مجلة العلوم الإنسانية العربية
المجلد (٣) العدد (٤)
الإصدار الحادي عشر
٢٠٢٢ (٢٨-١)

العوامل والفواعل المهيكلة لسيادة البيانات الصينية

حميل مصطفى
طالب سنة أولى دكتوراه علاقات دولية وقانون دولي، جامعة قاصدي مرباح ورقلة

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

نشر إلكترونياً بتاريخ: ١٢ ديسمبر ٢٠٢٢م

الملخص

إن الثورة الرقمية التي شهدها العالم في مطلع القرن العشرين ،أدت إلى تسارع وتيرة تدفق المعلومات والحركات التجارية الرقمية ،والمعاملات الرقمية ،وظهور المدن الرقمية و الدول الرقمية والعملات الرقمية،والدبلوماسية الرقمية حتى أصبح العالم يتحدث عن السيادة الرقمية،التي اتخذت بعدا رقميا وفضاء جغرافي وهمي بأشخاص وهميين ،يتفاعلون في فضاء سبراني مفتوح لاحدود له ولا قوانين فعالة تؤطر هذا الأخير ،كل هذه التطورات والتفاعلات سمحت ببروز تهديدات الكترونية وجرائم الكترونية،إرهاب الكتروني،عن طريق ما يسمى قراصنة الويب،عبر بث فيروسات فتاكة على غرار حصان طروادة، زومبي،دوس وستاكسنت وغيرها والتي غالبا ما تشل الحواسب وسرقة المعلومات الخاصة بالمستخدم، من اميلات ومعلومات مصنفة سرية جدا ،في وقت يتحدث فيه العالم عن السيادة الرقمية والتي يصعب بسط السيطرة عليها،و في ظل هذه التهديدات الجديدة ،ظهر النموذج الصيني الرائد في مجال السيادة الرقمية ،هذه الأخيرة التي سعت إلى تطبيق خطة الوقاية خير من العلاج وتكوين فرد شيوعي يؤمن بالصين وينبذ المنتج الغربي

الكلمات المفتاحية: الأمن السبراني، الحزب الشيوعي، الصين، الحرب الالكترونية، حوكمة النت

Abstract

The digital revolution that the world witnessed at the beginning of the twentieth century, led to the acceleration of the flow of information, digital trade movements, digital transactions, the emergence of digital cities, digital countries, digital currencies, and digital diplomacy until the world started talking about digital sovereignty, which took a digital dimension and an imaginary

geographical space. With imaginary people interacting in an open cyberspace that has no limits and no effective laws that frame the latter, all these developments and interactions allowed the emergence of cyber threats and cyber-crimes, electronic terrorism, through the so-called web hackers, through the transmission of deadly viruses such as Trojan horses, zombies, DOS and Stuxnet And others, which often paralyze computers and steal user information, from emails and information classified very confidential, at a time when the world is talking about digital sovereignty, which is difficult to control, and in light of these new threats, the leading Chinese model in the field of digital sovereignty has emerged, the latter Which sought to implement the prevention plan is better than cure, and to form a Chinese communist individual who believes, in the principle of protecting national security and being wary of every Western technological product, which according to them constitutes a threat to Chinese national security, in addition to developing local technology and achieving self-sufficiency in it, and developing data protection techniques through Hydrocoding,

Keywords: cyber security, Communist Party, China, electronic warfare, Internet governance

*** مقدمة**

غني عن البيان أن إتقان التقنيات كان دائمًا مجالًا تمارس فيه القوة الاقتصادية والعسكرية والسياسية ومع ذلك، من الشائع التقليل من أهمية الطبيعة الحاسمة لهذه السيطرة وإساءة تحديد التقنيات المعنية، إذا كان هناك اقتناع بأن إتقان تقنيات المعلومات – "التفوق ألمعلوماتي" هو اليوم أحد المحددات العالمية للقوة، وإذا تم الإدراك بسهولة أن الإنترنت هو المكان والرافعة، فإن القليل هم من يهتمون بالديناميكيات المحددة لهذه التقنيات، والطريقة التي يتم بها نشرها في مجال الدول والأنظمة التنظيمية الدولية.

في الوقت الذي تقوم فيه جميع البلدان ببناء جزء متزايد من بنيتها التحتية الاقتصادية والاجتماعية والسياسية على الإنترنت، من الضروري أن يهتم عدد أكبر من الجهات الفاعلة بالطريقة التي يتم من خلالها مباشرة التقنيات التي تشكل بنية الإنترنت بأكملها. أو بشكل غير مباشر، تطور المجتمعات والعلاقات بين الدول.

من تنفيذ أنظمة القياسات الحيوية إلى تعليم الأشياء بواسطة الرقائق الذكية والاتصال، بما في ذلك الاستخدامات المتعلقة بأنظمة تحديد الموقع الجغرافي أو تطوير الإدارة الإلكترونية، أصبح للأنظمة التقنية والمعايير التي تحكم الشبكات الآن تداعيات ملموسة على المواطنين والدول. ومع ذلك، فإن الآليات التنظيمية للإنترنت تعطي مكانًا محدودًا إلى حد ما للوائح التقليدية: في الواقع، كانت الإنترنت ولا تزال "تُدار" خارج – أو إلى جانب – النماذج التقليدية للتنظيم

الوطني وتطرح نفسها في هذا كمختبر لأشكال جديدة من الحكم

اليوم، وصلت هذه النماذج التنظيمية – الموروثة من فترة كان فيها الإنترنت فقط ربط العلماء والباحثين وطرح مشاكل السيادة لعشاق الخيال العلمي – حدودها. في عالم حيث الإنترنت على مفترق طرق لجميع الأنشطة البشرية، لم تعد القرارات التي توجه مستقبلها وتؤثر في استخداماتها تعتمد فقط على الفاعلين "التقنيين" في عصور ما قبل التاريخ الدول الأعضاء في الأمم المتحدة على تنظيم القمة العالمية لمجتمع المعلومات ولأول مرة، جمعت قمة للأمم المتحدة أطرافًا من القطاعات الرئيسية الثلاثة للإنترنت (الحكومات، والقطاع الخاص، والمجتمع المدني)، ومن ثم تم إضفاء الطابع المؤسسي على خصوصيات إدارة "شبكة الشبكات".

في نهاية المرحلة الأولى، أعدت الدول الأعضاء إعلان مبادئ، وهو أول نص ذي نطاق عالمي يكرس الحاجة إلى حكم "ديمقراطي ومتعدد الأطراف وشفاف". كان تعريف الحوكمة المعتمد في القمة واسعًا ومتطورًا بشكل متعمد الدول الأعضاء في الأمم المتحدة على تنظيم القمة العالمية لمجتمع المعلومات ولأول مرة، جمعت قمة للأمم المتحدة أطرافًا من القطاعات الرئيسية الثلاثة للإنترنت (الحكومات، والقطاع الخاص، والمجتمع المدني)، ومن ثم تم إضفاء الطابع المؤسسي على خصوصيات إدارة "شبكة الشبكات".

وتعنى "حوكمة الإنترنت"، تجاوز إدارة البنى التحتية الحيوية لتوسيع نطاقها لتشمل القضايا المتعلقة بهندسة الإنترنت. في الواقع ، كان السؤال المطروح خلال القمة هو معرفة المبادئ والقيم التي ستسود للشبكات في السنوات القادمة ، فضلاً عن الأساليب التي من شأنها أن تسمح بإدراج هذه القيم في هندسة الإنترنت، كل هذه الاحداث والتفاعلات في الفضاء السيبراني الجيبوبولتيكي الافتراضي المعلوماتي الهمي اسفر عن ظهور قوى سيبرانية رائدة وهما الصين والولايات المتحدة الامريكية، ويبقى النموذج الصيني، الاكثر قوة وفعالية على الساحة الدولية، بفضل تبني استراتيجية قوية هيكلها الحزب الشيوعي والمبادئ الشيوعية الصينية المناهضة للغرب خاصة امريكا اضافة بسط السيطرة وحوكمة الانترنت والبيانات في الصين لمنع الجوسسة والاختراقات وتطوير المواقع المحلية ونبذ المنتجات الغربية

انطلاقا من هذا المسار المقدماتي والمعطيات السابقة تطرح الاشكالية الاتية: ماهي العوامل والفواعل المؤثرة والمهيكلة للأمن السيبراني الصيني؟

تتفرع من الاشكالية الرئيسية التساؤلات الفرعية الاتية:-

١- ماهي الدوافع الصينية لبناء قوة سيبرانية فعالة في الفضاء السيبراني؟

٢- كيف لعب الرئيس تشي والحزب الشيوعي دورا رئيسا في هيكلة نظام المعلومات في الصين؟

للإجابة عن التساؤلات الفرعية والاشكالية الرئيسية تطرح الفرضيات الاتية:-

١- السعي للريادة والتحكم في مصدر المعلومة ودواليب الاقتصاد العالمي من دوافع الصين لتحقيق قوة سيبرانية

٢- سياسة الرئيس تشي والحزب الشيوعي المبنية على التحكم في المجتمع عبر التنقيط الاجتماعي، وحوكمة الانترنت كان سببا في نجاح وفقوية الامن المعلوماتي الصيني

لتحقيق لغاية الأكاديمية من الدراسة توظف المناهج والاقتراحات الاتية:-

ومن اجل التعمق الأمثل في فهم ودراسة الموضوع سيتم توظيف **مقاربة الأمن ألمعلوماتي** الخاص بالفضاء الالكتروني، والتي تركز في تحليلها على تحليل ثلاث جوانب جوهرية ،وهي والجانب الخاص بالمعلومات إضافة إلى الجانب الثالث والمتمثل في التطبيقات **والبرامج** الالكترونية والتفاعلات الالكترونية في الفضاء الجغرافي السبراني الوهمي، ومن رواد هذه المقاربة من مدرسة كوبن هاقن المنظر باري بوزان الذي ،حدد عدة مستويات للأمن مع تطور التهديدات الجديدة العابرة للحدود والقارات، ومن بين أنواع الأمن التي حددها الأمن الصحي ،الثقافي السياسي،الغذائي والأمن الالكتروني أو السبراني وهذه المقاربة تسعى لدراسة الفواعل والعوامل المؤثرة المسببة للتهديدات السبرانية و دينامكيتها وكيفية ادراكها قبل وأثناء وبعد وقوع التهديد أو الجريمة الالكترونية.

ومن رواد أيضا المقاربة جوزيف ناي الذي تحدث عن القوة **الناعمة** والتي خصص جانبا منها للتحدث عن الأمن الالكتروني والحروب الالكترونية والصراعات السبرانية، خاصة بين الولايات المتحدة الأمريكية والصين.

كما سيتم توظيف **المنهج التحليلي الوصفي** الذي يرتبط في كثير من **الأحيان** بالأبحاث العلمية، ويستخدم المنهج الوصفي التحليلي عن طريق ملاحظة الباحث لمشكلة أو ظاهرة علمية، والشروع في وصفها بأسلوب علمي دقيق، ومن ثَمَّ يقوم الباحث بجمع البيانات والمعلومات عنها، ويلي ذلك مرحلة صياغة أسئلة البحث، وتبويب وتحليل البيانات عن طريق الطرق الإحصائية المتنوعة، والخروج بنتائج تساعد على إيجاد حلول للمشكلة، أو استنباط نظرية جديدة يمكن تعميمها ،سيتم توظيف هذا المنهج من اجل وصف وتحليل السيادة الرقمية واهم التحديات التي تجابه هذه الأخيرة خاصة مع تنامي الهجمات الالكترونية الفتاكة.

المنهج الإحصائي: اللغة الرقمية مهمة في الأبحاث، لذلك يوظف المنهج الإحصائي لدراسة الظواهر رقميا،وإعطاءها الدقة العلمية والمصداقية،بالتالي سيتم توظيفه في هذه الدراسة لدراسة،موضوع رهانات السيادة الرقمية في الصين،معرفة باللغة الرقمية ما حققته الصين،في مجال المدن الرقمية،والصناعة التكنولوجية،حتى أصبحت قوة سبرانية رائدة في العالم.

المنهج التاريخي:وهو منهج يهتم بدراسة الظواهر تاريخيا أي تاريخ ظهور الظاهرة وتطورها ،في هذه الدراسة سيتم توظيفه لمعرفة،تاريخ تطور السيادة السبرانية،وتاريخ الاهتمام الصيني بهذا المجال،وكيف تطور إلى أن أصبحت الصين لما عليها الآن.

المقاربة البنيوية الوظيفية: تعتمد هذه النظرية على تحليل الظاهرة في بنيتها وتركيبتها وكذلك وظيفتها وتفاعلها على المستوى الداخلى والخارجي،ومن رواد النظرية،سبانسر وطالكوت،وفي هذه الدراسة سيتم توظيفها لمعرفة تركيبة الفضاء السبراني الذي بدور حوله الصراع بين الصين والولايات المتحدة الأمريكية،وظيفة سيادة البيانات في تحقيق القوة السبرانية للصين

الاقتراب النسقي: ومن رواده دافيد ايستن،يعتمد على دراسة المدخلات و المخرجات النظام السياسي او للظاهرة السياسية،في هذه الدراسة سيتم توظيفه لمعرفة المدخلات التي أثرت على الصين لهيكلة نظامها الاتصالي ،مثل المعتقدات ونبذ المنتج الغربي كل هذا اثر على النسق واخرج مخرجات هي

العمل على تحقيق الاكتفاء التكنولوجي ،وحوكمة الانترنت وتحقيق سيادة البيانات.

المنظار الابستمولوجي والتحليل المركب: ومن رواد هذا الاقتراب باشلار،ويعتمد على دراسة الظاهرة ونقدها علميا وكشف الجانب الخفي في الظاهرة،والفواعل والعوامل المؤثرة فيها وديناميكيتها،في هذه الدراسة سيتم توظيفها لمعرفة،أسباب الاهتمام الصيني بالسيادة الرقمية ،وكيف حققت شوطا كبيرا في هذا المجال،اهم الفواعل والعوامل المتحكمة في نظامها الاتصالي وكيف هيكلته.

نظرية الدور: يعتبر المنظر هولستي الأب الروحي للنظرية ،وهي تقوم على أساس أن الدولة لديها محددة داخلية ومقومات اقتصادية اجتماعية سياسية عقائدية تؤمن بها ما ينعكس ويؤدي بها وعلى أساسها دورا في السياسة الخارجية وعلاقتها مع الدول،من هذا المنطلق وفي موضوع السيادة السبرنية في الصين من الاهمية بمكان معرفة أن الصين بمنطق عقيدتها الشيوعية ونبذها للغرب خاصة الولايات المتحدة الأمريكية،مكنها من لعب دور في الفضاء السبراني،وفرض منطقها الرامي لحوكمة الفضاء السبراني لكي لا يكون حكرا على الفواعل غير دولتية

تم طرح الموضوع في قالب منهجي اين تم تناول العناصر الاتية:-

١- إطار نظري خاص بالفضاء السبراني والمصطلحات المرتبطة به

إن مصطلح الفضاء الالكتروني يعود إلى رواية ويليام جيبسون الذي قدم الفضاء الالكتروني بثلاث أبعاد افتراضية كما إن هذا الأخير غير مستقر بل في دينامكية دائمة ويتفاعل الناس فيه بشكل مستمر لذلك جذب هذا المجال العديد من المنظرين في مجال العلاقات الدولية للبحث فيه سيتم حصر أهم تصورات المنظرين لهذا المجال فيما يلي:-

١- جوزيف ناي يرى أن الفضاء السبراني فريد من نوعه مرتبط بالتكنولوجيا والقوة الالكترونية حسبه تؤثر على المجالات الاخرى

٢- الواقعية الجديدة ترى بانه ضابط للعلاقات الدولية الجديدة في توزنات القوة فالقوة التكتولوجية تحدد مدى قوة الدول واتخذ استرتجية الدفتع والهجوم وهذا ما ركز عليه جيرفيس

-اللبيرالية الجديدة ترى بان الفضاء السبراني يضعف الدول لظهور فواعل غير دولاتية تضعف سيادة الدول

٣- البنائيون ركزو على ضرورة بناء قيم تظبط الفضاء الالكتروني لحماية الدول من الهجومات والجوسسة الالكترونية[1]

ومحاوله لتلخيص وجهات نظر المدارس والمنظرين بالنسبة للفضاء السبراني فكلهم يتفقون على ان الفضاء السبراني مجال تبادل وتفاعلات بين الدول والمنظمات

[1] -السيادة السيبرانية في الصين بين متطلبات القوة وضروريات ألأمن القومي مقال-سميرة شرايطية-جامعة المجلة الجزائرية للأمن و التنمية. مج. 9، ع. 1 (كانون الثاني 2020)، ص ص. 396-410، 15ص

والموطنين ولكن يبقى الصراع قائما حول من يتحكم بهذا الفضاء الالكتروني فالمعلومة مهمة هنا كما قال الاستراتيجي كلوزفيتس من يتحكم في المعلومة بتحكم في الحرب لهذا تحدث حروب الكترونية وهجومات وجوسسة من قبل جهات معروفة اوغير معروفة سعيا من كل واحدة قلب موازين القوى في العلاقات الدولية واعادة رسم منظر وفظاء جيوبوليتيكي جديد تكون فيه الغلبة للذي يصنع المعلومة والتكتولوجيا ويتحكم فيها.

لقد أدى ظهور شبكة الإنترنت والفضاء الإلكتروني وتطورهما إلى إحداث ثورة تكنولوجية قي المجتمعات الانسانية المختلفة والأعمال التجارية والأعمال الحكومية في العالم ، وفي العقد الماضي برز الفضاء الإلكتروني بوصفه بؤرة مخاوف تتعلق بالأمن فتضاعفت التهديدات التي يواجهها أمن الفضاء الإلكتروني ، وتعاظمت تكاليف الاستجابات المناسبة لها بسرعة تفوق قدرة الحكومات على التعامل معها ،ان تأثير الثورة التكنولوجية والمعلوماتية في مسرح العمليات الحربية والعسكرية اصبح كبيرا، اذ أصبحت تقنية المعلومات مصدراً مهماً وأساسياً لتحقيق ميزة تنافسية في الميدان العسكري .

زادت العلاقة بين الحرب والتكنولوجيا وثوقاً مع إمكانية تعرض المصالح الإستراتيجية للدول للخطر الالكترونية الى أخطار بتحول الفضاء الالكتروني الى ساحة للصراع والحروب الدولية المقبلة

خاصة بعد دخول الدول ككل في مرحلة جديدة تلعب فيها الهجمات عن طريق الفضاء الالكتروني دوراً محوريا مهماً سواء من خلال تعظيم القوة أو الاستحواذ على أهم عناصرها ، واصبحت الدول في وضعية هشة وحرجة رغم على الرغم من التشريعات أو الهيئات المراقبة.

على الرغم من ان التقدم التكنولوجي له دور في دعم القطاعات الدفاعية والعسكرية والقيادة ورفع الكفاءة القتالية من خلال التدريب الحديث واستخدام الكومبيوتر في تطبيقات بحوث العمليات وايصال المعلومات بدقة وسرعة ، إلا أن وفرة تكنولوجيا المعلومات على وجه الخصوص ، يعد من الوسائل المبتكرة للغاية لممارسة التجسس على اختلاف أنواعه ، فأستبدل الجاسوس التقليدي البشري بالأجهزة العلمية الدقيقة كالاقمار الصناعية وطائرات الاستطلاع أي تمارس مهمة التجسس من الفضاء ، وتبعاً لذلك عرف كوينسي رايت الحرب تعريفاً مركباً مطوراً النظرية الأساسية للحرب موضحاً أن التكنولوجيا واحدة من اهم العوامل المؤثرة في الحروب والتي تتوافق مع المستويات التكنولوجية والسياسية والقانونية والبيولوجية والنفسية والاجتماعية والثقافية من حياة الانسان وتوجيهات القيادة العسركية فالصراع محتمل وتصبح الحرب حسب كوينسي رايت محتملة وطبيعية ومسرح للعمليات والهجومات والحروب الالكترونية[2]

١- الدوافع الصينية للاهتمام بالقوة السيبرانية

بذل الرئيس الصيني "شي جين بينغ" والحكومة المركزية جهداً كبيراً منذ عام 2012 للتوصل إلى نهج شامل وإعداد هيكل تنظيمي لأمن الشبكات، وفي هذا الإطار تم إنشاء لجنة الأمن القومي، ومجموعة قيادية مركزية لأمن ومعلومات الإنترنت يترأسها الرئيس الصيني وعلى الرغم من

[2]-المرجع نفسه

جهود بكين الجارية لتنظيم ودعم البنية التحتية لأمن الشبكات والمعلومات، فإن هذه الجهود لا تزال مشتتة، ويرجع ذلك إلى تعدد القطاعات والهيئات الإدارية المسؤولة مثل: (مكتب إدارة التشفير لأمن الدولة، ولجنة الأمن القومي، وجيش التحرير الشعبي.. وغيرها من الجهات)، فضلاً عن وجود تداخل وتضارب في المصالح بين بعضها البعض في كثير من الأحيان.[3]

وتوضح الدراسات وجود اختلاف بين واشنطن وبكين في تعريف عدد من المصطلحات المعنية بموضوع الفضاء والأمن الإلكتروني، الأمر الذي يتسبب في وجود فجوة إدراكية، خاصةً فيما يتعلق بتحديد معنى الأمن الإلكتروني (السيبراني)، وأمن الشبكات والمصطلحات الأخرى ذات الصلة. وتضيف الدراسة أن الإستراتيجية الصينية لأمن الشبكات تتضمن استخدام المعلومات للتأثير أو السيطرة على عملية صنع القرار لدى الأعداء وما يترتب عليها من أنشطة، وذلك لخدمة الأهداف الصينية الهجومية والدفاعية تعد أوسع نطاقاً من الرؤية الأمريكية في مجال الأمن الإلكتروني، حيث تعتبر المبادرة الأمريكية الوطنية الشاملة للأمن الإلكتروني[4]،

والتي انطلقت في يناير عام 2008، أكثر محدودية في نطاقها، إذ تركز على تعزيز القدرات الدفاعية التكنولوجية والبشرية[5]

تُفسر الدراسة السياسة الخارجية للصين، بما في ذلك نشاطها الإلكتروني (السيبراني)، في ضوء سياستها، وحماية واستمرار قوة **الحزب** الشيوعي الصيني الرامية لضمان استقرار الصين الداخلي وسلامة أراضيها وتحقيق التحديث والنمو الاقتصادي والحد من الاضطرابات الاجتماعية والاقتصادية، والاستعداد في نفس الوقت لاحتمال نشوب نزاع عسكري إلكتروني في المستقبل، كلها تمثل أهدافاً تدعم بشكل مباشر أو غير مباشر استمرار حكم الحزب الشيوعي الصيني، ومن ثم، تتمثل المحفزات الصينية في مجال الفضاء الإلكتروني، في الآتي:-

١- اقتصادياً: القرصنة والجرائم الإلكترونية تشمل الدوافع الاقتصادية للإستراتيجية الصينية لأمن الشبكات هدفين رئيسيين، هما: ضمان استمرار النمو الاقتصادي، وردع الجرائم الإلكترونية المحلية. وفيما يتعلق بالتجسس الإلكتروني الصناعي والذي يرتبط بالحصول على المعلومات الاقتصادية الصناعية بما في ذلك الأسرار التجارية الخاصة بالبحث والتطوير والإنتاج، فقد أشارت الدراسة إلى أن ذلك يحدث على نطاق واسع من قِبَل الصين، وأنه يكلف الولايات المتحدة خسائر تُقدر بالمليارات، وقد وصف مكتب الولايات المتحدة لمكافحة التجسس (NCIX) في تقرير صادر حول التجسس الإلكتروني الخارجي، القائمين على الجهات

[3] https://futureuae.com/m/Mainpagevue le07-07-2022a14H18min

[4] Amy Chang, Warring State: China's Cybersecurity Strategy Washington, Center for a New American Security, December 2014

[5] Op-cit

الإلكترونية الصينية، بـــ"الجناة الأكثر نشاطاً واستمرارية في مجال التجسس الاقتصادي ونظرا لصعوبة قياس الآثار المترتبة على هذه الجرائم، فمن الصعب معرفة المدى الحقيقي للجريمة الإلكترونية والتجسس الإلكتروني الصيني. ومن ناحيتها، تستمر الصين في دحض هذه الاتهامات، مُصرةً على أن الدولة لا تدعم أي نشاط متعلق بالقرصنة

٢- سياسياً: السيادة الصينية في مجال الفضاء الإلكتروني فيما يتعلق بالدوافع السياسية، تؤكد الكاتبة أن الحكومة الصينية تخشى من إتاحة استخدام الإنترنت دون قيود، ومن عدم السيطرة على عملية تدفق وانتشار المعلومات خاصةً من قِبَل المعارضة، الأمر الذي قد يشكل خطراً كبيراً على استقرار النظام الشيوعي الصيني وعلى السلطة الحاكمة، لذلك قامت الصين بتطبيق تدابير وقائية في إطار تبني مفهوم "احترام السيادة الصينية في مجال الفضاء الإلكتروني"، والذي من شأنه أن يسمح لبكين بالسيطرة على الإنترنت داخل حدود الدولة، في حين أن المفهوم الغربي للفضاء الإلكتروني يتبنى نهجاً مُنفتحاً من خلال التدفق الحر للمعلومات عبر الحدود[6]

وفيما يتعلق بالشؤون الخارجية، تقوم الحكومة الصينية بتوظيف جهات غير حكومية – أو على الأقل لا تمنعها – للقيام بأنشطة إلكترونية ضد الخصوم، تشمل التجسس الإلكتروني في المجالات المختلفة الاقتصادية والصناعية والعسكرية. ونظراً لعدم إمكانية إثبات وجود علاقة بين المؤسسات الحكومية والجهات الفاعلة التي ترعاها الدولة في هذا المجال، لذلك فمن الصعب إلقاء اللوم على الحكومة الصينية ومقاضاتها وفقاً للقانون الدولي في هذا الشأن

٣- عسكرياً: تذكر الدراسة أن الصين قامت باستخدام شبكة الإنترنت وتكنولوجيا المعلومات في المجال العسكري منذ عدة عقود، ولكن نقطة التحول الرئيسية في النهج الصيني حدثت بعد استخدام الولايات المتحدة للتكنولوجيا العسكرية المتقدمة في حرب الخليج، فمنذ ذلك الحين ركزت بكين على تكنولوجيا المعلومات والاتصالات من أجل توظيفها في الحروب المستقبلية، وتطمح في احتلال موقع متقدم في هذا المجال بحلول عام2050 وتضيف الدراسات أن الصين قد عملت على ترسيخ أُسس إستراتيجية الأمن الإلكتروني في العلوم والأدبيات على غرار العلوم العسكرية والإستراتيجية، والأوراق البيضاء للدفاع الحكومية، إضافة لمبادرة التاريخ الجديد لهوجين تاو[7]

ومن خلال هذه العلوم والأدبيات العسكرية، بحث العسكريون في استراتيجيات تُمكنهم من استغلال المجال الإلكتروني في مختلف السيناريوهات الهجومية والدفاعية. وتشير الكاتبة إلى أنه بسبب اختلاف الثقافات الإستراتيجية، فإن العلوم والأدبيات العسكرية لا تميز بوضوح في هذا المجال بين التدابير الدفاعية والهجومية، وبالتالي فإن ما قد تعتبره الصين آليات دفاعية، قد يتم تأويله على أنه آليات هجومية

[6] Op-cit

[7] Amy Chang, Warring State: China's Cybersecurity Strategy Washington, Center for a New American Security, December 2014

في الولايات المتحدة وغيرها من الدول الغربية ويتوقع أن تلعب العمليات العسكرية الإلكترونية دوراً هاماً في السيناريوهات العسكرية المتعلقة بتايوان، والنزاعات الإقليمية والبحرية الأخرى، وكذلك ضد الولايات المتحدة. وقد أشارت العديد من التقارير الخاصة بالتهديدات المتقدمة المستمرة الصادرة عن شركات الأمن الإلكتروني الأمريكية إلى تطور مستوى الهجمات الإلكترونية الصينية ضد الحكومة والمؤسسات الصناعية والتجارية الأمريكية، على الرغم من استمرار نفي الصين لهذه الاتهامات.[8]

تعتبر الصين إستراتيجية الأمن الإلكتروني الأمريكية بمثابة تهديد للمصالح الصينية، حيث يبرز العديد من المحللين الصينيين كيفية استخدام واشنطن لتكنولوجيا الشبكات والمعلومات للتدخل في الشؤون الداخلية للدول الأخرى، وكيف تهدد الهيمنة الأمريكية الإلكترونية الأمن الصيني في المجالات المختلفة، ومن المؤشرات التي تستدل بها الصين على ذلك، إعلان الولايات المتحدة في يوليو 2011 أن الفضاء الإلكتروني أصبح مجالاً جديداً للحرب، فضلاً عن تسريبات "سنودن" الاستخباراتية في مايو ويونيو 2013[9]، علاوة على اتهام وزارة العدل الأمريكية خمسة من ضباط "جيش التحرير الشعبي الصيني" بتهمة التجسس الاقتصادي في مايو2014

لذا وضعت الصين في مقابل هذه التحديات أهدافاً رئيسية لتعبئة الحرب الإلكترونية في بكين، من أبرزها تدريب الموظفين العسكريين والمدنيين على الحروب الإلكترونية، وتشكيل وحدات حربية ووحدات احتياط متخصصة في مجال الفضاء والأمن السيبراني وكذلك خلق مواقع خاصة بالين على غرار بايدو، على بابا وتانسنت[10]

قامت الصين بتعديل رؤيتها التي وضعتها في وقت سابق، والتي تمثلت في أن قوانين النزاع المسلح لا تنطبق على عالم الفضاء الإلكتروني (الإنترنت)، وكعضو في مجموعة الخبراء الحكوميين التابعة للأمم المتحدة – المختصة بدراسة وبناء قواعد الفضاء المعلوماتي – وافقت بكين على الالتزام بالقانون الدولي في مجال الفضاء الإلكتروني، وفقاً لتقرير يونيو 2013 الصادر عن فريق الخبراء الحكوميين

وعلى الرغم من أن ذلك أُعتبر مؤشراً على حدوث تغير في الموقف الصيني، وقبول بكين وتوافق رؤيتها مع المعايير الغربية، فإن تقرير الخبراء الحكوميين عاد وأكد في أجزاء أخرى منه تشبث الصين بمبدأ سيادة الدولة على الأنشطة المتعلقة بتكنولوجيا المعلومات والاتصالات، وهو ما أكدته الصين في اجتماع الدائرة المستديرة مع كوريا الجنوبية حول الفضاء ألمعلوماتي والإنترنت في شهر ديسمبر من نفس العام،

[8] https://futureuae.com/m/Mainpage/Item/684/%D8%A7%D9%84%D82022a14H18min

[9] https://futureuae.com/m/Mainpage/Item/%B186%D9%8Avue le07-07-2022a14H18min

[10] Hauke ,Johannes Gierow(April 2015). Cyber Security in China: Internet Security, Protectionism and Competitiveness: New Challenges to Western Businesses, mercator institute forchina studies pp1-10

وألان الصين تمكنت إلى حد كبير من كسب القبول الدولي لرؤيتها وإستراتيجيتها في مجال الفضاء الإلكتروني خاصةً مع الدول التي تشاطرها نفس الآراء، مع تفضيل الحكومة الصينية تجنب التعاون مع واشنطن، وذلك يرجع لثلاثة أسباب رئيسية، وهي:-

١- تصور بكين بأن السعي لإقامة علاقات تعاونية تتمتع بالشفافية مع الولايات المتحدة، يتعارض مع أولويات الحكومة الصينية

٢- لاحظت الصين استمرار حرص الولايات المتحدة على التعاون وتبادل المعلومات حول إستراتيجية الصين السيبرانية، دون ضمان المعاملة بالمثل[11]

٣- خسارة الولايات المتحدة لمكانتها القيمية، بعد واقعة تسريبات "سنودن" الاستخباراتية، الأمر الذي أعطى الصين المبرر لتأخير أو رفض أي طلبات متعلقة بتعديل توجهاتها في مجال الفضاء الإلكتروني[12]

*** الحزب الشيوعي تحت قيادة الرئيس تشي فاعل مؤثر ومهيكل للسيادة السيبرانية الصينية**

طيلة خمسة عقود تقريبا، كانت الولايات المتّحدة هي مَن يقود نمو الإنترنت، وصولا إلى المنصات الحالية العالمية التي تربط أكثر من نصف سكّان العالم وعشرات المليارات من الأجهزة بعضهم ببعض، عُرف الإنترنت على الدوام كمشروع أميركي، أما اليوم، فقد تنازلت الولايات المتّحدة عن ريادة الفضاء السيبراني إلى الصين، إذ أعلن الرئيس الصيني تشي جين بينغ عن مخططاته تحويل الصين إلى "قوة سيبرانية عظمى، والأمر يحدث بالفعل، فالصين تُتيح من اتصال الإنترنت لمواطنيها أكثر مما يفعل أي بلد آخر، لكنّ تشي لديه مخططات أكبر من ذلك بكثير. فمن خلال "منيع"، وإعلاء كلمتها في حكم الإنترنت، وتقديم الرعاية لمزيد من الشركات ذات الطراز العالميّ، وريادة العالم في التكنولوجيّات المتقدّمة غير أنّ صعود الصين المتواصل كقوة سيبرانية عظمى ليس بالأمر المضمون، فالجهود التي تبدأ من القمة وتنتهي بالقاعدة التي تقودها الدولة في ابتكارات الذكاء الصناعي، والحوسبة الكميّة، والروبوتات، وتقنيات واعدة أخرى، قد تبوء بالفشل، حيث ستواجه شركات التكنولوجيا الصينية ضغوطا سياسية واقتصادية مع انفتاحها على العالم. وبرغم الظاهر من توقعات قليلة للصينيين من حكومتهم فيما يتعلق بالخصوصية، فإنهم قد يطالبون الشركات الخاصة ببذل المزيد في هذا الشأن. لتُعيد الولايات المتحدة تنشيط دبلوماسيتها الرقمية الخاصة عندئذ، وقد يُعيد اقتصاد الولايات المتحدة اكتشاف الديناميات التي مكّنته من خلق الشيء الكثير من تكنولوجيا العالم الحديث لكن بالنظر إلى حجم الصين وتقدُّمها التكنولوجي، فثمة إمكانية واردة لنجاح بكين، وبالتالي لأن تُعيد تصميم الفضاء السيبراني على صورتها. إن حدث الأمر فسيكون الإنترنت أقل عالمية وانفتاحا، حيث سيجري جزء كبير منه عبر تطبيقات صينية على أجهزة رقمية مصنعة في الصين، وهو ما سيُمكّن الصين من الظفر بالغنائم الاقتصادية،

[11] https://futureuae.com/m/Mainpage/ItemAvuele07-07-2022a14H18min

[12] Ibem

والدبلوماسية، والمرتبطة بالأمن القومي، والاستخباراتية التي تدفقت ذات يوم إلى واشنطن

تقريبا، منذ اللحظة التي تسلّم فيها مقاليد السلطة عام 2012، أوضح تشي الدور الكبير الذي لعبه الإنترنت في رؤيته للصين. بعد سنوات من الجمود، كانت خلالها السياسة السيبرانية مبعثرة بين باقة واسعة من الأقسام الحكومية، أعلن تشي أنه سيرأس ما أسماه مجموعة قيادة مركزية لأمن الإنترنت والمعلومات وأنه سيقود السياسة السيبرانية إلى الأعلى[13]

فأسس وكالة جديدة، هي "إدارة الفضاء السيبراني الصينية"، وأوكل إليها مهمة السيطرة على محتوى الإنترنت، ورعاية الأمن السيبراني، وتطوير الاقتصاد الرقمي.

إن القوة السيبرانية هي العقدة التي تربط أربع أولويات قومية للصين ببعضها. الأولى، هي رغبة القيادة الصينية بضمان إنترنت متناغم، وهذا يعني شبكة عنكبوتية تقود الرأي العام، وتؤازر الحكم الرشيد، وترعى النمو الاقتصادي، على أن تكون في الوقت نفسه تحت السيطرة بهدف إحباط التعبئة السياسية ومنع تدفق المعلومات التي يمكن أن تقوّض النظام الحاكم ثانيا، تريد الصين أن تُقلّل اعتمادها على المزود الأجنبي في مجال المعدّات الرقمية ومعدّات الاتصال، وتأمل أن تتمكّن في النهاية من ريادة العالم في مجال التكنولوجيات المتقدمة مثل الذكاء الاصطناعي، والحوسبة الكمية، والروبوتات، كما أشار الرئيس تشي في مايو/آيار 2018 حينما قال: "إن مبادرات الإبداع والتطوير ينبغي أن تظل آمنة في قبضتنا[14].

ثالثا، إن قلق صناع السياسة الصينيين، كما هو حال أندادِهم حول العالم، من أن تؤدي الهجمات السيبرانية على الشبكات الحكومية والخاصة إلى تعطيل خدمات حساسة، وتُلحق الضرر بالنمو الاقتصادي، وأن تُسبِّب الدمار المادي، في ضوء ذلك، أعلن جيش التحرير الشعبي الصيني التركيز على الأمن السيبراني

يعتقد صناع السياسة الصينيون أن عليهم خفض اعتماد الصين على شركات التكنولوجيا الأميركية لكي يضمنوا أمنها القومي، وهو اعتقاد تقوّى عام 2013، عندما كشف إدوارد سنودن، المتعاقد السابق مع وكالة الأمن القومي، بأن وكالات الاستخبارات الأميركية قد انتهكت خصوصية بيانات ملايين من الناس التي بحوزتها والتي تنقلها لشركات داخل الولايات المتحدة وبهذا وضعت الصين مخططا لتسريع وتطوير قواها السيبرانية وتحسين شبكاتها الدفاعية.

هذه الأحداث والتفاعلات أدت بالصين لبلورة مفهوم "السيادة السيبرانية" كمبدأ تنظيمي لحكم الإنترنت[15]، في تعارض مباشر مع الدعم الذي توفره الولايات المتحدة

[13] https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web vue le 07-07-2022a14h25min

[14] Op-cit

[15] . Kolton, Michael. Inter pretng. (Winter 2017). China's Pursuit of Cyber Sovreignty and its Vies

للإنترنت العالمي، المفتوح، على حد تعبير تشي، فإن السيادة السيبرانية تُمثِّل "حق كل دولة باختيار طريقها الخاص إلى التنمية السيبرانية، وأسلوبها في التنظيم السيبراني وتنظيم السياسات العامة للإنترنت، والمشاركة في حكم عالمي للفضاء السيبراني بحيث تكون على قدم المساواة مع الدول الأخرى، إنّ الصين تتصور عالما مبنيا من شبكات إنترنت قومية، يتم تبرير السلطة الحكومية عليه بالاستناد إلى الحقوق السيادية للدول، كما أنها تريد إضعاف نموذج الإنترنت الذي يبدأ من القاعدة وينتهي بالقمة، والذي تقوده شركات القطاع الخاص عبر الولايات المتحدة وحلفائها، وهو نموذج ترى الصين أنّ شركات التكنولوجيا ومنظمات الحقوق المدنية الغربية تُهيمن عليه، ويؤمن صناع السياسة الصينيون أن من الممكن أن تكون لهم الكلمة العليا في تنظيم تكنولوجيا المعلومات وتحديد القواعد العالمية للفضاء السيبراني إن لعبت الأمم المتحدة دورا أكبر في حكم الإنترنت فالأولويات جميعها تتطلّب من الصين التصرف بحزم لتشكيل الفضاء السيبراني داخل البلاد وعلى المسرح العالمي[16]

وضع الرئيس تشي رفقة الحزب الشيوعي الفاعل في السيادة السيبرانية الصينية ، حدًّا لتفاؤلية الغرب بشأن إمكانية تحرير الإنترنت والسيطرة عليها وعلى بيانات الشركات والمستخدمين وتوظيفها كوسيلة ضغط، لقد قامت بكين وعلى مدار السنوات الخمس الماضية، بتضييق الخناق بقوة على المواقع الإلكترونية ووسائل التواصل الاجتماعي وتأسيس والمحلية على غرار تانسنت وبايدو ،هذه المواقع التي استُخدمت على نطاق واسع من قِبل الأعمال التجارية، ورواد المشاريع، والأكاديميين الصينيين، بهدف الالتفاف على الرقابة الحكومية، هذا الإجراء انطبق أيضا على الشركات الغربية، فعلى سبيل المثال شركة ايبل، حذفت خيار الشبكات الافتراضية الخاصة من النسخة الصينية ومتجرها.

كما أن بكين قد أعلنت عن تنظيمات ولوائح جديدة بهدف الحدّ بشكل إضافي من إمكانية التصفح بحسابات مجهولة عبر الإنترنت عبر تحميل القائمين على المنتديات الإلكترونية مسؤولية مساهمات الأعضاء[17]

إن الرقابة الصينية اليوم بارعة في تقليم المحادثات عبر وسائل التواصل الاجتماعي،،ففي عام 2017، ومع تفاقم مرض المعارض والمثقف الصيني الفائز بجائزة نوبل ليو شياوبو، كشفت الرقابة الصينية أنها قد تمكّنت من مسح صوره من المحادثات الدائرة حوله ،كما تم كشفت السلطات

on Cyber Deterrance. The Cyber Defense Riview vol2. 01.pp119-154.

16 https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web vue le 07-07-2022a14h25min

17 https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web vue le 07-07-2022a14h25min

عن نظام معقد للمراقبة يتألف من باقة ضخمة من الكاميرات والمجسات، المزودة ببرنامج لتمييز الوجوه والأصوات والذكاء الاصطناعي، وقد وظّفت الأداة بصورة أكبر في إقليم سنجان، ضمن جهود الصين لتعقّب المسلمين الإيغور هناك، لكن الحكومة تعمل على استخدامه على نطاق البلاد، بالإضافة إلى توظيف رقابة المحتوى والمراقبة، خلقت الصين أيضا إطارا متشابكا من القوانين، واللوائح، والمعايير، لزيادة أمنها السيبراني وحراسة بياناتها في الأنظمة الحكومية والخاصة على حدٍّ سواء، فاتخذت الحكومة إجراءات لحماية البنية التحتية الحساسة للإنترنت، إذ أمرت بالقيام بمراجعات أمنية لمنتجات وخدمات الشبكة، كما أنها تطلب من الشركات بأن تُخزِّن بياناتها داخل الصين

حيث ستواجه الحكومات الإقليمية عقبات بسيطة في الوصول إليها، كما قامت بكين بتقديم لوائح جديدة تتعلق بطريقة استجابة الوكالات الحكومية لحوادث الأمن السيبراني، وكيف ومتى ستتمكّن الحكومة من الإفصاح عن نقاط ضعف البرنامج إلى القطاع الخاص، وكيف سيشارك كلٌّ من الوزارات والشركات الخاصة المعلومات المتعلقة بالتهديدات بإمكان الوكالات والحكومات الإقليمية المختلفة ترجمة وتنفيذ هذه السياسات بطرق مختلفة أيضا، لكن على الأقل، فإن هذه اللوائح سترفع كلفة وصعوبة إجراء الأعمال التجارية لشركات التكنولوجيا المحلية والخارجية على حدٍّ سواء، كانت مسودة التنظيمات المنشورة في يوليو/تموز 2017 فضفاضة على نحو لافت، بحيث لم يُشِر تعبير "البنية التحتية الحساسة" فقط إلى الفئات التقليدية مثل شبكات الاتصال، والمالية، والطاقة، ولكن أيضا شركات الإعلام، والرعاية الصحية، ومزوّدي حوسبة السحاب[18].

يعتقد صناع السياسة الصينيون أن تحقيق الأمن فعلا يتطلّب من الصين تحقيق الاكتفاء الذاتي التكنولوجي، ولا عجب، أن يكون دعم العلم والتكنولوجيا أوّليا ومركزيا في أحدث خطّة خمسية وضعتها للبلاد، والتي بدأت عام 2016، فقد تنامى استثمار الصين في البحث والتطوير بنسبة 20% منذ عام 1999، وهو يقع الآن عند 233 مليار دولار أميركي، أي إنه يُشكِّل نسبة 20% من الإنفاق العالمي في مجال البحث والتطوير، يتخرج من طلاب تخصصات العلوم والهندسة بالصين ما يفوق أي بلد آخر في العالم، وفي عام 2018، حلّت الصين مكان الولايات المتحدة الأميركية في إجمالي عدد المنشورات العلمية، لطالما تجاهل العلماء الغربيون الأبحاث الصينية، لكنّهم في الوقت الحالي يستشهدون بها بأعداد متزايدة

هناك ثلاث تكنولوجيات سيكون لها الثقل الأكبر في قدرة الصين على تشكيل الفضاء السيبراني الصيني: أشباه الموصلات، والحوسبة الكمية، والذكاء الاصطناعي. طيلة سنوات، كانت الصين تحاول وتفشل في بناء صناعة قومية من أشباه الموصلات، وهذه القطع هي الدارات المدمجة أو "الرقائق متناهية الصِّغر" التي نجدها في كل جهاز تكنولوجي تقريبا، في عام 2016، قامت الصين باستيراد ما قيمته 228 مليار دولار أميركي من هذه القطع -أكثر مما أنفقته في استيراد النفط- والتي يُشكِّل شقها المستورد نسبة 90% من الاستهلاك الصيني، وفق شركة ماكنزي للاستشارات.

[18] Op-cit

وخطورة الاعتماد على المزودين في الولايات المتحدة قد تحقّقت في إبريل/نيسان 2018 حينما قامت إدارة ترامب بفرض عقوبات على"ZTE" ، رابع أكبر مشغّل لأشباه الموصلات، إذ تعتمد "ZTE" على القطع المصنّعة في الولايات المتحدة، بما فيها الرقائق متناهية الصّغر لتشغيل محطات الاتصال اللاسلكي لديها[19]، وعندما حالت العقوبات بين الشبكة ومزوّديها، اضطرت الشركات لإيقاف عملياتها الكبرى. في يونيو/حزيران 2018، عَدَل ترامب عن موقفه من العقوبات، لكن الأمر لم يكن كافيا لتهدئة المخاوف الصينية من الاعتماد على المزودين الأجانب. بعد الإعلان عن العقوبات بوقت قصير، دعا تشي لاجتماع ضمّ أبرز علماء البلاد بهدف إحراز اختراقات في مجال التكنولوجيات الدقيقة[20] .ففي عام 2015، أصدرت الصين إرشادات تهدف إلى دفع الشركات الصينية لإنتاج 70% من الرقاقات الدقيقة التي تستخدمها الصناعات الصينية بحلول عام 2025، منذ ذلك الحين، وفّرت الحكومةُ الدعمَ للشركات المحلية والأجنبية التي تنقل عملياتها إلى الصين، وشجعت المستهلك المحلي على الشراء من المزوّد الصينيّ فقط. وقد تعهّدت الحكومة بمبلغ 150 مليار دولار أميركي على مدار العقد القادم لكي تضمن قدرة الصين على تصميم وتصنيع المعالجات الدقيقة المتقدّمة. كما استحوذت الصين أيضا على تكنولوجيات أجنبية. وفقا لمجموعة "روديوم"، شركة الأبحاث، فبين العامين 2013-2016، قدمت الشركات الصينية 27 عرضا للاستحواذ على شركات أشباه الموصلات الأميركية، وتصل قيمة هذه العروض إلى 37 مليار دولار بالإجمال، مقارنة بـــ 6 صفقات تصل قيمتها إلى 214 مليون دولار أميركي بين عامي 2000-2013. لكن هذه المحاولات شابتها العديد من المشكلات؛ ذلك أنّ العديد من العروض المغرية، بما فيها عرض بقيمة 1.3 مليار دولار أميركي لشركة "أشباه موصلات لاتيس"، وصفقة بقيمة 2.4 مليار دولار أميركي لشركة "أشباه موصلات فيرتشايلد"، منعت إتمامها الحكومة الأميركية لأسباب تتعلّق بالأمن القومي

ثمّ هناك الحوسبة الكمية، التي تستخدم قوانين ميكانيكا الكم، أي قدرة البِتّ الكمومي أو "الكيوبت" على تأدية عدد من الحسابات في الوقت نفسه، لحل مشكلات محددة لا يمكن للحواسيب الكلاسيكية حلّها، التطورات في هذا المضمار قد تُتيح لخدمة الاستخبارات الصينية إنشاء محطات اتصال ضخمة مشفرة وأن تخترق التشفيرات المعروفة ويمكن للحواسيب الكمية المعروفة أيضا أن تعود بفوائد اقتصادية جمّة، عبر إعادة التصنيع، وتحليل البيانات، وعمليات تطوير العقاقير. في عام 2016، أطلقت الصين أول قمر صناعي في العالم بإمكانه التواصل عبر قنوات يؤمّنها التشفير الكمي، وشيّدت أطول كوابل الاتصالات الكمية في العالم التي تربط بين بكين وشنغهاي. من غير الواضح كم تنفق الصين على الحوسبة الكمية، لكن الأرقام ضخمة ولا شك،

[19] Op-cit

[20] Op-cit

ذلك أنها تنفق مليار دولار أميركي على مختبرات الحوسبة الكمية وحدها[21]

زيادة على استثماراها في أبحاث أشباه الموصلات وفي الحوسبة الكمية، فإن مخططات الصين الطموحة في مجال الذكاء الاصطناعي هي ما يُثير قلق الغرب بصورة أكبر، في مؤتمر الذكاء الاصطناعي العام الماضي، قال إريك شميدت، الرئيس السابق لغوغل، عن الصينيين: "بحلول عام 2020، سيكونون قد لحقوا بالركب، بحلول 2025، سيكونون قد تفوقوا علينا، بحلول 2030، سوف يفرضون هيمنتهم على صناعة الذكاء الاصطناعي". الصين تسابق الزمن لتطويع الذكاء الاصطناعي للأغراض العسكرية، بما فيها حشود الدرونز الأوتوماتيكية، وبرنامج يمكنه الدفاع عن نفسه ضد الهجمات السيبرانية، وبرنامج ينقّب في وسائل التواصل الاجتماعي بهدف رصد التحركات السياسية المحتملة[22]

في عام 2017، لخّصت الحكومة الصينية خريطة الطريق بعزمها تحويل نفسها إلى "مركز عالمي أساسي لابتكارات الذكاء الاصطناعي" بحلول عام 2030. والخطة أقرب لقائمة أمنيات منها لأن تكون إستراتيجية متماسكة، لكنها تتضمن أيضا توجيهات للوزارات المركزية والحكومات الإقليمية بشأن كيفية الاستثمار في تحقيق التقدم عبر التركيز على مجالات محددة في البحث والتطوير. وقد أعلنت الحكومة كلًا من"Baidu"، و"Tencent"، وعملاق التجارة الإلكترونية "علي بابا"، وشركة تمييز الأصوات "iFLYTEK"، أبطالا قوميين للصين في مجال الذكاء الاصطناعي، عبر تحديد هذه الشبكات كمجموعة أولى بهدف تطوير أنظمة بإمكانها توجيه السيارات ذاتية القيادة، وتشخيص الأمراض، والتصرف كدليل صوتي ذكي، وإدارة المدن الذكية، وهي مساحات حضرية تستخدم مجموعة واسعة من المجسات لحصد البيانات بشأن كيفية عيش الناس، ومن ثمّ تحلل تلك البيانات للحد من التأثير البيئي للمدن، ودفع عجلة النمو الاقتصادي، ورفع جودة حياة الأفراد كما أن الصين تصبو إلى تحديد الموجة القادمة من الابتكار، لا سيما تكنولوجيا الجيل الخامس من شبكات الهاتف المحمول، أي "G"5، التي ستُتيح سرعات أعلى من الإنترنت لمستخدمي الهاتف المحمول وتوفر استخدامات جديدة للأجهزة الموصولة بالإنترنت. بالنسبة للعديدين في سُدة القيادة الصينية، فإن مكانة الصين الحالية في التقسيم الحالي العولميّ للعمل تبدو أشبه بفخّ، حيث تحصد الشركات الأجنبية أرباحها من الملكيات الفكرية الخاصة بها، في حين تعتاش الشركات الصينية على هوامش بسيطة تُتاح لها من تصنيع وتجميع المنتجات المادية[23].

[21] Abdelhak bassouK, policy center for the new south, Rivalité sino-américaine : La Covid-19, frein ou amplificateur selon les comportements des acteurs, pp20-51, mai2020, rabat, maroc

[22] Op-cit

[23] https://www.hoover.org/research/cyberspectives-adam-segal-china-cybersecurity-and-global trade vue le24-07-2022a9H53min

إن استطاعت الصين أن تتحكم بالمعايير التكنولوجية، فإنها ستضمنُ أن تتلقى شركاتها دفعات مالية لقاء حقوق الملكية الفكرية والترخيص في حين تلتفت الدول الأخرى إلى تصنيع المنتجات التي يمكن أن تتلاءم مع منصات مملوكة لشركات صينية على مدار العقد الماضي، زادت الصين من براعة وتعقيد وحجم الوفود التي ترسلها إلى المنظمات الكبرى. لقد كانت الصين غائبة جوهريا عن النقاشات التي رافقت تكنولوجيات شبكات محمول الجيلين الثالث والرابع، لكن الحال تبدّل. ففي عام 2016، قامت هواوي، أكبر شركة للاتصالات الصينية، بإرسال ضِعفَيْ ما ترسله أي شركة أخرى من ممثلين إلى اجتماع فيينا حيث حُدِّدت مزايا الجيل الخامس القادم من شبكات الهاتف المحمول

تحت حكم تشي، كانت الصين تحاول أيضا أن تُشكِّل المؤسسات والأعراف الدولية التي تحكم الفضاء السيبراني، لفترة طويلة من العقد الماضي، كان المخترقون الصينيون هُم مَن يضعون تلك الأعراف عبرَ فرضِ الأمر الواقع من خلال المشاركة في حملات تجسُّس سيبرانية ضخمة مُصمّمة لسرقة الأسرار العسكرية، والسياسية، وأسوأها على الإطلاق في نظر الولايات المتحدة الأسرار التصنيعية. وقد ضغطت إدارة أوباما على الصين بشأن هذه الضغوط، عبر ربط الهجمات السيبرانية ضد الشركات الأميركية علنا بمخترقين مدعومين من الدولة الصينية والتلويح بفرض عقوبات على مسؤولين صينيين كبار، في عام 2015، اتفق الطرفان على ألا يدعم أيٌّ منهما السرقة الرقمية لأهداف تجارية، ومضت الصين إلى توقيع اتفاقيات مماثلة مع أستراليا، وكندا، وألمانيا، والمملكة المتحدة، وقد طرأ تراجع ملحوظ في أعقاب هذه الاتفاقيات، لكن التراجع يبدو بصورة أكبر نتيجة لإعادة ترتيب داخل الجيش الصيني عن أن يكون نتيجة للجهود الدبلوماسية الأميركية. بما أن جيش التحرير الشعبي قد عزّز من قبضته على القوات السيبرانية، فقد انتقل التجسس الصناعي إلى أيدي مخترقين أكثر براعة داخل وكالات استخبارية صينية، جهود الصين الأكثر وضوحا في وسم إشارات طريق الفضاء السيبراني قد تمحورت حول الأمم المتحدة. لقد عززت الولايات المتحدة وحلفاؤها نموذجا لحكم الإنترنت يتضمن الأجسام التكنولوجية، والقطاع الخاص، والمجتمع المدني، والحكومات، في حين تُفضِّل بكين اعتناق رؤية تتمحور حول الدولة، في عام 2017، على سبيل المثال، نادت الصين بـــ "نهج متعدد الجنسيات" في حكم الفضاء السيبراني، مع ضلوع الأمم المتحدة بدور ريادي في بناء التوافق الدولي حول القواعد"، تؤمن بكين بأن نهجا متعدد الجنسيات ينطلق من الأمم المتحدة سيحمل فائدتين مباشرتين؛ أولا أنه سيجعل الأولويةَ لمصالح الحكومات على مصالح الشركات التكنولوجية وجماعات المجتمع المدني، كما أنه سيسمح للصين بأن تحشد أصوات الدول النامية، التي يرغب العديد منها بالسيطرة على الإنترنت والتدفق الحر للمعلومة كما أن الصين قاومت جهود الولايات المتحدة في تطبيق القانون الدولي، وبالأخص قوانين الصراع المسلح، على الفضاء السيبراني. حيث قام "منتدى الخبراء الحكوميين" في الأمم المتحدة بتحديد بعض القواعد السلوكية للدول في سلسلة من اللقاءات والتقارير الممتدة من عام 2004 إلى عام

2017[24]. ومع أن الدبلوماسيين الصينيين في تقرير 2013 قد قبلوا بتطبيق مواثيق الأمم المتحدة والقانون الدولي على الفضاء السيبراني، ومع أنهم وافقوا في عام 2015 على أربعة أعراف تُحدِّد سلوك الدول

فإنهم ماطلوا في المناقشات المتعلقة بطريقة تطبيق الحيادية، والتكافؤ بين الدول، وحق الدفاع عن النفس، ومفاهيم أخرى من القانون الدولي على الصراع في الفضاء السيبراني. وجادلوا عوض ذلك بأن نقاشات القانون الدولي ستؤدي إلى عسكرة الفضاء السيبراني[25]

وأكد الدبلوماسيون الصينيون وأندادهم من الروس ضرورة التسوية السلمية للنزاعات. وفي عام 2017، فشلت الدول المشاركة في منتدى الخبراء الحكوميين في إصدار تقرير استكمالي، وكان ذلك في جزء منه بسبب اعتراض الصين وروسيا على اللغة التي تؤيد حق الدفاع عن النفس. بالإضافة إلى العمل من خلال الأمم المتحدة، فقد أسس صناع السياسة الصينيون لطريقتهم الخاصة في التعبير عن رؤيتهم لمستقبل الإنترنت وإعلاء كلمتهم في حكمه من خلال مؤتمر الإنترنت العالمي، الذي يُعقد سنويا في ووتشان. في عام 2017، حضر كلٌّ من تيم كوك، المدير التنفيذي لأبل، وسوندار بيتشاي، المدير التنفيذي لغوغل، المؤتمر لأول مرة، وهو مدافع صريح عن الخصوصية والخطاب الحر في الولايات المتحدة، صرّح أن أبل تشارك الصين رؤيتها في "تطوير اقتصاد رقمي يقوم على الانفتاح والمصالح المشتركة"[26]. في هذا الاتساق مع لغة المسؤولين الصينيين عن الانفتاح رغم تضييق الخناق الصيني على الإنترنت، إنما كان كوك يُسجّل عزم "أبل" على اللعب وفق قواعد اللعبة التي تضعها بكين من المحتمل أن تتمكّن الصين من فرض أقوى تأثير لها على حكم الإنترنت العالمي من خلال سياساتها التجارية والاستثمارية، بالأخص كجزء من مبادرة الحزام والطريق الصينية، وهي الجهود الجبارة لبناء بنية تحتية تربط الصين بالمحيط الهندي، والخليج العربي، وأوروبا. بجانب أكثر من 50 مليار دولار أميركي كانت قد تدفّقت إلى سكك الحديد، والطرق، وأنابيب الغاز، والموانئ، والمناجم، والخدمات على طول الطريق، فقد أكّد المسؤولون الحاجة إلى أن تقوم الشركات الصينية ببناء "طريق حرير رقمي"، يتألف من كوابل الألياف الضوئية، وشبكات الهاتف المحمول، ومحطات استبدال الأقمار الصناعية، ومراكز البيانات، والمدن الذكيةقسط كبير من الأنشطة الممتدة على طول طريق الحرير الرقمي قد جاء من تحالف شركات

[24] https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web vue le 07-07-2022a14h25min

[25] https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web vue le 07-07-2022a14h25min

[26] Séverine Arsène. La Chine et le contrôle d'Internet. Une cyber souveraineté ambivalente. Serge Sur. Annuaire Français de Relations Internationals, XX, Centre Thucydides, 2019.

التكنولوجيا والتصنيع، لا من الحكومة الصينية. حيث قدّمت "علي بابا" توسعها نحو جنوب شرق آسيا كجزء من مبادرة الحزام والطريق، فاستحوذت على شركة التجارة الإلكترونية الباكستانية "دراز" وأطلقت منطقة تجارة إلكترونية حرة بدعم من الحكومتين الماليزية والتايلاندية، اللتين ستعملانِ على تسهيل عمليات الفحص الجمركي، وتوفير الدعم اللوجستي للشركات، وتعزيز الصادرات من الشركات الصغيرة والمتوسطة في ماليزيا وتايلاند إلى الصين. بينما تعمل شركة "ZTE"في الوقت الحالي في أكثر من 50 بلدا من بين 64 بلدا على طريق مبادرة الحزام والطريق. بالإضافة إلى تمديد كوابل الألياف الضوئية وإعداد شبكات الهاتف المحمول، كانت الشركة توفر خدمات المراقبة، والرصد، والتخزين السحابي، وتحليل البيانات لمدن في إثيوبيا، ونيجيريا، ولاوس، وسريلانكا، والسودان، وتركيا[27]

وتأمل الحكومة الصينية بأن تتيح لها هذه الأعمال التأثير السياسي على المنطقة. لكن الشركات الخاصة تصب تركيزها على الربح، وبكين قلّما تنجح في تحويل العلاقات التجارية إلى ثقل سياسي، حتى عندما تتضمن المشاريع أعمالا ضخمة تديرها الدولة، بما أن هذه الشركات عادة ما تسعى أيضا خلف مصالحها التجارية التي تتعارض مع الأهداف الدبلوماسية. لكن على المدى القصير، فإن حضور المهندسين، والمديرين، والدبلوماسيين الصينيين، سيعزز اتجاها في أوساط البلدان النامية، لا سيما تلك التي لديها حكومات استبدادية، لاعتناق مفهوم الصين المغلق للإنترنت رؤية الصين للإنترنت آخذة في الانتشار، وبحسب جماعة التفكير " فريدوم هاوس"، فإن حرية الإنترنت، أي سهولة وصول الناس إلى الإنترنت واستخدامه للبوح بما يفكّرون به، قد تراجعت على مدار السنوات السبع الماضية، إذ تقوم مزيد من البلدان بدفع الشركات إلى تخزين بيانات مواطنيها المقيمين على أراضيها (وهو ما تقاومه الشركات لأن القيام بذلك سيكلّفها أثمانا باهظة ويحد من قدرتها على حماية خصوصية مستخدميها)، مما يُتيح للحكومات إجراء مراجعات أمنية لتعاون الشبكة. كل بلد يسعى خلف هذه السياسات في دعم غاياته الخاصة، لكن بإمكانهم جميعا اللجوء إلى الصين للدعم المادي، والتقني، والسياسي إن موقع الولايات المتحدة الحالي من الإنترنت العالمي قد عاد عليها بفوائد اقتصادية وعسكرية واستخباراتية ضخمة، فقد قامت الشركات الأميركية ببناء الموزعات والخوادم التي تحمل بيانات العالم بأسره، والهواتف والحواسيب الشخصية التي يستخدمها الناس للتواصل فيما بينهم، والبرنامج الذي يعمل بمثابة منفذ على الإنترنت. بطريقة مماثلة، يرى الحزب الشيوعي الصيني شركات التكنولوجيا موردا للدينامية الاقتصادية والقوة الناعمة، وبالتالي وسيلة لبسط نفوذه السياسي على عمالقة التكنولوجيا الصينيين[28].

[27] https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web vue le 07-07-2022a14h25min

[28] Op-cit

ومع تحوُّل هذه الشركات إلى مزوّد متنامٍ للبنية التحتية الرقمية العالمية، فإن أجهزة التجسس الصينية لن تقاوم إغواء حصد البيانات منها هناك عدة مزايا لشركات التكنولوجيا الصينية؛ ومنها الوصول إلى حجم ضخم من البيانات بالترافق مع القليل من القيود بشأن كيفية استخدامها، والعمالة الموهوبة، والدعم الحكومي. لكنّ إرث البلاد في التخطيط المركزي قد يؤدي بالشركات إلى الإفراط في الاستثمار، وبناء عمليات إضافية، وتبديد إبداعية موظفيها. وقد تحوّلت الشركات الصينية إلى أهداف للضغط السياسي في كلٍّ من أستراليا، والولايات المتحدة، وأوروبا، حيث تعتزم الحكومة الأسترالية منع هواوي من تزويد البلاد بتجهيزات شبكات الجيل الخامس للهاتف المحمول. أما واشنطن، فتعمل من جهتها على الحد من استثمار الشركات الصينية ووضع مزيد من العراقيل أمام قدرة لشركات الاتصالات الصينية إجراء أعمالها التجارية في الولايات المتحدة، فقامت برفض التماس شركة " تشاينا موبايل" بتوفير خدمات الاتصالات في الولايات المتحدة، وحظر مبيعات هواوي و "ZTE"من الهواتف الذكية لأسباب تتعلق بالأمن القومي، وسعت إلى منع شركات الاتصالات الأميركية من إنفاق الأموال على تجهيزات البنية التحتية الأساسية والخدمات القادمة من الصين[29]

لكن من المستبعد لأيٍّ من هذه التحديات أن يُلحق ضررا ضخما بالطموحات الصينية، فالبلاد كبيرة، وقوية، وبالغة التطوّر، ولكي تستعد لسيطرة صينية أكبر على الإنترنت، سيتعيّن على الولايات المتحدة العمل مع حلفائها وشركائها التجاريين للضغط على بكين بحيث تُتيح السوق الصيني للشركات الأجنبية، وتحد من معاملتها التفضيلية للشركات الصينية، وتحمي حقوق الملكية الفكرية للشركات الأجنبية بصورة أفضل، بينما يتعيّن على صناع السياسة الأميركيين الانتقال من الدفاع عن نموذج "القاعدة إلى القمة" الذي يقوده القطاع الخاص لرؤية إيجابية تُتيح للدول النامية بدائل واقعية عن العمل من خلال الأمم المتحدة وحدها. ينبغي لواشنطن إجراء محادثات مباشرة مع بكين بشأن الأعراف التي تُحدِّد سلوك الدول في الفضاء السيبراني، وينبغي للبلدين العمل معا لإعداد المعايير العالمية للصفقات الحكومية في التكنولوجيا، وتحديد طريقة لكي تؤمّن بها الشركات سلاسل تزويدها ضد الهجمات السيبرانية، وتخطيط التفتيش الحكومي لتجهيزات الاتصالات الحساسة. لكن هذه الجهود ستؤدي فقط إلى تشكيل الاتجاهات، لا إبطالها. فأيًّا كان ما تفعله واشنطن، فإنّ مستقبل الفضاء السيبراني سيكون صينيا أكثر منه أميركيا بكثير[30]

في نهاية هذا الفصل يمكن استخلاص نتيجة مفادها ان الصين حققت قفزة نوعية ،في هيكلة قطاعه الاتصالات، ومواكبة التكنولوجيا، ما مكنها خاصة بقيادة الحزب الشيوعي والرئيس شي من تحقيق أهداف استراتيجية جد مهمة خاصة في جعل الصين قوة سيبرانية، فقد أصبحت الصين ،تنتج المعلومة والتكنولوجيا وتتحكم في الانترنت، وخلق شبكات وتطبيقات وبرامج خاصة بها من اجل الفوز بالحرب السيبرانية ضد الولايات المتحدة الأمريكية، التي سعت مع الصين لتحقيق فضاء سيبراني امن لكن الاختلاف في الرؤى والأهداف

[29] Op-cit

[30] Op-cit

والسعي، لتحقيق القوة السيبرانية حال دون تحقيق ذلك، إضافة إلى الى أن الصين لا تستهلك أي منتج تكنولوجي غربي الذي تراه تهديدا للأمن القومي.

*** تحديات وأفاق حماية السيادة الرقمية الصينية**

١– تحديات الأمن ألمعلوماتي الصيني

أ– تحديات إستراتيجية أمنية جيبوبولتكية

الخوف من تسريب البيانات الصينية إلى الخارج، خاصة إلى الولايات المتحدة فمن من المهم الحفاظ على قدرة مستقلة للتقييم واتخاذ القرار والعمل الضروري الحفاظ على السيادة الوطنية في مواجهة التهديدات الجديدة الناتجة عن الرقمنة المتزايدة للمجتمع، قضية أمن قومي. تواجه الدول والشركات والمواطنون تهديدات كبيرة كل يوم مثل سرقة الهوية، والاحتيال على بطاقات الائتمان، والإرهاب، وما إلى ذلك) وفضيحة Facebook-Cambridge Analytica خير دليل على ذلك حيث تم استخدام البيانات، التي تم جمعها دون علم المستخدمين للتأثير على نوايا التصويت[31].

ولذلك ، فإن أحد التحديات الرئيسية للسيادة الرقمية هو جعل الفضاء الإلكتروني أكثر أمانًا للمواطنين وكذلك للشركات والدولة والصين حتى وان كانت رائدة في هذا المجال إلا أن قوة التهديدات الجديدة ،وتطوير برامج فتاكة على غرار بيغاسوس الإسرائيلي، ما يعرض السيادة الرقمية والأمن القومي للصين للخطر، كما يمكن التنويه لفكرة أخرى مفادها ان الضغط التي تمارسه الصين على المجتمع من خلال حوكمة الانترنت، ومنع التفاعل الخارجي، والتنقيط الاجتماعي أدى ببعض، الناشطين والحقوقيين، إلى الفرار إلى الدول الأوروبية، والأمريكية، والكشف عن عدة بيانات وأسرار، خاصة بالصين، وهذا بعد طلبهم اللجوء خوفا من العقوبات التي تصل إلى الإعدام بكشف أسرار الأمن القومي الصيني.

كما أن الجانب الجيبوبولتيكي التوسعي للصين يشكل تحديا فمع ظهور برامج الاختراقات والحرب الالكترونية، تمكنت الولايات المتحدة الأمريكية من دعم التايوان وحتى هونغ كونغ والدعوة للانفصال عن الصين وتجنيد مواقع وأشخاص عبر المواقع والإعلام لشن حرب معلوماتية ضد الصين ومنع بسط سيطرتها على هذه المناطق وبسط سيادتها والسيطرة على بيانات الأشخاص والمعارضين هناك وهذا ما يشكل تحدي للتوسع الصيني

٢– تحديات سوسيو–اقتصادية وتقنية

لا يوجد مجتمع محصن ضد التجسس العلمي والاقتصادي والتجاري، لذلك فإن حماية الشركات وسرية بياناتها أمران ضروريان، ومن هنا تأتي أهمية ضمان بقاء هذه البيانات مستضافة على الأراضي الصينية، كما أن السيادة الرقمية هي أيضًا وسيلة لمكافحة الحصول على البيانات

31 https://www.wimi-teamwork.com/fr/blog/souverainete-numerique-definition-et-enjeux-pour-votre-entreprise/#vue le08-07-2022a8h37min

واستخدامها لأغراض تجارية وتسويقية، دون موافقة الأشخاص المعنيين[32]

السيادة الرقمية هي وسيلة للإدارة والمؤسسات لاستعادة ثقة المواطنين في الدولة، والمشاركة في حمايتهم وحماية خصوصيتهم وبياناتهم الشخصية كما يجب أن تمكن من حماية البنى التحتية الحيوية للدول[33].

يشكل الاقتصاد الرقمي في الصين قوة لا يستهان بها، فالآن تمثل الصين 42% من التجارة الإلكترونية العالمية، وتتباهى بثلث الشركات البادئة الأكثر نجاحا في مجال التكنولوجيا على مستوى العالَم، وتدير مدفوعات عبر الهاتف المحمول أكثر من الولايات المتحدة بنحو 11 مرة ولكن هناك تحديات كبرى تنتظرها.

من المؤكد أن الصين تسير على المسار الصحيح لتحقيق تقدم مستمر، بفضل نظام بيئي ثري من المبدعين، وموقف داعم للتكنولوجيا بين الهيئات التنظيمية والحكومة، وسوق استهلاكية محلية هائلة. ويفوق عدد مستخدمي الإنترنت في الصين (731 مليون مستخدم) مجموع عدد المستخدمين في الاتحاد الأوروبي والولايات المتحدة.

وتدعم هذه العوامل توقعات النمو السريع في سوق التكنولوجيا المالية في الصين،إذ تتوقع مؤسسة جولدمان ساكس نمو قيمة مدفوعات الطرف الثالث المتصلة بالاستهلاك في الفترة من 2016 إلى 2020 من 1.9 تريليون دولار إلى 4.6 تريليون دولار، مع ارتفاع الإقراض من قِبَل جهات غير تقليدية ، من 156 مليار دولار إلى 764 مليار دولار، وزيادة حجم إدارة الأصول الجديدة الموجهة عبر الإنترنت من 8.3 تريليون دولار إلى 11.9 تريليون دولار وقد تضاعف كثيرا مع 2022[34].

كل هذه الأرقام تدعو إلى التفاؤل ولكن مع ظهور العملات المشفرة على غرار البتكوين، أدت بالصين إلى خلق عملة أيضا مشفرة بنظام شيا، للقيام بجميع المدفوعات والتعاملات، وهذا لمواكبة التطور الرقمي ومنافسة العملات الأخرى، وكذلك رغبة الصين في تقليص العقوبات الأمريكية عليها بفضل العملات المشفرة، خاصة وان الصين كانت تتعامل مع البنوك الأمريكية، سوفت، والتي أرهقت الصين كثيرا، فعلى سبيل المثال عندما تم معاقبة، الرئيسة التنفيذية، لهونغ كونغ، على دعمها للحركات المناهضة للديمقراطية، اضطرت إلى استلام راتبها من اليد إلى اليد، لكن تبقر المعضلة الكبرى ،في التعامل بالعملات المشفرة، تناقص دور المواقع المحلية الصينية على غرار تانست، وبايدو علي بابا وغيرها إضافة إلى الحرب بين العملات المشفرة والخوف الصيني، من اختراق بيانات وحسابات المواطنين، والتهرب الضريبي وتبيض الأموال، والتلاعب بالبيانات، عبر تطوير تقنيات من قبل القراصنة لفك تشفير العملات، فكلما تطور الاقتصاد الرقمي تطورت معه تقنيات القراصنة والجوسسة والاختراق، وهذا ما قد يؤثر على النظام الشيوعي الصيني، لان التأثير الاقتصادي يؤثر على الجانب السياسي، فالحزب الشيوعي

[32]Op-cit
[33] Op-cit

Op-cit

الحاكم سعى دائما الى السيطرة على المجتمع ومنع أي معارضة، وبالتالي، التفتح على العملات المشفرة واقتصاد الرقمي العالمي قد يفتح باب الاختراق انظام البيانات الصيني، وحتى فتح الباب امام المعارضة في تايوان وهونغ كونغ والانفصال عن الصين وهو جدي كبير للصين، وحتى لتوسعها الجيبوبولتكي وفرض هيمنتها على الفضاء السيبراني وريادة العالم، بالتعاون مع الحلفاء الروس وكوريا وغيرهم ليكون المستقبل ،للأسيويين، كما يجدر الانتباه لتحدي اخر لا يقل اهمية وهو الجانب الاجتماعي والتقني فالصين تواجه ربما انتفاضة داخلية جراء الضغط الداخلي على المجتمع ومنع التفتح على الفضاء الخارجي وتطبيق نظام التنقيط الاجتماعي، لذلك هناك تحدي تقني يصعب السيطرة عليه وهو التفاعلات الجارية بين المستخدمين في مواقع التواصل الاجتماعي الداخلي في الصين، وعدم القدرة على معرفة توجه الأشخاص والري العام

٣- تحديات بيئية صحية

لقد حققت الصين قفزة نوعية في المجال الرقمي،والتعاملات الرقمية،ولكن هناك تحديات بيئية صحية تواجه الصين، فتعيل الصين وانشاء تطبيقات عبر الهواتف اصبح الاشخاص يقومون بطلب الوجبات الغذائية عبر النت ،ولكن المعضلة هو تسب المتلكين في رمي العلب والبلاسبيك،ما سبب مشاكل بيئية صحية في الصين[35] ،خاصة وان الشعب الصيني،معروف بعدم تضييع الوقت والعمل بمبدأ الحياة السريعة ،ما تطلب الوجبات خفيفة والطلب والدفع عبر النت،وبالتالي،الاكثار من رمي القمامات وأحيانا بعشوائية ما تطلب إعادة النظر في التعاملات الرقمية خاصة في هذا الجانب ومحاولة اجاد البديل وهو بحد ذاته تحدي عويص لذلك

أعلنت أعلى هيئة تشريعية في الصين أنها ستنظر في إصدار قوانين ضد هدر الطعام، في حين هددت منصات البث الرئيسية مدوني الطعام باحتمال فرض حظر على الإفراط في تناول الطعام عبر الإنترنت، ويعد الطعام موضوعًا حساسًا في الصين، حيث لا تزال المجاعة التي شهدت موت 45 مليون شخص جوعاً خلال الخمسينيات والستينيات من القرن الماضي في الذاكرة الحية للكثيرين، إن القدرة على أكل ما يريدون، عندما يريدون، ينظر إليها من قبل الكثيرين على أنها علامة على ثروة الصين الجديدة، وثاني أكبر اقتصاد في العالم لديه ثقافة تركز على الأكل الجماعي، وحذر الخبراء من أن مراقبة أوقات الوجبات يمكن أن يُنظر إليها على أنها تدخل بعيد جدًا في الحياة الشخصية للمواطنين التي تخضع للمراقبة المتزايدة، وقال وو تشيانغ، المحلل السياسي في بكين وأستاذ العلوم السياسية السابق في جامعة تسينغهوا، إن "ثلاث وجبات في اليوم هي شيء شخصي للغاية بالنسبة لعامة الناس، حتى أكثر الأشخاص لامبالاة سياسيًا يمكن أن يشعر بأن عادات حياتهم اليومية تتعرض للتحدي والتهديد من خلال هذه الحملة عندما سحبت الحكومة الصينية قسائم الطعام في 1993، كان

35 https://arabic.cnn.com/world/article/2020/08/29/china-eating-food-waste-meals-campaignvue le28-07-2022a16h28min

رمزًا قويًا أن أيام نقص الغذاء قد ولت، وأصبح الناس أحرارًا في تناول الطعام كما يشاءون، مع انفتاح الاقتصاد الصيني على العالم، تم نقل الثروة الجديدة للبلاد على طاولات الطعام من خلال العناصر الفاخرة مثل زعانف القرش وحساء عش الطيور

وأوضح ألفريد ومولوان، الأستاذ المساعد في كلية لي كوان يو للسياسة العامة في جامعة سنغافورة الوطنية، أن طلب وفرة من الأطباق غالبًا ما يكون "مسألة وجاهة" – فكلما طلب الشخص أكثر، كلما زاد طلب المكانة والاحترام سيكون لديهم، لكن هذا ساهم أيضًا في كميات هائلة من النفايات. وفقًا لوسائل الإعلام التي تديرها الدولة، بين عامي 2013 و2015 أهدرت الصين حوالي 18 مليون طن من الطعام كل عام

عندما يُنظر إلى عدد سكان الصين الهائل البالغ 1.4 مليار نسمة، فهذا أفضل من بعض الدول الغربية، بالنسبة للفرد، تهدر الصين حوالي 72.4 رطلاً من الطعام سنويًا، وفقًا لمؤشر استدامة الغذاء لعام 2018 الصادر عن وحدة إيكونوميست إنتليجنس.

تفرز أستراليا 168 رطلاً من الطعام للفرد سنويًا، بينما تحتل الولايات المتحدة المرتبة الأدنى في المؤشر عند 209 أرطال من الطعام سنويًا، لكنها لا تزال كثيرة[36]

وقال تقرير عن نفايات الطعام في الصين نشرته الأكاديمية الصينية للعلوم الزراعية في 2015، ونقلته وسائل الإعلام الحكومية بعد إعلان شي، إن أسوأ مسبب لفقدان المنتجات في الصين هو صناعة المطاعم المتنامية في البلاد، وأن المشكلة أسوأ بشكل كبير لكن مطالبة المطاعم بتقديم كميات أقل من الطعام في أعقاب جائحة فيروس كورونا، الذي أغلق المطاعم معظم النصف الأول من هذا العام، أمر اثار الكثير من الجدل، إضافة الى كل هذا ظهور التحديات الصحية على غرارکوفيد ومتحورات عديدة،شكل تحدي للصين فعلى الرغم من أنها كانت رائدة في مجال السيطرة ،والتعامل الرقمي مع الازمة،بالدراسة عن بعد وطلب المستلزمات عبر النت،وكذلك تشكيل قاعدة بيانات ضخمة للمرضى للسيطرة على الفيروس،وبسط حوكمتها على بيانات المواطنين،إلا أن التحدي يبقى قائم،فقد تكون هناك متحورات وفيروسات أكثر قوة ،قد تحد من قوة الصين في المجال السبراني،خاصة بوجود الكم الهائل من المواطنين الصينيين ،إضافة إلى كل هذا فالتهديدات المناخية البيئية تشكل معضلة أيضا بالنسبة للصين من اجل تطوير تطبيقات وبرامج تمكن المواطنين والشركات من الحد في إضرار البيئة والمناخ فالصين لديها أكثر من 16منطقة ملوثة على غرار بكين وشنغهاي إضافة إلى تلوث المياه رغم وفرتها في الصين ما استدعى الكثير من الأشخاص الهروب إلى الأرياف لتفادي الإمراض التنفسية [37]و التسممات بسبب المياه والأطعمة المطبوخة بها.

[36] Op-cit

[37].منير مباركية،القوى الصاعدة والتحدي البيئي: حالة الصين، المجلة الجزائرية للأمن الإنساني، العدد السابع،14حويلية2022،ص50

٢- السيناريوهات المستقبلية لسيادة البيانات في الصين

أ- الصين كقوة سيبرانية

تشير الدراسات إلى أن الطموح الصيني للتحول إلى قوة سيبرانية وتزايدها في 2022ترجع إلى عام 2014، حيث قدم الرئيس الصيني ''شي جينغ بينغ'' مفهوم ''القوة السيبرانية العظمى''، عند إنشائه المجموعة القيادية المركزية من أجل الأمن السيبراني وتكنولوجيا المعلومات بالحزب الشيوعي الصيني، وهي أعلى هيئة على مستوى الحزب مختصة بقضايا تكنولوجيا المعلومات، ومنوط بها تحقيق هدف أن تصبح بكين قوة سيبرانية عظمى، ومنذ ذلك الحين برز مفهوم ''القوة السيبرانية العظمى'' كإطار رئيسي للإستراتيجية الصينية في مجال الاتصالات وتكنولوجيا المعلومات، فيكاد لا يخلو أي خطاب للرئيس الصيني من التأكيد على أهمية أن تصبح بكين قوة سيبرانية عظمى[38]، ويرى الرئيس الصيني الحالي أن الثورة التكنولوجية العالمية هي فرصة إستراتيجية للصين للتعويض عن الضرر النسبي الذي لحق بها في الثورات الصناعية السابقة، ففي حين استثمر الغرب (الولايات المتحدة وأوروبا) فرصة الثورات الصناعية لتعظيم مكاسبهم التنموية، ترى القيادة الصينية أن في الوقت الحالي، تستغل الصين التحول لشبكات الجيل الخامس (G-5) لتنتقل بكين من دولة صناعية كبرى إلى دولة سيبرانية كبرى بحسب تعبير نائب وزير وزارة الصناعة والتكنولوجيا الصيني ''تشين تشوكسيونغ''، في مقال نُشر عام 2019 في مجلة الاندماج العسكري-المدني في الفضاء الإلكتروني وفعلا حقت هذا الحلم، حيث ألان أصبحت الصين دولة سيبرانية، لا يستهان بها، فهي دولة رقمية بامتياز، وهناك دراسات تقول في 2025 ستغزو الصين الفضاء السيبراني، والعالم، وتتحكم في سيادتها السيبرانية وحتى الفضاء السيبراني العالمي، نظرا لجهودها المستمرة، الغير المتقطعة في تحقيق ،حلم أن يصبح العالم تحت الحكم الشيوعي، بفضل القوة التكنولوجية الصينية، وسرعتها وغزوها للعالم لهذا شدد الرئيس الصيني ''شي جينغ بينغ'' مرارا وتكرارا على أن العامل الرئيسي في بناء القوة العظمى السيبرانية للصين هو تعزيز الابتكار التكنولوجي المحلي، وهو ما سينعكس على تعزيز القدرة التكنولوجية الصينية التي تخلق اعتمادا دوليا عليها، دون أن تكون بكين معتمدة على التكنولوجيا الأجنبية بشكل كبير، كما دعا الرئيس الصيني إلى ضرورة ''استثمار الصين لمزيد من الموارد البشرية والمادية في البحث والتطوير التكنولوجي''، بالإضافة إلى جمع أفضل الكوادر لصياغة إستراتيجية تطوير التكنولوجيا والتقنيات التكنولوجية الرئيسية، وشدد ''شي جينغ بينغ'' في الخطاب ذاته على أهمية صياغة خارطة طريق، وجدول زمني، وقائمة من المهام لإنجازها على المدى القريب والمتوسط والطويل، أشار الرئيس

38 https://futureuae.com/ar/Mainpage/Itemvuele27-07-2022a17h03min

الصيني ''شي جينغ بينغ'' إلى أن تحقيق التقدم التكنولوجي والأمن السيبراني هما جناحان رئيسيان للتنمية الصينية[39].

وأوردت عدة دراسات أن هناك بنية رقمية عالمية جديدة في طور التشكل، وهو ما سوف يؤثر على ميزان القوى الدولي، حيث تسعى الصين إلى لعب دور أساسي في تطوير وتوجيه هذه البنية الرقمية الجديدة من خلال طريق الحرير الرقمي الذي تسعى الصين من خلاله إلى إعادة هيكلة نظام حوكمة الإنترنت العالمي[40]

وحال تمكن الصين من بناء شبكات الجيل الخامس من خلال اعتمادها على مكونات محلية بشكل كامل، فض لا عن تمكنها من وضع المعايير الدولية لعمل هذه الشبكات والتقنيات؛ فإن ذلك سيعني أنها قد أصبحت قوة سيبرانية ع ظمى مما يعني تعظيم قدرتها على الترويج لأفكار وقيم وخطا ب معين؛ وهو ما قد يؤهلها إلى قيادة النظام الدولي المستقبل ي، الذي سيعتمد بشكل أساسي على التقدم التكنولوجي.

ب- التهديدات الجديدة وتأثيرها على سيادة البيانات الصينية

على الرغم من أن الخطاب الصيني الداخلي يتحدث بشكل صريح عن رغبة بكين في أن تصبح قوة سيبرانية عظمى، فإن التقرير يشير إلى غياب الحديث بشكل شبه تام عن هذا الموضوع في الخطابات والبيانات التي يوجهها المسؤولون الصينيون إلى الغرب، فلم يتم الحديث عن ''القوة السيبرانية العظمى'' سوى مرة واحدة خلال ست سنوات، وذلك في بيان للمتحدث باسم وزارة الخارجية الصينية، بذلك، تبرز الورقة أن الصين تتعمد عدم الإفصاح أو الحديث عن طبيعة ومدى طموحاتها في مجال تكنولوجيا المعلومات عند التواصل مع الجماهير الأجنبية، ويتركز خطابها الخارجي على أهمية احترام قواعد الاقتصاد الحر، هذا ما يؤكد التخوفات التي أبداها العديد من الباحثين المقربين من النظام الصيني من وجود ''ثغرة أمنية'' في البنية التكنولوجية الصينية بسبب الاعتماد على الرقائق وأنظمة التشغيل الغربية، لذا يوصي الباحثون الصينيون بضرورة تطوير الصين لآليات وتقنيات للردع السيبراني، وإلا فإن جهود الصين للتطور التكنولوجي لن تؤتي ثمارها ولن تقوم بتعزيز وحماية أمنها القومي[41].

كما أن التحديات التقنية والإستراتيجية الأمنية بتطور التهديدات الالكترونية والحرب الالكترونية المستمرة مع الولايات المتحدة الأمريكية، والقرصنة والجوسسة قد تعيق تقوية القوة السيبرانية الصينية والتحكم في سيادة بياناتها، إضافة إلى التحديات الاجتماعية بعدم القدرة على التحكم في التفاعلات في الوسط الافتراضي داخل المجتمع الصيني،

39 https://futureuae.com/ar/Mainpage/Item/6269/%D9%87vue le27-07-2022a17h03min

40 https://geopolri.hypotheses.org/2690vue le29-07-2022a8h58min

41 https://www.revueconflits.com/chine-cybercriminalite-etats-unis-hackers-internet/vue le29-07-2022a9h04

وكذلك صعوبة التحكم وحوكمة الانترنت في المقاطعات الراغبة في الانفصال على غرار التايوان وهونغ كونغ المدعومة من الولايات المتحدة الأمريكية، إضافة لكل هذا هناك تحديات صحية بيئية تهدد الصين ما يشكل تحدي لإعادة صياغة تطبيقات وبرامج تراعي فيها الجانب البيئي والتصدي للتهديدات الصحية

* **الاستنتاجات**

خلصت الدراسة لما يلي:-

١- شهد العالم ثورة تكنولوجية رقمية هائلة، ما أدى إلى ظهور فضاء جيوبولتيكي افتراضي يسمى بالفضاء السبراني

٢- غلب على الفضاء السبراني طابع الصراع من قبل الفواعل غير دولتية والفواعل الدولتية خاصة من قبل القوى العظمى على غرار الصين والولايات المتحدة الأمريكية،بسب السباق نحو التسلح التكنولوجي ،كوسيلة ردعية بديلة عن السلاح النووي

٣- الصين تعتبر الولايات المتحدة محتكرة للفضاء السبراني خاصة من قبل شركة كان والولايات المتحدة تراها شرعية لانها المنتجة للنكنولجيا

٤- زاد الاهتمام الصيني بالفضاء السبراني بعد قضية سنودن والتجسس على اعلى نطاق

٥- الاتهامات المتبادلة بين الصين والولايات المتحدة الأمريكية،بخصوص الجوسسة والهجمات الالكترونية زادت من حدة الحرب السبرانية بين الطرفين

٦- الريبة والشك السائد بين الصين والولايات المتحدة الأمريكية ازداد حدة ،بالسعي نحو تطوير تطبيقات وبرامج وتطبيقات الكترونية للسيطرة على دواليب الاقتصاد والتجارة العالمية وحتى الجانب الأمني والسياسي،باعتبار الدول تتعامل بالعملات الرقمية والدبلوماسية الرقمية والاقتصاد الرقمي

٧- الاختلاف في الرؤى بين الصين والولايات المتحدة الأمريكية بخصوص المفاهيم والمصطلحات الخاصة بالفضاء السبراني حال دون تحقيق فضاء سبراني امن

٨- حوكمة الانترنت وتأسيس مواقع صينية خاصة بالصين على غرا ربايدو و تانست،وتحقيق اكتفاء تكنولوجي داخلي مكن الصين من بسط الصين سيطرتها على بياناتها

٩- لعب الحزب الشيوعي والرئيس شي دورا هاما ورئيسيا في هيكلة نظام الاتصالات في الصين وتحقيق السيادة الرقمية في الصين

١٠- طبقت الصين وصفة الوقاية خير من العلاج،بعدم استهلاك المنتج التكنولوجي الغربي ما مكنها من السيطرة على البيانات الداخلية

١١- طورت الصين عبر عمالقة الالكترونيات على غرار هواوي علي بابا وغيرها، أجهزة تشفير مائية مكنتها من حماية بياناتها من القرصنة

١٢- الصين طبقت نظام التنقيط الاجتماعي وتكوين فرد شيوعي على شكل روبوت يؤمن بالصين وحماية الأمن القومي الصيني ،هذا ما قوى نظام الرقمنة وتحقيق السيادة الرقمية في الصين

١٣- الضغط الداخلي الممارس على الشعب الصيني، والانغلاق على الفضاء الخارجي قد يشكل خطرا على نظام البيانات في الصين فهناك من يفرون إلى أوروبا وامريكا وغيرها ويسربون بيانات خاصة بالصين

١٤- تطور الهجمات الالكترونية وظهور تهديدات جديدة من شتى الأنواع على غرار كورونا وغيرها تشكل تحديات للسيادة الرقمية الصينية

١٥- هناك تحدي تقني يواجه الصين وهو عدم القدرة على السيطرة على التفاعلات والمحادثات الداخلية في المواقع الالكترونية الداخلية،بالتالي عدم معرفة توجه المستخدمين وما يدورفي أذهانهم

١٦- التعامل بالعملة المشفرة،قد يفتح باب أمام التلاعب الالكتروني بالضرائب،والبيانات الخاصة بالفساد ،كما انه قد تنشب حروب العملات المشفرة بين الصين والولايات المتحدة الأمريكية،كل هذه تحديات وعراقيل تواجه سيادة البيانات الصينية

١٧- الحروب الالكترونية بين الصين والولايات المتحدة الأمريكية في اكرانيا والتايوان تشكل تحديات للسيادة الالكترونية الصينية

١٨- الأوضاع الجيبوبولتكية الحالية،وما يشهده العالم من صراعات،عززت التحالف الصيني،مع حلفاءها خاصة روسيا والهند وكوريا والبرازيل في إطار البريكس، لتأسيس قوة مجابهة للولايات المتحدة والغرب وكذلك العمل على السيطرة على الفضاء السبراني لإضعاف أمريكا والدول الغربية

١٩- هناك سيناريوهين للسيادة الرقمية الصينية ،فالصين يمكن أن تتقوى سيادتها السبرانية،خاصة مع تفعيل نظام معلوماتي داخلي مشفر وفضاء معلوماتي مغلق ،ومن جهة أخرى يمكن أن تضعف نظرا للتهديدات الداخلية مثل الضغط الاجتماعي وصعوبة التحكم في المحادثات عبر النت وخارجيا والتي تتمثل أساسا في تطور الهجمات الالكترونية والحرب السبرانية المستمرة مع الولايات المتحدة الأمريكية وظهور تهديدات ذات طابع صحي على غرار كوفيد19 وكذلك بيئية.

*** المراجع**

أولاً- المراجع العربية

منير مباركية،القوى الصاعدة والتحدي البيئي: حالة الصين، المجلة الجزائرية للأمن الإنساني، العدد السابع،14حويلية2022،ص50

السيادة السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومي مقال-سميرة شرايطية-جامعة المجلة الجزائرية للأمن والتنمية. مج. 9، ع. 1 (كانون الثاني 2020)، ص ص. 396-410، 15ص

ثانياً- المراجع الأجنبية

Séverine Arsène. La Chine et le contrôle d'Internet. Une cyber souveraineté ambivalente. Serge Sur. Annuaire Français de Relations Internationals, XX, Centre Thucydides, 2019.

Hauke ،Johannes Gierow (April 2015). Cyber Security in China : Internet Security, Protectionism and Competitiveness : New Challenges to Western Businesses, mercator institute forchina studies pp1-10

Abdelhak bassouK ،policy center for the new south, Rivalité sino-américaine : La Covid-19, frein ou amplificateur selon les comportements des acteurs ، pp20-51, mai2020, rabat, maroc

Amy Chang, Warring State : China’s Cybersecurity Strategy Washington, Center for à New American Security, December 2014
https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web vue le 07-07-2022a14h25min
https://www.revueconflits.com/chine-cybercriminalite-etats-unis-hackers-internet/vue le29-07-2022a9h04
https://futureuae.com/ar/Mainpage/Item/6269/%D9%87vue le27-07-2022a17h03m---
https://geopolri.hypotheses.org/2690vue le29-07-2022a8h58min
https://arabic.cnn.com/world/article/2020/08/29/china-eating-food-waste-meals-campaignvue le28-07-2022a16h28min
https://www.wimi-teamwork.com/fr/blog/souveraine-numerique-definition-et-enjeux-pour-votre-entreprise/#vue le08-07-2022a8h37min
https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web vue le 07-07-2022a14h25min