التهديدات السيبرانية وإشكالية السيادة: إعادة قراءة لسيادة واستفاليا

Cyber Threats and the Problem of Sovereignty: A Re-reading of the Sovereignty of Westphalia

د/عبد الغاني شرقي

جامعة امحمد بوقرة بومرداس (الجزائر)

a.chergui@univ-boumerdes.dz

تاريخ الارسال: 2023/02/20 تاريخ القبول: 2023/05/24 تاريخ النشر: 2023/06/04

ملخص : *أفرزت الثورة الرقمية الحديثة العديد من التغيرات التي شهدتها العلاقات الدولية إن على مستوى الفاعلين أو على مستوى الوظائف لكن أيضا حتى على مستوى المفاهيم السائدة في حقل العلاقات الدولية ،فقد أكسبت هذه الثورة الرقمية مفاهيم كالقوة والحرب والأمن والتهديد وميدان القتال والسلاح والحدود مضامين جديدة تختلف عما كان سائدا في السابق ،فأمام مفاهيم كالقوة السيبرانية والميدان الخامس الفضاء السيبراني والحرب السيبرانية والأمن السيبراني والتهديدات السيبرانية والحدود السيبرانية لن يستطيع مفهوم كالسيادة كما حددته مؤتمرات واستفاليا من مقاومة هذه التغيرات / التحديات، لذلك تهدف هذه الورقة البحثية إلى إعادة قراءة في سيادة الدولة كما أقرتها مؤتمرات واستفاليا بالنظر الى التهديدات الأمنية السيبرانية التي لها القدرة العالية على اختراق سيادة الدولة بل والإضرار بها في كل لحظة .*

الكلمات المفتاحية :*التهديدات السيبرانية ،الدولة ، السيادة الرقمية ،الحدود .*

Abstract*: The modern digital revolution has resulted in many changes in international relations, whether at the level of actors or at the level of jobs, but also even at the level of prevailing concepts in the field of international relations. In the face of concepts such as cyber power, the fifth domain, cyberspace, cyber warfare, cyber security, cyber threats and cyber borders, a concept such as sovereignty as defined by the Westphalia conferences will not be able to resist these changes / challenges, so this research paper aims to re-read the state sovereignty as approved by the Westphalian conferences Given the cyber security threats that have the high ability to penetrate the sovereignty of the state and even harm it at every moment.*

key words: *Cyber threats, the state, digital sovereignty, borders.*

1. مقدّمة :

لطالما عمل المفكرون السياسيون والفلاسفة والباحثون الأكاديميون على التأريخ لسيادة الدولة انطلاقا من المؤتمر الأوروبي الذي أقيم في منطقة واستفاليا من سنة 1648، هذا المفهوم الذي نظر للدولة باعتبارها مجموعة مؤسسات تمارس سلطتها في إطار مجال إقليمي معلوم الحدود السيادية ، وتتساوى في ذلك مع مجموع الدول المشكلة معها لمنظومة الدول الأوروبية آنذاك، وبصرف النظر على ما تلا تلك الفترة من تعميم لمبدأ المساواة في السيادة إلى خارج أوروبا إلا أنه ينبغي الإقرار ببروز العديد من التحديات التي وضعت مفهوم السيادة كما تصوره المؤسسون لسيادة واستفاليا على المحك، ليس فقط بفعل التدخلات الدولية واختراق السيادة غير التماثلي من جماعات ارهابية وجريمة منظمة وهجرة غير شرعية، إنما بفعل نمط جديد من التهديدات ممثلة في التهديدات السيبرانية التي خلقت فجوة كبيرة في سيادة الدولة ليس من السهل احتواؤها، هذه التهديدات التي تتخطى الحدود السيادية للدولة بل إنها تتحرر من قيود الجغرافيا وتخترق مؤسسات الدولة السياسية ،الاقتصادية ،المالية ، المجتمعية ، الثقافية بل وحتى الأمنية والعسكرية منها، وتسبب الكثير من الخسائر في مختلف القطاعات في حين أن منفذيها قد يكونو شخصا واحدا وقد يكونو مجموعة وقد يكونو دولة أو مجموعة دول، يوجدون في أماكن متفرقة من العالم دون أن يكلفو أنفسهم عناء التواجد داخل الدولة المهددة بالهجوم السيبراني ودون أن يطلقو رصاصة واحدة، وتتساوى في ذلك كل الدول بصرف النظر عنها قوية أو ضعيفة فكلها عرضة للإختراق السيبراني، فأمام هذا النمط من التهديد تسعى هذه الورقة البحثية إلى محاولة ربط العلاقة السببية بين النمط الجديد من التهديدات ممثلة في التهديدات السيبرانية ومفهوم سيادة الدولة القانوني والسياسي، وهدفنا البحثي يرمي الى معرفة مدى مواكبة مفهوم السيادة للتطورات الحاصلة في العلاقات الدولية المرتبطة بالتهديدات السيبرانية، أم أن مفهوم السيادة هو في حد ذاته بحاجة الى إعادة أشكلة كالتي حصلت في واستفاليا وبالتالي بحاجة إلى إعادة ترميم و إعادة قراءة، بحيث رأينا أنه يمكن مناقشة ذلك من خلال إشكالية فحواها: كيف ساهمت التهديدات السيبرانية في إعادة أشكلة مفهوم السيادة الواستيفالي ؟

-أسباب ودو افع اختيار الموضوع : لقد تراكمت لدى الباحث مجموعة من الأسباب والدوافع التي حفزته لاختيار هذا الموضوع والبحث في الإشكالات التي يطرحها ،نذكر منها :

السبب الأول يتعلق بحيرة معرفية لدى الباحث تأسست من خلال سؤال التوفيق بين مفهوم السيادة التقليدي القانوني المرتبط بالسيادة على الجغرافيا المادية للدولة، والنمط الجديد من السيادة المرتبط بفضاءات افتراضية مفارقة وغير محايثة للواقع المادي، ومن هنا يظهر الإشكال المعرفي الذي يبحث في مدى صلاحية مفهوم السيادة التقليدي في استيعاب تلك الفضاءات غير المادية .

السبب الأخر يتعلق بالبحث عن كينونة التهديدات الافتراضية ذاتها، فإلى أي مدى هي موجودة؟ ماهي تجلياتها على أرض الواقع؟ ثم هل مجهودات الباحثين والدول ينبغي أن تتجه نحو معرفة الفاعل للتهديد السيبراني، أم الاكتفاء فقط بحصر الأثار السلبية التي يتركها على الدول والمجتمعات حتى نقر بوجوده؟

محاولة البحث في مدى تأثير التهديدات السيبرانية غير المادية على السيادة المادية للدولة، من خلال الاطلاع على كيفية توغل التهديدات السيبرانية الى داخل جغرافية الدولة لتؤثر عليها سياسيا، إقتصاديا، إجتماعيا، ثقافيا، وحتى أمنيا وعسكريا.

وبناء على الأسباب والدوافع سالفة الذكر يتراكم لدينا سبب أخر يتمثل في البحث عن كيفية التأسيس لمفهوم السيادة الرقمية، وهل يمكن أن يكون بديلا عن مفهوم السيادة التقليدي أم مكملا له؟

-**أهداف المقال:** إن الهدف البحثي من المقال هو التفسير، إذ تسعى الدراسة التي بين أيدينا إلى محاولة الربط بين مفهومين/متغيرين إثنين، متغير التهديدات السيبرانية باعتبارها متغيرا مستقلا وهو طارئ جديد على الساحة الدولية وله تأثيرات ثورية على العديد من المفاهيم التي استدعت من الباحثين في العلاقات الدولية إلى إعادة مراجعة على غرار مفهوم سيادة الدولة التي تعتبر ضمن هذه الدراسة متغيرا تابعا، باعتبارنا نبحث عن التغير الطارئ على الحيز الدلالي لمفهوم السيادة، حتى يتحقق الارتباط الأنطولوجي بالواقع الذي يغطيه والذي أصبح من بين ملامحه التهديدات السيبرانية.

-**خطة الورقة البحثية:** وكمحاولة للإجابة على إشكالية الدراسة قمنا بتقسيم العمل إلى عنوانين كبيرين :

- التهديد السيبراني : التعريف ،الفواعل وأنماط التهديد .
- التحولات الدلالية في مفهوم السيادة : من السيادة الإقليمية الى السيادة الرقمية.

2 .التهديد السيبراني : التعريف ،الفواعل و أنماط التهديد

لقد عملت الدول تاريخيا على تطوير إمكانياتها وقدراتها المادية في مختلف القطاعات السياسية، الاجتماعية، الاقتصادية وحتى العسكرية سعيا منها لمواكبة التحديات التي يفرضها واقع العلاقات الدولية، وقد انحصرت تلك التحديات أو التهديدات في المضامين المادية للتهديد سواء كان تماثليا أو غير تماثلي ويمكن إحاطته بالملاحظة والقياس وبالتالي يمكن حصره واستيعابه.

إلا أن ما شهده العالم من ثورة في التكنولوجيات الرقمية والانترنت ارتقت بالمجتمعات الى عصر سيبري محمل بمفاهيم غير المفاهيم التي كانت سائدة والتي أثبتت عدم صلاحيتها لاستيعاب التحولات والتغيرات التي فرضها عصر التكنولوجيا الرقمية، إذ يعد مفهوم الفضاء السيبراني Cyber Space باعتباره فضاء افتراضيا انفلت من هيمنة مفهوم الجغرافيا المادية للدولة، من بين المفاهيم التي حظيت بالاهتمام الأكاديمي وكذا السياسي نظرا لأهميته التحليلية، وكذا باعتباره أحد المجالات التي تستثمر فيها الدول إمكانياتها وقدراتها لتحقق فيه مستوى من القوة يحقق أمنها وبقاءها إلى جانب المجالات الأخرى: البر، الجو، البحر والفضاء.

كما يعد مفهوم القوة السيبرانية Cyber Power أيضا أحد المفاهيم المهيمنة في عصر التكنولوجيا الرقمية، والتي تعني قدرة الدولة على تحقيق مستوى متقدم من اكتساب التكنولوجيا الرقمية وبنية

تحتية رقمية لديها القدرة على حماية المجتمع ومؤسسات الدولة ككيانات مادية، وكذا حماية المعلومات والبيانات الرقمية من الإتلاف والتي تعد من ملامح سيادة الدولة.

ولم يبق مفهوم القوة السيبرانية حكرا على الدولة الأقوى في النظام الدولي فقط، بل أصبح متاحا امتلاكها أمام الدول الضعيفة أيضا كما القوية، بالإضافة إل أن هذا النوع من القوة أصبح في متناول فواعل أخرى من غير الدولة، وبالتالي يلاحظ أن أي فاعل في النظام الدولي مهما كانت قوته ومهما كانت صفته القانونية إن كان فاعلا رسميا أو غير رسمي أصبحت لديه القدرة على امتلاك القوة السيبرانية، وهو الأمر الذي سبب الكثير من الحرج للدولة لكنه دفع بالباحثين والأكاديميين في مجال العلاقات الدولية إلى إعادة النظر الى أنطولوجيا النظام الدولي باعتباره بنية هيراركية بدلالة مفهوم الفرق في القوة الصلبة، إلى أنطولوجيا من نمط أخر تتوزع فيه القوة السيبرانية بين فواعل العلاقات الدولية، دولا كانت أو شركات أو جماعات إرهابية أو إجرامية أو أفرادا أو أحلافا ...، توزيعا أفقيا وليس تراتبيا، جعل من تلك الفواعل فواعلا متجاورة من ناحية حجم قوتها ولا تخضع لمنطق هيراركي .

ومع امتلاك الفواعل غير الدولتية خاصة الإجرامية منها القوة السيبرانية، أو استعمال الدول للقوة السيبرانية لأغراض غير مشروعة كالإضرار بأمن دول أخرى، أصبح العالم أمام نمط جديد من التهديدات تسمى بالتهديدات السيبرانية، فنحن اليوم أمام جرائم سيبرانية مكتملة الأركان من سرقة للأموال، النصب والإحتيال، تخطيط وتنفيذ عمليات إرهابية عبر المنصات الرقمية، الدعاية ونشر الأخبار المضللة، التعبئة الأيديولوجية للأفراد والجماعات، تخريب الملفات الرقمية والبيانات الشخصية والمؤسسية ...، أين تلاشى مع هذا النمط من التهديدات مفهوم الحدود السيادية المادية وأصبحنا أمام مفهوم السيادة الرقمية، إذ يمكن أن نتفهم هذا الحجم الهائل من التهديدات السيبرانية إذا ما علمنا أن شبكة الأنترنيت تتوفر على اكثر من 1مليار و700 مليون موقع الكتروني خلال سنة 2018، كما أن 95 بالمئة من الشركات الكبرى في العالم أقرت بتعرضها لعمليات القرصنة الالكترونية، وكذا حوالي 135 حكومة في العالم اتخذت اجراءات تخص الفضاء السيبراني والأمن الالكتروني. (طالة، 2020، صفحة 57)

وينجر على ما تقدم من مفاهيم مفهوم حروب الجيل الخامس أو الحرب السيبرانية التي من الصعب تقييدها، فهي أكثر سرية وأكثر اثارة للدهشة في نطاقها وفي أهدافها غير الواضحة، وفي النهاية يصعب تمييز بدايتها ولا نهايتها ولا تحديد الخصوم فيها.(Jan-Frederik Kremer, 2014, p. 6)

لذلك ظهر تحد لدى علماء السياسة والعلاقات الدولية لتقديم رؤى عميقة حول كيفية التأقلم من الناحية المفاهيمية والنظرية والتجريبية مع علاقة الفضاء السيبراني بالعلاقات الدولية المرتكزة على مفهوم السيادة التقليدي.

1.2 الفضاء السيبراني والتهديد السيبراني: مقاربة في المفهوم

1.1.2 الفضاء السيبراني: يرتبط المضمون اللغوي للفضاء السيبراني بكلمة الفضاء والتي تعني الفراغ أو المكان المتسع وغير المحدود، ومصطلح cyber أو السيبراني يقابله في اللغة اليونانية كلمة kibernetes بمعنى الطيار. (سعد، 2022، صفحة 698)

كما ارتبطت عبارة Cyber بأعمال Norbert Weiner في منتصف القرن العشرين الذي قدم تعريفا لها باعتبارها التفاعل بين الانسان والألة والذي يخلق بيئة وفضاء بديلا للإتصال، إذ يمكن وصف هذا الفضاء" بالوطن بلا حدود"، خاصة بعد ربط جهاز الكمبيوتر وأجهزة الإتصال المحمولة بالأنترنت أين تم إحداث عالم إفتراضي إلى جانب العالم الواقعي. (بيرم، 2020، صفحة 792)

وقد عرف الاتحاد الدولي للإتصالات الفضاء السيبراني باعتباره المجال المادي وغير المادي الذي يتكون من أجهزة الحاسب الألي والشبكات والبرمجيات وحوسبة المعلومات والمحتوى المقدم ومعطيات النقل والتحكم ومستخدمي كل هذه المكونات. (سعد، 2022، صفحة 699)

كما عرفه القاموس العسكري لوزارة الدفاع الأمريكية بأنه حقل عالمي في بيئة المعلومات المؤلفة من شبكة مترابطة من البيانات والبنى التحتية لتكنولوجيا المعلومات، تضم شبكة الأنترنت، الحواسيب، شبكات الإتصال، أنظمة المعالجة والتحكم. (بيرم، 2020، صفحة 793)

عرفته وزارة الدفاع البريطانية باعتباره بيئة تشغيل تتكون من شبكة مترابطة من البنية التحتية التكنولوجية الرقمية، بما في ذلك المنصات والأنترنت وشبكة الإتصال السلكية واللاسلكية والشبكات والنظم الحاسوبية وأنظمة الكمبيوتر، بالإضافة إلى المعالجات المدمجة ووحدات التحكم، والبيانات الموجودة فيها تمتد إلى المجالات المادية والإفتراضية والمعرفية. (سعد، 2022، صفحة 699)

وبناء على ما سبق ذكره فإن الفضاء السيبراني هو عالم مفتوح غير محدود، أكثر اتساعا يضم العالمين الواقعي والإفتراضي، يشمل أساسا ماديا مرتبطا ببنية تحتية قوامها أجهزة الإعلام الألي ومنظومات الإتصالات السلكية واللاسلكية، كما يرتبط بمجال افتراضي يتأسس بربط البنية التحتية بشبكة الأنترنت العالمية وما تحتويه من بيانات ومعلومات ونقلها في مختلف الجهات من العالم الإفتراضي، مع ما صاحب ذلك من إلغاء للمسافات بين المعلومة وبين متلقيها، فالعالم بذلك أصبح قرية صغيرة.

وبذلك يظهر أن الفضاء السيبراني يتكون من ثلاث أركان أساسية: (سعد، 2022، الصفحات 699-700)

-ركن تقني (مادي): وهو الذي يجعل الفضاء السيبراني ماديا وبلا حدود.

-ركن منطقي: وهو بمثابة الجهاز العصبي المركزي للفضاء السيبراني الذي يربط بين الأجهزة وحزم شبكة التوجيه.

-ركن معرفي: والذي يتكون من المعلومات التي يتم إنشاؤها ونقلها وتخزينها في الفضاء السيبراني.

وبذلك فالفضاء السيبراني بحكم أنه متسع ومفتوح ومتخط لعالم السيادة الواقعي، إضافة إلى كونه مجالا تكنولوجيا فهو فضاء سياسي، إقتصادي، إجتماعي، ثقافي، عسكري وأمني بامتياز وذو طبيعة لا مركزية، لذلك يمكن أمننة استعماله إذا تحول إلى تهديد للدولة والمجتمع.

فبحكم توغل التكنولجيا الرقمية في مختلف مناحي الحياة وبحكم امتلاكها من فواعل رسمية لكن أيضا من فواعل أخرى غير رسمية، جعلت الدولة ليست فاعلا وحيدا ولا وحدويا في هذا المجال، مع رقمنة مختلف قطاعات الأمن : الأمن الرقمي العسكري، الأمن الرقمي السياسي، الأمن الرقمي الإقتصادي، الأمن

الرقمي الإجتماعي، الأمن الرقمي الثقافي ...، وهو الأمر الذي خلق تحديا أمام الدولة القومية بحيث لابد أن تكون لديها القدرة على إثبات سيطرتها الرقمية وبالتالي إثبات سيادتها على كل أنواع الأمن سالفة الذكر، لأن الفضاء السيبراني فتح الأفق أمام ساحات سيادية عديدة للدول.

لذلك يتبادر لدينا سؤال تقليدي مفاده: إلى أي مدى يمكن للدول السيطرة على الفضاء السيبراني؟

2.1.2 التهديد السيبراني: يقصد بالتهديدات السيبرانية تلك الهجمات التي تتم باستخدام آليات وشبكات الانترنيت وأجهزة الحاسوب الآلي ،وتهدف الى إلحاق الضرر بالأجهزة والشبكات الالكترونية ذات الاتصال بالانترنيت . (جعفري، 2022، صفحة 247)

كما تعرف التهذيذات السيبرانية بأنها : فعل يقوض من قذرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي ،من خلال استغلال نقطة ضعف ما تمكن المهاجم من التلاعب بالنظام . (البهي، 2018، صفحة 209)

يظهر أن التهديدات السيبرانية تهدف إلى تقويض وهدم وتجاوز الجدران الرقمية التي تقوم بوظيفة حمائية كحواجز أمنية أمام التهديدات السيبرانية، بغرض سرقة المعلومات والبيانات أو الإكتفاء بالاطلاع عليها أو تخريبها أو حتى تغيير مضمونها، وكل ذلك بهدف إلحاق الضرر بالطرف الضحية.

وقد تأخذ الهجمات السيبرانية عدة أشكال منها: (البهي، 2018، صفحة 209)

-هجمات التجسس التقليدي باستخدام تكنولوجيا عالية الدقة، تهدف إلى القيام بهجمات سرية للاطلاع على البيانات والمعلومات المتعلقة بمؤسسات الدولة سواء المدنية منها أو العسكرية، ويمكن القيام بهذه الهجمات من طرف دول ما على دول أخرى بهدف تحقيق مكانة متقدمة في الصراع والتنافس الدولي، بحيث حلت التكنولوجيا الرقمية محل الوسائل التقليدية في عملية التجسس لأغراض مختلفة سياسية أو مالية أو دينية ومذهبية.

-القيام بهجمات لتخريب نظم معلومات الخصم سواء كانت مدنية أو عسكرية، وكذا نشر معلومات مغلوطة داخل نظم ذكائه، وفي ذلك تحقيق لأسبقية تكتيكية واستراتيجية للطرف القائم بفعل الهجوم.

-القيام بتعطيل نظم المعلومات الخاصة بالضحية ما يتسبب في توقيف عديد المؤسسات عن الإشتغال، كنظم المواصلات ونظم النقل والأنترنت وكل المؤسسات التي تعتمد التكنولوجيا الرقمية في أداء مهامها، ويكون لهذا النوع من الهجمات أثار وخيمة على اقتصاد الدولة يصعب التعافي منها بسرعة.

2. 2 طبيعة الفواعل في الفضاء السيبراني: إن الحديث عن طبيعة الفواعل الناشطة في الفضاء السيبراني يحيلنا إلى الإطلاع على ما قدمه رواد البراديغم التعددي" الليبرالي" في هذا الإطار، بحكم أن الدولة ليست هي الفاعل الوحيد إنما هناك فواعل أخرى إلى جانب الدولة اتخذت من الفضاء السيبراني أحد المجالات المعتمدة في تحقيق مصالحها، بل إن هناك من الفواعل غير الرسمية من تمتلك قدرات سيبرانية تتجاوز قدرات عدة دول مجتمعة، حيث حدد "جوزيف ناي Joseph S.Nye " مجموعة من الفواعل في الفضاء السيبراني تمثلت في:

-**الدولة:** فالدولة تمتلك القدرة على امتلاك التكنولوجيا الرقمية والتي تشاعد على القيام بوظيفتين اثنتين: (طالة، 2020، صفحة 60)

أ/ وظيفة الردع والدفاع السيبراني لمواجهة التهديدات السيبرانية التي تتعرض لها من أطراف أخرى ومحاولة إفشالها.

ب/ وظيفة الهجوم السيبراني على دول وعلى كيانات أخرى لتحقيق مصالح معينة.

-**الشركات متعددة الجنسيات:** ينبغي الإشارة إلى أن الشركات التي تمثل القطاع الخاص هي التي أسهمت في تطوير التكنولوجيا الرقمية خاصة الشركات التي أسست على أراضي الولايات المتحدة الأمريكية، لذلك فشركات مثل google، facebook، microsoft، apple، amazon تتجاوز قواها السيبرانية قوة العديد من الدول، لذلك تعد هذه الشركات لاعبا أساسيا في الفضاء السيبراني. (زروقة، 2019، صفحة 1019)

-**جماعات الجريمة المنظمة:** استفادت جماعات الجريمة المنظمة كثيرا من التطور الذي شهدته التكنولوجيا الرقمية في تنفيذ هجماتها سواء على الكيانات الرسمية ممثلة في الدول أو غير الرسمية، إذ تقوم بعمليات القرصنة السيبرانية واختراق الحسابات خاصة منها المالية بهدف سرقة الاموال، وكذا استفادت من الفضاء السيبراني في تجارة ونقل الأسلحة، تجارة المخدرات، تجارة (تسليع) الهجرة غير الشرعية، المتاجرة بالأعضاء البشرية، التهريب،.. وهو ماكان له بالغ الأثر على اقتصادات الدول. (طالة، 2020، صفحة 60)

-**الجماعات الإرهابية** أول ظهور للإرهاب السيبراني Cyber Terrorism كان في ثمانينات القرن العشرين عندما عرفه باري كولين Barry Collin بأنه:"هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها سعيا لتحقيق أهداف سياسية أو دينية أو أيديولوجية ،وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب التقليدي ". (العودي، صفحة 05)

كما عرفه جيمس لويس بقوله:"الارهاب السيبراني هو استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنى التحتية الوطنية مثل الطاقة ، النقل ،الاتصالات ،بهدف ترهيب الحكومة والمدنيين ". (العودي، صفحة 07)

إلا أن الظهور الرسمي للإرهاب السيبراني ارتبط بقيام الرئيس الامريكي الأسبق بيل كلينتون سنة 1996 بتشكيل هيئة حماية منشئات البنية التحتية الحساسة ،حيث خلصت هذه الهيئة إلى أن مصادر الطاقة الكهربائية والاتصالات اضافة الى شبكات الكمبيوتر ضرورية بشكل قاطع لنجاة الولايات المتحدة الامريكية لأنها تعتمد على المعلومات الرقمية وبالتالي تكون عرضة لأي هجمات إرهابية . (العودي، صفحة 05)

واستتبع ذلك قيام وكالة الاستخبارات المركزية بإنشاء مركز حروب المعلوماتية قوامه 1000 خبير أمن المعلومات يعملون على مدى 24 ساعة لمواجهة خطر الارهاب السيبراني، وانخرطت باقي المؤسسات الأمنية الأمريكية في العملية، وعقب هجمات 11 سبتمبر 2001 تم التوقيع على اتفاقية دولية لمكافحة الإرهاب السيبراني من طرف30 دولة في العاصمة المجرية بودابست عام 2001 .

وتستغل الجماعات الارهابية الفضاء السيبراني في عمليات التجنيد والتعبئة والدعاية وجمع الاموال والمتطوعين، كما تعمل على جمع المعلومات حول الاهداف العسكرية، كيفية التعامل مع الأسلحة وتدريب المجندين الجدد عن بعد . (طالة، 2020، صفحة 61)

–الأفراد القراصنة :لقد أعطت التكنولوجيا الرقمية للأفراد ووفرت لهم سبل امتلاك القوة السيبرانية التي منحتهم تأثيرا مضاعفا في القيام بعمليات القرصنة الرقمية، وأعطتهم الفرصة للولوج إلى الحسابات المالية والمؤسسية وحسابات الشركات، للحصول على أموال أو تخريب مواقع بعض المؤسسات، وبدون التكنولوجيا الرقمية لن يستطيع الأفراد الولوج المادي إلى داخل تلك المؤسسات، ويمكن إجمال الفواعل الممارسة للهجمات السيبرانية وأهدافها وكذا دوافعها في الجدول التالي :

جدول رقم01 : فواعل الهجمات السيبرانية

الجهة التي تقف وراء التهديد	الدوافع	الأهداف	الأمثلة
- دول قومية ، مجموعات ترعاها دول .	-جغرافية ، سياسية ، أيديولوجية .	-زرع الاضطراب ، التدمير ،تسبيب الضرر ، السرقة ، التجسس ،الكسب المالي .	-تلف البيانات الدائم ، الضرر المادي المستهدف ، تعطيل شبكة الكهرباء ، تعطيل نظام الدفع ، التحويلات الاحتيالية ، التجسس .
-مرتكبو الجرائم الالكترونية .	-الإثراء .	-السرقة ، الكسب المالي .	-سرقة الأموال النقدية ،التحويلات الاحتيالية ، سرقة بيانات الاعتماد .
-الجماعات الارهابية ،القراصنة ،التهديدات الداخلية .	-أيديولوجية الاستياء .	-الاضطراب .	-التسريبات ، التشهير ،الهجمات الموزعة لتعطيل تقديم الخدمة .

المصدر: المجلس الأوروبي للمخاطر النظامية " المخاطر السيبرانية النظامية ":

https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

من خلال الجدول المبين أعلاه تتحدد دوافع وأهداف الفعل السيبراني حسب طبيعة الفاعل، بحكم أن كل فاعل له مصالح تختلف عن مصالح الفاعل الأخر، فالدول القومية والمجموعات التي ترعاها دول تتراوح دوافعها بين الجغرافية والسياسية والأيديولوجية، في حين أن جماعات الجريمة المنظمة تنحصر دوافعها في الحصول على المال، أما الجماعات الإرهابية والأفراد القراصنة فإن دوافعهم أيديولوجية، لذلك اختلفت أهداف وسلوكات تلك الفواعل حسب ما ورد في الجدول أعلاه.

3.2 أنماط التهديد في الفضاء السيبراني :تضطلع الفواعل الممارسة للهجمات السيبرانية بعدة طرق تقوض بها سيادة الدولة وكذا سلامة الأفراد والجماعات ،فيمكن حصر تلك الطرق فيما يلي : (العودي، صفحة 9)

-**الطريقة الأولى: هجوم الحرمان من الخدمة** :وهو هجوم يهدف إلى تعطيل قدرة الهدف على تقديم الخدمات المعتادة ،ويتم استخدام هذه الطريقة ضد مواقع الانترنيت أو البنوك أو المؤسسات بمختلف أصنافها للتأثير عليها .

-**الطريقة الثانية: إتلاف المعلومات أو تعديلها:** ويتم ذلك من خلال الوصول إلى معلومات الضحية عبر شبكة الانترنيت أو الشبكات الخاصة والقيام بعملية تعديل البيانات المهمة دون أن يكتشف الضحية ذلك ،فالبيانات تبقى موجودة لكنها مضللة قد تؤدي الى نتائج كارثية .

-**الطريقة الثالثة :التجسس على الشبكات:** من خلال الوصول إلى شبكة البيانات والمعلومات بهدف الحصول على معلومات تتعلق بالأمن القومي .

-**الطريقة الرابعة: تدمير المعلومات:** من خلال تدمير كامل لأصول المعلومات والبيانات ويسمى هذا الفعل " تهديد سلامة المحتوى ".

3. التحولات الدلالية في مفهوم السيادة :من السيادة الإقليمية الى السيادة الرقمية :

لقد سعت الدولة على مر التاريخ إلى محاولة إثبات سيادتها إما في مقابل مواطنيها محليا من خلال ممارستها للسلطة على عموم الشعب من دون أن تكون هناك أي هيئة أو قوة أو سلطة أخرى موازية لها تنازعها سلطانها، مع ضرورة الإقرار بالاختلاف في نمط ممارسة السلطة بين دولة و أخرى ، أو في مقابل دول أخرى من خلال تأكيدها على حدودها الإقليمية السيادية المعلومة وغير القابلة للتنازل، ولأجل ذلك كان تعريف الفقه السياسي و القانوني للدولة السيدة باعتبارها دولة كاملة الصلاحية في ممارسة سلطاتها و لا تعلوها أي سلطة ، و تكون قراراتها نافذة على إقليمها.

و أمام التغيرات التي شهدها الواقع الدولي و من ضمنها التغير في أنماط التهديد وصولا إلى التهديدات السيبرانية – الافتراضية – والتي كان لها تداعيات عميقة على العديد من المفاهيم المسلم بقدرتها على التحليل في مرحلة من المراحل، يأتي هذا العنصر من الدراسة لمحاولة تتبع مدى قدرة مفهوم السيادة الواستيفالي على مواكبة التغيرات التي افرزها العصر السيبراني .

1-3 السيادة الرقمية في مواجهة التهديدات السيبرانية :

لقد ارتبط مفهوم السيادة الرقمية بالتغيرات الثورية التي أحدثها عصر التكنولوجيا الرقمية على واقع المجتمعات و الدول في الآن ذاته، إذ تم إعطاء مفاهيم كالحدود الجغرافية للدول و السيادة الإقليمية و الحرب و الأسلحة مضامين جديدة غير تلك التي كانت عليها، إذ أصبح لهذه المفاهيم بعدا سيبرانيا على شاكلة الحدود الرقمية ، الحروب الرقمية و السيادة أيضا أصبحت رقمية، وما يلاحظ للدارس أن الفضاء

الالكتروني قد قوض أقدم الفروق بين الدولي و المحلي، بين السلام و الحرب، لكن أيضا بين الفاعلين الحكوميين و غير الحكوميين من ناحية حجم القوة الرقمية الممتلكة، وهو الأمر الذي أحدث تغييرات عميقة في طوبولوجيا النظام الدولي و التي يحتمل الدخول معها في واستفاليا سيبرانية Cyber Westphalian. (Jan-Frederik Kremer، 2014، صفحة 6)

1-1-3 مفهوم السيادة في الفضاء السيبراني :

إن الانفتاح المفرط على الفضاء السيبراني و التطور الثوري للتكنولوجيا الرقمية وكذا تحولها إلى قوة موزعة في امتلاكها بين فاعلين رسميين و غير رسميين جعل الحدود السيادية للدولة حدودا مستباحة و مخترقة، وهو الأمر الذي جعل الدول تقارب الفضاء السيبراني باعتباره من قضايا السياسة العليا، إلا أنه ينبغي الإشارة ابتداءا أن التكنولوجيا الرقمية و الانترنيت قد ارتبطت في بادئ الأمر ارتباطا وثيقا بأمن الدولة، فكانت البحوث في هذا المجال تابعة للدولة وتشرف عليها أجهزة الاستخبارات و الأمن.

ومع نهاية الحرب الباردة فتح المجال أمام المهندسين و الشركات الخاصة للإشتغال في مجال التكنولوجيا الرقمية وسمح لها بالانتشار عالميا، وما واكب ذلك هو اقتناع النخب السياسية و الإقتصادية في عديد دول العالم بإمكانية الإعتماد على التكنولوجيا الرقمية في إيجاد حلول لمجموعة متنوعة من العلل الإقتصادية و الإجتماعية .

إلا أنه ينبغي الإشارة أن منذ فترة التسعينات و نهاية الحرب الباردة تجسدت الهيمنة الأمريكية على الأنترنيت مع مارافق ذلك من تبني المجتمعات وجهة نظر حرة و مفتوحة للإنترنيت، تجسد معايير الديمقراطية الليبرالية الأمريكية، بما في ذلك حرية التعبير و الوصول إلى المعلومات و رأسمالية السوق الحرة و التي في معظمها تنبع من رحم الهيمنة الإقتصادية الأمريكية لصناعة التكنولوجيا وعلى رأسها الأنترنيت، إلا أن هذا النمط من الهيمنة الأمريكية على التكنولوجيا يكرس هيمنتها على العالم الرقمي، وبالتالي يكرس هيمنة الو.م.أ على كل معلومة رقمية في كل دولة في العالم، الأمر الذي أدى إلى بروز بعض الأصوات المتزايدة عددا تبنت نهجا قائما على السيادة الرقمية، وتدعو إلى المشاركة المتساوية في الحوكمة الدولية للفضاء الإلكتروني، في مقابل عدم انخراط الدول في البحث عن الهيمنة السيبرانية و كذا عدم التدخل السيبراني في الشؤون الداخلية للدول الأخرى و الإضرار بأمنها القومي . (Broeders & Berg, 2020, p. 109)

وبالنظر إلى أن نسبة 80% من البنية التحتية المادية للأنترنت تتواجد على الأراضي الأمريكية وهو الأمر الذي كرس الهيمنة الأمريكية الرقمية على العالم، إذ أصبح لديها القدرة على تقويض سيادة الدول رقميا كأحد تجليات تلك الهيمنة، وهو الأمر الذي دفع بعديد الدول إلى السعي لتفادي أن تصبح مستعمرات رقمية للولايات المتحدة الأمريكية، كالصين، فرنسا، ألمانيا، روسيا...، والتي رأت بضرورة السيطرة على الفضاء السيبراني تحقيقا لمفهوم السيادة الرقمية حماية للدولة و المجتمع في مواجهة الهيمنة الرقمية الأمريكية . (بيرم، 2020، صفحة 802)

فقد اقترحت الصين مثلا في مؤتمر بودابست حول القضايا السيبرانية في عام 2012 خمسة مبادئ للتعاون الدولي في الفضاء السيبراني وكان أول تلك المبادئ هو السيادة، معرفة إياها باعتبارها حق كل دولة في صياغة سياساتها و قوانينها في ضوء تاريخها و تقاليدها و ثقافتها و لغتها وعاداتها .

وبربطها لهذا التعريف للسيادة بالفضاء السيبراني و الأنترنت فقد ذهبت إلى القول :"بما أن الأنترنت يقع تحت سلطة سيادة الدولة فإن الجميع داخل أراضي تلك الدولة ملزم بالإمتثال لقوانينها و لوائحها".

كما جاء على لسان الرئيس الصيني في إعلان Wuzhen في المؤتمر العالمي الأول للأنترنيت في 2014 قوله:"ينبغي علينا احترام حقوق كل بلد في تطوير و استخدام و إدارة الانترنيت، و الامتناع عن استغلال الموارد و القوى التكنولوجية لانتهاك السيادة الرقمية للدول الأخرى". (Broeders و Berg، 2020، صفحة 113)

لذلك نجد أن الصين قد قطعت أشواطا كبيرة في التأسيس لسيادتها الرقمية، فقد أصدرت في 2017 "قانون الأمن السيبراني" من أجل تنظيم وضبط الفضاء السيبراني لتحقيق ميزة حمائية للدولة و المجتمع، إذ يشير مفهوم الأمن السيبراني إلى التدابير المتخذة للحفاظ على المعلومات الإلكترونية آمنة من التلف ومن السرقة، كما يتجه الأمن السيبراني نحو حماية كل شيء من المعلومات الشخصية إلى الأنظمة الحكومية المعقدة.(Commission, 2022, pp. 1-2)

كما نجد دولة أخرى وفي إطار سياساتها الحمائية و التأسيس لسيادتها الرقمية قامت بالاستغناء عن محركات البحث التابعة للشركات الأمريكية، مثل فرنسا التي استغنت عن محرك البحث غوغل واستبدلته بمحرك بحث ألماني-فرنسي المسمى كوانت ، إضافة إلى عديد الإصلاحات الوطنية في الجانب الرقمي لمواجهة الهيمنة الرقمية الأمريكية. (بيرم، 2020، صفحة 802)

وفي اطار سعي الدول لترميم سيادتها المخترقة من خلال التأسيس لسيادتها الرقمية سعيا منها لاستيعاب الثغرة الرقمية التي كرست الهيمنة الرقمية الأمريكية على النظام الدولي ، نجد هذه الأخيرة – الولايات المتحدة الأمريكية – تعترض على فكرة نقل مفهوم السيادة الرقمية للفضاء السيبراني بحجة أن هذا الأخير من المشاعات العالمية ولا يصح بناء حواجز سيادية حول دخول وخروج المعلومات من وإلى الدولة، وفي ذلك دفاع للولايات المتحدة الأمريكية على دور المهيمن في النظام الدولي. (بيرم، 2020، صفحة 802)

من خلال ما تم سرده حول السياقات الواقعية و العملياتية التي حفزت الدول على ضرورة التفكير في بناء و تشييد نوع جديد من السيادة يتم الدمج فيه بين الواقعي المادي و الافتراضي ، فإنه يمكن تقديم التعاريف التالية لمفهوم السيادة الرقمية :

-السيادة الرقمية مجال قانوني تقني يتميز بمطالبات الدول و الشركات و الأفراد بالتحكم فيه ، كما تعني خضوع الفضاء السيبراني لمصالح وقيم الدولة، وبالتالي قدرة الأخيرة بالتحكم في مجالها السيبراني بما يضمن أنه يتبع ذات القواعد و المعايير و الإعتبارات الموجودة في المجتمع. (سعد، 2022، صفحة 703)

-كما يتم الربط بين سيادة الدولة وحوكمة الشبكات، إذ تعني أنها جهد من قبل الكيان الحاكم ممثلا في الدولة لإنشاء حدود على الشبكة الإلكترونية ثم ممارسة شكل من أشكال السيطرة، تكون غالبا في شكل إنفاذ للقانون على هذه الحدود . (سعد، 2022، صفحة 703)

-كما يتم تعريفها باعتبارها قوة الدولة و استقلالها و تحكمها وسيطرتها على بناها التحتية الرقمية، وكذا التقنيات والمحتويات والإتصالات الرقمية وكافة المسائل المرتبطة بالفضاء السيبراني وعلى صلة بالدولة. (بيرم، 2020، صفحة 802)

-لقد وصفت" Ronder Leyen" السيادة الرقمية في معرض حديثها على أوربا بقولها:"هي القدرة على التصرف بشكل مستقل عندما وحيثما يكون ذلك ضروريا ومع الشركاء حيثما أمكن ذلك". (Broeders و Berg، 2020، صفحة 12)

-السيادة الرقمية هي قدرة الدولة على التحكم في مصيرها الرقمي ، وذلك بالحفاظ على البيانات و الأجهزة و البرامج التي تعتمد عليها و تقوم بإنشائها .

ميز "وليام بريك Wiliam Brake "بين نوعين في السيادة : السيادة الدستورية (الرسمية) لدولة ما على أراضيها والتي تتساوى فيها كل الدول، والسيادة العملياتية والتي تعني فعالية الدولة في الإشراف و الرقابة على كل أراضيها، وبرأي "بريك" فإن هذا النوع من السيادة هو الذي تهدده الثورة الرقمية، وليس النمط الأول المحمي بالقوانين والمعاهدات و المواثيق الدولية . (الله، 2013، صفحة 8)

وإجمالا يمكن تعريف السيادة الرقمية بأنها قدرة الدولة على الحماية الرقمية لمؤسساتها ومجتمعها في مواجهة قوى الهيمنة في الفضاء السيبراني .

لكن وفي إطار سعي الدولة لتحقيق و بناء سيادتها الرقمية، هل ينبغي لها أن تقوم بأدوار وقائية و استباقية لتلافي أي أضرار يمكن أن تلم بها في الفضاء الرقمي؟

يقترح الخبراء في هذا المجال مفهوم"المناعة السيبرانية"التي تعني القدرة على الإحساس و الإستعداد بشكل وقائي لمواجهة التهديدات السيبرانية و مقاومتها سواء كانت تلك الأخطار متوقعة أو غير متوقعة، وتمكين القدرة على التعافي بسرعة من آثارها في الوقت المناسب .

ويساهم التحليل الاستباقي لنقاط الضعف على جميع مستويات البيئة الرقمية الداخلية في تقليل مقدار الضرر المادي والمعنوي الذي يلحق بالمؤسسات في مختلف القطاعات التي تشمل قطاع الطاقة، الخدمات المصرفية، البنية التحتية، الإتصالات، الرعاية الصحية، الأمن والدفاع، سوق الأوراق المالية، الخدمات الحكومية...، وتتطلب تطبيقات المناعة السيبرانية أن تخضع جميع الخدمات الفنية لإجراءات عديدة مثل: النسخ الإحتياطي للبيانات، إدارة الأزمات ، تحديد أصول البنية التحتية الرقمية و المناطق الأكثر عرضة للتهديدات، تحقيق التميز في البعد الإستباقي، والعمل على تطوير الإمكانات الرقمية لمواجهة التسارع في مستوى التهديدات و طرق عملها . (عبدالصادق، 2021، صفحة 78)

2.3 البعد المعياري للسيادة الرقمية: تبعا لما أقرته هيئة الأمم المتحدة فيما يتعلق بضرورة احترام سيادة الدولة في الفضاء السيبراني، مستندة في ذلك أن الفضاء السيبراني لا يوجد من دون بنية تحتية مادية من

خوادم وكوابل وأجهزة إتصال والتي توجد فعليا داخل الدول وتخضع لسيطرتها ورقابتها، ومنه يمكن اتخاذ ذلك كخلفية للحديث عن البعد المعياري للسيادة في الفضاء السيبراني.

ينبغي الإشارة إبتداء أن الفضاء السيبراني لديه بعض الميزات الخاصة، وبعبارة أدق يحتوي على عنصر افتراضي لا يتضح فيه جليا الارتباط الإقليمي، مما يجعل الأمر صعب التطبيق بالقياس بمبدأ السيادة الإقليمية، وفي الواقع في العالم المادي الأعمال التي يمكن أن تشكل انتهاكات لمبدأ السيادة الإقليمية هي التي تحصل عادة من خلال التوغلات الجسدية في أراضي دولة أخرى، وعلى عكس السياق التناظري ففي الفضاء السيبراني مفاهيم الإقليمية والمادية الملموسة غالبا ما تكون أقل وضوحا، ومع ذلك، مع الإعتراف بوجود إختلافات ذات صلة بين المادية والسيبرانية تعتقد غالبية الدول أن مبدأ السيادة الإقليمية لا يزال من غير الواضح في الوقت الحالي كيف سيتم تطبيقه في الفضاء السيبراني على وجه الخصوص، لأن هناك حاجة إلى مزيد من ممارسات الدولة لأجل خلق تقاليد سلوك تتضمن دقة في المواقف الوطنية المعبر عنها حتى الأن، وقد تم تقديم إجابتين لحد الأن على سؤال: متى يكون الأنترنت برعاية الدولة أداة لانتهاك سيادة دولة أخرى:(Tanzi, 2021, pp. 2-3)

1/ الأول يأخذ في الإعتبار الإنتهاكات الجسدية: أي الأنشطة التي ينفذها موظف حكومي موجود فعلا في إقليم الدولة الضحية.

2/ والثاني يشير إلى الإنتهاكات البعيدة: أي العمليات التي يتم تنفيذها من خارج إقليم الدولة الضحية، ولكنها تنتج أثارا سلبية في إقليم الأخيرة.

وبناء عليه، يعتبر انتهاكا للسيادة الإقليمية كل نشاط يستخدم وسائل إلكترونية لإحداث أثار ضارة تظهر على أراضي دولة أخرى.

الجانب الأخر الذي يحتاج إلى توضيح هو تحديد الإجراءات التي يمكن أن تصل إلى حد انتهاك السيادة، حيث هناك العديد من الصعوبات في تحديد مثل هذا السلوك في الفضاء السيبراني على خلاف المفهوم التقليدي للسيادة والتي لها دلالات إقليمية مادية راسخة، وذلك نظرا لأن الفضاء السيبراني غالبا ما يكون فيه مفهوم الإقليمية المادية الملموسة أقل وضوحا، إلا أنه تم اقتراح بعض الأساليب الممكنة لحل هذه المعضلة، وذلك بالتركيز ليس على انتهاك السيادة في حد ذاته إنما في الأثر المادي الذي يتركه ذلك الإنتهاك للسيادة، إذ يجب أن يتسبب إنتهاك السيادة في ضرر مادي للبنية التحتية السيبرانية أو فقدان الوظائف والمعدات التي تعتمد عليها، أو تعديل أو حذف المعلومات التي تنتمي إلى الدولة المستهدفة، أو التدخل في البيانات أو الخدمات الضرورية لممارسة الخدمات الحكومية، وبذلك يتم الربط بين الإفتراضي والمادي في محاولة لتحديد حدود السيادة في الفضاء السيبراني.(Tanzi, 2021, pp. 7-8)

يمكن الحديث على ثلاث مبادئ اساسية يقوم عليها مفهوم السيادة الرقمية: (Broeders & Berg, 2020, p. 117)

-**المبدأ الأول:** هو أن الحكومات الوطنية تتمتع بحقوق سيادية ضد الحكومات الوطنية الأخرى، وهذا المبدأ في المقام الاول هو رد على الإدعاءات الكونية لمؤيدي الإنفتاح على الأنترنت، عن طريق حجز الحق في

التحكم في جميع الأنشطة عبر الأنترنت الخاضعة للولاية القضائية للحكومة الوطنية، وهذا المبدأ يرفض تطبيق الحقوق العالمية في المجال الرقمي خاصة، بما في ذلك حرية التعبير وحرية الوصول إلى المعلومات.

-**المبدأ الثاني:** أن الحكومات الوطنية تتمتع بالسيادة الكاملة على جميع الجهات الفاعلة غير الحكومية في المجال الرقمي وغيره، سواء كانت هذه الفواعل محلية أو أجنبية، فيجمع هذا المبدأ بين مظهر التعددية المؤسسية ومظهر الحفاظ على درجة كبيرة من السيطرة السياسية.

-**المبدأ الثالث:** هو المساواة بين الدول في إدارة الأنترنت، فبموجب هذا المبدأ لا ينبغي لأي دولة أن تتمتع بسلطة أكثر من غيرها أو تسعى للهيمنة السيبرانية على باقي الدول.

ورغم أن الجغرافيا ليس لها دور ذو مغزى في عمل الأنترنت حتى لو كانت البنية التحتية الاساسية إقليمية، إلا أنه وتبعا للمبادئ الثلاثة سالفة الذكر يمكن النظر إلى الفضاء الإلكتروني باعتباره إمتداد للفضاء الحقيقي، وبالتالي فهو ليس أرضا خارج القانون.

3.3 جدوى التنظيم المحلي وممكنات التعاون في الفضاء السيبراني: نظرا لما أفرزه الفضاء السيبراني من تحديات أمنية على الدولة والمجتمع، فإنه تظهر الحاجة إلى ضرورة تفكير الدول في كيفية ضبط وتنظيم حيازة واستعمال التكنولوجيا الرقمية محليا، وكذا البحث عن ممكنات التعاون بين الدول في الفضاء السيبراني، والهدف من ذلك إعادة ترميم سيادة الدولة المخترقة بفواعل رسمية وفواعل أخرى غير رسمية، لذلك يتبادر السؤال: كيف يتم ضبط الفضاء السيبراني محليا؟ وما مدى قدرة الدول على تنظيم التفاعل فيما بينها دوليا؟

أ/ضبط الفضاء السيبراني محليا: يجب النظر إلى نوعين مختلفين من الضبط المحلي للأنترنت :

-**التنظيم الشامل:** كون أن انتشار الأنترنت يعتمد على المكونات المادية، فيمكن للحكومة التي تتحكم في هذه المكونات تنظيم الإجراءات المتبعة على الأنترنت، كما يمكن للدولة إنشاء شبكة هرمية ومن ثم السيطرة على بوابة الشبكة، ما يمكنها من إعادة إنشاء الشبكة الداخلية في أراضيها، وبالتالي تتحكم الدولة في وصول مواطنيها إلى المواد المتاحة في الفضاء السيبراني.

-**التنظيم عبر البرامج:** وهو شكل أخر من أشكال تنظيم المحتوى ويسمى بحاجز البرامج، حيث يكون تنظيم البرامج أكثر فعالية على مستوى جهاز التوجيه وعلى مستوى المستخدم النهائي، فعلى مستوى جهاز التوجيه يكون تنظيم الأنترنت عادة من خلال استخدام جدار حماية أو نظام شامل يتحكم في الشبكة. (S.Wu, 1997, pp. 651-652)

ومن بين الدول الرائدة في ضبط الحصول على الأنترنت وبالتالي تقليص حجم اختراق السيادة الرقمية للدولة هي الصين، حيث قامت بتطوير ما يسمى "الجدار الناري العظيم"، وهي ألية للرقابة على الأنترنت، وبموجبها حجبت الصين عددا من مواقع الأنترنت الأجنبية محليا، ومن خلالها تراقب حركة البيانات من وإلى الأنترنت.

كما يمكن الإشارة إلى نظم الرقابة الحكومية الصارمة على الأنترنت في كوريا الشمالية لمواجهة ما يسمى الإنكشافية السيبرانية، لينتج عن ذلك نمط جديد من المجتمعات عرفت "بمجتمعات المراقبة".) سعد , 2022, p. 705)

ب/ممكنات تنظيم التفاعلات الدولية في الفضاء السيبراني: أما على المستوى الدولي فإن معضلة التعاون بين الدول لتنظيم الفضاء السيبراني قائمة بشدة، وهي مرتبطة بعدم اليقين بين الدول بشأن الادوار والتكاليف المطلوبة لتحقيق أمن جماعي سيبراني، وترجع أسباب عدم اليقين تلك إلى إنكفاء الدول على ذاتها في تحقيق أمنها السيبراني ضمن حدودها الجغرافية وكذا ارتفاع مستويات عدم الثقة بينها، وذلك لارتباط الأمن السيبراني بالمصالح الحساسة للأمن القومي، وبذلك يصبح التعاون متعدد الأطراف لتنظيم الفضاء السيبراني أمرا غير محبذ لكنه أمر ضروري.

وفي إطار البحث عن إستراتيجية فعالة تتحقق في إطارها السيادة الرقمية للدول في الفضاء السيبراني يمكن الإشارة إلى التقرير الصادر عن مؤسسة كارنيغي للسلام الدولي في نوفمبر 2020 بعنوان: إستراتيجية دولية لزيادة حماية النظام المالي العالمي من التهديدات السيبرانية International Strategy To Better Protect The Global Financial System Against Cyber Threats، فرغم أن هذه الإستراتيجية مرتبطة بالقطاع المالي إلا أنها يمكن أن تنسحب على باقي القطاعات السياسي، الثقافي والمجتمعي، الإقتصادي وحتى الأمني والعسكري، بحيث تهدف هذه الإستراتيجية إلى محاولة تجميع لجهود الدول والحد من تشتتها في مواجهة التهديدات في الفضاء السيبراني وتحقيق سيادة رقمية للدول مجتمعة، وتعتمد هذه الإستراتيجية على أربعة مبادئ: (نيلسون، مارس 2021، صفحة 26)

1-على المستوى المحلي يجب على كل دولة الا تترك نظم الدفاع السيبراني قطاعية ومنفصلة عن بعضها البعض وكأنها ضمن مجتمعات مختلفة، فالمؤسسة العسكرية منفصلة في ذلك عن المؤسسة الأمنية وكذا عن المؤسسات المالية والمؤسسات الاقتصادية والأجهزة التنفيذية ...، فلكل قطاع استراتيجيته رغم عدم إمكانية مواجهة التهديدات ذات الطابع السيبراني بصفة إنفرادية، فهذا التشتت المحلي في نظام الدفاع السيبراني يعيق لا محالة التعاون الدولي، إذ أن المؤسسات المحلية ينبغي أن تشكل بنية دفاع سيبراني واحدة تسهم بالضرورة في زيادة قدرات تشكيل نظام دفاع سيبراني جماعي.

2-بحكم أن التهديدات السيبرانية عابرة للحدود فإن فرادى الدول لا تستطيع أن توفر حماية فعالة ضد التهديدات السيبرانية وبالتالي حماية سيادتها الرقمية، لذلك تظهر ضرورة التعاون الدولي في هذا الإطار.

3-أشارت الإستراتيجية بوجود بعض مبادرات الدفاع السيبراني المعزولة لبعض الدول والتي أثبتت نجاعتها محليا، فيمكن تعميمها وتدويلها.

4-يمكن أن يكون النظام الدفاعي السيبراني لحماية النظام المالي العالمي قاطرة لتعميمه على باقي القطاعات السياسية، الإجتماعية، الإقتصادية، الأمنية،...

4-خاتمة واستنتاجات:

لقد ظهر جليا من خلال الدراسة أن التهديدات السيبرانية وليدة الثورة الرقمية والمعلوماتية الجديدة قد أحدثت في الأن ذاته ثورة على مجموعة من المفاهيم المتداولة في حقل العلوم السياسية والعلاقات الدولية، والتي اعتبرت مضامينها راسخة لفترة زمنية طويلة على غرار مفهوم السيادة، أين أصبح من غير المجدي في ظل العصر السيبري الإكتفاء في عملية التحليل بالحديث عن الحدود الجغرافية المادية ولا القوة الصلبة العسكرية ولا التهديدات التقليدية أيضا، وهي كلها مفاهيم يتأسس عليها مفهوم السيادة التقليدي كما أقرته مؤتمرات واستفاليا في 1648، والتي لا تسعفنا مضامينها أثناء مقاربتنا لأنماط التهديد السيبراني الحديثة التي لا تولي أي اعتبار للسيادة الجغرافية للدولة، الأمر الذي دفعنا إلى محاولة تقصي التغيرات التي حملها مفهوم السيادة بدلالة التأثيرات التي أحدثتها التهديدات السيبرانية عليه، أين ظهر مفهوم السيادة الرقمية الذي يدمج في مضمونه المعياري بين الاعتبارين المادي والافتراضي.

وبناء عليه فقد خلصت الدراسة إلى مجموعة من النتائج يمكن حصرها فيمايلي:

- أثبتت التهديدات السيبرانية نسبية وعدم مطلقية مفهوم السيادة الواستيفالي، لذلك تم التأسيس لمفهوم السيادة الرقمية لاستيعاب تلك التأثيرات على مفهوم السيادة التقليدي.
- يتأسس مفهوم السيادة الرقمية على البعد الإفتراضي، أين يتعين على الدولة إمتلاك عناصر القوة الرقمية لاعتماد سياسات حمائية لحدودها الإفتراضية.
- تعد التهديدات الأمنية السيبرانية وإرادة الهيمنة الأمريكية على العالم الرقمي سياقا مناسبا للدول لإعادة ترميم مفهوم السيادة التقليدي حتى لا تكون عبارة عن مستعمرات رقمية.
- يعد انتهاكا للسيادة الرقمية للدولة كل فعل خلف أثرا سيئا على البنية التحتية للدولة سواء كان مصدره فواعل رسمية أو غير رسمية.
- لا يزال التعاون الدولي لمواجهة التهديدات السيبرانية صعب التحقق، كون أن الدول المسيطرة على التكنولوجيا الرقمية هي ذاتها مصدر من مصادر التهديد السيبراني.

5.قائمة المراجع :

- Attilia Tanzi .(2021) .*International Law and Cyber Space* .The Study Group co-Organised by The University of BolognaMilan;Westminister.
- Benedikt Muler Jan-Frederik Kremer .(2014) .*Cyber Space and International Relations Theory,Prospects and Challenges* . Boon: Center For Global Studies University of Boon.
- Dennis Broeders و ،Bibi van den Berg .(2020) .*Governing Cyber Space :Behavior;Power and Diplomacy* .The Netherlands: Universiteit Leiden.
- Europan Commission .(2022) .*Eu Policy on Cyber Defence* .Joint Communicaton To The European Parlament and The Council.
- Timothy S.Wu .(1997) .CyberSpace Sovereignty?-The Internet and The Intrnational System . *Harvard Journal of Law and Technology*،

- إسماعيل زروقة. (أفريل, 2019). الفضاء السيبراني والتحول في مفاهيم القوة والصراع. *مجلة العلوم القانونية والسياسية*.
- تيم مورر و أرثر نيلسون. (مارس 2021). التهديد السيبراني العالمي. *التمويل والتنمية*.
- جلال فضل محمد العودي. (بلا تاريخ). *أثر الإرهاب السيبراني على الأمن القومي*.
- رغدة البهي. (1, 2018). الردع السيبراني :المفهوم والإشكاليات والمتطلبات . *مجلة الدراسات الإعلامية*.
- عادل عبدالصادق. (2021). المناعة السيبرانية والتنمية المستدامةفي منطقة الشرق الأوسط وشمال إفريقيا. تأليف المعهد الأوروبي للبحر الأبيض المتوسط، *توقعات كبيرة:تعريف أجندة الأمن السيبراني عبر البحر الأبيض المتوسط*. المعهد الأوروبي للبحر الأبيض المتوسط .
- عبد الحليم فضل الله. (2013). علاقة المواطن بالسلطة في العصر الرقمي. مركز *علوم الانسان ومنظمة الأونيسكو* المركز الاستشاري للدراسات والتوثيق.
- عبدالله جعفري. (31 12, 2022). التهديدات السيبرانية وتأثيرها على الأمن القومي الجزائري. *المجلة الإفريقية للدراسات القانونية والسياسية*.
- فاطمة بيرم. (جانفي, 2020). السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية: الصين نموذجا. *المجلة الجزائرية للأمن الإنساني*.
- لامية طالة. (21 12, 2020). التهديدات والجرائم السيبرانية :تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها. *مجلة معالم للدراسات القانونية والسياسية*.
- مروة زين العابدين سعد. (2022). تأثير تغير مفهوم السيادة على الإختصاص القضائي في الجرائم السيبرانية. *المجلة الدولية للفقه والقضاء والتشريع*.