



اسم المقال: قوة الفضاء السيبراني : ساحة الصراع الجديدة بين القوى الدولية والإقليمية في القرن الحادي والعشرين

اسم الكاتب: م.د. هديل حربى ذارى

رابط ثابت: <https://political-encyclopedia.org/index.php/library/1576>

تاريخ الاسترداد: 2025/05/18 23:39 +03

الموسوعة السياسية هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.

لمزيد من المعلومات حول الموسوعة السياسية – Encyclopedia Political ، يرجى التواصل على [info@political-encyclopedia.org](mailto:info@political-encyclopedia.org)

استخدامكم لأرشيف مكتبة الموسوعة السياسية – Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام

<https://political-encyclopedia.org/terms-of-use>

تم الحصول على هذا المقال من موقع مجلة قضايا سياسية الصادرة عن كلية العلوم السياسية في جامعة النهرين ورفده في مكتبة الموسوعة السياسية مستوفياً شروط حقوق الملكية الفكرية ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.



E-ISSN : 2790-2404

P- ISSN 2070-9250

Qadaya siyasiyyat

وزارة التعليم العالي والبحث العلمي

جامعة النهرين

كلية العلوم السياسية

Ministry of Higher Education  
& Scientific Research  
Al-Nahrain University  
College of Political Science



# قضايا سياسية

# Political Issues

مجلة فصلية محكمة

العدد ٧٢  
Issue 72

Arab Impact Factor  
معامل التأثير العربي  
2022:(2.11)  
(Arcif) معامل تأثير  
2022:(0.1712)

كانون الثاني - شباط - آذار / ٢٠٢٣

Jan. - Feb - Mar. / 2023



# قضايا سياسية

## Political Issues

جامعة النهرين  
كلية العلوم السياسية  
E-ISSN 2790-2404  
P- ISSN 2070-9250  
(معامل التأثير العربي 2022 : 2.11 )  
معامل ارسيف Arcif ( 2022 ) 0.1712  
DOI prefix: 10.58298

مجلة فصلية محكمة تعنى بنشر الأبحاث والدراسات السياسية العراقية والعربيّة والدولية

<http://pissue.iq>

مدير التحرير

أ. د. علي حسين حميد

كلية العلوم السياسية - جامعة النهرين

رئيس هيئة التحرير

أ. د. عماد صلاح الشيخ داود

كلية العلوم السياسية - جامعة النهرين

هيئة التحرير

المساعد الاسبق لرئيس جامعة بغداد للشؤون العلمية .  
جامعة كلکاری-قسم العلوم السياسية (كندا) .  
جامعة النهرين - كلية العلوم السياسية .  
المركز العربي للباحث (النوبة - قطر) ..  
عميد كلية الآمال الجامعية .  
جامعة النهرين - كلية العلوم السياسية.  
جامعة صلاح الدين - كلية العلوم السياسية.  
جامعة النهرين - كلية العلوم السياسية.  
الكلية الجامعية للاعنة حقوق وحقوق الانسان (بيروت-لبنان).  
جامعة ماري وود ( الولايات المتحدة الاميركية ).  
وزارة التعليم العالي ( المملكة المغربية ).

أ.م.د.رياض عزيز هادي  
أ.د. طارق يوسف اسماعيل  
أ.د. منعم صالح حسین  
أ.د. عبد الفتاح ماضي  
أ.د. عامر حسن فياض  
أ.د. قاسم محمد عبد علي  
أ.د. سرمد زكي حامد  
أ.د. عبد الصمد سعدون عبدالله  
أ.د. لبني خميس مهدي  
أ.د. هشام حكمت عبد السنوار  
أ.د. محمد ياس خضرير  
أ.د. نوزاد عبد الرحمن الهيتي  
أ.د. شيرزاد امين  
أ.د. احمد غالب محي  
أ.د. عبد الحسين شعبان  
د. الكسندر داودي  
د. فاطمة مهاجر

أ. د. نصر محمد علي  
تدقيق اللغة الانكليزية

أ. د. عبد العظيم جبر حافظ  
تدقيق ابحاث طلبة الدراسات العليا

أ.م.د.حذام بدر حسين  
تدقيق اللغة العربية

التنسيق الفني والمتابعة  
المدرس محمد محي الجنابي

تنسيق الموقع الالكتروني  
مبرمج . رؤى جعاز

الشئون المالية  
م. مدير علي عبد الله جابر

التنسيق الاداري  
م. مدير شيماء بشير موسى

البحوث المنشورة تعبر عن آراء أصحابها وليس بالضرورة عن رأي المجلة

## قواعد النشر

- لغة المجلة هي اللغة العربية والإنكليزية على أن يراعى الوضوح وسلامة النص.
- ترحب المجلة بنشر البحوث والدراسات السياسية النظرية والتطبيقية ولا سيما التي تجعل من قضايا المنطقة والعالم محط اهتمامها، ماضياً وحاضراً ومستقبلاً، وعلى وفق الآتي:
  - أن لا يزيد عدد صفحات البحث أو الدراسة عن (25) صفحة مطبوعة بثلاث نسخ مرفقة مع قرص مرن (CD)، مع مراعاة حجم الخط (14) والتبعاد (1,15) ونوع الخط Simplified Arabic على أن تكون الهوامش أسفل كل صفحة مطبوعة بالطريقة الإلكترونية وبحجم خط (11) ونوع الخط Simplified Arabic وتجمع بقائمة منفصلة عن المصادر في نهاية البحث.
  - أن تعتمد الأصول العلمية المتعارف عليها في إعداد البحوث والدراسات وكتابتها وبخاصة التوثيق حيث تتضمن:
    - بالنسبة للكتاب الآتي: أسم المؤلف، عنوان الكتاب، مكان النشر، الأسم الكامل للناشر، تاريخ النشر، أرقام الصفحات.
    - اما بالنسبة للمقالة: فتتضمن أسم الكاتب، عنوان المقالة، اسم الدورية، مكان صدورها، عددها، تاريخها، وأرقام الصفحات.
    - أن تتصف البحوث والدراسات بالموضوعية والدقة العلمية.
    - أن تعتمد الترقيم العشري للعناوين الأساسية والفرعية او التصنيف المعياري العام.
    - يرفق مع كل بحث او دراسة ملخصين (احدهما باللغة العربية والآخر باللغة الانكليزية) وقائمة بالمراجع والمصادر المعتمدة.
  - تخضع جميع البحوث المقبولة للنشر الى نظام الاستلال الإلكتروني في كلية العلوم السياسية – جامعة النهرين.
  - يرفق مع كل بحث ودراسة سيرة ذاتية مختصرة للباحث.
  - تقوم المجلة بإخطار الباحثين بإجازة بحوثهم أو دراساتهم بعد عرضها على محكمين تختارهم على نحو سري من بين أصحاب الاختصاص.
  - يجوز للمجلة أن تطلب إجراء تعديلات شكلية أو شاملة على البحث أو الدراسة قبل إجازتها للنشر بما يتماشى مع أهدافها.
  - لا تلتزم المجلة بإعادة البحوث والدراسات التي يعتذر عن نشرها.

- ترحب المجلة بالمناقشات الموضوعية لما ينشر فيها أو في غيرها من الدوريات وبأية ردود فكرية أو تصويب، وكذلك ترحب بنشر التقارير عن المؤتمرات والندوات ذات العلاقة ومراجعات الكتب وملخصات الرسائل الجامعية التي تم إجازتها على أن تكون من إعداد أصحابها.

توجه جميع المراسلات إلى رئيس التحرير على العنوان الآتي

مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين-بغداد - الجادرية.

E.mail: [pirj@ced.nahrainuniv.edu.iq](mailto:pirj@ced.nahrainuniv.edu.iq)

[www.Pol-Nahrain.org](http://www.Pol-Nahrain.org)

الرقم الدولي ISSN 2070-9250

## جدول المحتويات

رقم الصفحة	اسم البحث	المسلسل
15_1	اشكالية العلاقة بين الوكالات الدولية المتخصصة التابعة لمنظمة الامم المتحدة أ.د.أسامة مرتضى باقر م.م. سيف حمزة لفته	1
30_16	السياسة الإيرانية تجاه العراق في ظل المتغيرات الجيوسياسية في منطقة الشرق الأوسط (الأولويات، والرهانات، والتحديات) م. د امنة علي سعيد د. فراس عباس هاشم	2
49_31	إشكال تداعيات الإرهاب السياسية والاجتماعية على الشباب في العراق بعد العام 2003 أ.م.د. حمد جاسم محمد الخزرجي المدرس: سعد محمد حسن الكندي أ.م. علي مراد كاظم النصراوي	3
66_50	العلاقة بين روسيا واليمين الأوروبي الشعبي المتطرف: الدوافع والتوظيف السياسي أ. د عماد صلاح الشيخ داود خضير عباس حسين الدهلكي	4
96_67	الأطراف المصغرة في العلاقات الدولية ومستقبل تعددية الأطراف في النظام الدولي(تحليل مقارنٌ بين النظريتين الليبرالية والواقعية الجديدة) الدكتور سومر منير صالح	5
117_97	الاتجاهات الاستراتيجية لسياسة الولايات المتحدة الأمريكية تجاه القضية الفلسطينية بعد العام 2017 م. د. عباس فاضل علوان	6
149_118	عمالة الأطفال في العراق بعد العام 2003 ... الواقع والحلول م. د. عدنان عبد الامير مهدي الزبيدي	7
172_150	ملامح توظيف الفضاء السيبراني في عالمنا المعاصر (الحرب الروسية - الأوكرانية انماذجا) أ.د. علي حسين حميد أنقام عادل حبيب	8
196_173	السياسة الخارجية الصينية تجاه المنطقة العربية (2012 - 2017) أ. م. د. عمر عبد الله عفتان	9
213_197	الأهمية الاستراتيجية لمجموعة (بريكس) في مدرك الدول الساعية للانضمام م.م. فاطمة محمد رضا	10
226_214	دور مرتزقات الاقتصاد الأفغاني في علاقاته الدولية أ.م.د. فايلق حسن جاسم	11
257_227	توظيف القوة الذكية في الاستراتيجية التركية تجاه المنطقة العربية بعد عام 2011 أ.م.د. مروان سالم علي	12

283 _258	الامن المائي في العراق دراسة في التحديات والممكنا أ.م.د مصطفى فاروق مجید	13
310 _284	العقوبات الاقتصادية كوسيلة ضغط في السياسة الدولية: إيران إنماذجاً م.م . منى حبيب احمد محمد العبيدي	14
337 _311	تحديات السياسات الاقتصادية الاوربية المشتركة في ظل النظام الدولي الجديد أ.م.د نسرين رياض شنشول	15
367_338	قوة القضاء السبيراني : ساحة صراع جديدة بين القوى الدولية و الاقليمية في القرن الحادي والعشرين م.د هديل حربي ذاري	16
392 _368	ظاهرة الفساد السياسي في دولة غانا وانعكاسه على التنمية البشرية المستدامة م.م هند جمعه علي أ.م.د استبرق فاضل شعير	17
418_393	ظاهرة الإرهاب والتطرف وانعكاساتها على السلم والاستقرار الدولي أ.م.د. وفاء ياسين نجم	18
484 _419	الوعي الظبقي في الفكر السياسي الماركسي الحديث (نماذج مختارة) أ.م.د عبير سهام مهدي م. وليد مساهر حمد	19

قوة الفضاء السيبراني : ساحة صراع جديدة بين القوى الدولية والإقليمية في القرن الحادي والعشرين<sup>٧</sup>

The Power of Cyberspace: A New Arena of Conflict Between International and Regional Powers

م.د هديل حربي ذاري\*

hadeel harbi thare

الملخص :

أدت الثورة التكنولوجية والمعلوماتية إلى بروز الفضاء الإلكتروني ليكون أحد مجالات التنافس والصراع بين القوى الدولية والإقليمية ، الامر الذي دفع إلى ظهور مفهوم الحرب الإلكترونية أو السيبرانية، التي تتم من خلال الهجمات الإلكترونية ، والتحكم والسيطرة على أجهزة الحاسوبات والمعلومات والشبكات الإلكترونية والبنية التحتية المعلوماتية ، الامر الذي عدها البعض جزء من حروب المستقبل، وأنها لا تقل خطورة عن الحروب التقليدية ، من حيث التهديد الذي تتطوي عليه ، وحجم التدمير الذي يمكن أن تؤدي إليه ، اذ ما اخذ بنظر الاعتبار السرعة الفائقة ، والانتشار الواسع ، وكونها تتفّذ بأساليب يصعب تتبعها في كثير من الأحيان .

الكلمات المفتاحية : الصراع السيبراني ، الولايات المتحدة ، الصين ، روسيا ، ايران ، إسرائيل .

Abstract :

The technological and information revolution has led to the emergence of cyberspace as an area of competition and conflict between international and regional powers, which prompted the emergence of the concept of electronic or cyber warfare. The latter is carried out through electronic attacks and the control of computers, information, electronic networks and information infrastructure. Some see cyber wars as part of future wars, and they are no less dangerous than conventional wars, in terms of the threat they pose, and the size of the destruction they can lead to, given the high speed, wide spread, and the fact that they are implemented in ways that are often difficult to follow.

**Keywords:** cyber conflict, the United States, China, Russia, Iran, Israel.

المقدمة :

ادى اتساع تأثير العامل التكنولوجي في السياسات الدولية ، بعد انتهاء الحرب الباردة ، الى اضافة ابعادا اخرى للقوة العسكرية ، إذ تلاشت الفواصل والحدود بين ما هو مدنى وعسكري ، لاسيما بعد ان اخذت الصراعات سمات غير تقليدية ، سواء من حيث الفاعلون او القضايا او ديناميات التفاعل في عالمنا الحالى ، من خلال بروز المجال السيبراني كحالة جديدة من أنماط الصراع ، الامر الذي حول الفضاء السيبراني الى ساحة مشابهة للحرب الباردة الجديدة بين الولايات المتحدة والصين وروسيا ، للتنافس على قيادة النظام الدولي، فضلا عن التنافس الذي ولده بين بعض القوى الإقليمية كإيران وإسرائيل ، ذلك لإظهار نفسها كأحدى القوى المؤثرة في نظامها الإقليمي ، فضلا عن النظام العالمي ، الامر الذي افرز حالة من الاستقطاب بين الشرق والغرب ، ودور الثورة الصناعية الرابعة في تراتبية القوة في النظام الدولي.

**أهمية البحث :** يمثل الفضاء السيبراني كمجال خامس جديد في العلاقات الدولية ، تأثير ذات أبعاد مختلفة ، جراء الارتباط بمصالح الكترونية واسعة وممتدة وعابرة للحدود ، ما جعلها عرضة لخطر الاعتداء من قبل قوى أخرى ، لاسيما مع تحول الفضاء السيبراني إلى مجال عالمي مفتوح ، وتصاعد اتجاهها مضادا من قبل دول أخرى في محاولة لضبط حركة التفاعلات بين الداخل والخارج ، واستعادة وظيفة الدولة في الأمن والدفاع في ظل تلك المتغيرات الجديدة ، وتأثيرها على السيادة على الشعب ، والإقليم ، والثروة والأفكار ، وتصاعد دور للفاعلين من غير الدول ، لذا سعى البحث إلى توضيح الأهمية التي أحدثها الفضاء الإلكتروني ، ومدى انعكاسه على مفاهيم القوة والصراع ، من خلال تحول الصراع من مادي إلى افتراضي ، الامر الذي دفع الدول إلى تأمين الفضاء الخارجي .

**إشكالية البحث :** تتطرق الدراسة من إشكالية مفادها " لقد شكلت القوة السيبرانية عنصر قوة اضافي للدول من أجل الحفاظ على أنها القومي، الامر الذي جعلها تتسابق فيما بينها للوصول إلى عناصر القوة السيبرانية ، لمجارات التطورات الحاصلة في النظام الدولي ، وضافتها كعنصر قوة للدولة إلى جانب القوة العسكرية والاقتصادية " .

**فرضية البحث:** من الاشكالية المطروحة سنحاول اثبات الفرضية الآتية " إن من يمتلك القدرة على السيطرة على الفضاء الإلكتروني (السيبراني) ، سيمتلك التأثير في مسارات تدفق المعلومات والاتصال ،

بوصف ذلك معيارا اساسيا لنقدم الدول والمجتمعات من جهة، ومدخلا يمكن للاطراف المختلفة توظيفه في صراعاتهم نحو تحقيق اهدافهم ومصالحهم من جهة اخرى".

هيكلية البحث سيتم التطرق في هذه الدراسة ومن خلال ثلات محاور الى ، طبيعة ومفهوم الصراع السيبراني ، واهم القوى الدولية والاقليمية المتنافسة في هذا المجال من خلال اخذ نماذج مختارة ، فضلا عن تناول مستقبل القوة السيبرانية في القرن الحادي والعشرين .

### أولاً طبيعة ومفهوم الصراع السيبراني

شكلت القفزات التكنولوجية الهائلة في مجال الاتصالات والمعلومات في اواخر القرن العشرين وبداية القرن الحادي والعشرين ، سياقات جيدة لنشوب صراعات حول "النفوذ السيبراني" في الفضاء الالكتروني ، إذ عد الاخير ساحة واسعة للتفاولات العالمية ، انطوت في الاساس على شبكات رقمية ذات صلة بين اجهزة الحاسوب ، وانظمة الاتصال والانترنت المختلفة بغرض تدفق المعلومات ، لذا بدأت الدول تبحث عن كيفية الحفاظ على امن الشبكات والانظمة المعلوماتية ، والاجهزة المتصلة بالانترنت ، وفي هذا السياق قدمت وزارة الدفاع الامريكية "البنتاجون" تعريفا دقيقا لمصطلح الامن السيبراني بأنه " جميع الاجراءات التنظيمية ، الالزامية لضمان حماية المعلومات بجميع اشكالها ، الالكترونية والمادية من مختلف الجرائم ، والهجمات ، والتجسس ، والتخريب ، والحوادث"<sup>1</sup> ، وعرفت الوكالة الفرنسية لامن انظمة الاعلام (ANSSI) الفضاء السيبراني على انه : "فضاء التواصل المشكل من خلال الرابط البيئي العالمي لمعدات المعالجة الآلية للمعطيات الرقمية"<sup>(2)</sup> ، وعليه يتمحور مضمون الصراع السيبراني حول من يمتلك القدرة على التأثير في الفضاء الالكتروني ، سيمكن من تحقيق اهدافه ومصالحه ، وفي هذا الصدد بلور جوزيف ناي ما سمي " القوة السيبرانية Cyber Power " ، وحددها بأنها " محاولة تحقيق اهداف ومصالح معينة ، عبر استخدام مصادر المعلومات والادوات الاتصالية المرتبطة بالفضاء الالكتروني "<sup>(3)</sup>.

<sup>1</sup> صلاح مهدي هادي ، زيد محمد علي ، " الامن السيبراني كمركز جديد في الاستراتيجية العراقية " ، مجلة قضايا سياسية ، كلية العلوم السياسية ، جامعة النهرين ، العدد (62) ، 2020 ، ص 275.

<sup>(2)</sup> اسماعيل زروقة ، " الفضاء السيبراني والتحول في مفاهيم القوة والصراع " ، مجلة العلوم القانونية والسياسية ، المجلد (10) ، العدد (01) ، الجزائر ، 2019 ، ص 1017 .

<sup>(3)</sup> خالد حنفي علي ، " اشكاليات تداخل الصراعات السيبرانية والتقليدية " ، مجلة السياسة الدولية ، مركز الاهرام للدراسات السياسية والاستراتيجية ، القاهرة ، المجلد 52 ، العدد 208 ، 2017 ، ص 3 .

ويتناول مفهوم القوة السيبرانية جميع القضايا التي تتعلق بالتقاعلات الدولية سواء كانت عسكرية ، او اقتصادية ، او سياسية ، او ثقافية ، او اعلامية ، او غيرها ، وحتى تتمكن الدول من ممارسة نفوذها داخليا وخارجيا من خلال قوتها السيبرانية ، يجب ان توفر لديها مجموعة من العناصر<sup>(1)</sup> :

1. وجود بنية تحتية سيراني ؛ وتشمل : اجهزة الكمبيوتر ، وشبكات الاتصالات ، والبرمجيات ، وقواعد البيانات لمختلف الانظمة والقطاعات .
2. بنية مؤسسة ؛ تتولى ممارسة القوة السيبرانية وتحقيق الامن السيبراني للدولة .
3. بنية تشريعية ؛ تكون ضامنة ومحددة لاستخدام القوة السيبرانية .
4. إستراتيجية بأهداف واضحة ؛ بحيث تحدد طرق العمل والاهداف المرجوة .
5. تطوير اسلحة في مجال الحرب السيبرانية لاستعمالها في العمليات الهجومية او من اجل الردع .

في هذا السياق ادركت الولايات المتحدة كقوة باحثة عن استمرار هيمنتها العالمية ، اهمية تأثير العامل التكنولوجي والمعلوماتي في بنية موازين القوى العالمية ، اذ وضعت التقوّق المعلوماتي ك المجال لزيادة قدراتها ، وحرمان خصومها منه ضمن استراتيجيتها القومية لقرن الحادي والعشرين ، واتسع هذا الهدف الامريكي ليشمل مجال القرارات السيبرانية في مجال الاتصالات والمعلومات ، مع تزايد التنافس العالمي على حيارة النفوذ في الفضاء الالكتروني ، فضلا عن صعود مفهوم القوة الذكية ، الذي عبر عن التلاقي بين القوتين الصلبة والناعمة بغرض تحقيق اهداف السياسة الامريكية بفعالية اكبر<sup>(2)</sup> ، لاسيما مع توجّه الصين وفقا لاستراتيجيتها الجديدة "صنع في الصين 2025" ، والخطة الخمسية الثالثة عشر ، الى تسليط الضوء على امن الفضاء الالكتروني الوطني كمشروع سيكتمل في عام 2030<sup>(3)</sup> ، لذا اصبح الصراع السيبراني شكلا من اشكال التنافس والصراع العالمي ، اذ عد سلاح المعلومات احد اهم الاسلحة التي تستخدمها الدول ، لاسيما المتقدمة لتحقيق اهدافها الاستراتيجية وفقا لما اكده (ديفيد

<sup>(1)</sup> اسماعيل زروقة ، مصدر سبق ذكره ، ص ص 1018 – 1019 .

<sup>(2)</sup> خالد حنفي ، مصدر سبق ذكره ، ص 4 .

<sup>(3)</sup> President Xi Jin ping, "Speech to a National Conference on the Work of Cyber security and Informatization" . See: "Xi Outlines Blueprint to Develop China's Strength in Cyberspace," Xinhua, April 21, 2018, [http://www.xinhuanet.com/english/2018-04/21/c\\_137127374.htm](http://www.xinhuanet.com/english/2018-04/21/c_137127374.htm).

جومبرت) " إن أحد الآثار المهمة لثورة المعلومات هو احتمال الواقع الوشيك لحرب المعلومات ، أي الحرب التي يتم خوضها بالمعلومات بوصفها سلاحاً أو هدفاً رئيساً " <sup>(1)</sup> .

وعليه ، تبلورت ظاهرة " الصراع السيبراني Cyber Conflict " ، لتثير تحدياً أمام العلماء والباحثين من أجل فهم طبيعتها وقضاياها ، إذ ان السيبرانية كمصطلح تعني كل ما يتعلق بالنتاج الإلكتروني من حواسيب وشبكات إنترنت ، المعبّر عنه بـ (الفضاء السيبراني) ، وهو فضاء افتراضي وهمي ، تجريدي وتخيلي ، بل وتجريبي يخضع للمنزلة ، ولكنه ديناميكي تبعاً لما يضمه من تفاعلات الكترونية في فضاء أقل ما يقال عنه انه معقد ومتغير ، تبعاً لملامسة فاعلية للقوة النسبية بانماطها المختلفة لاسيما في عصر العولمة <sup>(2)</sup> ، لذا اختلفت التعريفات المتعلقة بمصطلح الصراع السيبراني بسبب اختلاف وجهات النظر لدى الباحثين والجهات المهتمة بهذه الظاهرة ، فيعرف Gartzke الصراع السيبراني بأنه ، " ذلك الصراع الذي يتم خوضه حصرياً في الفضاء السيبراني " <sup>(3)</sup> ، ويوصف بأن هذا التعريف مقيداً لأنّه لايشمل الدعاية والتجسس وزعزعة استقرار النظام المالي للدولة والنتائج النفسية المحتملة ان تحدث ، ووفقاً لتعريف آخر أقل تعقيداً ، فإنّ بعد العسكري للصراع السيبراني يتسع ليشمل مجالات وتهديدات غير عسكرية ، وبالتالي فهو شكل من أشكال الحرب المعلوماتية التي تم تطويرها في الفضاء السيبراني ، ويمكن أن يشمل الصراع السيبراني زعزعة استقرار الأنظمة المالية والبنية التحتية الحيوية للحكومة ، من خلال التسلل إلى أنظمة الكمبيوتر لاغراض التجسس <sup>(4)</sup> .

ومع تحول الفضاء السيبراني إلى مجال متزايد لتنافس السياسات الخارجية للدول وغيرها من الفاعلين ، بات يعرف هذا الصراع في هذه الساحة الافتراضية (الصراع السيبراني) كونه استخدم تكنولوجيا الحاسوب في الفضاء السيبراني (الإلكتروني) لاغراض التدمير من أجل التأثير او التغيير ، او التعديل في التفاعلات الدبلوماسية والعسكرية بين الكيانات المختلفة ، وذلك بعيداً عن ساحة المعارك ، وقد يأخذ ذلك الصراع نمطين ؛ الاول : الحوادث الفردية (Cyber Incidents) : ويقصد بها العمليات والحوادث

<sup>(1)</sup> عمار مرعي ، " مستجدات البيئة الدولية ومستقبل الدولة القومية " ، في كتاب : مجموعة بباحثين ، " مطاراتن النظام الدولي " ، مصدر سبق ذكره ، ص ص 118 .

<sup>(2)</sup> عادل عبد الصادق ، " الفضاء الإلكتروني وتهديدات جديدة لامن القومي " ، مجلة السياسة الدولية ، مؤسسة الاهرام للدراسات الدولية والاستراتيجية ، العدد (180) ، 2010 ، ص 104 .

<sup>(3)</sup> Rory Michael Hermann, "Cyber War In A Small War Environment", ProQuest LLC, April 2017, p 11, see : <https://pqdtopen.proquest.com/doc/1892789852.html>.

<sup>(4)</sup> حسين قوادرة ، منى كحلوش ، " التداعيات الاقتصادية لحرب المعلومات السيبرانية " ، مجلة الناقد للدراسات السياسية ، الجزائر ، العدد (01) ، 2021 ، ص ص 209 – 210 .

الفردية التي تتم على مرات مختلفة ، وليست مستمرة لمدة معينة ، اما النمط الآخر ؛ فهو النزاعات السيبرانية (Cyber Disputes) : ، التي تدار افتراضية بين دولتين في مدة زمنية معينة ، ويحتوي واحد او اكثر من الحوادث الفردية<sup>(1)</sup> .

وكيفيات مقاربة للصراع السيبراني ؟ عرفت القيادة الاستراتيجية الامريكية عام 2007 ، الهجمات السيبرانية بأنها " تطويق عمليات نظام الكمبيوتر ، بهدف منع الخصوم من الاستخدام الفعال لها ، فضلا عن التسلل الى انظمة المعلومات وشبكات الاتصال ، بهدف جمع وحيازة ، وتحليل البيانات التي تحتويها"<sup>2</sup> ، اما الحرب السيبرانية ؛ فقد عرفتها وزارة الدفاع الامريكية بأنها " توظيف القدرات السيبرانية بهدف تحقيق غرض اساس يتمثل في تحقيق الاهداف او الاثار العسكرية في الفضاء السيبراني او من خلاله "<sup>3</sup> ، اما الردع السيبراني ، فيقصد به " منع الاعمال الضارة ضد الاصول الوطنية في الفضاء السيبراني ، ويرتكز على ثلاث ركائز ، تعد عماد استراتيجية الدفاع السيبراني ، وهي ؛ مصداقية الدفاع ، القدرة على الانتقام ، الرغبة في الانتقام "<sup>4</sup> اما الارهاب السيبراني ، فقد عرفته وزارة الدفاع الامريكية بأنه " عمل اجرامي يتم الاعداد له باستخدام الحاسوب ووسائل الاتصالات ، ينتج عنه عنف وتدمير ، او بث الخوف تجاه تلقي الخدمات بما يسبب الارياك وعدم اليقين ، وذلك بهدف التأثير على الحكومة او السكان ، لكي تمثل لاجندة سياسية او اجتماعية او فكرية معينة "<sup>5</sup> ، اما الجريمة السيبرانية ، فتعرف بأنها " هي التي تتم بواسطة الكمبيوتر او احد وسائل التقنية الحديثة على كمبيوتر اخر ، مع ضرورة توفر شبكة الاتصال فيما بينهما " ، او هي " نشاط اجرامي تستخدم فيه تقنية الحاسوب الالي بطريقة مباشرة او غير مباشرة كوسيلة او هدف لتنفيذ الفعل الاجرامي المقصود"<sup>6</sup> .

ما تقدم يمكن القول ، على الرغم من الفوائد الكبيرة التي يمكن ان يحققها الفضاء السيبراني ، والتي تعزز من قدرة الدول ، الا ان الفضاء السيبراني كمفهوم اضافي خامس للدول محفوف بالمخاطر

<sup>(1)</sup> Brandon Valeriano & Ryan C .Maness, "The Dynamics Of Cyber Conflict Between Rival An tagonists , , 2014 , Vol .51 , No :3, p.48 .

<sup>2</sup> احمد عبيس الفتلاوي ، " الهجمات السيبرانية : مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر " ، مجلة المحقق الحلي للعلوم القانونية والسياسية ، جامعة بابل العراقية ، العدد (4) ، 2016 ، ص ص 616 – 617 .

<sup>3</sup> Alex Michael , " Cyber Probing : The Politicization of Virtual Attack " , Defense Academy of the United Kingdom , 2010 , p.68 .

<sup>4</sup> علاء الدين فرات ، " من الردع النووي الى الردع السيبراني : دراسة لمدى تحقيق مبدأ الردع في الفضاء السيبراني " ، مجلة المفكر ، العدد 1، المجلد (16) ، الجزائر ، 2021 ، ص 272 .

<sup>5</sup> صلاح مهدي هادي ، زيد محمد علي ، مصدر سبق ذكره ، ص 281 .

<sup>6</sup> محمود احمد القرعان ، " الجرائم الالكترونية " ، (عمان : دار وائل للنشر والتوزيع ، 2017 ) ، ص 19 .

والتحديات التي تهدد البنية التحتية ، حتى اصبح اذا جاز القول " سلاح ذو حدين" ، اذ اصبحت العلاقة بين الامن والتكنولوجيا علاقة طردية ، مع امكانية تعرض المصالح الاستراتيجية ذات الطبيعة السيبرانية الى اخطار الكترونية ، الامر الذي اعاد التفكير في مفهوم الامن القومي للدول الكبرى ، الذي يعني بحماية قيم المجتمع الاساسية ، لذا يثار لنا التساؤل الاتي ، ما هي اهم سمات هذا الفضاء السيبراني ، ومن هم ابرز الفاعلين فيه ، وما هي التداعيات التي يفرضها هذا الصراع ، وهو ما سيتم تناوله في الاتي:

### 1 : سمات الفضاء السيبراني

اختصر الفضاء السيبراني حاجز الزمان والمكان ، وخلق مساحات للتفاعلات الداخلية والدولية في الواقع الافتراضي ، ومن ثم برزت فضاءات جديدة للصراع بأدوات مختلفة ، وانماط تختلف عن الصراعات التقليدية ، وتعود اسباب اهتمام الفاعلين سواء ا كانوا دولا او غيرها بهذا الفضاء ، ك المجال لتحقيق الهيمنة، وتنفيذ الاهداف ، وادارة الصراعات ، الى امتلاكه عدة سمات اساسية ، ابرزها ما يأتي:<sup>(1)</sup>

أ. ساحة صراع افتراضية : بما ان الفضاء السيبراني ليس مساحة جغرافية ، لذلك فأنه يتخطى العديد من الثنائيات التي تظهر في الصراعات التقليدية ، اذ يشارك في الصراعات ذات الطبيعة الالكترونية المدنيون والعسكريون ، كما ترتبط ايضا بالتطورات المادية السياسية والعسكرية على الارض ، كما انها تعد اقل تكلفة من حيث الخسائر المادية ، واكثر تحديا للهدف ، مقارنة بنظيرتها التقليدية .

ب. زيادة الاعتماد الالكتروني : اذ باتت الدول الحديثة تربط بنيتها التحتية بالفضاء السيبراني ، لاسيما شبكات الكهرباء والمياه ، والبنوك ، والبورصة ، والاتصالات وغيرها ، فضلا عن انظمة السيطرة والتحكم العسكرية ، وجمع المعلومات ، مثل الاقمار الصناعية ، والطائرات دون طيار في الحروب ، وعليه اصبح استهداف تلك البنية التحتية للدولة ذات الطابع الالكتروني احد عوامل الصراع السيبراني.

ج. تماهي حدود الداخل والخارج ، اي وجود حالة من التأثير الشبكي المتزايد داخل الدول وخارجها ، اذ اتسع استخدام الافراد ، والجماعات ، والدول للتكنولوجيا الحديثة المرتبطة بالفضاء السيبراني ، سواء اكانت موقع تواصل اجتماعي على الانترنت ، او هاتف ذكي ، او موقع للتعاملات المالية

<sup>(1)</sup> سماح عبد الصبور ، " الصراع السيبراني : طبيعة المفهوم وملامح الفاعلين " ، مجلة السياسة الدولية ، القاهرة ، العدد (208) ، 2017 ، ص 5.

والتجارية والخدمية ، ويتصل كل ذلك بشبكة مرتبطة من خلال انظمة تحكم تكنولوجية ترتبط بالانترنت ، بما يجعل الخدمات والمعلومات متاحة للجميع ، الامر الذي قد يعرضها للاستهداف . د. غياب الشفافية الالكترونية ، اذ مع عدم القدرة على معرفة هويات القائمين على هجمات القرصنة ، نشبت معضلة غياب الشفافية والقوانين المقيدة للصراعات في المجال الالكتروني ، فضلا عن ذلك ، فإن مصدر الهجمات الالكترونية قد يسبب خسائر واسعة ، دون ان يعني ذلك وجود عنف ملموس ، مما لا يعني بالضرورة وجود هجوم مضاد او استمرار الصراع .

## 2: طبيعة الفاعلين في الصراع السيبراني

تتوزع القوة وأدوات إدارة الصراعات في الفضاء السيبراني على فاعلين، مثل الدول وغير الدول ، ولكل منها أهدافه ، إذ تسعى الدول من خلال دخولها هذه الصراعات إلى الحفاظ على مصالحها، وتأمين بنيتها التحتية، وأمنها القومي من الهجمات الإلكترونية ، بينما تباين أهداف الفاعلين من غير الدول في الصراعات السيبرانية ، لكنها في نهاية الامر تخدم طبيعة الأنشطة التي يمارسونها على أرض الواقع، مثل الأفراد، والتنظيمات السياسية، وشبكات الجريمة المنظمة، والمنظمات الإرهابية، والشركات متعددة الجنسيات ، وتتجدر الاشارة هنا، إلى أن اختلاف القدرات بين الدول والفاعلين من غير الدول يصبح أقل حدة في الفضاء الإلكتروني، بعيدا عن العتاد والأسلحة التقليدية التي تميز فيها الدول <sup>(1)</sup> . ويمكن تفصيل طبيعة الفاعلين في الصراعات السيبرانية على النحو الآتي :

أ. الدول والحكومات: إذ يتم تنفيذ الهجمات الإلكترونية من قبل الجهات الفاعلة الحكومية، سواء لأغراض متعددة (أمنية، وسياسية، وأيديولوجية، وغيرها)، وقد تستغل الحكومات هنا فواعل دون الدول، سواء الأفراد أو الجماعات، للقيام بمثل هذه الهجمات على دولة معادية ، او يقوم بعض اجهزتها بهذا الامر ، وبذلك تصبح ذات خطورة عالية ، نظرا لامتلاك بعض الدول المتقدمة تكنولوجيات وإمكانات تقنية قد تفوق الأفراد في الصراعات السيبرانية ، في هذا السياق، يطرح جوزيف ناي أربعة تهديدات رئيسة على الأمن القومي للدول، عادة ما تكون محل اهتمام الحكومات في

<sup>(1)</sup> Steffen Westerburger, Cyber Conflict In The 21st Century The Future Of War And Security In A Digitalizing World, Master Thesis International Relations, Radboud School Of Management Redboud University, December 2014. Pp. 10-12.

الصراعات السيبرانية، وهي التجسس الاقتصادي، والجريمة الإلكترونية وال الحرب السيبرانية، والإرهاب الإلكتروني<sup>(1)</sup>.

بـ. الفاعلون من غير الدول : اصبح لهؤلاء الفاعلين انشطة تعاونية و أخرى صراعية في الفضاء السيبراني ، لما يمثله الاخير بديل منخفض التكلفة المادية ، والمؤسسة والتنظيمية ، والبشرية لتنفيذ اهدافهم ، ولعب هؤلاء الفاعلين دورا مهما لوضع قواعد ادارة الانترنت ، التي تقوم على الشراكة بين الدول والفاعلين من غير الدول على قدم المساواة ، في ظل عدم وجود وضع خاص للدول من قبل الكيانات المسئولة عن ادارة الانترنت<sup>(2)</sup> ، وابرز الفاعلين من غير الدول ما يأتي :

- الشركات المتعددة الجنسيات : التي لديها موارد مالية ضخمة وفروع في العديد من دول العالم ، مما يتيح لها السيطرة على التعليمات البرمجية تستكشف وتستغل الاسواق ، لذا يمكن ان تلعب تلك الشركات بسهولة دورا في صراعات الفضاء الخاصة ، التي توفر لها مصادر اكبر من العديد من الحكومات ، واهم تلك الشركات التي تمتلك موارد قوة تفوق قدرة بعض الدول ، (جوجل ، فيسبوك ، ميكروسوفت و آبل و آمازون) اذ تسمح خوادم هذه الشركات بأمتلاك قواعد البيانات العملاقة التي من خلالها السيبراني ، بسبب انخفاض تكلفة الاستثمار وصعوبة الكشف عن الهوية ، واحيانا تتصرف بموافقة الحكومة ، واحيانا ضدتها ، إذ ممكن ان تؤثر في اقتصاديات الدول وفي ثقافة مجتمعاتها وتوجيهها ، وهذا ما حدث في الازمة بين شركة جوجل والصين حول المحتوى .

- المنظمات الاجرامية : يسعى هذا الفاعل الى توظيف الادوات الإلكترونية في الفضاء السيبراني لتنسيق العمليات المسلحة على ارض الواقع ، إذ تقوم بعمليات القرصنة السيبرانية ، وسرقة المعلومات ، و اختراق الحسابات البنكية ، و تحويل الاموال ، كما توجد سوق سوداء على الانترنت العميق Deep Internet لتجارة المخدرات والأسلحة والبشر ،

- الجماعات المسلحة (الارهابية) : تعد من ابرز الفواعل الدولية ، لاسيما بعد احداث 11 ايلول 2001 ، إذ تستغل الفضاء السيبراني ، ومن خلال موقع التواصل الاجتماعي ، لتجنيد اتباع

<sup>(1)</sup> Joseph Nye, Cyber Power, Belfer Center For Science And International Affairs, May 2010, Pp. 11-13, at : [Https://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf](https://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf).

<sup>(2)</sup>Joseph Nye, Cyber Power, Belfer Center For Science And International Affairs, Op.Cit, p.16 .

<sup>(3)</sup> سماح عبد الصبور ، "الارهاب الرقمي : استخدامات الجماعات المسلحة لوسائل التواصل الاجتماعي " ، دورية اتجاهات الاحاديث ، المجلد (1) ، العدد (2) ، 2014 ، ص 4 .

جدد ، ونشر الافكار والمعتقدات ، فضلا عن جمع الاموال ، وجمع المعلومات حول الاهداف العسكرية وكيفية التعامل مع الاسلحة .

- الانونيموس و ويكيликس : فالانونيموس او المجهولون ؛ هم جماعات احتجاجية منتشرة حول العالم في الفضاء الالكتروني ، لهم اهداف سياسية ، ويقومون بتوزيع المعلومات السرية ، وتشويه الواقع ، وتوليد احتجاجات حول القضايا السياسية ، وهم نمط جديد من الفاعلين السياسيين الذين يعتمدون على اخفاء الهوية ، والقيادة بلا جسد ، وانخراط الافراد بلا عضوية دائمة ، ويعملون على تنفيذ هجمات افتراضية ضد اهداف مادية من اجل تشجيع التغيير السياسي . اما "ويكيликس" ؛ فهو موقع تم تأسيسه في عام 2007 ، يستهدف كشف وفضح الانظمة السياسية ، عبر تسريب الوثائق والاسرار حول الحكومات ، والشخصيات العامة . ويشكل كلا من الانونيموس و ويكيликس نماذج لما يمكن ان يسببه الفاعلون من غير الدول من تأثيرات صراغية في الحكومات والفضاء الالكتروني .<sup>(1)</sup>

### 3: مخاطر وتداعيات الصراع السيبراني

ادى اتساع علاقة الدول بالفضاء الالكتروني ، وما خلفته من حروب سيرانية ، الى جملة من المخاطر والتداعيات ، على تفاعلات السياسة الدولية ، يمكن طرح ابرزها على النحو الاتي :<sup>(2)</sup>

أ. تصاعد المخاطر الالكترونية ، لاسيما مع قابلية المنشآت الحيوية (مدنية وعسكرية) في الدول للهجوم الإلكتروني عليها عبر وسيط وحامل الخدمات أو شل عمل انظمتها المعلوماتية ، الأمر الذي يؤثر في وظائف تلك المنشآت ، وبالتالي، فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة استراتيجية بالغة الأهمية، سواء في زمن السلم أو الحرب .

ب. تعزيز القوة وانتشارها ، فمن جانب عزز الفضاء الإلكتروني ما يسمى بـ "القوة المؤسسية" في السياسة الدولية ، التي تعني أن يكون لها دور في قوة الفاعلين، وتحقيق أهدافهم وقيمهم في ظل التناقض مع الآخرين، والإسهام في تشكيل الفعل الاجتماعي في ظل المعرفة والمحددات المتاحة، التي تؤثر في تشكيل السياسة العالمية . ومن جانب آخر، عمل الفضاء الإلكتروني على إعادة تشكيل قدرة

<sup>(1)</sup> Wendy H. Wong And Peter A. Brown, E- Bandits . "Global Activism: Wikileaks, Anonymous,And The Politics Of No One", Perspectives On Politics, Vol. 11, No. 4, December 2013, p.234 .

<sup>(2)</sup> عادل عبد الصادق ، "انماط الحرب السيبرانية وتداعياتها على الامن العالمي " ، مجلة السياسة الدولية ، مركز الاهرام للدراسات السياسية والاستراتيجية ، العدد (208) ، 2017 ، ص 35 .

الأطراف المؤثرة، مثل الولايات المتحدة ؛ فبعدما إن كانت الأخيرة تملك ما يشبه الاحتكار لمصادر القوة، بعد انتهاء الحرب الباردة، برزت عملية انتشار القوة بين أطراف متعددة، سواءً أكانت دولاً، أم من غير الدول .

ج. عسکرة الفضاء الإلكتروني، وذلك سعياً لدرء تهدياته على أمن الفضاء الإلكتروني، وبرز في هذا الإطار اتجاهات، مثل التطور في مجال سياسات الدفاع والأمن الإلكتروني، وتصاعد القدرات في سباق التسلح السيبراني، وتبني سياسات دفاعية سيبرانية لدى الأجهزة المعنية بالدفاع والأمن في الدول، وتزايد الاستثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة .

د. إدماج الفضاء الإلكتروني ضمن الأمن القومي للدول، وذلك عبر تحديث الجيوش، وتدشين وحدات متخصصة في الحروب الإلكترونية، وإقامة هيئات وطنية للأمن والدفاع الإلكتروني، والقيام بالتدريب، وإجراء المناورات لتعزيز الدفاعات الإلكترونية، والعمل على تعزيز التعاون الدولي في مجالات تأمين الفضاء الإلكتروني، والقيام بمشروعات وطنية للأمن الإلكتروني .

هـ. الاستعداد لحروب المستقبل، حيث تبني العديد من الدول استراتيجية حرب المعلومات بحسبانها حرباً للمستقبل، التي يتم خوضها بهدف التشتيت، وإثارة الاضطرابات في عملية صناعة القرار لدى الخصوم، عبر اختراق أنظمتهم، واستخدام ونقل معلوماتهم. وهنا، ترى الدول الكبرى أن من يحدد مصير تلك المعركة المستقبلية ليس من يملك القوة فقط، وإنما القادر على شل القوة، والتلوиш على المعلومة<sup>(١)</sup> .

و. تحديث القدرات الدفاعية والهجومية، إذ سعت الدول إلى تحديث النشاط الدفاعي لمواجهة مخاطر الحرب السيبرانية ، والاستثمار في البنية التحتية المعلوماتية، وتأمينها، وتحديث القدرات العسكرية، ورفع كفاءة الجاهزية لمثل هذه الحرب عن طريق التدريب، والمشاركة الدولية في حماية البنية المعلوماتية، والاستثمار في رفع القدرات البشرية داخل الأجهزة الوطنية المعنية، وهنا يتعلق التوجه الأخطر بنقل تلك القدرات من الدفاع إلى الهجوم عن طريق استخدام تلك الهجمات في إطار إدارة الصراع والتوتر مع دول أخرى .

مما تقدم يمكن القول ، ان مع تغير منظور الحروب جذرياً بانتقالها من نسق الحروب التقليدية بين الدول ، التي كانت تدور في إطار تدمير الخصم اما بإحتلال ارضه او الاستيلاء على

<sup>(١)</sup>E.Nakashima ، "U.S Accelerating Cyber weapon Research" ، The Washington Post ، online e-article ، <http://www.washingtonpost.com/world/national-security>.

موارده ، الى حروب جديدة تستهدف التحكم في ارادة وخيارات المجتمعات ، ما يعني تركيزها على العامل النفسي والدعائي سيمما مع تنامي التغطية الاخبارية والسمعية والبصرية المباشرة للاحادث عبر موقع الانترنت ، فضلا عن بروز الصراعات ذات الابعاد المحلية - الدولية ، اذ ساعدت على اشغال الصراعات الداخلية في مرحلة ما بعد الحرب الباردة ، كذلك طبيعة السباق الدولي للفضاء الالكتروني في توفير بيئة مناسبة لدمج القوى والفنانات المهمشة في السياسة الدولية ، جميعها عوامل عملت على اذكاء وانتشار رقعة الصراع في الفضاء الالكتروني (السيبراني) ، وبالتالي فسح المجال لظهور الحروب السيبرانية .

### ثانياً اهم الصراعات السيبرانية الدولية والاقليمية

شهد العقدان الاخيران سباقا متشارعا بين بعض القوى الدولية والاقليمية في مناطق العالم المختلفة لتعظيم الاستفادة من الفضاء السيبراني ، إذ عدت هذه الدول القدرات السيبرانية وسيلة لبسط النفوذ سواء كان اقليميا ام دوليا ، لتحقيق مكاسب استراتيجية ، وسياسية ، ومالية ، لم تكن لتحققها عبر الوسائل العسكرية التقليدية ، إذ يدعم هذه الرؤية عاملان ؛ الاول يتعلق بالامكانات الفائقة للقدرات السيبرانية في تشكيل تهديدات صريحة للخصوم ، وهي تهديدات تتبع ما بين شن حملات دعائية مغرضة ، مرورا بالتجسس السيبراني ، واستخدام القدرات التكنولوجية في اعمال إرهابية والتهديدات المسلحة غير المباشرة ، وصولا الى التهديدات العسكرية الصريحة ، وفقا لورقة بحثية اصدرها مركز الدراسات البريطاني تشاتام هاوس عام 2010 ، حول الفضاء السيبراني <sup>(1)</sup> ، اما العامل الثاني فيشير الى ان امتلاك "القدرات السيبرانية" ، لم يعد حكرا على فاعل بعينه ، فقد اصبح في مقدور الدول الصغيرة والمتوسطة ، والفاعلين من غير الدول كذلك مهما صغر حجمهم ، وتواضع امكانياتهم ، الاستفادة من القدرات السيبرانية ، بما فيه تطوير اسلحة رقمية وتهديد الخصوم <sup>(2)</sup> .

وعليه سيتم التطرق في هذا المحور الى كيفية توظيف الدول القدرات السيبرانية في صراعتها ، من خلال اختيار نماذج محددة وكالاتي :

<sup>(1)</sup> Paul Cornish, David Livingstone, Dave Clemente, And Claire Yorke," Cyber War fare", Chatham House , 2010 , Link: <Http://www.nsci-va.org/cyberreferencelib/2010-11-on%20cyber%20warfare>.

<sup>(2)</sup> احمد زكي عثمان ، "تأثيرات القدرات السيبراني في الصراعات الاقليمية" ، مجلة السياسة الدولية ، مركز الاهرام للدراسات السياسية والاستراتيجية ، القاهرة ، العدد (208) ، 2017 ، ص 17 .

**١- الصراع السيبراني الامريكي - الصيني :** أصبحت حرب المعلومات شكلًا من اشكال التناقض والصراع ، إذ عُد سلاح المعلومات أحد أهم الأسلحة التي تستخدمها الدول ، لاسيما الدول المتقدمة ، لتحقيق أهدافها الإستراتيجية ، لذا ظهر ما يعرف بحرب المعلومات الإستراتيجية ، التي عرفها البعض بأنها : " أعمال تقوم بها دول تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى ، بهدف تحقيق أضرار بالغة أو تعطيلها أو سرقة المعلومات "<sup>(١)</sup> . لذا ادركت الولايات المتحدة كقوة عالمية باحثة عن استمرار هيمنتها ، على أهمية تأثير العامل التكنولوجي والمعلوماتي في بنية موازين القوى العالمية ، إذ وضعت التقوّق المعلوماتي كمجال لزيادة قدرتها اولاً ، وحرمان الخصوم المنافسين منه ثانياً، ضمن استراتيجيتها القومية للقرن الحادي والعشرين ، واتسع هذا الهدف الامريكي ليشمل جميع القدرات السيبرانية في مجال الاتصالات والمعلومات ، مع زيادة التناقض العالمي على حيارة النفوذ في الفضاء السيبراني ، فضلاً عن صعود مفهوم القوة الذكية ، الذي عبر عن التلاقي بين القوة الصلبة والناعمة ، لغرض تحقيق اهداف السياسة الخارجية الامريكية بفعالية اكبر <sup>(٢)</sup>.

لذا بدأت الادارة الامريكية وتحديداً في عهد الرئيس بيل كلينتون عام 1998 ، في الاشارة لمفهوم السيبرانية في جميع وثائقه المتعلقة بأستراتيجية الامن القومي (1998-2001) ، ونتيجة هذا التحول ، شددت الادارة الامريكية على بناء خطة شاملة للمرونة السيبرانية <sup>٣</sup> ، وبعد احداث 11 ايلول 2001 ، بدأ التركيز على الفضاء السيبراني كتهديد امني من حيث استخدام هذا المجال الحيوي من قبل المنظمات الإرهابية والقوى الإقليمية والدولية ، الذي يعد قليل التكلفة والجهد من ناحية التنفيذ وتحقيق الهدف <sup>٤</sup> ، لذا اطلق الرئيس الامريكي الاسبق جورج بوش عام 2003 ، الاستراتيجية الوطنية لحماية الفضاء السيبراني، وفي عام 2008 ، اطلق جورج بوش ايضاً مبادرة لامن الالكتروني الامريكي (CNCI) ، تسعى لتحديد وتقليل التهديدات الالكتروني الحالية والمستقبلية ، والحد من نقاط الضعف التي تواجه قطاع الاتصالات

<sup>(١)</sup> حنان علي الطائي ، " عقائد ومذاهب اقتصادية - عسكرية - تكنولوجية جديدة" ، في كتاب : مجموعة بباحثين ، " مطارحات النظام الدولي والقوى الكبرى .. تأملات في المسرح الجيوسياسي العالمي الجديد" ، (عمان : الاكاديميون للنشر والتوزيع ، 2019 ) ، ص ص 202 - 208 .

<sup>(٢)</sup> خالد حنفي علي ، مصدر سبق ذكره ، ص 3 .

<sup>٣</sup> يونس مؤيد يونس ، " استراتيجية الولايات المتحدة الامريكية لامن السيبراني " ، مجلة قضايا سياسية ، جامعة النهرین ، كلية العلوم السياسية ، العدد (55) ، 2018 ، ص ص 119 - 120 .

<sup>٤</sup> نورة شلوا ، " القرصنة الالكترونية في الفضاء السيبراني : التهديد المتتصاعد لامن الدول " ، مجلة مركز بابل للدراسات الانسانية ، العدد (2) ، 2018 ، ص 192 .

والامن الالكتروني<sup>1</sup> ، وفي عام 2010 ، اصدرت ادارة الرئيس الاسبق باراك اوباما " استراتيجية الامن القومي الامريكي" ، والتي حظي فيها الفضاء السيبراني بأهتمام كبير ، اذ اشار فيها الى ان "التهديدات السيبرانية تمثل واحدة من اخطر التهديدات التي تواجه الامن القومي والسلامة العامة للمواطنين"<sup>2</sup> وفي 2018 ، وقع الرئيس السابق دونالد ترامب على وثيقة قانون لتأسيس وكالة الامن السيبراني وامن البنية التحتية (CISA) ، لصبح قانونا فعليا<sup>3</sup> ، وفي كانون الثاني 2020 ، اكد الرئيس الامريكي جو بايدن ان الامن السيبراني سيكون على رأس اولويات الادارة الامريكية الجديدة<sup>4</sup> ، اذ في تموز 2021 ، وقع بايدن مذكرة امن قومي لتحسين الامن السيبراني لانظمة التحكم في البنية التحتية ، إذ ركزت المذكرة على طرق الحماية من الهجمات السيبرانية ، وخطط للطوارئ والتعافي والتعاون مع القطاع الخاص ، من اجل ضمان حماية الخدمات الحيوية التي يعتمد عليها الشعب الامريكي<sup>5</sup> ، وفي طار تعزيز الامن السيبراني وقع الرئيس الامريكي جو بايدن في عام 2022 ، مذكرة وسع من خلالها دور وكالة الامن القومي في حماية شبكات الكمبيوتر الاكثر حساسية للحكومة الامريكية ، التي تنص على ممارسات ومعايير اساسية لامن السيبراني مثل استخدام التشفير لما يسمى بـ "انظمة الامن القومي" ، والتي تشمل وزارة الدفاع ووكالات الاستخبارات والمقاولين الفيدراليين الذين يدعمونها<sup>6</sup> .

وفي هذا السياق رأت الولايات المتحدة الأمريكية أن أكبر التهديدات التي يواجهها الأمن القومي الأمريكي في القرن الحادي والعشرين ، هو قضية الأمن الإلكتروني ، وهذه التهديدات متأتية من الصين ، إذ تعمل الأخيرة على سرقة معلومات التجارة الأمريكية ، ومعلومات وأسرار عسكرية ، مع توجيه هجمات الكترونية تعمل على تعطيل المنظومة الإلكترونية لشبكات الدفاع والاستخبارات الأمريكية<sup>(7)</sup> ، لاسيما وان الصين تعد الدولة الوحيدة التي تمتلك القدرة على منافسة الولايات المتحدة كقوة عظمى،

<sup>1</sup> ايها خليفة ، " القوة الالكترونية : كيف يمكن ان تدير الدول شؤونها في عصر الانترنت " ، (القاهرة : العربي للنشر والتوزيع ، 2017 ) ، ص 138 .

<sup>2</sup> ايها خليفة ، القوة الالكترونية ... ، مصدر سبق ذكره ، ص 151 .

<sup>3</sup> ترامب يقيل المسؤول عن ضمان امن الانتخابات بسبب نفيه عمليات تزوير " ، شبكة المباديين الاعلامية ، بيروت ، 18 تشرين الثاني ، 2020 ، متاح على الرابط : [www.almayadeen.net/news/politics/1437412](http://www.almayadeen.net/news/politics/1437412) .

<sup>4</sup> المصدر نفسه .

<sup>5</sup> هبه القدسي ، " بايدن يحذر روسيا من هجمات الكترونية تعود الى حروب حقيقة " ، جريدة الشرق الاوسط ، 2021 ، متاح على الرابط : <http://aawsat.com/home/article/3103616> .

<sup>6</sup> " بايدن يوسع صلاحيات وكالة الامن لمواجهة خطر الهجمات السيبرانية " ، موقع الشرق ، دبي ، 2022 ، <http://asharq.com>

<sup>(7)</sup> Jacob Stokes and Nina Hachigian, " U.S – China Relations in an Election year", center for American Progress Action Fund, [www.Americanprogressaction.org](http://www.Americanprogressaction.org).

عظمى، إلكترونية أو غير ذلك ، إذ بالتواري مع قدرتها على الحرب الإلكترونية المترقبة ، تتسع قدرات الصين العسكرية والاقتصادية والتكنولوجية السيبرانية بسرعة ، وبدأت تبدو طموحاتها المعلنة في الفضاء تتجاوز طموحات الولايات المتحدة ، فالصين ادركت أهمية بعد السيبراني ، وحاجتها إلى أن تصبح قوة إلكترونية ، إلى جانب صعودها الاقتصادي ، لاسيما وان الفضاء الإلكتروني ، أصبح ركيزة جديدة للتنمية الاقتصادية والاجتماعية ، و مجالاً جديداً للأمن القومي ، لاسيما مع تزايد أهمية الفضاء الإلكتروني في الأمن العسكري ، لذا ادركت الصين بأن عليها الارساع في تطوير قوة إلكترونية لحفظ على الأمن القومي والاستقرار الاجتماعي ، وعليه ، أعلن الرئيس شي جين بينغ ، في عام 2017 ، عن طموح الصين لتحقيق قوة عظمى في مجال الإنترت ، وهو وضع يطلق استراتيجية تنمية متعددة الجوانب لبناء قدراتها التكنولوجية ، إذ يعطي هذا البناء الشامل كلًا من المقومات الاقتصادية والعسكرية ، مع الاعتراف من ناحية بحقيقة أنه "دون الأمن السيبراني لا يوجد أمن قومي" ، ومن ناحية أخرى حقيقة ، أن الاقتصاد الصيني سيحتاج أيضًا إلى التكيف مع عصر المعلومات ، بالنظر إلى أن استراتيجياتها الاقتصادية الحالية غير كافية لحفظ على معدلات النمو المطلوبة لتلبية مطالب السكان وإبقاء الحزب الشيوعي الصيني في السلطة على المدى الطويل<sup>(1)</sup>.

كما ان الصين ونتيجة استراتيجيتها الجديدة "صنع في الصين 2025" ، والخطة الخمسية الثالثة عشرة ، سلطت الضوء على امن الفضاء الإلكتروني الوطني كمشروع سيكتمل في عام 2030 ، لصالح كل من الاقتصاد الصيني وجيش التحرير الشعبي ، وبذلت جهودًا كبيرة للحاق بركب التطورات في المجال السيبراني ، ولتوضيح وجهة النظر الصينية ، حول حوكمة الفضاء الإلكتروني ذات الخصائص الصينية ، وتطوير فكر استراتيجي يقوم على "اغتنام الفرصة التاريخية لتطوير المعلوماتية ، في محاولة لبناء قوة البلاد في الفضاء الإلكتروني" ، أكد الرئيس الصيني (شي جين بينغ) في نيسان 2018 ، خلال مؤتمر عمل الامن السيبراني ، على أهمية هذا المجال لتنمية الصين ضمن التكامل المدني - العسكري ، مشيرًا إلى أن "تطوير الأمن السيبراني والمعلوماتية يجب أن يسهم إلى حملة الصين لتطوير اقتصاد حديث وتحقيق تنمية عالية الجودة ، وإلى النموذج الجديد للتصنيع والتحضر والتحديث الزراعي" ، واضاف قائلاً إنه "يجب بذل الجهود لتطوير الاقتصاد الرقمي ، وتعزيز التكامل

<sup>(1)</sup> " Global Cyber Rivalry Challenges American Geopolitical Leadership" , Greater Pacific Capital , December 2018 , available on : <https://www.greaterpacificcapital.com/thought-leadership/global-cyber-rivalry-challenges-american-geopolitical-leadership>

العميق بين الإنترت ، والبيانات الضخمة ، والذكاء الاصطناعي ، والاقتصاد الحقيقي ، وجعل قطاعات التصنيع والزراعة والخدمات أكثر رقمية وذكية ومتصلة بالإنترنت " <sup>(1)</sup> .

وفي هذا الصدد كشفت الصين في كانون الأول 2017 ، عن أول مركز ابتكار للامن السيبراني المدني - العسكري في البلاد في ميانيانغ بمقاطعة سيشوان ، الذي انشأته اكبر شركة لامن السيبراني في الصين ، وهي مجموعة Enterpris Security Group 360 ، تحت سلطة اللجنة المركزية للتنمية العسكرية والمدنية ، التي ستركت على بناء انظمة الدفاع السيبراني للاستخدامات العسكرية <sup>(2)</sup> ، كما باتت تمتلك اكبر شبكة واسعة النطاق للألياف البصرية في العالم ، التي كانت حافزا استراتيجيا لقوة شبكة الانترنت الصينية ، كما تبنت قوة سيرانية في القطاع الاقتصادي من خلال بناء إقتصاد رقمي قوي ، وتعتبر اكبر سوق الكترونية ، كما عززت المجتمع الرقمي لبناء قوة سيرانية لتحقيق الامن القومي <sup>(3)</sup> .

لذا تعد قضية الامن السيبراني من اهم القضايا المؤثرة في العلاقات التنافسية بين الصين والولايات المتحدة ، ولاسيما عام في 2013 ، إذ اتهمت الولايات المتحدة الأمريكية الصين بالقيام بأعمال تجسس لسرقة معلومات عسكرية وتجارية سرية ، وقامت شركة مانديانت الأمريكية للأمن الإلكتروني بتقديم تقرير اتهمت فيه الجيش الصيني بشن هجمات الكترونية واسعة النطاق على مؤسسات أمريكية <sup>(4)</sup> ، وإن الاتهامات المتبادلة بين الصين والولايات المتحدة الأمريكية تدلل على وجود تنافس دولي على ما يعرف بالذكاء الاصطناعي والقوة الإلكترونية ، وبالتالي استخدام هذه الإمكانيات في تنفيذ هجماتها ، وسعى الدولة المستهدفة للحصول على التطور التكنولوجي واستخدامه ، وهذا ما اكده ريفا جوجون كبيرة المحللين بمعهد ستراتفورد الأمريكي للدراسات الأمنية والإستراتيجية بقولها : " إن التنافس بين اقطاب

<sup>(1)</sup> President Xi Jinping, "Speech to a National Conference on the Work of Cybersecurity and Informatization" . See: "Xi Outlines Blueprint to Develop China's Strength in Cyberspace," Xinhua, April 21, 2018, [http://www.xinhuanet.com/english/2018-04/21/c\\_137127374.htm](http://www.xinhuanet.com/english/2018-04/21/c_137127374.htm).

<sup>(2)</sup>Meia Nouwens and Helena Legarda, "Emerging Technology Dominance: What China's Pursuit of Advanced Dual-use Technologies Means for the Future of Europe's Economy and Defence Innovation" , The International Institute for Strategic Studies,UK, December 2018, p.9.

<sup>(3)</sup> نصيرة الصالحي ، " القوة الذكية : التناقض العالمي على قوة الفضاء الإلكتروني والقدرات السيرانية" ، مجلة دفاتر السياسة والقانون ، جامعة عباس لغرور خنشلة ، الجزائر ، المجلد ، (13) ، العدد (1) ، 2021 ، ص 381 .

<sup>(4)</sup> ووشين بوا ، " الصين والولايات المتحدة وبناء نمط جديد للعلاقات بين الدول الكبرى : تقييمات ومقترحات " ، في كتاب : مجموعة باحثين ، " الحزام والطريق : تحولات الدبلوماسية الصينية في القرن 21" ، ترجمة : آية الغازي ، ( مصر : دار الصفصةفة ، 2017 ) ، ص ص 262 – 264 .

العالم ودوله الصغيرة على امتلاك أحدث برمجيات الذكاء الاصطناعي ، سيؤدي الى صراعات جديدة بسبب تخوف الأطراف الدولية من بعضها " ، وبالتالي فإن تقنية الذكاء الاصطناعي والحصول عليها أصبحت تحدياً للدول الكبرى <sup>(1)</sup>.

وعليه ، ركزت الولايات المتحدة في السنوات الأخيرة ، على إنشاء واحدة من أكبر القوى الأكاديمية في الذكاء الاصطناعي ، وهو تطور يسيطر القطاع الخاص على معظمها ، تتبعه استثمارات عسكرية وأجهزة استخباراتية ، مثل وكالة نشاط مشروعات الأبحاث المتقدمة للمخابرات The Intelligence Advanced Research Projects Activity (IARPA) ، ووكالة مشاريع البحث الداعية المتطرفة The Defense Advanced Research Projects Agency ( DARPA) السابق (دونالد ترامب) عن عزمه لتطوير استخدامات الذكاء الاصطناعي لتحسين الاقتصاد ومصلحة الأمن القومي ، على الرغم من تقليل حجم الاستثمار المقرر لعام 2018 ، بنسبة 15% ، حيث يقدر أن يضيف الذكاء الاصطناعي 15.7 تريليون دولار أمريكي إلى الناتج المحلي الإجمالي العالمي بحلول عام 2030 ، في حين اختارت الصين الحفاظ على استثمار عام قوي ، يقدر بنحو سبعة مليارات دولار سنوياً ، في إطار خطة عمل وطنية طموح لخلق صناعة يبلغ حجمها 150 مليار دولار بحلول عام 2030 <sup>(2)</sup>.

وفي سياق التناقض الأمريكي الصيني يمكن الاشارة الى بعض اهم الهجمات السيبرانية المتبادلة بين الجانبين ، وكالاتي :

1. في عام 2005 ، شنت الصين هجمات سيبرانية ضد اجهزة الكمبيوتر الخاصة في وزارة الدفاع الأمريكية ، كما حاولت الصين اعاقه اجهزة الاقمار الصناعية الامريكية عام 2006 <sup>3</sup> .

2. في عام 2007 ، تم قرصنة المواقع الالكترونية لشركة (لوكهيد مارتن) ، اذ سرقة منها معلومات ومستندات عن تكنولوجيا تصنيع مقاتلة F-35 ، التي استخدمتها الصين فيما بعد في تصميم مقاتلة Ty - 20 .

3. في عام 2019 اتهمت الحكومة الأمريكية القرصنة الصينيون بسرقة معلومات تخص العقود البحرية ، وامور تتعلق بصيانة السفن وخطط الصواريخ <sup>1</sup> .

<sup>(1)</sup> ابو الفضل الاسناوي ، " سباق القوة في عالم العلاقات الدولية " ، مجلة السياسة الدولية ، مؤسسة الاهرام ، العدد (215) ، 2019 ، ص 10 .

<sup>(2)</sup> سماء سليمان ، " تداعيات التناقض الامريكي - الصيني على مستقبل النظام الدولي " ، مجلة السياسة الدولية ، مؤسسة الاهرام ، القاهرة ، العدد (218) ، 2019 ، ص 132 .

<sup>3</sup> ايها خليفة ، " القوة الالكترونية ... " ، مصدر سبق ذكره ، ص ص 20 - 21 .

4. في كانون الاول 2020 ، اتهم الرئيس السابق دونالد ترامب قراصنة صينيون في تنفيذ هجمات سيرانية على مؤسسات وشركات امريكية من ضمنها وزارة الخزانة والتجارة الامريكيتين<sup>2</sup>.

5. وفي عام 2021 ، ذكرت شركة مايكروسوفت ، ان مجموعة تجسس الكتروني مرتبطة بالصين تحمل اسم هافنيوم HAFNIUM ، تقوم بسرقة صناديق البريد الالكتروني<sup>3</sup>.

6. بين ايار 2021 ، وشباط 2022 ، تم استهداف 6 ولايات امريكية على الاقل بهجوم سيراني شنه قراصنة صينيون عرفت باسم APT41 ، استغلو نقاط ضعف في برامج الكترونية<sup>4</sup>.

7. اتهمت الحكومة الصينية الولايات المتحدة الامريكية بشن هجمات سيرانية عليها وصلت الى نحو 34 الف هجوم عام 2011 ، كما اتهمت الصين الولايات المتحدة عام 2013 ، بأختراقها جامعة "سينغهوا" في بكين ذات المكانة العالمية ، فضلا عن اختراق واحدة من اهم ست شبكات اساسية تحكم بالبر و حركة المرور ، وشبكة الويب العالمية في الصين<sup>5</sup>.

8. في عام 2019 ، اتهمت شركة هواوي HUAWEI الصينية ، الحكومة الامريكية بأختراق شبكات المعلومات الداخلية والخارجية لتعطيل عملياتها التجارية .

9. في عام 2022 ، ذكرت الحكومة الصينية انها تتعرض للعديد من الهجمات السيرانية الامريكية ، اذ حددت شركة امن الكتروني صينية قرصنة مصدرها وكالة الامن القومي الامريكي ، كما اعلن مختبر بانغو الصيني اكتشاف قرصنة من الولايات المتحدة من خلال برامج ضارة على انظمة تكنولوجيا المعلومات المحلية ، تم انشاؤها عن طريق مجموعة القرصنة "ايكويشن" ، والتي يعتقد ارتباطها بوكالة الامن القومي الامريكية<sup>6</sup>.

<sup>1</sup> سرى غضبان غيدان ، محمد منذر جلال ، "الامن السيبراني وسياسات المواجهة الدولية" ، مجلة الدراسات الاستراتيجية والعسكرية ، المركز الديمقراطي العربي ، العدد (9) ، 2020 ، ص ص 200 - 201 .

<sup>2</sup> "ترامب يلمح الى تورط الصين في الهجوم السيبراني" ، موقع قناة المنار ، كانون الاول ، 2020 ، متاح على الرابط : <http://www.manartv.com.ib/7630163>

<sup>3</sup> "سرقت محتويات حسابات المستخدمين .. مجموعة مرتبطة بالصين تستهد ببرنامج بريد مايكروسوفت" ، موقع الجزيرة ، 2021 ، متاح على الرابط : <HTTPS://WWW.ALJAZEERA.NET/NEWS>

<sup>4</sup> "مؤيّكا تحت التيران .. صينيون اخترقوا 6 ولايات حكومية" ، موقع العربية نت ، 2022 ، متاح على الرابط : <http://www.alarabiya.net/>

<sup>5</sup> سرى غضبان ، محمد منذر جلال ، مصدر سبق ذكره ، ص 211 .

<sup>6</sup> "تقرير صيني حول اختراق وكالة الامن القومي الامريكي في الصين" ، موقع صحيفة الوثائق الالكترونية ، 2022 ، متاح على الرابط : <http://www.alwathaq.com/143720>

مما تقدم نستنتج ، بأن كل من الصين والولايات المتحدة تتسابقان لتطوير تقنيات الذكاء الاصطناعي ، وترسيخ مكانة قيادية في "سباق الفضاء" للقرن الحادي والعشرين ، إذ تستهدف الخطة الاستراتيجية الوطنية للذكاء الاصطناعي في الصين موقعاً رياضياً في الذكاء الاصطناعي بحلول عام 2025 ، إذ تم بناء خطة الصين على التعاون بين القطاعين العام والخاص ، التي تتroxى الاستفادة من الابتكار من شركات القطاع الخاص مثل Alibaba و Tencent ، للتطبيقات في الحرب والتجسس ، من ناحية أخرى ، لم تعلن الولايات المتحدة عن استراتيجية حكومية شاملة لتسريع تطوير الذكاء الاصطناعي واعتماده ، ومع ذلك لا تزال الولايات المتحدة حتى الوقت الحالي تقود هذا المجال ، مع أكثر من ثلاثة أضعاف عدد شركات الذكاء الاصطناعي ، وضعف عدد براءات اختراع الذكاء الاصطناعي التي تمتلكها الصين اليوم ، كما تتمتع الولايات المتحدة بميزة طبيعية كمجتمع مفتوح يوفر وصولاً واسع النطاق إلى المعلومات والأفكار ، مما يتيح الابتكار الجماعي ، ومع ذلك ، يبقى السؤال ما إذا كان بإمكان الصين التغلب على هذه الميزة من خلال إنفاق الأموال على المشكلة ، والتركيز على هدف واحد ، وهو القدرة على الحرب الإلكترونية ، بدلاً من الأهداف والتطبيقات العديدة لشركة America Inc.

**2\_ الصراع السيبراني الامريكي - الروسي:** أصبح التناقض للحصول على القدرات السيبرانية عنصراً أساسياً في سياسات القوة العظمى ، وكان يُعتقد في البداية أن الصين والولايات المتحدة هما القائدان الطبيعيان للفضاء ، مع قدرات وموارد فائقة لبناء وترسيخ موقعهما العالمي ، إذ على الرغم من أن الصين قد استطاعت بناء قدرات إلكترونية هائلة ، إلا أن روسيا ظهرت بوصفها الدافع الرئيس للولايات المتحدة للحصول على القوة السيبرانية ، لاسيما بعد أن عوضت عن تراجع أهميتها في الاقتصاد الدولي ، فضلاً عن تراجع قوتها العسكرية المادية بالتركيز المنهجي على الحرب الإلكترونية ، إذ قامت روسيا بدمج الإنترنـت كآلية أساسية لتمويلها الأوسع في مجال حرب المعلومات ، التي تشمل الحرب الإلكترونية والعمليات المعلوماتية والعمليات النفسية ونشرت قدراتها الهجومية عبر مجموعة من المناطق الجغرافية والساحات ، فضلاً عن التدخل وعلى نطاق واسع في الانتخابات الرئاسية الأمريكية ، كما تُتهم روسيا أيضاً ، بهجمات منسقة على قطاع الإعلام والتمويل في إستونيا والحكومة ، والبنية التحتية المادية لأوكرانيا أثناء غزو شبه جزيرة القرم ، والتسلل إلى محطات توليد الطاقة وتدميرها شبكة الكهرباء عبر أجزاء من البلاد. نتيجة لذلك ، تصدرت روسيا قائمة التهديدات السيبرانية للدول القومية في تقرير تقييم التهديد العالمي السنوي للولايات المتحدة الصادر عن مدير الاستخبارات الوطنية منذ عام 2015 ، بعد

عدة عقود من تراجع الأهمية الجيوستراتيجية في العالم المادي<sup>(1)</sup>، ما يعني ان روسيا لديها كل من القدرات والإرادة لتكون رائدا عالميا في العالم الرقمي.

وتحتفظ روسيا والولايات المتحدة بقدراتها في مجال تطوير واستخدام "الأسلحة السيبرانية" ، وباتت تدخل ضمن مخصصات الهيئات المعنية بالدفاع والامن ، وتعدان من ضمن الخمس دول كبرى في مجال "القوة السيبرانية" ، وفي سياق التوتر المتتسارع بين روسيا الاتحادية والولايات المتحدة الأمريكية ، حول العديد من القضايا الثانية والإقليمية، اضافت حدة المواجهة السيبرانية بينهما ، اهمية اخرى لهذا الصراع ، لاسيما مع استخدام الولايات المتحدة مبدأ حرية الانترنت كأداة من أدوات سياساتها الخارجية ، ووجهت التمويل وبناء القدرات لدعم حرية الانترنت في البلدان ، التي تقع في الفناء الاستراتيجي لروسيا في منطقة آسيا الوسطى ، لتحدث جملة من التغيرات فيما عرف بالثورات "الملونة" ، وإحداث تغييرات في سياسات تلك الدول ، تجاه التأييد للقيم الغربية والليبرالية ، وهو ما وصفته روسيا تهديدا لأمنها القومي ، إذ ترى إن الولايات المتحدة قد باتت خطرا على "الانترنت المفتوح" ، وحريته ، في العقد الأخير بعد الكشف عن عمليات التجسس الكبرى ، التي تقوم بها وكالة الامن القومي ، في السياق نفسه حققت روسيا تطورات مهمة في مجال التطبيقات الالكترونية الخاصة في مجال الشبكات الاجتماعية ، وحماية شبكة الانترنت المحلية ، والتطور في مجال البرمجيات الخاصة بالحماية<sup>(2)</sup>.

وتتطور الصراع بقيام روسيا الاتحادية بشن الهجمات السيبرانية ضد حلفاء الولايات المتحدة؛ مثل بريطانيا عام 2018 ، وأوكرانيا عام 2015 ، ضد جورجيا خلال العمليات الحربية عام 2008 ، وشن هجمات اخرى ضد استونيا عام 2007، ما دفع حلف الناتو على اثر ذلك بتأسيس مركز للدفاع الالكتروني بها، والبحث في موقف تجاه الرد على الهجوم الالكتروني، بوصفه "هجوما مسلحا"، وفق القانون الدولي ، ومدى إمكانية تطبيق المادة 5 من ميثاق حلف الناتو ، التي تنص "على أن أي هجوم أو عدوان مسلح على أي بلد من الحلف يعد اعتداء على جميع بلدانه وعليه يدخل نظام الدفاع المشترك للناتو حيز التنفيذ" ، وهو ما يهدد بتصاعد التوتر العسكري<sup>(3)</sup>، وفي سياق التوتر المتتسارع بين روسيا الاتحادية والولايات المتحدة الأمريكية ، حول العديد من القضايا الثانية والإقليمية، اضافت حدة المواجهة

<sup>(1)</sup> "Global Cyber Rivalry Challenges American Geopolitical Leadership" ، Greater Pacific Capital ، Op.Cit .

<sup>(2)</sup> عادل الصادق ، " صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية" ، المركز العربي لباحث الفضاء الالكتروني ، 24 مايو/حزيران 2022 ، متاح على الرابط : [https://accronline.com/article\\_detail.aspx?id=32528](https://accronline.com/article_detail.aspx?id=32528) <sup>(3)</sup> المصدر نفسه .

السيبرانية بينهما ، في ضوء الاتهامات المتبدلة بتوجيه هجمات إلكترونية ، على أهداف حيوية المزيد من عوامل التوتر، ارتبط أحدها بمقالة صحيفة "نيويورك تايمز" الأمريكية التي نُشرت في الـ 15 من يونيو / حزيران في عام 2019، إذ تضمنت تقارير تقيد بأن وكالة الاستخبارات المركزية الأمريكية تنشط عمليات قرصنة إلكترونية ضد مؤسسات حكومية روسية حيوية، وأن جنوداً في قيادة الحرب السيبرانية الأمريكية زرعوا شيفرة في أنظمة الطاقة الروسية لضربها حال تدهور العلاقات بين البلدين، ويسمح لهذه المجموعة من القرصنة العسكريين بتنفيذ "نشاط عسكري سري" على شبكات الكمبيوتر وفقاً لقانون تقويض الدفاع الوطني، الذي صدر في عام 2018 ، وعلى الرغم من أن الرئيس السابق دونالد ترامب قد نفى ذلك، إلا ان روسيا لم تستبعد أن مؤسسات أمريكية ما تابعة للدولة تفعل ذلك من دون إبلاغ الرئيس ترامب، مؤكداً أن المجالات الاستراتيجية الحيوية للاقتصاد الروسي كانت ولا تزال تتعرض لهجمات إلكترونية من الخارج، وأن موسكو تتعرض لهجمات إلكترونية أمريكية بشكل متكرر<sup>(1)</sup> .

على الجانب الآخر، تصاعد الاتهامات الأمريكية والغربية لروسيا الاتحادية بشن هجمات إلكترونية عليها، من أبرزها اتهام روسيا بالتدخل في الانتخابات الأمريكية لعام 2016، ومحاولة الهجوم السيبراني على منظمة حظر الأسلحة الكيميائية، واتهامات الاستخبارات الهولندية والبريطانية التي أسرفت عن اعتقال أربعة أشخاص قيل إنهم أعضاء في وكالة الاستخبارات العسكرية الروسية ، وكذلك اتهامات وزارة العدل الأمريكية ضد سبعة من علماء الاستخبارات الروسية بقرصنة منظمات مكافحة المنشطات الدولية<sup>(2)</sup>، كما كشف تقرير استخباراتي أمريكي بريطاني، أن فريقاً روسيّاً يقف وراء برمجية خبيثة تستخدمها الحكومة الروسية منذ 2019 ، وتم تطويرها ل تستهدف تقنيات حماية الشبكات الإلكترونية ، وأوضح تقرير نشرته وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية CISA، أن الفريق الروسي والذي يحمل اسم Sandworm، قد قام بتطوير برمجية خبيثة Cyclops Blink تستهدف أجهزة شركة Watchguard المتخصصة في تقديم أنظمة جدار الحماية البرمجية firewalls، التي تمثل أهميتها في حماية الشبكات الإلكترونية من أي هجمات سيرانية خارجية<sup>(3)</sup> .

<sup>(1)</sup> نورهان الشيخ ، " موسكو وواشنطن.. صراع سيراني " ، مجلة الخليج الإلكترونية ، 27 يونيو ، 2019 ، متاح على الرابط :

<https://www.alkhaleej.ae>

<sup>(2)</sup> نورهان الشيخ ، مصدر سبق ذكره .

<sup>(3)</sup> وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية CISA ، تقرير استخباراتي يكشف: هجوم سيراني روسي مستمر منذ سنوات" ، العربية نت ، 25 فبراير / شباط ، 2022 ، متاح على الرابط : <https://www.alarabiya.net/amp/technology>

بالمقابل نفت روسيا في أكثر من مناسبة هذه الاتهامات، من ناحية أخرى، تعزز الولايات المتحدة من دفاعاتها السيبرانية ، حيث أنشأت القيادة الإلكترونية الأمريكية مجموعة عمل خاصة لمواجهة أنشطة روسيا في الفضاء السيبراني، ووقع الرئيس الأمريكي دونالد ترامب مرسوماً في الـ 16 من أغسطس / آب في العام 2018 ، يلغى بموجبه التوجيه الرئاسي لسلفه باراك أوباما لتنظيم استخدام الأسلحة السيبرانية ضد معارضي الولايات المتحدة، رقم 20 لعام 2012، على النحو الذي يخفف القيود المفروضة على شن هجمات سiberانية ضد معارضي أمريكا<sup>(1)</sup> .

**3\_ الصراع السيبراني الإسرائيلي - الإيراني :** انتقل التنافس الإيراني - الإسرائيلي ، حول القوة والنفوذ في الشرق الأوسط إلى الفضاء السيبراني؛ إذ تخوض إيران حربا سiberانية متبادلة مع إسرائيل ، في إطار الصراعهما المرتبط بالمشروع النووي الإيراني ، إذ يعيش الطرفان حالة تأهب قصوى ضد أي هجمات إلكترونية قد تشنها أحدهما على الآخر .

فيما يتعلق بإسرائيل ، تشير إحدى الدراسات إلى امتلاكها وحدة لقيادة الحروب السيبرانية منذ عام 1952 ، واعترفت إسرائيل في العام 2008 ، بامتلاك قدرات سiberانية هائلة ، وبأنها استخدمتها في عملية "الرصاص المصوب" العسكرية التي شنتها ضد قطاع غزة في نهاية العام نفسه<sup>(2)</sup> ، كما تمتلك إسرائيل في هذا المجال قدرات سiberانية كبيرة، يجعلها قادرة على شن هجوم سiberاني ، والحق أضرار بالغة بالخصوم، فعلى سبيل المثال ، في نوفمبر/تشرين الثاني 2010 ، تمكنت إسرائيل من اختراق مفاعل نطنز (400 كيلومتر جنوب طهران)، فضلا عن منشآت نووية إيرانية أخرى ، عبر إدخال برنامج فيروسي "ستوكسنت" إلى أجهزة الكمبيوتر التي تحكم في أجهزة الطرد المركزي الإيرانية، لتخصيب اليورانيوم، وتسبب ذلك في إحداث فوضى وإخراج أجهزة الطرد المركزي عن نطاق السيطرة<sup>(3)</sup> ، وفي هذا المجال لا تعتمد إسرائيل على الدعم الغربي في تطوير قدراتها السيبرانية فحسب، بل تعتمد أيضا على خبراتها الذاتية بدرجة كبيرة ، اذ في عام 2011، أعلن رئيس الوزراء الإسرائيلي عن طموحه ، في أن تكون إسرائيل إحدى القوى السيبرانية العظمى، وبالفعل خلال عام 2012 ، أنسنت إسرائيل "المكتب الوطني للفضاء السيبراني" ، كما أنسنت في عام 2015 "الهيئة السيبرانية الوطنية" بهدف المشاركة في

<sup>(1)</sup> نورهان الشيخ ، مصدر سبق ذكره .

<sup>(2)</sup> ايهاب خليفة ، " ستوكسنت : سيناريو افتراضي للهجوم السيبراني على البرنامج النووي الإيراني " ، مركز المستقبل للدراسات والابحاث ، الامارات العربية المتحدة ، 15 ابريل / نيسان 2021 ، متاح على الرابط : <https://futureuae.com>

<sup>(3)</sup> أكبر هجوم إلكتروني على الإطلاق ضد إسرائيل.. خفايا الحرب السيبرانية بين طهران وتل أبيب " ، موقع الجزيرة ، 15 آذار 2022 ، متاح على الرابط : <https://www.aljazeera.net/encyclopedia>

صنع السياسات، كما أُسست "وحدة عسكرية" لتكون مسؤولة عن العمليات السيبرانية ، وبحلول عام 2016 ، كانت إسرائيل قد امتلكت فعليا نحو 300 شركة في مجال الأمن السيبراني، بل وأصبحت رائدة عالميا في هذا المجال ، وتعتمد على تصدير وبيع هذه التكنولوجيا المتقدمة إلى دول العالم<sup>(1)</sup> .

اما بالنسبة لایران فقد بدأ اهتمامها بتطوير قدراتها السيبرانية خلال العقد الأول من القرن الحادي والعشرين، إذ في العام 2005 ، أَسَّسَ كيان أطلق عليه "جيش فضاء إيران الإلكتروني" ، الذي يعد أحد الأذرع الرقمية ، التي يستخدمها النظام لشن هجمات إلكترونية على معارضي النظام في العالم، أو الدول الكبرى التي تقف عائقا أمام البرنامج النووي الإيراني ، وتطوير الصواريخ الباليستية، وفي المجالات الاستخباراتية وجمع المعلومات<sup>(2)</sup> .

وعليه ، أدى متغيران رئيسان الدور المحوري في تزايد الاهتمام بتطوير القدرات السيبرانية ؛ أولهما: إدراك قادة إيران بأن الولايات المتحدة تستهدف تغيير النظام الإيراني ، ودعم المعارضة الداخلية، وقد تأكّد هذا الإدراك عقب اندلاع "الثورة الخضراء" في إيران عام 2009، وذلك عقب فوز الرئيس الأسبق "أحمدي نجاد" بولاية رئاسية ثانية. ثانيهما: إدراك قادة إيران بأن الفضاء السيبراني ، أصبح أداة مهمة تُستخدم من قبل الخصوم ، في استهداف وتعطيل البرنامج النووي الإيراني، وقد تأكّد هذا الإدراك عقب هجوم "ستاكينت" الشهير عام 2010، ما أدى دوراً مهما في تحديد أهداف إيران من تطوير قدراتها السيبرانية ، فمن جانب تستهدف إيران بالأساس الحفاظ على استقرار نظامها السياسي ، واستخدام الفضاء السيبراني للتجسس على المعارضين للنظام السياسي الإيراني ، ومن جانب آخر تستهدف إيران استخدام الفضاء السيبراني ، لأغراض الهجوم والدفاع ، بهدف إدارة صراعاتها الدولية مع خصومها، لاسيما الولايات المتحدة ، وال سعودية، وإسرائيل ، وذلك من خلال صد أي هجوم سيبيري يستهدف برنامجها النووي، بل واستخدام الهجمات السيبرانية كأداة ضد الخصوم لتحقيق الاهداف السابعين<sup>(3)</sup> ، وتصاعد الإنفاق الإيراني على تحسين قدراتها السيبرانية منذ العام 2011 ، بدرجة ملحوظة ، إذ خلال مدة الرئيس السابق حسن روحاني (2013 - 2021)، تضاعفت ميزانية القوة السيبرانية إلى 12 مرة، ما جعل هذا إيران واحدة من القوى السيبرانية الكبرى الخمس في العالم ، وأنشأت إيران في العام 2012، جهاز

<sup>(1)</sup> عادل رفيق ، "الجيوبوليتكس السيبرانية والاستقرار في السرق الأوسط" ، ترجمات ، المعهد المصري للدراسات ، تركيا ، 2018 ، ص ص 7-6 .

<sup>(2)</sup> أكبر هجوم إلكتروني على الإطلاق ضد إسرائيل.. خفايا الحرب السيبرانية بين طهران وتل أبيب " ، المصدر السابق .

<sup>(3)</sup> Fareed Zakaria ، "Iran's Emergence as a Cyber Power" ، Studies Strategic Institute ، August 20 m 2014 ، <http://www.strategicstudiesinstitute.army.mil/index.cfm/articles>

"هاكتست" بهدف التجسس على المعارضة الإيرانية ، وفي العام ذاته أنشأت "المجلس الأعلى للفضاء السيبراني" بهدف رسم الإستراتيجية السيبرانية الإيرانية في مجالي الدفاع والهجوم ، وفي عام 2013 ، أنشأت الإنترنت الوطني والبريد الإلكتروني الوطني ، ومع تزايد عدد الهجمات السيبرانية التي تتعرض لها إيران ومنتجاتها سواء مدنية كانت أو نووية، طورت إيران ما يعرف بـ"القلعة الرقمية" التي بدأ تشغيلها عام 2019، وذلك بهدف صد أي هجوم سبيراني يهدف لإنكار وقطع الخدمات ، مثل إسرائيل، تهتم إيران بالاعتماد على الذات في مجال تطوير قدراتها السيبرانية ، قد نال المجال التعليمي حصة من الاهتمام الإيراني في هذا الشأن، حيث انتشرت في إيران مؤسسات دراسية، ومراكز بحوث علمية متخصصة في مجالات تكنولوجيا المعلومات، وبرمجة الحاسوب، وصد الهجمات الإلكترونية<sup>(1)</sup>.

لذا ، ونتيجة لتصاعد القدرات السيبرانية الإسرائيلية ، أكد المدير العام لمديرية الإنترنت الوطنية الإسرائيلية " غابي بورتنوي" ، فإن إيران هي المنافس الرئيس لإسرائيل في عالم الفضاء السيبراني ، وعليه أعلنت إسرائيل عن ما أسمته "قبة إلكترونية وطنية" ، في تشبهه بمنظومة القبة الحديدية ، التي تستخدمها إسرائيل لصد الصواريخ<sup>(2)</sup> ، وفي خضم تطور الصراع السيبراني الإيراني – الإسرائيلي ، شهدت السنستان الأخيرتان تصاعد في عدد الهجمات المنسوبة إلى إسرائيل ، كان أهمها تعطيل عمليات ميناء مرکزي في إيران، فضلا عن هجمات ارتبطت بالاستيلاء على كاميرات سجن إيراني، وتعطيل مرور القطارات، وإغلاق موقع حكومية، وأخيراً تعطيل العمل في مصنع للصلب ، والتي فسرها البعض نوع من الهجمات لتشديد الضغط على النظام الحاكم ، والسماح لإسرائيل بالرد على تطور القدرات السيبرانية الإيرانية<sup>(3)</sup>.

فضلا عن ذلك ، تتطلع إيران إلى الاعتماد على جهودها الذاتية في مجال تطوير الأسلحة السيبرانية ، ويشير المتابعون للشأن الإيراني بأن القدرات السيبرانية الإيرانية في حالة تطور مستمر منذ عام 2012، ولكن ما زال أمام إيران الكثير لتكون قوة عظمى في المجال السيبراني، فقدرتها الحالية لا تتنافس القدرات الأمريكية أو الإسرائيلية أو الروسية أو الصينية في هذا المجال؛ فعلى المستوى الهجومي، إيران غير قادرة حتى الآن على شن هجمات سيبرانية قوية وواسعة التدمير على الخصوم، بل تقتصر قدراتها على الأهداف الصغيرة المحلية ضعيفة التأمين مثل المصادر المحلية أو خطوط نقل الطاقة،

<sup>(1)</sup> ايهاب خليفة ، مصدر سبق ذكره

<sup>(2)</sup> عبد الرؤوف أرناؤوط ، " إيران تُنافسنا في الفضاء الإلكتروني" ، شبكة الاناضول الالكتروني ، 28.06.2022 ، متاح على الرابط : <https://www.aa.com.tr/ar>

<sup>(3)</sup> " حرب الإنترنت تغير استراتيجية إسرائيل" ، جريدة عمان اليوم الالكترونية ، 12 آب 2022 ، متاح على الرابط : <https://www.omandaily.om>

ورغم ذلك، تراهن إيران على صورتها وقدراتها على أن تكون تهديداً سبيرانياً ، أما على المستوى الدفاعي، قدرات إيران على صد الهجمات السيبرانية الموجهة إليها ضعيفة نسبياً ، في المقابل، قدرات إيران السيبراني الهجومية تتمحور حول أعمال القرصنة، وسرقة البيانات أو محوها، وإنكار الخدمة وتعطيل الواقع الإلكتروني<sup>(1)</sup> .

ومما تقدم ، يمكن الاشارة الى اهم الهجمات السيبرانية ، التي حدثت بين الجانبين الايراني والاسرائيلي ، وكالآتي<sup>(2)</sup> :

1. في عام 2010 ، تم اختراق مفاسع نطنز الايراني من خلال فايروس "ستوكسنت".
2. في فبراير/شباط 2020: تم حدوث هجوماً إلكترونياً استهدف شركات مزوّدة لخدمات الإنترنت في إيران، وأدى إلى اضطراب الاتصال بالشبكة .
3. في مايو/أيار 2020 ، حدوث هجوم معلوماتي لميناء الشهيد رجائي الإيراني .
4. في مايو/أيار 2020 ، هجوم إيراني على موقع إلكترونية تابعة لسلطات محلية اسرائيلية وشركات خاصة ومطاعم بهجوم سبيراني.
5. في 30 يونيو/حزيران 2020 ، تم استهداف سلسلة من المنشآت النووية الإيرانية في "نطنز" وموقع عسكرية في "بارشين" تم اتهام إسرائيل فيها ، بأحداثها هجمات سبيرانية لتعطيل برنامج إيران النووي.
6. في 26 أكتوبر/تشرين الأول 2021 ، وجهت إيران اتهام لدولة لم تعلن عن اسمها ، بالوقوف وراء الهجوم السيبراني ، الذي تعرضت له ، واستهدف الأنظمة الإلكترونية لمحطات الوقود.

ومن الجدير بالاشارة ، ان رغم التقديرات الهائلة للقدرات السيبرانية الإسرائيلية، سواء من جانب الإسرائيليين أنفسهم أو من جانب المحللين السياسيين، إلا إن مؤشر القوة السيبرانية لعام 2020 - التابع لكلية هارفارد كيندي- لم يضع إسرائيل ولا إيران ضمن القوى السيبرانية الكبرى، بل انتهى المؤشر إلى أن أكبر عشر قوى سبيرانية عالمياً على الترتيب من الأكثر إلى الأقل قوة هي: الولايات المتحدة، الصين، المملكة المتحدة، روسيا، هولندا، فرنسا، ألمانيا، كندا، اليابان، أستراليا. ووفقاً للمؤشر. مازالت القدرات السيبرانية الإسرائيلية والإيرانية لا تضاهي قدرات القوى السيبرانية العظمى، رغم أن كليهما لديه استعداد

<sup>(1)</sup>James Andrew Lewis , "Iran and Cyber Power", Center for Strategic and International Studies, June 25, 2019, available at: <https://www.csis.org/analysis/iran-and-cyber-power>

<sup>(2)</sup> "أكبر هجوم إلكتروني على الإطلاق ضد إسرائيل.. خفايا الحرب السيبرانية بين طهران وتل أبيب" ، مصدر سبق ذكره.

هائل لاستخدام القدرات السيبرانية في تحقيق أهدافهما الخارجية، أو على الأقل - كما أفاد التقرير - إن كلتا القوتين لا تكشفان عن قدراتهما السيبرانية الحقيقة<sup>(1)</sup>.

مما تقدم يتضح لنا انه من يمكن من الحصول على مقدرات القوة السيبرانية سيمكن من الإطاحة بالنظام العالمي الحالي ، إذ ان قدرات أمريكا الحالية في هذا الصدد لا تضمن لها هذا الدور، لاسيما مع لجوئها لاتباع سياسة "أمريكا أولاً" ، التي عملت على تقويض النظام العالمي الحالي ، وربما تعزز موقف منافسيها ، تاركة الولايات المتحدة وحلفائها عرضة لهجمات إلكترونية حكومية وغير متكافئة ، بالاستفادة من التكنولوجيا السيبرانية والإمكانيات التي توفرها ، لذا تتمتع الصين وروسيا بفرصة فريدة للتعجيل بانهيار القوة الأمريكية في النصف الأول من القرن الحادي والعشرين ، بمساعدة مجموعة واسعة من الجهات الفاعلة المستقلة وشبه المستقلة التي ترى أمريكا كقوة ، هي الهدف ليتم الاعتداء عليه .

وعليه نستنتج ، بأن الصراع الإلكتروني والسيبراني يعد أحد اهم القضايا المؤثرة في النظام العالم ، لأن امتلاك القوة التقنية والمعرفية تعد قوة اضافية لعناصر قوة الدولة الشاملة في القرن الحادي والعشرين ، وهذا يعني التأثير الإقليمي والدولي ، وهو ما لا ترغب به الدول المنافسة وبالذات الولايات المتحدة في سياق تطلعها المستمر للسيطرة والهيمنة على النظام العالمي ، وهنا يطرح السؤال التالي ، كيف ستتصرف الولايات المتحدة ، لمواجهة تطور القدرات السيبرانية للدول ، لحفظ على تصدرها وهيمنتها على هذه القدرات ، وبالتالي على مكانتها كدولة مهيمنة في النظام العالمي ، وهو ما سنحاول الاجابة عليه في المحور القادم .

### **ثالثاً: مستقبل الأمن السيبراني للقرن الحادي والعشرين**

على الرغم من أن القدرات السيبرانية ستكون عنصراً مهماً كأحد متطلبات التحول إلى القوة العظمى في القرن الحادي والعشرين ، فإن القدرات الإلكترونية المتقدمة لن تكون حكراً حصرياً على القوى العظمى ، بل ستكون للقوى الإقليمية الفاعلة دوراً مهماً في هذا المجال ، مما يتطلب إعادة التفكير بشكل أساسي في الشكل الذي قد تبدو عليه بنية الأمن المستقبلية ، ومن المرجح أن يؤدي الانتشار السريع للقدرات وتتوسيع التكنولوجيا إلى جعل نموذج حقبة الحرب الباردة ، من الإجراءات المتبعة في تطوير الإجراءات المضادة ، لاسيما وإن التفكير الاستراتيجي لبعض الدول التي تعدّها الولايات المتحدة

<sup>(1)</sup> Julia Voo, Irfan Hemani and others , "National Cyber Power Index 2020: Methodological and Analytical Considerations", Report, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge,(September 2020), p.2

عامل تهديد لامنها القومي ليست بعيدة عن امتلاك القوة السيبرانية ؛ إذ تؤكد الولايات المتحدة ؛ أن إيران و كوريا الشمالية قد طورتا قدرة نووية عابرة للcarat قبل أن تشعر بالتهديد الأمني ، ولكن مع الإنترن트 يصبح المجال عالميا ، ويمكن أن يصل التهديد النووي إلى قلب الولايات المتحدة<sup>(1)</sup>.

ومع الهجمات الإلكترونية التي يُحتمل أن تعيق البنية التحتية المدنية الوطنية مثل الطاقة والمياه وخدمات الطوارئ ، أو تحطم أسواق الأسهم العالمية وتسبب ركودا عالميا ، أو حتى إطلاق هجمات مضادة نووية آلية ، فإن الحرب الإلكترونية ستتجاوز كونها أداة لقوى العظمى للاستفادة منها ، وعليه فإن السعي إلى الهيمنة على الفضاء السيبراني ، يصبح قضية يجب على جميع الدولأخذها في الاعتبار ، وهي قضية لا يمكن إدارتها إلا بشكل توافق من خلال وضع قواعد جديدة لامن السيبراني ، وبما ان لا يوجد سوى دولة واحدة تمتلك الأصول والقدرات الازمة لتأمين الفضاء الإلكتروني على مستوى العالم في القرن الحادي والعشرين ، وهي الولايات المتحدة ، لذا فإن قضية الأمان السيبراني العالمي ليست مجرد مسألة وضع القواعد ، ولكن أيضا مسألة تنفيذ تلك القواعد ، لاسيما وان العديد من الدول والمؤسسات تفتقر ؛ إما إلى المصداقية لوضع القواعد ومثال على ذلك الصين ، أو الإرادة والقدرات لفرضها بالوسائل الضرورية ومثال ذلك الاتحاد الأوروبي ، لذا سيكون ذلك بمثابة اختبار للدبلوماسية والقدرة الأمريكية بشكل كامل في هذا المجال ، وسيتطلب وضع القواعد شمول مجموعة من الدول ذات القدرات التنافسية المستقلة للهجوم السيبراني ، بينما يتطلب تطبيق القواعد بناء والحفاظ على قدرات الانتمام المادية والرقمية للرد على الهجمات الإلكترونية<sup>(2)</sup>.

وعليه ، سيشمل مستقبل خارطة طريق البيئة الأمنية التي تقودها الولايات المتحدة للفضاء السيبراني الحادي والعشرين العناصر التالية ، والتي تتكون من التطورات الدولية والوطنية :<sup>(3)</sup>

1. المشاركة الدولية ، من خلال إعادة التأكيد على القيادة والمبادئ الدولية ، إذ لا يمكن للولايات المتحدة وضع قواعد أو قيادة وحدها ، من خلال نبذ مبدأ "أمريكا أولاً" .
2. إعادة التأكيد على مبادئ العولمة والتجارة الحرة واحترام حقوق الإنسان ، إذ ما أرادت الولايات المتحدة حشد الدعم الذي تحتاجه.

<sup>(1)</sup> Julia Voo, Irfan Hemani and others , "National Cyber Power Index 2020: Methodological and Analytical Considerations" , Op.Cit.

<sup>(2)</sup> Global Cyber Rivalry Challenges American Geopolitical Leadership" , Greater Pacific Capital , Op.Cit .

<sup>(3)</sup> Ibid.

3. تحديد مجموعة مقبولة عالمياً من قوانين الحرب السيبرانية والمعاهدات والبروتوكولات ، اذ لا يمكن تطبيق قواعد الحرب الحالية لتغطية نطاق الهجوم السيبراني وخيارات الدفاع ، لذلك ستكون هناك حاجة إلى قواعد جديدة.

4. الوكالات الدولية ؛ إذ يتطلب الدفاع السيبراني الفعال التعاون مع وكالات تنفيذ القانون بالولاية الأخرى ، لمواجهة الهجمات من الجهات الدولية غير الحكومية ، وهذا يتطلب العمل بشكل مباشر مع الدول الأخرى على الكشف عن التهديد والوقاية منه أيضاً.

5. الأدوار الدولية ومسؤوليات التنفيذ المشتركة ، إذ قد تحتاج الولايات المتحدة أن تكون الشرطي السيبراني العالمي ، وسيتطلب ذلك التنسيق مع خدمات تنفيذ القانون والأمن الدوليين ، لتعقب وإيقاف الجهات الفاعلة من غير الدول باستخدام بلددهم كقاعدة ، مع احتمال أن يوصف عدم التعاون شكلاً من أشكال الدعم الضمني .

6. تعزيز الأمن القومي والبنية التحتية المحلية ، إذ تحتاج جميع البلدان إلى الدفاع السيبراني الفعال عن بنيتها التحتية المدنية - العسكرية ، والحماية من هجمات سلطات المنافسين ، والدول المارقة ، والجهات الفاعلة من غير الدول والنشاط الإجرامي البسيط .

7. قواعد المشاركة الوطنية ؛ إذ بالنظر إلى ارتفاع معدل التطور التكنولوجي المستمر في جميع أنحاء العالم ، ستحتاج الدول إلى برامج دائمة للتنمية السيبرانية و التفكير بعناية في كيفية تطوير ونشر أعمالها ونشر الحماية الفعالة .

8. الدفاع الوطني والردع ، ذلك من خلال إنشاء وتنفيذ حملات الردع المصممة بالنظر إلى التدمير المحتمل الهائل للهجمات السيبرانية وصعوبة الدفاع ضدهم ، ويجب أن تستند استراتيجيات الدفاع السيبراني إلى الردع ، ما يعني ان الولايات المتحدة ستحتاج إلى وضع استراتيجيات ردع مخصصة مصممة خصيصاً لتهديدات ومهاجمين محددة ، والتخطيط للانتقام الهائل على نطاق متساو أو أكبر ، فضلاً عن ذلك ، ومن أجل موقعها كضامن للأمن السيبراني في القرن الحادي والعشرين لتكون ذات مصداقية ، ستحتاج الولايات المتحدة على الأرجح إلى إظهار قدرتها ، واستعدادها لتنفيذ مثل هذه الخطة في الرد على مخالف القواعد ، نظراً إلى أن المحرضين الأكثر ترجيحاً للهجمات السيبرانية العلنية ضد الولايات المتحدة وحلفائها يقدمون أنفسهم كمنافسين ، مثل الصين وروسيا ، فضلاً عن إيران ، وعليه ستحتاج الولايات المتحدة إلى تقييم استجاباتها بالنظر إلى التناقض الجيوستراتيجي الأوسع .

الخاتمة :

إن التطور في مجال القوة التكنولوجية قد هيأ مساحات جديدة للتنافس أدت إلى إنسار مجالات التنافس الواقعية لصالح مجالات تنافس تكنولوجية وسيبرانية ، مما ولد إدراكاً متزايداً لدى صانعي القرار ، لاسيما في الدول الكبرى أن المعركة لم تعد تقتصر على تعظيم القوة و الحصول على الموارد كما كان من قبل ، بل باتت مرهونة بمدى قدرة الدولة على التحكم في المجال التكنولوجي وتعزيز أنها السiberiani ، وهو ما يفسر التغير الذي بات يطرأ وبشكل كبير على إستراتيجيات الأمن القومي للدول الكبرى ، فالاستراتيجية الأمريكية للأمن القومي باتت أكثر إدراكاً لأهمية المزاوجة بين ثنائية الصلب والناعم لحفظها على هيمنتها على النظام العالمي ، وذلك من خلال توظيف القوة السiberiani ، ومحاولة استغلال تفوقها التكنولوجي للتسويق لصورتها كقوة عظمى لا يستقيم حال النظام العالمي ولا توازنها إلا من خلالها ، وباتت تستخدم في ذلك العديد من الوسائل ، التي تدخل ضمن الدبلوماسية العامة والرقمية ، أما الصين فإن إستراتيجيتها باتت تركز بشكل أكبر على بناء أنظمة الدفاع السiberiani للاستخدامات العسكرية والمدنية ، الذي يعد التفوق في مجال النطاق العريض للألياف البصرية للجيل الخامس نموذجاً مختصراً عن طبيعة التنافس في المرحلة القادمة ، وهذا ما يوضح قلق إدارة الرئيس السابق ترامب بشأن كيفية تأثير تلك المنافسة على الأمن القومي والاقتصادي للولايات المتحدة ، ولذا ركزت على ما يمكنها فعله لمنع وصول الصين إلى التكنولوجيا الفائقة ، فضلاً عن تشجيع الابتكار الأمريكي في الداخل من خلال زيادة التمويل الفيدرالي للبحث والتطوير ، كما ان تصاعد التوتر بين القوتين الأمريكية والروسية إلى جانب دول أخرى سيعمل على تهديد الأمن الجماعي الدولي وهو ما يعزز اتجاه إعادة الاعتبار للقانون الدولي والمنظمات الدولية في حفظ الأمن والسلم الدوليين ، لاسيما وأنه من المرجح أن تنتقل الحرب الباردة الجديدة عبر الفضاء السiberiani إلى داخل المعسكر الغربي من قبل روسيا والصين ، وحتى بالنسبة للقوى الإقليمية كإيران وإسرائيل لحين تحقيق التوازن الاستراتيجي في النظام الدولي . وعليه ، مما تقدم يمكن طرح أهم الاستنتاجات التي تم التوصل إليها وكالاتي :

1. تدل الاضطرابات السiberiani العالمية التي تحدث في العالم اليوم على تحول الحضارات من الصناعية إلى المعلوماتية ، مما ينذر بزوال النظام العالمي الحالي .
2. من بين هذه الاضطرابات الانتشار غير المسبوق في قدرات الحرب الإلكترونية ، مدفوعاً بنشر التكنولوجيا الرقمية بين الدول والجهات الفاعلة غير الحكومية ، بقيادة روسيا والصين ، فضلاً

عن امتلاك بعض القوى الاقليمية لهذه القدرات ، ولاسيما ايران في منطقة الشرق الاوسط ، مما يتسبب تهديد لامريكا وحليفتها اسرائيل .

3. أصبحت الهجمات الإلكترونية أكثر تعقيداً واستراتيجية ، حيث تطورت من السرقة الإلكترونية البسيطة إلى تأكيد السيطرة على البنية التحتية المادية وتقويض الحكومات والأنظمة السياسية بشكل حاسم .

4. علاوة على ذلك ، مع الانشار المتزايد للتكنولوجيا الرقمية ودمج أنظمة العالم الرقمي والمادي ، تصبح قدرة التدمير المادي المحتملة للفضاء الإلكتروني كارثية بشكل متزايد .

5. لم يقم أي بلد حتى الآن ببناء هجوم إلكتروني وقدرات دفاعية شاملة ، بينما تستمر أمريكا في قيادة العالم في مجال القدرات السيبرانية ، فإن الطبيعة غير المتكافئة للحرب الإلكترونية التي تفضل المهاجمين وسرعة الابتكار تمكن البلدان الأصغر من فرض تهديدات موثوقة للولايات المتحدة والدول الأخرى .

6. ستطلب إدارة هذه التهديدات السيبرانية العالمية المتزايدة أن تعمل البلدان على كل من المستوى الوطني (بناء القدرات ، والاستثمار في التكنولوجيا) وعلى المستوى الدولي (العمل مع الشركاء ووضع القواعد) .