The North African Journal of Scientific Publishing (NAJSP)
مجلة شمال إفريقيا للنشر العلمي (NAJSP)
EISSN: 2959-4820
Volume 1, Issue 4, October-December 2023, Page No: 154-168
Website: https://najsp.com/index.php/home/index
SJIFactor 2023: 3.733 معامل التأثير العربي (AIF) 2023: 0.63 ISI 2023: 0.383

الهجمات السيبرانية: الحرب الرقمية التي تجاوزت الحدود الجغرافية

د. ياسين محمد أحمد بونه *
محاضر، قسم الجغرافيا، كلية التربية، جامعة بني وليد، بني وليد، ليبيا

Cyber Attacks: Digital Warfare That Transcends Geographical Borders

Dr. Yasin Muhamad Ahmed Bona *
Lecturer، Department of Geography، College of Education، Bani Waleed University، Bani Walid، Libya

*Corresponding author yasin.bona@gmail.com *المؤلف المراسل
تاريخ النشر: 2023-11-07 تاريخ القبول: 2023-11-03 تاريخ الاستلام: 2023-09-21

الملخص

تهدف الدراسة إلى تبيان عالمية الفضاء السيبراني وتأثير ذلك على مفهوم الأمن والصراع في ظل تنامي الهجمات والاعتداءات الالكترونية وانعكاساتها على موازين القوة في العلاقات الدولية، مع التركيز على علاقة الأمن السيبراني بالأمن القومي، كما تهدف إلى تسليط الضوء على أهم المخاطر والتحديات المستقبلية، فالحروب السيبرانية التي تدور رحاها اليوم عبر شبكة الويب العالمية شكلت هاجسا استراتيجياً ومصدر قلق للدول، ما يضع مفهوم السيادة الوطنية على المحك، وقد قسمت الدراسة إلى ثلاثة محاور تناول الأول منها فضاء القوة السيبرانية ومفهوم وأبعاد الأمن السيبراني، اما المحور الثاني تناول موضع عسكرة الفضاء السيبري مع توضيح أهم الخاطر السيبرانية، وتناول المحور الثالث المجال السيبراني وتأكل مفهوم السيادة الوطنية والأمن القومي وسبل درء المخاطر، وختمت الدراسة بمجموعة من الاستنتاجات.

الكلمات المفتاحية: القوة الذكية، الأمن السيبراني، قراصنة، الرقمنة، الروبوتات القاتلة.

Abstract:

The study aims to show the universality of cyberspace and its impact on the concept of security and conflict in light of the growing cyber attacks and attacks and their repercussions on the balance of power in international relations, with a focus on the relationship of cybersecurity with national security, and also aims to highlight the most important risks and future challenges, as the cyber wars that are raging today through the World Wide Web have formed a strategic concern and a source of concern for countries, What puts the concept of national sovereignty to the test, the study was divided into three axes, the first of which dealt with the cyber power space and the concept and dimensions of cybersecurity, while the second axis dealt with the position of militarization of cyberspace with clarification of the most important cyber risks, and the third axis dealt with the cyber field and eroded the concept of national sovereignty, national security and ways to ward off risks, and the study concluded with a set of conclusions.

Keywords: Smart Power, Cyber Security, Hackers, Digitization, Killer Robots.

المقدمة:

مع تزايد اعتماد البشرية على خدمات الاتصالات والتقنية ومع سرعة التحول الرقمي الذي تشهده معظم القطاعات والمؤسسات والحكومات، ما جعل العالم اليوم يرزح تحت واقع الثورة المعرفية المرتكزة على تدفق المعلومات وتشابك الاتصالات، الأمر الذي أسس لعلاقة بين الواقع الافتراضي والواقع الحركي للنظام الدولي حيث أصبح الفضاء السيبراني مجتمعا مشتركا عالمياً لا يخضع لسيطرة وسيادة دولة واحدة ولا حتى مجموعة دول، فالنطاق العالمي لشبكة الانترنت جعل من إمكانية نقل وتبادل المعلومات والبيانات خارج مجال سيطرة الدول أمرا متصاعداً.

إن سهولة استخدام الفضاء السيبراني وتنوع فواعله كان سببا مباشراً في تنامي وانتشار القوة السيبرانية، فصعوبة تحديد مصدر الهجوم جعلت منه الأسلوب الأمثل لتنفيذ الهجمات السيبرانية، الأمر الذي دفع بالدول خاصةً منها الدول الكبرى إعادة النظر في مختلف المفاهيم والإجراءات المرتبطة بتحقيق الأمن السيبراني، والذي أصبح تحقيقه أمراً في غاية الصعوبة، على اعتبار أن عناصر القوة أصبحت أكثر انتشارا وتمدداً.

وتأسيساً على ما سبق ستحاول الدراسة الإجابة على **التساؤلات** التالية:

- إلى أي مدى أصبح الفضاء السيبراني مجالا جديداً للحرب وبعدا إضافياً مكملا للحرب التقليدية؟
- وهل تسير السيادة الوطنية نحو التآكل التدريجي في ظل تسارع التطور التكنولوجي والرقمنة؟

وللإجابة على التساؤلات السالفة سنعتمد على **الفرضيات** الأولية التالية:

- تمثل الحرب السيبرانية شكلا جديداً من أنظمة تكنولوجيا المعلومات حرب تدار عن بعد لا تعتمد على التصادم المباشر.
- أدى ظهور شبكة المعلومات الدولية إلى تدمير الرابط بين الموقع الجغرافي والحدود المادية للفضاء السيبري فمبدأ السيادة التامة والمطلقة للدولة على إقليمها صار من الماضي.

أهمية الدراسة:

تكمن أهمية الدراسة كونها تسلط الضوء على موضوع حديث نسبياً وهي الحرب السيبرانية، حيث أصبحت العوالم الافتراضية عالما موازياً لحياتنا الواقعية فالهجمات السيبرانية فرضت نفسها على ساحة العلاقات الدولية، وباتت تهدد الأمن القومي للدول نظراً لتأثيرها البالغ والخطير.

أهداف الدراسة:

تهدف الدراسة إلى تبيان عالمية الفضاء السيبراني وتأثير ذلك على مفهوم الأمن والصراع في ظل تنامي الهجمات والاعتداءات الالكترونية وانعكاساتها على موازين القوة في العلاقات الدولية، مع التركيز على علاقة الأمن السيبراني بالأمن القومي، كما تهدف إلى تسليط الضوء على أهم المخاطر والتحديات المستقبلية.

تقسيمات الدراسة:

للإجابة على الإشكالية المطروحة تم تقسيم الدراسة إلى ثلاثة محاور على النحو التالي:

المحور الأول: العصر السيبري وخلق بيئة جديدة.

المحور الثاني: الفضاء السيبراني مجالا للحرب والصراع.

المحور الثالث: الفضاء السيبراني واندثار الحدود الجغرافية للدول.

(1)العصر السيبري وخلق بيئة جديدة:

اوجدت الابتكارات التكنومعرفية المتسارعة في التطور بيئة جديدة يشغلها الانترنت عبر فضاءات افتراضية متشابكة إلكترونياً، أضحت تهدد سيادة ومصالح الدول كساحة حرب عالمية عابرة للحدود وعبر أدوات قوة الفضاء السيبراني، والذي أصبح يمثل البعد الخامس في المعركة لأنه يتخطى الأبعاد التقليدية (البر والبحر والجو والفضاء).

(1-1) فضاء القوة السيبرانية:

منذ بداية القرن الواحد والعشرون طغى عصر المعرفة الرقمية وانتشار شبكة المعلومات الدولية، حيث انتشرت التكنولوجيا الالكترونية في جميع المجالات واصبحت ركيزة محورية يستحيل تحقيق التقدم من دونها، لقد كان للتوسع في استخدام الإنترنت أكثر التطورات التقنية إثارة للاهتمام من قبل الباحثين والقادة السياسيين على اعتبار أنه خلق بيئة إلكترونية غير ملموسة معقدة التفاعل ذات عالم اقتراضي تتشابك مع عالمنا المادي وهو ما يعرف بالفضاء السيبراني، ليشكل بذلك حضوره كمجال يقابل المجال المادي التقليدي، ويتميز عنه بخصائص عديدة ومتنوعة ويطرح تحديات بالنسبة لمفهوم السيادة الوطنية، وإعادة تصور وتشكل سيادة الدولة في عصر الرقمنة (علاء الدين، عمارة،2021، ص163).

ويتكون الفضاء السيبراني من المكون الأول المادي الذي يتمثل في الاسلاك والمحولات والبنية التحتية المعلوماتية: كالكابلات "Hardware"، والمكون الثاني يتمثل في المحتوى المعنوي والذي يعكس شكل المعلومات في الفضاء السيبري "Software"، أما المكون الثالث فيتمثل في عملية التوصيل بين المعلومات والبشر وحركة التفاعل ما بين البرمجيات والمعدات، وارتباط ذلك بتصورات وقيم وسلوك المستخدمين من البشر(عبدالصادق، 2016،ص12)، ولقد ساهم الفضاء السيبراني من خلال العديد من الأدوات والآليات إلى تغيير كل من حدود الزمان والمكان، فالمفهوم التقليدي للسيادة الوطنية كان مرتبط ببسط الدولة لأمنها على كامل اقليمها الجغرافي برا وبحرا وجواً، أي سيطرتها على كامل حدودها الجغرافية، غير أن اليوم أصبح هذا المفهوم متار جدل مع ظهور الفضاء السيبراني الذي اتاح أمكانية التحرك والمناورة بمرونة بالغة، حيث أصبحت حقيقة تلاشي الحدود التقليدية واقع مرير أفرز تحديات تتعدى مبدأ السيادة الوطنية.

إن سهولة الولوج إلى الأغوار السيبرانية مع قلة ادوات الاستخدام جعلت منه ميدانا فريدا من نوعه، فقد تجاوز تأثير المجال السيبراني ما تصوره الخيال وفق توقعات المؤسسات والدول، فبعد أن اعتبر مظهرا من مظاهر التقدم التكنو معرفي في عصر الذكاء الاصطناعي (العو لمة) أصبح سلاحا ذو حدين، تغيرت به مفاهيم وعلاقات تقليدية كالأمن والسيادة والقوة وغيرها.

وتحوي عناصر وفواعل الفضاء السيبراني على أجهزة الحواسيب والشبكات وبرمجة المعلومات والمحتوى، كما تتمثل في العنصر البشرى كمستخدم لهذه الأدوات من حيث النقل والتحكم، وتعرف وزارة الدفاع الأمريكية الفضاء السيبراني بأنه: مجال يتسم باستخدام الإلكترونيات (أي تكنولوجيا المعلومات والطيف الكهرومغناطيسي)، كمجال لتخرين البيانات وتعديلها وتبادلها عن طريق أنظمة شبكات الاتصال و البنية التحتية المادية المرتبطة بها، وبالتالي فالفضاء السيبراني هو استخدام تقنيات التكنولوجيا وكل ما يتعلق بها من ذكاء اصطناعي من طرف الدول أو الوكلاء لتحقيق السيطرة على فضاء القوة السيبرانية، حيث يتم التحكم في كل ما يتعلق بالحياة المدنية والعسكرية، وبذلك يعتبر الفضاء السيبراني المجال الخامس لفضاء القوة الاستراتيجية (بتصرف عن كلاع ،2022، ص 294)، لقد أصبح واقع المجتمعات البشرية اليوم يعوم في بحار الثورة التكنولوجية، مجتمع يغمره الطيف المعلوماتي و تجرفه القوة الذكية فلا يمكن تخيل واقع بدون معلومات وبدون خدمة النت، إن الواقع اليوم يؤكد أن العالم أصبح في عصر الرقمنة التكنو معرفية وعالم الاتصالات فعليا قرية صغيرة، فعولمة الفضاءات جعلت من الخصوصيات القومية عابرة للحدود الوطنية وعلى الرغم من الخيرات والفوائد الكبيرة التي تحققت في ظل المجتمع المعلوماتي من تطورات تساعد العالم في تسهيل مختلف أوجه نمط واساليب الحياة، إلا أنها عملت ايضا على تسهيل الأعمال الضارة السلبية سواء على صعيد الأفراد أو المؤسسات وكذلك الدول، حيث أن التجسس المتعمد في المجال السيبراني يؤثر سلبا على معلومات الأفراد والدول، وهذه التهديدات تتيح تسريب أسرار و معلومات حساسة للدول الأخرى، لذلك تسعى معظم الدول لخلق جدار سيبراني أمني بهدف تحصين أمنها القومي من الهجمات السيبرانية مجهولة المصدر، غير أن تأمين سيادتها المطلقة في الفضاء السيبراني أمر بعيد المنال، لأن اعتماد المجتمع على هذا البعد التكنولوجي يجعله عرضة بشكل خاص للأعمال العدائية، فلا يزال المهاجمون السيبرانيون يتمتعون بمميزات تفوق إمكانات المدافعين، بسبب التأثير المفاجئ الذي لا يمكن أن يقلل من قوة أي

أسلوب أمني أو دفاعي سلبي أو حتى ايجابي بشكل تام، كما أن هؤلاء المهاجمين يمتلكون القدرة على اخفاء آثارهم، ولا تسمح الحالة المعرفة بوضع توصيف دقيق للعمليات التي تحدث في القضاء السيبراني الأمر الذي يجعل المواجهة تقبل جميع الاحتمالات. (فوشر، 2019، ص71)

(1-2) مفهوم وأبعاد الأمن السيبراني:

أصبح الفرد الرقمي ومن خلفه المجتمع السيبراني (مجتمع الأنترنت) يغوص شيئا فشيئا في الفضاء المعرفي الإلكتروني اللامتناهي، و من هنا دخل الفرد والمجتمع والدول بالفعل في لولبة الانكشافية السيبرانية فالكل مفتوح على الكل، فلم تعد هناك خصوصية ولا سرية للمعلومات والبيانات، فقد أصبح ارتكاب الافعال الضارة من جرائم التَصيد والاحتيال جرائم مختلفة تماماً عن الاجرام التقليدي، فهي لا تنال من الأفراد فحسب بل طالت تأثيراتها المجمعات والكيانات والدول.

إن عمليات السطو والتجسس والتضليل وغيرها من الجرائم السيبرانية التي اسقطت الخصوصية والسرية أصبحت اليوم خطر داهم وشر لابد منه خطر تعدى الافراد والمجتمعات خطر عابر لحدود الدول يصعب التصدي له أو التنبؤ به، جرائم وأفعال صعبة الإثبات لتعقيد الربط الالكتروني من خلال شبكة حواسيب معقدة عبر العالم، ومع تطور وسائل وتقنيات سريعة تتكون من دوائر وحقول كهرومغناطيسية غير محسوسة، يثم تنفيذها عن بعد بسرعة وسهولة فلا تحتاج إلى وقت ولا جهد.

واليوم جميع المؤسسات الحكومية والأهلية وحتى الاستخدامات الشخصية تستخدم المعلومات الرقمية وتقوم بمعالجتها وتخزينها ومشاركتها، ومع زيادة هذه المعلومات وانتشارها، أصبحت حماية هذه المعلومات أكثر حيوية ولها تأثير فعال على الأمن القومي والاستقرار الاقتصادي للدول، فالكل يدرك اليوم أن الحرب الحالية والقادمة هي حرب المعلومات، من هنا جاء مصطلح الأمن السيبراني Cybersecurity (محمود 2020، ص2).

ومن المؤكد أن الجهات التي تقف وراء هجمات البرمجيات الخبيثة المدمرة تستفيد من التحول الرقمي الغير مسبوق، فتصاعد هذا التحول يشكل تهديدا متناميا للنظام الأمني العالمي، وهذه التهديدات والتحديات الأمنية ساهمت في تبلور مظهر جديد للأمن والحماية كمحاولة لمجابهة هذه الهجمات والاعتداءات السيبرانية، فالأمن السيبراني يعد مجموع الادوات والجهد المتواصل لحماية الشبكات وضمان حفظ بيانات الأفراد والمؤسسات، من الاستخدام الغير مصرح به أو أي اختراق واذى يلحق بالشبكة، ويلاحظ أن هناك عدة تعريفات ومفاهيم تناولت الأمن السيبراني غير أنها اجتمعت كلها على أمن وحماية المعلومات والبيانات أي توفير الحماية اللازمة للشبكات والأنظمة والبرامج من كل أشكال الهجمات والعدوان التي تهدف إلى اختراق جدار المعلومات الحساسة أو تغييرها أو تخزينها والعبث بملفاتها، ويمكن تعريف الأمن السيبراني بانه أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والاجهزة المتصلة بالأنترنت، وعليه فهو المجال الذي يتعلق بإجراءات ومقاييس ومعايير الحماية المفروض اتخاذها، أو الالتزام بها لمواجهة التهديدات ومنع التعديات أو الحد من آثارها في أقصى وأسوأ الأحوال(جبور، 2017، ص 26).

وبتعبير آخر فأن الأمن السيبراني يرتكز على مجموع الأطر القانونية والتدابير التنظيمية التي تساهم في أمن الشبكات من المخاطر المحدقة بالمعلومات ومعالجتها، والتركيز على ضمان توافر أنظمة المعلومات وتمتين الخصوصية لمنع الاستخدام غير المصرح به، مع تعزيز حماية سرية البيانات وتنظيم أصول الاستخدام.

ونستخلص بأن الأمن السيبراني أصبح يتخذ عديد الأبعاد كونه يرتبط ارتباطا وثيقاً بسلامة مصادر بيانات مختلف المسائل الاجتماعية والانسانية ومن تم الاقتصادية والسياسية والامنية

أي باختصار أمن بيانات ومعلومات الاتصال والتواصل، منظومة أمن متكاملة تعمل على الحفاظ على الأمن القومي للدولة من كل التهديدات السيبرانية، وعليه لا بد من توضيح أبعاد الأمن السيبراني التي نوردها كالاتي (زروقة، ابريل 2019، ص 1022).

البعد العسكري:
يكمن في الحفاظ على قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية مما يسمح بتبادل المعلومات والأوامر وتدفقها (هي الفكرة التي خلقت وطورت من أجلها الشبكات ومن بعدها الأنترنت)، وإصابة الأهداف عن بعد، إلا أنها تمثل كذلك نقطة ضعف، خاصة إذا لم تكن مؤمنة جيدا من الاختراق الذي قد يؤدي إلى تدمير قواعد البيانات العسكرية، أو قطع الاتصال بين القيادة والوحدات العسكرية، فضلا عن امكانية التحكم في بعض الاسلحة وخروجها عن السيطرة كالصواريخ الموجهة والطيارات المسيرة.

البعد الاقتصادي:
أصبح الأنترنت أساساً للمعاملات التجارية والمالية والاقتصادية، حيث أصبحت الحواسيب تستعمل في تسيير وتطوير الصناعة وتحريك الاقتصاد وأصبح الكل مترابطاً عبر شبكات الكمبيوتر، مما يستدعي الحديث عن أهمية تحقيق الأمن السيبراني في المجال الاقتصادي.

البعد الاجتماعي:
يفوق مستخدمي الأنترنت 5 مليارات شخص في العالم، والذين اغلبيتهم يستخدمون مواقع التواصل الاجتماعي، مما يجعلها أكبر تجمع للتفاعل البشري وتفتح الباب واسعا لتبادل الافكار والخبرات الجيدة، لكن في المقابل يعرض أخلاقيات المجتمع للخطر نظرا لصعوبة مراقبة محتوى الشبكة، كما يعرض الهويات لعمليات اختراق خارجي قد تتسبب في تهديد السلم الاجتماعي للدولة، لذلك يجب توعية الأفراد بهذه المخاطر لتحقيق الأمن السيبراني في بعده الاجتماعي.

جدول (1) مستخدمو الانترنت في العالم (31-12-2021).

العالم	السكان (2022)	النسبة من سكان العالم	مستخدموالانترنت 31 -12-2021	معدل الاختراق %	مناطق نسبة استخدام الانترنت من العا لم %
أفريقيا	1.394.588.547	% 17.6	601.940.784	% 43.2	% 11.2
آسيا	4.352.169.960	% 54.9	2.916.890.209	% 67.0	% 54.2
أوروبا	837.472.045	% 10.6	747.214.734	% 89.2	% 13.9
أمريكا اللاتينية والكاريبي	664.099.841	% 8.4	534.526.57	% 80.5	% 9.9
أمريكا الشمالية	372.555.585	% 4.7	347.916.964	% 93.4	% 6.5
الشرق الأوسط	268.302.801	% 3.4	206.760.743	% 77.1	% 3.8
أوقيانوسيا/أستراليا	43.602.955	% 0.4	30.549.185	% 70.1	% 0.5
مجموع العالم	7.932.791.734	% 100.0	5.385.798.406	% 67.9	% 100.0

المصدر: الاتحاد الدولي للاتصالات https;//www.itu.int.

البعد السياسي:
يعد حماية النظام السياسي حق لكل الدول لأجل المحافظة على هيكلها وكيانها السياسي وكذلك مصالحها الاقتصادية كطريق إلى تحقيق رفاهية شعبها، ومن المعروف أن تقنية الاتصال اليوم أصبحت لاعب أساسي في اللعبة السياسية وخاصة في الترويج للأفكار المزيفة والهدامة وكذلك في المجالات الانتاجية، ويعد التدخل الروسي السيبراني في الانتخابات الأمريكية أبرز دليل على ضرورة واهمية الأمن السيبراني، في بعده السياسي اضافة إلى التسريبات للوثائق الحساسة والاختراقات التي غالبا ما تؤدي إلى أزمات دبلوماسية بين الدول، كما أن الفضاء السيبراني أصبح بيئة خصبة للحملات الانتخابية والدعاية لمختلف الفاعلين الدوليين.

البعد القانوني:
إن تطور التكنولوجية المتسارعة تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية في الفضاء السيبراني، والملاحظ أنا الجريمة السيبرانية تفتقد في معظم البلدان إلى الأطر القانونية الصارمة للتعامل معها، خاصة وأن قادم الأيام مع زيادة وثيرة التقدم التكنو معرفي لابد وأن هذه الأعمال والأفعال ستشهد تصاعدا، مما يحتم زيادة فرض القوانين الرادعة في حق المستخدمين الغير منضبطين كالقراصنة والمتصيدين لدا يجب زيادة التعاون بين الجهات والمؤسسات الأمنية وكذلك زيادة التعاون الدولي المشترك لمكافحتها.

(2) الفضاء السيبراني مجالا للحرب والصراع:
غدت الشبكات العنكبوتية المنتشرة في المجال الأرضي بيئة وحلبة لكل النشاطات المدنية والعسكرية، وخدمة الانترنت تحولت إلى وسيلة للتواصل عن طريق سرعة الحصول على المعلومة، بحيث تقوم الأجهزة بمعالجتها وتخزينها ومشاركتها، ومع التطور المستمر وتشابك المصالح الدولية أخذت الدول الكبرى المتقدمة تتسابق لتطوير برمجيات يكون من شأنها امتلاك قدرات هجومية وأخرى دفاعية، تعمل على درء جميع أنواع المخاطر التي تتعرض لها انظمتها السيبرانية من الهجمات المدمرة التي تقف ورائها دول أجنبية وكذلك تعمل على حماية شبكاتها من القراصنة الذين يهدفون إلى تعطيل الخدمات الأساسية، وهكذا تتحول مخاوف الدول من الاعتداءات ووقعها المحتمل إلى واقع أسمه الحرب السيبرانية.

وبالتالي أصبح الفضاء السيبراني ساحة جديدة للصراع ليس بشكله التقليدي، ولكنه ذو طابع معلوماتي يعكس النزاعات التي تخوضها الدول او الفاعلين من غير الدول، وتختلف دوافع هذه الصراعات فمنها مرتكز على خلفيات دينية أو عرقية وإيديولوجية أو اقتصادية أو سياسية، ويتمدد الصراع السيبراني عبر شبكات الاتصال والمعلومات متجاوزا الحدود التقليدية وسيادة الدول. (زروقة، ابريل، 2019، ص 1021).

(2-1) عسكرة القضاء السيبراني:
لقد غير التقدم التكنو معرفي موازين كل شيء فأصبحت الحياة العصرية اليوم رهينة التقنية الحديثة، فالفضاء المعرفي الالكتروني دخل في كافة جوانب الحياة الانسانية، وبقدر المميزات الهائلة التي جنتها البشرية من هذا التطور، بقدر ما صاحب هذه الخدمات والمميزات مخاطر وتحديات مدمرة فتاكة زادت من معاناة الأفراد والمجتمعات والدول، فلم يعد من هو في منأى من تيار العصرية الرقمية بمالها وبما عليها.

ومن أشد أنواع المخاطر اليوم ما يسمى بالحرب الالكترونية السيبرانية فالحرب الإلكترونية (Cyber Warfare) تعني صراع ميدانه شبكة الأنترنت، وينطوي على هذه الهجمات في الغالب الدوافع السياسية عن طريق السطو على المعلومات ونظمها، حيث يمكنها تعطيل مواقع الويب الرسمية والشبكات وكذلك تعطيل الخدمات الأساسية أو سرقة وتعديل البيانات السرية وتخريب الأنظمة المالية، وذلك من بين العديد من الاحتمالات الأخرى، فلم تعد الحروب تقتصر على استخدام الأسلحة الفتاكة فقط والتي تحملها الطائرات أو المدرعات أو الجنود، فهذه توشك أن تتوارى في المستقبل وراء ظل حروب ربما تكون أكثر فتكاً وهى الحروب الإلكترونية(بتصرف عن محمود،2020، ص 11)، وأصبح

التسليح التكنو معرفي اليوم ذو أهمية بالغة في توازن القوى على الصعيد العالمي، فقد جنحت الدول إلى نظام الحصانة المعلوماتية وذلك من خلال السعي إلى أمثلاك التكنولوجيا الرقمية كمحاولة لفرض وخلق أنظمة ضبطية، لأجل حفظ وحماية بنيتها الوطنية المعلوماتية وكذا الأسرار الأمنية، في ظل بيئة عالمية يسودها الشك وعدم اليقين مع قابلية تدمير المصالح الاستراتيجية بسرعة الضوء وهو ما يحمل خطورة عسكرة الفضاء السيبراني، ولهذا تتبنى عديد الدول استراتيجية الحرب السيبرانية كحرب للمستقبل، واعتبار أن النصر في المعركة حليف من يقدر على شل القوة والتشويش على المعلومة (طالة،2020،ص66).

إن تزايد الاعتماد على والوسائل والوسائط الذكية والحديثة من قبل الافراد والمجتمعات، وذلك بتبني كثير من الدول والأنظمة لنماذج الحكومات والمدن الذكية، الأمر الذي سيجعل من العالم أكثر انكشافاً لتكنولوجيا المعلومات، مما ييسر وبشكل مطرد من عمليات التصيد والهجمات السيبرانية والتي تعرض مصالح الأفراد والدول للخطر، ومن هنا كان لزاما تبني مفهوم واضح يعبر عن معنى الحرب السيبرانية، وعلى الرغم من جهود بعض الخبراء والمنظمات الدولية وكذلك مراكز الأبحاث المحلية والعالمية، فكل هذه الجهود عملت على صياغة مفهوم وتعريف متفق عليه عالمياً للحرب السيبرانية، إلا أنه لم يتم حتى الآن التوصل لتعريف موحد يوضح معنى الهجوم والحرب السيبرانية، ويعزى هذا التباين في طبيعة أهداف واستراتيجيات الدول من حيث مرتكزات و محددات التعريف، حيث تعتمد الولايات المتحدة الأمريكية وحلفائها، مقاربة اقتصادية ومادية، بينما تركز منظمة شنغهاي للتعاون على أهداف الصراع في الفضاء السيبراني مثل السيادة الوطنية والهوية الثقافية، ومن تم خرجت مجموعة الخبراء في الناتو بتعريف للحرب السيبرانية على انها: جميع العمليات السيبرانية سواء أكانت دفاعية أو هجومية والتي يمكن أن تسبب اصابات أو وفيات أو تلف وأضرار مادية (جبور،2017، ص66-67).

ونلاحظ أن هذه المقاربات والمفاهيم اغفلت الدور البشري الفني والاخلاقي، والذي يعد من العناصر الأساسية والذي يتمثل في أمن المعلومات، كما أن هذه المفاهيم كانت قاصرة من حيث التمييز فيما بين الحروب السيبرانية ومختلف أشكال حروب المعلومات، والتي من أهمها الجرائم والإرهاب السيبراني، لأن معظم الاعتداءات السيبرانية لا تنتج أضراراً مادية بل هي هجمات واعتداءات مباغتة شديدة التعقيد والتمويه، وليست بالضرورة ذات طابع عسكري ضاهر، فالسرقات التي تطال المصارف وعمليات التجسس الصناعي، ليست اعمالا حربية بالرغم من ابعادها الخطيرة على الأمن القومي لأنها تمس الاقتصاد الوطني ورفاه البلد، إلا أن الخبراء يرون انعكاسات الاعتداء على البنك المركزي الأمريكي مثلاً أشد وأدهى من اعتداءات الحادي عشر من سبتمبر على الاقتصاد العالمي (جبور، 2017، ص 67)، ويشير مكتب الأمم المتحدة المعني بالجريمة والمخدرات إلى الهجمات السيبرانية على أنها كل فعل ينطوي على استغلال الشبكات الحاسوبية بصورة متعمدة كوسيلة لشن هجوم، بهدف تعطيل النظم المستهدفة كنظم الحواسيب والخوادم وبنيتها التحتية الأساسية، وذلك بواسطة الاختراق الحاسوبي أو استخدام التقنيات المتقدمة بصورة تهديد مستمر، عن طريق الفيروسات الحاسوبية أو البرمجيات الضارة أو غيرها من وسائل الدخول غير المصرح به، كما أن هذه الاعتداءات قد تحمل سمات أعمال إرهابية أو اجرامية، بما في ذلك الرغبة في نشر الخوف لزعزعة المجتمعات دعما لأهداف اجتماعية أو سياسية أو أمنية.

وحاليا معظم الدول خاصة منها المتطورة تسابق في الزمن لأجل تطوير برمجيات وانظمة عالية الدقة، من شأنها توفير تقدم تكنومعرفي تعمل على امتلاك قدرات سيبرانية هجومية وأخرى دفاعية قادرة على التصدي لأي اختراقات، وايضا شن أي هجمات استباقية إلكترونية تلبي متطلبات أمنها القومي، لذا أصبحت قضية الدفاع عن البنك المعلوماتي الوطني ذات أولوية قصوى لعديد الدول، ورغم هذه الجهود والمحاولات فأن كثير من دول العالم بما فيها الدول الكبرى لم تستطع التصدي للجرائم السيبرانية حيث تعرضت للهجمات والاختراقات الالكترونية، كما حدث في الولايات المتحدة الأمريكية عند بداية حكم الرئيس الأمريكي جو بايدن، فقد تعرضت أهم المؤسسات الأميركية كالبيت الأبيض ووزارات الخارجية والتجارة والخزانة والأمن الداخلي ووكالات فدرالية أخرى لهجمات إلكترونية تعد واحدة من

أكبر الاختراقات وأشدها تعقيد في السنوات الخمس الأخيرة، وعلى إثر هذه الهجمات أصدر مكتب التحقيقات الفيدرالية ووكالة الأمن السيبراني، ومكتب التحقيقات الأمريكية بيانا مشتركا أكدوا فيه أن العمل مستمر لتقييم حجم الضرر الذى لحق بشبكات الحكومة الفيدرالية(العودي، تاريخ التصفح 2023//8/23، ص 11)، ويعد هجوم " ستا كسنت من أبرز الهجمات التي شنتها الولايات المتحدة الأمريكية والكيان الصهيوني ضد إيران، والتي كانت جزءً من هجمات أكبر عرفت باسم " الألعاب الأوليمبية " وقد هدفت ستاكسنت إلى تخريب برنامج إيران النووي، حيث تم إنزال فيروس على برنامج التشغيل الالكتروني الذي يدير عملية تخصيب اليورانيوم في موقع "ناتانز" النووي وتسبب ذلك في إتلاف عدد كبير من وحدات الطرد المركزي، وقد كان هذا الهجوم متطورا بالنظر لقدرته على اتخاد قرارات مستقلة في البيئة المستهدفة بدون التواصل مع الطرف منفذ الهجوم (Rid،2013 ،pp80-81) وقامت إيران بالمقابل بتطوير انشطتها السيبرانية لمحاولة ردع ومكافحة هذه الاعتداءات.

ومن الأمثلة الأخرى التي استخدمت فيها الهجمات الإلكترونية عبر الفضاء السيبراني، الهجوم الأمريكي الالكتروني سنة 1998 على منظومة الدفاع الجوي الصربي اثناء الحرب في البلقان، وكان الغرض من هذا الهجوم تعطيل منظومة الدفاع الجوية حتى يستطيع الطيران الحربي الأمريكي من قصف القوات الصربية ليتنيها على مواصلة الحرب والعدوان على البوسنة، وكذلك فقد تعطلت شبكة "أرامكو" النفطية السعودية والتي يعمل بها 30 ألف جهاز حاسوب وهددت بإعاقة قدرات إنتاج نحو 9 ملايين برميل يوميا من النفط للسوق العالمية بهدف خلق أزمة في سوق الطاقة العالمية، ويجزم الخبراء بأن هذا الهجوم قد تم عن طريق فيروس أطلق عليه اسم شامون 11، وهو جزء من الحرب الإلكترونية التي تزداد ضراوة في الشرق الأوسط، وقد استهدف هذا الهجوم إضافة إلى العربية السعودية، شبكات الغاز القطرية، وقد توجهت الاتهامات في هذه الحادثة إلى إيران (جبور، 2017، ص 69)، و غير ذلك كثير ومن الملاحظ أن هذه الهجمات والاعتداءات في تصاعد مستمر، ولعل أبرز ما يعزز انتشار الأنشطة غير السلمية في الفضاء السيبراني ارتباط العالم المتزايد بشبكة المعلومات الدولية، فقد أصبح الفضاء السيبراني ساحة للتفاعلات الدولية المختلفة، لهذا يعتبر تأمين المعلومات والشبكات عبر تطبيق التحديثات الأمنية المتواصلة على كافة الأنظمة أمر في غاية الاهمية، وذلك لغلق أي ثغرة في النظام يمكن استغلالها للنفاذ لقاعدة البيانات الوطنية، إن تطور شكل الحرب عبر التاريخ من الحجارة والرماح، إلى السهام والسيوف والانتقال إلى المسدسات والبنادق، وعالم الصواريخ والقاذفات ثم إلى الدبابات والطائرات والغواصات وصولاً إلى القنابل النووية والهيدروجينية ينذر بالقول: إن من لا يدرك جيداً تغيير طبيعة وعصر وسلاح المعركة القادمة ويسارع بالحصول عليه وتطويره سوف ينتهى به الأمر مهزوما تابعاً لغيره ضعيفاً بين الأمم، وكلما ازدادت الدول علما وتقدماً ازدادت معها القدرة التدميرية للأسلحة المستخدمة.

و سلاح الحرب القادمة سوف يكون أقوى وابشع من القنابل النووية والهيدروجينية، فالجنود المقاتلون في هذه المعركة هم من الروبوتات والدرونز والاسلحة عبارة عن شفرات وفيروسات و ديديان مبرمجة، لا يتعدى حجمها بضعة كيلو بايتيس، ولكنها قادرة على إحداث تأثير يفوق في قوته الأسلحة التقليدية (خليفة، 2020، ص 12).

جدول (2) طيف من الهجمات السيبرانية.

اسم الهجوم السيبراني	السنة
هجمات حلف الناتو الالكترونية على صربيا بهدف تعطيل منظومة الدفاع الجوية	**1998**
الحرب الالكترونية بين حزب الله والكيان الصهيوني	**2006**
الهجمات الروسية الالكترونية على استونيا	**2007**
الهجمات الروسية الالكترونية على جورجيا	**2008**
الهجمات الأمريكية الصهيونية على المنشآت النووية الإيرانية (فيروس ستاكسنت)	**2010**

المواجهات الالكترونية بين حماس والكيان الصهيوني(مواجهات قطاع غزة)	**2023 -2008**
هجمات فيروس " شمعون " ضد شركة آرامكو وبعض المنشآت الحيوية في العربية السعودية	**2017 -2012**
هجمات فيروس " دوكو " على شبكة فنادق استضافت محادثات تتعلق بالملف النووي الإيراني	**2015 -2014**
اتهام روسيا بالقرصنة الالكترونية في الانتخابات الأمريكية لدعم المرشح الجمهوري دونالد ترمب	**2016**
هجوم الكيان الصهيوتي على مفعل " نطنز " النووي الإيراني	**2021**
اتهام روسيا بشن هجمات الفدية Ransom Ware Attack على مؤسسات أمريكية	**2021**

المصدر: بتصرف عن، علاء السيد فرحات، عمارة عمروس، الفضاء السيبراني وتأكل مفهوم السيادة الوطنية (ص13).

(2-2) المخاطر السيبرانية:

منذ اتجاه طرق ووسائط التواصل الرسمي والاجتماعي إلى الشبكة العنكبوتية في الربع الاخير من القرن العشرين، والطلب العالمي على الانترنت في اضطراد، سواء من حيث الاتصال أو التوزيع والانتاج وصولا إلى الحوسبة السحابية وانترنت الاشياء، فباتت معظم خدمات العالم الانتاجية والخدماتية والمعلومات تعتمد بصورة جوهرية واساسية على تلك الشبكة، وهذا ما زاد من المخاطر جراء الاعتماد الكبير عليها، وزاد ايضا من مخاطر ما يمكن أن تتسبب به الهجمات الالكترونية التي يتعاظم دورها ويتسع نطاقها، في عالم أصبحت فيه شبكة الانترنت هشة يسهل اختراقها(محمود، سبتمبر2013، ص 2).

وكما أشرنا سابقا أن عمليات الحماية والمحافظة على سلامة الشبكة من الهجوم والاصطياد الالكتروني أمر صعب، نظرا لتطور البرمجيات والانظمة التقنية، أضافة إلى أن القراصنة والمهاجمون دائمًا يبحثون عن نقاط الضعف والثغرات التي من الممكن عن طريقهما استهداف الشبكة المراد اختراقها وسرقة أو تعطيل محتوياتها.

وتعد الفيروسات الأسلحة الأساسية في الهجوم حيث تؤدي إلى تعطيل عمل الشبكات الالكترونية والخوادم الرئيسية، أو يؤدي استخدامها لأرسال مختلف المعلومات من الأماكن التي تغزوها، ويمكن نشر الفيروسات عبر الرسائل الإلكترونية أو عن طريق نقل الملفات الالكترونية أو تحميلها على أداة لحفظ البيانات، ويشار هنا إلى أن فيروس ستاكسنت الذي ضرب المفاعل النووي الايراني، قد تم عبر استخدام هذه الطريقة : نقل بواسطة " usp " ، ولا سيما أن هدا المفاعل غير موصول بالشبكة العنكبوتية العالمية، (بتصرف عن جبور، 2017، ص 68) ومن المؤكد أن مخاطر الهجمات والاعتداءات السيبرانية لا تقتصر على استخدام الفيروسات فقط بل تتعداها إلى عمليات التشويش عبر الموجات الكهرومغناطيسية المتعلقة بموجات الاتصالات السلكية واللاسلكية لغرض التجسس وسرقة البيانات ، ولابد من الاشارة إلى أن الاعتداءات السيبرانية يمكن أن تكون ذات طابع عدواني أمني يمس كيان الدولة أو أن تكون ذات طابع جنائي وهي التي في الغالب تتعلق بسرقة المعلومات الخاصة بالأفراد والمؤسسات المالية ، ولعل أخطر ما يميز هذه المخاطر السيبرانية هو صعوبة الردع، ففي الحروب التقليدية يعد الهجوم المضاد هو الرادع الحقيقي امام التفكير في شن الحرب، وهو الأمر الذي يصعب القيام به في حالة الحروب السيبرانية ، ويرجع ذلك إلى عدة عوامل أهمها صعوبة اكتشاف الهجوم السيبراني في وقته الحقيقي فضلا عن صعوبة تقييم الاضرار الناتجة عن شن هذه النوعية من الهجمات، وكذلك صعوبة التحكم في مدى الهجوم السيبراني المضاد، إضافةً لصعوبة تحديد هوية الطرف القائم بالهجمات السيبرانية على وجه التحديد (بتصرف عن منصور،2019، ص 101)، ومن أهم الصعاب التي تواجه السيطرة على المخاطر السيبرانية سهولة تمكن أي فرد أن يكون هو الجاني في الهجمات السيبرانية، وذلك لسهولة الحصول على ادوات الهجوم التي تتمثل في جهاز حاسوب مرتبط بخدمة الانترنت والذي عن طريقه يحدث الاختراق.

أن تهديدات الفضاء الالكتروني كما رأينا لا تقتصر على الأمن الداخلي للدول بسبب ما يعرف بالجرائم السيبرانية، بل تعداه إلى تهديد السلم والأمن العالميين، فالتطورات الهائلة في وسائل التكنولوجيا والاتصالات قد وضعت أيضا في يد كل من الدول والفاعلون من غير الدول بما في ذلك الجماعات الارهابية مجموعة جديدة من الأسلحة الهجومية، تمكنهم من تنفيد هجمات واعتداءات سيبرانية لتحقيق أهدافهم، والتي تتنوع ما بين منشآت حيوية عسكرية أو مدنية وأصبح من الممكن تعطيل أو أتلاف شبكات الدفاع العسكرية من بعد، واختراق أو تعطيل أو تدمير شبكات القطاع الخاص وأيضا تعطيل البنية التحتية للبلد، كذلك أصبح من الممكن التدخل والعبث في سلامة البيانات العسكرية الداخلية لبلد أخر، ومحاولة ارباك أو التشويش على معاملاتها المالية أو تحقيق أي عدد من الأهداف الاخرى،(حسين، أبريل 2021، ص 1077)، وفي زمن التقدم التكنو معرفي والانفلات المعرفي، اختلف مفهوم العمليات العسكرية بحيث تغير أسلوب وميدان المواجهة كما تبدلت قدرة الرد والدفاع ولقد أصبح مفهوم القوة والأسلحة الذكية طموح للأمم والدول، ومن ابرز التطورات التي شهدتها الحروب الحديثة ظهور ما يعرف بالأسلحة ذاتية التشغيل والتي تعرف أيضا بالروبوتات القاتلة، والتي هي عبارة عن نظام تسليحي له قدرة على اتخاد قرارات مستقلة عن تدخل البشر، من حيث القيام بالبحث وتحديد وتعقب ومن تم مهاجمة الأهداف بصورة ذاتية ولقد زادت وثيرة انتشار الأسلحة الذكية وخاصة الطائرات المسيرة الدورنز، فأصبح التوسع في استخدامها سواء في الجو أو البحر أو البر ومع انتشار هذه التكنولوجيا واستخدامها لأغراض متعددة، فأنه أصبح بإمكان عدد كبير من الدول، بل والفواعل المسلحة من دون الدول استخدامها على نطاق واسع، وهو ما يجعل من الصعب تحديد هوية الطرف الذي قام باستخدام هذه الانظمة التسليحية في الهجوم على دول أخرى (منصور، 2019،ص 144).

ولقد أصبحت المخاطر السيبرانية في هذا الزمن معقدة وخطيرة وذات أبعاد متعددة، فقد انتقلت النشاطات الإنسانية إلى الفضاء السيبري وهذه النشاطات منها ما هو شرعي قدم فائدة وخدمات جلية للبشرية، ومنها ما هو غير شرعي كالإرهاب والخراب أفعال تحمل اتارا ضارة قام بصناعتها هواة أو مؤسسات، تقف وراءها جهات بهدف تحقيق مأرب متباينة، ومن أبرز مظاهر هذه المخاطر ظهر ما بات يعرف بالمتصيدون "الهاكرز" وهم الذين يعملون على الاختراق البرمجي لأجهزة الحواسيب ، ولقد عرف عالمنا المعاصر عاصفة الكترونية جامحة من خلال ما احدثته تسريبات ويكيلكس (storm Wikilex) والتي تضمنت استخدام موقعها على الانترنت في نشر صور ضوئية لألاف الوثائق السرية الرسمية المتبادلة بين وزارة الخارجية الأمريكية وبعثاتها بدول العالم، وما احدثته تلك التسريبات من توتر حاد في العلاقات الدولية على جميع الصعد(محمود، سبتمبر2013، ص6).

ونستخلص أن مخاطر واثار الهجمات السيبرانية عديدة ومتنوعة وتمس مختلف مناحي الحياة، فهي تؤثر على المجالات المدنية والعسكرية وتهدد البنى الاجتماعية والاقتصادية والصحية والبيئية، وأصبحت اليوم مصدر قلق للكل على اعتبار أن تحقيق الأمن السيبراني وثيق الصلة بالحفاظ على الأمن القومي للدول.

(3) الفضاء السيبراني واندثار الحدود الجغرافية للدول:

لقد تغيرت مفاهيم السيادة الوطنية للدول بحكم التطورات التقنية والمعلوماتية الهائلة، وما صاحب ذلك من تراجع واضح للدور التقليدي للدولة في الحفاظ على سيادتها وأمنها القومي، فقد أوجدت التطورات الجيوسيبرانية المتعاظمة، ساحات سيادية جديدة بسبب أن قدرة كل دولة لم تعد مؤكدة في الحفاظ على سيادتها السيبرانية، فالمجال الافتراضي المرتبط بشبكة الويب العالمية سهل من عمليات النفاذ للمعلومات الوطنية ومن تم نقل المعلومات خارج نطاق سيطرة الدول، لذلك أصبح الأمن السيبراني احد أهم اركان منظومة الأمن القومي لجل دول العالم.

(3-1). المجال السيبراني وتأكل مفهوم السيادة الوطنية:

كما اوضحنا سابقا أن التطورات المتسارعة في تقنيات الاتصالات والمعلوماتية، أدت إلى الانكشافية الرقمية بشكل جعلت من الخصوصية المعرفية تنتشر شيئا فشيئا، في ظل انصهار الحدود الجغرافية للدول نظرا لقوة التفاعل الرقمي وحوسبة المعلومات والذي جعل من فضاء المعلومات نوعا جديدا من

الفضاء الجيوسياسي، فمفهوم سيادة الدول لم يعد كما استقر عليه قبل المستحدثات التكنولوجية الجديدة التي لا تعترف بحدود دولية ، فباتت الدول تخشى منها على سيادتها وبالتالي أمنها القومي الذي بات قابل للاختراق في ظل التهديدات الجديدة ذات الطبيعة السيبرانية (بيرم، 2020، ص 791)، يعيش العالم اليوم في مرحلة مفصلية، مرحلة ينفصل فيها الماضي عن المستقبل ولقد تعالت الاصوات التي أصبحت تشكك في مفهوم قداسة السيادة الوطنية ليس بالمعنى الجيوسياسي فقط بل حتى في معناها الدستوري التقليدي، ومن المؤكد أن سيادة الدولة تتعرض لمنافسة شديدة من قبل اطرافا يزدادون عدداً وقوة بحيث يتجاوز التهديد الذي تتعرض له الدولة كيانها وهياكل أمنها القومي، الذي بات قابل للاختراق في ظل التهديدات الحديثة ذات الصبغة السيبرانية، فمسلمة الدول كوحدات سياسية كاملة السيادة والسيطرة أخده في الانكماش نحو الهجوم المتسارع لأدوات العولمة حيث أصبحت الدول لا تستطيع أن تعبر عن كامل سيادتها في الفضاء السيبراني الذي أضحى مجالا خامساً للصراع في العلاقات الدولية العابرة للحدود.

ومن خصائص هذا الفضاء تلاشي الحدود التقليدية للدول، حيث أسقطت تكنولوجيا الاتصالات والمعلومات مفهوم الحدود الجغرافية، ومعنى الحدود وفق المصطلح الجيوسياسي :هي الخطوط التي تحدد الأبعاد الجغرافية للدولة ورقعتها المساحية كدولة مستقلة ذات سيادة، والتي عندها تنتهي سيادة وقوانين دولة لتبدأ سيادة وقوانين دولة أخرى" أي أن الحدود موقع جغرافي تلتقي عنده قوى دولتين، وتنتهي عند هذه الحدود نفوذ كل منهما وقوانينها(جاد الرب،2008،ص 85)، هذا المفهوم للحدود شهد تحولات مع الثورة التكنومعرفية، فالشبكة العنكبوتية تجاوزت هذا المعنى حيث الانكشاف المعرفي الذي أوجد نشاطاً بشرياً مترابطاً سمح بتبادل المعلومات وتدفقها بسرعة وسهولة محولة العالم إلى قرية كونية صغيرة خالية من الحواجز والعراقيل، الأمر الذي جعل الدول تعاني من مشاكل أشد وأخطر من تلك التي واجهتها من قبل، فإلى مسائل الأمن عبر الحدود وفق وسائل الأمن التقليدية برزت مشكلة السيادة على الفضاء السيبراني، وعلى العلاقات التي تحاك عبر الأنترنت بين أشخاص موجودين على أراضي مختلفة خاضعة لعدد من السيادات، أذ يختلف بلد مصدر العمل وبلد تحقق نتائجه والبلدان التي تمر عبرها البيانات، فالفضاء السيبراني مكان مختلف لكنه شديد الارتباط بالعالم المادي وليس مستقلاً عنه(المشهدي، 2020،ص244).

ولقد أصبح موضوع السيادة على الفضاء السيبراني أكبر تحدي تواجهه الدول اليوم، فمفهوم سيادة الدول طبقا لمبادئ القانون الدولي لم يعد ممكناً تطبيقه على هذا الفضاء التكنومعرفي، وبالتالي فإن السيادة السيبرانية تعني خضوع القضاء السيبراني لصالح وقيم الدولة، أي قدرة الدول على التحكم في مجالها السيبراني بما يضمن أنه يتبع نفس القواعد والمعايير والاعتبارات من بقية المجتمع، فهي عبارة تستخدم في مجال حوكمة الانترنت لوصف رغبة الحكومات في ممارسة السيطرة على الانترنت داخل الحدود الوطنية التابعة لهذه الحكومات، أي أنها تطبيق لحقوق والتزامات سيادة الدول على الفضاء السيبراني (بيرم، 2020، ص 799)، وهذا يعني أن السيطرة المطلقة على الفضاء السيبراني قد أثر في سيادة الدولة ولم يلغيها بل فرض وظيفة جديدة على أمن وسيادة الدول، لأنها ببساطة تتشابك وارتباط مصالح الدول بعضها ببعض، فتقدم والوسائط المعلوماتية أجبر الدول على تنويع اتصالاتها وعلاقاتها الخارجية فلم يعد بالإمكان لأي دولة الانكفاء والاعتماد على الذات فقط، فحتى الدول المتقدمة كالولايات المتحدة الأمريكية لا تستطيع الاكتفاء بوسائلها ومنتجاتها المعلوماتية، فالتطور الهائل المتعلق بتقنية المعلومات والرقمية حتم على الدول الانفتاح والتعاون مع شركات تكنولوجيا المعلومات والاتصالات، واليوم لم يعد امتلاك القوة الإلكترونية حكراً على الدول الكبرى، بل تعددت الفواعل وأصبح انتقال القوة وانتشارها بين اطراف متعددة ميسور بحكم وجود المهارات البشرية وسهولة توافر البنية المعلوماتية.

فمبدأ السيادة التامة والمطلقة للدولة على نطاقها الجغرافي أي في كافة مجالاتها الأرضية والبحرية والجوية، صار من الماضي لصالح وسائل تكنومعرفية تتغلغل بكافة الأشكال والطرق، وأصبح على الدول الانخراط بواقع وحال السيادة المتقاسمة.

(2-3) الأمن القومي وسبل درء المخاطر:

تصارع الدول اليوم تيارات العولمة بمختلف ادواتها ووسائلها، ففي ظل ازدياد مخاطر الانكشافية المعلوماتية، أصبح من الضروري إعادة النظر في مختلف الوسائل الرقمية والمفاهيم التقليدية كالأمن بكافة أبعاده والقوة ومن تم السيادة الوطنية، لذلك أصبح أمن الدولة في عصر الرقمية وتدفق المعرفة من الأولويات القصوى ويعد أكبر تحدي لكافة الدول، فتحدي الأمن السيبراني والذي بكل تأكيد ذلك الأمن الذي لا يقتصر على الجوانب العسكرية، بل أخذ يجاري كل التهديدات والمخاطر التي تعترض سبل بسط الأمن في المجال السيبراني، والذي اضحى أعلى تحديات الأمن القومي في القرن الواحد والعشرين، ومع زيادة الحاجة للأنظمة الإلكترونية من قبل الدول والحكومات ومع احتدام الصراع التقني حول الاستحواذ على سبق التقدم التكنولوجي، اتجه العالم نحو التنافر و التعارض في القيم والمصالح والاحتياجات وهذا بدوره ساهم في بروز طرق واساليب جديدة لحالة التصادم الدولي، تباينت بين الأوجه التقنية والاقتصادية والأمنية كما أن هذه الحالة من الصراع أوجدت طرق بديلة عن الحرب التقليدية أي الصدام المباشر بين الدول، إلى صراع طيفي مجاله الفضاء الإلكتروني عبر شبكات الويب العالمية.

ومن هنا جاء مفهوم الأمن الإلكتروني والذي يعد ركنا اساسيا من أركان الأمن القومي، ولقد تزايدت العلاقة بين الأمن والتكنولوجيا خاصة مع إمكانية تعارض المصالح الاستراتيجية للدول إلى أخطار وتهديدات، الأمر الذي حول الفضاء الإلكتروني كوسيط ومصدر لأدوات جديدة للصراع الدولي، وفرضت تلك التطورات إعادة التفكير في مفهوم الأمن القومي للدولة، والذي يُعنى بحماية قيم المجتمع الأساسية وإبعاد مصادر التهديد عنها (عبد الرحمن،2022، ص 437- 438)، ومما لاشك فيه أن القوة السيبرانية ترتبط بدرجة تملك القوة الذكية، فحيازة المعرفة التقنية مع القدرة على استخدامها بدرجة تسمح للفاعلين السيبرانيين تحقيق كامل الأهداف المرجوة من استخدام هذه الوسائل والأدوات التكنولوجية المتعلقة بالتحكم والسيطرة أي محاولة احتكار مصادر القوة السيبرانية.

ولهذا نجد أن معظم دول العالم قد استشعرت مخاطر الفضاء السيبراني، لذلك اخذت عديد الدول خطوات عاجلة من خلال تبني استراتيجية تقنية شاملة بغرض تطوير القدرات الوطنية في مجال أمن المعلومات والاتصالات، وقد تفطنت الولايات المتحدة الأمريكية إلى حجم التهديدات الذي يطرحه الفضاء السيبراني، فقامت باء دراجه في أجندة أمنها الوطني مند سنة 1996، وفي هذا الصدد أشار الرئيس الأمريكي الأسبق "باراك أوباما" إلى أن التهديدات التي تأتي من خلال الفضاء تطرح تحديات أمنية واقتصادية كثيرة، وذلك بالنظر إلى أن معظم الخدمات والبنى التحتية والمعلومات والأنظمة المالية ترتبط بالأنترنت.

كما كيفت الدول الأوروبية على غرار إستونيا وفرنسا، رؤيتها الأمنية مع التهديدات الجديدة بعد أن عرفت إستونيا هجوما إلكترونيا في سنة 2007 ، مسٌ مواقع حكومية وتضمن حرمانها من الخدمة (علاء الدين، عمارة، 2021، ص171)، ومن الملاحظ أن مفهوم الأمن القومي قد أخذ في التطور ليتعدى مفاهيم التهديدات التقليدية بحيث يشمل، التهديدات غير التقليدية المتعلقة بمختلف جوانب القوة الذكية، فقد اتسع مجاله ليمتد من الجانب العسكري لمجالات أخرى عديدة نظراً لبروز شكل جديد للقوة ألا وهي القوة الافتراضية والتي ترتكز على البيانات المرقمنة المرتبطة الكترونيا بالميدان المعلوماتي وفق فضاء مفتوح لا يعترف بحدود جغرافية ، ما يعني بعالمية الفضاء السيبراني الذي جعل السيادة الوطنية تسير نحو التأكل التدريجي في ظل تسارع عصر التقدم التكنومعرفي، وعليه يمكن القول أن هناك علاقة طردية بين تأثر سيادة الدول بمتغيرات الفضاء السيبراني والتغيير في مضمون الوظائف التي تقوم بها الدولة، كما يمكن القول أيضا أن هناك علاقة عكسية بين تقدم الدولة تكنولوجياً ومدى تأثرها بمتغيرات هذا الفضاء، فهناك دول مسيطرة وأخرى خاضعة ورغم أن كل الدول بغض النظر عن موقعها سوف تعاني بشكل أو بأخر إلا أن الدول الخاضعة تبقى الأكثر تأثيراً، لأن الدول القوية والمسيطرة تكنولوجيا تمتلك القدرة على توجيه مسارات التحول وتحدد قواعده وهنا يكمن واقع العلاقة بين حماية السيادة الوطنية وضرورة تحقيق الأمن السيبراني(بيرم،2020، ص812)، وترى أن واقع التهديدات الجديدة المرتبطة بالوسائل التقنية قد اوجدت واقعا جديداً أمام الدول بحيث أصبحت طبيعة

العنف متوارية، فوسائل التسلل والاختراقات وصل إلى نقطة أصبح فيها التمييز بين حالة الحرب واللا حرب أقل وضوحاً، بسبب انتهاج الفواعل لطرق بديلة عند الحرب المباشرة بين الدول أو بين الخصوم، وقد ساعد البراح السيبراني على انتشار القوة بين فاعلين متعددين، ومما لاشك فيه أن زيادة القوة القومية للدولة تتشابك فيه عناصر ومكونات الترابط القومي بصور مادية ومعنوية.

ولهذا نجد أن عناصر قوة الأمن القومي وعوامل تهديده ترتكز أساساً في أن عناصر القوة هي تلك الأسس التي تشارك في تحديد الأمن القومي للدولة وتمثل قاعدة عمل لها، ويمكن تحديدها في العنصر الجيوبولتيكي والديموغرافي والاقتصادي والسياسي والعسكري، في حين أن عوامل التهديد هي كل ما من شأنه تهديد القيم الداخلية للدولة وكيانها بفعل عوامل داخليه أو عوامل خارجية تشكل جوانب الضعف في كيان الدولة، ويمكن أن تستغلها القوى المعادية لتهديد الأمن القومي للدولة، والأمن القومي للدولة ينبع أساساً من معرفتها لمصادر قوتها ونقاط ضعفها والعمل على تنمية مصادر القوة والتغلب على عوامل الضعف (عبد الحفيظ، 2020،ص10)، ومن تداعيات الحروب السيبرانية على الأمن القومي تصاعد المخاطر السيبرانية والتي من اخطرها توجه الدول الكبرى نحو عسكرة الفضاء السيبراني، وذلك بتصاعد الاستثمار في مجال تطوير أدوات الحرب السيبرانية والذي يطلق عليها بالقوة الذكية والاستعداد لحروب المستقبل حيث تتبنى العديد من الدول استراتيجية حرب المعلومات باعتبارها حرباً للمستقبل، وترى الدول الكبرى أن من يحدد مصير تلك المعركة المستقبلية ليس من يملك القوة فقط، وانما القادر على شل القوة والتشويش على المعلومة (طالة، 2020،ص 59)، غير أن تحقيق الأمن القومي بشكل مطلق أمر لا يمكن تحقيقه مهما بلغت الدولة من قوة وتفوق خاصة في عصر الانكشافية المعرفية، لأن الأمن المطلق لأي وحدة سياسية يعنى التهديد المطلق لأمن كل الوحدات السياسية المجاورة، كما أن الأمن ليس بالحقيقة الثابتة الجامدة تصل إليه الدولة وإلى الأبد، فالأمن القومي كظاهرة جيوبولتيكية يتصف بالحركة والتغيير تبعاً لمجموعة من المتغيرات الجيوسياسية الدولية وكما وأن للظروف المحلية والدولية انعكاسات جوهرية حيال قضية الأمن، ومن ثم فأن ما تسعى إليه كل الدول عادة هو تحقيق الأمن القومي النسبي لها آخذه في الاعتبار أمن الدول المجاورة، أو تلك التي تدخل معها في علاقات وثيقة (عبد الحفيظ ، 2020، ص22).

وكمحاولة لدرء التهديدات التي تواجهها الدول في هذا الاطار وفي ظل زيادة الهجمات السيبرانية بين الدول بما يؤثر على أمنها القومي، سعت الدول فرادى ومجتمعة إلى بذل قصارى الجهد من أجل تطوير قدراتها، واتخاذ الاجراءات الوقائية الكافية لحمايتها من أي هجمات سيبرانية محتملة، حيث قامت بتشكيل وحدات الاستجابة لطوارئ الانترنت والهيئات الوطنية للأمن السيبراني، كما شكلت جيوشا سيبرانية لتقوم بمهام الدفاع والهجوم والحماية، أما في الجانب القانوني فطورت من منظومتها القانونية لتتلائم مع التهديدات الجديدة (بتصرف عن طالمة، 2020، ص 69).

وفي عصر الشبكات لم تعد الجغرافيا درعا للوقاية من التحديات العالمية حيث يتشاطر العالم اليوم هموما أمنية مشتركة، هي الأخطار السيبرانية، ولذلك أضحى التعاون هو النموذج الأمني الجديد في عصرنا هذا، حيث أصبح الأمن متشابكا بوتيرة متزايدة وأصبح الدفاع يتطلب مزيدا من العمل مع الدول والمؤسسات والمنظمات (جبور، 2017، ص 100).

الخاتمة:

لقد ساهم الفضاء السيبراني عن طريق العديد من آليات التفاعل في تغيير كل من حدود الزمان والمكان، فالمجال العالمي لشبكة الأنترنت أوجد نطاقا تفاعليا افتراضاً مفتوح لا يخضع لسيطرة وسيادة دولة واحدة ولا حتى مجموعة من الدول، لقد أثرت الانكشافية السيبرانية المليئة بالتهديدات والمخاطر على الأمن القومي للدول، فقد أسقط تدفق المعرفة الحواجز والحدود الأمر الذي جعل العالم يسبح في فضاء جديد يختلج بكميات كبيرة من المعلومات والمعرفة.

ومع تزايد اعتماد البشرية على خدمات الاتصالات والتقنية الذكية اكتسبت الصراعات الجيوسياسية الدولية بعدا إلكترونيا رقمياً، فالحروب السيبرانية التي تدور رحاها اليوم عبر شبكة الويب العالمية شكلت هاجسا استراتيجياً ومصدر قلق للدول، ما يضع مفهوم السيادة الوطنية على المحك.

توصلت الدراسة إلى مجموعة من الاستنتاجات نورد أهمها:

- أن مخاطر واثار الهجمات السيبرانية عديدة ومتنوعة وتمس مختلف مناحي الحياة فهي تؤثر على المجالات المدنية والعسكرية، وتهدد البنى الاجتماعية والاقتصادية والصحية والبيئية، وأصبحت اليوم مصدر قلق للكل على اعتبار أن تحقيق الأمن السيبراني وثيق الصلة بالحفاظ على الأمن القومي للدول.
- من خصائص الفضاء السيبراني تلاشي الحدود التقليدية للدول، حيث أسقطت تكنولوجيا الاتصالات والمعلومات مفهوم الحدود الجغرافية، فالشبكة العنكبوتية تجاوزت هذا المعنى حيث الانكشاف المعرفي الذي أوجد نشاطاً بشرياً مترابطاً سمح بتبادل المعلومات وتدفقها بسرعة وسهولة محولة العالم إلى قرية كونية صغيرة خالية من الحواجز والعراقيل.
- من أهم الصعاب التي تواجه السيطرة على المخاطر السيبرانية سهولة تمكن أي فرد أن يكون هو الجاني في الهجمات السيبرانية، وذلك لسهولة الحصول على ادوات الهجوم التي تتمثل في جهاز حاسوب مرتبط بخدمة الانترنت والذي عن طريقه يحدث الاختراق.
- نجد أن معظم دول العالم قد استشعرت مخاطر الفضاء السيبراني، لذلك اخذت عديد الدول خطوات عاجلة من خلال تبني استراتيجية تقنية شاملة بغرض تطوير القدرات الوطنية في مجال أمن المعلومات والاتصالات، وذلك باستخدام الوسائل والأدوات التكنولوجية المتعلقة بالتحكم والسيطرة أي محاولة احتكار مصادر القوة السيبرانية.

قائمة المصادر والمراجع:

1- جاد الرب حسام الدين، (2008)، الجغرافيا السياسية، الدار المصرية اللبنانية، ط1، القاهرة.
2- جبور منى الأشقر، (2007)، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت، لبنان.
3- خليفة إيهاب، (2020)، الحرب السيبرانية الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، العربي للنشر والتوزيع، ط ا، القاهرة.
4- عبد الصادق عادل، (2016)، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مكتبة، الإسكندرية وحدة الدراسات المستقبلية، الاسكندرية، مصر.
5- فونتر دانيال، (يونيو 2019)، الاستراتيجية السيبرانية، ترجمة أمين منير، عالم المعرفة، سلسلة كتب ثقافية شهرية يصدرها المجلس الوطني للثقافة والفنون والآداب، الكويت.
6- محمود خالد وليد، (سبتمبر 2013)، الهجمات عبر الانترنت: ساحة الصراع الالكتروني الجديدة، المركز العربي للأبحاث ودراسة السياسات، الدوحة، قطر.
7- منصور شادي عبد الوهاب، (2019)، حروب الجيل الخامس أساليب التفجير من الداخل على الساحة الدولية، العربي للنشر والتوزيع، ط ا، القاهرة.
8- العودي جلال فضل محمد، مقالات في الجريمة السيبرانية، https://www.noor،book.com
9- عبد الحفيظ علاء، (مارس 2020)، الأمن القومي المفهوم والأبعاد، دراسات سياسية، المعهد المصري للدراسات،www.EIPSS-EG ORG
10-محمود محمد سعد، الحرب السيبرانية ادواتها وقودها خسائرها، https://www.noor، book.com
11-الاتحاد الدولي للاتصالات https;//www.itu.int
12-بيرم فاطمة، (يناير 2020)، السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية: الصين نموذجا، المجلة الجزائرية للأمن الانساني، السنة الخامسة، المجلد05، العدد 01، الجزائر.
13-حسين حياة، (ابريل 2021)، الفضاء الإلكتروني وتحديات الأمن العالمي، مجلة العلوم القانونية والسياسية المجلد 12، العدد 01، الجزائر.
14-زروقة إسماعيل، (ابريل 2019)، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، المجلد10، العدد01، الجزائر.
15-طالة لامية، (2020)، التحديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجية مكافحتها، مجلة معالم للدراسات القانونية والسياسية، المجلد 4، العدد 02، الجزائر.

16-عبد الرحمن محمود علي، (يوليو2022)، الفضاء الإلكتروني وأثره على مفاهيم القوة والأمن والصراع في العلاقات الدولية، مجلة كلية السياسة والاقتصاد، المجلد السادس عشر العدد الخامس عشر، جامعة بني سويف، مصر.
17-علاء الدين فرحات- عمارة عمروس، (2021)، الفضاء السيبراني وتآكل مفهوم السيادة الوطنية، المجلة الجزائرية للدراسات السياسية، المجلد 08/ العدد02.
18-كلاع شريفة، (2002)، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الانسانية، المجلد 15/ العدد01، جامعة الجزائر3.
19- Rid Thomas، Cyberwar & Peace: Hacking Can Reduce Real World Violence، Foreign Affairs، Vol. 92، No. 6، November/ December 2013.
20- CapLan nathalie، Cyber war. The Challenge to National، Global Security Studies، Volume 4، Issue 1، winter 2013،