قضايا سياسية

الأمن السيبراني الصيني: دراسة في الدوافع والتحديات

Chinese cyber security

أ.د. إسراء شريف جيجان*

المستخلص:

برزت قضية الأمن السيبراني كأحد أهم التحوطات من الصراعات السياسية والاقتصادية بين الدول نتيجة الحروب الالكترونية أو الحروب السيبرانية، التي تستهدف البنى التحتية والمنشآت والمؤسسات الحكومية والشبكات الصناعية والأبحاث، وهي بشكل أو بآخر قادرة على تعطيل تشغيل البنى التحتية الحيوية، وفي هذا الصدد، كان للصين دوافع عديدة للقوة السيبرانية وتعزيزها منها سياسية، اقتصادية، عسكرية، أمنية، اذ تعد الصين الدولة الأولى التي أضفت الطابع السيادي للسيبرانية لأنها فرضت سيطرة مطلقة من جانب الدولة وأصبحت خاضعة لما يسمى (جدار الحماية العظيم) مع إبداء تعاون واسع النطاق مع الدول في هذا المضمار.

الكلمات المفتاحية: الصين، الامن السيبراني، حروب الجيل الخامس، مستقبل الامن السيبراني

Abstract

The issue of cyber security has emerged as one of the most important precautions against political and economic conflicts between countries as a result of electronic or cyber wars that target infrastructure, facilities, government institutions, industrial networks and research and are in one way or another able to disrupt the operation of vital infrastructure, and in this regard, China had many motives for force. Cyber and its enhancement, including political, economic, military, and security, as China is the first country to add a sovereign character to cyber because it imposed absolute control on the part of the state and became subject to the so-called (Great Firewall) with extensive cooperation with countries in this regard.

Keywords: China, cybersecurity, fifth generation wars, the future of cybersecurity.

* كلية العلوم السياسية / جامعة بغداد

المقدمة :

لقد برزت العديد من التحديات والتهديدات مع نهاية الحرب الباردة وهي حديثة العهد على المجتمع الدولي فبرزت العديد من أشكال التحديات والتهديدات كالتهديدات اللاتماثلية (asymmetric).

ومع ظهور الثورة المعلوماتية أصبحت التكنلوجيا إحدى أنماط القوة التي اكتسبت أهمية كبيرة ومضاعفة بعد الحرب الباردة لأنها استطاعت إلغاء المسافات بين الدول وأصبح العالم متسقاً ومتقارباً ودخلنا في العصر الرقمي مع انبلاج القرن الحادي والعشرون وما رافق هذا التطور الهائل من تهديدات من نوع جديد تضمنت أبعاد وخصائص وفواعل من نوع آخر، إذ عده المختصون في المجال الأمني والاستراتيجي والسياسي ضمن الجيل الخامس من الحروب بعد الحروب البرية والبحرية والجوية والفضائية وأصبح بمثابة جيل جديد من الحروب على صعيد الاستراتيجيات الدولية وهذا ما جعل الدول تبحث عن تحصينات وحلول وضمانات أمنية ضمن هذه البيئة الرقمية وظهر مصطلح الأمن السيبراني (Cyber Security)، ومن الدول الكبرى التي اهتمت به الصين وعي موضوع بحثنا.

أهمية البحث :

يعد موضوع الأمن السيبراني من الموضوعات المهمة التي تثير جدلاً واسعاً في العلاقات الدولية وهو أحد العناصر المؤثرة في السياسة والاقتصاد على الصعيد الدولي بسبب تحول الحيز الأكبر من الصراعات بين القوى الكبرى إلى أدوات ووسائل جديدة أنتجتها التطورات التقنية والعلمية المتمثلة بشبكة الانترنيت والوسيط الرقمي أو الفضاء السيبراني.

لقد عملت الصين على ترسيخ أسس استراتيجية الأمن الالكتروني ولها دوافع متعددة لهذا الأمر وبقدر تلك الدوافع هنالك تحديات تحاول الصين تذليلها للهيمنة في مجال الأمن السيبراني.

فرضية البحث :

تنطلق الدراسة من فرضية مفادها أن الأمن السيبراني الصيني متغير فاعل ومؤثر في العلاقات الدولية وخاصة بعد عام 2013 والسياسة الخاصة التي انتهجها الرئيس الصيني شي جين بنغ وإنشاءه مشروع جدار الحماية العظيم لمواجهة العقل الأمريكي وأن للصين دوافع سياسية، اقتصادية، أمنية، وعسكرية وهنالك تحديات تواجه السيادة السيبرانية والأمن السيبراني إلا أن الطموح الصيني الذي ينتهج السياسة السلمية والصعود السلمي يحاول كبح جماح تلك التحديات.

إشكالية البحث :

تتمثل إشكالية البحث من السؤال الأساس المحوري المتمثل ما هي دوافع وتحديات الأمن السيبراني الصيني ؟

يتشظى من ذلك السؤال المركزي عدة تساؤلات فرعية :

- ما هو الأمن السيبراني وما هي المفاهيم المقاربة ؟
- ما هي دوافع الأمن السيبرانية الصيني ؟
- ما هي التحديات التي تواجه الأمن السيبراني الصيني ؟
- ما هو مستقبل الأمن السيبراني الصيني ؟

منهجية البحث :

نظراً لتعدد القضايا التي تناولتها محاور البحث ومحاولة الإحاطة بالوقائع وتفصيلاتها اعتمدت الدراسة عدة مناهج إذ اعتمدنا المنهج الوصفي لمتابعة الأحداث التي رافقت نشوء والاهتمام الصيني بالجانب السيبراني ولتحليل الظواهر والأحداث تم اعتماد المنهج التحليلي للوقوف عند تأثير متغير الأمن السيبراني الصيني ولبيان مستقبل الأمن السيبراني الصيني تم تقديم رؤية استشرافية تضمنت الفرص والكوابح.

أولاً : الإطار المفاهيمي للأمن السيبراني والمفاهيم المقاربة.

أ – الإطار المفاهيمي للأمن السيبراني.

إن أساس نشأة كلمة السيبرانية (cybernetic) ارتبطت باللغة اليونانية والذي يعني التوجيه والسيطرة ومشتقة من كلمة (Kybernetes) أي الشخص الذي يدير دفة السفينة، إذ تستخدم مجازاً للمتحكم (governor). وبذلك بإمكاننا القول أن السيبرانية هي التحكم عن بعد، فهي عندما تأتي مع كلمة أخرى تعني التحكم بها أو إدارتها كما في الأمن السيبراني. [1]

أما الأمن فهو نقيض الخوف أي بمعنى السلامة والأمن مصدر الفعل أمن أمناً وأماناً وأمنة أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال أمن من الشر أي سلم منه في إشارة إلى غياب ما يهدد القيم النادرة.

[1] U.S Department of Defence, Dictionary of Military and Associated Terms, Publication 1 – 8 2010 as a mended through feb 15, 2012.

وهنالك العديد من التعريفات الخاصة بالأمن السيبراني فمنه من يعرفه على أنه أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والأجهزة المتصلة بالانترنت، وعليه فهو المجال الذي يتعلق بإجراءات ومقاييس ومعايير الحماية المفروض اتخاذها أو الالتزام بها لمواجهة التهديدات والحد من آثارها.[1]

ويعرفه رتشارد كمرر بأنه عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة.[2]

ويعني الأمن السيبراني مجموعة الاجراءات الواجب اتخاذها من قبل الأجهزة الأمنية أو الأجهزة والمؤسسات الأخرى للمحافظة على سرية المعلومات الالكترونية ومنع الاختراقات الفيروسية من أجل ضمان وصول المعلومات الحاسوبية إلى الجهات المختصة وفي الوقت ذاته ضمان عدم وقوعها في أيدي الأعداء أو الأصدقاء على حد سواء.[3]

في حين اعتبر الإعلان الأوروبي الأمن السيبراني أنه يعني ((قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات)).

وقد ينطلق الأمن السيبراني من التوجه نحو حماية الفضاء السيبراني التي تشمل محتويات هذا الفضاء من جهة وتتضمن عوامل معنوية مختلفة أخرى من جهة ثانية، وقد تشمل هذه المحتويات معلومات ترتبط بالأطراف المختلفة من مؤسسات وأفراد ضمن الفضاء السيبراني وتتضمن أيضاً تقنية تخزن هذه المعلومات وتعالجها وتنقلها عبر الشبكات، كما تشمل إجراءات أعمال تنفيذ مهمات تؤدي خدمات مختلفة ويضاف هنا أيضاً الأفراد القائمون على كل ذلك، وتضم العوامل المعنوية وهي كل من أطراف الفضاء السيبراني خصوصاً المؤسسات والدول المختلفة.

ب- المفاهيم المقاربة للأمن السيبراني.

نتيجة اتساع مفهوم الأمن السيبراني بسبب التقدم التكنلوجي والتقني وبعد انتهاء الحرب الباردة أي مطلع تسعينيات القرن الماضي ظهرت مفاهيم أخرى مقاربة منها على سبيل المثال كالآتي :

1- الفضاء السيبراني : أي فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية. وهو بيئة تفاعلية حديثة تشمل عناصر مادية ومعنوية، مكوّن من مجموعة

[1] منى جبور الأشقر، السيبرانية هاجس العصر، المركز العربي للبحث القانونية والقضائية، بيروت، 2017، ص25.

[2] Richard Akemmerer, Cyber Security, University of California Santa Barbara, Department Computer Science, 2003, P.3.

[3] دلال العودة، الصراعات الدولية الحديثة، ط1، دار الطلائع للنشر والطباعة، القاهرة، 2015، ص43.

من الأجهزة الرقمية وأنظمة الشبكات والبرمجيات ويطلق عليه الذراع الرابعة للجيوش الحديثة، وأصبح هذا الفضاء ساحة لنقل الصراعات وتصفية الخلافات بأنواعها بين أطراف الصراع كافة، وزادت التقنيات الرقمية ومدى التقدم العلمي بها من إضفاء درجة الفاعلية على ذلك النوع من الحروب عبر الفضاء الإلكتروني في الصراع الدولي وقد لا تؤدي هذه الحرب إلى مأساة الكترونية بالضرورة بل إلى فرض نوع من السيطرة على مجرى الأحداث في العالم.[1]

2- الصراع السيبراني : يأخذ الصراع السيبراني طابعاً تنافسياً من خلال السعي للسيطرة على أسماء النطاقات وعناوين المواقع والتحكم بالمعلومات والعمل على اختراق الأمن القومي للدول ولكن دون استخدام طائرات أو متفجرات أو حتى انتهاك للحدود السيادية والتي تتمثل بهجمات قرصنة الكومبيوتر وتدمير المواقع والتجسس بما يكون لذلك من تأثير على تدمير الاقتصاد والبنية التحتية بنفس القوة التي يحدثها تفجير تقليدي مدمر.

وقد أضحى الصراع السيبراني أحد أوجه التفاعلات الدولية الجديدة شأنه شأن الهجمات السيبرانية والحرب السيبرانية إلا إنه يمتاز بعدة خصائص أهمها :

أ) تنوع الفاعلين من الدول وغير الدول.

ب) يتسم بكونه غير مكلف مادياً.

ج) ليس من السهولة بمكان نزع سلاح الطرف الآخر أو تدميره كلياً أو احتلال إقليمه.

د) إمكانية استخدام الفضاء الالكتروني في القوة الناعمة أو الصلبة.[2]

3- الحرب الالكترونية : هي مستوى من التسلح العسكري المتقدم والذي من شأنه أن يتفوق على الخصم باستخدام وسائل عديدة كتقنية الاخفاء في الطائرات المقاتلة الحديثة ومنظومة الرصد الجوي (400S) ومنظومة (Thad) الامريكية وهي تكتيك يهدف إلى تعطيل فاعلية منظومات الدفاع والهجوم عن طريق التشويش والإعاقة الالكترونية.[3]

---

[1] عادل عبدالصادق، الإرهاب الالكتروني، القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والاستراتيجية، الأهرام، القاهرة، 2009، ص200-202.

[2] James Graham, Richard Howard Ryan Alson, Cyber Security Essentials, Françis group an informal business, 2011.

[3] سامر جمال، أثر المتغير السيبراني على العلاقات الأمريكية – الروسية، بحث مقدم إلى معهد الخدمة الخارجية، وزارة الخارجية العراقي، 2020، ص10-15.

4- الأمن السحابي : يعد الأمن السحابي تقنية سيبرانية تعتمد على ضغط المعلومات وهو جزء لا يتجزأ من الأمن السيبراني ويعرف الأمن السحابي بأنه سياسات وتقنيات وضوابط تعمل جميعها لحماية البيانات المنتشرة والتطبيقات المرتبطة بها والمكونة للحوسبة السحابية واجبها حماية البيانات والفصل بين الواجبات وأمن التطبيقات والأنظمة السرية وغيرها من واجبات.

إن أهمية حماية البيانات يتطلب معرفة أمن الحوسبة السحابية لتعلم كيفية حمايتها بعد تخزينها ومعرفة كيفية تحديد المشكلات الأمنية في التقنيات والإجراءات المعيارية المتعلقة بالحوسبة السحابية والصناعية لمنع المخاطر.[1]

5- القوة السيبرانية : مع ثورة تكنلوجيا المعلومات ظهر شكل جديد من أشكال القوة هي القوة السيبرانية Cyber Power والتي بدأ تأثيرها واضحاً على المستويين الدولي والمحلي فمن ناحية أدت إلى توزيع وانتشار القوة بين عدد أكبر من الفاعلين مما جعل قدرة الدولة على السيطرة موضع شك ومن ناحية أخرى منحت الفاعلين الأصغر قدرة أكبر على ممارسة القوة وهذا يعني تغيراً في علاقات القوى في السياسة الدولية.

يعد جوزيف س. ناي من أبرز المهتمين بالقوة السيبرانية حيث يعرفها بأنها القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني أي إنها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة والتأثير على الأحداث المتعلقة بالبيانات التشغيلية الأخرى وذلك عبر أدوات سيبرانية.[2]

يمكن القول أن عناصر القوة السيبرانية ترتكز على وجود نظام متماسك يعظم من القوة المحصلة من التناغم بين القدرات التكنلوجية والسكان والاقتصاد والصناعة والقوة العسكرية وإرادة الدولة وغيرها من العوامل.

وفي ميدان العلاقات الدولية أصبح امتلاك القوة السيبرانية أحد مفاتيح القوة في هذه العلاقات، وبات يمثل مجالاً لهيمنة الدول بعضها على بعض سواء بطريقة مباشرة أو غير مباشرة وتحولت القوة العسكرية من قوة استخدام الأسلحة إلى قوة الذكاء البشري.

من ذلك يتبين أن الأمن السيبراني كقضية ناشئة في حقل العلاقات الدولية من خلال حداثة هذا المجال إذ إن مع نهاية الحرب الباردة حدثت تحولات تدريجية ظهرت على مستوى التفكير الاستراتيجي إذ

[1] أمن الحوسبة السحابية، edilbre.com.

[2] Joseph S. Nyr, Cyber Power, Harvard Kennedy School, 2010, P.3.

تحولت واتسعت الرؤيا حول الدولة وأصبحت ديناميكية وأصبح مفهوم الأمن أكثر شمولاً واتساعاً وأصبح الباحثون في حقل العلاقات الدولية وبقية الحقول الفرعية في الدراسات الاستراتيجية والأمنية يركزون بشكل متزايد حول أثر التكنلوجيا على الأمن القومي والدولي ويشمل ذلك تأثيرها على المفاهيم ذات الصلة كالقوة والسيادة والحوكمة العالمية والأممية. وقد ارتبط ظهور الأمن السيبراني بظهور الهجمات السيبرانية.

ومن الدول التي أولت أهمية بالغة بهذا الجانب الصين إذ أصبح لها تأثير داخل وعبر الفضاء السيبراني من خلال امتلاك مقومات الدولة وقدرتها على تطوير موارد العمل.

ثانياً : دوافع القوة السيبرانية الصينية.

شرعت الصين ومنذ المؤتمر الثامن عشر للحزب الشيوعي الصيني بتطوير تكنلوجيا المعلومات، اتسمت الرؤية الصينية للسيادة السيبرانية كجزء من مصطلح أوسع للأمن المعلوماتي، الذي بدوره كان أمراً غاية في الأهمية عندما أكد الرئيس الصيني (شي جين بنغ) ((على الدول احترام حق كل طرف في اختيار طريقته الخاصة في تطوير الانترنت بما يحقق التفوق والأمن والمشاركة في الحكومة الدولية على الانترنت على قدم المساواة.[1]

وقد بذلت الصين جهوداً مكثفة للعمل الدؤوب لتأسيس فضائها السيبراني الوطني وقد كان هنالك عدة دوافع لذلك سياسية وعسكرية واقتصادية.

أ- الدوافع السياسية.

بدأ الاهتمام الصيني بشكل جدي في المجال الالكتروني منذ عقد التسعينات من القرن الماضي وسعت الصين إلى تحقيق تفوق نسبي على خصومها ومنافسيها في المجال الالكتروني والمعلوماتي وفي ظل المتغيرات السريعة في بيئة الفضاء السيبراني باعتباره مجالاً رئيساً للمواجهة ظهرت الحاجة إلى إعادة النظر في مفهوم السيادة السيبرانية.

بصورة عامة فإن الحكومة الصينية تخشى من إتاحة استخدام الانترنت دون قيود ومن عدم السيطرة على عدم تدفق وانتشار المعلومات خاصة من قبل المعارضة لذا عمدت الصين على تطبيق

[1] Baezner, Marie and Patrive Robin, Cyber Sovereignty and Data Sovereignty 2019, p.5 – 6.

تدابير وقائية في إطار تبني مفهوم ((احترام السيادة الصينية في مجال الفضاء الالكتروني)) والذي من شأنه أن يسمح للصين بالسيطرة على الانترنت داخل حدود الدولة بفاعلية.[1]

ب- الدوافع الاقتصادية.

هنالك عدة دوافع وأهداف اقتصادية في مجال القوة السيبرانية الصينية تتلخص بالآتي :

1- صعود الصين المتواصل كقوة سيبرانية عظمى ليس بالأمر المضمون فالجهود التي تبدأ من القمة وتنتهي بالقاعدة التي تقودها الدولة في ابتكارات الذكاء الصناعي والحوسبة الكمية والروبوتات وتقنيات أخرى رغم الضغوط الاقتصادية التي تواجهها الصين مع انفتاحها على العالم.

2- بالنظر إلى التقدم البارز الذي أحرزته الصين في المضمار التكنولوجي ومعظم التطبيقات هي صينية على أجهزة رقمية مصنعة في الصين وهذا بالتالي ما سيمكن الصين من تحقيق مكاسب اقتصادية.

3- مع وصول الرئيس الصيني شي جين بينغ إلى السلطة 2012 حرص على ترأس مجموعة قيادة مركزية لأمن الانترنيت والمعلومات أي قيادة دفة السياسة السيبرانية من خلال تأسيس وكالة جديدة تحت مسمى إدارة الفضاء السيبراني الصينية عملاً على تطوير الاقتصاد الرقمي في الصين.

4- محاولة تعويض الخسائر الاقتصادية التي نجمت عن الجرائم السيبرانية التي وصلت إلى (830) مليون دولار عام 2019 وقد طالت تلك الهجمات السيبرانية (20) مليون صيني من خلال سرقة بياناتهم الشخصية على أيدي الهاكرز.[2]

ج- الدوافع الأمنية.

للصين دوافع أمنية للحد من الهجمات السيبرانية وضمان الأمن السيبراني فعلى سبيل المثال دعت الصين إلى ضرورة إدانة الهجمات السيبرانية ضد المؤسسات التي تكافح جائحة فيروس (Covid 19) المستجد في جميع أنحاء العالم.

وأدلى المتحدث باسم وزارة الخارجية الصينية غينغ شوانغ بهذه التصريحات رداً على سؤال حول تقرير صدر عن شركة الأمن الالكتروني الأمريكية (FireEye) بأن مقرصنين فيتناميين مرتبطين بالحكومة حاولوا اختراق حسابات البريد الالكتروني والحكومة في ووهان المدينة الصينية التي ظهر فيها فيروس (Covid 19) للمرة الأولى العام الماضي ويعتقد صناع القرار الصيني أن تحقيق الأمن يتطلب تحقيق الاكتفاء الذاتي التكنلوجي لذا شرعت الصين بوضع خطة خمسية بدأت 2016 واستثمرت في هذا

[1] Baezner, Marie, Op.Cit, p.10.

[2] أحمد يوسف كيطان، استراتيجية الأمن السيبراني الصيني، قراءة في قانون الأمن السيبراني الصيني، 2019.

القطاع بحدود (233) مليار دولار أمريكي أي إنه يشكل نسبة 20% من الانفاق العالمي في مجال البحث والتطوير.

د- دوافع عسكرية.

إن التطبيقات الالكترونية في مجال تأمين الدفاع الوطني إذ ركزت الصين على تكنلوجيا المعلومات والاتصالات من أجل توظيفها في الحروب المستقبلية ذات الطابع الرقمي، وتطمح الصين لاحتلال مواقع متقدمة في هذا المجال بحلول عام 2050 إذ بذل الخبراء العسكريون جهود مضنية في بناء استراتيجيات تمكنهم من استغلال المجال السيبراني في مختلف الاحتمالات الهجومية والدفاعية، بناءً على ذلك تلعب العمليات العسكرية الالكترونية دوراً هاماً في السيناريوهات العسكرية المتعلقة بتايون والنزاعات الاقليمية والبحرية الأخرى.

لقد تطورت مستوى الهجمات السيبرانية الصينية ضد الإدارة الامريكية والمؤسسات الصناعية والتجارية الأمريكية وهذا ما أكدته شركات الأمن الالكتروني الأمريكية رغم إنكار الصين لهذه الاتهامات. (1)

ونتيجة للرؤية الصينية للرئيس شي جين بينغ انخرط القادة العسكريون بوضع استراتيجية عسكرية لتنفيذ هذه الرؤية في الجانب العسكري وكان التهديد المرصود من قبلهم هو الخشية من أن تؤدي الهجمات السيبرانية على الشبكات الحكومية والخاصة إلى تعطيل خدمات حساسة وأن يتم استغلالها في عمليات عدائية ضد الصين ومصالحها في المنطقة والعالم ونتيجة لذلك أعلن جيش التحرير الشعبي الصيني عن مخططاته لتسريع تطوير قواته السيبرانية وتحسين دفاعات الشبكة الصينية.

ثالثاً : السيادة السيبرانية من المنظور الصيني.

تعد الصين الدولة الأولى التي أطلقت مفهوم الانترنت السيادي في العالم. والمقصود هنا فرض سيطرة مطلقة من جانب الدولة على الشبكة العنكبوتية والتحكم ومراقبة تبادل المعلومات عبرها وحجب المواقع الخارجية المضرة بالأمن القومي الصيني. إن عمل الشبكة العنكبوتية في الصين خاضع لما يسمى (جدار الحماية العظيم) وهو عبارة عن مجموعة من الإجراءات القانونية والتقنية تهدف إلى جملة قرارات منها منع الأفراد من استخدام الشبكة لأغراض تضر بالأمن القومي.

[1] إسراء أحمد إسماعيل، السيادة السيبرانية، عناصر الاستراتيجية الصينية للأمن الالكتروني، 2019.

بدأت الصين بتنفيذ مشروع (جدار الحماية العظيم) 1998 وأنجزت جميع مراحل المشروع بحلول 2008 واستخدمت فيه تقنيات غربية متقدمة، إذ يقوم جدار الحماية بحجب المحتوى ومراقبة الفيديو والتعرف على الوجوه وفي عام 2013 تم تشكيل مجموعة القيادة المركزية لأمن المعلومات التي تعمل تحت إشراف مباشر من الرئيس الصيني شي جين بنغ الذي أعلن عن مخطط تحويل الصين إلى (قوة سيبرانية عظمى) وهو مشروع طموح حقق خطى متقدمة في هذا المجال كما تهدف الصين إلى بناء نظام دفاع سيبراني متين، وقبل هذا المشروع كانت السياسة السيبرانية مبعثرة بين عدد من الدوائر الحكومية المختلفة وتم تأسيس (إدارة الفضاء السيبراني الصينية) ومهمته السيطرة على محتوى الانترنيت وصيانة الأمن السيبراني والمشاركة في حكم عالمي للفضاء السيبراني.

وبذلك فإن المفهوم الصيني للسيادة السيبرانية يقدم لنا نموذج واسع وشامل أكثر اتساعاً وشمولية من الرؤية الأمريكية لأنه يتضمن استخدام المعلومات للتأثير أو السيطرة على عملية صنع القرار لدى الأعداء وما يترتب عليها من أنشطة وذلك لخدمة الأهداف الصينية الهجومية والدفاعية.

وأخيراً فقد قدمت الصين مفهوم السيادة السيبرانية كمبدأ تنظيمي لحكم الانترنت في تعارض مباشر مع الدعم الذي توفره الولايات المتحدة للأنترنيت العالمي مفتوح وعلى حد قول الرئيس شي جي بنغ فإن السيادة السيبرانية تمثل حق كل دولة باختيار طريقها الخاص إلى التنمية السيبرانية.

رابعاً : التحديات التي تواجه الأمن السيبراني الصيني.

على وجه العموم هنالك عدة تحديات تواجه الأمن السيبراني وقد تسببت جائحة (Covid 19) بمفردها في حدوث اضطراب غير مسبوق على الصعيد الدولي وتحول 96% من الموظفين إلى العمل الكامل من المنزل.

لقد واجه مسؤولوا تكنلوجيا أمن المعلومات العديد من التحديات الهائلة في مهمتهم لتوفير روابط آمنة للقوى العاملة المشتتة مع الحفاظ على الحماية الكامنة ضد الهجمات السيبرانية وأصبح عام 2021 يواجه عدة تحديات منها الذكاء الصناعي، الخداع السيبراني، العمل عن بُعد.[1]

تواجه الصين تحديات أمام اعتماد سيادتها السيبرانية أهمها :

[1] تحديات الأمن السيبراني، مركز النهرين للدراسات الاستراتيجية، مستشارية الأمن الوطني، بغداد، 2018.

أ) الاعتراف بالفضاء السيبراني كمجال حيوي سيادي، كون الدول تمارس سلطة عليه فوجوده يتطلب هندسة مادية وبحاجة إلى تقنين لكي يعمل بفاعلية، إضافة إلى انعدام الشفافية الحكومية في الصين يفاقم المشكلة ويعقدها.

ب) تأسيس نظام فعال قادر على تحديد الدول الفاعلة في الفضاء السيبراني بدقة وهذه تعد مهمة شاقة نظراً لعدم القدرة على إسناد مسؤولية الهجمات الالكترونية إلى طرف محدد، لذلك يبدو أن الدول مترددة في قبول المسؤولية عن الأنشطة السيبرانية الناشئة من أراضيها.

ج) رسم معالم حدود الفضاء السيبراني لكي تستطيع الدولة مراقبته والتحكم فيه فعدم التمكن من القيام بهذه الوظيفة يفرغ الفضاء السيبراني من مضمونه.

د) خلق توافق آراء بشأن ما يشكل رد فعل معقول دفاعاً عن السيادة والأمن الوطني فإن ضعف الإسناد يزيد من عدم التأكد من مدى صحة توجيه رد الفعل إضافة لذلك يمكن أن يكون الرد غير متكافئ أحياناً.

هـ) نمو النفقات في صناعة أمن المعلومات في الصين من نحو (527) مليون دولار في 2003 إلى (2.8) مليار دولار عام 2011 وكل ذلك التوسع يعاني من عدم وجود تخطيط شامل وكذلك لا مركزية في سلطة اتخاذ القرار.

و) هنالك تحديات إقليمية ودولية تواجه الصين وتؤثر في أمنها السيبراني وتدخل في إطار المصالح التي تحرص بعض الدول في مواجهة الصين، ورغم أن الأمن السيبراني هو أمن جماعي وبالتوافق الدولي وليس بالتحديات والمقاطعات الدولية.

تعتبر الصين استراتيجية الأمن السيبراني 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 السيبرانية الأمن الصيني في المجالات المختلفة.[1]

لذا وضعت الصين في مقابل هذه التحديات أهدافاً رئيسية لتعبئة الحرب السيبرانية في بكين ومن أبرزها تدريب الموظفين العسكريين والمدنيين على الحروب السيبرانية وتشكيل وحدات حربية ووحدات احتياط متخصصة في مجال الفضاء والأمن السيبراني.

[1] السيادة السيبرانية، عناصر الاستراتيجية الصينية للأمن الألكتروني، المستقبل للأبحاث والدراسات المتقدمة، 2015.

من ذلك يتبين أن الصين برزت من بين الدول التي تحاول الحفاظ على سيادتها السيبرانية واستقلالها عن الدول الأخرى وبنفس الوقت تعمل الحكومة الصينية على صيانة أمنها السيبراني من خلال مراقبة المواقع الغربية التي تقدم برمجيات ونشاطات ذات مساس خطير بالأمن القومي الصيني ودأبت على الحد من نشاط هذه المواقع في الصين وتحاول أن تطور وتعزز صناعة الأمن السيبراني الصيني وذلك انطلاقاً من إدراك الصين أن القوة السيبرانية مكون مهم لضمان مكانة الصين الاقليمية والدولية، رغم وجود العديد من التحديات والكوابح التي تواجه الصين ذلك أن تنسيق السياسات السيبرانية بين أجهزة الدفاع وإنفاذ القانون والهيئات التنظيمية يشكل تحدي كبير بالنسبة لأي دولة في العالم.

خامساً : مستقبل الأمن السيبراني الصيني.

لقد أشار الرئيس الصيني شيء جي ينغ إلى أن ((من أجل إضفاء قوة دافعة جديدة على نمو الاقتصاد العالمي نحتاج بشكل ملح إلى تسريع وتيرة نمو الاقتصاد الرقمي)) لذا فقد أطلقت الصين ((مبادرة أمن البيانات العالمية التي قدمت حلاً صينياً بوضع القواعد للحوكمة الرقمية العالمية الأمر الذي لاقى تقديراً إيجابياً واسع النطاق من قبل المجتمع الدولي.[1]

وبالنظر إلى حجم الصين وتقدمها التكنلوجي، ثمة إمكانية وإرادة لنجاح بكين وبالتالي لأن تعيد تصميم الفضاء السيبراني على صورتها وإن حدث ذلك فسيكون الانترنيت أقل عالمية وانفتاح حيث سيجري جزء كبير منه عبر تطبيقات صينية على أجهزة رقمية مصنعة في الصين وهو ما سيمكن الصين من الحصول على مكاسب اقتصادية ودبلوماسية وأمنية.

هنالك ثلاث تكنولوجيات سيكون لها الثقل الأكبر في قدرة الصين على تشكيل الفضاء السيبراني الصيني مستقبلاً، أشباه الموصلات والحوسبة الكمية والذكاء الصناعي.

ومن المحتمل أن تتمكن الصين من فرض أقوى تأثير لها على حكم الانترنيت العالمي من خلال سياستها التجارية والاستثمارية وعلى وجه الخصوص مبادرة الحزام والطريق الصينية[2] وهي الجهود الجبارة لبناء بنية تحتية تربط الصين بالمحيط الهندي والخليج العربي وأوروبا بجانب أكثر من (50) مليار دولار أمريكي كانت قد تدفقت إلى سكك الحديد والطرق وأنابيب الغاز والموانئ والمناجم والخدمات على

[1] http://gateahram.org.eg/news/2687031.aspx.

[2] وانغ أي وي، الحزام والطريق، ماذا ستقدم الصين للعالم، ترجمة رشا كمال وشيماء كمال، ط1، دار سما للنشر والتوزيع، القاهرة، 2017.

طول الطريق، فقد أكد 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 الذكية.

كما أن الصين تصبو إلى تحديد الموجة القادمة من الابتكار لاسيما تكنلوجيا الجيل الخامس من شبكات الهاتف المحمول (G5) التي ستتيح سرعات أعلى من الانترنيت لمستخدمي الهاتف المحمول وتوفر استخدامات جديدة للأجهزة الموصولة بالانترنيت.[1]

إن الطموحات الصينية كبيرة في هذا المضمار رغم التحديات[2*] التي يبدو أنها سوف لا تلحق ضرراً بالغاً فالبلاد كبيرة وقوية وماضية في التطور والصعود السلمي والتنمية السلمية، وهذا ما يجعل الولايات المتحدة الأمريكية تلجأ للعمل مع حلفائها وشركائها التجاريين للضغط على بكين بحيث تتيح السوق الصينية للشركات الأجنبية ويتعين على صناع السياسة الأميركان الانتقال من نموذج ((القاعدة إلى القمة)) الذي يقوده القطاع الخاص لرؤية إ]جابية تتيح للدول النامية بدائل واقعية عن العمل من خلال الأمم المتحدة وحدها ولكن رغم كل الاجراءات الأمريكية والجهود فإن مستقبل الفضاء السيبراني سيكون صينياً أكثر منه أمريكياً من خلال المعطيات الواقعية.

الخاتمة :

برزت قضية الأمن السيبراني كأحد أهم التحوطات من الصراعات السياسية والاقتصادية بين الدول نتيجة الحروب الالكترونية أو الحروب السيبرانية التي تستهدف البنى التحتية والمنشآت والمؤسسات الحكومية والشبكات الصناعية والأبحاث وهي بشكل أو بآخر قادرة على تعطيل تشغيل البنى التحتية الحيوية، وفي هذا السياق لابد من التركيز على القدرات الصينية السيبرانية التي شغلت لباب المعنيين بالشؤون الدولية سيما وأن القضية تتعلق بالأمن القومي الصيني. إذ يرى المحللون العسكريون الصينيون أن الحرب السيبرانية هي حرب استراتيجية في عصر المعلومات كما كانت الحرب النووية في القرن

[1] فرح عصام، استراتيجية (تشي) الثورية كيف تغير الصين مستقبل الانترنيت في العالم، مركز الجزيرة، 2020.

[2]* من هذه التحديات الهجمات الالكترونية التي تعرضت لها عام 2019 والتي بلغت (62) مليون هجوم ضد أجهزة الكومبيوترات الصينية وبحسب فريق الأمن السيبراني التابع للحكومة الصينية وقد تبين أن نصف هذه الهجمات كانت من مصادر أمريكية. صحيفة القدس العربي/ آب 2020.

العشرين وقد كانت المنافسة خارج إطار الجيش الصيني لأن الحرب السيبرانية كانت خارج هذا الإطار مما أثر سلباً على الاقتصاد الصيني وحتى على مستوى التنمية الاجتماعية.

إن الاستراتيجية الصينية العسكرية تشمل أهداف منها وحدة الوعي بالفضاء السيبراني وهنالك فرق وتشكيلات الدفاع السيبراني للدفاع عن المؤسسات الحساسة وأعطت الحكومة الصينية مع وصول الرئيس شي جين بنغ عام 2013 اهتماماً واسعاً بهذه المسألة نتيجة الأحداث التي عصفت بالعالم ومنها التظاهرات والاحتجاجات والصراعات التي اجتاحت الصين يوليو عام 2009 في إقليم سنجان بين الايغور والهان في الصين، وأحداث الربيع العربي والهجمات السيبرانية المتكررة التي وصلت إلى (800) مليون هجوم في اليوم الواحد عام 2018 مما دفع الحكومة الصينية إلى انتهاج استراتيجية هجومية وتشكيل مجموعة القيادة المركزية للأمن المعلوماتي مع مجيء الرئيس شي جين بنغ.

لقد كان للصين دوافع عديدة للقوة السيبرانية وتعزيزها منها سياسية، اقتصادية، عسكرية، أمنية. وتعد الصين الدولة الأولى التي أضفت الطابع السيادي للسيبرانية لأنها فرضت سيطرة مطلقة من جانب الدولة وأصبحت خاضعة لما يسمى (جدار الحماية العظيم) مع إبداء تعاون واسع النطاق مع الدول في هذا المضمار.

إن الصين ورغم التحديات والعقبات الكبيرة التي توجهها في مجال الفضاء السيبراني إلا إنها تمضى وبخطى سريعة نحو التطور والابتكار ليكون لها بصمة شاخصة وواضحة في الفضاء السيبراني مستقبلاً.