الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة محمد الصديق بن يحيى –قطب تاسوست– جيجل

كلية الحقوق والعلوم السياسية

قسم العلوم السياسية

مذكرة مقدمة لاستكمال متطلبات الحصول على شهادة ماستر أكاديمي، في ميدان الحقوق والعلوم السياسية، تخصص تعاون دولي

بعنوان:

الإستجابة الدولية للتهديدات السيبرانية

إعداد الطالبة:

بزير أمال

إشراف الأستاذ:

د.ريموش سفيان

لجنة المناقشة:

1- حموم فريدة (أستاذ ،جامعة جيجل)، رئيسا

2-ريموش سفيان (أستاذ محاضر ب، جامعة جيجل) مشرفـــا

3-أحسن خديم الله،(أستاذ محاضر أ، جامعة جيجل)، ممتحنا

السنة الجامعية 2022/2021

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة محمد الصديق بن يحيى –قطب تاسوست– جيجل

كلية الحقوق والعلوم السياسية

قسم العلوم السياسية

مذكرة مقدمة لاستكمال متطلبات الحصول على شهادة ماستر أكاديمي، في ميدان الحقوق والعلوم السياسية، تخصص تعاون دولي

بعنوان:

الإستجابة الدولية للتهديدات السيبرانية

إعداد الطالبة:

بزير أمال

إشراف الأستاذ:

د.ريموش سفيان

لجنة المناقشة:

1- حموم فريدة (أستاذ ،جامعة جيجل)، رئيسا

2-ريموش سفيان (أستاذ محاضر ب، جامعة جيجل) مشرفـــا

3-أحسن خديم الله،(أستاذ محاضر أ، جامعة جيجل)، ممتحنا

السنة الجامعية 2022/2021

إهـــــداء

الحمد لله الذي وفقني لأتم عملي هذا،

أهدي ثمرة جهدي المتواضع،

إلى أبي الغالي رحمه الله وطيب ثراه،

إلى أمي التي من دونها لا تحلو الحياة،

إلى زوجي الذي كان نعم السند ،

إلى عائلتي الصغيرة والكبيرة،

إلى رفيقاتي في العمـل

صليحة،ريـــم،فتيحة،مريـــم،

إلى أستاذي المشرف:ريموش سفيان

إلى أستاذي: قميحـــة رابـــح

شكرا للدعم والمساندة.

أمـــــال

مقدمة

تمهيد:

مع تزايد الاعتماد العالمي على تكنولوجيا المعلومات والاتصالات، أضحى التوجه نحو أكثر تمكين للأفراد والكيانات من آليات الانتشار للقوة المادية والفكرية بطرق لا تتأثر في معظمها بالحدود أو بالاعتبارات الدبلوماسية والسياسية، وأصبح بالإمكان لأي فرد أو جماعة أن يؤثر على المفاهيم والقيم والأفكار والتحيزات على الصعيد العالمي، بالسلب والايجاب.

هذا التسارع التكنولوجي وما رافقه من ثورة كبيرة في مجال المعلوماتية والانترنيت، أفرز واقعا جديدا وبيئة مجالية للتعاون والتنافس الدول تختلف عن بقية الفضاءات، حيث أصبح الفضاء السيبراني أحد مجالات الصراع والتنافس بين القوى العظمى وأحد العناصر المؤثرة في النظام الدولي بما يحمله من أدوات التأثير، مما فرض على الجميع ضرورة إعادة النظر في جملة من المفاهيم والأدوات والسياسات.

ساهمت الثورة المعلوماتية وسهولة وسرعة الوصول إل ى المعلومة، في انتشار القوة بين مجموعة فواعل أفرزتهم التغيرات التي رافقت صعود دور الفضاء السيبراني في الحياة اليومية، فتعددت بهذا العناصر المالكة للقوة والممارسة لها، ما سمح بأن تخترق سياد ة الدول في ظل فضاء إلكتروني لا يوجد فيه حدود ولا ضواب ط، ويظهر بهذا دور الفرد والجماعات كأحد الفاعلين المالكين للقوة السيبرانية.

إن توجه العالم نحو الاعتماد الكبير على التقنيات الذكية والحديثة، رفع من حالة الانكشاف الأمني للدول، خاصة بعد اعتمادها الكبير على الفضاء الإلكتروني ، لتصبح عرضة للاختراق والهجوم بالفيروسات وسرقة المعلومات أو إتلافها وبرامج ضارة وتصيد عبر البريد الإلكتروني وغيرها ، لتخلق لنا معضلة جديدة للأمن بتحوله إلى نوع جديد يعتمد على الشبكات والإنترنت، وتضاعفت مخاوف إمكانية اتجاه الجماعات الإرهابية في التأثير على أمن الفضاء الإلكتروني.

لقد كان من تداعيات الثورة المعلوماتية والعصر الرقمي ظهور تهديدات سيبرانية تتعلق أساسا بالفضاء السيبراني، وأصبحت تمثل تحديا كبيرا للأمن القومي وكذلك الدولي،

وهو ما دفع بالدول إلى اتخاذ مجموعة تدابير واليات بشكل فردي أو جماعي في سبيل مواجهة هذه التهديدات، لتظهر بهذا استراتيجيات الأمن السيبراني ويظهر مفهوم الأمن السيبراني كبعد جديد من أبعاد الأمن.

مبررات اختيار الموضوع:

يقول مالك بن نبي : "لست كاتبا بالمعنى المهني الذي صاحبه يبحث عن الموضوع ليخرجه للناس ولكني أشعر بواقع من حولي فيدفعني لإخراجه للناس"..

وعلى هذا الأساس، تعود مبررات اختيار هذا الموضوع أساسا إلى أهميته التي تنبع من عدة اعتبارات موضوعية وذاتية، تزيد من دفع الباحث في محاولة الوصول إلى نتائج علمية هادفة:

مبررات موضوعية:

تنطوي دراسة موضوع الاستجابة الدولية للتهديدات السيبرانية على أهمية بالغة في الأدبيات السياسية، اعتبارا من كون التهديدات السيبرانية من أهم المواضيع التي تحض ى باهتمام من قبل الباحثين في مجال الدراسات الدولية والاستراتيج ية، ذلك لأنه يتعلق مباشرة بالأمن القومي للدول المخترق من قبل فواعل استطاعت من خلال سهولة الحصول عل المعلومات وامتلاك التكنولوجيا أن تمتلك عنصر من عناصر القوة هو القوة السيبرانية، والتي من خلالها تهدد أمن الدول والمؤسسات والأفراد، لهذا وجب الاهتمام بموضوع البحث هذا.

محاولة الباحث للإحاطة بهذا المجال المعرفي بدافع التخصص والتجديد، فتحت المجال للنظر في آليات خرق المجال السيبراني، ومحاولة كشف الممارسات المرتبطة بازدواجية توظيف التكنولوجيا لخدمة المصالح الحيوية.

مبررات ذاتية:

إنتماء الباحث إلى مجال الدراسة، بإعتبار البيئة العلمية والعملية مجالا خصبا لأي تهديد سيبراني، فمن خلال الاستكشاف والتوسع في الموضوع، يتم الإطلاع على أبرز طرق

خرق المجال الإلكتروني سواء الشخصي أو الوطني أو الدولي، والاطلاع على آليات وضوابط التحكم فيه.

أهداف الدراسة: تهدف هذه الدراسة للوصول إلى جملة من الأهداف أهمها ما يلي:

- ✓ معرفة طبيعة التهديدات السيبرانية كتهديدات جديدة للأمن الدولي.
- ✓ الوقوف على أهم المفاهيم الجديدة المقترنة مع ظهور التهديدات السيبرانية.
- ✓ معرفة الآليات والسياسات المنتهجة من قبل الدولة في سياستها الداخلية في سبيل تحقيق أمنها السيبراني وتأمين بنيتها التحتية وضمان منع اختراق خصوصياتها السرية.
- ✓ إبراز مظاهر التعاون على المستوى الدولي في سبيل مواجهة التهديدات السيبرانية.
- ✓ كشف أهم التحديات التي تعيق تحقيق الأمن السيبراني بين الدول وداخل الدول.

أدبيات الدراسة:

من خلال الإطلاع على الدارسات المتعلقة بالموضوع يتضح أنه رغم حداثة موضوع البحث، إلا أنه هناك العديد من الدراسات والمؤلفات حول الموضوع، وفي هذا الصدد نجد:

-دراسات الباحث **إيهاب خليفة*** منها كتاب "**القوة الالكترونية وأبعاد التحول في خصائص القوة**"، وهو كتاب صادر عن وحدة الدراسات المستقبلية في مكتبة الإسكندرية ضمن سلسلة "أوراق"، تناول فيه الباحث التحولات التي لحقت بمفهوم القوة في السياسة الدولية وتأثير الفضاء الالكتروني في الأشكال التقليدية للقوة، وخلصت الدراسة إلى صعود مفهوم القوة الالكترونية والسيبرانية كمفهوم جديد وتعدد الفاعلين الممارسين للقوة وانتشار القوة بينهم،

***إيهاب خليفة**: رئيس وحدة التطورات التكنولوجية بمركز المستقبل للأبحاث والدراسات المتقدمة، حاصل على ماجيستير من كلية الاقتصاد والعلوم السياسية بجامعة القاهرة حول القوة السيبرانية 2015،حاصل على الدكتوراه من كلية الاقتصاد والعلوم السياسية بجامعة القاهرة حول المدن الذكية 2020، له العديد من المؤلفات حول الأمن السيبراني الذكاء الاصطناعي والمدن الذكية أهم مؤلفاته "مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي" الصادر عام 2019، "القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت" الصادر عام 2017، "حروب مواقع التواصل الاجتماعي" الصادر عام 2015، متحدث ومحاضر في مجال التطورات التكنولوجية والحروب السيبرانية والمدن الذكية ومحركات الثورة الصناعية الرابعة.

إضافة إلى ظهور أشكال جديدة من الأسلحة ذات قدرة واسعة على إلحاق خسائر فادحة على كافة المستويات.

– دارسة أعدتها الدكتورة **منى الأشقر جبور** صادرة عن المركز العربي للبحوث القانونية والقضائية، تلقي الضوء على المفاهيم والمسائل المرتبطة بالأمن السيبراني عبر تشريحها وتشخيص واقعها ورصد أبعادها.

–دراسة للباحث **جوزيف ناي JOSEPH S.NYE.JR** بعنوان"CYBER POWER"، الصادرة، في ماي 2010 ،تناول فيها تأثير التطور التكنولوجي، على مفهوم القوة منذ ظهور الطباعة، إلى ظهور الأنترنت، ودوره في تحول الصراع الدولي، كما تناول متطلبات القوة السيبرانية، وخصائص الفضاء السيبراني والصراع داخله.

– دارسة أعدها **الإتحاد الدولي للإتصالات** سنة 2011 بعنوان:" **البحث عن السلام السيبراني**" بقلم **حمدون توريه** وفريق الرصد بالاتحاد، والذي تم فيها استعراض جملة من التهديدات السيبرانية حول العالم والتعاون الدولي في سبيل مواجهتها، وسبل تحقيق السلام السيبراني عبر العالم.

– دراسة للدكتور **عادل عبد الصادق** بعنوان "**القوة الالكترونية: أسلحة الانتشار الشامل في عصر الفضاء الالكتروني**" ، صادرة عن المركز العربي لأبحاث الفضاء الالكتروني في أكتوبر 2012، تستعرض هذه الدراسة علاقة الفضاء الالكتروني بإحداث تغييرات في البيئة الأمنية الدولية، وكيفية تغير مفهوم القوة، وبروز أنماط جديدة للصراع الدولي

ودراسات أخرى على شكل مقالات متخصصة، على سبيل الذكر لا الحصر:

–دراسة للدكتور **إسماعيل زروفة** بعنوان " **الفضاء السيبراني والتحول في مفاهيم القوة والصراع**"، وهي عبارة عن مقال بمجلة العلوم القانونية والعلوم السياسية في عددها الأول الصادر في أفريل 2019، تناول فيها الباحث مفهوم الفضاء السيبراني وأهم التحولات في مفهوم القوة، وأهم أنماط التهديدات السيبرانية وعلاقتها بالأمن القومي للدول.

-دراسة الدكتور **بارة سمير** بعنوان "**الأمن السيبراني في الجزائر السياسات والمؤسسات** "، وهي دراسة في المجلة الجزائرية للأمن الإنساني في عددها الرابع في جويلية 2017، تناولت الأمن السيبراني وآليات مواجهة التهديدات السيبرانية في الجزائر.

حدود الدراسة:

لكل دراسة حدودها المكانية والزمنية وعليه فإن هذه الدراسة تتخذ حدودها من خلال:

المجال الزماني: تركز هذه الدراسة على الفترة الزمنية الممتدة من ظهور واستعمال الانترنيت وثورة المعلومات إلى غاية يومنا هذا، وهذا وفق ما تتطلبه مقتضيات الدراسة.

المجال المكاني: انطلاقا من أن ثورة المعلومات تخطت حدود دول العالم ، عبر شبكات عنكبوتية مترابطة، فإن التهديدات السيبرانية تمس كافة الدول والفواعل الأخرى، لتتخذ هذه الدراسة إطارها المكاني بكل ما يتصل بالفضاء السيبراني ، لكن الضرورة المنهجية تتطلب التركيز على بعض الدول التي تعرضت لهجمات سيبرانية، والتعرض لتجارب وجهود بعض الدول في مواجهة التهديدات السيبرانية.

إشكالية الدراسة:

إذا كان واقع الحال يعتبر أنه في ظل تزايد ترابط العالم رقميا ، وضرورة التحرك الدولي فرديا وجماعيا لمواجهة التهديدات السيبرانية، فالإشكال الرئيسي الذي يبقى مطروحا هو حول: فعالية نجاعة الدول في الاستجابة لمختلف التهديدات السيبرانية؟.

التساؤلات: تتطلب الضرورة المنهجية إلحاق الإشكالية بالتساؤلات التالية:

1-ما هو مفهوم التهديدات السيبرانية؟ ما هي أهم مظاهرها؟.

2-كيف ساهم ظهور ثورة المعلومات في تغيير في مفهومي القوة والحرب وفي طبيعة الفواعل؟.

3-ما هي أهم الجهود الوطنية والدولية المبذولة من قبل الدول في سبيل مواجهة التهديدات السيبرانية؟.

فرضيات الدراسة: الفرضيات عبارة عن تقريرات واضحة، تشير إلى طريقة تفكير الباحث في العلاقة بين الظواهر المعنية بالدراسة، وتشير إلى الطريقة التي يظن بها أن متغيرا مستقلا يؤثر أو يعدل متغيرا تابعا، وعلى هذا الأساس، يمكن الاعتماد على الفرضيات التالية:

الفرضية الرئيسية: الإستجابة الإيجابية للتهديدات السيبرانية مبنية أساسا على تقريب الرؤى والتوافق الدولي لخدمة المصالح الجماعية لا الفردية؟.

الفرضيات الثانوية:

-كلما زاد استعمال الفضاء الإلكتروني كلما زادت التهديدات السيبرانية.

- وجود استراتيجيات وطنية ودولية لمواجهة التهديدات السيبرانية يضيق مجال الخطر ودائرة الأمن الدولي.

الإطار المهنجي للدراسة:

بناء موضوع الدراسة قائم أساسا على توظيف مجموعة من المناهج والإقترابات في إطار التكامل المنهجي، وفق منطق العملية البحثية: وصف، تحليل، تنبؤ، حيث:

تم الاعتماد على المنهج التاريخي الذي ساعد على وضع الظاهرة في محيطها وظروفها الأساسية، والغرض من استخدامه هو استقراء ظهور التهديدات السيبرانية ونشأتها وتطورها، كما تمت أيضا الاستعانة بالمنهج المقارن من خلال المقارنة بين تجارب بعض الدول في إطار مواجهة التهديدات السيبرانية، إضافة إلى استخدام المنهج الكمي عبر توظيف مجموعة من البيانات والإحصائيات التي تدعم البحث والتحليل.

تحديد المصطلحات :

تم بناء هذه الدراسة على مجموعة من المفاهيم الإجرائية يمكن تحديدها كالآتي:

التهديدات السيبرانية: تشير إلى التهديدات التي يكون مصدرها الأنترنت، أو التي يكون مصدرها إلكتروني، تقوم بها أفراد وجماعات ودول، الغاي ة منها إلحاق الضرر بالطرف المعتدى عليه واختراق أمنه المعلوماتي وتحقيق أهداف عن طريق هذا الاختراق.

الأمن السيبراني: عبارة عن تقنيات حماية أجهزة الكمبيوتر والشبكات والبرامج والبيانات والوصول غير المصرح به، أو الهجمات التي تهدف الى الاستغلال، وهو يغطي تطبيق الأمن، أمن المعلومات، التعافي من الكوارث، أمن الشبكات.[1]

تقسيم الدراسة:

تم تقسيم هذه الدراسة وفق الطرح المنهجي ومتطلبات المضمون إلى ثلاث فصول أساسية حيث:

تناول الفصل الأول الإطار التهديدات السيبرانية: تحديد المفاهيم والمظاهر، والذي تم تقسيمه إلى مبحثين، تطرق المبحث الأول منه بعنوان التهديدات السيبرانية مقاربة مفاهيمية إلى مفهوم التهديدات السيبرانية والمفاهيم المرتبطة بها ، أما المبحث الثاني بعنوان مظاهر التهديدات السيبرانية فتم فيه عرض أهم مظاهر التهديدات السيبرانية.

الفصل الثاني بعنوان تطور التهديدات السيبرانية وتأثيرها على الأمن الدولي، تم تقسيمه إلى ثلاث مباحث: المبحث الأول بعنوان التحول في مفهوم القوة والمبحث الثاني التحول في طبيعة الفواعل أما المبحث الثالث فقد تم فيه التطرق إل التحول في طبيعة الصراع والحروب.

الفصل الثالث: الجهود الدولية والوطنية في مواجهة التهديدات السيبرانية ، بحيث أبرز المبحث الأول منه الاتفاقيات والمعاهدات الدولية والإقليمية، وتناول المبحث الثاني الجهود الوطنية لمواجهة التهديدات السيبرانيةِ، أما المبحث الثالث فقد تناول تحد يات تحقيق الأمن السيبراني.

[1]–إسماعيل جابوري، "دور الأمن السيبراني في مواجهة التهديدات الإلكترونية: دراسة حالة الجزائر"، **مجلة تحولات** ، ديسمبر 2020، ص 73.

الفصل الأول:

التهديدات السيرانية: تحديد المفاهيم والمظاهر

إن مهمة تحديد المصطلحات هي أول تحد يواجهه المفكرون ويتعرض له الباحثون في جميع التخصصات ومختلف الدراسات، وذلك لما تطرحه من إشكاليات تجعل من الصعوبة بمكان الاتفاق على تعريفات واضحة وشاملة وموحدة بين فرقاء المجتمع العلمي يمكن تعميمها على جميع الحقول المعرفيۃ، ويعد مفهوم التهديدات السيبرانية أحد أهم المصطلحات التي تعرف تعددا في التعريفات المقدمة لها، ويتناول هذا الفصل من الدراسة التهديدات السيبرانية: تحديد المفاهيم والمظاهر ، بحيث يتناول المبحث الأول منه مفهوم التهديدات السيبرانية والمفاهيم المرتبطة به، في حين يتناول المبحث الثاني منه مظاهر التهديدات السيبرانية.

المبحث الأول: التهديدات السيبرانية: مقاربة مفاهيمية

تتطلب الضرورة المنهجية استعراض مفاهيمي لمؤشرات الدراسة وكل ما يرتبط بها من دلالات وتداخلات مفاهيمية.

المطلب الأول: التهديدات السيبرانية (cyber threads):

قبل التطرق إلى مفهوم التهديدات السيبرانية يتوجب التعرض لمصطلح التهديد من جهة، ومصطلح السيبرانية من جهة أخرى في محاولة تقديم تعريف إجرائي للمصطلح المركب.

1-مفهوم التهديد: لغة التهديد مشتق من هدد يهدد تهديدا وهو ناتج عن إلحاق الأذى والضرر.[1]

في اللغة الإنجليزية يقابل المعنى اللغوي للتهديد إلى" **Threat**" ،وفي اللغة الفرنسية يشير إلى معنى الخطر "**Menace**" .

ووفق قاموس **وبستر** فالتهديد هو تصريح أو تعبير عن نية لإيداء أو تدمير أو معاقبة في الانتقام أو الترهيب.[2]

---

[1]- الموسوعة السياسية، "التهديدات الأمنية"، متاح على الرابط:

https://bit.ly/3Nf6Xtv (2022/02/01)

[2]– بلعسل بنت نبي ياسمين، عمروش الحسين، "التهديدات الاكترونية والأمن السيبراني في الوطن العربي"، **مجلة نوميروس الاكاديمية**، المجلد 02، العدد 02، 2021، ص 163.

ويشير معنى مصطلح تهديد حسب معجم Le Petit Robert إلى: "الطريقة التي يرسم بها الرعب على وجه شخص ما، مع وجود النية لجعله يخشى الأذية التي أراد إلحاقها به."[1]

ورد في قاموس **أكسفورد Oxford** على أن التهديد هو : محاولة شخص أو شيء الإضرار بحياة الآخرين".[2]

يعرف **باري بوزان** (Barry Buzan) التهديد على أنه: "تهديد لمؤسسات الدولة باستخدام الإيديولوجيا أو استخدام مكونات القدرة للدولة ضد دولة أخرى، حيث يمكن أن يكون إقليم الدولة مهددا بضرر أو غزو أو احتلال، وقد تكون التهديدات من الخارج أو من الداخل".[3]

ويرى "**تيري ديبيل** (Terry L. Debel) أن التهديد: "عمل نشط وفعال تقوم به دولة معينة للتأثير في سلوك دولة أخرى، ويشترط نجاحه توفر عدة عوامل أبرزها المصداقية والجدية والقدرات التي تتناسب مع التهديد".[4]

وحسب تيري ديبيل هناك ثلاث سمات يتميز بها التهديد، وهي:

- ✓ درجة الخطورة .
- ✓ مدى احتمالية وقوع التهديد.
- ✓ وعنصر التوقيت".

بحسب الدراسات الأمنية فإن "التهديد " يستخدم كمصطلح سياسي، وبوصفه كمفهوم علمي، لا يزال غير معروف في الكثير من قواميس العلوم الاجتماعية.

---

[1]- بلعسل بنت نبي ياسمين، عمروش الحسين، "التهديدات الاكترونية والامن السيبراني في الوطن العربي"، **مجلة نوميروس الاكاديمية**، المجلد 02، العدد 02، 2021، ص 163.

[2]–عادل جارش، "مقاربة معرفية حول التهديدات الأمنية الجديدة"، **مجلة العلوم السياسية والقانون**، العدد01، 2017، ص 252.

[3]- عادل جارش، مرجع سابق، ص 253.

[4]- المرجع نفسه، الصفحة نفسها.

2-مفهوم السيبرانية: كلمة سيبرانية مشتقة من كلمة سايبر cyber وهي كلمة يونانية الأصل وترجع إلى مصطلح Keybernetes والتي تعني القيادة أو التحكم عن بعد.[1]

ولفظ سيبار أصلها يوناني ، وهي كلمة مشتقة من كلمة Kybernetes والتي تعني الشخص الذي يدير دفة السفينة Steersman، ويتم استخدامها للتعبير عن المتحكم governor.

ويشير قاموس **المورد** إلى السيبرانية بأنها علم الضبط، ومصدرها cybernetics وهو مصدر يتطابق مع مفهوم الهجمات السيبرانية، أي ضبط الأشياء عن بعد والسيطرة عليها.[2]

يعرف قاموس مصطلحات الأمن المعلوماتي السيبرانية على أنها"هجوم عبر الفضاء الإلكتروني يهدف إلى السيطرة على مواقع إلكترونية أو بنى محمية إلكترونيا لمعطلها أو تدميرها أو الإضرار بها".[3]

ويعرفها قاموس المصطلحات العسكرية على أنها "أي فعل يستخدم عن طريق شبكات إلكترونية بهدف السيطرة أو التعطيل لبرامج إلكترونية أخرى".[4]

ويشير معنى سايبر cyber في بعض المراجع إلى معنى تخيلي وافتراضي ، وتستخدم في وصف الفضاء الذي يضم الشبكات العنكبوتية المحسوبة، ومنظومات الاتصال والمعلومات وأنظمة التحكم عن بعد وتعني " كل ما يتعلق أو يرتبط بالحواسيب وتكنولوجيا المعلومات والواقع الافتراضي، ومنها اشتقت صفة السيبرانية والسيبراني cybernetics

---

[1]- عبد الرضا أسعد طارش ،علي إبراهيم مشجل المعموري، "الأمن السيبراني ودوره في انتشار ظاهرة الإرهاب في العراق بعد العام 2003"، **مجلة دراسات دولية**، العدد 80، (د.س.ن)، ص 153.

[2]-منير البعلبكي، **المورد: قاموس انكليزي عربي**. دار العلم للملايين، بيروت، 2004 ، ص 243 .

[3]-صفاء تغريد و لبنى خميس مهدي،"أثر السيبرانية في تطور القوة"، **مجلة حمورابي**، العدد 33-34، السنة 8، 2020، ص 149.

[4]- المرجع نفسه، ص 150.

وتعني علم التحكم الأوتوماتيكي أو علم الضبط وتعني أيضا القيادة أو التوجيه، والذي يعني "علم الاتصالات والأنظمة والتحكم الآلي في كل الآلات والأشياء الحية".[1]

يرجع أصل الكلمة إلى منتصف القرن العشرين مع عالم الرياضيات **نوبرت وينر** (Nobert winer's) صاحب كتاب Cybernetics or control and communication in the animal and the machine والذي قام باستخدامها للتعبير عن التحكم الآلي، وعرفها على أنها " التحكم والتواصل عند الحيوان والآلة"، وحسبه فإن السيبرنيتيقية هي "علم نقل الرسائل بين الإنسان والآلة أو بين الآلة والآلة"، أو علم ال قيادة والتحكم في الأحياء والآلات ودراسة آليات التواصل في كل منهما".[2]

أما **وليام جيبسون** (William Gibson) فقد استخدم كلمة Cyber مقترنة بكلمة space لتظهر في مصطلح الفضاء السيبراني Cyber Space في كتابه الكلاسيكي عام 1984.

وتشير كلمة Cybernetics إلى "نظرية الاتصالات والتحكم المنظم في التغذية المرتدة التي تعتمد عليها دراسات الاتصالات والتحكم في الحياة وفي الآليات التي صنعها الإنسان، أي علم دراسة الاتصال والتحكم الآلي في النظم العصبية للكائنات الحية و محاكاة الآلات لها".[3]

أما في اللغة العربية ، يجد المختصون صعوبة في اختيار مصطلح يقترب من السيبرانية أو يعبر عنها، لذا نجد استخدام مصطلحات أخرى للتعبير عنها منها مصطلح القوة الإلكترونية ، وهذا للدلالة على القوة السيبرانية ، رغم أن استخدام مصطلح القوة

---

[1]–صلاح مهري هاوي الشمري وآخرون ، الأمن السيبراني كمركز جديد في الإستراتيجية العراقية"، **مجلة قضايا سياسية،العراق**، العدد 62، السنة 12، 2020، ص 276.

[2]–عنترة بن مرزوق ، محمد الكر، "البعد الإلكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب"، **مجلة العلوم الإنسانية والإجتماعية**، العدد38، جوان 2018، ص 35.

[3]–حكيم غريب، "الإرهاب السيبراني والأمن الدولي: التهديدات العالمية الجديدة وأساليب المواجهة"، **المجلة الجزائرية للدراسات السياسية**،المجلد 05، العدد 02، 2018، ص 108.

الإلكترونية Electronic Cyber لا يعبر تعبيرا دقيقا عن مصطلح القوة السيبرانية غير أنه هو التعبير الأقرب لذلك.[1]

كتعريف إجرائي، يمكن القول أن التهديدات السيبرانية هي تهديدات مصدرها الانترنيت، الهدف منها اختراق النظام الأمني للدول والحكومات أو اختراق الحياة الشخصية للأفراد أو إختراق مؤسساتها وأنظمتها.

تتميز التهديدات السيبرانية بصعوبة التحديد وهذا نظرا للتطور التكنولوجي الهائل والمستمر، بحيث لم تعد الدول لوحدها معرضة لهذه التهديدات فقط بل أصبح الفرد أيضا معنيا بها، وهذا بسبب اتساع الاعتماد على الانترنيت في التعاملات اليومية، من جهة أخرى تنامي دور الفواعل الأخرى الجديدة في المجال السيبراني، وقد ظهرت أهمية التهديدات السيبرانية بصفة خاصة بعد استخدام تنظيم القاعدة للفضاء السيبراني في هجومات 2001/09/11، ثم برز التهديد أكثر خلال الحرب السيبرانية بين روسيا واستونيا 2008 ثم بين روسيا وجورجيا 2010 وصولا إلى دور التكنولوجيا في ثورات الربيع العربي.[2]

[1]–المرجع نفسه، ص 151.

[2]-كرار فرحان هاني الطائي، "أثر الأنترنيت العميق في أمن الدول"، **مجلة الدراسات الاستراتيجية والعسكرية**، المجلد 02، العدد 8، سبتمبر 2020، ص 67.

المطلب الثاني: المفاهيم المرتبطة بالتهديدات السيبرانية

هناك مجموعة من المصطلحات المترابطة مع مصطلح التهديد السيبراني، نتناول منها على سبيل المثال لا الحصر ما يلي:

1-الأمن السيبراني: يدخل الأمن السيبراني في إطار العناصر أو المكونات الجديدة للأمن القومي غير التقليدي، والتي ظهرت بعد الحرب الباردة، بحيث كان سائدا قبل هذه الأخيرة أن الأمن هو أمن عسكري بالأساس، فكلما زاد إنفاق الدولة عسكريا كلما زاد أمنها أي مدى قدرة الدولة على مواجهة التهديدات العسكرية بقوة عسكرية وفق ما تذهب إليه النظرية الواقعية.

يعرفه المعهد الوطني للمعايير التقنية في الولايات المتحدة الأمريكية على أنه:"النشاط أو العملية أو الإمكانية أو الحالة التي يتم بموجبها حماية نظم المعلومات والاتصالات والمعلومات الواردة إليها، والدفاع عنها ضد الضرر أو الاستخدام أو التعديل أو التجسس أو التدمير أو الدخول غير المسموح به".[1]

يعرفه الإتحاد الدولي للإتصالات بأنه" مجموعة الأدوات والسياسات والمفاهيم الأمنية، والحماية الأمنية والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريبات والممارسات الفضلى، والضمانات التكنولوجية التي يمكن استعمالها لحماية البيئة السيبرانية والمنظمة وأصول المستعمل".[2]

والهدف من كل هذه الممارسات والسياسات هو حماية الفضاء السيبراني ، وسرية الخدمات واستمراريتها في الفضاء السيبراني دون تعرضها لمختلف المخاطر التي تتعرض إليها البيئة السيبرانية.

يعبر الأمن السيبراني عن عملية وضع المعايير والإجراءات المتخذة ، لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين بها عبر الاتصالات ، ولضمان أصالة وصحة

---

[1]-مصطفى إبراهيم سلمان الشمري، "الأمن السيبراني وأثره في الأمن الوطني العراقي"، **مجلة العلوم القانونية والسياسية**، المجلد 10، العدد1، 2021، ص 12.

[2]-إيهاب خليفة، "الأمن السيبراني: الماهية والإشكاليات"، **مجلة رؤى مصرية**، أكتوبر 2016، ص 5.

هذه الاتصالات، والسعي لمنع الاستخدامات غير السلمية للفضاء الإلكتروني وما تمثله هذه الأخيرة من تهديد للأمن السيبراني العالمي والبنية التحتية الكونية للمعلومات من جانب كافة الفاعلين في مجتمع المعلومات العالمي.

كما يعبر عن مجمل القوانين والسياسات والأدوات والنصوص والمفاهيم وميكانيزمات الأمن، وطرق تسيير الأخطار والممارسات التكنولوجية المتعلقة بتكنولوجيا المعلومات والاتصالات المستخدمة لحماية الدول والمنظمات والأشخاص.[1]

من خلال هذه التعاريف يمكن القول أن ظهور هذا المفهوم ارتبط بالتطور التكنولوجي الذي توصلت إليه البشرية، ورغم تعدد التعاريف المقدمة له، كل حسب منطلقاته، فإنها كلها تجتمع في أنه تعبير عن قدرة الدولة على حماية معلوماتها، والحفاظ على سريتها ومنع اختراقها من قبل الأفراد والجماعات والدول، على اعتبار أن أي اختراق لهذه المعلومات يشكل تهديدا للأمن القومي للدول.

ويعود ظهور مفهوم الأمن السيبراني إلى سنة 1972، إذ كان مجرد فكرة نظرية في ذلك الوقت، واستمرت النقاشات والتحليلات حول المفهوم طوال فترة السبعينات ، ليتحول من مجرد مشروع بحث إلى مفهوم فعلي قابل للتطبيق ، ففي ظل تزايد الاعتماد على أجهزة الكمبيوتر ونمو الشبكات وانتشارها، ازدادت المناقشات حول أمن الكمبيوتر وأهميته ما بين عام 1972–1974، وكان من الضروري جدا تحديد نقاط الضعف، لذا أقرت الحكومات والدول بأهمية الأمن الإلكتروني، وأن الوصول غير المصرح به إلى البيانات والأنظمة يمكن أن يكون له عواقب كارثية بحيث تهدد الأمن القومي للدول وتمس بخصوصياتها وأفرادها، لذا تم إنشاء العديد من مشاريع الأمن المبكر في سبيل حماية المعلومات وسريتها.

وفي فترة الثمانينات ازدادت الهجمات الإلكترونية والتهديدات الجاسوسية، وظهرت مصطلحات جديدة على الساحة مثل فيروسات الحاسوب (Trojan Horse)، لينطلق بعدها

[1]– صلاح مهري هاوي الشمري، وزيد محمد علي إسماعيل، مرجع سابق، ص 277.

في عام 1987 أول برنامج تجاري لمكافحة الفيروسات، ثم توالت شركات تطوير برامج مكافحة الفيروسات في الظهور عام 1988، ومنها شركة (Avast)، وكان عمل المكافحة محصورا بالرد على الهجمات الحالية، وقد ساهم عدم وجود شبكة واسعة في الحد من نشر التحديثات.[1]

كما شهدت هذه الفترة تأسيس أول منتدى إلكتروني مخصص لأمن مكافحة الفيروسات، بالإضافة إلى تأسيس مطبعة مكافحة الفيروسات، لحماية بيانات مستخدمي الفضاء السيبراني من أي قرصنة إلكترونية إجرامية، وهو ما مهد لظهور الأمن السيبراني.

وقد أصبح المصطلح يستخدم على نطاق واسع بعد استخدامه من قبل الرئيس الأمريكي باراك أوباما في خطابه سنة 2009، ودعوته إلى تعزيز ما يسمى بالأمن السيبراني للولايات المتحدة الأمريكية بغية تعزيز الأمن القومي للدولة.

وحسب **جوزيف ناي** *(*Joseph Nye) فإن الفاعلين الأساسيين في الأمن السيبراني والمتحكمين فيه هم:[2]

أ-**الدول:** بغض النظر عن كونها صغيرة أو كبيرة، باتت مسألة الشراكة في الفضاء السيبراني ميسرة لأصحاب العقول، غير أن الهجومات السيبرانية ربما هي التي تحتاج إلى دول كبرى فاعلة تمتلك بنى تحتية سيبرانية لإحداث خسائر في أعدائها على المستوى الدولي.

ب-**الفواعل من غير الدول :** هي تلك الكيانات التي تجاري أو تنافس الدولة على سيادتها ، وهي أصغر في مقدراتها من الدول، لها أهداف تخريبية، تلجأ إلى مساعدة من الأجهزة الإستخباراتية العالمية لأجل القيام باختراق المواقع.

---

[1]-أثير الخندق، "**ما هو الأمن السيبراني؟ ومتى نشأ؟**"، متاح على الرابط:

https://bit.ly/395VxJW (2022/04/02)

[2]- إيهاب خليفة، "الأمن السيبراني: الماهية والإشكاليات"، مرجع سابق، ص 08.

ج-وسائط التواصل الاجتماعي العالمية الكبرى: أهمها "فيسبوك"،"غوغل" وتويتر"، تمتلك قدر من المعلومات مكنها من التفوق على الدول، ومن خلال تلك المعلومات تستطيع اختراق الأسواق السيبرانية، بل لها قدرة كبيرة على توجيه المجتمعات وتشكيل الرأي العام.

د-الجماعات الإرهابية:وهنا تتضح المخاطر الحقيقية للعالم السيبراني، إذ تستخدم هذه الجماعات الفضاء الإلكتروني بغية سرقة المعلومات، وتسهيل كل ما هو غير مسموح به مثل تجارة البشر والسلاح، في إطار السوق السوداء على الشبكة العنكبوتية.

هـ-الأفراد: قدرة الأفراد على الإختراقات الالكترونية حالة ويكليكس، إذ استطاع مخترق الأمن المعلوماتي الأميركي أن يهدد أكبر دولة في العالم، الولايات المتحدة الأميركية، ويكشف أوراقها وتحالفاتها حول الكرة الأرضية.

2- القوة السيبرانية Cyber Power:

ظهر هذا المصطلح في خضم الثورة المعلوماتية والاستخدام المتزايد للانترنيت، وأثار المصطلح جدلا واسعا حول تعريفه، لهذا تعددت التعاريف المقدمة له، ويعد جوزيف ناي (Nye Joseph) من أبرز المهتمين بالقوة السيبرانية أو ما يسميه بالقوة الناعمة، إذ أدخل مفهوم القوة الناعمة في العلاقات الدولية سنة 2004، في كتابه " Soft Power: The Means To Success In World politics" ، الذي قام بإصداره بعد الغزو الأمريكي للعراق، ثم رسخ لمفهوم القوة السيبرانية في سنة 2010 في كتابه Cyber Power.[1]

حيث عرف جوزيف ناي القوة السيبرانية بأنها: "القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة، والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات سيبرانية".[2]

---

[1]- صفاء تغريد و لبنى خميس مهدي، مرجع سابق، ص 150.

[2]- عمرو صبحي، "**تكتيك الدرع والسيف في استخدام القوة السيبرانية**"، متاح على الرابط: https://bit.ly/39aeXNt **(2021/02/12)**

في حين يعرفها **دانيال كوهل** (daniel T kuehl) على أنها القدرة على استخدام الانترنيت لخلق مزايا التأثير على الأحداث في البيئات التشغيلية كافة من خلال أدوات القوة.[1]

تتطلب القوة السيبرانية توفير أقصى درجات الأمن الالكتروني، عبر تبني مجموعة من السياسات الدفاعية الهادفة إلى حماية المعلومات وتطوير آليات الدفاع ضد الأخطار المحتملة، وهناك نمطين أساسيين للقوة السيبرانية:

- ✓ **نمط القوة الصلبة :** تعبير عن استخدام المقدرات والأدوات في عمل تخريبي، عبر قطع كابلات الاتصالات أو تدمير أنظمة المعلومات أو الأقمار الصناعية، وتنفيذ عمليات سرقة منظمة للمعلومات.
- ✓ **نمط القوة الناعمة :** أي استخدام القوة السيبرانية في جانب التأثير على الطرف الأخر، من خلال التلاعب بالمعلومات وتوظيفها لخدمة أغراض خاصة.

وفي ظل التطور التكنولوجي ودخول شبكات الاتصال والمعلومات إلى بنية الاستخدام الحربي ومجالاته، برزت القوة السيبرانية في العلاقات الدولية كمجال للتحليل الاستراتيجي، وهو ما يظهر جليا في الصراع بين **روسيا واستونيا** 2007، ثم الحرب بين **روسيا وجورجيا** 2008، كذلك الهجوم الإسرائيلي، بالاتفاق مع الولايات المتحدة، على البرنامج النووي الإيراني بفيروس "ستكسنت Stuxnet" في 2010، والذي دمر نحو ألف جهاز طرد مركزي إيراني، ثم فيروس "**فليم** Flame" في 2012، بالإضافة للهجمات الإلكترونية المجهولة على شبكة كهرباء أوكرانيا في سنة 2015، والتي تسببت في تعطيلها ، ثم الحدث الأبرز من خلال التدخل الروسي في التلاعب بالانتخابات الأمريكية لصالح مرشح الحزب الجمهوري دونالد ترامب.[2]

3-الفضاء السيبراني: يعرفه الاتحاد الدولي للاتصالات ووكالة الأمم المتحدة المتخصصة في مجال تكنولوجيا المعلومات والاتصالات بأنه "الحيز المادي وغير المادي الذي ينشأ أو

---

[1]- إيهاب خليفة، "الأمن السيبراني: الماهية والإشكاليات"، مرجع سابق، ص 5.

[2]- عمر حامد شكر، **المجال الخامس الفضاء الإلكتروني**. المعهد المصري للدراسات، 2019، (د.ب.ن)،ص 10.

يتكون من جزء أو من كل العناصر التالية: حواسيب أجهزة ممكنة وشبكات ومعلومات محوسبة وبرامج ومضامين ومعطيات مرور ورقابة والذين يستخدمون كل ذلك.[1]

وعرفته الوكالة الفرنسية لأمن أنظمة الأعلام ANSSI وهي وكالة حكومية مكلفة بالدفاع على أنه :"فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية".[2]

ومن خلال استقراء خصوصيات الفضاء السيبراني يمكن تمييز ما يلي:[3]

- ✓ مجال عملياتي إذ يعد الفضاء السيبراني الميدان الخامس للحروب المدنية.
- ✓ تعد البنى التحتية لأنظمة الاتصالات وتقنية المعلومات جزء أساسي من الفضاء السيبراني.
- ✓ الفضاء السيبراني لا يقتصر على شبكة الانترنت فقط، إنما على شبكات عالمية وخاصة أخرى مثل:GPS / ACARS/ SWIFT/ PSTN.

يعتبر الفضاء السيبراني واحدا من المحددات الجديدة للقوة وأبعادها، من حيث طبيعتها وأنماط استخدامها، بل وأيضا طبيعة الفاعلين،وهو ما كان له انعكاس على قدرات الدول، وأضفى خصائص جديدة للقوة.

ويمكن القول أن الفضاء السيبراني هو مجال عالمي داخل بيئة المعلومات، تم تشكيله من خلال استخدام الإلكترونيات واستغلال المعلومات عبر الشبكات المترابطة والمرتبطة باستخدام تكنولوجيا المعلومات والاتصالات، وهو امتداد للوسائط الرقمية عبر خطوط نقل مختلفة معدنية وألياف بصرية ولا سلكية وقنواتها على شبكات الإنترنت، إذ يعد الفضاء السيبراني التعبير التكنولوجي الفائق السرعة للمعلومات.

---

[1]- صفاء تغريد و لبنى خميس مهدي، مرجع سابق، ص 149.

[2]- علاء الدين فرحات، الفضاء السيبراني تشكيل ساحة المعركة في القرن الحادي والعشرين"، **مجلة العلوم القانونية والسياسية** ، المجلد 10، العدد3،2019،ص92.

[3]-. صفاء تغريد و لبنى خميس مهدي، مرجع سابق، ص 150.

4-الردع السيبراني: يعرف الردع على أنه منع الخصم من القيام بفعل عدائي إما بسبب تخوفه من هجوم مضاد يفوق قدراته الدفاعية، أو ارتفاع تكلفة الهجوم مقارنة بالمكاسب التي يمكن أن يحققها.[1]

أما الردع السيبراني فهو منع الأعمال الضارة ضد الأصول الوطنية في الفضاء و الأصول التي تدعم العمليات الفضائية.[2]

وهو قدرة الدولة على تطوير قدرات عسكرية موثوقة ومتبادلة ومتماثلة في الفضاء الالكتروني، وتكون قادرة على التأثير في قرارات الخصم ومنعه من شن هجمات عسكرية عبر الفضاء الالكتروني.[3]

يقوم الردع السيبراني على ثلاث مرتكزات في مجال إستراتيجية الدفاع متمثلة في: مصداقية الدفاع،القدرة على الانتقام، الرغبة في الإنتقام.

---

[1]-إيهاب خليفة، **مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي** ،العربي للنشر والتوزيع، القاهرة، 2019،ص 160.

[2]-رغدة البهي، "الردع السيبراني:المفهوم والإشكاليات والمتطلبات"، **مجلـــة الدراسات الإعلاميـــة**، العدد 01، يناير 2018، ص 202.

[3]-إيهاب خليفة، **مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي**، مرجع سابق، ص 161.

المبحث الثاني: مظاهر التهديدات السيبرانية

تتعدد مظاهر التهديدات السيبرانية وتتنوع، لذا سيتم التطرق في هذا المبحث إلى أهم أنماط التهديدات السيبرانية:

المطلب الأول: الهجمات السيبرانية

1-مفهوم وخصائص الهجمات السبيرانية: هناك عدة تعاريف لمصطلح الهجمات السيبرانية:

تعرف الهجمات السيبرانية على أنها: "فعل يقوض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام".[1]

يعرفا فيورتش (Fuertes) بأنها هجوم عبر الانترنيت، يقوم على التسلل إلى مواقع الكترونية غير مرخص بالدخول إليها، بهدف تعطيل أو إتلاف البيانات المتوفرة فيها أو الاستحواذ عليها.[2]

ويعرفها **مايكل شميت** على أنها:"مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية بهدف التأثير والإضرار بها، أو للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة".[3]

يعرفه كل من **زيمت وباري** (zimet et barry) على أنها" مجموعة من العمليات القائمة على الحرب الإلكترونية والخداع النفسي، فضلا عن استهداف شبكة تواصل العدو العسكرية وعملياته الأمنية الإلكترونية".[4]

---

[1]- منى عبد الله السمحان، "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود"، **مجلة كلية التربية**، العدد 111، 2020، ص11.

[2]- نور أمير الموصلي، "**الهجمات السيبرانية في ضوء القانون الدولي الإنساني** "، بحث مقدم لاستكمال متطلبات نيل درجة ماجيستر التأهيل والتخصص في القانون الدولي الإنساني، الجامعة الافتراضية السورية، 2021، ص 9.

[3]-أميرة عبد العظيم محمد عبد الجواد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، **مجلة الشريعة والقانون**، العدد53، الجزء3، 2020، ص 395 .

[4]-أحمد عبيس نعمة الفتلاوي، "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، **مجلة المحقق الحلي للعلوم القانونية والسياسية**، العدد 4، السنة8، 2016، ص 616.

أما فيما يتعلق **باللجنة الدولية للصليب الأحمر** فقد عرفت الهجوم السيبراني على أنه استخدام أنشطة متعددة، لتغيير أو إفساد أو خداع أو إضعاف أو تدمير أنظمة الحاسوب أو شبكات الحاسوب للخصم أو المعلومات أو البرامج المدرجة في هذه الأنظمة أو الشبكات التي ترسل من خلالها، وقد تؤثر هذه الأنشطة أيضا في الكيانات المرتبطة بهذه الأنظمة والشبكات.[1]

كما يعرفها **جونيدو ماشال** على أنها: "عملية الاستغلال المتعمد لأنظمة الكمبيوتر والشبكات المعتمدة على التكنولوجيا من خلال البرمجيات الضارة".[2]

غير أن خبراء القانون الدولي في **دليل تالين** الصادر عام 2013 عرفوا الهجمات السيبرانية على أنها: "عمليات سيبرانية، سواء كانت هجومية أو دفاعية، يهدف من خلالها التسبب بالإصابة أو الوفاة لأشخاص أو الإضرار وتدمير الأهداف".[3]

من خلال التعريفات السابقة وكتعريف إجرائي، يمكن أن نعرف الهجومات السيبرانية بأنها هجوم يقوم به مجموعات أو منظمات أو حتى دول وحكومات، بغية تحقيق هدف معين من خلال الدخول غير المشروع إلى مواقع إلكترونية، أو معلومات خاصة بطرف معين قصد التغيير فيها (بالحذف أو الإضافة)، أو تسريبها، أو تشفيرها وتغيير رموز المرور لمنع الوصول إليها من قبل صاحبها، وهو ما يمس بسرية معلومات الطرف المقصود من الهجوم السيبراني، وهذا من خلال مجموعة من البرامج والتطبيقات الضارة والفيروسات.

تشترك الهجومات السيبرانية والجرائم السيبرانية في المجال الذي تحدث فيه، غير الأولى تهدف إلى جمع معلومات وتحقيق دوافع سياسية أما الثانية فهدفها تحقيق مكاسب مالية وإحداث اضطراب، إضافة إلى أن مرتكبي الهجمات السيبرانية هم الدول والمجموعات

---

[1]– نور أمير الموصلي، مرجع سابق، ص 9.

[2]–سامي محمد بونيف، "دور الاستراتيجيات الإستباقية في مواجهة الهجمات السيبرانية: الردع السيبراني نموذجا"، **المجلة الجزائرية للحقوق والعلوم السياسية**، المجلد 04، العدد07، جوان 2019، ص 124.

[3]– نور أمير الموصلي، مرجع سابق، ص 10.

الحكومية وغير الحكومية ضد دولة أخرى، بهدف استهداف الأمن القومي والسياسي لها عن طريق تخريب البنى التحتية لها وزعزعة الاستقرار فيها، في حين الجرائم السيبرانية يقوم بها الأفراد ضد مؤسسات مالية أو شركات بهدف التسلية وتحقيق مكاسب شخصية عبر اختراق الحواسيب والتسلل إلى المصارف والتلاعب بالحسابات.[1]

تعتبر الجرائم السيبرانية إحدى أهم الجرائم المعاصرة وواحدة من أهم التهديدات السيبرانية، ارتبط ظهورها مع التطور التكنولوجي ودخول العالم العصر الرقمي، الذي وسع من اعتماد الحكومات والخواص على الفضاء السيبراني الذي أصبح كل التعاملات وتبادل المعلومات عبره.

تتميز الهجومات السيبرانية في معظمها بالطابع الدولي، فهي عابرة للحدود، وقد تتضمن أكثر من عنصر، إضافة إلى كونها تتميز بالتشعب، فيمكن أن تحدث في بلد في حين أثارها تكون في بلد أخر وهو ما يزيد من خطورة الوضع، كما أنه يصعب تحديد مصدرها والجهات التي تقف وراء تنفيذها، وفي معظمها لا يتم الوصول إلى منفذيها، ويبين الشكل التالي الأطراف التي يمكن أن تقوم بهجمات سيبرانية:

[1]– المرجع نفسه، الصفحة نفسها.

الشكل رقم01: الجهات التي تقوم بالهجمات السيبرانية ودوافعها وأهدافها.[1]

نظرة أقرب على الهجمات السيبرانية

الجهات التي تقف وراء هذه الحوادث لا تشمل فقط مجرمين يزدادون جرأة، بل تشمل أيضا دولا ومجموعات ترعاها دول، تختلف أهداف ودوافع كل منها.

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

والأكثر خطورة أنها لا تطال جهة واحدة فقط، فيتضرر منها الأفراد والمنظمات والشركات والحكومات والدول، من جهة أخرى فالهجومات السيبرانية يشترك فيها أفراد وجماعات إجرامية منظمة، وحتى هذه الجماعات المنظمة قد تتكون من أفراد من عدة بلدان يقودها مركز في دولة وفروع في دول أخرى، ومرتكبيها يمتلكون أحدث التقنيات في تنفيذ هجماتهم، مما يحقق لهم النتائج المرجوة عبر إلحاق الضرر المطلق بضحيتهم.

ويؤكد الاتحاد الدولي للاتصالات في دراسة صادرة عنه أن وضع إستراتيجية لمكافحة التهديدات والجرائم السيبرانية هو عنصر لا يتجزأ من إستراتيجية الأمن السيبراني.[2]

تتميز الهجمات السيبرانية بسهولتها وقلة تكلفة وسائل تنفيذها، حيث يمكن للجهة التي تقوم بها (دول، أفراد، أو مؤسسات) أن تلحق أضرار وخيمة على المقصود بتكلفة بسيطة،

---

[1]– التمويل والتنمية،" التهديد السيبراني العالمي"، التمويل والتنمية،(د.ب.ن)، 2021 ،ص25.

[2]– اللجنة الاقتصادية والاجتماعية لغربي آسيا إلإسكوا، **الأمن في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية توصيات سياساتية**، الأمم المتحدة، نيويورك، 2015، ص 17.

كما أن هذه الهجمات تكلف 4% فقط من تكلفة القوة العسكرية، وهي تحقق ما لا تحققه الحرب التقليدية، ولعل هذا هو ما أدى إلى تزايد عدد الهجمات، إذ تشير الإحصائيات إلى حدوث هجوم واحد كل 39 ثانية[1] .

وفي شهر واحد سنة 2017 تعرض أكثر من 74 دولة في العالم لهجمات إلكترونية متزامنة خطيرة، أدت إلى مجموعة من التعطيلات، وأصابت دولا عظمى منها الصين وروسيا، فمثلا حجم الخسائر التي يتكبدها العالم تقدر بمليارات الدولارات سنويا جراء الهجمات الإلكترونية، وتخلف الهجمات السيبرانية عبر العالم خسائر عظمى إذ تشير الإحصائيات إلى حوالي 6 تريليونات دولار فقط في عام 2021.

وللهجمات السيبرانية تأثير مدمر، إذ تؤدي إلى إحداث شلل تام في البنية التحتية للدول، فهجوم سيبراني واحد كفيل بتعطيل كل شيء دفعة واحدة بغض النظر عن المدة الزمنية التي يستغرقها هذا التعطيل، وفي تقرير أعدته لجنة الدفاع والأمن القومي بالبرلمان البريطاني وصف الهجمات السيبرانية بأنها: "أكثر دمارا من التفجير الذري، باستطاعتها تدمير أنظمة الإلكترونيات، ومحطات ضخ المياه، والهواتف، ومحطات الإذاعة والتلفزة، وتوقيف الاتصالات، وانهيار الأنظمة المالية".[2]

3-تطور الهجمات السيبرانية:

ارتبط ظهور الهجمات السيبرانية وتطور أشكالها وأنواعها بمجموعة من العوامل، بداية من ظهور أجهزة الكمبيوتر مطلع الخمسينات من القرن العشرين كأداة لحفظ المعلومات رقميا، وتطور ذلك وصولا إلى مرحلة أصبح فيها جهاز الكمبيوتر لا يمكن الاستغناء عنه في كل المؤسسات، وتزايد ت أهمية دور الكمبيوتر مع ظهور شبكة الانترنيت واتساع استخدامها وانتشارها بسبب سرعتها في نقل المعلومات، ما جعل الدول مع مطلع التسعينات

---

[1]- داليا السيد،"**الهجمات السيبرانية... تهديد متعاظم للأمن والاستقرار والاقتصاد العالمي**"، متاح على الرابط: https://bit.ly/3xbO6J9(2022/02/22)

[2]- المرجع نفسه.

من القرن العشرين تسعى إلى تحسين استخدام الانترنيت، لأجل إحداث قفزات نوعية في المجال الأمني والعسكري، غير أن هذا التوسع في الاعتماد على الانترنيت والقدرة على الوصول على المعلومات، أدى إلى وصول أطراف متعددة إلى منظومة المعلومات للدول والحكومات، مما عرضها في عديد من الأحيان إلى هجومات سيبرانية اخترقت بناها التحتية وعطلت خدماتها أو سربت ما لا يجوز تسريبه.[1]

من جهة أخرى ساهمت الثورة الرقمية والمعلوماتية التي شكلت مجتمعا رقميا حسب تعبير **ألفين وهايدي توفلر** (Alvin Toffler)في تسهيل قدرة الوصول إلى المعلومة، لاسيما مع مطلع التسعينات، حيث أصبح العالم قرية صغيرة، وتزايد التفاعل داخل الفضاء الإلكتروني الذي يحوي العديد من العناصر والمعلومات في مختلف الجوانب الأمنية والإقتصادية والسياسية، وفسح هذا التطور المجال أمام الفواعل الدولاتية وغير الدولاتية للقيام بهجمات الكترونية تحدث أضرار بالغة الخطورة وتؤثر على الأمن القومي للدول.

ارتبطت الهجمات السيبرانية في الثمانينات بما يسمى بالهاكرز، أي مجموعة من المبرمجين الأذكياء الذين يتحدون الأنظمة المختلفة ويحاولوا اقتحامها بغية تحقيق مكاسب مالية أو إبراز أنفسهم، غير أنه ومع مطلع التسعينات تزايد عدد الهجمات وأصبحت مواقع الانترنيت أكثر عرضة لها، وأشهر أنواع الهجمات هنا نجد تعطيل النظام التقني ومنعه من القيام بعمله المعتاد، والذي يتسبب في انقطاع النظام عن الخدمة لمدة زمنية قصيرة مما يؤدي إلى خسائر مالية فادحة، وأشهر الهجمات في هذه الفترة نجد: **دودة موريس** الفيروس الالكتروني الذي نشر عبر ألاف الكمبيوترات سنة 1988، وفي سنة 1990 نجد ما عرف بعملية Ip-spoofing ثم بروز قضية الجحيم العالمي الذي اختص بها مكتب التحقيقات الفيدرالية، إضافة إلى حادثة شركة أوميغا وفيروس ميلسا.[2]

---

[1]- علاء الدين فرحات، مرجع سابق،ص92.

[2]–طلال ياسين العيسى، عدي محمد عناب،"المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر"، **مجلة الزرقاء للبحوث والدراسات الإنسانية**، المجلد 19،العدد01، 2019، ص83.

من أهم الهجمات السيبرانية التي تعرض لها العالم نجد:[1]

- ✓ تعطيل الخدمات العمومية لإستونيا من قبل روسيا في 27 أفريل 2007 بحيث تعطلت مؤسسات الدولة ولم تعد قادرة على العمل.
- ✓ هجوم فيروس إسرائيلي على أنظمة الدفاع أرض–جو السورية، وهو ما جعلها معطلة وغير قادرة على توفير الأمن لقاذفات القنابل الإسرائيلية أثناء هجومها على المفاعل النووي السوري.
- ✓ انخراط الجيش الجورجي والروسي أثناء حرب أوسيتيا الجنوبية سنة 2008 في حرب سيبرانية، نتج عنها اختراق عدة مواقع رسمية لجورجيا بهدف زعزعة الاستقرار فيها نفسيا.
- ✓ هجمات رفض الخدمة ضد مواقع الحكومة المالية ووسائل الإعلام الكورية الجنوبية والولايات المتحدة 13 سنة 2009.
- ✓ تعرض إيران لهجوم سيبراني من قبل إسرائيل والولايات المتحدة الأمريكية بواسطة دودة الكمبيوتر **ستكسنت**، بغرض إصابة أنظمة نظنز للطاقة النووية ومحطة بوشهر للطاقة النووية مما أدى إلى إبطاء تطوير محطة الطاقة النووية الإيرانية.
- ✓ نجاح إدخال فيروس إلى قاعدة نيفادا الجوية سنة 2011 في إصابة نقاط تفتيش الطائرات الأمريكية بدون طيار المنتشرة في أفغانستان وتعطيلها بالكامل لمدة قصيرة.
- ✓ استهداف شركة النفط السعودية أرامكو وشركة الغاز الرباعي رأس غاز من قبل فيروس كمبيوتر في 2012 الذي عطل حوالي 30 ألف جهاز كمبيوتر لشركة أرامكو.
- ✓ تعرض ستة بنوك أمريكية كبرى في 2012 لهجوم سيبراني من قبل مجموعة من المتسللين وقد اتهم الأمريكيون إيران بالوقوف وراء هذه الهجمات.

---

[1]– معهد التطوير،"**معنى هجوم سيبراني وأنواع الهجمات السيبرانية**"، متاح على الرابط:
https://bit.ly/38VPc3p (2022/02/15)

4-أنواع الهجمات السيبرانية من أهم طرق الهجوم نجد:[1]

أ- **التجسس:** هذا النوع من الهجمات يمثل تهديدا كبيرا وحقيقيا للأمن القومي لمختلف الدول، لأنه يهدف لاختراق نظم حماية وتأمين الشبكات الإلكترونية لهذه المؤسسات، والتجسس عليها ونقل المعلومات منها وقرصنة وسرقة المعلومات السرية التي لم يتم تأمينها بشكل صحيح بحيث يتم قرصنتها بواسطة استخدام برامج خبيثة وفيروسات، وتسمى أيضا ب **أحصنة طروادة،** من الأمثلة الواردة هنا نجد: الهجوم السيبراني الذي تعرضت له الولايات المتحدة الأمريكية في شهر ديسمبر 2020، بحيث تم اختراق بنجاح مؤسسات حيوية وحساسة كوزارات الدفاع والخارجية والخزانة والتجارة والطاقة والأمن الداخلي، ومجموعة من الوكالات الفيدرالية الرسمية ومراكز الأبحاث والمنظمات غير الحكومية.

ب-استهداف البنى التحتية الحساسة والتعطيل التام عن الخدمة : من هذه البنى محطات الطاقة وتوزيع المياه وأنابيب النفط والاتصالات ووسائل النقل والمستشفيات، من أمثلتها الهجوم السيبراني الذي استهدف خط أنابيب نفط **كولونيال بايبلاين** في الساحل الشرقي بالولايات المتحدة في ماي 2021، والذي أدى لنقص واسع النطاق في إمدادات الطاقة بجميع أنحاء الولايات المتحدة، خاصة أن هذا الخط ينقل ما لا يقل عن 45 بالمئة من البنزين والديزل والكيروسين الأمريكي من مصافي التكرير في خليج المكسيك إلى الساحل الشرقي للولايات المتحدة.

كما تستهدف أيضا مؤسسات الرعاية الصحية كاختراق نظام الرعاية الصحية في جمهورية إيرلندا في ماي 2021 من جانب قراصنة مجهولين، الأمر الذي أثر بالسلب على معظم الخدمات الصحية. وتسجل الدول الأوروبية أكبر نسبة للهجمات على أنظمة الرعاية الصحية.

[1]- داليا السيد، مرجع سابق.

ج-استهداف المنشآت ذات الطابع العسكري: مثل المحطات النووية والأقمار الصناعية ومحاولة تخريبها وإحداث أكبر ضرر بها، نجد هنا استهداف أجهزة الطرد المركزي للمفاعل النووي الإيراني بفيروس **ستاكسنت**، من قبل الولايات المتحدة وإسرائيل طورتا هذا الفيروس عام 2010 بعد استخدامه لمهاجمة منشأة لتخصيب اليورانيوم في موقع نطنز النووي الإيراني، وكان هذا أول مثال معروف لفيروس يستخدم لمهاجمة معدات صناعية ومنشآت نووية، وهذا الهجوم يعتبر من أشهر أنواع الهجمات السيبرانية على الإطلاق.[1]

المطلب الثاني: الإرهاب الإلكتروني

يمثل الإرهاب الإلكتروني واحدا من أهم مظاهر التهديدات السيبرانية، بحيث تعددت الدراسات المقدمة حوله، كما اختلفت التعاريف المقدمة له:

1-تعريف الإرهاب الالكتروني: لم تتضمن الكتب القديمة معنى كلمة إرهاب بسبب حداثة ظهور المصطلح واستخدامه، فنجد أن المفهوم اللغوي للمصطلح مشتق من كلمة أخافه رَهِبَ، بالكسر، يَرْهَبُ رَهْبَةً ورُهْباً، بالضم، ورَهَباً، بالتحريك، أَي خافَ، ورَهِبَ الشيءَ رَهْباً ورَهَباً ورَهْبةً: خافَه، أما مصطلح الإرهابي فهو وصف يتم إطلاقه على الذين يسلكون سبيل العنف والإرهاب لتحقيق أهدافهم.[2]

يعرف الإرهاب على أنه الاستخدام غير المشروع للقوة، والعنف ضد الأشخاص والممتلكات لترويع وإجبار الحكومات أو الأفراد لأجل تحقيق أهداف إجتماعية أو سياسية.[3]

عرفه **ابن خلدون** في كتابه المقدمة على أنه: "القهر والبطش بالعقوبات والتنكيل، والكشف عن عورات الناس".[4]

---

[1]- طلال ياسين العيسى، عدي محمد عناب، مرجع سابق، ص 86.

[2]-إبن منظور، **لسان العرب**. دار صادر، بيروت، (د.س.ن)، ص 436.

[3]- لحمر حميدة وحموم فريدة، "التعاون الأمني في جنوب شرق آسيا في مواجهة التهديدات الأمن السيبراني"، **مجلة طبنة للدراسات العلمية الأكاديمية**، العدد 01، المجلد 4، 2021،ص 532.

[4]-منى الأشقر جبور، **السيبرانية هاجس العصر**، المركز العربي للبحوث القانونية والقضائية،(د.ب.ن)،(د.س.ن)، ص81.

عرف قاموس **أكسفورد** كلمة الإرهاب بأنها "استخدام العنف والتخويف بصفة خاصة لتحقيق أغراض سياسية".[1]

أما **الموسوعة السياسية** فقد عرفت الإرهاب على أنه:" استخدام العنف غير القانوني أو التهديد به، بأشكاله المختلفة كالاغتيال والتشويه والتخريب والنسف، بغية تحقيق هدف سياسي معين مثل كسر روح المقاوم ة والالتزام عند الأفراد، وهدم المعنويات عند الهيئات والمؤسسات، أو كوسيلة من وسائل الحصول على معلومات، وهو استخدام الإكراه لإخضاع طرف مناوئ لمشيئة الجهة الإرهابية".[2]

تعرفه "اتفاقية جنيف" 1937 الخاصة بمنع وقمع الإرهاب على أنه: "الأعمال الإجرامية الموجهة ضد دولة، والتي يكون من شأنها إثارة الفزع والرعب لدى شخصيات معينة أو جماعات من الناس أو لدى الجمهور".[3]

وفي قرارها رقم 94/60 الصادر سنة 1994 قدمت الجمعية العامة للأمم المتحدة محاولة لتعريف الإرهاب، وحسبها فالإرهاب عبارة عن "الأعمال والطرق والممارسات التي تشكل مخالفة صارخة لأغراض ومبادئ الأمم المتحدة، والتي قد تشكل تهديدا للسلام والأمن العالميين، وتهديد علاقات الصداقات بين الدول، وتعيق التعاون الدولي وتهدف إلى تدمير حقوق الإنسان والحريات الأساسية والأسس الديمقراطية للمجتمع".[4]

نتيجة لتعدد أنواع الإرهاب وطرقه وممارسيه والأهداف المرجوة منه والجهات المستهدفة منه، يجد المختصين صعوبة في إيجاد تعريف موحد أو متفق حوله للإرهاب،

---

[1]–منى جلال عواد،" مقاربة تحليلية لظاهرة الإرهاب الالكتروني"، **مجلـــة تكريت للعلوم السياسية**، العدد 19، 2020، ص 28.

[2]–وفاء لطفي، "الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني: التجربة الماليزية نموذجا "، **مجلة دراسات**، المجلد23، العدد1، 2022. 158.

[3]– منى الأشقر جبور، مرجع سابق، ص 82.

[4]– منى جلال عواد، مرجع سابق، ص 29.

بحيث وصل عدد التعاريف المقدمة له إلى 109 تعريف، غير أن جل التعاريف المقدمة تشترك في الطابع العنيف للإرهاب وفي النتيجة المدمرة له.

وتتعدد أنواع الإرهاب من إرهاب تقليدي إلى إرهاب حديث مرتبط بالتطور التكنولوجي والتحول في امتلاك القوة، بحيث نتج عن قدرة وصول فواعل غير دولاتية إلى القوة الالكترونية وامتلاكها القدرة على التأثير بواسطتها إلى ما يعرف بالإرهاب السيبراني، والذي هو بالأساس تزاوج مابين الإرهاب والتكنولوجيا، ويعتبر جوزيف ناي الإرهاب الإلكتروني من بين أهم التهديدات الجديدة.

وتعود البدايات الأولى لاستخدام مصطلح الإرهاب السيبراني إلى فترة الثمانينات من القرن الحادي والعشرين، من قبل الباحث الكندي **باري كولن** barry cillin الذي خلص في دراسته إلى صعوبة تقديم تعريف للإرهاب التكنولوجي واستبدله بالإرهاب الالكتروني والذي عرفه على أنه "هجمة الكترونية غرضها تهديد الحكومات أو العدوان عليها، لتحقيق أهداف سياسية أو دينية أو إيديولوجية،وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي ومكافئ للأفعال المادية للإرهاب".[1]

في 1980 كان المصطلح يشير إلى الهجمات التي يستخدم فيها الكمبيوتر ضد اقتصاد وحكومة الولايات المتحدة، ومع بداية التسعينات ونتيجة لتزايد انتشار أدوات تكنولوجيا الاتصال والمعلومات والاعتماد الكبير على التكنولوجيا بدأ المفهوم.

أما مجمع الفقه الإسلامي، فيعرف الإرهاب السيبراني على أنه " العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الالكترونية، ويكون صادرا عن الدول أو

[1]–عادل عبد الصادق، **الإرهاب الالكتروني: القوة في العلاقات الدولية: نمط جدد وتحديات مختلفة** ، مركز الدراسات السياسية والإستراتيجية، القاهرة، 2009، ص 111.

الجماعات أو الأفراد على الإنسان أو دينه أو نفسه أو عرضه أو عقله أو ماله، بغير حق بشتى صنوفه (العدوان) وصور الإفساد في الأرض".[1]

وتعرف وكالة المخابرات المركزية الأمريكية الإرهاب السيبراني على أنه:" اعتداء قصدي، ذي دوافع سياسية، على المعلومات، أو النظام المعلوماتي أو البرامج أو البيانات، ينتج عنه أعمال عنف ضد مدنيين، سواء ارتكبته مجموعة وطنية أو عملاء غير مرئيين".[2]

أما اللجنة الدولية للصليب الأحمر فتعرف الإرهاب السيبراني بأنه: "عمليات تشن ضد أو عبر حاسوب بواسطة تيار بيانات، وتهدف إلى تحقيق أغراض منها اختراق النظام المعلوماتي أو جمع أو نقل أو تشفير البيانات أو التلاعب بها من قبل منفذ عملية الاختراق، واستخدام هذه الوسائل لتدمير أو تعطيل مجموعة متنوعة من الأهداف في العالم الحقيقي كالصناعات والبنى الأساسية".[3]

تعتبر الجماعات الإرهابية أحد أهم الفواعل في الإرهاب الإلكتروني حيث يتم التعبئة والحشد عبر الفضاء الإلكتروني ، إذ تمثل تنظيم القاعدة نموذجا يجسد استخدام الجماعات الإرهابية للفضاء الالكتروني من خلال الاعتماد على الانترنيت في الحشد والتجنيد والتعبئة والتمويل من خلال موقعها النداء، إضافة إلى تنظيم داعش الذي يملك أكثر من 53 ألف موقع الكتروني و 90 ألف صفحة باللغة العربية، ولا يقتصر استخدام الإرهاب الالكتروني على هذه الجماعات فقط، بل أحيانا تكون الدول إحدى الفواعل أيضا من خلال استخدام الفضاء الالكتروني في مجال الاستخبارا ت ضد دول أخرى أو عن طريق التحالف مع تنظيمات إرهابية، وارتفع عدد المواقع الالكترونية للإرهابيين من 12 موقع الكترونيا في

[1]–ياسين أحمد صالح،"الإرهاب الإلكتروني في ظل أزمة فيروس كورونا:الأنماط والتداعيات"، **مجلة كلية السياسة والاقتصاد**، العدد 9، 2021، ص24.

[2]– عادل عبد الصادق، مرجع سابق، ص 113.

[3]– ياسين أحمد صالح، مرجع سابق، ص 25.

1997 إلى 4350 موقع قي 2005 وإلى 4800 موقع في 2006 وأكثر من 6000 موقع الكتروني في 2008. [1]

إن كون المعلومات متاحة أمام الجميع فقد أصبح الفرد واحدا من الفواعل أيضا في الإرهاب الإلكتروني.

يهدد الإرهاب الإلكتروني المجتمع الدولي ككل، فهو يتميز بالتشعب والتداخل والتوسع عبر مجموعة من الدول، يعود اعتماد الجماعات والتنظيمات الإرهابية للفضاء السيبراني لعدة أسباب من بينها:[2]

- ضمان السرية في العمل ونقل المعلومات وتبادلها بين أفراد التنظيمات، إضافة لصعوبة تحديد مركز الهجمة الإرهابية والجهة المسؤولة عنها، وبالتالي عدم معاقبة مرتكبيها ما يشجعهم على إعادة الهجمة مرة أخرى.
- تحقيق الانسجام والتنسيق بين أعضاء التنظيم عبر ضمان استمرارية نقل وتبادل المعلومات والأفكار.
- انخفاض التكلفة المالية، فلا يحتاج إلى أسلحة عسكرية وتكلفة مالية بل يستخدم القوة الناعمة في ممارساته.

وتعتمد التنظيمات الإرهابية في إرهابها على مجموعة من الوسائل أهمها:

أ-مواقع التواصل الاجتماعي: أخصب مكان لعمل التنظيمات الإرهابية، والوسيلة الفعالة في أعمالهم الإجرامية، بحيث يستخدمون شبكة التواصل الإجتماعي **فايسبوك وتويتر** لإنشاء منصات وصفحات خاصة بهم بلغات مختلفة، ينشرون عبرها أفكارهم وإنجازاتهم وأبطالهم

---

[1]-علي عبد الرحيم العبودي، "هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين "، **مجلة قضايا سياسية** ، العدد 57، 2019، ص 103.

[2]– عبد الله جعيجع، "تطور الإرهاب وانعكاسه على استقرار المجتمعات: قراءة في ظاهرة الإرهاب الالكتروني وإستراتيجية المواجهة"، **مجلة دفاتر السياسة والقانون**، المجلد 13، العدد 01، 2021،ص 548.

وأهدافهم السياسية والإيديولوجية للترويج لأفكارهم، وهذا لجلب أكبر عدد من المنظمين إلهم ولكسب الدعم والتأييد، ولمهاجمة الحكومات والأجهزة الأمنية مما يؤثر على الأمن الدولي.

وتشير الإحصائيات أن وسائل التواصل الاجتماعي تمثل 90% من وسائل التواصل المستخدمة بين التنظيمات الإرهابية، كقناة لتبادل الخطط والمعلومات وتصنيع القنابل والمتفجرات ومهاجمة المواقع المستهدفة، إضافة إلى جمع التبرعات والتحويل بين الحسابات وتجنيد الأفراد.[1]

ب-البريد الإلكتروني: يتميز البريد الإلكتروني بالسرعة في تبادل الرسائل والتواصل بين الأفراد، وكان أول وسيلة استعان بها الإرهابيون في التخابر وتبادل المعلومات، نجد هنا مثلا تنظيم القاعدة ودوره في ما سمي بالجهاد الالكتروني.[2]

ج-**تدمير مواقع الخصوم:** عن طريق التجسس واختراق شبكات المعلومات الرسمية للوزارا ت والإدارات الحكومية والمصارف، بغية تخريبها والحصول على الأسرار منها وتدمير مواقعها، نجد هنا **جوليان أسانج** صاحب موقع **ويكليكس** والذي استطاع تسريب عدد كبير من برقيات الخارجية الأمريكية والذي أضعف صورة الولايات المتحدة الأمريكية.

3-التزاوج بين الإرهاب والتكنولوجيا:

نتيجة للتقدم الهائل في وسائل الاتصال والثورة العلمية في مجال تكنولوجيا المعلومات والانترنيت، ظهر التنافس بين الفواعل في

النظام الدولي حول التفوق التكنولوجي الذي يمكنها من تحقيق قوة اقتصادية، رافق هذا التطور ظهور فواعل أخرى من غير الدول تسعى هي الأخرى إلى فرض وجودها عن طريق التدمير والتخريب.

---

[1]-عمار ياسر زهير البابلي، "التحديات الأمنية المعاصرة للإرهاب السيبراني"، **الفكر الشرطي**، المجلد 30، العدد 118، 2021، ص 44.

[2]- عبد الله جعيجع، مرجع سابق، ص 447.

لقد كان لشبكات تكنولوجيا الاتصال والمعلومات دورها في تحويل الإرهاب إلى تهديد عالمي يهدد الأمن القومي ككل، وأصبحت التكنولوجيا من أهم الوسائل الداعمة للأعمال الإرهابية، من خلال سرعة انتشاره وتعاظم أثره بحيث أصبح من ميزات الأعمال الإرهابية هو التدمير واتساع نطاق المتضررين منه، إذ يمكن أن يمتد التأثير إلى عدة دول، من جهة أخرى ساهم هذا التزاوج بين الإرهاب والتكنولوجيا في جعل التنظيمات عابرة للحدود والقارات تتجاوز في أعمالها حدود الدول، إذ تقوم الجماعات الإرهابية باستخدام الفضاء الالكتروني للتخطيط وتنفيذ عملياتهم الإرهابية في مختلف دول العالم.

خلاصة واستنتاجات:

يعد مفهوم التهديدات السيبرانية من المفاهيم الجديدة في حقل العلاقات الدولية والدراسات الأمنية، كونه مرتبط بالتطورات التقنية والتكنولوجية وثورة المعلومات التي غيرت من طبيعة التهديدات ومن طرق الإستجابة لها ومواجهتها.

وتتعدد أنواع التهديدات السيبرانية، ويعد الإرهاب الإلكتروني والهجمات السيبرانية من أهم أنواعها، وهي مخاطر مصدرها الفضاء الإلكتروني، وتمثل تهديدا رهيبا للأمن القومي والعالمي نظرا لما تلحقه من أضرار وخيمة، فتزاوج الإرهاب مع التكنولوجيا وسع من حدوده وزاد من حدته.

الفصل الثاني:

تطور التهديدات السيرانية وتأثيرها على الأمن الدولي

مثلت التحولات والتغيرات الكبيرة التي شهدتها فترة ما بعد الحرب الباردة منعرجا حاسما عل مستوى التنظير في العلاقات الدولية، فكان التغير في العديد من المفاهيم الكلاسيكية، والتي من أهمها مفهوم القوة وطبيعة القوة والحرب، رافق هذا التغير في محتوى ومضمون المفاهيم تغيرا آخرا على مستوى الفواعل التي تمارس القوة على الساحة الدولية، في ظل تقدم تكنولوجي هائل واعتماد واسع على الإنترنيت في التواصل والتعاملات على مستوى داخل الدول وخارج الدول، وهو الذي ولد وضعا دوليا جديد بمعطيات جديدة وتهديدات جديدة متعلقة في معظمها بالفضاء السيبراني.

المبحث الأول: التحول في مفهوم القوة

يعد مفهوم القوة من المفاهيم المحورية في العلاقات الدولية، وتسعى الدول عبر تفاعلها مع غيرها إلى امتلاك القوة بغرض فرض خياراتها وإرادتها على غيرها من جهة، ومن أجل الحفاظ على مصالحها الحيوية من جهة أخرى، في ظل نظام فوضوي يتميز بالصراع والتنافس وعدم التجانس والتوافق في المصالح، بحيث كان التفوق في القوة العسكرية مبتغى الدول في سبيل حماية وضمان أمنها وأمن حدودها، غير أن التطورات التي حدثت لاسيما بعد نهاية الحرب الباردة وما أفرزته نهاية هذه الأخيرة من نهايات على كافة الأصعدة والمستويات قد أدخل أبعادا أخرى جديدة في القوة، بحيث لم تعد القوة العسكرية قادرة على ضمان الأمن القومي للدولة ليظهر بهذا التعدد في أبعاد القوة.

ولم يعد الأمن القومي للدولة مرتبط بالعنصر المادي فقط بل تعداه إلى ضرورة الحفاظ على أمنها في ظل التطورات التكنولوجية الحاصلة لتختلف بهذا طرق وليات التعامل مع ما ظهر من تحديات وتهديدات جديدة للأمن القومي في ظل تغير أساليب الصراع الدولي وغلبة الصراع التقني والتجاري على الصراع العسكري.

المطلب الأول: مفهوم القوة السيبرانية

تعرف القوة على أنها القدرة على التأثير في الآخرين لفعل ما تريده [1]، ويعرفها **هانس مورغانتو** على أنها القدرة على التأثير في سلوك الآخرين.[2]

يذهب **جوزيف ناي** * إلى أن القوة العسكرية والاقتصادية لم تعد كافية من أجل السيطرة والهيمنة، لدى من الضروري إدخال أبعاد أخرى في القوة ، والتي يسميها بالقوة الناعمة*، وتشمل المساعدات والعقوبات الاقتصادية كوسيلة للتأثير، غير أن ظهور ثورة المعلومات قد أحدث تأثيرا كبيرا على القوة الناعمة حسبه، فظهرت بهذا القوة الإلكترونية، وقد أدت الثورة المعلوماتية إلى ظهور شكل جديد من أشكال القوة هي القوة الإلكترونية، وذلك نتيجة للتقدم التكنولوجي السريع في أجهزة الكومبيوتر والاتصالات والبرمجيات، بحيث لم تعد مقتصرة على القوة الصلبة المتمثلة في القوة الاقتصادية و العسكرية والتي كانت الشكل المميز لحركة التفاعلات الدولية وتحتكرها الدول الكبرى على رأسها الولايات المتحدة الأمريكية التي كانت محتكرا لمصادر القوة طوال فترة الحرب الباردة، ومع ثورة المعلومات تم إضافة عنصر جديد لقوة الدولة هو القوة الالكترونية ، لذا أصبح من عناصر قوة الدولة امتلاك التكنولوجيا

---

[1]– صفاء تغريد و لبنى خميس مهدي ، مرجع سابق، ص 174.

[2]– إيهاب خليفة، **القوة الالكترونية وأبعاد التحول في خصائص القوة**، مكتبة الإسكندرية، مصر، 2014، ص 11.

*__جوزيف صموئيل ناي__ Joseph Nye مفكر أمريكي وأستاذ العلوم السياسية وعميد سابق لمدرسة جون كينيدي الحكومية في جامعة هارفارد، أسس بالاشتراك مع روبرت كوهين، مركز الدراسات الليبرالية الجديدة في العلاقات الدولية. وتولى عدة مناصب رسمية منها مساعد وزير الدفاع للشؤون الأمنية الدولية في حكومة بل كلينتون ورئيس=

=مجلس الاستخبارات الوطني، اشتهر بابتكاره مصطلحي القوة الناعمة والقوة الذكية وشكلت مؤلفاته مصدر رئيسي لتطوير السياسة الخارجية الأمريكية في عهد باراك أوباما.

*-**القوة الناعمة** هو مفهوم حديث، عرف استعمالا واسعا بعد نهاية الحرب الباردة، يعبر عن استخدام أدوات الإقناع والاستمالة وليس الضغط والإكراه في إدارة العلاقات الدولية، ويرى جوزيف ناي أن القوة الناعمة هي قدرة أمة معينة على التأثير في أمم أخرى وتوجيه خياراتها العامة استنادا إلى جاذبية نظامها الاجتماعي والثقافي ومنظومة قيمها ومؤسساتها بدل الاعتماد على الإكراه والتهديد.

والمعلومات والقدرة على إنتاج التكنولوجيا المتطورة عن طريق الاختراع والإبداع ونشر الإبداع[1].

يشير **ألفن توفلر** إلى أهمية ودور المعرفة في قوة الدولة بقوله "المعرفة هي القوة، وإن امتلاك المعرفة هو الأساس لامتلاك الثروة والقوة العسكرية[2]".

وبفضل ثورة المعلومات وظهور الانترنيت ومواقع الويب web، أصبح الفضاء الالكتروني واحد من أهم العناصر التي تؤثر في النظام الدولي بما يحمله من أدوات تكنولوجية تلعب دورا مهما في عملية التعبئة والحشد في العالم، إضافة إلى التأثير في القيم السياسية وأشكال القوة المختلفة سواء كانت صلبة أو ناعمة.[3]

كما خلقت هذه الثورة مزايا جديدة ومختلفة بين الدول، أهمها :المنافسة على إنتاج المعلومات، والتي أصبحت مصدرا جديدا وهاما من مصادر قوة الدول في السياسة الدولية.

يعرف جوزيف ناي القوة الإلكترونية على أنها:" القوة التي تعتمد على مصادر المعلومات والسيطرة على الأنشطة الإلكترونية والحواسيب والبنية التحتية ذات الصلة بالفضاء الإلكتروني".[4]

ترتكز عناصر تلك القوة على وجود نظام متماسك يعظم القوة المتحصلة من التناغم بين القدرات التكنولوجية، والسكانية، والاقتصادية، والصناعية، والقوة العسكرية، وإرادة الدولة، وغيرها بما يسهم في دعم إمكانات الدول على ممارسة الإكراه، أو الإقناع، أو ممارسة التأثير السياسي في أعمال الدول الأخرى بغرض الوصول للأهداف الوطنية، من خلال قدرات التحكم، والسيطرة على الفضاء الإلكتروني.[5]

---

[1]–إيهاب خليفة، **القوة الالكترونية وأبعاد التحول في خصائص القوة**، مرجع سابق، ص 18.

[2]– إيهاب خليفة، **القوة الالكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الانترنيت " الولايات المتحدة الأمريكية نموذجا**"، العربي للنشر والتوزيع، القاهرة،لاص 41.

[3]– مولود بلقاسمي وحادي إبراهيم،**تحولات مفهوم القوة في الفضاء الالكتروني: مقاربة سياسية**،(د.س.ن)، ص 532.

[4]-Nye Joseph, **cyber power**, belfer center for science and international affairs, Britain, 2010,p03.

[5]- محمد صخري، "الحرب السيبرانية وتداعياتها علي الأمن العالمي"، متاح على الرابط:

https://bit.ly/3GPM6KM (2022/02/22)

لقد ساهمت القوة السيبرانية في تدعيم القوة الناعمة للدول، بحيث أصبح الفضاء الإلكتروني مسرحا للقيام بهجمات تخريبية ترتبط بنشر المعلومات المضللة، والحرب النفسية، والتأثير في توجهات الرأي العام، والنشاط السري والاستخباراتي ، ومن جهة دفعت الدول لزيادة الإنفاق في سياسات الدفاع الإلكتروني من أجل حماية شبكاتها الوطنية من خطر التهديدات، وبناء مؤسسات وطنية للحماية الإلكترونية. [1]

المطلب الثاني: إستخدام القوة السيبرانية

وحدد جوزيف ناي مصطلح القوة السيبرانية لفهم الدور الذي يؤديه الانترنيت في تشكيل قدرات الأطراف الدولية، وبين أنماطا لاستخدام القوة الإلكترونية مميزا بين الاستخدام الناعم لها والاستخدام الصلب، ويوضح هذا كما يلي[2]:

1-**قدرة الفاعل أ على التأثير في سلوكيات الفاعل ب** : وهذا من خلال دفعه إلى القيام بأعمال لم يكن ليقوم بها، هنا تكون القوة الالكترونية مصدر للقوة الناعمة.

- **قدرة الفاعل الدولي على التحكم في أجندة الآخرين** : عن طريق إقصاء بعض استراتيجيهم، من خلال أن يقوم الفاعل أ بمنع تنفيذ أجندة الفاعل ب من خلال العمل على إقصاء بعض استراتجياته.
- **ترتيب أولويات الفواعل الأخرى:** يقوم هنا الفاعل أ بترتيب أولويات الفاعل ب.

وتتكون القوة السيبرانية من مجموعة عناصر أساسية هي:[3]

1 بنية تكنولوجية.

2 الأسلحة الإلكترونية.

3 إدارة العمليات الإلكترونية.

---

[1]-صباح عبد الصبور عبد الحي، **استخدام القوة الالكترونية في التفاعلات الدولية تنظيم القاعدة نموذجا**، المعهد المصري للدراسات السياسية والإستراتيجية، مصر، 2016، ص 20.

[2]- إيهاب خليفة، **القوة الالكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الانترنيت " الولايات المتحدة الأمريكية نموذجا"**، مرجع سابق، ص 31

[3]-المرجع نفسه، ص 81.

4 بنية مؤسسة وتشريعية

5 خطة استراتيجية لتوظيف القوة الالكترونية.

6 العنصر البشري.

ويمثل الجدول التالي أنماط استخدام القوة السيبرانية حسب جوزيف ناي:

الشكل رقم02: أوجه إستخدام السلطة في المجال السيبراني.[1]

1st Face:	(A induces B do what B would initially otherwise not do)	
	Hard Power:	denial of service attacks, insertion of malware, SCADA disruptions, arrests of bloggers
	Soft Power:	information campaign to change initial preferences of hackers, recruitment of members of terrorist organizations
2nd Face:	(Agenda control: A precludes B's choice by exclusion of B's strategies)	
	Hard Power:	firewalls, filters, and pressure on companies to exclude some ideas
	Soft Power:	ISPs and search engines self monitor, ICANN rules on domain names, widely accepted software standards
3rd Face:	(A shapes B's preferences so some strategies are never even considered)	
	Hard Power:	threats to punish bloggers who disseminate censored material
	Soft Power:	information to create preferences (eg. stimulate nationalism and "patriotic hackers,"), develop norms of revulsion (eg. child pornography)

[1]- Nye Joseph, op.cit ,P 07.

المبحث الثاني:التحول في الفواعل

من إفرازات الثورة التكنولوجية والمعلوماتية أن الدولة لم تعد الفاعل الأساسي والوحيد في التفاعلات الدولية، إضافة إلى أن القوة لم تعد حكرا على الدول فقط إنما أصبح هناك انتشار للقوة بين الفواعل من الدول إلى غير الدول ، وهو أمر غير مسبوق من قبل ، فقد مكنت القوة الإلكترونية الفاعلين الأصغر في السياسة العالمية، من ممارسة القوة الصلبة والناعمة أكبر من ذي قبل من خلال الفضاء الإلكتروني.

المطلب الأول:انتشار القوة السيبرانية بين الفواعل

يعرف **جوزيف ناي** انتشار القوة Diffusion of power على أنها " تزايد القضايا ومجالات التأثير والتفاعل الواقعة خارج نطاق السيطرة الكلية للدولة، بما فيها الدول الأكثر قوة مع ظهور فاعلين جدد يتمتعون بصورة جديدة من القوة".[1]

ويميز ناي بين مستويات الانتشار هذه في مستويين:[2]

-**المستوى الأول:** يقصد به السلطة التي تتمتع بها الدولة في مواجهة المواطنين.

-**المستوى الثاني:** القوة التي تتمتع بها الدولة في مواجهة الدول الأخرى.

إن هذا النوع الجديد من القوة لم يعد يقتصر على الدول فقط، وإنما كل من له القدرة على امتلاك المعرفة التكنولوجية والقدرة على استخدامها وتوظيفها لتحقيق أهدافه، سواء أكان دولة أو أفراد أو فاعلين آخرين من غير الدول، وتعاظم دور هؤلاء الفاعلين ذلك أن القطاع الخاص أصبح يساهم بنسبة كبيرة من امتلاك وإدارة التكنولوجيا الحديثة ووسائل الاتصالات والمعلومات والتحكم فيها أفضل من الدولة.[3]

---

[1]- صباح عبد الصبور عبد الحي، مرجع سابق، ص22.

[2]- إيهاب خليفة، **القوة الالكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الانترنيت " الولايات المتحدة الأمريكية نموذجا"**، مرجع سابق، ص 32.

[3]-نصيرة صالحي، القوة الذكية: التنافس العالمي على قوة الفضاء الالكتروني والقدرات السيبرانية"، **دفاتر السياسة والقانون**، المجلد 13، العدد1، 2021،ص382.

وترتكز عناصر القوة السيبرانية على وجود نظام متماسك يعظم من القوة المتحصلة من التناغم بين القدرات التكنولوجية والسكان والاقتصاد والصناعة والقوة العسكرية وإرادة الدولة، وهو ما يدعم قوة الدولة وقدرتها عل التأثير والقدرة على تحقيق أهدافها من خلال التحكم في الفضاء الالكتروني، وكان للبعد الالكتروني والاتصالي دور في تغيير طبيعة القوة في العلاقات الدولية.[1]

وخلال الفترة الزمنية الأخيرة وصلت كثافة التفاعلات الدولية في تكنولوجيا الاتصال والمعلومات إلى إن عدد مستخدمي الأنترنت 2.1 مليار مستخدم و 2.4 مليار يستخدم الشبكات الاجتماعية و 3.146 مليار حساب بريد الكتروني و 5.9 مليار مستخدم للحاسوب، وبليار فيديو تم فتحه في يوتيوب إلى غاية 2018[2]، والعدد في تزايد رهيب ومرعب يهدد الأمن على كافة المستويات حيث بلغ عدد مستخدمي الانترنيت إلى 4.6 مليار مستخدم في فيفري 2021.[3]

ويستخدم الفاعلين من غير الدول والأفراد هذا النوع الجديد من القوة لأغراض هجومية مثل اختراق مواقع الكترونية، اختراق شبكات معلومات، التجسس الإلكتروني، نشر فيروسات تدمر أجهزة الدولة، فالأخطر من ذلك هو استخدام الجماعات الإرهابية للفضاء الإلكتروني للتخطيط وتنفيذ عملياتهم الإرهابية في مختلف دول العالم.[4]

في تراجع دور الدولة وظهور دور الفواعل الجديدة، يقول **زبيغنيو بريجنسكي:** "يبدو أن دور الدولة يتراجع كوحدة أساسية في المجتمع الدولي وفي حياة الفرد ويعود هذا الانحسار إلى نهاية الحرب الباردة، عندما بزغت فواعل غير الدول على حساب الأخيرة قوة

---

[1]– نورة شلوش، "القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول"، **مجلة مركز بابل للدراسات الإنسانية**، المجلد 07، العدد 02، 2018، ص 197.

[2]–كرار فرحان هاني الطائي، مرجع سابق، ص70.

[3]- محمد صخري، "الحرب السيبرانية وتداعياتها علي الأمن العالمي"،مرجع سابق.

[4]– ريهام عبدالرحمن رشاد العباسى ،"**أثر الإرهاب الالكتروني على تغير مفهوم القوة في العلاقات الدولية دراسة حالة: تنظيم الدولة الإسلامية**"، متاح على الرابط:

https://bit.ly/3mnfwXa(2022/05/10)

التغيير الرئيسية، خاصة بعدما أصبحت المصارف الدولية والشركات المتعددة الجنسيات والجماعات الراديكالية والإرهابية ذات البعد العالمي تنشط بشكل أكبر متجاوزة المفاهيم السياسية للدولة".[1]

صاحب انتشار الموجة الهائلة لتكنولوجيا الاتصال والمعلومات ظهور تهديدات متصاعدة نتيجة البيئة الأمنية الجديدة لعدة أسباب منها:

- ارتباط العالم المتزايد بالفضاء الإلكتروني بما عمل على زيادة خطر تعرض البنية التحية الكونية للمعلومات لهجمات إلكترونية.
- استخدام الفاعلين من غير الدول للفضاء الإلكتروني لتحقيق أهدافهم وتأثير ذلك على سيادة الدولة.
- انسحاب الدولة من قطاعات إستراتيجية لصالح القطاع الخاص وخاصة بالمنشآت الحيوية.
- تأثير مواجهة الحرب الإلكترونية على حرية استخدام الفضاء الإلكتروني.
- إشكالية تعامل الدول مع الشركات التكنولوجية متعدية الجنسيات والتي أصبحت تفوق قدراتها مثل مواقع الشبكات الاجتماعية كالفيس بوك وتويتر واليويتوب الذين أصبحوا فاعلين دوليين.

[1]- صفاء تغريد و لبنى خميس مهدي ، مرجع سابق، ص151.

المطلب الثاني: الفواعل المالكة للقوة السيبرانية

يميز جوزيف ناي بين ثلاث أنواع من الفاعلين الذين يمتلكون القوة السيبرانية: [1]

- ✓ **الدولة:** والتي يكون للدولة القدرة على تنفيذ هجمات الكترونية ، وتطوير البنى التحتية وممارسة السلطات داخلها، ففي نهاية العام 2008 استطاعت حوالي 180 دولة أن تمتلك ترسانة من الأسلحة السيبرانية ، وعادة ما تكون الدول مدفوعة بجداول أعمال سياسية أو اقتصادية أو تقنية أو عسكرية، وتشارك الدول في عمليات التجسس، كما تقوم باستهداف معلومات تحديد الهوية الشخصية للتجسس على أفراد معنيين، كما قد تقوم بتدمير إحدى الشركات في الدول المستهدفة. [2]
- ✓ **الفاعلون من غير الدول:** يستخدمون القوة الالكترونية لأغراض الهجوم ، غير أن قدرتهم على تنفيذ أي هجوم الكتروني مؤثر تتطلب مشاركة وكالات استخبار ايتة متطورة وفك رموز مشفرة وعموما لا تملك هذه الجماعات إمكانيات بحجم إمكانيات الدولة نفسها في مجال استخدام القوة الالكترونية، ولكن يمكن ن ينفد الفاعلون من غير الدول هجمات متنوعة تشمل اختراق مواقع الكترونية واستهداف أنظمة الاتصالات الدفاعية.
- ✓ **الأفراد:** أصبح الفرج عنصرا فعالا في التفاعلات الدولية، وأصبح يمارس من الأنشطة عبر الفضاء السيبراني ما يؤثر به في العلاقات الدولية، فالأفراد يمتلكون معرفة تكنولوجية وقدرة على توظيفها ، وعادة ما تكون هناك صعوبة في الكشف عن هويتهم ويصعب ملاحقتهم وعقابهم [3]، وساعدهم الفضاء الالكتروني من خلق قنوات اتصال مع بعض المنظمات أو الشبكات الاجرامية من أجل تنفيذ هجماتهم ، كأحسن مثال

---

[1]- نفس المرجع السابق الذكر، ص150.

[2]–علم الدين بانقا، "مخاطر الهجمات الالكترونية (السيبرانية) وقارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي"، **سلسلة دراسات تنموية**، العدد 63، 2019،ص 15.

[3]- إيهاب خليفة، **القوة الالكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الانترنيت " الولايات المتحدة الأمريكية نموذجا**"، مرجع سابق، ص 74.

هنا نجد **مجموعة أنونيموس Anonymous** ، وهي مجموعة غير مركزية من القراصنة المنتشرين في العالم ذات ثقل الحرب السيبرانية، وقد كانت مسؤولة عن تسريب ألاف من رسائل البريد الالكتروني الخاص بالرئيس بشار الأسد، كما هاجمت مواقع حكومية أمريكية وبريطانية وأخرى تابعة لحلف الناتو وأخرى لإسرائيل، إضافة إلى قيامها باختراق بيانات شخصية من بينها أرقام ائتمان خاصة بآلاف عملاء شكة خاصة بتحليل المخاطر السياسية والاقتصادية والعسكرية منهم وزارة الدفاع الأمريكية ومنظمات إعلامية وأجهزة أمنية.

وميز جوزيف ناي بين صورتين أساسيتين لانتشار القوة على المستوى العالمي :[1]

- انتقال القوة من ظاهرة القطب الواحد المهيمن إلى التعددية القطبية وظهور قوى جديدة من الدول، وهى ظاهرة قد تكون مألوفة وتقليدية.
- انتقال القوة من الدول بشكل عام إلى الفاعلين من غير الدول، وهى ظاهرة غير تقليدية، وتفرض تحديات على الدول وسيادتها.

ويمثل الجدول التالي أهداف القوة السيبرانية حسب جوزيف ناي:

الشكل رقم03: أشكال القوة السيبرانية حسب جوزيف ناي.[2]

	Targets of Cyber Power	
	Intra cyber space	Extra cyber space
Information Instruments	Hard: Denial of service attacks Soft: Set norms and standards	Hard: Attack SCADA systems Soft: Public diplomacy campaign to sway opinion
Physical Instruments	Hard: Government controls over companies Soft: Infrastructure to help human rights activists	Hard: Bomb routers or cut cables Soft: Protests to name and shame cyber providers

[1]–صباح عبد الصبور عبد الحي، مرجع سابق، ص 22 .

[2]- Nye Joseph,op.cit,P 05.

المبحث الثالث: التحول في طبيعة الصراع والحروب

لقد غيرت التكنولوجيا من أشكال الحروب والصراعات البشرية على مر العصور، بحيث أدت الثورة المعلوماتية إلى نوع جديد من الحروب أطلق عليها اسم الحروب السيبرانية، التي تستخدم نوعا آخر من الأسلحة والتي تتمثل في فيروسات الكمبيوتر التي لديها القدرة على إلحاق الدمار الذي يوازي أو يفوق دمار الأسلحة التقليدية.[1]

المطلب الأول:مفهوم الحروب السيبرانية

يعود التنبأ بالحرب السيبرانية إلى ما طرحه كل من **جون آركيلا** (John Arquilla) و **دافيد رونفيلدت** (David Ronfeldtt) سنة 1993 في مقال بعنوان " **الحرب السيبرانية قادمة Cyber-war is Coming**" من خلال تعريفها على أنها :"تنفيذ والاستعداد لتنفيذ العمليات العسكرية وفقا للمبادئ المعلوماتية من خلال تعطيل –إن لم يكن تدمير–نظم المعلومات والاتصالات على أوسع نطاق، وتدمير القاعدة العسكرية للعدو ومنعه من معرفة أي شيء عن الطرف الآخر، وتحويل ميزان المعرفة ليكون في صالح هذا الطرف".[2]

مع هذا النوع الجديد من الحروب ت غيرت الأدوات المستخدمة في شن الحرب فقد ظهرت تحولات عميقة في طبيعة الحروب التقليدية التي تعتمد على الأسلحة والجيوش العسكرية بحيث تمت إضافة تقنيات جديدة عززت من قدرات الدول في الإدراك البصري واستخدام الخوارزميات في صنع القرار لتنفيذ مجموعة العمليات ما يسمح بتحقيق أهداف دقيقة.[3] بحيث لم تعد بالضرورة قصف لمواقع عسكرية مادية، فأضحى الفضاء الإلكتروني بمثابة وسيلة للقيام بحروب غير تقليدية، والتي حددها جوزيف ناي في أربعة تهديدات رئيسية هي" التخريب الاقتصادي، والجريمة، والحرب الإلكترونية، والإرهاب الإلكترونى".

---

[1]–إيهاب خليفة، **مجتمع ما بعد المعلومات، تأثير الثورة الصناعية الرابعة على الأمن القومي**، مرجع سابق، ص 148.

[2]- دليلة العوفي، "الحرب السيبرانية في عصر الذكاء الإصطناعي ورهاناتها على الأمن الدولي"، **مجلة الحكمة للدراسات الفلسفية**، المجلد 9، العدد 02، 2021، ص 780.

[3]–المرجع نفسه، ص 730.

وتعرف الحرب السيبرانية على أنها " حروب تجري في الفضاء السيبراني باستعمال واستهداف تكنولوجيا المعلومات والاتصالات"[1]

وهي "حروب تستخدم فيها الآليات والأسلحة الإلكترونية في الهجوم الذي يكون موجها إلى أجهزة الحاسب الآلي أو الشبكات الإلكترونية الخاصة بالعدو أو بالأنظمة الإلكترونية وما تحتويه من معلومات والخاصة بالدول، مما يحول دون استخدام هذه الأنظمة والأجهزة والشبكات أو تدميرها بالكامل"[2]

وهي هجوم متعمد يقوم به الدول والجماعات والأفراد بغرض تعطيل عمل أو خداع أو إضعاف أو تدمير أنظمة الكمبيوتر وشبكات الاتصالات والمعلومات والبرامج الموجودة في هذه الأنظمة أو الشبكات التي تمر من خلالها.

كما أنها هجوم متعمد، الغرض منه تعطيل عمل أو خداع أو إضعاف أو تدمر أنظمة الكمبيوتر وشبكات الاتصالات والمعلومات والبرامج الموجودة في هذه الأنظمة أو الشبكات التي تمر من خلالها، ويمكن للدول والجماعات والأفراد القيام بتنفيذ هذه الهجمات".[3]

وفقا للقرار الصادر عن مجلس الأمن الدولي الصادر في 2015 فإن الحرب السيبرانية تعبير عن استخدام أجهزة الحاسوب أو الوسائل الرقمية من قبل حكومة، أو بمعرفة أو موافقة صريحة من تلك الحكومة ضد دولة أخرى، أو ملكية خاصة داخل دولة أخر بما في ذلك الوصول المتعمد أو اعتراض البيانات، أو تدمير البنية التحتية الرقمية وإنتاج وتوزيع الأجهزة التي يمكن استخدامها لتخريب النشاط المحلي.[4]

---

[1]–حمدون توريه،**البحث عن السلام السيبراني**، الاتحاد الدولي للاتصالات، (د.ب.ن)، 2011، ص 11.

[2]-دليلة العوفي، مرجع سابق، ص 782.

[3]- شادي عبد الوهاب، التحولات الرئيسية في المواجهات العنيفة غير التقليدية في العالم، **دراسات المستقبل**، الإمارات العربية المتحدة، 2017،ص 21.

[4]- زينب شنوف، "الحرب السيبرانية في العصر الرقمي: حرب ما بعد كلاوزفيتش"، **المجلة الجزائرية للأمن والتنمية** ، المجلد 09، العدد 02، جويلية 2020، ص 91.

إن الحروب السيبرانية هي حروب تخيلية أو إفتراضية ذات طبيعة غير ملموسة تحاكي الواقع بشكل شبه تام، وهي حرب خفية قد تكون بدون دماء بأسلحة إلكترونية وذكية.

يتم من خلال الحروب السيبرانية استهداف القدرات والأنظمة العسكرية، إضافة إلى استهداف البنية التحتية الحيوية للمجتمع بما في ذلك الشبكات الذكية وشبكات المراقبة الإشرافية وحيازة البيانات التي تسمح لها بالعمل والدفاع عن نفسها، كما تنطوي على جمع البيانات أو التسلل إلى الأنظمة المحوسبة لإحداث الضرر في الأنظمة الحرجة أو تعطيلها أو تدميرها كليا وتوقيفها عن العمل كليا.[1]

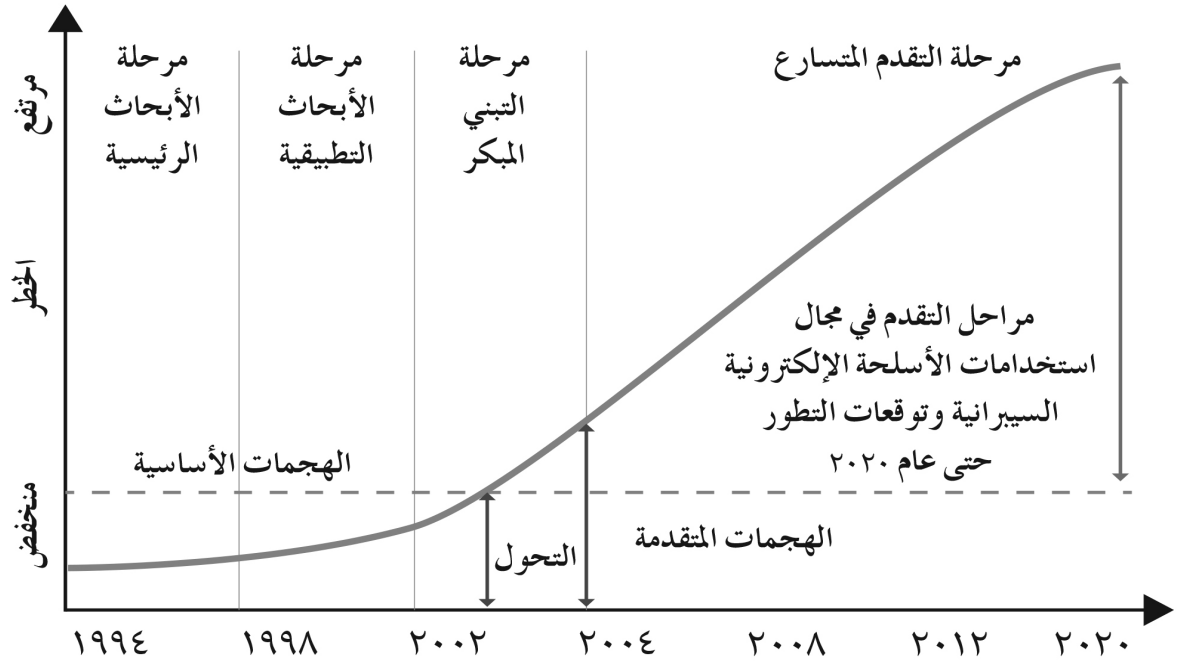
وتشمل الأسلحة السيبرانية الفيروسات والديدان الحاسوبية، وعمليات جمع البيانات السيبرانية وأجهزة تشويش اتصالات البيانات اللاسلكية وبرمجيات الحاسوبية المزيفة المشبوهة وأسلحة النبض الكهرومغناطيسي وأدوات استطلاعات الحاسوب والشبكات والقنابل الزمنية الطروادية المدمجة الهدف منها تدمير البنية التحتية للدول واختراق الأنظمة العسكرية وسرقة حقوق الملكية الفكرية وبراءة الاختراع وغيرها من العمال التخريبية مما يهدد السلم والأمن الدوليين.[2]

ويبين المنحنى البياني الموضح في الشكل تطور استخدام الأسلحة الالكترونية في الفترة الممتدة من 1994 إل غاية سنة 2020، بحث يلاحظ من خلاله ارتفاع كبير لنسبة مرتفعة في السنوات من 2004 إلى غاية 2020.

[1]-يونس مؤيد يونس مصطفى، "إستراتيجية الولايات المتحدة الأمريكية للأمن السيبراني"، **مجلة قضايا سياسية**، العدد 55، 2018، ص124.

[2]- إيهاب خليفة، **مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي** ص 115.

الشكل رقم 04: تطور استخدام الأسلحة الإلكترونية حتى سنة .2020[1]



المطلب الثاني:مميزات وأنواع الحروب السيبرانية

أهم ما يميز الحروب السيبرانية عن الحروب التقليدية هو مجموعة خصائص أهمها:

- ✓ أنها حروب تدميرية بدون دماء أو جثث، فهي تتم من خلال التجسس ثم التسلل ثم النسف، دون أثر ولا دليل، لذا يصعب تمييز مرتكبيها.
- ✓ حروب هلامية الشكل والملامح لأنها متعددة بميادينها ومتنوعة ومتطورة تتطور بتطور التقنيات، كما أنها غير محددة الأهداف والتأثير في هذا يقول نائب وزير الدفاع الأمريكي السابق ويليام لين في 2010 "في حين أن الصاروخ يتم إرساله مع عنوان المرسل فإن فيروس الكمبيوتر من الصعب ربطه بدولة محددة، إذ أن العمليات اللازمة لتحليل هوية المهاجم قد تأخذ شهرا وربما تفشل في النهاية في التوصل إلى هويته".[2]

[1]–عادل عبد الصادق، **أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني**، مرجع سابق،ص60.

[2]- شادي عبد الوهاب منصور، **حروب الجيل الخامس أساليب التفجير من الداخل على الساحة الدولية** ، العربي للنشر والتوزيع، القاهرة، 2019 ،ص105.

- ✓ –حروب يصعب ردعها كما في الحروب التقليدية التي يعد الهجوم المضاد هو الرادع الحقيقي أمام التفكير في شن الحرب، وهو مالا يمكن القيام به في الحروب السيبرانية بسبب صعوبة تقييم الأضرار الناتجة عن شن هذه النوعية من الحروب، وصعوبة التحكم في مدى الهجوم السيبراني المضاد،إضافة إلى صعوبة تحديد مرتكبيها.[1]
- ✓ أنها حروب غير محددة المجال وغامضة الأهداف، كونها تتحرك عبر شبكات المعلومات والاتصالات المتعدية للحدود الدولية، إضافة لاعتمادها على أسلحة الكترونية جديدة في طبيعتها تتوافق مع طبيعة السياق الالكتروني، ويتم توجيهها ضد المنشآت الحيوية أو دسها عن طريق عملاء لأجهزة الاستخبارات.[2]
- ✓ تتسم الحرب السيبرانية بانخفاض تكلفتها، وسهولة تنفيذها، وتتزايد تهديداتها إذا ما تم استهداف البنية التحتية الحيوية بعمليات تخريبية من خال المجال السيبراني، مثل محطات الكهرباء، وأنابيب النفط، والخطوط الجوية والسكك الحديدية والبنوك.[3]

تكون الحروب السيبرانية وفق ثلاثة أنماط كالتالي:[4]

1–الحرب السيبرانية الباردة منخفضة الشدة: صراع مستمر بين الفاعلين المتنازعين، وقد يكون ذا طبيعة ممتدة، ودائمة النشاط العدائي أو غير السلمي، بخلاف أنه عميق الجذور ومتداخل، وله نواح متعددة، وعادة ما يتم اللجوء إلى القوة الناعمة للحروب السيبرانية في مثل صراعات كهذه، وإن كانت لا تتطور بالضرورة إلى استخدام القوة المسلحة بشكلها التقليدي، أو شن حرب إلكترونية واسعة النطاق، نجد هنا شن الحروب النفسية، والاختراقات المتعددة، والتجسس، وسرقة المعلومات، وشن حرب الأفكار، والتنافس بين الشركات التكنولوجية العالمية وأجهزة الاستخبارات الدولية، وهنا يظهر بقوة نشاط الجماعات الدولية

---

[1]– شادي عبد الوهاب، مرجع سابق، ص 22.

[2]-ياسين يحيى، "الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني"، **المجلة القانونية المتخصصة في الدراسات والبحوث القانونية**، ص84.

[3]-محمد صخري، "الحرب السيبرانية وتداعياتها علي الأمن العالمي"، مرجع سابق.

[4]–المرجع نفسه.

للقرصنة مثل "ويكيليكس"، و"أنونيموس"، وكذلك أيضا في حالات الأزمات الدولية، مثل ما حدث بين استونيا وروسيا 2007.

2- نمط الحرب السيبرانية متوسطة الشدة : يتحول الصراع عبر الفضاء الإلكتروني إلى ساحة موازية لحرب تقليدية، تعبيرا عن حدة الصراع القائم بين الأطراف، كما قد يمهد لعمل عسكري، هنا تكون الحرب عن طريق اختراق المواقع الإلكترونية، وتخريبها، وشن حرب نفسية ضد الخصوم.

من أمثلة هذا النمط نجد هجمات حلف الناتو عام 1999 على يوغوسلافيا، حيث استهدفت الهجمات الإلكترونية تعطيل شبكات الاتصالات للخصوم، الحرب بين حزب الله وإسرائيل عام 2006، الحرب بين روسيا وجورجيا في عام 2008، والمواجهات بين حماس وإسرائيل في عامي 2008 و2012.

3-**الحرب السيبرانية "الساخنة" مرتفعة الشدة** : أي نشوء حروب في الفضاء الإلكتروني منفردة، وغير متوازية مع الأعمال العسكرية التقليدية، ولم يشهد العالم هذا النوع من الحروب، وإن كانت احتمالات حدوثها واردة في المستقبل في ظل التطورات التكنولوجية.

ويطرح **توماس ريد** أربع وسائل أو أسلحة أساسية توظف من أجل تحقيق هدف الحرب السيبرانية، والتي تتمثل في:[1]

1-لغة الاستعلام الهيكلية: وتعبر عن البرمجة النصية للمواقع من أجل تشويه صفحات الويب أو إتلافها، ويستخدم هذا النوع من الفيروسات ضد المواقع لساعات أو أيام.

2-الحرمان من خدمة الموزع: ويؤدي هذا النوع من الأسلحة دور رئيسي في الحروب السيبرانية، الهدف منها هو التعطيل المؤقت من الخدمة.

3-الإختراقات: يعتمد على برامج فعالة لسرقة المعلومات الحساسة من المواقع الأمنية، مما يكون له آثار مدمرة ومهددة للمصالح الوطنية والقومية للدول المستهدفة.

---

[1]- كرار عباس متعب فرج، "الحرب السيبرانية: دراسة في إستراتيجية الهجمات السيبرانية بين الولايات المتحدة وإيران"، **مجلة حمورابي للدراسات**، العدد 40، شتاء 2021، ص 203.

4-التسلل: من أهم أساليبه الديدان والفيروسات، ويسبب التسلل إلحاق الضرر في الجهاز المضيف وإرساله إلى الخوادم البعيدة.

خلاصة واستنتاجات:

من خلال ما سبق، يمكن القول أن ظهور الانترنيت وثورة المعلومات وتزايد الاعتماد على الانترنيت، قد أفرز جملة من التغيرات فكان ظهور مفهوم القوة السيبرانية كأحد أهم المفاهيم الجديدة وما رافقها من تغيرات، بحيث لم يعد يقتصر امتلاك القوة على الدول فقط وإنما كل من له القدرة على امتلاك المعرفة التكنولوجية والقدرة على استخدامها وتوظيفها لتحقيق أهدافه، سواء أكان دولا أو أفرادا أو فواعل من غير الدول.

الفصل الثالث:

الجهود الدولية والوطنية لتحقيق الأمن السيبراني

في ظل تزايد حدة التهديدات السيبرانية وما تخلفه من خسائر باهظة على الدول، وفي ظل تزايد تأثيرها الواضح على الأمن القومي للدول، كان لزاما على هذه الأخيرة في سبيل تحقيق أمنها القومي اتخاذ جملة من السياسات والتدابير والآليات بغية حماية بنيتها التحتية من الهجمات السيبرانية المحتملة، فظهرت جهود دولية فردية وجماعية من قبل كافة الفاعلين في مجتمع المعلومات العالمي، وهذا في سبيل الحفاظ عل الطابع السلمي للفضاء الالكتروني، بحيث وضع الأمن السيبراني على رأس الأجندة الدولية وفي مقدمة أولويات السياسة الخارجية للدول وضمن استراتيجيات الأمن القومي لها،

المبحث الأول: الجهود الإقليمية والدولية لمواجهة التهديدات السيبرانية

كانت الاستجابة الدولية للتهديدات والمخاطر السيبرانية في شكل جماعي من خلال مجموعة من الإتفاقيات الدولية والإقليمية والتي من أهمها الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية و إنشاء الاتحاد الدولي للاتصالات.

المطلب الأول: الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية –اتفاقية بودابست–

من الأسباب الجوهرية التي أدت إلى عقد اتفاقية بودابست هي ظهور الحاجة الدولية إلى ضرورة اتخاذ التدابير التشريعية من أجل مكافحة الجرائم السيبرانية، ومواجهة المخاطر المدمرة لهذه الأخيرة على الدول كافة لاسيما في ظل انتشار شبكات المعلومات وتوسع ونمو أنظمة الحوسبة المفتوحة ونقل وتدفق المعلومات، إضافة إلى ضرورة التأكيد على أهمية مكافحة الأنشطة التي تستهدف أمن المعلومات ونظم الكمبيوتر.[1]

وقد جاءت الاتفاقية بعد محاولات وجهود دولية وإقليمية عديدة لاسيما من قبل المنظمات الدولية كهيئة الأمم المتحدة، منظمة التعاون الإقتصادي والتنمية، الإتحاد الأوروبي ومجموعة الدول الصناعية.

[1]– مراد مشوش، "الجهود الدولية لمكافحة الإجرام السيبراني"، **مجلة الواحات للبحوث و الدراسات**، المجلد 12، العدد 2، 2019، ص712.

وتعد الإتفاقية بمثابة دعوة موجهة إلى كافة دول العالم للتعاون معا وجنبا إلى جنب في مواجهة التهديدات التي مصدرها الفضاء السيبراني، والتي باتت تشكل أكبر تهديد للأمن القومي للدول، وتسبب خسائر كبيرة لاسيما في الدول المتقدمة منها جراء تنامي الاعتماد على الكمبيوتر.

تم عقد الإتفاقية في العاصمة المجرية بودابست في 23 نوفمبر 2001، ووقعت عليها 26 دولة أوروبية إضافة إلى كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية، وتتكون من ثمانية وأربعين مادة موزعة على أربعة أبواب: [1]

- ✓ الجزء الأول حول القواعد الموضوعية للجرائم.
- ✓ الجزء الثاني حول إجراءات التحقيق.
- ✓ الجزء الثالث حول آليات التعاون الدولي.

وتناولت المعاهدة الجرائم التي تعتبر من أكثر الجرائم شيوعا على مستوى العالم مثل الإرهاب الالكتروني، كما حددت الطرق الواجب إتباعها في التحقيق في جرائم الإنترنت، وتعهدت الدول الموقعة بالتعاون من أجل محاربتها.

توزعت بنود الاتفاقية على ثلاث محاور هي: [2]

- ✓ الانسجام بين التشريعات الوطنية، التي تجرم الأعمال غير القانونية في الفضاء السيبراني.
- ✓ تحديد وسائل التحقيق والملاحقة الجزائية، التي تنسجم مع الطبيعة العالمية للشبكة.
- ✓ وضع نظام تعاون بين الدول يتصف بالسرعة والفاعلية.

وتبرز المعاهدة ضرورة التعاون والتضامن الدولي في محاربة الجرائم الإلكترونية، ويعد التوقيع عليها الخطوة الأولى في مجال تكوين التضامن الدولي ضد تلك الجرائم التي تتم

---

[1]–شيخة حسين الزهواني، "التعاون الدولي في مواجهة الهجوم السيبراني"، **مجلة جامعة الشارقة** ، المجلد 17، العدد 1، جوان 2020، ص753.

[2]– منى الأشقر جبور، مرجع سابق،ص 105.

عبر شبكة الإنترنت و ضد الاستخدام السيئ لها ، وتعد الاتفاقية نموذجا تشريعيا، حيث اقتبست العديد من الدول عبر العالم من نصوص هذه الاتفاقية عند إعداد قوانينها الوطنية.[1]

ترتكز أهمية هذه الاتفاقية بفعاليتها على إقرارها لإجراءات عملية، والتي تلتزم الدول المنظمة إليها بإدراجها في قوانينها الوطنية، لاسيما منها ما تعلق بجمع بيانات الاتصال وحفظها بما يسمح بتحديد مصدرها ونقطة وصولها، وتعتبر الاتفاقية أول أداة إقليمية ملزمة لمكافحة الجرائم السيبرانية عبر تحسين تقنيات التحقيق والبحث وزيادة التعاون الدولي.[2]

لكن على الرغم من أن الاتفاقية تقدم بعض الحلول القانونية للجرائم السيبرانية، إلا أنها لا تعالج بعض الأنواع من عمليات الهجوم السيبراني الأكثر تهديدا مثل التجسس للحصول على البيانات وأعمال التخريب ، وعلى الرغم من أن الاتفاقية تساعد على تعزيز التعاون الدولي من خلال تجريم التهديدات السيبرانية الأساسية، فإن قوتها الإلزامية محدودة بسبب محاولة الجهة التي قامت بصياغتها عدم مخالفة تشريعات وطنية أخرى يحتمل أن تتعارض معها ، وتؤدي الاختلافات الثقافية والقانونية الكبيرة إلى جعل إصدار قانون موحد أمرا بطيئا إن لم يكن مستحيلاً تماما في إطار هذا النهج.

---

[1]– اللجنة الاقتصادية والاجتماعية لغربي آسيا(الإسكوا)، مرجع سابق، ص 11.

[2]–منى الأشقر جبور، مرجع سابق،ص 104.

المطلب الثانـــي: جهود الاتحاد الدولي للاتصالات

الاتحاد الدولي للاتصالات وكالة متخصصة تابعة لمنظمة الأمم المتحدة ، مسؤولة عن مسائل تقنية المعلومات والاتصالات، عملت منذ نشأتها في القرن التاسع عشر –في شكل هيئة دولية مستقلة– على تنسيق عمليات استغلال شبكات الاتصال على مستوى العالم، وتحفيز الفاعلين في القطاع باستمرار على تطوير تكنولوجيا المعلومات والاتصال.

تأسس الاتحاد سنة 1865، حيث اجتمع ممثلو عشرين دولة في باريس من أجل عقد أول مؤتمر دولي للتلغراف، ووقعوا على أول اتفاقية دولية للتلغراف أنشأ المؤتمرون بموجبها الاتحاد الدولي للتلغراف، تطورت هذه الأخيرة من أجل استيعاب تقنيات الاتصال الجديدة التي ظهرت بعد التلغراف، كالهاتف وأنظمة الراديو والتلفاز،لتصبح في 1932 الاتحاد الدولي للاتصالات بجنيف.[1]

ويسعى الاتحاد جاهدا من أجل جعل خدمات الاتصال أكثر كفاءة، وتحسين ولوج المجتمعات في كل مكان إلى تكنولوجيات المعلومات والاتصال بغية تمكين الجميع من حق التواصل.

بالنسبة للعضوية في الاتحاد يجمع الاتحاد الدولي للاتصالات في عضويته ومنذ نشأته بين الحكومات والقطاع الخاص، إعمالا لمبدأ الشراكة بين القطاعين، وفي عام 2016 بلغ عدد أعضائه 193 بلدا، إضافة إلى ما يزيد عن ثمان مئة مؤسسة خاصة منها الشركات، مؤسسات البحث والتطوير، وهيئات أكاديمية.

يرمي برنامج الأمن السيبراني العالمي إلى تحقيق سبعة أهداف إستراتيجية رئيسية هي[2]:

- ✓ وضع استراتيجيات لاستحداث تشريع نموذجي لمكافحة الجريمة السيبرانية يمكن تطبيقه عالميا وقابل للاستخدام مع التدابير التشريعية القائمة على الصعيدين الوطني والإقليمي.

---

[1]– الاتحاد الدولي للاتصالات، "**نبذة عن الاتحاد الدولي للاتصالات(ITU)** "، متاح على الموقع الرابط: https://bit.ly/3mkar1Q (2022/05/12)

[2]–حمدون إ. توريه ، مرجع سابق، ص 97.

- ✓ وضع استراتيجيات عالمية لإيجاد الهياكل التنظيمية والسياسات العامة الملائمة على الصعيدين الوطني والإقليمي بشأن الجريمة السيبرانية.
- ✓ وضع إستراتيجية لصوغ معايير أمنية وخطط اعتماد للأجهزة الحاسوبية ولتطبيقات البرمجيات والأنظمة تكون مقبولة عالميا.
- ✓ وضع استراتيجيات لإيجاد إطار عالمي للرصد والإنذار والاستجابة للحوادث لضمان التنسيق عبر الحدود بين المبادرات الجديدة والقائمة.
- ✓ وضع استراتيجيات عالمية لإنشاء وإقرار نظام هوية رقمي عام عالمي، والهياكل التنظيمية اللازمة لضمان الاعتراف بوثائق التفويض الرقمية عبر الحدود الجغرافية.
- ✓ وضع إستراتيجية عالمية لتيسير بناء القدرات البشرية والمؤسسية ، من أجل تعزيز المعارف والمهارات عبر القطاعات وفي المجالات السابقة الذكر.
- ✓ وضع مقترحات بشأن إطار لإستراتيجية عالمية لأصحاب المصلحة المتعددين ، من أجل لتحقيق التعاون والحوار والتنسيق على الصعيد الدولي في جميع المجالات السابقة الذكر.

وقد قام الاتحاد الدولي للاتصالات بإنشاء مؤشر للأمن السيبراني على المستوى العالمي، حيث تم إطلاق مؤشر الأمن السيبراني العالمي (GCI) لأول مرة في العام 2015، لقياس مدى التزام 193 دولة عضوا في الاتحاد الدولي للاتصالات بمرتكزات الأمن السيبراني.[1]

إضافة إلى مساعدة الدول من خلال زيادة الوعي بحالة الأمن السيبراني في جميع أنحاء العالم عبر تحديد مخاطر الأمن السيبراني والأولويات والموارد، وقد تكيفت GCI أيضا لتقديم المزيد من تدابير الأمن السيبراني، كذلك يهدف المؤشر إلى فهم التزامات البلدان تجاه الأمن السيبراني بشكل أفضل وتحديد الثغرات و تشجيع دمج الممارسات الجيدة، وتقديم رؤى

[1]- الاتحاد الدولي للاتصالات، "**دليل لوضع إستراتيجية وطنية للأمن السيبراني التزام استراتيجي بالأمن السيبراني**"،الاتحاد الدولي للاتصالات،(د.ب.ن) 2017، ص 17.

مفيدة للدول لتحسين مواقف الأمن السيبراني الخاصة بهم، ورفع مستوى الوعي بين مختلف أصحاب المصلحة بشأن احتياجات التنسيق على المستوى الوطني.

يقوم الاتحاد الدولي للاتصالات كل سنة بإعداد تقرير فيما يخص تطور المجتمعات في مجال مجتمع المعلومات ويتم فيه قياس درجة هذا التطور، ويقدم التقرير حوصلة عالمية لمجمل ما توصل إليه العالم من أحدث التطورات التكنولوجية، إضافة إلى تقديم تقرير شامل عن أداء الدول الأعضاء في الإتحاد، ويتم إنجاز التقرير من طرف خبراء متخصصين في المجال، إعتمادا على بيانات إحصائية موثوقة.

كما قام الإتحاد الدولي للإتصالات بإطلاق عدة مبادرات بالشراكة مع المنظمات الدولية، من أهم هذه المبادرات نجد:[1]

1-المركز العالمي لقدرات الأمن السيبراني: هو مركز دولي للبحوث المتعلقة ببناء القدرات الكفؤة والفعالة في مجال الأمن السيبراني، وقد تعاون المركز مع الاتحاد في تطوير دليل لوضع إستراتيجية وطنية للأمن السيبراني ، يجري استخدامه لتقديم تدريبات عملية بشأن الاستراتيجيات الوطنية للأمن السيبراني، إضافة إلى تدريب الدول على الممارسات الجيدة من أجل وضع إطار استراتيجي وطني فعال للأمن السيبراني.

2-المنتدى العالمي للخبرة السيبرانية : أنشئ في 2015 هدفه تبادل الممارسات الجيدة وتقديم الخبرة في مجال بناء القدرات السيبرانية للبلدان والمنظمات الدولية والقطاع الخاص ، ويشارك المنتدى إلى جانب الاتحاد في مبادرة نضج أفرقة الاستجابة للحوادث الأمنية الحاسوبية، وقد تعاونا بشأن أنشطة الأمن السيبراني مثل " مجموعة أدوات مكافحة الجرائم السيبرانية".

3-المجمع العالمي للابتكار التابع للإنتربول : أنشأ في 2015 لأجل الدعم والتدريب التشغيليين المتخصصين في مجال إنفاذ القانون الوطني استجابة للتغيرات في طبيعة

[1]-الإتحاد الدولي للإتصالات، **المبادئ التوجيهية لاستعمال البرنامج العالمي للأمن السيبراني** ، تقرير من الأمن العام، المجلس 2020، جينيف، 5 ماي 2020، ص 22.

الجرائم، ووقع في 2018 الاتحاد والإنتربول اتفاق تعاون لإنشاء إطار رسمي ل لإنتربول والاتحاد من أجل التعاون لما فيه مصلحتهما المشتركة وفي نطاق ولاية وموارد كل منها، في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات.

4-مركز التميز المعني بالدفاع الحاسوبي التعاوني : تابع حلف شمال الأطلسي ، أطلق بتالين في 2008، يقدم نتائج أبحاثه بشأن تدابير الدفاع السيبراني ويعزز الأمن السيبراني من خلال تمارين تستهدف الخبراء التقنيين والموظفين العسكريين والدول الأعضاء المعنية بوضع القرار.

5-المنتدى الاقتصادي العالمي : الذي أطلق مركزا عالمي للأمن السيبراني في 2018 لإنشاء منصة عالمية للحكومات والشركات والخبراء ووكالات إنفاذ القانون، من أجل التعاون بشأن تحديات الأمن السيبراني، ووافق الاتحاد والمنتدى الاقتصادي العالمي على التعاون بشأن تعزيز مشاريع ومبادرات الأمن السيبراني التي تهدف إلى التخفيف من التهديدات السيبرانية، وكذلك استكشاف المزيد من الفرص للتعاون بشأن تعزيز الأمن السيبراني.[1]

[1]-المرجع نفسه، ص 23.

المبحث الثاني: الجهود الوطنية لاحتواء الخطر والتهديد السيبراني

في ظل تصاعد التهديدات السيبرانية وتأثيراتها على أمن الدولة الداخلي، ظهرت جهود وطنية قامت بها الدول في سبيل مواجهة هذه التهديدات، منها الاستراتيجيات الوطنية للأمن السيبراني من جهة وإنشاء الجيوش السيبرانية من جهة أخر.

المطلب الأول: وضع الإستراتيجية الوطنية للأمن السيبراني

نتيجة للثورة التكنولوجية الهائلة ، استطاعت الدول تحقيق مكاسب في مختلف المجالات، غير أنها أصبحت عرضة لتهديدات أخرى مرتبطة بالفضاء الالكتروني، وهي تهديدات تتطلب تكاليف باهظة لمواجهتها نظرا للأضرار الخطيرة التي تسببها التهديدات السيبرانية على الأمن القومي وعلى البنية التحتية للدول، فاتجهت إلى وضع سياسات وقائية ودفاعية ضد الهجمات السيبرانية ، وخصصت مبالغ ضخمة من أجل تأمين فضائها السيبراني وحمايته من الهجمات والاختراقات، وهو ما انعكس في شكل سياسات واستراتيجيات وطنية.

فلتجهت الدول نحو تأسيس مؤسسات بحثية وأمنية تهتم بدراسة الفضاء السيبراني وكيفية توظيفه بالشكل الذي يساهم في تحقيق مصالحها السياسية والأمنية والاقتصادية، ليكون التحدي المستقبلي الذي يفرضه الفضاء السيبراني متمثلا في قدرة الدول على التكيف مع التغيير السريع والتحديات التي يفرضها الفضاء السيبراني في المجالات العامة عموما والمجال الأمني خصوصا، إلى جانب امتلاك القدرات والبنى المادية والبشرية التي تمكنها من أن تكون مؤثرة وفاعلة فيه.

تعرف الإستراتيجية الوطنية للأمن السيبراني **(NCSS) national cyber security strategies** بأنها:"الإستراتيجية التي تحدد الأهداف السياسية والتدابير الواجب اتخاذها والمسؤوليات، وذلك من أجل ضمان حماية الشبكات والإنترنت والفضاء السيبراني الذي تعتمد عليه المجتمعات الحديثة المرتبطة بهذه التقنيات، والتي تشمل سرية عمليات

التبادلات، وتكامل البيانات، وتوافر الأنظمة والحماية ضد الخلل التقني والهجمات السيبرانية، وذلك من خلال الأولويات المتاحة لتأمين البنية التحتية الخاصة بالمعلومات الحساسة".[1]

وتعبر الإستراتيجية الوطنية للأمن السيبراني عن مدى استعداد الدول والحكومات لتوفير مجموعة من الإجراءات المتماسكة والمترابطة ، في سبيل ضمان أمنها وحماية وجودها في الفضاء السيبراني، وتكون عبر استراتيجيات قصيرة أو طويلة المدى وتشمل كافة الأولويات الوطنية، وتحدد توجه الدولة في تنفيذ السياسة الوطنية للأمن السيبراني والتدابير الواجب إتخادها في حالة التعرض لهجوم سيبراني.[2]

وتهدف الإستراتيجية الوطنية للأمن السيبراني إلى تعزيز ومرونة البنيات التحتية، والمساهمة في حماية المواطنين والمهنيين والفاعلين في الحياة العامة في إطار البيئة الرقمية، وقد طورت مختلف الدول إستراتيجية أمنها القومي من خلال:[3]

- ✓ ترتيب وإحداث وتنفيذ الحد الأدنى من المتطلبات لحماية البنية التحتية الحيوية.
- ✓ تأمين وحماية الأنظمة الحكومية.
- ✓ تطوير التعاون الوطني والدولي.
- ✓ تنمية ثقافة الوعي بالأمن السيبراني على المستوى الوطني وتعزيز قدرات الموارد البشرية وتطوير الخبرة الوطنية والتوعية بأمن المعلومات.
- ✓ تحديث الإطار القانوني لدعم الاستخدام الآمن لنظم المعلومات.

---

[1]– عبد الواحد البيديري، "إستراتيجية الأمن السيبراني: دراسة حالة المغرب"، **مجلة الدراسات الإستراتيجية والعسكرية**، المركز الديمقراطي العربي، العدد 11، جويلية 2021، ص 104.

[2]– أمانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات، **إستراتيجية الأمن السيبراني العراقي** ، مستشارية الأمن الوطني، ص2.

[3]– عبد الواحد البيديري، مرجع سابق، ص 104.

وبناء على التجارب الناجحة في مجال وضع الاستراتيجيات والسياسات الوطنية للأمن السيبراني، وضعت الأمم المتحدة مجموعة من التدابير يجب أن تتضمنها أي إستراتيجية وهي:[1]

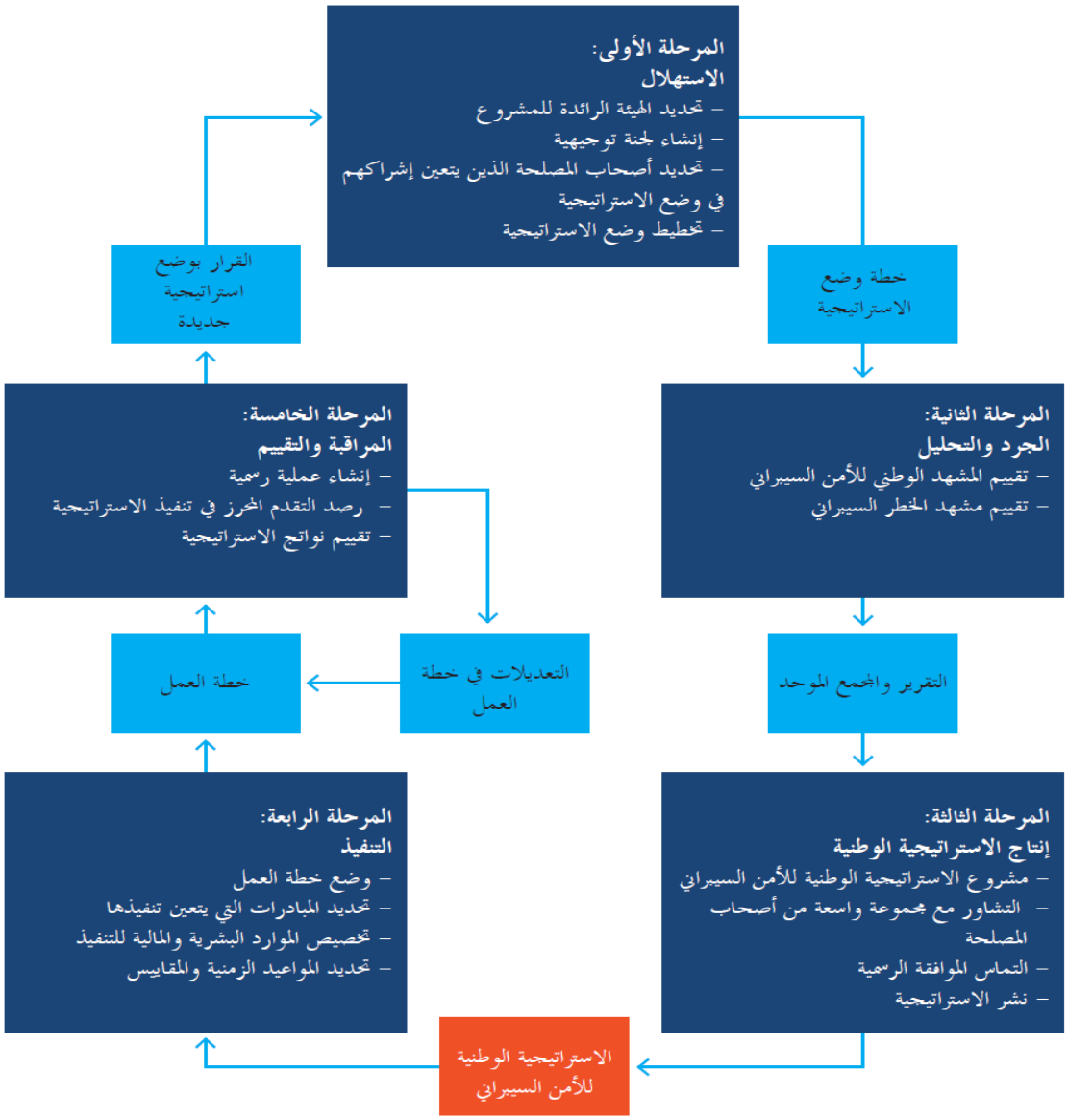
- ✓ إصدار التشريعات.
- ✓ القيادة الفعالة.
- ✓ تطوير قدرات الفضاء الجزائي وأجهزة تطبيق القانون.
- ✓ التعليم والتوعية.
- ✓ تطوير قاعدة المعلومات.
- ✓ التعاون بين الحكومة والمجتمعات والقطاع الخاص ومع الدول والمنظمات.
- ✓ ضرورة وضع خطة وطنية للوقاية من الهجمات السيبرانية مع أهداف وأولويات محددة.

تمر عملية وضع إستراتيجية وطنية للأمن السيبراني بمجموعة مراحل وقد تمتد على سنوات حسب ما تقرره الدولة بناءا على إمكانياتها وعلى وضعها الأمني، ويوضح الشكل التالي دورة حياة الإستراتيجية الوطنية للأمن السيبراني:[2]

[1]– اللجنة الاقتصادية والاجتماعية لغربي آسيا(الإسكوا)، **الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياسية**، الأمم المتحدة، نيويورك، 2015، ص 16.

[2]- الاتحاد الدولي للاتصالات، دليل لوضع إستراتيجية وطنية للأمن السيبراني التزام استراتيجي بالأمن السسيبراني،

الشكل رقم05: دورة حياة الإستراتيجية الوطنية للأمن السيبراني.[1]



من جهة أخرى سعت الدول في سبيل مواجهة التهديدات السيبرانية بمختلف أنواعها إلى تشكيل هيئات متخصصة في الأمن السيبراني، تتمثل مهمة هذه الأخيرة في:[2]

- ✓ إعداد الإستراتيجية الوطنية للأمن السيبراني والإشراف على تنفيذها.
- ✓ وضع السياسات وآليات الحوكمة والإرشادات المتعلقة بالأمن السيبراني وتعميمه.

---

[1]- الاتحاد الدولي للاتصالات، "**دليل لوضع إستراتيجية وطنية للأمن السيبراني التزام استراتيجي بالأمن السيبراني**"،مرجع سابق، ص 18.

[2]–لامية طاية، "التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها"، **مجلة معالم للدراسات القانونية والسياسية**، المجلد 4، العدد 2، 2020،ص 65.

- ✓ وضع أطر إدارة المخاطر المتعلقة بالأمن السيبراني.
- ✓ وضع أطر الاستجابة للحوادث والاختراقات.
- ✓ وضع السياسات والمعايير الوطنية للتشفير.
- ✓ رفع مستوى الوعي بالأمن السيبراني.

تأكيدا على أهمية أمن الفضاء الالكتروني في استراتيجيات الأمن القومي نجد التركيز البريطاني على أمن الفضاء الالكتروني في إستراتيجية الأمن القومي للحكومة البريطانية سنة 2010، وهو ما أعلن عنه **إيان لوبان** مدير المقر الرئيسي للاتصالات الحكومية بأن المملكة المتحدة تواجه هجمات في الفضاء الإلكتروني على نطاق غير مسبوق، وبوتيرة متسارعة وبتعقيد يتراوح ما بين نشاط إجرامي خفيف المستوى وعمليات أكثر تطورا، وبحسب إستراتيجية الأمن القومي لبريطاني 2010، فقد تم تصنيف الفضاء الالكتروني من بين التهديدات الأربع الأكثر خطورة في بريطانيا، وهو ما جعلها تقوم بإضافة 650 مليون جنيه إسترليني إلى التمويل المتاح خلال 2011 و 2015 لتعزيز أمن الفضاء الالكتروني للمملكة المتحدة.[1]

على هذا الأساس تم تأسيس مكتب الأمن السيبراني الذي يعمل على تعزيز عمليات الأمن السيبراني، كما تم وضع منهاج خاص بتطوير القدرات تحت مسمى خطوط الدفاع من التنمية للعمل على تطبيق مجال الأمن في الحروب السيبرية ، وهذا في إطار إستراتيجية **Tepidoil** التي طبقت عقيدة حرب الانترنيت ووفرت منصات وأنظمة الأسلحة الخاصة بالبيانات والمعلومات.[2]

---

[1]– جون باسيت، "حرب الفضاء الالكتروني: التسلح وأساليب الدفاع الجديدة"، الحروب المستقبلية في القرن الحادي والعشرين"، **مركز الإمارات للدراسات والبحوث الإستراتيجية**، الإمارات العربية المتحدة، 2014، ص54.

[2]– سرى غضبان غيدان، محمد منذر جلال الربيعي،"الأمن السيبراني وسياسات المواجهة الدولية"، **مجلة الدراسات الإستراتيجية والعسكرية**، المجلد 2، العدد 9، ديسمبر 2020 ، ص212.

في الصدد نفسه، قامت الصين بإضافة عنصر توجيه أمن الشبكات والمعلومات إلى قانونها الجديد الخاص بالأمن السيبراني الوطني الذي تبناه البرلمان الصيني في نوفمبر 2016 والذي أصبح نافذا بشكل كامل في ديسمبر 2017، يحدد فيه مسؤوليات الوكالات الحكومية ذات الصلة ومزودي خدمات الإنترنت ومستخدمي الإنترنت، ويلزم القانون الشركات باتخاذ تدابير تقنية لضمان عمل الإنترنت بشكل آمن ومستقر، وللتعامل مع حوادث الأمن السيبراني بشكل فعال ولمنع النشاطات السيبرانية الإجرامية، وفي سبيل الحفاظ على سلامة وسرية بيانات الإنترنت بالإضافة إلى قابليتها للاستعمال.[1]

أما الولايات المتحدة الأميركية فقد اعتبرت التهديدات السيبرانية على أنها تهديدات عسكرية تمس الرفاه الوطني، على هذا الأساس أعطت اهتماما كبيرا لوضع إستراتيجية تخص الأمن السيبراني، لاسيما وأنها تعتمد على التكنولوجيا في بنيتها التحتية واقتصادها وبرامجها الطاقوية، لذا فأي هجوم محتمل قد يلحق بها أضرار وخيمة، لذا تم تصنيف الحروب والهجمات السيبرانية على أنها تهديدات خطيرة للأمن القومي الأمريكي خاصة تهديدات من قبل وروسيا والصين، على هذا الأساس تم إطلاق الإستراتيجية القومية لتأمين الفضاء الالكتروني من قبل الرئيس الأمريكي بوش الإبن في 2003، وأهم ما جاء فيها:[2]

- ✓ منع الهجمات الإلكترونية.
- ✓ تقليل نقاط الضعف التي تسهل عملية الإختراق.
- ✓ سرعة التعامل مع الهجمات الإلكترونية.
- ✓ تحقيق التفوق وبسط النفوذ الأمريكي في الفضاء الالكتروني عبر:عمليات المعلومات والشبكات، التطبيقات الحركية، تطبيق القانون وردع الجناة، مكافحة التجسس.

[1]– ميليسا هاتاواي، إدارة الخطر السيبراني الوطني، فهم الخطر السيبراني، (د.ب.ن)، (د.س.ن)، ص 04.

[2]– سرى غضبان غيدان، محمد منذر جلال الربيعي، مرجع سابق، ص 206.

على المستوى العربي طبقت العديد من الدول استراتيجيات إستباقية للأمن السيبراني في محاولة منها للتصدي للتهديدات السيبرانية.

في هذا نجد أن عمان احتلت المرتبة الرابعة عالميا في مؤشر قياس جاهزية الدول تجاه الأمن السيبراني العالمي لسنة 2017، والمرتبة 16 في 2018 حسب الاتحاد الدولي للاتصالات، وتهدف الإستراتيجية الوطنية للأمن السيبراني في الإمارات العربية المتحدة إلى إنشاء بنى تحتية الكترونية آمنة وقوية للمواطنين والأنشطة التجارية، كما أطلقت الهيئة العامة لتنظيم قطاع الاتصالات الإستراتيجية الإستباقية في 2019، والتي تهدف إلى زيادة ثقة المواطنين في العالم الرقمي، وتشجيع الابتكار وريادة الأعمال في مجال الأمن السيبراني، وحماية أصول البنية التحتية للمعلومات المهمة ، إضافة إلى تكوين قوة عاملة ذات مستوى عالمي للأمن السيبراني.[1]

وفي سبيل تحقيق الأمن السيبراني قامت الإمارات العربية المتحدة بإنشاء بنية تحتية إلكترونية آمنة وقوية للمواطنين، وأطلقت الهيئة العامة لتنظيم قطاع الاتصالات النسخة المحدثة من الإستراتيجية لعام 2019 والتي تتضمن تعبئة النظام البيئي للأمن السيبراني وزيادة ثقة المواطنين في العالم الرقمي إضافة إلى تشجيع الابتكار وريادة الأعمال في مجال الأمن السيبراني.[2]

أما الجزائر فقد وضعت قيادة الدفاع مسألة الأمن السيبراني ضمن أهم أولوياتها، عن طريق مراجعة سياستها الأمنية وإدخال مجموعة من الآليات الجديدة في مواجهة التهديدات السيبرانية، بحيث قامت مؤسسة الدفاع الوطني بإعداد برامج خاصة لمواجهة والحد من انتشار الجرائم الالكترونية،وأصبحت الحماية السيبرانية جزء من منظومة الدفاع في الجزائر.[3]

---

[1]– مجتمـــع المعلومات، **المبادئ التوجيهية المتعلقـة بأمن البنيـــة التحتية للانترنيت فـي الدول العربية** ، مارس 2020، ص 18.

[2]–المرجع نفسه،ص36.

[3]–بارة سمير، "الأمن السيبراني في الجزائر: المؤسسات والسياسات"، **المجلة الجزائرية للأمن الإنساني**، العدد 04، جويلية 2017، الجزائر، ص 264.

ومن أهم الهياكل المنشأة لتقصي الجرائم السيبرانية نجد:[1]

1-مركز الوقاية من جرائم الإعلام الآلي وجرائم المعلوماتية للدرك الوطني : أنشأ في 2008 بهدف تأمين منظومة المعلومات لخدمة الأمن العمومي، استطاع المركز معالجة أكثر من 500 قضية رقمية في 2015.

2-المعهد الوطني للأدلة الجنائية وعلم الإجرام : تم إنشائه سنة 2004، يعمل تحت الوصاية المباشرة لوزير الدفاع الوطني ويعمل عل المشاركة في تحديد سياسة جنائية مثلى لمكافحة الإجرام، وتقديم المساعدة العملية أثناء عمليات البحث والتحري.[2]

3-المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني : أنشأت في 2011 من أجل محاربة الجريمة الالكترونية.

4-الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها: تقوم باقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا المعلومات، وتساعد السلطات القضائية ومصالح الشرطة القضائية في مكافحة هذه الجرائم.

إلى جانب هذه الهياكل، أنشأت القيادة العليا للجيش الوطني مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة بغية تأمين وحماية المنظومات والمنشآت الحيوية للقوات المسلحة ضد التهديدات السيبرانية، وعززت الإستراتيجية بمصلحة الدفاع السيبراني ومراقبة أمن الأنظمة في 2015 تحرص على وضع وتطبيق السياسة العامة للدفاع السيبراني في الجيش الشعبي الوطني، كما تساهم في وضع السياسة الوطنية المتعلقة بالدفاع السيبراني.[3]

المطلب الثاني: بناء الجيوش السيبرانية Cyber Armies

---

[1]- إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري"، **مجلة مصداقية** ، ص 112.

[2]- إسماعيل جابوري، مرجع سابق، ص78.

[3]- عائشة عبد الحميد، "الإطار القانوني والتشريعي للرقمنة والذكاء الاصطناعي"، **المجلة الدولية للتعليم بالانترنيت** ، جويلية 2020، ص 104.

نتيجة للتحول في طبيعة الحروب بات لزاما على الدول أن تغير من طبيعة المواجهة، فالجيوش التي تقاتل في الميدان لا يمكنها أن تواجه وتتصدى للهجمات التي تكون عبر الفضاء السيبراني، من هنا ظهر توجه العديد من البلدان حول العالم نحو بناء جيوشها السيبرانية، وهي جيوش إلكترونية نظامية لها ميزانيتها الخاصة، وتسعى للدفاع عن البلاد ضد الهجمات الإلكترونية .

تعرف الجيوش السيبرانية على أنها مجموعات مدربة تعمل وفق أجندة خاصة هدفها اختراق مواقع الخصوم، والترويج لوجهة نظر معينة عبر مختلف منصات الإنترنت، وإسكات وتشويه سمعة المناوئين، إلى جانب ترويج الإشاعات والأكاذيب وخلق البلبلة، وقد بدأت الدول في إنشاء وحدات إلكترونية داخل أجهزتها العسكرية والأمنية لحماية أمنها القومي[1].

عرف المصطلح انتشارا بشكل كبير سنة 2011 عقب الكشف عن الجيش الإلكتروني السوري الذي نجح في اختراق مواقع أوروبية وأميركية وعربية بعد أحداث 2011، لتوجيه رسائل داعمة لنظام بشار الأسد بعد اندلاع الثورة السورية في العام نفسه.[*]

تعمل الجيوش السيبرانية على متابعة كل ما ينشر على الإنترنت ويخص مصالح الجهات التي يعملون لصالحها، ومن خلال اختراق المواقع الشهيرة بإمكانهم بث الإشاعات والأكاذيب بغرض إرباك الأوضاع، وإضعاف معنويات الطرف الآخر، وتختلف الجيوش السيبرانية من حيث الأهداف والوسائل فقط غير أنها تتشابه في الوسائل المتبعة، إذ ي تطلب تكوين جيش سيراني إلى طاقم فني مدرب ووسائل تقنية حديثة ومتطورة، حيث يتم في الغالب إرسال فيروسات تعمل على السيطرة على الموقع المستهدف بطريقة لا يمكن معها

---

[1]– الجزيرة، **ماذا تعرف عن الجيوش الإلكترونية؟**، متوفر على الرابط:
https://bit.ly/3x9RELO (2022/04/12)

[*]– من أشهر المواقع التي اخترقها الجيش الالكتروني السوري في هذه الفترة نجد: BBC رويترز_اسوشيتد برس _ هيومن رايتس ووتش _ نيويورك تايمس _ وكالة الأنباء الفرنسية.

الكشف بسهولة عمن يقف وراء العملية برمتها، وهو ما يؤكد أن الجيوش الإلكترونية مرتبطة بمؤسسات الدولة الأمنية.

هناك ثلاثة أنواع من هذه الجيوش الإلكترونية:[1]

1-الجيوش الإلكترونية ذات القبعة البيضاء الصالحة : التي تستخدم قدرتها بصورة شرعية لا تضر بمصالح الآخرين وتشكل خط الدفاع والحماية.

2- الجيوش الإلكترونية ذات القبعة السوداء : وهي المضرة التي تضر بمصالح الآخرين لتحقيق أهداف غير شرعية مثل السرقات والاختراقات وغيرها من التنمرات عبر وسائل التواصل الاجتماعي في ظل الحروب الباردة والناعمة وحروب العالم الافتراضي.

3- الجيوش الإلكترونية ذات القبعة الرمادية: والمتراوحة ما بين الإصلاح والعبث.

تقوم هذه الجيوش بالعديد من المهام، والتي يحددها رئيس مركز زيكوريون للاستشارات الأمنية وتحليل المعلومات فلاديمير أوليانوف في ثلاث نقاط رئيسية هي:[2]

- ✓ **التجسس:** أي العمل في الحصول على المعلومات السرية والتنصت على شخصيات ومؤسسات.
- ✓ **الهجمات الإلكترونية:** التي يكون التركيز الفعلي لها على نظم المعلومات المستخدمة ووسائل حمايتها وشبكات الاتصالات وعناصر للبنية التحتية الهندسية.
- ✓ **الحرب الإعلامية الإلكترونية** بمفهومها الواسع وبمختلف وسائلها التأثيرية على أمزجة سكان البلاد وسلوكياتهم، ومسرحها الرئيس وسائل الإعلام، وشبكات التواصل الاجتماعي، والتي يصعب تقييم فعاليتها بشكل متزن قبل الحصول على نتائج نشاطها التي ستحدد مستقبلاً لكون هذا الاتجاه جديدا وواعدا، وهذا ما يجب التركيز

---

[1]- سهير المهندي، دور الجيوش الإلكترونية في زمن الحروب المعلوماتية، متاح على الرابط:
https://bit.ly/3mEsvnT (2022/03/20)

[2]-المرجع نفسه.

عليه والاهتمام به أكثر عن غيره من المهام ضمن الأنواع الثلاثة للجيوش الإلكترونية.

ويشير معهد **راند** إلى أن هناك خمسة دول حول العالم هي الأقوى في الجيوش الإلكترونية، وقد رتبها معهد **راند** من الأقوى إلى الأضعف بحسب البنية التحتية والقدرات ومواقع الرصد بالإضافة إلى الميزانية التي تخصصها كل دولة للحرب الإلكترونية، حيث تأتي الولايات المتحدة في المركز الأول بأقوى جيش إلكتروني يضم 9 آلاف فرد بميزانية تصل إلى 7 مليارات دولار سنويا، تليها الصين التي تضم 20 ألف فرد بميزانية 1.5 مليار دولار ثم روسيا ثم إسرائيل في المركز الرابع وبريطانيا في المركز الخامس بـ 2000 فرد بميزانية 450 مليون دولار، بالإضافة إلى بعض ال لاعبين البارزين من غير هذه الدول أبرزهم إيران وكوريا الشمالية.[1]

من الدول التي قامت بإنشاء جيوش سيبرانية في سبيل حماية أمنها الإلكتروني، نجد:[2]

1- الوحدات الست في الولايات المتحدة : تعتمد الولايات المتحدة في الحروب الإلكترونية على ست عناصر هي الوحدة الأمريكية لقيادة "الفضاء الإلكتروني"، وهي المختصة بالتخطيط والتنسيق وإدارة عمليات الحروب الإلكترونية مع باقي الفروع التي تتبعها.

2- المكتب 121 في كوريا الشمالية : تمتلك كوريا الشمالية وحدة خاصة بالحروب الإلكترونية هي المكتب 121 " Bureau 121" وأهدافه الرئيسية هي كوريا الجنوبية والولايات المتحدة واليابان وأنشئ عام (1998).

---

[1]- الأضواء، "نظرية الحرب السيبرانية والجيوش السيبرانية: جيوش السوشيال ميديا والأمن السيبراني"، متاح على الرابط: https://bit.ly/3NYU2f4 (2022/03/18)

[2]- أمير مازن، الحرب السيبرانية"، متاح على الرابط:

https://bit.ly/3Mk07lj (2022/03/20)

3- اللواء 77 البريطاني: انضمت بريطانيا للحروب الإلكترونية باللواء (77) في بداية 2015، و يعمل على صد الهجمات المعادية ومراقبة المواقع والحسابات التي تدعو إلى الإرهاب والمؤيدة له، حيث يعمل اللواء البريطاني على شن الحروب النفسية ويتكون من 2000 جندي.

4- مخابرات الإشارة الروسية : وتتمثل في مجموعات من الهاكرز يعملون لصالح استخبارات الإشارة الروسية، ومن الهجمات التي شنها هاكر روس بحسب " سي إن إن" هو اختراق وزارة الخارجية الأمريكية واختراق أنظمة البيت الأبيض لدرجة تسريب جدول أعمال الرئيس الأمريكي باراك أوباما.

5- الوحدة 8200 الإسرائيلية : اشتهرت إسرائيل باستخدام تلك الوحدة من أجل الحرب النفسية على الانترنت ، حيث تركز على 30 موقع بالإضافة إلى العديد من مواقع التواصل الاجتماعي وتبث رسائلها بعدة لغات منها العربية والإنجليزية والعبرية والفرنسية والإسبانية .

6- **الجيش الإلكتروني بإيران:** والذي أظهر القدرة على اختراق أهدافه ببراعة على حد قول معهد الدراسات الإستراتيجية الأمريكي ، ما ساهم في بروز إيران كقوة في الحروب الإلكترونية.

7- **الوحدة (61398) في الصين:** تشتهر الصين بامتلاكها أحد أفضل الجيوش في الحروب الإلكترونية في العالم ، ورغم عدم الكشف رسميا عن الوحدة المسؤولة عن عمليات الاختراقات الصينية إلا أن وزارة العدل الأمريكية قالت أن الوحدة هي مصدر حروب الصين الالكترونية، وتقوم بشكل سري بتكوين وإنشاء محطات رصد ومراقبة، وهذا من خلال تأسيس وحدات عسكرية خاصة هدفها شن الهجمات الإلكترونية وسرقة الأسرار العسكرية للدول المعادية أو التي تحاول تفكيك رموز التنين الصيني[1].

المبحث الثالث:تحديات تحقيق الأمن السيبراني

[1]- مهدي سلمان الرسام،" **الجيش الإلكتروني العصر الجديد للحرب الافتراضية**"، متاح على الرابط: https://bit.ly/3Q196e6 (2022/03/22)

في إطار محاولاتها لإحتواء التهديدات السيبرانية، واجهت الدول مجموعة من التحديات التي أعاقت جهودها في تحقيق الأمن السيبراني، من هذه تحديات صعوبة تحقيق الردع السيبراني بمختلف أنواعه واستراتيجياته، وقد ساعدت الظروف التي رافقت ظهور فيروس كورونا من تصعيد حدة التهديدات السيبرانية وزيادتها مما صعب من المهمة الملقاة على الدول.

المطلب الأول: قصور إستراتيجية الردع السيبراني في مواجهة التهديدات السيبرانية

يعرف الردع السيبراني على أنه : "قدرة الدولة على تطوير قدرات عسكرية موثوقة ومتبادلة ومتماثلة في الفضاء الإلكتروني، وتكون قادرة على التأثير في قرارات الخصم ومنعه من شن هجمات عسكرية عبر الفضاء الإلكتروني".[1]

وهو تعبير عن قدرة الدولة على إنشاء نظم دفاع إلكترونية صعبة الاختراق، وتحتاج إلى وقت وجهد كبير لاختراقها، مع تطوير قدرات تتبع الهجمات السيبرانية واكتشاف مصدرها، بما يؤدي في النهاية إلى التأثير على قرارات الخصم وردعه عن شن هجمات سيبرانية على الدولة.[2]

يكمن الجوهر الأساسي لعملية الردع في الجدية في تنفيذ التهديد أو كما ذهب إلى ذلك **توماس شيلينج** (Thomas Schelling) بقوله:" كقاعدة عامة، يجب على المرء أن يهدد بأنه سوف يتصرف، وليس أنه قد يتصرف إذا فشل التهديد".[3]

وينقسم الردع السيبراني إلى عدة أنواع أهمها:

أ-الردع السيبراني حسب النوع: والذي ينقسم إلى قسمين:

---

[1]-إيهاب خليفة، **مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي**، مرجع سابق، ص 161.

[2]- شريفة كلاع، "الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني"، **مجلة الحقوق والعلوم الإنسانية**، المجلد 15، العدد 01، 2022، الجزائر، ص 39.

[3]-حسين قوادرة، "الردع السيبراني بين النظرية والتطبيق"، **المجلة الجزائرية للأمن والتنمية**، المجلد 09، العدد 16، جانفي 2020، ص 532.

- ✓ **الردع بالمنع :** في هذه الحالة يكون فيها الردع فعالا بمجرد جعل حسابات التكلفة لدى المهاجمين سلبية، من خلال إقناع المهاجم مهما كان فردا أو دولة أو جماعة بأنه لن تكون هناك مكاسب تتناسب مع تكلفة الهجوم، وهنا تتضح أهمية النظم الدفاعية الجيدة التي تجعل فرص نجاح أي هجوم ضئيلة، كما تضفي مصداقية على التدابير الانتقامية، وتحد من فكرة وجود الطرف الثالث، ومنه فإن "الردع بالمنع" موجود بصفة "دفاعية" قبل وقوع الحدث، وبصفة "صمودية" بعد الحدث.[1]

الردع بالانتقام: أو الردع الإيجابي، وهو يقوم على فكرة العقاب، وفيه يدرك الخصم أن أي هجوم سيتبعه هجوم آخر انتقامي لا يستطيع تفاديه أو تحمله، ويشمل ذلك الإعلان عن المصالح الحيوية واستعراض القوة والتهديد باستخدامها في حالة المساس بها.[2]

ويتضمن الردع با لمقاومة والردع بالصمود أي القدرة على استعادة الشيء الاصلي قبل وقوع

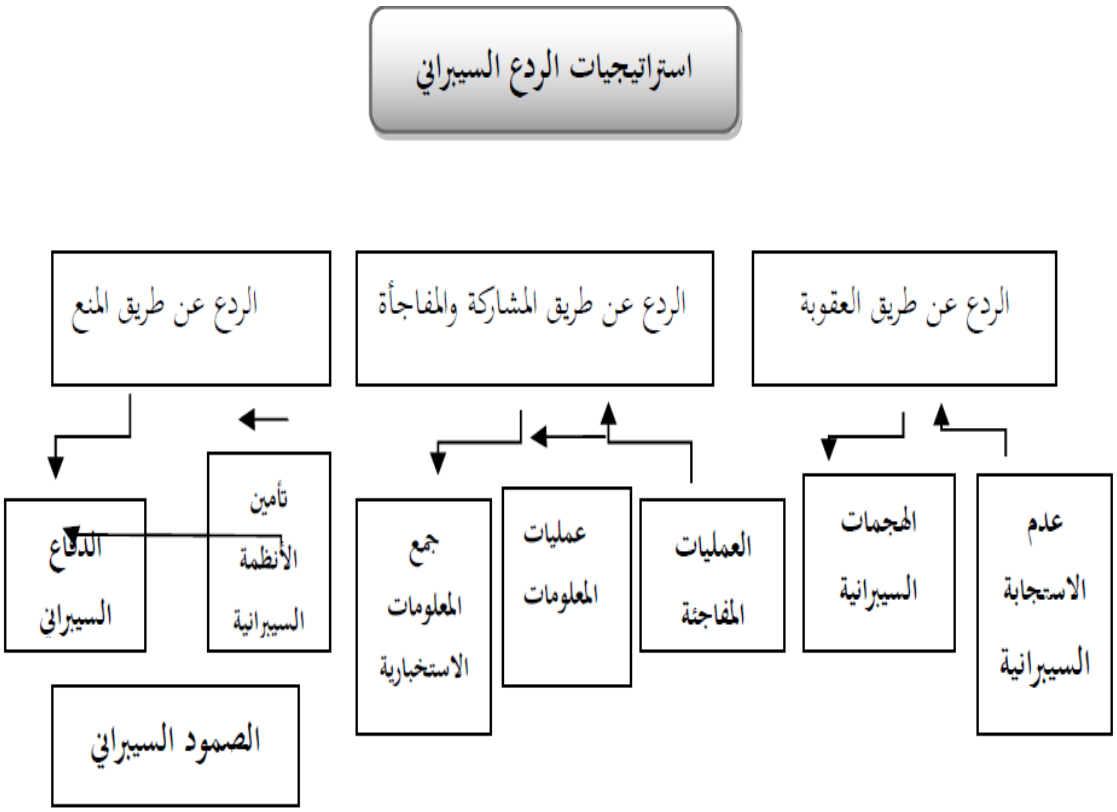
الهجوم، ويبين الشكل التالي تصنيفات الردع السيبراني من حيث النوع:

---

[1]– Annegret Bendiek and Tobias Metzger, **Deterrence theory in the cyber-century**, German Institute for International and Security Affairs, May 2015, Berlin, p556.

[2]–

الشكل رقم06: عناصر استرتيجية الردع السيبراني.[1]



ب-الردع من حيث الفعل: يستند هنا حدود الفعل في الردع في ثلاثة ركائز والتي تتمثل في: مصداق الدفاع عن أنظمة المعلومات ومنع أي محاولات لاختراقها عبر توافر أنظمة نسخ احتياطية، وهو ما يعني أن أي هجوم في هذه الحالة يسفر عن التدمير الكلي في ظل إمكانيات الاستعادة الذاتية، أما الركيزة الثانية فتتمثل في القدرة على الانتقام التي تتطلب وجود آليات الرد على الهجمات، وهو ما يمنح الطرف المتعرض للهجوم الدرة على إعادة بناء الذات وتحقيق التوازن مع الطرف المهاجم، أما العنصر الثالث فهو عملية الرغبة في الرد أي وجود نوايا للرد مع وجود القدرة على القيام بالفعل.[2]

---

[1]-علاء الدين فرحات، من الردع النووي إلى الردع السيبراني: دراسة لمدى تحقيق مبدأ الردع في الفضاء السيبراني"، **مجلة المفكر**، المجلد 16، العدد 01، 2021، ص 274.

[2]- سامي محمد بونيف، "دور الاستراتيجيات الإستباقية في مواجهة الهجمات السيبرانية –الردع السيراني أنموذجا–"، **المجلة الجزائرية للحقوق والعلوم السياسية**، المجلد 04، العدد 07، 30 جوان 2019، ص 130.

ويواجه تطبيق الردع السيبراني جملة من المعوقات والتحديات التي تجعل منه غير فعالا في ردع الهجمات السيبرانية، في هذا الصدد يذهب كل من ريتشارد كلارك Richard Clark وروبرت كناك Robert KNAKE إلى أنه "من بين جميع مفاهيم الاسترتيجية النووية فإن نظرية الردع هي على الأرجح الأقل قابلية للتحويل إلى الحرب السيبرانية".[1]

أ- **صعوبة معرفة مصدر الهجمات** : يعتبر معرفة مصدر الهجمات من أحد أهم شرو ط نجاح الردع السيبراني، إذ يتطلب هذا ضرورة توفر أربع عناصر أساسية تتمثل في: التتبع، التواصل والمصداقية.

فيما يخص عنصر التتبع ATTRIBUTIO فإنه يصعب تحديد هوية من قام بالهجوم والذي يمكن أن يكون فردا واحدا،جماعة إرهابية، تنظيم إجرامي، منظمة دولية أو حتى دولة، كما يصعب تتبع مكان تواجد الفاعل، والذي قد يكون من دولة واحدة أو من دول متعددة، إذ نجد أنه ورغم التطور التكنولوجي الهائل في وسائل وطرق التتبع والبحث والتحري إلا أن القصور في عمليات التمويه والإخفاء كان أكبر، وهو الأمر الذي جعل معرفة مصدر الهجمة يكاد مستحيلا عدا في حالة بعض الهجمات الصغيرة البسيطة، إذ يبق التحقيق والتحري حول مصدر الهجوم قائما لسنوات دون القدرة على الوصول إلى الفاعل.

في هذا الصدد نجد مثلا الهجمات السيبرانية التي قامت بها روسيا على إستونيا في سنة 2007، والهجمات الأمريكية الإسرائيلية على المفاعل النووي الإيراني عام 2010، والهجمات الكورية على شركة سوني عام 2015 ، والرد الأمريكي بقطع الإنترنت عن كوريا لمدة 10ساعات، وجميع هذه الهجمات لم يتم تبني الهجوم صراحة من قبل الدول المعتدية، بل إن بعضها أنكر القيام بذلك من الأساس، على الرغم من توفر الأدلة.[2]

---

[1]- علاء الدين فرحات، مرجع سابق، ص 276.

[2]- إيهاب خليفة، **مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي**، مرجع سابق، ص 162.

أما فيما يخص عنصر التواصلSIGNALING فإنه وبسبب عدم التعرف على الفاعل لا يمكن التواصل معه التواصل، ومن ثم يصعب إرسال الرسالة إلى الجمهور أو الفاعل المُستهدف.

وبالنسبة للمصداقية Credibility، فإن معظم الهجومات السيبرانية لا يتم الإعلان عنها من قبل الفاعل، إضافة إلى أن معظم الدول تنكر الاتهامات الموجهة إليها بشن هجمات سيبرانية رغم مسؤوليتهم في ذلك، لاسيما في ظل فضاء سيبراني يحترف رواده التخفي.

إضافة إلى عدم توفر إسناد الهجوم إلى مرتكبيه لأن الأسلحة السيبرانية خفية وغير مرئية إلى أن يقدم طرف ما على استخدامها على هذا لا يمكن للمهاجم أن يعرف إذا امتلك الخصم القدرة على الرد أو الانتقام.[1]

ب- تدخل الفاعلين من غير الدول: يمكن للفاعلين من غير الدول – بما في ذلك المنظمات الإجرامية والجماعات الإرهابية، والنشطاء السياسيين، وغيرهم – إحداث أضرار كبيرة بدرجات مختلفة. فكثيرا ما يشن الفاعلون من غير الدول هجمات سيبرانية لتحقيق مكاسب مالية أو لتقويض مصداقية الدول وهو ما يضفي مزيدا من التعقيد على الردع السيبراني؛ نظرا لصعوبة استهداف هؤلاء الفاعلين، مما يدعو للتساؤل عن جدوى الرد الانتقامي، ماذا إذا وجد هذا الفاعل داخل دولة ما، ووفرت له دولة أخرى الحماية، أيهما يتحمل المسئولية. [2]

ج- صعوبة تطبيق العقوبات القانونية على مرتكبي الهجمات السيبرانية : على أساس أن القانون الدولي يطبق على ارتكاب العدوان العسكري، وفي ظل القانون الدولي تنص المادة 51 من ميثاق الأمم المتحدة بأنه يجوز لدولة أن تتصرف بصورة شرعية للدفاع عن نفسها عندما تواجه هجوما مسلحا، أما في سياق الحرب السيبرانية، تطرح هذه المسألة المنطقية

[1]- رولا حطيط ، السيبرانية الحرب الخفية غي المنطقة المظلمة، مرجع سابق،ص 15.

[2]- رغدة البهي، مرجع سابق، ص 214.

تساؤلا مهما حول الحالات التي يمكن فيها اعتبار هجوم سيبراني معادلا لهجوم مسلح ومن ثم ما إذا كان من الممكن أن يعزى الهجوم إلى دولة ما، ففي هذا الصدد لا يمكن لدولة شن هجمات عسكرية على المعتدي لغياب ما يبيح ذلك، بالرغم من وجود بعض الهجمات السيبرانية يسفر عنها أضرار مادية كإنفجار القواعد العسكرية، وفي حالة قيام دولة برد عسكري على هجمات إلكترونية فإنها تعتبر من وجهة نظر القانون الدولي دولة معتدية.[1]

2- صعوبة وضع الخصم في تهديد حقيقي: إن الدول التي تتعرض لهجمات إلكترونية هي التي تستطيع أن تقدر مدى فداحة هذه الهجمات والخسائر المترتبة عليها، ومن ثم فقد تقوم دولة بشن هجوم إلكتروني انتقامي على دولة أخرى بهدف تحقيق الردع بالانتقام، وأن تستطيع إصابة أهداف معينة داخل الدولة.

المطلب الثاني: تهديدات الأمن السيبراني في زمن وباء كورونا

كان لأزمة **فيروس كورونا** * تأثير كبير على كافة مناحي الحياة عبر كافة دول العالم، تميزت هذه الفترة بإجراءات تم إتخادها من قبل دول العالم تمثلت في غلق الحدود ومنع التجمعات واللقاءات تفاديا لانتشار فيروس كورونا، تزايد خلال هذه الفترة الإعتماد الكبير جدا على الإنترنيت والأدوات الرقمية، واتجهت كثير من الشركات والمؤسسات في هذه الدول لتبني نمط العمل عن بعد والتعليم عن بعد في محاولة للتكيف مع هذا الوضع الدولي الجديد.

تزايدت أيضا في هذه الفترة الإختراقات والهجمات الإلكترونية وارتفع حجم التهديدات السيبرانية لعدة أسباب منها:

---

[1]- حمدون إ. توريه، مرجع سابق، ص91.

*-**فيروس كورونا** : أو مرض الفيروس التاجي COVIDE 19، أو هو مرض معد ظهر في مدينة ووهان بالصين في أواخر 2019، ثم بدأ بالانتشار عبر دول العالم ليصل إلى 200 دولة، تم خلالها فرض مجموعة من الإجراءات في سبيل محاصرة الفيروس ومنعه من الانتشار إلى مناطق أوسع، ومن أهم هذه الإجراءات غلق الحدود ومنع الاجتماعات وتطبيق تقنية العمل عن بعد.

1- **التوسع في العمل عن بعد:** بحيث تم التوسع من قبل مؤسسات ومنظمات في إنشاء شبكات تتيح لموظفيها إمكانية العمل من المنزل ، والولوج إلى بيانات مؤسساتهم عن بعد من أجل استمرار تلك المؤسسات، في سبيل ذلك استعانت باستخدام تطبيقات عبر الانترنت لانعقاد الاجتماعات وأي أنشطة أخرى لازمة، وهو ما سهل عملية قرصنة قاعدة البيانات للشركات من قبل مجرمي الانترنيت، ذلك أن هذه الاجتماعات قد تحتوي على معلومات سرية تم تسريبها أو استغلالها بصورة إجرامية أخرى.[1]

2- **صعوبة تأمين بيئة الأعمال السيبرانية:** بسبب ضعف الإجراءات السيبرانية الأمنية، وصعوبة السيطرة على البيئة الإلكترونية الخاصة المؤسسات والشركات.

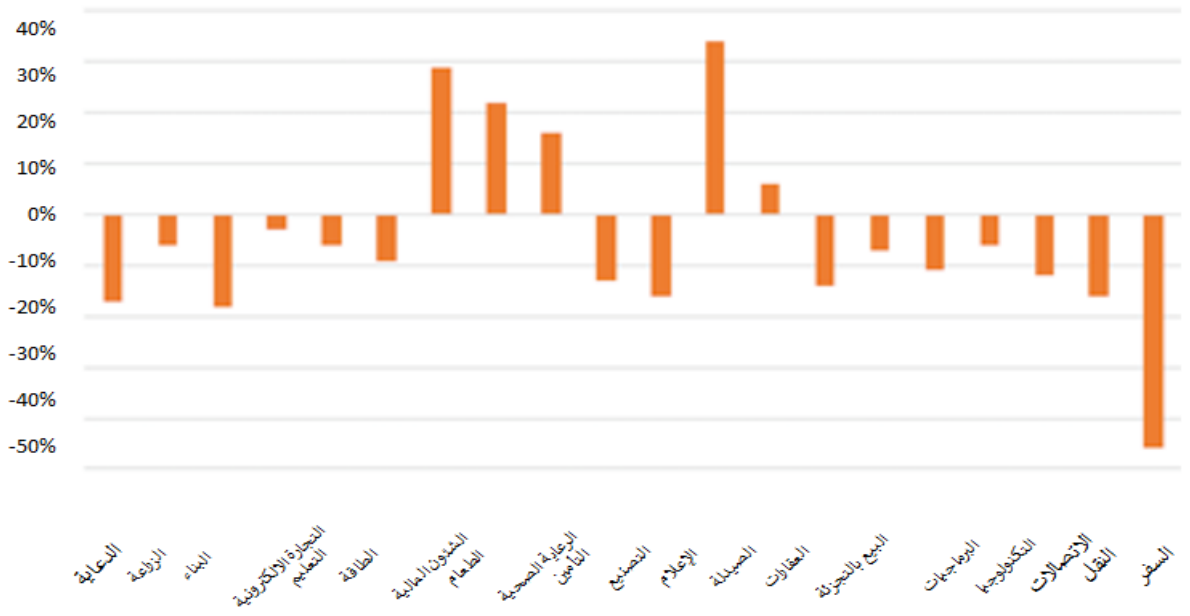
3- **زيادة الاعتماد على تطبيقات التواصل الاجتماعي:** من خلال تطبيقات التواصل الاجتماعي ومكالمات الفيديو، وتزايد المخاوف والقلق من قبل الأفراد والبحث عن المعلومات حول الوباء واستغلال القراصنة لهذا الموضوع من خلال إنشاء تطبيقات موهمة بتقديم المعلومات بحيث يتم الاختراق بمجرد الدخول إليها خاصة في ظل عدم وجود رقابة صارمة على عمليات إدخال المحتوى عبر منصات تطبيقات الهواتف الجوالة.[2]

---

[1]- مكتب الأمم المتحدة المعني بالمخدرات والجريمة، كوفيد 19: تحليل التهديدات الإلكترونية ، **مكتب الأمم المتحدة المعني بالمخدرات والجريمة** ، ماي 2020، ص 10.

[2]-نيكي أوبراي وآخرون، حماية نظم الرعاية الصحية إطار عالمي للأمن السيبراني، تقرير شبكة الأنظمة الصحية الرائدة، تقرير إلكتروني، معهد الإبتكار في مجال الصحة العالمية في إمبريال كوليدج، لندن، نوفمبر، 2020، ص 08.

الشكـــــــل رقم07: رسم بياني يبين نسبة استخدام مواقع التواصل الاجتماعي نتيجة لكوفيد 19[1]



4- زيادة فترة الاستخدام وزيادة معدل التعرض للهجمات السيبرانية: في هذا أعلنت شركة فودافون بلوغ نسبة الزيادة في تحميل البيانات الخاصة بها وصلت إلى 50% في بعض البلدان، كما زاد استهلاك الإنترنت في بعض البلدان مثل إيطاليا بنسبة 30%، وزاد استهلاك الولايات المتحدة الأمريكية بنسبة 18%.[2]

5-التطبيق المتسرع لحلول رقمية جديدة دون أن يؤثر ذلك على وصول المرضى لخدمات الرعاية الصحية. وتكتنف هذه التكنولوجيات الجديدة مخاطر عديدة تعرض الأنظمة لمخاطر الاختراق، مثل الثغرات التصميمية التي تهدد أمن البيانات المحفوظة بها.

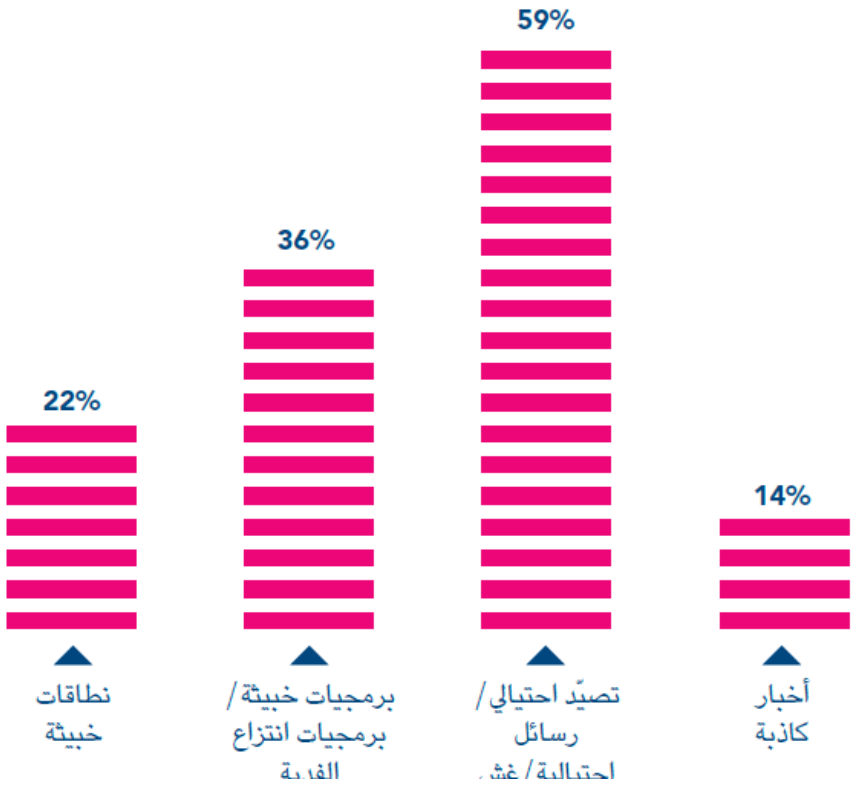
ويقدم الأنتربول مجموعة من الإحصائيات تبين مدى توسع التهديدات السيبرانية خلال فترة أزمة كورونا استنادا إلى تحليل شامل للبيانات الواردة من الدول الأعضاء فيه، والشركاء

[1]- مكتب الأمم المتحدة المعني بالمخدرات والجريمة، مرجع سابق، ص 08.

[2]-إيهاب خليفة، " الأمن المعلوماتي: لماذا تصاعدت التهديدات الإلكترونية مع انتشار "كورونا"؟، متاحة على الرابط: https://bit.ly/3NWFOeJ .(2022/05/12)

من القطاع الخاص، والمركز المتعدد الاختصاصات لمكافحة الجريمة السيبرانية، وهي تهديدات ذات مخاطر رئيسية مرتبطة بوباء كوفيد 19، كما يوضحه الشكل التالي:

الشكل رقم08: توزع التهديدات السيبرانية الرئيسية الناجمة عن كوفيد 19.[1]



وخلال فترة كورونا تعرضت الحكومات لتهديدات مباشرة تؤثر على الأمن القومي، فنتيجة للعمل عن بعد تمت سرقة بيانات ومعلومات هامة، تضر بالدولة وأجهزتها لاسيما منها الوثائق السرية المسربة، على هذا اضطر عدد كبير من الحكومات إلى إعادة توجيه الموارد للاستثمار في قطاعات حيوية مثل الخدمات الصحية وبحوث استشراف ومعالجة الأوبئة ومؤسسات الأمن السيبراني وغيرها من القطاعات التي تقف على خط الصد الأول في مواجهة هذا الوباء وتداعياته على الأمن الوطني.

[1]- الإنتربول، "الجريمة السيبرية كوفيد 19 "، تقرير تقييم صادر عن الأنتربول، فرنسا، أوت 2020، ص08.

خلاصة واستنتاجات:

من خلال ما سبق، يمكن القول أن الدول استجابت وواجهت التهديدات السيبرانية المختلفة من خلال جملة من التدابير عل المستوى الداخلي تجلت في مجموعة من الاستراتيجيا ت الوطنية للأمن السيبراني وإنشاء هيئات مختصة بحماية البنية التحتية للدولة من المخاطر الالكترونية، وعلى المستوى الدولي تجلى هذا الاهتمام في شكل اتفاقيات دولية ومنظمات تسعى إلى تأمين الفضاء السيبراني العالمي وحمايته وتحقيق الأمن السيبراني العالمي، وفي ظل التغيرات التي رافقت ظهور فيروس كورونا والتحول إل العمل من المنازل تفاقمت عمليات القرصنة والاختراقات الالكترونية وبلغت حدتها ما فرض ضرورة تكثيف وتشديد آليات الحماية وتطويرها، في مقابل صعوبة عملية الردع السيبراني في مواجهة التهديدات السيبرانية بسبب صعوبة تحديد المتسبب في الهجمات من جهة وتطور وتعدد طرق ممارسة الهجمات والفواعل المتداخلة في الهجوم، وهو أمر يفرض تحديات عديدة تواجهها الدول بغية تحقيق الأمن السيبراني.

الخاتمة

تعد التهديدات السيبرانية واحدة من أهم إفرازات التطور التكنولوجي المتسارع وثورة المعلومات الواسعة، ففي الوقت الذي ساهمت فيه التكنولوجيا في تحقيق التقدم في مختلف المجالات، وفي تقريب المسافات بين شعوب العالم، وتسهيل حياة الأفراد، فإنها في المقابل أفرزت مجموعة من التهديدات لم تكن موجودة سابقا، تختلف عن التهديدات التقليدية من حيث الطبيعة والوسائل والفواعل والنتائج، فأصبحت هذه التهديدات تشكل مصدر قلق لأمن الفرد والدول، بحيث لم يعد يخترق الأمن المعلوماتي للفرد فقط إنما تعداه إلى البنية التحتية للدولة ككل.

ساعدت الثورة التكنولوجية في إحداث تغييرات عدة من حيث طبيعة الحروب والأدوات المستخدمة في الحروب ، وظهرت حرب الشبكات وحرب الفضاء الإلكتروني أو ما تم تسميته بالحروب السيبرانية ، والتي جاءت مواكبة أو معبرة عن استخدام الآليات التقليدية للصراع ولكن بوجه تكنولوجي يتواكب مع العصر ، من أهم مميزات هذه الحروب أنها حروب مخفية لا يظهر مرتكبوها ويصعب الوصول إليهم، ولا تظهر قطرة دم فيها، غير أن خسائرها تكون باهضة كونها تمس البنية التحتية والحرجة للدول.

ظهر تأثير التكنولوجيا الرقمية أيضا على استخدامات مفهوم القوة في الصراعات الدولية، فظهر سعي كثير من الدول نحو الولوج لمجال الفضاء الإلكتروني ، وظهر تأثر مفهوم القوة بالتكنولوجيا الرقمية في إطار ما سمي القوة السيبرانية التي أصبحت أحد أهم معايير القوة في العلاقات الدولية.

أدت سهولة الحصول على التقنيات المتطورة وتوفرها إلى انتشار القوة بين مجموعة فاعلين جدد، أصبح لهم القدرة على ممارسة التهديد وتنفيذه وإلحاق الضرر بالدول والأفراد، إذ أصبح يكفي امتلاك جهاز ذكي موصول بشبكة انترنيت فقط من أجل تنفيذ هجوم على كبرى الدول وأقواها، وبات ممكنا استهداف أي دولة مهما كانت درجة تأمينها.

ظهر التزاوج بين الإرهاب وتكنولوجيا الاتصال والمعلومات كشكل جديد آخر من أشكال التهديدات الأمنية الجديدة للمجتمع الدولي ، وإمكانية استخدامه في كافة الأنشطة الحساسة والأكثر تهديدا للأمن الدولي.

بعد استعراض الاستجابة الدولية للتهديدات السيبرانية والتي كانت في شكلين، أحدهما على المستوى الداخلي للدول تمثل في استراتيجيات وطنية للأمن السيبراني، والتي نجحت في تحقيق أشواط معتبرة في الأمن السيبراني، واستراتيجيات أخرى على المستوى الدولي تمثلت في جهود جماعية في إطار الأمم المتحدة واتفاقيات دولية واقليمية، و التي وعلى رغم الجهود المبذولة من قبلها إلا أنها لم تحقق نتائج مبهرة في مواجهة التهديدات السيبرانية، ولعل السبب في هذا العجز هو غياب رغبة وتجاوب من طرف الدول وضعف الأداء من جهة أخرى، في ظل غياب أطر قانونية تحدد التعاملات في الفضاء السيبراني وتضبطها، وصعوبة تطبيق مبدأ الرد المادي في حالات الهجومات السيبرانية.

يكمن التحدي الذي يواجه تحقيق الأمن السيبراني في الطبيعة المتطورة للتهديدات السيبرانية، وكيفيات معالجتها التي تعتمد على الطرق التقليدية المستخدمة في مواجهة التهديدات التقليدية، وغياب أطر قانونية يمكن من خلالها التصدي لهذه التهديدات.

من أهم التوصيات التي توصي بها الدراسة ، ضرورة تعزيز درجة التعاون الدولي بين الجهات الوطنية والدولية لتحفيز بيئة تعاونية ينصب تركيزها على تحقيق الأهداف الأساسية وتعزيز مستويات التعاون بين الدول كون هذه التهديدات عالمية وليست موجهة لدولة فقط مادام الكل مندمج في الفضاء السيبراني الذي لا حدود ولا سيادة فيه لأحد.

قائمة المراجع

قائمة المراجع:

أ-القواميس:

1-البعلبكي منير، **المورد: قاموس انكليزي عربي**. دار العلم للملايين، بيروت، 2004.

2-إبن منظور، **لسان العرب**. دار صادر، بيروت، (د.س.ن)

ب-الكتب:

باللغة العربية:

1-جبور منى الأشقر، **السيبرانية هاجس العصر** ، المركز العربي للبحوث القانونية والقضائية، (د.ب.ن)،(د.س.ن).

2-عبد الصبور عبد الحي صباح، **استخدام القوة الالكترونية في التفاعلات الدولية تنظيم القاعدة نموذجا**، المعهد المصري للدراسات السياسية والإستراتيجية، مصر، 2016.

3-عبد الصادق عادل، **الإرهاب الالكتروني: القوة في العلاقات الدولية: نمط جدد وتحديات مختلفة**، مركز الدراسات السياسية والإستراتيجية، القاهرة، 2009.

4-عبد الوهاب منصور شادي، **حروب الجيل الخامس أساليب التفجير من الداخل على الساحة الدولية**، العربي للنشر والتوزيع، القاهرة، 2019.

5-عمر حامد شكر، **المجال الخامس الفضاء الإلكتروني**. المعهد المصري للدراسات، 2019، (د.ب.ن).

6-خليفة إيهاب، **مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي**،العربي للنشر والتوزيع، القاهرة، 2019.

7- (ـــــــــــــــ)، **القوة الالكترونية وأبعاد التحول في خصائص القوة** ، مكتبة الإسكندرية، مصر، 2014.

8-(ـــــــــــــــ)، **القوة الالكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الانترنيت " الولايات المتحدة الأمريكية نموذجا**"، العربي للنشر والتوزيع، القاهرة، 2017 .

9- توريه حمدان،**البحث عن السلام السيبراني**، الاتحاد الدولي للاتصالات، (د.ب.ن)، 2011.

باللغة الإنجليزية:

1-Annegret Bendiek and Tobias Metzger, **Deterrence theory in the cyber-century**, German Institute for International and Security Affairs, May 2015, Berlin, p556.

2-Nye Joseph, **cyber power**, belfer center for science and international affairs, Britain, 2010.

المجلات:

1-أحمد صالح ياسين،"الإرهاب الإلكتروني في ظل أزمة فيروس كورونا:الأنماط والتداعيات"، **مجلة كلية السياسة والاقتصاد**، العدد 9، 2021، ص24.

2-باسيت جون، "حرب الفضاء الالكتروني: التسلح وأساليب الدفاع الجديدة"، الحروب المستقبلية في القرن الحادي والعشرين"، **مركز الإمارات للدراسات والبحوث الإستراتيجية** ، الإمارات العربية المتحدة، 2014.

3-بانقا علم الدين ، "مخاطر الهجمات الالكترونية (السيبرانية) وقارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي"، **سلسلة دراسات تنموية**، العدد 63، 2019.

4-البابلي عمار ياسر زهير ، "التحديات الأمنية المعاصرة للإرهاب السيبراني"، **الفكر الشرطي**، المجلد 30، العدد 118، 2021.

5-بارة سمير، "الأمن السيبراني في الجزائر: المؤسسات والسياسات"، **المجلة الجزائرية للأمن الإنساني**، العدد 04، جويلية 2017.

6- البهي رغدة ، "الردع السيبراني:المفهوم والإشكاليات والمتطلبات"، **مجلـــة الدراسات الإعلاميـــة**، العدد 01، يناير 2018.

07- بونيف سامي محمد، "دور الاستراتيجيات الإستباقية في مواجهة الهجمات السيبرانية: الردع السيبراني نموذجا"، **المجلة الجزائرية للحقوق والعلوم السياسية** ، المجلد 04، العدد 07، جوان 2019.

08-البيديري عبد الواحد ، "إستراتيجية الأمن السيبراني: دراسة حالة المغرب"، **مجلة الدراسات الإستراتيجية والعسكرية**، المركز الديمقراطي العربي، العدد 11، جويلية 2021.

09-بن مرزوق عنترة، الكر محمد ، "البعد الإلكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب"، **مجلة العلوم الإنسانية والإجتماعية**، العدد38، جوان 2018.

10-بلعسل بنت نبي ياسمين، عمروش الحسين، "التهديدات الالكترونية والأمن السيبراني في الوطن العربي"، **مجلة نوميروس الأكاديمية**، المجلد 02، العدد 02، 2021.

11-بلقاسمي مولود، حادي إبراهيم،تحولات مفهوم القوة في الفضاء الالكتروني: مقاربـــة سياسية، **مجلة القانون والعلوم السياسية**، المجلد 02، العدد 01، جانفي 2016.

12-جابوري إسماعيل ، "دور الأمن السيبراني في مواجهة التهديدات الإلكترونية: دراسة حالة الجزائر"، **مجلة تحولات**، ديسمبر 2020.

13-جارش عادل ، مقاربة معرفية حول التهديدات الأمنية الجديدة، **مجلة العلوم السياسية والقانون**، العدد01، 2017.

14-جلال عواد منى ،" مقاربة تحليلية لظاهرة الإرهاب الالكتروني"، **مجلة تكريت للعلوم السياسية**، العدد 19، 2020.

15-جعيجع عبد الله ، "تطور الإرهاب وانعكاسه على استقرار المجتمعات: قراءة في ظاهرة الإرهاب الالكتروني وإستراتيجية المواجهة"، **مجلة دفاتر السياسة والقانون** ، المجلد 13، العدد 01، 2021.

16-هاتاواي ميليسا، إدارة الخطر السيبراني الوطني، فهم الخطر السيبراني، (د.ب.ن)، (د.س.ن).

17- الزهواني شيخة حسين ، "التعاون الدولي في مواجهة الهجوم السيبراني"، **مجلة جامعة الشارقة**، المجلد 17، العدد 1، جوان 2020.

طارش عبد الرضا أسعد ، المعموري علي إبراهيم مشجل ، "الأمن السيبراني ودوره في انتشار ظاهرة الإرهاب في العراق بعد العام 2003"، مجلة **دراسات دولية**، العدد 80، (د.س.ن).

18-الطائي كرار فرحان هاني ، "أثر الأنترنيت العميق في أمن الدول"، **مجلة الدراسات الإستراتيجية والعسكرية**، المجلد 02، العدد 8، سبتمبر 2020، ص 67.

19- طلال ياسين العيسى، عدي محمد عناب،"المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر"، **مجلة الزرقاء للبحوث والدراسات الإنسانية** ، المجلد 19،العدد01، 2019.

20- طاية لامية، "التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها"، **مجلة معالم للدراسات القانونية والسياسية**، المجلد 4، العدد 2، 2020.

21-ياسين يحيى، "الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني"، **المجلة القانونية المتخصصة في الدراسات والبحوث القانونية**.

22-يونس مصطفى يونس مؤيد ، "إستراتيجية الولايات المتحدة الأمريكية للأمن السيبراني "، **مجلة قضايا سياسية**، العدد 55، 2018.

23-كلاع شريفة،"الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني"، **مجلة الحقوق والعلوم الإنسانية**، المجلد 15، العدد 01، 2022، الجزائر.

24-لحمر حميدة، حموم فريدة، "التعاون الأمني في جنوب شرق آسيا في مواجهة التهديدات الأمن السيبراني"، **مجلة طبنة للدراسات العلمية الأكاديمية**، العدد 01، المجلد 4، 2021.

25-لطفي وفاء ، "الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني: التجربة الماليزية نموذجا"، **مجلة دراسات**، المجلد23، العدد1، 2022.

26-مصطفى إبراهيم سلمان الشمري، "الأمن السيبراني وأثره في الأمن الوطني العراقي"، **مجلة العلوم القانونية والسياسية**، المجلد 10، العدد1، 2021، ص 12.

27-مشوش مراد، "الجهود الدولية لمكافحة الإجرام السيبراني"، **مجلة الواحات للبحوث و الدراسات**، المجلد 12، العدد 2، 2019.

28-صالحي نصيرة ، القوة الذكية: التنافس العالمي على قوة الفضاء الالكتروني والقدرات السيبرانية"، **دفاتر السياسة والقانون**، المجلد 13، العدد1، 2021.

29-عبد الله السمحان منى ، "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود"، **مجلة كلية التربية**، العدد 111، 2020.

30-عبد الحميد عائشة، "الإطار القانوني والتشريعي للرقمنة والذكاء الاصطناعي"، **المجلة الدولية للتعليم بالانترنيت**، جويلية 2020، ص 104.

31-عبد الوهاب شادي، التحولات الرئيسية في المواجهات العنيفة غير التقليدية في العالم، **دراسات المستقبل**، الإمارات العربية المتحدة، 2017.

32-عبد العظيم محمد عبد الجواد أميرة ، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، **مجلة الشريعة والقانون**، العدد53، الجزء3، 2020.

33-العبودي علي عبد الرحيم ، "هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين"، **مجلة قضايا سياسية**،العدد 57، 2019.

34-العوفي دليلة ، "الحرب السيبرانية في عصر الذكاء الإصطناعي ورهاناتها على الأمن الدولي"، **مجلة الحكمة للدراسات الفلسفية**، المجلد 9، العدد 02، 2021.

35-عطية إدريس، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري"، **مجلة مصداقية**، (د.س.ن).

36-فرحات علاء الدين ، الفضاء السيبراني تشكيل ساحة المعركة في القرن الحادي والعشرين"، **مجلة العلوم القانونية والسياسية** ، المجلد 10، العد3 ،2019.

37-فرحات علاء الدين، من الردع النووي إلى الردع السيبراني: دراسة لمدى تحقيق مبدأ الردع في الفضاء السيبراني"، **مجلة المفكر**، المجلد 16، العدد 01، 2021.

38-فرج كرار عباس متعب، "الحرب السيبرانية: دراسة في إستراتيجية الهجمات السيبرانية بين الولايات المتحدة وإيران"، **مجلة حمورابي للدراسات**، العدد 40، شتاء 2021.

39-الفتلاوي أحمد عبيس نعمة ، "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، **مجلة المحقق الحلي للعلوم القانونية والسياسية** ، العدد 4، السنة8، 2016.

40-تغريد صفاء، لبنى خميس مهدي،"أثر السيبرانية في تطور القوة"، **مجلة حمورابي**، العدد 33-34، السنة 8، 2020.

41-قوادرة حسين ، "الردع السيبراني بين النظرية والتطبيق"، **المجلة الجزائرية للأمن والتنمية** ، المجلد 09، العدد 16، جانفي 2020.

42-شلوش نورة ، "القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول"، **مجلة مركز بابل للدراسات الإنسانية**، المجلد 07، العدد 02، 2018.

43-الشمري صلاح مهري هاوي وآخرون، الأمن السيبراني كمركز جديد في الإستراتيجية العراقية"، **مجلة قضايا سياسية،العراق**، العدد 62، السنة 12، 2020.

44-شنوف زينب، "الحرب السيبرانية في العصر الرقمي: حرب ما بعد كلاوزفيتش"، **المجلة الجزائرية للأمن والتنمية**، المجلد 09، العدد 02، جويلية 2020.

45-خليفة إيهاب ، "الأمن السيبراني: الماهية والإشكاليات"، **مجلة رؤى مصرية**، أكتوبر 2016.

غريب حكيم، "الإرهاب السيبراني والأمن الدولي: التهديدات العالمية الجديدة وأساليب المواجهة"، **المجلة الجزائرية للدراسات السياسية**،المجلد 05، العدد 02، 2018.

46-غيدان سرى غضبان، الربيعي محمد منذر جلال،"الأمن السيبراني وسياسات المواجهة الدولية"، **مجلة الدراسات الإستراتيجية والعسكرية**، المجلد 2، العدد 9، ديسمبر 2020.

التقارير:

1- أمانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات، **إستراتيجية الأمن السيبراني العراقي**، مستشارية الأمن الوطني،(د.س.ن).

2-أوبراي نيكي وآخرون، حماية نظم الرعاية الصحية إطار عالمي للأمن السيبيراني، تقرير شبكة الأنظمة الصحية الرائدة، تقرير إلكتروني، معهد الإبتكار في مجال الصحة العالمية في إمبريال كوليدج، لندن، نوفمبر، 2020.

3-الإتحاد الدولي للإتصالات، **المبادئ التوجيهية لاستعمال البرنامج العالمي للأمن السيبراني** ، تقرير من الأمن العام، المجلس 2020، جينيف، 5 ماي 2020.

4-الاتحاد الدولي للاتصالات، "**دليل لوضع إستراتيجية وطنية للأمن السيبراني التزام استراتيجي بالأمن السيبراني**"،الاتحاد الدولي للاتصالات،(د.ب.ن)، 2017.

5- الإنتربول، "الجريمة السيبرية كوفيد 19 "، تقرير تقييم صادر عن الأنتربول، فرنسا، أوت 2020.

6-اللجنة الاقتصادية والاجتماعية لغربي آسيا الإسكوا،**الأمن في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية توصيات سياساتية**، الأمم المتحدة، نيويورك، 2015.

7- مكتب الأمم المتحدة المعني بالمخدرات والجريمة، كوفيد 19: تحليل التهديدات الإلكترونية ، **مكتب الأمم المتحدة المعني بالمخدرات والجريمة** ، ماي 2020.

8- مجتمـــع المعلومات، **المبادئ التوجيهية المتعلقــة بأمن البنيـــة التحتية للانترنيت فـي الدول العربية**، مارس 2020.

9- التمويل والتنمية،" التهديد السيبراني العالمي"، التمويل والتنمية،(د.ب.ن)، 2021.

الدراسات الغير منشورة:

-1نور أمير الموصلي، "ا **لهجمات السيبرانية في ضوء القانون الدولي الإنساني** "، بحث مقدم لاستكمال متطلبات نيل درجة ماجيستر التأهيل والتخصص في القانون الدولي الإنساني، الجامعة الافتراضية السورية، 2021.

المواقع الالكترونية:

1-الأضواء، "نظرية الحرب السيبرانية والجيوش السيبرانية: جيوش السوشيال ميديا والأمن السيبراني"، متاح على الرابط:

https://bit.ly/3NYU2f4 (2022/03/18)

2-الاتحاد الدولي للاتصالات،"**نبذة عن الاتحاد الدولي للاتصالات(ITU)** "، متاح على الرابط:

https://bit.ly/3mkar1Q (2022/05/12)

3-الجزيرة،" **ماذا تعرف عن الجيوش الإلكترونية؟**"، متوفر على الرابط:

https://bit.ly/3x9RELO (2022/04/12)

4-داليا السيد،"**الهجمات السيبرانية... تهديد متعاظم للأمن والاستقرار والاقتصاد العالمي**"، متاح على الرابط:

https://bit.ly/3xbO6J9(2022/02/22)

5-مازن أمير، الحرب السيبرانية"، متاح على الرابط:

https://bit.ly/3Mk07lj (2022/03/20)

06-الموسوعة السياسية، "التهديدات الأمنية"، متاح على الرابط:

https://bit.ly/3Nf6Xtv (2022/02/01)

07-معهد التطوير،"**معنى هجوم سيبراني وأنواع الهجمات السيبرانية**"، متاح على الرابط:
https://bit.ly/38VPc3p (2022/02/15)

08-المهندي سهير، دور الجيوش الإلكترونية في زمن الحروب المعلوماتية، متاح على الرابط:
https://bit.ly/3mEsvnT (2022/03/20)

09-العباسى ريهام عبد الرحمن رشاد ،" **أثر الإرهاب الالكتروني على تغير مفهوم القوة في العلاقات الدولية دراسة حالة: تنظيم الدولة الإسلامية"،متاح على الرابط:**
https://bit.ly/3mnfwXa (2022/05/10)

10-عمرو صبحي، "**تكتيك الدرع والسيف في استخدام القوة السيبرانية**"، متاح على الرابط:
https://bit.ly/39aeXNt**(2021/02/12)**

11-صخري محمد ، "**الحرب السيبرانية وتداعياتها علي الأمن العالمي**"، متاح على الرابط:
https://bit.ly/3GPM6KM (2022/02/22)

13-الرسام مهدي سلمان،"الجيش الإلكتروني العصر الجديد للحرب الافتراضية "، متاح على الرابط:
https://bit.ly/3Q196e6 (2022/03/22)

14-الخندق أثير، "**ما هو الأمن السيبراني؟ ومتى نشأ؟**"، متاح على الرابط:
https://bit.ly/395VxJW (2022/04/02)

15-خليفة إيهاب، " **الأمن المعلوماتي: لماذا تصاعدت التهديدات الإلكترونية مع انتشار "كورونا"؟**، متاحة على الرابط:
https://bit.ly/3NWFOeJ (2022/05/12)

قائمة الجداول و الأشكال

قائمة الأشكال والجداول:

رقم الشكل	عنوان الشكل	الصفحة
01	الجهات التي تقوم بالهجمات السيبرانية ودوافعها وأهدافها	24
02	أوجه إستخدام السلطة في المجال السيبراني	41
03	أشكال القوة السيبرانية حسب جوزيف ناي	46
04	تطور استخدام الأسلحة الإلكترونية حتى سنة **2020**	50
05	دورة حياة الإستراتيجية الوطنية للأمن السيبراني	65
06	عناصر استرتيجية الردع السيبراني	76
07	رسم بياني يبين نسبة استخدام مواقع التواصل الاجتماعي نتيجة لكوفيد 19	81
08	توزع التهديدات السيبرانية الرئيسية الناجمة عن كوفيد 19	82

فهرس المحتويات

فهرس المحتويات:

مقدمـــــة.....أ
الفصل الأول: التهديدات السيبرانية: تحديد المفاهيم والمظاهر..... 9
المبحث الأول: التهديدات السيبرانية: مقاربة مفاهيمية..... 9
المطلب الأول:مفهوم التهديدات السيبرانية..... 9
المطلب الثاني: المفاهيم المرتبطة بالتهديدات السيبرانية..... 14
المبحث الثاني: مظاهر التهديدات السيبرانية.....21
المطلب الأول:الهجمات السيبرانية..... 21
المطلب الثاني:الإرهاب السيبراني..... 29
الفصل الثاني: تطور التهديدات السيبرانية وتأثيرها على الأمن الدولي.....36
المبحث الأول: التحول في مفهوم القوة.....37
المطلب الأول:مفهوم القوة السيبرانية..... 38
المطلب الثاني: استخدام القوة السيبرانية..... 40
المبحث الثاني: التحول في طبيعة الفوعل..... 42
المطلب الأول:انتشار القوة السيبرانية بين الفواعل..... 42
المطلب الثاني: الفواعل المالكة للقوة السيبرانية..... 45
المبحث الثالث:التحول في طبيعة الصراع والحروب.....47
المطلب الأول:مفهوم الحروب السيبرانية..... 47
المطلب الثاني: مميزات وانواع الحروب السيبرانية..... 50
الفصل الثالث:الجهود الدولية والوطنية لتحقيق الأمن السيبراني.....54
المبحث الأول: الاتفاقيات والمعاهدات الدولية والإقليمية..... 55
المطلب الأول: الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية.....55
المطلب الثاني: برنامج الأمن السيبراني العالمي: الاتحاد الدولي للاتصالات.....58
المبحث الثاني: الجهود الوطنية لمواجهة التهديدات السيبرانية..... 61
المطلب الأول: الإستراتيجية الوطنية للأمن السيبراني..... 62
المطلب الثاني:بناء الجيوش السيبرانية..... 69
المبحث الثالث: تحديات تحقيق الأمن السيبراني..... 73

المطلب الأول:قصور الردع السيبراني في مواجهة التهديدات السيبرانية 73
المطلب الثاني: تهديدات الأمن السيبراني في زمن وباء كورونا..... 78
الخاتمـــــــــــــة..... 84
فهرس الأشكال والجداول..... 87
فهرس المحتويات..... 89

ملخص الدراسة:

لقد كان للثورة المعلوماتية والرقمية التي شهدها العالم خاصة في القرن 21 تأثير كبير في ظهور وضع دولي جديد، يتميز بتحولات عديدة أفرزها التزايد المتسارع في استخدامات الفضاء السيبراني، فكان أبز معالم هذه التحولات هو التغييرات التي مست أهم المفاهيم الكلاسيكية على غرار مفهوم القوة ،الحرب والفواعل.

لقد كان من تداعيات الثورة المعلوماتية ظهور تهديدات سيبرانية أصبحت تشكل تحديا كبيرا للأمن القومي والدولي، بحيث بات من الصعب حصرها في ظل تعدد أشكالها ومصادرها، وتطورها المتسارع والمستمر، وهو ما استدعى ضرورة التحرك لمواجهة هذه التهديدات التي باتت تكبد الدول خسائر كبيرة، فكانت الاستجابة من قبل الدول عن طريق تطوير استراتيجيات محكمة لمواجهتها بشكل كامل عبر استراتيجيات وطنية للأمن السيبراني، واتفاقيات دولية وإقليمة في إطار التعاون الدولي لمواجهة التهديدات السيبرانية.

Study Summary:

The information and digital revolution that the world witnessed, especially in the 21st century, had a great impact on the emergence of a new international situation, characterized by many transformations caused by the fast increase in the uses of cyberspace.

The most prominent features of these transformations were the changes that affected the most important classical concepts such as the concept of power, war and actors. One of the repercussions of the information revolution has been the emergence of cyber threats that have become a major challenge to national and international security, so it became difficult to restrict them in light of their multiplicity of forms and sources, and their fast and continuous development, which required a necessity to move and confront these threats that have become incurring great losses for countries.

The response from the different states was by developing tight strategies and confront them through national cybersecurity strategies also trough international and regional agreements within the framework of international cooperation.