المخاطر السيبرانية: التهديد الجديد لأستقرار الدولة

أ.م. د. منى جلال عواد
كلية العلوم السياسية/ جامعة بغداد

أ.م.عماد وكاع عجيل
كلية التربية الاساسية/ الشرقاط/ جامعة تكريت

المقدمة:

لقد أدت نهاية الصراع السياسي والتوتر العسكري، التي شكلتها مرحلة الحرب الباردة إلى بروز العديد من التحديات والتهديدات التي لم يشهدها المجتمع الدولي العابرة للحدود التي لا تعترف لا بالحدود أو السيادة الوطنية أو فكرة الدولة القومية، الأمر الذي أدى إلى حدوث تحولات في حقل الدراسات الأمنية والاستراتيجية وكذلك على مستوى استقرار الدولة، وإن التحول إلى عصر ثورة المعلومات، ودخول العصر الرقمي خاصة في القرن الحادي والعشرون وما نتج عنه من تداعيات عديدة بسبب ظهور تهديدات وجرائم سيبرانية أصبحت تشكّل تحدياً كبيراً للأمن القومي وكذلك الدولي، لدرجة أن العديد من الباحثين اعتبر الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر، والبحر، والجو، والفضاء، وهو ما استدعى ضرورة وجود ضمانات أمنية ضمن هذه البيئة الرقمية، تبلورت بشكل أساسي في ظهور الأمن السيبراني cyber security كبُعد جديد ضمن حقل الدراسات الأمنية، وقد اكتسب اهتمامات العديد من الباحثين في هذا المجال.

لذلك تتخذ الدول تدابير دائمة ومتطورة من أجل ان تكون مستعدة لمواجهة مخاطر التهديدات السيبرانية على بنيتها التحتية ضمن فضاء معلوماتها الرقمية وما يرتبط بنشاطاتها على مواقع الشبكة العنكبوتية العالمية، والتي تستدعي تعزيز وتعضيد مقومات ترسانتها الالكترونية بالاعتماد على عناصر قوتها الوطنية وبالمشاركة مع القطاع الخاص لتفادي عواقب الإضرار بمصالحها الاستراتيجية ومرتكزات أمنها القومي.

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

من هذا المنطلق أصبح الباحثون في الدراسات الأمنية والدراسات الاستراتيجية يركزون بشكل متزايد حول أثر التكنولوجيا على امن واستقرار الدولة.

أهمية البحث:

تنبع أهمية الدراسة من أهمية الأمن وضرورته لإستمرار الدول وبقائها، كونه ركن أساسي ومهم من اركان بقاء الدول، لا سيما ونحن ونعيش في ظل الفضاء السيبراني، والذي يعد تحديداً كبيراً يواجه الدول وتهديداً لامنها واستقرارها، لذلك اصبح من الضروري مواجهة هذا التحدي الخطير، فالامن العالمي اصبح في خطر اكثر من اي وقت مضى، خاصة بعد اتساع احتمالية اختراقه تزامناً مع تشابك مصالح العالم في ظل التطور التكنولوجي والمعلوماتي مما يجعل موضوع الامن السيبراني من أهم المواضيع التي تتطلع الدول الى تحقيقها.

إشكالية البحث:

بعد التطور الكبير الذي حصل في عالمنا نتيجة ثورة المعلومات والاتصالات وما نتج عنها من تشابك المصالح في ظل العولمة، اصبح العالم امام تحدي كبير وصراع خطير لا يقل أهمية الصراعات العسكرية والاقتصادية، لا بل يمكن القول انها تفوق عليها احياناً، خاصة وانها تستخدم ادوات تختلف عن تلك الادوات المستخدمة في الحروب والنزاعات المسلحة، فتحدي الامن السيبراني اصبح اليوم من أخطر التحديات التي تشهدها الدول، بالمقابل فان اغلب الدول لاتعطي لهذا التحدي الاهتمام الكافي بما يمنع اختراق امنها القومي في ظل العالم الرقمي والفضاء السيبراني وتشابك المصالح، ومن هنا تبرز الحاجة إلى ضرورة فهم ماهية الأمن السيبراني كمتغير جديد في المجتمع ، اذ تسمح طبيعة الإنترنت المفتوحة عبر شبكات التواصل الاجتماعي لكل مواطن بان يعبر عن أفكاره والاطلاع على مختلف المعلومات والانفتاح عبر جميع الثقافات المختلفة، وهنا يكمن أهمية الأمن السيبراني في حماية وصيانة القيم الجوهرية في المجتمع كالانتماء، المعتقدات الدينية، والعادات والتقاليد.

فرضية البحث:

تندرج فرض

ية هذه الدراسة في اطار معرفة التهديدات و المخاطر السيبرانية من خلال وجود احتمال تهديد وهشاشة داخل الفضاء الالكتروني وبالتالي تعطل عمليات البنية التحتية الحيوية للمعلومات، والعمليات الحكومية، ...الخ. وبشكل يؤثرعلى امن واستقرار الدولة، اذ ان الامن السيبراني اصبح ركن اساسي ومهم من اركان امنها الدول واستقرارها، وان تحدي الامن السيبراني اصبح من التحديات الخطيرة والكبيرة للدول، وان تأثيره يمكن ان يشكل خطر على حياة المواطنين بشكل مباشر وليس فقط على امن الدول، لذلك افضى هذا التحدي الى ايلاء موضوع الامن السيبراني أهمية كبيرة في الدول المتقدمة لما يمثله من خطر على امنها القومي، ومن اجل اثبات الفرضية فقد تبنت الدراسة عدد من التساؤلات والتي نحاول الاجابة عنها في هذه الدراسة ومن هذه الاسئلة:

- ماهو مفهوم الامن السيبراني.
- ماهي خصائص الامن السيبراني وابعاده.
- ماهي انواع الهجمات السيبرانية التي تأثر على أمن الدول.

- كيف تأثر الهجمات السيبرانية على استقرار الدول وكيف يمكن التصدي لها.

منهجية البحث:

من أجل الاجابة على التساؤلات التي تتبناها الدراسة تم الاعتماد على عدة مناهج علمية، فقد تم الاعتماد على المنهج التحليل النظمي بشكل اساسي، للوقوف على أهمية الامن السيبراني في حياة الدول، أضافة الى المنهج التأريخي والمنهج الوصفي.

هيكلية البحث:

بناءً على أهمية وإشكالية وفرضية البحث ومن اجل الالمام بالموضوع بشكل متكامل فقد تم تقسيم البحث مبحثين رئيسيين فضلاً عن مقدمة وخاتمة:

المبحث الاول: الامن السيبراني : المفهوم _ الخصائص _الابعاد

المطلب الاول: مفهوم الامن السيبراني

المطلب الثاني:خصائص وابعادالامن السيبراني

المبحث الثاني :المخاطر السيبرانية :دراسة في الانواع _التاثير _سبل المواجهة

المطلب الاول : أنواع للهجمات السيبرانية

المطلب الثاني: تاثير المخاطر السيبرانية على استقرار الدولة وسبل المواجهة.

المبحث الاول: الامن السيبراني : المفهوم _ الخصائص _الابعاد

تُعد مهمة ضبط المفاهيم والمصطلحات تحدياً يواجه مختلف الباحثين والدارسين في مختلف التخصصات، وذلك لما يطرحه من إشكاليات تجعل من الصعوبة بمكان الاتفاق على تعريفات واضحة وشاملة وموحّدة بين أعضاء المجتمع العلمي، ويعد الأمن السيبراني واحداً من المفاهيم المعقدة التي قدمت لها العديد من التعريف المختلفة.

وعلى الرغم من الإيجابيات الهائلة التي تحققت بفضل تقنية المعلومات، فإن تلك الثورة المعلوماتية المتصاعدة قد صاحبتها في المقابل جملة من الانعكاسات السلبية الخطيرة نتيجة سوء الاستخدام، ومن بين تلك الانعكاسات المستحدثة، ظاهرة الجريمة الرقمية والتهديدات السيبرانية والامن السيبراني، والتي تصاعدت أخطارها بدورها مما افرز نوعاً جديداً من الجرائم العابرة للقارات، التي لم تعد أخطارها وأثارها محصورة في نطاق دولة بعينها مما أثار بعض التحديات القانونية أمام الأجهزة المعنية.

ظهر مفهوم الامن السيبراني بعد الحرب الباردة استجابة للمزيد من الابتكارات التكنولوجية- والظروف الجيوسياسية المتغيرة ، تم استخدامه لأول مرة من قبل علماء الكمبيوتر في اوائل التسعينات للتأكيد عل سلسلة من حالات عدم الامان المرتبرة بأجهزة الكمبيوتر لكنه تجاوز مفهومه التقني لأمن الكمبيوتر عندما حث المؤيدين على ان التهديدات الناشئة عن التقنيات الرقمية يمكن ان يكون لها اثار اجتماعية مدمرة، لذا تعد قضية العالم الافتراضي والامن السيبراني من اهم القضايا التي باتت تشغل العالم اليوم، فقد اضحى العالم الافتراضي موازي

للعالم الحقيقي، وقد انتقلت كثير من الحروب والصراعات بين الدول من ميادين القتال الكلاسيكية الى العالم الرقمي والافتراضي.

المطلب الاول: الامن السيبراني: الأمن السيبراني مكوّن من لفظتين: (الأمن)، و(السيبراني)، وسنبحث معنى اللفظتين بشيء من التفصيل.

اولاً:الأمن: يمكن تعريف الأمن لغةً بأنه نقيض الخوف، أي بمعنى السلامة. والأمن مصدر الفعل أَمِنَ أَمْناً وأَمَاناً وأَمَنَةً: أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أَمِنَ من الشر، أي سَلِمَ منه. وقد عرّفه قاموس بنغوين للعلاقات الدولية بأنه مصطلح يشير إلى غياب ما يُهدد القيم النادرة، فالامن تعني الأمان وهي ضد الخوف، وتعني ايضاً تحقيق الطمأنينة والعهد والحماية والصدق والذمة وكلها ضد الخوف، اما اصطلاحاً فهي تعني القدرة على مواجهة الأخطار والتحديات وتأمين الحاجات الاساسية للانسان[١].

ويعرف الأمن كذلك بأنه قدرة الدول على الحفاظ على كيانها المستقل وتماسكها الاجتماعي ضد قوى التغيير التي تعدها معادية، وأساس الأمن هو البقاء لكنه في نفس الوقت يحتوي على العديد من الاهتمامات الجوهرية حول شروط الوجود والبقاء، ففي ظل الفوضوضية والتغيير يمكن القول بأن الأمن يمكن ان يكون نسبياً ولا يمكن ان يكون مطلقاً، فالامن يعني قدرة الأمة على حماية قيمها الذاتية من الأخطار الخارجية بغض النظر عن الشكل الذي يمكن ان تتخذه التهديدات الخارجية، بالمقابل فأن الأمن لا يعني فقط رغبة الدولة والامة في البقاء بل رغبتها أيضاً في العيش بدون خطر او تهديد خارجي، اذ عرف هنري كيسنجر الأمن بأنه: أي تصرف يسعى المجتمع عن طريقها الى تحقيق البقاء[٢].

ثانياً: السيبراني: مصطلح السيبرانية الآن هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي، وتشير المقاربة الإيتيمولوجية لكلمة (cyber) إلى أنها لفظة يونانية الأصل مشتقة من كلمة (kybernetes) بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للمتحكم (governor)، وتجدر الإشارة إلى أن العديد من المؤرخين يرجعون أصلها إلى عالم الرياضيات الأمريكي norbert wieners 1894-1964 وذلك للتعبير عن التحكم الآلي[٣].

---

(١) ابن منظور، معجم لسان العرب، ج٢، دار احياء التراث العربية، بيروت، ١٩٩٩، ص٢٢٣.

(٢) رفعت سيد احمد، الأمن القومي العربي بعد حرب لبنان، مجلة الشؤون العربية، العدد ٣٥، ١٩٨٤ ص٨.

(٣) فارس قرة، الامن السيبراني، الموسوعة السياسية، ٢٠١٥ على الموقع التالي:
https://political-encyclopedia.org

اصطلاحاً يعرف السيبراني بأنه: عبارة عن مجموعة من التقنيات والانظمة الحديثة والتي تهدف الى حماية الشبكات والانظمة الالكترونية والاداوات التكنولوجية الحديثة للمؤسسات ومختلف القطاعات للحد من الهجمات الالكترونية بغير وجه حق(٤).

بعد ان عرفنا مصطلح (الامن) و (السيبرانية) يمكننا الان تعريف الامن السيبراني، اذ يُعرّف بأنه: مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة، وهذا ما ذهب إليه الكاتبان (نيتانميكي بيكا وليتو مارتي) في كتابهما الموسوم Cyber Security: Analytics, Technology and Automation، حيث اعتبر أن الأمن السيبراني: عبارة عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة، بينما عرّفه إدوارد أمورسو Amoroso Edward بأنه: وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة(٥).

بينما عرّفه إدوارد أمورسو (Amoroso Edward) بأنه: وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة.(٦)

فريتشارد كمرر (Richard A.Kemmerer) يعرف الأمن السيبراني بأنه": عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة.(٧)

فالباحث حسن طاهر عرف الأمن السيبراني بأنه: العمليات التي تؤمن حماية كافة الموارد والآليات المستخدمة والمتبعة في معالجة المعلومات أمنياً، اذ يتم تأمين كافة الموارد البشرية وغير البشرية المختصة بجهة معينة وبوسائل وجراءات وعمليات أمنية وتقنية توفر لها سلامة محتواها المعلوماتي من مخاطر، فالمعلومات هي الكنز الثمين الذي يتوجب على اية دولة في العالم حمايته من أية مخاطر داخلية أو خارجية(٨)، كما عرفه الباحث السياسي باري بوزان بأنه: العمل على التحرر من التهديد، وفي سياق النظام الدولي فهو قدرة الدول والمجتمعات على

---

(٤) انواع التهديدات السيبرانية ومجالاتها، مجلة رواد الاعمال، مؤسسة سواحل الجزية للاعلام، المملكة العربية السعودية، ٢٠٢٠، على الموقع التالي: https://www.rowadalaamal.com

(٥) فارس قرة، مصدر سبق ذكره.

(٦) المصدر نفسه.

(٧) اسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، العدد (١) المجلد (١٠)، جامعة محمد بوضياف، الجزائر، ٢٠١٩، ص ١٠٢١.

(٨) حسن طاهر، الحاسب وأمن المعلومات، مكتبة الملك فهد الوطنية، المملكة العربية السعودية، ٢٠٠٠، ص٢٣.

الحفاظ على كيانها المستقل وتماسكها الوظيفي ضد قوى التغيير التي تعدها معادية في سعيها للأمن، فأساس الامن هو البقاء لكنه يحوي على جملة من الاهتمامات الجوهرية حول شروط الوجود، ولا يعني العمل على التتحرر من التهديدات تحييده كلياً لان الامن يكون نسبياً ولا يمكن ان يكون مطلقاً.[٩]

ويعرف ايضاً بأنه: هي العملية التي يتم بموجبها حماية انظمة الاتصالات والمعلومات الواردة اليها والدفاع عنها ضد الضرر او الاستخدام غير المصرح به او التعديل او الاستغلال، ويعرف ايضاً بأنه: أمن الشبكات والانظمة المعلوماتية والبيانات والمعلومات والاجهزة المتصلة بالانترنيت ، وعليه فهو المجال الذي يتعلق بإجراءات مقاييس ومعايير الحماية المفروض إتخاذها والالتزام بها لمواجهة التهديدات ومنع التعديات أو للحد من أثارها في أسوأ الاحوال[١٠].

كذلك يعرف الامن السيبراني انطلاقاً من أهداف بأنه: النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات ويضمن امكانات الحد من الخسائر والاضرار التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح اعادة الوضع الى ما كان عليه بأسرع وقت ممكن، بحيث لا تتوقف عجلة الانتاج، ولا تتحول الاضرار الى خسائر دائمة[١١].

هناك العديد من المفاهيم المرتبطة بالأمن السيبراني، ومن أهمها ما يلي:

اولاً:الفضاء السيبراني: يعد الفضاء السيبراني السمة التي تتميز بها الحياة العصرية والمكون الاساسي للبنة التحتية لمؤسسات الدولة المختلفة، اذ أصبح منبراً للتعبير عن حرية الرأي والتجمع والخصوصية الفردية والتدفق الحر للمعلومات والاتصالات الالكترونية، وعرف جوزيف ناي الفضاء السيبراني بأنه: نطاق تشغيلي محكم باستخدام الالكترونيات لإستكشاف المعلومات عبر انظمة مترابطة ببعضها البعض وبنية تحتية لها، كذلك عرفته جامعة الدفاع الوطني الامريكية بأنه: مجال تشغيلي تجري فيه مجموعة من العمليات ذات الطابع الالكتروني الفريد والمحكم بمجموعة من الاستخدامات التي تعتمد على الالكترونيات والأطياف الكهرومغناطيسية لإنشاء

---

(٩) تباني وهيبة، الامن المتوسطي في استراتيجيات الحلف الاطلسي: دراسة حالة ظاهرة الارهاب، كلية الحقوق والعلاقات الدولية، جامعة مولود معمري، الجزائر، ٢٠١٤، ص٢٠.

(١٠) نسرين الشحات الصباحي علي، الأبعاد العسكرية للقوة السيبرانية على الأمن القومي للدول دراسة حالة (اسرائيل) منذ عام ٢٠١١، المركز الديمقراطي العربي للدراسات الاستراتيجية والاقتصادية والسياسية، ٢٠١٦، على الموقع التالي: https://democraticac.de

(١١) منى الاشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، اللقاء السنوي الاول للمختصين في أمن وسلامة الفضاء السيبراني، بيروت، ٢٧-٢٨ اب ٢٠١٢، ص٣.

وتخزين وإبدال وتبادل المعلومات من خلال مجموعة من نظم المعلومات المترابطة مع بعضها البعض والمتصلة عبر شبكة الانترنيت[١٢].

نلاحظ ان التعريفات السابقة ركزت على الجاني التقني وأهملت الجانب البشري الذي يعد جزءاً أساسياً في الفضاء السيبراني، لذا جاء تعريف الاتحاد الدولي للاتصالات اشمل، لذا عرف الفضاء السيبراني بانه: المجال المادي وغير المادي الذي يتكون وينتج عن عناصر عدة وهي: اجهزة الكومبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل، التحكم، ومستخدموا كل هذه العناصر، وبالتالي يعد الفضاء السيبراني عبارة عن فيض رقمي من المعلومات لا يعتمد بشكل كامل على البيئة المحوسبة التي توفرها شبكات المعلومات، بل تتعامل أيضاً مع مفرداته مثل سرعة تناقل البيانات وصلاحية الدخول الى الشبكة بالاضافة الى المعالجات التي تناول البيانات المتدفقة ضمن البيئة السيبرانية[١٣].

ثانياً: الهجوم السيبراني: عرف فيورتس الاستاذ في قسم الكيمياء في جامعة تكساس للتكنولوجيا الهجوم السيبراني بأنه: هجوم عبر الانترنيت يقوم على التسلل الى مواقع اللكترونية غير مرخص بالدخول اليها، بهدف تعطيل البيانات المتوفرة أو اتلافها او الاستحواذ عليها، فهي عبارة عن سلسلة هجمات اللكترونية تقوم بها دولة ضد دولة اخرى، في حين عرف شميث المتخصص بالقانون الدولي الانساني والعضو البارز في مركز الدفاع السيبراني التعاوني التابع لحلف الشمال الاطلسي بأنه: اي تصرف اللكتروني دفاعياً كان أم هجومياً يتوقع منه وعلى نحو معقول في التسبب بجروح أو قتل شخص او الحاق أضرار مادية او دمار بالهدف المهاجم، إضافة الى ذلك فقد عرفت القيادة العسكرية الامريكية الهجمات السيبرانية بأنها: تطويع عمليات نظام الكومبيوتر بهدف منع الخصوم من الاستخدام الفعال لها، فضلاً عن التسلل الى أنظمة المعلومات وشبكات الإتصال بهدف جمع البيانات التي تحتويها وحيازتها وتحليلها[١٤].

ثالثاً: الجريمة السيبرانية: مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية أو شبكة الإنترنت أو تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها، فهي الجريمة المتصلة باستخدام الكمبيوتر، أي تصرف غير قانوني، يرتكب باستخدام تقنيات المعلومات والاتصالات[١٥].

---

(١٢) إيهاب خلفة، القوة الالكترونية: كيف يمكن ان تدير الدولة شؤونها في عصر الانترنيت، دار العربي للنشر والتوزيع، بيروت، ٢٠١٧، ص٢٧.

(١٣) عادل عبد الصادق، اسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني، مكتبة الاسكندرية، وحدة الدراسات المستقبلية، الاسكندرية، ٢٠١٦، ص١١

(١٤) احمد عبيس نعمة، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، العدد (٤٤)، كلية القانون، جامعة الكوفة، ٢٠٢٠، ص ٥١

(١٥) فارس قرة، مصدر سبق ذكره.

المطلب الثاني: خصائص وابعاد الأمن السيبراني

اولاً: خصائص الأمن السيبراني:

يعتمد الأمن السيبراني كمجال افتراضي على نظم الكمبيوتر وشبكات الانترنت ومخزون هائل من البيانات والمعلومات، بحيث يتم الاتصال بالشبكات غير الحواسيب أو الهواتف أو غيرها من دون تقيد بالحدود الجغرافية، ويوصف العصر الحالي بأنه العصر الرقمي، فهو يتضمن تطورات تكنولوجية هائلة تخدم جميع مناحي الحياة العامة والخاصة، وتنعكس على خدمة المجتمع الدولي بأكمله، حيث بات العصر يتحرك من خلال تكنولوجيا المعلومات والاتصالات التي واكبتها حركة إجرامية كبيرة، فانتشرت الجرائم المعلوماتية بشكل خطير في جميع دول العالم التي أصبحت عرضة للوقوع تحت تهديد هذه الجرائم باستخدام الفيروسات وبرامج التجسس وغيرها وهي أدوات يمكن وصفها مجازاً بالجراثيم المستحدثة أو المختلفة[١٦].

إضافة الى ذلك القدرة على التشبيك وبناء روابط افتراضية، اذ تتيح الادوات السيبرانية للأفراد والجماعات قدرة أكبر على التواصل والتشبيك وبناء مجتمعات أفتراضية بأشكال مختلفة للتأثير في القضايا عبر وسائل التواصل الاجتماعي والمنتديات الالكترونية وغيرها، خاصة تلك المنتديات والمواقع التي تنشر وتدعوا الى التطرف والارهاب، وهذا الامر لا يتوفر في المجال التقليدي، خاصة مع القيود التي تفرضها الانظمة السلطوية في الواقع، اما في المجال الافتراضي فيتسم بضعف السيطرة الحكومية، فطبيعة المجال السيبراني والذي تحفل بملائيين النقاشات اليومية تصعب من سيطرة الحكومات عليه، لذلك يستطيع الأفراد والجماعات التعبير عن مواقفهم وأرائهم في وقت وفي أي مكان، فالفضاء الالكتروني لا حدود له، اذ يشارك كل الفاعلين بما فيهم الدول من الاستخدام الشخصي الى البرامج الإقتصادية الى التطبيقات العسكرية، كلها تعتمد على تعتمد على الفضاء السيبراني، على العكس من التهديدات التقليدية الملموسة والتي يمكن التنبؤ بها، فان تهديدات الامن السيبراني يمكن ان تأخذ شكل أو مصدر افتراضي وتفرض أخطاراً لا يمكن التنبؤ بها[١٧].

اذن يمكن القول ان الامن السيبراني، أحدث بدوره تغييراً في مفاهيم العلاقات الدولية، كمفهوم القوة والصراع والحرب، اذ انتشرت القوة بين الفاعلين، وتحول الصراع من المادي الى الافتراضي، واصبحت الحروب تخاض بالأصفار والآحاد، وبدأ واضحاً أن الدول تتجه نحو عسكرة الفضاء السيبراني، مما نتج عنه ظهور تهديدات جديدة تتزايد في الحجم والشدة، وتشكل تهديدا خطيرا للأمن القومي، فكلما زاد التشابك، زادت التهديدات السيبرانية، وأثر ذلك على الأمن القومي، مما زاد من أهمية الامن السيبراني، بأبعاده المختلفة، والذي تحاول الدول من

---

(١٦) نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني (التهديد المتصاعد لأمن الدول) مجلة بابل للدراسات الانساني، العدد (٢) المجلد (٨) مركز بابل للدراسات الحضارية والتاريخية، ٢٠١٨، ص ١٩٠

(١٧) ابتسام علي حسين، فرص وقيود الاطراف المتنازعة في المجال العام السيبراني، ملحق مجلة السياسة الدولية، العدد (٢٠٨) مركز الاهرامات للدراساتت، القاهرة، ٢٠١٧، ص١٢.

خلاله الحد من المخاطر والتهديدات في الفضاء السيبراني، فالأمن السيبراني أصبح على رأس أوليات قضايا الأمن القومي، حيث قامت معظم الدول بإعادة صياغة عقيدتها الأمنية لتتلاءم مع المتغير الجديد، وهذا في محاولة لمواجهة التهديدات السيبرانية التي تزداد وتتطور بسرعة، فالجريمة والارهاب والحرب في الفضاء السيبراني تعد من بين التحديات الأمنية الجديدة أمام الدول[١٨].

فالأمن السيبراني يتميز بأنه ذو طابع متعدد التخصصات الاجتماعية والتقنية، فهو شبكة خالية من الحجم وقدرات الفاعلين يمكن أن تكون مماثلة على نطاق واسع، ويمتاز درجة عالية من التغيير والترابط وسرعة التفاعل.

ثانياً: ابعاد الأمن السيبراني

يطال الأمن السيبراني جميع المجالات الاقتصادية والسياسية والاجتماعية والانسانية وغيرها من المجالات، انطلاقاً من الأمن السيبراني ودوره في حماية جميع مجالات الحياة، لذا لابد من التوقف عند ابعاد الأمن السيبراني وعلى النحو الأتي:

اولاً: البعد العسكري: تتراكم الامثلة التي يمكن ان نوردها في هذا المجال، والتي توضح الأبعاد العسكرية للأمن السيبراني وخطورة الهجمات السيبرانية، فعلى سبيل المثال ما حصل في جورجيا واستونيا وكوريا الجنوبية وايران، من هجمات واختراقات ادت فيما بعد الى اندلاع صراع مسلح كما حصل بين جورجيا وروسيا، او بانقطاع الاتصال بالانترنيت في استونيا، بين الدولة والمواطنين والتشويش على الادارات الحكومية، كذلك اختراقات أنظمة المنشأت النووية الايرانية، وتحقيق امكانات التلاعب بها، فهذا يعني تهديد للأمن القومي للدولة المعنية، أضافة الى الاختراق الذي حصل في البرلزيل والمملكة المتحدة للبنية التحتية للطاقة، اذ انقطع التيار الكهربائي، مما طالت أثاره السلبية ملائين الاشخاص والمؤسسات والمصالح، وفي هذا السياق حذر خبراء أميركيون الرئيس الامريكي جورج بوش في ايلول عام ٢٠٠٧ من خطر الهجمات السيبرانية على البنة التحتية الأمريكية، والتي تضم الى جانب الدفاع، امدادات الطاقة الكهربائية والمياه والاتصالات السلكية واللاسلكية والخدمات الصحية والنقل والانترنيت[١٩].

ثانياً: البعد الاقتصادي: أصبح الانترنيت أساساً للمعاملات التجارية والاقتصادية، كما تستعمل الحواسيب في تسيير وتطوير الصناعات وتحريك عجلة الاقتصاد، فاصبح الكل مترابط عبر شبكات الكومبيوتر والانترنيت، فأصبح الأمن السيبراني مرتبط ارتباطاً وثيقاً بالاقتصاد، فالتلازم اصبح واضحاً جداً بين اقتصاد المعرفة وتوسيع استخدام تقنيات المعلومات والاتصالات، إضافة الى القيمة التي تمثلها البيانات والمعلومات المتداولة والمخزونة والمستخدمة، كذلك تتيح تقنيات

([١٨]) اسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مصدر سبق ذكره، ص١٠٢٩.

([١٩]) منى الاشقر جبور، السيبرانية: هاجس العصر، المركز العربي للبحوث القانونية والسياسية، جامعة الدول العربية، ٢٠١٢، ص ٢٨.

الاتصالات الى تعزيز التنمية الاقتصادية لبلدان عديدة عن طريق افادتها من فرص الاستخدام التي تقدمها الشركات الدولية والشركات الكبرى، إضافة الى ذلك دخول العالم الى عصر المال الإلكتروني، ضمن بيئة تقنية متحركة، بعد إطلاق خدمات المحفظة الالكترونية، اذ تتزايد استثمارات المصارف والمؤسسات المالية في مجال المال الرقمي، اذ تتنافس الشركات على غصدار تطبيقات تسمح بآليات دفع آمنة، وبحفظ المال في المحفظة الإلكترونية وبالايفاء من خلالها، وباستخدامها كرصيد افتراضي، لذلك وضعت بعض الدول تشريعات خاصة بهذا المال، مما يمكن ان يثير هذا الامر من صعوبات وما يتطلبه من تشريعات للحد من بعض الجرائم الاقتصادية والمالية الخطرة والعابرة للحدود، كتبييض الاموال والتهرب من الضريبة، فالأمن السيبراني يضمن ركود الجمهور الى الخدمات التي تقدم بواسطة تقنيات المعلومات والاتصالات، كما يضمن الاقبال عليها بشكل واسع[٢٠].

ومن الامثلة التي يمكن ان نوردها في هذا المجال[٢١]:

١- في سنة ٢٠١٢ قام فريق من القراصنة السيبرانيين الايرانيين أطلق على نفسه أسم (سيف العدالة القاطع) بإقحام فايروس خبيث أطلق عليه أسم (شمعون 01) في شبكة المعلومات الداخلية لشركة أرامكو السعودية النفطية، فقام بإلغاء بيانات مهمة في أكثر من ٣٠,٠٠٠ حاسب من حواسيب الشركة.

٢- في سنة ٢٠١٤ نفذت أخطر الهجمات الالكترونية في منطقة الشرق الاوسط والخليج العربي والتي سميت بعملية (كليفر) على قطاع النفط والغاز، بإلاضافة الى المطارات ومواقع حكومية حساسة وشركات الاتصالات، وتعد من أشد الهجمات السيبرانية تأثيراً على المنطقة.

٣- في سنة ٢٠١٧ هاجم فيروس (الصخرة الدوار) المملكة العربية السعودية، اذ استهدف قطاع الطيران والبتروكيماويات، وقد أحدث هذا البرنامج الخبيث تأثيرات كبيرة على شركات الطيران وشركات االبتروكيماويات في المملكة العربية السعودية.

٤- في سنة ٢٠١٩ تم تنفيذ تهديدات سيبرانية متقدمة مستمرة APT، وهي هجمات سيبرانية بالغة التأثير، مارسها قراصنة إيرانيون سيبرانيون، لاستهداف شبكات المعلومات وبنيتها التحتية في كل من قطر والكويت والسعودية والامارات والبحرين، من خلال مدة زمنية متطاولة لضمان بلوغ أهدافها وتعميق مستويات تأثيرها.

ثالثاً: الابعاد السياسية: تتمثل الابعاد السياسية للامن السيبراني بشكل أساسي في حق الدولة في حماية نظامها السياسي وكيانها ومصالحها الاقتصادية والتي تعني حقها في السعي الى تحقيق

---

(٢٠) المصدر نفسه، ص٢٩.

(٢١) حسن مظفر الرزو، النزاعات والمواجهات السيبرانية في فضاء منطقة الخليج العربي، مركز الجزيرة للدراسات، ٢٠١٩، متاح على الرابط التالي:
https://studies.aljazeera.net › reports › 2019/

رفاه شعبها، في وقت اصبح للتقنيات الالكترونية تأثير وأضح في موازين القوى داخل المجتمع نفسه، اذ اصبح بإمكان المواطن ان يتحول الى لاعب أساسي في اللعبة السياسية، كما أصبح بالامكان الاطلاع على خلفيات ومبررات القرارات السياسية التي اتخذتها حكومته من خلال الكم الهائل من المعلومات التي يمكنه الوصول اليها، أو التي يمكن ان توزع وتنشر عبر الانترنيت، اما على الصعيد الدولي يعد التدخل الروسي السيبراني في الانتخابات الأمريكية أبرز دليل على ضرورة وأهمية الأمن السيبراني في بعده السياسي، إضافة إلى التسريبات للوثائق الحساسة والاختراقات التي غالباً ما تؤدي إلى أزمات دبلوماسية بين الدول، كما ان الفضاء السيبراني اصبح بيئة خصبة للحملات الانتخابية لمختلف الفاعلين الدوليين[٢٢].

رابعاً: الأبعاد القانونية: ان التطورات التكنولوجية المتسارعة، تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية في الفضاء السيبراني، فالملاحظ أن الجريمة السيبرانية تفتقد في معظم البلدان إلى الأطر القانونية الصارمة للتعامل معها، إضافة إلى ضرورة تفعيل التعاون الدولي المشترك لمكافحتها، ولعل من أبرز الممارسات القانونية في مجال الأمن السيبراني هو ضمان بعض الحقوق في هذا المجال كحق النفاذ إلى الشبكة العالمية للمعلومات، وأيضاً توسعت بعض المفاهيم لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات الإلكترونية، والحق في إنشاء التجمعات على الإنترنت، وأيضاً الحق في حماية ملكية البرامج المعلوماتية[٢٣].

خامساً: الأبعاد الاجتماعية: يفوق مستخدمي الانترنيت ٤ مليارات شخص في العالم، منهم أكثر من ٢,٦مليار يستخدمون مواقع التواصل الاجتماعي، مما يجعلها أكبر تجمع للتفاعل البشري، ويفتح الباب واسعا لتبادل الأفكار الخبرات الجيدة، لكن في المقابل يعرض أخلاقيات المجتمع للخطر، نظرا لصعوبة مراقبة محتوى الانترنيت، كما يعرض الهويات لعمليات اختراق خارجي قد تتسبب في تهديد السلم الاجتماعي للدولة، وعليه فلابد من العمل على توعية المواطن بهذه المخاطر لتحقيق الأمن السيبري في بعده الاجتماعي[٢٤].

المبحث الثاني: المخاطر السيبرانية: دراسة في الانواع _التاثير _سبل المواجهة

اختصر الفضاء السيبراني حاجز الزمان والمكان، وخلق مساحات للتفاعلات الداخلية والدولية في الواقع الافتراضي، ومن ثم برزت فضاءات جديدة للصراع بأدوات مختلفة، وأنماط جديدة تختلف عن الصراعات التقليدية، بعد أحداث ١١ ايلول ٢٠٠١ التي تعد مفصلية في تاريخ العلاقات الدولية، لبداية استعمال الجماعات الارهابية للانترنت بشكل بارز في الترويج للفكر

---

(٢٢) إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، العدد (١) المجلد (١٠) جامعة محمد بوضياف، الجزائر، ٢٠١٩، ص ١٠٢٣.

(٢٣) فارس قرة، مصدر سبق ذكره.

(٢٤) عادل عبد الصادق، القوة الالكترونية :اسلحة الانتشار الشامل في عصر الفضاء الالكتروني، مجلة السياسة الدولية، العدد 188 ، مؤسسة الأهرام، مصر، ٢٠١٢ ، ص٣٢.

المتطرف كان الفضاء السيبراني ساحة للصراع والقتال وتصفية الحسابات بين الدول والجماعات المتطرفة، وبالتالي أصبح الفضاء السيبراني ساحة جديدة للصراع بشكله التقليدي ولكنه ذو طابع سيبراني يعكس النزاعات التي تخوضها الدول أو الفاعلين من غير الدول على خلفيات دينية أو عرقية وإيديولوجية أو اقتصادية أو سياسية، ويتمدد الصراع السيبراني بداخل شبكات الاتصال والمعلومات متجاوزاً الحدود التقليدية وسيادة الدول، وكشف استخدام الفضاء السيبراني عن حالة التعارض الحقيقي للاحتياجات والقيم والمصالح بين العديد من الفاعلين، وساعد ذلك على ظهور أساليب جديدة للصراع الدولي، تباينت بين الطابع التقني والتجاري والاقتصادي والعسكري، إلى جانب ظهور طرق بديلة عن الحرب المباشرة بين الدول عبر شبكات الاتصال والمعلومات، فهناك صراع سيبراني تحركه دوافع سياسية، ويأخذ شكلا عسكريا، ويتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء السيبراني، ويوجد صراع سيبراني ذو طبيعة ناعمة، حول الحصول على المعلومات والتأثير في المشاعر والأفكار وشن حرب نفسية وإعلامية ،كما يأخذ الصراع السيبراني طابعا تنافسيا حول الاستحواذ على سبق التقدم التكنولوجي وسرقة الأسرار الاقتصادية والعلمية، والتحكم بالمعلومات، والعمل على اختراق الأمن القومي للدول، كهجمات قراصنة الكمبيوتر والتجسس بما يكون له من تأثير على تدمير الاقتصاد والبنية التحتية بنفس القوة التي قد يسببها تفجير تقليدي مدمر، ويمكن أن يستخدم الفضاء السيبراني كوسيلة من وسائل الصراع داخل الدولة، بين مكوناتها، على أساس طائفي أو اقتصادي أو ديني[٢٥].

المطلب الاول : أنواع الهجمات السيبرانية

اصبح الفضاء السيبراني (Cyberspace) عنصرا مؤثرا في النظام الدولي المعاصر نظرا لما يحمله من ادوات تكنولوجيه متطورة ،اذ كشف عن محاور جديدة ، وبات اكثر تاثيرا في الحسابات الاستراتيجية للدول ،والدولة التي لاتمتلك التكنولوجيا السيبرانية المحصنة امنيا سيتعرض فضاؤها السيبراني المتضمن للاصول والموارد والمعلومات والخدمات والبنية التحتية الحيوية ،بما في ذلك الامنية والعسكرية والمصرفية والتجارية والتعليمية والصحية والاقتصادية الى الهجمات السيبرانية التي تسبب دمار هائل فيها[٢٦].

اي بعبارة اخرى المخاطر السيبرانية هي احتمال وجود تهديد وهشاشة داخل الفضاء الالكتروني للبلد يضر بامن وسلامة نظم المعلومات وهياكل البنى التحتية المعلوماتية الاساسية .وعلاوة على ذلك ، فاءن التهديدات يمكن ان تستغل الثغرات الموجودة وبشكل يؤثر على سلامة وامن نظام المعلومات او شبكات المعلومات او البنى التحتية للشبكات.[٢٧]

([٢٥]) إسماعيل زروقة، مصدر سبق ذكره، ص ١٠٢١.

([٢٦]) نور امير الموصلي :الهجمات السيبرانية في ضوء القانون الدولي الانساني ،رسالة ماجستير، الجامعة الافتراضية السورية، ٢٠٢١، ص ٧.

([٢٧]) استراتيجية الامن السيبراني العراقي : مستشارية الامن الوطني امانة سر اللجنة الفنية العليا لامن الاتصالات والمعلومات، ص ٤ ، ينظر الى شبكة المعلومات الدولية (الانترنت)

وللخطر السيبراني الوطني مكونان رئيسيان.[٢٨]

١- التهديدات السيبرانية.

٢- مدى كوننا معرضين للهجمات السيبرانية (الثغرات الموجودة)

واصبحت الهجمات السيبرانية معقدة وخطيرة ولها انواع متعددة وهي على نحو متزايد، وعندما وصلت اهدافها لمحاولة تدمير البنية التحتية لدول باكملها، اصبح تطويرها في مقدمة اهداف الدول، فهي تعد قدرة ثانية لاتقل اهمية عن القدرة العسكرية وحتى النووية، اذ ان القدرة السيبرانية يمكنها اختراق المنشات والقاذفات النووية والقواعد العسكرية وتعطيلها او التحكم بها.[٢٩]

وتتنوع الجهات التي تقف وراء ظاهرة تنامي الهجمات السيبرانية على الصعيد العالمي في الآونة الأخيرة، وتشمل ما يلي:[٣٠]

١- الدول التي تمتلك قدرات تقنية وتكنولوجية متطورة تتيح لها توظيفها في القيام بهجمات سيبرانية في مواجهة خصومها سواء لأغراض عسكرية (تدمير منشآت – وقف مشروعات) أو تجسسية كالحصول على معلومات أو إحداث تدمير في البنية التحتية الأساسية، كشبكات الكهرباء والمياه والمواصلات والاتصالات.

٢- عصابات الجريمة المنظمة، والتي غالباً ما تلجأ إلى الهجمات السيبرانية للحصول على فدية مالية، وتلجأ في ذلك إلى اختراق أنظمة المعلومات التي تدير الخدمات الأساسية في بعض الدول، لمساومتها للحصول على مبالغ مالية.

٣- القراصنة من الأشخاص العاديين والذين يمتلكون مهارات تقنية فائقة، يتم توظيفها في الحصول على مبالغ مالية أو في اختراق الأمن المعلوماتي للدول، والحصول على معلومات حساسة عن قضايا السياسة الخارجية للدول، على النحو الذي جسدته (ظاهرة ويكليكس)، حينما حيث استطاع الصحفي الاسترالي جوليان أسانج (Julian Paul Assange)أن يكشف العديد من أسرار السياسة الخارجية الأمريكية وعلاقات الولايات المتحدة مع العديد من القوى الكبرى.

وهناك عدة أنواع من الهجمات السيبرانية لعل ابرزها ما يلي:

---

https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy

(٢٨) المصدر نفسه.

(٢٩) نور امير الموصلي :الهجمات السيبرانية في ضوء القانون الدولي الانساني ، مصدر سبق ذكره، ص ١٦.

(٣٠) د.داليا السيد: الهجمات السيبرانية .. تهديد متعاظم للأمن والاستقرار والاقتصاد العالمي، ينظر الى شبكة المعلومات الدولية :http://www.nationshield.ae

اولا: الهجمات السرية: وتعد أحد أنواع التجسس التقليدي باستخدام وسائل التكنولوجيا الفائقة؛ ولعل معظم الهجمات السيبرانية المتطورة التي أطلقت من قبل الدول القومية أوالجماعات الإجرامية تقع ضمن هذه الفئة. ولكن، لا يمكن تصور الرد بهجوم ساحق أو مدمر على التجسس السيبراني، مهما بلغت تداعياته على الأمن القومي. ودون التهديد برد واسع النطاق، ستهوى الركيزة الأساسية للردع، وسيفشل في منع الهجمات السيبرانية.[٣١]

ثانيا : الهجمات الالكترونية الفعالة (Active).[٣٢] يركز المخترقون الى ايجاد الثغرات الامنية ((Security Vulnerabilities))، او الابواب الخلفية (Back doors) , لهذه الانظمة فعندها يمكن ان تنصب او تزرع البرامج الخبيثة, ويتم التحكم عن بعد عن طريق ارسال الاوامر, لغرض سرقة البيانات او تعطيل الحاسبات. ومن هذه الهجمات:

١. هجمات الحرمان من الخدمة (Denial of Service Attacks)

٢.فايروسات الحاسوب (Computer Virus) : وهي برامج صنعت بطريقة متعمدة لتغيير خصائص الملفات, والحاق الضرر بالحاسوب, واعطاء اوامر اما بالتخريب او الازالة, وهذه الفيروسات تؤدي الى تعطيل شبكات الخدمات والبنية التحتية للطرف المستهدف او احداث فشل في الاتصالات لدولة ما

٣. دودة الحاسوب (computer worm)، هي برامج خبيثة تتكاثر بنسخ نفسها, وتنتقل من نظام الى اخر باستغلال الثغرات الامنية) (, صنعت للأعمال التخريبية كأن تعمل على قطع الاتصال بالشبكة او سرقة البيانات، اثناء تصفح المستخدمين بالأنترنت, وتمتاز بسرعة الانتشار والقدرة الفائقة على التلون والتكاثر ويصعب التخلص منها, وتستهدف عادة الشبكات المالية, وشبكات البنوك

٤. احصنة طروادة (Trojan Horse): وهو شفرة او برنامج صغير مختبئ في برنامج كبير من البرامج ذات الشعبية المالية وهو مبرمج بمهارة عالية, حيث يقوم بالمهام الخفية مثل نشر دودة او فايروس, ومن الصعوبة اكتشافه, حيث يعمل دائماً على مسح آثارهُ التي لا تحمل صنعة تخريبية, ويقوم بأضعاف قوة الدفاع للمستهدف وسهولة اختراق جهازهُ وسرقة بياناته)

---

(٣١) د. رغدة البهي: الردع السيبراني: المفهوم والإشكاليات والمتطلبات،من مجلة العلوم السياسية والقانون، العدد الأول لسنة "٢٠١٧،المركز الديمقراطي العربي، برلين ، ص ٥٣.

(٣٢) سرى غضبان غيدان، محمد منذر جلال الربيعي: الامن السيبراني وسياسات المواجهة الدولية، مجلة الدراسات الاستراتيجية والعسكرية، المركز الديمقراطي العربي – برلين، المجلد الثاني -العدد التاسع، ديسمبر/ كانون الأول ٢٠٢٠ م، ص ص ١٩٠_١٩١

ثالثاً: أهم انواع الهجمات الالكترونية غير الفعالة:[٣٣]

١- برامج التجسس (Spy ware)، وهي برامج تثبت خلسة على اجهزة الحاسوب للتجسس والسيطرة عليها من دون علم المستخدم.
٢- التصيد (phishing)، ويعرف ايضاً بالخداع الالكتروني التي يتم بها خداع المستخدمين ليشاركوا بياناتهم الشخصية مثل تفاصيل بطاقات الائتمان وكلمات المرور.
٣- راصد لوحة المفاتيح (Key logger)، وهو احد اشهر برامج التجسس, ومن اقدم اشكال التهديد السيبراني, يقوم بسرقة المعلومات الشخصية او المالية مثل التفاصيل المصرفية, حيث يقوم (key logger) بجمع المعلومات وارسالها الى طرف ثالث.
٤- انظمة الدعم الاعلامي (Ad wa)، هو عبارة عن حزمة من البرامج الدعائية, حيث ان اي تطبيق برمجي يتم فيه عرض لافتات اعلانية اثناء تشغيل البرنامج, ف (Ad ware) , هو برنامج اعلاني, ليس فايروس, لكن في بعض الاحيان يكون فايروس, ويلجأ العديد من المستخدمين الى تنزيل التطبيقات المجانية التي تحمل بطياتها (Ad ware) , لكن في بعض الاحيان تكون هذه الاعلانات مشبوهة.
٥- جهاز راصد لوحة المفاتيح التجسسي: هو مكون مادي (Hard ware) , يستخدم للاختراق او التجسس, عن طريق قطعة يتم توصيلها بين لوحة المفاتيح واللوحة الام.

المطلب الثاني: تاثير المخاطر السيبرانية على استقرار الدولة وسبل المواجهة.

اولاً: تأثير المخاطر السيبرانية على استقرار الدولة.

ليس لآثار الهجمات السيبرانية حدود، فباماكنها التسبب بانفجارات في مخازن الوقود والمحطات النووية وكافة المراكز الحيوية أو تعطيل وسائل النقل برا ، بحرا، جوا او تغيير مسار الرحلات.[٣٤]

ويمكن أن يستخدم الفضاء الإلكتروني كوسيلة من وسائل الصراع داخل الدولة، بين مكوناتها على أساس طائفي أو اقتصادي أو ديني، وهو ما يساعد على كشف ديناميكيات التفاعل الداخلي إلى الخارج بما يسهل من عملية الاختراق الخارجي عبر شبكات الاتصال بدعم أحد أطراف الصراع بأدوات غير قتالية.[٣٥]

وسوف نبين أهم الآثار الناشئة عن الهجمات السيبرانية:[٣٦]

---

(٣٣) سرى غضبان غيدان، محمد منذر جلال الربيعي: الامن السيبراني وسياسات المواجهة الدولية ، مصدر سبق ذكره ، ص١٩١.

(٣٤) نور أمير الموصلي: الهجمات السيبرانية في ضوء القانون الدولي الانساني، مصدر سبق ذكره ، مصدر سبق ذكره، ص١٨.

(٣٥) نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني التهديد المتصاعد لامن الدول، مصدر سبق ذكره، ص ١٩٦.

(٣٦) نور أمير الموصلي: الهجمات السيبرانية في ضوء القانون الدولي الانساني، مصدر سبق ذكره ، مصدر سبق ذكره ، ص ص١٩_٢٠.

اولاً: الآثار الناشئة عن الهجمات السيبرانية في المجال العسكري

لقد لعبت التكنولوجيا دورا مهماً في المجال العسكري، حيث تعتمد عليها معظم الأنظمة العسكرية اليوم، وتتمثل الميزة النسبية للتكنولوجيا في قدرتها على ربط الوحدات العسكرية معاً، لتسمح بتبادل المعلومات وتدفقها بسهولة، والسرعة في إعطاء الأوامر العسكرية، والقدرة على تدمير الأهداف عن بعد.

ثانياً_ الآثار الناشئة عن الهجمات السيبرانية في المجال الاقتصادي

أصبحت صناعة تكنولوجيا المعلومات والاتصالات مورداً اقتصادياً مهماً للكثير من الدول، حيث أسهمت ثورة تكنولوجيا المعلومات والاتصالات في جعل أصحاب القرار يتخذون قرارات ا استثمارية رشيدة وبالتالي ساهمت في زيادة معدلات التنمية الاقتصادية، ومن الأمثلة على استخدام التكنولوجيا في المجال الاقتصادي : اعلانات المنتجات الجديدة، والأخبار الصحفية عنها، ومعلومات ترويجية حول مبيعات محددة وخاصة ، وجمع المعلومات الخاصة بخدمة العملاء، التسويق الالكتروني فأي هجوم سيبراني على هذا المجال سوف يؤثر ويخلف العديد من الآثار السلبية وسيكون المدنيين عاطلين عن العمل وغير محميين وستتعطل العمليات من منطقة إلى أخرى مسببة تدهورا اقتصادياً على مستوى الدولة، ومثال على ذلك الاحتيال في تحويل الأموال بالوسائل السيبرانية وسرقة الارصدة وتحويلها الى انشطة اجرامية .

ثالثا: الآثار الناشئة عن الهجمات السيبرانية في المجال الصحي

أصبح استخدام أجهزة وبرامج الكمبيوتر في الوقت الحالي دورا مهماً في تحسين جودة وكفاءة الرعاية الصحية وتقليل تكلفتها، ومن أهم ما تم تطويره فكرة السجلات الطبية الإلكترونية التي تشمل المعلومات الخاصة بالمريض والعلاجات السابقة،والأدوية المستخدمة سابقاً...الخ . ويعد الهجوم السيبراني على هذه السجلات الطبية بمثابة خرقاً خطيرا للأمن السيبراني للرعاية الصحية، وبالتالي إحداث كبير في المجال الصحي للدولة.

رابعاً_ الآثار الناشئة عن الهجمات السيبرانية في المجال البيئي

لقد تم استخدام أنظمة الاستشعار عن بعد ونظم المعلومات الجغرافية في مجال الحفاظ على البيئة، حيث تسهل دراسة تلوث المياه والهواء وسطح الأرض من خلال صور من خلال صور الأقمار الصناعية بعد معالجتها بجهاز الكمبيوتر، في تحديد مصادر التلوث ومراقبة الامتداد الموضعي للتلوث، خاصة أثناء حدوث تلوث جارئ معين، بالإضافة إلى دراسة تركيز هذا التلوث، وسرعة جريانه وتدفقه، ومقدار تشتته أيضاً. وفيما يتعلق بالكوارث الطبيعية، يمكن لصور الاستشعار عن بعد أن توفر معلومات دقيقة وسريعة عن مثل هذه الكوا رث قبل أو أثناء حدوثها أو بعد حدوثها توقت قصير، كالفيضانات والأعاصير، وحرائق الغابات ، والكوارث والاندفعات البركانية ،يظهر جلياً أهمية التكنولوجيا في مجال حماية البيئة من التلوث والحد منه بأسرع وقت ، او اي هجوم سيبراني على هذا المجال سوف يتسبب في الكثير من الدماروالاذى للنظام البيئي ومن خلال ما تقدم يتبين لنا ان تصنيف التهديدات حسب الاهداف أدى بصورة

تلقائيـة الى فهم الاثار التي تترتب على هذه التهديدات تستطيع ان تشكل عائق كبير امام العصب الاساسي للبنى التحتية للدول.[٣٧]

ثانياً: سبل مواجهة المخاطر السيبرانية

تعد الهجمات السيبرانية هجمات خليطة ، بمعنى استخدام خليط بين اكثر من تقنية واكثر من طريقة للهجوم على النظام .ولذلك فان التحدي لدى مهنيو الامن السيبراني يكون اقوى .فاءن لم تستطيع ايقاف الهجمة فعليك على الاقل بتقليل الضرر الناجم عنها.[٣٨]

لان المجتمع يشهد تطوراً متسارعاً لتكنولوجيا المعلومات والاتصالات، كما يشهد تزايداً وتنوعاً في التطبيقات والخدمات الإلكترونية التي تعتمد الفضاء السيبراني أساساً لها. ولأن تكنولوجيا المعلومات والاتصالات أصبحت الركيزة الأولى لبناء مجتمع المعرفة ولبنة أساسية في نموه وازدهاره، يتطلع العديد من الدول ، المتقدمة منها أو النامية، إلى بناء مجتمع معرفي جديد يعتمد على التنوع الاقتصادي، وعلى الابتكار والإبداع، وكذلك على التبادل المعرفي والفكري في المجالات الحيوية المختلفة.[٣٩]

لذلك، لا بد ان تنطلق الحلول في هذا المجال، من فهم الطبيعة الخاصة لتقنيات المعلومات والاتصالات، لاسيما الجزء الخاص بتجاوزها للحدود، وللمجتمعات، والانظمة، كما لطبيعة البنى التحتية نفسها، بما يعني الطبيعة غير الملموسة للبيانات، وامكانات تناقلها، واختراق الانظمة التي تحويها. ويعني هذا، بالدرجة الاولى، فهما مشتركا، للإمكانات التي تقدمها تقنيات المعلومات والاتصالات، بوجهيها السلبي والايجابي، ووعيا لضرورة ايجاد ارضية مشتركة، لمواجهة تحديات بناء الثقة في مجتمع المعلومات، انطلاقا من تحقيق بيئة آمنة.[٤٠]

عن طريق تبـادل الحكومـات بتوعيـة أفـراد المجتمـع بالتهديـدات القادمـة مـن الفضـاء الإلكترونـي، والتطبيقـات التكنولوجيـة المختلفـة، حتـى يدركـون كيفيـة الاستفادة مـن مميـزات هـذه التقنيـات وتلافي تهديداتهـا، ويتحقـق ذلـك عبـر شـراكة بيـن الحكومـة والقطـاع الخـاص والمجتمـع المدنـي.[٤١]

---

(٣٧) كرار فرحان هاني الطائي: أثر "الانترنت العميق" في أمن الدول، مجلة الدراسات الإستراتيجية والعسكرية، المركز الديمقراطي العربي ، ألمانيا – برلين، المجلد الثاني– العدد الثامن– سبتمبر ٢٠٢٠، ص ٧٤.

(٣٨) مقدمة في الامن السيبراني : ترجمة اسامة حسام الدين ، جامعة طيبة، المملكة العربية السعودية ، اكاديمية سيسكو ٢٠١٧ ، ص٢٠.

(٣٩) إرشادات الإسكوا للتشريعات السيبرانية: مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية، بيروت، ٢٠١٢، ص أ .

(٤٠) منى الأشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة، ص١٨.

(٤١) إيهاب خليفة: اليوم الأسود: أساليب الاستعداد لتطور الهجمات السيبرانية ، دورية اجاهات الاحداث ، مركز المستقبل للابحاث والدراساتالمتقدمة ، أبوظبي، العدد ٢١، مايو _يونيو ٢٠١٧، ص٤٥.

إن الردع السيبراني صعب التنفيذ، كما أن هناك العديد من العوامل التي يجب أن تحدث لضمان تحقيق النتائج المرجوة منها. ويتطلب الردع السيبراني طرق واساليب جديدة ، واعادة تكييف مفاهيم الردع التقليدية لتتناسب مع هذا المجال الجديد، فلا يمكن معرفة الهدف من الهجمات دون معرفة من شنها ودون معرفة الخصم وهدفه، ، لا يمكن للردع أن ينجح وسرقة المعلومات قد تتكرر مستقبلا، من هذه المتطلبات : الردع السلبي، الاحتجاجات الدبلوماسية، التدابير القانونية، العقوبات الاقتصادية، الانتقام في الفضاء الافتراضي، الانتقام العسكري.[٤٢]

تتعدد الأساليب و الطرق الإستباقية والتي بدورها تساهم في التصدي للهجمات السيبرانية، وتتمثل في صنفين اساسيين هما.[٤٣]

اولاً: الاستراتيجيات الهجومية: وهي تلك الطرق التي يتم استخدامها ضد اطراف معينة قد تشكل خطر مستقبلي على بيانتها ،وتعتمد بالاساس على عملية اطلاق نوع من الهجمات السيبرانية ، ولعل اشهرها مايسمى بحصان طروادة التي تعتمد على حزمة الفيروسات الخفية التي تهاجم الخصم بشكل فجائي وطريقة الابواب الخلفية المعتمدة على استغلال ثغرات نظام العدو واستراتيجية حجب الخدمة ، وتهدف كلها شل طرف معين او زعزعة قدراته الهجومية .

ثانياً: الإستراتيجية الدفاعية: وتتمثل في مجموعة الاجراءات الدفاعية التي تتمثل في تطوير الذات وتقوية القدرات لمواجهة الاخطارالممكنة ، وتتركز أغلبها في تجهيز مجموعة من الانظمة ذات ابعاد مختلفة تتمثل في:

١- البعد العسكري: وهي عملية الحماية الامنية للمعلومات من خلال بلورة انظمة الدفاع السيبراني ، وغالبا ما تكون هذه الانظمة والاستراتيجيات ذات مستوى عالي من السرية.
٢- البعد الاجتماعي : وهي عملية تامين البيانات للافراد وتختلف مابين اساليب الردع القانوني مثل اجراءات ردعية لمعاقبة المخترقين للحسابات الشخصية وسرقة الملكية المعلوماتية وغيرها والردع المعلوماتي المتمثل في انشاء انظمة الحماية ونشر التوعية الاجتماعية حول الاستخدام الامن.
٣- البعد السياسي: وهو امتلاك الدولة الحق في حماية نظامها السياسي ومصالحها ومصالح مواطنيها ، وذلك من خلال اعتماد استراتيجيات داخلية متمثلة في اجراءات محلية او خارجية من خلال العمل على التوافق الدولي لحماية الامن السيبراني.

---

(٤٢) نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني التهديد المتصاعد لامن الدول، مصدر سبق ذكره، ص٢٠٢ .

(٤٣) سامي محمد بو نيف:دور الاستراتيجيات الاستباقية في مواجهة الهجمات السيبرانية _الردع السيبراني انموذجا، المجلة الجزائرية للحقوق والعلوم السياسية ، معهد العلوم القانونية والادارية ، المركز الجامعي احمد بن يحيى الونشريسي، تيسمسيلت ، الجزائر ، العدد(٧)،٢٠١٩، ص ص ١٢٧_١٢٨.

ان الحديث عن الردع السيبراني بات أكثر مرونة، وباقترابات مختلفة، وتلك المرونة يمكن تداولها بطريقتين مختلفتين.[٤٤]

الأولى: الأنظمة البديلة: إن اعتماد دولة ما على نظام واحد، وتم اختراقه، سيسفر عن عواقب وخيمة؛ وبخاصة إذا تعلق هذا النظام بالبنية التحتية الرئيسية للدولة. لذلك، يمكن للدول خلق أنظمة بديلة لتكون في حوزة الدولة نفسها أو الدول الصديقة. وفي حالة حدوث هجوم سيبراني، يمكن الاستعانة بتلك الأنظمة البديلة أو الاحتياطية.

الثانية: إعادة التأسيس: فإذا أمكن للدولة التغلب على الهجوم الذي تعرضت له بسرعة، وإعادة تشغيل النظام، ستكون الآثار هامشية. ولكن الطريقة الوحيدة لتجنب الهجوم هي الاحتجاب عن الجميع، ورغم كونه السبيل الأفضل للردع، إلا أنه يكتنفه مسائل قانونية عدة.

من هنا تأتي أهمية تعاون كافة الفاعلين لترسيخ ثقافة عالمية امن الفضاء الالكتروني ، وأهمية الموازنة بين اعتبارات الامن وحرية استخدام الفضاء الالكتروني، والاحتكار العالمي للتكنولوجيا والعمل على انتقالها في دول العالم، ومن ثم فإن التعامل مع النمط الجديد من التهديدات يتطلب تعاوناً دولياً.[٤٥]

فضلا عن قرار الجمعية العامة للأمم المتحدة في الدورة ٢٣٩/٥٧ في ديسمبر٢٠٠٢ بشان ارساء ثقافة عالمية لأمن الفضاء الالكتروني ، و٧٢/٥٥ في ديسمبر٢٠٠٠ و١٢١/٥٦ في ١٩ ديسمبر٢٠٠٢ ، والدورة ١٩٩٩/٥٨ في ٢٣ ديسمبر٢٠٠٣[٤٦]، كما كان قرار الجمعية العامة للأمم المتحدة بإرساء ثقافة عالمية للأمن الإلكتروني من القرارات الهامة التي استهدفت العمل على حماية البنية التحتية الحيوية للمعلومات وحث وتفعيل دور المنظمات الدولية ذات الصلة، ودعوة الدول إلى وضع استراتيجيات لتقليل حجم التعرض للاخطار التي تشكل تهديدا للبنية التحتية الحيوية للمعلومات، واتخذت الجمعية العامة للامم المتحدة في الدورة ٢٥٨/٥٦ في ٣١/يناير ٢٠٠٢ قرارا يدعو الى استخدام تكنولوجيا الاتصال والمعلومات من اجل التنمية.[٤٧]

فالهجمات السيبرانية او الإلكترونية أصبحت خطراً يؤثر على أمن الدول، ولذلك بدأت تلقى اهتماماً متصاعدا على صعيد الأمن الدولي، في محاولة لمواجهة تصاعد التهديدات الإلكترونية ودورها في التأثير على الطابع السلمي للفضاء الإلكتروني.

([٤٤]) رغدة البهي: لردع السيبراني: المفهوم والإشكاليات والمتطلبات، مصدر سبق ذكره ، ص ص ٦٠_٦١

([٤٥]) دنيا جواد مطلك، احمد عبد الجبار عبد الله : انعكاسات تطور القوة المعلوماتية الامريكية في البيئة الداخلية، مجلة حمو راب للدراسات ، مركز حمورابي ، بغداد ، العدد ٣٥ السنة الثامنة ، ٢٠٢٠، ص١٦١.

([٤٦]) رائد العدوان: المعالجة الدولية لقضايا الإرهاب الإلكتروني، (دورة تدريبية تحت عنوان (توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب،٢٣_٢٠١٣/٢٧، الرياض ، ٢٠١٣) ، ص٩.

([٤٧]) المصدر نفسه، ص ص ٩-١٠.

الخاتمة

من خلال ما تقدم يمكن القول ان الامن السيبراني بات من المفاهيم الرئيسية التي تتطلب البحث والدراسة فيها كثيراً من قبل المختصيين والاكاديمين، فتهديدات الامن البشري لم تعد تنشأ من الادوات التقليدية كالصراع المسلح والقتال والحروب، ولكن ايضاً من خلال التهديدات والمخاطر السيبرانية والاختراقات الالكترونية في ظل العالم الرقمي.

إن الأمن السيبراني هو بُعد جديد ضمن أبعاد الأمن القومي، أحدث تغييرات جوهرية في مفاهيم العلاقات الدولية كالصراع والقوة والتهديد، حيث حتّم على فواعل المجتمع الدولي الانتقال من عالم مادي إلى عالم افتراضي في غاية التعقيد والتشابك، وبالتالي أصبح مفهوم الأمن السيبراني ضرورة حتمية في عالم اليوم، خاصة في ظل ارتباط كافة التفاعلات الدولية بالجانب الرقمي والتكنولوجي، الأمر الذي يستدعي على الدول ضرورة إيجاد وسائل فعالة لمواجهة المخاطر والتهديدات السيبرانية التي تتميز بالسرعة والغموض والدقة، ومن ثمة تحقيق الأمن السيبراني والحفاظ على مكاسب الدولة وأمنها القومي.

ان استنتاجات وتوصيات البحث هي الغاية التي من أجلها قمنا بدراسة الموضوع وإجراء البحث وهذه مجموعة من الاستنتاجات والتوصيات:

اولاً: الاستنتاجات:

١- يعد الامن الركيزة الاساسية لاستقرار الدولة، اذ يعد الأهم على الاطلاق بين مجمل المتغيرات التي تتصل بكيان الدول، ومدى قدرتها على الاستمرار والبقاء.

٢- الهجمات السيبرانية: يمكن تعريفها بكونها "فعلاً يقوّض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف معينة تُمكّن المهاجم من التلاعب بالنظام.

٣- الفضاء السيبراني يطرح العديد من التحديات على مستويات مختلفة داخل الدولة وبالتالي لابد ان تكون هناك استراتيجيات المواجهة.

٤- وتعمل هذه الاستراتيجيات على تغطية المجالات التالية: وجود الحكومة الفعالة، الاطار التشريعي، ثقافة الامن السيبراني وبناء القدرات، الاستعداد لحوادث الهجمات السيبرانية، التعاون الدولي.

ثانياً: التوصيات:

١- إعادة النظر بمفهوم الأمن السيبراني، اذ ينبغي أن يأخذ بنظر الاعتبار التطورات السريعة التي يشهدها العالم، خاصة في مجال الاتصالات والمعلومات.

٢- زيادة التعاون بين الدول للقضاء على المخاطر والجرائم والتهديدات السيبرانية، وذلك لما تختص به تلك الجريمة من خاصية اللاحدودية حيث لا تستطيع دولة بمفردها مهما بلغ تقدمها ان تحمي نفسها من تلك الهجمات السيبرانية دون التعاون مع دول العالم الأخرى.

٣- التطوير المستمر لبرامج الحماية داخل أجهزة الحاسبات الآلية للمؤسسات الحكومية والاقتصادية داخل الدول بشكل يصعب معه اختراقه من أي مجرم سيبراني.

٤- وضع قانون دولي موحد لمكافحة الجرائم السيبرانية، وتشريع قوانين حاكمة للفضاء السيبراني، وإيجاد طريقة مناسبة لتطبيقها، عن طريق الاستعانة بخيراء في هذا التخصص.
٥- تدريب أفراد الأمن القائمون على مكافحة الجريمة السيبرانية بشكل مستمر يتواكب ويتزامن مع التطور التكنولوجي الذي قد تكون عليه الهجمات السيبرانية.