الأمن السيبراني وتحديات الأمن العالمي بعد عام ٢٠٢٠

م. م محمد اسماعيل حماد

رئاسة جامعة النهرين

Email: mohammed.ismail@nahrainuniv.edu.iq

https//:doi.org/10.61884 /hjs.v14i58.756

ملخص :

يشير تصاعد التهديدات السيبرانية بعد عام 2020 إلى تحوّل عميق في بنية الأمن الدولي، حيث بات الفضاء الرقمي ساحة صراع تتجاوز قدرات الجيوش التقليدية وتعيد تعريف مفاهيم السيادة والردع، ومع تعاظم الاعتماد على البنى التحتية الرقمية، أصبحت الهجمات أكثر ترابطاً وتأثيراً في مؤسسات الدولة الحيوية وسلاسل الإمداد والمعلومات، كما أسهمت طبيعة الفاعلين الجدد وتراجع التعاون الدولي في تعقيد تحديد المسؤولية وتطوير أطر استجابة فعّالة، ويمثل هذا التحوّل انتقال القوة نحو من يمتلك القدرة على إدارة المخاطر والحوكمة والصمود السيبراني، ما يجعل الأمن الرقمي محوراً لإعادة تشكيل التوازنات في النظام الدولي المعاصر.

الكلمات المفتاحية: الأمن السيبراني، الردع، البنى التحتية، التحول الرقمي، التهديدات الهجينة

Cyber security and the Challenges of Global Security After 2020

Assistant Lecturer Mohammed Ismail Hammad

Office of the President – Al-Nahrain University

Email :mohammed.ismail@nahrainuniv.edu.iq

ABSTRACT

The growing escalation of cyber threats after 2020 indicates a profound transformation in the structure of international security. Cyberspace has increasingly become a domain of conflict that extends beyond the capabilities of conventional military forces and is reshaping fundamental concepts such as sovereignty and deterrence. With the expanding reliance on

digital infrastructures, cyber-attacks have become more interconnected and capable of exerting significant influence on critical state institutions, supply chains, and information systems. Moreover, the diversity of actors operating in cyberspace ranging from state to non-state entities—along with the decline in effective international cooperation, has further complicated the attribution of cyber-attacks and the development of effective response frameworks. This transformation reflects a shift in power toward actors capable of managing cyber risks, establishing effective governance mechanisms, and enhancing cyber resilience. Consequently, cyber security has emerged as a central pillar in the reconfiguration of power balances and strategic interactions within the contemporary international system.

KEYWORDS: Cyber security, Deterrence, Infrastructure, Digital Transformation, Hybrid Threats

المقدمة:

في عالم ما بعد ٢٠٢٠، أصبح الفضاء السيبراني محوراً للصراع تتجاوز حدوده التقنية والتكنولوجية الحديثة إلى رهانات استراتيجية تعيد تشكيل مفاهيم الأمن والسيادة والردع، وقد كشف الاتكال المتزايد على البنى الرقمية هشاشة عميقة في أدوات الحماية التقليدية، وفتح الباب أمام تهديدات لا تُقاس بثقل الجيوش ولا بعدد الأسلحة، بل بقدرة الفاعلين على التخريب الرقمي والتأثير في الأنظمة الحيوية للدولة، من المصارف والمستشفيات إلى شبكات الطاقة ومؤسسات صناعة القرار، وحتى المؤسسات العسكرية.

أصبح الأمن السيبراني، في الوقت الحاضر من أكثر الملفات إلحاحاً على الأجندة الدولية مع تصاعد حجم وتعقيد الهجمات التي تنفذها جهات لا حكومية ودول تسعى لأهدافها بوسائل غير تقليدية، باتت جهات المواجهة ملتبسة.

أهمية البحث:

تستمد هذه الدراسة أهميتها من ربط التحولات البنيوية في مشهد التهديدات ما بعد ٢٠٢٠ بإعادة تعريف مقومات الأمن القومي والأمن الجماعي، وانتقال النقاش من حماية تقنية موضعية إلى إدارة مخاطر نظامية تمس الاستقرار الدولي ومشروعية السلطة العامة، مع توضيح التحول في طبيعة الخطر من خلال إبراز انتقال الهجمات من اختراقات معزولة إلى مخاطر مترابطة تطال البنى التحتية الحيوية وحملات المعلومات، بما ينعكس مباشرة على أمن الدولة والنظام الدولي.

فرضية البحث:

تفترض هذه الدراسة أن الأمن السيبراني، منذ ٢٠٢٠، انتقل من هامش المعادلات الأمنية إلى مركزها، بحيث أصبح اختراق الفضاء الرقمي، وتعطيل البنى التحتية الحيوية، والتلاعب بالبيانات والمعلومات، أدوات مباشرة لإعادة توزيع النفوذ وإضعاف منظومات الردع التقليدية، وتستند الفرضية إلى أن تسارع التحول الرقمي، وتكدس الأصول الحساسة على منصات سحابية عابرة للحدود، وتداخل سلاسل الإمداد البرمجية، قد خفض كلفة الهجوم ورفع أثره الاستراتيجي، بينما بقيت إسنادات المسؤولية ومعايير الردع الدولية غير محسومة وبناءً عليه، تغدو القدرة المؤسسية على الحوكمة السيبرانية، وإدارة المخاطر، والصمود والاستجابة، معياراً محدداً لوزن الدول ومصداقية مؤسساتها، فإذا ثبتت صحة الفرضية، يُتوقع أن تظهر أنماط توازن جديدة تقاس فيها القوة بامتلاك البيانات، والسيطرة على البنى الرقمية.

اشكالية البحث:

تتمحور إشكالية الدراسة حول فهم الكيفية التي غيّر بها تصاعد التهديدات السيبرانية بعد عام ٢٠٢٠ بنية الأمن العالمي، من حيث قواعد الردع، وهندسة التحالفات، وأدوار الفاعلين من غير الدول، وتسعى إلى تحديد الأثر الفعلي لتلك التهديدات على الأمن القومي للدول عبر استهداف البنى التحتية الحيوية.

منهجية البحث:

تعتمد الدراسة على المنهج التحليلي من خلال تفكيك التغيرات الدولية المرتبطة بالفضاء السيبراني وربطها بالأطر المفاهيمية للأمن والسيادة كما توظف المنهج الاستقرائي لرصد التحولات في سلوك الفاعلين وتحديد أنماط الاستجابة الدولية لهذه التهديدات الجديدة.

هيكلية الدراسة

لغرض الإحاطة موضوع الدراسة فقد تم تقسيم المبحث إلى مبحثين، خصصنا المبحث **الأول للحديث عن التحولات في البيئة السيبرانية** وذلك في مطلبين **المطلب الأول، تصاعد التهديدات السيبرانية**، أما **المطلب الثاني تناولنا فيه الفاعلون الجدد في الفضاء السيبراني** وفي **المبحث الثاني نناقش تداعيات التهديدات السيبرانية على الأمن القومي** وهو الآخر يقسّم إلى مطلبين **المطلب الاول نبحث فيه عن التأثير على الأمن القومي للدول**، أما **المطلب الثاني: التحديات القانونية والدبلوماسية في ظل الفضاء السيبراني.**

المبحث الأول

التحولات في البيئة السيبرانية

مع التعمق المتزايد للاعتماد العالمي على الفضاء السيبراني وتحوله إلى مسرح محوري لتفاعل الدول والفاعلين من غير الدول، شهدت هذه الساحة تحولات بنيوية أثرت في النظام الدولي بأبعاده الأمنية والسياسية والاقتصادية ولم يعد الفضاء السيبراني طبقة رقمية تابعة للبنى التقليدية، بل أصبح بنية قائمة بذاتها تعيد توزيع عناصر القوة وتعيد تعريف مفاهيم التهديد والتأثير في العلاقات الدولية، لذلك يغدو فهم ديناميكيات هذا التحول مدخلاً حاسماً لقراءة ملامح النظام العالمي الراهن واستشراف مسارات تطوره المقبلة، **وعليه فقد قسم هذا المبحث إلى مطلبين، هما:**

المطلب الأول: تصاعد التهديدات السيبرانية.

المطلب لثاني: الفاعلين الجدد في الفضاء السيبراني.

المطلب الأول: تصاعد التهديدات السيبرانية

غدا الفضاء السيبراني ركناً محورياً في تشكيل النظام الدولي، لما يوفره من تقنيات فعّالة للحشد والتعبئة عبر العالم، ولقدرته على إعادة توجيه المنظومات والقيم السياسية. إن بساطة الاستخدام وانخفاض الكلفة ضاعفا أثره في شتى مجالات الحياة العامة، السياسية والاقتصادية والعسكرية والاجتماعية، وحتى على المستويات الفكرية والأيديولوجية ومن يحسن استثمار أدوات البيئة الرقمية ومواردها يغدو أقدر على بلوغ أهدافه وتشكيل سلوك الفاعلين المستفيدين منها ضمن تفاعلات القوة والتأثير الدولية المعاصرة اليوم[١].

من الأمور المتعارف عليها في العلاقات الدولية أن مصادر قوة الدولة وأشكالها تتغير، فإلى جانب القوة الصلبة ممثلة في القدرات العسكرية والاقتصادية تزايد الاهتمام بالأبعاد غير المادية للقوة، ومن ثم بروز القوة الناعمة التي تعتمد على جاذبية النموذج والإقناع، ومع ثورة المعلومات ظهر شكل جديد من أشكال القوة هو القوة السيبرانية التي لها تأثير كبير على المستوى الدولي والمحلي، فمن ناحية أدت إلى توزيع وانتشار القوة بين عدد أكبر من الفاعلين مما جعل قدرة الدولة على السيطرة موضع شك، ومن ناحية أخرى منحت الفاعلين الأصغر قدرة أكبر على ممارسة كل من القوة الصلبة والقوة الناعمة عبر الفضاء السيبراني، وهو ما

(١) اسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، المجلد ١٠، العدد ١، (الجزائر، ٢٠١٩)، ص١٠١٨.

يعني تغيراً في علاقات القوى في السياسة الدولية[١].

أصبح الفضاء السيبراني ساحة مركزية للصراعات والتجاذبات الدولية حيث تعتمد الدول على هذا الفضاء في إدارة بنيتها التحتية العسكرية والمصرفية والحكومية والتجارية مما جعله عاملاً رئيساً في تحقيق الأمن القومي وتعزيز النمو الاقتصادي غير أن هذا التوسع في الاعتماد على الفضاء السيبراني ترافق مع تحديات كبيرة أبرزها تنامي الهجمات السيبرانية التي باتت وسيلة فعّالة في تحقيق الأهداف السياسية والعسكرية وهذه الهجمات قادرة على إلحاق أضرار جسيمة بالبنى التحتية للدول المستهدفة ما يجعلها أداة فعالة في إدارة الصراعات الدولية[٢].

تجدر الاشارة أن الهجمات الإرهابية على الولايات المتحدة جسدت التغيير في تطور شكل الإرهاب الذي انتقلت المواجهة فيه من المجال المادي وبطريقة مباشرة إلى ما يعرف بالمواجهة غير المرئية وهذا بسبب بروز الفضاء السيبراني الذي ساعد على انتشاره واعطاءه أهمية كبرى بوصفه تهديد العصر فقد جعل الفضاء السيبراني الذي عرفته مجلة الإيكونيميست بالمجال الخامس للحرب بعد البر والبحر والجو والفضاء، اختراق الدول أمر سهل لأن سيادة الدولة في هذا الفضاء الافتراضي ناقصة في ظل عدم وجود قوانين وآليات تساعد على تنظيم استخدام هذا الفضاء[٣].

ما يؤكد على أن حروب اليوم لم تعد تعتمد على القوة العسكرية في تحقيق الانتصار ولا على الدول بوصفها فاعل وحيد وأساسي، حيث يشير في هذا السياق جاك دريدا "JackDerrida" إلى أن العالم سيشهد بدلا من الحروب التقليدية العسكرية حروباً جديدة تكنولوجية تعتمد بشكل كبير على شبكات الأنترنت التي لا نعرف فيها من يحارب ومن أجل من وكيف يحارب، وهذا بفضل ثورة المعلومات التي جعلت الإرهاب السيبراني عبارة عن حرب غير تماثلية من حيث طبيعة الفواعل - دولة ضد فاعل غير دولاتي - فضلا عن طبيعة الوسائل المستخدمة في القتال داخل هذا النوع من الحروب التي تم استبدال الدبابة فيها بما يعرف بالفيروس لتهديد مصالح العدو[٤].

(١) عباس بدران الحروب الالكترونية الاشتباك في عالم متغير مركز دراسات الحكومة الالكترونية، (بيروت، ٢٠١٠)، ص ٤.

(٢) خالد وليد محمود، **الفضاء السيبراني وتحولات القوة في العلاقات الدولية** الدوحة: (المركز العربي للأبحاث ودراسة السياسات: ٢٠٢٥)، ص ١١٢.

(٣) ربيع محمد يحي، اسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط دراسة حول استعدادات ومحاور عمل الدولة العبرية في عصر الانترنت، ٢٠٠٢/٢٠١٢ رؤى استراتيجية،٢٠١٣، ص٦٧.

(4) cyber terrorism, in:http://searchsecurity.techtarget.com/definition/cyberterrorism, Logged on:152025/10/

من أبرز التحولات السيبرانية في العقدين الأخيرين يتمثل في تنامي دور الفاعلين غير الدوليين الذين أصبحوا يشكلون تهديداً جدياً ومتزايداً في الفضاء الرقمي فقد تجاوزت التهديدات السيبرانية حدود الدول لتدخل في نطاق الحروب غير المتماثلة التي يقودها أفراد وجماعات منظمة وشركات خاصة تمتلك أدوات رقمية عالية التقنية وقدرات اختراقية هائلة[١].

هذه الجهات قد تكون مجموعات إجرامية منظمة تهدف إلى الكسب المالي عبر الابتزاز الإلكتروني وقد تكون جهات ذات دوافع سياسية أو أيديولوجية تتبنى أساليب الحرب السيبرانية لتعطيل مصالح دول معينة أو التأثير على الرأي العام المحلي والدولي أو حتى تنفيذ أجندات تخريبية تتجاوز المفهوم التقليدي للإرهاب إذ إن هذه الفواعل السيبرانية باتت تمتلك قدرة على تنفيذ هجمات سيبرانية تضاهي في خطورتها ما تقوم به بعض أجهزة الاستخبارات الحكومية.

وبالتالي أصبحت التحولات الأمنية السيبرانية ساحة جديدة للصراع بشكله التقليدي ولكنه ذو طابع سيبراني يعكس النزاعات التي تخوضها الدول أو الفاعلين من غير الدول على خلفيات دينية أو عرقية وإيديولوجية أو اقتصادية أو سياسية، ويتمدد الصراع السيبراني بداخل شبكات الاتصال والمعلومات متجاوزا الحدود التقليدية وسيادة الدول، حيث يكشف استخدام الفضاء السيبراني عن حالة التعارض الحقيقي للاحتياجات والقيم والمصالح بين العديد من الفاعلين، وساعد ذلك على ظهور أساليب جديدة للصراع الدولي، تباينت بين الطابع التقني والتجاري والاقتصادي والعسكري، إلى جانب ظهور طرق بديلة عن الحرب المباشرة بين الدول عبر شبكات الاتصال والمعلومات[٢].

فهناك صراع سيبراني تحركه دوافع سياسية، ويأخذ شكلا عسكريا، ويتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء السيبراني، ويوجد صراع سيبراني ذو طبيعة ناعمة، حول الحصول على المعلومات والتأثير في المشاعر والأفكار وشن حرب نفسية وإعلامية، كما يأخذ الصراع السيبراني طابعا تنافسيا حول الاستحواذ على سبق التقدم التكنولوجي وسرقة الأسرار الاقتصادية والعلمية، والتحكم بالمعلومات، والعمل على اختراق الأمن القومي للدول، كهجمات قراصنة الكمبيوتر والتجسس بما يكون له من تأثير على تدمير الاقتصاد والبنية التحتية بنفس القوة التي قد يسببها تفجير تقليدي مدمر، ويمكن أن يستخدم الفضاء السيبراني كوسيلة من وسائل الصراع داخل الدولة بين مكوناتها، على أساس طائفي أو اقتصادي أو ديني[٣].

(1) Alan Freedman et al, Cyber security and Cyber war: What Everyone Needs to Know(London: Oxford University Press 2014, p 36.

(٢) عادل عبد الصادق أسلحة الفضاء الالكتروني في ضوء القانون الدولي، سلسلة أوراق العدد ٢٣ مكتبة الاسكندرية، مصر، ٢٠١٦، ص ١٨-١٧.

(٣) اسماعيل زروقة، مصدر سابق، ص١٠٢١.

المطلب الثاني: الفاعلون الجدد في الفضاء السيبراني

شهد الفضاء السيبراني بعد ٢٠٢٠ بروز فاعلين جدد يتجاوزون الثنائي التقليدي دولة-جريمة، وفي مقدمتهم منظومات الجريمة كخدمة التي تتيح تأجير أدوات وهياكل الهجوم لغير المختصين، تتجلى هذه النماذج في ورانسوموير-كخدمة وسماسرة الوصول الأولي، ما خفّض عتبة الدخول، ووسّع قاعدة المهاجمين، ورفع تواتر الحوادث عالمياً، إلى جانب ذلك، تزايدت جماعات الهاكتيفيزم والفاعلون المدعومون من الدول ووكلاؤها، بما يعقّد الإسناد القانوني ويُربك قواعد الردع ومسارات المساءلة الدولية[١].

تجدر الاشارة أن الصين تعد الدولة الأولى التي أطلقت مفهوم الانترنت السيادي في العالم والمقصود هنا فرض سيطرة مطلقة من جانب الدولة على الشبكة العنكبوتية والتحكم ومراقبة تبادل المعلومات عبرها وحجب المواقع الخارجية المضرة بالأمن القومي الصيني، إذ إن عمل الشبكة العنكبوتية في الصين خاضع لما يسمى (جدار الحماية العظيم)[٢].

بدأت الصين بتنفيذ مشروع الجدار ١٩٩٨ وأنجزت جميع مراحل المشروع بحلول ٢٠٠٨ واستخدمت فيه تقنيات غربية متقدمة، إذ يقوم جدار الحماية بحجب المحتوى ومراقبة الفيديو والتعرف على الوجوه وفي عام ٢٠١٣ تم تشكيل مجموعة القيادة المركزية لأمن المعلومات التي تعمل تحت إشراف مباشر من الرئيس الصيني شي جين بنغ الذي أعلن عن مخطط تحويل الصين إلى قوة سيبرانية عظمى وهو مشروع طموح حقق خطى متقدمة في هذا المجال كما تهدف الصين إلى بناء نظام دفاع سيبراني متين، وقبل هذا المشروع كانت السياسة السيبرانية مبعثرة بين عدد من الدوائر الحكومية المختلفة وتم تأسيس إدارة الفضاء السيبراني الصينية ومهمته السيطرة على محتوى الإنترنيت وصيانة الأمن السيبراني والمشاركة في حكم عالمي للفضاء السيبراني[٣].

تستهدف الجماعات التي تستخدم الفضاء السيبراني البنى التحتية الحرجة في الطاقة والنقل والتمويل والأنظمة الرقمية، مع غلبة هجمات الفدية، وأساليب الهندسة الاجتماعية،

---

(١) منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، (بيروت، ٢٠١٧)، ص٢٥.

(٢) جدار الحماية العظيم: وهو مجموعة من الإجراءات القانونية والتقنية تهدف إلى جملة قرارات منها منع الأفراد من استخدام الشبكة لأغراض تضر بالأمن القومي، إسراء شريف جيجان، الامن السيبراني الصيني: دراسة في الدوافع والتحديات، قضايا سياسية، العدد ٥٦، (كلية العلوم السياسية -جامعة بغداد، ٢٠٢١)، ص٤١.

(٣) إسراء شريف جيجان، المصدر السابق، ص٤٢.

ويمتد الطيف ليشمل منظمات إجرامية عابرة للحدود، وإرهابيين يستغلون المنصات، وعناصر داخلية قادرة على تسريب أو تخريب أنظمة حيوية وتدعم الأسواق الإجرامية أنماطاً تسليعية للهجوم عبر تسويق بيانات مسروقة وأدوات جاهزة وخدمات دعم تقنية، ما يعمّق اقتصاد الجريمة ويسر تكرار الهجمات، وتفرض هذه التحولات توسيع أدوار الدولة والقطاع الخاص ومراكز العمليات الأمنية وتبني استخبارات التهديد وإدارة المخاطر المتكاملة لتعزيز الكشف والاستجابة وبناء الصمود[١].

وقد أصبحت الشركات التقنية الكبرى مثل جوجل وأبل ومايكروسوفت فاعلين رئيسيين في الفضاء السيبراني حيث تمتلك هذه الشركات بنى تحتية رقمية هائلة وبيانات ضخمة عن المستخدمين مما يمنحها قوة تأثير تتجاوز الحدود الوطنية وتلعب هذه الشركات أدواراً متعددة تشمل توفير الخدمات الرقمية وتطوير تقنيات الأمن السيبراني وحتى المشاركة في صياغة السياسات العامة المتعلقة بالفضاء الرقمي وقد أدى ذلك إلى إعادة تشكيل موازين القوى التقليدية في العلاقات الدولية[٢].

برزت مجموعات القراصنة والهاكرز كأحد الفاعلين الجدد في الفضاء السيبراني حيث تقوم هذه المجموعات بشن هجمات سيبرانية تستهدف مؤسسات حكومية وشركات خاصة وقد تكون هذه الهجمات بدوافع سياسية أو اقتصادية أو حتى ترفيهية وتتميز هذه المجموعات بقدرتها على العمل بسرية تامة وباستخدام تقنيات متقدمة مما يصعب من عملية تتبعها ومحاسبتها وقد أدى ذلك إلى زيادة التحديات الأمنية التي تواجهها الدول في الفضاء السيبراني[٣].

لم تعد القدرة على إحداث تأثير في الفضاء السيبراني حكرا على الدول، إذ باتت الكيانات غير الحكومية منظمات إجرامية، جماعات إرهابية، وناشطون سياسيون—تُحدث أثرا متنامي ومباشر في الأمن والاقتصاد والرأي العام عبر هجمات متنوعة الأدوات والمسارات، وتتراوح دوافع هذه الأطراف بين تحصيل مكاسب مالية سريعة، وتقويض الثقة العامة ومصداقية الحكومات، وإرباك عمل المؤسسات الحيوية، ضمن مشهد تتدنى فيه عتبات الدخول وتتوافر فيه أدوات هجومية جاهزة[٤].

---

(١) إيهاب خليفة، تأثيرات قوة الفضاء الإلكتروني على التفاعلات الأمنية في العالم، دورية اتجاهات الأحداث العدد ١،(المجلد ١، آب ٢٠١٤)، ص٢٣.

(٢) خالد وليد محمود، مصدر سبق ذكره، ص١١٠-١١٣.

(٣) (١٤) عمران طه عبد الرحمن، **الفضاء السيبراني في ضوء نظريات العلاقات الدولية، (لندن: المركز الديمقراطي العربي: ٢٠٢٤)**، ص١٠-١٢.

(٤) لبنى خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حمورابي، (العراق، المجلد ٠٨ العدد ٣٣-٣٤ ٢٠٢٠)، ص ١٤٨

يضاعف هذا الواقع تعقيد الردع السيبراني، لأن الإسناد الفنّي للهجمة إلى جهة بعينها يبقى إشكالا بنيويا يقيد المساءلة ويُربك معادلات الرد، كما تصبح جدوى الرد موضع تساؤل عندما يكون الخصم شبكي البنية وموزعا جغرافيا ويستفيد من تباين الأطر القانونية وضعف آليات الإنفاذ العابرة للحدود، ففي القانون الدولي، تُنسب أفعال الفاعلين من غير الدول إلى الدولة إذا ثبت أنهم خاضعون لتوجيهها أو سيطرتها أو تعليماتها، أو إذا أخلّت الدولة بواجب العناية الواجبة بمنع الأنشطة الضارة المنطلقة من إقليمها[1]،تؤكد هذه التعقيدات الحاجة إلى معايير إسناد أوضح وتعاون وإنفاذ دوليَّين للحد من الإفلات وتعزيز الردع.

المبحث الثاني

تداعيات التهديدات السيبرانية على الأمن العالمي

باتت التهديدات السيبرانية تُحدث أثراً مباشراً في بنية الأمن العالمي، إذ لم تعد حوادث معزولة بل موجات مستمرة تُقوّض الثقة في الأنظمة والمؤسسات وتعيد تشكيل تصوّرات المخاطر العابرة للحدود، وتتسارع الهجمات التي تطال مؤسسات الدولة الحيوية والقطاعات الاقتصادية الحساسة والبنى التحتية الأمنية والخدمية، فيما ترتفع درجة تعقيد الأساليب واحترافية الفاعلين بصورة تُصعّب الكشف المبكر والاستجابة المتزامنة، إذ تعوق ضبابية المصدر تحديد المسؤولية، ما يربك خيارات الردع، ويزيد كلفة الخطأ السياسي والقانوني والدبلوماسي، وتنعكس هذه الهجمات على العلاقات الدولية بتصعيد التوتر وفتح ملفات المساءلة ومن ثمّ لا تكفي المقاربات التقنية الصرفة لفهم المشهد، لأن التداعيات تمتد إلى كل ما يشكل تهديد أمني على أي دولة يطالها الهجوم السيبراني وباعتبار الأمن العالمي نظاماً مترابطاً، تنتقل الآثار عبر سلاسل الإمداد الرقمية والخدمات الأساسية والتجارة، فتتحول الأعطال المحلية إلى مخاطر نظامية واسعة التأثير، لذا تقتضي الدراسة إطاراً تكاملياً يلقي الضوء على المخاطر، واستخبارات التهديد،، وبناء الصمود المؤسسي للحد من الأثر وتعزيز الاستقرار عليه سنتناول في هذا المبحث مطلبين رئيسيين يعالجان أبرز تداعيات التهديدات السيبرانية على النظام الدولي، **تتمثل** في الآتي: تأثير التهديد السيبراني على الأمن القومي للدول، التحديات القانونية والدبلوماسية في تنظيم الفضاء السيبراني.

يعد التهديد السيبراني، إلى جانب التهديد السياسي والاقتصادي، أحد وسائل الحرب الناعمة التي تهدف إلى زعزعة نظام حكم أي دولة يطالها هذا التهديد، مما يشكل تهديداً للدولة

(١) ساعد بوقرص الأمن السيبراني مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة مجلة الأبحاث في الحماية الاجتماعية، (الجزائر، المجلد ٣، العدد ١، ٢٠٢٢)، ص ٦٥.

وسياساتها وثرواتها، و لشن هجماتها فإنها تستند على الشبكة العنكبوتية والتقنية الإلكترونية وتكنولوجيا المعلومات والاتصالات لغرض التجسس على أسرارها العسكرية والاقتصادية والعلمية والسياسية، والكشف عن معلومات مرتبطة بالوزارات والمؤسسات الرسمية والخاصة والقطاعات المالية، وتعزيز الحرب النفسية عبر الاستعمال الممنهج للدعاية والإشاعات والأكاذيب والخلافات الدينية والعقائدية للتأثير في عقول مواطني تلك الدولة المعادية، أو غير المعادية، وأفكارهم ومشاعرهم وآرائهم وسلوكياتهم لتوجيههم نحو الأهداف المطلوبة[١].

ولعل عملية شبكة العنكبوت الأوكرانية خير مثال على ذلك حيث غيرت من قواعد القتال العسكري بالتكنولوجيا الحديثة، إذ قامت بهجوماً متزامناً بالطائرات المسيّرة في ١ حزيران ٢٠٢٥ استهدف خمس قواعد جوية روسية بعيدة، مستخدماً ١١٧ مسيّرة أُدخلت وخُبئت داخل روسيا لإطلاقها من مسافات قريبة شتت الدفاعات مما يعطي دلالة إظهار فعالية مسيّرات منخفضة الكلفة وتأثيرها على معادلات حماية القواعد الجوية التقليدية[٢].

تعكس العملية علاقة الحرب بالطيف السيبراني، إذ استخدمت شبكات اتصال، توجها عبر الإنترنت، وعمليات اختراق-تضليل واتصالات مشفرة لتنسيق إطلاق المسيرات من عمق الأراضي الروسية من هنا تُبرز ثغرات أمنية في حماية القواعد والبنية الرقمية استهداف أنظمة الإنذار والقيادة والسيطرة عبر تشتيت المستشعرات وازدحام القنوات، ما يفرض هندسة دفاعية سيبرانية مادية مشتركة لرصد منصات الإطلاق المخفية ومنع اختراق الشبكات الداعمة. للتوقف غاية الحرب السيبرانية في الاستخدامات العسكرية بل تذهب الى ابعد من ذلك كاحتلال العقول، وسلب الدول مقدراتها، والحد من إمكانية تطورها ونهوضها لتظل راضخة سياسياً واقتصادياً وثقافياً وعسكرياً للدول المتطورة، إن الدول المتملكة عناصر قوة الحرب السيبرانية المتجلية بشبكات الاتصالات الرقمية، وتكنولوجيا المعلومات، والأجهزة الإلكترونية الحديثة، وظفت برامج الكترونية ذات قدرة عالية لتدمير أنظمة السيطرة المستخدمة من قبل بعض الدول المعادية، في تسيير بناها التحتية، وقد تكون النتيجة مشابهة لما تُخلّفه الحرب الكلاسيكية، وأسلحة الدمار الشامل، إن الحرب السيبرانية لا تميز بين المقاتل والمدني، أو بين الأعيان المدنية والعسكرية[٣].

(١) ماجد محمد الحنيطي، تكنولوجيا الصراعات الدولية المعاصرة الآن، (ناشرون وموزعون، ط١، عمان، الأردن)، ٢٠٢١، ص ٤١-٤٢.

(٢) د. إيهاب خليفة، الحرب في عصر الذكاء الاصطناعي، مقال متاح على الموقع الالكتروني: https://futureuae.com/ar/Mainpage/Item/10219 آخر زيارة ٢٠٢٥/١١/٧

(٣) محمد رمضان أبو شعشيع إيران. تركيا. إسرائيل وصراع القوى في الشرق الأوسط، (العربي للنشر والتوزيع، القاهرة مصر، ٢٠٢٣)، ص ٧٣.

فمن ناحية تأثير السيبراني العسكري تكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الإلكتروني، بما يسمح بسهولة تبادل المعلومات وتدفقها، وكذا السرعة وإعطاء الأوامر العسكرية والقدرة على إيصال الأهداف عن بعد وتدميرها، وقد تتحول هذه الميزة إلى نقطة ضعف لا قوة إن لم تكن شبكة الإلكترونية المستخدمة في ذلك مؤمنة جيدا من أي إختراق خارجي قد ينسب في شن هجمات إلكترونية مضادة على شبكات القوات المسلحة وأجهزة الاستخبارات، ومن ثم تجسس على الأمن العسكري للدول وتعطيل قدرة الدولة على النشر السريع لقدراتها وقواتها، أو قطع أنظمة الإتصال في ما بين الوحدات العسكرية وتعطيل شبكات الكمبيوتر، كما يمكن أن يتم شل وتعطيل عمل أنظمة الدفاع الجوي أو التوجيه الإلكتروني فضلا عن إمكانية فقدان السيطرة على وحدات القيادة[١].

ومن الناحية السياسية فتقوم أبعاد الأمن السيبراني على أساس حماية نظام الدولة السياسية وكيانها، حيث يمكن أن تستخدم التقنيات في بث معلومات وبيانات قد يحدث من خلالها زعزعة لاستقرار أمن الدول والحكومات حيث تصل بسرعة فائقة إلى أكبر شرائح من المواطنين بغض النظر عن صحة البيانات والمعلومات التي يتم نشرها، كالتسريبات المختلفة للوثائق الحساسة التي تؤدي إلى مشكلات كبيرة جداً على المستوى الخارجي والدولي، كما أنه لا أحد ينكر الدور المتعاظم لشبكات التواصل الاجتماعي على المستوى السياسي مثل: حملات إنتخابية، تظاهرات افتراضية، حركات إحتجاجية إلكترونية، كما يتم استغلال هذه المواقع من طرف العديد من الحكومات لتمريرها[٢].

وإذا ألقينا الضوء على بعض الهجمات السيبرانية، نجد شواهد عديدة في الواقع، من أبرزها الهجوم على البرنامج النووي الإيراني بفيروس (ستاكسنت) عام ٢٠١٠، الذي استُخدمت فيه أدوات الفضاء السيبراني لتحقيق أهداف صراعية على أرض الواقع بين طهران من جهة، والقوى المناهضة لمشروعها النووي، ولا سيما (إسرائيل) والولايات المتحدة، من جهة أخرى، ولا يختلف الأمر عند النظر إلى الترابط المنطقي بين استخدام المتظاهرين أدوات الفضاء الإلكتروني خلال الثورات العربية عام ٢٠١١، حيث كانت تلك الأدوات وسيلة فعّالة للحشد وتعبئة الشارع في مواجهة الأنظمة الحاكمة[٣].

(١) منى الأشقر جبور، مصدر سابق، ص ٢٩.

(٢) ماجد عزيز إسكندر، التوظيف السياسي للهجمات السيبرانية ومخاطرها على الأمن القومي، مركز الإمارات للدراسات والبحوث الاستراتيجية، (أبو ظبي، دولة الإمارات العربية المتحدة، الطبعة الأولى، ٢٠٢٣)، ص ٩.

(٣) د. خالد حنفى علي، إشكاليات تداخل الصراعات السيبرانية والتقليدية، مجلة السياسة الدولية، العدد ٢٠٨-المجلد ٥٢، (مؤسسة الأهرام، القاهرة، ٢٠١٧)، ص٤.

يُلاحظ كذلك توظيف أساليب القرصنة والاختراق الإلكتروني للتأثير في المجال العام داخل المجتمع الأميركي، بغية توجيه النقاشات والحوارات المرتبطة بالسياسات الداخلية، وما تلاه من اتهامات أميركية لروسيا بمحاولات استهداف أنظمة التصويت الإلكتروني خلال الانتخابات الرئاسية التي فاز فيها المرشح الجمهوري دونالد ترامب على منافسته الديمقراطية هيلاري كلينتون، إلى جانب اتهامات أخرى لموسكو باختراق رسائل كلينتون الإلكترونية بقصد التأثير في موقفها الانتخابي وصورتها لدى الناخبين[١].

أصبح الفضاء السيبراني ساحةً جديدة للصراع والمواجهة بين الدول والتنظيمات ومن أمثلة ذلك استخدام تنظيم القاعدة والولايات المتحدة كوسيلة للقتال وتبادل الهجمات المعلوماتية، وفي عام ٢٠٠٧ شهد العالم أولى العمليات العدائية الواسعة في الفضاء السيبراني بين إستونيا وروسيا، تلتها هجمات مشابهة عام ٢٠٠٨ خلال الحرب بين روسيا وجورجيا، وفي عام ٢٠١٢، تعرّضت شركة النفط السعودية (أرامكو) لهجوم سيبراني ضخم أدى إلى تدمير نحو ٣٥ ألف جهاز كمبيوتر بهدف تخريب صادرات النفط السعودية، وقد نسبت وكالة الاستخبارات الأمريكية الهجوم حينها إلى إيران، كما تكرّر المشهد عام ٢٠١٦ عندما استهدفت هجمات سيبرانية عدداً من الوكالات الحكومية السعودية، إلى جانب منظمات في قطاعات الطاقة والصناعة والنقل، وامتد التأثير ليشمل الهيئة العامة للطيران المدني، ما أبرز تصاعد استخدام الفضاء السيبراني كأداة استراتيجية في النزاعات الإقليمية والدولية [٢].

في ضوء ما تقدم نجد انه رغم اختلاف غرض وهدف كل حالة من الحالات السابقة، إلا أنه من الواضح أن حجم الهجمات السيبرانية يتزايد بشكل حاد، ولذا يصعب تحديد حجمها الحقيقي وبخاصة أن عديد منها لا يتم التبليغ عنه وتتمثل القواسم المشتركة بين تلك الحالات في صعوبة تحديد مرتكبي تلك الهجمات على وجه الدقة، وصعوبة معرفة الدولة الراعية لهذه التهديدات وغياب الرد المضاد، كنتيجة لها والأهم أنها ليست حكرا على الدول المتقدمة ذات أنظمة المعلومات الهائلة والمتطورة فحسب مما يزيد المشهد تعقيداً ويقوض وسائل الردع.

الخاتمة

ويتضح من كل ما سبق في ظل التغيرات المتسارعة التي شهدها العالم بعد عام ٢٠٢٠ أصبح الأمن السيبراني أحد المفاتيح الحاسمة لفهم منظومة الأمن العالمي الجديدة فقد

(١) د. ابتسام على حسين، فرص وقيود الأطراف المتنازعة على «المجال العام السيبراني، مجلة السياسة الدولية، العدد ٢٠٨-المجلد ٥٢، (مؤسسة الأهرام، القاهرة، ٢٠١٧)، ص١٣.

(٢) د. رغدة البهي، الردع السيبراني، المفهوم والإشكاليات والمتطلبات، مجلة الدراسات الإعلامية -المركز الديمقراطي العربي العدد الأول (القاهرة، كانون الاول ٢٠١٨)، ص٢١١.

تحولت الفضاءات الرقمية من مجرد منصات تواصل وتبادل معلومات إلى ساحات فعلية للنزاع والتأثير والاختراق وهو ما أفرز أنماطاً غير تقليدية من التهديدات التي لا تستهدف فقط البنى التحتية التكنولوجية، بل تمس جوهر السيادة الوطنية واستقرار الدول من الداخل منذ عام ٢٠٢٠ وغدا الأمن السيبراني مفتاحاً تفسيرياً رئيساً لفهم منظومة الأمن العالمي الناشئة؛ إذ انتقلت البيئات الرقمية من منصات للتواصل وتبادل البيانات إلى ساحات فعلية للصراع والتأثير والاختراق، بما أفرز تهديدات غير تقليدية لا تطال البنى التقنية وحدها، بل تمس جوهر السيادة واستقرار الدول من الداخل، ولم يعد مفهوم القوة حبيس أدواته الصلبة، بل بات يقاس بقدرة الفاعلين على امتلاك مفاتيح السيطرة على الفضاء السيبراني وتوجيهه، وقد أظهرت أحداث حديثة هشاشة أنظمة متقدمة أمام عمليات دقيقة بدوافع سياسية واقتصادية وأيديولوجية، بما يفرض الانتقال من منطق صدّ الهجمات إلى بناء بيئات رقمية مرنة وقابلة للصمود، فلا لا تعترف هذه التهديدات الرقمية بالحدود الجغرافية، إذ أصبح الأمن السيبراني مسؤولية جماعية تستلزم تعاونا متعدد الأطراف وصياغة أطر قانونية تتجاوز تعقيدات السيادة التقليدية، لتتقدم الدبلوماسية السيبرانية بوصفها أداة لازمة لوضع قواعد سلوك ملزمة لجميع الفاعلين في الفضاء الرقمي، بما يحفظ الاستقرار الدولي ويعزز مقتضيات الأمن الجماعي، **وفي نهاية البحث توصلت الدراسة الى جملة من الاستنتاجات:**

١- تغير مفهوم التهديد الأمني بعد عام ٢٠٢٠، إذ أصبح الهجوم السيبراني يُعامل بوصفه تهديد مباشر للسيادة الوطنية والشرعية السياسية للدول.

٢- الفضاء السيبراني أصبح ميداناً استراتيجيا للصراع الدولي تتنافس فيه القوى الكبرى عبر أدوات غير تقليدية مثل الذكاء الاصطناعي والهجمات السيبرانية المدارة عن بُعد.

٣- ضعف الأطر القانونية الدولية المنظمة للفضاء السيبراني يجعل من الصعب فرض قواعد ملزمة للردع والمساءلة وهو ما يزيد من مخاطر الانفلات السيبراني.

٤- الفاعلون من غير الدول مثل الجماعات المنظمة والمرتزقة الرقميين باتوا يشكلون تهديداً لا يقل خطورة عن الدول ويصعب تتبعهم أو إخضاعهم للمحاسبة الدولية.

٥- الحاجة إلى دبلوماسية سيبرانية متعددة الأطراف باتت ضرورة وليست خياراً وذلك بهدف صياغة نظام رقمي عالمي يقوم على قواعد واضحة للتعاون وتبادل المعلومات والردع المشترك.

قائمة المصادر

أولاً: المصادر العربية:

أ- الكتب العربية والمترجمة:

١- عباس بدران، الحروب الالكترونية الاشتباك في عالم متغير، مركز دراسات الحكومة الالكترونية، بيروت، ٢٠١٠.

٢- خالد وليد محمود، الفضاء السيبراني وتحولات القوة في العلاقات الدولية، الدوحة: المركز العربي للأبحاث ودراسة السياسات، ٢٠٢٥.

٣- ربيع محمد يحي، اسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط: دراسة حول استعدادات ومحاور عمل الدولة العبرية في عصر الانترنت، ٢٠٠٢/٢٠١٢، رؤى استراتيجية، ٢٠١٣.

٤- عادل عبد الصادق، أسلحة الفضاء الالكتروني في ضوء القانون الدولي، سلسلة أوراق، العدد ٢٣، مكتبة الاسكندرية، مصر، ٢٠١٦.

٥- منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت، ٢٠١٧.

٦- عمران طه عبد الرحمن، الفضاء السيبراني في ضوء نظريات العلاقات الدولية، لندن: المركز الديمقراطي العربي، ٢٠٢٤.

٧- ماجد محمد الحنيطي، تكنولوجيا الصراعات الدولية المعاصرة، الآن ناشرون وموزعون، ط١، عمان، الأردن، ٢٠٢١.

٨- محمد رمضان أبو شعشيع، إيران.. تركيا.. إسرائيل وصراع القوى في الشرق الأوسط، العربي للنشر والتوزيع، القاهرة، مصر، ٢٠٢٣.

٩- ماجد عزيز إسكندر، التوظيف السياسي للهجمات السيبرانية ومخاطرها على الأمن القومي، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، دولة الإمارات العربية المتحدة، الطبعة الأولى، ٢٠٢٣.

١٠- رغدة البهي، حرب موازية: البعد السيبراني في الحرب الروسية -الأوكرانية، في: روسيا وأوكرانيا من الأزمة إلى أيام الحرب: البدايات والمآلات، المركز المصري للفكر والدراسات الاستراتيجية، الإصدار الأول، القاهرة، ٢٠٢٢.

١١- محمد منذر جلال، تكنولوجيا الحروب السيبرانية واستراتيجيات المواجهة الدولية، منشورات دار ومكتبة عدنان للطباعة والنشر والتوزيع، ٢٠٢١.

ب- المجلات والصحف:

١- اسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، المجلد ١٠، العدد ١، الجزائر، ٢٠١٩.

٢- إيهاب خليفة، تأثيرات قوة الفضاء الإلكتروني على التفاعلات الأمنية في العالم، دورية اتجاهات الأحداث، العدد ١، المجلد ١، آب ٢٠١٤.

٣- لبنى خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حمورابي، العراق، المجلد ٠٨، العدد ٣٣-٣٤، ٢٠٢٠.

٤- ساعد بوقرص، الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة، مجلة الأبحاث في الحماية الاجتماعية، الجزائر، المجلد ٠٣، العدد ١، ٢٠٢٢.

٥- د. خالد حنفي علي، إشكاليات تداخل الصراعات السيبرانية والتقليدية، مجلة السياسة الدولية، العدد ٢٠٨، المجلد ٥٢، مؤسسة الأهرام، القاهرة، ٢٠١٧.

٦- د. ابتسام علي حسين، فرص وقيود الأطراف المتنازعة على المجال العام السيبراني، مجلة السياسة الدولية، العدد ٢٠٨، المجلد ٥٢، مؤسسة الأهرام، القاهرة، ٢٠١٧.

٧- د. رغدة البهي، الردع السيبراني: المفهوم والإشكاليات والمتطلبات، مجلة الدراسات الإعلامية، المركز الديمقراطي العربي، العدد الأول، القاهرة، يناير ٢٠١٨.

٨- علي زياد فتحي، رؤية استراتيجية: العمليات السيبرانية الأوروأطلسية ومهددات الجيوسيبرانية الروسية (بحث)، مجلة حمورابي للدراسات، السنة السابعة، العدد ٣٠، مركز حمورابي للبحوث والدراسات الاستراتيجية، ٢٠١٩.

٩- بيداء علي ولي، المبادئ الأساسية التي تحكم خوض الحرب في القانون الدولي الإنساني (بحث)، مجلة القادسية للقانون والعلوم السياسية، كلية القانون، جامعة القادسية، ٢٠١٠.

١٠- شريف نسيم بخيت، الهجمات الإلكترونية وحظر استخدام القوة، موقع المركز العربي للأبحاث، الفضاء الإلكتروني، ٢٠١٧.

١١- بيداء علي ولي، التجسس السيبراني على المحفوظات الدبلوماسية (بحث)، مجلة القادسية للقانون والعلوم السياسية، المجلد ١٣، العدد ١، جامعة القادسية، ٢٠٢٢.

ثانياً: المصادر الأجنبية

1- Cyberterrorism,in:http://searchsecurity.techtarget.com/definition/cyberterrorism, Logged on: 15/10/2025.

2- Alan Freedman et al., Cyber security and Cyber war: What Everyone Needs to Know, London Oxford University Press, 2014.

3- Tim Maurer, Cyber Mercenaries: Hackers of the State and Power, London: Cambridge University Press, 2018.

4- Klemburg Alexander, the Dark Web: Cyber warfare, New York: Penguin Books, 2017.

5- Paul Cornish, "Cyber security and Politically, Socially, and Religiously Motivated Cyber Attacks," NATO Review: A Security and Intellectual Survey, 2011.

6- Ronald Debert, Black Code: Privacy, Surveillance and the Dark Side of the Internet, New York: Signal Books, 2013.

7- Muller Milton, Networks and States: The Global Politics of Internet Governance, London: MIT Press, 2010.