المخاطر السيبرانية
وسبل مواجهتها في القانون الدولي العام

الدكتورة
أميرة عبد العظيم محمد عبد الجواد
مدرس القانون الدولي العام بكلية
الدراسات الإسلامية والعربية بنات القاهرة

المخاطر السيبرانية
وسبل مواجهتها في القانون الدولي العام

أميرة عبد العظيم محمد عبد الجواد.
قسم القانون العام/ شعبة الشريعة والقانون/ كلية الدراسات الإسلامية والعربية بنات القاهرة/ جامعة الأزهر.
البريد الالكتروني: AmiraAbdelgawad.2057@azhar.edu.eg

ملخص البحث :

نعيش اليوم العصر الرقمي، بفضل الثورة الهائلة في تكنولوجيا المعلومات والاتصال ، فزيادة التشابك في جميع المجالات أدى إلى خلق بيئة جديدة للتفاعل بين الأفراد والمجتمعات والدول، وهو ما اصطلح عليه بالفضاء السيبراني، هذا الفضاء الذي يتميز بالتطور السريع ، والغموض الشديد، وقد خلق الاستخدام السيئ لهذا الفضاء بيئة مليئة بالمخاطر والتهديدات ، شكلت تهديدا خطيرا للأمن القومي للدول حيث تغيرت مفاهيم القوة والصراع والحرب، وارتبطت طبيعتها بالفضاء السيبراني.

ومع بروز الأمن السيبراني كركيزة أساسية في بناء الأمن القومي، سارعت الدول ، لتشكيل الهيئات والمؤسسات المدنية والعسكرية ، وسن التشريعات القانونية ووضع إستراتيجية خاصة لمواجهة التهديدات السيبرانية الحالية والمستقبلية والدفاع عن أمنها، إضافة إلى العمل على المستويين الإقليمي والدولي من أجل فضاء سيبراني آمن وسلمي.

ولذا يعد من أبرز القضايا التي خلفتها القدرات التكنولوجية الحديثة أنها قد أفرزت أسئلة قانونية جديدة ومعقدة يتمثل أبرزها في السبل القانونية المتاحة أمام الدولة للتعامل مع الحالة التي تتعرض فيها إلى اعتداء سيبراني من قبل دولة أخرى.

وبالتحديد تتمحور المسألة حول مدى ملاءمة القواعد القانونية التقليدية الخاصة باستخدام القوة وبالدفاع عن النفس واستيعابها لفكرة الاعتداءات السيبرانية. فهل يمكن للهجمة السيبرانية أن تحقق المحددات القانونية الخاصة بالدفاع عن النفس حسب ما تقضي به المادة ٥١ من ميثاق الأمم المتحدة؟ أم هي مجرد استخدام للقوة في إطار المادة(٢/ ٤) من الميثاق، وبالتالي تضع الدولة المعتدى عليها أمام خيارات قانونية ما دون الدفاع عن النفس؟ أم أن هنالك نهجا آخر للتعامل مع الهجمات السيبرانية؟

وعلى هذا يسعى هذه البحث وراء وضع إجابات قانونية لهذه الأسئلة المحورية، من خلال مراجعة لقواعد القانون الدولي العام المتعلقة باستخدام القوة عموما، والدفاع عن النفس خصوصا والربط بينهما، وإلى الآراء الاستشارية لمحكمة العدل الدولية، وأيضا يتطرق البحث إلى استراتيجيات الدول بهذا الخصوص.

الكلمـات الدالـة:
المخـاطر الـسيبرانية ، الهجمـات الـسيبرانية، الفـضاء الـسيبراني، المخـاطر الالكترونية، المخاطر المعلوماتية أو مخاطر تقنية المعلومـات ، الأمـن الـسيبراني، مخاطر الانترنت، القوة السيبرانية، الحرب السيبرانية، دليـل تاليـن .

Cyber dangers and How to Confront Them in Public International Law

Amira Abdel Azeem Mohammed.

Department of Public Law / Sharia and Law / Faculty of Islamic and Arabic Studies, Cairo Girls/ Al-Azhar University.

Email: AmiraAbdelgawad.2057@azhar.edu.eg.

Abstract:

Today, We living the Cyber age, as a result of the Information and communication technology's revolution, the increase of the connectivity of all sectors, creating a new environment for interaction between individuals, communities and nations, which is called Cyberspace, which is characterized by rapid development, Full of dangers and threats, It posed a serious threat to the national security, where the concepts of power, conflict and war have changed, and their nature has been linked with Cyberspace.

Cyber-security as a key to building national security, States, have accelerated to create civil and military institutions, enacting legislations and developing a special strategy to fight current and future cyber threats, Also, they work at the regional and international levels, for a future Cyberspace safe and peaceful.

One of the most important issues brought about by modern technological capabilities is that they have produced new and more complex legal questions These questions were unprecedented and inconceivable not long ago. One of the most current complicated questions concerns the availability of legal means to the state to deal with situations where it is subjected to Cyber aggression by another State .

More specifically, the question is whether or not traditional legal rules on the use of force and self-defense are consistent

with the notion of cyber attacks. Is a cyber attack legally entitled to self-defense as required by Article 51 of the Charter of the United Nations? Or is it merely a use of force under Article)2 /4(Charter that leaves the aggressor state with no legal option to defend itself? Or else, is there another distinct approach particularly designed to deal with cyber attacks؟

This paper handles these important legal questions through a comprehensive review of the rules of international law on the use of force in general and self-defense in particular and the relation between them. In addition, the paper looks at the advisory opinions of the International Court of Justice the research also deals with the strategies of the countries in this regard.

Keywords :

Cyber dangers, Cyber space, Cyber Attacks, Electronic dangers, Information Technology dangers, Cyber Security, Internet dangers, Cyber Power, Cyber War, Tallinn Manual.

المخاطر السيبرانية
وسبل مواجهتها في القانون الدولي العام

مقدمة:

لقد أحدثت تكنولوجيا المعلومات والاتصالات ثورة شاملة في جميع نواحي الحياة وزادت هيمنة تكنولوجيا المعلومات والاتصالات على نسق الحياة العام، وصاحب ظهور الحاسب الآلي والتوسع في استخدام شبكة الإنترنت في مجالات الحياة المختلفة ظهور بعض الآثار السلبية والمخاطر المترتبة على هذا التوسع الكبير؛ إذ كلما زاد الاعتماد على هذه التقنيات في التنمية زادت المخاطر الخاصة بحماية المعلومات.

ومع تزايد الاعتماد العالمي على تكنولوجيا المعلومات والاتصالات تزايد أيضاً التعرض للهجمات من خلال الفضاء السيبراني، إذ أصبح الفضاء السيبراني عرضة للانتهاكات من قبل مخترقي الشبكات سواء أكانوا دولا أو غيرها مما يملكون هذه التقنيات المعلوماتية، فتوجهت الأنظار إلى الاهتمام وبشدة إلى الأمن السيبراني، وأصبح الحفاظ عليها حفاظا على الأمن القومي للدول.

ورغم أن المعالم الدقيقة لأي "حرب سيبرانية" لا تزال غير محددة فإن الهجمات الكبيرة ضد البنية التحتية للمعلومات وخدمات الإنترنت في العقد الأخير تُعطي صورة ما عن الشكل والنطاق المحتملين للنزاع في الفضاء السيبراني.

فبعد أحداث ١١ سبتمبر ٢٠٠١م بدأ التركيز على الفضاء السيبراني كتهديد أمني جديد بفعل أحداث دولية كان أبرزها استخدام تنظيم القاعدة له

كساحة قتال ضد الولايات المتحدة، وفي عام ٢٠٠٧م برز بوضوح دور الفضاء السيبراني كمجال جديد في العمليات العدائية في الصراع بين "استونيا" و"روسيا" وفي ٢٠٠٨ في الحرب بين "روسيا" و "جورجيا"، وجاء الهجوم السيبراني بفيروس "ستاكسنت" على برنامج "إيران" النووي عام ٢٠١٠ ليمثل نقلة هامة بالتطور في مجال الأسلحة السيبرانية. ولا نغفل الدور السياسي الذي لعبته شبكات التواصل الاجتماعي في حالة الثورات العربية في مطلع عام ٢٠١١م.

لذا أصبح أمن الفضاء السيبراني يدخل ضمن أولويات السياسة الخارجية للعديد من الدول وضمن استراتجيات الأمن القومي لديها، ودفعت التهديدات المتزايدة لأمن الفضاء السيبراني العديد من الدول للعمل على بذل جهود مضنية في استحداث قوانين لمكافحة الجريمة السيبرانية وإنشاء قيادة عسكرية لحماية الفضاء الالكتروني، وإنشاء هيئات لمواجهة الطوارئ المعلوماتية، واستحداث وحدات للحرب السيبرانية داخل الجيوش العسكرية.

لذا قامت العديد من الدول باعتماد استراتيجيات من شأنها دعم الجانب العسكري في الفضاء السيبراني ليس فقط ضد الهجمات التي قد يقوم بها الأفراد والقراصنة بل أيضا ضد احتمال استخدام الدول لمثل هذا المجال الجديد في الصراع، ولذلك بات من الضروري توحيد الجهود الدولية لوضع الأطر القانونية والتنظيمية والإجرائية لمواجهة المخاطر السيبرانية، وآثارها على المستوى الدولي.

ومن ثم فإن التعامل مع النمط الجديد من التهديدات يتطلب تعاونا دوليا، وبذل جهود دولية عاجلة ومتكاتفة لمواجهة تهديدات أمن الفضاء السيبراني بإمكانية العمل على حل الصراعات على أرض الواقع لمنع انتقالها إليه، والعمل على استجابة القانون الدولي لما يحدث من تهديدات في الفضاء السيبراني، وتعزيز أشكال التعاون الدولي في سبيل مكافحتها من أجل حفظ أمن الفضاء السيبراني باعتباره مرفقا دوليا وتراثا مشتركا للإنسانية.

وقد أطلقت العديد من المبادرات التي تقوم بها المنظمات الدولية لدعم الأمن السيبراني مثل الاتحاد الدولي للاتصالات الذي أطلق مبادرة للأمن السيبراني وحلف شمال الاطلنطي الذي أنشا وحدة للدفاع السيبراني، وأطلق الاتحاد الأوربي مبادرة للأمن السيبراني، فضلا عن مجهودات الدول في هذا الشأن فقد تبنت الولايات المتحدة الأمريكية "الإستراتيجية الدولية للفضاء السيبراني" وهي أول وثيقة سياسية من هذا النوع، تبين الرؤية الشاملة لمستقبل التعاون الدولي المتعلق بالفضاء السيبراني.

وبالرغم من أن الفضاء السيبراني له جوانب إيجابية عديدة تتمثل في سهولة الحصول على المعلومات وسرعة تبادلها، والمرونة في التعاملات على كافة المستويات الاجتماعية والتجارية والاقتصادية إلا أن جوانبه السلبية تفوق تلك المزايا بمراحل، فوفقاً للمعهد الدولي للدراسات الإستراتيجية بلندن، سيشكل الفضاء السيبراني أحد أهم ميادين الصراعات والحروب المستقبلية. فلا توجد

دولة مهما عظمت قدراتها العسكرية، ولا مؤسسة مهما عظمت قوتها الاقتصادية في مأمن من خطر الهجمات السيبرانية. (١)

وقد رُبطت هجمات في "جورجيا" و"إستونيا" و"كوريا الجنوبية" و"الولايات المتحدة" بالحرب السيبرانية. ورُبطت انقطاعات الكهرباء المتعددة في "البرازيل" بهجمات سيبرانية، وفي عام ٢٠٠٨ تمكن القراصنة من الدخول إلى الموقع الشبكي للحكومة والسيطرة عليه لمدة تزيد عن أسبوع. وتوضح انقطاعات الكهرباء في البرازيل الاتساع المحتمل للأنواع الجديدة من الهجمات السيبرانية، وجاء في التقارير تشبيه المشهد بفيلم من أفلام الخيال العلمي حيث توقفت تماماً قطارات الأنفاق وإشارات المرور وثاني أكبر محطة إنتاج قوى كهربائية وهو "سد إيتايبو"، وتأثر أكثر من ٦٠ مليون شخص. (٢)

وتتنوع هذه الهجمات الخطرة ما بين تدمير أنظمة إلكترونية لمنشآت حيوية عسكرية أو مدنية. وتعطيل أو إتلاف شبكات الدفاع العسكرية عن بعد، واختراق أو تعطيل أو تدمير شبكات القطاع الخاص، وتعطيل البنية التحتية

---

(١) - Matthew C. Waxman، "Cyber-Attacks and the Use of Force: Back to the Future of Article 2 (4) " The Yale Journal of International Law، Vol. 36، 2011، P423.

(٢) للكزيد: انظر: د/ عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، وحدة الدراسات المستقبلية، قوانين وتشريعات، إصدارات مكتبة الإسكندرية، العدد ٢٣، ٢٠١٦، ٤٠ - ٤٢.

للدول، والتدخل في سلامة البيانات العسكرية الداخلية لدول آخر، ومحاولة إرباك أو التشويش على معاملاتها المالية.

فأصبحنا الآن أمام جرائم حقيقية متكاملة تتم عن طريق شبكات الانترنت، وأجهزة الحاسوب من التخطيط والترويج لعمليات إرهابية، والنصب والاحتيال لسرقة الأموال، والتجسس وكذلك القرصنة باعتبارها الجريمة الأكثر شيوعا. . . الخ.

وأصبحت الجريمة السيبرانية تكلف الاقتصاد العالمي ما يزيد على ٢٣٠ مليار دولار سنويا ويتعرض الفضاء السيبراني إلى ١٠٠٠ هجوم كل دقيقة يتمثل في قيام بعض العناصر المدربة تدريباً جيداً بالتغلغل في مجتمع ما وتهديد أمن المطارات والمصانع الكيمائية ومحطات الطاقة النووية فيه وغيرها من المؤسسات التي تسير بنظام الحاسوب ولا تطبق إجراءات أمنية بشكل كاف.

ولقد حدثت بالفعل هجمات من هذا النوع من قبل جماعات إرهابية في كل من "فرنسا" و"إيطاليا". ولاشك أن وصول المجرمين أو الجماعات الإجرامية إلى هذه القواعد وتدميرها أو حتى مجرد تعطيلها يشكل خطراً بالغاً على الأمن القومي للدول، حيث إن هذا من شأنه أن يقوض بنيتها ويعطل العمل في هذه المجالات.

وعلى هذا فيمكن اعتبار تحدي الأمن السيبراني أعلى تحديات الأمن القومي في القرن الواحد والعشرين، مع الإشارة إلى أن المفهوم الحديث للأمن لا يقتصر فقط على الجوانب العسكرية، بل يواكب كل التهديدات والتحديات التي يمكن أن شكل حجر عثرة أمام الاقتصاد الرقمي وتدفق المعرفة، فقد

أسقطت تكنولوجيا المعلومات والاتصالات مفهوم الحدود الجغرافية بين الدول مما يضع السيادة الوطنية على المحك، خاصة مع اختراق المواقع الحكومية الرسمية والتجسس المعلوماتي على الدول.

وسوف أتعرض في هذا البحث للوضع الراهن للجرائم السيبرانية والأمن السيبراني إقليمياً ودولياً من خلال عرض وسائل تعزيز وتنسيق الجهود لمكافحة مخاطر الفضاء السيبراني وضمان سلامته مما يعرض السلم والأمن الدوليين للخطر. من خلال مقدمة وثلاث مباحث وخاتمة، وذلك على النحو التالي:

خطة البحث

مقدمة:

المبحث الأول: في ماهية المخاطر السيبرانية.

المطلب الأول: التعريف بمصطلح المخاطر السيبرانية

المطلب الثاني: المفاهيم المرتبطة بالمخاطر السيبرانية.

المطلب الثالث: طبيعة المخاطر السيبرانية وسماتها.

المطلب الرابع: صور المخاطر السيبرانية.

الفرع الأول: الاختراقات السيبرانية.

الفرع الثاني: التجسس السيبراني.

الفرع الثالث: الإرهاب السيبراني.

الفرع الرابع: الهجمات الإستراتيجية والعسكرية السيبرانية.

أولا: استهداف البنية التحتية للدولة:

ثانيا: السيطرة على الأنظمة العسكرية:

المبحث الثاني: المخاطر السيبرانية وأثرها على تهديد السلم والأمن الدوليين.

المطلب الأول: المخاطر السيبرانية وموقف ميثاق الأمم المتحدة من استخدام القوة السيبرانية.

المطلب الثاني: المخاطر السيبرانية وحق الدفاع الشرعي وفق المادة ٥١ من ميثاق الأمم المتحدة.

المطلب الثالث: المخاطر السيبرانية وحقوق الإنسان الرقمية.

المطلب الرابع: العمليات السيبرانية والقانون الدولي الإنساني.

المبحث الثالث: الجهود الدولية لمواجهة المخاطر السيبرانية.

المطلب الأول: قرارات المنظمات الدولية.

أ. قرارات الأمم المتحدة. ب. الاتحاد الدولي للاتصالات.

ج. اتفاقية بودابست لمقاومة جرائم السيبرانية والاتصالات ٢٠٠١.

د. قرارات بعض المنظمات الأخرى.

المطلب الثاني: المجهودات الفقهية لمواجهة المخاطر السيبرانية.

الفرع الأول: دليل تالين والهجمات السيبرانية.

الفرع الثاني: إعلان إيريتشي لمبادئ الاستقرار السيبراني والسلام السيبراني(الاتحاد العالمي للعلماء).

المطلب الثالث: استراتيجيات الدول لحماية أمنها من المخاطر السيبراني.

الخاتمة:

المبحث الأول
في ماهية المخاطر السيبرانية

لاشك أن التطور السريع في تكنولوجيا الكمبيوتر، دفع المجتمع الدولي للدخول في مرحلة جديدة يلعب فيها الأمن السيبراني دورا أساسيا سواء في الاستحواذ على عناصره الأساسية أو في تعظيم القوة، لظهور محددات جديدة للقوة من حيث طبيعتها و أنماط استخدامها وطبيعة الفاعلين فيها، وانعكاس ذلك على قدرات الدول وعلاقاتها الخارجية مما جعل هذه البيئة السيبرانية حقيقة غير مسبوقة، واتجهت الدول إلى الحفاظ على أمنها القومي لمواجهة ما يعرف بصراع "عصر المعلومات".

ومن ثم فإن الفضاء السيبراني قد فرض إعادة التفكير في مفهوم الأمن والذي يتعلق بتلك الدرجة التي تمكن الدولة من أن تصبح في مأمن من المخاطر التي تتعرض لها ومن حماية البنية التحتية للمنشآت الحيوية من الاستخدام غير المشروع لتكنولوجيا الاتصال والمعلومات بهدف محاوله السيطرة على الأجهزة وسرقة المعلومات وإفسادها أو تعطيلها.

ولذا فسوف أتطرق في هذا المبحث الأول إلى ماهية المخاطر السيبرانية. مبينة ما يأتي من خلال المطالب الآتية:

المطلب الأول: التعريف بمصطلح المخاطر السيبرانية.

المطلب الثاني: المفاهيم المرتبطة بالمخاطر السيبرانية.

المطلب الثالث: طبيعة المخاطر السيبرانية وسماتها.

المطلب الرابع: صور المخاطر السيبرانية.

المطلب الأول
التعريف بمصطلح المخاطر السيبرانية

كلمة السيبرانية، مشتقة من الكلمة اللاتينية" سايبر "Cyber" ومعناها تخيلي أو افتراضي، والسايبر كلمة يجري استخدامها لوصف الفضاء الذي يضم الشبكات العنكبوتية المحوسبة، ومنظومات الاتصال والمعلومات وأنظمة التحكم عن بعد. وتعني: كل ما يتعلق أو يرتبط بالحواسيب وتكنولوجيا المعلومات والواقع الافتراضي، ومنها اشتقت صفة السيبرانية والسيبراني Cybernetics وتعني علم التحكم الأوتوماتيكي، أو علم الضبط. و تعني أيضا القيادة أو التوجيه، والذي يعني: "علم الاتصالات وأنظمة التحكم الآلي في كل من الآلات والأشياء الحية.[1]

وتجدر الإشارة إلى أنه تعددت المصطلحات التي تصف المخاطر فمنها مخاطر الحاسب الآلي (Computer dangers)، أو المخاطر الالكترونية (Electronic dangers)، أو المخاطر المعلوماتية أو مخاطر تقنية المعلومات (Information Technology dangers)، أو مخاطر الانترنت (Internet dangers)، أو المخاطر السيبرانية (Cyber dangers)

---

(١) منير البعلبكي"المورد: قاموس إنكليزي-عربي"، دار العلم للملايين، بيروت٢٠٠٤،ص٢٤٣.

وقاموس أكسفورد https: //en. oxforddictionaries. com/definition/cyber:

وجميعها تعكس مسمى واحدا فهى تشير إلى تطور الأنماط المختلفة[١] للمخاطر في مجال تكنولوجيا المعلومات، وإلى الأثر الكبير الذي أحدثه التطور العلمي التكنولوجي في مجال برمجة المعلومات، ويفضل الباحث استخدام مصطلح السيبرانية لوصف المخاطر لوروده في العديد من الوثائق القانونية، كما أن ذلك المصطلح يشير بصورة أدق لإجمالي أنماط المخاطر سواء تعلقت بالحاسب الآلي أو بشبكات التكنولوجيا أو تقنية المعلومات.

وتختلف استخدامات السايبر وأشكاله من دولة إلى أخرى تبعًا لأولويات هذه الدول، فمنها الأمني والسياسي والاستخباراتي والمدني والمهني والمعلوماتي البحت. ويتشكل كيان السايبر في الدول كلها بشكلٍ عام من وجود ثلاثة

(١) رغم أنه يمكن مناقشة الفوارق بين هذه الطوائف المختلفة من المخاطر سواء أكانت مخاطر الحاسب الآلي وما يتعلق بها من برمجيات وأدوات، أو مخاطر الانترنت وما يتعلق بها من تطور في نظم الشبكات وتبادل المعلومات والاتصالات، أو مخاطر المعلوماتية وما يتصل بها من تقنيات لمعالجة البيانات وتقديم الخدمات، إلا أن الواقع التقني، وكذلك الواقع القانوني الدولي يشير إلى اندماج هذه المجالات جميعا (الحوسبة، وتكنولوجيا المعلومات والاتصالات) تحت مصطلح يعد حديث نسبيا ألا وهو (Cyber) ، وفي ظل غياب مقابل لهذا المصطلح في اللغة العربية، وبدأت ترجمته الحرفية تظهر في العديد من الكتابات، فضلا عن ظهور بعض الكيانات والمؤسسات التي تعتمد هذا الاسم مثل اللجنة الدولية للصليب الأحمر ودليل تالين.

عناصر أساسية تضم: - الأجهزة الصلبة (Hardware)، والبرمجيات الرقمية (Software)، والعامل البشري من مبرمجين ومستخدمين. [١]

ولبيان كلمة المخاطر لابد أن نعرف البيئة التي تحدث فيها هذه المخاطر وهى الفضاء السيبراني: -

ويعرف الفضاء السيبراني: - بأنه الوسط الذي توجد به، وتعمل فيه شبكات الحواسيب السيبرانية، وتشمل أجهزة الكمبيوتر، وأنظمة الشبكات، والبرمجيات، وحوسبة المعلومات، ونقلها، وتخزينها، بالإضافة إلى مستخدميها من البشر والهيئات والمؤسسات. [٢]

فالفضاء السيبراني: تلك البيئة الافتراضية التي تعمل بها المعلومات السيبرانية والتي تتصل عن طريق شبكات الكمبيوتر، وكما يعرف أيضاً بأنه المجال الكهرومغناطيسي لتخزين وتعديل أو تغيير البيانات المتصلة والمرتبطة بشبكة البنية التحية الطبيعة، ويتضمن عملية الاندماج ما بين الانترنت والمحمول وأجهزة الاتصالات والأقمار الصناعية، والفضاء الالكتروني أكبر

---

(١) المنطقة المعتمة. . التاريخ السري للحرب السيبرانية، تأليف: فرد كابلان، ترجمة: لؤي عبدالمجيد السيد، سلسلة عالم المعرفة، ص٨.

(٢) للمزيد أنظر: عادل عبد الصادق، " الفضاء الالكتروني والرأي العام: تغير المجتمع والأدوات والتأثير "، المركز العربي لأبحاث الفضاء الالكتروني: قضايا استراتيجية، العدد ٢٤٥٩، (٢٠١٣)، ص ٣٥.

من الانترنت، لما يحتويه من قدرات توجيهية للطاقة التي توجد في جزء من الموجات الكهرومغناطيسية. (١)

وقد عرفه الاتحاد الدولي للاتصالات بأنه: " المجال المادي وغير المادي الذي يتكون وينتج من عناصر هي: أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكم، ومستخدمو كل هذه العناصر. (٢)

كما عرفت الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI)(٣) الفضاء السيبراني بأنه: " فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية". فهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكوّن من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين". (٤)

ومن ثم فالفضاء السيبراني هو بيئة تفاعلية مكونة من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين. وأن كافة التهديدات

---

(١) للمزيد أنظر: عادل عبد الصادق، " الفضاء الالكتروني والرأي العام: تغير المجتمع والأدوات والتأثير "، مرجع سابق، ص ٣٩.

(٢) ١ The International Télécommunication Union، ITU Toolkit for CybercrimeLégislation، Geneva، 2010، P 12.

(٣) هي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي.

(٤) Olivier KEMPF، Introduction à la Cyberstratégie، Paris، 2012، P. 19.

والتأثيرات التي تحيط بتلك البيئة ومكوناتها يعد مخاطر سواء وقعت بالفعل أو على وشك الوقوع ويلزم العمل على مواجهتها.

وتعرف المخاطر بأنها: عبارة عن الضرر الذي يهدد أمن الأفراد والبيئة والجماعات البشرية لكنه يوشك أن يحدث – أو حدث فعلاً – ويمكن احتواؤه إن لم يتفاقم.(١)

فالمخاطر تشتمل على كل تهديد يستهدف مؤسسات الدولة باستخدام الأيديولوجيات أو استخدام مكونات القدرة لدولة ضد دولة أخرى حيث يمكن أن يكون إقليم الدولة أو استقلالها أو أمنها مهددا بضرر ويمكن أن تأتي التهديدات من الخارج أو من الداخل الدولة .(٢)

ويتضح من ذلك أن المخاطر تشمل التهديدات التي تتعرض لها الدولة سواء على وشك الحدوث أم حدثت فعلا، وفي هذه الحالة لابد للدولة أن يكون لها استراتيجيات تستطيع من خلالها مواجهة تلك التحديات التي تتعرض لها.

---

(١) LivierNay، Lexique de Science politique vie et Institutions politiques، Europe Media Duplication SAS، Toulouse، 2008، P 482.

(٢) تيري ديبيل استراتيجية الشؤون الخارجية منطـــق الحكم الأمريكي، ترجمة وليد شحادة دار الكتاب العربية، مؤسسة محمد بن آل راشد آل مكتوم، بيرو، ٢٠٠٩ ص، ٢٥٨.

وتتمثل التحديات في المشاكل والصعوبات التي تواجه الدولة وتحد أو تعوق من تقدمها وتشكل حجر عثرة أمام تحقيق أمنها واستقرارها ومصالحها الحيوية الذاتية أو المشتركة [١]

ويتحدد أن هناك خطراً ما حسب وقت وقوع الخطر أو الضرر [٢] فقد تتغير حالة الخطر بالاعتماد على الإجراءات التي يتخذها كلتا الأطراف الفاعلة وهما المهاجم الذي تكون لديه القدرة على إحداث الأذى ويستخدمه. والجهة المستهدفة التي يمكنها اتخاذ الاحتياطات لتحمل أو إحباط الخطر الذي ينوي المهاجم إحداثه، وبالرغم من أن الاعتماد على التقنية الرقمية آخذ بالنمو كل يوم، ولكن فهم المخاطر المرتبطة بهذا الاعتماد لا يزال في مراحله الأولى.

ويمكن القول إن الدول تكون في حالة التهديد عندما يصل تعارض المصالح والغايات القومية مرحلة يتعذر معها إيجاد حل سلمي يوفر للدول الحد الأدنى من أمنها السياسي والاقتصادي والاجتماعي والعسكري، بالإضافة إلي قصور قدرتها لموازنة الضغوط الخارجية الأمر الذي

---

(١) LivierNay، Lexique de Science politique vie et Institutions politiques، Europe Media Duplication SAS، Toulouse، 2008، P. 482.

(٢) قاموس أكسفورد. المنشور الخاص بالمعهد الوطني للمعايير والتقنية (المراجعة أ) يُعرف الخطر بـ: الخطر = التهديد x نقطة الضعف. CRM تُعّرف بيانات الخطر بـ: الخطر = الحالة الاحتمالية + النتيجة (الأثر)، ص ٣٠، ود. محمد فهمي طلبة، الموسوعة الشاملة لمصطلحات الحاسب الآلي، مطابع المكتب المصري الحديث ١٩٩١، ص ٢٣

قد يضطر الأطراف المتنازعة إلي اللجوء إلى استخدام القوة العسكرية، معرضة الأمن القومي للخطر .[١]

والخطر السيبراني يزداد بسبب توفر سوق للبرامج والأدوات الخبيثة والخدمات غير المشروعة والبيانات الحساسة (غير المتاحة للعامة) بأسعار زهيدة. فعلى سبيل المثال، يمكن شراء برنامج خبيث مقابل دولار واحد ويمكن إطلاق هجمات الحرمان من الخدمات (DDoS) بأقل من ألف دولار. كما تتوفر هجمات برامج الفدية مقابل مئتي دولار وخدمات الرسائل الإلكترونية غير المرغوبة (سبام) بمبلغ أربعمائة دولار تقريباً، كما يمكن أيضاً استهداف أسلحة معقدة من خدمات الاستخبارات الحكومية.[٢]

ويمكن لأي دولة شن هجمات ناجحة وإحداث الأذى للوصول لهذه القدرات.

---

(١) انظـــــر: د/ أحمد عبد الحليم، أمن الخليج: إلى أين؟ ، أوراق الشرق الاوسط، ، ١٩٩٢، ص ٢٨- ٢٩.

(٢) انظر: د/ نيكولاس راب وروبرت هاكيت، "أدوات الهاكرز. " مقال منشور في مجلة فورتشن ٢٥ أكتوبر ٢٠١٧-.

http: fortune. com /25/10/2017/cybercrimecom. spyware-marketplace.

مجلة فورتشن هي مجلة دولية، تصدر من أمريكا، تُعنى بقضايا المال والأعمال. تصدرها شركة تايمز الإعلامية. أنشئت سنة ١٩٣٠ على يد مؤسس مجلة تايمز هنري لوس. تعد مجلة فورتشن من أكثر الإصدارات تأثيراً في العالم

كما حدث عام٢٠١٧ حيث وقعت مجموعة من الهجمات السيبرانية نذكر بعض منها: -

ففي مايو ٢٠١٧، استهدف أحد برامج الفدية (WannaCry) بعض الثغرات في أنظمة التشغيل "مايكروسوفت ويندوز" وأصاب الملايين من الحواسيب في ١٥٠ دولة في مختلف قطاعات الأعمال. وأدى هذا الهجوم العالمي إلى توقف عمليات التصنيع وأنظمة النقل وأنظمة الاتصالات. كما أصاب هذا البرنامج ما لا يقل عن ٨١ منظمة من منظمات هيئة الخدمات الصحية الوطنية مما عطل المعدات الطبية عن العمل وأثر بشكل كبير على صحة وسلامة عامة الناس. [1]

وفي يونيو ٢٠١٧، تم إطلاق برنامج مدمر (NotPetya) بين الشركات التجارية العالمية المتصلة بالشبكات بواسطة آلية لتحديث البرامج لأحد برامج المحاسبة شائعة الاستعمال(me. doc.)وفي غضون دقائق معدودة، أصاب البرنامج الخبيث عشرات آلاف الأنظمة المتصلة بالإنترنت في أكثر من ٦٥ دولة، من بينها أنظمة تعود لمؤسسات حكومية ومصارف وشركات للطاقة وغيرها من الشركات مثل هجوم NotPetya على. -P. A Maersk

(١) مكتب التدقيق الوطني، "تحقيق عن هجوم WannaCry السيبراني وهيئة الخدمات الصحية الوطنية، " ٢٧ أكتوبر ٢٠١٧، لمزيد من التفاصيل عن التحقيق على موقع: - https: //www. nao .org .uk/report/cyber-wannacry-investigation-and-the-nhs/.

Moller -أكبر شركة للشحن في العالم -مما أدى إلى تشفير ومسح أنظمة تقنية المعلومات الخاصة بالشركة في جميع أنحاء العالم.[١]

ومن ثم كان للنشاطات السيبرانية الغير مشروعة في عام ٢٠١٧ أثر كبير من حيث الخسائر والأضرار التي تسببت بها، ومع ذلك، كانت الأدوات التي استخدمت لإحداث الأذى بسيطة وغير معقدة. لقد تضاعف عدد الهجمات المستهدفة لأنظمة الطاقة والاتصالات والنقل ولأنظمة المالية في السنوات الخمس الأخيرة. ويشكل هذا الاتجاه خطراً أمنياً واقتصادياً ووطنياً للدول،

---

(١) وعلى إثر ذلك، اضطرت Maerskلإيقاف عملياتها في معظم محطاتها المينائية الـ٧٦ حول العالم مما أدى إلى تعطيل التجارة البحرية لأسابيع عدة. تجاوزت خسائر Maersk بفعل NotPetya 300 مليون دولار حيث اضطرت لإعادة بناء كامل لبنيتها التحتية، بما في ذلك ٤٠٠٠ خادم جديد و٤٥٠٠٠ حاسوب جديد و٢٥٠٠ تطبيق جديد. وتُقدر الخسائر التي تسبب بها NotPetya بمليارات الدولارات بسبب تعطل الأعمال وتدمير الممتلكات في جميع أنحاء العالم. وكانت الخسائر الأولية والاحقة للاقتصاد الرقمي كبيرة واستغرق الأمر عدة أشهر للتعافي من الضرر الذي تعرضت له الخدمات والبنى التحتية الحساسة. NotPetya يعطل الأعمال ويُدمر أصول رؤوس أموال الشركات في مختلف أنحاء العالم. التقارير العامة تُظهر خسائر لا تقل عن ٢.٥ مليار دولار. وتحذر من أن أي هجوم سيبراني محكم التنفيذ قد يتسبب بأضرار حول العالم تتراوح من ١.٥٣ مليار دولار إلى ١٢١.٤ مليار دولار.

أنظر :لويدز لندن، "هجوم سيبراني خطير قد تبلغ تكلفته نفس تكلفة إعصار ساندي، ١٧" يوليو ٢٠١٧، لمزيد من التفاصيل:

-press/insight-risk-and-news/com .oydsll .www// :https
report-attack-cyber/٠٧/٢٠١٧/releases.

لذا، فإن هناك حاجة ماسة لاشتراك قادة الحكومات والشركات للانخراط في العمليات الفعالة لإدارة الخطر السيبراني ولمعالجة المخاطر الرقمية ضمن عملياتهم للتخطيط الاستراتيجي[1].

وتعمل الدول والمنظمات الدولية والمؤسسات الأكاديمية على تطوير أطر عمل لمساعدة الحكومات والشركات على تشخيص الخطر السيبراني وعلى خفضه. فهناك حاجة ماسة لمثل هذه الأطر. فالمخاطر تتزايد، ومن ثم لابد من مواجهتها والعمل على التصدي لها.

المطلب الثاني
المفاهيم المرتبطة بالمخاطر السيبرانية

هناك العديد من المفاهيم المرتبطة بالمخاطر السيبرانية، ومن أهمها ما يلي:

الأمن السيبراني يتمثل في مجموعة الآليات والإجراءات والأطر التي تهدف إلى حماية البرمجيات وأجهزة الكمبيوتر من مختلف الهجمات والاختراقات السيبرانية التي قد تهدد الأمن القومي للدول.

وعرف الاتحاد الدولي للاتصالات الأمن السيبراني بأنه: "مجموعة من المهمات والوسائل والسياسات والإجراءات الأمنية والمبادئ التوجيهية والمقاربات لإدارة المخاطر، والتدريبات والممارسات الفضلى والتقنيات التي

---

(١) إدارة الخطر السيبراني الوطني إعداد ميليسا هاثاواي ضمن المنهجية التي وضعتها باسم "مؤشر الجاهزية السيبرانية". وبالإمكان الإطلاع على مؤشر الجاهزية السيبرانية منشور على موقع http: //www. potomacinstitute .org/academic-centers/cyber-readiness-index.

يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين". [١]

ويعرف البعض الأمن السيبراني بأنه: " عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة". [٢]، بينما يعرفه البعض الآخر على أنه: " 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،. . إلخ" [٣].

ومن ثم فالأمن السيبراني يمكن تعريفه بأنه: مجموعة من الإجراءات التي يتم اتخاذها للحد أو الدفاع ضد هجمات الكمبيوتر أو البرمجيات، ويتضمن تنفيذ التدابير المضادة المطلوبة، ويشمل الوسائل والأدوات المستخدمة في مواجهة المخاطر.

وأما **أمن المعلومات**: - يقصد به: " حماية المعلومات من المخاطر التي تهددها ويتم ذلك من خلال وسائل وأدوات وإجراءات من أجل ضمان حمايتها

---

(١) التقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في الاتصالات لعام ٢٠١٠ -٢٠١١.

The International Télécommunication Union، ITU Toolkit for CybercrimeLégislation، Geneva، 2010، P 12.

(٢) Richard A. Kemmerer، Cyber security، University of California Santa BarbaraDepartment of Computer Science، 2003، P. 3.

(٣) Edward Amoroso , Cyber Security, SiliconPress, 2007,p,5.

من المخاطر سواءً كانت تهديدات داخلية أو خارجية". فأمن المعلومات يهدف إلى حماية الأنظمة الحاسوبية من الوصول غير الشرعي لها، أو العبث بالمعلومات أثناء التخزين أو المعالجة أو النقل.

فالأمن السيبراني مفهوم أوسع من أمن المعلومات، فالأمن السيبراني يهتم بأمن كل ما هو موجود على السايبر، بينما أمن المعلومات لا يهتم بذلك، كما أن أمن المعلومات يهتم بأمن المعلومات الفيزيائية "الورقية"، بينما لا يهتم الأمن السيبراني بذلك.

والقوة السيبرانية: هي 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.[١]

وتعد الحرب السيبرانية:[٢] أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو

---

(١) Joseph S. Nye: The Future of Power. Press Release، Harvard Kennedy School، Belfer Center for Science and International Affairs، January 31، 2011 .

(٢) وعلي الرغم من الاستخدام الواسع في وسائل الإعلام لمسمي "الحرب السيبرانية "، فإنه لم يعد كافيا إثر اتساع مدلولاته بعد أن كان مقصورا في التشويش علي أنظمة الاتصال والرادار وأجهزة الإنذار، بينما يكشف الواقع الحالي عن دخول شبكات الاتصال والمعلومات إلي بنية ومجال الاستخدامات الحربية، أما إطلاق مسمي "الحرب"

تعطيلها. [١] ويعرفها آخرون بأنها: " مفهوم يشير إلى أي نزاع يحدث في الفضاء الإلكتروني ويكون له طابع دولي". [٢]

ومصطلح القوة السيبرانية أكثر شمولا من مصطلح الحرب السيبرانية

فمفهوم القوة السيبرانية "cyber power " يتضمن كافة مجالات القوة التي تندرج تحت إطار الصراع السيبراني بشكل يختلف عن مسمى الحرب السيبرانية " cyber war " والذي يشير إلى القوة العسكرية للفضاء

علي هجمات الكمبيوتر، فهو أيضا بحاجة إلي نظر كون "الحرب" مفهوما يرتكز بالأساس علي استخدام الجيوش النظامية، وكان يسبقها إعلان واضح لحالة الحرب وميدان قتال محدد. أما في هجمات الفضاء السيبراني، فإنها غير محددة المجال أو الأهداف، كونها تتحرك عبر شبكات المعلومات والاتصال المتعدية للحدود الدولية أو اعتمادها علي أسلحة إلكترونية جديدة تلائم السياق التكنولوجي لعصر المعلومات، والتي يتم توجيهها ضد المنشآت الحيوية أو دسها عن طريق العملاء لأجهزة الاستخبارات، وتجعل عملية استخدام هجمات الكمبيوتر سياسيا في أي صراع أقرب إلي توصيفها بالإرهاب عن كونها حربا، ولا يحمل ذلك تقييما أخلاقيا لها بقدر ما هو تعبير عن طبيعتها الفنية وطرق حدوثها.

(١) Bonnie N. Adkins ، " The Spectrum of Cyber Conflict from Hacking to Information Warfare: What is Law Enforcement's Role?" A Research Report Submitted to the Faculty In Partial Fulfillment of the Graduation Requirements ، Maxwell Air Force Base ، Alabama April ، 2001.

(٢) Kevin Coleman ، The Challenge of Unrestricted Warfare ، A Look Back and a Look Ahead Articles ، http: // www. directionsmag .com.

السيبراني، ويتم الإشارة إليه بالهجوم السيبراني عندما يتم اعتباره نمطا من الهجوم يتم شنه من قبل الدولة أو الفاعلين من غير الدول والتي يكون لها تداعيات على الأمن القومي للدول والأمن العالمي.

والجريمة السيبرانية[١]: عبارة عن الفعل غير المشروع الذي يمس مصلحة أو حقاً ويتعلق بالمكونات المادية وغير المادية للوسائل السيبرانية، ويكون المشرع قد قدر حمايتها بنصوص التجريم والعقاب بأن اعتبر الاعتداء عليها جريمة معاقب عليها بجزاء جنائي. [٢]

ويمكن تعريف الجريمة السيبرانية بأنها[٣]: " كل فعل أو امتناع عن فعل باستعمال نظام معلوماتي معين للإضرار بمصلحة أو حق يحميه القانون من

---

(١) وهناك من يطلق عليها مصطلح الجريمة المعلوماتية أو الجرائم التقنية ويقصد به: " جملة البيانات والمعلومات التي تخضع لعمليات آلية من جمع وتحليل وتخزين ومعالجة وصياغة واسترجاع ونقل وتداول، وذلك وفقاً للتقنيات الحديثة لنظام معلوماتي معين يتمثل في نظم الحاسبات الآلية وما يقوم مقامها من النظم المطورة وشبكات الاتصال " انظر: د/ هلالي عبد اللاه أحمد، جرائم الحاسب والانترنت بين التجريم الجنائي وآليات المواجهة، دار النهضة العربية، ٢٠١٥، ص ٤٤.

(٢) انظر: د/ راشد محمد المري، الجرائم السيبرانية في ظل الفكر الجنائي المعاصر، دراسة مقارنة، مرجع سابق، ص ٢١.

(٣) اختلفت الاجتهادات الفقيه المحاولة وضع تعريف للجريمة المعلوماتية ويمكن ردها إلى أربعة طوائف:

الطائفة الأولى: عرفتها بالنظر إلى وسيلة ارتكاب الجريمة، وبالتالي عرفت الجريمة المعلوماتية على أنها: " كل أنواع السلوك غير المشروع الذي يرتكب عن طريق الحاسب

الآلي أو بمساعدته أو أن يكون أداة رئيسية في ارتكابه، أو له دوراً هاماً إيجابياً في هذا الارتكاب. "

الطائفة الثانية: نظرت إلى محل الجريمة باعتباره أساساً لتعريف هذه النوعية من الجرائم، وبتالي عرفت الجريمة المعلوماتية بأنها كل سلوك أو نشاط غير مشروع يتعلق بنسخ أو تغيير أو حذف البيانات أو المعلومات المخزنة داخل النظام أو الوصول إليها أو تلك التي يتم تحويلها عن طريقه أو هي كل سلوك أو نشاط غير مشروع موجه إلى المعالجة الآلية للبيانات أو نقلها.

الطائفة الثالثة: حاولت الجمع بين الوسيلة التي يتم بها ارتكاب الجريمة ومحل أو موضوع هذه الجريمة، ومن ثم عرفت الجريمة المعلوماتية بأنها: " كل عمل غير قانوني أو كل سلوك غير مشروع يستخدم فيه الحاسب كأداة أو موضوع للجريمة أو هي كل فعل جنائي يكون الحاسب أداة أو موضوع للنشاط غير المشروع، أو هي كل فعل أو امتناع عن فعل من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية، أو التقنية المتقدمة لنظم التطورات.

الطائفة الرابعة: ويحاول أصحاب الطائفة الأخيرة، التركيز على شخص الجاني ومدى الدراية التقنية والفنية لنظم المعلومات، ومن ثم قامت بتعريف الجريمة المعلوماتية على أنها: " تلك الجريمة التي يقوم بها شخص لديه إلمام خاص بتقنيات الحاسب ونظم المعلومات. يراجع في ذلك: - د/ هشام محمد فريد رستم، قانون العقوبات ومخاطر المعلومات، أسيوط، مكتبة الآلات الحديثة، ١٩٩٢ ط ٢٩. ود/ محمود أحمد عباينة، جرائم الحاسوب وأبعادها الدولية، عمان، دار الثقافة والنشر والتوزيع، ط ٢٠٠٤، ص١٤، ود/ جواهر آل سعود، الحاسب الآلي أداة جريمة، بحث مقدم لمؤتمر الجرائم السيبرانية ومكافحتها، الرياض في ١٠ جمادي الأول ١٤٢٨ – عام ٢٠٠٩. ص ١٧، ١٨. وأ/ مصطفى السامر، الجريمة السيبرانية، بحث مقدم لمؤتمر حول الجرائم المرتبطة

خلال جزاء جنائي، سواء كانت هذه المصالح أو الحقوق المحمية جنائياً تمثل نماذج معلوماتية مستحدثة، أو كانت تدخل في نطاق المصالح أو الحقوق المحمية جنائياً فيما سبق بالطرق التقليدية وسواء كان الاعتداء واقعاً داخل حدود الدولة أو يتجاوزها إلى مجموعة من الدولة[1]. "

وقد ذهب مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا عام ٢٠٠٠ إلى تعريف الجريمة السيبرانية بأنها: " أي جريمة يمكن ارتكابها على نظام حاسوبي أو شبكة حاسوبية، وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"[٥].

ولعلنا نلاحظ أن هذا التعريف قد حاول الإحاطة بجميع الأشكال الإجرامية للجريمة السيبرانية، سواء تلك التي تقع بواسطة النظام المعلوماتي، أو داخل هذا النظام على المعطيات والبرامج والمعلومات، كما يشمل التعريف جميع الجرائم التي يمكن أن تقع في بيئة سيبرانية، فلم يحصر الجريمة المعلوماتية في مجال محدد حتى لا يتيح للعديد من الأفعال السيبرانية الإفلات من دائرة العقاب، ولعلنا نؤيد هذا التعريف نظراً لشموله لجميع أشكاله الجرائم السيبرانية.

بالإنترنت والحاسب الآلي، بالمعرض الرابع عشر لتكنولوجيا المعلومات والاتصالات، في ١٢ إلى ١٧ من شهر مايو ٢٠٠٨، ص ١ - ٢.

(١) انظر: د/ هلالي عبد اللاه أحمد، جرائم الحاسب والانترنت بين التجريم الجنائي وآليات المواجهة، مرجع سابق، ١١٧.

وأما الهجمات السيبراني: يمكن تعريفها بكونها: " فعلاً يقوض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف معينة تُمكن المهاجم من التلاعب بالنظام". (١)

كما عرفها 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. (٢)

وتجدر الإشارة إلى أن هناك فروق جوهرية بين الجريمة السيبرانية والهجمة السيبرانية (الحرب أو القوة السيبرانية) والذي يتمثل في الباعث، حيث أن الباعث على الهجمة السيبرانية يتمثل أساساً في إضعاف وظيفة شبكات الحاسوب المستهدفة في دولة أخرى' لتحقيق هدف سياسي، يضاف إلى ذلك أن القواعد القانونية التي تقرأ من خلالها الهجمات السيبرانية هي قواعد القانون الدولي العام، تحديداً قواعد اللجوء إلى استخدام القوة. (٣)

---

(١) Matthew C. Waxman، "Cyber-Attacks and the Use of Force: Back to the Future of Article 2 (4) " The Yale Journal of International Law، Vol. 36، 2011، P423

(٢) Michael N. Schmitt، " Computer Network Attack and THE USE OF Force IN International Law"، Thoughts on a Normative Framework"، Journal Columbia of Transnational Law 37، 1998، 885-937 ..

(٣) tin Roesler، When Do We Call a Cyber Attack an Act of Cyber War?، March 2013، P 15R

أما الجريمة السيبرانية تصدر عن جهة لا تمثل الدولة أو إحدى مؤسساتها، سواء كان شخصاً عادياً أو اعتبارياً، سعياً وراء هدف إجرامي يتحقق عند اختراق أجهزة إلكترونية معينة لأغراض شخصية، وهذا التصرف لا يرقى إلى مستوى الجريمة السيبرانية إلا إذا شكل جريمة وفقاً للقانون الجنائي الداخلي استناداً إلى مبدأ "لا جريمة ولا عقوبة إلا بنص" وهو أحد المبادئ الأساسية التي تقوم عليها أنظمة العدالة الجنائية. (١)

فضلا عن ذلك فإن الأضرار المحتملة لكل من الهجمة السيبرانية والجريمة السيبرانية تختلف بشكل كبير، على اعتبار أن الهجمة السيبرانية تهدف إلى إلحاق ضرر شامل سواء للأشخاص أو الممتلكات في الدولة الأخرى، وهو ما يختلف جذرياً عن الجريمة السيبرانية والتي ينحصر ضررها عموماً في مستخدمين معينين.

(١) يضاف إلى ذلك أن الباعث على هذا العمل يبقى دائماً باعثاً جنائياً بحتاً، إذ تجدر الإشارة أيضاً إلى أن التصرف الذي يعد جريمة سيبرانية لا يهدف أساساً إلى إضعاف الوظيفة التي تقوم بها الأجهزة السيبرانية المراد اختراقها، لأن هدف الفاعل من خلال استخدام الشبكة المعلوماتية يكون لأغراض محددة، واستخدام يساهم في الإبقاء على وظيفة الشبكة السيبرانية، علاوة على ذلك فإنه من مصلحة الجاني الإبقاء على النظام دون أي خلل حتى يحقق أكبر المكاسب التي تضاف إليه من خلال ارتكابه للجريمة وعدم لفت الأنظار إليه.

المطلب الثالث
طبيعة المخاطر السيبرانية وسماتها

المخاطر في حد ذاتها لا تتغير ولكن سماتها هي التي تتغير مع تطور الأدوات والوسائل المستخدمة، فقد أصبحت الدول تهتم بتكنولوجيا المعلومات ودورها في الصراعات والحروب المستقبلية استعدادا لمواجهة ما ينشأ عنها من مخاطر، والتي يتوقع الكثير حدوثها في الفضاء السيبراني، ولذا نجد أن هناك مناورات يتم إجراؤها للتدريب على هذا النوع الجديد من الصراع وكيف يمكن مواجهته والاستعداد له.

وبات من الصعب تخيل صراعاً عسكرياً اليوم دون أن يكون لهذا الصراع أبعاداً سيبرانية، وأصبحت في صلب اهتمامات الأنظمة الدفاعية لأي صراع يمكن أن يحدث في المستقبل، فالحرب التي تم شنها ما بين روسيا واستونيا عام ٢٠٠٧، وبين جورجيا وروسيا عام ٢٠٠٨، دفع العديد من الدول مثل الولايات المتحدة الأمريكية وغيرها من الدول الأخرى مثل الصين - على الرغم من التقدم التكنولوجي لها- ببناء وحدات إلكترونية على شبكات الانترنت، للحماية من مئات وآلاف القراصنة المحترفين [١].

بل يرى البعض أن الحروب السيبرانية أصبحت بديلاً لتلك الحروب التقليدية التي كانت تعتمد على جيوش عسكرية وأسلحة قتالية، فالحرب السيبرانية بالرغم من أنها حرب من دون نار أو قصف ولكن لها جانب عنيف

---

(١) انظر: د/ عباس بدران، الحرب السيبرانية: الاشتباك في عالم المعلومات، مركز دراسات الحكومة السيبرانية، بيروت، ٢٠١٠، ص ١١٠.

من حيث الاختراقات والقرصنة ونشر الفيروسات وغيرها من الأساليب، وبالرغم من فداحة الخسائر، فإن الأسلحة بسيطة لا تتعدى في أغلب الأحوال "الكيلو بايتس" والتي تتمثل في فيروسات إلكترونية تخترق شبكة الحاسب الآلي، وتنتشر بسرعة بين الأجهزة، وتبدأ عملها في سرية تامة وبكفاءة عالية. وتتميز هذه الحروب بالسرعة والدقة في تنفيذ العمليات العسكرية وتعتبر من أدوات الحرب الشاملة [١]، وهذه الحروب بعد أن كانت تستهدف أجهزة الإنترنت والحواسيب الآن تستهدف قطاعات وصناعات محددة [٢].

ويتميز الصراع السيبراني Cyber Conflict بأن به تدمير لا تصاحبه دماء وأشلاء بالضرورة، بل يتضمن التجسس والتسلل ثم النسف لكن لا دخان ولا أنقاض، ويتميز أطرافه بعدم الوضوح وتكون تداعياته خطيرة سواء عن طريق تدمير المواقع على الإنترنت ونسفها وقصفها بوابل من الفيروسات أو العمل على استخدام أسلحة الفضاء السيبراني المتعددة للنيل من سلامة تلك المواقع، وهي أسلحة يسهل الحصول عليها من خلال مواقع الإنترنت وتعلم

---

(١) جمال محمد غيطاس، الحرب وتكنولوجيا المعلومات، ط١ (القاهرة: دار نهضة مصر، ٢٠٠٦).

(٢) "الحروب السايبرية من الخيال إلى أرض الواقع"، مجلة درع الوطن:
http: //www. nationshield. ae/home/details/files/ .

كيفية استخدامها كما إن انتشار الفضاء السيبراني وسهولة الدخول إليه يمكن أن يوسع دائرة استهداف المواقع بالإضافة إلى زيادة عدد المهاجمين. (١)

وهناك صراع سيبراني تحركه دوافع سياسية ويأخذ شكلا عسكريا ويتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء الإلكتروني وذلك بهدف إفساد النظم المعلوماتية والشبكات والبنية التحتية وبما يتضمن استخدام أسلحة وأدوات إلكترونية من قبل فاعلين داخل المجتمع المعلوماتي أو من خلال التعاون ما بين قوى أخرى لتحقيق أهداف سياسية. (٢)

ويوجد صراع ذو طبيعة ناعمة عن طريق الصراع حول الحصول على المعلومات والتأثير في المشاعر والأفكار وشن حرب نفسية وإعلامية، ويتم أيضا من خلال تسريب المعلومات واستخدامها عبر منصات إعلامية بما يؤثر على طبيعة العلاقات الدولية كالدور الذي لعبه موقع ويكيليكس في الدبلوماسية الدولية. (٣)

---

(١) Jennie M. Williamson. " Information Operations: Computer Network Attack in the 21st Century"، Carlisle Barracks، PA، U. S. Army War College، 2002. pp 15

(٢) Myriam Dunn، " Information Age Conflicts: A Study of the Information Revolution and a Changing Operating Environment"، Center for Security Studies (CSS)، ETH Zurich، Issue No. 64، 2002.

(٣) انظر: د/ عادل عبد الصادق، موقع ويكيليكس وتحدي عالم الاستخبارات الأمريكي، ملف الأهرام الاستراتيجي، مركز الأهرام للدراسات السياسية والإستراتيجية، أكتوبر ٢٠١٠.

ويمكن أن يستخدم الفضاء السيبراني كوسيلة من وسائل الصراع داخل الدولة، بين مكوناتها على أساس طائفي أو اقتصادي أو ديني، وهو ما يساعد على كشف ديناميات التفاعل الداخلي إلى الخارج بما يسهل من عملية الاختراق الخارجي عبر شبكات الاتصال بدعم أحد أطراف الصراع بأدوات غير قتالية. (١)

وتعد الدولة الفاعل الرئيس في هذا العالم الافتراضي فهى من تمتلك القوة السيبرانية بامتياز لما لها من مقومات التفوق التكنولوجي بما يمكنها من قدرة كبيرة على تنفيذ هجمات سيبرانية وتطوير البنية التحتية وممارسة السلطات داخل حدوده. (٢)

وهناك أيضا من يمتلك القوة السيبرانية من غير الدول إلا أن قدرتهم على تنفيذ أي هجوم سيبراني مؤثر تتطلب مشاركة ومساعدة أجهزة استخباراتية متطورة، ولكن يمكنهم اختراق المواقع الإلكترونية واستهداف الأنظمة الدفاعية. ويمكن أن يكون مثال ذلك ما يلي: (٣)

---

(١) انظر: د/ عادل عبد الصادق، القوة الالكترونية " أسلحة الانتشار الشامل في عصر الفضاء الالكتروني"، المركز العربي لأبحاث الفضاء الإلكتروني، قضايا استراتيجية، ٢٠١٢.

(٢) انظر: د/ إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، المجلد ١٠، أبريل ٢٠١٩، ص ١٠١٦.

(٣) المرجع السابق، نفس الموضع.

- **الشركات المتعددة الجنسيات**: حيث تمتلك بعض شركات التكنولوجيا موارد للقوة تفوق قدرة بعض الدول، ولا تنقصها سوى شرعية ممارسة القوة التي ما زالت حكراً على الدول، فخوادم شركات مثل: جوجلGoogle، وفيسبوك Facebook ومايكروسوفت Microsoft، تسمح لها بامتلاك قواعد البيانات العملاقة التي من خلالها تستكشف وتستغل الأسواق، وتؤثر في اقتصاديات الدول وفي ثقافة المجتمعات وتوجهاتها.

- **المنظمات الإجرامية**: تقوم هذه المنظمات الإجرامية بعمليات القرصنة السيبرانية، وسرقة المعلومات واختراق الحسابات البنكية وتحويل الأموال، كما توجد سوق سوداء على الإنترنت المظلم لتجارة المخدرات والأسلحة والبشر.

- **الجماعات الإرهابية**: تعد من أبرز الفواعل الدولية، خاصة بعد أحداث ١١ سبتمبر، حيث تستغل الفضاء السيبراني في عمليات التجنيد والتعبئة والدعاية وجمع الأموال والمتطوعين، كما تحاول جمع المعلومات حول الأهداف العسكرية، وكيفية التعامل مع الأسلحة وتدريب المجندين الجُدد عن بعد، رغم أنها لم تصل بعد إلى مرحلة القيام بهجوم سيبراني حقيقي على منشآت البنية التحتية للدول.

- **الأفراد**: أصبح الفرد بفضل الفضاء السيبراني فاعلاً مؤثراً في العلاقات الدولية، ومن أبرز النماذج ظاهرة

الـويكيليكس "Wikileaks" [١] الـذي نجـح في نـشر ملايـين الوثـائق السرية لـلإدارة الأمريكيـة وقنـصلياتها، ممـا خلـق مـشاكل دبلوماسـية بـين الولايات المتحدة الأمريكية وحلفائها.

فمع ظهور تقنيات حديثة في تـداول المعلومـات والبيانـات وتقـدم وسـائل الاتـصالات، ودخـول تكنولوجيـا تقنيـة المعلومـات إلى كافـة صـور الحيـاة في مجتمعنا المعاصر، ظهر ما يسمى بالصراع السيبراني، الذي يرتكبـه فئـات معينـة مستخدمين في ذلك أدواته ووسائله الخاصة في تحقيق مقاصدهم.

ومـن ثـم يـتم تـسخير تكنولوجيـا تقنيـة المعلومـات في إحـداث مثـل هـذه الصراعات، وخطورة هذه الظاهرة أنه يسهل ارتكابها على الأجهزة الـسيبرانية أو من خلال الحواسيب المتصلة بالإنترنـت، كـما أن تنفيـذها قـد لا يـستغرق في بعض الأحيان إلا دقائق معدودة، أو أحياناً تتم بشكل لحظي، كما أن محـو آثـار

---

(١) ويكيليكس هي منظمة دولية غير ربحية تنشر تقارير وسائل الإعلام الخاصة والسرية من مصادر صحفية وتسريبات أخبارية مجهولة. بدأ موقعها على الإنترنت سنة ٢٠٠٦ تحت مسمى منظمة سن شاين الصحفية، وادعت بوجود قاعدة بيانات لأكثر من ١.٢ مليون وثيقة خلال سنة من ظهورها. وتصف ويكيليكس مؤسسيها بأنهم مزيج من المنسقين الصينيين والصحفيين والرياضيين وتقنيون مبتدؤون لشركات عاملة في الولايات المتحدة وتايوان وأوروبا وأستراليا وجنوب أفريقيا. ومديرها جوليان أسانج وهو ناشط إنترنت.

https: //ar.wikipedia.org/wiki/ ويكيليكس

الجريمة أو إتلاف أدلتها غالباً ما يلجأ إليه الجاني عقب ارتكابه للجريمة، مما يثير مشكلات كبيرة في جميع الأدلة الجنائية أو في إثبات هذه الجرائم قبلهم. [1]

ولا يكفي لمجابهة ومواجهة هذه الظاهرة بحث سبل توفير وسائل تكنولوجية وبرامج حاسوبية لحماية البيانات وتوفير أمن المعلومات المخزنة إلكترونياً، بل يجب تكثيف الجهود لتنمية الحماية لمقدرات الدول وحماية بياناتهم ومعلوماتهم، وكذلك لتتمة الحماية لحرمة حياتهم الخاصة والحيلولة دون السماح لهؤلاء المجرمين من الدخول غير المشروع إلى أجهزة وحواسيب أفراد المجتمع مما يسمح لهم من الوصول إلى بياناتهم أو المعلومات المخزنة على هواتفهم المحمولة أو حواسيبهم، وابتزازهم بها لتحقيق منافع غير مشروعة وتهديد أمنهم وسلامتهم.

فالمخاطر السيبرانية ذات أثر غير مادي –غالبا-: إذ تعد نتاجاً لتقنية المعلومات وهو ما أكسبها طابعاً خاصاً يميزها عن غيرها من الجرائم التقليدية[2] حيث لا تترك

---

(١) انظر: د/ راشد محمد المري، الجرائم السيبرانية في ظل الفكر الجنائي المعاصر دراسة مقارنة، ص ٢٩٦، ط دار النهضة العربية ودار النهضة العلمية بالإمارات عام ٢٠١٨.

(٢) انظر: د/ محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات – دار النهضة العربية، ط٢، ١٩٩٨، ص٥٦.

أي أثراً مادياً، وإنما معلومات يمكن شطبها فور تنفيذ الجاني لفعله السيبراني[١].

ومن ثم فهي ترتكب في نطاق تقنية وتكنولوجيا متقدمة يتزايد استخدامها يوماً بعد آخر في إدارة مختلف المعاملات الاقتصادية والمالية حيث تمس هذه الجرائم المركز الحسابي والإداري وتنقلات الأموال والاستثمارات سواء في المنشآت العامة أو الخاصة، وقد تهدد هذه الاعتداءات مباشرة قدسية وسرية الحياة الخاصة أو الحرية السياسية، ناهيك عن الخطورة التي تشكلها هذه الجرائم إذا ما تعلقت بالمعلومات الخاصة بإدارة الدولة وعمل الحكومة وخاصة في ميادين الأمن والدفاع والمشروعات النووية والتصنيع الحديث للأسلحة، ويبدو أن هذه المعلومات هي الأكثر رواجاً في سوق (المعلومات السوداء)[٢].

ارتكاب الجرائم السيبرانية في مراحل تشغيل نظام المعالجة الآلية للبيانات:على الرغم من إمكانية ارتكاب الجريمة السيبرانية في أية مرحلة من مراحل تشغيل نظام المعالجة الآلية للبيانات في الحاسب الآلي (الإدخال – المعالجة – الإخراج)، غير أن لكل مرحلة من هذه المراحل نوعية خاصة من الجرائم لا يمكن بالنظر لطبيعتها ارتكاب الجريمة السيبرانية إلا في وقت محدد

---

(١) انظر: د/ مصطفى، خالد حامد أحمد، السيبرانية والمسؤولية الجزائية، محل الفكر الشرطي مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات، مجلد ٢٠، عدد ٧٩، دار المنظومة، ص ١٥٩.

(٢) انظر: د/ محمد سامي الشوا ــ، ثورة المعلومات وانعكاساتها على قانون العقوبات،مرجع سابق. ص٦٧.

يعتبر هو الأمثل بالنسبة لمراحل التشغيل، ففي مرحلة الإدخال حيث تترجم المعلومات إلى لغة مفهومة من قبل الآلة، يسهل إدخال معلومات غير صحيحة أو إدخال غير الوثائق الأساسية والمعلومات المطلوبة، ومن هذه المرحلة يتم ارتكاب أكثر الجرائم السيبرانية.

أما في مرحلة المعالجة الآلية للبيانات فيمكن إدخال أي تعديلات على برامج الحاسب الآلي تحقق الهدف الإجرامي عن طريق التلاعب في برامج النظام المعلوماتي كدس تعليمات غير مصرح بها أو تشغيل برامج جديدة تلغي كلياً أو جزئياً عمل البرامج الأصلية، وتتطلب الجرائم المرتكبة في هذه المرحلة معرفة فنية عميقة لدى الجاني بتلك التقنية، كما أن اكتشافها يكون صعب للغاية، وكثيراً ما تقف الصدفة وراء اكتشافها. بينما في المرحلة الأخيرة المتعلقة بالمخرجات وفيها يقع التلاعب في النتائج التي يخرجها النظام المعلوماتي بشأن بيانات صحيحة أدخلت فيه وعالجها بطريقة صحيحة[1].

وقوع الجريمة في بيئة المعالجة الآلية للبيانات والمعلومات: ويشترط لقيام الجريمة السيبرانية في هذه المرحلة التعامل مع بيانات مجمعة ومجهزة للدخول للنظام المعلوماتي وذلك من أجل معالجتها إلكترونياً بما يمكن المستخدم من إمكانية كتابتها من خلال العمليات المتبعة والتي يتوافر فيها إمكانية تصحيحها أو تعديلها أو محوها أو تخزينها أو استرجاعها أو طباعتها وهذه العمليات

(١) انظر: د/ حاتم عبد الرحمن منصور الشحات ـ الاجرام المعلوماتي ـ دار النهضة العربية ـ القاهرة ط١ ـ ٢٠٠٣ ـ ص٣٧ وما بعدها .

وثيقة الصلة بارتكاب الجرائم السيبرانية، ولابد من فهم وإتقان الفاعل لها أثناء ارتكابها وخاصة في جرائم التزوير والتقليد[١].

فضلا عن ذلك فالجرائم السيبرانية جرائم عابرة للحدود الوطنية: الجرائم السيبرانية جرائم غير إقليمية في أغلب الأحيان، مما يؤدي إلى توزيع أركانها على عدة دول، كما أن أدلة إثباتها يسهل طمثها ومحوها، مما يجعل هناك صعوبة قائمة ضد القوانين الوطنية التقليدية في مواجهة هذا النوع من الجرائم، وهذا ما جعل المجتمع الدولي يتجه نحو إنشاء أجهزة تعاونية تعمل على مستويات حكومية أو غير حكومية من أجل ضمان التنسيق والمتابعة فيما يتخذ من تدابير دولية وداخلية لوضع الالتزام الدولي بالتعاون موضع التنفيذ الإيجابي والمتكامل.

وقد ثار التساؤل عما إذا كانت المعرفة العلمية والتكنولوجية متعلقة بالنطاق الجغرافي لإحدى الدول، أو بقطاع علمي أو إنتاجي معين، أم أنها معرفة عالمية ولا تعرف تمييزاً بين فروع العلم أو قطاعات الإنتاج.

وقد أجابت على هذه التساؤلات محكمة العدل الأوربية في حكمها الصادرة في ٢٩/ ٥/ ١٩٩٧، حيث انتهت المحكمة إلى تحديد مخاطر التطور بوصفها المعرفة العلمية والتكنولوجية على مستوى العالم، وليس فقط على مستوى دولة معينة، أو بصدد قطاع صناعي أو إنتاجي معين ولا يقف الأمر

---

(١) د/ أحمد خليفة الملط - المرجع السابق - ص١٠٥.

عند حد ما وصل إلى علم المنتج، ولكن يجب أن يقاس بمدى ما كان يجب أن يعرفه المنتج، أي أن المعيار موضوعي.

كما تواجه الأسلحة السيبرانية بمشكلات في استخدامها حيث تكون هجماتها عشوائية وذلك لانطلاقها عبر الحدود الدولية بما قد يعمل على الإضرار بطرف ثالث وبأمن الفضاء السيبراني بشكل عام. ويمكن أن ينمو سوق لتجارة الأسلحة السيبرانية تنافس قدرات الدول والتي يتم فيها توظيف المجرمين أو القراصنة أو المتطوعين بما يعمل على سرعه انتشارها ويفاقم من تأثيرها ويحد من قدرة الدول على تنظيم استخدام القوة عبر الفضاء السيبراني. (١)

المطلب الرابع
صور المخاطر السيبرانية

معظم دول العالم أصبحت الآن تلجأ إلى نظام الإدارة السيبرانية – في كافة المجالات الاجتماعية والاقتصادية والعسكرية وغيرها – والتي تقوم على فكرة إحلال العمل السيبراني محل الورقي أو التقليدي في كافة جهات الإدارة تماشياً مع التطور القائم من حولها في العالم.

---

(١) حيث جاءت نسبة الإصابة في إيران و الهند في المرتبة الأولى والثانية واندونيسيا في المرتبة الثالثة من البلدان التي تمكن فايروس Stuxnet التغلل في نظم معلومات منشاتها الصناعية.

انظر: د/ عادل عبد الصادق، القوة الالكترونية: أسلحة الانتشار الشامل في عصر الفضاء الالكتروني، مرجع سابق، ص ١٤.

ومن ثم فإن جوهر النظام الجديد يقوم على فكرة نقل كافة البيانات والخدمات بالدولة من واقعها التقليدي أو الورقي إلى الواقع الجديد والمتمثل في المجتمع السيبراني عبر الإنترنت بصورة تؤدي إلى القضاء على العيوب التي لازمت النظام القديم لاسيما القضاء على الإجراءات الروتينية المعقدة والطويلة التي تلازم المعاملات الورقية وإنجازها، وذلك بالنفاذ إلى إجراءات إلكترونية دقيقة تسير بسرعة عالية وفائقة وتؤدي بذلك إلى تنمية الواقع العملي بالدولة والنهوض به إلى أفضل مستوى.

وبالنظر إلى عنصر الإتاحة الكبير الذي تقدمه هذه التكنولوجيا للمجتمع من إمكانية استخدام أدواتها ووسائلها ووسائطها بكل سلاسة وسهولة سواء داخل المجتمع أو خارجه بفضل الميدان الافتراضي لعمل تلك التقنيات الحديثة، وإتاحة استخدام تلك التكنولوجيا بلا أي حدود ولا رقابة أدى إلى ظهور أفعال تستهدف أمن وسلامة المجتمعات مما يشكل مخاطر لابد من إيجاد السبل واتخاذها لمواجهة هذه المخاطر.

فالصراع السيبراني يتمثل في استخدام تقنيات الحاسوب لتخريب أو تهديد نشاطات دولة أو منظمة دولية، وبخاصة الهجوم على نظم المعلومات الخاصة، وذلك لغايات استراتيجية أو عسكرية.

فالهجوم الافتراضي يتم بدوافع سياسية على أجهزة العدو السيبرانية وشبكات الإنترنت وأنظمة المعلومات الخاصة به، لتعطيل منظوماته في كافة المجالات، وذلك من خلال سرقة قواعد معلوماته السرية أو تخريبها أو تعطيلها أو تعديلها لتقويض الشبكات العنكبوتية والمواقع ونظم الخدمات.

وسوف نبين أهم الصور التي يمكن أن تشكل مخاطر سيبرانية وذلك على النحو التالي: -

الفرع الأول
الاختراقات السيبرانية

لم تعد القرصنة تتم بصورتها التقليدية، بل استفاد القراصنة من وسائل وتقنيات المعلومات حيث أصبح الجناة بفضل تلك التقنيات يرتكبون جرائم القرصنة بصور مستحدثة من خلال العثور على مواقع الإنترنت لترويج البرامج المقرصنة مجاناً أو بمقابل مبلغ رمزي، مما ألحق العديد من الخسائر المادية الباهظة بالشركات المتخصصة في صناعة البرامج، ودعى هذه الشركات إلى إنشاء منظمة خاصة لمراقبة وتحليل ما يعرف بسوق البرمجيات، ومنها منظمة اتحاد برمجيات الأعمال التي تجري دراسات حول هذا وتتبنى الحلول المناسبة.

والقرصنة السيبرانية تتمثل في عملية نسخ البرمجيات غير المصرح به، أو إعادة إنتاجها، أو استخدامها أو تصنيع نسخ بطريقة غير شرعية أو نشر وتوزيع المنتج البرمجي أو استغلاله على نحو مادي أو تقليدها أو محاكاتها والانتفاع بها على نحو يخل بحقوق الدول والمؤسسات بدون الحصول على إذن أو تفويض.[1]

---

(١) انظر: د/ خالد مصطفى فهمي، الحماية القانونية لبرامج الحاسب الآلي في ضوء قانون حماية الملكية الفكرية طبقا لأحدث التعديلات "دراسة مقارنة"، ٢٠٠٥، بدون ناشر، ص ٢١٠.

ويستطيع قراصنة الحاسب الآلي (Hackers) التوصل إلى المعلومات السرية والشخصية، واختراق الخصوصية وسرية المعلومات بسهولة، وذلك راجع إلى التطور المذهل في عالم الحاسب الآلي والشبكات المعلوماتية وما صحبه من تقدم في الجرائم المعلوماتية وسبل ارتكابها، فضلا عن أن مرتكبيها ليسوا مستخدمين عاديين، بل لديهم خبرة فائقة في مجال الحاسب الآلي.

ونظرا لأهمية التوصل إلى حلول لظاهرة قرصنة البرمجيات كان هناك توجه عالمي بإنشاء منظمات عالمية تتابع تتطور هذه الظاهرة في جميع دول العالم إضافة إلى اقتراح الحلول المناسبة. وأبرز هذه المنظمات اتحاد صناعة البرمجيات والمعلومات(SIIA) الذي يبحث في طرق حماية الملكية الفكرية المعلوماتية، واتحاد برمجيات الأعمال(BSA) المدعوم من شركات البرمجيات الكبرى والذي يسعى إلى خلق مجتمع رقمي آمن، واتحاد البرمجيات الرقمية التفاعلية(IDSA) المعني بمحاربة أنظمة المحاكاة غير الشرعية كالأنظمة التي تسمح مثلا بتشغيل برمجيات أنظمة playstation بواسطة الكمبيوتر الشخصي بصورة غير قانونية. (١)

ويمكن أن تتخذ الاختراقات السيبرانية إحدى الصور الآتية:

أ- اختراق المواقع والصفحات السيبرانية على الإنترنت وتدميرها، أو إلغائها، أو إتلافها، أو التعديل والعبث بالبيانات والمعلومات المتوفرة عليها.

---

(١) انظر: د/ عماد محمد سلامة، الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنة البرامج. دار وائل للنشر، ٢٠٠٥، ص ٦٥.

ب- شغل العنوان (الرابط) السيبراني للموقع أو تحويله لعنوان موقع آخر على الإنترنت.

ت- اختراق البريد السيبراني للأخرين والاستيلاء عليه واستخدامه في انتحال شخصية الغير.

ج- اختراق قواعد البيانات وحذف أو تعديل المعلومات الموجودة عليها، أو الاستيلاء على المعلومات المتوفرة عليها كأسماء المستخدمين وأرقامهم السرية وعناوين الاتصال الخاصة بهم واستخدامها لأغراض غير مشروعة أو بيعها إلى جهات مستفيدة (جهات اقتصادية وتجارية أو سياسية، أو أمنية).

وينشط دور القراصنة في التعبير عن المواقف السياسية بقيامها بهجمات على مواقع حكومية مثل جماعة ويكيليكس و أنونيموس[1] والتي أصبحت تهدد شركات ودولا بالاختراق. وقد تم استخدام هذه الاختراقات في الفضاء السيبراني في إطار الصراعات بين الدول، كما حدث بين إستونيا وروسيا في عام

---

(١) مجموعة دولية من نشطاء القراصنة الذين يرفضون الكشف عن أسمائهم ويدعون أنهم ليسوا شخصًا واحدًا بل عدة أشخاص من مختلف دول العالم فعناصر التحكم في Anonymous لامركزية، ولا يوجد لدى المجموعة قيادة معلنة وأعضائها غير معروفين، بدأت المجموعة في عام ٢٠٠٣ على chan٤، وهو موقع ويب باللغة الإنجليزية، وتطلق المجموعة هجمات إلكترونية ضد الحكومات والمؤسسات والشركات والأشخاص من مختلف دول العالم، وأيقونة المجموعة أو شعارها عبارة عن قناع، حيث يستخدم الأعضاء قناع جاى فوكس، الذى اشتهر برواية وفيلم " V for Vendetta". . https: ///ar. wikipedia. org/wiki _ (مجموعة أنونيموس) .

٢٠٠٧، والاختراقات المتبادلة بين الصين والولايات المتحدة أو ما بين كوريا الجنوبية. [١]

ويمثل النموذج الإيراني حالة فريدة لتحول الفضاء السيبراني لساحة قتال ذي طابع مرن وآخر ذي طابع صلب [٢] وذلك في إطار المواجهة بين إيران وإسرائيل والولايات المتحدة والتي منها استخدامه في تحريك القوه الناعمة داخل إيران بدعم الاحتجاجات في عام ٢٠٠٩، وتقديم دعم فني للمعارضة عقب الانتخابات الرئاسية، وفي نهاية ٢٠١١ دشنت الولايات المتحدة "سفارة إلكترونية" لتزويد الإيرانيين بالمعلومات حول التأشيرات عبر الإنترنت، والتواصل مع الطلاب الإيرانيين وهو ما يلائم عملية قطع العلاقات الدبلوماسية بين إيران والولايات المتحدة منذ ثلاثين عاما[٣]. وهو ما دفع إيران

---

(١) David E Sanger، Confront and Conceal Obama's Secret Wars and Surprising Use of American Power، New York Crown2012: 188

" Ralph Langner Cracking Stuxnet A 21 Century Cyber Weapon، TED.
www: //http. ted. com. /talk/ ralph cyberweapon_ A_21 century st_ langner _ cracking _ stuxnet _ cyberweapon

للمزيد: انظر: د/ عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، وحدة الدراسات المستقبلية، مرجع سابق، ص ٤٣.

(٢) انظر: د/ عادل عبد الصادق، الإنترنت والدبلوماسية ومعركة القوة الناعمة بين الولايات المتحدة وإيران، مختارات إيرانية، مركز الأهرام للدراسات السياسية والاستراتيجية، نوفمبر ٢٠١١.

(٣) U. S. launches 'virtual' embassy for Iran، us today، 12/6/2011

إلى حجب موقع السفارة وتجريم محاولة الدخول عليها على أنها تمثل تهديدا للأمن القومي لديها. [١]

هذا إلى جانب التعرض إلى القوة الصلبة عبر الفضاء السيبراني عبر شن هجمات التخريب للبرنامج النووي للعمل على تعطيله وكان آخر الهجمات في ١٧ فبراير ٢٠١٢ حين أعلنت الاستخبارات الإيرانية أن فيروس ستاكسنت [٢] أصاب ما يقدر بستة عشر ألف جهاز كمبيوتر [٣] و تبنت إسرائيل شن هجمات ستاكسنت بالتعاون مع الولايات المتحدة للعمل على تعطيل المنشآت

---

http: //www. usatoday. com/news/washington/story/2011-12-06/us-embassy-iran/51673966/1

(١) انظر: د/ عادل عبد الصادق، المرجع السابق.

December ،the new York times ،Iran Blocks American 'Virtual Embassy

http: //thelede. blogs. nytimes. com/2011/12/07/iran-blocks-2011 ،7

/american-virtual-embassy

(٢) عبارة عن برنامج كومبيوتر خبيث يهاجم أنظمة التحكم الصناعية المستخدمة على نطاق واسع في مراقبة الوحدات التي تعمل آليا، يقوم بعد اختراق الأجهزة والحواسيب بالتفتيش عن علامة شركة "سيمنز الألمانية"، ليبدأ بالعمل على تخريب وتدمير التقنيات الذكية. . . المجال الخامس. . . الحروب الإلكترونية في القرن الـ٢١، مركز الجزيرة للدراسات، على الرابط

http: //studies. aljazeera. net/ar/issues/2010/20117212274346868. html

(٣) Iran says Stuxnet virus infected 16،000 computers ،fox news ،

Published February 18 2012 ،Read more: http: //www. foxnews. com/world/2012/02/18/iran-says-stuxnet-virus-infected-16000-computers/#ixzz1ntBzAB47

النووية [١] ويمثل ذلك جزءا من منصة لإطلاق الفيروسات الخطرة، تم تطويرها عام ٢٠٠٧. وتمت تجربته في إسرائيل. [٢]

وأصبحت الفيروسات [٣] إحدى الوسائل المهمة في الأمن السيبراني، ورغم وجود برامج للحماية من الفيروسات، إلا أنها لا تستطيع حماية جميع الأجهزة، والبرمجيات، من الهجمات السيبرانية المعقدة، والتي تعتمد علي ثغرات أمنية في البرمجيات، والأنظمة، قد لا يعرفها بالأساس مصممو هذه

---

(١) انظر: د/ عادل عبد الصادق، أمريكا وتشكيل قيادة عسكرية في الفضاء الإلكتروني. هل بدأ الاستعداد لحروب المستقبل؟ تعلقيات مصرية، مركز الأهرام للدراسات السياسية والاستراتيجية، العدد١٣٠، ١٢ يوليو٢٠٠٩

.http: //acpss. ahram. org. eg/Ahram/2009/7/12/COMM0. HTM

Robert McMillan ، ،Was Stuxnet Built to Attack Iran's Nuclear Program ،؟pc world ،Sep 21

//www.pcworld.com/businesscenter/article/205827/was_stuxnet_built_to_attack_irans_nuclear program. html

(٢) William. J. BROAD ،JOHN MARKOFF and DAVID E. SANGER ، Israeli Test on Worm Called Crucial in Iran Nuclear Delay ،the New York times ،January 15 ،2011.

http: //www. nytimes. com/2011/01/16/world/middleeast/16stuxnet. html?_r=1&pagewanted=all

(٣) الفيروسات: هي برامج خبيثة تقوم بنسخ نفسها على أجهزة المستخدمين من غير معرفتهم وتسعى إلى إحداث خلل أو تدمير في ملفات أو جهاز المستخدم.

السياسات الوطنية لأمن وحماية المعلومات، إعداد: اللجنة الوطنية الفنية لأمن وحماية المعلومات، الحكومة السيبرانية الأردنية (٢٠٠٨).

البرمجيات، والأنظمة، قد لا يعرفها بالأساس مصممو هذه البرمجيات. ومن أمثلة هذه الفيروسات، فيروس ستاكس نت عام ٢٠١٠، وشمعون[١]، حشرة الحب، الفدية Ronmsoware [٢].

---

(١) من أخطر الفيروسات هجومًا على الحواسيب، ويستهدف أكبر الشركات والجهات الحكومية حول العالم، وصممت النسخة الثانية منه لاستهداف الأجهزة العاملة بنظام ويندوز، وتهدف الهجمة السيبرانية إلى تعطيل الخوادم والأجهزة للمنشآت، بحيث يؤثر على جميع خدماتها المقدمة، يعمل الفيروس على حذف محتويات الأقراص الصلبة، ويتسبب بتعطيل أجهزة الكمبيوتر المصابة به عن طريق استبدال ملفات أساسية لتشغيله واستبدالها بملفات خاصة به، مما يتسبب بعدم قدرة الجهاز على الإقلاع، ويتكون الفيروس من مجلد بحجم ٩٠٠ كيلوبايت يحتوي على عدد من المصادر المشفرة، تم اكتشاف الفيروس في عام ٢٠١٢ بواسطة شركة سيمانتيك، وهاجم في البداية شركة رأس غاز القطرية وشركة أرامكو السعودية، مما أدى لتعطيل حوالي ٣٠ ألف حاسب وتسبب بخسائر بملايين الدولارات، وأدى تعطيل إنتاج النفط عبر أربع قارات في العالم. للمزيد انظر: " عوامل اقتصادية وسياسية وراء الهجمات السيبرانية على الخليج"، مصر العربية: http: //www. masralarabia .com.

(٢) يعمل على تشفير بيانات المستخدم في شركة ما ويجبر أصحاب الشركة من أجل استعادة البيانات دفع رسوم ويمكن له ان يصيب منظمة بأكملها ويتضمن دفع الرسوم الكترونياً مثل بيتكوين BTC، وهناك آلاف الضحايا لهذا الفيروس في مدرسة نيوجيرسي وفى ولاية ماين، وشيكاغو وماساتشوستس، للمزيد أنظر:

Ronsomware، " hostage rescue manual "، know BE. "، Alessandrini، Adam

الفرع الثاني
التجسس السيبراني

تعتبر هذه الجريمة من أخطر الجرائم السيبرانية فهي نتاج ما أسفر عنه التقدم العلمي والتكنولوجي الحديث في شأن أجهزة التصنت الحديثة ذات القدرة الفائقة والدقة البالغة في أعمال التجسس حيث تهدف إلى جمع المعلومات العسكرية أو السياسية أو حتى جمع المعلومات غير العسكرية كجمع تلك المتعلقة بالمجال الاقتصادي والتجاري أو المجال الثقافي.

والتجسس قد يهدف إلى تعطيل عمل الشبكات العنكبوتية وحواسيبها، وأنظمتها بهدف سرقة معلومات سرية سياسية، أو عسكرية أو مالية من دولة ونقلها إلى دولة أخرى.

ولا شك أن التجسس المعتمد على المجال السيبراني يؤثر سلبًا - سواء على المستوى الاستراتيجي أو التشغيلي- على المعلومات وأنظمة المعلومات، مما يتيح إمكانية تسريب أسرار ومعلومات حساسة للدول الأخرى.

وساعد في ظهور هذا النوع من الجرائم خصوصاً إلى ما بعد أحداث الحادي عشر من سبتمبر التي شهدتها الولايات المتحدة الأمريكية، حيث تعمد بعض الحكومات إلى استخدام تقنية المعلومات لإدارة أعمال التجسس ضد الأهداف التي قد تشكل خطراً مستقبليا على بلادها سواء أكانت تلك الأهداف أفرادا أو مؤسسات عسكرية كانت أو مدنية، فعلى سبيل المثال: فقد أعلن أمين مجلس الأمن الروسي (نيكولاي باتروشيف) في ٢٦/ ٨/ ٢٠١٥ على العثور على برامج تابعة للاستخبارات الأجنبية في نظم المعلومات

للمؤسسات الحكومية الروسية وأكد على تزايد حالات التجسس على نظم المعلومات الحكومية.[١]

وفي واقعة مماثلة قامت شبكة دولية ضخمة للتجسس السيبراني تعمل تحت إشراف وكالة الأمن القومية الأمريكية بالتعاون مع أجهزة الاستخبارات في كندا وبريطانيا برصد المكالمات الهاتفية بهدف التعامل مع الأهداف غير العسكرية، ولا يقتصر الرصد على المحطات الموجهة إلى الأقمار الصناعية والشبكات الدولية بل يشمل الاتصالات التي تجري عبر أنظمة الاتصالات الأرضية.[٢]

وتجدر الإشارة إلى أن التجسس السيبراني يعتبر من الأساليب التي تلجأ إليها التنظيمات الإجرامية والإرهابية لجمع معلومات حول المؤسسات والقطاعات الحكومية، العسكرية والسياسية والاقتصادية، ليتم استخدامها من أجل الإضرار بالمجتمع ومصالحه، وهو ما يهدف إليه الإرهاب في عمومه. ويعرف البعض التجسس السيبراني على أنه "عدة طرق لاختراق المواقع السيبرانية، ومن ثم سرقة بعض المعلومات والتي قد تكون في غاية الأهمية والخطورة للطرف المتلقي والمسروق منه".

فعمل أجهزة الاستخبارات السيبرانية لا يقتصر علي وجهة النظر الرسمية للدول والحكومات، بل تعدي ذلك لدور الأفراد في إنتاج المعلومات

---

(١) عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت. دون ذكر دار النشر ص ٣٨٢.

(٢) عبد الفتاح بيومي حجازي،الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية – ٢٠٠٧، ص ٢٩.

وترويجها، وفي توافر كم هائل للتحليلات السياسية والاقتصادية مع تعدي الحدود الدولية وشكل ذلك ثورة معلوماتية هائلة لا حدود لها عكفت عليها أجهزة الاستخبارات الكبرى للحصول عليها أولا، والبحث فيها ثانيا، وتوظيف نتائجها ثالثا. (١)

ومن الجهود التي بذلت لمكافحة هذا النوع من الإجرام - على الصعيد التقني - ولحماية المعلومات التي تتعرض لأعمال التجسس السيبراني، العمل على تشفير البيانات وإخفائها، والاهتمام ببروتوكولات الحماية، ونظم منع المتطفلين، وتشير تلك الجهود أيضاً إلى أن أهداف وطرق الحماية تتمثل في أمرين:

الأول: هو "الوثوقية" بمعنى الاحتفاظ بسرية المعلومات قبل الجميع، باستثناء الذين لديهم صلاحية للاطلاع عليها.

الثاني:هو "تكامل البيانات" بمعنى التأكد من أن المعلومات لم تتغير من قبل أشخاص غير مخولين لذلك، والتحقق من الشخصية.(٢)

---

(١) انظر: د/ عادل عبد الصادق، الإنترنت والاتصالات "ساحة جديدة للتجسس الدولي "، مقالات، المركز العربي لأبحاث الفضاء الإلكتروني، ٢٧ أغسطس ٢٠١١. http: //www. accr. co/?p=341.

(٢) انظر: د/ مصطفى جاد، مقال بعنوان "مستقبل الإرهاب السيبراني"، في ندوة نظمها المركز الدولي للدراسات المستقبلية والاستراتيجية في ١١ أبريل ٢٠١٢، جريدة السياسة الدولية التابعة لمؤسسة الأهرام، إعداد / شريهان نشأت المنيري، على الموقع السيبراني:

http://www.siyassa.org.eg//newsContent/6/51/2450

والتجسس السيبراني قد يتم عن طريق اختراق المواقع والصفحات السيبرانية على الإنترنت بغرض التجسس أو التنصت على ما تحتويه من بيانات ومعلومات (نصية، أو صوتية، أو مرئية) تهم الجهة المستفيدة من التجسس (جهات اقتصادية وتجارية، أو سياسية، أو أمنية).

أو يتم عن طريق إرسال رسائل بريدية إلكترونية لمستخدمي الإنترنت تتضمن ملفات برمجية لديها القدرة على الإرسال بشكل آلي للمعلومات المتوفرة على جهاز المستخدم من ملفات (نصية، أو صوتية، أو مرئية). كما لديها القدرة على إرسال أي معلومات تتعلق بمستخدم الإنترنت مثل سجل زياراته لمواقع الإنترنت والبيانات التي يدخلها المستخدم في مواقع الإنترنت كاسم المستخدم وكلمة السر، بالإضافة إلى كلمات البحث التي يدخلها المستخدم في محركات البحث العالمية.

ومن أهم ما يندرج تحت مسمى جرائم التجسس السيبراني[1] ما يلي:

- جرائم التجسس الاقتصادية والتجارية: وهي جرائم التجسس التي يكون الهدف منها الحصول على معلومات اقتصادية وتجارية. ويعد التجسس الصناعي نوعا من التجسس ينفذ لأغراض تجارية وتقوم به بعض الشركات والمؤسسات التجارية بهدف الحصول على أسرار صناعية من الشركات المنافسة، وهذا النوع من

(١) انظر: د/ ممدوح عبد الحميد عبد المطلب – جرائم استخدام شبكة المعلومات – الجريمة عبر الإنترنت، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات عام ٢٠٠٠، ص٢٠.

التجسس غالباً ما يرتبط بالصناعات التقنية، مثل البرمجيات والتقنية الحيوية، وتقنيات الفضاء والاتصالات والمواد والطاقة.

٢-جرائم التجسس العسكرية والأمنية والسياسية: وهي جرائم التجسس التي يكون الهدف منها الحصول على معلومات عسكرية أو أمنية أو سياسية.

جرائم التجسس الثقافية والتعليمية: وهي جرائم التجسس التي يكون الهدف منها الحصول على معلومات ثقافية وتعليمية. ومن أمثلتها التجسس على الأبحاث والمخترعات والدراسات العلمية والتعاون الثقافي والتعليمي بين الدول.

وقد أعلن أمين مجلس الأمن الروسي (نيكولاي باتروشيف) في ٢٦/ ٨/ ٢٠١٥ عن العثور على برامج تابعة للاستخبارات الأجنبية في نظم المعلومات للمؤسسات الحكومية الروسية وأكد على تزايد حالات التجسس على نظم المعلومات الحكومية.

الفرع الثالث
الإرهاب السيبراني

الإرهاب السيبراني هو استخدام شبكات المعلومات والكمبيوتر من أجل التخويف والإرغام لتحقيق أهداف سياسية، حيث تقوم الجماعات الإرهابية بالتهديد عبر وسائل الاتصالات من خلال الشبكة العالمية للمعلومات، وتتعدد أساليب التهديد وتتنوع طرقه، وذلك من أجل نشر الخوف والرعب بين الأشخاص والدول والشعوب ومحاولة الضغط عليهم للرضوخ لأهداف

تلك التنظيمات الإرهابية من ناحية، ومن أجل الحصول على التمويل المالي أو إبراز قوة التنظيم الإرهابي من ناحية أخرى.(١)

وقد ذهب البعض إلى تعريف الجريمة الإرهابية السيبرانية بأنها:" أي نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإرهابي المقصود".(٢)

وذهب رأي آخر في تعريفة للإرهاب السيبراني الدولي بأنه" استخدام الاتصالات الهاتفية ونظم المعلوماتية ومواردها أو التأثير عليها في مجالات المعلوماتية الدولية بهدف القيام بأعمال إرهابية".(٣)

وعرفه مكتب الأمم المتحدة المعنى بمكافحة الإرهاب CTITF بأنه:" عمل يرتكب من خلاله هجمات إرهابية عن طريق التغيير عن بعد معلومات وأنظمة الكمبيوتر أو تعطيل تدفق البيانات بين أنظمة الكمبيوتر.(٤)

---

(١) THE NEW ،TERROR ON THE INTERNET: THE NEW ARENA ،CHALLENGES ،UNITED STATES INSTITUTE OF PEACE PRESS .2006. Page. 243-249

(٢) د/ عبد الفتاح بيومي حجازي، الأحداث والإنترنت مرجع سابق ص ١٧.

(٣) د/ محمد البخاري طشقند، الإنترنت ومبادئ الأمن المعلوماتي الدولي "الثورة المعلوماتية فجرت الحواجز القائمة بين الشعوب والدول" بحث منشور على شبكة ضياء للمؤتمرات والدراسات في ٢٩/ ٧/ ٢٠١١ على الموقع الإلكتروني.

(٤) CTITF. Countering the use of internet for terrorism purposes, working group report, CTITF publications Series, Feb 2009

كما عرف مشروع مدونة اتفاقية ستانفورد لتعزيز الحماية من الإرهاب السيبراني عام ٢٠٠٠م أنه "الاستخدام العمدي أو التهديد باستخدام بدون إذن من سلطة معترف بها قانوناً العنف بتعطيل وتشويش ضد الأنظمة الإلكترونية قد ينجم عنها ما من شأنه أن يؤدي إلى وفاة أو إصابة شخص أو أكثر أو إحداث أضرار مادية جسيمة للممتلكات المادية أو اضطرابات مدنية أو اقتصادية".(١)

ويرى آخرون أن الإرهاب السيبراني هو:" استخدام الهجمات المستندة إلى الإنترنت في أنشطة إرهابية، بما في ذلك أعمال متعمدة لتعطيل واسع النطاق، في شبكات الكمبيوتر، وخاصة في أجهزة الكمبيوتر الشخصية المتصلة بالإنترنت، عن طريق أدوات مثل فيروسات الكمبيوتر".(٢)

ويشمل الإرهاب السيبراني أي نشاط إجرامي يتم من خلال شبكة الإنترنت بهدف بث الأفكار المتطرفة، سواء كانت سياسية أو دينية أو عنصرية للسيطرة على وجدان الأفراد، وإفساد عقائدهم، وإذكاء تمردهم، واستغلال معاناتهم في تحقيق مآرب خاصة تتعارض مع مصالح المجتمع".(٣)

---

(١) Devost M.G, National security in the information age, Unpublished Master thesis, University of Vermont, Burlington, May 2007.

(٢) انظر: د/ عبد الفتاح بيومي حجازي، الأحداث والإنترنت، المرجع السابق ص١٩.

(٣) انظر: د/ حسنين المحمدي بوادي، الإرهاب الدولي بين التجريم والمكافحة، دار الفكر العربي، ٢٠٠٦، ص ٥٤.

فعن طريق شبكة الإنترنت يمكن للإرهابيين الالتقاء بسهولة في أي مكان، إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة وفي زمن معين، ويتبادلوا الحديث والاستماع لبعضهم عبر شبكة الإنترنت، بل يمكن أن يجمعوا لهم أتباعاً عبر نشر أفكارهم ومبادئهم من خلال المواقع والمنتديات وغرف الحوار الإلكترونية، كذلك أيضاً يعتبر البريد الإلكتروني (E-mail) من أعظم الوسائل المستخدمة في الإرهاب الإلكتروني، وذلك من خلال استخدامه في التواصل بين الإرهابيين وتبادل المعلومات فيما بينهم."

ومن أشكال الإرهاب الإلكتروني، التجنيد السيبراني من خلال ما يطلق عليه "التلقين السيبراني " وأخيراً التهديد والترويع السيبراني".[1]

وتجدر الإشارة إلى أن الطرق الفنية للتجسس السيبراني سوف تكون أكثر الطرق استخداماً في المستقبل من قبل التنظيمات الإرهابية، وخصوصاً ضد المؤسسات والقطاعات الحكومية، العسكرية والسياسية والاقتصادية، لأن هذه المعلومات إذا تعرضت للتجسس والحصول عليها فسوف يساء استخدامها من أجل الإضرار بمصلحة المجتمع والوطن، وهو ما يهدف إليه الإرهاب في عمومه.

وبالتالي استطاعت الجماعات الإرهابية من خلال استخدام الإنترنت في التواصل مع بعضها البعض عبر القارات، وهو الأمر الذي كان يستغرق

---

(١) د/ عبد بن عبد العزيز بن فهد، بحث بعنوان "الإرهاب الإلكتروني في عصر المعلومات"، مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت" المنعقد بالقاهرة في الفترة من ٢-٤ يونيو ٢٠٠٨.

شهورًا في الماضي. ليس هذا فحسب، بل استطاعت الجماعات الإرهابية تبادل المعارف بطرق جديدة ومبتكرة. وهو ما يسميه خبراء الأمن TTPs، وهو اختصار لـ"تكتيكات وتقنيات وإجراءات". فوصفات المتفجرات متوفرة بسهولة على شبكة الإنترنت، وكذلك طرق تجهيز العبوات الناسفة التي كان يتم استخدامها في مناطق الصراع من العراق إلى أفغانستان. وبذلك يكون الإنترنت قد وفّر لهذه الجماعات مساحات افتراضية للتدريب بعيدًا عن خطر قصف الطائرات بدون طيار. (١)

ومن ثم تحدث هجمات سيبرانية إرهابية مدمرة على المواقع الحيوية على الشبكة المعلوماتية وإلحاق الضرر بأنظمة القيادة والسيطرة والاتصالات ومحطات الطاقة الدولية وأسواق المال وإطفاء مصابيح ممرات هبوط الطائرات وغيرها، بحيث يؤدي توقفها أو العبث بأنظمتها إلى حدوث آثار تدميرية تفوق ما تحدثه القنابل والمتفجرات، كما قد يحدث هجوم إلكتروني على المواقع السيبرانية بقصد الاستيلاء على محتوياتها، كشن هجوم على المصارف المالية للاستيلاء على ما بها من أموال من أجل تمويل التنظيم. (٢)

---

(١) Gabriel Weimann، Terror on the Internet: the new arena، the new challenges، United States Institute of Peace Press، 2006. pp 243-249.

(٢) يتم التدمير السيبراني أو نظم المعلومات عن طريق الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالشبكة المعلوماتية من خلال نظام آلي SERVER-PC أو مجموعة نظم مترابطة شبكياً بهدف تخريب نقطة الاتصال أو النظام، وللمزيد

أهم الاتفاقيات الدولية التي تتعلق بالإرهاب السيبراني:

- الاتفاقية الدولية المعنية بمكافحة الإرهاب الدولي ضد سلامة الطيران المدني الدولي ١٩٧١.

– اتفاقية مناهضة الأعمال غير المشروعة في المطارات.

- اتفاقية دول جنوب شرق أسيا ASEAN والتي تعد الاتفاق الإقليمي الوحيد الذي يشير بشكل مباشر إلى الإرهاب السيبراني وقد نصت المادة السادسة منه على التدابير المتخذة لتعزيز القدرات والاستعداد للتعامل مع الإرهاب السيبراني وأي شكل من أشكال الإرهاب باعتبارها من مجالات التعاون بين الدول الأطراف، ولكنها لم تعرف الإرهاب السيبراني.

ومن الجدير بالذكر أن أول هجوم إرهابي ضد أنظمة الكمبيوتر وجد في سيريلانكا، وكذلك عام ١٩٩٩م خلال الحرب في إقليم كوسوفو عندما حاول الضرب استهداف مواقع حلف الناتو على الإنترنت، كما أن فيروس Stuxnet الذي استهدف البرنامج الدوري الإيراني كان من الممكن أن يكون

والاستفاضة حول طرق تدمير وإتلاف المواقع السيبرانية: انظر: د/ عادل عبد الصادق " هل يمثل الإرهاب الإلكتروني شكلا جديدا من أشكال الصراع الدولي " ملف الأهرام الاستراتيجي، مركز الدراسات السياسية والاستراتيجية بالأهرام، العدد ١٥٦ – ديسمبر ٢٠٠٧، ود/ محمد سليمان الخوالدة: جريمة الدخول غير المشروع على الموقع السيبراني أو نظام معلومات وفق التشريع الأردني، رسالة ماجستير في القانون العام، كلية الدراسات العليا، الجامعة الأردنية، ٢٠١٢م، ص ٦٦.

له نتائج كارثية ليس على إيران وحدها فقط بل وعلى جميع الدول المجاورة لها.[١]

ومن الجهود الدولية لمكافحة الجرائم الإرهابية أنه تم إنشاء لجنة خاصة لحماية البنية التحتية في الولايات المتحدة الأمريكية، وتم تحديد الأهداف المحتملة من قبل الإرهابيين وهي مصادر الطاقة الكهربائية، والاتصالات، وشبكات الحاسب الآلي.[٢]

ونخلص من ذلك أنه نتيجة لزيادة الانكشاف الأمني للدول وذلك باعتمادها على الفضاء السيبراني كبرنامج الحكومات السيبرانية والتي تصبح عرضة للاختراق والهجوم بالفيروسات وسرقة المعلومات أو إتلافها والتي أصبحت معضلة جديدة للأمن بتحوله إلى نوع جديد يعتمد على الشبكات والإنترنت، ولبروز مخاوف من ممارسة الدول لمثل تلك المعطيات إلى إمكانية اتجاه الجماعات الإرهابية في التأثير على أمن الفضاء السيبراني. ومهاجمة نظم شبكاتها السيبرانية وتأثير هذا الهجوم- التخريبي-على المؤسسات المالية والمصرفية والتحكم في الطيران المدني والنظم المالية.

---

(١) للمزيد راجع:

- Walker Gerke, Understanding cyber crime, 2009, at:

(٢) انظر: د/ عادل عبد الصادق ، "الإرهاب الإلكتروني. القوة في العلاقات الدولية. نمط جديد وتحديات مختلفة"، الفصل الثالث ، تداعيات الإرهاب الإلكتروني علي الصراع والأمن الدوليين، مركز الدراسات السياسية والاستراتيجية بالأهرام، القاهرة ٢٠٠٩، ص١٥٥-٢٢٩.

وأيضا تقوم التنظيمات الإرهابية بشن هجمات سيبرانية من خلال الشبكة المعلوماتية، بقصد تدمير المواقع والبيانات السيبرانية والنظم المعلوماتية وإلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها، وتستهدف الهجمات الإرهابية في عصر المعلومات ثلاث أهداف أساسية غالباً، وهي الأهداف العسكرية، والسياسية، والاقتصادية، وفي عصر ثورة المعلومات تجد الأهداف الثلاثة نفسها، وعلى رأسها مركز القيادة والتحكم العسكرية، ثم مؤسسات المنافع كمؤسسات الكهرباء والمياه، ومن ثم تأتي المصارف والأسواق المالية، وذلك لإخضاع إرادة الشعوب والمجتمعات الدولية.

الفرع الرابع
الهجمات الاستراتيجية والعسكرية السيبرانية

الحرب السيبرانية هي أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها.

وتتعرض حواسب الأنظمة العسكرية والمالية لخطر التخريب بهدف تعطيل عملياتها الطبيعية وتجهيزاتها. الثاني: ويكون للتخريب المعتمد على المجال السيبراني تداعيات مادية خطيرة، خاصةً عند استهداف البنية التحتية للدول مثل شبكات الطاقة أو النقل أو عند التلاعب بالبيانات لإرباك الهدف وتعطيل الأوامر والسيطرة على اتخاذ القرار.

وقد تقوم دولة باستخدام هجمات الفضاء السيبراني كجزء من الاستعداد لنشوب هجوم تقليدي ضد دولة معادية وخاصة أن هجمات الفضاء السيبراني

استباقية من دون سابق إنذار، وإنها غير محدده المجال أو المدى وتكون أهدافها غير مأمونة بخلاف الحرب التقليدية التي تكون أهدافها ومكانها محددا، وفي الغالب تكون قوات الحرب السيبرانية غير معروفة وليست محددة في دولة ما سواء أكانت تلك الدولة هدفا للحرب أو مشاركا فيها حيث لا تصبح بالضرورة الدولة هي الهدف.(١)

وبدون معرفة من وراء الهجوم وكيفية نجاحه وطرق تنفيذه وأطرافه الحقيقية، يجعل القضية متشابكة وتأتي عملية الاستجابة للهجمات وعملية رد الفعل مع ضعف إجراءات الوقاية ضد التعرض لمثل تلك الهجمات، والتي يمكن أن يتم شنها عبر الفضاء السيبراني والشبكات، أو من خلال استخدام الهجوم العسكري التقليدي، وللحصول على تأييد دولي للإجراءات الوقائية السلبية تكون هناك حاجة ملحة إلى تقديم الدليل أو إثبات تورط طرف ما في مثل هذا الهجوم – والذي يكون من الصعب التأكد بشأنه – بما يشكل ضمانه لوجود إجماع دولي للتعاون في المكافحة أو الحرب ضد طرف أخر أو فرض عقوبات دولية ما، حيث تكون الدول معرضة لانتهاك سيادتها وأمنها الداخلي.(٢)

---

(١) Kevin Coleman، The Challenge of Unrestricted Warfare، A Look Back and a Look Ahead، Articles، directionsmag. com، http: //www. .

(٢) Bonnie N. Adkins، " The Spectrum of Cyber Conflict from Hacking to Information Warfare: What is Law Enforcement's Role?" A Research Report Submitted to the Faculty In Partial Fulfillment of the

ومن ثم فإن الدولة يمكن أن يتم استهدافها دون النظر إلى حدودها أو نطاقها الجغرافي بل ومن الممكن أن يكون الهجوم من الداخل من قبل عملاء دولة ما أو عملاء مقيمين في دولة أخرى يقومون بشن هجمات من خلال نطاقها الجغرافي دون تورط تلك الدولة في دعم مباشر لها.

ويرجع السبب في شن تلك الهجمات لما تتميز به الحرب السيبرانية من خصائص تؤثر علي البنية التحتية للمنشات الحيوية، نتيجة اعتماد منشآت الطاقة والكهرباء على النظم المتقدمة في المعلومات. ولا يلقى هذا النمط الجديد من الصراع تنديدا دوليا مثل الهجوم التقليدي، وتتميز تلك الهجمات أنها سريعة الانتشار ورخيصة التكلفة وعدم معلومية مصدر الهجوم مما يؤدي إلى ارتباك الخصم وقد تتم تلك الهجمات عبر الشبكات عابرة الحدود الدولية.[١]

ومن المتوقع أن يشهد القرن ٢١ انتشار استخدام الأسلحة السيبرانية سواء بمفردها أو بالارتباط بأسلحة أخرى وخاصة في ظل صعوبة فرض حظر استخدامها في الفضاء السيبراني وصعوبة وصف العمل على أنه هجوم مسلح وهي المشكلة التي واجهت موقف حلف الناتو من الهجوم على "استونيا".[٢]

April ،Alabama ،Maxwell Air Force Base ،Graduation Requirements .2001

(١) انظر: د/ على حسين باكير، الحروب السيبرانية في القرن الواحد والعشرين، مركز الجزيرة للدراسات ٧/ ١٢/ ٢٠١٠.

(٢) حيث تنص المادة الخامسة من ميثاق حلف الناتو على أن الدول الأعضاء تتحرك بشكل جماعي للدفاع عن أي عضو بالحلف يتعرض إلى هجوم. وانتهت اللجنة التي تم

وذلك على الرغم من قدرة الحرب عبر الفضاء السيبراني على إحداث ذات الضرر الناتج من استخدام أسلحة تقليدية وبما يعنى تحول الفضاء السيبراني إلى ميدان للقتال ولممارسة الأعمال العدائية بين الأطراف المتحاربة.

ويتم في كل عام نشر ما يزيد على مليون فيروس جديد ومن مصادر متعددة منها العصابات الإجرامية أو من الدول أو الإرهابيين أو حتى من شركات منافسة أو ما يطلق عليهم بالفاعلين السيبرانيين cyber actors.

وفي السنوات القليلة الماضية حدث تطور في أنواع الأسلحة السيبرانية وتخطت القدرة على تعطيل أنظمة المعلومات إلى تعطيل أنظمة التشغيل المادية للآلات، ويفرض ذلك أن تكون آثار تلك الحرب أوسع نطاقا وأقل توقعا بنتائجها مع ازدياد حجم ومدى الفضاء السيبراني.

فمثلا تم إجراء **تدريبات لحلف شمال الأطلسي "التحالف السيبراني"**، **لاختبار قدرات قوات الناتو في مجال مواجهة التهديدات السيبرانية** والذي شاركت فيه ٢٧ دولة من أصل ٢٩ من حلف شمال الأطلسي، و٦ دول متحالفة أخرى هي، اليابان والجزائر والنمسا وفنلندا وايرلندا والسويد، في تدريبات "التحالف السيبراني" والتي عقدت في الفترة من ٢ إلى ٦ ديسمبر. وقد مثل هذه الدول نحوا من ٧٠٠ مختص من المختصين في الأمن السيبراني والتقنيين والمسؤولين العسكريين والحكوميين وممثلي قطاع الأعمال.(١)

تشكيلها من الحلف إلى عدم اعتبار الهجوم على استونيا هجوما مسلحا لعدم معرفة أو تحديد المسئول عن تلك الهجمات.

(١) بيان وزارة الدفاع الإستونية الصادر في يوم الاثنين٢ / ١٢/ ٢٠١٢ في إستونيا.

ويعتبر الهدف الرئيسي من هذه التدريبات هو اختبار قدرات قوات الناتو في مجال مواجهة التهديدات السيبرانية، ووفقا لخطة هذه التدريبات، سيحاول المشاركون في صد عملية قرصنة من بلد افتراضي يحاول مهاجمة شبكات معلومات الناتو باستخدام جميع الأساليب الممكنة. ويذكر أنه سبق واتخذ الحلف في الفترة الأخيرة عددا من الإجراءات في مجال الأمن السيبراني، مما أعطى له الفرصة لزيادة سرعة وفاعلية صد التهديدات في المجال السيبراني.[1]

والهجمات السيبرانية يمكن أن تتخذ الصور الآتية:ـ

أولاً: استهداف الأنظمة العسكرية:

تستهدف هذه النوعية من الهجمات عادة الأهداف العسكرية غير المدنية، والمرتبطة بشبكات المعلومات، من خلال سرقة المعلومات والبيانات العسكرية أو التلاعب بها وتعد هذه من أخطر الهجمات.

ويتم من خلالها نقل كميات هائلة من المعلومات عبر شبكات المعلومات بصورة يومية، وتتميز كثير من هذه المعلومات بكونها على درجة كبيرة من الأهمية. وعلى الرغم من استخدام أجهزة تشفير تتولى تشفير الوسائل والمعلومات المهمة عند إرسالها وفك شفرتها عند استقبالها، إلا أن الاستيلاء على المعلومات التي يتم نقلها عبر شبكات المعلومات قد أصبح يشكل خراً كبيراً يهدد أمن وسلامة هذه المعلومات.

---

(١) وأعلن الأمين العام لحلف الناتو، ينس ستولتنبيرغ، في وقت سابق، أن جميع محاولات الهجوم السيبراني على شبكات الحلف المحمية تم صدها في الفترة الأخيرة، ولم يؤثر أي من الهجمات على أنشطة المنظمة، مؤكدا أنه يتم صد الهجمات بشكل يومي.

فالهجمات السيبرانية على الأهداف العسكرية: تستهدف الأهداف العسكرية دون المدنية، ورغم محاولات حكومات الدول عزل المعلومات العسكرية عن العالم، عن طريق التدقيق في اختيار الأشخاص المتعاملين معها[١]، إلا أنها قد تتعرض لهجمات إلكترونية مثل تعرض البرنامج النووي الإيراني ٢٥ سبتمبر ٢٠١٠ وكذلك محطة **"تشرنوبل"** في أوكرانيا لهجمة إلكترونية في يونيه ٢٠١٧.

ثانياً: استهداف البنية التحتية للدولة:

يتم استخدام الفضاء السيبراني كنمط من أنماط استخدام القوة عن طريق التأثير على عمل مصادر المعلومات وإتلافها وأنظمة الاتصالات عن طريق الهجوم الإلكتروني أو هجوم المعلومات من خلال الأدوات والوسائل الإلكترونية بما يؤدي إلى شلل هذه الأنظمة وتدمير أنظمة التشغيل الخاصة بها والتأثير على تدفق المعلومات بما يؤدي إلى إرباك عمل البنية التحتية الحيوية.[٢]

ومن ثم يشمل هذا الاستهداف سلسلة من الهجمات المعلوماتية على نظم الحواسيب والشبكات المعلوماتية التي تنهض بمهام التحكم بشبكات توزيع الطاقة الكهربائية الوطنية، وينشأ عن مثل هذه الهجمات تعطيل العديد من

---

(١) انظر: د/ صفوت أمين سلامة – أسلحة حروب المستقبل بين الخيال والواقع – دراسات استراتيجية – مركز الإمارات للدراسات والبحوث الاستراتيجية – للعدد ١١٢ – ٢٠٠٥ – ص ٩ – ٥٩.

(٢) د/ عادل عبد الصادق، القوة الالكترونية: أسلحة الانتشار الشامل مرجع سابق، ص١٠.

مرافق الحياة في البلاد، وسيادة الفوضى، نتيجة لانعدام مصادر الطاقة الكهربائية وشل الحركة في عموم البلاد.

ولا يتوقف الأمر عند هذا الحد، حيث إن هناك الكثير من الأهداف الأخرى، التي يمكن استهدافها لإحداث الفوضى في الحياة المدنية. فهناك مثلاً شبكات المعلومات الطبية، والتي يمكن لمهاجمتها، واختراقها ومن ثم التلاعب بها أن يؤدي إلى خسائر في أرواح المرضى من المدنيين. كأن يتم النفاذ إلى سجلات المستشفيات والتلاعب بسجلات بها بشكل يؤدى إلى حقن هؤلاء بأدوية وعلاجات كانت مميتة بالنسبة لهم. حتى لو افترضنا أن شبكة المعلوماتية الخاصة بالمؤسسات الطبية منيعة، فإن رسالة واحدة تنشر مثلاً بالبريد السيبراني، مفادها أن هناك دماء ملوثة في المستشفيات وما إلى ذلك، يمكن لها أن تحدث آثاراً مدمرة على الصعيد الاجتماعي.[1]

وقد يتضمن استهداف نظم المواصلات والاتصالات من خلال اختراق نظم التحكم بخطوط الملاحة الجوية والبرية والبحرية، وإحداث خلل في برامج هبوط الطائرات وإقلاعها، مما قد ينجم عنه حصول تصادم فيها بينها، أو اختراق الشبكات المعلوماتية الهاتفية، وإيقاف محطات توزيع الخدمة الهاتفية، وقد تمارس سلسلة من الهجمات على خطوط الهواتف المحمولة ومنع الاتصال بين أفراد المجتمع ومؤسساته الحيوية، الأمر الذي ينشر حالة من الرعب والفوضى، وعدم القدرة على متابعة تداعيات الهجمات الإرهابية المعلوماتية.

---

(١) المرجع السابق، ص ١١.

أو الهجمات على شبكات الطاقة حيث أصبح الاعتماد على شبكات المعلومات من الوسائل الهامة في إدارة نظم الطاقة، ويمكن لتلك الهجمات أن تؤثر بشكل كبير على الإنسان في استخدام الطاقة الكهربائية مما ينتج عنه أضرار كثيرة لا يمكن تداركها.

أو الهجمات على أهداف اقتصادية: حيث أصبح الاعتماد على شبكات الكمبيوتر شبه مطلق في عالم المال والأعمال مما جعلها هدفاً مغرياً للهجمات السيبرانية مما يؤثر على النظام الاقتصادي العالمي مثال هجمات نادي الفوضى في عام ١٩٩٧.

ومن ثم هناك محاولة للسيطرة الواسعة على المؤسسات الحيوية للدول الأخرى عن طريق استخدام أسلحة تكنولوجيا الاتصال والمعلومات ضد المنشآت المدنية والعسكرية وأنظمة الدولة والمؤسسات السياسية وإفساد عملها بما يمثل تهديدا مباشرا للأمن القومي الذي يتمثل في الدخول غير المشروع في المؤسسات المالية والاقتصادية والتدمير الواسع للبنية التحتية للاتصالات من خلال استخدام تكنولوجيا الاتصال والمعلومات بما يعد هجوماً على أنظمة صنع القرار والسيطرة والهجوم على الأنظمة الدفاعية للدولة الأخرى بما يمثل إمكانية تعرضها لهجوم محتمل بما يمكن أن يأتي في شكل رد فعل يتمثل في الحق الشرعي للدفاع عن النفس، ويؤدي استهداف الاتصالات وأنظمة المواصلات وخدمات الطوارئ والخدمات الحكومية إلى الأضرار بالحياة والممتلكات والمرافق الحيوية.

المبحث الثاني
المخاطر السيبرانية وأثرها على تهديد السلم والأمن الدوليين

أصبحت قضية أمن الفضاء السيبراني من استراتيجيات الأمن القومي للعديد من الدول من أجل الاستحواذ على مصادر القوة داخل الفضاء السيبراني، للعمل على الحيلولة دون تعرض بنيتها التحتية الحيوية للخطر الذي ينجم جراء قطع خدمة الإنترنت أو ضرب مواقعها أو توقف رسائل البث الإذاعي أو التلفزيوني أو توقف موجات الراديو أو سقوط شبكات المحمول أو البث الفضائي، وأصبح لها تأثير عميق على المجتمع والاقتصاد على النطاق الدولي. (١)

وبذلك دخل المجال السيبراني ضمن المحددات الجديدة للقوة وأبعادها الجديدة من حيث طبيعتها وأنماط استخدامها بل وأيضا طبيعة الفاعلين وهو ما كان له انعكاس على قدرات الدول وعلاقاتها الخارجية، وأضفي خصائص جديدة للقوة والتي تمتد لتشمل كافة الوسائل والطاقات والإمكانيات المادية وغير المادية، المنظورة وغير المنظورة والتي بحوزة الدولة، ويستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة، وتؤثر في سلوك الوحدات السياسية الأخرى. (٢)

---

(١) Tim Jordan، " Cyber power: The Culture and Politics of Cyberspace and the Internet"، Rout ledge، 254- 160 pp 2000.

(٢) انظر: د/ جوزيف ناي الابن، المنازعات الدولية، ترجمة: احمد أمين الجمل ومجدي كامل، القاهرة، ١٩٩٧، ص ٨٢.

فالعلاقة بين الأمن السيبراني والأمن القومي تزداد كلما زاد نقل المحتوى المعلوماتي والعسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي إلى الفضاء السيبراني، خاصة مع تسارع الدول في تبني الحكومات الإلكترونية والمدن الذكية في العديد منها، واتساع نطاق وعدد مستخدمي الانترنت في العالم، مما أدى إلى أن تكون قواعد البيانات القومية في حالة انكشاف خارجي، إضافة إلى حملات الدعاية والمعلومات المضللة ونشر الشائعات أو الدعوة لأعمال تحريضية أو دعم المعارضة أو الأقليات، مما يساهم في تلاشي سيادة الدولة ويشكك في قدرتها على الحفاظ على أمنها القومي.[1]

ومن ثم نجد الأمن السيبراني قد فرض نفسه كبعد جديد ضمن أبعاد الأمن الدولي، وترتب عليه إحداث تغييرات جوهرية في مفاهيم العلاقات الدولية كطبيعة الصراعات والتهديدات بين الدول، مما حتم على 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 ميكانيزمات ووسائل فعالة لمواجهة المخاطر والتهديدات السيبرانية التي تتميز بالسرعة

---

(١) انظر: د/ إيهاب خليفة، القوة الالكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الانترنيت، دار العربي، ٢٠١٧، ص ٥.

والغموض والدقة، ومن ثمة تحقيق الأمن السيبراني والحفاظ على مكاسب الدول وأمنها القومي.

ولذا كان لابد من بحث مدى مشروعية استخدام القوة السيبرانية في مجال العلاقات الدولية ومتى تعد تلك الهجمات حقا مشروعا في حالة الدفاع الشرعي أو غير مشروع في حالة التهديد أو الإضرار بالسلم والأمن الدوليين فضلا عن دور المنظمات الدولية والدول في مواجهة مثل تلك الهجمات دون المساس بالحقوق والحريات الأساسية.

وعلى هذا سوف يعمد هذا الجزء من البحث، بشكل أساسي، إلى المقارنة بين قواعد القانون الدولي القائمة، وتحديداً تلك المتعلقة باستخدام القوة والدفاع عن النفس ومحاولة إسقاطها على الهجمات السيبرانية، إضافة إلى ذلك سيتم الاسترشاد بجهود المنظمات والمؤسسات الدولية والفقهاء في بذل جهد مستفيض سعياً وراء فهم ملامح القانون الدولي العام القائمة حيال هذه الظاهرة المتنامية.

وفي إطار مدى انطباق أحكام المادتين م٢/ ف٤، م ٥١ من ميثاق الأمم المتحدة على الهجمات السيبرانية يبرز تساؤلان جوهريان هما: -

أولاً: هل يمكن أن تشكل الهجمة السيبرانية مخالفة للمادة ٢/ ف٤ من ميثاق الأمم المتحدة التي تحظر على الدول "استخدام القوة أو التهديد بها ضد سلامة الأراضي أو الاستقلال السياسي لأي دولة أخرى؟ تنبع أهمية هذا التساؤل تحديداً في ضوء عدم وضوح المعنى الدقيق لمصطلح "استخدام القوة" وفق هذه المادة.

ثانياً: هل يمكن أن تصل الهجمة السيبرانية إلى مستوى "الهجوم المسلح" الوارد في المادة ٥١ حتى يثبت للدولة "المعتدى عليها إلكترونيا" حق الدفاع عن نفسها كما هو الحال بالنسبة للدولة المعتدى عليها عسكرياً في سياق هذه المادة؟

وفي ظل خلو الاتفاقات الدولية أو العرف الدولي المستقر من إجابة واضحة عن هذه الأسئلة فليس لدينا سوى اللجوء إلى موقف محكمة العدل الدولية، وبالتحديد موقف المحكمة في قضية نيكاراجوا لعام ١٩٨٦، وأيضاً دليل تالين "Tallinn Manual"، وتحديداً الجزء الأول الخاص بسيادة الدولة، والجزء الثاني المتعلق باستخدام القوة، بالإضافة إلى مجموعة من الآراء الفقهية لبلورة فهم ملامح قواعد القانون الدولي العام بخصوص هاتين المسألتين.(١)

المطلب الأول
المخاطر السيبرانية وموقف ميثاق الأمم المتحدة من استخدام القوة السيبرانية

يعد الهدف الأساسي للأمن السيبراني هو القدرة على مقاومة المخاطر السيبرانية التي تهدد الدول، وبالتالي التحرر من الخطر أو الأضرار الناجمة عن إساءة استخدام تكنولوجيا المعلومات والاتصالات مما يتطلب حماية

---

(١) Judgment of the International Court of Justice in Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States)، 1986، I. C. J. 14، See also; 96-97، Malcolm Shaw، International Law، (7th edition)، 2014; Cambridge University Press، Yoram Dinstein، War، Aggression and Self-defence، 3ed edition2011.

الشبكات وأجهزة الكمبيوتر، والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به، ونتيجة لأهمية الأمن السيبراني في الآونة الأخيرة فقد جعلته العديد من الدول على رأس أولوياتها، خاصة بعد الحروب السيبرانية التي بدأت تظهر تجلياتها بين بعض الدول الكبرى، في إشارة صريحة إلى أن هناك نوعا من الحروب الجديدة ألا وهى الحروب السيبرانية.

ومن أهم الإشكاليات التي تواجه المجتمع الدولي في هذا الصدد كيفية التعامل مع الأسلحة السيبرانية، وما يتعلق بالجدل حول مدى اعتبار الأسلحة السيبرانية كالأسلحة غير التقليدية وإمكانية أن تخضع لقيود حظر استخدام القوة في العلاقات الدولية ولاتفاقيات الحد من التسلح وغيرها.

ويضاف إلى ذلك أن كثيرا من المواثيق والاتفاقيات الدولية مثل ميثاق الأمم المتحدة، واتفاقيات لاهاي وجنيف تتناول مصطلحات عامة من قبيل "السلامة الإقليمية"، و"استخدام القوة المسلحة"، و" النزاع المسلح"، و"عمل من جانب القوات الجوية أو البرية أو البحرية" و"هجوم مسلح"، وهي مصطلحات اختلف الفقه حولها في مدى انسجامها مع التصورات السيبرانية.

وإذا كان مبدأ حظر استخدام القوة أو التهديد بها في العلاقات الدولية من المبادئ الأساسية التي نص عليها ميثاق الأمم المتحدة في المادة ٢ الفقرة ٤ منه، حيث نص على أن: "يمتنع أعضاء الهيئة جميعا في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة".

إلا أن الميثاق لم يتعرض لما هو المقصود بالقوة التي يمتنع على أعضاء المنظمة التهديد بها أو استخدامها في علاقاتهم الدولية، وقد جرى العرف الدولي على أن مجموعة من الأعمال غير الودية مثل الإكراه الاقتصادي والسياسي، أعمال التجسس، المقاطعة الاقتصادية، العقوبات التجارية وغيرها، لا ترقى إلى عتبة "استخدام القوة" بغض النظر عن حجم آثارها. (١)

الأمر الذي يثير التساؤل حول ما إذا كان استخدام القوة السيبرانية أو التهديد باستخدامها يندرج تحت نطاق "القوة " المحظورة، بموجب المادة ٢ فقرة ٤، والتي يتطلب الإخلال بها تطبيق العقوبات المنصوص عليها في الفصل السابع من ميثاق الأمم المتحدة؟ أم أنها خارج نطاق الحظر المقصود؟

ولقد ثار خلاف حول مفهوم القوة المحظور استخدامها في العلاقات الدولية حيث يتنازع اتجاهان رئيسيان بشأن تكييف القوة السيبرانية وفقاً للمادة ٢ فقرة ٤:

يرى الاتجاه الأول – الاتجاه المضيق – أن لفظ القوة الوارد في المادة(٢ / ف ٤) من الميثاق يجب تفسيره تفسيراً ضيقاً، من ثم فإن القوة غير المسلحة لا تدخل ضمن التعريف، وأن تلك الأشكال المختلفة من القوة لا تدخل ضمن هذا الحظر والدليل على ذلك ما جاء في ديباجة الميثاق بمنع استخدام القوة المسلحة إلا للأغراض العسكرية، كما تؤكد الأعمال التحضيرية للمادة (٢ / ف٤) من الميثاق أن المراد من لفظ القوة هو القوة المسلحة فحسب ولذا تم

---

(١) **Myriam A. Dunn**، "The Internet and the Changing Face of International Relations and Security"، **Volume number: 7**، **Issue number: 1**، **ProCon Ltd.**، **Sofia**، **Bulgaria**، **2001**.

استبعاد اقتراح "البرازيل" اعتبار إجراءات الضغوط الاقتصادية ضمن الاستخدام غير المشروع للقوة.[١]

ومن ثم فهذا الاتجاه يأخذ بالتفسير الحرفي للمادة ٢/ ٤ حيث يعتمد أنصاره على فكرة ضرورة إحداث تأثيرات جسيمة مادية وبشرية لتكييف الهجمات السيبرانية كاستخدام للقوة وفقا للمادة ٢/ ٤، وعليه فيرى أنصار هذا الاتجاه أن الهجمات السيبرانية مشابهة في تأثيراتها للإكراه السياسي أو الاقتصادي، أى لا تحدث أضرار مادية جسيمة ومن ثم لا تندرج الهجمات السيبرانية ضمن نطاق المادة ٢/ ٤، بغض النظر عن تأثيراتها السلبية على الأمن الدولي. وعليه، يعتبر أنصار هذا الاتجاه أن الهجوم السيبراني "ستاكنست" على المنشات النووية الإيرانية عام ٢٠١٠ مثال واضح للهجوم السيبراني كاستخدام للقوة، حيث تسبب في تدمير بعض أجهزة الطرد المركزي. [٢]

ويرى الاتجاه الثاني – الاتجاه الموسع – أن الضغوط الاقتصادية، وكافة الأعمال الانتقامية سواء منها ما اتخذ شكل القوة المسلحة أو غيرها من الأعمال التي لا تصل إلى هذا الحد تدخل في نطاق استعمال القوة التي حظرها الميثاق، وأن المادة(٢ / ف ٤) حددت الصور المحظورة للقوة وبينت أنها تلك الموجهة

---

(١) Kamal Ahmad Khan، Use of Force and Human Rights under International Law، Athens Institute for Education and Research، Conference Paper Series BLE 2017- 2205.

(٢) Sophie Barnett، "Applying Jus Ad Bellum in Cyberspace"، International Relations Studies، 1 Septmber، 2016.

ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة والتي تتفق مع مقاصد الأمم المتحدة وليست القوة المسلحة وحدها، بل إن ممارسة الضغوط الاقتصادية ضد دولة معينة قد يؤدي إلى نتائج مماثلة وبطريقة ملموسة وأن المادة (٢/ ف٤) من الميثاق استعملت لفظ القوة فقط وذلك يفيد بأن الحظر شمل القوة المسلحة وسائر وسائل وأساليب القهر الأخرى، كما أن هذا التفسير يتفق مع آراء قضاة محكمة العدل الدولية في رأيهم الاستشاري بشأن نفقات الأمم المتحدة عام ١٩٦٢. (١)

---

(١) قام – مايكل شميت –بوضع عدد من المؤشرات حول متى يمكن اعتبار هجمات الفضاء السيبراني استخداماً للقوة وذلك من درجات تتراوح ما بين (١–١٠) وفي حالة تطبيق تلك المؤشرات لتصل إلى درجة ٧ فإنها تعد استخداماً للقوة وهذه المؤشرات هي:

١. قسوة الهجوم Severity: إذا ما كان المدنيون معرضين لقتل أو الضرر الجسيم بالممتلكات فإن ذلك يعد عملاً عسكرياً ويعد استخداما للقوة.

٢. توافر الفورية Immediacy: حيث يتم رؤية آثار الهجوم في دقائق أو ثواني، كما يحدث عند انفجار قنبلة تقليدية.

٣. عمل مباشر Directness: حيث يكون الحدث هو نتيجة مباشرة للهجوم.

٤. القياس والملاحظة Measurability: حيث يمكن قياس الحدث وملاحظته كمياً كحجم الخسائر المادية.

٥. الاختراق Invasiveness: حيث يتم انتهاك الحدود الدولية والدخول غير الشرعي إلى المنشآت أو المؤسسات المحمية.

٦. افتراض شرعية العمل Presumptive: حيث يكون للدول الحق في احتكار الاستخدام الشرعي للقوة.

وهذا الاتجاه على عكس الأول حيث يتبنى أنصاره التفسير الواسع للمادة ٢/ ٤، حيث يرى أنه ليس بالضرورة أن تحدث الهجمات السيبرانية أضرارا مادية جسيمة حتى يمكن اعتبارها استخداما للقوة فأية هجمات إلكترونية تتسبب في حدوث تعطيل لأنظمة الحواسب الرئيسية للدولة وتتسبب في شل مفاصل الدولة أو إحداث أضرار اقتصادية يمكن اعتبارها استخداما للقوة وفقاً للمادة ٢/ ٤. (١)

وحاول الفقيه "Michael Schmitt" التوفيق بين الاتجاهين السابقين عبر تأكيده بأن الهجمات السيبرانية يجب أن تنسجم مع الاقتراب التقليدي القائم على إحداث الأضرار الجسيمة كاستخدام للقوة، لكن ليس بالضرورة أن تكون تلك التأثيرات أو الأضرار عسكرية فقط، فالهجمات التي تتسبب في حدوث أضرار اقتصادية جسيمة تعد إذن استخداما للقوة. ووضع

المسؤولية Legitimacy / Responsibility: حيث يترتب على مسؤولية الدولة عن العمل العسكري التزامات قانونية.

"Computer Network Attack and The Use of Force ،Michael N. Schmitt in International Law: Thoughts on a Normative Framework"، *Columbia Transnational Law Journal of Iss*، ٣٧، No. 3، 1999، PP 914. 915.

انظر: د/ نبيل أحمد حلمي – القانون الدولي وفقاً لقواعد القانون الدولي العام – دار النهضة العربية – القاهرة – ١٩٩٩ – ص ١٢٠ – ٢٠٠.

(١) "Cyber-Attacks and International law of Armed ،Titiriga Remus Conflicts; a "Jus ad Bellum" perspective"، *Journal of International Commercial Law and Technology Issue*، ٨، No. 3، 2013، P 179.

Schmitt، خمسة معايير رئيسية لتكييف الهجوم السيبراني كاستخدام للقوة هي:

شدة الضرر، الضرر الفوري اللاحق، وجود صلة مباشرة بين القوة المسلحة وعواقبها، عبور الهجوم الالكتروني الحدود الدولية، وأخيراً القدرة على تقييم أو تمييز الفعل المادي. (١)

وأعتقد أن تبني أي من الاتجاهين له أثر في ترتيب النتائج وذلك لأن الأخذ بالاتجاه الأول – التفسير للمضيق – سيحرم الدول المعتدى عليها من اتخاذ أي إجراء دفاعاً عن نفسها تجاه أي اعتداء غير مسلح والعكس صحيح، وعليه فإننا مع رأي الفقيه مايكل شميث – وأن العبرة بما تحدثه الهجمات السيبرانية من أضرار جسيمة ومن ثم يمكن أن تشمل القوة كافة الضغوط السياسية والاقتصادية، إضافة إلى استخدام كافة أشكال القوة الأخرى وتكون هجمات الفضاء السيبراني من القوى المحظور استخدامها في العلاقات الدولية – ويعد ذلك التطور الطبيعي لمفهوم القوة تماشياً مع المستحدثات العالمية في مجال الاتصالات والتكنولوجيا وأثرها على سيادة الدول.

---

(١) Michael N. Schmitt، "Computer Network Attack and The Use of Force in International Law: Thoughts on a Normative Framework"، *Columbia Journal of Transnational Law*، Iss، ٣٧، No. 3، 1999، PP 914. 915.

ويمكن القول بأن العرف الدولي قد استقر على أن مفهوم القوة وفقا للمادة ٢ الفقرة ٤، هو القوة المسلحة أي استخدام الدولة لقواتها العسكرية الحركية ضد دولة أخرى أو على أراضيها.

وجاء في الرأي الاستشاري لمحكمة العدل الدولية بشأن مشروعية التهديد أو استخدام الأسلحة النووية، بأن المادة ٢ فقرة ٤ من الميثاق تحظر استخدام القوة بغض النظر عن السلاح المستخدم. ومع ذلك لا يوجد حتى الآن إجماع عالمي بخصوص اعتبار الهجمات السيبرانية بمثابة استخدام للقوة في إطار المادة ٢ الفقرة ٤ من الميثاق.

وقد تصدت محكمة العدل الدولية في قضية النشاطات العسكرية وشبه العسكرية في نيكاراجوا[1] Nicaragua Case إلى المادة ٢/ ٤ من ميثاق الأمم المتحدة من زاويتين:- **الزاوية الأولى**: عندما تعرضت المحكمة إلى طبيعة هذه المادة، حيث أكدت في الفقرة ١٨٧ من حكمها على تحول مبدأ حظر استخدام القوة أو التهديد بها إلى قاعدة عرفية دولية يقع على جميع الدول واجب الالتزام بها.[2] يشار إلى أن ذلك يأتي منسجماً مع حقيقة أن معظم بنود

(1) - Kriangsak Kittichaisaree, "Public International Law of Cyberspace, Law, Governance and Technology Series", Vol 32, Springer International Publishing, Switzerland, 2017, P163.

(2)) Id. Para. 187.

ميثاق الأمم المتحدة قد وصلت إلى كونها مبادئ أساسية لا يجوز لأي دولة مخالفتها أو الخروج عنها.[١]

أما الزاوية الثانية: فتتمثل في الحالات التي يمكن أن تعتبر استخداماً للقوة خلافاً لهذه المادة.

وفي هذا الصدد أقرت المحكمة بشمولية المادة وعدم اقتصارها على استخدام القوة بالمعنى التقليدي، والمتمثل في استخدام قوات عسكرية نظامية خارج حدود الدولة، حين أسهبت وأقرت أن "إرسال القوات من لدن الدولة أو بالنيابة عنها سواء كانت على شكل مجموعات نظامية أو غير نظامية أو أية أدوات أخرى" يعتبر مخالفة للمادة ٢/ ٤ من الميثاق، ويمكن لمثل هذا التصرف أن يعتبر هجوماً مسلحاً وفقاً لأحكام المادة ٥١ من الميثاق بالاستناد إلى حجم وتأثير استخدام القوة[٢]

ويلاحظ أن هناك نقطة جوهرية يجب الوقوف عندها تتمثل في الخروج الواضح للمحكمة عن النهج التقليدي لفهم استخدام القوة ذلك الاستخدام للأدوات التقليدية في الاعتداء، والذي كان يشترط قراراً مباشراً من الدولة

(1) See, Kamrul Hossain, The Concept of Jus Cogens and the Obligation under the U.N. Charter, Santa Clara Journal of International Law, Vol.3, Issue 1, 2005

(2) ICJ, Nicaragua Case. 1986, Para, 195.

باتجاه استخدام القوة في إقليم دولة أخرى[١]، وهذا الموقف للمحكمة جاء تأكيداً على النية الحقيقية للدول المشاركة في صياغة المادة ٢(٤) من الميثاق، حيث إن الأعمال التحضيرية لهذه المادة تشير وبوضوح إلى أن أي تهديد أو استخدام للقوة بين الدول الأعضاء سوف يشكل خرقاً لهذه المادة، شريطة أن يكون مخالفاً لمبادئ الميثاق.[٢]

وهذا الموقف من المحكمة يعد تأكيداً لفكرة مسؤولية الدولة عن الممارسات الخاطئة المباشرة وغير المباشرة، بما فيها تلك الناشئة عن تقصيرها بواجب عدم التسبب بأذى للأخرين خارج نطاق إقليمها، وهو ما يعرف بـ " Due Diligence"، والذي تطور بدوره من خلال المحكمة في قضية قناة كورفو بين ألبانيا والمملكة المتحدة في العام ١٩٤٩م.[٣]

ويمكن بهذا أن نصل إلى نتيجة محددة مفادها أن المحكمة من خلال حكمها في قضية نيكاراغوا قد كانت مهيأة لضم فئات أخرى غير الهجوم العسكري التقليدي في إطار التصرفات التي يمكن أن تشكل خرقا للمادة ٢(٤) من

---

(1) Milorad Petreski, The International Public Law and the Use of Force by States, Journal of Liberty and International Affairs | Vol. 1, No. 2, 2015.

(2) Doc. 784 1/1/27, 6 U.N.C.I.O Docs. (1945(

3)) ICJ, Corfu Channel Case (UK. v. Albania), Judgment, 1949 I.C.J. Rep. 4, 22 (Apr. 9); also Rorbert P. Barnidge, The Due Diligence Principle under International Law, International Law Community Law Review, Vol.81, Issue 8, (2006(

الميثاق، ويجب أن نشير إلى أن موضوع النزاع أمام المحكمة في هذه القضية لم يكن في إطار الهجمات السيبرانية، وإنما كان يتمحور حول الدعم العسكري غير المباشر الذي كانت تقدمه الولايات المتحدة لمجموعات مناهضة للحكومة في نيكاراغوا، وبسبب الاتصال بين هذه المجموعات وحكومة الولايات المتحدة أقرت المحكمة بالخرق من جانب الولايات المتحدة للمادة ٢(٤) حيث حكمت المحكمة لصالح نيكاراغوا.

وانطلاقاً من المعايير آنفة الذكر والتي استندت إليها المحكمة، فيمكن لنا أن نتخيل تصوراً مشابها في حالة ادعاء دولة معينة على أخرى بشأن هجمة إلكترونية عندما تحقق هذه الهجمة معيار ال حجم والتأثير على الدولة التي تتعرض للهجوم بشرط اتصالها بالدولة المدعي عليها، وهذا ينطبق مع ما جاءت به النسخة الأولى من دليل "تالين" للعام ٢٠١١ لكي تدعم هذه النتيجة حيث جاءت القاعدة ١١ منه لتؤكد على أن "العمليات السيبرانية تعتبر استخداماً للقوة عندما يكون مستواها وتأثيرها متقارباً مع العمليات غير السيبرانية".[1] (كما سيأتي توضيحه).

(١) Michael N. Schmitt (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge University Press, 2013) at paragraph 11.

المطلب الثاني
المخاطر السيبرانية وحق الدفاع الشرعي
وفقا للمادة ٥١ من ميثاق الأمم المتحدة

يعتبر حظر استخدام القوة أو التهديد باستخدامها في العلاقات الدولية الوارد في المادة ٢(٤) من ميثاق الأمم المتحدة مبدأً أساسياً من مبادئ القانون الدولي العام، والتي تنص على أن: " على جميع الأعضاء في علاقاتهم أن يمتنعوا من التهديد باستخدام القوة أو استخدامها ضد سلامة الإقليم أو الاستقلال السياسي لأي دولة، أو في أي حالة أخرى تتعارض مع مبادئ الأمم المتحدة".[1]

بالرغم من ذلك فإن هذا الحظر العام لاستخدام القوة أو التهديد بها ليس مطلقاً، حيث إن بنود الميثاق أجازت استخدام القوة في حالتين استثنائيتين أوردهما الميثاق استناداً إلى ذيل المادة ٢(٤) والتي بمفهوم المخالفة تجيز استخدام القوة في الحالات التي لا تتعارض مع مبادئ الأمم المتحدة، وهذا الاستثناءان هما:

أولاً: حالة الأمن الجماعي وفقاً لقرار يصدر عن مجلس الأمن بالاستناد إلى المادة ٤٢ من الميثاق.

ثانياً: حالة الدفاع الشرعي الفردي أو الجماعي وفقاً للمادة ٥١ من الميثاق.

ووفقا لهذا يكفل القانون الدولي للدول حق الدفاع عن نفسها عبر ممارسات فردية أو جماعية ويعني ذلك أن لكل دولة الحق في أن تتصرف لنفسها

---

(١) ميثاق الأمم المتحدة، ١٩٤٥، المادة ٢(٤)

على أي نحو يكفل لها بقاءها ويضمن استقرارها، ويترتب على ذلك أن يكون من حقها أن تتخذ ما تراه مناسباً من الوسائل الدفاعية ضد الأخطار – داخلية أو خارجية – التي تهدد أمنها ومصالحها العليا،[١] نظراً لأن تلك الهجمات السيبرانية يمكن أن يكون لها أبعاد دولية خارج حدود السيادة الوطنية للدولية، لذا يلزم لمواجهتها تكاتف وتعاون دولي لتحقيق السلم والأمن الدوليين.

لذا يرى البعض أن ما قامت به دولة "إسبانيا" في مواجهة إقليم "كتالونيا" للاستقلال هو دفاع شرعي عن أمن واستقرار الدولة وقد حصلت على دعم دولي في مواجهة تلك المحاولة – وأكد غالبية الدول أن ما يحدث شأن داخلي لا يمكن التدخل فيه – وما تفعله "إسبانيا" يعد من مظاهر السيادة الوطنية احتراماً لدستورها وتشريعاتها الداخلية – مما أضعف من قوة تلك المحاولة البائسة للانفصال من جانب إقليم "كتالونيا".[٢]

تنص المادة ٥١ على أنه "لا يوجد في هذا الميثاق ما ينقص أو يضعف الحق الطبيعي للدول، بشكل فردي أو جماعي، في الدفاع عن النفس في الحالات التي تتعرض فيها إلى اعتداء مسلح. . .".[٣]

---

(١) انظر: د/ إسماعيل صبري مقلد – أصول العلاقات الدولية إطار عام – دار النهضة العربية – الطبعة الأولى – القاهرة – ٢٠٠٧ ص ٦ – ٢٠.

(٢) A. Randelzhofer، Article 51، in The Charter of the United Nations: A Commentary 661، 1995 (B. Simma ed.) 664.

(٣) المادة (٥١) من ميثاق الأمم المتحدة.

إن أبرز الشروط التي أوردتها هذه المادة يتمثل في "**وقوع اعتداء مسلح**" على دولة ما حتى تتمكن هذه الأخيرة من استخدام القوة كرد على هذا الاعتداء[٣]. إن أول ما يجب أن يثار في هذا السياق يتمثل في الاختلاف حول المصطلح المستخدم في المادة ٥١، وهو شرط الاعتداء المسلح لتفعيل الحق في الدفاع عن النفس، ومصطلح استخدام القوة أو التهديد بها حسب المادة ٢/ ٤.

ويلاحظ أن هاتين المادتين استخدمتا مصطلحات مختلفة كل منها يؤدي إلى خيارات قانونية متباينة أمام الدولة المعتدى عليها، فـ "الاعتداء المسلح" يضع الدولة المعتدى عليها أمام خيار استخدام القوة، فيكون استخدام القوة هذا في سياق الدفاع عن النفس الذي قد يكون فردياً أو جماعياً حسب المادة ٥١، أما "استخدام القوة أو التهديد بها" والذي لا يرقى إلى كونه اعتداء مسلحاً، فيضع الدولة المعتدى عليها أمام خيارات قانونية أخرى أبرزها الإجراء المضاد والذي يعطي الدولة المتضررة القدرة للرد على الاعتداء بطرق ما دون استخدام القوة.[١]

ومن الجدير ذكره أن فكرة الإجراء المضاد كخيار أمام الدولة المعتدى عليها والتي جاء النص عليها في المادة ٢٢ من مشروع مواد مسؤولية الدول عن الأفعال غير المشروعة ٢٠٠١ قد جاء مقيداً بمجموعة من الشروط أهمها

---

(١) See، Omer Elegab، The Legality of Non-forcible Counter-measures in International Law (Oxford Monographs in International Law)، 1988.

شروط التناسب بين الفعل ورد الفعل، وهذا ما أكدت عليه محكمة العدل الدولية في قضية "كوبسكوفو" للعام ١٩٩٧.[١]

وقد جاءت هذه التفرقة على اعتبار أن القانون الدولي قد وفر بعض الحماية للدولة التي تستخدم القوة في مواجهة دولة أخرى، عندما لا يرقى استخدام للقوة هذا إلى مستوى الاعتداء المسلح الفعلي.[٢]

وبالرغم من وضوح هذا الفرق في التعبيرات ونتائجه القانونية فإنه يبرز التعقيد عند رسم الخط الفاصل بين استخدام القوة والاعتداء المسلح، والذي قد يكون في كثير من الحالات غير واضح المعالم، خاصة وأن ميثاق الأمم المتحدة ذاته قد خلا من أي نص يوضح هذا الفرق، وبالرغم من ذلك، يمكن الاستهداء إلى معالم هذا الخط الفاصل من خلال العودة إلى قرار محكمة العدل الدولية في قضية نيكاراغوا، حين وصفت "الاعتداء المسلح" بأنه أخطر شكل من أشكال استخدام القوة، وفي هذا الخصوص، بينت المحكمة في هذا القرار أن المناوشات المسلحة على الحدود – مثلاً – لا ترقى إلى مرتبة الاعتداء المسلح الذي من شأنه تفعيل خيار الدفاع عن النفس وفقاً للمادة ٥١.[٣]

---

(1) ICJ, Case Concerning Gabčíkovo–Nagymaros Project (HUNGARYISLOVAKIA), 1997, paragraph 71

(2) A. Randelzhofer, Article 51, in The Charter of the United Nations: A Commentary 661, 664 (B. Simma ed.) 1995

(3) ICJ, case concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), Reports 1986, p. 191

وكررت محكمة العدل الدولية هذا الموقف في عام ٢٠٠٣ في قضية منصات النفط بين إيران والولايات المتحدة، والتي تمحورت حول حادثة قيام الولايات المتحدة بتدمير مجموعة من منصات النفط الإيرانية في منطقة الخليج لعام ١٩٨٧، وفيما إذا كانت الولايات المتحدة مسؤولة عن هذا التصرف في ضوء اتفاقية الصداقة الموقعة بين البلدين.[١]

إلى جانب ذلك جاء قرار الجمعية العامة للأمم المتحدة رقم ٣٣١٤ لعام ١٩٧٤ الخاص بتعريف العدوان مشترطاً "الخطورة الكافية" (Sufficient Gravity) كأحد متطلبات الهجوم العسكري.[٢]

أما الفقه الدولي فقد كان واضحا في تحديد هذا الخط الفاصل، وذلك يتجلى في مساهمات الفقيه الدولي "Jean-Piclet" حين جاء بمجموعة من المعايير أو المتطلبات لاعتبار الاعتداء هجوماً عسكرياً وهي النطاق والشدة والمدة الزمنية[٣]، ويلاحظ أن هناك عاملاً مشتركاً بين مجمل هذه التعريفات للهجوم العسكري وهو – باعتقادي – الغموض، إذ أن من الصعوبة بمكان في كثير من الحالات بناء على هذه التعاريف تحديد ما إذا كان استخدام معين للقوة يرقى إلى حد الهجوم المسلح. ولكن بالرغم من هذا الغموض، إلا أن

(1) CJ, case concerning Oil Platforms, (Islamic Republic of Iran v. United States of America), Reports 2003, p. 51.

(2) UN General Assembly Res. 3314 (XXIX), Definition of Aggression, Adopted 14 December 1974

(3) Cited in: Jeffry Car, Inside Cyber Warfare, O'Reilly Media, Inc., 2011, p.114

هذه التعاريف تقود إلى نتيجة مفادها أن كل اعتداء مسلح في ضوء المادة ٥١ يعد في الوقت ذاته استخداماً للقوة ولكن العكس غير صحيح، فالهجوم بالأسلحة الفتاكة مثلاً يعد استخداماً للقوة وهجوماً مسلحاً في آن واحد، وبالتالي يجيز تفعيل المادة ٥١ لأنها قد حققت الشرط الوارد في المادة.

وتجدر الإشارة إلى أن تفعيل المادة ٥١ واللجوء إلى الدفاع عن النفس في مواجهة هجوم مسلح لا يعني بأية حال أن الدولة التي تدافع عن نفسها غير مقيدة في طريقة رد الهجوم، بل على العكس من ذلك، لقد تضمنت قواعد العرف الدولي، إلى جانب المادة ٥١ من ميثاق الأمم المتحدة مجموعة من الشروط الواجب توافرها حتى يبقى التصرف متوافقاً مع أحكام المادة، وهذه الشروط هي أولاً: الضرورة، وثانياً التناسب، وثالثاً الفورية.(١)

أما شرط الضرورة فيقصد به الحالة التي تجبر فيها الدولة على اللجوء للدفاع عن النفس باستخدام القوة، حيث لم يعد اللجوء إلى "الطرق السلمية" لفض النزاع بحسب الفصل السادس من الميثاق خياراً(٢)، أو أن هذه الطرق قد تم اللجوء إليها ولكنها أثبتت عدم فعاليتها في مواجهة الدولة

(١) أكدت على هذه الشروط محكمة العدل الدولية في قرارها في قضية نيكاراغوا ١٩٨٦ وأيضا في رأيها الاستشاري في قضية الأسلحة النووية ١٩٩٦.

(٢) تحديدا المادة ٣٣ والتي حددت أن هذه الطرق تشمل المفاوضات والتحقيق والوساطة والتوفيق والتحكيم والوسائل القضائية بالإضافة إلى الوكالات الإقليمية.

الأخرى[١]، ويضاف إلى ذلك أن شرط الضرورة قد جاء كمساحة إضافية للتأكد من نية الدولة المهاجمة والظروف التي تحيط بالهجوم، إذ خلال هذه المساحة الزمنية تعطي الدولة المعتدية فرصة إضافية يمكن أن تثبت خلالها – مثلاً – أن الاعتداء لم يكن مقصوداً وأنها لا تسعى إلى حرب مع الدولة الأخرى.

وأما التناسب فإن معناه يتجسد في مصطلح "الدفاع" والدفاع يعني اتخاذ الإجراءات اللازمة والضرورية لرد الاعتداء وعدم تجاوزها، وهذا يتحقق في شبه التماثل بين الاعتداء والإجراءات المتخذة لرده من لدن الدولة المعتدى عليها، وأن لا تتجاوز الإجراءات المتخذة الهدف التي يجب أن تسعى وراءه الدولة المعتدى عليها، وهو تحقيق الأمن والسلم الدوليين.[٢]

أما شرط الفورية فيقصد به أساساً أن لا تفوت الدولة المعتدى عليها فترة زمنية طويلة على الاعتداء قبل أن تقوم باتخاذ إجراءات الدفاع عن النفس، لأنه في هذه الحالة سوف ينتفي المنطق من إعطاء الدولة الحق في الدفاع عن نفسها دون اللجوء إلى مجلس الأمن صاحب السلطة الأساسية في حفظ الأمن والسلم الدوليين.

---

(1) Lee Stuesser, Active Defense: State Military Response to International Terrorism, 17, California Western International Law Journal, 1987, p.31.

(2) Micheal Newton & Larry May, Proportionality in International Law, Oxford University Press, 2014; Arbitral Award in the Naulilaa Case 1928, 2 Reports of the International Arbitral Awards 1011-1028.

وبالرغم من وضوح هذا الفرق في التعبيرات ونتائجه القانونية فإنه يبرز التعقيد عند رسم الخط الفاصل بين استخدام القوة والاعتداء المسلح، والذي قد يكون في كثير من الحالات غير واضح المعالم، خاصة وأن ميثاق الأمم المتحدة ذاته قد خلا من أي نص يوضح هذا الفرق، وبالرغم من ذلك، يمكن الاستهداء إلى معالم هذا الخط الفاصل من خلال العودة إلى قرار محكمة العدل الدولية في قضية نيكاراغوا، حين وصفت "الاعتداء المسلح" بأنه أخطر شكل من أشكال استخدام القوة، وفي هذا الخصوص، بينت المحكمة في هذا القرار أن المناوشات المسلحة على الحدود – مثلاً – لا ترقى إلى مرتبة الاعتداء المسلح الذي من شأنه تفعيل خيار الدفاع عن النفس وفقاً للمادة ٥١.[١]

وكررت محكمة العدل الدولية هذا الموقف في عام ٢٠٠٣ في قضية منصات النفط بين إيران والولايات المتحدة، والتي تمحورت حول حادثة قيام الولايات المتحدة بتدمير مجموعة من منصات النفط الإيرانية في منطقة الخليج لعام ١٩٨٧، وفيما إذا كانت الولايات المتحدة مسؤولة عن هذا التصرف في ضوء اتفاقية الصداقة الموقعة بين البلدين.[٢]

---

(1) ICJ, case concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), Reports 1986, para. 191.

(٢) ICJ ،case concerning Oil Platforms ،(Islamic Republic of Iran v. United States of America) ،Reports 2003 ،p. 51.

إلى جانب ذلك جاء قرار الجمعية العامة للأمم المتحدة رقم ٣٣١٤ لعام ١٩٧٤ الخاص بتعريف العدوان مشترطاً "الخطورة الكافية" (Sufficient Gravity) كأحد متطلبات الهجوم العسكري[٢].

أما الفقه الدولي فقد كان واضحا في تحديد هذا الخط الفاصل، وذلك يتجلى في مساهمات الفقيه الدولي "Jean-Piclet" حين جاء بمجموعة من المعايير أو المتطلبات لاعتبار الاعتداء هجوماً عسكرياً وهي النطاق والشدة والمدة الزمنية،[1] ويلاحظ أن هناك عاملاً مشتركاً بين مجمل هذه التعريفات للهجوم العسكري وهو – باعتقادي – الغموض، إذ أن من الصعوبة بمكان في كثير من الحالات بناء على هذه التعاريف تحديد ما إذا كان استخدام معين للقوة يرقى إلى حد الهجوم المسلح. ولكن بالرغم من هذا الغموض، إلا أن هذه التعاريف تقود إلى نتيجة مفادها أن كل اعتداء مسلح في ضوء المادة ٥١ يعد في الوقت ذاته استخداماً للقوة ولكن العكس غير صحيح، فالهجوم بالأسلحة الفتاكة مثلاً يعد استخداماً للقوة وهجوماً مسلحاً في آن واحد، وبالتالي يجيز تفعيل المادة ٥١ لأنها قد حققت الشرط الوارد في المادة.

وتجدر الإشارة إلى أن تفعيل المادة ٥١ واللجوء إلى الدفاع عن النفس في مواجهة هجوم مسلح لا يعني بأية حال أن الدولة التي تدافع عن نفسها غير مقيدة في طريقة رد الهجوم، بل على العكس من ذلك، لقد تضمنت قواعد العرف الدولي، إلى جانب المادة ٥١ من ميثاق الأمم المتحدة مجموعة من

(1) Cited in: Jeffry Car, Inside Cyber Warfare, O'Reilly Media, Inc., 2011, p.114.

الشروط الواجب توافرها حتى يبقى التصرف متوافقاً مع أحكام المادة، وهذه الشروط هي أولاً: الضرورة، وثانياً التناسب، وثالثاً الفورية.[١]

أما شرط الضرورة فيقصد به الحالة التي تجبر فيها الدولة على اللجوء للدفاع عن النفس باستخدام القوة، حيث لم يعد اللجوء إلى "الطرق السلمية" لفض النزاع بحسب الفصل السادس من الميثاق خياراً،[٢] أو أن هذه الطرق قد تم اللجوء إليها ولكنها أثبتت عدم فعاليتها في مواجهة الدولة الأخرى[٣]، ويضاف إلى ذلك أن شرط الضرورة قد جاء كمساحة إضافية للتأكد من نية الدولة المهاجمة والظروف التي تحيط بالهجوم، إذ خلال هذه المساحة الزمنية تعطي الدولة المعتدية فرصة إضافية يمكن أن تثبت خلالها – مثلاً – أن الاعتداء لم يكن مقصوداً وأنها لا تسعى إلى حرب مع الدولة الأخرى.

وأما التناسب فإن معناه يتجسد في مصطلح "الدفاع" والدفاع يعني اتخاذ الإجراءات اللازمة والضرورية لرد الاعتداء وعدم تجاوزها، وهذا يتحقق في شبه التماثل بين الاعتداء والإجراءات المتخذة لرده من لدن الدولة المعتدى

---

(١) أكدت على هذه الشروط محكمة العدل الدولية في قرارها في قضية نيكاراغوا ١٩٨٦ وأيضا في رأيها الاستشاري في قضية الأسلحة النووية ١٩٩٦.

(٢) تحديدا المادة ٣٣ والتي حددت أن هذه الطرق تشمل المفاوضات والتحقيق والوساطة والتوفيق والتحكيم والوسائل القضائية بالإضافة إلى الوكالات الإقليمية.

(3) Lee Stuesser, Active Defense: State Military Response to International Terrorism, 17, California Western International Law Journal, 1987, p.31

عليها، وأن لا تتجاوز الإجراءات المتخذة الهدف التي يجب أن تسعى وراءه الدولة المعتدى عليها، وهو تحقيق الأمن والسلم الدوليين.[١]

أما شرط الفورية فيقصد به أساساً أن لا تفوت الدولة المعتدى عليها فترة زمنية طويلة على الاعتداء قبل أن تقوم باتخاذ إجراءات الدفاع عن النفس، لأنه في هذه الحالة سوف ينتفي المنطق من إعطاء الدولة الحق في الدفاع عن نفسها دون اللجوء إلى مجلس الأمن صاحب السلطة الأساسية في حفظ الأمن والسلم الدوليين.[٢]

بالرغم من ذلك يمكن لهذه الفترة الزمنية أن تمتد بصورة معقلة، وفي هذا تحقيق لشرط الضرورة آنف الذكر، والذي يوجب على الدولة المعتدى عليها التحقق من نية الدولة المعتدية، وتجدر الملاحظة أن شرط الفورية ينظر إليه بنوع من الخصوصية في سياق الهجمات السيبرانية، حيث يمكن لهذه الفترة الزمنية أن تمتد، آخذين بعين الاعتبار خاصية جوهرية للهجمات السيبرانية تتمثل في التعقيد الذي يكتنف عملية التحقق من مصدر الاعتداء.

غير أن كفاءة الردع تتوقف على بعض الظروف والافتراضات التي لا ينطبق معظمها على الفضاء السيبراني. فمسألة الدفاع الشرعي (الردع) تتطلب بصورة عامة أربعة عناصر رئيسية هي: **العزو** (معرفة من المهاجم)؛

---

(1) Micheal Newton & Larry May, Proportionality in International Law, Oxford University Press, 2014; Arbitral Award in the Naulilaa Case 1928, 2 Reports of the International Arbitral Awards 1011-1028

(2) Yoram Dinstein, Computer Network Attacks and Self-Defense, 76 U.S. Naval War College of International Law Studies (2002(

والموقع (معرفة مصدر الهجوم)؛ **والاستجابة** (القدرة على الاستجابة حتى وإن تعرضت للهجوم أولاً)؛ والشفافية (إدراك العدو لقدراتك على الرد بقوة كبيرة).[١]

ومن ثم يثير الفضاء السيبراني والحرب السيبرانية مشاكل جديدة تقوض الافتراض الأساسي بوجود هذه العناصر الأربعة عند إعداد البلدان لقواعدها الدفاعية العسكرية. فتكنولوجيا المعلومات والاتصالات تسمح بزيادة عدد الطرق التي يمكن بها للمهاجم إخفاء هويته وموقعه؛ ويمكن للمهاجم استعمال وكلاء أو خدمات مثل أجهزة الإنترنت العمومية والشبكات اللاسلكية والخدمات المتنقلة مسبقة الدفع التي لا تتطلب التيقن من مستعمل الخدمة.

ويمكن أيضاً استخدام تكنولوجيا التشفير التي تعتبر من الحلول التكنولوجية الرئيسية لضمان السرية والسلامة والتيسر، لإخفاء الهوية أو على الأقل إبطاء تقدم البحث في مصدر الهجوم السيبراني. ويمكن للعمليات التقنية والسياسات التي تحد من احتجاز البيانات المتوفرة عبر حركة الإنترنت أن تساهم أيضاً في هذه المشكلة المتعلقة بالعزو والموقع.[٢]

---

(١) Tang Lan and Zhang Xin، "Can Cyber Deterrence Work؟"
في الردع السيبراني العالمي: وجهات نظر من الصين والولايات المتحدة وروسيا والهند والنرويج، أبريل ٢٠١٠ في ١، East West Institute،
www.ewi.info/system/files/CyberDeterrenceWeb.pdf .

(٢) المرجع نفسه .

المطلب الثالث
المخاطر السيبرانية وحقوق الإنسان الرقمية

حقوق الإنسان الرقمية هي حقوق الإنسان التي تسمح للفرد بالوصول إلى الإعلام الرقمي واستخدامه وإنشائه ونشره أو الوصول إلى أجهزة الحاسوب وغيرها من الأجهزة الإلكترونية أو شبكات الاتصال واستخدامها.

ويتعلق هذا المصطلح بشكل خاص بحماية وإعمال الحقوق الموجودة، مثل الحق في الخصوصية أو حرية التعبير في سياق التقنيات الرقمية الجديدة، وخصوصًا شبكة الإنترنت.[1]

ومن ثم تعد 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 السيبرانية، والحق في إنشاء التجمعات على الإنترنت، وأيضاً الحق في حماية ملكية البرامج المعلوماتية.

(1) N. Lucchi, "Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression", Journal of International and Comparative Law (JICL), Vol. 19, No. 3, 2011. at http://www.cjicl.com/uploads/2/9/5/9/2959791/cjicl_19.3_lucchi_article.pdf.

وهناك العديد من الأطر القانونية التي تدعم حقوق الإنسان كالإعلان العالمي لحقوق الإنسان لعام ١٩٤٨ في المواد(١٢، ١٨ ، ١٩)[١] ، وكذا العهد الدولي الخاص بالحقوق المدنية والسياسية، والعهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية اللذين أقرتهما الجمعية العامة في ١٦ ديسمبر ١٩٦٦، ويضاف إلى ذلك ما تم وضعه من مبادئ دولية لتطبيق حقوق الإنسان فيما يتعلق بمراقبة الاتصالات في مايو ٢٠١٤ .[٢]

وكذلك أكدت القمة العالمية لمجتمع المعلومات في إعلان المبادئ الصادر عنها في جنيف عام٢٠٠٣م[٣] على مفهوم حرية الاتصال باعتبارها قاعدة

---

(1) وتنص المادة ١٩ بالتحديد من الإعلان العالمي لحقوق الإنسان على الحق في حرية الرأي والتعبير الذي يشمل حرية استقاء المعلومات والأفكار وتلقيها ونقلها عبر أي وسيلة كانت دون التقيد بالحدود الجغرافية.

(٢) لمزيد من المعلومات مبادئ دولية لتطبيق حقوق الإنسان فيما يتعلق بمراقبة الاتصالات – مجلس الأمم المتحدة لحقوق الإنسان – جنيف – سبتمبر ٢٠١٣.

(٣) في ديسمبر عام ٢٠٠٣، تم عقد القمة العالمية حول مجتمع المعلومات تحت رعاية الأمم المتحدة . وبعد مفاوضات طويلة بين الحكومات والشركات وممثلي المجتمع المدني، تم تبني إعلان مبادئ القمة العالمية حول مجتمع المعلومات[والذي يعيد التأكيد على حقوق الإنسان وجاء فيه:" إننا نعيد تأكيدنا على شمولية كل حقوق الإنسان والحريات الأساسية وعدم تجزئتها والترابط بينها، بما في ذلك حق التطوير على النحو الموضح في إعلان فيينا. كما أننا نعيد تأكيدنا كذلك على أن الديمقراطية والتطوير المستدام واحترام حقوق الإنسان والحريات الأساسية بالإضافة إلى الحوكمة الرشيدة على كل

أساسية لمجتمع المعلومات. ويسلط الإعلان الضوء على دور الاتصالات بوصفها عملية اجتماعية أساسية وحاجة إنسانية أساسية تشكل دعامة أساسية لكل تنظيم اجتماعي. لذا ينبغي تأمين نفاذ الجميع على قدم المساواة إلى تكنولوجيا المعلومات والاتصالات.[١] وأعلنت الأمم المتحدة عن التزامها بضمان هذا النفاذ للجميع وتسخير إمكانات الثورة الرقمية تسخيراً كاملاً لتحقيق هذه الغاية.[٢]

كما جاءت القمة العالمية لمجتمع المعلومات التي عقدت في تونس في دورتها الثانية عام ٢٠٠٥ [٣] لتؤكد على الطابع العالمي لجميع حقوق الإنسان والحريات

المستويات هي عوامل مترابطة ويقوي بعضها بعضًا. كما أننا نعقد العزم كذلك على تقوية سيادة القانون في الشئون الدولية وكذلك الشئون القومية".

(١) إعلان المبادئ الصادر عن القمة في جنيف، الفقرة ٤ القمة العالمية لمجتمع المعلومات، ٢٠٠٣؛ www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf

(٢) " Ban urges greater use of digital technology to improve living conditions"، مركز أخبار الأمم المتحدة، ١٧ مايو ٢٠١٠، www.un.org/apps/news/story.asp?NewsID=34716

(٣) كانت القمة قد تم الاتفاق على عقدها بناء على قرار اتخذته الجمعية العامة للأمم المتحدة في ديسمبر ٢٠٠١، ٢٠٠٢. وعقد مؤخرا منتدى القمة العالمية لمجتمع المعلومات ٢٠٢٠ لتعزيز التحول الرقمي والشراكات العالمية لتحقيق أهداف التنمية المستدامة ويمثل مؤتمر القمة العالمي لمجتمع المعلومات ٢٠٢٠ أكبر تجمع سنوي في العالم لمجتمع "تكنولوجيا المعلومات والاتصالات من أجل التنمية". وأثبت منتدى القمة العالمية

الأساسية وعدم قابليتها للتجزئة، وتؤكد المادة (٥٥/ ف ٤ ، ٥) من إعلان مبادئ جنيف الذي يعترف بأن حرية التعبير وحرية تدفق المعلومات والمعارف والأفكار الأساسية في مجتمع المعلومات وأن هذه الحريات تعود بالنفع على التنمية [١] وأن يتم التعامل مع الفضاء الإلكتروني وفق القيم الأخلاقية والمبادئ القانونية الموجود في مختلف الأدوات الدولية.

وقد صدر في مايو ٢٠١١ تقرير تضمن **توصيات المقرر الخاص للأمم المتحدة** والتي قدمها إلى مجلس حقوق الإنسان في الجمعية العامة للأمم المتحدة، ذكر هذا التقرير أن شبكة الإنترنت هي واحدة من أقوى أدوات القرن

لمجتمع المعلومات ، الذي شارك في تنظيمه الاتحاد الدولي للاتصالات واليونسكو وبرنامج الأمم المتحدة الإنمائي والأونكتاد ، بالتعاون الوثيق مع جميع المشاركين في خط العمل للقمة العالمية لمجتمع المعلومات ، أنه آلية فعالة لتنسيق أنشطة التنفيذ بين أصحاب المصلحة المتعددين ، وتبادل المعلومات ، وإنشاء من المعرفة وتبادل أفضل الممارسات وتواصل تقديم المساعدة في تطوير الشراكات بين أصحاب المصلحة المتعددين والقطاعين العام والخاص للنهوض بأهداف التنمية. سيوفر هذا المنتدى فرصًا منظمة للتواصل والتعلم والمشاركة في مناقشات أصحاب المصلحة المتعددين والمشاورات حول تنفيذ القمة العالمية لمجتمع المعلومات. سيتم بناء جدول أعمال وبرنامج المنتدى على أساس التقديمات التي وردت خلال عملية المشاورة المفتوحة.

(١) للمزيد حول أهداف القمة ومبادئها وأطر عملها يمكن الدخول إلى موقع الأمم المتحدة على الرابط التالي:

http://www.un.org/arabic/conferences/wsis

التي تمكن من زيادة الشفافية ومن سرعة الحصول على المعلومات. وتسهيل مشاركة المواطنين في بناء مجتمع ديموقراطي. واستناداً إلى وقائع من المظاهرات الأخيرة في جميع بلدان الشرق الأوسط وشمال أفريقيا. أدت شبكة الإنترنت دوراً رئيسياً في تعبئة السكان للدعوة للتظاهر من أجل العدالة والمساواة والمساءلة واحترام أفضل لحقوق الإنسان. ويدعو التقرير جميع الدول إلى تجنب اعتماد القوانين التي تحظر الدخول إلى شبكة الإنترنت بحجج زائفة كالحاجة إلى حماية خصوصية الأفراد، والأمن القومي أو مكافحة الإرهاب.[1]

---

(١) وهذا هو مضمون ما تضمنه الإعلان الخاص باستخدام التقدم العلمي والتكنولوجي لصالح السلم وخير البشرية،اعتمد ونشر بموجب قرار الجمعية العامة للأمم المتحدة ٣٣٠٤ (د-٣٠) المؤرخ في ١٠ تشرين الثاني/ نوفمبر ١٩٧٥. حيث نص على أن:" الجمعية العامة، إذ تلحظ أن التقدم العلمي والتكنولوجي قد أصبح أحد أهم العوامل في تطور المجتمع الإنساني، وإذ تضع في اعتبارها أن التطورات العلمية والتكنولوجية، علي كونها تتيح باستمرار فرصا متزايدة لتحسين أحوال معيشة الشعوب والأمم، يمكن أن تولد في عدد من الحالات مشاكل اجتماعية، وأن تهدد كذلك ما للفرد من حقوق الإنسان والحريات الأساسية.

وإذ تري مع القلق أن المنجزات العلمية والتكنولوجية يمكن أن تستخدم لزيادة حدة سباق التسلح، وقمع حركات التحرر الوطني، وحرمان الأفراد والشعوب من حقوقهم الإنسانية وحرياتهم الأساسية، وإذ تري أيضا مع القلق أن المنجزات العلمية والتكنولوجية يمكن أن تعرض للأخطار الحقوق المدنية السياسية للفرد أو للجماعة، والكرامة البشرية، وإذ تلحظ الحاجة الملحة إلي الاستفادة كليا من التطورات العلمية

ومن ثم أصبحت شبكة الإنترنت تشكل قوة اجتماعية واقتصادية وسياسية مؤثرة في العالم. وبالمقابل فإن التحديات القانونية الناتجة عن استخدام شبكة الإنترنت قد كثرت وازدادت بحيث أصبحت الجرائم السيبرانية من الجرائم الكبرى في القرن الـ ٢١. وأصبح الإنترنت حقا من حقوق الإنسان بناء على هذا التقرير الذي صدر عن الأمم المتحدة حول شبكة الإنترنت في يونيو ٢٠١١. اعتبر أن الحصول على خدمة الإنترنت حق من حقوق الإنسان الأساسية.

ويحتوي التقرير على العديد من التوصيات التي تؤثر على موضوع الوصول إلى شبكة الإنترنت والمتعلقة بتعزيز وحماية الحق في حرية التعبير والرأي وأهم تلك التوصيات هي:-

أن شبكة الإنترنت تتيح للشخص القدرة على البحث عن المعلومات والأفكار وتلقيها والتعرف عليها من كل الأنواع بشكل فوري وبدون تكلفة وبما يتجاوز الحدود الوطنية. ومن خلال توسيع قدرات الأفراد بشدة للاستمتاع بحقوقهم في حرية الرأي والتعبير، والتي تعد "أحد عوامل التمكين" للبشر الأخرين، فإن شبكة الإنترنت تعزز التنمية الاقتصادية والاجتماعية والسياسية، كما أنها تساهم كذلك في تطوير البشرية ككل. وفي هذا الخصوص، يشجع المقرر الخاص المفوضين الأخرين بتنفيذ إجراءات

والتكنولوجية من أجل رفاهية الإنسان ولإبطال مفعول الآثار الضارة المترتبة حاليا أو التي يمكن أن تترتب في المستقبل علي بعض المنجزات العلمية والتكنولوجية.

خاصة بالمشاركة في موضوع شبكة الإنترنت فيما يتعلق بالتفويضات الخاصة بهم.[١]

وذكر التقرير أن بعض الدول اتخذت إجراءات للمنع وللترشيح تمنع وصول المستخدمين إلى محتويات بعينها على شبكة الإنترنت، إلا أن البعض الآخر قد اتخذ كذلك إجراءات لقطع الوصول إلى شبكة الإنترنت بمجملها. ويرى المفوض الخاص أن قطع شبكة الإنترنت عن مستخدميها، بغض النظر عن التبريرات التي يتم توفيرها، بما في ذلك أسس انتهاك قوانين حقوق الملكية الفكرية، أمر غير مناسب، وبالتالي فإنه يعد انتهاكا للبند ١٩/ ف٣ من المعاهدة الدولية للحقوق المدنية والسياسية.[٢] كما يدعو المقرر الخاص كل الدول إلى ضمان توفير الوصول إلى شبكة الإنترنت بصفة دائمة، بما في ذلك فترات الاضطرابات السياسية.[٣]

وعندما نأخذ في الاعتبار أن شبكة الإنترنت قد أصبحت أداة لا غنى عنها لتوفير مجموعة من حقوق الإنسان ومكافحة عدم المساواة وتسريع التنمية والتطور البشري، يجب أن نضمن أن يكون الوصول العالمي إلى شبكة الإنترنت أولوية لكل الدول. وبالتالي، يجب أن تقوم كل دولة بتطوير سياسة راسخة وفعالة، بالتشاور مع الأفراد من كل قطاعات المجتمع، بما في ذلك

---

(١) البند ٧٦ من التوصيات الـ ٨٨،التي قدمها المقرر الخاص للأمم المتحدة في مايو ٢٠١١.

(٢) البند ٧٨ من التوصيات السابقة.

(٣) البند ٧٩ من التوصيات السابقة.

القطاع الخاص ووزراء الحكومة ذوي الصلة، من أجل إتاحة شبكة الإنترنت وتسهيل الوصول لها على نطاق واسع، بالإضافة إلى جعلها متاحة لكل قطاعات المجتمع[١] ولقد أدت هذه التوصيات إلى اقتراح أن يعتبر الوصول إلى شبكة الإنترنت في حد ذاته حقًا جوهريًا من حقوق الإنسان، أو يجب اعتباره كذلك في المستقبل.

ويدعو التقرير أيضاً الدول إلى تبني سياسات فعالة وملموسة والاستراتيجيات التي يجب أن توضع بالتعاون مع الأفراد من جميع شرائح المجتمع. لجعل الإنترنت متاحا على نطاق واسع وميسرا وبأسعار معقولة للجميع. ويضيف التقرير: "وبالنظر إلى أن شبكة الإنترنت أصبحت أداة لا غنى عنها لتحقيق عدد من مبادئ حقوق الإنسان، ومكافحة عدم المساواة، وتسريع التنمية والتقدم الإنساني، ينبغي ضمان حصول الجميع على خدمة شبكة الإنترنت وأن يكون من أولويات جميع الدول".[٢]

ومن ثم فإن الفضاء السيبراني أصبح له دور بالغ الأهمية في ممارسة حقوق الإنسان، وأن أي مخاطر في هذا الفضاء تؤثر على تلك الحقوق لاسيما في الصحة البشرية والسلامة والرفاهية، بالإضافة إلى ما تقدمه شبكة المعلومات الدولية مجموعة متنوعة ومعقدة من الاستخدامات في جميع المجالات العسكرية

---

(١) البند٨٥ من التوصيات الـ ٨٨ التي قدمها المقرر الخاص للأمم المتحدة في مايو ٢٠١١.

(2) *Klang, Mathias; Murray, Andrew (2005).* Human Rights in the Digital Age. *Routledge.* ٢٤ *Oct.* ٢٠١٣ .*P.1.*

والاقتصادية والثقافية والأمنية، الأمر الذي يزيد يومياً من حالات الاعتداء على خصوصية وسرية المعلومات بقصد التجسس أو السرقة والتخريب.

ولذلك نادى البعض بضرورة إنشاء وحدات خاصة لمكافحة الجريمة المعلوماتية بواسطة الحاسب والإنترنت. أسوة بجهات البحث الجنائي الدولية "الإنتربول" لإثبات الجريمة وتحديد أدلتها وفاعليها. وإيجاد صيغة ملائمة للتعاون الدولي لمكافحة هذه الجرائم الخاصة بالحاسب وشبكة المعلومات الدولية وتبادل الخبرات والمعلومات حول هذا النوع من الجرائم ومرتكبها وسبل مكافحتها.[١]

كما أن ظهور الإرهاب على المستوى الدولي أدى إلى التذرع بمواجهته في سبيل انتهاك تلك الحقوق والحريات الرقمية مما يستوجب أن تكون حماية تلك الحقوق هي القاعدة والاعتداء عليها للحفاظ على السلم والأمن الدوليين هو على سبيل الاستثناء.

فمع كل عملية إرهابية وكل خطوة من الحرب على الإرهاب تتقلص في المقابل الحريات الشخصية حيث زيادة سطوة العامل الأمني ورجاله على العامل القانوني حين تمكن حقوق الإنسان، ولا يختلف في ذلك كون تلك الحكومات ديمقراطية أو ديكتاتورية، فالانتهاك شمل الجميع.[٢]

---

(١) انظر: د/ هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة ، ١٩٩٢، ص ٤٧.

(٢) انظر: د/ حسنين المحمدي بوادي، الإرهاب الدولي بين التجريم والمكافحة، دار الفكر العربي، ٢٠٠٦، ص ٥٤.

وعلى هذا فلا يجوز التذرع بالإرهاب في تمرير تشريعات تحد من الحقوق والحريات الفردية، واستخدام تقنيات متقدمة لمراقبة وبحث وتتبع وتحليل الاتصالات مما يحمل معه أخطاراً أخرى تتعلق بانتهاك حقوق الإنسان.

وبالرغم من محاولة إسبانيا الحفاظ على وحدة أراضيها وتطبيق واحترام دستورها الذي ينظم قواعد إجراءات محاولات الانفصال مما يجعل من ذلك شأنا داخليا لا يجوز للمجتمع الدولي التدخل فيه، ولكن ما حدث من إساءة التعامل مع حقوق الإنسان الرقمية وحقهم في التعبير عن آرائهم ومحاولة السيطرة على كل وسائل الاتصال داخل الإقليم يعد اعتداء ينتج عنه تحمل المسئولية أمام المجتمع الدولي.

خلاصة القول: أن الحقوق والحريات تتمتع بالحماية في ظل المواثيق الدولية مما لا يجوز انتهاكها والاعتداء عليها، ومع ذلك نجد أن المبالغة في الحفاظ على الأمن والاستقرار قد يؤدي إلى استباحة تلك الحقوق وانتهاكها دون تفرقة بين دول متقدمة ودول نامية مما يضعف حق الفرد في الخصوصية والتواصل بدون تدخل أو هجمات، ويتعارض مع حرية الفكر والوجدان والدين، وينتقص من حرية الرأي والتعبير، ويحد من الحق في تلقي المعلومات والأفكار ونقلها عبر أي وسيلة كانت دون التقيد بالحدود الجغرافية. ومن ثم أصبحت عملية مواجهة الهجمات السيبرانية تتطلب التوفيق ما بين الحرية والمصالح الفردية للإنسان من جانب، وبين الأمن القومي من جانب آخر.

المطلب الرابع
العمليات السيبرانية والقانون الدولي الإنساني

أفرد القانون الدولي الإنساني مجموعة من القواعد التي تهدف إلى الحد من آثار النزاعات المسلحة سواء أكانت دولية أم غير دولية، إذ تضمن مبادئ وقواعد أساسية تحكم اختيار وسائل القتال وأساليبه. وتنبثق مبادئ القانون الدولي الإنساني من فكرة مفادها أن هذه المبادئ لا تمنع الأعمال القتالية في النزاعات المسلحة، إنما وُجدت لتقييد وسائل القتال وأساليبه في هذه النزاعات.

ولهذا يتم قبول مستوى معين من العنف والخسارة في الأرواح والدمار من جانب الأطراف المتحاربة كافة كنتيجة طبيعية لمباشرة الأعمال العدائية. آخذا في اعتباره المبادئ التي تحكم سير العمليات العدائية وهي التمييز، التناسب والاحتياطات.

وفي هذا الشأن قامت اللجنة الدولية للصليب الأحمر برصد كافة التطورات التكنولوجية التي يمكن استخدامها كوسائل أو سبل للحرب، وتقييم المخاطر والتحديات التي تتولد عنها من منظور تقني وإنساني وعسكري وقانوني. وفي هذا الشأن، دعت اللجنة الدولية في العام الماضي عددًا من الخبراء من جميع أنحاء العالم للاجتماع لوضع تقييم واقعي للتكلفة البشرية المحتملة من جراء العمليات السيبرانية.[١]

(١) https://www.icrc.org/ar/doc/war-and-law/conduct-hostilities/information-warfare/overview-information-warfare.htm

وذكرت اللجنة الدولية أنها:" ترحب بقيام الخبراء بدراسة تبعات الحرب السيبرانية والقانون المنطبق عليها، وإن اللجوء إلى العمليات في الفضاء السيبراني أثناء النزاعات المسلحة يحتمل أن تكون له تبعات إنسانية وخيمة، وترى اللجنة الدولية أنه من الضروري تحديد سبل للحد من التكلفة الإنسانية للعمليات السيبرانية، لاسيما إعادة التأكيد على الصلة بين القانون الدولي الإنساني وهذه التكنولوجيا الجديدة عند استخدامها أثناء النزاعات المسلحة.[١]

وهذا ما ذكره الخبراء في دليل تالين:" أن وسائل الحرب وأساليبها تتطور مع مرور الوقت، ومن الواضح أنها لم تعد مثلما كانت عليه عند صياغة اتفاقيات جنيف عام ١٩٤٩، ولكن لا يزال القانون الدولي الإنساني منطبقا على كافة الأنشطة التي تقوم بها الأطراف أثناء النزاع المسلح وينبغي احترامه، ولا يمكن مع ذلك استبعاد حقيقة مؤداها أنه قد تكون ثمة حاجة إلى تطوير القانون لضمان توفيره الحماية الكافية للسكان المدنيين لمواكبة تطور التكنولوجيا السيبرانية، وينبغي للدول أن تقرر هذا الأمر بنفسها.[٢]

والهجوم السيبراني وفق لدليل تالين وبالاستناد إلى القانون الدولي الإنساني يعرف:" بأنه عملية إلكترونية سواء هجومية أو دفاعية يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بأعيان أو تدميرها.

---

(١) دليل تالين حول القانون الدولي المنطبق على الحرب السيبرانية من إعداد اللجنة الدولية للخبراء بدعوة من مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي (الناتو) ، مطابع جامعة كمبريدج، ٢٠١٣، ١٥٧.

(٢) المرجع السابق، نفس الموضع .

ويلزم البرتوكول الإضافي الأول كل دولة من الدول الأطراف التحقق من امتثال أي أسلحة جديدة تقوم بنشرها أو تدرس مسألة نشرها لقواعد القانون الدولي الإنساني[١]، وطالبت الدول الأطراف في اتفاقيات جنيف أثناء المؤتمر الدولي الثامن والعشرين للصليب الأحمر والهلال الأحمر بأن تخضع جميع الأسلحة الجديدة ووسائل وأساليب الحرب الجديدة لاستعراض دقيق ومتعدد التخصصات، وذلك لضمان ألا يتخطى تطور التكنولوجيا الحماية القانونية المكفولة. ويعد استخدام العمليات السيبرانية في النزاعات وما يمكن أن يترتب عليها من آثار تدخل في هذا.[٢]

حيث تتسبب الهجمات السيبرانية التي نشهدها اليوم في تكلفة اقتصادية كبيرة، وإن كان الجزء الأعظم منها ليس في إطار نزاع مسلح، ولم يتسبب لحسن الحظ في أضرار جوهرية للناس، غير أن هجمات أكثر تعقيدًا نجحت في تعطيل إمدادات خدمات أساسية لسكان مدنيين.

فقد يتمثل الاعتداء في سلسلة من الهجمات المعلوماتية على نظام الحواسيب والشبكات المعلوماتية التي تنهض بمهام التحكم بشبكات توزيع الطاقة الكهربائية الوطنية، وينشأ عن مثل هذه الهجمات تعطيل العديد من مرافق الحياة في البلاد، وسيادة الفوضى، نتيجة لانعدام مصادر الطاقة الكهربائية وشل الحركة في عموم البلاد.

---

(١) المادة ٣٦ من البرتوكول الإضافي الأول لعام ١٩٧٧.

(٢) المؤتمر الدولي الثامن والعشرين للصليب الأحمر والهلال الأحمر المنعقد عام ٢ -٦ ديسمبر/ كانون الأول ٢٠٠٣.

ولا يتوقف الأمر عند هذا الحد، حيث أن هناك الكثير من الأهداف الأخرى، كشبكات المعلومات الطبية، والتي يمكن لمهاجمتها، واختراقها ومن ثم التلاعب بها أن يؤدي إلى خسائر في أرواح المرضى من المدنيين، ويمكن أن يتحقق ذلك بمجرد قيام القراصنة بالنفاذ إلى سجلات المستشفيات والتلاعب بسجلات المرضى بشكل يؤدي إلى حقن هؤلاء بأدوية وعلاجات كانت مميتة بالنسبة لهم.

حتى لو افترضنا أن شبكة المعلوماتية الخاصة بالمؤسسات الطبية منيعة، فإن رسالة واحدة تنشر مثلاً بالبريد السيبراني، مفادها أن هناك دماء ملوثة في المستشفيات وما إلى ذلك، يمكن لها أن تحدث آثاراً مدمرة على الصعيد الاجتماعي، ويعد القطاع الصحي أكثر عرضة للهجمات السيبرانية ويتأثر كثيرًا بها. كما تأثرت قطاعات أخرى من البنية التحتية المدنية من بينها أنظمة الكهرباء والمياه والصرف الصحي. وتفيد التقارير أن هذه الهجمات تزداد تواترًا، وتتعاظم حدتها بسرعة أكبر من أي توقعات. ومن ثم لا يجوز بأي حال الهجوم علي المستشفيات المدنية المنظمة لتقديم الرعاية للجرحى والمرضي والعجزة والنساء النفاس. (١)

ومن ثم يمكن أن تتضمن الهجمات المسلحة "هجمات الفضاء السيبراني" التي يكون لها تداعيات مدنية. فالقانون الدولي الإنساني يمكن أن يطبق على هجمات الفضاء السيبراني إذا ما كانت تلك الهجمات تستهدف القتل أو

(١) اللجنة الدولية للصليب الأحمر، الحرب السيبرانية: القانون الدولي الإنساني يوفر طبقة إضافية من الحماية، ١٠ أيلول ٢٠١٩.

التدمير، وفي ذلك اختلاف كبير عن طبيعة الهجمات التقليدية. وتأتي تلك الهجمات في طبيعة وطرق مختلفة، وتتم عبر وسيط مختلف لكي تتمكن هجمات الكمبيوتر من إصابة المطارات والبنية التحتية و أنظمة الاتصالات، بما يحمل تداعيات سياسية واقتصادية واجتماعية جسيمة تتعلق بالحياة المدنية بصفة عامة، وذلك مقارنة بالهجمات التقليدية.(١)

ومن ثم فإنه بالنظر للنتائج المترتبة على تلك الهجمات التي يتم تنفيذها عبر الفضاء الإلكتروني فإنه يمكن القول بأن تلك الهجمات تخضع للقانون الدولي الإنساني في مبادئه العامة، فهجمات الفضاء الإلكتروني أوجدت تداخلا؛ فقد تقوم الدولة باستهداف الأشخاص وحرياتهم في صورة إرهاب الدولة، أو أن تتعرض الدول لمخاطر تهدد سلامتها و أمنها القومي وبنياتها الأساسية الحيوية.(٢)

وفي رأي اللجنة الدولية للصليب الأحمر أن اتفاقيات جنيف ١٩٤٩ والبروتوكول الإضافي ١٩٧٧ أخذت بعدا أكثر اتساعا في تناولها مفهوم "النزاع المسلح"؛ حيث تم تعريف النزاع المسلح بأنه:"أي خلاف ينشب بين دولتين ويقود إلى تدخل القوة المسلحة"، حتى في حالة إنكار أحد الأطراف وجود حالة الحرب. وإنه بإعادة النظر فيما يتعلق بمبد أ "النسبية" الذي

---

(١) Michael N. Schmitt, " Computer Network Attack and THE USE OF Force IN International Law, op. cit., .920.

(٢) انظر: د/ عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مرجع سابق، ٤٠.

يتحدث عن وقوع أخطار تصيب الحياة المدنية وجرحى مدنيين ومنشآت مدنية أو التسبب في وقوع كل ما سبق.[١]

وحيث إن هجمات الكمبيوتر بإمكانها توسيع مدى ومجال الهجوم، فإن فرص استهدافه المنشآت ذات الطابع المدني تكون أكبر. وهذا ما وصف ذلك على أنه يمثل ضعفا في بنية وطبيعة هجوم الفضاء يجعل من الظلم البين أن يتم النظر إليه على أنه توسع في وسائل الحرب المستخدمة وطرقها والتي تعتمد على التكنولوجيا المتقدمة. وهذا من شأنه أن يعني توسيع حجم الضرر الذي يمكن أن يلحق بالسكان المدنيين إذا ما تم التسليم بأن هجمات الفضاء السيبراني نوعا من أنواع الهجوم.[٢]

وقد اختلف الفقه حول ذلك فهناك من يرى أنه يمكن تطبيق القانون الدولي الإنساني على هذه الهجمات عن طريق القياس والاجتهاد في المقارنة. وهناك من رأى أن القانون الدولي الإنساني لا يمكن أن يطبق على تلك الهجمات التي تحمل طبيعة خاصة، وتحتاج إلى نموذج قانوني جديد يتعامل معها وينظم استخدامها، والتي تصنف على أنها نوع من الأعمال التي تقوم بها

---

(١) المرجع السابق، ص ٤١

(٢) حماية الأشخاص المدنيين والسكان في وقت الحرب" المقتطف من القواعد الأساسية لاتفاقيات جنيف وبروتكوليها، اللجنة الدولية للصليب الأحمر، ٣١ ديسمبر ١٩٨٨، www.icrc.org/web/eng/siteeng0.nsf/html/57JMJV

وأيضا د/ عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مرجع سابق ، ٤٠ - ٤٢.

دولة أو أكثر للإضرار برعايا دولة أخرى. ولا تتوقف الهجمات على عمليات القتل أو الخطف أو التدمير، وإنما تمتد إلى أي فعل من شأنه الإضرار بالأفراد بأي شكل كان. حيث لم يعد الأمر يقتصر على التصور التقليدي للصراعات المسلحة، وإنما يمتد إلى شتى الأضرار التي تترتب على هذه الأفعال، وما تمثله من تهديد للأهمية الاستراتيجية للفضاء السيبراني. (١)

تقارب هجمات الفضاء السيبراني الهجمات التقليدية في النتائج، لكنها تختلف عنها في الوسائل واستراتيجيات التنفيذ؛ حيث ينتج عن استخدامها خسائر مادية في الطرف الآخر، إلى جانب: شن حرب نفسية، وخلق حالة من شدة التنافس في الحصول على المعلومات، تطوير وامتلاك واستخدام ونقل الأسلحة الإلكترونية في الفضاء السيبراني. كما حدث تنوع في وسائل الحرب أو الصراع، وكذلك في الفاعلين في هذه الحرب من جماعات إرهابية أو شركات عاملة في تكنولوجيا المعلومات أو حكومات أو أفراد. وهذا من شأنه أن يؤدي إلى خلق حرب مفتوحة، كما يفتح الباب إلى تطوير أساليب جديدة في الحرب مستقبلا. (٢)

ويستكمل البروتوكول الأول من اتفاقية جنيف الاتفاقية الرابعة ويوسِّع نطاق حماية الأشخاص المدنيين في وقت الحرب. وتتسم المواد ٥٩-٤٨ من هذا

---

(١) James R. Hosek , at ei., Attracting the Best: How the Military Competes for Information Technology, Personnel Santa Monica), 2004, RAND: CA: RAND, 2004, P. 16.

(٢) انظر: د/ عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مرجع سابق، ٤٠ – ٤٢.

البروتوكول بأهمية خاصة. ويتمتع المدنيون بحماية عامة ضد الأخطار الناجمة عن العمليات العسكرية، ولا يجوز أن يكونوا محلاً للهجوم أو أن يتعرضوا لأعمال تستهدف بث الذعر أو لهجمات العشوائية غير موجهة إلى هدف عسكري محدد (تعتبر الهجمات التي ينتظر أن تتسبب في خسائر عرضية في الأرواح البشرية، أو إصابات، أو إتلاف للأعيان المدنية بشكل يفرط في تجاوز الأهداف العسكرية هجمات عشوائية)، ولا تكون الأعيان المدنية محلاً للهجوم أو لعمليات الثأر؛ وإذا ثار الشك حول عين ما فيجب اعتبارها مدنية .[١]

ويحظر ارتكاب أي من الأعمال العدائية الموجهة ضد الآثار التاريخية أو الأعمال الفنية أو أماكن العبادة[٢]. ومن المحظور مهاجمة الأعيان التي لا غنى عنها لبقاء السكان المدنيين (مثل المواد الغذائية، والمناطق الزراعية، والمحاصيل، والماشية، ومرافق مياه الشرب وشبكاتها، وأشغال الري.[٣]

ولا تكون الأشغال الهندسية أو المنشآت التي تحوي قوى خطرة، ألا وهي السدود والجسور والمحطات النووية، محلاً للهجوم، حتى ولو كانت أهدافاً عسكرية مشروعة، إذا كان من شأن مثل هذا الهجوم أن يتسبب في انطلاق "قوى خطرة ترتب خسائر فادحة بين السكان المدنيين"[٤].

---

(١) المادتين (٥١/ ٥٢) من البروتوكول الأول.

(٢) المادة (٥٣) من البروتوكول الأول.

(٣) (المادة ٥٤) من البروتوكول الأول.

(٤) (المادة ٥٦) من البروتوكول الأول.

وتبذل رعاية متواصلة من أجل تفادي السكان المدنيين، وعلى المخطط لهجوم أن يبذل ما في طاقته عملياً للتحقق من أن الأهداف المقرر مهاجمتها ليست أشخاصاً مدنيين أو أعياناً مدنية وأنها غير مشمولة بحماية خاصة، وأن يتخذ جميع الاحتياطات المستطاعة عند تخير وسائل وأساليب الهجوم من أجل تجنب إحداث خسائر عرضية في أرواح المدنيين [١]. ويحظر على أطراف النزاع أن تهاجم بأية وسيلة كانت المواقع المجردة من وسائل الدفاع (ليس فيها عمليات أو قوات عسكرية) [٢].

وبالإضافة إلى ذلك فإن القوانين الدولية للنزاع المسلح تتضمن أحكاماً عديدة أضيفت على مر السنين لحظر استخدام التكنولوجيات مفرطة الأذى أو ذات الآثار العشوائية. فمنذ عهد بعيد يرجع إلى عام ١٨٩٩ تم اعتماد إعلانات في إطار اتفاقية لاهاي تحظر إطلاق القذائف والمتفجرات من المناطيد أو غيرها من الوسائل الجديدة المماثلة، [٣] واستخدام القذائف التي تشتمل على

(١) (المادة ٥٧) من البروتوكول الأول.

(٢) (المادة ٥٩) من البروتوكول الأول من اتفاقية جنيف الاتفاقية الرابعة.

(٣) إعلان حول منع إطلاق القذائف والمتفجرات من المناطيد (اتفاقية لاهاي الرابعة)؛ ٢٩ يوليو عام ١٨٩٩، http://avalon.law.yale.edu/19th_century/dec99-03.asp.

نشر الغازات الخانقة أو المؤذية، [١]، واستخدام الطلقات المتمددة أو المتسطحة.[٢]

وفي عام ٢٠٠١ تم اعتماد اتفاقية حظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر، وحظرت هذه الاتفاقية طائفة واسعة من الأسلحة الخطرة، بما في ذلك الألغام، والشراك، والأسلحة الحارقة، وأسلحة الليزر المسببة للعمى، والمتفجرات من مخلفات الحرب. وبالإمكان تعديل هذه الاتفاقية لتشمل الهجمات السيبرانية ضد البنى التحتية الحيوية المحددة.

ويمكن أيضاً أن تقوم اللجنة الدولية للصليب الأحمر بتشجيع الأمم على إبرام اتفاقات ثنائية أو متعددة الأطراف بشأن عدم الاعتداء السيبراني. ويمكن أن تكون هناك التزامات متبادلة بعدم مهاجمة الهياكل الأساسية الوطنية الحساسة (لا سيما تلك التي لها أهداف إنسانية أو التي تلبي احتياجات الناس الأساسية، والتي يكفل القانون الدولي الحالي حمايتها نوعاً ما) ويمكن تأكيد ضرورة عدم الإضرار بشبكات البيانات العابرة للحدود. ومن ثم لابد من

---

(١) Declaration on the Use of Projectiles the Object of Which is the Diffusion of Asphyxiating or Deleterious Gases, The Hague Conference of 1899, 29 July 1899, http://avalon.law.yale.edu/19th_century/dec99-02.asp

(٢) Declaration on the Use of Bullets Which Expand or Flatten Easily in the Human Body, The Hague Conference, 29 July 1899, http://avalon.law.yale.edu/19th_century/dec99-03.asp.

التأكيد في صك دولي على عدم شرعية الأسلحة السيبرانية المؤذية والاستراتيجيات العدوانية لاستخدامها.

ووفق هذا التعريف الوارد في الدليل المذكور أعلاه، فقد اتفق معظم الفقهاء القانونيين على أنه قد يتحقق الضرر أيضًا بتوقف أحد الأعيان عن العمل، علاوة على الضرر المادي، وليس من المهم كيف يحدث ذلك.

ونخلص من ذلك أنه يقع على عاتق الدول أثناء سير العمليات السيبرانية التزام بتجنب الإصابات العرضية في صفوف المدنيين والإضرار بالبنية التحتية المدنية أو الحد منها على أقل تقدير، ودون التقليل من شأن التحديات ، فلا يمكن بحال استبعاد إمكانية أن يؤدي التطور التكنولوجي في المستقبل إلى تطوير أسلحة سيبرانية من شأنها التسبب في إصابات وأضرار عرضية تماثل الأسلحة التقليدية في ظروف معينة، لتحقيق الميزة العسكرية نفسها.

المبحث الثالث
الجهود الدولية لمواجهة المخاطر السيبرانية

أدى انتشار تقنيات المعلومات وكذا الجرائم المرتبطة بها إلى اهتمام الدول والمنظمات الدولية ببذل وتكثيف الجهود الرامية لمواجهة ومجابهة الخطورة التي يشكلها هذا الإجرام المستحدث لا سيما وأنه من الجرائم العابرة للحدود، وفيما يلي سوف نستعرض أهم الجهود الدولية سواء تمثل ذلك في قرارات المنظمات الدولية أو المجهودات الفقهية أو الدول.

ولذا تعمل عدد من المنظمات الدولية باستمرار لمواكبة التطورات في شأن أمن الفضاء السيبراني، وقد أسست مجموعات عمل لوضع استراتيجيات لمكافحة جرائم الإنترنت. ويستخدم مصطلح «الأمن السيبراني» لتلخيص أنشطة مختلفة كجمع المعلومات ووضع السياسات العامة والتدابير الأمنية، والمبادئ التوجيهية، وطرق إدارة المخاطر، والحماية، والتدريب، ودليل أفضل الممارسات المهنية، ومختلف التقنيات التي يمكن استخدامها لحماية شبكة الإنترنت.

ومن ثم يشمل الأمن السيبراني كافة الاستراتيجيات والسياسات المتعلقة بالمعلومات وأجهزة الكمبيوتر، والأفراد، والبنية التحتية، وبرامج المعلوماتية، والخدمات، ونظم الاتصالات السلكية واللاسلكية، ومجمل المعلومات المنقولة أو المخزنة في الأجهزة الإلكترونية. فالجهود الدولية تسعى جاهدة من خلال

الأمن السيبراني لضمان تحقيق سلامة المؤسسات والأفراد في مواجهة المخاطر الأمنية وكل ما يتعلق بشبكة الانترنت [١].

وسوف نوضح الجهود التي اتخذتها المنظمات الدولية في هذا الشأن والمساهمات الفقهية بشأن المخاطر السيبرانية فضلا عن الاستراتيجيات التي تتخذها الدول لحماية أمنها السيبراني ضد المخاطر التي تجابهها، وذلك على النحو التالي:

المطلب الأول
قرارات المنظمات الدولية

اتخذت مبادرات من قبل العديد من المنظمات الدولية منها: منظمة الأمم المتحدة (UN)، والاتحاد الدولي للاتصالات (ITU)، ومنظمة التعاون الاقتصادي والتنمية (OECD)، ومنظمة الدول الأميركية (OAS)، وغيرها .

وأهم هذه الجهود على المستوى الدولي قرارات الأمم المتحدة المختلفة لمنع الجرائم السيبرانية ومكافحتها، وجهود الإتحاد الدولي للاتصالات بشأن توحيد آليات تطوير الاتصالات السلكية واللاسلكية، وأما المبادرة الأكثر تقدمًا لتنظيم الشبكة العنكبوتية ومحاربة الجرائم السيبرانية فهي اتفاقية بودابست بشأن الجرائم السيبرانية والاتصالات، وكذلك هناك قرارات مهمة في هذا الشأن صادرة عن بعض المنظمات الأخرى. وهذا ما سوف أتناوله على النحو التالي:-

---

(١) United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org

أ. قرارات الأمم المتحدة .

ب. الاتحاد الدولي للاتصالات.

ج. اتفاقية بودابست لمقاومة جرائم السيبرانية والاتصالات ٢٠٠١.

د. قرارات بعض المنظمات الأخرى.

أ. **قرارات الأمم المتحدة**

هناك العديد من القرارات الصادرة عن منظمة الأمم المتحدة في مجموعة من المجالات ذات الصلة بأمن الفضاء السيبراني نوضح منها:

أولاً: قرارات الجمعية العامة للأمم المتحدة:

تعد أبرز قرارات الجمعية العامة للأمم المتحدة في هذا المجال هى:

- القرار ٥٧/ ٢٣٩ الصادر عن الجمعية العامة للأمم المتحدة في ٢٠ كانون الأول/ ديسمبر ٢٠٠٢ ، بشأن إرساء ثقافة عالمية للأمن السيبراني، حيث اعتمدت فيه قراراً بشأن الأمن السيبراني والذي سلمت فيه بضرورة دعم الجهود الوطنية بتبادل المعلومات والتعاون في هذا المجال على الصعد الوطنية والإقليمية والدولية، كي يتسنى التصدي الفعال لما تتسم به هذه التهديدات السيبرانية، بصفة متزايدة، من طابع عابر للحدود الوطنية. ويشهد هذا القرار على التزام العالم بإنشاء ثقافة عالمية للأمن السيبراني. وأهم ما في القرار أنه يؤكد أن الأمن السيبراني للهياكل الأساسية الحيوية للمعلومات مسؤولية ملقاة على عاتق الحكومات ومجال يجب عليها أن تحمل فيه لواء الصدارة وطنياً، بالتنسيق مع أصحاب المصلحة ذوي الشأن

- القرار ٥٨/ ١٩٩ الصادر عن الجمعية العامة للأمم المتحدة في ٣٠ كانون الثاني/ يناير ٢٠٠٤، بشأن إرساء ثقافة عالمية للأمن السيبراني وحماية البنية التحتية الأساسية للمعلومات.
- القرارين ٥٥/ ٦٣ و٥٦/ ١٢١ الصادرين عن الجمعية العامة للأمم المتحدة، اللذين يضعان الإطار القانوني بشأن مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية.
- القرار رقم ٦٥/ ٤١ والذي صادقت الجمعية العامة للأم المتحدة عليه في كانون الأول/ يناير ٢٠١١ على تقرير فريق الخبراء الحكوميين في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. وتضمنت استنتاجات فريق الخبراء من بينها ما ذكرته من أن هناك دول تستحدث تكنولوجيا المعلومات والاتصال كوسائل للحرب والاستخبارات، وتلفت اللجنة الدولية في هذا الصدد انتباه الدول إلى عواقب الحرب السيبرانية. وهي مجموعة من الهجمات على شبكة الحواسيب خلال حالات النزاع المسلح، وقد تشمل هذه العواقب سيناريوهات كارثية مثل التشويش على نظم مراقبة الملاحة الجوية والتسبب بتصادم الطائرات أو تحطمها، أو قطع إمدادات الكهرباء أو الماء على السكان المدنيين، أو إلحاق أضرار بالمرافق الكيمائية أو النووية. وتذكر اللجنة الدولية بالتزام كل الأطراف في النزاعات المسلحة باحترام قواعد القانون الدولي الإنساني إذا لجأت إلى وسائل وأساليب الحرب السيبرانية ومن هذه القواعد مبادئ التمييز والتناسبية والحيطة.[1]

(١) بيان اللجنة الدولية للصليب الأحمر للأمم المتحدة،٢٠١١ بشأن المناقشات العامة لكافة بنود جدول الأعمال في ما يتعلق بنزع السلاح والأمن، الجمعية العامة للأمم المتحدة، الدورة

- القرارات ٧٠/ ٥٣ في ٤ كانون الأول / ديسمبر ١٩٩٨، و٤٩/ ٥٤ في ١ كانون الأول / ديسمبر ١٩٩٩، ٢٨/ ٥٥ في ٢٠ تشرين الثاني / نوفمبر ٢٠٠٠، و١٩/ ٥٦ في ٢٩ تشرين الثاني / نوفمبر ٢٠٠١، و٥٣/ ٥٧ في ٢٢ تشرين الثاني / نوفمبر ٢٠٠٢، و٣٢/ ٥٨ في ١٨ كانون الأول / ديسمبر ٢٠٠٣ حول موضوع التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي.
- القرارات ٦٣/ ٥٥ في ٤ كانون الأول / ديسمبر ٢٠٠٠، و٢١/ ٥٦ في ١٩ كانون الأول / ديسمبر ٢٠٠١ بشأن مكافحة استخدام نظام المعلومات الإدارية الجنائية لتقنية المعلومات. يدعو هذا القرار الدول الأعضاء، عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات، على أن تأخذ بالاعتبار عمل لجنة منع الجريمة والعدالة الجنائية.

وتدعو الجمعية العامة في قراراتها المختلفة - التي غالبًا ما تكون مماثلة لقرارات الاتحاد الدولي للاتصالات - الدول الأعضاء، إلى إرساء ثقافة عالمية للأمن السيبراني وحماية البنية التحتية الأساسية للمعلومات ، ووضع القوانين الوطنية والسياسات العامة لمكافحة إساءة استعمال تكنولوجيا المعلومات، وأن تأخذ في اعتبارها عواقب الحرب السيبرانية.

٦٦، اللجنة الأولى، البندان ٨٧ و١٠٦ من جدول الأعمال، بيان اللجنة الدولية للصليب الأحمر، نيويورك، ١١ تشرين الأول/ أكتوبر ٢٠١١.

ثانيا: قرارات المجلس الاقتصادي والاجتماعي:

-قرارات المجلس الاقتصادي والاجتماعي ٢٠٠٦/ ٤٦ ، ٢٠٠٧/ ٨ ، ٢٠٠٨/ ٣ ،٢٠٠٩/ ٧ والتي أحاطت فيه اللجنة المعنية بتسخير العلم والتكنولوجيا لأغراض التنمية علماً بنتائج تنفيذ مؤتمر القمة العالمي لمجتمع المعلومات، استناداً إلى ما ورده من مساهمات من كيانات الأمم المتحدة ذات الصلة وغيرها من الكيانات، حسب الاقتضاء.

فضلا عن ذلك افتتح المجلس الاقتصادي والاجتماعي دورته لعام ٢٠١٠ بجلسة إعلامية عن التحديات التي يطرحها الأمن السيبراني، فضلاً عن التهديدات والفرص التي يتيحها استخدام الإنترنت الآخذ في الاتساع. وقد شدد المجلس من بين عدة أمور على الحاجة إلى اتخاذ مبادرات دولية تكفل تبادل المعلومات وأفضل الممارسات والتدريب والبحث. وإضافة إلى ذلك، أعلن المشاركون في المناقشة أنه يتعين على الأمم المتحدة أن "توحد أداءها" بشأن هذه القضية، مما سيؤدي حتماً إلى زيادة التعاون بين البلدان بل وبين الدول والقطاع الخاص أيضاً لضمان الأمن السيبراني.[1] وحذروا من النطاق الدولي لحرب سيبرانية فعلية وعواقبها الوخيمة سوف تحدث بشكل خطير إن

---

(١) المجلس الاقتصادي والاجتماعي الدورة الموضوعية لعام ٢٠١٠ نيويورك، ٢٨ حزيران/ يونيه - ٢٣ تموز/ يوليه ٢٠١٠ البند ١٣(ب) من جدول الأعمال المؤقت المسائل الاقتصادية والبيئية: تسخير العلم والتكنولوجيا لأغراض التنمية والتقدم المحرز في تنفيذ ومتابعة نتائج مؤتمر القمة العالمي لمجتمع المعلومات على الصعيدين الإقليمي والدول.

لم يتم تدارك هذا الأمر، ومن ثم لابد أن تكون هناك استجابة منسقة بين الدول ؛ ولا تكفي الآن استراتيجيات اعتماد حلول على أساس مخصص وتقوية الدفاع.[١]

ودعا القرار أيضاً إلى اتباع نهج قائم على إدراك المخاطر، بحيث يحاط جميع أصحاب المصلحة علماً بالمخاطر ذات الصلة والتدابير الوقائية والردود الفعالة على نحو مناسب، كلٌ في إطار الدور المنوط به. وأشار القرار إلى أن الجهود الوطنية الرامية إلى حماية الهياكل الأساسية الحيوية للمعلومات تستفيد من التقييم الدوري للتقدم الذي تحرزه هذه الجهود.

وطالب القرار بمزيد من العناية لموضوع الأمن السيبراني، حيث دعا الدول الأعضاء إلى تقديم موجزات لمبادراتها الرئيسية بشأن الأمن السيبراني وحماية الهياكل الأساسية الحيوية للمعلومات، كي يتسنى إبراز "ما يتم تحقيقه من الإنجازات وأفضل الممارسات والدروس المكتسبة والاجمالات التي تتطلب مزيداً من التدابير على الصعيد الوطني". وقدم استقصاء طوعي في شكل تقييم ذاتي للأمن السيبراني الوطني باعتباره أداة يمكن أن تساعد البلدان على استعراض الجهود الوطنية المبذولة في مجال الأمن السيبراني وحماية الهياكل الأساسية الحيوية للمعلومات.

ومع تكاثر الهجمات السيبرانية، يلزم استقدام موظفين مهرة جدد لمكافحتها. ويجب أن تعترف الاستراتيجيات الوطنية للأمن السيبراني بضرورة

---

(١) المرجع نفسه (مناقشة "الأوراق المالية الرقمية" أو النظام النقدي الرقمي المستخدم في البلدان الإفريقية).

زيادة الوعي وبناء القدرة عن طريق وضع برامج تعليمية وتدريبية مناسبة في المدارس والجامعات . ويتطلب إرساء ثقافة عالمية للأمن السيبراني نظاماً تعليمياً يساعد على إيجاد مواهب تعي التحديات والصعوبات التي تواجه هيكل الإنترنت العالمي وتجيد التعامل مع الظروف المحلية المحددة . وتعد الشهادات الجامعية في مجال الأمن السيبراني، الذي ينطوي على جوانب تقنية صعبة، ضرورية للغاية وينبغي إتاحتها في الجامعات ومراكز التدريب في العالم أجمع.

ثالثا: مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء .. هافانا ١٩٩٠ بشأن الجرائم ذات الصلة بالكمبيوتر:[1]

يعتبر مؤتمر هافانا ١٩٩٠ من أبرز جهود الأمم المتحدة المتعلقة بالجرائم ذات الصلة بالكمبيوتر حيث أنه حث الدول أعضاء الأمم المتحدة على أن

---

(١) مؤتمر الأمم المتحدة لمنع الجريمة هو المحفل الأكبر والأكثر تنوُّعاً على مستوى العالم الذي يجمع الحكومات والمجتمع المدني والأوساط الأكاديمية والخبراء في مجال منع الجريمة والعدالة الجنائية. وكان لهذه المؤتمرات أثرها، على مدار ستين عاماً، في سياسات العدالة الجنائية وفي تعزيز التعاون الدولي على التصدِّي للمخاطر التي تهدِّد العالم من جراء الجريمة المنظَّمة العابرة للحدود الوطنية. من أجل التصدِّي للتحدِّيات الاجتماعية والاقتصادية وتعزيز سيادة القانون على الصعيدين الوطني والدولي ومشاركة الجمهور. وتعقد هذه المؤتمرات الدولية كل خمس سنوات ويعود منشؤها إلى عام ١٨٧٢، وكانت هذه المؤتمرات تُعقد تحت رعاية اللجنة الدولية للسجون، التي أصبحت فيما بعد اللجنة الدولية للشؤون الجزائية والإصلاحية. ثم عقد مؤتمر الأمم المتحدة الأول في جنيف في عام ١٩٥٥.
https://www.un.org/ar/events/crimecongress2015. /

تكثف جهودها لمكافحة إساءة استعمال الحاسب الآلي وذلك على المستوي الوطني وعلى المستوى الدولي:

- فعلى المستوى الوطني حث مؤتمر هافانا ١٩٩٠ الدول أعضاء الأمم المتحدة على ضرورة تجريم الأفعال التي تنطوي على المساس بسلامة المعلومات أو البيانات المعالجة والمخزنة الكترونيا عليه[١]

علاوة على ذلك، اعتمد المؤتمر الثامن قرارا بشأن الجرائم المتعلقة بالحاسوب، دعا فيه الدول الأعضاء إلى النظر في عدد من التدابير، منها تحسين الأمن الحاسوبي واتخاذ تدابير وقائية، آخذة بعين الاعتبار المشاكل المتصلة بحماية الحُرمة الشخصية ومراعاة حقوق الإنسان وحرياته الأساسية وأي آليات تنظيمية تتعلق باستخدام الحواسيب.[٢]

ضمان الدول الأعضاء النص في قوانينها الوطنية على إجراءات جنائية تلائم هذا الإجرام المستحدث في حالة عدم وجود قوانين تنطبق على نحو ملائم[٣].

- **أما جهود هذا المؤتمر على المستوى الدولي فنجد أنه قد حث** الدول الأعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من أجل

---

(١) عبد الفتاح مراد – شرح جرائم الكمبيوتر والإنترنت، مرجع سابق، ص ٢٣٧.

(٢) مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، هافانا، ٢٧ آب/ أغسطس – ٧ أيلول/ سبتمبر ١٩٩٠ :تقرير أعدته الأمانة العامة (منشورات الأمم المتحدة، (.IV.91.A الفصل الأول، الباب جيم-٩ .

(٣) انظر: د/ عبد الفتاح مراد – شرح جرائم الكمبيوتر والإنترنت مرجع سابق ، ص ٢٣٧.

مكافحة الجرائم المتصلة بالكمبيوتر بما في ذلك دخولها كأطراف في المعاهدات المتعلقة بتسليم المجرمين وتبادل المساعدة في المسائل الخاصة المرتبطة بهذه الجريمة، ونصح هذا القرار الدول الأعضاء بالعمل على أن تكون تشريعاتها ذات العلاقة بتسليم المجرمين وتبادل المساعدة في المسائل الجنائية تنطبق بشكل تام على الأشكال الجديدة للإجرام مثل الجرائم السيبرانية، وأن تتخذ خطوات محددة نحو تحقيق هذا الهدف، كما تكمل الأمم المتحدة رؤيتها بشأن الجريمة السيبرانية بصفة عامة بضرورة وضع أو تطوير[1]:

(١) معايير دولية لأمن المعالجة الآلية للبيانات.

(٢) اتخاذ تدابير ملائمة لحل إشكاليات الاختصاص القضائي التي تثيرها الجرائم السيبرانية العابرة للحدود أو ذات الطبيعة الدولية.

(٣) إبرام اتفاقيات دولية تنطوي على نصوص تنظيم وإجراءات التفتيش والضبط المباشر الواقع عبر الحدود، على الأنظمة السيبرانية المتصلة فيما بينها والأشكال الأخرى للمساعدة المتبادلة مع كفالة الحماية في الوقت ذاته لحقوق الأفراد وحرياتهم وسيادة الدولة.

رابعا: مؤتمر الأمم المتحدة لمنع الجريمة والعدالة الجنائية:

قامت لجنة الأمم المتحدة لمنع الجريمة والعدالة الجنائية في أبريل ٢٠١٠ في دورتها الثانية عشرة بصياغة مجموعة من الإعلانات التي تشمل حكماً يدعو إلى إنشاء فريق خبراء حكومي دولي لبحث مشكلة الجريمة السيبرانية

---

(١) انظر:د/ عبد الفتاح حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، مرجع سابق،ص ١٩٠.

والاستجابات الدولية لها.[١] ووفقاً لذلك، أعدت الدول الأعضاء في اللجنة المعنية بمنع الجريمة والعدالة الجنائية أثناء دورتها التاسعة عشرة، التوصية ذات الصلة التي تطلب من اللجنة إنشاء فريق خبراء حكومي دولي مفتوح العضوية لتنفيذ الحكم الصادر عن هذه اللجنة.[٢] وعلى الرغم من أن المؤتمر لم يتوصل إلى توافق في الآراء بشأن إعداد معاهدة جديدة للجريمة السيبرانية، أدت إلى إبرام اتفاقات بشأن المساعدة التقنية وبناء القدرات التي تشكل أساساً جيداً لمناقشة المزيد من الإجراءات.[٣]

---

(١) "Draft Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention andCriminal Justice Systems and Their Development in a Changing World"، الإعلان ٤٢، مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، ١٨ أبريل ٢٠١٠.

-Crime-th١٢/congress-crime/documents/org.unodc.www
A/nsessio-In/Documents/Congress

(٢) تقرير مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، UNODC، سلفادور، البرازيل، ١٩-١٢ أبريل ٢٠١٠.

www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053828e.pdf

(٣) ملخص النتائج المتعلقة بالجريمة السيبرانية: مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، مشروع عن الجريمة السيبرانية، ٢٦ أبريل ٢٠١٠.

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/2079_UNCC_cyberoutcome.pdf

ب: الاتحاد الدولي للاتصالات "I TU":[١]

بغية معالجة مسألة الأمن السيبراني المتنامية، قام الاتحاد الدولي للاتصالات بإنشاء فريق متخصص معني بالشبكات الذكية من أجل جمع وتوثيق المعلومات والمفاهيم التي ستكون مفيدة من أجل إعداد توصيات لدعم تلك الشبكات من منظور الاتصالات.[٢]

---

(١) الاتحاد الدولي للاتصالات هو وكالة الأمم المتحدة الرائدة في قضايا تكنولوجيا المعلومات والاتصالات ونقطة التنسيق العالمية للحكومات والقطاع الخاص بشأن تطوير الشبكات والخدمات. ويتكون هذا الإتحاد من ١٩٢ دولة و٧٠٠ شركة من القطاع الخاص والمؤسسات الأكاديمية، ويعتبر منبراً "استراتيجياً" للتعاون بين أعضائه باعتباره وكالة متخصصة داخل الأمم المتحدة حيث يعمل الاتحاد على مساعدة الحكومات في الاتفاق على مبادئ مشتركة تفيد الحكومات أو الصناعات التي تعتمد على تكنولوجيا المعلومات والبنية التحتية للاتصالات.

(٢) والفرق المتخصصة هي أداة من أدوات الاتحاد التي تعزز برنامج عمل لجان الدراسات من خلال توفير بيئة عمل بديلة لتطوير المواصفات بسرعة في مجالات عملها. مما يجعلها مثالية للتكنولوجيات المتغيرة والمتطورة بسرعة مثل الشبكات الذكية. ويتألف الفريق المتخصص المعني بالشبكة الذكية من ممثلين من مختلف الدول الأعضاء وسيقوم بالتعاون مع مجتمعات الشبكة الذكية في جميع أنحاء العالم (مثل معاهد البحوث والمنتديات والأوساط الأكاديمية).

لمزيد من المعلومات بشأن الفرق المتخصصة التابعة لقطاع تقييس الاتصالات ، يرجى زيارة الموقع: www.itu.int/ITU-T/focusgroups/smart/

وكان أحد الأدوار الأساسية التي أنيطت بالاتحاد الدولي للاتصالات في أعقاب القمة العالمية لمجتمع المعلومات ومؤتمر المندوبين المفوضين لعام ٢٠٠٦ يتمثل في بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات.

فقد قام رؤساء الدول والحكومات وغيرهم من قادة العالم المشاركين في القمة العالمية لمجتمع المعلومات، وكذلك الدول الأعضاء في الاتحاد، بتكليف الاتحاد باتخاذ خطوات ملموسة للحد من التهديدات وانعدام الأمن فيما يتصل بمجتمع المعلومات. ولتحقيق هذه الولاية أطلق الأمين العام للاتحاد " الدكتور حمدون إ. توريه" برنامج الأمن السيبراني العالمي في عام ٢٠٠٧ ليكون إطاراً للتعاون الدولي.

وهكذا، أطلق الأمين العام في مايو ٢٠٠٧ برنامج الأمن السيبراني العالمي (GCA) لتوفير إطار يمكن من خلاله لجميع أصحاب المصلحة تنسيق استجابة دولية للتحديات المتنامية التي يطرحها الأمن السيبراني. ويقوم برنامج الأمن السيبراني العالمي على التعاون الدولي ويرمي إلى إشراك جميع أصحاب المصلحة المعنيين في جهود متضافرة لبناء الثقة والأمن في مجتمع المعلومات. وقبل وقت قصير، أكدت الدول الأعضاء عمل الاتحاد في هذا المجال في مؤتمر المندوبين المفوضين لعام ٢٠١٠، من خلال إعادة التأكيد على برنامج الأمن السيبراني العالمي باعتباره إطاراً للتعاون الدولي في القرار ١٣٠.

ويكلف القرار الأمين العام بمواصلة استعراض التقدم المحرز في نطاق اختصاصه وتعزيزه. وبالتحديد، لاحظت الدول الأعضاء تعزيز دور الاتحاد في بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات إلى جانب

المبادرة العالمية للاتحاد بالتعاون مع الشراكة الدولية متعددة الأطراف لمكافحة الإرهاب السيبراني ومنتدى فرق التصدي للحوادث والأمن. ويقرر هذا القرار أيضاً الاستمرار في إعطاء أولوية عالية داخل الاتحاد لأعماله المتعلقة بأمن شبكات المعلومات والاتصالات.

ويقترح الأمين العام للاتحاد الدولي للاتصالات، خمسة مبادئ توجيهية لإحلال السلام وحفظه في العالم السيبراني الناشئ إدراكا منه للخطر المتنامي للهجوم السيبراني. وقد أعدت لوائح الاتصالات الدولية كإطار تنظيمي لمعالجة القضايا الناشئة والتحديات التي تصاحب عالم الاتصالات الجديد الذي تجسد في أواخر ثمانينات القرن الماضي.[١] وقد صيغت هذه اللوائح لتعزيز الكفاءة والتنمية الدوليين، فضلا عن أنها تبرز تركيز الاتحاد على حماية الحق في الاتصال وفي الوقت نفسه تفادي إلحاق الضرر بالمرافق.

وعلى غرار ذلك، تتضمن المبادئ الخمسة التي اقترحها الأمين العام للاتحاد الدولي للاتصالات فيما يتعلق بالسلام السيبراني هذه القيم الجوهرية مع تحديد إجراءات والتزامات محددة من شأنها أن تضمن السلام والاستقرار في الفضاء السيبراني. وتنص هذه المبادئ على ما يلي:[٢]

---

(١) لوائح الاتصالات الدولية: الوثائق الختامية للمؤتمر الإداري العالمي للبرق والهاتف، الاتحاد الدولي للاتصالات . http://www.itu.int/osg/spu/intset/

(٢) قرارات المؤتمر العالمي لتنمية الاتصالات لعام ٢٠١٧ (WTDC-١٧) المرفوعة إلى عناية مؤتمر المندوبين المفوضين، مؤتمر المندوبين المفوضين (PP-18) دبي، ٢٩ أكتوبر - ١٦ نوفمبر ٢٠١٨، الاتحاد الدولي للاتصالات.

١ أن تلتزم كل حكومة بإتاحة نفاذ شعبها إلى الاتصالات.

٢ أن تلتزم كل حكومة بتأمين الحماية لشعبها في الفضاء السيبراني.

٣ أن يلتزم كل بلد بعدم إيواء الإرهابيين/ المجرمين في أراضيه.

٤ أن يلتزم كل بلد بألا يكون الطرف الذي يبدأ بشن هجوم سيبراني على غيره من البلدان.

٥ أن يلتزم كل بلد بالتعاون مع غيره ضمن إطار دولي للتعاون لضمان السلام في الفضاء السيبراني.

ويهدف هذا البرنامج إلى تعزيز الثقة والأمن في مجتمع المعلومات. وقد وُضع بحيث يحقق التعاون والكفاءة ويشجع التنسيق بين جميع أصحاب المصلحة المعنيين ويستفيد من المبادرات القائمة لتجنب ازدواج الجهود. والبرنامج هو أول تحالف عالمي حقاً بين أصحاب المصلحة والقطاعين العام والخاص لمكافحة التهديدات السيبرانية.

وفي عام ٢٠٠٨ وقع الاتحاد الدولي للاتصالات والشراكة الدولية المتعددة الأطراف لمكافحة التهديدات السيبرانية (إمباكت) (IMPACT) مذكرة تفاهم رسمياً بعدها أصبح مقر شراكة إمباكت في سايبر جايا بماليزيا، الذي يضم أحدث ما توصلت إليه التكنولوجيا، المقر الفعلي للبرنامج.[١]

---

(١) إمباكت هي مبادرة دولية مشتركة بين القطاعين العام والخاص لتعزيز قدرة المجتمع الدولية على منع الهجمات السيبرانية والدفاع ضدها والتصدي لها. ويوفر هذا التعاون للدول الأعضاء في الاتحاد البالغ عددها ١٩٢ دولة وغيرها من الجهات الخبرات الفنية والتسهيلات والموارد اللازمة لتعزيز قدرات المجتمع العالمي تعزيزاً فعالاً وزيادة القدرة

د. اتفاقية بودابست لمقاومة جرائم السيبرانية والاتصالات ٢٠٠١:

اعتمد المجلس الأوروبي الطابع الدولي للجرائم السيبرانية منذ العام ١٩٧٦. وفي العام ١٩٩٦، أنشأت اللجنة الأوروبية لمشاكل الجريمة (CDPC) لجنة خبراء للتعامل مع مشاكل الجريمة السيبرانية. عملت اللجنة بين العامين ١٩٩٧، و٢٠٠٠ على مشروع الاتفاقية التي اعتمدها البرلمان الأوروبي في الجزء الثاني من جلسته العامة في شهر نيسان / أبريل ٢٠٠١. وتم التصديق على الاتفاقية من قبل ٣٠ دولة بحلول العام ٢٠١٠. (١)

وتتضمن الاتفاقية التعاون والعمل المشترك ما بين الدول الأعضاء وأعضاء القطاعات وأصحاب المصلحة ذوي الصلة ضروريان لبناء ثقافة

على منع الهجمات السيبرانية والدفاع ضدها والتصدي لها. وقد جذب هذا البرنامج منذ إطلاقه دعم واعتراف الزعماء وخبراء الأمن السيبراني في أنحاء العالم.
https://www.itu.int/ar/ITU-D/Cybersecurity/Pages/default.aspx

(١) إدراكاً من الدول بمدى خطورة الجريمة السيبرانية بوصفها جريمة عابرة للحدود فقد تم التوقيع عليها من طرف ثلاثون دولة في العاصمة المجرية "بودابست" نذكر منها: دول أعضاء من الاتحاد الأوروبي، إضافة إلى كندا، اليابان، جنوب إفريقيا، أمريكا، وجاءت هذه الاتفاقية لتعالج إشكالية دولية الجريمة السيبرانية وتجاوزها للحدود الدولية بما يساعد الدول على مكافحة هذه الجريمة وتعقب مرتكبيها والمساعدة على الاستدلال عليهم وضبطهم ، كما تشمل جوانب عديدة من جرائم الإنترنت من بينها الإرهاب، عمليات تزوير بطاقات الائتمان وغيرها.
/https://www.itu.int/ar/mediacentre/backgrounders/Pages

للأمن السيبراني وفي الحفاظ عليها، وسبل مكافحة الجرائم السيبرانية، إذ تقرر: [١]

١ -مواصلة اعتبار الأمن السيبراني في صدارة أنشطة الاتحاد ذات الأولوية، والاستمرار، في إطار مجالات اختصاصاته الرئيسية، بدراسة مسألة توفير الأمن وبناء الثقة في استعمال الاتصالات/ تكنولوجيات المعلومات والاتصالات من خلال إذكاء الوعي وتحديد أفضل الممارسات وتطوير مواد التدريب المناسبة لتعزيز ثقافة الأمن السيبراني.

---

(١) وتعود أهمية توقيع هذه الاتفاقية إلى رغبة المجتمع الدولية لإيجاد صيغة دولية لمكافحة ومواجهة هذا الإجرام المستحدث، وعلى ذلك بذلت الجهود الدولية لتحقق هذه الرغبة فبتاريخ ٢٠ نوفمبر ٢٠٠٠ تقدمت اللجنة الأوروبية لمشكلات الجريمة CDBC ولجنة الخبراء في حقل جرائم التقنية – pc-cy) -CYBERCRIME) بمشروع اتفاقية جرائم الكمبيوتر وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلال الفترة من إصدار مشروعها الأول وحتى إعداد مسودتها النهائية التي أقرت لاحقاً في بودابست ٢٠٠١ وتعرف باتفاقية بودابست ٢٠٠١ (اتفاقية الجرائم السيبرانية – سايبر كرايم) ولاشك في أن الاتفاقية قد بذل فيها جهد واسع ومميز يذكر للاتحاد الأوروبي ومجلس أوروبا لاسيما في المسائل المتعلقة بجرائم الكمبيوتر وأغراضها منذ أواخر القرن الواحد والعشرون.

للمزيد: انظر: د/ هلالي عبداللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية (معلقا عليها)، دار النهضة العربية، ط٢، ٢٠١١، ص ١٣٠.

٢-تعزيز العمل والتعاون وتبادل المعلومات مع جميع المنظمات الدولية والإقليمية ذات الصلة فيما يتعلق بالمبادرات المتصلة بالأمن السيبراني في مجالات اختصاصاتها، مع مراعاة احتياجات مساعدة البلدان النامية.

٣-تعيين نظام سريع وفعال للتعاون الدولي. الحفاظ بشكل سريع على البيانات المخزنة على أجهزة الكمبيوتر وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة على الكمبيوتر.[١]

ومن ثم تعتبر اتفاقية بودابست الاتفاقية الأوربية لمكافحة الجرائم السيبرانية والتي دخلت حيز التنفيذ عام ٢٠٠٤ [٢]، خطوة مهمة على مستوي التعاون بين الدول لوضع إطار عالمي للتعاون الدولي في مواجهة تلك الجرائم المرتبطة بالفضاء السيبراني ونجحت في ذلك من خلال إعطاء حق الانضمام للاتفاقية لأي دولة ولم يقصر ذلك الحق على الدول الأوربية فقط.

د. قرارات بعض المنظمات الدولية الأخرى

أ. جامعة الدول العربية

صدر عن **جامعة الدول العربية** قانونا استرشاديا لمكافحة جرائم تقنية المعلومات وما في حكمها عام ٢٠٠٤، ونظراً للتطور السريع والهائل في مجال

---

(1) https://www.itu.int/ar/mediacentre /

(٢) تم اعتماد الاتفاقية وتقريرها التفسيري من لدن لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة (٨ نوفمبر/ تشرين الثاني ٢٠٠١ (وفتح باب التوقيع على الاتفاقية في بودابست، في ٢٣ نوفمبر/ تشرين الثاني ٢٠٠١، بمناسبة المؤتمر الدولي حول الجريمة الإلكترونية.

الفضاء السيبراني سعت الدول العربية لتقنين وتجريم الأعمال الغير مشروعة المرتكبة من خلال استخدام الفضاء السيبراني بالتوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢١/ ١٢/ ٢٠١٠ لتعزيز التعاون بين الدول العربية لمكافحة الجرائم السيبرانية والحفاظ على أمنها وسلامة مجتمعاتها.(١)

ودعا المجلس، الدول العربية المصدقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى موافاة الأمانة الفنية للمجلس بما اتخذته من إجراءات لمواءمة تشريعاتها مع أحكام الاتفاقية وتجريم الصور المستحدثة من الجرائم الإلكترونية لمنع الإرهابيين من استخدام الإنترنت وتعزيز التعاون مع المنظمات الدولية والإقليمية المعنية بمواجهة كافة أشكال جرائم الإرهاب الإلكترونية.

كما دعا المجلس، الدول العربية إلى التعاون لمنع الإرهابيين من استغلال تكنولوجيا المعلومات والاتصالات والإنترنت للتحريض على دعم أعمالهم الإرهابية وتمويل أنشطتهم والتخطيط والإعداد لها.

وأكد المجلس، على أهمية تعزيز التعاون مع المنظمات والوكالات الدولية المتخصصة للحصول على المساعدات المطلوبة في بناء القدرات اللازمة لمواجهة

---

(١) القرار رقم (٤٩٥) الدورة ١٩، الأربعاء، ٨ تشرين الأول(أكتوبر)، ٢٠٠٣، اعتمده مجلس وزراء الداخلية العرب في دورته ٢١ بالقرار رقم ٤١٧ سنة ٢٠٠٤، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية. https://carjj.org/legal-terms/4780

خطر استخدام الإرهابيين لأسلحة الدمار الشامل أو مكوناتها ودعم أمن المطارات والموانئ والحدود.

ب. منظمة حلف شمال الأطلسي (الناتو)

دفع عجز حلف الناتو في مواجهة الهجمات السيبرانية على استونيا عام ٢٠٠٧ وجورجيا عام ٢٠٠٨ [١] إلى تكوين وحدة للدفاع السيبراني مقرها تالين عاصمة استونيا وعمل على تطوير المفهوم الاستراتيجي للحلف بحيث أصبح الفضاء السيبراني منطقة لعمليات الحلف وأن عليه أن يطور قدراته الدفاعية السيبرانية بما يشمل مساندة ودعم حلفائه الذين يتعرضون لهجمات سيبرانية وأنه وفقا لذلك فإن أي هجوم يتم علي أوروبا أو أمريكا الشمالية يعتبر هجوما ضد الجميع. [٢]

---

(١) للاطلاع على مناقشة مستفيضة عن النزاعين الإستوني والجورجي والردود والمسائل القانونية انظر:

Jody R. Westby, "The Path to Cyber Stability," Rights and Responsibiliites in Cyberspace: Balancing the Need for Security and Liberty", EastWest Institute and World Federation of Scientists, 2010 at 1,www.ewi.info/rights-and-responsiblities-cyberspace-balancing-need-security-and-liberty.

(٢) تقرير التوازن العسكري ٢٠١١ الذي يصدر سنويا عن المعهد الدولي للدراسات الاستراتيجية، هو تقرير مستقل وشامل يعرض للقدرات العسكرية العالمية واقتصاديات الدفاع لنحو ١٧٠ دولة حول العالم. يشير للتطور العسكري العالمي والقضايا الأمنية الراهنة.

ولذا نفذت الناتو السياسة الخاصة بها في مجال الدفاع السيبراني في ٢٠٠٨ من أجل حماية مواردها التكنولوجية وتلك الخاصة بالدول الأعضاء.[١] وكجزء من هذه السياسة، أنشأ الحلف هيئة معنية بإدارة الدفاع السيبراني، وفريقاً للاستجابة للحوادث الحاسوبية يكفل إرسال فرق الدعم السريع إلى فرادى البلدان الأعضاء، ومركزاً للتميز من أجل الدفاع السيبراني التعاوني.[٢] ويضم هذا المركز الذي يوجد مقره في إستونيا خبراء يضطلعون بالبحث والتدريب في مجال الأمن السيبراني. وتضم البلدان التي ترعى هذا المركز: إستونيا ولاتفيا وليتوانيا وألمانيا وإيطاليا والجمهورية السلوفاكية وإسبانيا.[٣]

وإضافة إلى ذلك، قدمت الناتو تمارين في مجال الدفاع السيبراني حيث تقوم فرق من الدول الأعضاء بمحاولة الدفاع عن الشبكات الحاسوبية الافتراضية من الهجوم السيبراني. ويُقصد بهذه التمارين زيادة فهم البيئة السيبرانية الدولية وتعزيز التعاون الدولي لمعالجة الحوادث التقنية.[٤] ووقعت الناتو أيضاً مذكرة

---

(١) الدفاع ضد الهجمات السيبرانية"، الناتو

https://www.nato.int/cps/en/natohq /

(٢) https://www.nato.int/cps/en/natolive/official_texts_

(٣) مركز التميز للدفاع السيبراني التعاوني،

www.ccdcoe. org

(٤) "Defence exercise to boost skills for countering cyber attacks"، NATO-News، 10 مايو ٢٠١٠، www.nato.int/cps/en/SID-012B6A76-D60B9579/natolive/news_63177.htm.

تفاهم بشأن الأمن السيبراني مع إستونيا والولايات المتحدة والمملكة المتحدة وتركيا وسلوفاكيا.[١]

في عام ٢٠٠٢ وضعت مجموعة بلدان الكومنولث قانوناً نموذجياً لمكافحة الجريمة السيبرانية، إضافة إلى قانون الإثبات الرقمي.

في عام ٢٠٠٩ بادرت المجموعة الاقتصادية لغرب إفريقيا، إلى إقرار توصية لمكافحة الجريمة السيبرانية لتشكيل الإطار القانوني لعمل الدول الأعضاء.

المطلب الثاني
المجهودات الفقهية لمواجهة المخاطر السيبرانية

في إطار غياب توجه رسمي من الأمم المتحدة، ظهرت اجتهادات فقهية عديدة لمعالجة مسألة الهجمات السيبرانية. والاستجابة الدولية الأهم والأبرز لمعالجة هذه المسألة جاءت فيما يسمى دليل تالين "Tallinn Manual" للقانون الدولي المنطبق على الحرب الإلكترونية والذي قام بإعداده مجموعة من أبرز فقهاء القانون الدولي، نشر الإصدار الأول منه عام ٢٠١٣، ويحتوى على ٩٥ قاعدة قانونية إرشادية لعمل أو سلوك الدول في سياق الحرب الإلكترونية [٢].

---

(١) أبرمت الناتو وإستونيا اتفاقاً بشأن الدفاع السيبراني، NATO-News، 23 أبريل ٢٠١٠، www.nato.int/cps/en/natolive/news_62894.htm

(٢) Priyanka R. Dev, " Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response", Texas International Law Journal, Vol. 50, Issue 2, 2015, P380.

وصدر الإصدار الثاني منه في العام ٢٠١٧، ويحتوي على ١٥٤ قاعدة، ليشكل مستوى أكثر اتساعاً لمعالجة العمليات الإلكترونية، ومراجعة وحسم لنقاط عدم الاتفاق في الإصدار الأول [١].

بالإضافة إلى المبادئ الواردة في إعلان إريتشي بشأن مبادئ الاستقرار السيبراني والسلام السيبراني والذي أعده فريق الرصد الدائم المعني بأمن المعلومات التابع للاتحاد العالمي للعلماء (WFS) .

الفرع الأول
دليل تالين والهجمات السيبرانية

عرف خبراء دليل تالين العمليات السيبرانية بأنها: " تلك التي تتضمن استخدام القوة أو التهديد بها ضد سلامة الأراضي أو الاستقلال السياسي لأي دولة، أو على أي وجه أخر لا يتفق ومقاصد الأمم المتحدة ". [٢]

وذكروا أن العملية السيبرانية تشكل استخداما للقوة عندما يكون حجمها و أثارها قابلة للمقارنة مع العمليات غير السيبرانية التي تصل لمستوى استخدام القوة.[٣]

---

(١) Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights", Research Paper, No. 17, Georgetown Journal of International Law, 2017, P1

(٢) القاعدة ١٠ من دليل تالين والمعنونة بـ" حظر التهديد أو استخدام القوة".
Tallinn Mnnual on The International Law Applicable To Cyber Warfare (Michael N. Schmitt ed., 2013), PP106. 107.

(٣) القاعدة ١١ من دليل تالين والمعنونة بـ" تعريف استخدام القوة ".

ففي سياق هذا النص أقر خبراء دليل تالين أنهم قد استندوا إلى معيار الحجم والتأثير في تحديد فيما إذا كانت الهجمة السيبرانية ترقى إلى استخدام غير مشروع للقوة، وأيضاً فيما إذا كان هجوماً عسكرياً يبرر الدفاع عن النفس وفقاً للمادة ٥١.

ومن ثم فوفقا لدليل تالين العمليات السيبرانية تعتبر استخداماً للقوة عندما يكون مستواها وتأثيرها متقارباً مع العمليات غير السيبرانية، وذلك اعتمادا على معيار النطاق والأثر في تحديد الدرجة التي يجب أن يصل إليها الهجوم السيبراني كاستخدام للقوة أو هجوم مسلح، وعليه، يمكن اعتبار هجوم سيبراني كهجوم مسلح إذا أحدث ضرر، أو يصل إلى درجة الشدة، والمقصود بذلك أن يحدث أضرار مادية جسيمة. وأستند خبراء تالين في اعتماد هذا الاختبار على رأى محكمة العدل الدولية في قضية "نيكاراجوا"، على أساس أنه الأنسب لتحديد الدرجة المناسبة للأعمال التي تصل إلى حد استخدام القوة والهجمات المسلحة.

وبالقياس على الهجمات السيبرانية، أتفق خبراء دليل تالين في الإصدار الثاني Tallinn Manual 2، على أن قيام دولة بتزويد قوات أو أفراد بأجهزة وتدريبهم، لشن هجمات سيبرانية ضد دولة أخرى يعد ذلك استخدام غير مشروع للقوة[1].

---

(١) Michael N. Schmitt, "Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum", Harvard National Security Journal, Vol. 8, 2017, P245.

وتعرف الحرب السيبرانية وفق خبراء دليل تالين وبالاستناد للقانون الدولي الإنساني بأنها: " وسائل وأساليب القتال التي تتألف من عمليات في الفضاء الإلكتروني ترقى إلى مستوى النزاع المسلح أو تجرى في سياقه".

وطبق هذا المعنى بصورة واضحة في عملية استخدام الهجمات السيبرانية في الحرب بين جورجيا وروسيا في أغسطس ٢٠٠٨ وفي الهجمة السيبرانية العالمية – فيروس الفدية – التي طالت أكثر من ٦٠ دولة على مستوى العالم في ٢٧ يونيو ٢٠١٧ – منهم بريطانيا ومصر وروسيا وأوكرانيا وألمانيا والمكسيك وإسبانيا إلى ظهور القضاء السيبراني على الساحة الدولية على نحو مباشر وعلني في الصراع الدولي، وكأداة ووسيلة في الصراع المسلح، لذلك ثار الجدل حول مدى اعتبار تلك الهجمات عملاً من أعمال الحرب، وتقارب الهجمات السيبرانية الهجمات التقليدية في النتائج مع اختلاف الوسائل واستراتيجيات التنفيذ، مما أدى إلى خلق حرب مفتوحة يمكن أن يكون هناك صعوبة في تحديد أطرافها، لذا تسعى الدول إلى تطوير أساليب جديدة في الحروب المستقبلية.[1]

وقد وضعت اللجنة مجموعة من الصفات التي يجب أن تتسم بها الهجمات السيبرانية حتى ترقى إلى درجة الهجوم المسلح، وبالتالي تعطي الدولة المعتدى حق الدفاع الشرعي وتفعيل المادة ٥١ من الميثاق:

حيث اعتبرت اللجنة أن أهم المعايير التي يجب الاستناد إليها في تحديد المستوى المطلوب لوصول العمليات السيبرانية إلى درجة الهجوم المسلح يتمثل

(1) Routledge: the Internet and Cyberspace of Politics and Culture of The Cyber power, Jordan Tim, London, p. 254-160

في جسامة هذا التصرف أو حدته، ومدى تأثيره على الدولة المعتدى عليها، وأن يكون هناك ضررا ماديا حالاً على الأفراد والممتلكات في الدولة المعتدى عليها بهجوم سيبراني، وفي سبيل ذلك قامت اللجنة بالمقارنة بين أثر الهجمات العسكرية التقليدية والهجمات السيبرانية استناداً إلى قياس نتائج الأخيرة، وفيما إذا كانت منتجة لأضرار مماثلة للهجمات العسكرية التقليدية أم لا.

فالهجمات السيبرانية يمكن لها أن تنتج مثل هذا الضرر المماثل للهجمات العسكرية التقليدية أو يفوقه كما لو حدث اعتداءً سيبرانيا على شبكات الكمبيوتر الخاصة بمطار إحدى الدولة مما أدى إلى مقتل الآلاف بسبب الخلل الذي أحدثته الهجمة وأدى إلى تصادم الطائرات هبوطاً وصعوداً، ففي مثل هذه الحالة تعتبر العملية السيبرانية هجوماً عسكرياً، أما تلك التصرفات التي لا تلحق مثل هذا النوع من الضرر فتخرج حسب اللجنة من دائرة الهجوم العسكري، إلا في الحالة التي تضر فيها هذه العمليات السيبرانية بمصلحة وطنية حساسة للدولة المعتدى عليها دون أن تتصل بضرر مادي محسوس.

في هذا السياق قامت اللجنة بإخراج مجموعة من العمليات السيبرانية من دائرة كونها تشكل هجوماً مسلحاً مثل تلك المؤدية إلى خلق "حالة من الانزعاج" في الدولة المتضررة، دون أن تقترن بضرر في مصلحة أساسية من مصالح الدولة، فحالة الانزعاج التي يخلفها الاعتداء على دولة ما لا يرقى إلى كونه هجوماً يستدعي تطبيق المادة ٥١، ولكن العملية السيبرانية التي تؤثر مباشرة في حركة الطائرات أو في سير العملية الانتخابية في دولة ما فإنها تضيف إلى انزعاج الدولة المعتدى عليها ضرراً بمصلحة وطنية للدولة، وبالتالي تشكل

وفقاً لهذا المعيار هجوماً عسكرياً يبيح اللجوء إلى الدفاع عن النفس وفقاً للمادة ٥١ من الميثاق.[١]

وبالعودة إلى الضرر المادي على الممتلكات أو الأفراد والذي اعتبرته اللجنة محققاً لمعيار الجسامة، يلاحظ أن هذا التوجه جاء متوافقاً أيضاً مع موقف محكمة العدل الدولية في قضية نيكاراغوا عندما فرقت بين الأعمال الأكثر خطورة والأقل خطورة، وفي هذا الشأن قررت اللجنة بأن الأضرار غير الجسيمة على الأفراد أو الممتلكات لا تشكل هجمة عسكرية، وهو ما عبرت عنه المحكمة مصطلح "الأعمال الأقل خطورة"، مثل المناوشات الحدودية إذ لا يمكن أن تعتبر شكلاً من أشكال استخدام القوة، ومع ذلك تبقى الحاجة قائمة إلى وضع معيار لتحديد ما يعتبر جسيماً وما يعتبر أقل جسامة بهذا الصدد. وحول المعنى الدقيق لمصطلح الآنية، والفرق بين الضرر الآني والضرر غير الآني في سياق العمليات السيبرانية.[٢]

وفي هذا الإطار استندت اللجنة إلى معيار "الفترة الزمنية الكافية" التي يمكن تستغلها الدولة "المعتدى عليها" لتجنب وقوع الضرر من خلال تواصلها بالدولة منشأ الاعتداء للتراجع عن هذا التصرف، فلا يمكن للتصرف وفقاً لهذا المعيار أن يرقى إلى كونه استخداماً للقوة إذا أثبت أن الدولة

---

(١) انظر: د/ رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، بحث منشور في مجلة جامعة الشارقة للعلوم القانونية، المجلد ١٥، العدد ٢، ربيع الثاني ١٤٤٠، ديسمبر ٢٠١٨، ص ٣٣٨.

(٢) المرجع السابق، ص ٣٣٩.

المستهدفة في هذا الهجوم قد فرطت بأي نافذة زمنية كان يمكن لها استغلالها لدرء الضرر، بكلمات أخرى فإن الخطر الأدنى أو الحال هو الذي سوف يقع لا محالة دون أي قدرة للدولة المعتدى ولا بأي طريق على درءه.

ويجب أن يكون الهجوم ذا أثر مباشر واضح، ويعد هذا من أهم الفروقات بين الهجمات التقليدية بالأسلحة التقليدية والهجمات السيبرانية يتمثل في أن نتائج الأخيرة قد لا تكون واضحة أي بمعنى عدم القدرة على تحديد العلاقة السببية بين الفعل والضرر، وذلك نتيجة لما يطلق عليه الانفصال الزمني بين التصرف الأساسي الذي يعد مخالفة والنتائج التي يمكن أن يرتبها هذا التصرف، وهذه صفة ملازمة للهجمات السيبرانية.

فمثلا لو أن عمليات سيبرانية قد وجهت إلى سوق الأسهم في دولة ما، مما يؤثر سلباً – ولكن ببطء شديد – في أداء الأسواق بشكل عام، وبالتالي ترتب عليه انكماش اقتصادي في تلك الدولة، ففي هذه الحالة يمكن لهذه العمليات السيبرانية أن تقرأ في إطارين، الأول: أن الانكماش الاقتصادي كان نتيجة مباشرة للعملية السيبرانية، ولكنه خرج بشكله النهائي بعد فترة طويلة من الزمن. أما الإطار الثاني: أن اقتصاد تلك الدولة كان أصلاً ضعيفاً ومتهالكاً، ولكن العملية السيبرانية لم تكن هي السبب الجوهري وراء هذا الانكماش، بل كانت كاشفة له، وبالتالي لا يوجد علاقة مباشرة بين التصرف والنتيجة.[1]

---

(١) انظر: د/ رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، المرجع السابق ، ص ٣٣٨.

استناداً إلى شرط "الاتصال المباشر" الوارد في دليل تالين، فإن هذا الإطار الأخير لا يمكن أن يرتقي بالتصرف إلى درجة الهجوم المسلح استناداً إلى عدم القدرة على تحديد العلاقة السببية بين الفعل ولضرر، ولذلك يجب عدم الخلط بين الآنية والمباشرة كشرطين متميزين جاء بهما الدليل، حيث أن الأول يتمثل في خروج الضرر إلى حيز الوجود والثاني يرتبط بالعلاقة بين التصرف والضرر.[1]

ويشار إلى أنه وبالرغم من كون هذين الشرطين متمايزين، إلا أنهما في أغلب الأحيان متلازمان بحيث من الصعوبة بمكان تصور هجمة سيبرانية غير حالة ومباشرة في ذات الوقت، فالهجوم الحال غير المباشر كان تعتقد دولة ما – مثلاً – أن هجوماً سيبرانية حالا على شبكة معلوماتية مدمرة أصلاً سيحدث بحيث لا يمكن لهذه الهجمة أن تحدث ضرراً إضافياً، لا يرقى بهذا التصرف إلى درجة الهجوم العسكري بسبب عدم الاتصال بين الفعل والنتيجة ويبقى لنا أن نتصور الحالة التي يمكن فيها أن تكون الهجمة السيبرانية مباشرة ولكنها ليست حالة وتتمثل عموماً في الأضرار الاقتصادية بعيدة المدى التي يمكن أن تقع على الدولة "المعتدى عليها".

على هذا الأساس جاء دليل تاليل متضمناً شرط العدائية، والذي يتمثل في النية خلف العملية السيبرانية، فبحسب هذا الشرط ترتقي العملية السيبرانية إلى درجة الهجوم المسلح كلما كانت الدولة المعتدى عليها قادرة على إثبات أن هذا التصرف يسعى إلى تحقيق أهداف عدائية في الدولة الأخرى، كإضعاف القدرة العسكرية من خلال التأثير على برامجها السيبرانية العسكرية.

---

(١) المرجع السابق، ص ٣٣٩.

ويعد شرط اتصال التصرف بالدولة من أهم وأبرز الشروط لنهوض المسؤولية الدولية عموماً، حيث يتضمن هذا الشرط ضرورة أن يكون التصرف صادراً عن من يمثل الدولة، سواء السلطة التشريعية أو التنفيذية أو القضائية أو أي جهة أخرى يعهد إليها مهمة القيام بعمل معين بالنيابة عن الدولة[٢]، ويثير هذا الشرط أمرين [١]:-

الأول: يتمثل في صعوبة تحديد ما إذا كان هذا العمل منسوباً للدولة فعلاً، وهذا مرتبط بالقدرة التكنولوجية المتنامية، والتي يمكن أن يمكن الدولة منشأ التصرف أن تطمس هوية الفاعل الحقيقي، إضافة إلى ذلك فإن عملية نسبة العمل الدولية تزداد تعقيداً في الحالة التي لا تكون الشبكات السيبرانية هي الوسط الذي تمت من خلاله هذه الهجمات، كإرسال فيروسات توضع مباشرة في أجهزة الحاسوب الخاصة بالدولة المستهدفة، أو في الحالة التي يستخدم فيها إقليم دولة أخرى لتنفيذ هذه الهجمات، فلنا أن نتخيل مثل أن الدولة (أ) قد استخدمت إقليم الدولة (ب) من خلال عملاء لها لتنفيذ هجمة إلكترونية في الدولة (ج) دون علم الدولة (ب).

أما السبب الثاني للإشكالية الخاصة بنسبة العمليات السيبرانية للدولة فيتمثل في الحالة التي ينسب فيها التصرف إلى مجموعة خارجة عن سلطات الدولة، ولكن هذه المجموعات استخدمت إقليم الدولة لتنفيذ العملية، حيث

---

(١) انظر: د/ رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، المرجع السابق، ص ٣٣٨.

أثارت هذه الحالة نقاشاً مستفيضاً بين لجنة الخبراء حول دليل تالين، حيث – في نهاية المطاف – أقرت اللجنة بشكل ضمني في الفقرة الثانية من القاعدة ١٣ أن التحكم الفعال هو فقط ما ينهض بالمسئولية في مواجهة الدولة مصدر الاعتداء، وهو موقف متوافق مع قرار محكمة العدل الدولية في قضية نيكاراغوا[١].

إضافة إلى الشروط السابقة، قامت اللجنة بوضع شروط أخرى تتمثل في وضوح نتائج الهجمات أو القدرة على قياسها، بمعنى قدرة الدولة المعتدى عليها تحديد الضرر الذي تسببت به الهجمة السيبرانية، إضافة إلى شرط الطابع العسكري للعملية السيبرانية وهو شرط مستمد من مجمل مواد ميثاق الأمم المتحدة الخاصة باستخدام القوة والتي تربط بين استخدام القوة وبين الطبيعة العسكرية لهذه النشاطات.

(١) ICJ, case concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), Reports 1986, para. 191.

الفرع الثاني
إعلان إيريتشي بشأن مبادئ الاستقرار السيبراني والسلام السيبراني (الصادر عن الاتحاد العالمي للعلماء)

أعد إعلان إريتشي بشأن مبادئ الاستقرار السيبراني والسلام السيبراني بواسطة فريق الرصد الدائم المعني بأمن المعلومات التابع للاتحاد العالمي للعلماء (WFS)[1]، حيث اعتمدته الجلسة العامة للاتحاد العالمي للعلماء في

---

(١) في عام ١٩٧٣ قامت مجموعة من العلماء البارزين بإنشاء الاتحاد العالمي للعلماء في إيرتشه بجزيرة صقلية. ومنذ ذلك الحين انضم كثير من العلماء الأخرين إلى الاتحاد، والاتحاد تجمع حر أخذ ينمو حتى أصبح يضم أكثر من ١٠٠٠ عالم من ١١٠ دولة. ويتقاسم جميع الأعضاء نفس الأهداف والمثل العليا ويساهمون طواعية في الدفاع عن مبادئ الاتحاد. ويُشجع الاتحاد على التعاون الدولي في العلم والتكنولوجيا بين العلماء والباحثين من كل أنحاء العالم . ويسعى الاتحاد وأعضاؤه إلى تحقيق حرية تبادل المعلومات كهدف مثالي، بحيث لا تكون الاكتشافات والتقدمات العلمية قاصرة على قلة مختارة. والهدف هو تقاسم هذه المعارف بين شعوب كل الدول ليتمتع كل شخص بفوائد تقدم العلم.

وكان إنشاء الاتحاد العالمي للعلماء ممكناً بفضل وجود مركز للثقافة العلمية أُقيم في إريتشه لتخليد ذكرى عالم الفيزياء إيتوري مايورانا باسم "مؤسسة إيتوري مايورانا ومركز الثقافة العلمية (المركز). وأصبح، هذا المركز الذي أُطلقت عليه تسمية "جامعة الألفية الثالثة" قوة تعليمية عالمية. وقام هذا المركز منذ إنشائه في عام ١٩٦٣ بتنظيم ١٢٣ مدرسة و١٤٩٧ دورة دراسية حضرها ١٠٣ ٤٨٤ مشاركاً (منهم ١٢٥ من الحاصلين على جائزة نوبل) من ٩٣٢ جامعة ومختبراً في ١٤٠ دولة.

الدورة الثانية والأربعين للحلقات الدراسية الدولية بشأن الطوارئ العالمية، في إريتشي (صقلية) في ٢٠ أغسطس ٢٠٠٩.

وكان من أبرز التقارير لهذا الاتحاد التقرير المعنون بـ :" نحو نظام عالمي للفضاء السيبراني: إدارة التهديدات من الجريمة السيبرانية إلى الحرب السيبرانية" ، والذي يعد إحدى الوثائق الرئيسية التي قدمها المجتمع المدني إلى القمة العالمية لمجتمع المعلومات التي عقدتها الأمم المتحدة في جنيف في ٢٠٠٣.

وقد نشر فريق الرصد ورقات عديدة بشأن الأمن السيبراني والحرب السيبرانية ويتناول بانتظام قضايا أمن المعلومات باعتبارها موضوعاً من

وكان مركز إيتوري مايورانا هو الكيان الذي تولد عنه الاتحاد العالمي للعلماء ببرنامج عمله لتخفيف حالات الطوارئ الكوكبية. وسارع الاتحاد العالمي للعلماء إلى تحديد ١٥ فصلاً دراسياً لأغراض الطوارئ الكوكبية وبدأ تنظيم أعمال مكافحة هذه التهديدات. ومن بين الإنجازات الرئيسية للمعهد وضع بيان إيريتشه، في عام ١٩٨٢ الذي قام بصياغته بول ديراك، وبيوتر كابيتزا وأنطونيو زيكيكي، ويعرض بوضوح المثل العليا للاتحاد كما يُقدم مجموعة من الاقتراحات لترجمة هذه المثل العليا إلى واقع عملي. وكانت إحدى العلامات البارزة الأخرى هي انعقاد سلسلة من الحلقات الدراسية الدولية بشأن الحرب النووية أثرت بشكل هائل على تقليل خطر وقوع كارثة نووية تعم الكوكب بأكمله وساهمت في نهاية المطاف في إنهاء الحرب الباردة. وفي عام ١٩٨٦، ومن خلال عمل مجموعة من العلماء البارزين (ومعظمهم أعضاء في الاتحاد) تم تأسيس المختبر العالمي التابع للمركز الدولي للثقافة العلمية في جنيف للمساعدة على إحراز الأهداف المعروضة في بيان إيريتشه.

موضوعات الطوارئ الحرجة أثناء الدورات العامة للاتحاد العالمي للعلماء التي تنعقد في شهر أغسطس من كل عام في إيريتشي. وفي أغسطس ٢٠٠٩، أعرب فريق الرصد عن قلقه من إمكانية وقوع حرب سيبرانية تُعطل المجتمع وتُسبب ضرراً لا داعي له ومعاناة لا لزوم لها ولذلك عمد إلى صياغة **إعلان إيريتشي لمبادئ الاستقرار السيبراني والسلام السيبراني**، الذي اعتمدته الجلسة العامة للاتحاد بمناسبة الدورة الثانية والأربعين للحلقات الدراسية الدولية بشأن الطوارئ في إيريتشه يوم ٢٠ أغسطس ٢٠٠٩. وتم توزيع هذا الإعلان على كل الدول الأعضاء في الأمم المتحدة.[١]

كما قام الاتحاد بترجمة المبادئ العامة التي يتضمنها القرار، وغيرها من المبادئ العامة التي أقرتها الأمم المتحدة والتي يمكن تطبيقها في البيئة السيبراني.[٢]

ويبين هذا الإعلان أن تحقيق الاستقرار السيبراني وتحقيق السلام السيبراني أمران متداخلان تداخلاً وثيقاً. ويتسم الإعلان بالإيجاز ويركز على العناصر التشغيلية الأساسية للسلام السيبراني. وهي كالتالي:

---

(١) السلام السيبراني بقلم حمدون إ. توريه (لأمين العام للاتحاد الدولي للاتصالات وفريق الرصد الدائم لأمن المعلومات)، إصدار الاتحاد العالمي للعلماء يناير ٢٠١١.

(٢) "إعلان إيريتشي بشأن مبادئ الاستقرار السيبراني والسلام السيبراني"، اتحاد العلماء العالمي، أغسطس ٢٠٠٩، على الموقع التالي:

www.ewi.info/system/files/Erice.pdf.

١- ينبغي لجميع الحكومات الاعتراف بأن القانون الدولي يضمن للأفراد التدفق الحر للمعلومات والأفكار؛ وتنطبق هذه الضمانات أيضاً على الفضاء السيبراني. وينبغي عدم فرض القيود إلا عند الاقتضاء، على أن تخضع لعملية مراجعة قانونية.

٢- ينبغي لجميع البلدان العمل معاً لوضع مدونة مشتركة للسلوك السيبراني وإطار قانوني عالمي منسق، بما في ذلك أحكام إجرائية تتعلق بالمساعدة في التحقيق والتعاون بما يكفل احترام الخصوصية وحقوق الإنسان. وينبغي لجميع الحكومات وموزودي الخدمات والمستعملين دعم الجهود المبذولة في سبيل إنفاذ القانون الدولي ضد مرتكبي الجرائم السيبرانية.

٣ -ينبغي لجميع المستعملين وموزودي الخدمات والحكومات العمل معاً لضمان ألا يستخدم الفضاء السيبراني بأي شكل من شأنه أن يفضي إلى استغلال المستعملين، لا سيما الشباب والمستضعفين منهم، من خلال العنف أو الإذلال.

٤ -ينبغي للحكومات والمنظمات والقطاع الخاص بما في ذلك الأفراد، تنفيذ برامج شاملة للأمن وتحديثها بناءً على أفضل الممارسات والمعايير المقبولة دولياً واستعمال تكنولوجيات حماية الخصوصية والأمن.

٥- ينبغي لمطوري البرمجيات والمعدات السعي إلى تطوير تكنولوجيات آمنة تعزز القدرة على التصدي وتقاوم نقاط الضعف.

٦- ينبغي للحكومات أن تشارك بفعالية في جهود الأمم المتحدة الرامية إلى النهوض بالأمن السيبراني والسلام السيبراني في العالم وأن تتفادى استعمال الفضاء السيبراني من أجل النزاعات.

ويمكن أن نستشف من وراء هذه المبادئ، ولا سيما المبدأ السادس، الإرادة الصارمة من أجل كبح إمكانية النزاعات في الفضاء السيبراني. وفي الواقع لا بد، في إطار السعي إلى السلام السيبراني، وفي ضوء الزيادة المهولة لقدرات "الحرب السيبرانية" العدوانية، من التركيز بشكل خاص على الجانب الحربي للأنشطة في الفضاء السيبراني التي تقوم بها الحكومات وجهات فاعلة غير حكومية على حد سواء.

وبناءً على ذلك، فإننا نؤيد المبادئ التالية لتحقيق الاستقرار والسلام السيبراني وحفظهما.

وقد دعا الاتحاد العالمي للعلماء منذ سنة ٢٠٠٢ إلى العمل من أجل وضع قانون عالمي للفضاء السيبراني- وأنه من الأفضل أن يكون تحت رعاية الأمم المتحدة.[١] - خاصة في مجال الاستخدامات العدوانية والعسكرية للفضاء السيبراني.

---

(١) انظر " Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwa"، تقرير وتوصيات، فريق الرصد الدائم المعني بمجتمع المعلومات والتابع لاتحاد العلماء العالمي، ١٩ نوفمبر ٢٠٠٣، تقرير مقدم إلى القمة العالمية لمجتمع المعلومات، www.itu.int/dms_pub/itu-s/md/pdf.

فضلا عن ضرورة وجود إطار قانوني لتعريف ما الذي يشكل خرقاً للسلام، وقد اقترح الأمين العام للاتحاد الدولي للاتصالات، في مفهومه الذي ينطلق من المبادئ الخمسة للاتحاد، أنه ينبغي للأمم أن تتعهد في هذا الإطار بألا تبدأ بالعدوان السيبراني ضد أمة أخرى ("عدم المبادأة")، وينبغي أن تلتزم بعدم حماية الإرهابيين السيبرانيين والمهاجمين في بلدانها دون أن تعاقبهم.

المطلب الثالث
استراتيجيات الدول لحماية أمنها من المخاطر السيبراني

أدت علاقة الفضاء السيبراني بعمل المنشآت الحيوية سواء أكانت مدنية أو عسكرية لقابلية تعرضها لهجوم سواء عن طريق استهدافها كوسيط وحامل للخدمات أو بشلل عمل أنظمتها المعلوماتية، ويكون من شأنه التأثير على القيام بوظيفتها ومن ثم فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة ونفوذ استراتيجية بالغة الأهمية سواء في زمن السلم أو الحرب. وأصبح التفوق في مجال الفضاء السيبراني عنصرا حيويا في تنفيذ عمليات ذات فاعلية في الأرض وفي البحر والجو والفضاء. واعتماد القدرة القتالية في الفضاء السيبراني على نظم التحكم والسيطرة. (١)

ولقد استجابت بلدان عديدة للتهديد الجديد للحرب السيبرانية من خلال تكليف عدد كبير من الأفراد العسكريين بمهمة التدريب والاستعداد القتال

(١) Arsenio T. Gumahad, Cyber Troops and Net War: The Profession of Arms in the Information Age. Maxwell AFB, AL: Air University, Air War College, April 1996, pp.57-156

الافتراضي.[١] ويمكن أن يشمل هذا التحول السياسي إنشاء فرق حربية للإنترنت تكون مكرسة لتحقيق الأمن السيبراني، ويمكن دمجها في وكالات استخبارات أخرى، أو حتى إنشاء قطاعات جديدة تماماً ضمن الهيكل العسكري المكرس للنشاط السيبراني.[٢] وتقام هذه العدة العسكرية الجديدة لدمج وإعداد الموارد العسكرية من أجل جميع أنواع عمليات الفضاء السيبراني.[٣] ويمكن أن تكون أيضاً مسؤولة عن تأمين الشبكات الخاصة التي تشغّل جزءاً كبيراً من العمليات العسكرية، وإن كان تركيزها في المقام الأول

---

(١) كشفت بعض البلدان عن تحولات مكثفة في ملاك الموظفين. انظر Cyber General (يشير إلى أن الولايات المتحدة أعلنت عن إعادة توزيع ٣٠ ٠٠٠ مجموعة للدفاع السيبراني). غير أن المعلومات المتعلقة بالاستراتيجيات المعتمدة في كثير من البلدان ليست متاحة بسهولة. انظر

Robert McMillan, "Black Hat Talk on China's 'Cyber Army' Pulled After Pressure", InfoWorld, 15 July 2010, http://www.infoworld.com/print/130362 .

(٢) أعلنت الولايات المتحدة على سبيل المثال، إنشاء وحدة جديدة للشؤون العسكرية السيبرانية في ٢٠٠٩. Cyber General. وأعلنت المملكة المتحدة مؤخراً إنشاء مركز لعمليات الأمن السيبراني كجزء من استراتيجيتها للأمن السيبراني. Corera.

(٣) انظر "U.S. Cyber Command Fact Sheet"، وزارة الدفاع الأمريكية، ٢٥ مايو ٢٠١٠.

https://www.defense.gov/Home/features/2010/0410_cybersec/docs/CYberFactSheet%

على حماية الشبكات العسكرية وتسيير العمليات العسكرية في الفضاء السيبراني.[١]

وتجري الولايات المتحدة سنويا محاكاة التعرض لحرب السيبرانية فيما يطلق عليها بعاصفة الحواسيب cyber storm وخصصت ٥٠٠ مليون دولار في ميزانية عام ٢٠١٢ لمواجهة التهديدات السيبرانية وعملت على تطوير أسلحة وأدوات للحرب السيبرانية تشمل فايروسات قادرة على تخريب شبكات العدو الحساسة، وذلك لتحسين درجات الاستعداد لحرب الكمبيوتر.[٢]

وأعلنت الولايات المتحدة عن جهود تصنيع لأسلحة إنترنت هجومية لمواجهة احتمال تعرضها لهجوم، وزادت تمويل الأبحاث السيبرانية من ١٢٠ مليون دولار إلى ٢٠٨ ملايين دولار عام ٢٠١٢.حيث تبلغ تكلفة الهجمات

---

(١) Siobhan Gorman, "U.S. Backs Talks on Cyberwarfare", The Wall Street Journal، 4 june 2010، http://www.wsj.online/article/com.wsj.html (مشيراً إلى أن ٩٠ بالمائة من القوة العسكرية يوفرها القطاع الخاص، وفقاً لمسؤولين عسكريين في الولايات المتحدة) (فيما بعد، Gorman"").

(٢) Ellen Nakashima, List of cyber-weapons developed by Pentagon to streamline computer warfa Washington Post, Published: June 1, 2011 .
http://www.washingtonpost.com/national/list-of-cyber-weapons-developed-by-pentagon-to-streamline-computer-warfare-by-elopedev-AGSublFH/٣١/٠٥/٢٠١١/warfare.html.print

السيبرانية ١١ بليون دولار و٩ مليون مواطن تم اختراق خصوصياتهم وتكلف الجريمة السيبرانية٨ٍ٣ بليون دولار.[١]

وأعلنت روسيا عزمها عن تطوير السلاح الجوّي والفضائي ردا على الدرع الصاروخي وخصصت ٥٩٠ مليار يورو لإعادة التسليح خلال العقد المقبل والعمل على استعادة موقع الزعامة في كافة التكنولوجيّات العسكرية [٢]

وتعد كل من السويد وفنلندا وإسرائيل من أفضل الدول التي لديها جاهزية لمواجهة الهجمات السيبرانية مقارنة بالولايات المتحدة وألمانيا وبريطانيا [٣].

فهذه التهديدات السيبرانية تتطلب التعاون الدولي، والمساعدة في التحقيق والأحكام الإجرائية والموضوعية المشتركة لمعالجتها على نحو ملائم. وإضافة إلى ذلك، من المعترف به على نطاق واسع أن التعاون الدولي يمثل أحد المتطلبات الرئيسية لضمان الأمن السيبراني على الصعيد العالمي. وفي ٢٠٠٣ و٢٠٠٥، اتفقت الدول في القمة العالمية لمجتمع المعلومات (WSIS) على

---

(١) المرجع السابق، نفس الموضع.

(٢) بوتين يطلق سباق التسلّح مع الغرب ، صحيفة الجمهورية،٢١ فبراير٢٠١٢
http://www.aljoumhouria.com/articles/print_article/29687

(٣) Brigid Grauman, Cyber-security:The vexed question of global rules, A Security & Defence Agenda report, Geert Cami, February 2012
http://www.securitydefenceagenda.org/Portals/14/Documents/Publications/SDA_Cyber_report_FINAL.pdf

ضرورة وضع أدوات تتسم بالفعالية والكفاءة على المستويين الوطني والدولي للنهوض بالتعاون الدولي بشأن الأمن السيبراني.[١]

وإزاء تزايد هذه الجرائم السيبرانية الخطيرة فقد بذلت جهوداً كبيرة لمحاربتها من مختلف جوانبها، حيث لجأت العديد من الدول إلى تشريع القوانين التي تقضي بمعاقبة المتسببين في زرع الفيروسات، كما فرضت العديد من الشركات ما يعرف "بنظام الحجر الصحي" على أجهزتها السيبرانية بحيث تمنع الاتصال بالأجهزة خارج الشركة على الرغم من أن عزل هذه الأجهزة يلغي العديد من الفوائد التي توفرها السيبرانية، وفي المقابل هناك فيروسات لا تزرع في البرامج وإنما تصيب الجهاز مباشرة[٢].

ومن ثم لابد من تعاون الدول لتحقيق السلام السيبراني، بالنظر في الخصائص المميزة للفضاء السيبراني وأبرز التحديات التي تطرحها هذه السمات. ويمكن الاستفادة من الجهود الدولية في مكافحة تهديدات شبيهة عبر وطنية، مثل اتفاقية مكافحة الجريمة المنظمة عبر الوطنية، فالهجمات السيبرانية تمتد عبر الحدود الوطنية وتعمل من خلال شبكات معقدة تضاهي الأنظمة السلمية أو تتعداها. وتقدم هذه الاتفاقية فهماً مشتركاً يفيد أن هذه المشاكل المتفشية العابرة للحدود الوطنية يلزم معالجتها بواسطة التعاون الدولي الوثيق

---

(١) "القمة العالمية لمجتمع المعلومات: برنامج عمل تونس بشأن مجتمع المعلومات"، الفقرة ٤٠، (فيما بعد، WSIS-05/TUNIS/DOC/6(Rev.1)-E، 18نوفمبر ٢٠٠٥، "Tunis Agenda").www.itu.int/wsis/docs2/tunis/off/6rev1.html

(٢) انظر: د/ عبد الفتاح مراد – شرح جرائم الكمبيوتر والإنترنت، ص ٤٢٤.

وأنها تقتضي اعتماد أطر جديدة والمساعدة القانونية والإنمائية المتبادلة وتبادل المعلومات والتعاون في مجال إنفاذ القانون.[١]

ولذا يعد التعاون من الأمور الضرورية بهذا الشأن نظرا للطبيعة المتغيرة للتكنولوجيا ذاتها مع تداخلات متزايدة بين السلطات القضائية الوطنية وتكنولوجيا المعلومات والاتصالات المرتبطة بها، والموارد والأنظمة مما يجعل اعتماد استراتيجيات جديدة والتعاون الدولي يتسمان بأهمية أكثر لضمان السلام السيبراني.[٢]

كما بذلت جهوداً دولية لمواجهة القرصنة السيبرانية لحماية العلامات التجارية من مسجلي العناوين السيبرانية من خلال بروتوكول مشترك للعناوين السيبرانية الدولية وهو أيضاً يعد من المجهودات الدولية لمحاربة القرصنة السيبرانية وحماية مالكي العلامات التجارية وفي المقابل تم تكوين لجنة دولية خاصة بهدف الوصول إلى أفضل الحلول والاقتراحات. والعمل على

---

(١) اتفاقية منع الجريمة المنظمة العابرة للحدود، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، ٢٠٠٤، www.unodc.org/unodc/en/treaties/CTOC/index.html.

(٢) انظر: د/ عادل عبد الصادق، أمريكا وتشكيل قيادة عسكرية في الفضاء السيبراني. هل بدأ الاستعداد لحروب المستقبل؟ تعلقيات مصرية، مركز الأهرام للدراسات السياسية والاستراتيجية، العدد ١٣٠: ١٢/ يوليو ٢٠٠٩. http://acpss.ahram.org.eg/Ahram/2009/7/12/COMM0.HTM

خلق تعاون دولي شامل خاصة في إجراءات التحقيق والملاحقة خارج الحدود وهي كانت ولا تزال محل اهتمام على الصعيدين الوطني والدولي.[١]

كما يعتبر الإنتربول الدولي الأداة المثلى لتفعيل القوانين المختلفة وتنفيذها لما لها من دور رئيسي في المحافظة على الأمن العام لذلك فهي أيضاً تتمتع بالمؤهلات اللازمة لقيامها بهذا الدور من خلال تعقب الجريمة والمجرمين [٢]. وعلى الرغم من تنوع الجهود إلا أنها تشترك جميعاً في أنها تتضمن مجرد توجيهات وتوصيات للجهات المسؤولة في تسجيل العناوين السيبرانية.

وهناك العديد من الوسائل الحديثة التي على الدول أن تبتغيها للوصول إلى مواجهة شاملة للجرائم السيبرية ومنها:

تأمين الشبكات على نحو يمنع من اختراقها ولعل في محاولة الشركات والمؤسسات والحكومات تأمين شبكاتها المعلوماتية ضد الاختراق بمثابة وسيلة تحد – إن لم تمنع مطلقاً – من عملية الاختراق لهذه الشبكات، ومن ثم فهي تؤدي بطريقة غير مباشرة إلى منع اختراق هذه الشبكات.

---

(١) انظر: د/ سامي علي حامد عياد، الجريمة السيبرانية وإجرام الإنترنت ، دار الفكر الجامعي الإسكندرية ، ٢٠٠٧، ص ١٠٣ .

(٢) انظر: د/ فتوح الشاذلي، عفيفي كامل عفيفي – جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون – دراسة مقارنة منشورات الحلبي الحقوقية، ص ٣٤٩، ود/ مصطفى محمد موسى – الجهاز السيبراني لمكافحة الجريمة – دار الكتب القانونية – مصر، ص ٢٢٣.

ومن طرق تحصين الشبكات الداخلية كذلك من الاختراق عملية التشفير، والتشفير يعني تحويل البيانات المكتوبة إلى أرقام أو رموز لا يمكن حلها إلا بالنسبة لمن يمتلك شفرة حل هذه الرموز والأرقام، وتستخدم عملية التشفير في تداول النقود والبيانات عبر الشبكة في التجارة الإلكترونية، وفي تداول غيرها من البيانات التي تتعلق بالأمن القومي.

وهناك برامج تشفير متقدمة لحماية البيانات المخزنة على شبكات الحاسب الآلي للعبور، والتوقيع السيبراني، وهناك شهادات التصديق على هذا التوقيع السيبراني، وجميعها برامج معلوماتية تساعد في حماية نظام وبيانات الحكومة السيبرانية. وتتمثل **وسائل تأمين بيانات الحكومات السيبرانية فنياً** في الآتي:

(١) **الجدار الناري أو حوائط المنع Fire Walls**:

الجدار الناري عبارة عن مجموعة أنظمة معلوماتية – برامج – توفر سياجات أمنية ما بين شبكة إنترنت وشبكة المؤسسة –أو الحكومة السيبرانية– حتى يتم إجبار جميع عمليات الخروج من الشبكة والدخول إليها، بأن تمر من خلال هذا الجدار الناري، والذي يمنع أي مخترق أو متطفل من الوصول إلى الشبكة.

فهى برامج تقوم بصد محاولات الاختراق أو الهجوم الوافد من شبكة إنترنت لتهديد الشبكة الداخلية أو النظام المعلوماتي، وتوجد برامج كثيرة لجدران النار من ذلك برنامج شبكة (DAN) والذي يتضمن مزايا أمنية عديدة عبارة عن برامج جدران النار Firewalls، ومزودات بروكسي Proxy

Servers التي تحتفظ بصفحات الشبكة – للويب – على القرص الصلب، ومرشحات عناوين arl filters. [١]

(٢) مكافحة الفيروس المعلوماتي:

يعرف الفيروس المعلوماتي بأنه "برنامج للحاسب الآلي مثل أي برنامج آخر، لكنه يهدف إلى إحداث أكبر ضرر بنظام الحاسب الآلي، وله القدرة على ربط نفسه بالبرامج الأخرى، وكذلك إعادة إنشاء نفسه حتى يبدو كأنه يتكاثر ويتوالد ذاتياً، ويقوم الفيروس بالانتشار بين برامج الحاسب الآلي المختلفة، وبين مواقع مختلفة في الذاكرة. "[٢]

ومشكلة الفيروس المعلوماتي هو قدرته على الاختفاء والقدرة على الانتشار والتدمير، وتتم مواجهته ببرامج حماية "anti–virus".

وهو ما يتطلب تأهيل وتدريب المعنيين على مكافحة المخاطر السيبرانية فلابد من وضع سياسة رشيدة تستند على تدريب المختصين، وقد تنبهت الدول إلى أهمية هذا التدريب، وظهر هذا الاهتمام في توصيات العديد من المؤتمرات الدولية الخاصة بمنع الجريمة ومعاملة المجرمين، منها ما جاء في القاعدة (٢٢/ ١) من (قواعد

---

(1) Martin C Libicki. "Conquest in Cyberspace: National Security and Information Warfare", New York, Cambridge University Press, 2007. pp 323- 13.

(٢) د / عبادة أحمد عبادة – التدمير المتعمد لأنظمة المعلومات السيبرانية – بحث منشور لدى مركز البحوث والدراسات، الإدارة العامة لشرطة دبي – مارس ١٩٩٩.

وكذلك د / هدى قشقوش – جرائم الحاسب الآلي في التشريع المقارن – دار النهضة العربية – القاهرة – ١٩٩٢، ص ٩٩.

بكين) من التأكيد على الحاجة إلى التخصص المهني والتدريب وورد فيها أنه "يستخدم التعليم المهني والتدريب أثناء الخدمة ودورات تجديد المعلومات وغيرها من أساليب التعليم المناسبة من أجل تحقيق واستمرار الكفاءة المهنية اللازمة لجميع الموظفين". لأنهم يواجهون أنشطة سيبرانية معقدة وتنفذ بطريقة دقيقة[1].

وعلى هذا لابد من توظيف أفراد ذو معرفة تقنية عالية ومواكبة لأحدث التقنيات في هذا المجال. وينبغي إنشاء مختبرات الطب الشرعي على الكمبيوتر لجمع الأدلة الرقمية من أجهزة الحاسوب وتوفير التدريب للمختصين.

ومن ثم تنوعت الجهود الدولية في مكافحة الجريمة السيبرانية حيث تم اتخاذ العديد من الآليات والإجراءات للحد والتقليل منها إلا أن هذه الجهود تبقى غير كافية مقارنة بالتقدم التكنولوجي الذي تشهده الدول على مستوى السيبرانية والاستعمال اللامتناهي للكمبيوتر والإنترنت وسنتطرق إلى إبراز هذه الجهود مع تبيان صعوبة التعاون الدولي للقضاء على هذه الجريمة الدولية العابرة للحدود لتظافر العديد من العوامل سيتم توضيحها لاحقاً.

ومن ثم ينبغي أن تكون هناك استراتيجيات فعالة للأمن السيبراني مرنة وقابلة للتكييف بشكل كافٍ لتتسنى مواكبة التقدم التكنولوجي السريع وتحديات الأمن المرتبطة بها والاستجابة لها. كما يتعين على البلدان أن تتفق بشأن إجراءات ونهج لتحديد مصدر الهجمات وهوياتها من أجل التصدي

---

(١) راجع د / محمد الأمين البشري في "التحقيق في جرائم الحاسب الآلي" بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت. مقدم إلى كلية الشريعة والقانون – جامعة الإمارات العربية المتحدة – الفترة من ١-٣ مايو ٢٠٠٠م.

للهجمات السيبرانية المجهولة الهوية والاشتباكات الدولية التي تهدد بنشوبها. وإن ربط المسؤولية بالمصدر الجغرافي قد يؤدي إلى تفادي العملية المعقدة لتحديد هوية مرتكب الهجوم السيبراني تحديداً دقيقاً.(١)

وقد أثبتت حوادث الاعتداءات التي قامت بها الجماعات الإرهابية أو حتى التي اتهمت بها الدول أنه ما زالت هناك حالة ضعف في دفاعات الدول وأمنها المعلوماتي أمام الهجمات السيبرانية. مما يوضح بجلاء قصور في النهج التقليدي المتبع في مجال الأمن الدولي لبعض الدول ومن ثم لابد من تبني استراتيجيات جديدة للتصدي لتحديات الأمن وضمان تحقيق سلام سيبراني دائم.

(١) نقلاً عن مستشار الأمن الرئاسي الأمريكي السابق ريتشارد كلارك في حلقة مناقشة بشأن الأمن السيبراني ١١ مارس ٢٠١٠.

www.networkworld.com/community/node/58450

الخاتمة

لا شك أن التطور السريع في تكنولوجيا الكمبيوتر، دفع المجتمع الدولي للدخول في مرحلة جديدة أصبح فيها للأمن السيبراني دورا أساسيا سواء في الاستحواذ على عناصره الأساسية أو في تعظيم القوة، لظهور محددات جديدة لهذه القوة سواء من حيث طبيعتها أو أنماط استخدامها أو طبيعة الفاعلين فيها، وانعكاس ذلك على قدرات الدول وعلاقاتها الخارجية مما جعل هذه البيئة السيبرانية حقيقة غير مسبوقة، واتجهت الدول إلى الحفاظ على أمنها القومي لمواجهة ما يعرف بصراع "عصر المعلومات".

وفي ظل هدا البحث المعنون بـــ " المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام " قد انتهينا إلى نتائج وتوصيات تتمثل في:-

أولا: النتائج:-

نجد أن الفضاء السيبراني قد فرض على الدول والعديد من المنظمات الدولية إعادة التفكير في مفهوم الأمن الدولي، والذي يتعلق بتلك الدرجة التي تتمكن الدول من أن تصبح في مأمن من المخاطر التي تتعرض لها سواء في سلامة أراضيها أو استقلالها السياسي أو حماية البنى التحتية لمنشأتها الحيوية ومن كافة أوجه الاستخدام غير المشروع لتكنولوجيا الاتصال والمعلومات.

وأن من أهم الإشكاليات التي تواجه المجتمع الدولي هو ما يتعلق بالجدل حول مدى اعتبار الأسلحة السيبرانية كالأسلحة غير التقليدية من إمكانية إخضاعها لقيود الاتفاقيات الدولية، وممارسة حق الدفاع الشرعي وفق المادة (٥١) من الميثاق سواء عبر ممارسات فردية أو جماعية.

وخلصنا أن فقه القانون الدولي - الخبراء القائمين على دليل تالين، والاتحاد العالمي للعلماء - يدعم اعتبار الأسلحة السيبرانية كالأسلحة غير التقليدية بمحددات معينة، وذلك استنادا إلى آراء محكمة العدل الدولية والتي كانت مهيأة في العديد من القضايا التي عرضت أمامها كما في قضية "النشاطات العسكرية وشبه العسكرية في نيكاراجوا" ١٩٨٦، وأيضاً قضية منصات النفط بين إيران والولايات المتحدة ٢٠٠٣ إلى ضم فئات أخرى غير الهجوم المادي لكي يعطي الحق للدولة التي تتعرض إلى هجوم الارتكاز إلى المادة ٥١ والدفاع عن نفسها ولكن ضمن شروط أبرزها الحجم والتأثير.

والذي نتبين من خلاله أن محكمة العدل الدولية قد ركزت على نتائج الهجوم أكثر من تركيزها على الوسائل المستخدمة في تنفيذ الهجوم مما يفيد أن المحكمة مهيأة لإدخال الهجمات السيبرانية ضمن فئة الهجمات التقليدية لما لها من حجم وتثير في الدول محل الهجوم السيبراني.

وبالرغم من ذلك تبقى مسألة المقارنة بين الهجوم المسلح المادي والهجوم السيبراني غير عملية وذلك بسبب الفوارق الجوهرية بين هاتين الفئتين من الهجمات وعدم إمكانية إسقاط بعض الشروط الواجب توافرها من أجل تفعيل المادة ٥١ على الهجمات السيبرانية. على وجه التحديد فإنه من الصعوبة بمكان إسقاط شروط الضرورة والسرعة والفورية في رد الهجوم لكي تقوم الدولة المعتدى عليها باتخاذ إجراءات الدفاع عن النفس – وذلك بسبب الصعوبة التي تصاحب عملية تحديد الجهة مصدر الهجوم إلا بعد مدة زمنية طويلة والتي يمكن عندها أن ينتفي المنطق من إعطاء الدولة الحق في الدفاع

عن نفسها دون اللجوء إلى مجلس الأمن صاحب السلطة الأساسية في حفظ الأمن والسلم الدوليين.

ومن ثم لابد من تكاتف الجهود لإبرام اتفاقيات دولية تكون مهمتها الأساسية مواجهة المخاطر السيبرانية واحتوائها ومحاولة التخفيف منها.

ثانيا:التوصيات :ـ

وبعد أن انتهينا من عرض نتائج البحث نبين ما خلصنا إليه من توصيات والتي تتمثل في:-

*ضرورة العمل على وضع قواعد دولية موحدة تحكم حالات الحرب والنزاع في الفضاء السيبراني، وإدخال العدوان السيبراني ضمن صور العدوان من أجل دعم الاستخدام السلمي للفضاء السيبراني، ووضع الأمن السيبراني ضمن استراتيجيات الأمن القومي للدول من أجل تحقيق السلم والأمن الدوليين.

*استنهاض دور الأمم المتحدة للقيام بدورها في تطوير النظام التشريعي والعقابي لمواجهة الهجمات السيبرانية وتنظيم الفضاء السيبراني وفق مبدأ حظر استخدام القوة في العلاقات الدولية.

*وضع أطر قانونية لحماية حقوق الإنسان الرقمية وعدم المساس بها وجعل الأمن السيبراني الجماعي أحد أشكال الأمن الجماعي الإنساني الجديد.

*وضع استراتيجيات لتطوير نموذج التشريعات السيبرانية يكون قابلاً للتطبيق محلياً وعالمياً بالتوازي مع التدابير القانونية الوطنية والدولية المعتمدة.

*وضع استراتيجية لتحديد الحد الأدنى المقبول عالمياً في موضوع معايير الأمن ونظم تطبيقات البرامج والأنظمة.

*وضع استراتيجيات عالمية للمراقبة والإنذار المبكر في الفضاء السيبراني مع ضمان قيام التنسيق عبر الحدود.

*تقديم المشورة بشأن إمكانية اعتماد إطار استراتيجي عالمي لأصحاب المصلحة من أجل التعاون الدولي والحوار والتعاون والتنسيق في جميع المجالات .

*توظيف الخبراء وتدريبهم لمواكبة أحدث التطورات التكنولوجية وفهمها وتطوير القوانين الوطنية وفق ذلك.

*لابد من تكاتف الجهود الداخلية والدولية لإنشاء منظمات دولية وإقليمية، وإبرام اتفاقيات ثنائية وجماعية وتكون متخصصة مهمتها الأساسية التنسيق بشأن مواجهة الجرائم الإلكترونية واحتوائها ومحاولة التخفيف منها.

*تبادل الخبرات بين الدول كافة، وخاصة التي لها خبرات واسعة في هذا مجال مكافحة المخاطر السيبرانية.

*مساعدة البلدان بعضها البعض في هذا الشأن لمواجهة تلك المخاطر والتي يتم من خلاله أبشع ما يمكن تصوره وهو "الإرهاب" الذي لا يعرف ديناً ولا وطن، والذي من الممكن أن يذهب ضحيته الملايين من البشر الأبرياء، والذي لا يعرف حينها الدولة النامية من الدولة المتقدمة، ومن هذا المنطق "دعوة للتعاون الدولي من أجل حماية البشرية".

ثبت بأهم مراجع البحث

أولا: المراجع العربية:

أ- الكتب

- د/ إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، المجلد ١٠، أبريل ٢٠١٩م.
- د/ إسماعيل صبري مقلد – أصول العلاقات الدولية إطار عام – دار النهضة العربية – الطبعة الأولى – القاهرة – ٢٠٠٧ م.
- د/ إيهاب خليفة، القوة الإلكترونية، كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت، دار العربي، ٢٠١٧ م.
- د/ جميل عبد الباقي الصغير – أدلة الإثبات الجنائي والتكنولوجيا الحديثة – دار النهضة العربية – القاهرة – ٢٠٠١م.
- د/ راشد محمد المري، الجرائم السيبرانية في ظل الفكر الجنائي المعاصر دراسة مقارنة، ط دار النهضة العربية، ٢٠١٨م.
- د/ سامي علي حامد عياد – الجريمة السيبرانية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، ٢٠٠٧م.
- د/ عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، وحدة الدراسات المستقبلية، قوانين وتشريعات، إصدارات مكتبة الإسكندرية، العدد ٢٣، ٢٠١٦م.
- د/ عادل عبد الصادق، الفضاء الإلكتروني والرأي العام: تغير المجتمع والأدوات والتأثير، المركز العربي لأبحاث الفضاء الإلكتروني، قضايا استراتيجية، العدد ٢٤٥٩، ٢٠١٨.

- د/ عباس بدران، الحرب السيبرانية: الاشتباك في عالم المعلومات، بيروت: مركز دراسات الحكومة السيبرانية، ٢٠١٠م.
- د/ على حسين باكير، الحروب السيبرانية في القرن الواحد والعشرين، مركز الجزيرة للدراسات، قطر، ٧/ ١٢/ ٢٠١٠م.
- د/ عماد محمد سلامة. الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنة البرامج. دار وائل للنشر، ٢٠٠٥م.
- د/ مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، مطابع الشرطة، القاهرة ٢٠٠٩م.
- د/ نبيل أحمد حلمي – القانون الدولي وفقاً لقواعد القانون الدولي العام – دار النهضة العربية – القاهرة – ١٩٩٩ م.
- د/ هدى قشقوش – جرائم الحاسب الآلي في التشريع المقارن – دار النهضة العربية – القاهرة – ١٩٩٢م.
- د/ هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية (معلقا عليها)، دار النهضة العربية، ط٢، ٢٠١١م.
- د/ جمال محمد غيطاس، الحرب وتكنولوجيا المعلومات، ط١، القاهرة، دار نهضة مصر، ٢٠٠٦م.
- فرد كابلان، المنطقة المعتمة. التاريخ السري للحرب السيبرانية، ترجمة: لؤي عبد المجيد السيد، سلسلة عالم المعرفة، بدون تاريخ نشر.

ب- الأبحاث والرسائل: -

- د/ جواهر آل سعود، الحاسب الآلي أداة جريمة، بحث مقدم لمؤتمر الجرائم السيبرانية ومكافحتها، الرياض في ١٠ جمادي الأول ١٤٢٨ – عام ٢٠٠٩.
- د/ حسن بن أحمد الشهري، الأنظمة الإلكترونية الرقمية المطورة لحفظ وحماية وسرية المعلومات من التجسس، بحث منشور في المجلة العربية للدراسات الأمنية والتدريب، العراق، المجلد ٢٨، العدد٥، ٢٠١٢م.
- د/ رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، بحث منشور في مجلة جامعة الشارقة للعلوم القانونية، المجلد ١٥، العدد ٢، ربيع الثاني ١٤٤٠، ديسمبر ٢٠١٨م.
- د/ عبادة أحمد عبادة – التدمير المتعمد لأنظمة المعلومات السيبرانية، بحث منشور لدى مركز البحوث والدراسات، الإدارة العامة لشرطة دبي، مارس ١٩٩٩م.
- د/ محمد البخاري طشقند، الإنترنت ومبادئ الأمن المعلوماتي الدولي "الثورة المعلوماتية فجرت الحواجز القائمة بين الشعوب والدول"، بحث منشور على شبكة ضياء للمؤتمرات والدراسات بتاريخ ٢٩/ ٧/ ٢٠١١ م.
- د/ محمد الأمين البشري في "التحقيق في جرائم الحاسب الآلي" بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت. مقدم إلى كلية الشريعة

والقانون – جامعة الإمارات العربية المتحدة – الفترة من ١ -٣ مايو ٢٠٠٠م.

- د/ محمد سليمان الخوالدة: جريمة الدخول غير المشروع على الموقع السيبراني أو نظام معلومات وفق التشريع الأردني، رسالة ماجستير في القانون العام، كلية الدراسات العليا، الجامعة الأردنية، ٢٠١٢م.
- د/ مصطفى خالد حامد أحمد، السيبرانية والمسؤولية الجزائية، محل الفكر الشرطي مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات، عدد ٧٩، دار المنظومة.

ج. التقارير والبيانات

- بيان اللجنة الدولية للصليب الأحمر للأمم المتحدة٢٠١١ م بشأن جدول الأعمال في ما يتعلق بنزع السلاح والأمن، الجمعية العامة للأمم المتحدة، الدورة ٦٦، اللجنة الأولى. وبيان نيويورك، ١١ تشرين الأول/ أكتوبر ٢٠١١م.
- تقرير التوازن العسكري ٢٠١١ م يصدر سنويا باللغة الانجليزية عن المعهد الدولي للدراسات الاستراتيجية.
- تقرير مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، UNODC، سلفادور، البرازيل، ١٩-١٢ أبريل ٢٠١٠ م.
- تقرير وتوصيات، فريق الرصد الدائم المعني بمجتمع المعلومات والتابع لاتحاد العلماء العالمي، ١٩ نوفمبر ٢٠٠٣ م.
- مركز التميز للدفاع السيبراني التعاوني www.ccdcoe.org.

- دليل تالين حول القانون الدولي المنطبق على الحرب السيبرانية من إعداد اللجنة الدولية للخبراء بدعوة من مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي (الناتو)، مطابع جامعة كمبريدج، ٢٠١٣م.
- السلام السيبراني بقلم حمدون إ. توريه (الأمين العام للاتحاد الدولي للاتصالات)، إصدار الاتحاد العالمي للعلماء يناير ٢٠١١م.
- إعلان إيريتشي بشأن مبادئ الاستقرار السيبراني والسلام السيبراني"، اتحاد العلماء العالمي، أغسطس ٢٠٠٩ م.
- إدارة الخطر السيبراني الوطني إعداد ميليسا هاثاواي ضمن المنهجية التي وضعتها باسم "مؤشر الجاهزية السيبرانية".
- بيان وزارة الدفاع الإستونية الصادر في يوم الاثنين٢ / ١٢/ ٢٠١٢ م في إستونيا.

د. الاتفاقيات والوثائق الدولية:

- اتفاقيات جنيف ١٩٤٩ وبروتوكولاتها الإضافية.
- وثيقة مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، ١٨ أبريل ٢٠١٠م.
- وثيقة المؤتمر الدولي الثامن والعشرين للصليب الأحمر والهلال الأحمر المنعقد عام ٢ -٦ ديسمبر/ كانون الأول ٢٠٠٣ م.
- ميثاق الأمم المتحدة ١٩٤٥.
- النظام الأساسي لمحكمة العدل الدولية ١٩٤٥.

ثانيا: المراجع الأجنبية:

أ. الكتب:

-Arsenio T. Gumahad, Cyber Troops and Net War: The Profession of Arms in the Information Age. Maxwell
-AFB, AL: Air University, Air War College, April 1996.
-Black Hat Talk on China's 'Cyber Army' Pulled After Pressure", InfoWorld, 15 July 2010.
-Bonnie N. Adkins, ," The Spectrum of Cyber Conflict from Hacking to Information Warfare: What is Law
-Enforcement's Role?", A Research Report Submitted to the Faculty In Partial Fulfillment of the Graduation Requirements, Maxwell Air Force Base, Alabama, April 2001.
-Brigid Grauman, Cyber-security:The vexed question of global rules, A Security & Defence Agenda report, Geert
-Cami, February 2012.
David E Sanger., Confront and Conceal, Obama's Secret Wars and Surprising Use of American Power, New York Crown2012 .
-Edward Amoroso, Cyber Security, SiliconPress, 2007.
-Ellen Messmer ,Cyberattack Seen as Top Threat to Zap U.S. Power Grid," Network World, 2 June 2010 .
-Ellen Nakashima, List of cyber-weapons developed by Pentagon to streamline computer warfare, The Washington Post, Published: June 1, 2011.
-Gabriel Weimann Terror on the Internet: the new arena, the new challenges,, United States Institute of Peace Press, 2006.
-Joseph S. Nye: The Future of Power. Press Release, Harvard Kennedy School, Belfer Center for Science and International Affairs, January 31, 2011.

-Kamal Ahmad Khan, Use of Force and Human Rights under International Law, Athens Institute for Education and Research, Conference Paper Series BLE 2017.
-Kamrul Hossain, The Concept of Jus Cogens and the Obligation under the U.N. Charter, Santa Clara Journal of International Law, Vol.3, Issue 1, 2005.
-Klang, Mathias; Murray, Andrew (2005). Human Rights in the Digital Age. Routledge. 24 Oct. 2013 .
-Kriangsak Kittichaisaree, "Public International Law of Cyberspace, Law, Governance and Technology Series", Vol 32, Springer International Publishing, Switzerland, 2017.
-LivierNay , Lexique de Science politique vie et Institutions politiques, Europe Media Duplication SAS, Toulouse, 2008.
-Malcolm Shaw, International Law, (7th edition, 2014), Cambridge University Press; oram Dinstein, War, Aggression and Self-defence,3ed edition2011.
-Martin C Libicki. "Conquest in Cyberspace: National Security and Information Warfare", New York, Cambridge University Press, 2007.
-Michael N. Schmitt (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge University Press, 2013.
-Michael N. Schmitt, "Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum", Harvard National Security Journal, Vol. 8, 2017.
-Tim Jordan," Cyber power: The Culture and Politics of Cyberspace and the Internet", Rout ledge, 2000.

ب. الأحكام القضائية:

-I.C.J. Rep. 4, 22 (Apr. 9); also Rorbert P. Barnidge, The Due Diligence Principle under International Law, International Law Community Law Review, Vol.81, Issue 8, (2006.(

-ICJ, case concerning Oil Platforms, (Islamic Republic of Iran v. United States of America), Reports 2003

-ICJ, Corfu Channel Case (UK. v. Albania), 1949.

-ICJ, Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), 1986.

-ICJ, Oil Platforms Case, (Islamic Republic of Iran v. United States of America), Reports .

-Iran Blocks American 'Virtual Embassy, the new York times, December 7, 2011 .

ج. المواقع الالكترونية:

موقع الأمم المتحدة www.un.org/arabic/documents/docs_ar.asp

موقع الاتحاد الدولي للاتصالات www.itu.int/wsis/docs2/tunis/off/6rev1.

حلف شمال الأطلسي www.nato.int/cps/en/natolive/news_62894.htm

فهرس الموضوعات