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 العكّابي[1*]

الملخص:

يدور البحث حول الحروب الافتراضية السيبرانية التي بدأ الاداء 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 لتوظف فيها الحروب السيبرانية. ولعل الاستخدام المتزايد للفضاء السيبراني للأغراض العسكرية أحد اهم 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 عدها وسيلة ظهرت في هذا العصر، وان التركيز عليها تصاعد بفعل ما احدثه التطور في تكنولوجيا الاتصالات والتكنولوجيا العسكرية والرقمية من تأثيرات وتغييرات مباشرة على الساحة الدولية والتي اصبحت سلاحاً يمكن ان يستخدم للحفاظ على الامن القومي أو لدمار الدول وتفتيتها حيث جلب التطور التكنولوجي والمعلوماتي أعادة صياغة مفهوم القوة وظهور الفاعلين الجدد وبدورها بدأ تطور الاسلحة السيبرانية وانتشار شبكة الاقمار الصناعية ودخول الدول الكبرى مضمار الحروب السيبرانية مثل الولايات المتحدة الامريكية والصين وروسيا والهند والباكستان وكوريا الشمالية وايران

اهمية البحث:

تناولت الدراسة مسألة الحروب السيبرانية وما للفضاء 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 تغييرات على مفهوم القوة للدولة من حيث دخولها الى المجال السيبراني والذي اصبح مرتبط بالأفراد والدول واصبح مفهوم الحرب السيبرانية بمثابة تهديد قومي وفعلي للدول تستخدمه الدول الكبرى لتحقيق اهدافها.

اشكالية البحث:

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

ماهي 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 وظِفت من أجل استخدام القوة في السياسة الدولية والشؤون العالمية وتوزيعها بين القوى الكبرى. لذا فأن 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 (الاستنباطي) من اجل تحليل عوامل القوة والمراحل التطورية التي مرت بها حيث أدت الى بروز نوع جديد من الحروب لمعرفة مدى امكانية توظيفها على اداء الدول الكبرى .

أولاً: الفضاء السيبراني وتطور مفهوم القوة

احدث 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 يشكل عنصرا للأمن الدول الحيوي في تنفيذ عمليات ذات تأثير على الارض والبحر والجو والفضاء.

1: العلاقة الجدلية بين السيبرانية ومفهوم القوة

اضحى النظام العالمي اليوم يواجه احد أكبر التحديات الخطرة 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 وعلاقاتها 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 شل 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 يعنى 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 المتسارع والمستمر. ومن المعلوم ان الهجمات الالكترونية مثل القرصنة كأحد الاشكال الشائعة لجرائم الانترنت والجرائم السيبرانية التقليدية والتهديدات السيبرانية للأيدولوجيا 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 الالحلي 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 الجامعة، مجلة كلية بغداد للعلوم الاقتصادية ، الجامعة، العدد الخاص بمؤتمر الكلية، 2013، ص89.

اطراف الصراع قادراً على ايقاع خسائر فادحة بالطرف الأخر 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 أو حتى مسحها من الوجود. ان الارقام المتعلقة بالأمن السيبراني مقلقة جداً فمثلاً حجم الخسائر التي يتكبدها العالم تُقدر بمليارات الدولارات سنوياً 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 بأزدياد ايضاً حيث نرى الكثير من الخطط التي اعلنت عنها دول متقدمة وشرعت بزيادة نشاطها ووضع بنود في موازنتها العامة بملايين الدولارات بالأخص في الولايات المتحدة الامريكية والصن وروسيا وبعض الدول الاوربية تحديداً لمجابهة التحديات والمخاطر السيبرانية وتكثيف جهودها لحماية امنها الالكتروني وتحصين بنيتها التحتية الحيوية ، وتطوير سياسات لرفع الوعي حول قضايا الامن السيبراني وتطوير المخططات الوطنية لتحفيز وتعظيم الوسط الرقمي لها، بهدف تقليص مخاطر وآثار الهجمات السيبرانية التي يتعرض لها العالم بأستمرار. لهذا اولت القوى الكبرى اهتماماً واضحاً في توظيف الفضاء الالكتروني لتعزيز قوتها، من خلال ايجاد ميزة أو تفوق أو تأثير في بيئة الوسط الرقمي، وبالتالي ظهر ما يسمى ب" الاستراتيجية السيبرانية" للدول[6]، والتي تشير الى القدرة على التنمية وتوظيف القدرات للتشغيل في الفضاء الالكتروني وذلك بالاندماج والتنسيق مع المجالات العملياتية الاخرى لتحقيق أو 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 وانما 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، 10/11/2021 www.aljazeera.net

[5] فاتح حاريك، الفضاء السيبراني والتحول في شكل الحروب دراسة حالة روسيا، june 2021 www.reasearch gate.net

[6] وليام ستولينج، اساسيات امن الشبكات: تطبيقات وعايير، ترجمة: السيد محمد الالفي ورضوان السعيد عبدالعال،ط1، الرياض، العبيكان للنشر، ص78.

الى الثورة التكنولوجية المعلوماتية. فنحن على اعتاب الثورة الصناعية الخامسة القائمة على الذكاء الصناعي لم يعد بإمكان أي دولة ان تقيس مكانتها كقوة اقليمية أو دولية بالأعتماد فقط على عوامل القوة التقليدية (الصلبة)[7]، اذ باتت تحتم المعطيات امتلاك الدول للقوة السيبرانية التي ازاحت العديد من عناصر القوة التقليدية من مكانها حيث لم يعد امتلاك الدول للأموال والثروات والقدرات العسكرية والجغرافيا الشاسعة كافياً لبلورة دورها كقوة فاعلة ومؤثرة وذات نفوذ في السياسات العالمية. اليوم تسعى الكثير من الدول لأمتلاك القدرات السيبرانية وباتت هذه الاخيرة تأخذ شكلاً جديداً في طبيعتها ووسائلها وادواتها ونرى اليوم ان الصراع الدولي يتجه بالأساس نحو السباق والتنافس في ساحة الانجازات التكنولوجية التي غيرت من شكل الحروب وادواتها واثرت على الفاعلين بها وساهمت في إعادة التفكير في حركية وديناميكية الصراع.

2_ تطور مفهوم القوة

تتعدد الصور التي تتخذها القوة وتتغير وفقاً لطبيعة وشكل النظام القائم، فالقوة هي حجر الاساس لأي تنظيم سياسي حيث تُعرف بأنها القدرة على التأثير في الأخرين للحصول منهم على نتائج محددة يسعى الطرف الذي يقوم بعملية التأثير للحصول عليها. وكذلك هي علاقة خاصة بين طرفين يستلزم ان يكون احد الطرفين فيها على قدر اكبر من الامكانات ما يتيح له بعض التفوق في السلطة والسلطان. فالقوة مفهوم حركي ديناميكي غير ثابت يتكون من عناصر متغيرة مادية او غير مادية مترابطة مع بعضها البعض ، كما ان القوة شيْ نسبي تقيس قوة الدولة بالمقارنة بقوة الدول الاخرى واحياناً 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 كالتالي :[8]

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 الى قوة فعالة.
3. تتصف القوة بندرتها لذلك تحرص الدول على ما تمتلكه وتحاول عدم تشتيت جهودها.

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

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

4. القوة بطبيعتها شيء نسبي تُقاس قوتها بالمقارنة بقوة الدول الاخرى.
5. تندرج ممارسة القوة بين التأثير بالطرق الدبلوماسية من جهة وبين اسلوب الاجبار والقسر من جهة اخرى، 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 تتداخل معها اشكال جديدة في محاور التنافس 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 يتوافق مع اتجاهاتها ، حيث

---

[9] نقلاً عن الفن توفلر، تحول السلطة ، الجزء الاول، ترجمة، لبنى الريدي، الهيئة المصرية العامة للكتاب، ط1، الالف كتاب الثاني، المجلد 2 ، ص87.

[10] عباس بدران ، الحرب الالكترونية: الاشتباك في عالم المعلومات، ط1، بنان، بيروت، مركز دراسات الحكومة الالكترونية، ص45.

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 اعادة النظر فيه والإفصاح عن محتوى جديد في مفهوم القوة ومستقبلها في إدارة الصراع للقرن الحادي والعشرين، ان اتجاهات هذا التغيير الذي احدثته 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 فأن 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 التكاتف والتعاون الذي يجمع عناصر قوى مختلفة سيؤدي إلى حصيلة تراكم القوة التي تتفوق عن الجمع الفردي لعوامل القوة. وبالنتيجة لم يعُد 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 إختراق الحدود بخوض معارك برية، هذه العوامل بالإجماع قد تعطي قوة للعامل العسكري تدفعه إلى التطور والتقدم. لقد سعى متغير التطور التكنولوجي إلى فرز قواعد وسلوكيات بنمط جديد لم تعد الدول قادرة على ضبط آليات اقتصادها بمنأى عن هياكل وآليات اقتصاديات الدول الأخرى، لقد احدثت التغييرات الاقتصادية في ظل حقبة مجئ

[11] وليد عبد الحي، الدراسات المستقبلية في العلاقات الدولية، عيون المقالات ، مراكش، ط2، 1993، ص92 . انظر كذلك: محمد حسن آل ياسين، اندماج التكنولوجيا ومهام البحث والتطوير الجديد، النشرة الفصلية الصادرة عن المنظمة العربية للتنمية الادارية ، العدد29، 1999، ص9.

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

3: الحرب السيبرانية (المفهوم والدوافع)

سوف ننطلق في تحديد مفهوم السيبرانية والتي هي في اللغة مصطلح مشتق من الكلمة اليونانية (kybernetes) بمعنى القيادة والتحكم عن بُعد. وهي عملية استخدام تقنيات التواصل الاجتماعي على الانترنت لأنشاء وتشغيل وادارة النشاط من اي نوع. انها 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 المحوسبة وشبكات الاتصال والمعلومات وانظمة التحكم عن بُعد ، وتختلف استخدامات السايبر من دولة الى اخرى وفقاً لأولويات الدول : فهناك السايبر المدني والامني والاستخباراتي، ويتكون السايبر من ثلاث مكونات:

الاجهزة والبرمجيات الرقمية وطاقم المطورين والمبرمجين[13]

1-مفهوم الحرب السيبرانية

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

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

[13]نورة شلوش ، القرصنة الالكترونية في الفضاء السيبراني" التهديد المتصاعد من الدول، مجلة مركز بابل للدراسات الإنسانية، مجلد8، العدد2، جامعة بابل، 2018، ص87.

التي تتخذها الدولة من اجل الهجوم على نظم المعلومات للعدو وبهدف التأثير والأضرار فيها والدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة". واذا شكلت الهجمات السيبرانية وتبعأ للظروف نزاعاً مسلحاً فنكون امام مصطلح الحرب السيبرانية أو ما يعُرف بالهجوم السيبراني والتي تكون اوسع نطاقاً من الحرب السيبرانية وقد تحدث خارج اطار الحروب وقد تكون سبباً لبدء الحرب[14]. ان الهجمات السيبرانية يمكن ان تكون جزءاً من حرب سيبرانية متى ما استخدمت في اطار نزاع مسلح واستهدفت تحقيق اهداف عسكرية فبالتالي هي اجراءات تتخذها الاطراف في نزاع مسلح لكسب الميزة على خصومهم في فضاء السايبر بأستخدام مختلف الادوات التكنولوجية والاشخاص التقنيين ويحصل على المزايا من جراء تلك الهجمات من خلال اتلاف أو تدمير او تعطيل أو اغتصاب انظمة الحاسوب للعدو أو من خلال الحصول على معلومات التي يرغب العدو في ان تبقى سرية أو ما يعُرف بالتجسس السيبراني أو الاستغلال لشبكات الحاسوب متى ما كانت في أطار نزاع مسلح يصل الى مستوى الحرب[15].وتعرف أيضاً بأنها الحروب التي تستهدف تعطيل أو تدمير نظم المعلومات والاتصالات في الدولة العدو، وهي تشن اساساً داخل بيئة المعلومات بحيث تستهدف تعطيل كفاءة السيطرة والقدرة على التحكم في منظومة اجهزة أو شبكات الحاسوب وما تتضمنه من بيانات ومعلومات للفاعلين 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 للأنظمة 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 اهدافاً مدنية وقطاعات خدمية وانتاجية ، كذلك عززت الحروب السيبرانية من مستويات وفرص الحرب اللامتماثلة 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، ص57.

[15] عادل عبد الرزاق ، الارهاب الالكتروني: القوة في العلاقات الدولية : نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والاستراتيجية بالأهرام، القاهرة، القاهرة، 2009، ص87.

ضد الدول ذات القوة العسكرية والاقتصادية الاكبر أضافة الى انها 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 انها وسيلة غير مكلفة أذا ما قورنت بوسائل الهجوم العسكرية التقليدية فهي لا تحتاج الى معدات وجيوش مجهزة كما ان احتمالية وقوع الضحايا والخسائر البشرية في صفوف القوة المهاجمة تكون منعدمة . كما انها تلحق ضرراً كبيراً بالخصم هذا بالإضافة الى انها تتسم بصعوبة تحديد مصدر الهجوم وبالتالي تجنب الدول الأدانة والتبعات القانونية والتبعات العسكرية للهجوم بما في ذلك تجنبها اي ردود عسكرية مباشرة على الهجمات اي انها تتسم باخلاء المسؤولية وذلك بالنظر الى صعوبة تحديد الجهة والمكان الذي صدر منه الهجوم ، وكذلك امكانية التلاعب والتمويه العالية فيما يتعلق بمصدر ومكان توجيه شن الهجوم الالكتروني، أضافة الى استخدام سلسلة من الوكلاء في شن الهجوم بما يبدد اي احتمالية تتبع مباشر للدولة صاحبة القرار في شن الهجوم[17] . كما ان هذه الحروب مقترنة بالضرورة بنية الحاق 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 حيثيات الهجوم مثل حالات اختراق حسابات والوصول الى معلومات ، ولكنها تبقى مفتقدة عنصر النية بالحاق الضرر نوعاً من التصعيد وسبباً للضغط عليه بغية الوصول الى نوع من الأذعان وتقديم التنازلات من قبله وهو ما يكون متحققاً في حالة الهجمات الإلكترونية والتي تأتي ضمن سياق ما يمكن تسميته بالحرب الالكترونية.

وبالإمكان اعتبار حروب الفضاء الإلكتروني بمثابة الانعكاس والمخرجات للثورة الرقمية والإلكترونية في الميدان العسكري، وهي تقوم على اساس شن الهجمات على هياكل تكنولوجيا المعلومات الحيوية للخصم والتي تكون مشغلة لمصالحه المدنية وقدراته العسكرية بحيث يكون الحاق الضرر بها موازاً ومعادل للقصف العسكري المباشر بواسطة الاسلحة التقليدية وغير التقليدية.

---

[16] سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي: رؤية مستقبلية ، مجلة رسالة الحقوق ، العدد 2، السنة السابعة، مركز الدراسات القانونية والدستورية، جامعة كربلاء، 2015، ص90-95.

[17] ليتيم فتيحة وليتيم نادية، الامن المعلوماتي للحكومة الالكترونية وارهاب القرصنة، مجلة المفكر، العدد 12، كلية الحقوق والعلوم السياسية، جامعة محمد خضير، الجزائر، 2015، ص78.

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 ادوات الحرب التقليدية ، فضلاً عن ما يمكن ان تحققه من نتائج ملموسة في أطار الصراعات والنزاعات ، بالإضافة الى اختلاف عقيدتها 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 تناظرية[18]. 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 المتطورة لتفرض تهديداً خطيراً وحقيقياً على الاطراف الأخرى وانما يكفي تطوير البرمجيات الأزمة وامتلاك الاجهزة الحاسوبية[19]. 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 اطار منظومة الحرب التقليدية أما في الحرب الالكترونية فهي غائبة وذلك عائد الى خصائص عدة اذ ان هناك معضلة في تحديد الدولة والجهة التي قامت بالهجوم فبأمكان القوة المهاجمة شن هجوم على دولة لصالح دولة انطلاقاً من دولة ثالثة عبر استخدام خوادم تكون موجودة هناك بل ومن المستحيل في كثير من الاحيان تحديد مصدر الهجمات الالكترونية، ويقترن بهذه الخاصية خاصية اخرى تميز الحروب 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

[18] نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني" التهديد المتصاعد من الدول"، مجلة مركز بابل للدراسات الانسانية، مجلد8، العدد2، جامعة بابل، 2018، ص57.

[19] وفاء بوكابوس، تحول القوة في العلاقات الدولية: دراسة في انتقال القوة من التقليدية الى الحديثة، ط1، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، المانيا، 2019، ص69.

ان الحدود تتداخل مع بعضها حيث ان كل الدول صغيرة وكبيرة تشترك في نفس الشبكات تكون في كثير من الأحيان موجودة في بلدان اخرى غير البلدان المستخدمة لها والمشغلة لها. في الحروب السيبرانية تشتمل على عمليات تعتبر مساندة للعمل العسكري من التجسس على الاشارة أو التشويش على نظام الموقع العالمي واعاقته لدى العدو وعرقلة عمليات توجيه الأسلحة العسكرية المعادية[20].أما بخصوص طبيعة الأسلحة والأدوات المستخدمة وانواعها في هذا النوع من الحروب ، فأن القوة الألكترونية تعتمد بصفة اساسية على الاجهزة والبرامج ، الاجهزة تشتمل على انظمة الحاسوب مثل وحدة المعالجة المركزية أو محرك الاقراص الضوئية أو لوحة المفاتيح وكذلك الاقمار الصناعية. اما البرامج فهي الصياغات البرمجية المستخدمة لتوجيه عمليات الحاسوب والتي يستخدم فيها البرامج الضارة والفيروسات مثل لغة الاستعلام الهيكلية وهي عباة عن مجموعة من التعليمات المستخدمة للتفاعل مع قواعد البيانات ، وعمليات الحقن الإلكتروني عبر أدخال برمجيات ضارة في الأنظمة الحاسوبية المستهدفة أو البرمجة النصية للمواقع لتشويه صفحات الويب الخاصة بالعدو واتلافها كما حصل في الهجوم الالكتروني الروسي على استونيا عندما هاجم قراصنة روس مواقع تابعة للحكومة الأستونية[21]. 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 ونظراً لكونها ادوات جديدة وتتطور بسرعة وباستمرار والتي تحتاج الى فك شفرتها. وبهذا فأن 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 انظمة الدفاع السيبراني .

2 : استراتيجية وادارة التوظيف للحرب السيبرانية في اطار مفهوم القوة

هناك مجموعة من الاطر التفسيرية المرتبطة بالحرب السيبرانية منها ما يتعلق بمفهوم القوة ، حيث لعب الفضاء الالكتروني 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

[20] ريتشارد كلارك وروبرت كنيك، حرب الفضاء الالكتروني: الخطر القادم على الامن القومي وسبل مواجهته ، ط1، الامارات العربية المتحدة ، ابوظبي، مركز الامارات لدراسة السياسات، ص89.

[21] احمد عيسى الفتلاوي، الهجمات السيبرانية: دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط1، لبنان، بيروت، منشورات زين الحقوقية، ص68

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 والطاقات 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 مرتبط في ان استخدام القوة بصورة غير مشروعة انما يتمثل بمعيار استخدام القوة المسلحة بالإضافة الى انتهاك الامن القومي لدولة اخرى، وفي ضوء انماط متعددة للحروب السيبرانية في كون جميع درجاتها يمكن ان تشكل 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 تتطور بالضرورة الى استخدام الفضاء الالكتروني كقوة مسلحة أو شن حرب الكترونية واسعة النطاق، حيث يمكن ان تتجسد تلك الصراعات بوسائل عدة، منها الحرب النفسية والاختراقات المتعددة والتجسس وسرقة المعلومات وشن حرب الافكار وغيرها،[23] وهناك نمط آخر من الحروب السيبرانية يتمثل في تحويل الصراع عبر الفضاء الالكتروني كساحة موازية أو مرافقة أو مرتبطة لحرب تقليدية دائرة على الارض ومنها ما تعرضت له سوريا في 6/ 12/ 2007 لهجمة سيبرانية على دفاعاتها الجوية في أحدى المنشأت التي يشتبه في أنها منشأة نووية في مدينة دير الزور من قبل (اسرائيل) مما أدى الى تعطيل هذه الدفاعات لتمكين الطائرات الاسرائيلية من قصف هذا الموقع دون ان يتم الكشف عن هذا الهجوم. ونمط ثالث يُعبر 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 الأ ان هناك نماذج لتلك الحروب تتمثل على شكل رسائل تهديد مصحوبة بآثار محدودة جراء تلك الهجمات، ومنها ما تعرضت جمهورية استونيا عام 2007 من هجوم سيبراني مستقل بذاته موجه من روسيا الاتحادية وذلك عن طريق اغراق المواقع الالكترونية بسيل من البيانات غير اللازمة بهدف شل واسقاط الحكومة الاستونية. ووفقاً لما تقدم فأن الهجمات السيبرانية تثير اشكالية تتعلق بالقواعد المتعلقة بحق اللجوء الى الحرب من حيث طبيعة تلك

[22] وفاء بوكابوس، مصدر سبق ذكره، ص78.

[23] خضر مصباح اسماعيل، اساسيات امن المعلومات والحاسوب، ط1، الاردن، عمّان، دار حامد للنشر والتوزيع، 2019، ص60.

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 عدة 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 اكدت على ان الصراع الدولي المقبل سيدور حول المعرفة وستكون مسرحه وميدانه عقول البشر وما تحتويه من معلومات ومعارف 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 العنكبوتية بصورة قاطعة وما اذا كانت تدعمها حكومات ، الأ امها باتت تثير جدلاً متبادلاً بين الدول لا سيما بعد بروز معالم 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، ص27-30.

شبكات البيت الابيض[25]، وكذلك عام 2010 حين خرجت مزاعم بأن امريكا و(اسرائيل) هاجمتا البرنامج النووي الايراني بفيروس ستاكسنت ليمثل نقلة مهمة في تقدم الاسلحة الالكترونية واستخدامها ليتطور الامر لأحقاً في الاعوام الاخيرة وتطاول هجمات القراصنة قطاعات الطاقة والنفط والغاز والصناعة والنقل وشركات الطيران المدني فضلاً عن المنشآت النووية والبنى 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 الرئيسة للدفاع السيبراني ومجال الاقمار الصناعية والمجال المتعلق بتدريبات الدفاع السيبراني. وعليه نجد ان الولايات المتحدة ستعمل جاهدة بان 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 وخفر 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 السيناريو وفي ظل الاحداث 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: تقليص 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 السبراني (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 أو 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، العدد6، كانون الاول، 2018، ص89.

[26]نورة شلوش، مصدر سبق ذكره، ص67.

ان يبدأ القتال، سيتمكن الطرف الأخر من الرد في المقابل ، لا تعرف الدول الكبرى حتى الآن أية نظرية للردع الالكتروني 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 مجالاُ آخر لأستعراض 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 السيرانية يتطلب ايضاً من الباحثين ايجاد نماذج لقياس مؤشراتها وتصنيفها كما هو الحال للقوة الصلبة لأن بناء ادوات تقييس قدراتها الاساسية في فهم هذا الفضاء البالغ الاهمية لتحسين الاستراتيجية والسياسات الالكترونية لدول. مع التذكير 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 اللازمة لردع وتقييد هذا النوع من الحروب أضافة الى ما توفره الطبيعة والخصائص التقنية من امكانية ومجال 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.

[27] سامر مؤيد عبد اللطيف، مصدر سبق ذكره، ص99

وايأ كان الشكل أو المستوى فأن حروب الفضاء الالكتروني او السيبراني قد اصبحت واقعاً ليس بأمكان اي دولة التغاضي عنه أو اغفاله حيث لا تكاد دولة اليوم تسلم من التعرض لأحدى اشكالها بالاخص من قبل الدول الكبرى وسياساتها في الهيمنة والتنافس على موارد وقدرات الدول الاخرى بما في ذلك حرب المعلومات والشائعات أو التجسس والاختراقات وكل ذلك يستدعي المبادرة الاخذ بالتدابير الوقائية بداية من تطوير منظومات الدفاع الالكترونية 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 للفواعل من الدول الكبرى وغير الدول بالدخول الى سباق محموم للتنافس والتفوق السيبراني كما في العصر النووي سابقاً.

2-اصبحت الحروب السيبرانية دافعاً للدول الكبرى في زيادة قوتها وفاعليتها في النظام الدولي

3-باتت الحرب السيبرانية حقيقة تغلب على قوة الحرب التقليدية وداعمة للعمليات العسكرية والحربية والانشطة السياسية والاقتصادية والدبلوماسية حتى باتت انها تستطيع ان تصل الى اهدافها المرجوة بأقل التكاليف وبزمناً اقل.

4- اذا كانت القوة احدى ثوابت الدول فالسيبرانية وفرت لها مجالاً حركياً تتجاوز فيها الحدود الجغرافية للوصول لأهداف قد يصعب وصولها عن طريق القوة التقليدية.