الأمن السيبراني للدول: بعد افتراضي لواقع مادي

Cyber security of States : The Virtual Dimension of Physical Reality

مراد شحماط[1]، لبنى جصاص[2]

[1] جامعة باجي مختار– عنابة، chahmat.mourad@gmail.com

[2] جامعة باجي مختار– عنابة، loubnadjessas@gmail.com

تاريخ الاستلام: 2023/03/14 تاريخ القبول: 2023/09/12 تاريخ النشر: 2023/10/31

ملخص:

يهدف هذا المقال إلى تسليط الضوء على الجوانب المختلفة لمفهوم الأمن السيبراني، وعلاقته برسم قوة الدول من حيث النطاق والفاعلية، والبحث في مدى ارتباط أمن الدول في القرن الحالي بالقوة السيبرانية في اتجاهيها الدفاعي والهجومي، وبهذا صار يشكل المجال الجوي والفضاء ساحتين للصراع والتنافس الدوليين لتحقيق الهيمنة وضمان الريادة، وتعاظم هذا التنافس مع تطور البرمجيات وتكنولوجيات الاتصال، وارتباط معظم الأنظمة الحيوية للدول بما في ذلك الأنظمة الدفاعية والاستخباراتية بالإنترنيت، ما جعل مفاهيم السيطرة على المجال الجغرافي الواقعي يستلزم السيطرة على الفضاء السيبراني، ودفع الدول إلى التهافت على ارسال الأقمار الصناعية وتشييد القواعد الفضائية قصد ضمان أمنها السيبراني. وعليه تعتبر القوة السيبرانية والاهتمام بالبحث العلمي من أهم عوامل تحقيق الدول لأمنها وقوتها المادية في القرن الحادي والعشرين.

كلمات مفتاحية: الأمن السيبراني، الإنترنيت، الثورة الرقمية، أمن الدول، القوة.

Abstract:

This article aims at highlighting different aspects of the cyber security concept and its relation to determining the power of the state in terms of scope and effectiveness. It also aims to explore to which extent a country's security in the present century is linked to cyber power in its defensive and offensive directions. thus, airspace and space became arenas of international conflict and competition for hegemony and leadership. This competitiveness has increased as software and communication technologies have significantly evolved. Moreover, most vital systems of states, including defense and intelligence systems, are linked to the Internet. This has made the concepts of control over the realistic geographical

field requiring control over cyberspace. It has also prompted states to shun satellite transmission and build space bases to ensure their cyber security.
Accordingly, Cyber power and interest in scientific research are considered among the most important factors in states to achieve their security and material strength in the twenty-first century.
Keywords: cyber security, Internet, the digital revolution, state security, power.

المؤلف المرسل: مراد شحماط ، chahmat.mourad@gmail.com

مقدمة:

عرفت العديد من المفاهيم في العلاقات الدولية تغييرات وتحويرات تبعا لتطور البيئة الدولية من حيث الفاعل ومن حيث موضوع التفاعل، أين تداخلت الأنساق الدولية وصار من الصعب بما كان الفصل بين ما هو شأن داخلي وآخر خارجي، لدرجة أن أصبح التحكم في سلوك الفرد ومن ثم المجتمعات والدول ممكنا دون الحاجة إلى الحضور المادي، فقط من خلال برامج افتراضية ومواقع الكترونية، وهو ما نتج عنه الحديث عن الثورة الرقمية التي يشهدها العالم حاليا وانجر عنها جملة من المفاهيم من قبيل التجارة الإلكترونية، والعملة الرقمية وتقاطعها مع شبكات الجريمة المنظمة، والتهديدات السيبرانية، والانكشافات الأمنية، والجرائم الالكترونية، والدبلوماسية الرقمية، والحكومة الالكترونية، وحروب الجيل الخامس وحروب الظل... وغيرها كثير، وهي مفاهيم ترتبط في شق واسع منها بمفهوم الأمن الذي أخذ أبعادا وتفرعات متعددة ،من بينها الأمن السيبراني، الذي يتعدى أمن الدولة إلى أمن الأفراد والجماعات، الشركات ومختلف التنظيمات، أين أضاف الفضاء الإلكتروني تعقيدات وأبعاد جديدة للأمن القومي والعلاقات الدولية، فظاهر هذا الأمن افتراضي يتم عبر الكمبيوترات والبرمجيات الالكترونية، إلا أن مخرجاته تترجم على أرض الواقع.

استنادا على ذلك نطرح الاشكالية التالية: كيف يؤثر الأمن السيبراني على واقع الأمن الوطني للدول؟

لمعالجة هذه الاشكالية نطرح الفرضيتين التاليتين:

1- الأمن الوطني للدول في القرن الحادي والعشرين يرتبط بقدراتها الدفاعية السيبرانية.

2- كلما حققت الدول أمنها السيبراني كلما كانت أقل انكشافية.

للبحث في الاشكالية المطروحة تم تخصيص ثلاثة محاور هي:

أولا: مفهوم الأمن السيبراني.. التعريف والمستويات

ثانيا: أبعاد الأمن السيبراني

ثالثا: الأخطار السيبرانية وانعكاسها على واقع أمن الدول

وخاتمة تشمل أهم نتائج البحث المتعلقة بمستقبل أمن الدول في عصر المعلومات.

أولا: مفهوم الأمن السيبراني

أشار "كوب **Cobb** "سنة 1999 إلى أن الفضاء السيبراني أضاف بعدا جديد وأكثر تعقيدا للعلاقات الدولية والأمن الوطني. واعتبر أن "النزاعات التي تنطوي على الفضاء الالكتروني هي أخطر التهديدات على الأمن القومي للأمم منذ تطور الأسلحة النووية"[1] ، فأين يكمن التعقيد؟ وأين يكمن التحديث؟

إن التعقيد الذي فرضته الثورة التكنولوجية والمعلوماتية أو الرقمية على مفهوم الأمن، دفع الباحثين إلى إعادة النظر في تعريف الأمن القومي للدول والأمن العالمي على حد سواء، فالبعد السيبراني سهل من اختراق الحدود وخلق مناطق نفوذ دونما الحاجة للوجود المادي، أما التحديث فيكمن في إضافة البعد الإلكتروني في علاقات الدول إلى جانب كل من المجال الأرضي والبحري والجوي والفضائي، فالتكنولوجيا الرقمية صارت تشكل متغيرا أساسيا في تحديد قوة الدول، وذلك بحكم اتصالها بمختلف القطاعات الاقتصادية المالية الصناعية أو الفلاحية، الأنظمة العسكرية، الصحية وحتى الثقافية الاجتماعية.

يشير الأمن السيبراني *إلى الأمن الإلكتروني فنقول **cyber attacks** بمعنى الهجمات الالكترونية، والفضاء الالكترونيcyber space ، وعليه الأمن السيبراني يهتم بأمن كل ما هو موجود ضمن هذا الفضاء، ويعرف الاتحاد الدولي للاتصالات الأمن السيبراني بـ: "مجموع الأدوات والسياسات والمفاهيم

الأمنية والضمانات والمبادئ ومناهج إدارة المخاطر والإجراءات والتدريبات، وأفضل الممارسات والضمانات التكنولوجية التي يمكن استخدامها لحماية البيئة السيبرانية والمستخدم والمنظمة بصورة عامة.[2] "

ويعرف أيضا بأنه: "عملية الحد من خطر الهجمات الضارة على برامج وأجهزة الكمبيوتر والشبكات من خلال استخدام أدوات كشف الاختراقات، ووقف نشاط الفيروسات ومنع الدخول غير المصرح به، وتأكيد الهويات وتمكين الاتصالات المشفرة" [3]، وعليه فالأمن السيبراني يتعلق بتأمين الدول والأفراد من مخاطر الاستخدام السلبي لتكنولوجيا المعلومات وما ارتبط بها من تقنيات.

وتشير المخاطر السيبرانية التي من شأنها تهديد الأمن إلى احتمال وجود تهديد وهشاشة داخل الفضاء الالكتروني للبلد، يضر بأمن وسلامة نظم المعلومات وهياكل البنى التحتية المعلوماتية الأساسية، والتهديد السيبراني يمكن أن يتطور إلى هجوم الكتروني من قبل جهة التهديد عبر استخدام برمجيات ضارة لتغيير الرموز، البرمجة الرقمية والمنطق الرياضي أو البيانات مما يؤدي لعواقب تخريبية تضر بسرية وسلامة وتوافر البيانات، وبالتالي تؤدي للتلاعب في نظم المعلومات والبنية التحتية للشبكة[4] ، وقد يكون التهديد يستهدف توجيه الرأي العام نحو اتجاه معين؛ خاصة باختراق مواقع التواصل الاجتماعي وإنشاء منصات في إطار ما يعرف بالذباب الالكتروني وغيرها من عمليات الاختراق.

وفيما ارتبط بعمل الأجهزة الاستخبارتية فقد وفر الفضاء الالكتروني عددا من المزايا الاستراتيجية التي سهلت عملها تمثلت في[5]:

–زيادة حجم البيانات والمعلومات المتاحة أمام صانع القرار.

–زيادة عدد الخيارات والبدائل ما يوفر لصانع القرار المرونة وحرية الحركة في تبني السياسات.

–تقليل تكلفة جمع المعلومات.

–تطور مفهوم الحرب والتحول نحو إلحاق الخسائر بدلا من وقوع ضحايا.

–حرب المعلومات التي تقودها أجهزة الاستخبارات تتميز بكونها ليست مقيدة في المجال والمدى، هدفها غير مأمون العواقب وقد يستغرق عدة دقائق، أطرافها متعددة، صعوبة تحديد هوية المهاجم واكتشاف الهجوم.

–سهلت الثورة الاتصالية بما تتيحه من برامج وتطبيقات على الأجهزة الاستخباراتية مراقبة تحركات الشعوب والمجتمعات وتوجهاتها؛ ناهيك عن سهولة توجيهها.

يختلف مفهوم الأمن السيبراني عن أمن المعلومات أين يشير هذا الأخير إلى أمن كل المعلومات سواء كانت الكترونية أو ورقية (الأرشيف الورقي)، فأمن المعلومات يشير إلى مجموع الإجراءات والتدابير الوقائية التي تستخدم للمحافظة على المعلومات وسريتها من السرقة أو الاختراق... ويشمل المحاور التالية[6]:

–حماية المعلومات من الضرر بمختلف أشكاله سواء كان مصدر هذا الضرر أشخاص كالمخترقين أو برامج كالفيروسات.

–حماية المعلومات من الوصول غير المصرح به أو السرقة أو سوء الاستخدام.

–حماية قدرة المنشأ على أداء أعمالها بأحسن طريقة آمنة.

–تمكين أنظمة المعلومات والبرامج من العمل بشكل آمن ومستمر.

بناء على ما تقدم نطرح التساؤل التالي: هل التهديدات السيبرانية تتم فقط عبر الأجهزة الالكترونية وداخلها وبالتالي الأمن يتوقف عند هذه الأجهزة؟ طبعا لا لأن هناك ارتباط وتداخل بين العالم الافتراضي والعالم الواقعي وبالتالي فأمن العالم الافتراضي يساعد على تحقيق أمن الواقع. فالعلاقات الاقتصادية والتجارية، طرق المواصلات والإشارات الضوئية، نظام الملاحة، الأنظمة التعليمية والصحية، منظومات التسلح دفاعية كانت أم هجومية تتم عن طريق الشبكة العنكبوتية وعبر برامج الكترونية؛ حتى أن المجتمعات ومصائرها صارت هي الأخرى تحدد وترسم عبر شبكات الكترونية، وهو ما يحتم على الدول وضع استراتيجية لحماية أمنها السيبراني.

استنادا على ذلك سارعت الدول بإنشاء مجموعة من الوكالات والمؤسسات على اختلاف تسمياتها قصد تأمين حدودها الالكترونية وتحقيق أمنها القومي من قبيل: وكالات حماية البنية التحتية المعلوماتية، مكافحة الطوارئ المعلوماتية، شرطة الانترنيت، هيئات الدفاع عبر الفضاء الالكتروني... إلخ، كما عملت الدول على تحديث وحدات داخل الجيوش للتعامل مع الحروب أو الجرائم أو الهجومات الإلكترونية [7]، وفي ذلك صارت تنحى الدول باتجاه الفعل الاستباقي والوقائي أكثر من الوقوف في وضعية المدافع.

وتكمن أهمية الفضاء الالكتروني في الصراع والتنافس الدولي في كونه يسمح للدول بتحقيق أهدافها بتكلفة أقل، يصعب معه إثبات المسئولية والفاعل، صعوبة التعقب والردع، وفي هذا الصدد أردفت سماح عبد الصبور ميزات الصراع السيبراني في النقاط التالية الذكر[8]:

- تخطي الصراع السيبراني لعديد الثنائيات التي تبرز في الصراعات التقليدية، فهو ساحة افتراضية لواقع جغرافي.

- زيادة الاعتماد الالكتروني في الأنشطة الحيوية للدول، ومنه صار استهداف هذه البنى يشكل أحد أبرز أوجه الصراع السيبراني.

- تماهي حدود الداخل والخارج، أين أصبحت الخدمات والمعلومات متاحة للجميع عبر شبكة واحدة، الأمر الذي قد يعرضها للاستهداف.

- صعوبة الردع الالكتروني التي تكمن في صعوبة رسم سيادة الدول ضمن هذه المساحة الافتراضية.

- غياب الشفافية الالكترونية والقوانين المقيدة للصراعات نتيجة صعوبة التعرف على هوية المعتدي، ناهيك عن أن خسائر هذا النوع من الصراعات لا تنجم عنها في حالات عديدة عنف ملموس؛ ما يعني عدم وجود هجوم مضاد أو استمرار الصراع.

وقد استعرض "نعوم تشومسكي" في مقال له موسوم بـ: "الأسلحة الصامتة للحروب الهادئة" مجموعة من الاستراتيجيات التي تتبعها أنظمة دولية أو محلية للقمع والتحكم في البشر، وحاليا في إطار ما يعرف بحروب الجيل الخامس تحظى كيفية السيطرة على العقول باهتمام عالمي واسع خاصة من قبل القوى العاملة

على الحفاظ على صدارتها الدولية، أو تلك الطامحة لاحتلال مكانة دولية، وفي هذا الإطار أشار مارك فيليبس إلى مصطلح التحكم بالعقل **Mind Control** ويعني به: "كيفية السيطرة على العقول ومساسها بحقوق الفرد الذي تمارس بحقه هذه المسألة... بداية من السيطرة على المعلومات الواصلة إلى الفرد وصولا إلى عملية غسيل الدماغ الكاملة، والتحكم في كافة مناحي سلوك وتفكير الفرد ثم تطبيق الأساليب التي أدت إلى هذه النتائج على مستوى عموم المجتمعات المستهدفة، وتشمل عمليات التحكم في العقل عدة مسارات منها ما يتعلق بتوظيف الإلكترونيات في القيام بوظائف الجسد الإنساني، ومنها ما يتعلق باستخدام الفضاء الإلكتروني في تتبع ومراقبة وتوجيه أنماط التفكير والسلوك..."[9] وقد أشارت دراسات عديدة إلى دور وسائل التواصل الاجتماعي في بروز وتوجيه الأحداث التي شهدتها المنطقة العربية في إطار ما عرف بالثورات العربية، وما ارتبط بها من دور الفاعل الخارجي، الذي برز من خلال منصات معينة دعمت أفكار تخدم مصالح وأهداف قوى دولية وأطراف داخلية في المنطقة.

وفي السياق ذاته أشار حلف الشمال الأطلسي في قمة لشبونة 2010 أن: "الهجمات الالكترونية أصبحت أكثر تواترا، وأكثر تنظيما وأكثر تكلفة، مما تسبب في الحاق الضرر بالإدارة الحكومية، قطاع الأعمال والاقتصادات، والنقل والتزويد ."[10] "

ومن المفاهيم الهامة ذات العلاقة بالصراع السيبراني وما شابهه نجد مفهوم الحرب السيبرانية **cyber war**, **cyber warfare**التي تبرز عند الحديث عن الأمن السيبراني، والتي تنبأت بها كتابات كل من **John Arquilla**, **David Ronfeldt** بمقال موسوم بـ **cyber war is comming**:سنة 1993، وعرفاها بأنها: "تنفيذ والاستعداد لتنفيذ العمليات العسكرية وفقا للمبادئ المعلوماتية، من خلال تعطيل إن لم يكن تدمير نظم المعلومات والاتصالات على أوسع نطاق، ويتوسع المفهوم ليشمل أبعادا غير مادية كتدمير العقيدة العسكرية للعدو"[11]وهذه الحرب قد تشن من قبل دول أو فواعل من غير الدول، كما قد تستهدف أهداف دول أو تنظيمات من غير الدول.

وتختلف أهداف الحروب السيبرانية وفقا لطبيعة أهداف الصراعات السيبرانية كما يلي[12]:

- صراع سيبراني ذو طبيعة سياسية تحركه دوافع سياسية وقد يأخذ شكلا عسكريا.
- صراع سيبراني ذو طبيعة ناعمة، يهدف للحصول على المعلومات والتأثير في المشاعر والأفكار وشن حرب نفسية وإعلامية.
- صراع سيبراني على التقدم التكنولوجي، الذي قد يمتد للسيطرة على الانترنيت وأسماء النطاقات وعناوين المواقع والتحكم بالمعلومات واختراق الأمن القومي للدول.
- صراع سيبراني على المعلومات والاستخبارات.

ثانيا: أبعاد الأمن السيبراني

إن كان الأمن يقصد به انتفاء الأخطار والتهديدات التي تمس سيادة الدول أو وجود الفرد وحقوقه، فما هي إذن التهديدات أو الأخطار التي تجابه الأمن سيبراني؟ قصد الإجابة على هذا السؤال يمكن القول أن للأمن السيبراني أبعادا يمكن تقسيمها إلى:

ابعاد ذات اتصال بأمن الدولة مباشرة: وهنا يبرز أكثر شيء مفهوم الهجوم السيبراني**–cyber attack*** سواء كان يحدث كصراع بين الدول أو عمل إرهابي أو إجرامي، هو هجوم في الفضاء الالكتروني بهدف المساس بنظام كمبيوتر أو شبكة أو تهديد الأنظمة المادية...وقد قسم كل من **Janczewski, Colarik** الهجمات السيبرانية أو الالكترونية إلى مراحل يعتبرونها شبيهة بمراحل الجرائم الجنائية التقليدية[13]، كما يعرف الهجوم السيبراني على أنه: "الإجراءات المتخذة لتقويض وظائف شبكة الكمبيوتر لغرض سياسي أو وطني" في حين الإدارة الأمريكية تستخدم الهجوم السيبراني ليتم تطبيقه فقط على الهجمات التي تتسبب في أضرار مادية للممتلكات أو إصابة الأشخاص[14].

دوليا تشتهر الولايات المتحدة الأمريكية، روسيا والصين بوحداتها الالكترونية العسكرية الماهرة، كما تعمل كل من فرنسا والكيان الصهيوني على تطوير القدرات السيبرانية، وحسب ضباط المخابرات الأمريكية فهناك من 20 إلى 30 جيشا يتمتعون بقدرات محترمة للحرب الالكترونية تتضمن تايوان، ايران، استراليا، كوريا الجنوبية، الهند، باكستان، والعديد من دول الناتو[15].

وتأخذ القوة السيبرانية الوطنية للدولة حسب"كلارك **Clarke** "و"كنيك **Knake** "ثلاثة اعتبارات هي: القدرات السيبرانية الهجومية، الاعتماد الوطني على الشبكات السيبرانية– الالكترونية (الدرجة التي تعتمد عليها البنية التحتية الحيوية للدولة على نظم الشبكة، ممثلة في: الكهرباء، السكك الحديدية، سلاسل الإمداد)، قدرة الأمة على التحكم في الفضاء السيبراني والدفاع عنه وفق تدابير مدروسة[16].

وبناء على ذلك قدم الباحثين مصفوفة لتراتبية مجموعة من الدول فسرا من خلالها لماذا الولايات المتحدة الأمريكية لا تشكل القوة المهيمنة في الفضاء الالكتروني رغم حيازتها على المرتبة الأولى من حيث القدرات الهجومية، إلا أنها تعرف تراجعا فارقا من حيث القدرات الدفاعية مقارنة بالصين مثلا، ومرد ذلك كون هذه الأخيرة تسيطر حكومتها على الشبكات التي تشكل بنيتها التحتية للإنترنيت، كما تتمتع الحكومة الصينية بسلطة ووسائل لإغلاق الجزء الصيني من الانترنت عن بقية العالم (حالة الأزمات، تعارض مع أي دولة)، وأكثر من ذلك تعزم الصين حاليا على مطالبة الشركات بالحصول على موافقة حكومية مسبقة لنقل البيانات التي تعد هامة إلى خارج البلاد؛ وكل ذلك يدخل ضمن حيز الحفاظ على الأمن القومي الصيني، في حين أن الولايات المتحدة الأمريكية لا تتوفر على ذلك كون اتصالاتها الالكترونية يسيطر عليها القطاع الخاص، ناهيك عن أن بنيتها الحيوية الداخلية تعتمد بشكل كبير على أنظمة في الفضاء السيبراني، ما يجعلها أكثر انكشافية، وأكثر عرضة للحرب الالكترونية من روسيا أو الصين[17].

أبعاد ذات اتصال بأمن المجتمعات: هناك برامج الكترونية تستهدف تغيير هوية الأفراد والتأثير ان صح التعبير على تركيبتهم الثقافية ومقوماتهم القيمية الحضارية، وهو ما يتناسب وأهداف حروب الجيل الخامس، أين يتم توجيه المجتمعات إما اتجاه ثقافة معينة أو خلق تباينات من شأنها تفكيك المجتمعات وفقدانها للانسجام يسهل معها لاحقا السيطرة على موارد الدول.

وتلعب وسائل التواصل الاجتماعي دورا بارزا في ذلك لاعتبارات بينها عادل عبد الصادق في النقاط التالية[18]:

- التأثير النفسي للمشاركين عبر الشبكات الاجتماعية، فقد نجح الفيسبوك في توفير الاحتياجات النفسية والعقلية والفكرية للمشاركين.
- التأثير الإنجذابي من قبل المشاركين، خاصة الباحثين عن تقدير الذات وتعزيز الثقة بالنفس وغيرها.
- عوامل البيئة المحيطة بعملية التفاعل، حيث تنعكس العلاقات الاجتماعية المتولدة في هذا الفضاء الافتراضي على الواقع، وهذا ما من شأنه التأثير على الرأي العام في المجتمعات وخلق اتجاهات فكرية موجهة.

ثالثا: الأخطار السيبرانية وانعكاسها على واقع أمن الدول

تتمثل أهم الأخطار السيبرانية في [19]:

- اختراق وتخريب البنى التحتية للاتصالات وتكنولوجيا المعلومات.
- خطر الإرهاب والحرب السيبرانية.
- هجمات إعاقة أو تعطيل الخدمات **Distributed Denial of Service Attacks ((DDSA**
- انتهاك الخصوصية وسرقة البيانات والهوية الرقمية.
- هجمات الفيروسات الخبيثة.
- الإعلام والدعاية المغرضة.

أما الواقع الدولي للأمن السيبراني يترجم في سياسات منفردة للدول وهناك بعض المحاولات لإيجاد صيغة موحدة وتشاركية للتعاون والتعامل ضمن الفضاء الرقمي، وفي ذلك وضع الاتحاد الدولي للاتصالات التابع للأمم المتحدة عام 2008 الأجندة العالمية للأمن السيبراني **Global Cyber security Agenda**، ومن خلالها تم تحديد معايير(المعيار التقني، المعيار القانوني، المعيار التنظيمي، معيار بناء القدرات، معيار التعاون) من خلالها ترتب الدول حسب مؤشر جاهزيتها للأمن السيبراني **Global security cyber index** يصدر في تقرير سنوي [20].

وفي عام 2016 تم نشر نموذج أوكسفورد لنضج قدرات الأمن السيبراني بواسطة مركز قدرات الأمن السيبراني في جامعة أوكسفورد، يقوم على تحديد مستويات متفاوتة لنضج الأمن السيبراني لدى الدول المختلفة بالاعتماد على خمسة أبعاد للقدرات ممثلة في: سياسة واستراتيجية الأمن السيبراني، الثقافة السيبرانية والمجتمع، الأمن والتعليم والتدريب والمهارات السيبرانية، أطر العمل القانونية والتنظيمية، المعايير والمنظمات والتقنيات. وكل واحدة من هذه الأبعاد ينقسم إلى عوامل ومؤشرات أكثر تحديدا تبين مستوى نضج قدرات الأمن السيبراني الخاصة بالدولة[21] .

من جهة هناك تعاون كبير بين الدول لمكافحة الجرائم العابرة للقارات التي تستغل العالم الافتراضي لتصريف أعمالها، وعلى سبيل المثال لا الحصر منذ عام 2009 قام مكتب التحقيقات الفيدرالي بإرسال وكيل خاص في سفارة الولايات المتحدة في أوكرانيا للمساعدة في التحقيقات المتعلقة بجرائم الإنترنت التي تستهدف الولايات المتحدة[22] ، إلا أنه من جهة أخرى يمكن لذات الدول أن تستغل هذا التعاون كقناة للرقابة والتجسس.

وفي نفس السياق، تعتبر النزاعات ضمن الفضاء أو الحيز السيبراني من أكثر التهديدات للأمن القومي، فبعد البر والبحر والجو والفضاء، دخلت الحرب المجال الخامس في ظل الفضاء الإلكتروني"[23] ، ومن النماذج البارزة عن نزاع دولي نشأ عن قضايا تتعلق بالأمن السيبراني، تسريب **Edward Snowden** لوثائق حول برامج المراقبة التابعة للحكومة الأمريكية، ورفض كل من روسيا والصين تسليمه للسلطات الأمريكية، وذات الأمر مع مؤسس موقع ويكيليكس **Julian Assange**[24] ، وفي ذات السياق أرجأت رئيسة البرازيل "ديلما روساف" زيارتها الرسمية للولايات المتحدة الأمريكية التي كانت مقررة في أكتوبر من عام 2013، وأعربت عن غضبها بسبب اعتراض وكالة الأمن القومي اتصالاتها الخاصة، واختراق شركة **petrobras** النفطية المملوكة للدولة. ناهيك عن التوترات الأخيرة التي طالت العلاقات الأمريكية الروسية بعد اتهام هذه الأخيرة بالتدخل في الانتخابات الرئاسية الأمريكية الأخيرة التي أفضت إلى فوز "دونالد ترامب".

أما الحروب السيبرانية فكانت إستونيا أول المستهدفين سنة 2007، عن طريق هجمات إعاقة خدمات الاتصالات وتكنولوجيا المعلومات (**DDOS**) خاصة في القطاع الحكومي والمصرفي، دام لعشرة أيام، وهناك أيضا فيروس "ستاكس نت"* **Stuxnet**، الذي اكتشف عام 2010 وجه لتعطيل منظومة التحكم في المفاعلات النووية الإيرانية، وأعلن عنه مرة أخرى في نوفمبر 2013 باختراقه مفاعل نووي روسي موجه لتوليد الطاقة الكهربائية، ناهيك عن الهجمات على عديد الشركات واختراق وقرصنة بياناتها[25] .

وهنا تبرز عدة تساؤلات وإشكاليات يطرحها الأمن السيبراني، أهمها:

– هل يرتبط الأمن السيبراني بصناعة المعرفة التقنية الحديثة، أم يكفي الدول امتلاكها لبرامج دفاعية إلكترونية؟ الإجابة عن هذا السؤال تقودنا بالضرورة إلى أهمية اضطلاع الدول بالعالم الالكتروني ووضعها لبرامج حمائية ذاتية وعدم الخضوع للبرامج المستوردة، الأمر الذي يبقي الدول في حالة تبعية وانكشاف سيبراني.

– علاقة الأمن السيبراني بمفهوم سيادة الدول: فمع انتشار الثورة الرقمية صار مفهوم الحدود يعرف ميوعة وتعرض مفهوم السيادة إلى مرونة خاصة مع تفاقم الاختراقات الالكترونية لحدود الدولة بمختلف مجالاتها. وهنا تطرح اشكالية أين يبدأ الأمن السيبراني وأين ينتهي؟ متى يتوقف أمن الدولة السيبراني؟

– يرجع التعاون المحدود فيما ارتبط بالأمن السيبراني إلى عدم وجود قواعد ومعايير المشاركة في المسائل المتعلقة بالفضاء الالكتروني، كما أن معظم الاقتراحات المتعلقة بتورط الدول القومية في الهجمات الالكترونية ضد البلدان الأخرى يتم استنتاجها عموما من الأدلة الظرفية، بدلا من الأدلة المباشرة والوقائعية والشاملة، مثال ذلك فيروس **stuxnet** الذي كان مبرمجا لتدمير أجهزة الطرد المركزي الإيرانية في الموقع النووي **Natanz** أين تم اتهام الولايات المتحدة الأمريكية وإسرائيل بوصفهما منشئي الفيروس، ومنه فإن الفضاء الالكتروني لا يسمح بتتبع الأصل الفعلي للبرنامج، كما أن الدول قد ترتكب انتهاكات أكثر

تكرارا في الفضاء الإلكتروني مقارنة بالفضاء المادي، لأن المنتهكين نادرا ما يعاقبون، كما أن أدلة الخصوم يسهل تشويهها[26] .

– كيف يشعر الفرد والدولة بأنهما مؤمنان سيبرانيا؟ كما المواجهات العادية هناك جبهات قتال وأخرى دفاع ومناطق انكشافية في الفضاء الالكتروني، والإشكال يكمن في كونها افتراضية يصعب جدا التحكم فيها وضبطها، وتأتي برامج التجسس الالكتروني على هواتف الأفراد باختلاف انتماءاتهم الاجتماعية، السياسية والاقتصادية في مراتب متقدمة من التهديدات السيبرانية، وكمثال على ذلك ما أثاره برنامج بيغاسوس[27] في عديد دول العالم.

– تثير مسألة الأمننة السيبرانية **cybernetic securitization** إشكال آخر فيما يرتبط بالحرية الالكترونية للأفراد والشركات، فالشبكة الالكترونية تضم في طياتها كم هائل من المعلومات الشخصية التي قد تتعرض للاختراق من قبل الحكومات بحجة الحفاظ على أمن الدول، كما قد يكون التضييق على حرية الفرد في الولوج إلى مواقع معينة أو منصات ما من خلال حجبها أو التقليل من حجم التدفق، وعدم توسيع الاستفادة من خدمة الانترنيت من باب حماية أمن الدول.

– القوانين الدولية والأمن السيبراني: هناك دعوات عديدة للبحث القانوني في مجال مكافحة الجرائم الالكترونية وطرق وآليات الحد منها، وكذا تدعيم التنسيق بين الدول، لكن السؤال الذي يطرح في هذا السياق يرتبط بمدى قوة تطبيق القوانين الناتجة عن الاتفاقات السيبرانية.

خاتمة:

لقد فرضت الثورة الرقمية على الدول يوما بعد آخر صدمات لا يمكن التنبؤ بها، كما أن المخاطر والتهديدات الالكترونية لا يوجد تحديد نهائي لها، ناهيك عن أن التباين في ذلك يطال الدول كل حسب درجة اعتمادها على الشبكة الالكترونية، وحتى النظريات والاستراتيجيات التقليدية لم تعد صالحة للتعامل مع أخطار الفضاء الالكتروني، خاصة ما تعلق باستراتيجية التخويف التي وظفت كثيرا أثناء الحرب الباردة، إلا أنه في تلك المرحلة كان هناك عدد محدود من الدول النووية وبالتالي الأعداء المحتملين محدودين عدديا، إلا أنه في الفضاء الالكتروني كل الدول تتمتع بإمكانية الوصول للأسلحة السيبرانية[28] .

ففي حين غيَّر امتلاك الأسلحة النووية من نمط الحروب التقليدية وأدى إلى بلورة جملة من النظريات الاستراتيجية خاصة ما تعلق بنظرية الردع، كما أخذت هذه الأسلحة النزاعات منحى آخر، حيث أشارت بعض الدراسات إلى تراجع أو تقلص عدد النزاعات ذات الطابع التقليدي فقط كنتيجة لامتلاك الأسلحة النووية والتلويح باستخدامها، إلا أن الوضع مع الأسلحة السيبرانية ليس مماثلا، فهناك ضرورة لإعداد نموذج جديد للأمن الدولي في عصر الانترنت، ومراجعة الاتفاقيات وسياسات الدول في مجال مكافحة الجريمة، خاصة في ظل بروز عوالم افتراضية تؤثر على العالم الواقعي ولا يمكن التأثير فيها؛ كالحديث عن ما يعرف بالشبكة المظلمة **dark web**. وعليه فأمن الدول سيكون مرتبطا مستقبلا بشكل كبير بامتلاكها للتقنية التكنولوجية الرقمية وقدرتها على الاستثمار في البحث العلمي والإنسان، وسيكون العالم الافتراضي هو الراسم لحدود الدول على أرض الواقع ووجودها المادي، فإن كان في وقت مضى من يسيطر على الأرض سواء كانت يابسة أو مسطح مائي يسيطر على العالم، فإنه في القرن الحادي والعشرين من يسيطر على العالم الافتراضي سيسيطر على العالم المادي.

التهميش:

[1] - Nir Kshetri: Cyber security and International Relations: The U.S. Engagement with China and Russia, p. 2.(25/03/2022),in:
https://bit.ly/2PhvLF9.

[*] –cyber لفظة يونانية الأصل مشتقة من kybernetes بمعنى الشخص الذي يدير دفة السفينة، ويرجع عديد المؤرخين أصل الكلمة لعالم الرياضيات الأمريكي نوربرتوبينر Norbert Wieners للتعبير عن التحكم الآلي. في وقتنا الحالي تعني التحكم في الحاسوب وعالم الكمبيوتر وما ارتبط بهما.

[2] – إيهاب خليفة: مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي (القاهرة: مركز المستقبل للأبحاث والدراسات المتقدمة، 2018)، ص.137

[3]– المرجع السابق، ص. 138.

[4] – مستشارية الأمن الوطني: استراتيجية الأمن السيبراني العراقي، ص4 (2022 /09/25) في الموقع : https://bit.ly/3yvAxoQ

[5] – عادل عبد الصادق: "الفضاء الإلكتروني والتحول في سياسات أجهزة الاستخبارات الدولية"، كراسات استراتيجية، العدد247، السنة23، (2013) القاهرة: مركز الأهرام للدراسات السياسية والاستراتيجية، ص11.

[6] – عدنان مصطفى البار، خالد علي المرحي: أمن المعلومات والأمن السيبراني، ص. 2. (09/18/ 2022)، في الموقع: https://bit.ly/3JBtcKE

[7] – عادل عبد الصادق، مرجع سابق، ص. 10

[8] – سماح عبد الصبور: "الصراع السيبراني.. طبيعة المفهوم وملامح الفاعلين"، في: "الصراع السيبراني" التنازع العالمي على قوة الفضاء الالكتروني، ملحق مجلة السياسة الدولية، القاهرة، مركز الأهرام، عدد 208، المجلد 52، أفريل 2017، ص 5.

[9] – عادل عبد الصادق، مرجع سابق، ص13.

[10] - Duie, V. Cvrtila, T. Ivanjko :International cyber security challenges , p. 1525. (22/09/2022), in : https://bit.ly/2va9Wk1

[11]– إيهاب خليفة، مرجع سابق. ص 146.

[12] – عادل عبد الصادق: أنماط "الحرب السيبرانية" وتداعياتها على الأمن العالمي، في: "الصراع السيبراني" التنازع العالمي على قوة الفضاء الالكتروني، ملحق مجلة السياسة الدولية، القاهرة، مركز الأهرام، عدد 208، المجلد 52، أفريل 2017، ص. 34.

[*] – إلى جانب الهجوم السيبراني هناك أيضا مفاهيم أخرى ذات صلة به نذكر منها: الجريمة الالكترونية cyber-crime، الشبكة السوداء Black Web.

[13] – I. Duie, V. Cvrtila, T. Ivanjko, Op. Cit, p. 1526.

[14] - Oona A. Hathaway, Rebecca Crootof, and others, The Law of Cyber-Attack ,California Law Review, Vol. 100, No. 4 (August 2012), p. 821.

[15] - I. Duie, V. Cvrtila, T. Ivanjko, Op. Cit, p. 1526.

[16] - Ibid, p1527.

[17] - Ibidem.

[18] – عادل عبد الصادق، مرجع سابق، ص. 20.

[19] – الاستراتيجية الوطنية للأمن السيبراني (2017-2021)، المجلس الأعلى للأمن السيبراني، مصر،ص ص.4،7. (بتاريخ:2022/09/24) في الموقع: https://bit.ly/2PlzuBM

[20] - Global Cybersecurity Index 2018,p 8.(26/09/2022), in: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

[21] – ميليسا هاثاواي: إدارة الخطر السيبراني الوطني، ص 7. بتاريخ 2022/02/19 . في الموقع: https://potomacinstitute.org/images/CRI/Managing-National-Cyber-Risks_FINAL-Arabic.pdf

[22] -Nir Kshetri, Op. Cit, p. 10.

[23] - Ibid, p. 2.

[24] - ibidem.

[*] – هو فيروس متنقل ويطلق عليه غالبا في وسائل الإعلام بـ "هجوم القراصنة"، ويتم تطبيق أساليب متطابقة لهجوم القراصنة للأغراض العسكرية والإرهابية.

[25] – استراتيجية الوطنية للأمن السيبراني (2017-2021)، مرجع سابق.

[26] -Nir Kshetri, Op. Cit, p. 4.

[27] – برنامج بيغاسوس Pegasus هو برنامج للتجسس الالكتروني منتج من قبل الشركة الاسرائيلية NSO، وحسب ما تدعيه هذه الأخيرة فإن البرنامج موجَّه للحكومات فقط لاستخدامها في أعمال مكافحة الإرهاب وإنفاذ القانون، وكان أول تصريح باستخدام البرنامج من قبل الحكومة المكسيكية عام 2011 لتعقب أباطرة المخدرات، كما تم استخدامه أيضا لتعقب الأشخاص المقربين من الصحفي السعودي المغتال جمال خاشقجي. Bhanukiran Gurijala: What is Pegasus? A cybersecurity expert explains how the spyware invades phones and what it does when it gets in. 09/08/2021. https://bit.ly/3wKlC8K ويلقى البرنامج حاليا العديد من الاتهامات المؤكدة باختراقه هواتف صحفيين ونشطاء حقوق الإنسان، إلى جانب مسؤولين سياسيين ودبلوماسيين في عدد من الدول. https://bit.ly/3DgLQly

[28] – I. Duie, V. Cvrtila, T. Ivanjko, Op. Cit, 1526.