الحرب والأمن السيبراني في ساحة الفضاء الالكتروني

م.د أوراد محمد مالك كمونه

كلية التراث الجامعة

الملخص

أصبح الفضاء الإلكتروني ساحة جديدة للصراع بشكله التقليدي، ولكنه ذو طابع إلكترونى يعكس النزاعات التي تخوضها الدول أو الفاعلين من غير الدول على خلفيات دينية، أو عرقية، أو أيديولوجية، أو اقتصادية أو سياسية ، ويتمدد الصراع الإلكتروني بداخل شبكات الاتصال والمعلومات متجاوزا الحدود التقليدية وسيادة الدول، ويؤثر ذلك فى امتداد مجاله وآثاره وأضافت عملية تعدد الاستخدام والفاعلين والمصالح إلى تنوع أشكال الصراع وأهدافه.

Abstract

Cyberspace has become a new arena for conflict in its traditional form, but it has an electronic nature that reflects conflicts waged by states or non-state actors on religious, ethnic, ideological, economic or political backgrounds. Electronic conflict extends within communication and information networks, bypassing traditional borders and the sovereignty of states, and this affects the extension of its scope and effects. The process of multiplicity of use, actors and interests added to the diversity of conflict forms and objectives.

المقدمة

يؤدى الفضاء الإلكترونى (السيبراني) دورا أساسيا في تعظيم القوة، أو الاستحواذ على عناصرها الأساسية فى العلاقات الدولية، إذ أصبح التفوق فى هذا المجال عنصرا حيويا في تنفيذ عمليات ذات فاعلية فى الأرض والبحر والجو والفضاء، واعتماد القدرة القتالية في الفضاء الإلكتروني، وأدى ذلك الأمر إلى تغيير في مفهوم القوة الوطنية للدولة، فبات بالإمكان تعريفها بأنها مجموعة الوسائل والطاقات والإمكانات المادية وغير المادية المنظورة وغير المنظورة التي بحوزة الدولة ، وأصبح للفضاء الإلكترونى دور فى وجود أهداف ووسائل ومصالح إلكترونية جديدة، وفى الوقت نفسه أتاح القابلية لخطر التعرض للهجوم، وهو ما أوجد نوعا جديدا من التهديد بالضرر دون الحاجة للدخول الطبيعى والمادى لإقليم الدولة، وذلك لاعتماد الدول على الأنظمة الإلكترونية فى كل منشآتها الحيوية بما يجعل من تلك الأنظمة هدفا للهجوم، وخاصة أن تلك الأنظمة تحمل طابعا مدنيا وعسكريا مزدوجا ، وذلك بعد أن تمخض عن الثورة التكنولوجية ثورة أخرى هى الثورة فى الشؤون الإستراتيجية وتطور تقنيات الحرب ، إن معدلات التهديدات وفرص الحروب السيبرانية تتزايد مع توظيف القدرات السيبرانية في تحقيق المصالح، خاصة مع اتساع نطاق مخاطر العدائيات السيبرانية، ومع زيادة عدد الأطراف فى هذا المجال، أصبح الصراع ذا طبيعة سياسية متخذا شكلا عسكريا - إن صح التعبير - من حيث طبيعة الأضرار وتدمير الثروة المعلوماتية فى البنية التحتية للدولة بهدف سياسي .

وتكتنف ظاهرة الحرب السيبرانية حالة من الغموض البناء، وهو الأقرب إلى ما كان يسمى بالغموض النووى فى أثناء الحرب الباردة، لقد بدأت هذه الحرب فعليا، وقد تم رصد العديد من العمليات السيبرانية التي حققت أهدافها، وإن كانت بمنزلة إنذار لأخطار كبرى في حالة زاد وتوسع نطاقها ، واتجهت العديد من الدول إلى تحديث القدرات الدفاعية والهجومية لمواجهة مخاطر الحرب السيبرانية، والاستثمار في البنية التحتية المعلوماتية، وتأمينها، ورفع كفاءة الجاهزية لمثل هذه الحرب، من خلال الاستثمار فى رفع القدرات البشرية داخل الأجهزة الوطنية المعنية، وهنا، يتعلق التوجه الأخطر بنقل تلك القدرات من الدفاع إلى الهجوم عن طريق استخدام تلك الهجمات في إطار إدارة الصراع فى مجالات عديدة مسرحها الفضاء الإلكتروني.

المبحث الأول : القوة السيبرانية وخصائص الأمن السيبراني

بعد أحداث ١١أيلول ٢٠٠١ ، بدأ التركيز على الفضاء الإلكترونى كتهديد أمنى جديد بفعل أحداث دولية، كان أبرزها استخدام تنظيم القاعدة له كساحة قتال ضد الولايات المتحدة، وفي عام ٢٠٠٧ برز بوضوح دور الفضاء الإلكتروني

كمجال جديد فى العمليات العدائية فى الصراع بين إستونيا وروسيا، وفى ٢٠٠٨ أثناء الحرب بين روسيا وجورجيا ثم كوريا الجنوبية والولايات المتحدة عام ٢٠٠٩، وجاء الهجوم الإلكتروني بفيروس "ستاكسنت" على برنامج إيران النووى عام ٢٠١٠ ليمثل نقلة مهمة فى مجال الأسلحة الإلكترونية، لدعم الاهتمام الدولى بأمن الفضاء الإلكتروني، وبرزت محاولات للسيطرة عليها بعد تصاعد الاحتجاجات في أكثر البلدان ديمقراطية وهى بريطانيا والولايات المتحدة، وفي عام ٢٠١١ تم اختراق أحد المختبرات العلمية الرئيسية التابعة للولايات المتحدة، اما فى عام ٢٠١٢ تم الهجوم على ألالاف من أجهزة الكمبيوتر من شركة النفط السعودية أرامكو، وألقت المخابرات الأمريكية اللوم على إيران، وشهد عام ٢٠١٦، هجوم القراصنة على قطاعات الطاقة والصناعة والنقل وشركات الطيران المدني فى بعض دول الخليج، كما تم اختراق البريد الإلكترونى الخاص بجون بوديستا رئيس الحملة الانتخابية الرئاسية لهيلاري كلينتون، وقام وسطاء بتسريب رسائل إلكترونية إلى موقع ويكليكس ، ورغم اختلاف غرض وهدف كل حالة من الحالات السابقة، فإنه من الواضح أن حجم الهجمات السيبرانية يتزايد بشكل كبير، ولذا يصعب تحديد حجمها، وتتمثل القواسم المشتركة بين تلك الحالات في صعوبة تحديد مرتكبى تلك الهجمات على وجه الدقة، وغياب الرد المضاد كنتيجة لذلك[١].

المطلب الأول: المفاهيم الاساسية للقوة السيبرانية

يعد مفهوم القوة السيبرانية من المفاهيم الحديثة التي حظيت باهتمام الكثير من الباحثين في علم السياسة، وهو من أصعب المفاهيم التى يتناولها التحليل، لأنه مفهوم نسبى متغير ومركب وذو أبعاد عدة ومستويات مختلفة خاصة أن المجتمع العالمى يتعرض لتهديدات مباشرة وغير مباشرة من مصادر مختلفة، أن القوة السيبرانية مشتقة من شبكات السايبر Cyber وتعنى شبكات الإنترنت، وقدم "جوزيف نای" مصطلح القوة السيبرانية لفهم الدور الذي تؤديه شبكة الإنترنت في تشكيل قدرة الأطراف المؤثرة، التى يعد من أبرزها الأطراف الدولية وغير الدولية لتحقيق أهدافها، كما تعد البديل عن أساليب القوة العسكرية الصلبة لتحقيق الأهداف الوطنية، وتبنى مفهوم القوة الناعمة، التي تتضمن وسائل غير مادية، مثل الثقافة، والقيم السياسية والسياسات الخارجية، ولكى تمتلك الدول القوة الناعمة، ولتحسين مكاسبها على المسرح العالمي، من الضرورى أن تتميز بالسمات الثلاث التالية [٢]:

١- أن تنسجم الثقافة والأفكار السائدة مع المعايير العالمية والحرب التي تشمل الليبرالية، والتعددية، والاستقلالية.

٢- من الضرورى الوصول إلى قنوات اتصال متعددة، ونشر الرسالة المرغوبة بفاعلية للتمكين من التأثير على نطاق واسع من الوسائط.

٣- أن ينظر لمفهوم القوة الناعمة على أنه موثوق من حيث أداؤه المحلى والدولى، بحيث يكون جذابا للهدف الذي يرغب في التأثير عليه.

وقد أثر الفضاء الإلكترونى فى تغيير نمط القوة، من حيث طبيعة وخصائص الأمن والقوة والصراع فى المشهد الدولي، سواء على المستوى النظرى أو التطبيقى، وأصبح له تأثيرات وشواهد واضحة في العلاقات الدولية، وتم ذلك عبر متغيرات ثلاثة هى [٣] :

- **المتغير الأول :** إعادة التفكير في مفهوم الأمن القومى للدولة، إذ إن الأمن السيبراني لم يقتصر فقط على بعده التقني، بل تعداه إلى أبعاد أخرى، فى ظل تراجع سيادة الدولة وتزايد العلاقة بين الأمن والتكنولوجيا، وتأثير ذلك على المصالح الإستراتيجية للدول.

- **المتغير الثاني :** تعظيم القوة أو الاستحواذ على عناصرها الأساسية في العلاقات الدولية، إذ أصبح التفوق في ذلك المجال عنصرا حيويا فى تنفيذ عمليات ذات فاعلية في الأرض، والبحر، والجو، والفضاء، واعتماد القدرة القتالية في الفضاء الإلكترونى على نظم التحكم والسيطرة التكنولوجية، وبات الفضاء الإلكتروني مسرحا لشن هجمات مدمرة ماديا ومعنويا.

- **المتغير الثالث :** بروز أنماط جديدة من الصراع، كمجال تنشأ فيه نزاعات بين الفاعلين المختلفين، وتعبيرا عن تعارض المصالح والقيم، سواء بين الفاعلين من الدول أو الفاعلين من غير الدول ، ولكون الفضاء الإلكترونى عابرا للحدود.

ومن المفاهيم الأساسية المرتبطة بالقوة السيبرانية هي :

أولا : مفهوم الفضاء السيبراني

مع اندلاع الثورة المعلوماتية، ظهرت بيئة جديدة تتمثل في الفضاء السيبرانى ، وأضحى الفضاء السيبراني عنصرا مؤثرا فى النظام الدولي، نظرا لما يحمله من أدوات تكنولوجية متطورة، تلعب دورا وتؤثر في أنماط القوة والحرب والأمن، وتستخدم الكثير من الدول القدرات التي يوفرها الفضاء السيبراني لعدة أمور في مقدمتها الأمن والقوة العسكرية، إذ ظهر

بُعد جديد في الصراعات الدولية، هو "صراع الفضاء السيبراني"، إذ يستطيع أحد أطراف الصراع أن يوقع خسائر فادحة، وأن يتسبب فى شل البنية المعلوماتية والاتصالية الخاصة به وهو ما يسبب خسائر عسكرية واقتصادية فادحة(٤).

لقد بات الفضاء السيبراني تعبيرا متداولا حول العالم، يشير إلى كل ما يرتبط بالشبكات الحاسوبية والإنترنت، والتطبيقات المعلوماتية، وهذا الفضاء يحتاج إلى حماية من المخاطر المختلفة التي تواجهه كالهجمات السيبرانية التي تزداد تعقيداً والتي تعد نوعا من الحروب التي قد تقف خلفها منظمات أو دول لأهداف سياسية وعسكرية واقتصادية وهي حروب لا تنطبق عليها قوانين وأعراف الحروب التقليدية، ولا تقيدها الحدود السياسية للدول، فهى عابرة للقارات، ويعرف الفضاء أيضا بأنه المجال الكهرومغناطيسى لتخزين وتعديل أو تغيير البيانات المتصلة والمرتبطة بشبكة البنية التحتية الطبيعية ويتضمن عملية الاندماج بين الإنترنت والمحمول وأجهزة الاتصالات والأقمار الصناعية، ويعد الفضاء الإلكتروني أكبر من الإنترنت لما يحتويه من قدرات توجيهية للطاقة التي توجد في جزء من الموجات الكهرومغناطيسية(٥).

ثالثا : مفهوم البنية التحتية لتقنية المعلومات

هى مجموعة الوسائل والقدرات التي يتم تنسيقها عادتاً بواسطة منظمة مركزية للمعلومات، فمثلا، تشكل شبكة الاتصالات التي تستخدمها العديد من المؤسسات التجارية والخدمية بنية تحتية مشتركة وتشكل القوانين والأعراف والآليات التي تربط استغلال كل من الوسائل الفيزيائية والذهنية لبنية تقنية المعلومات، وتنمية قواعد البنية التحتية للمعلومات، وتعتمد البنية التحتية للمعلومات على وسائل وأدوات التقنية المتطورة، مثل الهواتف والحواسيب والاسطوانات المضغوطة، والأشرطة المرئية والمسموعة، والأقمار الاصطناعية، وخطوط الاتصال البصرية، وشبكات الموجات الدقيقة، وأجهزة الاستقبال وآلات التصوير، فضلا عن التقدم في عمليات الحوسبة والمعلومات وتقنيات الشبكات ، إن البنية التحتية لتقنية المعلومات تتجاوز المعدات والبرمجيات، فهى تحتوى على النظم التطبيقية والبرامج والنشاطات والعلاقات، وهناك المعلومات، بغض النظر عن الغرض منها أو شكلها، مثل: قواعد البيانات العلمية أو التجارية وتسجيلات الصوت والصورة، وأرشيف المكتبات، أو وسائط أخرى، ووسائط الاتصال وشفرات البث التي تسهل التعامل بين الشبكات، وتضمن الخصوصيات والأمان للمعلومات التي تنقل الشبكات، وأهم من ذلك كله "الإنسان" الذي يعمل على تكوين المعلومات والاستفادة منها، وبناء التطبيق (٦).

رابعا : مفهوم القدرات السيبرانية

لا توجد تعريفات أو معايير محددة لما تشكله القدرات الهجومية فى الفضاء السيبراني، وإن كان الباحثون حددوا بعضا منها مثل: أدوات الهجوم، وأدوات استغلال الشبكات، ونظم مراقبة أنشطة مكافحة الدعاية عبر الإنترنت ، ومنذ بداية عام ٢٠١٨ والفضاء السيبراني في مشهد ديناميكى وتشفير مستمر نتيجة حرية الحركة للدول والجهات الفاعلة، وتستفيد الدول من إخفاء هويتها فى هذا العالم الرقمي لإجراء مجموعة من العمليات السيبرانية الهجومية ضد دول معادية، سواء على مستوى سرقة المعلومات والأموال أو الهجوم على البنية التحتية والتأثير فى مسارات الانتخابات الوطنية(٧). إن الاهتمام المتزايد من المجتمع الدولى لم يردع الأطراف الفاعلة الدولية وغير الدولية، بل على العكس شهدت السنوات الماضية سعى بعض الحكومات لمزيد من النشاط في القدرات السيبرانية الهجومية مثل: روسيا والصين وإيران وكوريا الشمالية وهى من الجهات الفاعلة الرئيسية في مجال التهديد الإلكتروني، ويعتقد أن الولايات المتحدة الامريكية استخدمت أشكالا مختلفة من الأسلحة السيبرانية ضد البرنامج النووي الإيراني، وضد صواريخ كوريا الشمالية، وتنظيم "داعش" الإرهابي ، كما أسس حلف الناتو، لأغراض الدفاع الجماعي في المجالات القتالية المتقدمة نظما دفاعية مستغلا في ذلك قدرات البيئة العلمية التكنولوجية للدول الأعضاء ، وأعلن عن مبادرة التحالف الذكى لبناء نهج جديد هو الدفاع الذكى وبناء القدرات الضرورية لمواجهة التحديات الأمنية الحالية والمستقبلية من خلال مرحلتين **الأولى** تركز على الإصلاح التنظيمي للناتو وتحقيق الأمن السيبراني، **والثانية** كانت فى أثناء العمليات الجوية فى ليبيا ٢٠١١ وقد وضع الناتو مجموعة من العناصر تدعم بناء القدرات وذلك من خلال (٨):

١- إدراك أن الدفاع السيبراني مطلوب لتحقيق الدفاع الجماعي وإدارة الأزمات.
٢- الدفاع عن المنظومات والمؤسسات الحيوية السيبرانية للحلف.
٣-تحقيق الحد الأدنى للحماية السيبرانية، خاصة البنية التحتية الحيوية.
٤-التعاون مع الشركاء من المنظمات الدولية، والقطاع الخاص، والأوساط الأكاديمية.

خامساً : مفهوم الصراع السيبرانى

مع انتشار الفضاء السيبراني، وسهولة الدخول إليه، اتسعت دائرة الصراعات السيبرانية، وتطوير القدرات الهجومية السيبرانية التى تستهدف حيازة القوة، والتحكم فى المعلومات، وتعظيم القدرات القادرة على زيادة النفوذ والتأثير في المستويين المحلى والدولى، ومن أهم سمات الصراع السيبراني هي [٩]:

أ- تتسم أطرافه بعدم الوضوح، وتكون تداعياته خطيرة، سواء عن طريق تدمير المواقع على الإنترنت، أو نسفها وقصفها بوابل من الفيروسات.

ب - تحركه دوافع سياسية، ويأخذ شكلا عسكريا، تستخدم قدرات هجومية ودفاعية عبر الفضاء الإلكتروني، بهدف إفساد النظم المعلوماتية، والشبكات، والبنية التحتية.

ج- أنه ذو طبيعة ناعمة عن طريق الصراع حول الحصول على المعلومات، والتأثير فى المشاعر والأفكار، وشن حرب نفسية وإعلامية، بما يؤثر فى طبيعة العلاقات الدولية كالدور الذي لعبه موقع ويكيليكس فى الدبلوماسية الدولية.

سادساً : مفهوم الحرب السيبرانية

يشير مصطلح الحرب السيبرانية إلى وسائل وأساليب القتال التي تتألف من عمليات في الفضاء السيبراني ترقى إلى مستوى النزاع المسلح أو تجرى فى سياقه، ضمن المعنى المقصود في القانون الدولي الإنساني، كما يشير المصطلح إلى استخدام مجموعة من الممارسات والإجراءات التي تسعى لإلحاق الخلل والعطل بالأنظمة والوسائل الإلكترونية الخاصة بالعدو، فضلا عن تحقيق الحماية للذات من الاستطلاع الإلكترونى المعادى ومقاومته، وتحقيق الاستقرار للنظم الإلكترونية الصديقة، ويعد استخدام الطاقة الكهرومغناطيسية فى نطاق الحرب الإلكترونية ضروريا، وذلك لغايات تعطيل حركة العدو، ومنعها من استغلال المجال الكهرومغناطيسي الصديق، وأصبحت الحرب السيبرانية (الإلكترونية) تتخذ من شبكة الإنترنت حلبة صراع لها، وتأتى الهجمات التي تشن فيها بسبب دوافع سياسية، وتوجه الضربات الإلكترونية على مواقع الإنترنت الرسمية للعدو، وكل ما يتعلق بشبكاته وخدماته الأساسية، وتكون الضربات بقرصنة وتعطيل المواقع، وسرقة البيانات السرية، واختراق الأنظمة المالية [١٠].

ويمكن تعريف الهجمات السيبرانية بأنها "فعل يقوض قدرات وظائف شبكة الكمبيوتر، من خلال استغلال نقطة ضعف ما تمكن المهاجم من التلاعب بالنظام ، فهدف أنظمة المعلومات هو إتاحة المعلومات وضمان سلامتها، ولذا تهدف الهجمات السيبرانية إلى سرقة المعلومات، أو انتهاك سريتها أو تعديلها، أو منع الوصول إليها، كما توصف الهجمات الإلكترونية بأنها هجمات ذات دوافع اجتماعية أو سياسية يتم تنفيذها عبر شبكة الإنترنت وتزايدت حدة الهجمات الإلكترونية مع تزايد سهولة الوصول إلى الإنترنت [١١].

سابعاً : مفهوم الأمن السيبراني والتهديدات الناشئة

الأمن السيبراني هو عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح، وسوء الاستغلال، واستعادة المعلومات السيبرانية، ونظم الاتصالات والمعلومات التي تحتويها، وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات، وتعزيز حماية وسرية وخصوصية البيانات الشخصية، واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر فى الفضاء السيبراني، ومن ثم فإن الأمن السيبراني يشكل مجموع الأطر القانونية والتنظيمية، والهياكل التنظيمية، وإجراءات سير العمل، فضلاً عن الوسائل التقنية والتكنولوجية، والتى تمثل الجهود المشتركة للقطاعين الخاص والعام المحلية والدولية، والتي تهدف إلى حماية الفضاء السيبراني ، واتخاذ جميع الإجراءات الضرورية لحماية المواطنين من مخاطر الفضاء السيبراني، لقد أصبح الفضاء السيبراني، فيما يتعلق بعملية تزايد ترابط البنية التحتية الكونية للمعلومات دوليا أكثر عرضة للهجمات السيبرانية، نتيجة عدد من المتغيرات[١٢]، لعل من أهمها[١٣] :

١- العلاقة بين الأمن والتكنولوجيا علاقة طردية، مع إمكانية تعرض المصالح الإستراتيجية ذات الطبيعة السيبرانية إلى أخطار إلكترونية.

٢- يهتم الأمن السيبراني بعملية وضع المعايير والإجراءات لمنع الاستخدامات غير السلمية للفضاء السيبراني.

٣- أصبحت قضية أمن الفضاء السيبراني قضية دولية تتطلب إستراتيجية مرنة تتواءم مع المتغيرات المستمرة.

٤- لم يتم الاقتصار فى عملية الاهتمام بالأمن السيبراني على البعد التقنى وحسب، بل تجاوزه إلى أبعاد أخرى مثل: الأبعاد الثقافية والاجتماعية والاقتصادية والعسكرية .

٥- تصاعد دور الفاعلين من غير الدول في العلاقات الدولية قد أثر بدوره في سيادة الدول، خاصة مع بروز دور الشركات التكنولوجية عابرة للحدود الدولية.

المطلب الثاني : الأمن السيبراني وخصائصة

أولاً : الأمن السيبراني

يتحقق أمن الفضاء الإلكتروني حال وجود إجراءات الحماية ضد التعرض للأعمال العدائية، والاستخدام السئ لتكنولوجيا الاتصال والمعلومات ، ويعنى الأمن الإلكترونى بعملية وضع المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدى أشخاص غير مخولين بها عبر الاتصالات، لذا، أصبحت هناك مصلحة دولية، في الحفاظ على أمن الفضاء الإلكتروني، على أساس أن الأخير أصبح جزءا من الأمن العالمي ، ودعم ذلك الطبيعة المتغيرة للتفاعلات الإلكترونية، خاصة مع تطور القدرات البشرية على إنتاج تقنيات جديدة، فضلا عن تصاعد مخاطر التهديدات الإلكترونية على البنية التحتية الكونية للمعلومات ، وتراعى متطلبات الأمن الإلكتروني الدولي التأكد من سلامة الدفاعات الإلكترونية، وعدم تعرضها لأى خلل فني طارئ، وهى تتعامل مع تلك التهديدات التي تمثل خطرا على أمن الفضاء الإلكترونى بعده أصبح منظومة دولية [١٤].

ثانياً : خصائص الأمن السيبراني

أصبح العالم يواجه عددا من المحددات الجديدة للأمن العالمي، نتيجة عدد من المتغيرات، من أهمها ما يتعلق بعملية تزايد أرتباط البنية التحتية الكونية للمعلومات بالفضاء الإلكتروني، بما يجعلها عرضة للهجمات الإلكترونية، خاصة مع اتساع حركة الفاعلين من غير الدول في استخدامها، ومن أهم خصائص الأمن السيبراني ما يلى [١٥]:

١- **الأمن السيبرانى رافد جديد للأمن القومى** : باتت العلاقة بين الأمن والتكنولوجيا علاقة متزايدة مع إمكانية تعرض المصالح الاستراتيجية – ذات الطبيعة الإلكترونية - وتحول الفضاء الإلكترونى لوسيط ومصدر لأدوات جديدة للصراع الدولى المتعدد الأطراف، ومن جهة أخرى، فرضت تلك التطورات إعادة التفكير فى مفهوم الأمن القومي الذي يعنى بحماية قيم المجتمع الأساسية وإبعاد مصادر التهديد عنها.

٢- **الأمن الإلكترونى جزء من الأمن الجماعي :** يعنى الأمن الإلكترونى بعملية وضع المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدى أشخاص غير مخولين وجاءت تلك المظاهر لتبرز استخدامات غير سلمية للفضاء الإلكتروني، وما يمثله ذلك من تهديد للأمن الإلكتروني العالمي من جانب كافة الفاعلين فى مجتمع المعلومات العالمي، على أساس أن أمن الدول جزء من الأمن الجماعي.

٣- **تصاعد البعد الدولى فى مواجهة الأخطار السيبرانية :** أصبحت قضية أمن الفضاء الإلكترونى قضية دولية تتطلب إستراتيجية مرنة تتواءم مع المتغيرات المستمرة، سواء في الآليات، أو في التكتيكات الخاصة بالأمن مقابل التطور المستمر في الأخطار، ويرجع ذلك إلى الطبيعة المتغيرة للفضاء الإلكتروني وفقا للعامل الإنساني.

٤- **الأمن الإلكترونى كقضية عسكرية وإستراتيجية :** لم يتم الاقتصار على عملية الاهتمام بالأمن الإلكتروني على البعد التقنى وحسب، بل تجاوزه إلى أبعاد أخرى أصبحت ذات علاقة بتفسير القضية، مثل الأبعاد الثقافية والاجتماعية والاقتصادية، والعسكرية، كما يؤثر الاستخدام غير السلمي للفضاء الإلكتروني على كل من الرخاء الاقتصادي، والاستقرار الاجتماعي لجميع الدول.

٥- **تصاعد خطر الفاعلين من غير الدول على الأمن الإلكتروني:** إن تصاعد دور الفاعلين من غير الدول في العلاقات الدولية قد أثر بدوره على سيادة الدول، خاصة مع بروز دور الشركات التكنولوجية العابرة للحدود الدولية، وبروز أخطار القرصنة والجريمة الإلكترونية، والجماعات الإرهابية، وقد بدأ يظهر اتجاه التعددية في الحفاظ على الأمن بين كل أصحاب المصلحة من الحكومات والمجتمع المدنى، والقطاعين الأكاديمي والتقني والقطاع الخاص، ووسائل الإعلام.

ثالثاً : ردع الهجمات السيبرانية

لا يزال الردع ضروريا ومناسبا، لكن النظرية الكلاسيكية للردع لم تعد كافية لذا يجب تبنى مفهوم واسع من الردع يستخدم نهجاً لدمج كل عناصر السلطة الوطنية الدبلوماسية والعسكرية والاقتصادية والاستخباراتية والقانونية لتعزيز أمن المعلومات، وخلق حالة من عدم اليقين في أذهان الأعداء حول فاعلية أى نشاط سيبراني، وزيادة تكلفته وعواقبه ، فلابد من نشر دفاعات قوية والاعتماد على أنظمة مرنة يمكن أن تتعافى سريعا من الهجمات أو أى اضطرابات أخرى، وتلك التدابير لابد أن تتأسس على القدرة والرغبة في الرد على الهجمات السيبرانية من خلال جميع الوسائل اللازمة، مع تشديد الإجراءات القانونية الرادعة التي تحول دون التسبب في أضرار عابرة للحدود تتبع سيادة الدولة أو ولايتها القانونية، بل ومحاسبتها حال

فشلها في وضع تدابير تنظيمية لردع الهجمات السيبرانية داخل أراضيها، من خلال وضع تدابير قانونية لضمان فاعلية شبكات الاتصالات الدولية، وذلك يؤكد المسؤولية الجماعية للدول عن الأمن السيبراني[١٦].

ثمة معضلة هي أن متطلبات وشروط نظرية الردع لا تنطبق على الردع السيبراني ، فلا يوجد أى صراع بالمعنى العسكرى ، ولا يمكن التسليم بافتراض العقلانية الكلاسيكي، لما يلعبه الفاعلون من غير الدول من أدوار في الصراع السيبراني، وعدم معرفة موقفهم وهويتهم وقدراتهم، فضلا عن تقويض مفهوم التهديد بالانتقام ، وتحديد المواقع الجغرافية للخصوم، أما عن المصداقية فتواجه إشكاليات متعددة جراء عدم وجود قواعد للاشتباك، واحتمال وقوع خسائر مضادة.

المبحث الثاني:عوامل واسباب ومخاطر وإتجاهات الحرب السيبرانية

إن الحرب السيبرانية هى انعكاس للصراع بين الدول على جميع مستويات الصراع ، من صراع سياسي إلى صراع استخباراتي، إلى صراع اقتصادى، إذ يتم التعبير بالحرب السيبرانية (الإلكترونية) عن قيام دولة ما بشن هجمات إلكترونية على بيانات وبرمجيات دولة أخرى عن طريق مجموعة من المتخصصين في هذا المجال، وعلى الرغم من الاستخدام الواسع في وسائل الإعلام لمسمى "الحرب السيبرانية"، فإنه لم يعد كافيا أثر اتساع مدلولاته بعد أن كان مقتصرا في التشويش على أنظمة الاتصال والرادار وأجهزة الإنذار، بينما يكشف الواقع الحالى عن دخول شبكات الاتصال والمعلومات إلى بنية ومجال الاستخدامات العسكرية ، أما فى هجمات الفضاء السيبراني، فإنها غير محددة المجال أو الأهداف، كونها تتحرك عبر شبكات المعلومات والاتصالات المتعدية للحدود الدولية، وتلائم السياق التكنولوجي لعصر المعلومات.

المطلب الأول : عوامل واسباب الحرب السيبرانية

لقد اتسع نطاق أخطار الأنشطة العدائية التي يمارسها الفاعلون، سواء من الدول أو من غير الدول في الحرب السيبرانية، وقد قامت وزارة الدفاع الأمريكية (البنتاجون) بتصنيف الإنترنت على أنه الميدان الرابع من ميادين الحروب بعد الجو والبحر والبر، كما تقوم الولايات المتحدة الأمريكية بإجراء مناورة سنوية تحت اسم (سيبرستورم) لاختبار جاهزيتها لمواجهة أى هجمات إلكترونية معادية، كما قامت الصين بتخصيص قسم عسكرى كامل لعمليات التجسس الإلكتروني ، ويشهد العالم ظهور مجموعة من التقنيات ، وظهور أسلحة جديدة، ستستخدم في الحروب المستقبلية، تتراوح بين الحرب السيبرانية والطائرات بدون طيار، ومن الذكاء الاصطناعي إلى الواقع الافتراضي إلى الإرهاب الافتراضي، وتشمل حروب المستقبل مجموعة عالمية من الخبراء (الهاكرز المحترفين والمرتزقة)، التي تقاتل في البحر، واليابسة، والهواء، وفى الفضاء السيبراني، والفضاء الخارجى ، وتصبح التكنولوجيا الأساس للحرب فى القرن الـ ٢١ ، وقد بدأت بالفعل بعض جوانب هذه الاستراتيجية الجديدة [١٧].

أولاً : عوامل الحرب السيبرانية

شهد الفضاء السيبراني في السنوات الأخيرة تزايد عدد الهجمات السيبرانية، نظرا لتعدد التهديدات السيبرانية لتشمل الحروب والإرهاب والتجسس الرقمي وغيرها ، ولذا يصعب تحديد الحجم الحقيقي لتلك الهجمات، خاصة أن الكثير منها لا يتم الإبلاغ عنه، أو حتى الإشارة إليه، وهناك مجموعة من العوامل التى تزيد من فرص اندلاع الحروب السيبرانية ومن أهمها [١٨]:

١- تزايد ارتباط العالم بالفضاء الإلكتروني، فضلا عن استخدامه من قبل الفاعلين من غير الدول (الجماعات الإرهابية) لتحقيق أهدافها والتى تنال من الأمن القومى للدول.

٢- تراجع دور الدولة فى ظل العولمة وانسحابها من بعض القطاعات الإستراتيجية لمصلحة القطاع الخاص، مما أدى إلى تصاعد أدوار الشركات متعددة الجنسيات.

٣- نشوء نمط جديد من التهديدات على خلفية الهجمات الإلكترونية، خاصة مع تزايد اعتماد الدول على الأنظمة الإلكترونية في جميع منشآتها الحيوية.

٤- قلة تكلفة الحروب السيبرانية، مقارنة بنظيراتها التقليدية علاوة على أن هذا الهجوم قد يتم فى أى وقت، سواء كان في وقت السلم أو وجود أزمة أو حرب.

٥- تحول الحروب السيبرانية إلى أدوات التأثير على المعلومات المستخدمة في مستويات ومراحل الصراع المختلفة، بهدف التأثير بشكل سلبى فى هذه المعلومات ونظم عملها .

٦- توظيف الفضاء الإلكترونى فى تعظيم قوة الدول، من خلال إيجاد ميزة أو تفوق أو تأثير فى المجالات المختلفة وبالتالي ظهور ما يسمى "بالإستراتيجية السيبرانية" للدول.

٧- أدى تصاعد الأخطار والتهديدات في الفضاء الإلكتروني إلى بروز تنافس بين الشركات العاملة في مجال الأمن الإلكتروني، بغرض تعزيز أسواق الإنفاق العالمي على تأمين البني التحتية السيبرانية للدول، فى مواجهة شبكات الجريمة المنظمة.

ثانياً : أسباب الحروب السيبرانية

من أهم الأسباب التى تجعل الحرب السيبرانية أمرا ممكنا هي [١٩]:

١- **تغيير أيديولوجية الصراع الدولى :** (الفوضى الخلاقة) على سبيل المثال، من خلال تشكيل حالة سياسية بعد مرحلة فوضى متعمدة الأحداث يقوم بها أشخاص معينين بدون الكشف عن هويتهم، وذلك بهدف تعديل الأوضاع لمصلحتهم.

٢- **اتخاذ الإرهاب بعداً جديداً في القرن الحادى والعشرين :** إذ استخدمت التقنيات الحديثة والتكنولوجيا المتطورة فى تنفيذ عمليات إرهابية بأقل مجهود وتكلفة بفضل طبيعة الاتصالات التى تتجاوز الزمان والمكان.

٣- **التنافسية بين شركات البرمجيات الكبرى :** وتلك من أهم الساحات القائمة والقادمة، وتكون أكثر قوة من التنافسية بين الشركات الدولية الكبرى لصناعة السلاح.

٤- **ازدياد وتفشى العيوب التى تعترى البرمجيات والمعدات والأجهزة** : فكل تلك الأجهزة المتصلة بالإنترنت مثل، الحواسيب المحمولة وأجهزة الراوتر والمقسمات والأجهزة الخادمة للبريد الإلكتروني وصفحات الإنترنت وملفات البيانات وغيرها.

المطلب الثاني : مخاطر وإتجاهات الحرب السيبرانية

أولاً : مخاطر الحرب السيبراني

أدى اتساع علاقة الدول بالفضاء الإلكتروني، وما خلفته من حروب سيبرانية، إلى مجموعة من المخاطر على تفاعلات السياسة الدولية والعلاقات الدولية، يمكن طرح أبرزها على النحو التالي [٢٠]:

١- **تصاعد المخاطر الإلكترونية :** خاصة مع قابلية المنشآت الحيوية (مدنية وعسكرية) فى الدول للهجوم الإلكترونى عليها، عبر وسيط وحامل للخدمات، أو شل عمل أنظمتها المعلوماتية.

٢- **عسكرة الفضاء الإلكتروني :** وتصاعد القدرات في سباق التسلح السيبراني، وتبنى سياسات دفاعية سيبرانية لدى الأجهزة المعنية بالدفاع والأمن فى الدول، وهو ما يستدعى تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة.

٣- **تحديث القدرات الدفاعية والهجومية :** إذ سعت الدول إلى تحديث النشاط الدفاعى لمواجهة مخاطر الحرب السيبرانية وزيادة الاستثمارات في البنية التحتية المعلوماتية، وتأمينها ورفع كفاءة الجاهزية لمثل هذه الحرب والمشاركة الدولية في حماية البنية المعلوماتية.

٤- **الاستعداد لحروب المستقبل :** إذ تبنى كثير من الدول إستراتيجية حرب المعلومات بعدها حربا للمستقبل، والتي يتم خوضها بهدف إثارة الاضطرابات فى عملية صناعة القرار لدى الخصوم عبر اختراق أنظمتهم، واستخدام ونقل معلوماتهم.

ثانياً : إتجاهات الأمن السيبراني

في ضوء التهديدات والمبادئ والأولويات التي يتفق عليها الخبراء والمختصون إقليمياً ودولياً، يمكن وضع خطة للعمل في اتجاهين رئيسيين متوازيين، وذلك على النحو التالي [٢١]:

الاتجاه الأول وقائى : التعامل مع الصراع السيبراني كمشكلة أمن وطني لصانعي السياسة، وليس مجرد مسألة تقنية مهنية، وضرورة إدماج الفضاء الإلكترونى ضمن الأمن القومى للدول، وذلك عبر تحديث الجيوش، وتدشين فرق متخصصة فى الحروب السيبرانية وإقامة هيئات وطنية للأمن والدفاع الإلكتروني، والاستثمار في بحوث الجيل التالى من قدرات رجال المعلوماتية رواد الجيل السادس للحرب وإجراء بحوث التحليلات الأمنية المتقدمة مع وضع أجندة للعمل والتعاون مع القطاع الخاص، والجامعات ومراكز الأبحاث والدراسات.

الاتجاه الثاني دفاعي : النظر في تنظيم الخطط الدفاعية المستقبلية في مراحل متعددة، اعتمادا على التهديدات والتقنيات المستقبلية من خلال تحالفات مع مشغلى البنية التحتية الدولية، وإنشاء منظمة إلكترونية للإنذار والدفاعات، وزيادة مشاركة الشركات متعددة الجنسيات لزيادة القدرات السيبرانية وتقاسمها والتعاون من خلال تحالفات دولية، مثل الاتحاد الأوروبي، والمشاركة فى التدريب السيبراني المشترك، مع الاستفادة من تجربة الاتحاد الأوروبي في ذلك المجال.

الخاتمة

أصبح وجود الأمن السيبراني ضرورة لحماية الفضاء الالكتروني للدولة ضد الأعمال العدائية والاستخدام السيئ لتكنولوجيا الاتصال والمعلوماتية، مع تصاعد دور الفاعلين من غير الدول فى العلاقات الدولية، وفرض تحديات عديدة في الحفاظ على الأمن السيبراني العالمي دفع ذلك إلى بروز اتجاهات تعددية لتحقيق ذلك الأمن، عبر التنسيق بين أصحاب المصلحة من الحكومات والمجتمع المدنى، والشركات التكنولوجية ووسائل الإعلام وغيرها ، كما أصبح هناك مصلحة داخلية ودولية في الحفاظ على أمن الفضاء السيبراني، خاصة مع تطور القدرات البشرية على إنتاج تقنيات جديدة، فضلا عن تصاعد مخاطر

التهديدات السيبرانية على البنية التحتية الكونية للمعلومات، بدأت الحكومات في جميع أنحاء العالم في تطوير إستراتيجيات الأمن السيبراني والنظر إلى الفضاء الإلكتروني كمسألة دولية تتزايد أهميتها على مدى العقدين الماضيين، إذ كان لكل من الأمن السيبراني والفضاء الالكتروتي تأثير هائل على تكنولوجيا المعلومات والاتصالات.

الأستنتاجات

١-أن تحقيق الأمن السيبراني على المستوى الدولى أمرا بالغ الصعوبة في التوصل إلى اتفاق دولى لتقييد تطوير واستخدام الأسلحة السيبرانية الهجومية فى الحالة السلمية ، فالأسلحة النووية تخضع لأنظمة صارمة للقيادة والسيطرة، ولكن الأمر مختلف للسيطرة على جحافل من الكتائب السيبرانية وعلى شبكات الإنترنت الواسعة، وباتت عمليات الاختراق الإلكترونى عنصرا إضافيا، إذ تستخدم تارة فى زمن الحرب السيبرانية، وأخرى كنشاط مؤذ في زمن السلم، إن عمليات الاختراق الإلكتروني باتت قادرة على استهداف أعلى عتبات سلم الأمن الدولى.

٢-أن حماية الأمن السيبراني من الفضاء الالكتروني لا يقتصر على السياسة الخارجية للدول بل يشمل أيضا السياسة المحلية إذ إنه يستهدف بالدرجة نفسها، وأحيانا بدرجة أكبر في بعض الدول سواء كانوا معارضين أو منظمات غير حكومية أو أحزاب معارضة أو أنظمة حكومية ، وهو ما يستدعى زيادة الانتباه والاهتمام إلى أخطار انتشار الحروب السيبرانية، وأن تحث الحكومات على تطوير قدرات دفاعية، وليس هجومية ، ويمكن تطوير القدرات السيبرانية في إطار العديد من الاستراتيجيات الدولية التي تهدف إلى تحقيق الأمن السيبراني في نطاق تحالفاتها.

التوصيات

هناك الكثير من الإجراءات السريعة والحاسمة لتحقيق الأمن السيبراني وهي كالأتي:

١-تطوير سياسة وطنية لرفع الوعى حول قضايا الأمن السيبراني والحاجة إلى إجراءات وطنية، وإلى التعاون الدولى، أما الخطوة التالية، فتتمثل فى تطوير المخطط الوطني لتحفيزالأمن السيبراني، بهدف تقليص المشاركة في الجهود الدولية والإقليمية لتحفيز الوقاية الوطنية، والتعافى من الحوادث - السيبرانية.

٢-التوجه نحو حماية أرصدة الفضاء السيبراني وتتضمن عوامل معنوية مختلفة ومحتويات معلومات ومؤسسات وأفراد، وأيضا تقنية تخزن هذه المعلومات وتعالجها وتنقلها للشبكات.

٣-حماية الأرصدة بشروط ومؤشرات أداء، أشهرها عناصر ثلاثة هي حماية العمل، وإتاحة الخدمات دون انقطاع وحماية سلامة المعلومات من أي تخريب أو تشويه، أو تعديل، وحماية خصوصية المستخدم سواء كان فردا أو مؤسسة أو دولة.

المصادر

(١)ماهي الحرب السيبرانية؟ وما مدى خطورتها؟ ، على الرابط: www.cyberone.co

(٢) إيهاب خليفة، القوة الإلكترونية وأبعاد التحول في خصائص القوة، وحدة الدراسات المستقبلية، مكتبة الإسكندرية،٢٠١٨.

(٣)شموئيل إيفن ودايفيد بن سيمان، (ترجمة) محمود محارب، حرب في الفضاء الإلكتروني: إتجاهات وتأثيرات على إسرائيل، معهد دراسات الأمن القومي،٢٠٢٠.

(٤) عادل عبد الصادق ، الفضاء الإلكتروني والرأي العام: تغيير المجتمع والأدوات والتأثير، المركز العربي لأبحاث الفضاء الإلكتروني، قضايا إستراتيجية، العدد ٢٤٥٩، ٢٠١٧.

(٥)نسرين الصباحي، الحروب السيبرانية وتحديات الأمن العالمي، ٢٦سبتمبر٢٠١٧، على الرابط : www.cutt.us;63dwm

(٦)محمد أبو القاسم الرتيمي و وجدي سالم بسيوني ،البنية التحتية لتقنية المعلومات ومستقبل التعليم، جامعة السابع من أبريل، الجمعية الليبية للذكاء الاصطناعي، طرابلس، ٢٠١٥.

(٧) Ronald H. Brown,etal.2000 ,The global information infrastructure ; agenda for coop-eration,Posted on the intermet.

(٨)أحمد يوسف الجميلي، القدرات السيبرانية:الشؤون العسكرية والأمنية،مركز صنع السياسات،١٩-٦-٢٠١٨،على الرابط: www.makingpolicies.org

(٩)عادل عبد الصادق، موقع ويكيليكس وتحدي عالم الاستخبارات الأمريكي، ملف الأهرام الإستراتيجي ، مركز الأهرام للدراسات السياسية والإستراتيجية، اكتوبر ٢٠٢٠.

(١٠)ما هي الحرب السيبرانية، ٢٣-٣٠-٢٠٢٢،على الرابط: amp.dw.com

(١١)الحرب الإلكترونية والسيبرانية: تنوع اشكال والهدف واحد، على الرابط:www.alkhanadeq.com

(١٢)لغة العصر،مجلة الأهرام للكومبيوتر والإنترنيت ،على الرابط: http;//cut.us/HZjk2
(١٣)حسن مظفر الرزو، وماجد توهان الزبيدي، الفضاء المعلوماتي، مركز دراسات الوحدة العربية،٢٠٢١.
(١٤)عادل عبد الصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، قضايا إستراتيجية، مجلة السياسة الدولية ، العدد١٨٨،القاهرة ،٢٠١٢.
(١٥)عبد الغفار عفيفي الدويك، إستراتيجية الردع السيبراني.. التجربة الأمريكية ،دراسات إستراتيجية ، السياسة الدولية، مركز الأهرام ، العدد٢١٣، القاهرة ، ٢٠١٨.
(١٦) رغدة البهي ، الردع السيبراني:المفهوم والإشكاليات والمتطلبات، مجلة الدراسات الإعلامية - المركز الديمقراطي العربي – العددالأول ،يناير ٢٠١٨.
(١٧) حرب المعلومات مصطلح يستخدم لوصف استخدام وإدارة المعلومات للحصول على ميزة تنافسية على العدو وتتضمن حرب المعلومات جمع المعلومات الاستراتيجية، والتأكد من صلاحية المعلومات الموجودة، ونشر دعايات أو معلومات خاطئة لإحباط العدو أو الشعب، والتقليل من نوعية المعلومات التي توجد لدى العدو، والعمل على تقليل فرص جمع العدو للمعلومات للمزيد انظر : حرب المعلومات واقع أم خيال؟ /https://www.swissinfo.ch/ara
(١٨)عادل عبد الصادق ، الإرهاب الإلكتروني - القوة في العلاقات الدولية .. نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والاستراتيجية ، مركز الأهرام ، القاهرة ،٢٠٠٩.
(١٩) يحيى ياسين سعود ، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية ، مركز الدراسات والبحوث القانونية، على الرابط : https://jlaw.journals.ekb.eg
(٢٠) عادل عبد الصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مصدر سبق ذكره.
(٢١)كيف يمكن تحقيق الخداع الإستراتيجي في الفضاء الإلكتروني، مجلة المستقبل للأبحاث والدراسات المتقدمة ، ٣ /أغسطس/ ٢٠٢٠، على الرابط :www.futureuae.com