعي لجعل الاقتصاد الرقمي أقوى وأفضل وأكبر، وبناء مجموعة اقتصادية رقمية لها قدرات تنافسية دولية.

الحكومة، تطوير حكومة رقمية فعالة ومنسقة، تسريع وضع الأنظمة والقواعد وتعزيز بناء القدرات الرقمية وتحسين مستوى الخدمات الحكومية الرقمية.

المجتمع، بناء مجتمع رقمي شامل ومستقر، يتميز بتوفر الخدمات الرقمية، التعليم الذكي، الصحة الرقمية، تعزيز الحوكمة المجتمعية، تعميم الحياة المجتمعية الذكية وتجربة الخدمات المجتمعية الرقمية المستقبلية.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

الثقافة، خلق ثقافة رقمية مزدهرة تُعزز الثقة بالنفس لدى المواطن الصيني، حيث يتم رقمنة ما هو موجود من مواد ثقافية وتشجيع خلق وإبداع مواد ثقافية رقمية صحية وتقديم نموذج ثقافي رقمي رائد.

البيئة، بناء حضارة بيئية رقمية خضراء وذكية، وبناء نظام رقمي ذكي لتعزيز الحماية المتكاملة والإدارة المنهجية للموارد البيئية، الدعوة إلى نمط حياة أخضر وذكي.

وعليه، فإن خطة المجالات الخمس تسعى لتنمية متزامنة لمختلف المجالات (الكل في واحد) من خلال دمج التكنولوجيا الرقمية في مختلف نواحي الحياة.

ثالثاً، القدرتان (2)

يُشير إطار عمل الـ "الخطة" إلى سعي الصين إلى تطوير وتعزيز قدرتين رئيسيتين وحاسمتين لبناء الصين الرقمية، **الأولى** تتعلق بتعزيز **الأمن السيبراني الشامل**، ويتم من خلال بناء حاجز أمني سيبراني يضمن بيئة آمنة وموثوقة ويمكن التحكم فيها، حيث يتم تطوير الأنظمة والقدرات والقواعد والمعايير لبلوغ مستوى الأمن الشبكي الفعال، والثانية تتعلق ببناء **نظام ابتكار للتكنولوجيا الرقمية يعتمد على الذات (محلي)**، ويتم ذلك من خلال خلق بيئة دافعة للابتكار وتحقيق اختراقات تكنولوجية (الذكاء الاصطناعي الحوسبة الكمومية الرقائق ...).

رابعاً، البيئتان (2)

يتم تنفيذ الـ "الخطة" بالتزامن في بيئتين: محلية ودولية، **محلياً** يتم بناء نظام بيئي عادل وموحد للحكومة الرقمية، من خلال وضع وتحيين القوانين والقواعد والمعايير اللازمة للتحويل الرقمي مع التركيز على تصفية (تنقية) الفضاء السيبراني المحلي والشبكات النظيفة، أما **دولياً** تسعى الـ "الخطة" لبناء هيكل مفتوح ومربح للجانبين في المجالات الرقمية من خلال التخطيط الشامل للتعاون الدولي، إنشاء نظام دولي للتبادل والتعاون في المجالات الرقمية مع **تنسيق** متعدد المستويات ودعم متعدد المنصات ومشاركة متعددة الموضوعات.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

الفرع الرابع: التداعيات الجيوبوليتيكية لـ "الخطة"

ترتبط إستراتيجية بناء الصين الرقمية ارتباطاً وثيقاً مع رؤية الرئيس "شي" وجهوده كقائد للأمة الصينية ومنظر جديد للماركسية، فالتحديث على النمط الصيني التي تقوده التكنولوجيا تطور في خط مستمر من فكرة لـ "شي" كحاكم محلي إلى رؤية مركزية للحزب الشيوعي الصيني ترسم مستقبل الصين ومستقبل العالم.

على مستوى **التنظيم**، يردد القادة ووسائل الإعلام في الصين مصطلح "الفوز بالمستقبل" والذي يُشير في الغالب إلى الدور المركزي الذي من المتوقع أن تلعبه استراتيجية بناء الصين الرقمية في إعادة البناء الماركسي لـ "قوى الإنتاج"، حيث أصبحت البيانات الضخمة عامل إنتاج إلى جانب الأرض والعمل ورأس المال والتكنولوجيا، وبذلك حصل تحديث لأفكار المادية التاريخية في النظرية الماركسية وخلق مصدراً جديداً للتغيير في المجتمعات البشرية، حتى إن البعض يجادل بأن "شي" قد قام بوضع أسس "الماركسية الرقمية" أو "الماركسية 2.0" وبالتالي فقد أعاد تعريف المنافسة العالمية بين القوى العظمى.

أما على المستوى **الميداني**، فاستراتيجية الصين الرقمية تتمحور حول الفوز بالعصر الرقمي، فمساراتها الثلاث تتوجه نحو مركز واحد هو السيطرة على الفضاء السيبراني وعلى العالم، فالصين الرقمية ذات طبيعة **تحويلية** تنقل المجتمع والدولة في الصين إلى الحالة الرقمية المثلى، والقوة السيبرانية العظمى هي الأداة الرئيسية لكسب **الصراع (التنافس)** العالمي، وحوكمة البيانات الضخمة والتي تراه الصين عامل الإنتاج المهم للتنمية والتحديث وفق النمط الصيني يراه خصومها وسيلة لتقوية **النظام الاستبدادي** للحزب الشيوعي، فالـ "الخطة" هي استراتيجية شاملة تحويلية، شديدة التنافسية واستبدادية.

يعتقد الرئيس "شي" أن التحديث وفق النمط الصيني والذي يعتمد على التحول الرقمي للتحديث الاشتراكي يمنح الصين **الأفضلية محلياً** من خلال تحسين الكفاءة المجتمعية والعدالة الاجتماعية، و**التفوق عالمياً** وتحدي استراتيجية الاحتواء الأمريكية من خلال تقديم نموذج متطور من الاشتراكية الرقمية التي تتفوق على الرأسمالية، ذلك أن التغلب على ما تعتبره بكين نظاماً مهيمناً من القواعد والمؤسسات العالمية التي تركز توافقات العصر السابق، يمر حتماً عبر الباب

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

الذي فتحه العصر الرقمي لمراجعة هذه القواعد، لذلك فالصين الرقمية تسعى إلى المرور أولاً عبر المدخل.

تؤمن الصين بأن الوضع العالمي غير المستقر من حيث تعدد الأقطاب العالمي، وإفرازات العولمة الاقتصادية، وبروز التنوع الهوياتي والثقافي، والتشبيك الاجتماعي الرقمي العالمي، والتغيير العميق في نظام الحوكمة العالمية، يمنح من يتفوق (يحتل الريادة) في الفضاء السيبراني القدرة على اغتنام الفرصة الأولى، والفوز بالميزة، والفوز بالأمن، والفوز بالمستقبل.

المطلب الرابع: سياسات الصين للهيمنة في/على الفضاء السيبراني

تعددت سياسات الصين لبلوغ الريادة في الفضاء السيبراني، وجاءت ضمن جهود الصين في إطار التنمية الشاملة وتسريع التحديث وفق النمط الصيني، من هذه السياسات ما تم تربيته ليصبح استراتيجية وطنية ومنها ما تم صياغته في شكل مبادرات ومشاريع للتنمية، والهدف الأسمى فيما تعلق منها بالجانب الرقمي كان تطوير قدرات التكنولوجيا الرقمية داخل الصين لتبلغ مستوى قدرات الولايات المتحدة وتتجاوزها ومن ثم نشرها خارج الصين مع امتلاك القدرة على حمايتها، وترسم هذه السياسات خطاً يبدأ بتطوير سريع للتكنولوجيا المحلية مع السعي إلى نشرها بكثافة خارج الصين وتوفير حماية عسكرية موثوقة لما يرافقها وما ينتج عنها اقتصادياً، سياسياً، عسكرياً ومجتمعياً، ومن أهم وأبرز هذه السياسات نذكر مايلي:

الفرع الأول: استراتيجية صنع في الصين 2025 (Made In China 2025)

أطلق رئيس الوزراء الصيني "لي كه تشيانغ" في 2015 مبادرة "صنع في الصين 2025" وهي خطة استراتيجية وطنية مدتها عشر (10) سنوات لتحديث قاعدة التصنيع في الصين، ويتم ذلك من خلال التركيز على التصنيع الذكي بتسريع التطوير في عشر (10) صناعات (قطاعات) عالية التقنية، وكان الهدف المعلن للاستراتيجية هو تأمين مكانة الصين كقوة عالمية في صناعات التكنولوجيا الفائقة، تقليل اعتماد الصين على واردات التكنولوجيا الأجنبية والاستثمار بكثافة في تطوير الابتكار المحلي من أجل إنشاء شركات صينية قادرة على المنافسة محلياً وعالمياً، كما ترى الصين في الاستراتيجية فرصة للاندماج الكامل في سلسلة التصنيع العالمية والتعاون بشكل أكثر فاعلية مع الاقتصادات الصناعية.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

تسعى الصين من خلال استراتيجية "صنع في الصين 2025" إلى إنهاء الاعتماد على التكنولوجيا الأجنبية ورفع قدرتها التصنيعية والتصنيع الذكي من خلال ضمان أن الابتكار وجودة المنتج والكفاءة والتكامل يدفع التصنيع في القطاعات العشر المستهدفة، مع التركيز على تكنولوجيا المعلومات والاتصال من الجيل الجديد، الروبوتات، البيانات الضخمة والذكاء الاصطناعي، كأولية قصوى، إضافة إلى صناعة الطيران والفضاء، الهندسة البحرية العالية التقنية، السكك الحديدية، الطاقة والطاقة المتجددة، المعدات الطبية الحديثة، المعدات الزراعية، هذه القطاعات تُشكل صلب ما يسمى "الثورة الصناعية الرابعة" والتي تعتمد على دمج البيانات الضخمة والحوسبة السحابية والتقنيات الناشئة المختلفة في سلسلة التصنيع العالمية.

أولاً، التكتيكات المتبعة لتنفيذ استراتيجية "صنع في الصين 2025"

تعمل الصين على تسريع الجهود الموجودة مسبقاً من خلال تخصيص المزيد من الموارد وتكثيف التخطيط المركزي للتنسيق بين الحكومة والشركات الخاصة والجامعات ومراكز البحث والتطوير، وتشمل هذه التكتيكات:

أ. **تحديد الأهداف بدقة**، حيث إنه من خلال تحديد الأهداف العامة والتنسيق شبه الرسمي تشجع الحكومة الصينية الشركات (العامة والخاصة) على مؤامة عملية صنع القرار فيها مع أولوياتها الاستراتيجية.

ب. **تقديم الدعم المباشر**، زادت الحكومة الدعم المباشر للقطاعات (الصناعات) المستهدفة من خلال التمويل الحكومي الكبير والقروض منخفضة الفائدة والإعفاءات الضريبية وغيرها من الإعانات.

ج. **الاستثمار الأجنبي والاستحواذ**، حيث يتم تشجيع الشركات الصينية (العامة والخاصة) على الاستثمار في الشركات الأجنبية -ولا سيما شركات أشباه الموصلات- للوصول إلى التكنولوجيا الفائقة، إذ بلغت قيمة عمليات الاستحواذ الصينية في الولايات المتحدة الأمريكية ذروتها في العام 2016 بأكثر من 45 مليار دولار.

د. **تعبئة الشركات المدعومة من الدولة**، يأتي الكثير من هذا الاستثمار من الشركات المملوكة للدولة، أو الشركات والصناديق المدعومة من الحكومة، لذلك فإن العديد من شركات التكنولوجيا

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

الكبرى في الصين (مثل Huawei و ZTE) رغم أنها شركات خاصة إلا أنها تتلقى دعماً قوياً من الحكومة.

هـ - اتفاقيات نقل التكنولوجيا، حيث يتعين على الشركات الأجنبية الراغبة في الإستثمار أو القيام بأعمال تجارية في الصين الدخول في مشاريع مشتركة مع الشركات الصينية بموجب شروط تتطلب منها مشاركة الملكية الفكرية الحساسة والمعرفة التكنولوجية المتقدمة.

ثانياً، التداعيات الجيوبوليتيكية لاستراتيجية "صنع في الصين 2025"

يجادل القادة الصينيون بأن سيطرة الدولة على السياسة الصناعية أمر ضروري لرفع دخل الفرد في الصين الذي لا يزال أقل بكثير منه في الدول المتقدمة، إضافة إلى السعي لامتلاك القدرة على المنافسة في الأسواق العالمية الشديدة والسريرة التقلب، كما أن استراتيجية "صنع في الصين 2025" ما هي إلا نسخة مستلهمة من السياسات الصناعية للدول المتقدمة (خطة تطوير الصناعة 4.0 الألمانية) وأما القوانين الحمائية والدعم الحكومي فهو أمر قامت به كل الدول المتقدمة الناجحة في بداياتها (الو.م.أ، كوريا الجنوبية وغيرها).

في المقابل، يرى السياسيون في الولايات المتحدة والغرب عموماً أن استراتيجية الصين الصناعية هي استراتيجية تحويلية تسعى لتغيير مستقبل الصناعة والتجارة العالميين، فهي تُشوه الأسواق العالمية بإعطاء الأولوية للاعتبارات السياسية على الحوافز الاقتصادية، كما أنها تُشكل تهديداً مباشراً للابتكار العالمي.

يُشير تقرير صادر عن معهد ميركاتور للدراسات الصينية في 2016¹ أن سعي الصين للتحول إلى قوة عظمى في الصناعات عالية التقنية له تداعيات خطيرة على الدول الصناعية (الو.م.أ، الاتحاد الأوروبي، اليابان، كوريا الجنوبية) ويهدد مكانتها الريادية في الاقتصاد العالمي، ذلك أن إستراتيجية الصين تؤكد على بلوغ نسبة 70% من "الاكتفاء الذاتي" في المكونات والمواد الأساسية في الصناعات المستهدفة بحلول العام 2025 وهذا ما يدمر اقتصادات الدول التي تُشكل فيها هذه الصناعات عالية التقنية نسباً عالية من دخلها القومي (مثل: ألمانيا، كوريا الجنوبية)، إضافة إلى أن سلاسل التوريد للمنتجات عالية التقنية عادة ما تتوزع عبر العديد من الدول، غير أن استراتيجية الصين عازمة على استيعاب سلسلة التوريد

¹ Jost Wübbke, et all, **MADE IN CHINA 2025**, Mercator Institute for China Studies, December 2016, URL: <https://bit.ly/3qjGdkY>.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

العالمية للمنتجات عالية التكنولوجيا بالكامل وهو ما يجعل صناعات استراتيجية كاملة تحت سيطرة قوة جيوبوليتيكية واحدة منافسة (كما تصنفها الو.م.أ والغرب).

من جهة أخرى، يتعدى التهديد الذي تحمله إستراتيجية "صنع في الصين 2025" الجانب الاقتصادي إلى الجانب الأمني، ففي داخل الصين تُسيطر الحكومة على تدفق البيانات والمعلومات في الفضاء السيبراني وهو ما يؤثر على استخدام تطبيقات الأعمال للشركات الأجنبية العاملة في الصين ويكشف معلوماتها الحساسة وينتهك حقوق الملكية الفكرية، أما على المستوى الدولي، فقد أشار تقرير صادر عن البنّاغون حول إستراتيجية الصين لنقل التكنولوجيا¹ بأن "صنع في الصين 2025" تُشكل تهديداً حقيقياً للأمن القومي الأمريكي، حيث أقر بأن الصين سرعت من عمليات الاندماج والاستحواذ على شركات التكنولوجيا الناشئة في الولايات المتحدة عبر شركات صينية مدعومة من الدولة، وحيث إن التقنيات التي تستثمر فيها الصين هي نفسها التي تستثمر فيها الولايات المتحدة وتعتمد عليها وزارة الدفاع الأمريكية لبناء التفوق العسكري، فإن سرعة تطوير هذه التقنيات ذات الاستخدام المزدوج (تجاري-عسكري) لها تأثير على طبيعة الحرب وتحدد من يكسب حروب المستقبل، ويضيف التقرير أنه "إذا سمحنا للصين بالوصول إلى هذه التقنيات في نفس الوقت، فلن نفقد تفوقنا التكنولوجي فحسب، بل قد نساهم في التفوق التكنولوجي الصيني"²، فالتفوق التكنولوجي كما له دور في الريادة الاقتصادية له دور حاسم في التفوق العسكري وحماية الأمن القومي.

الفرع الثاني: مبادرة طريق الحرير الرقمي (Digital Silk Road)

جاءت مبادرة طريق الحرير الرقمي (DSR) كجزء من مبادرة أكبر هي "الحزام والطريق" التي تم طرحها في 2015، والتي قدمتها الصين كطريق للتعاون المربح للجميع لتعزيز التنمية المشتركة وتحقيق الرخاء المشترك، وكروية اقتصادية كبرى للانفتاح والتعاون بين دول آسيا، أوروبا وإفريقيا، ومثل طريق الحرير الرقمي الوجه التكنولوجي (السيبراني) من المبادرة، كما قدم الرئيس "شي" في خطابه في افتتاح منتدى الحزام والطريق في 2017 المجالات التي تشملها مبادرة طريق الحرير الرقمي، حيث صرح بأنه "يجب متابعة التنمية المدفوعة بالابتكار وتكثيف التعاون في المجالات الرائدة مثل الاقتصاد الرقمي والذكاء الاصطناعي وتكنولوجيا النانو

¹ Michael Brown , Pavneet Singh, **China's Technology Transfer Strategy**, Defense Innovation Unit Experimental (DIUx), January 2018, URL: <https://bit.ly/45DyRcf>.

² Ibid.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

والحوسبة الكمومية، ودفع تطوير البيانات الضخمة والحوسبة السحابية والمدن الذكية من أجل تحويلها إلى طريق الحرير الرقمي للقرن الحادي والعشرين¹.

أولاً، التكنولوجيات المستهدفة في طريق الحرير الرقمي

شهد قطاع التكنولوجيا في الصين تطوراً سريعاً وكبيراً قادته شركات التكنولوجيا الصينية الكبرى مثل هواوي و بايدو وغيرهما أو كما يسميهم الرئيس "شي" "الأبطال القوميون" وقد قدم طريق الحرير الرقمي فرصة جديدة لهاته الشركات للتوسع خارج الصين وزيادة حجمها وخبرتها، ومن أهم التكنولوجيات التي تم التركيز عليها نذكر ما يلي²:

1. نظام بايدو للتجوال عبر الأقمار الصناعية (BDS): وهو النظام المماثل لنظام GPS

الأمريكي (العالمي)، لنظام BDS فوائد اقتصادية في تشغيل الآلات المدنية (سيارات، عتاد فلاح، هواتف.. إلخ) وفوائد عسكرية في تشغيل العتاد الحربي (طائرات، صواريخ غواصات... إلخ)، وعليه فالصين تسعى لنشر هذا النظام وتشجيع دول الحزام والطريق على استعماله كبديل موثوق للنظام الأمريكي GPS.

2. المدن الذكية وتقنيات المراقبة: قدمت شركات التكنولوجيا الصينية حلولاً مبتكرة لإدارة

المدن وذلك من خلال منصات المراقبة وتقنيات التعرف على الوجوه والبيانات الضخمة وقد ساعد في ذلك جائحة كورونا، وقد سارعت العديد من دول الحزام والطريق في إطار مبادرة طريق الحرير الرقمي إلى عقد اتفاقيات مع الصين لاقتناء التجهيزات والبرامج تحت ذريعة السيطرة على الوباء.

3. كوابل الألياف البصرية (الأرضية والبحرية): تستثمر الشركات الصينية في بناء وتوسيع

البنية التحتية الرقمية على طول دول الحزام والطريق، ويشمل ذلك كوابل الألياف البصرية الأرضية والبحرية، مراكز البيانات، الحوسبة السحابية، وهو ما يُعتبر تطوراً لبنية تحتية رقمية منفصلة أو مستقلة يمكن التحكم بها بعيداً عن إملاءات وتهديدات الولايات المتحدة.

¹ Xinhua, **Full text of President Xi's speech at opening of Belt and Road forum**, xinhuanet.com, 14 May 2017, URL: <https://bit.ly/45XZitx>.

² Anahit Parzyan, **China's Digital Silk Road: Empowering capabilities for digital leadership in Eurasia**, In: *China and Eurasian Powers in a Multipolar World Order 2.0*, Routledge, 2023, pp 178-181.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

4. **شبكات الجيل الخامس 5G:** تحت قيادة شركة هواوي تسعى الشركات الصينية للسيطرة على بناء شبكات الاتصال من الجيل الجديد عبر دول الحزام والطريق، حيث أحرزت الشركات الصينية اختراقات كبيرة لتقنيات 5G و 6G وبلغت الريادة في هذا المجال مما أعطاهم ميزة تنافسية ومصادقية كبيرة، كما تراهن الصين على هذه التقنية لإنجاح مبادرة طريق الحرير الرقمي في دول الحزام والطريق كمرحلة أولى، وفي النهاية عبر العالم.

5. **وضع قواعد جديدة للفضاء السيبراني:** وهو من الأهداف النهائية لمبادرة طريق الحرير الرقمي، حيث إن الاختراقات التكنولوجية الصينية خاصة شبكات 5G والذكاء الاصطناعي وانتشارها عبر العالم يُخول للصين وضع القواعد التي تُنظم هذا الفضاء، حيث ضاعفت الصين من جهود الدبلوماسية الرقمية وحوكمة الأنترنت المتعددة الأطراف، وهذا ما تخشاه الولايات المتحدة والغرب من أن تُصبح دولة استبدادية (كما يرونها) تضع القواعد والمعايير التي تحكم التكنولوجيا، ويحذرون من مستقبل يسوده الاستبداد الرقمي.

ثانياً، التداعيات الجيوبوليتكية لمبادرة طريق الحرير الرقمي

يقدم طريق الحرير الرقمي دعماً سياسياً لشركات التكنولوجيا الصينية -التي تعتبر محركاً رئيسياً للمبادرة- من أجل التوسع التجاري، كما يخدم رؤية الصين العالمية التحويلية في العديد من المجالات الأخرى.

نقلت مبادرة طريق الحرير الرقمي الصين من وضع الدفاع ومحاولة الإفلات من الاحتواء التكنولوجي الأمريكي إلى وضع الهجوم وجعل سياسات الولايات المتحدة مجرد رد فعل على النجاحات الصينية، وهذا ما جعل المنافسة الاستراتيجية في الفضاء السيبراني تشتد بين الصين والولايات المتحدة، مع توسع الخطوط الفاصلة في مجالات التأثير للتقنيات الصينية والغربية خاصة في منطقتي المحيطين الهادي والهندي.

تتهم الولايات المتحدة الصين بأنها تسعى لبناء عالم سيبراني بعيداً عن سيطرة الولايات المتحدة يكون نقطة الارتكاز في خطتها لاستبدال النظام الدولي الليبرالي الحالي بنظام جديد تهيمن عليه الصين "الاستبدادية"، ذلك لأن مبادرة طريق الحرير الرقمي تمنح الصين ميزة استراتيجية واقتصادية وعسكرية وتضعف القدرات الأمريكية، فاقتماداً، تساهم المبادرة في تطوير الاقتصاد الرقمي الجديد وهو ما يُعطي للصين أفضلية للهيمنة على الأسواق على حساب شركات

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

التكنولوجيا الأمريكية، وعسكرياً، سيطرة الصين على البيانات من خلال البنية التحتية والتقنيات الصينية الجديدة يمنح جيش التحرير الصيني قدرات تتحدى القدرات الأمريكية.

وفي نفس السياق، تُظهر خرائط الدول التي شملتها مبادرة طريق الحرير الرقمي أن الصين تبني هلالاً سيبرانياً حول قلب الأرض (في الجيوبوليتيكا الكلاسيكية) الذي طالما كانت القوى العظمى تسعى للسيطرة عليه، لتتحول المعادلة إلى أنه من يسيطر على الفضاء السيبراني يسيطر على قلب الأرض ومن يسيطر على قلب الأرض يسيطر على العالم.

الفرع الثالث: استراتيجية الاندماج العسكري-المدني (MCF)

يُعتبر النظام السياسي في الصين نظاماً "مدنياً" وتتسم الدولة بطابعها "الشعبي"، ف "الشعب" يحتل مكانة بارزة في البيئتين السياسية والعسكرية، فجذور الحزب الشيوعي الصيني المؤسس والحاكم لجمهورية الصين الشعبية تعود للشعب ويتكون أساساً من أفراد مدنيين، في المقابل، نجد أن جيش التحرير الشعبي الصيني والذي يخضع لسلطة الحزب تأسس بداية من أفراد الشعب (الفلاحين والعمال) ثم تطور إلى مستوى الجيش الاحترافي وأوكلت له مهمة ضمان الأمن والاستقرار في الداخل والدفاع عن الأمة ضد التهديدات الخارجية.

أولاً، تطور مفهوم الاندماج العسكري-المدني وفق الرؤية الصينية

بناءً على ما تقدم، وضمن السياق الذي تطورت ثلاثية الحزب-الجيش-الشعب فإن علاقة العسكري-المدني وفق الرؤية الصينية كانت دائماً تحكمها تصورات الحزب عن التنمية ودور الجيش فيها، وكيفية التعامل مع ضغوط الوضع الجيوبوليتيكي العالمي والتهديدات الخارجية، لذلك، يمكننا رصد أربع مراحل لتطور هذه العلاقة هي¹:

1. مرحلة "ماو تسي تونغ"، وتميزت في البداية بتسخير القدرات الصناعية المدنية من أجل الانتاج العسكري استجابة للتوترات والصراعات الإقليمية (الصراع في شبه الجزيرة الكورية)، ثم تلتها مرحلة إزالة خطوط الإنتاج المدنية من الإنتاج العسكري.

¹ Saurabh Dixit, "Military-Civil Fusion in China and lessons for India", SYNERGY, Vol 2, Issue1, February 2023, pp 88-105.

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

2. مرحلة "دينغ شياو بينغ"، أعطيت الأولوية للتنمية الاقتصادية وجاء تطوير الجيش والقدرات العسكرية في مؤخرة الأولويات، وتم إعادة توجيه القدرات والموارد العسكرية نحو التنمية الاقتصادية.

3. مرحلة "التكامل العسكري- المدني MFI"، ظهر المصطلح في الخطط الخمسية للحزب، وسعت الحكومة إلى بناء بيئة تكنولوجية-صناعية مدنية-عسكرية متكاملة لتلبية حاجة الجيش الوصول إلى تقنيات الدفاع المتقدمة.

4. مرحلة "الاندماج العسكري- المدني MFC"، كان الرئيس "هو جينتاو" أول من استخدم مصطلح "الاندماج" وتم اعتماده رسمياً في الخطة الخمسية الثانية عشر للحزب كخطة لإعادة الموازنة من جديد نحو تطوير التكنولوجيا العسكرية، وفي 2015 جعل الرئيس "شي" مواءمة تطوير التكنولوجيا المدنية والدفاعية أولوية وطنية، وتم ترقيتها إلى استراتيجية وطنية في مؤتمر الحزب التاسع عشر في 2017.

وعليه، فإن استراتيجية الاندماج العسكري-المدني حسب المفهوم الصيني مصممة لتحقيق التوازن بين الأمن والتنمية، وهي إجراء أساسي استجابة للتهديدات الأمنية المعقدة ووسيلة لاكتساب مزايا استراتيجية في المنافسة الدولية، ومن خلال تصريح الرئيس "شي" في حديثه إلى اللجنة المركزية لتطوير الاندماج العسكري-المدني في 20 جوان 2017 قال بأنه "يجب الإسراع في تشكيل نمط تنمية عميق للاندماج العسكري-المدني ذي العناصر الكاملة، والمجالات المتعددة، والعائد المرتفع، وبناء النظام الموحد للاستراتيجيات وبناء القدرات الاستراتيجية للصين بشكل تدريجي"¹، وعليه، يمكننا تحديد الأهداف القريبة المدى المتمثلة في:

1. تحقيق حالة من الاندماج العميق بين البنيتين "العسكرية" و"المدنية" في جميع المجالات وخاصة مجال التكنولوجيات الناشئة والفضاء السيبراني والتي ترتبط ارتباطاً وثيقاً بخلق وتطوير قدرات قتالية للعصر الرقمي.

2. تحسين تخصيص الموارد الوطنية لضمان الاستعداد القتالي والفوائد الاقتصادية في آن واحد.

أما الهدف النهائي للاستراتيجية فهو "البناء التدريجي لنظام الصين العسكري-المدني الموحد للاستراتيجيات والقدرة الاستراتيجية".

¹ Saurabh Dixit, **Ibid.**

الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء السيبراني

في الفضاء السيبراني، تدعو الاستراتيجية إلى تعزيز العمل المشترك العسكري-المدني (الموارد والمواهب) في بناء خط دفاع سيبراني قوي، حماية الأمن الإيديولوجي، ودعم الجيش بالتقنيات الأساسية والمعلومات، مع التركيز على التقنيات الناشئة وعلى رأسها الذكاء الاصطناعي الذي يرى فيه الجيش فرصة تاريخية لتخطي الأعداء المحتملين والفوز بالحروب المستقبلية¹.

ثانياً، التداعيات الجيوبوليتيكية لاستراتيجية الاندماج العسكري-المدني

رغم إقرار القادة الصينيين وبعض المفكرين الأمريكيين² بالصعوبات والتحديات والتعقيدات التي تواجه تطبيق الاستراتيجية فإن المفكرين وصناع القرار في الولايات المتحدة والغرب عموماً يرون في استراتيجية الاندماج العسكري-المدني الصينية تهديداً اقتصادياً وأمنياً مباشراً لهم، ذلك أن مجتمع البحث العلمي وشركات التكنولوجيا الناشئة ومن خلال تعاونهم مع الشركات الصينية المدنية يساهمون بشكل غير مباشر في تطوير الجيش الصيني ويمنحونه عن غير قصد ميزة إستراتيجية لتحدي -أو حتى التفوق على- جيش الولايات المتحدة.

يرجع ذلك في الأساس إلى أن حماية المصالح الصينية المتزايدة في الخارج (سواءً في الفضاء السيبراني أو الفضاء المادي) تتطلب حضوراً لجيش قوي قادر على حماية هذه المصالح بشكل فعال في مختلف أنحاء العالم، وهذا ما تسعى لتحقيقه استراتيجية الاندماج من توازن الأمن والتنمية، وهو ما يؤدي في النهاية إلى زيادة احتمال الصدام بين الصين والولايات المتحدة.

كذلك، ترى الولايات المتحدة أن النشر العالمي للتقنيات الناشئة والتي لها علاقة بالصناعات الدفاعية العسكرية يجب أن يُدرك (من طرف الحلفاء والشركاء) على أنه مصدر قلق مثل نشر الأسلحة نفسها، ذلك أن نجاح استراتيجية الاندماج العسكري-المدني الصينية يجعل من الصين قوة اقتصادية وعسكرية أكبر، ويحولها إلى قوة جيوبوليتيكية أكبر، وهذا بدوره يؤثر على التسلسل الهرمي الدولي للسلطة.

¹ Alex Stone, Peter Wood, **China's Military-Civil Fusion Strategy: A view from Chinese strategists**, China Aerospace Studies Institute, USA, 2020, p 99-102.

² Elsa B Kania, Lorand Laskai, **Myths and Realities of China's Military-Civil Fusion Strategy**, Center for a New American Security, Washington (DC), 2021.

بدأ الفصل في **مبحثه الأول** برصد لأبرز المقاربات النظرية والمنطلقات الفكرية الحديثة التي تُؤطر استراتيجيات وسياسات كل من الولايات المتحدة والصين في إدارتهما للصراع في وعلى الفضاء السيبراني، حيث تم إبراز تنامي دور شركات التكنولوجيا لتصبح لاعباً جيوبوليتيكاً هاماً على الساحة الدولية، وتحول الفضاء السيبراني إلى مجال جديد للنفوذ تتنافس الدول للهيمنة عليه، وهذا ما جعله مجالاً للعبة جيوبوليتيكية رقمية تسعى فيها القوى العظمى إلى ردع خصومها أو على الأقل تحقيق التوازن معها.

أما **المبحث الثاني**، فقد تطرق لاستراتيجيات الولايات المتحدة للهيمنة في/على الفضاء السيبراني، حيث بدأ بشرح للمبادئ الجيوبوليتيكية التي توجه القادة الأمريكيين في الفضاء المادي وإسقاطها على الفضاء السيبراني، وخُصص إلى أن الهيمنة هي السمة البارزة والتي تطورت نتيجة للكيفية التي يُدرك بها صانع القرار الأمريكي الفضاء السيبراني (مصالحه، أهدافه، مرتكزاته الفكرية وتفاعلات البيئة الاستراتيجية)، وهو ما ينعكس حتماً على كيفية بناء الاستراتيجيات السيبرانية التي توسع نفوذ الولايات المتحدة في الفضاء السيبراني والتي تطورت من الدفاع إلى الردع وصولاً إلى الدفاع إلى الأمام، وتطبيق استراتيجيات كبرى للسيطرة على الفضاء السيبراني واحتواء الصعود التكنولوجي الصيني مع تطوير استراتيجية لفك الارتباط لقطع الترابط التكنولوجي المعقد بين البلدين.

في **المبحث الثالث**، ومن أجل فهم أعمق لاستراتيجيات الصين للهيمنة على الفضاء السيبراني، تطرقنا للمبادئ الجيوبوليتيكية للقادة الصينيين وأثر الفكر الكونفوشيوسي في سعيهم لتحقيق حلم الصين كمركز للعالم، ثم تم التفصيل في رؤية الصين للفضاء السيبراني كخيار وأولوية استراتيجية من خلال فهم لمصالحها الاقتصادية، السياسية والعسكرية، وهذا ما ظهر جلياً في الاستراتيجية السيبرانية الصينية الأحدث أو ما يطلق عليها "الصين الرقمية" والتي تنتهي غاياتها بعالم سيبراني مركزه الصين، كما تم التفصيل في أبرز الاستراتيجيات والمبادرات الفرعية لتحقيق هذه الغاية، والكيفية التي تدعم بها استراتيجية "صنع في الصين 2025" لتطوير القدرات التكنولوجية مبادرة "طريق الحرير الرقمي" لتوسيع النفوذ تحت حماية جيش قوي بفضل استراتيجية "الاندماج العسكري-المدني".

الفصل الرابع

مآلات الصراع الأمريكي الصيني

في الفضاء السيبراني

يسعى الفصل الأخير من الدراسة إلى تقديم رؤية مستقبلية لصراع الهيمنة الأمريكي الصيني في/على الفضاء السيبراني، ويستعمل لهذا الغرض تقنية السيناريوهات حيث يبني الفصل ثلاثة سيناريوهات تتباين احتمالية تحققها، سيناريو ضبط الصراع في الفضاء السيبراني (التفائلي)، سيناريو استمرار الصراع (الخطي) وسيناريو التغيير (الراديكالي)، وننطلق في التحقق من إمكانية تحقق كل سيناريو واحتمالية حدوثه من رصد المعطيات والمؤشرات والمؤثرات الحالية والمستقبلية التي تدعم أو تدحض حدوث سيناريو ما، مع استكشاف مدى استعداد ورغبة الطرفين في توجيه الصراع نحو سيناريو معين.

المبحث الأول : ضبط الصراع في الفضاء السيبراني

من أجل ضبط الصراع في/على الفضاء السيبراني يجب على كل من الولايات المتحدة والصين الاتفاق على أن المعايير والقواعد تساهم بشكل فعال في تخفيف وتجنب الأزمات التي تهدد استقرار الفضاء السيبراني، كما يجب على البلدين تجنب سوء الفهم والتقيد بحسن النية وتقليل حالة عدم اليقين، من أجل الدفع بالعلاقة الثنائية نحو التعايش السلمي وتعزيز المنافسة الحميدة.

لكن في ظل تصاعد حدة الصراع في الوقت الراهن، فإن بلوغ مرحلة السلام والاستقرار في الفضاء السيبراني يتطلب تطور الصراع إلى أحد هذه الحالات:

- إقتناع (أو إستسلام) الصين بأن (لأن) قدراتها التكنولوجية -رغم حجمها الكبير- لا تمكنها من تحدي الولايات المتحدة ومن ثم قبولها بقيادة الولايات المتحدة كقوة مهيمنة.
- تحقيق الصين لاختراقات علمية كبرى وتحقيق تقدم تكنولوجي كبير مما لا يدع مجالاً للشك للولايات المتحدة بأن الصين أصبحت قوة معادلة لها، وبذلك تزداد إمكانية إلحاق الأذى المتبادل بين الطرفين فيما يشبه "الدمار المتبادل الأكيد" وفي هذه الحالة يحاول الطرفان التعايش السلمي والمنافسة الحميدة (تهدئة الصراع) لتحقيق المنفعة المتبادلة.
- دخول الاتحاد الأوروبي كطرف ثالث يحقق التوازن في اللعبة الجيوبوليتيكية الرقمية، مما يخفف من حدة الصراع ويُجبر الطرفين على تقديم تنازلات والعمل المشترك على استقرار الفضاء السيبراني.

المطلب الأول: المعايير والقواعد لضبط الصراع في الفضاء السيبراني

يبدو واضحاً أن الفضاء السيبراني أصبح مجالاً رئيساً للمنافسة الاستراتيجية العالمية، وأن الأدوات السيبرانية وسياسات الدول المتنافسة تُشكل تهديداً لاستقرار الفضاء السيبراني وتعمل على زعزعة علاقات الدول العظمى من خلال خلق تهديدات مباشرة لأمنها الاقتصادي والعسكري، من جهة أخرى، لطالما كانت المعايير والقواعد عاملاً مساعداً وأحياناً حاسماً في تقليل المنافسة وتعزيز الاستقرار من خلال تقييد سلوك الفاعلين.

الفرع الأول: المعايير والقواعد لاستقرار الفضاء السيبراني

تتفق كل من الولايات المتحدة والصين على مبدأ أن المشاركة المتعددة الأطراف القائمة على القواعد والمعايير توفر وسيلة أكثر فعالية للحد من التهديدات في الفضاء السيبراني، وذلك يرجع لعدة أسباب، أولاً، يمكن للمعايير والقواعد أن تغير سلوك الخصوم، ثانياً، المشاركة في وضع المعايير والقواعد يعطيها أكثر مصداقية وإلزامية من أن تفرضها دولة واحدة، ثالثاً، المعايير الثابتة تجعل من السلوك الذي تم تحديده من الصعب معارضته أو إزالته.

في الواقع، تظهر صعوبة كبيرة في استعمال المعايير والقواعد الدولية كوسيلة يمكن من خلالها تقييد سلوك المتنافسين (الولايات المتحدة والصين) وتهدة الصراع وتعزيز الاستقرار في الفضاء السيبراني، فالتاريخ مليء بانتهاكات الدولتين للقواعد الدولية في المجالات الأخرى (حقوق الإنسان، العدوان الدولي، الحد من الأسلحة وغيرها) لذلك تبدو المعايير والقواعد كأداة إشكالية عند استخدامها في تعديل سلوك القوى العظمى وتزداد تعقيداً في حالة الصراع التكنولوجي الأمريكي-الصيني، وذلك لعدة أسباب منها¹:

- لا يوجد اتفاق على شكل دقيق للمعايير اللازمة، كما أن المبادئ الأساسية الموجودة لا تحترمها الدولتان بل تواصلان العمل بحرية في الفضاء السيبراني بعيداً عن المساءلة.
- رغم توافق رؤى الدولتان على بعض قواعد السلوك في الفضاء السيبراني (عدم مهاجمة البنية التحتية الحيوية) إلا أن الفجوة لا تزال واضحة حول الكثير من القضايا مع عدم اليقين من أن الطرف الآخر مستعد للموافقة والالتزام طوعية بقيود جديدة.
- طبيعة الفضاء السيبراني التي تعيق تطوير المعايير، خاصة ما تعلق بعملية الإسناد الضرورية لفرض التكاليف على المخالف.
- تتطور بعض المعايير مع الوقت بشكل تدريجي، فمثلاً الدولتان تلتزمان بعدم الاعتداء على البنية التحتية الرقمية لبعضهما البعض.

يُقر "جوزيف ناي" بصعوبة الوصول إلى اتفاقية أو معاهدة دولية تعالج مجموعة واسعة من قضايا الفضاء السيبراني الإشكالية، لذلك فهو يقترح بناء نظام معقد لتطوير المعايير والقواعد، يتصف هذا النظام بالمرونة والقدرة على التكيف، حيث يتم تطوير الروابط بين القضايا

1 Michael J. Mazarr, et al, *Competition and Restraint in Cyberspace: The Role of International Norms in Promoting U.S. Cybersecurity*, Cal: RAND Corporation, 2022.

الخلافة والجهات الفاعلة المتنافسة بتكوين مجموعات أصغر تتوافق رؤاها حول قضايا محددة أقل (مثلاً معايير تطوير الذكاء الاصطناعي)، ومن ثم تتطور وتمتد إلى مجموعات أكبر، وهذه المرونة تمنح الدول والجهات الفاعلة غير الحكومية القدرة على التكيف مع حالة عدم اليقين¹ التي تتسبب فيها المنافسة الاستراتيجية بين الولايات المتحدة والصين.

بناءً على ما تقدم، فإنه رغم وجهات النظر المتباينة حول قضايا الحوكمة والسيادة والشكوك المتبادلة بين الولايات المتحدة والصين حول نوايا كل طرف في الفضاء السيبراني، إضافة إلى ما ستؤول إليه المنافسة التكنولوجية بين الطرفين على المدى المتوسط، سواءً تسليم الصين بقيادة الولايات المتحدة للفضاء السيبراني أو اقتناع الولايات المتحدة بندية الصين أو بروز الاتحاد الأوروبي كطرف ثالث موازن في اللعبة الرقمية، فإن القوة أو القوى الفاعلة المستقبلية في الفضاء السيبراني ستسعى إلى تطوير المعايير وقواعد السلوك الضرورية للمحافظة على وجود واستقرار الفضاء السيبراني حماية لمصالحها السياسية والاقتصادية والأمنية بغض النظر عن شكل أو طبيعة هذه المعايير والقواعد.

الفرع الثاني: التعاون لتطوير معايير الذكاء الاصطناعي

تتبع أهمية الذكاء الاصطناعي من خاصية الاستعمال المزدوج لتطبيقاته (مدنية-عسكرية) ليتحول إلى بنية تحتية حيوية يدخل في مختلف مجالات الحياة، كما يُتوقع أن يُضيف 13 تريليون دولار إلى الناتج الاقتصادي العالمي بحلول 2030²، لذلك أصبح من الضروري للدول تطوير أنظمة الذكاء الاصطناعي وتنظيمه للاستفادة من إمكاناته الهائلة ومحاولة تخفيف مخاطره بشكل كاف، وعليه، فالذكاء الاصطناعي يشهد تنافساً شديداً بين الجهات الخاصة والحكومية لتشكيله (حوكمته) من خلال تطوير المعايير التي تحكمه، فوضع المعايير وإنفاذها غاية تسعى لها العديد من الحكومات والشركات والهيئات الدولية والجهات غير الحكومية، كما تتباين العلاقة بينهم من التنافس الشديد إلى التعاون الوثيق خدمة لأجنداتهم التجارية والسياسية والأمنية المتباينة.

¹ Joseph S Nye Jr, **Normative Restraints on Cyber Conflict**, Belfer Center, Havard Kennedy School, August 2018, URL: <https://bit.ly/3KxRWUt>.

² Nora Von Ingersleben-Seip, "Competition and cooperation in artificial intelligence standard setting: Explaining emergent patterns", **Review of Policy Research**, 2023.

تتبنى أكثر من 60 دولة في العالم سياسات تنظيمية للذكاء الاصطناعي، وتتصدر الولايات المتحدة والصين الريادة في تطوير هذه التكنولوجيا والسيطرة على وضع المعايير الخاصة بها، من جهة أخرى، ونظراً للمخاوف المتزايدة حول مخاطر التطوير المتسارع للذكاء الاصطناعي والأسئلة الملحة حول السلامة وقضايا حقوق الإنسان والتمييز أصبح الذكاء الاصطناعي يطرح مخاوف عالمية، فالأمين العام للأمم المتحدة "أنطونيو غوتيريش" صرح بأن "تطوير الذكاء الاصطناعي لصالح الجميع يتطلب حواجز حماية تركز على حقوق الإنسان والشفافية والمسائلة"¹، كما حذر مفوض الأمم المتحدة السامي لحقوق الإنسان من أن التطوير غير المقيد للذكاء الاصطناعي يهدد بشدة الكرامة البشرية وحقوق الإنسان²، لذلك، فقد أصبح وضع معايير للذكاء الاصطناعي مهمة ومسؤولية الجميع.

نظرياً، يمكن أن تغطي المعايير دورة حياة الذكاء الاصطناعي (جمع البيانات، التدريب والتعلم المستمر، التصميم، الاختبار، التقييم والاستخدام) كما يمكن أن تأخذ المعايير شكل؛ **معايير تقنية** أو مواصفات فنية تطورها الشركات من أجل أهداف تجارية حيث إنه كلما احترمت الشركات المعايير التقنية المعترف بها في منتجاتها زادت إمكانية تسويق هذه المنتجات في أسواق أكبر، لذلك ففرص التعاون فيها كبيرة جداً لأنها تتحكم في عملية التطوير الهندسية للأنظمة.

معايير أخلاقية أو مبادئ توجيهية أخلاقية تطورها الدول والهيئات الدولية والمنظمات غير الحكومية تضمن أن النظام يمثل للمعيار الأخلاقي (كالشفافية، احترام الخصوصية وحقوق الإنسان وغيرها) ويخضع تطوير هذه المعايير إلى منافسة جيوبوليتيكية شديدة، ذلك أن حالة الفوضى في النظام الدولي وعدم اليقين تُثني الدول عن تطوير واحترام المعايير خوفاً من إستغلال الخصوم الفرصة للهيمنة المستقبلية اقتصادياً وعسكرياً.

في نفس السياق، ترفض الصين المعايير المقيدة للمراقبة الجماعية لأنها ترى فيها ضرورة لحكومة المجتمعات ذات التكتلات السكانية الضخمة، في المقابل، كانت الولايات المتحدة ضد تطوير معايير عالمية للذكاء الاصطناعي بحجة أنها تقيد شركاتها وتكبح الابتكار وتمنح الفرصة للخصوم (الصين) للفوز بالمنافسة التكنولوجية، إستمر هذا الرفض خاصة لمبادرة GPAI المنبثقة عن مجموعة G7 والداعية لتطوير معايير الذكاء الاصطناعي ضمن الدول ذات التفكير المماثل

¹ UN news, UN chief says regulation needed for AI to 'benefit everyone', UN.org, July 2023, URL: <https://bit.ly/3OrGqLl>.

² Ibid.

(أو الدول الديمقراطية) حتى العام 2020 عندما أدركت الولايات المتحدة أن الصين قد بدأت العمل على جعل أفكارها حول تنظيم الذكاء الاصطناعي معايير عالمية على مستوى مجموعة العشرين ومنظمة العفو الدولية والاتحاد العالمي للاتصالات¹.

ومما سبق، فإن الصراع بين البلدين حول المعايير والذي قد يؤدي إلى بيئتين منفصلتين لتطوير الذكاء الاصطناعي والمعايير الخاصة به يواجهه رغبة من أغلب الأطراف (الباحثين والمطورين في الولايات المتحدة والصين وعبر العالم وبقية الحكومات والمنظمات) في الحفاظ على وحدة الفضاء السيبراني والتعاون لتطوير معايير مشتركة كحتمية لتجنيب البشرية السيناريو الأسوأ أي خروج الذكاء الاصطناعي عن السيطرة وانقلابه ضد مصالح البشر، إضافة إلى الرغبة في ضمان الوصول بالذكاء الاصطناعي إلى كامل إمكانياته لحل المشكلات العالمية كالمناخ والغذاء وغيرها مع منع الأضرار والتخفيف من حدتها.

وعليه، فإن تطوير معايير عالمية تشترك فيها الولايات المتحدة والصين ينبع من حاجة البلدين للتعاون مع بعضهما البعض، فالولايات المتحدة وإن كانت تملك الريادة في الحوسبة والخوارزميات فإنها بحاجة إلى المزيد البيانات اللازمة لتعليم وتدريب الذكاء الاصطناعي، وكذلك الحال بالنسبة للصين فامتلاكها لحجم هائل من البيانات يعوقه ضعف في الحوسبة واعتماد على خوارزميات أمريكية المنشأ، وعليه فحاجة الولايات المتحدة الوصول إلى بيانات بحجم أكبر بما فيها البيانات الصينية وحاجة الصين للحوسبة والخوارزميات القوية، تمثل دافعاً قوياً للبلدين نحو التعاون ووضع معايير موحدة يشارك فيها أصحاب المصلحة من دول وحكومات لتوجيه الذكاء الاصطناعي نحو خدمة البشرية.

كذلك، فالذكاء الاصطناعي الذي يُعد من بين أهم مجالات المنافسة الاستراتيجية بين الولايات المتحدة والصين قد يكون السبب الرئيس في تقريب الرؤى بين الطرفين وتخفيف حدة المنافسة والدفع بالبلدين نحو التعاون من أجل ضبط للفضاء السيبراني.

¹ Ibid.

المطلب الثاني: الاتفاقيات الثنائية والمتعددة الأطراف لضبط الصراع في الفضاء السيبراني

في ظل تدهور العلاقات بين الولايات المتحدة والصين وتصعيد المنافسة التكنولوجية من كلا الجانبين يبدو الحديث عن عقد اتفاقيات أو معاهدات ثنائية أو متعددة الأطراف للتخفيف من حدة الصراع بين الطرفين في الفضاء السيبراني نوعاً من الترف العلمي، لكنه في الحقيقة ليس مستبعداً على الإطلاق، ذلك أن الأمثلة من التاريخ كثيرة سواء تلك المعاهدات التي أبرمت للحد من الأسلحة بين الولايات المتحدة والاتحاد السوفياتي في أوج الحرب الباردة، أو حتى الاتفاقيات المتعلقة بالفضاء السيبراني الثنائية منها والمتعددة الأطراف، بل إن الولايات المتحدة والصين وقعا على اتفاقية حول التجسس السيبراني في 2015 في ظل التوترات بين البلدين، وعليه، فإن المفاوضات المؤدية إلى اتفاقيات أو معاهدات حول الفضاء السيبراني يُمكن أن تكون خياراً سياسياً قابلاً للتطبيق لصناع القرار في البلدين.

الفرع الأول: الاتفاقيات الثنائية لضبط الصراع في الفضاء السيبراني

من أبرز الاتفاقيات الثنائية التي عقدها الطرفان المتعلقة بالفضاء السيبراني والتي لها بعد سياسي هي: الاتفاقية الأمريكية-الصينية 2015 حول التجسس السيبراني لأغراض اقتصادية والاتفاقية الصينية-الروسية 2015 المتعلقة بالأمن السيبراني، وبالمبحث في خلفية الاتفاقيتين نجد أن الاتفاقية الصينية-الروسية جاءت تحت عنوان "عدم الاعتداء" وتعميق التعاون في مجال الأمن السيبراني لضبط عمليات القرصنة بين مجموعات البلدين، إضافة تمهيد الطريق لوضع أرضية مشتركة للعمل من أجل "السيادة السيبرانية" في تحد للولايات المتحدة ومبدأ "الحرية السيبرانية"، أما فيما يخص الاتفاق الصيني-الأمريكي فقد جاء في وضع عالمي شهد حملة انتقادات وتحذيرات واسعة من التجسس الصيني لأغراض اقتصادية، لذلك فإن توجس الصين من العقوبات الاقتصادية الأمريكية التي كانت إدارة "أوباما" بصدد فرضها، وحاجة الصين للحفاظ على الاستقرار والسلام الدوليين وحماية سمعة الصين الاقتصادية العالمية خاصة في الفضاء السيبراني من أجل مواصلة صعودها وتطورها التقني دفع بالرئيس "شي" لإبرام اتفاقية مع الرئيس "أوباما" كان عنوانها البارز العمل على ردع التجسس السيبراني لأغراض اقتصادية¹.

¹ Adam Segal, "Chinese cyber diplomacy in a new era of uncertainty", **Hoover Institution**, Aegis Paper Series N° 1703, 2017, pp 1-23.

أما فيما يتعلق بنتائج الاتفاقيتين، فتأثير العامل الجيوبوليتيكي واضح للغاية حيث يؤثر على توقيت ومحتوى وأطراف ونتائج الاتفاقيات، ففي حين أن عمليات التجسس بين الصين وروسيا انخفضت بنسبة كبيرة مع تشكيل تحالف بين البلدين للدفاع عن "السيادة السيبرانية" في المحافل الدولية¹، نجد أن نتائج الاتفاق الصيني-الأمريكي جد هزيلة، حيث لم تتوقف عمليات القرصنة المتبادلة بين الطرفين بل تحولت إلى منافسة تكنولوجية شاملة، وعليه، فمن البديهي توقع مثل هذه النتائج فالاتفاق بين "الأصدقاء" المبني على الثقة المتبادلة يختلف جذرياً عن الاتفاق بين "الخصوم" الذي يحتاج إلى ضبط دقيق لآليات المراقبة والتحقق، مع وضوح تام للنتائج المترتبة عن مخالفة الاتفاق، وهو ما نجده في المعاهدات الخاصة بالسلح والسلاح النووي لكنه غائب عن الاتفاق الصيني-الأمريكي بسبب خصوصية الفضاء السيبراني.

وبناءً على ما تقدم، فإن إمكانية التوصل إلى اتفاقية ثنائية حول الصراع في الفضاء السيبراني بين الولايات المتحدة والصين في الوقت الراهن ضئيلة، لكن على المدى المتوسط هناك بعض المؤشرات التي ترجح سيناريو الاتفاق ولعل أهمها أن السياسة الخارجية الصينية الغالب عليها الهدوء والرزانة والسعي للحفاظ على الاستقرار الدولي في مختلف المجالات، كما أن الصين كانت دوماً تبادر إلى إبرام الاتفاقيات مع الأطراف الأخرى، من جهة أخرى، هناك من الأمريكيين من طالب باتفاقية سيبرانية مع روسيا² للحد من التهديدات السيبرانية الروسية، لذلك حتى وإن كان طلب إبرام معاهدة مع روسيا للتفرغ للصراع مع الصين، إلا أن هذا يُعزز من إمكانية التفاوض مع الخصم حتى في أوج حالات الصراع.

إضافة إلى أن استعداد الولايات المتحدة والصين لعقد اتفاقية ثنائية يعكس تقييماهما لعلاقات القوى وحسابات الربح والخسارة (فاعل عقلاني)، وعليه، يمكن رسم سيناريوهين يعتمد كل منهما على تطورات الابتكار التكنولوجي في الصين وإدراكات صانعي القرار في البلدين لقدرات كل منهما؛

السيناريو الأول يميل فيه ميزان القوة التكنولوجي إلى الجانب الأمريكي وتترك القيادة الصينية عجزها عن تحدي الهيمنة الأمريكية وترضخ لقيادة الولايات المتحدة للفضاء السيبراني، وفي هذه

¹ Yuxi Wei, **China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty**, University of Washington.com, June 2016, URL: <https://bit.ly/443P0Wn>.

² Robert G. Papp, **A Cyber Treaty with Russia**, Kennan Kable, N° 41, Wilson Center, March 2019, URL: <https://bit.ly/3DONNHU>.

الحالة تقبل الصين بالتفاوض مع الولايات المتحدة مدفوعة برغبتها في الحفاظ الاستقرار الداخلي على الأقل ومواجهة التحديات الاجتماعية والاقتصادية الوطنية، أما الولايات المتحدة فتفرض شروطها وتدعم هيمنتها على الفضاء السيبراني العالمي.

في السيناريو الثاني، تحدث حالة من التوازن التكنولوجي بين القوتين وتتكافئ القدرات ويدرك الطرفان أنه لا يمكن لأحدهما الانتصار على الآخر وأن الاستمرار في الصراع يستهلك جهود كلا البلدين، هذه الوضعية تعزز من إمكانيات التفاوض وإبرام اتفاقيات لضبط الصراع في الفضاء السيبراني وتقاسم المنافع مع تقديم تنازلات متبادلة حول القضايا المتنازع عليها ووضع آليات دقيقة لمراقبة بعضهما البعض، بغية توفير الجهد والمال الذي سينفق خلال المنافسة الاستراتيجية خصوصاً أن كلا البلدين يعاني ولو بدرجة متفاوتة من مشاكل اقتصادية واجتماعية داخلية.

الفرع الثاني: الاتفاقيات متعددة الأطراف

رغم أن الصراع التكنولوجي الراهن تبرز فيه الولايات المتحدة والصين كقوتين عظميين إلا أن القوى التكنولوجية الصغرى يمكن أن تلعب دوراً فعالاً في توسيع أي اتفاق ثنائي بين القوتين أو عقد مفاوضات حول اتفاقية جديدة متعدد الأطراف، ومن جهة أخرى، لا يزال النقاش مستمراً حول مدى صلاحية (جدوى) تطبيق القانون الدولي في الفضاء السيبراني وحول كيفية تطبيقه.

لا يوجد لحد الآن قانون دولي شامل مخصص للفضاء السيبراني (مع استثناءات قليلة لقضايا محددة مثل اتفاقية بودابست بشأن الجرائم الالكترونية 2001) وهذا يرجع لطبيعة الفضاء السيبراني المتغيرة والمتجددة باستمرار، كما أن شركات التكنولوجيا والجهات الخاصة كانت سباقة في الدعوة لحكومة الفضاء السيبراني ثم تبعتها الدول بحساباتها الجيوبوليتيكية بعد ذلك، هذا ما يُفسر ظهور مقاربة أصحاب المصلحة المتعددين لحكومة الفضاء السيبراني في البداية ثم جاءت بعدها مقاربة السيادة السيبرانية كرد فعل عليها، هذا التنوع في الفاعلين انعكس على تنوع الآراء والتوجهات فالبعض يجادل بأنه لا حاجة لقانون دولي جديد وأن قواعد القانون الدولي الحالي كافية لتنظيم سلوك الدول في الفضاء السيبراني وأن الإشكالية التي يجب معالجتها هي تفعيل وتحسين آليات المساءلة، لكن المعارضين يقولون بأن الثغرات الموجودة في القانون الدولي الحالي

والناتجة عن التطور التكنولوجي السريع يتطلب التفاوض على قواعد جديدة من خلال معاهدة دولية جديدة أو تطوير للقانون الدولي العرفي¹.

وإضافة إلى ما سبق، تنقسم جهود الفاعلين في مجال حوكمة الفضاء السيبراني إلى مسارين متعاكسين، المسار الأول يعمل على حماية الدولة من الناس؛ وأصحاب هذا المسار هي الحكومات التي تضع الأمن القومي كأولوية يجب حمايتها من القرصنة وسيطرة الشركات والمجموعات الإجرامية فهدفها هو وضع قواعد لردع هذه السلوكات في الفضاء السيبراني، أما المسار الثاني يعمل على حماية الناس من الدولة؛ ويجمع هذا المسار مجموعة متنوعة من أصحاب المصلحة المتعددين مثل شركات التكنولوجيا والمنظمات غير الحوكمية ومجموعة من الدول، ويتبنى قضايا الفضاء السيبراني المفتوح وحماية البنية التحتية الرقمية إضافة إلى قضايا الخصوصية وحقوق الإنسان والحرية.

كذلك، يمكننا ملاحظة تواجد مجموعة من المنتديات البارزة والتي قدمت مقترحات لوضع القواعد التي تحدد السلوك في الفضاء السيبراني نذكر منها: مجهودات الأمم المتحدة من خلال منتدى فريق الخبراء الحكوميين المعني بتعزيز السلوك المسؤول للدولة في الفضاء السيبراني في سياق الأمن الدولي والذي قدم تقريراً في جويلية 2021 ومجموعة العمل مفتوحة العضوية في اللجنة الأولى للجمعية العامة للأمم المتحدة والتي قدمت تقريرها النهائي في مارس 2021، مجموعة العمل المؤلفة من الأكاديميين وخبراء حلف الناتو واللجنة الدولية للصليب الأحمر الذين قدموا دليل تالين لتطبيق القانون الدولي في العمليات السيبرانية، والمبادرة الأبرز التي قدمها الاتحاد الأوروبي والخاصة بحماية البيانات "اللائحة الأوروبية لحماية البيانات" والتي تعتبر تقدماً كبيراً في التشريعات الإقليمية والدولية وما يميزها هو صفة الإلزام لجميع دول الاتحاد الأوروبي.

وبناءً على ما تقدم، ففي ظل استمرار وتصعيد الصراع التكنولوجي بين الولايات المتحدة والصين فإن إمكانية التفاوض حول معاهدة دولية بوجود أطراف أخرى تكاد تكون معدومة خاصة مع توسع استراتيجية الفصل التكنولوجي الأمريكية، فالفضاء السيبراني اليوم ينقسم إلى معسكرين، الولايات المتحدة وحلفائها وشركائها ممن استطاعت ضمهم إلى معسكرها بالتخويف أو بالضغط، من جهة، الصين والدول المناهضة للهيمنة الأمريكية، من جهة أخرى، لكن عند التمعن في موقع

¹ Duncan Hollis, **International Law and Cyberspace**, Carnegie Endowment For International Peace, June 2021, URL: <https://bit.ly/4543S8F>.

الاتحاد الأوروبي من المنافسة التكنولوجية بين القوتين ورؤيته لمستقبل الفضاء السيبراني، نجد رغبة لدى دول الاتحاد الأوروبي في لعب دور فعال في **حوكمة الفضاء السيبراني** (التقنيات التي تسمح للفضاء السيبراني العالمي بالعمل) وسعيه لتعزيز الريادة التكنولوجية الأوروبية¹، و**الحوكمة في الفضاء السيبراني** (كيفية استغلال الدول والشركات للفضاء السيبراني) من خلال تقديم الدعم لللائحة الأوروبية لحماية البيانات رغم محاولات الولايات المتحدة المتواصلة للتوصل إلى اتفاقية تسمح للشركات الأمريكية بنقل بيانات المواطنين الأوروبيين إلى الولايات المتحدة².

وعليه، فإن السيناريو المفترض يعتمد على بروز الاتحاد الأوروبي كقوة ثالثة ولو بدرجة أقل في المنافسة التكنولوجية لتصبح اللعبة الرقمية ثلاثية، ومن ثم فإن الولايات المتحدة والصين بدافع من التنافس مع الطرف الثالث أو رغبة في التوافق تجنباً للمزيد من تكاليف الصراع الثنائي قد يلجئان لإقترح التفاوض مع القطب الجديد أو قبول مقترحات يقدمها الاتحاد الأوروبي والتي تتبع من محاولته حماية مصالحه الاقتصادية والأمنية، وبالتالي يكون الأطراف الثلاثة أمام خيار الوصول إلى معاهدة متعددة الأطراف تتوسع لاحقاً لتشمل مختلف الدول وأصحاب المصلحة لإرساء القواعد الملزمة لتحديد سلوك الفاعلين في الفضاء السيبراني وجعله أكثر استقراراً وأمناً.

المطلب الثالث: إدارة المنافسة الاستراتيجية والتعايش السلمي النسخة 2.0

تشهد العلاقات الأمريكية-الصينية تدهوراً مستمراً وتصعيداً للصراع خاصة في شقه التكنولوجي، لقد انهار الإطار الأصلي للعلاقة بين الولايات المتحدة والصين والذي استمر أكثر من أربعة عقود والمبني على التعاون والشراكة ولم يتم التوصل لصيغة الإطار الجديد لحد الآن، فالاختلافات بين الطرفين عميقة وتقوض فرص التعاون الثنائي المستقبلي في الفضاء السيبراني، قد تكون "المنافسة الاستراتيجية" على المدى القصير والمتوسط هي الوضع الطبيعي للعلاقة بين البلدين، كما تزداد مخاطر التفسيرات الخاطئة وسوء الفهم لإجراءات ونوايا الخصم وتحولها إلى صراعات أكبر أو إلى حروب مادية، لذا ينبغي على الطرفين العمل على إدارة المنافسة بينهما من خلال وضع ترتيبات وآليات للحد من التصعيد وتجنب المواجهة والسعي إلى جعل المنافسة عادلة ومنصفة من أجل بلوغ مرحلة التعايش السلمي المفيدة لكلا البلدين وللعالم.

¹ انظر: الحزمة التشريعية الأوروبية لأشباه الموصلات، على الرابط: <https://bit.ly/456Y7H4>.

² Clothilde Goujard, Alfred Ng, **EU and US reach a deal to let data flow across the Atlantic**, politico.eu, July 2023, URL: <https://bit.ly/3qqjfsV>.

إن التاريخ الحديث يثبت أن العلاقة بين البلدين كانت مثمرة ومفيدة لكلا الطرفين، كما أن حكومتي البلدين لا تسعيان ولا تريدان الوصول بالصراع إلى مستوى الحرب، يدعو الرئيس الصيني "شي" إلى جعل المنافسة عادلة ومنصفة، مثل منافسة في مضمار السباق، وليس مثل الضرب في حلبة المصارعة¹، في المقابل، يُبقي صناع القرار الأمريكيون أبواب التعاون والتقارب مفتوحة.

الفرع الأول: رؤية الولايات المتحدة للتعايش السلمي

صنفت استراتيجية الأمن القومي 2017 الصين كـ"منافس استراتيجي" لكن النسخة نفسها نصت على أن "المنافسة لا تعني دوماً العداء، ولا تؤدي حتماً إلى الصراع" وعلى نهجها نصت استراتيجية الأمن القومي 2021 على أن "المنافسة الاستراتيجية لا تمنع ولا ينبغي أن تمنع العمل مع الصين"، حتى العسكريون كان لهم نظرة مؤيدة لمزيد من التواصل للحد من مخاطر التصعيد، ففي أوج تدهور العلاقات في العام 2021 صرح وزير الدفاع الأمريكي بأن الولايات المتحدة "لا تبحث عن صراع، نحن ملتزمون بعلاقة بناءة مع الصين"².

وفيما يتعلق بالفضاء السيبراني والتكنولوجيا، تعرضت استراتيجية الفصل التكنولوجي للنقد من قبل شركات التكنولوجيا التي تتوقع خسائر مالية كبيرة بخسارة السوق الصينية، كذلك الباحثون ودعاة التعاون³ - وإن كان صوتهم لا يزال خافتاً - يرون أن الفصل التكنولوجي قد خلق نوعاً من التذمر لدى الحلفاء والشركاء، كما أنه على المدى المتوسط قد يُحفز الصين على مضاعفة جهود الابتكار للحاق بالتكنولوجيا الأمريكية والتفوق عليها وبالتالي تكون نتائج الفصل معاكسة لأهدافه التي وضع لأجلها، أما بالنسبة للمجتمع الأكاديمي الأمريكي، أكد تقرير لمعهد ماساتشوستس للتكنولوجيا MIT أن هناك مجالات مهمة للبحث والتعليم سيكون فيها المعهد، والمجتمع الأكاديمي، والأمة، والعالم أفضل حالاً من خلال التعاون العلمي مع الصين بدلاً من تقليده⁴.

¹ 新华社[وكالة أنباء شينخوا]، 数字中国建设整体布局规划[إلى طريق البشرية إلى]، xinhuanet.com, Jan 2021, URL : <https://bit.ly/456T09R>.

² Fan Jishe, "Managing China-US "strategic competition": potential risks and possible approaches", **China International Strategy Review**, Vol 3, Issue 2, 2021, pp 234-247.

³ انظر: رسالة مفتوحة من مدير الأعمال الأمريكي مورييس جرينبيرج إلى الرئيسين "شي" و"بايدن" يدعوهم فيها إلى إصلاح العلاقات بين الصين والولايات المتحدة، والتي وقعها خبراء في السياسة الخارجية وخبراء في الاقتصاد ومفكرون آخرون، على الرابط: <https://bit.ly/3Yxz4uk>.

⁴ Richard Lester, et al, **University Engagement with China: An MIT Approach**, The MIT China Strategy Group, November 2022, URL: <https://bit.ly/3OVHcBG>.

انعكست هذه الرؤى على الموقف الأمريكي تجاه الصين، فرغم مواصلة إدارة الرئيس "بايدن" التوسع في ضوابط التصدير وإصدار قوانين لمنع الصين من الوصول إلى التكنولوجيات الحرجة فإن الصين شهدت بداية العام 2023 زيارات رسمية متعددة لسياسيين، قادة شركات تكنولوجية وشخصيات أمريكية، فوزير الخارجية "بليكن" بعد زيارته للصين صرح بأن "الهدف الواقعي" لسياسة الولايات المتحدة تجاه الصين هو "إيجاد طريقة للتعايش السلمي"¹، ووزيرة الخزانة الأمريكية بعد زيارتها للصين قالت بأن الولايات المتحدة "تسعى لإقامة علاقة اقتصادية بناءة وعادلة مع الصين ... وعلينا أن نعمل معاً عندما يكون ذلك ممكناً"²، إضافة إلى السياسيين توافد قادة كبريات شركات التكنولوجيا الأمريكية على الصين حيث قدم "تيم كوك" الرئيس التنفيذي لشركة "آبل"، "إيلون ماسك" مؤسس شركة "تسلا" ورئيس "تويتر" و"بيل غيتس" مؤسس شركة ميكروسوفت الذي أُنْتُقِل من طرف الرئيس الصيني "شي" والذي قال له بأنه "أول لقاء مع صديق أمريكي هذا العام"، ويرى المراقبون أن هذه الزيارات جاءت لتهدئة التوترات بين البلدين والتفاوض حول إمكانية مواصلة الاستثمارات والوصول إلى السوق الصينية في ظل التوترات الجيوبوليتيكية وعدم وضوح الرؤية المستقبلية³، كذلك التقى الرئيس الصيني "شي" الدبلوماسي السابق "هنري كيسنجر" الذي يعتبره الصينيون "صوتاً بعيد النظر وعقلاني بشأن العلاقات الأمريكية الصينية" حيث صرح بأن "العلاقات الأمريكية الصينية ذات أهمية حيوية لسلام وازدهار الولايات المتحدة والصين والعالم، وأنه على استعداد لمواصلة بذل الجهود لتعزيز التفاهم المتبادل بين الشعبين الأمريكي والصيني"⁴.

¹ Zhao Huanxin, Wang Qingyun, **Blinken: Peaceful coexistence 'base line' of ties**, chinadaily.com.cn, Juin 2023, URL: <https://bit.ly/3OTHEAL>.

² Janet L. Yellen, **Remarks by Secretary of the Treasury Janet L. Yellen on the U.S. - China Economic Relationship at Johns Hopkins School of Advanced International Studies**, treasury.gov, April 20, 2023, URL: <https://bit.ly/3DTBiuv>.

³ Tanaka Akito, Grace Li, **U.S. big tech won't shake its China addiction**, asia.nikkei.com, July 2023, URL: <https://bit.ly/3KFX7Bx>.

⁴ 孙成昊 [صن تشنغهاو], **百岁老人基辛格访华 · 释放了中美关系的何种信号？** [زيارة المنوي هنري]، **كيسنجر للصين: موانع الإشارات التي ترسلها العلاقات الأمريكية الصينية؟**, ciss.tsinghua.edu.cn, July 2023, URL: <https://bit.ly/3OVRbqQ>.

الفرع الثاني: رؤية الصين للتعايش السلمي

قدم "دا وي" ملخصاً للرؤية الصينية لتجاوز المنافسة الثنائية بين الولايات المتحدة والصين والحفاظ على الإتصال (العلاقات) وتحسينه مع الولايات المتحدة والعالم ككل¹، يرى "دا وي" أن القيادة تنطلق من ركيزتين أساسيتين، أولاً، الاستراتيجية الشاملة لتجديد الأمة الصينية، وثانياً، التغييرات الكبرى التي لم تحدث منذ قرن من الزمان.

منذ سبعينيات القرن المنصرم عملت الصين على تحسين بيئتها الدولية وهو ماسمح لها بتحقيق نمو اقتصادي كبير والذي أصبح يمثل جوهر التجديد العظيم للأمة الصينية، وللمحافظة على الوتيرة العالية للنمو يجب زيادة إنتاجية العمل والتي تتطلب بدورها العمل على محورين؛ **تقسيم العمل والتكنولوجيا**، وبسبب البيئة الدولية المعقدة وشديدة الترابط فإن كلا المحورين يتميزان بتوزيع عالمي شديد وسلسلة معقدة من الروابط الدولية لذلك فهما يفرضان على الصين توسيع الاتصال وزيادة الترابط وتحسين العلاقات مع كل دول العالم.

من جهة أخرى، يُعتبر صعود الصين السلمي التغير الكبير الأبرز في هذا القرن وهذا ما جلب لها تأثير المواجهة والقطيعة مع العالم خاصة مع الولايات المتحدة، هذه الأخيرة وتحت تأثير مخاوف جيوبوليتيكية بدأت سلسلة من سياسات الفصل وتقطيع سلاسل الترابط وبناء الجدران بين الصين والعالم، فالولايات المتحدة تسعى لفصل الصين عن العالم المترابط (الشبكة العالمية)، وعندما تحاول الصين الرد بأخذ احتياطاتها الأمنية فإن ذلك يتسبب في المزيد من قطع الاتصال مع العالم.

وعليه، ففي عالم مترابط شديد التعقيد يكمن التحدي الصيني في المحافظة وتحسين الاتصال مع الشبكات العالمية وفق معادلة مضبوطة من **الطرح والإضافة**، بحيث كلما كان الفصل (الطرح) في مكان معين سعت الصين إلى الربط (الإضافة) في مكان أو أمكنة أخرى حسب القدرات وحسابات الربح والخسارة:

1. في مجال القضايا الأساسية كالسيادة الإقليمية واستقرار النظام السياسي لا يمكن للصين سوى "الطرح" والرد بقوة مع تقييم مستمر لنتائج الرد وتعديله حسب الظروف الجديدة.

للفوز في مسابقات "المضمار والميدان" يجب [跑赢“田径赛”，需超越中美双边竞斗]، [دا وي] 达巍¹، [تخطي المنافسة الثنائية الأمريكية الصينية]، ciss.tsinghua.edu.cn، February 2023، URL:https://bit.ly/3YCBPKT.

2. في مجال التكنولوجيا قامت الولايات المتحدة بعمليات فصل "طرح" كثيرة لذلك على الصين إجراء تقييم دقيق لتأثير هذا "الطرح" والتركيز على تعزيز الاتصال "الإضافة" في الجوانب التي بقي فيها الاتصال (تقييم أين تحتاج إلى الرماح وأين تحتاج إلى الجسور).
3. إذا كانت الولايات المتحدة تقوم بـ "الطرح" مع الصين، فيجب على الصين أن تقوم بـ "الإضافة" في أوروبا، آسيا، أفريقيا والبلدان النامية الأخرى.
4. إذا قامت الولايات المتحدة بـ "الطرح" في قضية واحدة (التكنولوجيا) تقوم الصين بـ "الإضافة" في قضايا أخرى (التعاون الدولي حول المناخ، الأوبئة ... إلخ)
5. إذا كان الكونغرس يقوم بـ "الطرح" تسعى الصين لأن تقوم بـ "الإضافة" مع الحكومة، مجتمع الأعمال، الجامعات وغيرها.

وعليه، فإن رؤية القادة في الصين تتمحور حول استغلال كل فرصة سانحة لتحسين العلاقات وتكثيف الترابط مع العالم، وتجاوز المنافسة الثنائية مع الولايات المتحدة نحو التعايش السلمي والتعاون المفيد للجانبين.

وبناءً على ما تقدم، ومن خلال المعطيات والمؤشرات السابق ذكرها يتمحور سيناريو التعايش السلمي في نسخته الثانية حول بروز القوى التعاونية في كلا البلدين وتغليب المصالح الاقتصادية على المخاوف الجيوبوليتيكية من خلال إنشاء وتفعيل قنوات للحوار والتواصل حول القضايا الخلفية وتعزيز آليات التعاون في القضايا ذات الاهتمام العالمي.

المبحث الثاني: سيناريو استمرار الصراع: الحرب الباردة الجديدة

يُعتبر سناريو استمرار الصراع بين الولايات المتحدة والصين في الفضاء السيبراني السيناريو الأكثر ترجيحاً على المدى القريب والمتوسط، فالقدرات الكبيرة التي يملكها الطرفان والحسابات العقلانية لنتائج حرب مادية تنتج عن سوء تقدير (بشري أو ذكاء اصطناعي) لحدث سيبراني أو مادي تجعل من الصراع يستمر ويتطور ليصبح حرباً باردة شاملة محورها التكنولوجيا والفضاء السيبراني، تماشياً مع الحكمة الصينية لـ "صن تزو" حول كيفية الفوز على الخصم دون قتال.

المطلب الأول: محركات استمرار المنافسة الاستراتيجية

أثرت التغيرات العميقة والمتعددة في المشهد الاستراتيجي العالمي التي أعقبت الأزمة المالية العالمية 2008 في السياق العالمي للعلاقات بين الولايات المتحدة والصين، حيث فقدت العولمة الاقتصادية والتعددية زخمها، كما عملت المنافسة التكنولوجية والجيوبوليتيكية الممزوجة بالشعبوية والحمائية على إضعاف الروابط التي تم بناؤها بين البلدين في العقود الأخيرة، وعليه، يرى عديد من الباحثين أن المحركات الرئيسية للمنافسة الاستراتيجية بين الولايات المتحدة والصين والتي قد تؤدي في النهاية إلى حرب باردة جديدة تتوزع عبر أربعة مسارات بحثية¹:

الفرع الأول: التفوق التكنولوجي

لطالما لعبت التكنولوجيا والابتكار دوراً حاسماً في صعود وسقوط الإمبراطوريات عبر التاريخ، حيث يوفر الابتكار التكنولوجي الوسائل اللازمة للقوى الصاعدة لتحل محل القوى القديمة، فالابتكار العسكري يسمح بالغزو والتمدد عبر الأراضي، والابتكار الاقتصادي يضمن زيادة الإنتاج والنمو، والابتكار السياسي والاجتماعي يضمن للقادة الاستقرار في الداخل والنفوذ والتأثير في الخارج².

على مدى العقود الثلاثة الماضية كانت للولايات المتحدة ميزة الريادة والسبق في التطوير والابتكار الرقمي، وحلت شركاتها التكنولوجية محل الشركات الصناعية الكبرى محلياً وعالمياً، ونشأت قطاعات جديدة تقودها التكنولوجيا الرقمية أعادت تشكيل الاقتصاد والجيش والسياسة،

¹ Zhao Minghao, "Is a New Cold War Inevitable? Chinese Perspectives on US-China Strategic Competition", *The Chinese Journal of International Politics*, Vol 12, Issue 3, 2019, pp 371-394.

² , *The Cold War for Supremacy in the Information Age*, Greater Pacific Capital, September 2020, URL: <https://bit.ly/3rQa3hO>.

وفي خضم ذلك، ظهر منافس للريادة والقيادة الأمريكية في مجال التكنولوجيا والابتكار، إذ عملت الصين على سد الفجوة الرقمية بينها وبين الولايات المتحدة في وقت قصير، حيث كان عقد من الزمن كافياً للصين لكي تقدم للعالم شركات تكنولوجيا عملاقة تتنافس الشركات الأمريكية حتى في داخل الولايات المتحدة نفسها، وهو ما أطلق موجة من الخوف والقلق في الأوساط الأمريكية من أن زمن الهيمنة والريادة قد ولى، فالصين التي كانت إلى عهد قريب مكاناً لنسخ وتقليد كل ما هو أمريكي وغربي تسعى اليوم لتصبح مكاناً للابتكار وخلق التكنولوجيا.

وعليه، فإن المنافسة الاستراتيجية بين الولايات المتحدة والصين في القرن الحادي والعشرين تدور حول الابتكار والتكنولوجيا، ومن يُحقق الإختراقات التكنولوجية في مجالات الذكاء الاصطناعي والبيانات والحوسبة مع القدرة على تحويلها إلى ميزة صناعية سيحقق التفوق التكنولوجي وسيصبح المهيمن القادم على العالم.

الفرع الثاني: النهج الواقعي ونظرية انتقال القوة

حيث ينبغي النظر إلى المنافسة المتزايدة بين البلدين كنتيجة حتمية للتغير الحاصل في توزيع القوة على المستوى العالمي، مع الأخذ بعين الاعتبار أن الفضاء السيبراني والتكنولوجيا بصفة عامة تساهم بشكل كبير في ترتيب وإعادة ترتيب وانتشار القوة بين الفاعلين الدوليين من خلال معيار القوة السيبرانية، كما تلعب التناقضات الهيكلية بين القوة المهيمنة والقوة الصاعدة في الدفع نحو المزيد من المنافسة، قدم "ميرشايمر" رؤيته حول الصعود الصيني في كتابه "مأساة القوى العظمى" وجادل بأن الصين في حالة نجاحها في الحفاظ على سرعة نموها الاقتصادي ستسعى حتماً إلى الهيمنة على منطقة آسيا (المهيمن الإقليمي) كمرحلة أولى، لكن في المقابل ستحاول الولايات المتحدة منعها من تحقيق هدفها من خلال الاحتواء والتحالفات في المنطقة¹، ويُعد هذا السبب الجذري للصراع بين القوتين، وإذا عدنا إلى الواقع نجد أن قدرات الصين الاقتصادية والتكنولوجية والعسكرية -بدرجة أقل- تقترب بسرعة من القدرات الأمريكية بل تتجاوزها في بعض المجالات، لذلك فالصراع يدور حول استغلال هذه القدرات في زيادة النفوذ والقيادة الإقليمية والعالمية خاصة في دول آسيا والمحيط الهادي، كما يُشير الخبير الصيني "وانغ جيسي" إلى تفصيل دقيق يتعلق بعدم قبول الأمريكيين بفكرة أن القوة الصينية في تزايد والقوة الأمريكية

¹ جون ميرشايمر، مرجع سابق.

في تراجع، إن عدم رغبة الولايات المتحدة في الاعتراف بضعفها في مواجهة الصين يجعل من المنافسة الاستراتيجية والحرب الباردة الجديدة أمر لا مفر منه.

إضافة إلى ماسبق، تولي الصين أهمية كبرى لمعيار "القوة الوطنية الشاملة" والذي تعتبره مقياساً رئيسياً للقوة والقدرة الشاملة للدولة في جميع جوانب التنمية الوطنية، ويشتمل هذا المعيار كما يشرحه "هو أنجانج" و"مان هونغ هوا" في مقالهما المعنون بـ "نهوض الصين الحديثة: قوة وطنية شاملة واستراتيجية كبرى" على مؤشرات القوة الاقتصادية والعسكرية والتكنولوجية والثقافية والدبلوماسية¹، لذلك كان تركيز الحكومة الصينية على رفع هذا المعيار كجزء من منافستها الاستراتيجية مع الولايات المتحدة معتقدة أن بلوغ وتجاوز القوة الوطنية الأمريكية سيمنح البلاد من حماية مصالحها الوطنية وتعزيز نفوذها العالمي وتحقيق أهدافها الاستراتيجية طويلة المدى، وفي العام 2015، أكد "هو أنجانج" الأستاذ بجامعة "تسينغهوا" أن القوة الوطنية الشاملة للصين قد تجاوزت فعلياً القوة الوطنية للولايات المتحدة، ورغم أن هذا الإدعاء لم يوافق عليه إلا قلة من الباحثين في الصين² إلا أنه لفت الإنتباه إلى أن الفجوة تتقلص بين قوة وطنية شاملة صينية في تزايد وقوة وطنية أمريكية في انحدار، وهذا ما يُعتبر الأساس الموضوعي لتحول الولايات المتحدة من استراتيجية "الشراكة والتعاون" مع الصين إلى استراتيجية "المواجهة" مع نهاية فترة "أوباما" وبداية فترة "ترمب" مع التركيز على ضرورة الفوز والريادة في مجال التكنولوجيا والفضاء السيبراني في فترة "بايدن".

الفرع الثالث: التصورات والإدراكات المتبادلة

تُشكل التصورات والإدراكات المتبادلة للولايات المتحدة والصين المنافسة الاستراتيجية بينهما، كما أن لها تأثيراً حاسماً في ديناميكيات العلاقة بين البلدين، ومن جهة أخرى، فإن الجمع بين البيئة الدولية المتغيرة والتحولات الداخلية الصعبة لكلا الدولتين يجعل بيئتهما الخارجية غير مؤكدة ويغلب عليها الشك وعدم اليقين، وبالتالي يصبح تفسير النوايا الاستراتيجية لكلا الطرفين عملية شديدة الصعوبة مما يغذي المنافسة ويدفع بها نحو الصراع.

¹ Hu Angang, Men Honghua, **The rising of modern China: Comprehensive national power and grand strategy**, In: international conference of the Korea Institute of International Economic Policy (KIEP), Seoul, 2004.

² Zhao Minghao, **Op.cit.**

بالنسبة للولايات المتحدة، أجبت الموجة الجديدة من تصورات "التهديد الصيني" - خاصة ما تعلق بتقنيات الجيل الخامس لشركة هواوي وتطبيق تيك توك - المخاوف من نوايا القوة الصينية الصاعدة، فازدياد الثقة لدى النظام الصيني في "النموذج الصيني" وإحكام الحزب الشيوعي قبضته على الحكم زاد من قلق الأمريكيين من سياسة الصين الخارجية ومن توسع نفوذها إقليمياً وعالمياً والذي يتجلى في المشاريع التوسعية كمشروع الحزام والطريق ومشروع طريق الحرير الرقمي، كما عزز من دعوات السياسيين والباحثين الأمريكيين للمواجهة والتصدي لهذا التهديد.

أكد استطلاع للرأي قام به مركز بيو للأبحاث في مارس 2023 أن غالبية الأمريكيين (83%) لديهم آراء سلبية تجاه الصين، وصنف أربعة من كل عشرة أمريكيين الصين بأنها عدو وليست منافساً أو شريكاً للولايات المتحدة، كما يشعر الأمريكيون بالقلق من دور الصين في العالم خاصة من الناحية الجيوبوليتيكية، إذ يرى أكثر من 62% من المستجوبين أن الشراكة الصينية الروسية خطيرة للغاية على الولايات المتحدة، كما يرى 40% من الأمريكيين أن القوة التكنولوجية المتنامية للصين مشكلة خطيرة للغاية ويدعم أكثر من نصف الأمريكيين إجراءات الحكومة لحظر تطبيق تيك توك، كما أن قلة قليلة من الأمريكيين يثقون في الرئيس الصيني "شي" وينظر الغالبية من الأمريكيين بشكل سلبي لنوايا الصين الدولية، وكنتيجة لهاته النظرة السلبية تجاه الصين يرى أكثر من نصف الأمريكيين - خاصة الجمهوريين وكبار السن - أن التعاون بين الولايات المتحدة والصين أمر غير محتمل¹.

أما على الجانب الصيني، يرى النقاد أن السياسة الأمريكية أصبحت أكثر استقطاباً وأن التصورات السلبية تجاه الصين تغذيها الشعبوية حيث تبالغ في تقدير قدرات الصين وتشوه نواياها السلمية، وهو ما يؤدي في النهاية إلى تآكل الثقة الاستراتيجية بين البلدين ويجعل العلاقة بينهما صراعية أكثر منها تنافسية.

في استطلاع للرأي قام به "آدم ليو" وآخرون في جانفي 2023 حول موقف الصينيين من الولايات المتحدة وأوروبا أظهر أن أكثر من 70% من المستجيبين ينظرون للولايات المتحدة نظرة سلبية في نتيجة مفاجئة حيث إنه قبل عامين كان 17% فقط يحملون نظرة سلبية عن الولايات المتحدة، وهذا ما تم تفسيره أن العداء للولايات المتحدة قد اتسع بشكل كبير بين الجمهور الصيني،

¹ Laura Silver, et al, **Americans Are Critical of China's Global Role – as Well as Its Relationship With Russia**, Pew Research Center, April, 2023, URL: <https://bit.ly/3YatrCj>.

واللافت للنظر أن نسبة كبيرة من المستجيبين لديهم نظرة إيجابية لبقية الدول الأوروبية¹، ما يعني أن "الغرب" في نظر الصينيين "غربان" وأن العدو الوحيد هو الولايات المتحدة.

الفرع الرابع: الاختلافات الإيديولوجية وتضارب الأجندات السياسية

إن الاختلافات الجوهرية في المؤسسات السياسية ونظم القيم للبلدين يشكل مصدراً مهماً للتناقضات الهيكلية، فالأمريكيون ينظرون إلى الصين كدولة استبدادية وأن إيديولوجية النخبة الحاكمة الصينية تتعارض مع المثل والقيم السياسية الأمريكية والعالمية، ليس هذا فحسب بل يرون أن الحزب الشيوعي يسعى لتصدير نموذج الرأسمالي-الاستبدادي للعالم، أما على الجانب الصيني، فنجد استعمالاً مكثفاً لمصطلحات مثل "عقلية الحرب الباردة" و"عقلية الهيمنة" لوصف سياسات الولايات المتحدة ضد الصين، حيث يرى "ما تشن قانغ" السفير السابق والعضو في العديد من الهيئات الحكومية والأكاديمية الصينية أن "عقلية الحرب الباردة" تغذي العداء الأمريكي تجاه النظام السياسي الصيني، وأن "عقلية الهيمنة" تُفسر النوايا الأمريكية لعرقلة صعود أي دولة كبرى أخرى²، وما القوانين الجديدة حول الرقائش وشركات التكنولوجيا إلا نتاج لهذه العقلية.

والظاهر أن الولايات المتحدة تريد أن تفرض الإيديولوجيا فرضاً في صراعها مع الصين من أجل مصالحها في توحيد الجبهة الداخلية والخارجية، لأن القادة الصينيين أنفسهم يقرون بأن النموذج الاشتراكي خاص بهم فقط ولا ينوون تصديره لأية دولة في العالم، حيث يقول الرئيس "شي" "لن نستورد نماذج من دول أخرى ولن نصدر النموذج الصيني"³، كما يؤكد "أميتاي إيتزيوني" الأستاذ بجامعة جورج واشنطن بأن الصين "أظهرت القليل من الدلائل على أنها تسعى لفرض هذا النوع من النظام [النظام الرأسمالي الاستبدادي] على دول أخرى"⁴، لذلك فالمنافسة الاستراتيجية بين الولايات المتحدة والصين يمكن اعتبارها منافسة داخل الرأسمالية نفسها.

وعليه، فإن تضارب الأجندات السياسية يُعد من أبرز محركات المنافسة الاستراتيجية بين الولايات المتحدة والصين، فأهداف السياسة الأمريكية تتعارض مع أهداف السياسة الصينية

¹ Adam Liu, et al, "Unpacking "the West": Divergence and Asymmetry in Chinese Public Attitudes Towards Europe and the United States", **Journal of Current Chinese Affairs**, Vol 52, Issue 1, 2023, pp 119–133.

² Zhao Minghao, **Op.cit.**

³ Reuters Staff, **President Xi says China will not export its political system**, Reuters, December 1, 2017, URL: <https://bit.ly/3Y9E2xn>.

⁴ Amitai Etzioni, **China is Not the Soviet Union**, The National Interest, 2018, URL: <https://bit.ly/3qaxwcZ>.

وتصطدم بها في كثير من الحالات خاصة ما يتعلق بالسياسيات الإقليمية في منطقة آسيا والمحيط الهادي، فالأهمية الجيوستراتيجية للمنطقة جعلت من الولايات المتحدة ترى أي تدخل فيها من قبل قوى أخرى تهديداً صريحاً لمصالحها الحيوية، لذلك، فسياسة الجوار التي تنتهجها الصين تتعارض مع الممارسات الأمريكية كحامٍ للنظام الإقليمي في المنطقة، كما يُشير "مايكل بيكلي" من معهد أمريكان انتربرايز في مقاله "أفضل خيار هو الحرب الباردة مع الصين" إلى أن معظم القضايا الجوهرية الخلافية بين الولايات المتحدة والصين ذات محصلة صفرية، فتايوان إما أن تكون مستقلة أو تحت الحكم الاستبدادي الصيني، وبحر الصين الجنوبي إما أن يكون ممراً دولياً حراً للملاحة وإما أن يكون بحيرة صينية، وروسيا إما علينا شلها بالعقوبات أو دعمها بصفقات النفط والغاز، والفضاء السيبراني إما أن يكون مفتوحاً ومجانياً أو يكون تحت سلطة الدولة¹، ومع وجود هذه المفارقات يُصبح الصراع أمراً لا مفر منه وتُدفع المنافسة بين البلدين إلى مستويات أكثر عنفاً.

المطلب الثاني: الحرب الباردة النسخة الثانية (Cold War 2.0)

صرح وزير الخارجية الأمريكي "أنتوني بلينكن" في أكتوبر 2022 أمام طلاب جامعة ستانفورد بعد اجتماعات عقدها مع شركات التكنولوجيا في وادي السيلكون بأن عالم مابعد الحرب الباردة قد وصل إلى نهايته، وأن العالم يشهد منافسة شديدة لتشكيل ما بعده، وتقع التكنولوجيا في قلب هذه المنافسة²، لم يعترف بلينكن ولا غيره من السياسيين الأمريكيين بأن العالم يدخل مرحلة "حرب باردة جديدة" لكن المفكرين والباحثين يرون غير ذلك، فالدبلوماسي "هنري كيسنجر" تطورت رؤيته للعلاقة بين الولايات المتحدة والصين؛ من أن الدولتين على سفوح حرب باردة جديدة في العام 2018، إلى أنهما في الممرات الجبلية للحرب الباردة في العام 2020، وأخيراً أن الدولتين تقريباً قد دخلتا في حرب باردة نهاية 2022، كما يؤكد أن الحرب الباردة الجديدة ستكون أسوأ وأكثر خطورة³.

¹ Michael Beckley, **Accepting a Cold War with China Is the Best Option**, The American Enterprise Institute, December 06, 2022, URL: <https://bit.ly/3KeI164>.

² Antony J. Blinkin, **Remarks to the Press**, US department of State, state.gov, October 17, 2022, URL: <https://bit.ly/3K2LIM2>.

³ Niall Ferguson, **Cold War II: Niall Ferguson On The Emerging Conflict With China**, hoover.org, May 1, 2023, URL: <https://bit.ly/44tDJ2M>.

في المقابل، حذر الرئيس الصيني "شي" من "حرب باردة جديدة" تحاول بعض الدول إثارتها في خطابه الموجه لقمة منظمة شنغهاي للتعاون المنعقدة في جوان 2023¹، كما أن الباحثين الصينيين يستخدمون المصطلح بكثرة عند الحديث عن المنافسة بين الدولتين أو لوصف السياسات الأمريكية أو التصريحات المعادية للصين الصادرة من المسؤولين في واشنطن.

الفرع الأول: وجهة النظر الأمريكية حول الحرب الباردة الجديدة

يقدم "نيال فرغيسون" من معهد "هوفر" الأمريكي مقارنة بين الحرب الباردة في نسختها الأولى (الأمريكية-السوفياتية) والنسخة الثانية (الأمريكية-الصينية) مؤكداً على خطورة الحرب الباردة الجديدة حيث يجادل بأنه من ناحية الوقت، فالحرب الباردة الأولى دامت أربعة عقود وانتهت بشكل مفاجئ في حين أن الحرب الباردة الجديدة لا يمكن التكهّن بمدتها لأن الصين خصم أكثر شراسة من الاتحاد السوفياتي، أما من الناحية الاقتصادية، فالصين تفوقت على الولايات المتحدة في الناتج المحلي، في حين لم يبلغ الاتحاد السوفياتي نصف الناتج المحلي الأمريكي في أفضل حالاته، أما السلاح النووي الذي كان محور التهديد في الحرب الباردة الأولى فقد شهد تطوراً كبيراً اليوم إضافة إلى مزجه بالتكنولوجيا، فالتهديد اليوم هو تهديد تكنولوجي للجنس البشري، كما أن الولايات المتحدة كانت محصنة استخباراتياً في الحرب الباردة الأولى فالسوفيّات لم يعلموا إلا القليل، إلا أن الصين اليوم تعلم الكثير عن الولايات المتحدة من خلال تواجد الأفراد أو التجسس السيبراني وهذا راجع للتداخل الاجتماعي والاقتصادي الكثيف بين البلدين.

واستناداً إلى محاور المقارنة بين الحرب الباردة الأولى والجديدة التي قدمها "نيال" وما جاء في استراتيجيات الأمن القومي لإدارتي "ترمب" و"بايدن" من توصيف للعلاقة بين الولايات المتحدة والصين على أنها منافسة استراتيجية طويلة الأمد، إضافة إلى السياسات المعادية للصين التي اتخذها كل من الرئيسين "ترمب" و"بايدن" يذهب العديد من الباحثين الأمريكيين إلى إطلاق مصطلح "الحرب الباردة الجديدة" على واقع العلاقة بين البلدين، حيث كتب "دان نيغري" و"جيمس جاي كارافانو" في مجلة "المصلحة الوطنية" ذات النزعة الواقعية بأن منافسة القوى العظمى مفهوم

¹ Xinhua, Full text of Xi's address at SCO summit, gov.cn, July 4, 2023, URL: <https://bit.ly/3K242oB>.

تجاوز الزمن، وأن الحرب الباردة الجديدة قد بدأت وحن الوقت للاعتراف بذلك وبدء القتال¹، حتى إن تقريراً صادراً عن مؤسسة التراث البحثية بعنوان "الفوز في الحرب الباردة الجديدة: خطة لمواجهة الصين" قدم وصفاً للغايات والطرق والوسائل الضرورية للفوز بالحرب الباردة الجديدة وتأمين مستقبل الولايات المتحدة، حيث أكد التقرير أن الصين خصم للولايات المتحدة وأن الاستراتيجيات السابقة قد أضرت بالأمة الأمريكية وعرضت اقتصادها للخطر، لذلك فإن حماية الوطن الأمريكي وازدهاره والتقليل من قدرة الصين على إلحاق الضرر به يحتاج إلى نهج يشمل الحكومة بأكملها والمجتمع بأسره².

ومن المثير للإهتمام أن السياسيين الأمريكيين وبعض المفكرين يتجنبون تشبيه المنافسة بين الولايات المتحدة والصين بـ "الحرب الباردة"، ويعتبرون هذا الوصف مضلل إلى حد بعيد وأن نتائجه سلبية على الولايات المتحدة، فمثلاً "كارافانو" الذي يدعو للفوز بالحرب الباردة الجديدة في 2023 كان قبل سنة واحدة يقول: "دعونا لا نسمي المنافسة بين الولايات المتحدة والصين حرباً باردة"، يجب أن يكون لهذا الصراع المستمر اسماً خاصاً به³ ويرجع السبب إلى أن اعتماد مصطلح الحرب الباردة في الصراع الأمريكي الصيني يُشجع القادة في واشنطن على التفكير القديم، حيث يفترضون أن استراتيجيات الحرب الباردة مع الاتحاد السوفياتي والتي ضمنت الفوز يمكن إعادة تطبيقها مرة أخرى مع الصين وستضمن الفوز لا محالة، ويُعقب "كارافانو" على هذا بأنه "فكرة خطيرة" فالمواجهة اليوم تختلف، فإذا كان الصراع السابق يتمحور فقط حول القوة العسكرية لضعف واضح لاقتصاد الخصم، فالصين اليوم منافس إقتصادي ضخم وتحد عسكري متزايد، من جهته، يرى "جوزيف ناي الابن" أن كل الاستعارات التاريخية لتوصيف العلاقة بين الولايات المتحدة والصين غير كاملة، مع إقراره بأن استعارة وصف "الحرب الباردة" يمكن أن يحشد الجماهير من أجل منافسة طويلة الأمد، إلا أنه يرى في المقابل أنها تضلل صانعي القرار بشأن طبيعة التحدي الاستراتيجي الذي تطرحه الصين، حيث يُصرح بأن فكرة "حرب باردة" مع الصين هي فكرة سيئة تاريخياً، سياسياً وخطيرة لمستقبلنا⁴، لذلك، قدم "ناي" وصفاً للحرب الباردة

¹ Dan Negrea, James J. Carafano, **The Pretend Phase of Cold War II Is Over**, Thenationalinterest.org, June 2, 2023, URL: <https://bit.ly/43uBBGo>.

² James J. Carafano, et al, **Winning the New Cold War: A Plan for Countering China**, The Heritage Foundation, Report n° 270, March 2023, URL: <https://herit.ag/43Cs3cw>.

³ James J. Carafano, "Is There a U.S.-China Cold War" Is the Wrong Question, heritage.org, Nov 2022, URL: <https://bit.ly/43BUeZ9>.

⁴ Joseph S Nye JR, **With China, a "Cold War" Analogy Is Lazy and Dangerous**, belfercenter.org, November 2021, URL: <https://bit.ly/44Gilr1>.

مع الاتحاد السوفياتي بأنها "لعبة شطرنج ثنائية الأبعاد" في إشارة إلى الصراع العسكري الإيديولوجي، أما المنافسة مع الصين فهي "لعبة شطرنج ثلاثية الأبعاد" تشمل الجوانب العسكرية، الاقتصادية والاعتماد المتبادل بين دول العالم¹، يرى "تاي" كذلك أن التوصيف المناسب للوضع الراهن ليس العام 1945 بل العام 1914 حيث لم يُعر القادة السياسيون في ذلك الوقت اهتماماً لخطورة القومية وتوقعوا حرباً قصيرة في البلقان لتنتهي بحرب عالمية دمرت أربعة إمبراطوريات².

أما بالنسبة للسياسيين، فالتصريحات الرسمية لا تستعمل مطلقاً مصطلح "الحرب الباردة" ولكن سياساتها واستعاراتها دوماً حاضرة، يجادل الرئيس "بايدن" وفريقه للأمن القومي بأن المقارنات بين الوضع الحالي والحرب الباردة مضللة وهي تبسيط مفرط للحظة جيوبوليتيكية معقدة، لكن في تصريح للرئيس "بايدن" في ليتوانيا أمام حشد من الجماهير بعد أن استحضر نضال دول البلطيق ضد الاتحاد السوفياتي واستعداد الولايات المتحدة وحلفاءها للدفاع عن أوكرانيا ودول أوروبا قال "سندافع عن الحرية اليوم وغداً وطالما استغرق الأمر"، هذه العبارة يُشبهها النقاد بوصف الرئيس "كينيدي" للـ "الحرب الباردة" في خطابه الافتتاحي سنة 1961 بأنه يجب على الولايات المتحدة "تحمل عبء صراع طويل وشاق".

وعليه، فرغم عدم الاعتراف الرسمي بدخول العالم مرحلة حرب باردة جديدة إلا أن سياسات الحرب الباردة حاضرة بقوة في العلاقة بين الولايات المتحدة والصين خاصة من الجانب الأمريكي، حيث نجد ممارسات الاحتواء والتحالفات هي السمة الأبرز للسياسة الخارجية الأمريكية، كما يرى العديد من النقاد أن الولايات المتحدة والصين في مرحلة مبكرة من حرب باردة جديدة، وأن إنكار السياسيين لوجودها يرجع في الأساس لعدم اليقين لدى الطرفين في حسمها لصالحهم، فواشنطن لم تتجح لحد الآن في تعبئة مواردها المحلية في القطاعين الحكومي والخاص وتوحيد صفوف حلفائها لمحاربة "خصومها" بشكل فعال، وهو ما انعكس على قدرتها في تحقيق هدف احتواء الصين أو عزلها عن العالم، من جهتها، تحتاج الصين إلى مزيد من أوقات السلام العالمي لمواصلة صعودها ومواجهة التحديات الداخلية والخارجية التي تعطل مسيرتها.

¹ Joseph S Nye JR, **Cracking China**, the-security-times.com, February 2022, URL: <https://bit.ly/3Q82gpz>.

² Joseph S Nye JR, **Popping China's Balloon**, project-syndicate.org, March 2021, URL: <https://bit.ly/3K9dINZ>.

الفرع الثاني: وجهة النظر الصينية حول الحرب الباردة الجديدة

كان السياسيون والباحثون الصينيون سباقين في توصيف المنافسة الأمريكية الصينية وممارسات الإدارة الأمريكية بأنها "حرب باردة" تُشن على الصين، فالرئيس الصيني "شي" حذر دوماً من "الحرب الباردة" بين البلدين وعبر عن أمله في عدم تدهور العلاقة بين البلدين لتصل إلى مستوى "حرب باردة"، هذه الرؤية يتشاركها جميع المسؤولين في الصين، حيث أكد " تشانغ جون" الممثل الدائم للصين لدى الأمم المتحدة في اجتماع لمجلس الأمن في مارس 2022 بأن الحرب الباردة قد انتهت ويجب التخلي عن عقلية الحرب الباردة القائمة على المواجهة بين التكتلات، كما أن التمسك بمنطق الهيمنة لا يؤدي إلا إلى المزيد من عدم الاستقرار والانقسام في العالم الذي ليس بحاجة لـ "حرب باردة جديدة"¹.

أما على المستوى الأكاديمي، يؤكد عديد من الباحثين الصينيين أن الأزمة المالية 2008 كانت حداً فاصلاً في تاريخ العلاقة بين الولايات المتحدة والصين، وأن بداية التحولات العميقة في النظام الدولي وضعت حداً لثلاثة عقود من التعاون والشراكة بين البلدين، حيث اتخذت المنافسة الأمريكية الصينية سياقاً عالمياً، يؤكد ذلك استراتيجية "إعادة التوازن" أو "محور آسيا" التي انتهجتها إدارة "أوباما" والتي عبرت عن مخاوف واشنطن من الصعود الصيني وجعلت العلاقة بين البلدين أكثر تصادمية، ثم ما تلا ذلك من ممارسات تجارية تصعيدية ضد الصين خلال إدارة "ترمب"، إضافة إلى التصريح بالعلاقة الصراعية بين البلدين في استراتيجيات الأمن القومي التي أصدرتها إدارتا "ترمب" و"بايدن" اللتان اعتبرت الصين "دولة تعديلية" وأقوى منافس استراتيجي مع الإعلان عن عودة المنافسة بين القوى العظمى، كل هذا جعل من المفكرين الصينيين يدركون التغير في طبيعة العلاقة بين الولايات المتحدة والصين والتي تنزلق تدريجياً نحو حرب باردة جديدة.

إضافة إلى ماسبق، يعزو الباحثون في الصين استخدامهم مصطلح "الحرب الباردة الجديدة" إلى وجود أوجه تشابه بينها وبين الحرب الباردة الأولى مثل الصراع بين القوى العظمى والصراع

¹ [مندوب الصين الدائم لدى الأمم المتحدة: "الولايات المتحدة: لا تحتاج إلى "حرب باردة جديدة" | جياو يوان]، 2022، URL : <https://bit.ly/44woR3w>، [وكالة شينخوا]، 2022، URL : <https://bit.ly/44woR3w>.

الإيديولوجي، مع الإقرار بوجود اختلافات بين الحربيين أهمها حسب "تشاو مينغ هاو" أن الصراع في الحرب الباردة الأمريكية السوفياتية كان بين نظامين سياسيين واقتصاديين واجتماعيين متباينين مع روابط أقل، كما كان التركيز على الجانب العسكري والإيديولوجي للصراع مع وجود حدود واضحة بين المعسكرين، أما في الحرب الباردة الجديدة الأمريكية الصينية، فالصراع إقتصادي تكنولوجيا بالدرجة الأولى مع ترابط اقتصادي مكثف، إضافة إلى تباين في نماذج التنمية للبلدين، مع إمكانية كل طرف في الوصول والتأثير على مناطق نفوذ الطرف الآخر من خلال الفضاء السيبراني، لذلك، فخصائص الحرب الباردة الجديدة تنعكس على المنافسة الحادة بين القوى العظمى حول المشاعات العالمية كالفضاء السيبراني والفضاء الخارجي¹، وهذا النوع من الصراع يتعلق بدرجة التحكم في التكنولوجيا وليس بالسيطرة المباشرة على الأراضي.

إضافة إلى ذلك، جاءت نتائج استبيان قام به معهد تشونغ يانغ للدراسات المالية بجامعة رينمين الصينية شمل 100 باحث صيني أن أكثر من 62% من المستجوبين يعتقدون أن الولايات المتحدة تشن بالفعل حرباً باردة جديدة ضد الصين، وعبر أكثر من 90% منهم عن اعتقادهم بأن الصين قادرة على التعامل بشكل جيد مع هذه الحرب، وفي سؤال حول ما إذا كان البلدان سيدخلان حرباً باردة مشابهة للحرب الباردة السابقة ساند 13% فقط هذا الطرح، فيما يرى 82% أن هذه الحرب مختلفة لطبيعة المصالح المتشابهة بين البلدين، وأن الصين لا تريد حرباً باردة مع الولايات المتحدة بل هذه الأخيرة هي التي تروج لها من خلال سياسات "المواجهة" و"الاحتواء"². في نفس السياق، يؤكد باحثون صينيون لديهم خلفية عسكرية حتمية المواجهة بين الولايات المتحدة والصين، إذ يصرح العقيد "ليو مينجفو" من جامعة الدفاع الوطني في كتابه "الحلم الصيني - 中国梦" المنشور في 2010 أن الصراعات بين الولايات المتحدة والصين أمر لا مفر منه بغض النظر عن مدى التزام الصين بالصعود السلمي، ووصف المنافسة بين البلدين بـ"الماراطون" حيث يمكن رؤية "مواجهة القرن"، يشاطره هذه الرؤية زميله في نفس الجامعة البروفيسور "تانغ يونغ شنغ" والذي يجادل بأنه يجب أن تكون المنافسة الاستراتيجية بين البلدين "معركة طويلة الأمد"³.

¹ تحليل "المنافسة الاستراتيجية" [赵明昊: 试析中美“战略竞争”及其管理], [تشاو مينغ هاو] 赵明昊

[الصينية الأمريكية وإدارتها], ciss.tsinghua.edu.cn, 2021, URL : <https://bit.ly/3Oa04va>.

² Yang Yuntao, Zhang Tingting, **China can deal with the US**, Chongyang Institute for Financial Studies, zhuanlan.zhihu.com, URL: <https://bit.ly/3rIMxmJ>.

³ Zhao Minghao, **Op.cit.**

من جهة أخرى، قدم الخبير "يوان بينغ" من معهد الصين للعلاقات الدولية (CICIR) تقييماً للوضع الدولي وهيكل العلاقات بين الولايات المتحدة والصين منذ العام 2005 مروراً بالأزمة المالية لسنة 2008 وخلص إلى أن النظام الدولي يشهد تحولاً فعلياً، كما أكد على أن المنافسة بين البلدين جاءت نتيجة تطور رؤية الولايات المتحدة للصين التي تحولت من "قوة كبرى" إلى "الرقم اثنان عالمياً" وأن التنافس العالمي بين "الرقم واحد والرقم اثنان" قد يجر البلدين إلى حرب باردة جديدة¹، كما يجادل "جين كانرونغ"، العميد المشارك لكلية الدراسات الدولية في جامعة رنمين الصينية بأن الولايات تشن فعلاً حرباً باردة جديدة ضد الصين رغم رفض رؤسائها وكبار المسؤولين في واشنطن الاعتراف بذلك، كما أنهم يرفضون رؤية التنمية في الصين كفرصة للتعاون بل يعتبرونها "تهديداً"².

وبناءً على ما تقدم، فالنخب في الولايات المتحدة تدفع نحو تصعيد الصراع نحو الحرب الباردة، ورغم عدم تصريح السياسيين بذلك إلا أن سياسات المواجهة والاحتواء ضد الصين تُظهر ما لا يتم التصريح به، من جهتها، ترفض الصين الدخول في حرب باردة وتتهم الجانب الأمريكي بأنه يريد تحويل الصين إلى "اتحاد سوفياتي جديد" لكي تُدفع للرد على طريقة الحرب الباردة وهو ما يخدم أجندة الولايات المتحدة لتوحيد الداخل وتجميع الخارج، يبرز هذا التصعيد الأمريكي في الحروب التجارية والتكنولوجية بدرجة أولى، وكمحور للمنافسة الاقتصادية مع ضغوطات عسكرية حول تايوان وبحر الصين الجنوبي، إضافة إلى تركيز واشنطن على محاصرة الصين وحرمانها من تحقيق اختراقات تكنولوجية والتي تعتبرها الصين الركيزة الأساسية في ردها على الولايات المتحدة.

وعليه، فإن مواصلة الولايات المتحدة استهداف مصالح الصين الجوهرية والرئيسية يدفع بالمنافسة الاستراتيجية بين البلدين حول النفوذ والقيادة العالمية نحو "حرب باردة" محورها التكنولوجيا (هناك من الباحثين من يستعمل مصطلح الحرب الباردة الرقمية)، والفائز هو الذي يستطيع إحداث أكبر تأثير في النظام العالمي المتغير، لذلك فكل طرف سيسعى إلى بسط رؤيته وإضفاء الشرعية على المعتقدات والمعايير والقواعد والأنظمة العالمية التي تخدم أهدافه الخاصة وتجعل من الصعب على منافسه المضي قدماً في أجندته، كما تعمل كل من واشنطن وبكين

¹ Ibid.

² Yang Sheng, Qi Xijia, US signals to fix China ties but 'credible sincerity' needed; Washington to be 'lone wolf' in 'new cold war' against China, globaltimes.cn, Apr 11, 2023, URL: <https://bit.ly/3DgiQfh>.

لزيادة نفوذهما وسيطرتهما على المنظمات الدولية والإقليمية والمحافل والتحالفات التكنولوجية، وتنفيذ استراتيجيات للتفوق التكنولوجي، التجاري والعسكري إقليمياً ودولياً.

المطلب الثالث: ديناميكيات الحرب الباردة الرقمية

تتمحور الحرب الباردة الرقمية (أو الثانية) حول الصراع التكنولوجي حيث تتنافس الولايات المتحدة والصين في العديد من المجالات والتقنيات الرقمية، تترابط هذه المجالات والتقنيات وتتداخل فيما بينها كما تُعد بعض التقنيات تأسيسية أو توليدية حيث تُعتبر محركاً لتطوير بقية التقنيات نذكر منها: الذكاء الاصطناعي والرقائق الفائقة والحوسبة الكمومية، وعند تتبع قدرات البلدان الرقمية غالباً ما نجد الولايات المتحدة في الريادة متبوعة مباشرة بالصين، وفي بعض الأحيان نجد تكافؤاً في القدرات أو تقدماً بسيطاً لصالح الصين، مع فارق كبير بينهما وبين بقية الدول الأخرى، لكن هذه القاعدة تشذ في حالة صناعة الرقائق، حيث نجد دولاً أخرى مع الولايات المتحدة والصين تتصدر القائمة كما يمكن ملاحظة أن صناعة الرقائق تتوزع عبر العديد من الدول، لذلك فعالم الرقائق عالم متعدد الأقطاب، وفهم جيوبوليتيكيته يسمح لنا من الاقتراب من ديناميكيات الحرب الباردة الرقمية ولما سيؤول إليه صراع الهيمنة التكنولوجي بين الولايات المتحدة والصين.

الفرع الأول: تأطير الصراع حول صناعة الرقائق

في قلب صراع الهيمنة التكنولوجي بين القوتين العظميين نجد صراعاً ذا محصلة صفرية حول صناعة أشباه الموصلات (الرقائق أو أنصاف النواقل)، تنظر كل من الولايات المتحدة والصين إلى هذا الصراع من خلال إطار "الفائز يأخذ كل شيء" لذلك فاننتصار أحد الطرفين في الحرب الباردة الرقمية وفرض هيمنته التكنولوجية مرهون بقدرته على التفوق والسيطرة على هذه التقنية مع منع الطرف الآخر من الحصول على هذه الميزة.

تمثل الرقائق قلب الصناعة التكنولوجية فهي تدخل في صناعة كل شيء من أجهزة الكمبيوتر والهواتف، حتى المعدات والآليات العسكرية، لذلك فهي ميزة رئيسة في النمو الاقتصادي خاصة الاقتصاد الرقمي والتفوق العسكري خاصة الحروب المستقبلية، والمهيمن عليها يحوز أحقية قيادة العالم في القرن الحادي والعشرين.

بالنسبة للولايات المتحدة، تم اختراع الرقاقة الأولى في الولايات المتحدة في خمسينيات القرن المنصرم كما كانت صناعة الرقائق في قلب الحرب الباردة بينها وبين الاتحاد السوفياتي خاصة فيما يتعلق بسباق الفضاء والتسلح، وبينها وبين اليابان في الحرب التكنولوجية في ثمانينيات القرن الماضي، إلا أنها فقدت هذه الميزة التنافسية في بعض أجزاء صناعة الرقائق لصالح الشركات الآسيوية، ورغم أن الولايات المتحدة لاتزال رائدة في معدات التصنيع وبرامج التصميم الإلكتروني المستقلة وبرامج تصميم الرقائق إلا أن حصتها العالمية من صناعة الرقائق (المنتج النهائي) انخفضت من 40% سنة 1990 إلى أقل من 15% سنة 2021، ويرجع ذلك إلى عمليات العولمة المكثفة وتخصيص العمل حيث أدى ارتفاع تكاليف الإنتاج في الولايات المتحدة والاستثمار الكبير في قطاع الرقائق في دول شرق آسيا إلى جعل صناعة الرقائق المصممة في الولايات المتحدة تتم في مصانع (مسابك) في تايوان، كوريا الجنوبية والصين، وأصبحت شركة TSMC التايوانية اليوم تحتكر إنتاج أكثر من 90% من الرقائق الفائقة¹.

تطور إدراك الإدارة الأمريكية لصناعة الرقائق كتقنية استراتيجية تحتاج إلى الحماية منذ 2015، حيث أحبطت إدارة "أوباما" عمليات الاستحواذ الصينية على شركات صناعة الرقائق الأمريكية في 2016، كما صرحت وزيرة خارجيته بأن خطة "صنع في الصين 2025" بُنيت خصيصاً للسيطرة على قطاع الرقائق، تغيرت العلاقة بين الولايات المتحدة والصين في فترة "ترمب" الذي بدأ "حرباً تجارية" ضد الصين التي شوهدت في نظره نظام السوق والتجارة العادلة وصنفت الصين على أنها "منافس استراتيجي"، وبدأ العمل بتدابير الحماية وقاعدة المنتج الأجنبي ووضعت قائمة سوداء للشركات الصينية التي يُحظر التعامل معها في مجال الرقائق.

تحولت هذه الحرب التجارية إلى "حرب تكنولوجية" حول الرقائق مع وصول "بايدن" إلى الحكم، إذ أن عدم استقرار سلاسل توريد الرقائق العالمية والنقص في الإمدادات مقابل الطلب المرتفع الذي سببته جائحة كورونا كشفت الضعف الاستراتيجي الأمريكي في قطاع الرقائق، وزاد من إمكانية أن تُعزل الولايات المتحدة عن الرقائق الفائقة القادمة من تايوان وكوريا بسبب توترات جيوبوليتيكية أو كوارث طبيعية أو صحية، لذلك أحدث "بايدن" تغييراً شاملاً بشأن ضوابط التصدير الخاصة بالرقائق، وتخلت الإدارة الأمريكية عن الثنائية مدني-عسكري في

¹ Y Luo, Van Assche A, "The rise of techno-geopolitical uncertainty: Implications of the United States CHIPS and Science Act", **Journal of International Business Studies**, Vol 18, issue 01, 2023.

تصنيفها للجهات الصينية المسموح التعامل معها، حيث قدمت استراتيجية الاندماج المدني - العسكري الصينية حجة قوية للإدارة الأمريكية للعمل على ليس فقط على ضمان التقدم التقني الأمريكي بجيل أو جيلين عن الصين بل ضمان تراجع صناعة الرقائق الصينية¹.

وعليه، فالسياسة الأمريكية واضحة فيما يتعلق بصناعة الرقائق، العزم على منع الصين من امتلاك صناعة متطورة للرقائق والعمل على تراجع صناعيتها من خلال وضع حاجز جيوبوليتيكي تقني قوي (يشبه الستار الحديدي في الحرب الباردة) بينها وبين الحصول على رقائق فائقة أو تطوير صناعيتها محلياً، ومن جهة أخرى، الدفع بصناعة الرقائق في الداخل الأمريكي واستعادة الريادة في التصميم والإنتاج واحتكار قطاع الرقائق الفائقة من خلال تقديم الدعم المالي لشركات الرقائق الأمريكية والضغط على الشركات الرائدة (TSMC التايوانية و Samsung الكورية) لنقل المسابك المتطورة إلى داخل الولايات المتحدة.

أما بالنسبة للصين، تكافح الصين منذ اعتماد نظام الاقتصاد الرأسمالي للحصول على مكان بين كبار شركات الرقائق العالمية، وقد حققت بعض النجاح، إذ تطور إنتاجها للرقائق عالمياً من الصفر سنة 1990 إلى 25% سنة 2022²، في المقابل، تحتاج الصين لتلبية طلب الصناعة المحلي إلى استيراد ما يقارب 400 مليار دولار سنوياً من الرقائق، هذه التبعية للخارج جعلت القادة الصينيين يجعلون تطوير صناعة محلية للرقائق أولوية استراتيجية، حيث دعا الرئيس "شي" إلى "مسار عملي وثابت للابتكار"³ في إشارة للنهوض بصناعة الرقائق داخل الصين، كما أن خطة "صنع في الصين 2025" صممت سابقاً خصيصاً لسد هذا الخلل الاستراتيجي، ولكن لاتزال الجهود المبذولة لا تحقق النتائج المرجوة، فالحصار التقني الذي فرضته الولايات المتحدة وحلفاؤها يظهر تأثيره جلياً في تراجع مداخل شركات التكنولوجيا الصينية مثل "هواوي" كما أن واردات الصين من الرقائق تتراجع بشكل مستمر وخطير⁴ وهو ما

¹ Konark Bhandari, **The Geopolitics of the Semiconductor Industry and India's Place in it**, Carnegie India, India, June 2023, pp 9-11.

² Michael A Peters, "Semiconductors, geopolitics and technological rivalry: the US CHIPS & Science Act 2022", **Educational Philosophy and Theory**, 2022, pp 1-5.

³ Sylvie Zhuang, **US tech war: China's Xi Jinping urges 'solid path of innovation' as he tours semiconductor firms**, South China Morning Post, July 2023, URL: <https://bit.ly/3qoeIXR>.

⁴ Tracy Qu, **China's chip imports slump in first half as US sanctions and ongoing tech war take a toll on trade**, South China Morning Post, July 2023, URL: <https://bit.ly/3rWX3Hk>.

يعني تراجع التصنيع وتأخر الأبحاث والابتكار في التقنيات الأخرى كالذكاء الاصطناعي والحوسبة.

وعليه، فالصين تراهن على تخطي الحصار التقني الأمريكي والهيمنة الأمريكية على سلاسل التوريد العالمية من خلال خلق صناعة رقائيق محلية متكاملة تضمن على الأقل إستمرار الصعود التكنولوجي الصيني والإبقاء على حظوظ الصين كاملة للفوز بالحرب الباردة الرقمية.

وبناءً على ما تقدم، يرى صناع القرار الأمريكيون في صناعة الرقائيق تقنية استراتيجية (يفوق أثرها الأسلحة النووية) لها تأثيرات اقتصادية وعسكرية مستقبلية لذا يجب أن تكون حكرًا على الولايات المتحدة، كما يجب العمل بكل الوسائل لمنع الخصوم من الحصول عليها، هذا ما جعل سلاسل التوريد العالمية تُستعمل كسلاح لتحقيق المصالح السياسية والجيوبوليتيكية وصعد من القومية التكنولوجية لدى كل من الولايات المتحدة والصين.

الفرع الثاني: جيوبوليتيكا صناعة الرقائيق

تبرز أهمية الرقائيق من خلال استعمالاتها في جميع الصناعات التكنولوجية الحديثة، فهي المحرك الرئيس والمستقبلي للاقتصاد والحرب، ومن المتوقع أن يصل سوق الرقائيق إلى 726 مليار دولار في 2027¹، كما أن طبيعتها المادية تضعها في قلب الصراع على الطبقة المادية للفضاء السيبراني حيث تبرز الصراعات الجيوبوليتيكية بقوة، ويرجع سبب التركيز عليها من قبل الولايات المتحدة لأنها نقطة اختناق استراتيجية تضع الصين في خطر²، ذلك يرجع إلى أنها تحتاج في تطويرها لمدة زمنية طويلة حسب "قانون مور" وتمويل مالي ضخم (ملايير الدولارات) للأبحاث والتطوير وكذلك تتطلب وجود المعرفة والمواهب الفنية العالية.

في الوقت الراهن، تسيطر الولايات المتحدة على عمليات البحث والتطوير والتصميم، كما تتواجد بعض الشركات الأمريكية ضمن فئة التصنيع (مسابك انتل وميكرون)، وتتفرد شركة ASML الهولندية بصناعة آلات الطباعة المتطورة (EUV) والتي تستعمل فيها تكنولوجيا أمريكية، تهيمن شركة TSMC التايوانية Samsung الكورية على تصنيع الرقائيق الفائقة، وتشترك الشركتان مع شركات يابانية وصينية وأوروبية في تصنيع الرقائيق ذات العقد الكبيرة (أكبر من 14 نانومتر)، وعليه، فإن النظر إلى خريطة توزيع شركات صناعة الرقائيق نجد أن

¹ Michael A Peters, Op.cit.

² Eurasia Group, The Geopolitics of Semiconductors, Op.cit.

مركزاً شديداً لمصانع الرقائق في جنوب شرق آسيا (تايوان، كوريا، اليابان، الصين)، مع انفراد للولايات المتحدة بكل ما يتعلق ببرامج التصميم، وانفراد هولندا بصناعة آلات الطباعة.

من جهة أخرى، يُعتبر قانون الرقائق والعلوم (CHIPS and Science Act) الأمريكي لحظة تحول حاسمة من النظام الليبرالي والأسواق المفتوحة نحو القومية التكنولوجية التي ترتبط مباشرة بالأمن القومي والمصالح الجيوبوليتيكية، كما يؤكد على أولوية الجيوبوليتيكا على الأعمال التجارية العالمية¹، وأصبحت معركة الرقائق العالمية تقودها الحكومات وليس الشركات، تقودها الايديولوجيا والحسابات السياسية وليس الاقتصاد، وعليه، فالتفاعلات بين الفاعلين الرئيسيين في قطاع الرقائق تؤثر وتتأثر بالتوترات الجيوبوليتيكية العالمية، كما أن لكل فاعل مصالحه الخاصة بحسب وزنه الجيوبوليتيكي.

الولايات المتحدة، تهيمن على أجزاء كبيرة من صناعة الرقائق ولكن سلاسل التوريد العالمية غير الآمنة تضعها في حالة من الانكشاف الاستراتيجي، ففي أي لحظة يمكن للصين أو لحادث طبيعي أو توتر جيوبوليتيكي أن يقطع إمدادات الرقائق الضرورية لاقتصادها ولجيشها.

هولندا، تعتبرها الولايات المتحدة من الدول الحليفة ذات التفكير المماثل، حيث رضخت للضغوطات الأمريكية ووافقت على المشاركة في الحصار التقني على الصين بحجة أن شركة ASML تستعمل التكنولوجيا الأمريكية وقد تقع تحت طائلة العقوبات في حالة الرفض، إضافة إلى الحماية التي يوفرها حلف الناتو ضد التهديد العسكري الروسي والتكنولوجي الصيني، صرحت وزيرة التجارة الهولندية بأنه بعد نظر الحكومة في "التطورات التكنولوجية والسياق الجيوبوليتيكي" ترى هولندا أنه "على أسس أمنية وطنية ودولية من الضروري أن تتم السيطرة على هذه التكنولوجيا بأسرع وقت ممكن"².

اليابان، حليف لأمريكا، وتوجد بينها وبين الصين توترات جيوبوليتيكية حول جزر متنازع عنها، جربت الحرب التكنولوجية مع الولايات المتحدة في ثمانينيات القرن لماضي وخسرتها، انضمت إلى الحصار التقني على الصين لكن بضوابط مختلفة عن ضوابط التصدير الأمريكية، حيث

¹ Y Luo, Van Assche A, **Op.cit.**

² Annabelle Liang, **US-China chip war: Netherlands moves to restrict some tech exports**, BBC.com, March 2023, URL: <https://bit.ly/3OLEleH>.

صرح وزير التجارة الياباني¹ بأن "الإجراءات الجديدة تهدف إلى منع تحويل المعدات للاستعمال العسكري".

كوريا الجنوبية، دولة صغيرة عالقة بين شراكة أمنية أمريكية وشراكة اقتصادية صينية، لكنها تتوجه ببطء نحو اعتماد الرؤية الأمريكية والانفصال الاقتصادي عن الصين، والمواقف الكورية تتأرجح بين الخوف من انتقام صيني، وبين قبول المغريات الأمريكية من دعم مالي لشركات الرقائق ودعم أمني ضد كوريا الشمالية.

الصين، لم تتجح مقاربتها في أن الترابط الاقتصادي المكثف وحسابات الربح والخسارة يمنع الآخرين من معاقبتها وعزلها تكنولوجياً، فالاعتبارات الأمنية والمصالح الجيوبوليتيكية كانت أقوى من الاقتصاد، وحتى لو نجحت في تحقيق بعض النجاح في صناعة رقائق محلية إلا أنها ستجد صعوبة تدراك الفجوة التكنولوجية بالنسبة للرقائق الفائقة وكذا تلبية طلب الصناعة المحلية من الرقائق أكبر من 14 نانومتر.

تايوان، أصبحت الجزيرة من أخطر نقاط التوتر الجيوبوليتيكي في العالم، حيث تعتبرها الصين أرضاً صينية يجب أن تعود للبر الصيني وتريدها الولايات المتحدة وحلفاؤها دولة مستقلة ديمقراطية حرة على الطريقة الغربية، لذلك يعتبر القادة في تايوان صناعة الرقائق صناعة استراتيجية لأمن الجزيرة، حتى أن مسابك الجزيرة تدعا بـ "درع السيلكون" الذي يحميها من العدوان الصيني ويضمن لها الحماية الأمريكية الدائمة، فرغم أنها أنشأت مصانع في الولايات المتحدة واليابان لصناعة الرقائق الفائقة إلا أنها تتقدم دائماً بخطوة إلى الأمام وتحفظ بتكنولوجيا الرقاقة الأحدث (الآن رقاقة 2 نانومتر) داخل الجزيرة، حتى إن الناس في تايوان يتداولون نكتة تقول: "إذا غزت الصين الجزيرة فإن المكان الأكثر أماناً للاختباء هو مصانع الرقائق".

وبناءً على ما تقدم، تعمل الولايات المتحدة وحلفاؤها - الذين يتم إقناعهم أو الضغط عليهم تحت طائلة العقوبات - على تشديد الحصار التقني على الصين في قطاع الرقائق، والذي يهدف لخنق الصناعة التكنولوجية الصينية ليس فقط لكبحها بل لتحطيمها وإعادةتها إلى الوراء، والصين في المقابل تكافح للحفاظ على نموها التكنولوجي وخلق صناعة رقائق محلية تضمن على الأقل نمواً اقتصادياً مقبولاً على المدى القريب.

¹ Michelle Toh, Junko Ogura, **Japan joins the US and Europe in chipmaking curbs on China**, CNN.com, March 2023, URL: <https://bit.ly/3DIM2Mn>.

وعليه، فالصراع بين الطرفين صراع صفري مستمر يرقى لتسميته بـ "حرب باردة رقمية"، إذ أنه بوجود الرقائق الفائقة المتطورة حصرياً على جزيرة تايوان فالمنافسة ستستمر ولا يمكن لأي طرف التغلب على الطرف الآخر، فاللعبة الجيوبوليتيكية لصناعة الرقائق أصبحت لعبة ثلاثية، حيث تسعى الولايات المتحدة للهيمنة المطلقة على صناعة الرقائق الفائقة للحفاظ وتعزيز هيمنتها الاقتصادية والعسكرية، والصين تسعى للحصول عليها لمواصلة صعودها التكنولوجي، وتايوان لن تفرط في أسرارها لأنها ببساطة هي الضامن الوحيد لحماية وجودها.

المبحث الثالث: سيناريو التغيير (السيناريو الراديكالي)

يبدأ هذا السيناريو بتفكك للفضاء السيبراني وانقسامه إلى كتلتين كبيرتين، مع استمرار الصراعات بين الدولتين وتطوير مكثف للتقنيات الجديدة، ثم تستغل كل دولة الإختراقات العلمية الجديدة في شن حرب سيبرانية على الخصم مما قد يؤدي إلى نزاعات عسكرية محدودة قد تتوسع بمرور الوقت وتتحول إلى نزاعات عالية الشدة لا تنتهي إلا بخضوع أحد طرفي الصراع واستسلامه وقبول تبعيته للطرف المنتصر.

المطلب الأول: تفكك الفضاء السيبراني

يفترض سيناريو التفكك انقساماً حاداً للفضاء السيبراني، يشتمل هذا السيناريو على انقسامات رأسية وأفقية في الفضاء السيبراني، حيث يحدث تفكك للانترنت العالمي إلى كتل سيبرانية جيوبوليتيكية متباينة، كما يبرز فضاءان سيبرانيان كبيران ومستقلان يُمثّلان الانقسام الرأسي؛ يتميز الأول بخصائص تكنولوجية صينية والثاني بخصائص تكنولوجية أمريكية إلى جانب فضاءات سيبرانية أصغر في الحجم والطبيعة، تتداخل فيها التكنولوجيا الأمريكية والصينية مع امكانية بروز ميزة معينة في طبقة من طبقات الفضاء السيبراني (مثل: قانون خاص لإدارة البيانات).

لكن قبل التعمق في شرح سيناريو التفكك لابد من معرفة أين نحن الآن؟ منذ الأيام الأولى لبداية تشبيك أجهزة الكمبيوتر كانت الولايات المتحدة تهيمن على تشكيل وتطوير هذا الفضاء الرقمي الجديد وفق مصالحها الوطنية وصورتها العالمية، كما عملت على نشر رؤيتها لفضاء عالمي موحد، مفتوح، قابل للتشغيل البيني، آمن وموثوق، ورغم ظهور بوادر لرفض هذا الانفتاح غير المنضبط لدى بعض الدول -حتى الغربية منها- إلا أنها استسلمت في النهاية أمام إغراء التأثير الليبرالي على السياسة العالمية لهذا الفضاء والذي سمح بتدفق الأفكار الغربية نحو شعوب العالم بعيداً عن أعين الحكومات الوطنية، وأصبحت حكومات العالم بين خيارين، إما الاتصال والسماح بالتدفق الحر للبيانات والاستفادة من النمو والازدهار في العالم الرقمي، وإما الانفصال عنه وتحمل العزلة والخسارة الاقتصادية والسياسية¹.

¹ Adam Segal, Goldstein Gordon, **Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet**, The Council on Foreign Relations, United States of America, 2022.

غير أن عودة الحكومات للاهتمام بقضايا الفضاء السيبراني مع بداية الألفية الجديدة وعزمها على التصدي للتهديدات التي حملها معه جعل الرؤية الأمريكية حول حرية الاتصال موضع شك، وبدأت تلوح في الأفق محاولات للسيطرة على هذا الفضاء والتي ينتج عنها بالضرورة نوع من أنواع التقسيم، فدعوات ألمانيا وفرنسا للمنصات الأمريكية لمراقبة الخطاب النازي والمعادي للسامية كانت البداية لإعطاء صبغة جغرافية للفضاء السيبراني، فما يمكن الوصول إليه من معلومات في بلد ما يعتبر محظوراً في بلد آخر تماشياً مع المقاربات المتباينة لحرية التعبير، واليوم تعتبر هذه الممارسات شائعة في الكثير من البلدان حتى في الولايات المتحدة نفسها مما يُعطي لوحة جيوبوليتيكية مقسمة للفضاء السيبراني حسب مفهوم الحرية والقضايا التي تشغل المجتمعات والحكومات.

من جهة أخرى، تلقى مفهوم "الفضاء السيبراني العالمي" انتقاداً حاداً من الحليف التقليدي للولايات المتحدة، فبعد تسريبات "سنودن" تزايدت الشكوك لدى دول الاتحاد الأوروبي حول مخاطر الاعتماد على تكنولوجيا المعلومات والاتصالات الأمريكية، وتم اعتماد "اللائحة العامة لحماية البيانات" في 2016 التي تعزز التحكم الأوروبي الخالص في بيانات مواطنيه، ثم انتشرت مفاهيم اللائحة ليتم اعتمادها عبر دول مختلفة مثل البرازيل واليابان وكوريا الجنوبية وغيرها، كما تسارعت عمليات توطين البيانات في عملية معاكسة لمبدأ أساسي قام عليه الفضاء السيبراني وفق الرؤية الأمريكية والذي يدعو لحرية نقل البيانات والمعلومات، كما أن خبراء الاتحاد الأوروبي لم يكتفوا بقضايا البيانات بل دعت المفوضية الأوروبية في 2022 لتعزيز الاكتفاء الذاتي من أشباه الموصلات والترويج لبدائل للمنصات الأمريكية الكبرى¹، كما دعا مجلس التعاون الأوروبي إلى اتخاذ المزيد من الخطوات الحاسمة نحو بناء السيادة السيبرانية وتقليل التبعية التكنولوجية للآخرين، وإذا تحقق ذلك فسيحدث انقسام رأسي للفضاء السيبراني وتتشكل منطقة سيبرانية أوروبية جديدة.

في الجهة المقابلة، سعت الدول التي تصنفها الولايات المتحدة كمنافسين، خصوم وحتى أعداء إلى السيطرة على الفضاء السيبراني في مجالها الجغرافي الوطني على الأقل، ففي روسيا، سعت الحكومة بعد احتجاجات 2012 إلى فرض رقابة مشددة على محتوى الأنترنت وفرضت Roskomnadzor الهيئة الروسية المنظمة للأنترنت ضوابط صارمة لحجب المواقع المناهضة للكرملين والضغط على المنصات العالمية (الأمريكية) لإزالة المحتوى غير القانوني، كما سعى

¹ European Commission, Versailles Declaration: Informal meeting of the Heads of State or Government, March 2022, URL: <https://bit.ly/46wgk1Z>.

الرئيس "بوتين" إلى تطوير أنترنت محلي "Runet" يمكن فصله عن الأنترنت العالمي ويُعطي إمكانية نقل المستخدمين في روسيا من المنصات الأمريكية إلى المنصات ومحركات البحث الروسية، وقد تم فعلاً حظر المنصات الأمريكية بعد بداية العملية العسكرية الروسية في أوكرانيا في 2022، من جهتها تمتلك كل من إيران وكوريا الشمالية شبكة أنترنت محلية يمكن فصلها عن الشبكة العالمية عند الضرورة، فمشروع "أنترنت حلال" الإيراني الذي بدأ منذ 2005 عكس رغبة الحكومة الإيرانية في خلق فضاء سيبراني محلي غير متصل بالشبكة العالمية يمكن التحكم فيه وقد ظهرت قدرة الحكومة الإيرانية على التحكم في الأنترنت منذ احتجاجات 2019، أما كوريا الشمالية فهي المثال الأبرز للفصل التام عن الشبكة العالمية، فالأنترنت لدى المستخدم الكوري الشمالي مرادف لما تقدمه شبكة "كوانغ ميونغ Kwangmyong" من خدمات، حيث لا يمكن الوصول إلى هذه الخدمات من خارج كوريا كما لا يمكن الوصول للشبكة العالمية من الداخل الكوري¹.

ورغم الانتشار الواسع لعمليات المراقبة والحجب وفصل الشبكة المحلية عن الشبكة العالمية في الكثير من دول العالم فإن التطور التكنولوجي يُقوض في كثير من الأحيان سياسات الرقابة والحجب، ويُجبر الدول على إعادة الإتصال بالشبكة العالمية، إلا أن الصين أثبتت أنها الدولة الأقوى من حيث امتلاك القدرة على صنع وإدارة فضاء سيبراني موازٍ للفضاء السيبراني الحالي، ذلك أنها سعت منذ البداية لتطويق نفسها بجدار حماية ضخم وعززت قدراتها التكنولوجية المحلية متحدية هيمنة الولايات المتحدة، وتكمن قوة الصين في أن تطورها التكنولوجي يشمل جميع طبقات الفضاء السيبراني (الأجهزة، البرامج، عدد المستخدمين، القواعد والمعايير، القوانين) وهذا ما يمنحها فرصة لتقديم نموذج مختلف للفضاء السيبراني تسعى لنشره عبر العالم، إضافة إلى أن الصراع بين القوتين العظميين الولايات المتحدة والصين قد توسع ليشمل مختلف المجالات (السياسة، الاقتصاد، الجيش... إلخ) وترى كل دولة الدولة الأخرى كمنافس جيوبوليتيكي يشكل تهديداً، حيث تشغل التكنولوجيا والفضاء السيبراني محور هذه المنافسة.

وبما أن الاختلاف في الرؤى حول قضايا الفضاء السيبراني للدولتين يزداد اتساعاً فإن تفكك هذا الفضاء العالمي إلى جزئين منفصلين يحمل كل منهما تكنولوجيا مختلفة هو سيناريو محتمل جداً، وذلك لوجود عوامل عديدة تدفع نحو هذا التقسيم نذكر منها:

¹ Adam Segal, Goldstein Gordon, op.cit.

الفرع الأول: العوامل الأمنية

يتحول الفضاء السيبراني بسرعة ليصبح مكاناً أكثر خطراً تنتشر فيه الجرائم والتهديدات، وتتزايد الاتهامات بالاختراقات السيبرانية بين الولايات المتحدة والصين، حيث تتهم الولايات المتحدة الصين بالتجسس على القطاعين الحكومي والخاص وسرقة الملكية الفكرية خاصة من الشركات التي تربطها علاقة عمل مع البنتاغون، ولعل أشهر عمليات التجسس هي ما يتعلق بالطائرة الشبحية الصينية من الجيل الخامس J-20 والتي تقول المصادر الأمريكية¹ إنها نسخة معدلة عن الطائرة الأمريكية F-22 Raptor وأن الصين لا تملك قدرات لتطوير طائرة بهاته المواصفات لولا عمليات التجسس السيبراني وسرقة البيانات والمخططات من خوادم شركة "لوكهيد مارتين"، كما أن هذه العمليات تُضعف قدرة الجيش الأمريكي وتهدد الأمن القومي بشدة حيث تفقد الولايات المتحدة ميزة التفوق العسكري عالمياً، من جهتها تنفي الصين هذه الاتهامات بل تتهم في المقابل الولايات المتحدة باستغلال هيمنتها على الفضاء السيبراني للتجسس على الصين اقتصادياً وعسكرياً في محاولة منها لكبح التطور الكبير لجيش التحرير الصيني وإضعاف قدراته على حماية الأمة الصينية.

إضافة إلى ذلك، تستغل الصين ضبابية الخط الفاصل بين الفواعل الحكومية والجهات الخبيثة للتجسس الاقتصادي والعسكري على الولايات المتحدة، وتستغل الولايات المتحدة قدراتها السيبرانية الكبيرة من خلال أجهزتها الأمنية لتهديد الأمن القومي الصيني، ويساهم التشبيك العالمي بدوره في المزيد من عمليات التجسس والتلاعب بالمعلومات الاستخباراتية وعمليات مكافحة التجسس، كما أن الذكاء الاصطناعي والتقنيات الناشئة تؤدي إلى مزيد من عدم التوازن الاستراتيجي في إطار سعي الدولتين لتحقيق ميزة عسكرية في الفضاء السيبراني تمنحهما التفوق في الحروب المستقبلية، لذلك فاحتمالات فصل حاد للشبكات الأمريكية عن الشبكات الصينية وارد جداً تحت ذرائع متعددة على رأسها حماية الأمن القومي.

الفرع الثاني: العوامل الاقتصادية

يُشكل الاقتصاد أحد محاور المنافسة الاستراتيجية بين الولايات المتحدة والصين، فالدولتان تملكان أكبر اقتصادين في العالم، كما أن قوة الاقتصاد ترتبط طردياً مع التطور والتفوق

¹ Peter Aitken, **China has stolen US military secrets to create formidable J-20 knockoff of America's F-22 Raptor**, foxnews.com, March 9, 2023, URL: <https://bit.ly/3XCoKkw>.

التكنولوجي، فمن جهة، تشهد الصين صعوداً سريعاً لتصبح أكبر سوق للتجارة الرقمية في العالم، كما أن الحكومة والشركات التكنولوجية الصينية تعمل على تعزيز الاقتصاد الرقمي والذي يعتبره الرئيس الصيني "شي" القوة الحاسمة لإعادة تشكيل الهياكل الاقتصادية ومحددات الهيكل المنافسة العالمية، في المقابل، رغم إدراكها لأهمية الاقتصاد الرقمي في الحفاظ على الهيمنة العالمية إلا أن الولايات المتحدة فشلت في مواكبة التطورات المتسارعة للتجارة الرقمية، فرغم نجاحها في تقديم حماية قوية لتدفق البيانات عبر الحدود من خلال الاتفاقيات الثنائية (مع اليابان، كوريا، المكسيك وكندا) فإنها فشلت في بناء اتفاقيات متعددة الأطراف مع باقي الدول (خاصة دول المحيط الهادي والهندي) نظراً لحساسية قضايا الخصوصية وحماية البيانات في الداخل الأمريكي، وهذا ما يجعلها متخلفة على الصين¹.

لتدارك هذا التخلف سعت الولايات المتحدة إلى محاولات لكبح الصعود الصيني عبر استراتيجيات الفصل التكنولوجي والسياسات التجارية الحمائية، وهو ما يساهم في تقويض مبادئ التجارة الحرة والنظام الليبرالي ككل، إضافة إلى أن صعود مفاهيم القومية التكنولوجية وعدم اليقين في سلاسل التوريد الذي صاحب جائحة كورونا سرع من ظهور بيئتين متباينتين لتطوير تكنولوجيات الفضاء السيبراني.

من جهة أخرى، أصبحت البيانات مصدراً رئيساً للقوة ومحركاً للمنافسة الجيوبوليتيكية، فهي تغذي الابتكار والنمو الاقتصادي لذلك فكل من الولايات المتحدة والصين تنتظر إلى البيانات الضخمة كأصل إستراتيجي ضروري لتحقيق الأمن الاقتصادي، وهذا ما فرض تقسيماً للأسواق، فالشركات الصينية (Alibaba،Tencent) تسيطر على الداخل الصيني وعلى دول الحزام والطريق وتسعى للتوسع، والشركات الأمريكية (Alphabet، Amazon، Meta) تفقد نفوذها في هذه المناطق، وتتجه الأمور نحو تحديد لمناطق النفوذ لكل دولة من خلال منتجات، قواعد ومعايير متباينة للفضاء السيبراني في سبيل حماية نشاط شركاتها ومن ثم تحقيق أمنها الاقتصادي.

الفرع الثالث: العوامل السياسية والاجتماعية

في الجانب الأمريكي هناك اتفاق بين السياسيين (الديمقراطيين والجمهوريين) على أن الصين هي المنافس الاستراتيجي الأقوى وأن هذه المنافسة طويلة الأمد، كما يتفق الحزبان على ضرورة

¹ Adam Segal, Goldstein Gordon, **op.cit.**

العمل على كبح الصعود التكنولوجي الصيني والإبقاء على ريادة الولايات المتحدة في الفضاء السيبراني، في المقابل، تم تمديد حكم الرئيس "شي" في الصين والذي يرى في الفضاء السيبراني والتكنولوجيا فرصة مواتية لإعادة بعث وتجديد الأمة الصينية وتحقيق الحلم الصيني في قيادة العالم.

هذا الصراع بين الدولتين ينعكس في اختلاف الرؤى حول حوكمة الفضاء السيبراني، حيث نجد المقاربة الأمريكية لفضاء سيبراني مفتوح يديره أصحاب المصلحة في مقابل المقاربة الصينية التي تتمحور حول مفهوم السيادة السيبرانية، بعبارة أخرى، تدفع قوة شركات التكنولوجيا الأمريكية نحو الإنفتاح والتوسع عبر الحدود مع التركيز على الخصوصية وحماية البيانات (التركيز على الفرد) في مقابل قوة الطرح الصيني حول أحقية الحكومات في تنظيم فضاءها السيبراني بحجة حماية الأمن القومي (التركيز على الدولة) خاصة مع التطور التكنولوجي لشركاتها في مجال المراقبة.

هذا التباين في الرؤى يدفع الدول للاختيار بين المفاهيم والتكنولوجيا الأمريكية أو الصينية مما يؤدي في نهاية الأمر إلى تشكل فضاءين سيبرانيين منفصلين.

الفرع الرابع: طبيعة تفكك الفضاء السيبراني

تتمثل نقطة البداية لفهم طبيعة تفكك الفضاء السيبراني في فهم مبدأ التوصيل العالمي الذي رافق تطور الأنترنت، حيث كانت الرؤية المشتركة لبناء الأنترنت هي أن كل جهاز على الشبكة يمكنه تبادل حزم البيانات مع أي جهاز آخر يرغب في تلقيها، ولا يتم ذلك إلا عبر إمكانية التوصيل البيني بين الأجهزة والتطبيقات المختلفة، وعليه، فإن تفكك الفضاء السيبراني يكون عبر تقسيم وتجزئة الطبقات المشكلة له ويشمل ثلاثة مستويات:

أولاً، التفكك التقني: في هذه الحالة يكون التقسيم بنيوياً يمس هيكلياً الأنترنت الأساسية، حيث يتم قطع الروابط بين الشبكات لتصبح شبكات مستقلة، أي أن البنية التحتية المادية للكتل السيبرانية منفصلة عن بعضها البعض انفصلاً تاماً أو مع وجود نقاط اتصال قليلة متحكم فيها بصرامة.

ثانياً، الفضاء السيبراني الوطني: ويُشار إليه كذلك ببلقنة الأنترنت¹، حيث يتم تقسيم الفضاء السيبراني العالمي إلى فضاءات سيبرانية وطنية في إطار تطبيق مفهوم السيادة السيبرانية، ويخضع الفضاء السيبراني الوطني لقوانين الدولة المعنية، كما تقوم الدولة بسن القوانين والقواعد والسياسات التي تراها مناسبة لإدارة فضاءها السيبراني.

ثالثاً، التفكك التجاري -الاقتصادي: حيث إن دعوات تنظيم أسواق التكنولوجيا الناتجة عن سياسات الفصل التكنولوجي وحظر منتجات التكنولوجيا (أجهزة، تطبيقات، بيانات) يجعل من هذه المنتجات حكرًا على مجموعات محددة (دول أو شركات)، وهو ما يلغي بالضرورة مبدأ حيادية الشبكة، كما أن انتشار القومية التكنولوجية يجعل من تطور الفضاء السيبراني وما ينتج عنه من فوائد اقتصادية يسير وفق خطين متوازيين (أمريكي-صيني).

وبناءً على ماسبق، فإن قدرات الدولتين الاقتصادية والسياسية والعسكرية والسيبرانية تجعل من الصعب على إحدهما حسم الصراع لصالحها، وعليه فعلى المدى المتوسط فإن الأنترنت العالمي سيصبح من الماضي وتحل محله شبكات وطنية، إقليمية وكتل سيبرانية، يصعب من خلالها الوصول إلى المحتوى والخدمات من خارج البلد أو المنطقة أو الكتلة، ويصبح قلة من المستخدمين -ماعدا المتخصصين والجواسيس والمجرمين- يملكون المهارة أو الرغبة في تجاوز الأسوار والوصول إلى شبكات الآخرين.

يتفكك الفضاء السيبراني العالمي إلى قسمين كبيرين فضاء أمريكي وآخر صيني، ويُشكل كل فضاء الدول ذات التفكير المماثل للولايات المتحدة أو الصين إضافة إلى قاعدة المستخدمين التابعين لشركات التكنولوجيا الأمريكية أو الصينية.

حيث يشمل الفضاء السيبراني الصيني كلاً من الصين ودول الحزام والطريق في آسيا وإفريقيا ودولاً في أمريكا اللاتينية، ويتميز بالأمن السيبراني القوي والمراقبة الشاملة للحكومة بفضل التكنولوجيا التي توفرها شركات التكنولوجيا الصينية، ويفضل فيه الأفراد (خاصة من يستعمل الأنترنت للمرة الأولى) التخلي عن الخصوصية مقابل الاتصال والتنمية، يصفه خصومه بالأنترنت الاستبدادي، أما الفضاء الأمريكي فيشبه ما هو معروف اليوم، تقوده كبرى شركات التكنولوجيا الأمريكية مع استبعاد مقنن للشركات الصينية، ويشمل الولايات المتحدة وحلفاءها، مع

¹ يُشير مصطلح "البلقنة" إلى التقسيم الإثني والسياسي لمنطقة البلقان بعد نهاية الدولة العثمانية، كما أعيد استخدام المصطلح للمرة الثانية إبان الحروب اليوغسلافية في نهاية القرن المنصرم.

وضع خاص لأوروبا فيما يتعلق بالبيانات، يتميز بتواصل المناقشات حول الخصوصية وحماية البيانات والأمن السيبراني، كما ستظهر مناطق للصدام تتداخل فيها التكنولوجيا الأمريكية والصينية مثل دول المحيطين الهادي والهندي ودول الشرق الأوسط، وتتميز بضعف الأمن السيبراني وانتشار كبير للجرائم السيبرانية والإحتيال، كما أن إمكانية هذه المناطق للاختبار بين التكنولوجيا الأمريكية والصينية تغذي الابتكار التكنولوجي المتوازي الأمريكي والصيني خاصة ما يتعلق بتكنولوجيا الأنترنت الفضائي.

المطلب الثاني: سيناريو الحرب السيبرانية الشاملة

يفترض هذا السيناريو أن زيادة الانفصال التكنولوجي وتضيق الصراع في المجال السياسي والاقتصادي وتآكل الثقة الاستراتيجية بين الولايات المتحدة والصين يُحفز الدولتين على تكثيف الهجمات السيبرانية المتطورة والمعقدة خاصة على البنية التحتية الحيوية مع اختيار دقيق للأهداف داخل كلا الدولتين و/أو في الدول الحليفة، مع محاولة الإبقاء على الصراع دون عتبة النزاع المسلح، إلا أن اشتداد هذه الحرب السيبرانية وتوظيف الدولتين لأحدث تكنولوجيا الذكاء الاصطناعي غير المتوافقة (أمريكية/صينية) وغير المتأكد من سلامتها يزيد من احتمالات سوء الفهم والحسابات الخاطئة لدى الطرفين مما يفجر حرباً سيبرانية تسبق وترافق مواجهة عسكرية بين القوتين أو بين الصين وأحد حلفاء الولايات المتحدة على الأقل في منطقة المحيطين الهادي والهندي.

في البداية، لابد من الأخذ بعين الاعتبار أن مصطلح "الحرب السيبرانية" مصطلح مثير للجدل خاصة في الأوساط الأكاديمية، فرغم أنه ظهر مع بدايات تشكل الفضاء السيبراني في مقال منشور في العام 1993 لـ "جون أركيلا وديفيد رونفالت" بعنوان "Cyber war is coming" حذر فيه الكاتبان من أن الحرب السيبرانية قادمة، إلا أن المفهوم حتى اليوم يعاني من حالة من الغموض وعدم الاتفاق، يرجع ذلك في الأساس إلى التطور السريع لتقنيات الفضاء السيبراني واستعمالها المزدوج (مدني-عسكري)، لذلك فكل حسب تعريفه للحرب السيبرانية إما يرى أنها قادمة، وإما أنها فعلاً قائمة، وهناك من يرى أنها لن تأتي أبداً، وعليه، فالحرب السيبرانية في هذه الدراسة تتوافق مع ما يراه "جوزيف ناي" الذي يعرفها بأنها "الأعمال العدائية في الفضاء السيبراني

التي لها آثار تعادل أو تفوق العنف الحركي التقليدي"¹، حيث إن العنف التقليدي غالباً ما ينتج عنه وفيات بين البشر وتدمير للممتلكات، حيث نعتقد أن عمليات التجسس في الفضاء السيبراني ما هي إلا امتداد للتجسس التقليدي، كما أن هجومات منع الخدمة أو تخريب البيانات أو مواقع الأنترنت أحداث يكمن أن تقع دون هجوم بسبب مشاكل في الأجهزة أو الأنظمة.

محفزات الحرب السيبرانية بين الولايات المتحدة والصين

يمكن تقسيم المحفزات التي تدفع الدولتين نحو حرب سيبرانية قد تكون شاملة إلى ثلاثة أنواع؛ أولاً، محفزات تتعلق بخصائص الفضاء السيبراني، ثانياً، تداعيات العلاقة الثنائية الصراعية بين البلدين، ثالثاً، تقنيات الذكاء الاصطناعي والتقنيات الناشئة.

أ. محفزات الحرب السيبرانية من داخل الفضاء السيبراني²

تزايد الاعتماد على الفضاء السيبراني في تسيير حياة الدول والأفراد خاصة بعد جائحة كورونا، إذ دفعت إجراءات الحجر الصحي التي فرضتها أغلب دول العالم على مواطنيها التحول إلى الفضاء السيبراني لمواصلة أداء مهام الحكومات، الشركات والأفراد، وقامت العديد من الحكومات بتسريع التحول التكنولوجي في بلدانها، هذا التحول بقدر ما هو ضروري لاستمرار وبقاء الدول فإنه حمل معه مزيداً من نقاط الضعف للأمن القومي بأبعاده المختلفة.

من ناحية أخرى، أغرى هذا التوسع الكبير للفضاء السيبراني الجهات الخبيثة والهيئات الأمنية للدول باستغلاله من خلال تطوير آليات ونطاق الهجمات السيبرانية، حيث تعددت أشكالها لتمس كل التقنيات الناشئة كإنترنت الأشياء والذكاء الاصطناعي، كما زادت الهجمات التي توصف بالكبرى في العدد ودرجة التعقيد وتقلصت الفجوة الزمنية بينها، كما لعبت العملات الرقمية دوراً مهماً في حماية الهاكرز وشجعتهم على المزيد من الهجمات (مثلاً: دور البتكوين في انتشار فيروس الفدية).

إضافة إلى ماسبق، تتسابق الدول لتطوير وامتلاك أسلحة سيبرانية، كما يتزايد اعتماد الجيوش في العالم على تقنيات الفضاء السيبراني (خاصة تقنيات الذكاء الاصطناعي) في اللوجستك،

¹ Joseph S Nye Jr, Nuclear Lessons for Cyber Security, *Strategic Studies Quarterly* vol 5 n° 4, 2011, pp 18-38.

² خليفة إيهاب، الحرب السيبرانية: الإستعداد لقيادة المعارك العسكرية في الميدان الخامس، القاهرة: العربي للنشر والتوزيع، 2021، ص ص 79-98.

نظم القيادة والتحكم، تحديد الأهداف بما فيها منظومات ومحطات الأقمار الصناعية، وهذا ما يزيد من احتمالية تعرضها للهجوم بغرض السيطرة على الأنظمة العسكرية، سرقة المعلومات والتلاعب بها أو حتى تدمير البنية التحتية العسكرية.

ولعل أخطر القضايا ما يتعلق بالمجال النووي، إذ تعتمد الصناعة النووية المدنية والعسكرية بشكل متزايد على أنظمة المعلومات والاتصال، ورغم التدابير الأمنية الصارمة في المحطات النووية وفصل كل ما يتعلق بالنشاط النووي عن الشبكات العالمية إلا أن تاريخ الهجمات السيبرانية عليها ينبئ بإمكانية تعرضها للهجوم، وقد تكون أهدافاً ذات أهمية قصوى في حالة الحرب السيبرانية الشاملة.

ب. العلاقة الصراعية بين الولايات المتحدة والصين تحفز الحرب السيبرانية

تتخبط الولايات المتحدة والصين في منافسة استراتيجية شاملة تؤثر على كل المجالات السياسية، الاقتصادية والعسكرية وتُشكل التكنولوجيا محور هذه المنافسة، وفي سعيها للفوز بالمنافسة تستخدم الدولتان جميع الأساليب شرعية كانت أو غير شرعية، وكلما زادت حدة الصراع بين الطرفين تآكلت الثقة الاستراتيجية بينهما، وزاد عدم اليقين والشك في نوايا الطرف الآخر، وأصبح كل قرار أو إجراء يتعلق بالفضاء السيبراني يتخذ من طرف ما، يراه الطرف الآخر أنه ضده.

من جهة أخرى، فإن احتمال وقوع نزاع مسلح كبير بين الدولتين يكاد يكون منعدماً، فحسب تقرير لمؤسسة راند صدر في 2015 بعنوان "الحرب ضد الصين: التفكير فيما لا يتقبله العقل" فإن دخول الولايات المتحدة والصين في نزاع مسلح بمنطقة المحيطين الهادي والهندي لا يُسفر عن منتصر بحسابات الكلفة والفائدة، رغم إعطاء الأفضلية للولايات المتحدة بخسائر وتداعيات أقل¹، لكن تقرير 2022 لنفس المؤسسة بعنوان "عودة حرب القوى العظمى: سيناريوهات الصراع المنهجي بين الولايات المتحدة والصين" رجح سيناريو حرب منخفضة الكثافة طويلة الأمد تركز على الضربات الدقيقة والحرب السيبرانية²، لذلك ستلجأ الدولتان إلى الهجمات السيبرانية المتطورة والمعقدة ضد بعضهما البعض، إما لتحقيق التفوق في الفضاء السيبراني وتعطيل مساعي الخصم لذلك أو على الأقل تحقيق التوازن في القدرات السيبرانية.

¹ ديفيد سي جومبرت وآخرون، الحرب ضد الصين: التفكير فيما لا يتقبله العقل، كاليفورنيا: مؤسسة راند، 2016.

² Timothy R Heath et al, **The Return of Great Power War: Scenarios of Systemic Conflict Between the United States and China**, Calif: RAND Corporation, 2022.

إضافة إلى ذلك، تُدرك الصين مدى خبرة الولايات المتحدة في استعمال الأسلحة السيبرانية في تعطيل وتدمير البنية التكنولوجية المادية للخصوم (فيروس ستكسنت الشهير لتعطيل البرنامج النووي الإيراني)، لذلك فهي لن تتوانى عن استخدام نفس المبدأ والعمل على شن هجمات سيبرانية على البنية التكنولوجية المادية لتعطيل الصعود التقني الصيني مع مراعاة البقاء دون عتبة الصراع العسكري، ومن جهتها، تُدرك الولايات المتحدة قدرات الصين في الإختراق والتسلل السيبراني في الداخل الأمريكي وإمكانية تدمير للبنية التحتية الحيوية الأمريكية المدنية والعسكرية، لذلك، ففي ظل إدراك الطرفين لقدرات بعضهما البعض مع حالة عدم اليقين فإن أبسط خطأ في تفسير العمليات السيبرانية لطرف ما يُعطي إشارة للطرف الآخر على بداية الحرب السيبرانية الشاملة.

ج. الذكاء الاصطناعي والتقنيات الناشئة

يسرع الذكاء الاصطناعي أتمتة العمليات ويعالج كمّاً هائلاً من البيانات، وينظم ويعيد تنظيم العالمين المادي والاجتماعي، كما تزايدت استخداماته العسكرية في التقنيات الناشئة كالتطورات بدون طيار والدرون، الآليات المقاتلة، لذلك فالصراع محتدم بين الولايات المتحدة والصين حول مرتكزاته الثلاث: البيانات، الحوسبة الكمومية والخوارزميات، وبسبب أن من يصل أولاً يأخذ كل المزايا تفرض المنافسة نشرًا واسعاً للذكاء الاصطناعي دون إعطاء الوقت الكافي لتقييم مخاطره أو تجاهلها، وهذا ما يزيد من احتمالات أن تنزلق الدولتان نحو حرب مدمرة.

يجادل "كيسنجر" أن الذكاء الاصطناعي يعمل كما نتوقع إلا أنه يعطي نتائج غير متوقعة، وعليه، فإن الاستخدامات غير المدروسة والمتسعة للذكاء الاصطناعي خاصة في المجالات العسكرية قد تؤدي في النهاية إلى كارثة غير معروفة العواقب، ويضرب مثالاً من الحرب العالمية الأولى، حيث فشل صناع القرار في إدراك أن المزوجة بين المنطق العسكري القديم والتكنولوجيا الحديثة دفعت أوروبا نحو الحرب، وبنفس الطريقة قد تؤدي المنافسة غير المنضبطة لتطوير الذكاء الاصطناعي إلى نزاع عسكري كبير¹.

تتفوق الصين على الولايات المتحدة في بعض تقنيات الذكاء الاصطناعي مستفيدة من البيانات الضخمة التي يوفرها نظام المراقبة مع السيطرة الكاملة للحكومة على البيانات، كما حقق الباحثون الصينيون اختراقات علمية في مجال الحوسبة الكمومية، من جهتها، وضعت الشركات الأمريكية بعض تقنيات الذكاء الاصطناعي قيد الاستخدام (Chat GPT)، كما ضاعفت الإدارة

¹ Henry A Kissinger, Eric Schmidt, Daniel Huttenlocher, Op.cit.

الأمريكية من التمويل الحكومي لمشاريع الرقائق والذكاء الاصطناعي وفرضت حظراً على التكنولوجيا الأمريكية من أن تصل إلى الصين، لكن اللافت للانتباه هو الدعوات الأمريكية¹ لتوقيف تطوير الذكاء الاصطناعي على الأقل لفترة من الزمن وإعطاء فرصة لوضع القواعد والمعايير اللازمة للتحقق من سلامة استخدامه وتجنب مخاطر خروجه عن السيطرة، هذه الدعوات تحمل في طياتها اتهاماً للصين بأنها تُغامر بتطوير ذكاء اصطناعي دون رادع قد تكون نتائجه مدمرة للبشرية جمعاء، كما يُستشف منها أن الصين فعلاً قد حققت تقدماً كبيراً وأنها في طريقها للفوز بميزات هذه التقنية الاقتصادية والعسكرية، لكن في المقابل، لا أحد يضمن بأن البنّاعون ووكالات الأمن القومي الأمريكية لا تفعل الشيء نفسه، لذلك ففي ظل عدم اليقين والمخاطر العالية التي تميز الوضع الأمني العالمي الراهن يُمكن لتقنيات الذكاء الاصطناعي أن تفجر حرباً سيبرانية كبرى بين البلدين.

وخلاصة لما سبق، فإن اجتماع العديد من العوامل والمحفزات داخل الفضاء السيبراني نفسه أو ما ارتبط بالعلاقة الثنائية بين البلدين والوضع غير المستقر للنظام الدولي الحالي يدفع بالولايات المتحدة والصين نحو الحرب السيبرانية وقد يجعل من حظوظ نجاة الدولتين من "فخ ثيوسيديس" في الفضاء السيبراني ضئيلة جداً.

المطلب الثالث: هيمنة الولايات المتحدة / الصين على الفضاء السيبراني

تتضارب التقارير والتحليلات حول الفائزين والخاسرين في صراع الهيمنة بين الولايات المتحدة والصين، مما يؤكد حدة المنافسة وصعوبة تحقيق طرف معين الهيمنة المطلقة في جميع مجالات الفضاء السيبراني.

الفرع الأول: وجهات النظر المختلفة حول الفائز في المنافسة التكنولوجية

أولاً، وجهة النظر الأمريكية، لا يتوقف الأكاديميون وصناع القرار في الولايات المتحدة عن تضخيم قوة الصين والتحذير من أنها على وشك الفوز بالصراع التكنولوجي والهيمنة على الفضاء السيبراني، ما يعني بالضرورة خسارة الولايات المتحدة وتتحيزها عن الريادة، جاءت التحذيرات

¹ وقع العديد من الشخصيات المرموقة في مجال التكنولوجيا على عريضة تدعو للوقف الفوري لتطوير الذكاء الاصطناعي، من بين الشخصيات "إيلون ماسك" و "جيفري هنتون" الذي يُلقب بـ "الأب الروحي" للذكاء الاصطناعي والعديد من رؤساء الشركات ومراكز البحث في الذكاء الاصطناعي، ويصرح الجميع بأن البشرية ليست مستعدة بعد لتحمل تبعات تطوير هذه التقنية التي قد تنقلب عليها وتكون سبباً في فناء الجنس البشري، انظر الرابط: <https://bit.ly/44bgEl3>.

مبكرة حيث أكد "آدم سيغال" في مقاله المنشور في مجلة "فورين آفرز" سنة 2018 بعنوان "عندما تحكم الصين الويب" أنه بالنظر إلى حجم الصين وتطورها التكنولوجي فإن لديها فرصة كبيرة للنجاح¹، كما يُشير تقرير صدر سنة 2022 بعنوان "تحديات منتصف العقد للتنافسية الوطنية"² عن مركز الأبحاث الأمريكي "مشروع الدراسات التنافسية الخاصة" والذي يرأسه "إيريك شميدت" إلى أن الفترة ما بين 2025-2030 ستكون الوقت الذي تتحدد فيه القيادة التكنولوجية العالمية، وقد لا تتمكن الولايات المتحدة وحلفائها من الحفاظ على الريادة، كما أكد أن الصين إذا استولت على مصانع الرقائق الفائقة وقطعت إمدادات المعادن النادرة اللازمة لصناعتها فإن الجيش الأمريكي سيصاب بالشلل ويدخل الاقتصاد في ركود كبير.

هذا الاتجاه الذي يُعظم قوة الصين ويُقوي فرصها في تحقيق الهيمنة التكنولوجية مستقبلاً هو الأكثر شيوعاً بين الباحثين والسياسيين والاستراتيجيين الأمريكيين، ويبدو الأمر استساقاً لـ "تأثير سبوتنيك" أثناء الحرب الباردة ومحاولة للنهوض بالأمة الأمريكية (مجتمع، حكومة وشركات) وتوحيد صفوفها في مواجهة الخطر الصيني، وينتج عن هذه الرؤية تقديم العديد من المقترحات والتوصيات لكيفية تجنب هذا السيناريو الكارثي تشمل التقنيات التي يجب التركيز عليها والسياسات التي يجب اتباعها وصولاً إلى النقد العنيف لغياب استراتيجية واضحة للإدارة الأمريكية وأن ما تقوم به مجرد تكتيكات قصيرة الأمد في مواجهة استراتيجية صينية واضحة وطويلة الأمد.

ثانياً، وجهة نظر حلفاء الولايات المتحدة، تتباين الآراء لدى حلفاء الولايات المتحدة حول الفائز بالصراع التكنولوجي، لكنهم يتفقون على خطورة الصعود التكنولوجي الصيني، إذ اعتبر حلف الناتو من خلال "المفهوم الاستراتيجي 2022" أن جهود الصين للهيمنة التكنولوجية تمثل تحدياً جدياً لمصالحه الأمنية³، مع تنبيه الباحثين⁴ لقادة الدول الأوروبية على ضرورة التصدي للفجوة الرقمية وجعل أوروبا لاعباً جيوبوليتيكياً فعالاً في اللعبة التكنولوجية، من جهتها، ترى صحيفة "الغارديان" أن الصراع التكنولوجي بين الولايات المتحدة والصين محصلته صفرية وأن العالم كله

¹ Adam Segal, **When China rules the web: technology in service of the state**, Op.cit.

² Eric Schmidt, et al, **Mid-decade challenges to national competitiveness**, Special Competitive Studies Project, September 2022, URL: <https://bit.ly/3pDXa9Z>.

³ NATO, **NATO 2022 Strategic Concept**, Madrid summit, June 2022, p 5, URL: <https://bit.ly/3Q08sQF>.

⁴ سفين سميت وآخرون، حماية قدرة أوروبا التنافسية: التصدي للفجوة التكنولوجية، معهد ماكنزي، سبتمبر 2022، على الرابط: <https://bit.ly/46PsyD9>.

سيخسر في هذا الصراع¹، كما لم تخفي أن المملكة المتحدة ستكون مع الجانب الأمريكي في هذه الحرب، أما في أستراليا، فقد طور "المعهد الاسترالي للسياسات الاستراتيجية ASPI" أداة لمتابعة سباق التكنولوجيات الفائقة (الحرجة) وتُظهر النتائج بأن الديمقراطيات (الولايات المتحدة وحلفاؤها) خسرت المنافسة التكنولوجية العالمية، إذ تتقدم الصين في 37 من بين 44 تقنية حرجية².

وعليه، فإن حلفاء الولايات المتحدة مجمعون على ضرورة التصدي للصعود التكنولوجي للصين التي تتقدم بسرعة قد تمكنها من الهيمنة التكنولوجية، لكن في المقابل، تتباين أهدافهم ومصالحهم، كما لا يوجد إجماع بينهم على ضرورة الخضوع لواشنطن من أجل هيمنة تكنولوجية أمريكية.

ثالثاً، وجهة النظر الصينية، لا يوجد اتفاق بين الخبراء الصينيين حول رؤية الحكومة والحزب الشيوعي بأن الصين تسير (أو يجب أن تسير) بخطى ثابتة نحو الفوز بالصراع التكنولوجي وتحقيق الهيمنة على الفضاء السيبراني، فالمتفائلون مثل "روان زونغتسي" نائب مدير مركز شي جين بينغ لدراسة الفكر الدبلوماسي يرى أن الوقت والزخم في جانب الصين³، وعلى النقيض من ذلك، جاء في تقرير صادر سنة 2022 عن "المعهد الدولي للدراسات الاستراتيجية" التابع لجامعة بكين بعنوان "المنافسة الاستراتيجية بين الولايات المتحدة والصين في مجال التكنولوجيا" ووقع عليه "وانغ جيسي" أحد كبار الشخصيات في ميدان العلاقات الدولية أن المنافسة التكنولوجية بين الولايات المتحدة والصين وسياسات الفصل التكنولوجي ستضر بكلا الطرفين، إلا أنه في المرحلة الحالية ستكون خسارة الصين أكبر، كما أشار التقرير إلى أن الصين تعاني من نقاط ضعف شديدة في مجال تكنولوجيا المعلومات والفضاء والذكاء الاصطناعي، ويخلص التقرير إلى أن الصين قد تحقق السيطرة في بعض المجالات وتضيق الفجوة التكنولوجية، إلا أنها أمام معركة شاقة وطويلة لتجاوز الولايات المتحدة⁴، يُذكر أن التقرير قد تم سحبه من الموقع الرسمي لجامعة بكين في إشارة إلى تخوف الحكومة الصينية من استعمال مثل هذه التقارير المتشائمة لتقويض الخطاب التي تتبناه الحكومة داخلياً ونحو الخارج.

1 , The Guardian view on US-China chip wars: no winners in zero-sum battles, theguardian.com, April 2023, URL: <https://bit.ly/3PUYwaR>.

2 Jamie Gaida et al, The global race for future power, ASPI, Report N° 63, 2023, URL: <https://bit.ly/3ObBU4H>.

3 Valarie Tan, Winning the tech war with Chinese characteristics, merics.org, Jan 2022, URL: <https://bit.ly/3pLsu6E>.

4 يمكن الإطلاع على نسخة مؤرشفة من التقرير على الرابط: <https://bit.ly/44qeuy3>.

الفرع الثاني: مؤشرات الفوز بالمنافسة التكنولوجية

بناءً على ما تقدم، فتضارب الآراء والرؤى حول مستقبل الصراع التكنولوجي بين الولايات المتحدة والصين ناتج عن الغموض وعدم اليقين والتعتيم عن الإنجازات والخسائر لدى الطرفين، وعليه، يتم الإسترشاد في هذه الدراسة بمؤشرين يراهما الباحث مهمين ويمكن من خلالهما رسم سيناريوهات فوز طرف ما بالمنافسة والهيمنة على المستقبل، يتعلق المؤشر الأول بالفضاء السيبراني وهو الصراع حول صناعة الرقائق الفائقة، أما الثاني فيتعلق بالوضع الأمني الدولي وما ستؤول إليه الحرب في أوكرانيا.

أولاً، حرب الرقائق الفائقة كمؤشر مهم للفائز بالصراع التكنولوجي

تُعتبر صناعة الرقائق (أشباه الموصلات) صناعة تأسيسية، فهي تدخل في صناعة جميع الأجهزة الالكترونية الحديثة، لذلك فإن الضوابط الجديدة للتصدير وقانون الرقائق والعلوم الذي وقعه الرئيس "بايدن" في أكتوبر 2022 وضعت الرقائق المتطورة والآلات اللازمة لصناعتها والموهبة الأمريكية لاستخدامها بعيداً عن متناول الصين، وهذا ما جعل الوصول للتكنولوجيا الفائقة أو الحرمان منها يقع في قلب الجيوبوليتيك في المستقبل المنظور، وتكمن أهمية هذا المؤشر في أن قيمة ما تستورده الصين (مصنع العالم الأكبر) من الرقائق أكبر من قيمة واردات النفط الخام¹، إضافة إلى أن صراع الرقائق أجبر الصين -رغم ما تتميز به دبلوماسيتها من الرزانة والردود الهادئة- أخيراً على الرد بوضع ضوابط على تصدير معادن نادرة (الغاليوم والجرمانيم) أساسية لصناعة الرقائق، وعليه، فإنه من يفوز بصراع الرقائق ستزيد حظوظه للفوز بالصراع التكنولوجي.

على الجانب الأمريكي، يتوقف الفوز بصراع الرقائق على قدرة الشركات الأمريكية على الابتكار وإيجاد بدائل لفقدان السوق الصينية الكبيرة، إضافة إلى قدرة حلفاء الولايات المتحدة على تحمل تبعات سياسات الفصل التكنولوجي الأمريكية والخسائر التي تتكبدها شركاتهم، أما على الجانب الصيني، فإن قدرة الصين على تجاوز العجز في الرقائق الفائقة ونجاح شركاتها التكنولوجية في تطوير صناعة محلية للرقائق الفائقة هو مفتاح الفوز بالمنافسة.

ثانياً، الحرب في أوكرانيا.

تأخذ الحرب في أوكرانيا أهميتها في حسم الصراع التكنولوجي من أنها مثال حي لعودة صراع القوى العظمى، فالولايات المتحدة تعتبر كلاً من روسيا والصين خصماً جيوبوليتيكياً، والمنافسة

¹ إحصائيات واردات الصين من السلع الرئيسية لسنة 2022 على موقع Statista: <https://bit.ly/44KlaHb>.

الاستراتيجية بينها وبين روسيا جارية وآنية، أما مع الصين فهي طويلة الأمد، من جهة أخرى، تربط كلاً من الصين وروسيا شراكة استراتيجية، لذلك فالولايات المتحدة حاولت جمع تحالف دولي تحت قيادتها ضد روسيا، وقد نجحت في الدائرة الجيوبوليتيكية الأقرب المشكلة من حلفائها التقليديين خاصة في أوروبا، اليابان وأستراليا، لكنها فشلت في تجميع باقي دول العالم تحت قيادتها، لأن هذا التحالف يُعيد للولايات المتحدة سمعتها الدولية كقائد للنظام الدولي، ويضمن لها اختبار مدى فعالية "العقوبات الاقتصادية" التي إن نجحت في دحر روسيا عسكرياً واقتصادياً وتحديد الخصم الجيوبوليتيكي الآني، فإن تطبيقها ضد الصين سيكون بقوة وشدة أكبر.

وبناءً على ما تقدم، فإن هزيمة روسيا تحفز الدول القريبة من النهج الأمريكي والمتردة إلى اختيار الجانب الأمريكي والخضوع للهيمنة الأمريكية وهو ما ينعكس على الفضاء السيبراني من اعتماد معظم الدول للتكنولوجيا الأمريكية، ومن ثم يأتي الدور على الصين من مضاعفة حُرم العقوبات وانتقالها من عقوبات تكنولوجية إلى عقوبات اقتصادية وحصار سياسي يؤدي في النهاية إلى تدمير للاقتصاد الصيني، واضطرابات اجتماعية تزعزع الحزب الشيوعي، ومن الممكن حتى أن تُغير النظام السياسي ككل.

في المقابل، بقاء الوضع على ما هو عليه واستمرار حرب الإستنزاف يصب في فائدة الصين، حيث يمنحها الوقت لتجاوز العقوبات التكنولوجية الأمريكية ويُبقي الولايات المتحدة والغرب إلى حد ما منشغلين بالحرب في أوكرانيا، كما أن انتصار روسيا يمهّد ويعزز الشراكة الاستراتيجية بين موسكو وبكين، ويحفز دول العالم المترددة في الاختيار بين التكنولوجيا الصينية والأمريكية لاختيار الصين.

الفرع الثالث: سيناريو...عندما تحكم الصين الفضاء السيبراني

إذا نجحت الصين في التغلب على الفجوة التكنولوجية وطورت رقائق فائقة محلياً فإن هذا النجاح يطلق موجة ابتكارات للتكنولوجيات الأساسية والتحويلية، وتصبح المختبرات والجامعات والشركات الصينية أول من يُعلن عن الابتكارات والاخترقات العلمية الجديدة وأول من يحولها إلى تكنولوجيا ذات قيمة اقتصادية، وعلى المستوى السياسي، تتحكم الصين بحكنة شديدة في التصعيد الجيوبوليتيكي بينها وبين الغرب خاصة فيما يتعلق بالقضايا الإقليمية مثل: تايوان، وتتجنب قدر الإمكان الدخول في حرب مباشرة مع القوى العظمى، وتعزز من الدبلوماسية الذكية والهادئة في مواجهة الإستفزازات الأمريكية، تسرع الصين نشر التقنيات الحديثة في أرجاء العالم، في آسيا، الشرق الأوسط، إفريقيا وأمريكا اللاتينية، كما تزيد الصين الضغط على حلفاء الولايات

المتحدة (الاتحاد الأوروبي، كندا، اليابان، أستراليا وغيرها) وتضعها بين خيارين إما التفاوض على استخدام التقنيات الصينية أو البقاء خلف الصين وبقية دول العالم.

تُشكل الصين القواعد والمعايير العالمية التي تُدير وتحكم الفضاء السيبراني، ويختفي الأنترنت المفتوح غير المنضبط لصالح النموذج الصيني المبني على تحكم الدول في المعلومات والمراقبة الشاملة، حيث يصبح الأنترنت أقل أمركة وأكثر صيننة.

من جهة أخرى، فإن استمرار الحرب في أوكرانيا أو حسم روسيا لهذه الحرب لصالحها يُعطي للصين الوقت والزخم اللازمين لتجاوز مشكلة الرقائق الفائقة، ويزيد من فرصها للنجاح وإعادة تشكيل الفضاء الإلكتروني وفق نموذجها الخاص، ويُصبح جزء كبير من الفضاء السيبراني يعمل على تشغيل التطبيقات والبرامج الصينية على أجهزة صينية الصنع، ومحصلة كل هذا، أن بكين ستجني فوائد الفضاء السيبراني الاقتصادية، الدبلوماسية، الأمنية والاستخباراتية التي تدفقت ذات مرة إلى واشنطن.

الفرع الرابع: سيناريو...محافظة الولايات المتحدة على الريادة وتراجع الصين

إن استعادة الولايات المتحدة لزخم الابتكار والإبداع وجذب المواهب والهيمنة على صناعة الرقائق الفائقة يضمن لها ريادة التصنيع التكنولوجي المستقبلي والاستئثار بمزايا التقنيات التأسيسية المستقبلية والفوز بالفوائد الاقتصادية والأمنية والسياسية، وهذا ما تخطط له الولايات المتحدة من خلال ضوابط التصدير وقانون الرقائق والعلوم 2022 لجعل الفجوة التكنولوجية ثابتة بينها وبين الصين، أي أنه يجب على الصين أن تبقى دائماً متأخرة تكنولوجياً عن الولايات المتحدة على الأقل بعقد من الزمن.

وعليه، فإن هيمنة الولايات المتحدة على الفضاء السيبراني يرتبط ارتباطاً وثيقاً بنجاح سياساتها المتعلقة بالرقائق من جهة، ومن جهة أخرى بالانتصار على روسيا في حربها ضد أوكرانيا، حيث يُصبح المشهد العالمي شبيهاً بالمشهد بعد نهاية الحرب العالمية الثانية، إلا أنه توجد قوة عظمى وحيدة هي الولايات المتحدة، تستفيد من هيمنتها التكنولوجية سياسياً وأمنياً لقيادة دول العالم وتشكيل قواعد ومعايير النظام الدولي الجديد، واقتصادياً في إعادة بناء الاقتصاد العالمي لمصلحتها من خلال إعادة بناء أوكرانيا المدمرة، وأوروبا المستنزفة، روسيا والصين المنهزمتين.

خلاصة الفصل

قدم الفصل الأخير من الدراسة رؤية استشرافية لمآلات صراع الهيمنة في الفضاء السيبراني بين الولايات المتحدة والصين، ففي سيناريو ضبط الصراع (التفاؤلي) يتطور الصراع على المدى المتوسط إلى حالات متعددة ليفضي إلى إقرار صيني بالهيمنة الأمريكية أو إلى توازن للقوى بين الطرفين أو إلى دخول الاتحاد الأوروبي كطرف ثالث يجعل اللعبة الرقمية ثلاثية، وفي هذه الحالات الثلاث يُضطر الطرفان إلى التفاوض وإبرام المعاهدات والاتفاقيات الثنائية والمتعددة الأطراف والالتزام بالقواعد والمعايير ليُصبح الفضاء السيبراني أكثر استقراراً ومكاناً للتعايش السلمي والمنافسة الحميدة.

أما سيناريو استمرار الصراع (الخطي)، وهو السيناريو الأكثر ترجيحاً، فإنه يتمحور حول استمرار الصراع وزيادة حدته استجابة لمجموعة من الدوافع المتعلقة بالصراع التكنولوجي والإيديولوجي واختلاف الأجندات السياسية العالمية للطرفين، ومن ثم يتحول إلى حرب باردة جديدة شاملة تتمحور حول حرب باردة رقمية تأججها المحددات الجيوبولتيكية لصناعة أشباه الموصلات.

وأخيراً سيناريو التغيير (الراديكالي)، وفي هذا السيناريو يتفكك الفضاء السيبراني إلى كتل سيبرانية جيوبولتيكية تمثل الكتلتين الأمريكية والصينية أكبرهما، هذا الانقسام يعزز العداء بين الطرفين ويزيد من احتمالية نشوب حرب سيبرانية شاملة تستخدم أحدث التقنيات السيبرانية، مع إمكانية انتصار أحد الطرفين (الولايات المتحدة أو الصين) وفرض رؤيته ومقاربتة وهيمنته على الفضاء السيبراني المستقبلي.

الخاتمة

اهتم موضوع بحثنا بإخضاع ظاهرة صراع الهيمنة بين الولايات المتحدة الأمريكية والصين في الفضاء السيبراني إلى دراسة وفق المقاربات الجيوبوليتيكية لاستراتيجيات كلا البلدين وقدم رؤية استشرافية لمآلات هذا الصراع، فمن خلال تفكيك إشكالية الدراسة والبحث في العلاقة بين متغيراتها واختبار فروضها العلمية، أبرزت الدراسة ملاءمة المقاربات الجيوبوليتيكية لدراسة ظواهر الفضاء السيبراني، حيث تم تأكيد أنه وفقاً للجيوبوليتيكا فإن الاستراتيجيات الأمريكية في الفضاء السيبراني تنتهي إلى تحقيق الهيمنة وكبح صعود الصين ومن ثم دمجها في نظام دولي تقوده الولايات المتحدة الأمريكية، في مقابل الاستراتيجيات الصينية التي تنتهي إلى جعل الصين نموذجاً سيبرانياً مركزياً في عصر الابتكار الصيني.

وقد تمخض النقاش حول قدرة المقاربات الجيوبوليتيكية وملاءمتها لتحليل الظواهر في الفضاء السيبراني عن مجموعة نتائج نلخصها فيما يلي:

1. تُعتبر الجيوبوليتيكا بتشكيلاتها النظرية المتعددة ومفاهيمها المتنوعة منظومة تفسيرية رائدة تقرض ثبوتيتها في تفسير الماضي وفعاليتها في تنظيم الحاضر وتصميم آفاق المستقبل، كما تعتبر الأداة الأكثر أهمية كمنهج تحليل يسمح بتطوير الاستراتيجية الأقوى تأثيراً في السياسة الدولية.
2. تطور منهج التحليل الجيوبوليتيكي من الحتمية الجغرافية، إلى التركيز على علاقات القوة بشتى تمثالاتها و جوانبها وتقصي الكيفية التي يساهم بها المجال/الفضاء في تحديد وتوجيه تفاعلات القوة بين مختلف الفاعلين، لذلك فإن بناء ونجاح الاستراتيجيات الكبرى للدول يعتمد على قدرتها في وضع المبادئ الجيوبوليتيكية الملائمة لوضعها في النظام الدولي.
3. الفضاء السيبراني هو فضاء تتفاعل فيه الآلات والبشر والبيانات سمته المميّزة هي الفوضى، كما أنه أنتج نوعاً جديداً من القوة هي القوة السيبرانية والتي تتمحور حول امتلاك القدرة على السيطرة والتأثير في التفاعلات التي تحدث في هذا الفضاء، وبدورها خلقت نوعاً جديداً من الصراع في/على الفضاء السيبراني غايته الانفراد بالموارد والميزات التي يتيحها الفضاء السيبراني على حساب الطرف أو الأطراف الأخرى.

4. تقدم هندسة الطبقات في الفضاء السيبراني رؤية واضحة لمجموعة متباينة من الفاعلين، القضايا، التفاعلات والصراعات حول النفوذ والسيطرة والتحكم في كل طبقة، وإذا كانت الطبقة المادية يبدو فيها تأثير الجغرافيا واضحاً فإن باقي الطبقات يتم فيها الاستعانة بالجغرافيا الماورائية أو ظاهرة تخيل المكان ليُصبح الفضاء السيبراني مشكلاً من مجموعة من الأقاليم غير الحصرية المتداخلة والمتقاطعة، يتم باستمرار إعادة التفاوض على أشكالها (حدودها) وخصائصها (من يُسيطر عليها)، وعليه، فالجيوبوليتيك تُقدم فهوماً مميزة حول تكوين الفضاء السيبراني، الصراعات التي تحدث فيه، من يحكمه وإلام ستؤول الصراعات فيه.
5. أصبح الفضاء السيبراني ظاهرة أمنية متعددة للحدود القومية، تتفاقم فيه المعضلة الأمنية، ويزداد الجدل حول السيادة السيبرانية، وهذا ما جعل الصراع حول هذه القضايا يتعدى المستوى الأكاديمي والتقني ليصبح انعكاساً للصراع الجيوبوليتيكي العالمي بين القوى الكبرى المتنافسة خاصة الولايات المتحدة والصين، ويُفسر سعيها للتعديل المستمر لاستراتيجيات الأمن القومي وتطويرها لاستراتيجيات خاصة بالفضاء السيبراني.
- أما ما يتعلق بمظاهر وتجليات الصراع الأمريكي الصيني في الفضاء السيبراني فقد أبرزت الدراسة وأظهرت تجليات الصراع في كل طبقة من طبقات الفضاء السيبراني كما يلي:
6. إن امتلاك القوة السيبرانية وزيادة وتضخيم القدرات في الفضاء السيبراني مع تطبيقها في المنطقة الرمادية للعمليات (Gray Zone Operations) يُمكن أن يحدث تأثيراً بالغاً بالتوازنات الثنائية والإقليمية والدولية، لذلك فالولايات المتحدة الأمريكية تتصدر قائمة الدول الأقوى في الفضاء السيبراني تليها الصين التي تنمو قدراتها السيبرانية بسرعة والفجوة بين البلدين تتقلص.
7. بالاعتماد على هندسة الطبقات للفضاء السيبراني فإننا نرصد تنافساً حاداً بين الولايات المتحدة الأمريكية والصين، حيث تحدث في كل طبقة صراعات جيوبوليتيكية بين الدولتين حول النفوذ والسيطرة، يحدث هذا الصراع عبر كل طبقات الفضاء السيبراني وحول كل القضايا المتعلقة به: الجيل الخامس، الكوابل البحرية، الرقائق، حوكمة الأنترنت، برامج التشغيل والتطبيقات، البيانات، الحوسبة، الذكاء الاصطناعي، ولعل المثال الأبرز على تأثير الجيوبوليتيكا على الصراع بين البلدين هو: قضية تايوان والصراع حول أشباه الموصلات.

8. تطورت العلاقة بين الولايات المتحدة والصين من الشراكة والتعاون، إلى عدم اليقين، إلى المنافسة الاستراتيجية كنتيجة حتمية للصراع في الفضاء السيبراني، والذي أثر بشدة على ديناميكية العلاقات بين البلدين وساهم في خلق تحالفات أمنية وتكنولوجية جديدة كما أثر على توازنات القوى في النظام الدولي.

وعند تطبيق منهج التحليل الجيوبولتيكي في تحليل بناء كل من الولايات المتحدة والصين لاستراتيجياتهما في الفضاء السيبراني، أفرزت الدراسة النتائج التالية:

9. أصبحت شركات التكنولوجيا تمتلك قوة ووزناً سياسياً وجيوبولتيكاً مؤثراً على الساحة الدولية، وأصبحت مفتاحاً لفهم واستيعاب صراع الهيمنة في الفضاء السيبراني، كما لا تزال مجالات النفوذ سمة غالبية على التفكير الاستراتيجي للولايات المتحدة والصين، وتظهر جلية في المقابلة الجيوبولتيكية بين مشروع طريق الحرير الرقمي الصيني ومشروع البنية التحتية العالمية الرقمية الذي قدمته الولايات المتحدة وحلفاؤها، لذلك فالصراع بين القوى العظمى في الفضاء السيبراني عبارة عن مزيج من المفاهيم الجيوبولتيكية التقليدية والخصائص الجديدة للفضاء السيبراني (اللعبة الجيوبولتيكية الرقمية).

10. اللوحة الجيوبولتيكية الراهنة تشهد صراع قوتين عظميين في الفضاء السيبراني، الولايات المتحدة القوة المخترعة والمهيمنة والصين القوة الصاعدة المتحدية.

11. "الهيمنة في الفضاء السيبراني" هي المبدأ الجيوبولتيكي الذي تدير وفقه الولايات المتحدة في تفاعلاتها الدولية، لذلك فهي ترى أن واجبها الجيوبولتيكي الأساسي هو منع منافستها التكنولوجي من إزاحتها من موقعها القيادي العالمي.

12. يساهم مزيج من العقيدة الدينية (الطهورية) وأفكار عصر النهضة (الحرية، الفردانية، البراغمية) والمصالح الاقتصادية السياسية والأمنية في الفضاء السيبراني في تشكيل المدرك الاستراتيجي لصانع القرار الأمريكي، كما تعمل المبادئ الجيوبولتيكية العالمية للولايات المتحدة كإطار عام يضبط أهداف الاستراتيجيات المختلفة لزيادة النفوذ وبسط السيطرة والحفاظ على الريادة في الفضاء السيبراني.

13. المبادئ الجيوبولتيكية الصينية هي مزيج من الموروث الفكري والحضاري الصيني المتمحور حول "المركزية الصينية" والمبادئ والتوجهات التي يقرها قادة الحزب الشيوعي الصيني الحاكم،

ولابد من الإشارة إلى التحول الذي حدث في كيفية بناء الاستراتيجيات المختلفة مع بداية القرن الحالي إذ أصبح الفضاء السيبراني المصلحة الأكثر أهمية.

14. يعتمد الفهم الصحيح لمحركات السلوك الصيني والسياسات المتبعة في الفضاء السيبراني على فهم المصالح الاستراتيجية للصين في هذا الفضاء والتي عبر عنها الرئيس "شي" بجعل الأولوية القصوى للمجال السيبراني كمبادرة استراتيجية كبرى لها تأثيرات سياسية (الحفاظ على نظام الحكم)، اقتصادية (الدفع بالنمو الاقتصادي نحو قيادة العالم) وعسكرية (بلوغ مستوى الجيوش العظمى منافستها والتغلب عليها).

15. تُعد استراتيجية "الصين الرقمية" أحدث استراتيجيات الصين في الفضاء الرقمي، يعتبرها الحزب الشيوعي المحرك الأساس لبلوغ التحديث ذو النمط الصيني والتجديد العظيم للأمة الصينية (المركزية الصينية)، ويعتبرها "الغرب" استراتيجية عالمية كبرى تُصَبِّغُ عليها جذورها الماركسية طليعةً تنافسية تحويلية، حيث تحاول تقديم أول نموذج ناجح من الاشتراكية طيلة صراعها مع الرأسمالية، أو بلغة الجيوبوليتيكا التيلوروكراتيا ضد التالاسوكراتيا.

16. تسعى السياسات والمشاريع والمبادرات الصينية المتعلقة بالتكنولوجيا للهيمنة على الفضاء السيبراني وفق ثلاث خطوط متوازية، أولاً، تطوير سريع للتكنولوجيا الرقمية المحلية (استراتيجية صنع في الصين 2025)، ثانياً، السعي إلى نشر التكنولوجيا الصينية بكثافة في الخارج (طريق الحرير الرقمي)، ثالثاً، توفير حماية عسكرية موثوقة لما يرافقها وما ينتج عنها اقتصادياً، سياسياً، عسكرياً ومجتمعياً (الاندماج المدني-العسكري).

وقدّمت دراسة رؤية مستقبلية لما سيؤول إليه الصراع من خلال تحليل المعطيات والمؤشرات الحالية والمحتملة لتتوصل إلى بناء السيناريوهات والنتائج التالية:

السيناريو التفاؤلي ويتم فيه ضبط الصراع واستقرار الفضاء السيبراني، وهو سيناريو محتمل على المدى المتوسط إلى البعيد، ويتم ذلك من خلال:

17. تحول التكنولوجيا إلى تهديد عالمي (خاصة الذكاء الاصطناعي) يساهم في الضغط على الولايات المتحدة والصين لتطوير المعايير والقواعد النازمة للفضاء السيبراني والالتزام بها.

18. إن صعود الاتحاد الأوروبي كطرف ثالث في اللعبة الرقمية و/أو تزايد تكلفة الصراع يُلجئ البلدين إلى التفاوض وإبرام اتفاقيات ثنائية ومتعددة الأطراف لتطوير القواعد والمعايير الضابطة للفضاء السيبراني وجعله أكثر استقراراً.

19. سيناريو التعايش السلمي في نسخته الثانية يرتبط ببروز القوى التعاونية في كلا البلدين وتغليب المصالح الاقتصادية على المخاوف الجيوبوليتيكية من خلال إنشاء وتفعيل قنوات للحوار والتواصل حول القضايا الخلافية وتعزيز آليات التعاون في القضايا ذات الاهتمام العالمي.

السيناريو الخطي ويستمر فيه الصراع في شكل حرب باردة رقمية، وهو سيناريو محتمل جداً على المدى القصير والمتوسط، ويتم ذلك من خلال:

20. يستمر صراع الهيمنة بين الولايات المتحدة والصين مدفوعاً بالصراع حول التفوق التكنولوجي والحسابات الجيوبوليتيكية بدرجة أولى مع تأثير للاختلافات الإيديولوجية والإدراكات المتبادلة المشوّهة للطرفين وتباين الأجندات السياسية العالمية.

21. نهاية عالم مابعد الحرب الباردة وبداية تشكل عالم الحرب الباردة الجديدة التي تتمحور حول حرب باردة رقمية ذات أساس تكنولوجي تتحكم في مصيرها جيوبوليتيكا صناعة أشباه الموصلات.

السيناريو التحولي أو الراديكالي ويتغير فيه شكل الصراع حيث ينتهي إلى تفكك الفضاء السيبراني أو حرب سيبرانية شاملة أو هيمنة أحد طرفي الصراع، وهذا السيناريو احتمالية حدوثه متوسطة إلى ضعيفة على المدى المتوسط والبعيد، وذلك من خلال:

22. تفكك الفضاء السيبراني إلى كتل جيوبوليتيكية سيبرانية أكبرها الفضاء السيبراني الأمريكي والفضاء السيبراني الصيني مع وجود مناطق للصدام، تدفع بهذا الاتجاه مجموعة عوامل أمنية (تجسس، هجومات سيبرانية، تخريب..)، عوامل اقتصادية (هيمنة على الأسواق)، عوامل سياسية (رؤى متضاربة حول حوكمة الفضاء السيبراني).

23. تحفز مجموعة من العوامل (خصائص الفضاء السيبراني، تآكل الثقة الاستراتيجية، مخاطر الذكاء الاصطناعي غير المقيد) على انخراط البلدين في حرب سيبرانية مدمرة تسبق وترافق

اشتباكات مادية بين القوتين، رغم أن احتمال حدوث هذا السيناريو ضئيل لكنه وارد استثناساً برأي كيسنجر الذي يعتقد أن الوضع الدولي اليوم (المنافسة الاستراتيجية بين الولايات المتحدة والصين) أشبه بالوضع الدولي قبيل العام 1914 أكثر منه بعد العام 1945.

24. تتوقف هيمنة الولايات المتحدة الأمريكية في/على الفضاء السيبراني على عودة عجلة الابتكار الأمريكية للدوران مع كبج الصعود التكنولوجي الصيني وتحييد/اضعاف الطرف الروسي.

25. إن نجاح الصين في تحقيق اختراقات علمية (خاصة في صناعة الرقائق الفائقة) يضمن لها مواصلة تحدي الهيمنة الأمريكية، ويفتح للصين آفاقاً جديدة لبلوغ الهيمنة الصينية في/على الفضاء السيبراني.

على ضوء هذه النتائج والإثباتات، تخلص الدراسة في النهاية إلى تأكيد أن كلاً من الولايات المتحدة الأمريكية والصين في الوقت الراهن على قناعة بأن المعادلة الجيوبولتيكية الأشد تأثيراً في صراعهما في الفضاء السيبراني هي:

من يُسيطر على صناعة الرقائق يُسيطر على الفضاء السيبراني

ومن يُسيطر على الفضاء السيبراني يُسيطر على العالم (اقتصادياً وعسكرياً).

قائمة المصادر والمراجع

المراجع:

1. باللغة العربية:

الكتب:

1. أحمد الورداني، أيمن، حق الشعب في استرداد السيادة، القاهرة: مكتبة مدبولي، 2008.
2. البديوي، عادل، الإدراك الاستراتيجي للولايات المتحدة الأمريكية: دراسة في المبادئ الجيوبوليتيكية، عمان: دار الجنان للنشر والتوزيع، 2015.
3. بدران، عباس، الحروب الالكترونية: الاشتباك في عالم متغير، بيروت: مركز دراسات الحكومة الالكترونية، 2010.
4. بريجينسكي، زيبغنيو، رقعة الشطرنج الكبرى: الأولوية الأمريكية و متطلباتها الجيوستراتيجية، ترجمة: أمل الشرقي، عمان: الأهلية للنشر والتوزيع، 1999.
5. تيلور، بيتر، كولن فلنت، الجغرافيا السياسية لعالمنا المعاصر (الاقتصاد العالمي، الدولة القومية، المحليات)، تر: عبد السلام رضوان واسحق عبيد، الكويت: مطابع السياسة، 2002.
6. حمه خورشيد، فؤاد، الجيوبوليتيك المعاصر تحليل، منهج، سلوك، مؤسسة هنداوي للتعليم والثقافة، 2013.
7. خليفة، إيهاب، الحرب السيبرانية: الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، القاهرة: العربي للنشر والتوزيع، 2021.
8. دودز، كلاوس، ديفيد أتكينسون، الجغرافيا السياسية في مائة عام (التطور الجيوبوليتيكي العالمي)، ج1، تر: عاطف معتمد، عزت زيان، المركز القومي للترجمة، العدد 1592، 2010.
9. دوغين، ألكسندر، أسس الجيوبوليتيكا، مستقبل روسيا الجيوبوليتيكي. تر: عماد حاتم، بيروت: دار الكتاب الجديد المتحدة، 2004.
10. ديسوا، جيرار، دراسة في العلاقات الدولية، الجزء الأول: النظريات الجيوسياسية، تر: قاسم المقداد، دمشق: دار نينوى للدراسات والنشر والتوزيع، 2014.

11. رياض، محمد، الأصول العامة في الجغرافيا السياسية والجيوبوليتيكا، القاهرة: مؤسسة هنداوي للتعليم والثقافة، 2014.
12. شيلينغ، توماس، استراتيجية الصراع، تر: نزهت طيب وأكرم حمدان، بيروت: الدار العربية للعلوم ناشرون، 2010.
13. صبري مقلد، إسماعيل، العلاقات السياسية الدولية: النظرية والواقع، الجيزة: المكتبة الأكاديمية، 2011.
14. صبري مقلد، إسماعيل، العلاقات السياسية الدولية: دراسة في الأصول والنظريات، الجيزة: المكتبة الأكاديمية، 1991.
15. علي أحمد، هارون، أسس الجغرافيا السياسية، القاهرة: دار الفكر العربي، 1998.
16. فهمي، عبد القادر محمد، الفكر السياسي والاستراتيجي للولايات المتحدة الأمريكية: دراسة في الأفكار والعقائد ووسائل البناء الإمبراطوري، عمان: دار الشروق، 2009.
17. فهمي، عبد القادر محمد، المدخل إلى دراسة الاستراتيجية، ط2، عمان: دار المجدل لوي للنشر والتوزيع، 2013.
18. فوكوياما، فرانسيس، نهاية التاريخ وخاتم البشر، تر: حسين أحمد أمين، القاهرة: مركز الاهرام للترجمة والنشر، 1993.
19. لامبرت، فرانك، الدين في السياسة الأمريكية: تاريخ موجز، تر: عبد اللطيف أبو البصل الرياض: نمور للنشر، 2015.
20. ميرشايمر، جون ، مأساة القوى العظمى، تر: مصطفى محمد قاسم، الرياض: النشر العلمي والمطابع، 2012.
21. نعمة كاظم، هاشم، العلاقات الدولية، ج1، بغداد: مطبعة إياد، 1979.
22. نوح، فلدمان، الحرب الهادئة مستقبل التنافس العالمي، تر: هشام سمير، الخبر: الدار العربية للطباعة والنشر، 2016.
23. هنتنغتون، صمويل، صدام الحضارات إعادة صنع النظام العالمي، تر: طلعت الشايب، ط2،، 1999.

24. وهبان أحمد، محمد، تحليل إدارة الصراع الدولي "دراسة مسحية"، سلسلة إصدارات الجمعية السعودية للعلوم السياسية 14، جامعة الملك سعود، 2014.

المقالات:

1. لغوتسكا، أغنيتشكا، الجيوبوليتيك الجديدة: ما الجديد فعليا في هذا الحقل؟، تر: جلال خشيب، مركز إدراك للدراسات والاستشارات، 2018، ص 3.

التقارير

1. سميت، سفين وآخرون، حماية قدرة أوروبا التنافسية: التصدي للفجوة التكنولوجية، معهد ماكنزي، سبتمبر 2022.

2. سي جومبرت، ديفيد وآخرون، الحرب ضد الصين: التفكير فيما لا يتقبله العقل، كاليفورنيا: مؤسسة راند، 2016.

مواقع الأنترنت:

1. رويترز، بايدن يقول الصين ستهزمنا ما لم نتحرك والرئيس الصيني يحذر من مواجهة ستكون "كارثة"، موقع رويترز، فيفري 2021، على الرابط: <https://reut.rs/3CqdYVZ>.

2. موسوعة Britannica الموقع على الأنترنت: <https://bit.ly/3qB7S1t>.

3. نبذة عن الاتحاد الدولي للاتصالات ITU على الموقع الرسمي: <https://bit.ly/3skQ8b8>.

2. باللغات الأجنبية:

1.2. باللغة الإنجليزية:

Books:

1. Allison, Graham, **Destined for War: Can America and China Escape Thucydides's Trap?**, Harvard Kennedy School, 2017.
2. Amy, Chang, **Warring State China's Cybersecurity Strategy**, December 2014.
3. Blount, Percy Judkins, **Reprogramming the world: cyberspace and the geography of global order**, E-International Relations publishing, Bristol, England, 2016.

4. Choucri, Nazli, **Cyberpolitics in international relations**, MIT press, 2012.
5. Colin, Flint, **Introduction to geopolitics**, Routledge, 2006.
6. Fang, Binxing, Fang Zhang, **Cyberspace sovereignty**, Springer Singapore, 2018.
7. Gaddis, John Lewis, **Strategies of containment: a critical appraisal of American national security policy during the Cold War**, Oxford University Press, 2005.
8. GRAY, Colin S, **The strategy bridge: theory for practice**, Oxford: Oxford University Press, 2010.
9. GRAY, Colin S, **The future of strategy**, John Wiley & Sons, 2015.
10. Harvey, David, **Time-space compression and the postmodern**, Modernity: After Modernity, 1999
11. Kissinger, Henri A, **The White House Years**, Boston: Little Brown, 1979
12. Kissinger, Henry A, Eric Schmidt, Daniel Huttenlocher, **The Age of AI and Our Humain Future**, John Murray Press, London, 2021.
13. Krasner, Stephen D, **Sovereignty**, Princeton University Press, 1999.
14. Li, Zhengmao, Xiaoyun Wang, and Tongxu Zhang, **5G+: How 5G change the society**, Springer Nature, 2020.
15. McKenzie, Timothy M, **Is Cyber Deterrence Possible?**, Air University Press, 2017.
16. Modelski, George, **Long cycles in world politics**, Springer, 1987.
17. Morgan, Patrick M, **Deterrence now**, Cambridge University Press, 2003.
18. Murray, Michelle, **The Struggle for Recognition in International Relations: Status, Revisionism, and Rising Powers**, Oxford University Press, 2019.
19. Ning, An, **Confucian Geopolitics**. Springer Singapore, 2020.
20. Nye Jr, Joseph S, **Cyber power**, Harvard Univ Cambridge MA Belfer Center for Science and International Affairs, 2010.

21. Nye Jr, Joseph S, **The future of power**, Public Affairs, 2011.
22. Organski, Abramo Fimo Kenneth, **World Politics**, Knopf, New York, 1968.
23. Palladino, Nicola, Mauro Santaniello, **Legitimacy, Power, and Inequalities in the Multistakeholder Internet Governance: Analyzing IANA Transition**, Springer Nature, 2020.
24. Richard, Clarke & Knake Robert, **Cyber war: The next threat to national security and what to do about it**, Haper Collins, 2010.
25. Rid, Thomas, **Cyber war will not take place**, Oxford University Press, USA, 2013.
26. Rosenbach, Eric, and Katherine Mansted, **The geopolitics of information**, Belfer Center for Science and International Affairs, 2019.
27. Schmitt, Carl, **The nomos of the earth**, Trans: GL Ulmen, Telos Press, New York, 2003.
28. Tianliang, Xiao & all, **Science of Military Strategy (2020)**, Traduction in English: China Aerospace Studies Institute, National Defense University Press, Beijing, 2020.
29. Valeriano, Brandon, Ryan C. Maness, **Cyber war versus cyber realities: Cyber conflict in the international system**, Oxford University Press, 2015.
30. Wallensteen, Peter, **Understanding conflict resolution**, Sage, 2018.
31. Waltz, Kenneth, **Man, the state, and war**, Columbia University Press, 2018.
32. Wiener, Norbert, **Cybernetics or Control and Communication in the Animal and the Machine**, MIT press, 2019
33. Xiaosong, Shou & all, **Science of Military Strategy (2020)**, Traduction in English: China Aerospace Studies Institute, Academy of Military Science, Beijing: Military Science Press, 2013.

Chapter in Book:

1. Angang, Hu, Men Honghua, **The rising of modern China: Comprehensive national power and grand strategy**, In: international conference of the Korea Institute of International Economic Policy (KIEP), Seoul, 2004.
2. Parzyan, Anahit, **China's Digital Silk Road: Empowering capabilities for digital leadership in Eurasia**, In: China and Eurasian Powers in a Multipolar World Order 2.0, Routledge, 2023.

Articles:

1. Allison, Graham, “The new spheres of influence: sharing the globe with other great powers”, **Foreign Affaires**, 99, 2020, p 30.
2. Arquilla, John & David Ronfeldt, “Cyberwar is coming!”, **Comparative Strategy**, Vol 12, N°2, 1993, pages 141-165.
3. Benson, David, “Not Cyberwar, but Cyberbalance”, **Æther: A Journal of Strategic Airpower & Spacepower**, Vol 1, N° 2, 2022.
4. Black, Michelle, Lana Obradovic, “Multi-Actor deterrence defining the concept”, **Æther: A Journal of Strategic Airpower & Spacepower**, Vol 1, N° 2, 2022, pp69–80.
5. Bull, Hedley, “Kissinger: The Primacy of Geopolitics”, **International Affairs (Royal Institute of International Affairs 1944)**, Vol 56, No 3, 1980, pp 484-487.
6. Chawki, Mohamed, “Anonymity in cyberspace: Finding the balance between privacy and security”, **International Journal of Technology Transfer and Commercialisation**, Vol 9 Issue 3, 2010, pp 183-199.
7. Cohen, Raymond, “Threat perception in international crisis”, **Political Science Quarterly**, Vol 93, N° 1, 1978.

8. Couture, Stéphane, Sophie Toupin, “What Does the Concept of ' Sovereignty' Mean in Digital, Network and Technological Sovereignty?”, **GigaNet: Global Internet Governance Academic Network, Annual Symposium**, 2017.
9. Degterev, D. A., M. S. Ramich, D. A. Piskunov, “US—China approaches to global Internet governance: “New bipolarity” in terms of “the network society””, **International Organisations Research Journal** , Vol 16 Issue 3 , 2021, pp 7-33.
10. Deibert, Ronald, “Cybersecurity: the new frontier”, **Foreign Policy**, 2012, pp 45-58.
11. Dixit, Saurabh, “Military-Civil Fusion in China and lessons for India”, **SYNERGY**, Vol 2, Issue 1, February 2023, pp 88-105.
12. Dorman, David & John Hemmings, “Digital China The Strategy and Its Geopolitical Implications”, **Pacific Forum International, Issues & Insights**, Vol 23, Wp 2, Feb 2023.
13. Ducheine, Paul AL, Peter BMJ Pijpers, “The notion of cyber operations”, **Research Handbook on International Law and Cyberspace**, Edward Elgar Publishing, 2021.
14. Egan, Brian J, “International Law and Stability in Cyberspace”, **Berkeley Journal of International Law**, Vol 35, Issue 1, 2017, pp 169-180.
15. Ensafi, Roya, et al, “Analyzing the Great Firewall of China Over Space and Time”, **Proceedings on Privacy Enhancing Technologies**, Vol 1, 2015, pp 61-76.
16. Ferdinand, Peter, “Westward ho—the China dream and ‘one belt, one road’: Chinese foreign policy under Xi Jinping”, **International Affairs**, Vol 92, Issue 4, July 2016, Pages 941–957.

- 17.Gartzke, Erik, Jon Lindsay, and Michael Nacht, “Cross-Domain Deterrence: Strategy in an Era of Complexity”, **International Studies Association Annual Meeting**, Toronto, 2014.
- 18.Gearóid Ó Tuathail, “Understanding critical geopolitics: Geopolitics and risk society”, **Journal of Strategic Studies**, Vol 22, N° 2, 1999.
- 19.Granåsen, Dennis, Margarita Jaitner, “The Offensive Cyber Operations Playbook”, **18th European Conference on Cyber Warfare and Security (ECCWA 2019)**, University of Coimbra, Portugal, 2019.
- 20.Greathouse, Craig B, “Cyber war and strategic thought: Do the classic theorists still matter?”, **Cyberspace and International Relations**, Springer, Berlin, Heidelberg, 2014, pp 21-40.
- 21.Hansen, Lene, Helen Nissenbaum, “Digital disaster, cyber security, and the Copenhagen School”, **International studies quarterly**, Vol 53, N°4 , 2009, pp1155-1175.
- 22.Harknett, Richard J & Joseph S Nye Jr, “Is Deterrence Possible in Cyberspace?”, **International Security**, Vol 42, N° 2 ,2017, pp196-199.
- 23.Hepple, Leslie W, “The revival of geopolitics”, **Political Geography Quarterly**, Vol 5, N° 4, 1986, pp S22-S23.
- 24.Herz, John H, “Idealist internationalism and the security dilemma”, **World politics**, Vol 2, N° 2, 1950, pp 157-180.
25. Holsti, Kalevi J, “National role conceptions in the study of foreign policy”, **International studies quarterly**, Vol 14, N°3,1970, pp 233-309.
- 26.Jishe, Fan, “Managing China–US “strategic competition”: potential risks and possible approaches”, **China International Strategy Review**, Vol 3, Issue 2, 2021, pp 234-247.
- 27.Johnson, David R, David Post, “Law and borders: The rise of law in cyberspace”, **stanford law review**, Vol 48, N° 5 ,1996, pp 1367-1402.

- 28.Keohane, Robert O & Joseph S Nye Jr, “Power and interdependence in the information age”, **Foreign Affairs**, Vol 77, N° 5,1998, pp 81-94.
- 29.Kerr, Orin S, “Internet surveillance law after the USA Patriot Act: The big brother that isn't”, **SSRN Electronic Journal**, Vol 97 No 2, 2002, pp 607-674.
- 30.Kleinwächter, Wolfgang, “Cybersecurity, Internet Governance, and the Multistakeholder Approach”, **New Conditions and Constellations in Cyber** , 2021, pp 41-58.
- 31.Lambach, Daniel, “The territorialization of cyberspace”, **International Studies Review**, Vol 22, N°3, 2020, pp 482-506.
- 32.Liff, Adam P, “China and the US alliance system”, **The China Quarterly**, vol 233, 2018, pp 137-165.
- 33.Lin, Herbert, “Cyber conflict and international humanitarian law”, **International Review of the Red Cross**, Vol 94, N° 886 ,2012, pp 515-531.
- 34.Liu, Adam, et al, “Unpacking “the West”: Divergence and Asymmetry in Chinese Public Attitudes Towards Europe and the United States”, **Journal of Current Chinese Affairs**, Vol 52, Issue 1, 2023, pp 119–133.
- 35.Luo, Y, Van Assche A, “The rise of techno-geopolitical uncertainty: Implications of the United States CHIPS and Science Act”, **Journal of International Business Studies**, Vol 18, issue 01, 2023.
- 36.McEvoy Manjikian, Mary, “From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik”, **International Studies Quarterly**, Vol 54, Issue 2, 2010, pp 381–401.
- 37.Meinig, Donald W, “Heartland and rimland in Eurasian history”, **Western Political Quarterly**, Vol 9, N° 3, 1956, p 553-569.
- 38.Minghao, Zhao, “Is a New Cold War Inevitable? Chinese Perspectives on US–China Strategic Competition”, **The Chinese Journal of International Politics**, Vol 12, Issue 3, 2019, pp 371–394.

- 39.Moyihan, Harriet, “The application of international law to state cyberattacks: Sovereignty and non-intervention”, **Royal Institute of International Affairs**, 2019.
- 40.Mueller, Milton L, “Against sovereignty in cyberspace”, **International Studies Review**, Vol 22, issue 4, 2020, pp 779-801.
- 41.Naji, Saeid, Jayum A. Jawan, “US Hegemonic Leadership and its Geopolitical Codes”, **International Journal of Business and Social Science**, vol 2, n° 7,2011.
- 42.Negro, Gianluigi, “A history of Chinese global Internet governance and its relations with ITU and ICANN”, **Chinese Journal of Communication**, Vol 13, N°1 ,2020, pp 104-121.
- 43.Nye Jr, Joseph S, Nuclear Lessons for Cyber Security, **Strategic Studies Quarterly** vol 5 n° 4, 2011, pp 18-38.
- 44.Oxford Analytica, **Balkanisation of the internet will rise**, Emerald Expert Briefings oxan-db ,2021.
- 45.Oxford Analytica, **Digital authoritarianism in Africa is evolving.**, Emerald Expert Briefings oxan-db, 2022.
46. Pang, Zhongying, “From Tao Guang Yang Hui to Xin Xing: China's Complex Foreign Policy Transformation and Southeast Asia”, **ISEAS-Yusof Ishak Institute**, N° 7, 2020.
- 47.Peters, Michael A, “Semiconductors, geopolitics and technological rivalry: the US CHIPS & Science Act 2022”, **Educational Philosophy and Theory**, 2022.
- 48.Phil, Kelly, “A critique of critical geopolitics”, **Geopolitics**, vol 11, N° 1, 2006.
- 49.Popielec, Dominika, “From Edward Snowden to Christopher Wylie: The Face of the Second Generation Whistleblowing”, **Zeszyty-Prasoznawcze**, t. 62, nr 3(239), s. 39–51, Kraków 2019, p 46-47.

50. Quan, Emily, "Censorship Sensing: The Capabilities and Implications of China's Great Firewall Under Xi Jinping", **Sigma: Journal of Political and International Studies**, Vol 39, Article 4, 2022.
51. Raud, Mikk, "China and Cyber: Attitude, Strategies and Organization", **Cyber research Workshop 2015**, 2015.
52. Rowland, Jill, Mason Rice, and Sujeet Shenoi, "The anatomy of a cyber power", **International Journal of Critical Infrastructure Protection**, Vol 7, N°1, 2014, pp 3-11.
53. Sawant, Mangesh, "Why China Cannot Challenge the US Military Primacy", **Journal of Indo-Pacific Affairs**, Air University Press, 2021.
54. Segal, Adam, "Chinese cyber diplomacy in a new era of uncertainty", **Hoover Institution**, Aegis Paper Series N° 1703, 2017, pp 1-23.
55. Sharikov, Pavel A, "Evolution of American cyber security policies", **Mirovaia ekonomika i mezhdunarodnye otnosheniia**, vol 63, N° 10, 2019.
56. Sheldon, John B, "Geopolitics and cyber power: Why geography still matters", **American Foreign Policy Interests**, Vol 36, N° 5, 2014, pp 286-293.
57. Sloan, Geoffrey & Colin S. Gray, "Why geopolitics?", **Journal of Strategic Studies**, Vol 22, N°2-3, 1999, pp 1-11.
58. Sun, Haiyong, "US-China tech war: Impacts and prospects", **China Quarterly of International Strategic Studies**, Vol 5, Issue 02, 2019, pp 197-212.
59. Trujillo, Clorinda, "The limits of cyberspace deterrence", **NATIONAL DEFENSE UNIV FORT MCNAIR DC**, 2014.
60. Uren, Tom, Bart Hogeveen, and Fergus Hanson, "Defining offensive cyber capabilities", **Briefing and Memos from the Research Advisory Group, The Hague Centre for Strategic Studies**, 2018, pp 73-90.
61. Vidal, Clément, "What is a worldview?.", **De wetenschappen en het creatieve aspect van de werkelijkheid**, 2008.

62. Von Ingersleben-Seip, Nora, “Competition and cooperation in artificial intelligence standard setting: Explaining emergent patterns”, **Review of Policy Research**, 2023.
63. Weber, Valentin, “Linking cyber strategy with grand strategy: the case of the United States”, **Journal of Cyber Policy**, Vol 3, N° 2, 2018.
64. Wu, X, “Technology, power, and uncontrolled great power strategic competition between China and the United States”, **China International Strategy Review**, Vol 2, issue 1, 2020, pp 99–119.
65. Zimmermann, Hubert, “OSI reference model-the ISO model of architecture for open systems interconnection”, **IEEE Transactions on communications**, Vol 28 Issue 4, 1980, pp 425-432.

Dissertation:

1. Craig, Anthony, **Capabilities and conflict in the cyber domain: an empirical study**, Dissertation, Cardiff University, 2020.
2. Domanski, Robert J, **Who Governs the Internet? The Emerging Policies, Institutions, and Governance of Cyberspace**, CUNY Academic Works, 2013.
3. Hersee, Steven, **The Cyber Security Dilemma and the Securitisation of Cyberspace**, Dissertation, Royal Holloway, University of London, 2019.

Public and Official documents:

1. Ann Davidson, Mary, **The Monroe Doctrine in Cyberspace**, testimony to the Homeland Security Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, March 10, 2009, URL: <https://bit.ly/3KDO4QF>.
2. Barbieri, Cristian, Jean-Pierre Darnisand, Carolina Polito, **Non-proliferation Regime for Cyber Weapons. A Tentative Study**, Istituto Affari Internazionali, March 2018, p 6, URL : <http://www.iai.it/sites/default/files/iai1803.pdf>

3. Barlow, John Perry, **A Declaration of the Independence of Cyberspace**, Switzerland, 1996.
4. **Bureau of Industry and Security**, Addition of Entities to the Entity List, federalregister.gov, May 21, 2020, URL: <https://bit.ly/3o4PwAX>.
5. **Bureau of Industry and Security**, Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List, federalregister.gov, May 19, 2020, URL: <https://bit.ly/3o4PwAX>.
6. **Committee on National Security Systems**, Committee on National Security Systems (CNSS) Glossary, CNSSI 4009, March 2, 2022, URL: <https://bit.ly/3KTV3e2>.
7. **Department of Defense**, Department of Defense Cyber Strategy, 2018, URL: <https://bit.ly/3Yaobh6>.
8. **Department of Defense**, Department of Defense Cyber Strategy, April 2015, URL: <https://bit.ly/3FzcyZ5>.
9. **Department of Defense**, Department of Defense Cyber Strategy, October 2022, URL: <https://bit.ly/3JJKmGE>.
10. **Department of Defense**, Department of Defense Strategy for Operating in Cyberspace, July 2011, URL: <https://bit.ly/3HVvswb>.
11. **Department of Homeland Security**, Creation of the Department of Homeland Security, dhs.gov, URL: <https://bit.ly/3iSmXHC>.
12. **Department of State**, Department of State International Cyberspace Policy Strategy, March 2016, URL: <https://bit.ly/3Wkbzm9>.
13. **European Commission**, Versailles Declaration: Informal meeting of the Heads of State or Government, March 2022, URL: <https://bit.ly/46wgk1Z>.
14. Executive Order 13873 of May 15, 2019, **Securing the Information and Communications Technology and Services Supply Chain**, Federal Register, Vol 84, No 96, May 17, 2019.
15. Harold, Scott W, Martin C. Libicki, and Astrid Stuth Cevallos, **Getting to Yes with China in Cyberspace**, CA: RAND Corporation, 2016, URL: <https://bit.ly/3BwDpEF>.

16. Hollis, Duncan, **International Law and Cyberspace**, Carnegie Endowment For International Peace, June 2021, URL: <https://bit.ly/4543S8F>.
17. Information Office of the State Council of the People's Republic of China, **China's National Defense in 2008**, January 2009, Beijing, URL: <https://bit.ly/3E6pWmX>.
18. **International Telecommunication Union**, Global Cybersecurity Index 2020, ITU Publications, 2020, URL: <https://bit.ly/3svomsc>.
19. **National Security Council**, NSC 68, United States Objectives and Programs for National Security, April 14, 1950, URL: <https://bit.ly/3x9izbx>.
20. **National Security Council**, Presidential Directive/NSC-18, U.S. National Strategy, The White House, Washington, DC, 1977.
21. NATO, **NATO 2022 Strategic Concept**, Madrid summit, June 2022, URL: <https://bit.ly/3Q08sQF>.
22. Papp, Robert G., **A Cyber Treaty with Russia**, Kennan Kable, N° 41, Wilson Center, March 2019, URL: <https://bit.ly/3DONNHU>.
23. Pollpeter, Kevin L, Michael S. Chase, and Eric Heginbotham, **The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations**, Cal: RAND Corporation, 2017.
24. Research Department of Military Strategy, **The Science of Military Strategy**, Military Science Press, 2013.
25. S.1260-117th Congress, **United States Innovation and Competition Act of 2021**, Congress.gov, Library of Congress, Jun 8, 2021, URL: <https://bit.ly/3JhxHdp>.
26. Schmidt, Eric E., **Emerging Technologies and Defense: Getting the Fundamentals Right**, Testimony Before the Senate Committee on Armed Services, February 23, 2021, URL: <https://bit.ly/3bSDGri>.
27. **Secretary of State**, The Clean Network, 2020, URL: <http://bit.ly/38a9t1p>.
28. Standing Committee of the National People's Congress, **National Intelligence Law of the People's Republic of China**, Order No. 69, 2017, URL: <https://bit.ly/45CF87a>

29. Stanley, Jay, **The surveillance-industrial complex: How the American government is enlisting private parties in the construction of a surveillance society**, National Headquarters, 2004.
30. The International Institute for Strategic Studies, **CYBER CAPABILITIES AND NATIONAL POWER: A Net Assessment**, June 2021, p 175, URL: <https://bit.ly/45CKorA>.
31. **The International Télécommunication Union**, ITU Toolkit for Cybercrime Legislation, Geneva, 2010.
32. **The People's Republic of China, Ministry of Foreign Affairs**, International Strategy of Cooperation on Cyberspace, fmprc.gov.cn, March 1, 2017, URL: <https://bit.ly/3uSBfLx>.
33. **The White House**, AUKUS Leaders' Level Statement, April 05, 2022, URL: <https://bit.ly/3dc40wC>.
34. **The White House**, FACT SHEET: President Biden Signs Executive Order to Implement the CHIPS and Science Act of 2022, August 25, 2022. URL: <http://bit.ly/3SIw3UY>.
35. **The White House**, FACT SHEET: U.S.-EU Trade and Technology Council Establishes Economic and Technology Policies & Initiatives, May 16, 2022, URL: <https://bit.ly/3SAIKCa>.
36. **The White house**, International strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World, Washington, May 2011, URL: <https://bit.ly/3zbUMsU>.
37. **The White house**, National Cyber strategy of the United states of America, September 2011, URL: <https://bit.ly/3zek9u3>.
38. **The White House**, National Strategy to Secure Cyberspace, Washington, 2003, URL: <https://bit.ly/3s0WOaR>.
39. **The White House**, Notice on the Continuation of the National Emergency with Respect to Securing the Information and Communications Technology and Services Supply Chain, May 11, 2021.
40. **The White House**, Quad Joint Leaders' Statement, whitehouse.gov, May 24, 2022, URL: <https://bit.ly/3Qq65U8>.

41. **The White House**, Remarks by President Biden at Indo-Pacific Economic Framework For Prosperity Launch Event, May 23, 2022, URL: <https://bit.ly/3p36qQS>.
42. **The White House**, Remarks by President Biden at the Office of the Director of National Intelligence, Virginia, July 27, 2021, URL: <https://bit.ly/3z18gHj>.
43. **The White House**, Remarks by President Biden on America's Place in the World, Washington, February 04, 2021, URL: <https://bit.ly/3Tma5H4>.
44. **The White House**, The National Cyber Strategy of the United States of America, Washington, September 2018, URL: <https://bit.ly/3zek9u3>.
45. **The White House**, The National Cyber Strategy of the United States of America, Washington, October 2022, URL: <https://bit.ly/3eTqx2n>.
46. **The White House**, The National Security Strategy of the United States of America, Washington, March 2006, URL: <https://bit.ly/3D59rry>.
47. **The White House**, The National Security Strategy of the United States of America, Washington, December 2017, URL: <https://bit.ly/3Bx13kh>.
48. **The White House**, The National Security Strategy of the United States of America, Washington, October 2022, URL: <https://bit.ly/3eTqx2n>.
49. **The White House**, The National Security Strategy of the United States of America, Washington, September 2002, URL: <https://bit.ly/3DbdTnw>.
50. Theohary, Catherine A, **Defense primer: Cyberspace Operations**, Congressional Research SVC, 2021, URL: <https://sgp.fas.org/crs/natsec/IF10537.pdf>
51. Trump, Donald J, **National security strategy of the United States of America**, Executive Office of The President Washington DC Washington United States, 2017, URL: <https://bit.ly/3Bx13kh>.
52. **U.S Office of the Federal Register, National Archives and Records Administration**, Executive Order 14034 of June 09, 2021, Protecting Americans' Sensitive Data From Foreign adversaries, Federal Register, June 09, 2021.
53. **U.S Office of the Federal Register, National Archives and Records Administration**, Executive Order 14073 of May 04, 2022, Executive Order on

Enhancing the National Quantum Initiative Advisory Committee, Federal Register, May 04, 2022.

54. **U.S The White House, NATIONAL SECURITY MEMORANDUM/NSM-10**, National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, whitehouse.gov, MAY 04, 2022, URL: <https://bit.ly/3BqzCsF>.
55. **U.S. Department of Defense**, The Department of Defense Releases the President's Fiscal Year 2023 Defense Budget, defense.gov, March 28, 2022, URL: <https://bit.ly/3Aovo3u>.
56. **Unit, Economist Intelligence**, Cyber power index: findings and methodology, Booz Allen Hamilton, 2011.
57. **US Cyber Command**, Achieve and Maintain Cyberspace Superiority, 2018, URL: <https://bit.ly/3QydfiT>.
58. **US Cyber Command**, Vision 2018, april 2018, URL : <https://bit.ly/3QydfiT>.
59. **US. Department of Defense**, Dictionary of military and associated terms, Joint Publication 1-02, 2010 (As Amended Through 15 February 2016, p 58, URL: <https://bit.ly/47GExTP>.
60. Voo, Julia, et al, **National Cyber Power Index 2020: Methodology and Analytical Considerations**, China Cyber Policy Initiative, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2020.

Reports:

1. Allison, Graham, et al, **The Great Tech Rivalry: China vs. the US**, Belfer Center, Havard Kennedy School, March 2021, URL: <https://bit.ly/3dx0YDv>.
2. Anderson, Justin V., Jeffrey A. Larsen, and Polly M. Holdorf, **Extended Deterrence and Allied Assurance: Key Concepts and Current Challenges for US Policy**, Air force academy, Colorado springs Co Inst for national security studies, 2013.

3. Bateman, Jon, **US-China technological “Decoupling”: a strategy and policy framework**, Carnegie Endowment for International Peace, 2022.
4. Bhandari, Konark, **The Geopolitics of the Semiconductor Industry and India’s Place in it**, Carnegie India, India, June 2023.
5. Brown, Michael, Pavneet Singh, **China’s Technology Transfer Strategy**, Defense Innovation Unit Experimental (DIUx), January 2018, URL: <https://bit.ly/45DyRcf>.
6. Carafano, James J., et al, **Winning the New Cold War: A Plan for Countering China**, The Heritage Foundation, Report n° 270, March 2023, URL: <https://herit.ag/43Cs3cw>.
7. Green, Michael J., et al, **Asia-Pacific rebalance 2025: Capabilities, presence, and partnerships**, CSIS, 2016.
8. Gruver, Patricia, **Korea-U.S International Exchange and Cooperation in Tech Diplomacy**, Pacific Council on International Policy, June 2022, URL: <https://bit.ly/3AI16cq>.
9. Heath, Timothy R., et al, **The Return of Great Power War: Scenarios of Systemic Conflict Between the United States and China**, Calif: RAND Corporation, 2022.
10. Heginbotham, Eric, Michael Nixon, et al, **The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996–2017**, Cal: RAND Corporation, 2015.
11. Hitchens, Theresa, Nilsu Goren, **International Cybersecurity Information Sharing Agreements**, Center for International & Security Studies, 2017.
12. Hunt, Glen, **5G Mobile Core: Competitive Landscape Assessment**, Globaldata.com, November 2021, URL: <https://bit.ly/3yC03th>.

13. **J.P. Morgan**, Global e-commerce trends report, jpmorgan.com, 2021, URL: <https://bit.ly/3njKIHu>.
14. Kania, Elsa B, Lorand Laskai, **Myths and Realities of China's Military-Civil Fusion Strategy**, Center for a New American Security, Washington (DC), 2021.
15. Kemp, Simon, **DIGITAL 2022: April Global Statshot Report**, datareportal.com, 21 APRIL 2022, URL: <https://bit.ly/3P7OySN>.
16. Lester, Richard, et al, **University Engagement with China: An MIT Approach**, The MIT China Strategy Group, November 2022, URL: <https://bit.ly/3OVHcBG>.
17. Mazarr, Michael J., et al, **Competition and Restraint in Cyberspace: The Role of International Norms in Promoting U.S. Cybersecurity**, Cal: RAND Corporation, 2022.
18. **National Security Commission on Artificial Intelligence**, Final Report, 2021, URL : <https://bit.ly/3JctHsX>.
19. Nye Jr, Joseph S, **Normative Restraints on Cyber Conflict**, Belfer Center, Havard Kennedt School, August 2018, URL: <https://bit.ly/3KxRWUt>.
20. Pohlmann, Tim, Magnus Buggenhagen, **Who is leading the 5G patent race?**, Iplytics, June 2022, URL: <https://bit.ly/3YJNTu1>.
21. Schmidt, Eric E., et al, **Final Report**, National Security Commission on Artificial Intelligence, 2021, URL: <https://bit.ly/3bSDGri>.
22. Scobell, Andrew, et all, **China's Grand strategy: Trends, Trajectories, and Long-Term Competition**, Cal:RAND Corporation, 2020.
23. Segal, Adam, Goldstein Gordon, **Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet**, The Council on Foreign Relations, United States of America, 2022.

24. Seosanto, Stefan, **The Evolution of US Defense Strategy in Cyberspace (1988–2019)**, ETH Zurich, 2019.
25. Silver, Laura, et al, **Americans Are Critical of China's Global Role – as Well as Its Relationship With Russia**, Pew Research Center, April, 2023, URL: <https://bit.ly/3YatrCj>.
26. Stone, Alex, Peter Wood, **China's Military-Civil Fusion Strategy: A view from Chinese strategists**, China Aerospace Studies Institute, USA, 2020.
27. **UNCTAD**, DIGITAL ECONOMY REPORT 2021 iii Cross-border data flows and development: For whom the data flow, United Nations Publications, 2021, URL: <https://bit.ly/47K7Y7n>.
28. US-China Perception Monitor, **U.S.-China Strategic Competition in Technology: Analysis and Prospects (Chinese language)**, uscnpm.org, February 2022, URL: <https://bit.ly/44qeuy3>.
29. Wübbeke, Jost, et al, **MADE IN CHINA 2025**, Mercator Institute for China Studies, December 2016, URL: <https://bit.ly/3qjGdkY>.

Websites:

1., **The Guardian view on US-China chip wars: no winners in zero-sum battles**, theguardian.com, April 2023, URL: <https://bit.ly/3PUYwaR>.
2. "X" (George F. Kennan), **The Sources of Soviet Conduct**, foreignaffairs.com, July 1, 1947, URL: <http://bit.ly/3Ygd1H3>.
3., **China Orders Government, State Firms to Dump Foreign PCs**, bloomberg.com, Mai 6, 2022, URL: <https://bloom.bg/3cEH5tq>.
4., **G7 summit: Leaders detail \$600bn plan to rival China's Belt and Road initiative**, BBC.com, June 27, 2022, URL: <https://bbc.in/3c841Bd>.

5., **Whoever leads in AI will rule the world': Putin to Russian children on Knowledge Day**, RT.com, Sep 2017, URL: <https://bit.ly/3zCU7Rk>.
6., **The Cold War for Supremacy in the Information Age**, Greater Pacific Capital, September 2020, URL: <https://bit.ly/3rQa3hO>.
7. Aaron, Smith, **How China surpassed the U.S. in the race for AI supremacy**, uscgpi.com, Jan 6, 2022, URL: <https://bit.ly/3cIyuWS>.
8. Aitken, Peter, **China has stolen US military secrets to create formidable J-20 knockoff of America's F-22 Raptor**, foxnews.com, March 9, 2023, URL: <https://bit.ly/3XCoKkw>.
9. Akito, Tanaka, Grace Li, **U.S. big tech won't shake its China addiction**, asia.nikkei.com, July 2023, URL: <https://bit.ly/3KFX7Bx>.
10. Atkinson, Robert D., **Biden's Indo-Pacific Economic Framework Is a Paradigm Shift**, foreignpolicy.com, July 1, 2022, URL: <https://bit.ly/3vQiXuO>.
11. Barton, James, **"4G changed lives. 5G will change society" – Huawei's Steven Wu**, developingtelecoms.com, March 2019, URL: <https://bit.ly/3nmSroi>.
12. Beals, Monique, **Former Pentagon official says China has won artificial intelligence battle**, theHill.com, Nov 10, 2021, URL: <https://bit.ly/3vm6BKH>.
13. Beckley, Michael, **Accepting a Cold War with China Is the Best Option**, The American Enterprise Institute, December 06, 2022, URL: <https://bit.ly/3KeI164>.
14. Beinart, Peter, **America needs an entirely new foreign policy for the Trump age**, TheAtlantic, Sep 16, 2018, URL: <https://bit.ly/3Tmt30q>.
15. Benitez, Christopher, **27 Latest WeChat Statistics: Usage, Facts, And Trend**, startupbonsai, June 16, 2022, URL: <https://bit.ly/3PTm4cO>.
16. Bischoff, Paul, **Surveillance camera statistics: which cities have the most CCTV cameras?**, comparitech.com, May 17, 2021, URL: <https://bit.ly/3b7hYyP>.
17. Bischoff, Paul, **Which countries have the worst (and best) cybersecurity?**, comparitech.com, Sept 26, 2022, URL: <https://bit.ly/3mLNx3X>.
18. Blinken, Antony J., **A Foreign Policy for the American People**, US department of state, state.gov, MARCH 3, 2021, URL: <https://bit.ly/3gp2GYT>.

19. Blinkin, Antony J. , **Remarks to the Press**, US department of State, state.gov, October 17, 2022, URL: <https://bit.ly/3K2LIM2>.
20. Brady, James S., **Press Conference by the President**, obamawhitehouse.archives.gov, December 20, 2013, URL: <https://bit.ly/3EWWFHb>.
21. Brake, Doug, **Submarine Cables: Critical Infrastructure for Global Communications**, itif.org, April 19, 2019, URL: <https://bit.ly/3RdZBZu>.
22. Burdette, Lane, **Leveraging Submarine Cables for Political Gain: US Responses to Chinese Strategy**, Journal of Public & International Affairs, 2021, URL: <https://bit.ly/3Pjfw72>.
23. Carafano, James J., “ **Is There a U.S.-China Cold War**” **Is the Wrong Question**, heritage.org, Nov 2022, URL: <https://bit.ly/43BUeZ9>.
24. Carpenter, Galen, **Accepting Spheres of Influence in the 21st Century**, CATO Institute, May7, 2014, URL: <https://bit.ly/3AjsYSw>.
25. Center Mandiant Intelligence, **APT1: Exposing one of China’s cyber espionage units**, Mandian.com, 2013, URL: <https://bit.ly/3QQxP7Y>.
26. Choudhury, Saheli Roy, **As information increasingly drives economies, China is set to overtake the US in race for data**, cnbc.com, 2019, URL: <https://cnb.cx/3OxTcpE>.
27. **Council on foreign relations**, 1949–2023 U.S.-China Relations, cfr.org, URL: <https://bit.ly/47GmI7o>.
28. Cramer-Flood, Ethan, **China Ecommerce 2020**, insiderintelligence.com, Jun 10, 2020, URL: <https://bit.ly/3njY7zm>.
29. **Cybersecurity and Infrastructure Security Agency**, About CISA, cisa.gov, URL: <https://bit.ly/3E93sBZ>.
30. Desheng, Cao, **Xi calls for expansion of global partnerships**, China daily, Sept 9, 2019, URL: <https://bit.ly/3domQRq>.
31. Dixon Stacy Jo., **Share of U.S. population who use social media 2008-2021**, Statista.com, Jul 27, 2022, URL: <https://bit.ly/3tizo1Q>.
32. Etzioni, Amitai, **China is Not the Soviet Union**, The National Interest, 2018, URL: <https://bit.ly/3qaxwcZ>.

33. Eurasia Group, **The Geopolitics of Semiconductors**, eurasia group.net, SEPTEMBER 2020, URL: <https://bit.ly/3PtNqq4>
34. Ferguson, Niall, **Cold War II: Niall Ferguson On The Emerging Conflict With China**, hoover.org, May 1, 2023, URL: <https://bit.ly/44tDJ2M>.
35. Fowdy, Tom, **New China-made operating system to offer an alternative**, china.org.cn, June 9, 2021, URL: <https://on.china.cn/3PxDFHD>.
36. Goodman, Matthew P., Matthew Wayland, **Securing Asia's Subsea Network: U.S. Interests and Strategic Options**, CSIS Briefs, CSIS, April 5, 2022, URL: <https://bit.ly/3Pd9RzD>.
37. Gorwa Robert, Anton peez, **Tech Hits the Diplomatic Circuit**, berlinpolicyjournal.com, June 27, 2019, URL: <https://bit.ly/3T9IsBk>.
38. Goujard, Clothilde , Alfred Ng, **EU and US reach a deal to let data flow across the Atlantic**, politico.eu, July 2023, URL: <https://bit.ly/3qqjfsV>.
39. Graham, Bradley, **Bush Orders Guidelines for Cyber-Warfare**, washingtonpost.com, February 7, 2003, URL: <https://bit.ly/3PgKVZf>.
40. Haranas, Mark, **AWS, Google, Microsoft are taking over the Data Center market**, crn.com, January 27, 2021, URL: <https://bit.ly/3PUrLHJ>.
41. Huanxin, Zhao, Wang Qingyun, **Blinken: Peaceful coexistence 'base line' of ties**, chinadaily.com.cn, Juin 2023, URL: <https://bit.ly/3OTHEAl>.
42. Huld, Arendse , **“Eastern Data, Western Computing” – China's Big Plan to Boost Data Center Computing Power Across Regions**, china-briefing.com, March 30, 2022, URL: <https://bit.ly/3zB0jJz>.
43. **Internet Governance Forum**, Donors to the IGF Trust Fund, intgovforum.org, URL: <https://bit.ly/3RQRRwT>.
44. Jennings, Ralph, **China's Economy Could Overtake US Economy by 2030**, voanews.com, January 04, 2022, URL: <https://bit.ly/3QG4HwG>.
45. Johnson, Alex , **Pompeo suggests God sent Trump to save Israel**, nbcnews.com, March 22, 2019, URL: <https://nbcnews.to/3DqoOeo>.
46. Kagan Robert, **Backing Into World War III**, ForeignPolicy, Feb 6, 2017, URL: <https://bit.ly/3Cwpj6D>.

47. Kaur, Dashveenjit, **Chip war: Is China still lagging in the semiconductor race?**, Techwire Asia, March 24, 2022, URL: <https://bit.ly/3o8qXCY>.
48. Kendall, Sandy, **Did the National Strategy for Securing Cyberspace Wimp Out?**, csoonline.com, FEB 24, 2003, URL: <https://bit.ly/3iQSOIC>.
49. Klebanov, Sam, **Who's winning the quantum computing race? China and the U.S. are neck and neck**, businessofbusiness.com, February 24, 2022, URL: <https://bit.ly/3S5zlB5>.
50. Kurlantzick, Joshua, James West, **Assessing China's Digital Silk Road Initiative**, Council on Foreign Relations, 2020, URL: <https://on.cfr.org/3Pq95iU>.
51. L. Ceci, **TikTok: number of users in the United States 2020-2023**, Statista, Jan 28, 2022, URL: <https://bit.ly/3Bdmlhn>.
52. Lampton, David M., **The Tipping Point - Can We Amplify What We Have in Common?**, cirsd.org, URL: <https://bit.ly/3S8o6lh>.
53. Liang, Annabelle, **US-China chip war: Netherlands moves to restrict some tech exports**, BBC.com, March 2023, URL: <https://bit.ly/3OLEleH>.
54. Ma, Yihan, **Main goods imported in China 2022**, Statista.com, Mar 2, 2023, URL: <https://bit.ly/44KlaHb>.
55. MacAskill, Ewen, **George Bush: 'God told me to end the tyranny in Iraq'**, theguardian.com, October 7, 2005, URL: <https://bit.ly/3St8Fcn>.
56. Mauldin, Alan , **A Complete List of Content Providers' Submarine Cable Holdings**, blog.telegeography, Nov 9, 2017, URL: <https://bit.ly/3bOsCuF>.
57. Mauldin, William, Michael R. Gordon, **Blinken Backs Tough Approach to China, Says Will Work With GOP**, wsj.com, Jan. 19, 2021, URL: <http://bit.ly/3KHSjwB>.
58. Musgrave, Paul, **The Slip That Revealed the Real Trump Doctrine**, foreignpolicy.com, MAY 2, 2019, URL: <http://bit.ly/3xROFbM>.
59. Myerson, Terry, **Announcing Windows 10 China Government Edition and the new Surface Pro**, Windows Experience Blog, May 23, 2017, URL: <https://bit.ly/3czRJ4F>.

60. Nakashima, Ellen, Jeanne Whalen, **Barr suggests U.S. consider investing in Nokia, Ericsson to counter Huawei**, The Washington Post, February 6, 2020, URL: <https://wapo.st/3ydPQ4T>
61. Navarro, Peter, **Mearsheimer on Strangling China & the Inevitability of War**, huffpost.com, Mar 10, 2016, URL: <http://bit.ly/3Z25RXS>.
62. Negrea, Dan, James J. Carafano, **The Pretend Phase of Cold War II Is Over**, Thenationalinterest.org, June 2, 2023 , URL: <https://bit.ly/43uBBGo>.
63. Nye JR, Joseph S , **America's strategy towards the new superpower**, project-syndicate.org, Aug 3, 2021, URL: <https://bit.ly/3B6uN6R>.
64. Nye JR, Joseph S, **Cracking China**, the-security-times.com, February 2022, URL: <https://bit.ly/3Q82gpz>.
65. Nye JR, Joseph S, **Deterrence in Cyberspace**, Australian Strategic Policy Institute, Jun 7, 2019, URL: <https://bit.ly/3CU6UkD>.
66. Nye JR, Joseph S, **Popping China's Balloon**, project-syndicate.org, March 2021, URL: <https://bit.ly/3K9dINZ>.
67. Nye JR, Joseph S, **With China, a "Cold War" Analogy Is Lazy and Dangerous**, belfercenter.org, November 2021, URL: <https://bit.ly/44Glr1>.
68. Page, Jeremy, Kate O'Keeffe, Rob Taylor, **America's Undersea Battle with China for Control of the Global Internet Grid**, Wall Street Journal, March 12, 2019, URL: <https://on.wsj.com/3Rv6VAg>.
69. Payton, Theresa, **America is Losing the Quantum Race with China**, newsweek.com, May 12, 2022, URL: <https://bit.ly/3z8fLM1>.
70. Pelosi, Nancy, **Transcript of Pelosi, Congressional Delegation Press Conference on Conclusion of 2020 Munich Security Conference**, **speaker.gov**, February 16, 2020, URL: <https://bit.ly/3CfQN07>.
71. Qu, Tracy, **China's chip imports slump in first half as US sanctions and ongoing tech war take a toll on trade**, South China Morning Post, July 2023, URL: <https://bit.ly/3rWX3Hk>.
72. Reuters Staff, **President Xi says China will not export its political system**, Reuters, December 1, 2017, URL: <https://bit.ly/3Y9E2xn>.

73. Roosevelt Room, **Remarks by President Trump on United States 5G Deployment**, trumpwhitehouse.archives.gov, April 12, 2019, URL: <https://bit.ly/3IaEeEi>
74. Rubio Arroyo, Isabel, **How the Internet extends across the sea floor**, sacyr.com, URL: <https://bit.ly/3OOkN74>.
75. Sanders, Bernie, **Washington's Dangerous New Consensus on China**, foreignaffairs.com, June 17, 2021, URL: <http://bit.ly/3kUTjmf>.
76. Schwartz, John, Ariana Eunjung Cha, **Clinton Pledges to Help Industry Fight Hackers**, washingtonpost.com, February 16, 2000, URL: <https://wapo.st/3CyOVhI>.
77. Segal, Adam , **A New U.S. Foreign Policy for Cyberspace**, cfr.org, July 12, 2022, URL: <https://on.cfr.org/3DAmt1a>.
78. Segal, Adam, **When China rules the web: technology in service of the state**, Foreign Affaires, september/october 2018, URL: <https://fam.ag/3PYiY7N>.
79. Shambaugh, David , **In a fundamental shift, China and the US are now engaged in all-out competition**, scmp.com, Jun11,2015, URL: <https://bit.ly/3zHHmVM>.
80. Sheng, Yang, Qi Xijia, **US signals to fix China ties but 'credible sincerity' needed; Washington to be 'lone wolf' in 'new cold war' against China**, globaltimes.cn, Apr 11, 2023, URL: <https://bit.ly/3DgiQfh>.
81. STAMFORD, Conn, **Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed \$150 Billion in 2021**, gartner.com, May 17, 2021, URL: <https://gtmr.it/3N29Z3g>.
82. Statcounter, **Desktop Operating System Market Share Worldwide July 2022 - July 2023**, gs.statcounter.com, URL: <https://bit.ly/3OwvRo5>.
83. Statcounter, **Operating System Market Share Worldwide, July 2022 - July 2023**, gs.statcounter.com, URL: <https://bit.ly/3OL7ZiW>.
84. Statista Research Department, **Amount of data created, consumed, and stored 2010-2025**, Statista.com, May 23, 2022, URL: <https://bit.ly/3vf9YDc>.
85. Statista Research Department, **Revenue of the e-commerce industry in the U.S. 2017-2027**, statista.com, Aug 16, 2023, URL: <https://bit.ly/3QNPAC6>.

86. Summers, Josh, **List of Websites and Apps Blocked in China for 2022**, travelchinacheaper.com, July 1, 2022, URL: <https://bit.ly/3RYXB84>.
87. Tan, Valarie, **Winning the tech war with Chinese characteristics**, merics.org, Jan 2022, URL: <https://bit.ly/3pLsu6E>.
88. Thomala Lai lin, **Number of internet users in China 2012-2022**, Statista.com, Apr 19, 2023, URL: <https://bit.ly/3sfWvfC>.
89. Thomala Lai lin, **Penetration rate of social media in China 2016-2022**, Statista.com, Apr 27, 2023, URL: <https://bit.ly/47KW2m8>.
90. **Times higher education**, World University Rankings 2022, timeshighereducation.com, 2022, URL: <https://bit.ly/3b1qtvj>.
91. Toh, Michelle, Junko Ogura, **Japan joins the US and Europe in chipmaking curbs on China**, CNN.com, March 2023, URL: <https://bit.ly/3DIM2Mn>.
92. Tucker, Patrick, **China Will Surpass US in AI Around 2025, Says Google's Eric Schmidt**, defenseone.com, Nov 1, 2017, URL: <https://bit.ly/3zbtTUB>.
93. **U.S Cyber Command**, OUR HISTORY, cybercom.mil, URL: <https://bit.ly/3YKJ1EQ>.
94. UN news, **UN chief says regulation needed for AI to 'benefit everyone'**, UN.org, July 2023, URL: <https://bit.ly/3OrGqLl>.
95. Varas, Antonio, Raj Varadarajan, **How Restricting Trade with China Could End US Semiconductor Leadership**, bcg.com, MARCH 2020, URL: <https://on.bcg.com/3yJw2GK>.
96. Waters, Richard, **US rushes to catch up with China in supercomputer race**, Financial times.com, May 18 2022, URL: <https://on.ft.com/3vlOUuF>.
97. Wearesocial, **DIGITAL 2022: ANOTHER YEAR OF BUMPER GROWTH**, 26 Jan 2022, URL: <https://bit.ly/3sgqnse>.
98. Weber, Valentin, **Making Sense of Technological Spheres of Influence**, LSE IDEAS, Mar 31, 2020, URL: <https://bit.ly/3ANbgbl>.
99. Wei, Yuxi, **China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty**, University of Washington.com, June 2016, URL: <https://bit.ly/443P0Wn>.

100. **World bank**, Individuals using the Internet (% of population) - United States, data.worldbank.org, 2021, URL: <https://bit.ly/3KR97jS>.
101. **World Bank**, High-technology exports (current US\$), 2021, URL: <https://bit.ly/3xWxMgU>.
102. **World Intellectual Property Organization**, Patent applications, residents, data.worldbank.org, 2020, URL: <https://bit.ly/3Hu0Xv0>.
103. Xinhua, **China forges ahead for brighter future in digital economy**, english.scio.gov.cn, April 25, 2022, URL: <https://bit.ly/3PmsIrx>.
104. Xinhua, **Full text of President Xi's speech at opening of Belt and Road forum**, xinhuanet.com, 14 May 2017, URL: <https://bit.ly/45XZitx>.
105. Xinhua, **Full text of Xi's address at SCO summit**, gov.cn, July 4, 2023, URL: <https://bit.ly/3K242oB>.
106. Xuanzun, Liu , **China boosts defense budget by 7.1% for 2022 amid complex global situation**, globaltimes.cn, Mar 05, 2022 , URL: <https://bit.ly/3SMgBqR>.
107. Yellen, Janet L., **Remarks by Secretary of the Treasury Janet L. Yellen on the U.S. - China Economic Relationship at Johns Hopkins School of Advanced International Studies**, treasury.gov, April 20, 2023, URL: <https://bit.ly/3DTBiuv>.
108. Yue, Shi, Xu Zihe, **Achievements in building China's strength in cyberspace in the past decade**, globaltimes.cn, Aug 19, 2022, URL: <http://bit.ly/42t4803>.
109. Yuntao, Yang, Zhang Tingting, **China can deal with the US**, Chongyang Institute for Financial Studies, zhuanlan.zhihu.com, URL: <https://bit.ly/3rIMxmJ>.
110. Zhuang, Sylvie, **US tech war: China's Xi Jinping urges 'solid path of innovation' as he tours semiconductor firms**, South China Morning Post, July 2023, URL: <https://bit.ly/3qoeIXR>.

2.2 باللغة الصينية:

1. China International Economic Exchange Center, **2020 China 5G Economic Report** (2020 中国 5G 经济报告), 2020, URL: <https://bit.ly/3yDXo2w>.

2. Cybersecurity Association of China (CAICT), **China Network Security Industry Analysis Report 2021** (中国网络安全产业分析报告 2021 年), 2021, URL: <https://bit.ly/3zDSLX2>.
3. جمهورية الصين الشعبية، المكتب الوطني لمعلومات الإنترنت الاستراتيجية الوطنية لأمن الفضاء الإلكتروني، الاستراتيجية الوطنية لأمن الفضاء الإلكتروني، على الرابط: <https://bit.ly/45EbcYl>.
4. 中国保密协会[جمعية السرية الصينية]، 数字空间的大国博弈笔谈 [لعبة القوى العظمى في الفضاء]، zgbmxh.cn, Jan 21, 2022, URL: <https://bit.ly/3pN5wZh>.
5. 人民日报، 捍卫“数据主权” (环球走笔) [الدفاع عن "سيادة البيانات"]، opinion.cntv.cn, Jan 14, 2015, URL : <https://bit.ly/3pLFyp4>.
6. 孙成昊 [صن تشنغهاو]، 百岁老人基辛格访华 · 释放了中美关系的何种信号？ [زيارة المنوي]، هنري كيسنجر للصين: مانوع الإشارات التي ترسلها العلاقات الأمريكية الصينية؟، ciss.tsinghua.edu.cn, July 2023, URL: <https://bit.ly/3OVRbqQ> .
7. 新华 [شينخوا]، 美式“数字霸权” 是全球互联互通最大障碍 [الهيمنة الرقمية الأمريكية أكبر عقبة]، chinanews.com.cn, Dec 15, 2021, URL: <https://bit.ly/3CxJPEa>.
8. 新华社[شينخوا]، 数字中国建设整体布局规划[خطة التخطيط الشاملة لبناء الصين]، وكالة أنباء شينخوا [وكالة أنباء شينخوا]، gov.cn, Feb 2023, URL: <https://bit.ly/3BP4DWa>.
9. 新华社[شينخوا]، 数字中国建设整体布局规划[دعوا شلعة التعددية تضيء طريق]، وكالة أنباء شينخوا [وكالة أنباء شينخوا]، xinhuanet.com, Jan 2021, URL: <https://bit.ly/456T09R>.
10. 新华网[شينخوا نت]، 习近平:把我国从网络大国建设成为网络强国 [شي جين بينغ: تحويل الصين]، من قوة سيبرانية كبرى إلى قوة سيبرانية عظمى، xinhuanet.com , February 27, 2014, URL: <http://bit.ly/3JQjcNX>.
11. 焦元[جياو يوان]، 中国常驻联合国代表：世界不需要“新冷战” [مندوب الصين الدائم لدى الأمم المتحدة: العالم لا يحتاج إلى "حرب باردة جديدة"]، 新华网 [وكالة شينخوا]، 2022, URL: <https://bit.ly/44woR3w>.

12. 王磊 [وانغ لي], “清洁网络”计划的实质是数字霸权 [الهيمنة هو النظيف هو الويب النظيف هو الهيمنة], china.com.cn, Nov 02, 2020, URL: <https://bit.ly/3wuxZqw>.
13. 翟 崑 [تشاي كون], 数字全球化的战略博弈态势及中国应对 [الوضع الاستراتيجي للعولمة الرقمية], rmlt.com.cn, Juin 29, 2020, URL: <https://bit.ly/3CyArQA>.
14. 赵明昊 [تشاو مينغ هاو], 赵明昊：试析中美“战略竞争”及其管理 [تحليل "المنافسة الاستراتيجية"], ciss.tsinghua.edu.cn, 2021, URL: <https://bit.ly/3Oa04va>.
15. 达巍 [دا وي], 跑赢“田径赛”· 需超越中美双边竞斗 [للفوز في مسابقات "المضمار والميدان"], ciss.tsinghua.edu.cn, February 2023, URL: <https://bit.ly/3YCBPKT>.

3.2 باللغة الفرنسية:

Livres :

1. Brisset, Jean-Vincent, **La chine, une puissance encerclée**, Paris: IRIS (collection Enjeux stratégiques), 2002.
2. Henri, Lefebvre, **La production de l'espace**, Éditions Anthropos, 1986.
3. Kempf, Olivier, **Introduction à la Cyberstratégie**, Paris, Economica, 2012.

Articles:

1. Douzet, Frédérick, « La géopolitique pour comprendre le cyberspace », **Hérodote**, vol :152-153, N° 1-2, 2014, pp 3-21.
2. Zyw Melo, Anna, « Un câble pour les BRICS : un défi stratégique insurmontable », **Hermès La Revue**, Vol 79, N° 3, 2017, pp 145-149.

Sites Web:

1. **Commission européenne**, Paquet législatif sur les semi-conducteurs, commission.europa.eu, 2022, URL : <https://bit.ly/456Y7H4>.

فهرس الموضوعات

01.....	مقدمة
73-12.....	الفصل الأول: جيوبوليتيكا الفضاء السيبراني
13.....	المبحث الأول: الجيوبوليتيكا... تطور النظرية ومنهج التحليل
13.....	المطلب الأول: الجيوبوليتيكا رؤية للعالم
17	المطلب الثاني: الجيوبوليتيكا التقليدية: الآباء المؤسسون
25.....	المطلب الثالث: الجيوبوليتيكا المعاصرة: إعادة الإحياء
29.....	المطلب الرابع : التحليل الجيوبوليتيكي والمدرک الاستراتيجي
34.....	المبحث الثاني: الفضاء السيبراني بعد جديد في العلاقات الدولية
34.....	المطلب الأول : مفهوم الفضاء السيبراني، خصائصه وفواعله
39.....	المطلب الثاني: علاقة التأثير والتأثر بين الفضاء السيبراني والعلاقات الدولية
43.....	المطلب الثالث: القوة السيبرانية
47.....	المطلب الرابع: الصراع السيبراني
54.....	المبحث الثالث : التحليل الجيوبوليتيكي للفضاء السيبراني
55.....	المطلب الأول : الطبقات لفهم جيوبوليتيكا الفضاء السيبراني
60.....	المطلب الثاني : نوموس الفضاء السيبراني
63.....	المطلب الثالث: أمنة الفضاء السيبراني
67.....	المطلب الرابع: السيادة السيبرانية
139-75.....	الفصل الثاني: مضامين الصراع الأمريكي - الصيني في الفضاء السيبراني
76.....	المبحث الأول: القدرات السيبرانية للولايات المتحدة الأمريكية والصين
76.....	المطلب الأول: مؤشر القدرات السيبرانية للدولة
85.....	المطلب الثاني: الولايات المتحدة الأمريكية القوة السيبرانية الرائدة (مهد الأنترنت)
91.....	المطلب الثالث: الصين ... قوة سيبرانية متنامية بسرعة

المبحث الثاني: تجليات الصراع الأمريكي الصيني في/على الفضاء السيبراني.....	97
المطلب الأول: الصراع على البنية التحتية المادية.....	97
المطلب الثاني: حوكمة الفضاء السيبراني (الأنترنت).....	108
المطلب الثالث: التنافس على البرمجيات.....	114
المطلب الرابع: البيانات الضخمة (Big Data) نطف القرن الواحد والعشرين.....	119
المبحث الثالث : تداعيات الصراع الأمريكي-الصيني على العلاقات والتحالفات الدولية..	125
المطلب الأول: تداعيات الصراع التكنولوجي على العلاقات الثنائية بين الو.م.أ والصين...	125
المطلب الثاني: تداعيات الصراع التكنولوجي على التحالفات الاستراتيجية الجديدة.....	129
المطلب الثالث: تداعيات الصراع التكنولوجي على توازن القوى والنظام الدولي.	133
الفصل الثالث: استراتيجيات الولايات المتحدة والصين لإدارة الصراع في الفضاء	
السيبراني.....	141- 222
المبحث الأول : المقاربات النظرية والمنطلقات الفكرية الحديثة لإدارة الصراع في الفضاء	
السيبراني	142
المطلب الأول: دبلوماسية الشركات.....	142
المطلب الثاني: الهيمنة الرقمية ومجالات النفوذ الجديدة.....	145
المطلب الثالث: اللعبة الجيوبوليتيكية الرقمية.....	148
المطلب الرابع: الردع وتوازن القوى في الفضاء السيبراني.....	150
المبحث الثاني: استراتيجيات الولايات المتحدة الأمريكية في الفضاء السيبراني.....	155
المطلب الأول: المبادئ الجيوبوليتيكية الأمريكية والهيمنة العالمية.	155
المطلب الثاني: الفضاء السيبراني في المدرك الاستراتيجي الأمريكي.	159
المطلب الثالث: الاستراتيجيات الأمريكية للنفوذ في الفضاء السيبراني.	168
المطلب الرابع: الاستراتيجيات الأمريكية للسيطرة على الفضاء السيبراني.	183
المبحث الثالث : الاستراتيجية الصينية لإدارة الصراع في الفضاء السيبراني.	195

فهرس الموضوعات

المطلب الأول: المبادئ الجيوبوليتيكية الصينية: من حلم الصين إلى حلم العالم.	195
المطلب الثاني: الفضاء السيبراني كخيار استراتيجي للصين.....	200
المطلب الثالث: الاستراتيجية السيبرانية الصينية:الصين الرقمية، من فوجيان نحو العالم...205	
المطلب الرابع: سياسات الصين للهيمنة في/على الفضاء السيبراني.....	213
الفصل الرابع: مآلات الصراع الأمريكي الصيني في الفضاء السيبراني.....	224- 275
المبحث الأول : ضبط الصراع في الفضاء السيبراني.....	225
المطلب الأول: المعايير والقواعد لضبط الصراع في الفضاء السيبراني.....	225
المطلب الثاني:الاتفاقيات الثنائية والمتعددة الأطراف لضبط الصراع في الفضاء السيبراني	230
المطلب الثالث: ادارة المنافسة الاستراتيجية والتعايش السلمي النسخة 2.0.....	234
المبحث الثاني: سيناريو استمرار الصراع: الحرب الباردة الجديدة.	239
المطلب الأول: محركات استمرار المنافسة الاستراتيجية.	239
المطلب الثاني: الحرب الباردة النسخة الثانية (Cold War 2.0).	244
المطلب الثالث: ديناميكيات الحرب الباردة الرقمية.	251
المبحث الثالث: سيناريو التغير (السيناريو الراديكالي).	258
المطلب الأول: تفكك الفضاء السيبراني.	258
المطلب الثاني: سيناريو الحرب السيبرانية الشاملة.	265
المطلب الثالث: هيمنة الولايات المتحدة / الصين على الفضاء السيبراني.	269
الخاتمة.....	277
قائمة المصادر والمراجع	284
فهرس الموضوعات	315
قائمة الجداول	318
قائمة الأشكال	319

الرقم	العنوان	الصفحة
01	مقارنة بين مؤشرات القوة السيبرانية.	84
02	مقارنة ترتيب 10 دول الأوائل في مختلف مؤشرات القوة السيبرانية.	85
03	نسب براءات الاختراع لتقنيات 5G حسب الشركات والدول.	99
04	شركات تصنيع الرقائق المتقدمة فئة مادون 16Nm حسب البلدان.	106
05	أفضل تطبيقات الهاتف الصينية التي تقدم خدمات شبيهة بالتطبيقات الأمريكية.	118
06	حالات التهديد ومجالات الردع.	151
07	وثائق الاستراتيجيات الخاصة بالفضاء السيبراني لأهم الهيئات الأمريكية.	170

الرقم	العنوان	الصفحة
01	نموذج تمثيلي للفضاء السيبراني.	37
02	تغلغل الفضاء السيبراني عبر الفضاءات المادية والقيمية.	38
03	تحويل نموذج OSI إلى نموذج الطبقات الأربع.	56
04	التوزيع الجغرافي لأفضل 100 منصة رقمية للتجارة الإلكترونية لسنة 2021	95
05	خريطة كوابل الألياف البصرية البحرية.	101
06	خريطة الكابل البحري "السلام".	104
07	تطور سوق أنظمة التشغيل لأجهزة الكمبيوتر 2009 - 2022	115
08	تطور سوق أنظمة التشغيل للهواتف الذكية 2009 - 2022	115
09	خريطة استخدام شبكات التواصل عبر العالم - احصائيات جانفي 2022.	118
10	ترتيب الدول حسب عدد مراكز البيانات لسنة 2022.	121
11	تحولات ميزان القوى حسب الناتج الإجمالي الخام GDP	135
12	الإطار العام للبناء الرقمي في الصين (مترجم).	209

المخلص:

لطالما كان الفضاء السيبراني (الأنترنت) مشروعاً أمريكياً، قادت الولايات المتحدة تطوره منذ بدايته كمشروع لربط جهازي كمبيوتر في وزارة الدفاع إلى أن أصبح أكبر منصة استراتيجية عالمية تربط أكثر من ثلثي سكان العالم تتحكم في تواصلهم وآرائهم، تُشكل اقتصادهم وأمنهم، ومع ذلك، فإن هذه الميزات التي كانت تتدفق على واشنطن بدأت في تغيير وجهتها نحو بكين، ذلك أن صعود الصين التكنولوجي في العقد الثاني من الألفية الثالثة هدد الريادة الأمريكية وخلق تحدياً حقيقياً لقيادتها، فالصين وتحت حكم الرئيس "شي" لديها خطط كبرى لتحويل الصين إلى "قوة سيبرانية عظمى" و"دولة ذكية" كنموذج لقيادة العالم.

وعليه، تبين لنا من خلال تطبيق المقاربات الجيوبولتيكية التي أثبتت ملاءمتها وقدرتها في تفسير تجليات الصراع بين الولايات المتحدة والصين في الفضاء السيبراني عبر كل طبقاته، أن كلا القوتين تنطلقان من رؤيتهما الجيوبولتيكية وإدراكهما الاستراتيجي للفضاء السيبراني في تطوير وبناء استراتيجيات لإدارة هذا الصراع.

فالولايات المتحدة تهدف استراتيجياتها المتعددة لزيادة النفوذ والسيطرة على الفضاء السيبراني وتحقيق والحفاظ على وضع الهيمنة مع احتواء وتقيد للصعود التكنولوجي الصيني، ومن جهتها الصين تسعى من خلال استراتيجياتها للصمود وجعل الصين مركزاً رائداً للتكنولوجيا، تنطلق من خلاله نحو العالم.

كما تم التوصل إلى أن جيوبولتيكا صناعة الرقائق تتحكم في مستقبل الصراع، فعلى المدى القريب يستمر الصراع في شكل حرب باردة رقمية، وعلى المديين المتوسط والبعيد يتأرجح بين ضبط للصراع واستقرار للفضاء السيبراني، وبين هيمنة طرف وفرض رؤيته على الطرف الآخر وعلى العالم، تفكك الفضاء السيبراني، أو حدوث حرب سيبرانية تدمر الفضاء السيبراني في أسوأ الاحتمالات.

Abstract:

Cyberspace (Internet) has always been an American project. The United States led its development from its beginning as a project to connect two DoD's computers until it became the largest strategic platform in the world, this platform connects more than two-thirds of the world's population, controls their communication, opinions, shapes their economy and security. However, Cyberspace advantages that were flowing to Washington began to change direction towards Beijing. Wherefore, the technological rise of China in the second decade of the third millennium threatened US leadership and created a real challenge. Under the rule of President Xi, China has major plans to transform China into a "super cyberpower." And make a "smart country" as a world leadership model.

Accordingly, the application of geopolitical approaches has proven their suitability and ability to explain the US-China conflict in cyberspace across all its layers, it has become clear to us that both powers are starting from their geopolitical vision and strategic awareness of cyberspace to develop and build their Conflict Management Strategies.

In one hand, the US strategies aims to increase their influence and control over cyberspace, achieve and maintain a hegemonic position, while containing and restricting the Chinese technological rise. In the Other hand, China seeks, through its strategies, to remain steadfast and make China a leading center for technology, through which it will move towards the world.

At the end, we concluded that the Semiconductors geopolitics controls the future of the US-China conflict in Cyberspace. In short term, this conflict continues in the form of Cyber Cold War. However, in the medium/long term, it fluctuates between, firstly, controlling the conflict and stabilizing cyberspace, secondly, the dominance of one power and imposing its vision on the other powers and on the entire world, thirdly, the disintegration of Cyberspace. finally, a cyber war destroys the Cyberspace in the worst scenario.