مجلة روح القوانين – كلية الحقوق جامعة طنطا

عدد خاص – المؤتمر العلمى الدولى الثامن – التكنولوجيا والقانون

الدفاع الشرعي وإشكاليات الرد على الهجمات السيبرانية في ضوء ميثاق الأمم المتحدة

إعداد الدكتور/ أميرة عبد العظيم محمد عبد الجواد

أستاذ القانون الدولي العام المساعد بجامعة الأزهر

والأستاذ المشارك بكليات الشرق العربي بالرياض

ملخص البحث:

تهدف هذه الدراسة إلى معرفة الهجمات السيبرانية، ومدى خطورتها على تهديد الأمن القومي والاستراتيجي للدول، حيث أصبحت الهجمات السيبرانية تتقدم بوتيرة سريعة باستخدام أحدث التقنيات والبرمجيات في تنفيذ تلك الهجمات والتي يجعل من الصعوبة بمكان تحديد مصدر تلك الهجمات ذات الزخم العالي وتحديد مسؤولية الدول التي قامت بها، مما يستلزم أن يكون هناك تحركا دوليا لمواجهة هذه المخاطر، ولكن هل تدخل هذه الهجمات ضمن المادة ٢ (٤) من ميثاق الأمم المتحدة والتي تحظر استخدام القوة أو التهديد باستخدامها في العلاقات الدولية والتي تعد مبدأً أساسياً من مبادئ القانون الدولي العام، بحيث تشكل المخاطر السيبرانية تهديدا للسلم أو إخلال به أو وقوع عدوان يمكن مجلس الأمن وفق المادة (٣٩) من الميثاق بأن يتدخل باتخاذ إجراءات عقابية ضد الدولة الفاعلة، وهل يمكن ذلك الدول الموجهة إليها بأن تستخدم حق الدفاع الشرعي إعمالا للمادة (٥١) من ميثاق الأمم المتحدة، واستخدام هذا الحق يعد استثناء على مبدأ حظر استخدام القوة أو التهديد باستخدامها في العلاقات الدولية.

ومن ثم تتمحور هذه الدراسة حول مدى ملائمة القواعد القانونية التقليدية الخاصة باستخدام القوة وبالدفاع الشرعي لاستيعاب خطورة الاعتداءات السيبرانية. فهل يمكن للهجمة السيبرانية أن تحقق المحددات القانونية الخاصة بالدفاع الشرعي حسب ما تقضي به المادة ٥١ من ميثاق الأمم المتحدة؟ أم مازال ميثاق الأمم المتحدة عاجزا عن استيعاب تلك الهجمات مما يستلزم معه وضع اتفاقية دولية لتنظيم مواجهة الهجمات السيبرانية بصفة خاصة لحماية أمن الدول.

ومن هنا جاءت فكرة هذا البحث ليلقي مزيدا من الضوء حول وضع إجابات قانونية لهذه الأسئلة المحورية، من خلال مراجعة قواعد القانون الدولي العام

المتعلقة باستخدام القوة عموما، والاستثناء الوارد عليها والمتمثل في الدفاع الشرعي خصوصا والربط بينهما، وإلى القرارات والآراء الاستشارية لمحكمة العدل الدولية.

وسوف أتناول هذا من خلال ثلاثة مباحث: المبحث الأول: أتعرض فيه لماهية الهجمات السيبرانية، والمبحث الثاني: أتناول فيه صور الهجمات السيبرانية، والمبحث الثالث سأتحدث فيه عن الهجمات السيبرانية واستخدام حق الدفاع الشرعي في ميثاق الأمم المتحدة.

الكلمات الدالة:

الهجمات السيبرانية، الفضاء السيبراني، مخاطر تقنية المعلومات، الأمن السيبراني، الحرب السيبرانية.

Abstract:

This study aims to know the cyber-attacks, and the extent of their danger to threaten the national and strategic security of countries, as cyber-attacks have become progressing at a rapid pace using the latest technologies and software in the implementation of these attacks, which makes it difficult to determine the source of those attacks with high momentum and determine the responsibility of the countries that carried them out, which requires that there be international action to confront these risks, but do these attacks fall within Article 2 (4) of the Charter of the United Nations, which prohibits the use of force Or the threat of their use in international relations, which is a basic principle of public international law, so that cyber risks constitute a threat to the peace or breach of it or the occurrence of

aggression that enables the Security Council, in accordance with Article (39) of the Charter, to intervene by taking punitive measures against the active state, and whether this can be done by the States to which it is directed to use the right of legitimate defense pursuant to Article (51) of the Charter of the United Nations, and the use of this right is an exception to the principle of prohibiting the use of force or the threat of its use In international relations.

This study then focuses on the adequacy of traditional legal rules on the use of force and legitimate defense to understand the seriousness of cyber-attacks. Can a cyber-attack achieve the legal limitations of legitimate Defence as required by Article 51 of the Charter of the United Nations? Or is the Charter of the United Nations still unable to accommodate such attacks, which necessitates the development of an international convention to regulate the response to cyber-attacks in particular to protect the security of States?.

Hence the idea of this research to shed more light on the development of legal answers to these questions.

Keywords:

Cyber Attacks, Cyberspace, Information Technology dangers, Cyber Security, Cyber War.

مقدمة:

لقد أحدثت تكنولوجيا المعلومات والاتصالات ثورة شاملة في جميع نواحي الحياة وزادت هيمنة تكنولوجيا المعلومات والاتصالات على نسق الحياة العام، وصاحب هذا ظهور العديد من المخاطر المترتبة على هذا التوسع الكبير، ويعد أهمها تزايد 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 عليه 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.

ولا أدل على ذلك من التحذيرات التي أطلقتها مايكروسوفت في فبراير ٢٠٢٢م والتي تتعلق بشن حملة تصيد احتيالي من قبل مجموعة قرصنة روسية تستهدف الوكالات الحكومية الأوكرانية المنظمات غير الحكومية.

وكذلك في عام ٢٠١٩، شنّت الولايات المتحدة مجموعة من الهجمات الإلكترونية على شبكة الكهرباء الروسية كرد فعل على حملة تضليل الكرملين، ومحاولات القرصنة خلال الانتخابات الأمريكية لعام ٢٠١٨ والشكوك حول اختراق روسيا لقطاع الطاقة.

ولقد استجابت بلدان عديدة للتهديد الجديد للحرب السيبرانية من خلال تكليف عدد كبير من الأفراد العسكريين بمهمة التدريب والاستعداد للقتال الافتراضي. 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(١).

وتقام هذه العدة العسكرية الجديدة لدمج وإعداد الموارد العسكرية من أجل جميع أنواع عمليات الفضاء السيبراني(٢).

ويمكن أن تكون أيضاً مسؤولة عن تأمين الشبكات الخاصة التي تشغّل جزءاً كبيراً من العمليات العسكرية، وإن كان تركيزها في المقام الأول على حماية الشبكات العسكرية وتسيير العمليات العسكرية في الفضاء السيبراني(٣).

---

(١) أعلنت الولايات المتحدة -على سبيل المثال- عن 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.

(٢) انظر تقرير وزارة الدفاع الأمريكية، ٢٥ مايو ٢٠١٠ م:
https://www.defense.gov/Home/features/2010/0410_cybersec/docs/CYberFactSheet

(٣) Siobhan Gorman, "U.S. Backs Talks on Cyberwarfare"", The Wall Street Journal, 4 june 2010, http://online.wsj.com/article/.html.
مشيراً إلى أن ٩٠ % من القوة العسكرية يوفرها القطاع الخاص، وفقاً لمسؤولين

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

وقد ارتفعت الهجمات السيبرانية بنسبة ٣٨% في عام ٢٠٢٢ مقارنة بالعام السابق، بمتوسط ١١٦٨ هجوما أسبوعيا لكل منظمة تم تسجيلها.

وأعلنت الولايات المتحدة عن جهود تصنيع لأسلحة إنترنت هجومية لمواجهة احتمال تعرضها لهجوم، حيث تبلغ تكلفة الهجمات السيبرانية ١١ بليون دولار و٩ مليون مواطن تم اختراق خصوصياتهم وتكلف الجريمة السيبرانية ٣,٨ بليون دولار [١].

وأعلنت روسيا عزمها عن تطوير السلاح الجوي 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].

عسكريين في الولايات المتحدة، فيما بعد Gorman.

(١) المرجع السابق، نفس الموضع.

(٢) بوتين يطلق سباق التسلّح مع الغرب، صحيفة الجمهورية٢١ فبراير ٢٠١٢.
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,

وإزاء تزايد هذه الهجمات بدأت تتأثر سيادة الدول في ظل هذا الفضاء السيبراني. ولتلافي المخاطر المستقبلية بدأت العديد من الدول فى تطوير التشريعات الوطنية لاستيعاب الجرائم التى تحدث فى نطاق إقليمها والتنسيق مع الدول الأخرى عن طريق إبرام الاتفاقيات الدولية لتنظيم الجرائم السيبرانية وتحديد الآليات الواجب اتباعها في حال حدوث تلك الجرائم كالتوصية الصادرة من مجلس أوروبا بشان المشاكل الإجرائية المرتبطة بتكنولوجيا المعلومات(١) واتفاقية بودابست عام ٢٠٠١ وبروتوكول ستراسبورغ عام ٢٠١٣ والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠ ويرى خبراء الأمن السيبراني في حلف الشمال الأطلسي وجوب منع الدول من استخدام البنية التحتية السيبرانية الواقعة في اقليمها او التي تخضع لسيطرتها الكاملة في نشاطات تمس الحقوق السيادية للدول الأخرى.

وسوف أتناول هذا من خلال ثلاثة مباحث: المبحث الأول أتعرض فيه لماهية الهجمات السيبرانية، والمبحث الثاني صور الهجمات السيبرانية، والمبحث الثالث في استخدام حق الدفاع الشرعي في مواجهة الهجمات السيبرانية. وسوف تكون خطة البحث على النحو التالي:

February.2012.
http://www.securitydefenceagenda.org/Portals/14/Documents/Publications/SDA_Cyber_report_FINAL.pdf.

(١) اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية، مجموعة المعاهدات الأوربية رقم ١٨٥، بودابست ٢٠٠١.

- **مقدمة:**
- **المبحث الأول:** ماهية الهجمات السيبرانية.

✓ المطلب الأول: التعريف بمصطلح الهجمات السيبرانية

✓ المطلب الثاني: طبيعة الهجمات السيبرانية وسماتها.

- **المبحث الثاني: صور الهجمات السيبرانية.**

✓ المطلب الأول: الهجمات السيبرانية الاستراتيجية (استهداف البنية التحتية للدولة).

✓ المطلب الثاني: الهجمات السيبرانية العسكرية (السيطرة على الأنظمة العسكرية السيبرانية).

✓ المطلب الثالث: القرصنة والتجسس السيبراني.

- **المبحث الثالث: الهجمات السيبرانية واستخدام حق الدفاع الشرعي في ميثاق الأمم المتحدة.**

✓ المطلب الأول: الهجمات السيبرانية ومدى انطباقها على تهديد السلم والأمن الدوليين.

✓ المطلب الثاني: استخدام حق الدفاع الشرعي وفق المادة ٥١ من ميثاق الأمم المتحدة في مواجهة الهجمات السيبرانية.

- **الخاتمة.**

المبحث الأول

ماهية الهجمات السيبرانية

تعد الهجمات السيبرانية تهديدا لمبادىء القانون الدولى التى تقوم على مبدأ احترام سيادة الدول لما فيها من اختراق للأمن السيبراني للدولة من خلال اختراق معلومات استراتيجية وعسكرية تصنف بالسرية، وتصطدم مع حظرا دوليا وهو الامتناع عن استخدام القوة او التهديد بها في العلاقات الدولية، فالهجمات والأضرار التى تتعرض لها الدولة يؤثر على سيادتها بل وعلى استقلالها السياسي في اتخاذ القرارات ومداها(١).

ومن ثم تشكل الهجمات السيبرانية إحدى التحديات الراهنة لسيادة الدول، والتي باتت الدول معه تتسابق على استغلاله لمصلحتها والقيام بتطوير قدراتها الهجومية والدفاعية ضمن شكل جديد من اشكال سباقات التسلح.

وهو ما يتطلب في هذا المبحث: توضيح تحديد لمصطلح الهجمات السيبرانية في المطلب الأول، وبيان خصائصها وطبيعتها في المطلب الثاني.

المطلب الأول

التعريف بمصطلح الهجمات السيبرانية

كلمة السيبرانية، مشتقة من الكلمة اللاتينية" سايبر "Cyber" ومعناها تخيلي أو

(١) - Matthew C. Waxman، "Cyber-Attacks and the Use of Force: Back to the uture of Articl0065
The Yale Journal of International Law، عدد 2011 ص 423.

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. وتعني أيضا القيادة أو التوجيه، والذي يعني: "علم الاتصالات وأنظمة التحكم الآلي في كل من الآلات والأشياء الحية"(١).

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 الإلكتروني أكبر من الانترنت، لما يحتويه من قدرات توجيهية للطاقة التى توجد فى جزء من الموجات الكهرومغناطيسية(٢).

الهجمات السيبرانية: يمكن تعريفها بكونها: " فعل يقوض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف معينة

(١) منير البعلبكي "المورد: قاموس إنكليزي–عربي"، دار العلم للملايين، بيروت٢٠٠٤،ص٢٤٣. وقاموس أكسفورد.
https//:en.oxforddictionaries.com/definition/cyber

(٢) للمزيد انظر: عادل عبد الصادق، الفضاء الإلكترونى والرأي العام: تغير المجتمع والأدوات والتأثير، مرجع سابق، ص ٣٩.

تُمكن المهاجم من التلاعب بالنظام.

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[١].

وعرف "دليل تالين" الهجمات السيبرانية بأنها " عمليات سيبرانية، سواء أكانت هجومية أم دفاعية، والتي يهدف من خلالها بصورة معقولة التسبب بالإصابة أو وفاة الأشخاص أو الأضرار أو تدمير الأعيان والأهداف"[٢].

وعلى هذا يمكن تعريف الهجمات السيبرانية بأنها: أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها.

المطلب الثاني

طبيعة الهجمات السيبرانية وسماتها

أصبحت الدول تهتم بتكنولوجيا المعلومات ودورها فى الصراعات والحروب

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

(٢) دليل تالين وهو مجموعة من المبادىء أعدها بعض الخبراء في القانون الدولي الإنساني عام ٢٠١٣ بالتعاون مع حلف شمال الأطلسي، وبدعم من فريق مؤلف من خبراء السيبرانية، واللجنة الدولية للصليب الأحمر والقيادة السيبرانية الأميركية الذين شاركوا في المداولات كافة.

المستقبلية استعدادا لمواجهة ما ينشأ عنها من مخاطر، والتي يتوقع الكثير حدوثها فى 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 التى تم شنها ما بين روسيا واستونيا عام ٢٠٠٧، وبين جورجيا وروسيا عام ٢٠٠٨، دفعت 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).

ومن أشهر الهجمات السيبرانية الحديثة ما يتم استخدامه حاليا ضمن الحرب بين روسيا وأوكرانيا حيث تستخدم روسيا طريقة التصيّد بالرمح، والتي أعلنتها مايكروسوفت عندما أطلقت تحذيرات في فبراير ٢٠٢٢ تتعلق بشن حملة تصيد احتيالي من قبل مجموعة قرصنة روسية تستهدف الوكالات الحكومية الأوكرانية والمنظمات غير الحكومية.

تستهدف هذه المجموعة المعروفة باسم Gamaredon منذ عام ٢٠٢١ المنظمات الحساسة والتي تعتبر ذات أهمية كبيرة في عملية الاستجابة لحالات

(١) د/عباس بدران، الحرب السيبرانية: الاشتباك في عالم المعلومات، مركز دراسات الحكومة السيبرانية، بيروت٢٠١٠، ص ١١٠.

الطوارئ وضمان أمن الأراضي الأوكرانية. وتعتمد هذه المجموعة في عملياتها الإجرامية على رسائل التصيّد الاحتيالي التي تتضمن روابط مزيفة تحتوي على برامج ضارة، ويتم ارسالها مرفقة مع كود تتبع يساعد بإعلام المهاجمين الإلكترونيين بما إذا كان قد تم فتح الرابط أم لا(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 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 فى تنفيذ العمليات العسكرية وتعتبر من أدوات الحرب الشاملة(٢)، وهذه الحروب بعد أن كانت تستهدف أجهزة الإنترنت والحواسيب الآن تستهدف قطاعات وصناعات محددة(٣).

ويتميز الصراع السيبراني Cyber Conflict بعدم وضوح أطرافه وتكون تداعياته خطيرة سواء عن طريق تدمير المواقع على الإنترنت ونسفها وقصفها بوابل من

(١) https://www.rmgsa.com/%D8%A3%D8%B4%D9%87%D8%B

(٢) جمال محمد غيطاس، الحرب وتكنولوجيا المعلومات، ط١القاهرة: دار نهضة مصر ٢٠٠٦م.

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

الفيروسات أو العمل على استخدام أسلحة الفضاء السيبراني المتعددة للنيل من سلامة تلك المواقع، وهي أسلحة يسهل الحصول عليها من خلال مواقع الإنترنت وتعلم 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، 2002م. P 15.

(1) 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) د/ عادل عبد الصادق، موقع ويكيليكس وتحدي عالم الاستخبارات الامريكي، ملف الاهرام

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).

ولا يكفي لمجابهة ومواجهة هذه الظاهرة بحث سبل توفير وسائل تكنولوجية وبرامج حاسوبية لحماية البيانات وتوفير أمن المعلومات المخزنة إلكترونياً، بل يجب تكثيف الجهود لتنمة الحماية لمقدرات الدول وحماية بياناتهم ومعلوماتهم، وكذلك لتنمة الحماية لحرمة حياتهم الخاصة والحيلولة دون السماح لهؤلاء المجرمين من الدخول غير المشروع إلى اجهزة وحواسيب افراد 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 حيث لا تترك أي أثراً مادياً، وإنما معلومات يمكن شطبها فور تنفيذ الجاني لفعله السيبراني(٢).

الاستراتيجي، مركز الاهرام للدراسات السياسية والاستراتيجية، اكتوبر ٢٠١٠.

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

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

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 محكمة العدل الأوربية على هذه التساؤلات في حكمها الصادرة في ١٩٩٧/٥/٢٩، 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 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 الاسلحة 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).

(١) حيث جاءت نسبة الاصابة في إيران والهند في المرتبة الاولي و الثانية و اندونيسيا في المرتبة الثالثة من البلدان التي تمكن فايروس Stuxnet التغلل في نظم معلومات منشاتها الصناعية. د/ عادل عبد الصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مرجع سابق، ص ١٤.

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(١).

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

المبحث الثاني

صور الهجمات 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.

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.

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

المطلب الأول

الهجمات السيبرانية الاستراتيجية

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(١).

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

---

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

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(١).

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.

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

(١) المرجع السابق، ص ١١.

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.

المطلب الثاني

الهجمات السيبرانية العسكرية (السيطرة على 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.

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[1]، إلا أنها قد تتعرض لهجمات إلكترونية مثل تعرض البرنامج النووي الإيراني ٢٥ سبتمبر ٢٠١٠ وكذلك محطة "تشرنوبل" في أوكرانيا لهجمة إلكترونية في يونية ٢٠١٧.

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 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

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

الحاسوب من التخطيط والترويج لعمليات إرهابية، والنصب والاحتيال لسرقة الأموال، والتجسس وكذلك القرصنة باعتبارها الجريمة الأكثر شيوعا... الخ.

وهذه الهجمات تكلف الاقتصاد العالمي ما يزيد على ٢٣٠ مليار دولار سنويا ويتعرض الفضاء السيبراني إلى ١٠٠٠ هجمة 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.

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 يوكب 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.

المطلب الثالث

القرصنة والتجسس السيبراني

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، ودعا 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[١].

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

(١) 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.

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 القرصنة السيبرانية إحدى الصور الآتية:

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

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

(٣)- اختراق البريد السيبراني للآخرين والاستيلاء عليه واستخدامه في انتحال شخصية الغير.

(٤)- 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

---

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

مواقع حكومية مثل جماعة ويكيليكس وأنونيموس[١] 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 ٢٠٠٧، والاختراقات المتبادلة بين الصين والولايات المتحدة أو ما بين كوريا الجنوبية[٢].

ويمثل النموذج الإيراني حالة فريدة لتحول الفضاء السيبراني لساحة قتال ذى

(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"

(مجموعة أنونيموس). https//:ar.wikipedia. org/wiki/ _

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

طابع مرن وآخر ذى طابع صلب[١] 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. وهو ما دفع إيران إلى حجب موقع السفارة وتجريم محاولة الدخول عليها على أنها تمثل تهديدا للأمن القومي لديها[٢].

وأصبحت الفيروسات إحدي 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 البرمجيات. ومن أمثلة هذه الفيروسات، فيروس ستاكس نت عام ٢٠١٠، وشمعون[٣]، حشرة الحب، الفدية

---

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

(٢) د/ عادل عبد الصادق، المرجع السابق. وانظر:

Iran Blocks American ‘Virtual Embassy، the new York times، December 7، 2011 http: //thelede. blogs. nytimes. com/2011/12/07/iran-blocks-american-virtual-embassy/

(٣) من أخطر الفيروسات هجومًا على الحواسيب، ويستهدف أكبر الشركات والجهات

Ronmsoware[1].

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

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.

(١) يعمل على تشفير بيانات المستخدم فى شركة ما ويجبر أصحاب الشركة من أجل استعادة البيانات دفع رسوم ويمكن له أن يصيب منظمة بأكملها ويتضمن دفع الرسوم الكترونياً مثل بيتكوين BTC، وهناك آلاف الضحايا لهذا الفيروس فى مدرسة نيوجيرسي وفى ولاية ماين، وشيكاغو وماساتشوستس، للمزيد انظر: Adam ،Alessandrini ،"know BE. ،"hostage rescue manual ،Ronsomware

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 وترويجها، وفي توافر كم هائل للتحليلات السياسية والاقتصادية مع تعدي الحدود الدولية وشكل ذلك ثورة معلوماتية هائلة لا حدود لها عكفت عليها أجهزة الاستخبارات الكبري 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

---

(١) 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.

أشخاص غير مخولين لذلك، والتحقق من الشخصية[١].

المبحث الثالث

الهجمات السيبرانية واستخدام حق الدفاع الشرعي في ضوء ميثاق الأمم المتحدة

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[٢].

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

(١) 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

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

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(١).

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 الى 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(٢).

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.

---

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

(٢) د/ ايهاب خليفة، القوة الالكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت، دار العربي، ٢٠١٧، ص ٥.

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 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].

(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، 96-97; See also، Malcolm Shaw، International Law، (7th edition، 2014)، Cambridge University Press; Yoram Dinstein، War، Aggression and Self-defence، 3ed edition2011.

المطلب الأول

الهجمات السيبرانية

ومدى انطباقها على تهديد السلم والأمن الدوليين

يعد الهدف الأساسى 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 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 فى العلاقات الدولية من المبادئ الأساسية التي نص عليها ميثاق الأمم المتحدة فى المادة ٢ الفقرة ٤ منه، حيث نص على أن: "يمتنع أعضاء الهيئة جميعا فى علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسى 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 الدولى 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:

(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.

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 استبعاد اقتراح "البرازيل" اعتبار إجراءات الضغوط الاقتصادية ضمن الاستخدام غير المشروع للقوة(١).

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

(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"،

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 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].

2016) ، (Septmber 1،International Relations Studies

(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:

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

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

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

القياس والملاحظة Measurability: حيث يمكن قياس الحدث وملاحظته كمياً

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

وحاول الفقيه "Michael Schmitt" التوفيق بين الاتجاهين السابقين عبر تأكيده بأن الهجمات السيبرانية يجب أن تنسجم مع الاقتراب التقليدى القائم على

كحجم الخسائر المادية.

الاختراق Invasiveness: حيث يتم انتهاك الحدود الدولية والدخول غير الشرعي إلى المنشآت أو المؤسسات المحمية.افتراض شرعية العمل Presumptive: حيث يكون للدول الحق في احتكار الاستخدام الشرعي للقوة.

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

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، 37، No. 3، 1999، PP 914. 915.

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

(١) Titiriga Remus، "Cyber-Attacks and International law of Armed Conflicts; a "Jus ad Bellum" perspective"، Journal of International Commercial Law and Technology، Issue 8، No. 3، 2013، P 179.

إحداث الأضرار الجسيمة كاستخدام للقوة، لكن ليس بالضرورة أن تكون تلك التأثيرات أو الأضرار عسكرية فقط، فالهجمات التى تتسبب فى حدوث أضرار اقتصادية جسيمة تعد إذن استخداما للقوة. ووضع Schmitt، خمسة معايير رئيسية لتكييف الهجوم السيبراني كاستخدام للقوة هي:

(شدة الضرر، الضرر الفوري اللاحق، وجود صلة مباشرة بين القوة المسلحة وعواقبها، عبور الهجوم الإلكترونى 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، 37، 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 فى 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 فى إطار المادة ٢ الفقرة ٤ من الميثاق.

وقد تصدت محكمة العدل الدولية في قضية النشاطات العسكرية وشبه العسكرية في نيكاراجوا ١ Nicaragua Case إلى المادة ٤/٢ 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(٢). يشار إلى أن ذلك يأتي منسجماً مع حقيقة أن معظم بنود ميثاق الأمم المتحدة قد وصلت إلى كونها مبادئ أساسية لا يجوز لأي دولة مخالفتها أو الخروج عنها(٣). أما الزاوية الثانية: فتتمثل في

(١) Kriangsak Kittichaisaree, "Public International Law of Cyberspace, Law, Governance and Technology Series", Vol 32, Springer International Publishing, Switzerland, 2017, P163.
(٢) See, Id. Para. 187.
(٣) See, Kamrul Hossain, The Concept of Jus Cogens and the

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(١).

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 باتجاه استخدام القوة في إقليم دولة أخرى(٢)، 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(٣).

Obligation under the U.N. Charter, Santa Clara Journal of International Law, Vol.3, Issue 1, 2005.

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

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

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

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 للآخرين 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(١).

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 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 الحجم والتأثير على الدولة التي تتعرض للهجوم

(١) 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).

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"(١). (كما سيأتي توضيحه).

المطلب الثاني

استخدام حق الدفاع الشرعي

(وفق المادة ٥١ من ميثاق الأمم المتحدة في مواجهة الهجمات السيبرانية)

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"(٢).

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

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

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

استناداً إلى ذيل المادة (٤/٢) 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 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

(١) د/ إسماعيل صبري مقلد (أصول العلاقات الدولية إطار عام) دار النهضة العربية / الطبعة الأولى / القاهرة ٢٠٠٧م ص ٦،٢.

الداخلية – مما أضعف من قوة تلك المحاولة البائسة للانفصال من جانب إقليم "كتالونيا"[١].

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..."[٢].

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 الاعتداء3. 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، ف "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

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

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

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 شروط التناسب بين الفعل ورد الفعل، وهذا ما أكدت عليه محكمة العدل الدولية في قضية "كوبسكوفو" للعام ١٩٩٧[٢].

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[٣].

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

(١) See، Omer Elegab، The Legality of Non-forcible Counter-measures in International Law (Oxford Monographs in International Law)، 1988.
(٢) ICJ, Case Concerning Gabčíkovo–Nagymaros Project (HUNGARYISLOVAKIA), 1997, paragraph 71.
(٣) A. Randelzhofer, Article 51, in The Charter of the United Nations: A Commentary 661, 664 (B. Simma ed.) 1995.

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].

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[٣].

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

(١) ICJ, case concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), Reports 1986, p. 191.
(٢) CJ, case concerning Oil Platforms, (Islamic Republic of Iran v. United States of America), Reports 2003, p. 51.
(٣) UN General Assembly Res. 3314 (XXIX), Definition of Aggression, Adopted 14 December 1974

المتطلبات لاعتبار الاعتداء هجوماً عسكرياً وهي النطاق والشدة والمدة الزمنية[١]، 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 الشروط الواجب توافرها حتى يبقى التصرف متوافقاً مع أحكام المادة، وهذه الشروط هي:

أولاً: الضرورة. ثانياً: التناسب. ثالثاً: الفورية[٢].

أما شرط الضرورة فيقصد به الحالة التي تجبر فيها الدولة على اللجوء للدفاع عن

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

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

النفس باستخدام القوة، حيث لم يعد اللجوء إلى "الطرق السلمية" لفض النزاع بحسب الفصل السادس من الميثاق خياراً[١]، أو أن هذه الطرق قد تم اللجوء إليها ولكنها أثبتت عدم فعاليتها في مواجهة الدولة الأخرى[٢]، 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[٣].

أما شرط الفورية فيقصد به أساساً أن لا تفوت الدولة المعتدى عليها فترة زمنية

---

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

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

(٣) Michael 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.

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.

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)؛ والموقع (معرفة مصدر الهجوم)؛ والاستجابة (القدرة على الاستجابة حتى وإن تعرضت للهجوم أولاً)؛ والشفافية (إدراك العدو لقدراتك على الرد بقوة كبيرة)[1].

ومن ثم يثير الفضاء السيبراني والحرب السيبرانية مشاكل جديدة تقوض الافتراض الأساسي بوجود هذه العناصر الأربعة عند إعداد البلدان لقواعدها الدفاعية العسكرية.

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

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[١].

(١) المرجع السابق نفسه.

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 والمنظمات 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.

واستنادا 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

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 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.