

اسم المقال: توظيف الحروب السiberانية في تطوير مفهوم القوة للدول الكبرى
اسم الكاتب: أ.م.د. أنعام عبد الرضا سلطان العكابي
رابط ثابت: <https://political-encyclopedia.org/library/7532>
تاريخ الاسترداد: 2025/04/20 08:06 +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

استخدامكم لأرشيف مكتبة الموسوعة السياسية – Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع <https://political-encyclopedia.org/terms-of-use>

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



توظيف الحروب السيبرانية في تطوير مفهوم القوة للدول الكبرى

Employing cyber warfare in developing the concept of power for major powers

أ. م. د. أنعام عبد الرضا سلطان العكابي^١

الملخص:

يدور البحث حول الحروب الافتراضية السيبرانية التي بدأ الأداء الاستراتيجي للدول الكبرى تعمل بها بشكل جدي بعد نهاية الحرب الباردة حيث طرأ تغيير في مفهوم الحروب الذي بدوره أحدث تغيير في تطور ممارسة القوة. وقد تناولت هذه الدراسة تأثير التطور العلمي والتكنولوجي على مقومات القوة العسكرية والتغييرات على مفهوم القوة لتوظيف فيها الحروب السيبرانية. ولعل الاستخدام المتزايد لفضاء السيبراني للأغراض العسكرية أحد أهم اسباب تطور القوة لدى القوى الكبرى.

الكلمات المفتاحية: القوة، الحروب السيبرانية، القوى الكبرى، التطور العلمي والتكنولوجي، الفضاء السيبراني

Abstract

The research revolves around virtual cyber wars, in which the strategic performance of the major powers began to operate seriously after the end of the Cold War, when there was a change in the concept of wars, which in turn brought about a change in the development of the exercise of power. This study dealt with the impact of scientific and technological development on the constituents of military power and the changes in the concept of force to employ cyber warfare. Perhaps the increasing use of cyberspace for military purposes is one

^{1*} جامعة بغداد/ كلية الاعلام/ قسم الصحافة

of the most important reasons for the development of power among the major powers.

Keywords: power, cyber wars, superpowers, scientific and technological development, cyberspace

المقدمة

ان اسس العلاقات الدولية تقوم على ثلاثة ركائز اساسية وهي المصلحة والقوة والتنظيم الدولي وبموجبها شهد النظام الدولي تنظيم علاقات وحداته الاساسية ، وشهد تنظيم الهرمية والقطبية ، وعند تتبع عوامل القوة التي يتضمنها النظام الدولي وما به من علاقات دولية نجدها تتعلق بعوامل عديدة ونما عوامل القوة التقليدية وعوامل القوة غير التقليدية والتي جرت فيها تغيرات بين مرحلة واخرى بحسب ما يستجد من تغيرات تكنولوجية وغيرها من عوامل القوة التي يزداد وزنها في العلاقات الدولية هي القوة السيبرانية التي يمكن عدتها وسيلة ظهرت في هذا العصر ، وان التركيز عليها تصاعد بفعل ما احدثه التطور في تكنولوجيا الاتصالات والتكنولوجيا العسكرية والرقمية من تأثيرات وتغيرات مباشرة على الساحة الدولية والتي اصبحت سلاحاً يمكن ان يستخدم للحفاظ على الامن القومي او لدمار الدول وتقتيتها حيث جلب التطور التكنولوجي والمعلوماتي أعادة صياغة مفهوم القوة وظهور الفاعلين الجدد ودورها بدأ تطور الاسلحة السيبرانية وانتشار شبكة الاقمار الصناعية ودخول الدول الكبرى مضمون الحرب السيبرانية مثل الولايات المتحدة الامريكية والصين وروسيا والهند والباكستان وكوريا الشمالية وایران

أهمية البحث :

تناولت الدراسة مسألة الحرب السيبرانية وما للقضاء السيبراني من دور مهم ومؤثر على تطور ممارسة القوة والتأثير والنفوذ لدى القوى الكبرى. لذا فالدراسة تهدف الى بيان ان توظيف الدول والقوى الكبرى للقوة العسكرية غير التقليدية أوجب احداث تغيرات على مفهوم القوة للدولة من حيث دخولها الى المجال السيبراني والذي اصبح مرتبط بالأفراد والدول واصبح مفهوم الحرب السيبرانية بمثابة تهديد قومي وفعلي للدول تستخدمنه الدول الكبرى لتحقيق اهدافها.

اشكالية البحث:

مع تحول الفضاء السيبراني إلى ساحة للتقاعلات الدولية من الجانب التناصي والتصارعي الذي تكلل ببروز الحرب السيبرانية والانماط التوظيفية له بالأخص ذات الطبيعة العسكرية الامر الذي جعل هذا الفضاء منفذ للصراعات المختلفة وقياس القوة من خلاله من هنا تمحورت اشكالية الدراسة في التساؤلات التالية :

ما هي العوامل المحفزة التي اسهمت في ظهور حروب الفضاء السيبراني وتوظيفها من قبل الدول الكبرى؟

ما هي عناصر توظيف الحرب السيبرانية لتعزيز مفهوم القوة لدى القوى الكبرى؟

كيف ستوظف الحرب السيبرانية لدى القوى الكبرى في تطوير مفهوم القوة مستقبلاً؟

فرضية البحث:

دخلت الحرب السيبرانية بقوة في معادلات الصراع والمواجهة بين الدول الكبرى حيث وظفت من أجل استخدام القوة في السياسة الدولية والشؤون العالمية وتوزيعها بين القوى الكبرى. لذا فإن الحروب السيبرانية مجال لأستعراض القوة وممارسة النفوذ وتحقيق التفوق والتنافس ، واصبحت احدى عوامل مضاعفة قوة الدول الكبرى وفاعليتها.

منهجية البحث:

ان طبيعة البحث وموضوعه تستدعي الاعتماد بدرجة كبيرة على المنهج التحليلي (الاستباطي) من اجل تحليل عوامل القوة والمراحل التطورية التي مررت بها حيث أدت إلى بروز نوع جديد من الحروب لمعرفة مدى امكانية توظيفها على اداء الدول الكبرى .

أولاً: الفضاء السيبراني وتطور مفهوم القوة

أحدث التطور السريع للتكنولوجيا المعلوماتية وخاصة في الشبكات تحولا كبيرا في مفهوم القوة ترتب عليه دخول العالم في مرحلة جديدة تلعب فيها هجمات الفضاء السيبراني دورا اساسياً سواء في تعظيم القوة أو الاستحواذ على عناصرها الاساسية واصبح التفوق والتسابق المحموم للسيطرة على هذا الفضاء بشكل عنصرا للأمن الدولي في تنفيذ عمليات ذات تأثير على الارض والبحر والجو والفضاء .

1: العلاقة الجدلية بين السيبرانية ومفهوم القوة

اضحى النظام العالمي اليوم يواجه احد اكبر التحديات الخطيرة بعد دخول المجال الالكتروني ضمن المحددات الجديدة لمؤشرات القوة وابعادها الجديدة من حيث طبيعتها وانماط استخدامها ، بل وايضاً طبيعة الفاعلين وهو ما كان انعكاس على قدرات الدول وعلاقتها الخارجية. اليوم مع تدفق المعلومات والبيانات الهائل في الفضاء الرقمي وهيمنة العالم الافتراضي على تفاصيل حياتنا، ظهرت العديد من التحديات الجديدة المرتبطة بسيطرة هذا العالم على حياة الانسان في ظل اكتسابه قوة عالمية من خلال قدرة الثورة المعلوماتية والاتصالية الطاغية على جذب كافة شرائح المجتمعات وتقديمها لبدائل تواصلية مجانية وفعالة.²

فكثير من الدول وغير الدول تسعى للدخول لهذا الفضاء كساحة للصراعات الدولية، حيث يستطيع احد اطراف الصراع ان يوقع خسائر فادحة ويتسبب في شلل البنية المعلوماتية والاتصالية للطرف المستهدف عن طريق اسلحة وقدرات تكنولوجية وعسكرية كبرامج التجسس والفيروسات. وبالتالي اضحى المفهوم الجديد للأمن يدور في فلك الحفاظ على سلامة الدولة في ظل تلك التطورات التكنولوجية، ومن هنا أصبح الصراع الجديد يعني بكل ما من شأنه التنافس والترابط التكنولوجي وارتباط شكله وانماطه في عصر المعلومات.³

لا أحد ينكر ان الهجمات السيبرانية التي يواجهها المجتمع الدولي يومياً وتجري لأغراض التجسس والتخريب والتلاعب باتت اكثر تعقيداً من اي وقت مضى على مدار السنوات الاخيرة أذ عانت انواع التكوينات الالكترونية المختلفة والعديد من القطاعات الصناعية والمالية والاقتصادية من مجموعة كبيرة من الهجمات السيبرانية والتهديدات الالكترونية. وقد تجلت تلك السبل في هيئة برمجيات وفيروسات ضارة خبيثة وطرائق تلاعب وتصيد الكتروني احتيالي. حتى اصبحت هذه التهديدات من الصعب حصرها أو تطوير استراتيجيات محكمة لمواجهتها بشكل كامل ، خاصة مع تعدد وتنوع اشكالها ومصادرها وتطورها المتتابع والمستمر. ومن المعلوم ان الهجمات الالكترونية مثل القرصنة كأحد الاشكال الشائعة لجرائم الانترنت والجرائم السيبرانية التقليدية والتهديدات السيبرانية للأيدلوجيا اصبحت كأحد اهم العناصر المؤثرة في أوجه الصراع الدولي. بعد انتقال جزء كبير من الصراعات بين القوى المؤثرة الى الشبكة العنكبوتية والوسط الرقمي. لقد بات احد

² احمد عيسى الفتلاوي، الهجمات السيبرانية : مفهومها والمسؤولية الدولية الناتجة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الالحي للعلوم القانونية والسياسية، المجلد 8، العدد 4، جامعة بابل، 2016، ص57.

³ خلود عاصم ومحمد ابراهيم، دور تكنولوجيا المعلومات والاتصالات في تحسين جودة المعلومات وانعكاساته على التنمية الاقتصادية الجامعية، مجلة كلية بغداد للعلوم الاقتصادية ، الجامعة، العدد الخاص بمؤتمر الكلية، 2013، ص89.

اطراف الصراع قادرًا على ايقاع خسائر فادحة بالطرف الآخر وشل بنيته المعلوماتية والاتصالية الخاصة به.⁴ وما ترتب على ذلك من خسائر عسكرية أو اقتصادية أو امنية من خلال قطع انظمة الاتصال او بث فيروسات او تضليل معلومات او سرقتها والتلاعب بالبيانات الاقتصادية والمالية وتزيفها او حتى مسحها من الوجود. ان الارقام المتعلقة بالامن السيبراني مقلقة جدًا فمثلاً حجم الخسائر التي يتكبدها العالم تقدر بbillions الدولارات سنويًا جراء الهجمات الإلكترونية حيث يتوقع الخبراء بأن هذه الهجمات ستكلف العالم اكثر من 10 تريليونات دولار بحلول عام 2025.⁵

نجد ان حجم الانفاق العالمي على الامن السيبراني بأزيداد ايضاً حيث نرى الكثير من الخطط التي اعلنت عنها دول متقدمة وشرعت بزيادة نشاطها ووضع بنود في موازنتها العامة بـbillions الدولارات بالأخص في الولايات المتحدة الامريكية والصين وروسيا وبعض الدول الاوربية تحديداً لمجابهة التحديات والمخاطر السيبرانية وتكثيف جهودها لحماية امنها الالكتروني وتحسين بنيتها التحتية الحيوية ، وتطوير سياسات لرفع الوعي حول قضايا الامن السيبراني وتطوير المخططات الوطنية لتحفيز وتعظيم الوسط الرقمي لها، بهدف تقليل مخاطر وآثار الهجمات السيبرانية التي يتعرض لها العالم بـاستمرار. لهذا اولت القوى الكبرى اهتماماً واضحاً في توظيف الفضاء الالكتروني لتعزيز قوتها، من خلال ايجاد ميزة او تفوق او تأثير في بيئه الوسط الرقمي، وبالتالي ظهر ما يسمى بـ"الاستراتيجية السيبرانية" للدول⁶، والتي تشير الى القدرة على التنمية وتوظيف القدرات للتشغيل في الفضاء الالكتروني وذلك بالاندماج والتنسيق مع المجالات العملياتية الاخرى لتحقيق او دعم انجاز الاهداف عبر عناصر القوة القومية، بحيث اصبح التفوق في ذلك المجال عنصراً حيوياً في تنفيذ عمليات ذات فاعلية في الارض والبحر والجو والفضاء واعتماد القدرة القتالية في الفضاء الالكتروني على نظم التحكم والسيطرة التكنولوجية والذكاء الصناعي. أما بالنسبة لمفهوم القوة فلم تعد قوة الدول تُقاس بالمساحة وعدد السكان والثروة الطبيعية والقدرة العسكرية وإنما باتت تتحدد بامتلاك وسائل العلوم والمعلومات والتكنولوجيا. فالقوة كمفهوم نسبي ومتغير لم يبقى بالمعنى التقليدي في الادبيات الكلاسيكية هناك مؤشرات القوة والنفوذ للدول اليوم تبدو مختلفة بعد انتقال العالم من تقانات الثورة الصناعية

⁴ خالد وليد ، الفضاء السيبراني .. نحو امتلاك ناصية القوة، www.aljazeera.net 10/11/2021

⁵ فاتح حاريك، الفضاء السيبراني والتحول في شكل الحروب دراسة حالة روسيا، www.reasearchgate.net june 2021

⁶ وليام ستولينج، اساسيات امن الشبكات: تطبيقات وعاییر، ترجمة: السيد محمد الالفي ورضوان السعيد عبدالعال، ط، 1، الرياض، العبيكان للنشر، ص 78.

إلى الثورة التكنولوجية المعلوماتية. فنحن على اعتاب الثورة الصناعية الخامسة القائمة على الذكاء الصناعي لم يعد بإمكان أي دولة أن تقيس مكانتها كقوة إقليمية أو دولية بالأعتماد فقط على عوامل القوة التقليدية (الصلبة)⁷، إذ باتت تحدّم المعطيات امتلاك الدول لـ"القدرة السيبرانية" التي أزاحت العديد من عناصر القوة التقليدية من مكانها حيث لم يعد امتلاك الدول للأموال والثروات والقدرات العسكرية والجغرافية الشاسعة كافياً بلبورة دورها كقدرة فاعلة ومؤثرة ذات نفوذ في السياسات العالمية. اليوم تسعى الكثير من الدول لأمتلاك القدرات السيبرانية وباتت هذه الأخيرة تأخذ شكلاً جديداً في طبيعتها ووسائلها وادواتها ونرى اليوم أن الصراع الدولي يتوجه بالأساس نحو السباق والتنافس في ساحة الانجازات التكنولوجية التي غيرت من شكل الحروب وادواتها واثرت على الفاعلين بها وساهمت في إعادة التفكير في حركية وдинاميكية الصراع.

2 _ تطور مفهوم القوة

تتعدد الصور التي تتخذها القوة وتتغير وفقاً لطبيعة وشكل النظام القائم، فالقدرة هي حجر الأساس لأي تنظيم سياسي حيث تُعرف بأنها القدرة على التأثير في الآخرين للحصول منهم على نتائج محددة يسعى الطرف الذي يقوم بعملية التأثير للحصول عليها. وكذلك هي علاقة خاصة بين طرفين يستلزم أن يكون أحد الطرفين فيها على قدر أكبر من الامكانات ما يتيح له بعض التفوق في السلطة والسلطان. فالقدرة مفهوم حركي ديناميكي غير ثابت يتكون من عناصر متغيرة مادية أو غير مادية متراقبة مع بعضها البعض ، كما ان القوة شيءٌ نسبي تقيس قوة الدولة بالمقارنة بقوة الدول الأخرى وأحياناً توجد بعض الدول الصغيرة التي تمتلك قوة تجبر الدول الكبرى على تغيير سياستها وفقاً لسياسة الدولة الصغيرة ، وممكن ان نحدد خصائص القوة

بعدة نقاط وهي كالتالي⁸:

1. القوة وسيلة لممارسة النفوذ والتأثير ويهدف لتحقيق مصالح الدولة سواء كانت مصالح قومية او حماية الامن القومي.
2. يتغير وزن قوة الدولة وفقاً لقدرتها على تحويل مصادر القوة المتاحة أو الكامنة إلى قوة فعالة.
3. تتصف القوة بقدرتها لذلك تحرص الدول على ما تمتلكه وتحاول عدم تشتيت جهودها.

⁷ايها خليفة ، القوة الالكترونية : كيف يمكن ان تدير دولة شؤونها في عصر الانترنت" الولايات المتحدة نموذجاً " ط1 ، العربي للنشر والتوزيع، القاهرة، ص90-94.

⁸علي زياد العلي، المرتكزات النظرية في السياسة الدولية، ط1، القاهرة ، دار الفجر للنشر والتوزيع، ص34.

4. القوة بطبعتها شيء نسبي تُقاس قوتها بالمقارنة بقوة الدول الأخرى.
5. تدرج ممارسة القوة بين التأثير بالطرق الدبلوماسية من جهة وبين اسلوب الاجبار والقسر من جهة أخرى، واللجوء الى القوة غالباً يكون نتيجة العجز للوصول لحلول بالطرق السلمية.

1- التحول في عوامل القوة

يشهد العالم تحول نحو تبني قوة المعرفة والمعلومات، لكن هذا لا يفسر تراجع معايير القوة التقليدية للدول مثل الموارد الاولية وحجم اصناف القوة التقليدية والقوة الاقتصادية ، ولكن سوف تتدخل معها اشكال جديدة في محاور التناقض والصراع، حيث يؤكد الباحث الامريكي (الفن توفلر) في كتابه تحول السلطة : " ان العالم يشهد الان انتقال في القوة الأساسية المسيطرة على حركته والتحول من القوة الصلبة بعواملها المتمثلة بالقوة العسكرية والقوة الاقتصادية إلى نسق جديد يعتمد على المرونة والجذب القائمة على قوة المعرفة والمعلومات " .⁹

2- تراجع عوامل القوة التقليدية

وعلى الصعيد العسكري والتكنولوجي، نجد ان تقنية التكنولوجيا النووية لم تعد حكراً على الدول العظمى فقط حيث أصبحت اليوم في متناول عدد كبير من الدول، وهذه المتغيرات من شأنها ان تفرض حدوداً معينة على الخيارات السياسية والعسكرية المتوفرة لدى الولايات المتحدة، وعليها ان تتعامل مع هذا الواقع الجديد، وان تتنازل عن فكرة قيادة

العالم من خلال القوة وسياسة التدخل العسكري في الشؤون الداخلية للدول.¹⁰

لقد أدركت الدول حجم الخسائر الفادحة من جراء استخدام القوة العسكرية وعبء التكاليف المالية التي تحملتها وحدها في ادارة النظام الدولي والتي اثقلت كاهل ميزانيتها مما أدى الى ضرورة التفكير ببدائل في التراجع عن استخدام القوة العسكرية إضافة الى استثمار القوى الكبرى احتكارها الكبير لوسائل الاتصال والإعلام الجماهيري المعدة مسبقاً لصياغة نمط الحياة وقواعد السلوك بما يتواافق مع اتجاهاتها ، حيث

⁹نقلأً عن الفن توفار ، تحول السلطة ، الجزء الاول ، ترجمة ، لبنى الريدي ، الهيئة المصرية العامة للكتاب ، ط1 ، الالف كتاب الثاني ، المجلد 2 ، ص 87.

¹⁰عباس بدران ، الحرب الالكترونية: الاشتباك في عالم المعلومات ، ط1 ، بنان ، بيروت ، مركز دراسات الحكومة الالكترونية ، ص 45.

عملت التكنولوجيا على اضعاف وازاحة وتحييد الكثير من عناصر القوة عن مراكزها التي هيمنت عليها فترة طويلة من الزمن ، مما عرض المفهوم التقليدي للقوة إلى إعادة النظر فيه والإفصاح عن محتوى جديد في مفهوم القوة ومستقبلها في إدارة الصراع لقرن الحادي والعشرين، ان اتجاهات هذا التغيير الذي أحدثه الثورة التكنولوجية في مستقبل مفهوم القوة وآلياته ومكوناته في حالة حركة مستمرة ومتصاعدة وهو في مراحل تكوين جديدة لقد أحدث المتغير التكنولوجي تغييرات ملموسة في مفاهيم القوة والاستقطاب والتوازن ، فمن الجانب النظري فإن القوة بدلالة التكنولوجيا تتميز عن القوة بدلالة الإكراه التي انطبع عليها المفهوم التقليدي للقوة بالجوانب التالية-¹¹:

- 1-القوة بدلالة التكنولوجيا لا تعرف النضوب، حيث أن بمقدورها ان تمنح المزيد من الابتكارات على عكس القوة بمفهومها التقليدي والتي تتسم بكونها محدودة فيما يتعلق بكافة الشؤون العملية، إذ ان هناك حدوداً لمقدار وكمية القوة الذي يمكن استخدامها في تدمير ما تطمح في السيطرة عليه أو الدفاع عنه.
- 2-تقوم القوة بدلالة التكنولوجيا بعمل مضاعف بالمقارنة مع القوة العسكرية والاقتصادية، بمعنى ان الاولى يمكن ان يتم استخدامها اما لزيادة المتاح من الامكانات أو التقليل من القدر المطلوب من أجل تحقيق أهداف معينة مما يجعلها اداة هيمنة وتغيير في آن واحد .
- 3-الترابط الاندماجي، والذي يعني ان التكافف والتعاون الذي يجمع عناصر قوى مختلفة سيؤدي إلى حصيلة تراكم القوة التي تتفوق عن الجمع الفردي لعوامل القوة. وبالنتيجة لم يُعد المعيار العسكري يمثل العنصر الأول لمعرفة قياس قوة الدول ، حيث اتسمت الثورة التكنولوجية للمعلومات والاتصالات والمواصلات بالأهمية النوعية والعددية، ولكي يتم استخدام هذه الآلية بفعالية يجب إضافة عوامل أخرى عليها كالتقنية والمعلوماتية والاتصالاتية وكذلك إمكانية التحرك والتدخل بعيداً عن إمكانية اختراق الحدود بخوض معارك برية، هذه العوامل بالإجماع قد تعطي قوة للعامل العسكري تدفعه إلى التطور والتقدير. لقد سعى متغير التطور التكنولوجي إلى فرز قواعد وسلوكيات بنمط جديد لم تعد الدول قادرة على ضبط آليات اقتصادها بمنأى عن هيكل وآليات اقتصاديات الدول الأخرى، لقد أحدثت التغييرات الاقتصادية في ظل حقبة مجئ

¹¹ وليد عبد الحي، الدراسات المستقبلية في العلاقات الدولية، عيون المقالات ، مراكش، ط2، 1993، ص 92 . انظر كذلك: محمد حسن آل ياسين، اندماج التكنولوجيا ومهام البحث والتطوير الجديد، النشرة الفصلية الصادرة عن المنظمة العربية للتنمية الادارية ، العدد 29، 1999، ص 9.

الثورة التكنولوجية المعاصرة وثورة الاتصالات والمعلومات تغيرات في أغلب المفاهيم الاقتصادية. بالإضافة إلى العامل العسكري الذي نتج عنه تطور في امكانيات وأدوات الرصد والمراقبة من خلال استخدام الأقمار الصناعية وشبكات الرادار المثبتة تقنياً ووسائل الاتصالات والإعلام، فضلاً عن العامل الثقافي الذي تأثر بمجئ ثورة الاتصالات والإعلام والتغيرات التي طرأت عليها ، والتي أفضت إلى بروز ظاهرة العولمة التي أدت إلى توحيد الأسواق العالمية ودمج الاقتصاد العالمي ، وفي الوقت ذاته فإنها تسعى إلى تفتيت الثقافات الوطنية واحتراقها . وبهذا اتخذ المفهوم الثقافي للعولمة بعداً اقتصادياً ومالياً وإعلامياً من خلال توظيف الإعلام كأداة للتوصيل والتأثير تجاه الأفكار الثقافية.¹²

3: الحرب السيبرانية (المفهوم والدّوافع)

سوف ننطلق في تحديد مفهوم السيبرانية والتي هي في اللغة مصطلح مشتق من الكلمة اليونانية (kybernetes) بمعنى القيادة والتحكم عن بعد. وهي عملية استخدام تقنيات التواصل الاجتماعي على الانترنت لأنشاء وتشغيل وإدارة النشاط من أي نوع. إنها تتيح لأي فرد أو مؤسسة استخدام الشبكات الاجتماعية وغيرها من التقنيات عبر الانترنت للوصول الى المتابعين وجمعهم وبث الرسائل. وايضاً هو مصطلح درج استخدامه لوصف الفضاء الذي يضم الشبكات المحسوبة وشبكات الاتصال والمعلومات وانظمة التحكم عن بعد ، وتحتختلف استخدامات السيبر من دولة الى اخرى وفقاً لأولويات الدول : فهناك السيبر المدني والامني والاستخباراتي ، ويكون السيبر من ثلاثة مكونات:

الاجهزه والبرمجيات الرقمية وطاقم المطوريين والمبرمجين¹³

1-مفهوم الحرب السيبرانية

والتي تسمى بالحرب الإلكترونية عبر الانترنت وهي اجراء عسكري يتضمن استخدام الطاقة الكهرومغناطيسية للتحكم في المجال الذي يتميز باستخدام الإلكترونيات والطيف الكهرومغناطيسي لاستخدام بيانات التبادل عبر الانظمة الشبكية والبني التحتية المرتبطة بها. وقد عرفها Michael nschmit (Michael nschmit). " بأنها تلك الاجراءات

¹² مايكيل ديرتوزوس، ماذا سيحدث كيف سيغير عالم المعلومات الجديد حياتنا، ترجمة وتقديم بهاء شاهين، مركز الحضارة العربية، ط2، 2000، ص55.

¹³ نوره شلوش ، القرصنة الإلكترونية في الفضاء السيبراني " التهديد المتصاعد من الدول ، مجلة مركز بابل للدراسات الإنسانية ، مجلد8، العدد2، جامعة بابل، 2018 ، ص87.

التي تتخذها الدولة من أجل الهجوم على نظم المعلومات للعدو وبهدف التأثير والأضرار فيها والدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة". وإذا شكلت الهجمات السيبرانية وتبعاً للظروف نزاعاً مسلحاً فنكون أمام مصطلح الحرب السيبرانية أو ما يعرف بالهجوم السيبراني والتي تكون أوسع نطاقاً من الحرب السيبرانية وقد تحدث خارج اطار الحروب وقد تكون سبباً لبدء الحرب¹⁴. ان الهجمات السيبرانية يمكن ان تكون جزءاً من حرب سيرانية متى ما استخدمت في اطار نزاع مسلح واستهدفت تحقيق اهداف عسكرية وبالتالي هي اجراءات تتخذها الاطراف في نزاع مسلح لكسب الميزة على خصومهم في فضاء الساير باستخدام مختلف الادوات التكنولوجية والاشخاص التقنيين ويحصل على المزايا من جراء تلك الهجمات من خلال اتلاف أو تدمير أو تعطيل أو اغتصاب انظمة الحاسوب للعدو أو من خلال الحصول على معلومات التي يرغب العدو في ان تبقى سرية أو ما يُعرف بالتجسس السيبراني أو الاستغلال لشبكات الحاسوب متى ما كانت في أطار نزاع مسلح يصل الى مستوى الحرب¹⁵. وتعرف أيضاً بأنها الحروب التي تستهدف تعطيل أو تدمير نظم المعلومات والاتصالات في الدولة العدو، وهي تشن اساساً داخل بيئه المعلومات بحيث تستهدف تعطيل كفاءة السيطرة والقدرة على التحكم في منظومة اجهزة أو شبكات الحاسوب وما تتضمنه من بيانات ومعلومات لفاعلين الآخرين أو تقليلها أو حتى تدميرها سواء كان ذلك على مستوى البنية التحتية الوطنية لدولة أو على مستوى منظومات قوتها العسكرية. وهناك تنوع في الأدوات والوسائل واشكال الهمات والحروب السيبرانية بما في ذلك بث فيروسات والبرامج التخريبية والمدمرة لأنظمة والشبكات الحاسوبية أو اختراق حسابات والوصول الى معلومات سرية وتسريبها أو الاستفادة منها لأغراض عسكرية وامنية عدائية.

2- دوافع الحرب السيبرانية

هناك تنوع في الأهداف المراد التعرض لها وعدم اقتصارها على اهداف عسكرية ، أذ يمكن ان تستهدف الضربات الإلكترونية اهداً مدنية وقطاعات خدمية وانتاجية ، كذلك عززت الحروب السيبرانية من مستويات وفرص الحرب الالكترونية وذلك مع تمكن دول متقاربة القوة وحتى تنظيمات من غير الدول من شن الهجمات

¹⁴ خالد وليد محمود، الهجمات عبر الانترنت ، ساحة الصراع الالكتروني الجديدة ، سلسلة دراسات ودراسة السياسات ، المركز العربي للأبحاث ، قطر ، 2013 ، ص 57.

¹⁵ عادل عبد الرزاق ، الإرهاب الالكتروني: القوة في العلاقات الدولية : نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والاستراتيجية بالأهرام، القاهرة، 2009، ص 87.

ضد الدول ذات القوة العسكرية والاقتصادية الأكبر أضافة إلى أنها باتت اسلوباً معتمداً بشكل متزايد ضمن استراتيجية الحروب الهجينة من قبل عدد متزايد من الدول.¹⁶

من ابرز دوافع شن الحروب السيبرانية هي الدول باتت تعتمد بشكل متزايد على خيار شن الهجمات الإلكترونية بهدف إلحاق الضرر بالخصوم والأعداء وذلك بأعتبار أنها وسيلة غير مكلفة أذا ما قورنت بوسائل الهجوم العسكرية التقليدية فهي لا تحتاج إلى معدات وجيوش مجهزة كما ان احتمالية وقوع الضحايا والخسائر البشرية في صفوف القوة المهاجمة تكون منعدمة . كما أنها تلحق ضرراً كبيراً بالخصم هذا بالإضافة إلى أنها تتسم بصعوبة تحديد مصدر الهجوم وبالتالي تجنب الدول الأدلة وال subsequences القانونية وال subsequences العسكرية للهجوم بما في ذلك تجنبها اي ردود عسكرية مباشرة على الهجمات اي أنها تتسم باخلاء المسؤولية وذلك بالنظر إلى صعوبة تحديد الجهة والمكان الذي صدر منه الهجوم ، وكذلك امكانية التلاعب والتمويه العالى فيما يتعلق بمصدر ومكان توجيه شن الهجوم الإلكتروني ، أضافة إلى استخدام سلسلة من الوكلاء في شن الهجوم بما يبده اي احتمالية تتبع مباشر للدولة صاحبة القرار في شن الهجوم¹⁷ . كما ان هذه الحروب مقتنة بالضرورة بنية الحق الضرر بالخصم وذلك في إطار حالة من الخصومة والعداء بين الدول والاطراف وهذا ما يجعلها مختلفة عن الهجمات ذات الطابع الجنائي التي قد تتشابه في بعض حيئات الهجوم مثل حالات اختراق حسابات والوصول إلى معلومات ، ولكنها تبقى مفنة عنصر النية بالحق الضرر نوعاً من التصعيد وسبباً للضغط عليه بغية الوصول إلى نوع من الأذعان وتقديم التنازلات من قبله وهو ما يكون متحققاً في حالة الهجمات الإلكترونية والتي تأتي ضمن سياق ما يمكن تسميته بالحرب الإلكترونية.

وبالإمكان اعتبار حروب الفضاء الإلكتروني بمثابة الانعكاس والمخرجات للثورة الرقمية والإلكترونية في الميدان العسكري، وهي تقوم على أساس شن الهجمات على هيكل تكنولوجيا المعلومات الحيوية للخصم والتي تكون مشغلاً لمصالحه المدنية وقدراته العسكرية بحيث يكون الحق الضرر بها موازاً ومعادل للفحص العسكري المباشر بواسطة الأسلحة التقليدية وغير التقليدية.

¹⁶سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي: رؤية مستقبلية ، مجلة رسالة الحقوق ، العدد 2 ، السنة السابعة ، مركز الدراسات القانونية والدستورية ، جامعة كربلاء ، 2015 ، ص 90-95.

¹⁷ليتيم فتحية وليتيم نادية، الامن المعلوماتي للحكومة الإلكترونية وارهاب القرصنة، مجلة المفكر ، العدد 12 ، كلية الحقوق والعلوم السياسية ، جامعة محمد خضرير ، الجزائر ، 2015 ، ص 78.

ثانياً: توظيف الحرب السيبرانية في الدول الكبرى

1: خصائص وعناصر توظيف الحرب السيبرانية:

امتازت الحروب السيبرانية بخصائص عديدة كانت الدافع وراء اعتماد العديد من الفاعلين الدوليين عليها سواء كانوا دول أو فاعلين من دونها وفي مقدمة هذه الخصائص انخفاض تكلفتها بالمقارنة مع أدوات الحرب التقليدية ، فضلاً عن ما يمكن ان تتحققه من نتائج ملموسة في إطار الصراعات والنزاعات ، بالإضافة إلى اختلاف عقidiتها العسكرية وقواعد الاشتباك فيها عن نظيرتها في سائر اشكال الحروب السابقة التي عرفتها البشرية ، على مستوى الفاعلين تركت حروب الفضاء السيبراني تأثيرات هامة في طبيعة المواجهات حيث بات بالإمكان ان يكون هناك اطراف فاعلة من غير الدول أذ ان الاسلحة المستخدمة في هذه الحروب ليست حكراً بيد الدولة وبحيث بات يتردد الوصف لحروب الفضاء الالكتروني بأنها حروب غير تناظرية¹⁸. وذلك عائد للتكلفة المتدنية نسبياً للأدوات اللازمة لشن هكذا حروب فلكي ينخرط فيها طرف من غير الدول فليس هناك حاجة لأن يقوم بتصنيع اسلحة مكلفة جداً مثل حاملات الطائرات والمقاتلات المتغيرة لتفرض تهديداً خطيراً و حقيقياً على الاطراف الأخرى وإنما يكفي تطوير البرمجيات الأزمة وامتلاك الأجهزة الحاسوبية¹⁹. ويتصل بذلك احدى اهم خصيصات الحرب السيبرانية وهي فشل امكانية تطبيق فكرة ومبدأ الردع والتي عادة ما تستخدم من قبل دولة ضد دولة اخرى في إطار منظومة الحرب التقليدية أما في الحرب الالكترونية فهي غائبة وذلك عائد الى خصائص عده اذ ان هناك معضلة في تحديد الدولة والجهة التي قامت بالهجوم فبإمكان القوة المهاجمة شن هجوم على دولة لصالح دولة اطلاقاً من دولة ثالثة عبر استخدام خوادم تكون موجودة هناك بل ومن المستحيل في كثير من الاحيان تحديد مصدر الهجمات الالكترونية، ويقترن بهذه الخاصية اخرى تميز الحرب السيبرانية وهي انه لا توجد حدود جغرافية واضحة في هذه الحروب ، كما لا يتواجد مفهوم السيادة بمعناه السائد في العالم الواقعي بحيث يتم منع الأطراف الأخرى من الدخول الى المناطق الخاضعة لسيادة دولة ما مثلاً، بل أنه بالإمكان وصف الحدود في الفضاء الإلكتروني بأنها حدود مائعة أو بالأحرى لا توجد حدود في الفضاء الالكتروني أو في العالم الافتراضي أذ

¹⁸نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني "التهديد المتتصاعد من الدول" ، مجلة مركز بابل للدراسات الإنسانية، مجلد8، العدد2، جامعة بابل، 2018، ص 57.

¹⁹وفاء بوكابوس، تحول القوة في العلاقات الدولية: دراسة في انتقال القوة من التقليدية إلى الحديثة، ط1، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، المانيا، 2019، ص 69.

ان الحدود تتداخل مع بعضها حيث ان كل الدول صغيرة وكبيرة تشارك في نفس الشبكات تكون في كثير من الأحيان موجودة في بلدان أخرى غير البلدان المستخدمة لها والمشغلة لها. في الحروب السيبرانية تشمل على عمليات تعتبر مساندة للعمل العسكري من التجسس على الاشارة أو التشويش على نظام الموقع العالمي واعاقته لدى العدو وعرقلة عمليات توجيه الأسلحة العسكرية المعادية²⁰. أما بخصوص طبيعة الأسلحة والأدوات المستخدمة وانواعها في هذا النوع من الحروب ، فإن القوة الالكترونية تعتمد بصفة اساسية على الاجهزه والبرامج ، الاجهزه تشمل على انظمه الحاسوب مثل وحدة المعالجة المركزية أو محرك الاقراص الضوئية أو لوحة المفاتيح وكذلك الاقمار الصناعية. اما البرامج فهي الصياغات البرمجية المستخدمة لتجهيز عمليات الحاسوب والتي يستخدم فيها البرامج الضارة والفيروسات مثل لغة الاستعلام الهيكلية وهي عبارة عن مجموعة من التعليمات المستخدمة للتفاعل مع قواعد البيانات ، وعمليات الحقن الإلكتروني عبر أدخال برمجيات ضارة في الأنظمة الحاسوبية المستهدفة أو البرمجة النصية للموقع لتشويه صفحات الويب الخاصة بالعدو واتلافها كما حصل في الهجوم الإلكتروني الروسي على استونيا عندما هاجم قراصنة روس موقع تابعة للحكومة الأستونية²¹. وتتنوع البرمجيات المستخدمة في عملية التسلل والاختراق ومن اهمها القنابل المنطقية والتي هي عبارة عن قطع من التعليمات البرمجية المدرجة عمداً في نظام برمجي يقوم بأطلاق وظيفة ضارة عند استيفاء شروط محددة ، والديدان الحاسوبية ونظرأً لكونها ادوات جديدة وتطور بسرعة وباستمرار والتي تحتاج الى فك شفرتها. وبهذا فإن جوهر العقيدة العسكرية في الحرب السيبرانية تقوم على اساس السعي لكسب الحروب من خلال ضرب القلب الاستراتيجي للهياكل الالكترونية للخصم. وذلك مع الاستمرار في تطوير استراتيجيات وقدرات للحماية عبر انظمه الدفاع السيبراني .

2 : استراتيجية وادارة التوظيف للحرب السيبرانية في اطار مفهوم القوة

هناك مجموعة من الاطر التقسيمية المرتبطة بالحرب السيبرانية منها ما يتعلق بمفهوم القوة ، حيث لعب الفضاء الإلكتروني دوراً اساسياً في تعظيمها والاستحواذ على عناصرها الاساسية في العلاقات الدولية، حيث اصبح التفوق في ذلك المجال عنصراً حيوياً في تنفيذ عمليات ذات فعالية على الارض والبحر والجو

²⁰ريشارد كلارك وروبرت كنيك، حرب الفضاء الإلكتروني: الخطر القادم على الامن القومي وسبل مواجهته ، ط1، الامارات العربية المتحدة ، ابوظبي ، مركز الامارات لدراسة السياسات ، ص 89.

²¹احمد عيسى الفلاوي، الهجمات السيبرانية: دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر ، ط1، لبنان، بيروت، منشورات زين الحقوقية، ص 68

والفضاء الخارجي من خلال اعتماد القدرة القتالية في الفضاء الخارجي على نظم التحكم والسيطرة التكنولوجية، وهذا الامر يستدعي بالضرورة تغير في مفهوم القوة حيث بات بالامكان تعريفها بأنها : (مجموعة الوسائل والطاقة والامكانيات المادية وغير المادية المنظورة وغير المنظورة التي بحوزة الدولة ويستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة وتؤثر في سلوك الوحدات السياسية الاخرى) ²². ومن هنا تبين لنا فيما تقدم ان مفهوم القوة في اطار الحرب السيبرانية له مدلولاته عن مفهومها التقليدي حيث أن هناك اطار تفسيري آخر مرتبطة في ان استخدام القوة بصورة غير مشروعة انما يتمثل بمعايير استخدام القوة المسلحة بالإضافة الى انتهاء الامن القومي لدولة اخرى، وفي ضوء انماط متعددة للحروب السيبرانية في كون جميع درجاتها يمكن ان تتشكل استخدام غير مشروع للقوة؟ فقد يتم استخدام الفضاء الالكتروني كساحة لصراع منخفض الشدة من خلال التأثير على النواحي الاقتصادية أو الثقافية أو الاجتماعية وهي لا تتطلب بالضرورة الى استخدام الفضاء الالكتروني كقوة مسلحة أو شن حرب الكترونية واسعة النطاق، حيث يمكن ان تتجسد تلك الصراعات بوسائل عده، منها الحرب النفسية والاختراقات المتعددة والتتجسس وسرقة المعلومات وشن حرب الافكار وغيرها،²³ وهناك نمط آخر من الحروب السيبرانية يتمثل في تحويل الصراع عبر الفضاء الالكتروني كساحة موازية أو مرفقة أو مرتبطة لحرب تقليدية دائرة على الارض ومنها ما تعرضت له سوريا في 6 / 12 / 2007 لهجمة سيرانية على دفاعاتها الجوية في أحدى المنشآت التي يشتبه في أنها منشأة نووية في مدينة دير الزور من قبل (اسرائيل) مما أدى الى تعطيل هذه الدفاعات لتمكن الطائرات الاسرائيلية من قصف هذا الموقع دون ان يتم الكشف عن هذا الهجوم. ونمط ثالث يعبر عنه في نشوء حروب في الفضاء الالكتروني بصورة منفردة واذا لم يشهد

العالم هكذا نوع من الحروب وفقاً لأثارها المدمرة من خلال اختراق العمليات العسكرية عالية التقنية أو استهداف الحياة المدنية أو البنية التحتية بالشكل الذي يمكن تصوره الا ان هناك نماذج لتلك الحروب تمثل على شكل رسائل تهديد مصحوبة بآثار محدودة جراء تلك الهجمات، ومنها ما تعرضت جمهورية استونيا عام 2007 من هجوم سيراني مستقل بذاته موجه من روسيا الاتحادية وذلك عن طريق اغراق المواقع الالكترونية بسيل من البيانات غير الالزمة بهدف شل واسقاط الحكومة الاستونية. ووفقاً لما تقدم فإن الهجمات السيرانية تثير اشكالية تتعلق بالقواعد المتعلقة بحق اللجوء الى الحرب من حيث طبيعة تلك

²² وفاء بوكابوس، مصدر سبق ذكره، ص 78.

²³ خضر مصباح اسماعيل، اساسيات امن المعلومات والحوسبة، ط1، الاردن، عمان، دار حامد للنشر والتوزيع، 2019، ص 60.

الهجمات في امكانية وصفها استخدام للقوة وبالتالي البحث في مشروعية أو عدم مشروعيتها وفي ضوء المبادئ والقواعد القانونية، لاسيما بعد انشاء الامم المتحدة والتي تتعلق بضرورة عدم استخدام القوة أو التهديد بها في ميدان العلاقات الدولية، ما خلا الاستثناءات المتعلقة بحق الدفاع الشرعي أو بموجب قرار صادر من مجلس الامن وفقاً للفصل السابع من الميثاق والامر يزداد صعوبة في ظل عدم الاتفاق حول مفهوم القوة المستخدمة والتي توصف كونها غير مشروعة لتشكل ما يعرف جريمة العدوان لاسيما وان ميدان الهجمات السيبرانية يمكن ان يأخذ اشكال عده منها الاقتصادية والثقافية عن ما يمكن وصفه بأنه هجوم مسلح.²⁴

3: دور الحرب السيبرانية في تطوير القوة للدول الكبرى (سيناريوهات مستقبلية)

ان العصر الراهن بما فيه من متغيرات جمة وتحولات شاملة اكدهت على ان الصراع الدولي المقبل سيدور حول المعرفة وستكون مسرحه وميدانه عقول البشر وما تحتويه من معلومات و المعارف بحيث ان قضايا التكنولوجيا ستحتل مكانة رئيسة في التنافس الدولي خصوصاً بين الولايات المتحدة وبقية الدول الكبرى.

ومن التنافس الى الصراع تحولت سريعاً معالم التهديدات المعلوماتية بين الدول الكبرى في ظل بيئة تكنولوجية عالمية ومعقدة مثلت الحروب السيبرانية فيها عناصر مؤثرة في السياسة والاقتصاد على الصعيد الدولي بعد انتقال جزء كبير من الصراعات بين القوى المؤثرة في العالم الى شبكة الانترنت والوسط الرقمي. ومن هنا يمكن ان نقسم السيناريوهات المستقبلية المتعلقة بموضوع الدراسة الى اثنين.

السيناريو الاول: تزايد دور الحروب السيبرانية في سياسات القوى الكبرى

تقول الدراسات المتخصصة في هذا المجال ان الحروب السيبرانية باتت تتسم بدرجة كبيرة من النمو السريع والصراع الشديد وتجاوزها لما هو اقتصادي الى ما هو سياسي بسبب المنافسة القائمة بين شركات البرمجيات الكبرى. وعلى الرغم من عدم امكانية معرفة مصدر الهجمات على الشبكة العنکبوتية بصورة قاطعة وما اذا كانت تدعمها حكومات ، الا امها باتت تشير جدلاً متبادلاً بين الدول لا سيما بعد بروز معايير العمليات العدائية عبر الفضاء الالكتروني في النصف الثاني من العقد الاول في الألفية الجديدة ، وكانت ابرز صور تلك الصراعات ما حدث بين روسيا واستونيا عام 2007، وخلال الحرب بين روسيا وجورجيا عام 2008، وبين كوريا الجنوبية والولايات المتحدة الامريكية عام 2009 التي شهدت هجمات الكترونية كورية على

²⁴ عمر حامد، المجال الخامس، الفضاء الالكتروني، تركيا، اسطنبول ، المعهد المصري للدراسات، 2019، ص 27-30.

شبكات البيت الابيض²⁵، وكذلك عام 2010 حين خرجت مزاعم بأن امريكا و(اسرائيل) هاجمتا البرنامج النووي الايراني بفيروس ستاكسنت ليتمثل نقلة مهمة في تقديم الاسلحة الالكترونية واستخدامها ليتطور الامر لاحقاً في الاعوام الاخيرة وتطاول هجمات القرصنة قطاعات الطاقة والنفط والغاز والصناعة والنقل وشركات الطيران المدني فضلاً عن المنشآت النووية والبني التحتية الكهربائية والبنوك. وفيما لا تزال البيانات قليلة حول حجم التنافس الدولي وما تمتلكه البلدان من قدرات وامكانات على صعيد الفضاء الالكتروني ، اورد احدث تقارير التوازن العسكري لعام 2022 اربعة مجالات كمؤشرات استرشادية يمكن من خلالها اظهار القدرات السيبرانية للدول الابرز في النظام الدولي والتي شملت مجال الاستراتيجية والعقيدة ومجال الوحدات الرئيسية للدفاع السيبراني ومجال الاقمار الصناعية والمجال المتعلقة بتدريبات الدفاع السيبراني. وعليه نجد ان الولايات المتحدة ستعمل جاهدة با ان تبقى الدولة الاكثر تفوقاً في مجال امتلاك القدرات السيبرانية والعسكرية اذ تعتمد على خمسة مكونات اساسية هي القيادة السيبرانية للجيش وقيادة الاسطول السيبراني والقيادة الالكترونية لقوات مشاة البحرية وخر السواحل اضافة الى وحدات الحرس الوطني، حيث يبلغ عدد الفرق السيبرانية في هذه القيادة نحو 133 فريقاً تضطلع بمهمات مختلفة في مجال حماية الامن السيبراني.²⁶

ومن هنا يتبنى هذا السينario وفي ظل الاصدارات العالمية المتواترة سيكون اعتماد القوى الكبرى في تفعيل المكانة الدولية وزيادة حدة التنافس الدولي بمحاولة تبني العقيدة السيبرانية لاسيما تفعيل الهجمات والحروب السيبرانية فالفضاء الالكتروني الشاسع.

السيناريو الثاني: تقليل توظيف الحروب السيبرانية في سياسات القوى الكبرى

على الرغم من حدة التنافس في هذا المجال لكن لم يحدث بعد اي من السيناريوهات الكارثية ولكن من المؤكد انها غير مستبعدة حيث ان مبدأ الردع ستكون استراتيجية غير فاعلة في الفضاء السيبراني (شبكة الانترنت) بسبب الصعوبات التي تحيط بتحديد مصدر الهجوم وبسبب العدد الكبير والمتنوع من الهجمات المتورطة في مثل هذه الامور سواء كانت عناصر تابعة لدول بعينها او مستقلة عن اية دولة . وتعد نظرية الردع التبادل احدى السياسات الحاكمة للعلاقات الدولية بين الدول الكبرى منذ انتهاء الحرب العالمية الثانية عام 1945 وتعني خلق توازن يقود الى منع وقوع حروب بين الدول انطلاقاً من اعتقاد ان اي طرف يستطيع

²⁵ عبد القادر فهمي، الحروب التقليدية وحروب الفضاء الالكتروني، دراسة مقارنة في المفاهيم وقواعد الاشتباك، مجلة العلوم القانونية والسياسية، جامعة بابل، المجلد 16، السنة الثامنة، العدد 6، كانون الاول، 2018، ص 89.

²⁶ نورة شلوش، مصدر سبق ذكره، ص 67.

ان يبدأ القتال، سيمكن الطرف الآخر من الرد في المقابل ، لا تعرف الدول الكبرى حتى الآن أية نظرية للردع الإلكتروني ولا توجد قواعد حاكمة للصراع السيبراني الأمر الذي يمثل جدالاً واسعاً في الاوساط العالمية من ضرورة تقييم المخاطر السيبرانية العالمية .²⁷

الخاتمة والاستنتاجات:

ان الثابت اليوم في العلاقات الدولية وتوازنات القوى ان الحرب الباردة والصراع السياسي والاقتصادي والتجاري بين الأقطاب في العالم تحول الى حرب سيبرانية صامتة وقد تكون مدمرة في الأعوام المقبلة ، من هنا بدأت دول العالم الواحدة تلو الأخرى تستكشف الخيارات المتاحة لتعزيز قدراتها الهجومية في الفضاء السيبراني وقد أعدت دول كثيرة عدتها للتحول الى مرحلة جديدة لأعادة حساباتها ومراجعة اولوياتها حتى تكون على الاستعداد الكامل للتعامل مع حروب المستقبل التي بالضرورة مبنية على مخرجات تكنولوجيا الجيل الخامس والذكاء الصناعي، واضحى من يسيطر ويحكم قبضته على الفضاء الرقمي هو من يفوز بالرهانات المستقبلية.

باتت السيبرانية مجالاً آخر لاستعراض القوى وممارسة النفوذ وتحقيق التفوق والتنافس الدولي ، فلم تعد ترسانات الاسلحة التقليدية واسلحة الدمار الشامل هي المعيار الأساس لقياس القوة بعد الثورة المعلوماتية مع ان امتلاك ناصية القوة السيبرانية يتطلب ايضاً من الباحثين ايجاد نماذج لقياس مؤشراتها وتصنيفها كما هو الحال للقوة الصلبة لأن بناء ادوات تقدير قدراتها الاساسية في فهم هذا الفضاء البالغ الاهمية لتحسين الاستراتيجية والسياسات الالكترونية لدول. مع التكير ان تدفق المعلومات التي تمارسها الدول المتقدمة اليوم تحمل في طياتها تهديدات ومخاطر جديدة على معظم دول عالم الجنوب ومنها العالم العربي ، الامر الذي يحتم عليه تحصين أمنه والحفاظ عليه وسط كم هائل من المتغيرات والتطورات المعلوماتية الكبيرة. حيث اصبح هناك ادراك متزايد بأن هذه الحروب لها القدرة على تحقيق آثار بالغة على الدول الأخرى ، كما يأتي هذا اللجوء لخيار الحرب السيبرانية اغتناماً واستفادة من الغياب للأنظمة التشريعية الازمة لردع وتقيد هذا النوع من الحروب أضافه الى ما توفره الطبيعة والخصائص التقنية من امكانية و المجال للتملص من المسؤولية والمحاسبة. كما تشير الى ان التوقعات العسكرية المستقبلية تتجاوز ما سبق الرجة اعلى من الحرب السيبرانية تتمثل في تجهيز واعداد روبوتات آلية فتاكة تقوم بالهجوم المباشر على منشآت العدو.

²⁷سامر مؤيد عبد اللطيف، مصدر سبق ذكره، ص99

وأيًّا كان الشكل أو المستوى فإن حروب الفضاء الإلكتروني أو السيبراني قد أصبحت واقعًا ليس بأمكان أي دولة التغاضي عنه أو إغفاله حيث لا تكاد دولة اليوم تسلم من التعرض لأحدى أشكالها بالخصوص من قبل الدول الكبرى وسياساتها في الهيمنة والتنافس على موارد وقدرات الدول الأخرى بما في ذلك حرب المعلومات والشائعات أو التجسس والاختراقات وكل ذلك يستدعي المبادرة الأخذ بالتدابير الوقائية بداية من تطوير منظومات الدفاع الإلكترونية والامن السيبراني وحتى المشاركة والدفع باتجاه تطوير منظومات تشريعية دولية تسهم في تحديد وتقييد هذه الحروب بشكل حاسم وفعال. وعلى ضوء مما سبق يمكن استنتاج ما يأتي:

- 1- اسست القوة السيبرانية رغبة للفاعل من الدول الكبرى وغير الدول بالدخول إلى سباق محموم للتنافس والتقوّق السيبراني كما في العصر النووي سابقاً.
- 2- اصّبحت الحروب السيبرانية دافعاً للدول الكبرى في زيادة قوتها وفعاليتها في النظام الدولي
- 3- باتت الحرب السيبرانية حقيقة تغلب على قوة الحرب التقليدية وداعمة للعمليات العسكرية والحربية والأنشطة السياسية والاقتصادية والدبلوماسية حتى باتت أنها تستطيع أن تصل إلى أهدافها المرجوة بأقل التكاليف وبزمناً أقل.
- 4- اذا كانت القوة احدى ثوابت الدول فالسيبرانية وفرت لها مجالاً حركيًّا تتجاوز فيها الحدود الجغرافية للوصول لأهداف قد يصعب وصولها عن طريق القوة التقليدية.