مواجهة الحرب السيبرانية أثناء النزاعات المسلحة في ضوء القانون الدولي الإنساني

مصطفى السيد عبد السلام أبو النور١*، محمد سيد محمد عبد اللطيف٢، أحمد ربيع محمد٣.
١قسم هندسه الحاسب والمعلومات، كلية الهندسة، جامعة الأمير سطام بن عبد العزيز، المملكة العربية السعودية.
٢قسم علم النفس، كلية التربية، جامعة الأمير سطام بن عبد العزيز، المملكة العربية السعودية.
٣ قسم القانون الخاص، كلية الشريعة والقانون بالقاهرة، جامعة الأزهر، مصر.

ملخص البحث

يهدف هذا البحث إلى دراسة التحديات القانونية التي تواجه القانون الدولي الإنساني في التعامل مع الهجمات السيبرانية أثناء النزاعات المسلحة. مع تطور التكنولوجيا واعتماد الدول المتزايد على الفضاء السيبراني، أصبحت الهجمات السيبرانية من أبرز المخاطر التي تهدد البنى التحتية الحيوية، مما يفرض ضرورة تقييم قدرة القانون الدولي الإنساني على حماية المدنيين والحد من الأضرار الناتجة عن تلك الهجمات. يركز البحث على تحليل مدى ملاءمة القواعد التقليدية للقانون الدولي الإنساني، التي وُضعت في الأصل للنزاعات المسلحة التقليدية، للتعامل مع خصائص الهجمات السيبرانية.

اعتمد الباحثون في هذا الدراسة على منهج وصفي لتحليل التحولات التكنولوجية السريعة ودور الذكاء الاصطناعي في تغيير طبيعة النزاعات، بالإضافة إلى المنهج التحليلي لدراسة النصوص القانونية ذات الصلة بموضوع الهجمات السيبرانية، وآراء الفقهاء في هذا الشأن. وتوصلت الدراسة إلى أن الهجمات السيبرانية تختلف في طبيعتها وآلياتها عن الحروب التقليدية، مما يتطلب وضع تشريعات حديثة تتماشى مع قواعد القانون الدولي الإنساني، وخاصة فيما يتعلق بمبادئ التمييز والتناسب.

الكلمات المفتاحية :القانون الدولي الإنساني، النزاعات المسلحة، الأمن السيبراني، الهجمات السيبرانية.

Cyber Warfare during Armed Conflicts considering International Humanitarian Law

==========

١Mustafa El-Sayed Abdel-Salam Aboulnour*

٢ Mohamed Sayed Abdellatif

٣ Ahmed Rabie Mohamed ٣.

١ Department of Computer and Information Engineering, College of Engineering, Prince Sattam bin Abdulaziz University, Kingdom of Saudi Arabia.

٢ Department of Psychology, College of Education, Prince Sattam Bin AbdulazizUniversity , Kingdom of Saudi Arabia.

٣ Department of Private Law, College of Sharia and Law, Cairo, Al-Azhar University, Egypt.

Corresponding Author: m.aboelnour@psau.edu.sa

Abstract:

This study aims to examine the legal challenges faced by international humanitarian law in addressing cyber warfare during armed conflicts. With technological advancement and the growing reliance of nations on cyberspace, cyber-attacks have become one of the primary threats to critical infrastructure, necessitating an assessment of the capacity of international humanitarian law to protect civilians and mitigate the resulting damage from these attacks. The research focuses on analyzing the applicability of traditional international humanitarian law rules, originally designed for conventional armed conflicts, to address the unique characteristics of cyber warfare. The researchers utilized a descriptive approach to analyze the rapid technological transformations and the role of artificial intelligence in altering the nature of conflicts, along with an analytical method to examine relevant legal texts on cyber warfare and scholarly perspectives in this area. The study concludes that

cyber warfare differs in nature and mechanisms from traditional warfare, necessitating the development of modern regulations aligned with international humanitarian law principles, especially regarding the principles of distinction and proportionality.

Keywords: International Humanitarian law, Armed Conflicts, Cybersecurity, Cyber, Attacks.

□

مقدمـــــــة

نتيجة للتطور الهائل في تكنولوجيا الفضاء والاتصالات بدأت الهجمات السيبرانية في الظهور عن طريق مخترقي الشبكات وأنظمة الحواسيب وبنوك المعلومات للمؤسسات والكيانات المدنية والعسكرية سواء كانوا دولا أو أشخاصا يمتلكون خبرة كبيرة في ميدان تقنيات المعلومات والحواسيب الذكية، ولديهم القدرة على اختراق المواقع المحظورة في نظم شبكات الحواسيب وبنوك المعلومات بمختلف أشكالها، لاستهداف المواقع الإلكترونية الحساسة مدنية كانت أم العسكرية، بقصد الحصول على أسرار حيوية، أو وثائق مهمه أو تدمير بنية معلوماتية مهمة.

ونتيجة لذلك تغير مفهوم الأمن القومي لدي الدول حيث تنبهت الدول إلي أنه يلزم للمحافظة علي البنى التحتية في مجالات الطاقة والمياه والزراعة والتجارة والحوسبة والاتصالات والمواصلات والاقتصاد والأمن المعلوماتي وجود نظم تكنولوجية متطورة للتصدي لأي هجوم سيبراني من قبل دول أو قراصنة أو أفراد.

فأصبح مقياس الأمن القومي للدول في الوقت الراهن ومدي صلابته يقاس بمدى قوة دفاعات الدولة السيبرانية وطنيا وإقليميا ودوليا وبالنظر إلي المدي الذي توصلت إليه الدولة من امتلاكها لتكنولوجيا المعلومات والتعاطي معها وقدرتها على توظيفها لبناء حدود فضاء سيبراني استراتيجي وإنشاء أنظمة دفاعية تعتمد علي الذكاء الاصطناعي والتكنولوجي للدفاع عن هذا الفضاء وقدره هذه الأنظمة علي قراءة وتحليل وبرمجة الكيانات الفضائية السيبرانية المعادية لصدها عن اختراق الفضاء السيبراني للدولة، فضلا عن ضرورة وجود قوات وأنظمة سيبرانية هجومية لتحقيق الردع والزود عن انتهاك أو نيل من مقدرات الدولة مما يستدعي إيجاد سياسة تشريعية شاملة تعالج جميع هذه الجوانب من حيث كيفيه رسم الحدود الفضائية السيبرانية وآليات إنشاء وتشغيل أنظمة الدفاع السيبراني وحالاته وكذلك إنشاء وتشغيل أنظمة الهجوم السيبرانية وحالاته وكيفيه المسائلة

المدنية والجنائية حال نسبتها للدولة "جاني" أو عليها "مجني عليه".

أهمية الدراسة:

تتمثل أهمية دراسة موضوع "الوضع القانوني للهجمات السيبرانية علي ضوء القانون الدولي الإنساني"أولا: في حداثة هذا الموضوع وخطورته وتطوره بشكل متسارع، ثانيا: من حيث الآثار المترتبة علي الهجمات السيبرانية لا تقف عند حد الآثار التي تحدثها الحروب التقليدية والتي يمكن توقعها، وإنما تعدت ذلك لتشمل البنى التكنولوجية والمعلوماتية التي يقوم عليها النظام المعلوماتي للدولة من خلال قرصنة المعلومات العسكرية والاستراتيجية حيث تتم عبر فضاء خارجي سيبراني باستخدام برامج ذكية وأنماط خفية غير ملموسة تحاكي عمل الأنظمة المستهدفة، الأمر الذي يتعين معه التعامل مع هذه الظاهرة الخطيرة من خلال وضع تشريعات ملاءمة تحد من خطورتها وتقلل من أضرارها الكارثية.

ثالثا: كما تتجلي أهمية هذا الموضوع أيضا في الحاجة إلى التعرف على طبيعة الهجمات السيبرانية وما وصلت إليه من تطور هائل تخلف عنه آثار سلبية مدمرة وجب التصدي لمعالجتها معالجة قانونية دولية من خلال ما تحتاج إليه الدول والمنظمات الأممية من تشريعات تكميلية وكيفية حماية المدنيين والعسكريين جراء الأضرار الناجمة عن الهجمات السيبرانية.

إشكالية البحث:

تتمثل إشكالية البحث في مدى ملائمة قواعد القانون الدولي الإنساني الحالي للهجمات السيبرانية باعتبارها من ركائز الحروب المعاصرة والتي باتت الدول تنتهجها بعد تخليها عن شن الحروب بالطرق التقليدية، حيث تستخدم فيها تكنولوجيا قتالية تختلف عن وسائل وأساليب الحروب التقليدية تحدث أضرارا جسيمة تفوق أضرار الجروب التقليدية، سواءً كانت مرئية كتلك التي تضر بالبنية التحتية لشبكات المياة أو الكهرباء أو الاتصالات، أو المحطات النووية أو التي تحدث أضرارا عسكرية، وتؤدي إلي إزهاق أرواح مدنيين أو

عسكريين، كما أن ميدان المعركة يدور في الفضاء السيبراني على خلاف الحرب التقليدية، وتكمن المشكلة فيما يتعلق بمدى سريان قواعد القانون الدولي الإنساني على الهجمات السيبرانية بكافة جوانبها، حيث إنها حديثة العهد منذ ما شهده العالم من ثورة تكنولوجية، في حين أن قواعد القانون الدولي الإنساني التي تتعلق بالحرب التقليدية تم صياغتها في اتفاقيات جنيف الأربعة ١٩٤٩م، وبروتوكولاتها الإضافية ١٩٧٧م، منذ عقود طويلة، ولم يتم تطويرها بما تتلاءم مع العمليات السيبرانية.

وتثير تلك الإشكالية عدة تساؤلات هي:

ماهية الحرب السيبرانية؟

ماهية الفضاء السيبراني؟

هل يعد الفضاء السيبراني عنصرا من عناصر الأمن القومي للدول؟

هل تعامل الهجمات السيبرانية معاملة الأسلحة من منظور القانون الدولي الإنساني؟

ما مدي مخاطر الاختراق السيبراني لأنظمة تشغيل البني التحتية للدول؟

ما مدي ملائمة تطبيق قواعد القانون الدولي الإنساني على الهجمات السيبرانية؟

ما هي الجهود الدولية المبذولة لمواجهة الهجمات السيبرانية؟

منهجية الدراسة:

اعتمدت خلال هذه الدراسة على المنهج الوصفي من خلال وصفي للتحول السريع والهائل في مجال تكنولوجيا المعلومات والذكاء الإصطناعي، ما دعي الدول إلي السعي بجد نحو تغيير كامل لأنماط الحرب التقليدية إلي العمليات السيبرانية، والمنهج التحليلي لتحليل النصوص القانونية والآراء الفقهية حول كيفيه الحفاظ علي الفرد والمجتمع من الأثار المدمرة للهجمات السيبرانية،

ومواجهتها وفقا لمبادئ القانون الدولي والقانون الدولي الإنساني، وقرارات المنظمات الدولية ذات الصلة.

خطة البحث:

وصولا الي الهدف المرجو من هذه الدراسة قسمت البحث الي ثلاثة مباحث:

المبحث الأول: مفهوم العمليات السيبرانية وتطورها.

المطلب الأول: نشأة وتطور العمليات السيبرانية واستخدامها في النزاعات المسلحة.

الفرع الأول: نشأة وتطور العمليات السيبرانية.

الفرع الثاني: مفهوم النزاعات المسلحة.

النقطة الأولي: مفهوم النزاعات المسلحة الدولية.

النقطة الثانية: مفهوم النزاعات المسلحة غير الدولية.

المطلب الثاني: أنواع العمليات السيبرانية

الفرع الأول: الفضاء السيبراني.

الفرع الثاني: الأمن السيبراني.

الفرع الثالث: الجريمة السيبرانية.

الفرع الرابع: الحرب السيبرانية.

المبحث الثاني: خضوع العمليات السيبرانية لقواعد القانون الدولي الإنساني.

المطلب الأول: ماهية الهجمات السيبرانية والآثار المترتبة عليها.

الفرع الأول: ماهية الهجمات السيبرانية.

الفرع الثاني: الآثار المترتبة علي الهجمات السيبرانية.

الفرع الثالث: الهجمات السيبرانية أسلحة باعتبار سماتها ومؤثراتها.

الفرع الرابع: مدي انطباق مفهوم الحرب على الهجمات السيبرانية.

المطلب الثاني: العمليات السيبرانية ومبدأ حظر استخدام القوة.

المطلب الثالث: خضوع العمليات السيبرانية لقواعد القانون الدولي الإنساني.

المبحث الثالث: التدابير الدولية لمواجهة العمليات السيبرانية.

المطلب الأول: مدى التزام العمليات السيبرانية بمبادئ القانون الدولي الإنساني.

الفرع الأول: مبدأ التمييز.

الفرع الثاني: مبدأ التناسب.

الفرع الثالث: مبدأ الاحتياط أثناء الهجوم.

المطلب الثاني: جهود المجتمع الدولي لمواجهة الهجمات السيبرانية.

الفرع الأول: قرارات الأمم المتحدة.

الفرع الثاني: الإتحاد الدولي للاتصالات.

الفرع الثالث: اتفاقية بودابيست.

الفرع الخامس: منظمة حلف شمال الأطلسي "الناتو".

الفرع السادس: جامعة الدول العربية.

المطلب الثاني: مواجهة أحكام "دليل تالين" للهجمات السيبرانية.

□

المبحث الأول

مفهوم العمليات السيبرانية وتطورها

تمهيد وتقسيم:

بعد دخول المجتمع الدولي عصر الثورة التكنولوجية أصبحت الدول والمجتمعات والمؤسسات والأفراد تعتمد علي استخدام شبكة المعلومات الدولية في قضاء حوائجها وتحقيق أهدافها المختلفة، وبدأت الدول والجماعات في إدخال الذكاء الاصطناعي وتكنولوجيا المعلومات في شن هجمات عدائية لأغراض مختلفة بصرف النظر عن مشروعية هذه الهجمات وما يمكن أن تحدثه من أضرار، وبذلك أصبح الأمن السيبراني يشكل جزءاً أساسياً من أي سياسة أمنية وطنية، فمستقبل الحروب والصراعات ليس كما كان عليه من قبل، فالعمليات السيبرانية وسيلة حديثة لم تكن معلومة من قبل، ولم يتصورها واضعو القانون الدولي، وقد ألغي الفضاء السيبراني الحدود الجغرافية التقليدية، وأصبح الأفراد والمنظمات مرتبطون اليوم بشبكات واسعة تعمل على نشر المعلومات والبيانات بمعدل أسرع، فأصبحت هذه العمليات تسيطر على التعامل اليومي بين الأفراد والدول مما يحث خطرا كبيرا يتمثل في أن تصبح هذه الأنظمة والشبكات المرتبطة والبيانات الواردة فيها هدفًا لأفعال كيدية متعمدة من قبل الدول، والجهات الفاعلة من غير الدول، فلم يعد غريبا أن يصبح الفضاء السيبراني جبهة جديدة للهجوم، نظرا لسهولة الاتصال السيبراني والاستيعاب العالمي له.

كما بات من الواضح أن سوء الاستغلال المتنامي للشبكات الإلكترونية يؤثر سلبا على سلامة البنى التحتية للمعلومات والخزن الأمنية الاستراتيجية للسفن والطائرات وأجهزة الحاسوب المرتبطة بتشغيل المنشئآت النووية ومحطات توليد الطاقة الكهربائية ومحطات تحلية المياه ومنظومة النقل والمواصلات لا سيما ما يعتمد منها علي الطاقة الكهربائية.

وعليه ومما تقدم أتناول دراسة هذا المبحث من خلال مطلبين: المطلب الأول نعرض من خلاله نشأة وتطور العمليات السيبرانية واستخدامها في

النزاعات المسلحة، والمطلب الثاني نعرض من خلاله أنواع العمليات السيبرانية، وذلك علي النحو التالي:

المطلب الأول

نشأة وتطور العمليات السيبرانية واستخدامها في النزاعات المسلحة

الفرع الأول

نشأة وتطور العمليات السيبرانية

منذ سنة ١٩٩٠، ظهر اهتمام المجتمع الدولى بالعمليات السيبرانية وكان مفهوم الحرب السيبرانية يتسم بالغموض لذا نلاحظ أنه أطلق عليها عدة مسميات منها الحرب الافتراضية أو الحرب الإلكترونية أو الهجمات السيبرانية أو الحرب السيبرانية التي يتم من خلالها قيام القراصنة (**Hackers**) بمهاجمة الملفات والمواقع التي تخص المواقع الإلكترونية للمنشآت المهمة أو مهاجمة الحواسيب التابعة للوحدات العسكرية أو الوحدات الاقتصادية لدول معينة بقصد تدميرها، أو تعطيلها والسيطرة عليها، وزاد الاهتمام الدولي بحرب تكنولوجيا المعلومات لا سيما بعد هجمات الحادي عشر من سبتمبر عام ٢٠٠١، وهجمات ٢٧ ابريل ٢٠٠٠ الإلكترونية التي نفذت ضد استونيا وامتدت لأسابيع، وقد تعرض موقع الرئيس الاستونى وموقع رئيس الوزراء وموقع البرلمان للاختراق، وتعرضت هذه المواقع لسيل من الرسائل مما أدى إلى إغلاقها، وفي عام ٢٠٠٧، تعرضت شركة **TJX** وهي شركة متعددة الجنسيات، حيث تمكنت مجموعة من القراصنة من سرقة بيانات البطاقات الائتمانية وحسابات البنوك وعناوين أكثر من ٤٥ مليون عميل، وفي عام ٢٠٠٩ أكدت وزارة الدفاع الأمريكية تعرض قاعدة بيانات تصميمات الطائرة المقاتلة **F٣٥** التي تكلف تطويرها أكثر من ٣٠٠ مليار دولار أمريكي - للاختراق من قبل قراصنة تمكنوا من سرقة بيانات من المرجح تأثيرها علي نظم تأمين الطائرة وحمايتها.

ومن ثم اعتبرت الدول الفضاء السيبراني أحد ركائز استراتجيات الأمن

القومي لديها، ودفعت الاختراقات المتزايدة والمتكررة لأمن الفضاء السيبراني الدول للعمل على بذل جهود حثيثة في استحداث قوانين لمكافحة الجريمة السيبرانية وإنشاء وحدات عسكرية متخصصة لحماية الفضاء الإلكتروني، لذا عملت الدول علي توحيد الجهود الدولية لوضع الأطر القانونية والتنظيمية والإجرائية لمواجهة المخاطر السيبرانية والحد من آثارها المدمرة.

ومن المبادرات الفعالة التي أطلقتها الدول والمنظمات الدولية لدعم الأمن السيبراني مبادرة الإتحاد الدولي للاتصالات الذي أطلق مبادرة للأمن السيبراني وحلف شمال الأطلنطي الذي أنشا وحدة للدفاع السيبراني، وأطلق الاتحاد الأوربي مبادرة للأمن السيبراني.

كما تبنت الولايات المتحدة الأمريكية الإستراتيجية الدولية للفضاء السيبراني، والتي تعتبر أول وثيقة سياسية تكشف عن الرؤية الشاملة لتكاتف المجتمع الدولي في مجال الحفاظ علي أمن الفضاء السيبراني.

وقد أقر المعهد الدولي للدراسات الإستراتيجية بلندن، بأن الفضاء السيبراني أحد أهم ميادين الصراعات والحروب المستقبلية، فلا توجد دولة مهما عظمت قدراتها العسكرية، ولا مؤسسة مهما عظمت قوتها الإقتصادية في مأمن من خطر الهجمات السيبرانية(١).

وقد شنت هجمات سيبرانية عنيفة علي كل من "جورجيا" و "إستونيا" و"كوريا الجنوبية" و " الولايات المتحدة" وكذلك أدي شن هجمات سيبرانية إلي انقطاعات الكهرباء المتعددة في "البرازيل "، وفي عام ٢٠٠٨ تمكن القراصنة من

---

(١) "Cvber-Attacks and the Use of Matthew C. Waxman The Yale Journal Force: Back to the Future of Article ٢ (٤) "P٤٢٣ ٢٠١١ Vol. ٣٦ of International Law.

الدخول إلى الموقع الشبكي للحكومة والسيطرة عليه لمدة تزيد عن أسبوع، وتوضح انقطاعات الكهرباء في البرازيل الاتساع المتزايد لأنواع أخري مستحدثة 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 ستون مليون إنسان(١).

وبذلك يعد الحفاظ علي الأمن السيبراني للدول بمفهومه الواسع الذي يشمل بالإضافة للجوانب الحربية التحديات التي تعيق الإقتصاد الرقمي وتدفق المعرفة، من أبرز التعقيدات التي تواجه المجتمع الدولي في القرن الواحد والعشرين(٢)، مما دفع المجتمع الدولي إلي إعادة النظر حول المفاهيم التقليدية مثل: الأمن، والسيادة، والقوة، والصراع، والحرب وذلك لتحديد مفهومها في ثوبها الجديد بعد دخول الأنماط السيبرانية في مختلف أنشطة العمليات الحربية بين الدول أو علي صعيد الأفراد ومجموعات القرصنة، كذلك مراجعة الاستراتيجيات الأمنية والأدوات القانونية والسياسية لتحديد وحماية الفضاء السيبراني.

---

(١) د/ عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، وحدة الدراسات المستقبلية، قوانين وتشريعات، إصدارات مكتبة الإسكندرية، العدد ٢٣، سنة ٢٠١٦، ص ٤٠ ، ٤٢.

(٢) د أميرة عبد العظيم محمد – المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام ، مجلة الشريعة والقانون، العدد ٣٥، الجزء ٣، ١٤٤٢ هـ - ٢٠٢٠م، ص ٣٦٦.

الفرع الثاني

مفهوم النزاعات المسلحة

تمهيد وتقسيم

لا شك أن مجال تطبيق القانون الدولي الإنساني هو النزاعات المسلحة سواء كانت نزاعات مسلحة دولية أو نزاعات مسلحة غير دولية، وقد تطور مفهومها ليتحول من نظرية الحرب بمفهومها التقليدي القديم إلى المبدأ الدولي الحديث المتمثل في منع استخدام القوة المسلحة، والنزاعات المسلحة عبارة عن صراعات بين مجموعات مسلحة مختلفة أو بين مجموعات مسلحة والحكومة، وتتضمن استخدام القوة العسكرية والأسلحة، وتعتبر النزاعات المسلحة من أخطر الظواهر التي تواجه المجتمعات، وتؤدي إلى الفوضى والتخريب، كما تؤدي إلى التدمير والحرمان الاجتماعي والاقتصادي والبيئي والثقافي، ويمكن أن يؤثر سلبا على السلم والأمن الدوليين ويشكل تهديدا لحقوق الإنسان والحريات الأساسية، كما يؤدي أيضا إلي إصابة بل ووفاة الكثيرين من المدنيين والعسكريين، ويمكن أن يكون النزاع المسلح نتيجة صراعات سياسية أو اقتصادية أو اجتماعية؛ أو ثقافية؛ أو طائفية؛ أو عرقية أو تاريخية، وقد يتم استخدام الأسلحة والقوة العسكرية لتحقيق أهداف سياسية أو اقتصادية أو تاريخية أو دينية أو لإيجاد حلول للمشاكل والصراعات بين الدول.

وقد ارتكز اهتمام القانون الدولي الإنساني بتنظيم وحفظ العلاقات بين الدول – في إطار تطبيق مبدأ الأمم المتحدة في المحافظة علي السلم والامن الدوليين –، وحديثا بدأ يظهر عناية متزايدة بالفرد، عن طريق وضع كثير من القواعد القانونية لحمايته، وقد ركزت هذه القواعد علي حالة النزاع المسلح بالإضافة أيضا لحاله السلم، لكون حماية الإنسان من أهم المصالح الجديرة بالحماية أثناء النزاعات المسلحة، وأن هذه النزاعات لا تقتصر على النزاعات التي تحدث على الصعيد الدولي، وإنما تمتد لتشمل فضلاً عن ذلك النزاعات التي تحدث على الصعيد الداخلي.

ولبيان مفهوم النزاعات المسلحة سنتطرق إلى المقصود بالنزاعات المسلحة الدولية في نقطة أولي والنزاعات المسلحة غير الدولية في نقطة ثانية علي النحو التالي:

النقطة الأولي: مفهوم النزاعات المسلحة الدولية:

يعرف النزاع المسلح الدولي بأنه: تلك النزاعات التي تشتبك فيها دولتان بالأسلحة وتلك التي تكافح فيها الشعوب ضد السيطرة الاستعمارية، أو الاحتلال الأجنبي، أو ضد جرائم التمييز العنصري وتخضع هذه النزاعات لعدد كبير من القواعد بما فيها تلك المنصوص عليها في اتفاقيات جنيف الأربع والبروتوكول الإضافي الأول لسنة ١٩٧٧١.

كما عرف بعض الفقه النزاعات المسلحة الدولية بأنها: بدء الأعمال القتالية بين دولتين أو أكثر ولا يغير في التكييف القانوني شيء إن كان القتال على إقليم أرضي، أو جوي، أو بحري يعود لأحد أطراف النزاع أو يدخل في تكييف الملكية المشتركة كالفضاء الخارجي أو البحر العالي وما يعلوه من إقليم جوي، أو ما يحتويه من جزر طافية طبيعية أو صناعية، حتى وإن لم يعلن عن الحرب، لأن مصطلح النزاع المسلح أوسع وأشمل من مصطلح الحرب، وما يتطلبه من تعقيدات قانونية[٢].

وتنص المادة الثانية من اتفاقية جنيف الثانية لعام ١٩٤٩ على أن: "علاوة على الأحكام التي تسري في وقت السلم، تنطبق هذه الاتفاقية في حالة الحرب

---

(١) بقرين عبد الصمد صالح حماية المرأة أثناء النزاعات المسلحة في ضوء أحكام القانون الدولي العام، دار الفكر الجامعي، الإسكندرية ٢٠١٧، ص ٣٧.

(٢) هشام بشير وإبراهيم عبد ربة إبراهيم، المدخل لدراسة القانون الدولي الإنساني، ط١، القاهرة: المركز القومي للإصدارات القانونية، ٢٠١٢، ص ١٢٤.

المعلنة أو أي اشتباك مسلح آخر ينشب بين طرفين أو أكثر من الأطراف السامية المتعاقدة، حتى لو لم يعترف أحدها بحالة الحرب".

وتنطبق الاتفاقية أيضا في جميع حالات الاحتلال الجزئي أو الكلي لإقليم أحد الأطراف السامية المتعاقدة حتى لو لم يواجه هذا الاحتلال مقاومة مسلحة.

ويمكن تحديد المقصود بالتزاع المسلح الدولي وفق ما نصت عليه الفقرة (٣) من المادة الأولى من البروتوكول الإضافي الأول لعام ١٩٧٧ المتعلق بحماية ضحايا النزاعات المسلحة الدولية، حيث نصت على أن: "ينطبق هذا البروتوكول الذي يكمل اتفاقيات جنيف لحماية ضحايا الحرب الموقعة في ١٩٤٩/٨/١٢على الأوضاع التي نصت عليها المادة (٢) المشتركة بين الاتفاقيات والتي تنص على أنه: "علاوة على الأحكام التي تسري في وقت السلم، تنطبق هذه الاتفاقية في حالة الحرب المعلنة أو أي اشتباك آخر ينشب بين طرفين فأكثر من الأطراف المتعاقدة، حتى لو لم يعترف أحدها بحالة الحرب وتنطبق الاتفاقية أيضاً في جميع حالات الاحتلال الجزئي أو الكلي لإقليم أحد الأطراف المتعاقدة، حتى لو لم يواجه هذا الاحتلال مقاومة مسلحة".

كما نصت المادة (١) فقرة (٤) من البروتوكول ذاته على أن يشمل مفهوم النزاع المسلح الدولي المنازعات المسلحة التي تناضل بها الشعوب ضد التسلط الاستعماري والاحتلال الأجنبي وضد الأنظمة العنصرية، وذلك في ممارستها لحق الشعوب في تقرير المصير، كما كرسه ميثاق الأمم المتحدة والإعلان المتعلق بمبادئ القانون الدولي الخاصة بالعلاقات الودية والتعاون بين الدول طبقا لميثاق الأمم المتحدة.

ومن الجدير بالذكر أن نشير إلى أن ما يتعلق بسريان القانون الدولي الإنساني وكفالة احترامه على المنازعات المسلحة الدولية قد مر بمراحل، أهمها مرحلة ما قبل عام ١٩٤٩م، حيث كان يسمى القانون الدولي الإنساني باسم "قانون الحرب" ويسري فقط على حالات الحرب المعلنة التي ينظمها ويبين

أحكامها اتفاقية لاهاي المبرمة في عام ١٨٩٩ ، والتي أعيد النص عليها في اتفاقية لاهاي الثانية عام ١٩٠٧، حيث نصت المادة (١) من اتفاقية لاهاي لعام ١٩٠٧ على أن: تعترف جميع الدول المتعاقدة بعدم جواز بدء العمليات العدائية دون إنذار مسبق وصريح، في شكل إعلان صريح مع ذكر الأسباب، أو إنذار آخر مع إعلان مشروط للحرب.

وتجد في هذه المرحلة(i) أن سريان القانون الدولي الإنساني الذي كان يهتم بتنظيم الأعمال العدائية كان مشروطاً بقيام الأطراف في هذه الاتفاقية بأن تسبق حربها بإنذار على شكل إعلان يبين فيه إعلان الحرب، أو بشكل إنذار يتضمن إعطاء مهلة أخيره للطرف الآخر مع إعلان مشروط للحرب عليه.

أما بعد عام ١٩٤٩ و بصدور قانون جنيف (اتفاقيات جنيف الأربع) فقد بينت المادة (٢) المشتركة بين اتفاقيات جنيف الأربع لعام ١٩٤٩م شمول حالات الحرب المعلنة والاشتباكات المسلحة، حتى إذا كان أحد الأطراف لا يعترف بقيام حالة الحرب، أما البروتوكول الإضافي الأول لعام ١٩٧٧م، فقد نص على شمول حروب التحرير الوطنية ضمن نطاق النزاعات المسلحة الدولية.

وعليه فيمكن تمييز النزاعات المسلحة الدولية عن النزاعات المسلحة غير الدولية بوجود استخدام القوة المسلحة من قبل طرفين متحاربين أحدهما علي الأقل جيش نظامي وتنشب خارج حدود أحد الطرفين المتحاربين، ويبدأ النزاع عادة بإعلان حالة الحرب، وتتوقف لأسباب ميدانية كتحقيق الأهداف التي نشبت من أجلها الحرب أو دخول طرف ثالث وتوقيع هدنة أو اتفاق صلح مناسب للطرفين.

وبالتالي فإن النزاع المسلح الدولي يتسم بشكل أساسي بطابعين جوهريين هما الطابع المسلح والطابع الدولي وكلاهما يميزان بين النزاع المسلح الدولي والنزاع المسلح غير الدولي علي خلفية تعارض مصالح بين الطرفين المتنازعين في الظاهر وفي حقيقة النزاع توجد أطراف أخري لها مصالح وأهداف غير

مشروعة تطمع لتحقيقها عن طريق إثارة النزاع وتفاقمه.

النقطة الثانية: مفهوم النزاعات المسلحة غير الدولية

لم يتفق الفقهاء على تعريف موحد للنزاعات المسلحة غير الدولية، ويمكن تحليل هذا المصطلح من خلال وجود نصين أساسيين هما: المادة الثالثة المشتركة بين اتفاقيات جنيف سنة ١٩٤٩ ، والمادة الأولي من البروتوكول الإضافي لسنة ١٩٧٧.

وتعتبر المادة الثالثة المشتركة من اتفاقيات جنيف الأربع لعام ١٩٤٩ هي المادة المعنية بالنزاعات المسلحة الداخلية والتي تشكل مدونة إلزامية واجبة التطبيق كحد أدنى في النزاعات المسلحة الداخلية، إلا أنها صدرت خالية من أي إشارة إلى تعريف لهذه النزاعات، كما لم تحدد أية شروط أو معايير موضوعية يمكن الاستناد عليها للفصل فيما إذا كان نزاع مسلح دولي داخلي قائم من عدمه(١).

كما أن هذه المادة لم تأخذ بالمصطلحات المستخدمة في ظل القانون الدولي التقليدي للتعبير عن النزاعات المسلحة الداخلية، الحرب الأهلية، والثورة، والتمرد وإنما جاءت بمصطلح جديد لتطبق أحكامها عليه وهو مصطلح النزاعات المسلحة غير ذات الطابع الدولي، دون أن تضع له تعريفا واضحا، وانما اكتفت بذكر صفته غير الدولية، والدائرة في أراضي أحد الأطراف السامية المتعاقدة(٢).

---

(١) سيف غانم السويدي، النطاق المادي للقانون الدولي الانساني"، مجلة جنوب الوادي للدراسات القانونية، العدد الثالث ٢٠١٨، ص ٥٣٦.

(٢) حيدر كاظم عبد علي ، القواعد المتعلقة بوسائل وأساليب القتال أثناء النزاعات المسلحة غير الدولية ، مجلة المحقق الحلي للعلوم القانونية والسياسية ، العدد الثاني ،

=

و تنص المادة الثالثة المشتركة لاتفاقيات جنيف الأربع لعام ١٩٤٩ على ما يلي:

"في حالة قيام اشتباك مسلح ليست له صفة دولية في أراضي أحد الأطراف السامين المتعاقدين يتعين على كل طرف في النزاع أن يطبق كحد أدنى الأحكام التالية:

- الأشخاص الذين سلموا أسلحتهم أو أبعدوا عن القتال بسبب المرض أو الجروح أو الأسر أو أي بسبب آخر يعاملون في جميع الأحوال معاملة إنسانية.

فلم تعرف هذه المادة النزاع المسلح غير الدولي إلا أنها حددت أطرافه وواجباتهم، وتشترط لتوفر صفة نزاع مسلح غير دولي ما يلي:

امتلاك الطرف المعادي للحكومة المركزية تنظيما عسكريا له قيادة مسؤولة عن سلوك مرؤوسيها وله نشاط في أرض معينة ويكفل احترام الاتفاقيات وله نظام تتوافر فيه خصائص الدولة.

أن تلجأ الحكومة الى قواتها العسكرية الرسمية لمحاربة الثوار.

- اعتراف الحكومة بصفة المحاربين للثوار.

- اعتراف الحكومة بأنها في حالة حرب.

- ادراج النزاع على جدول أعمال مجلس الأمن أو الجمعية العامة التابعين للأمم المتحدة بصفته مهددا للسلم والأمن الدوليين أو خارقا له أو يشكل عملا عدوانيا.

- تلتزم سلطات الثوار المدنية بمراعاة أحكام اتفاقيات جنيف.

أما المادة الأولى من البروتوكول الإضافي الثاني لاتفاقية جنيف ١٩٧٧ فقد

السنة الرابعة، ص٥.

عرفت النزاعات المسلحة غير الدولية بأنها .... جميع النزاعات المسلحة ... التي تدور على إقليم أحد الأطراف السامية المتعاقدة بين قواته المسلحة وقوات مسلحة منشقة وجماعات نظامية مسلحة منشقة وجماعات نظامية مسلحة أخرى، وتمارس تحت قيادة مسؤول على جزء من إقليمه من السيطرة على ما يمكنها من القيام بعمليات عسكرية متواصلة ومنسقة، وتستطيع تنفيذ هذا الملحق "البروتوكول."

ونجد أن التعريف الموجود في البروتوكول قد ضيق من مفهوم النزاعات المسلحة غير الدولية عن ذلك الموجود في نص المادة الثالثة المشتركة، وذلك بتحديده شرطين مهمين لاعتبار نزاع ما نزاع غير دولي:

الشرط الأول هو شرط ممارسة السيطرة على الإقليم من طرف القوات المسلحة غير الحكومية بما يمكنها من القيام بعمليات عسكرية متواصلة ومنسقة وتستطيع تنفيذ هذا البروتوكول.

الشرط الثاني: كان تطبيق هذا البروتوكول محدد فقط على النزاعات المسلحة بين القوات المسلحة للدولة وقوات مسلحة منشقة، أو جماعات نظامية مسلحة أخرى تكون تحت قيادة مسؤولة.

وقد نص البروتوكول الإضافي الثاني لاتفاقيات جنيف ١٩٧٧ والخاص بالنزاعات المسلحة ذات الطابع غير الدولي مكملا للأحكام التي تضمنتها المادة الثالثة المشتركة من إتفاقيات جنيف وأبقى عليها كما هي، حيث نص البروتوكول في الفقرة الأولى من مادته الأولى علي ما يلي:

يسري البروتوكول الذي يطور ويكمل المادة الثالثة المشتركة بين اتفاقيات جنيف الأربعة المبرمة في ١٢ أغسطس ١٩٤٩ دون ما كان يعمل من الشروط الراهنة لتطبيقها على جميع المنازعات المسلحة التي لا تشملها المادة الأولى من "البروتوكول الإضافي إلى اتفاقيات جنيف الأربعة المتعلق بحماية ضحايا المنازعات الدولية المسلحة، والتي تدورعلى إقليم أحد الأطراف السامية

المتعاقدة بين قواته المسلحة وقوات مسلحة منشقة أو جماعات نظامية مسلحة أخرى وتمارس تحت قيادة مسؤولة على جزء من إقليمه من السيطرة ما يمكنها من القيام بعمليات عسكرية متواصلة ومنشقة، وتستطيع تنفيذ البروتوكول[١].

ومن خلال هذه المادة نجد بأن الأطراف السامية المتعاقدة يقع على عاتقها الإلتزام بأحكام هذه المادة بصورة آلية، ولقد حاول الكثير من مندوبي الدول عام ١٩٤٩ تقديم بعض الملامح الخاصة بالنزاع غير الدولي وإدراجها في تعريف يمكن قبوله، وقدم آخرون عدة معايير لبلورة تعريف هذا النوع من النزاعات، ولكن هناك مقاييس موضوعية، حسب هذه المادة تجعلنا نميز النزاع المسلح غير الدولي عن أي نزاع آخر وهي:

- لابد للطرف المناهض للحكومة المركزية من تنظيم عسكري له قيادة مسؤولة عن سلوك مرؤوسيها وله نشاط في إقليم معين.
- لجوء الحكومة الشرعية إلى القوات العسكرية لمحاربة الثوار.
- اعتراف الحكومة بصفة المحاربين للثوار.
- أن يكون للثوار نظام تتوفر فيه بعض خصائص الدولة ومنها:
- أن يباشر الثوار سلطة فعلية على السكان في جزء معين من التراب الوطني.
- تخضع القوات المسلحة لأوامر سلطة منظمة تعبر عن استعدادها لاحترام قوانين الحرب وأعرافها.

ويعرف النزاع المسلح غير الدولي بأنه على حد تعبير الفقيه مارتينز: " الحروب التي تقوم بين الأعضاء الدولة الواحدة.

---

(١) عصام عبد الفتاح مطر، القانون الدولي الإنساني مصادره، مبادئه أهم قواعده، دار الجامعة الجديدة، الإسكندرية، بدون طبعة ٢٠١١، ص٦٥.

فقد كان التحليل المعاصر لهذه النزاعات يعتبرها فئة من النزاعات المسلحة في مقابل الاضطرابات والتوترات الداخلية المنشأة أصلا من تعريف النزاعات المسلحة(١).

كما عرفت النزاعات المسلحة غير الدولية على أنها تلك النزاعات التي تشهد قتالا بين القوات الحكومية ومتمردين مسلحين، أو النزاعات التي تتقاتل خلالها جماعات متمردة(٢).

ومن الملاحظ٣ أن البروتوكول الإضافي الثاني لعام ١٩٧٧ مال إلى تضييق مفهوم النزاع المسلح غير الدولي مقارنة بمفهوم المادة الثالثة المشتركة لاتفاقيات جنيف الأربعة لعام ١٩٤٩، وذلك باشتراط عنصر الرقابة الإقليمية وأن تكون الدولة طرفا في النزاع، مما يجعل هذا المفهوم قاصرا على الحرب الأهلية فقط، في حين لا تعد النزاعات التي تدور بين مجموعتين أو أكثر من الجماعات المتمردة وفق البروتوكول بأنها من النزاعات المسلحة غير الدولية، حتى وإن توفرت فيها الشروط السالفة.

كما أن القانون الدولي الإنساني ينطبق في زمن النزاعات المسلحة، سواء كانت دولية أم غير دولية.

---

(١) عمر سعد الله تطوير و تدوين القانون الدولي الإنساني، دار الغرب الإسلامي، لبنان ، ١٩٩٧ ، ص ٢٠٦.

(٢) نوال أحمد بسج، القانون الدولي الإنساني وحماية المدنيين والأعيان المدينة في زمن النزاعات المسلحة، منشورات الحلبي الحقوقية، بيروت، لبنان سنة ٢٠١٠، ص ٤٥.

(٣) هاشمي عفاف ، فنيدس عبير حماية الفرق الطبية خلال النزاعات المسلحة مذكرة مكملة لمتطلبات نيل شهادة الماستر في القانون ، كلية الحقوق والعلوم السياسية ، جامعة ٠٨ ماي ١٩٤٥ قالمة ص ٢٥.

المطلب الثاني

أنواع العمليات السيبرانية

تمهيد وتقسيم:

من أهم الأسباب التي دعت المجتمع الدولي للاهتمام بالعمليات السيبرانية وأدواتها هي دخول الفضاء السيبراني حيز الاستغلال بصورة متصاعدة، وشروع عديد من الدول في استخدامه عسكريا.

وتعد الهجمات السيبرانية أهم الوسائل التي تستخدم في القتال العسكري في عصرنا الحالي، وتستهدف العمليات السيبرانية عادة مهاجمة تكنولوجيا المعلومات، ونظم إمدادات الطاقة والخدمات اللوجستية، ووسائل الاتصال الإلكترونية، وكافة المنشآت الحيوية التي تعتمد وسائل تقنية المعلومات أساسا لعملها، بحيث تستهدف الهجمات السيبرانية تعطيل هذه المرافق عن أداء الدور المنوط بها أو تدميرها بالكلية، أو الاستيلاء على المعلومات المخزنة على مواقعها، أو تناولها بالمحو أو التعديل وذلك لضمان إحداث خلل بنظم العمل بها بحيث تخرج عن السبيل الذي ترسمه الدولة للاستفادة من هذه المرافق[١].

ولا يمكن النظر للعمليات السيبرانية باعتمادها صورة وحيدة للهجمات، وإنما تتعدد صور هذه العمليات بطريقة كان لا بد معها للقانون الدولي أن يعيد صياغة قواعده لمعالجة هذه الهجمات بحيث يتصدى لها بالمواجهة أو على الأقل بالتنظيم الذي يتناسب مع قواعد الحروب وفقا لما آلت إليه من تغير في الوسائل والآثار المترتبة عليها.

---

(١) عبد القادر دندن، العلاقات الدولية في عصر التكنولوجيا الرقمية، مركز الكتاب الاكاديمي، عمان، ٢٠٢١، ص ١٦.

وعلي ذلك أتناول دراسة هذا المطلب " أنواع العمليات السيبرانية " من خلال تقسيمه إلى أربعة أفرع، الفرع الأول حول: الفضاء السيبراني، والفرع الثاني حول: الأمن السيبراني، ويأتي الفرع الثالث لبيان: الجريمة السيبرانية، وأخيرا يوضح الفرع الرابع: الحرب السيبرانية، وذلك علي النحو التالي:

الفرع الأول

الفضاء السيبراني

يمكن تعريف الفضاء السيبراني على أنه: عبارة عن حيز سوسيو - مكاني أنتجه الدمج بين التكنولوجيات الوسائطية والإنترنت ضمن مصفوفة تشابكية تتيح إنتاج وتبادل مختلف أشكال البيانات والمضامين النصية والسمعية البصرية والتفاعل بين المستخدمين بكيفيات محكومة بأطر الواقع الاجتماعي وأنظمته الثقافية ورموزه التداولية ومحدداته(١).

ويمكن القول أيضاً بأن الفضاء السيبراني يشمل جميع الحواسيب والمعلومات التي بداخلها والأنظمة والبرامج والشبكات المفتوحة لاستعمال الجمهور العام، وتلك الشبكات التي صممت لاستعمال فئة محددة من المستعملين ومنفصلة عن شبكة الإنترنت العامة(٢).

ومعني ذلك أن الفضاء السيبراني هو المجال المادي وغير المادي الذي يتكون وينتج عن عناصر مثل: أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة

---

(١) Marcelo Mendonça Teixeira، Cyberculture: From Plato to The Virtual Universe، Munich، GRIN Verlag، ٢٠١٢، https://www.grin.com/document/٢٠٠٨٣٢.

(٢) محمود محارب إسرائيل والحرب الإلكترونية - قراءة في كتاب حرب في الفضاء الإلكتروني اتجاهات وتأثيرات . على إسرائيل، المركز العربي للأبحاث ودراسة السياسات، بيروت ٢٠١١، ص١١.

المعلومات، المحتوى معطيات النقل والتحكم، ومستخدمو كل هذه العناصر[١] ويعتمد في حركته على ثنائيات من الآحاد والأصفار المتناهية الصغر في تغيير حركة العالم، وهي التي تدير شبكات من ملايين النظم والبرامج والتطبيقات.

(١) The International Télécommunication Union، ITU Toolkit for CybercrimeLégislation،

مشار اليه في: دلالي، الجيلالي و بلبشير يعقوب (٢٠٢١). رهانات الأمن السيبراني الوطني في ظل التحول الرقمي : قراءة في التأصيل المعرفي واستراتيجية المواجهة التشريعية . مجلة كلية القانون الكويتية العالمية مج ١٠، ع٣٧، ص ٨.

الفرع الثاني

الأمن السيبراني

العمليات السيبرانية تعد نوعا جديدا من الحروب العسكرية تستهدف من خلالها الدولة المتحاربة أن تضعف من قدرات الدولة المعادية، وهو الأمر الذي يوجب على المجتمع الدولي الاهتمام بحماية الأمن السيبراني للدول كافة.

وقد عرف الأمن السيبراني ريشارد كومرو بأنه: عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة(١).

وعرفه آخرون بأنه: عبارة عن مجموعة من الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام من قبل غير المصرح له على شبكات الكمبيوتر، أو سوء الاستغلال واستعادة المعلومات الإلكترونية التي تحتويها بهدف ضمان واستمرارية عمل نظم المعلومات، وتأمين حماية وسرية وخصوصية البيانات الخاصة بفواعل الفضاء السيبراني(٢).

كما عرفته وكالة الأمن الرقمي الأوروبية في أول تشريع أصدرته في هذا الشأن سنة ٢٠٠١، بأنه: قدرة النظام المعلوماتي على مقاومة محاولات الاختراق أو الحوادث غير المتوقعة، التي تستهدف البيانات المتداولة أو المخزنة وفق إطار توافقي، تنتظم فيه الأدوات القانونية والسياسات الأمنية ووسائل الدفاع

---

(١) Richard A. Kemmerer، Cyber security، University of California Santa Barbara، Department of Computer Science، ٢٠٠٣، p.٣.

(٢) يوسف بوغرارة، الأمن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري مجلة الدراسات الإفريقية وحوض النيل المركز الديمقراطي العربي، برلين ألمانيا، المجلد ١، العدد ٣. ص١٧.

الإلكتروني لتحقيق أهداف الأمان السيبراني المنشودة وطنيا وإقليميا ودوليا[١].

الفرع الثالث

الجريمة السيبرانية

لا يزال تحديد مفهوم الجرائم السيبرانية محل جدل فقهي، وذلك يعزوه حداثة النظام السيبراني واتساع نطاق الإعتماد على المعلوماتية في المجالات التقنية والاقتصادية والعسكرية والشخصية؛ لذا بات من المتطلبات الضرورية وضع مفهوم دقيق لكل فعل يمكن أن يوصف بالجريمة في نطاق الفضاء السيبراني.

وقد عرفت الجريمة السيبرانية بأنها: الجريمة التي يكون النظام المعلوماتي فيها وسيلة لارتكاب جريمة تقليدية، إما ضد الأموال كالتحويل الإلكتروني غير المشروع للأموال، أو ضد الأشخاص كجريمة السب أو القذف عبر الإنترنت[٢].

وعرفها البعض بأنها: كل ما يقع على الشبكات وأنظمة تقنية المعلومات والأنظمة التشغيلية ومكوناتها الأجهزة والبرمجيات والخدمات من اختراق أو تعطيل أو تعديل أو استخدام أو استغلال غير مشروع[٣].

---

(١) جمال بوازدية، الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية – التحديات والآفاق المستقبلية. مجلة العلوم القانونية والسياسية، جامعة الوادي الجزائر، المجلد ١٠، العدد ١، أفريل / أبريل ٢٠١٩، ص٢٩.

(٢) نبيل إدريس الجريمة السيبرانية بين المفاهيم والنصوص التشريعية – الجزائر أنموذجا مجلة القانون والمجتمع، جامعة أحمد دراية أدرار الجزائر، المجلد ٥ العدد ٢ سنة ٢٠٠٧، ص ٣٠.

(٣) عبد العزيز بن فهد بن محمد بن داود الجرائم السيبرانية : دراسة تأصيلية مقارنة مجلة الاجتهاد للدراسات القانونية والاقتصادية، جامعة تمنراست، الجزائر، المجلد ٩ ، العدد ٣، سنة ٢٠٢٠، ص ١٤٩ .

ويؤخذ علي التعريفين السابقين للجريمة السيبرانية التركيز علي الجانب الفني فقط علي الرغم من أن لها أبعادا أخري اقتصادية وسياسية وعسكرية، كما تعد الجريمة السيبرانية من الجرائم العابرة للحدود التي يكون من الممكن طمس أدلة إثباتها في الوقت الذي يصعب التحري والتحقيق فيها، كما أنها ترتكب من قبل الأفراد والجماعات وكثيرا ما تكون مجالاً للاتفاق الجنائي والتنسيق الإجرامي الذي يتطلب بدوره تنسيقا أمنيا وجهوداً دولية لمواجهتها.

وقد أبدي المشرع الجزائري اهتماما ملحوظا بالجريمة السيبرانية وتحديد مفهومها حيث أفرد قسما كاملا للجرائم المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات في القانون رقم ٠٤-١٥ المعدل والمتمم في قانون العقوبات، حيث نصت المادة (٠٢/٠١) من القانون رقم ٠٩-٠٤ المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها على أن: الجرائم المتصلة بتكنولوجيا الإعلام والاتصال هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية، وما يعاب على هذا التعريف أنه تقني بحت يركز على المعطى المادي والفاعل الرقمي كوسيلة لارتكاب الجريمة السيبرانية، ويهمل العامل البشري والمعطيات الأخرى ذات الصلة وذات الانعكاس الاقتصادي والبعد الجيو - سياسي والأمني[1].

---

(١) القانون رقم ٠٤-١٥ المؤرخ في ١٠ نوفمبر ٢٠٠٤ المعدل والمتمم للأمر رقم ٦٦-١٥٦ المؤرخ في ٨ يونيو ١٩٦٦، المتضمن قانون العقوبات الجريدة الرسمية، الجزائر، العدد ٧١ ، بتاريخ ١٠ نوفمبر ٢٠٠٤ ، والقانون رقم ٠٩-٠٤ المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المؤرخ في ٥ أوت أغسطس ٢٠٠٩ الجريدة الرسمية، الجزائر، العدد ٤٧، بتاريخ ١٦ أوت أغسطس =

وعرفها النظام السعودي بأنها: "أي فعل يرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام".(١)

وعرفها المشرع القطري بأنها: «أي فعل ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية، بطريقة غير مشروعة بما يخالف أحكام القانون(٢).

كما عرفها المعهد الاسترالي لعلم الإجرام بأنها : تسمية عامة لجرائم ارتكبت باستخدام تخزين البيانات الإلكترونية أو جهاز الاتصالات(٣).

ومن وجهة نظري يمكن تعريف الجريمة السيبرانية بأنها: الفعل الذي يتم عبر بيانات إلكترونية ويتسم بعدم المشروعية بالنظر إلي الهدف منه أو الأثر المترتب علي حدوثه.

٢٠٠٩ (٣٢).

(١) نظام مكافحة جرائم المعلوماتية، المادة الأولى.

(٢) القانون رقم ١٤ لسنة ٢٠١٤، الصادر بتاريخ ١٥/٠٩/٢٠١٤، وللمزيد راجع أيضاً: مجمع البحوث والدراسات أكاديمية السلطان قابوس العلوم الشرطة الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، البحث الفائز بمسابقة الأمير نايف بن عبد العزيز للبحوث الأمنية لسنة ٢٠١٥ – ٢٠١٦ ص ٢٣.

(٣) Cameron S. D. Brown، «Investigating and Prosecuting Cyber Crime: Forensic Depende cies and Barriers to Justice»، International Journal of Cyber Criminology، Vol ٩، Issue ١، January June ٢٠١٥، p. ٥٧.

الفرع الرابع

الحرب السيبرانية

لا يوجد اتفاق حول تعريف واضح ومحدد لمفهوم الحرب السيبرانية وذلك راجع إلي حداثة هذا المصطلح وتعدد مترادفاته وكذلك صعوبة تحديد الطبيعة القانونية لهذا النوع المستحدث من الحروب والذي فرض نفسه علي الساحة الدولية بشكل موسع.

وكلمة السيبرانية مشتقة من الكلمة اللاّتينية سايبر (**cyber**) والتي تعني افتراضي، والسايبر كلمة يجري استخدامها لوصف الفضاء الذي يضم الشبكات العنكبوتية المحوسبة، ومنها اشتقت صفة السيبرانية والتي تعني علم التحكم الأوتوماتيكي، أو علم الضبط وتعني (**Cybernetics**) أيضا القيادة أو التوجيه، والذي يعني علم الإتصالات وأنظمة التحكم الآلي في كل من الآلات والأشياء الحية[١].

ويري البعض أن الهجمات السيبرانية هي: استمرار للحروب التقليدية والمادية، إذ يتألف جندها من المدنيين والعسكريين في آن واحد، كما أنها حرب أدمغة بالدرجة الأولى، كونها تستهدف في المقام الأول تدمير البنية العلمية والمعلوماتية للهدف وتأخذ أشكالا عدة، كشكل الإتصالات بين الجيوش وقياداتها، وإضعاف شبكات النقل والإمدادات اللوجستية، وضرب المعلومات الإقتصادية، والعبث بالمحتوى التقني والرقمي وغيرها[٢].

---

(١) خليفة إيهاب – القوة الإلكترونية وأبعاد التحول في خصائص القوة – مكتبة الاسكندرية – مصر ٢٠١٤م، ص ٢٥.

(٢) سعيد درويش – الحروب السيبرانية وأثرها علي حقوق الإنسان دراسة في ضوء أحكام دليل "تالين" – المجلة الجزائرية للعلوم القانونية والإقتصادية والسياسية – مجلد ٥٤ عدد ٥ – ٢٠١٧م، ص٢٥.

وقد عرف الحرب السيبرانية الأستاذ (SHIN) بأنها: استخدام الطيف الإلكتروني أو الكهرومغناطيسي لتخزين وتعديل وتبادل البيانات وجها لوجه مع أنظمة تحكم في بنى تحتية مرتبطة بها(١).

ويؤخذ علي هذا التعريف من وجهة نظري عدم الدقة والخروج علي المعني حيث أن الحرب السيبرانية ليست استمرارا للحروب التقليدية، بل هي تعبر عن ظهور لنوع جديد من أنواع الحروب يختلف كليا عن أشكال وأنماط الحروب التقليدية من حيث الآليات والتخطيط والتنفيذ وكذلك الآثار المترتبة عليها.

وعرفها عدد من الفقهاء التابعين للناتو الوارد في القاعدة (٣٠) من دليل تالين المتعلق بتطبيقات القانون الدولي في مجالات الصراع والحروب السيبرانية بأنها: كل العمليات السيبرانية سواء كانت دفاعية أوهجومية، والتي يعتقد أنها قد تسبب إصابات أو وفيات للبشر، أو تلف وضرر للأشياء المادية(٢).

وعرفت اللجنة الدولية للصليب الأحمر الحرب السيبرانية بأنها: الأفعال التي يتخذها أطراف النزاع لتحقيق ميزة على خصومهم في الفضاء الإلكتروني باستخدام أدوات تقنية مختلفة وتقنيات تعتمد على الطاقة البشرية من الناحية النظرية، ويمكن تحقيق المزايا عن طريق اتلاف أو تدمير أو اعطاب أو نهب أنظمة الحاسوب لدى الخصم "الهجوم السيبراني" أو بالحصول علي معلومات يفضل الخصم أن تبقي سرية "التجسس السيبراني" أو من خلال الإستغلال

---

(١) حكيم غريب ، صبرينة شرقي تداعيات الحرب الإلكترونية علي العلاقات الدولية "دراسة في الهجوم الإلكتروني علي إيران" فيروس ستكنست، دفاتر السياسة والقانون المجلد ١٢ عدد ٢ – ٢٠٢١م. ص٣٤.

(٢) علي حسين باكير – الحروب الإلكترونية في القرن الواحد والعشرين – مركز الجزيرة للدراسات – قطر ٢٠١٠م، ص٥.

السيبراني[١].

وبرأيي فإنه يمكن تعريف الحرب السيبرانية بأنها: أنظمة دفاع أو هجوم خفية مختلقة في فضاء سيبراني له حدود وأنماط دقيقة وتعمل باستخدام أوصناعة برامج إلكترونية ذكية بهدف الوصول إلي اختراق أو سرقة أو إتلاف بنوك معلومات أو أنظمة تشغيل معدات أو آلات حربية أو مصانع مدنية أو عسكرية أو تعطيل كيان سيبراني هجومي أو دفاعي.

(١) إيهاب خليفة – كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت – دار العربي للنشر والتوزيع – القاهرة ٢٠١٧م، ص٢١.

المبحث الثاني

خضوع العمليات السيبرانية لقواعد القانون الدولي الإنساني

تمهيد وتقسيم:

من المسلم به أن القانون الدولي الإنساني هو القانون المخول له تنظيم النزاعات المسلحة والحروب التي تقع بين الدول، ونظرا لظهور العمليات السيبرانية التي تبنتها الدول والجماعات عند نشوب نزاعات مسلحة، إذ تخضع العمليات السيبرانية لذات القانون الذي يحكم النزاع المسلح الذي تمت في ظله(١).

ولا تثار مشكلة تطبيق القانون الدولي الإنساني في هذه الحالة، أما بالنسبة للهجمات السيبرانية التي تنشب دون أن ترتبط بنزاع مسلح، فهنا يثار التساؤل حول اختصاص القانون الدولي الإنساني بشأنها حيث تقع العمليات السيبرانية بدون خضوعها لتنظيم قانوني الأمر الذي يستدعي تطبيق المبادئ القانونية، لحماية قطاعات البنية التحتية.

كما يقع على عاتق أطراف العمليات السيبرانية الالتزام بمبدأ "حياد الدول"، وبموجب هذا المبدأ يحظر استخدام الشبكات المحلية للدول غير الأطراف في النزاعات السيبرانية، حيث يعد استخدام الشبكات الأجنبية نوعا من اقحام الدول المحايدة ودخولها طرفا في النزاع(٢).

وبالرغم من إمكانية الدول الأطراف تطبيق هذه المبادئ علي الهجمات

---

(١) موسى بن تغري، الحرب السيبرانية والقانون الدولي الانساني، بحث منشور في مجلة الاجتهاد القضائي مجلد ١٢، عدد خاص جامعة محمد خيضر بسكرة الجزائر، ٢٠٢٠، ص ٢٠٧.

(٢) ستار عبد عودة الفهداوي، حماية المدنيين وقت الحرب في الشريعة الاسلامية والقانون الدولي العام، مركز البحوث والدراسات الإسلامية، عمان ٢٠١٧ ص ١٣١.

السيبرانية، إلا أن الواقع العملي يظهر تفلت الدول المتحاربة من الامتثال لهذه المبادئ؛ حيث تتم هذه الهجمات بسرية تامة(١).

وإذا كانت بعض قواعد القانون الدولي الإنساني في شموليتها قد تفيد في تطبيق قواعده على العمليات السيبرانية - إلا أن ذلك لا يعنى بأي حال من الأحوال أن هذه القواعد يمكن تطبيقها على العمليات السيبرانية، حيث أن هذه الأخيرة لها خصوصيتها في وسائل وأساليب الحرب - وأن قواعد القانون الدولي الإنساني قديمة وبحاجة إلي تطور.

وبالرغم من عدم وجود تنظيم تشريعي دولي شامل للعمليات السيبرانية إلا أن هناك مبادئ متعارف عليها وفقا لقواعد القانون الدولي والقانون الدولي الإنساني لذا نقسم هذا المبحث إلي ثلاث مطالب نعرض في المطلب الأول: ماهية الهجمات السيبرانية والآثار المترتبة عليها، المطلب الثاني: العمليات السيبرانية ومبدأ حظر استخدام القوة، وفي المطلب الثالث: خضوع العمليات السيبرانية لقواعد القانون الدولي الإنساني، وذلك علي النحو التالي:

(١) إسلام رمضان هديب، الحرب السيبرانية في ضوء القانون الدولي، مجلة البحوث القانونية والاقتصادية كلية الحقوق جامعة بني سويف، س٣٦، ع١، ٢٠٢٤، ص ١٥١.

المطلب الأول

ماهية الهجمات السيبرانية والآثار المترتبة عليها

تمهيد وتقسيم:

تعد الهجمات السيبرانية حديثة العهد نسبيًا، وهو ما يشكل إحدى أهم التحديات الراهنة التي يواجهها المختصون فى القانون الدولي العام، وبالخصوص في تحديد طبيعتها أو عناصرها، فضلاً عن نطاق هذه الهجمات، وما يترتب عليها من تبعات المسؤولية الدولية، وما يزيد في اتساع التحدى الذي يواجهه المختصون في القانون الدولي العام، إنما يتجسد في غموض مفهوم الهجمات السيبرانية، وعدم الاتفاق على تعريف محدد يمكن الاستدلال في ضوئه لتنظيم استخدامها بالحظر، أو التقييد لمواجهة عواقبها الخطرة على الصعيد الدولي.

كما يعد مصطلح الهجوم السيبراني الأكثر شيوعا في النقاشات حول العمليات السيبرانية، فقد تم استخدام مصطلح "هجوم" لوصف تشوية المواقع الإلكترونية أو اختراق الشبكات أو سرقة المعلومات، أو تعطيل خدمة الإنترنت بشكل كامل، والتي لها أهمية قانونية في إطار قانون الحرب، مما يمنح حق الدفاع الشرعي ضد هذه الهجمات.

كما أن التقدم التكنولوجي سلاح ذو حدين، حيث إن أنظمة الكمبيوتر التي تراقب وتتحكم في البنية التحتية لمختلف المجالات تجلب الكفاءة، ولكن في نفس الوقت تفرض تحديات أمنية بالغة التعقيد.

ومن هذا المنطلق أتناول دراسة هذا المطلب "ماهية الهجمات السيبرانية والآثار المترتبة عليها" من خلال تقسيمة إلي فرع أول حول: ماهية الهجمات السيبرانية، وفرع ثان حول: الآثار المترتبة علي الهجمات السيبرانية، وفرع ثالث حول: الهجمات السيبرانية أسلحة باعتبار سماتها ومؤثراتها، وفرع رابع حول: مدي انطباق مفهوم الحرب على الهجمات السيبرانية، وذلك علي النحو التالي:

الفرع الأول

ماهية الهجمات السيبرانية

اختلف الفقه حول وضع تعريف للهجوم السيبراني من قبل الدول، بل أطلق عليه البعض الحرب الإلكترونية ورغم الاختلاف اللفظي بين كلا المصطلحين إلا انهما يتقابلان في مضمونهما، حيث أن السلوك السيبراني يتشابه مع السلوك التقليدي من حيث القائم بهذا الهجوم، اما الاختلاف الحقيقي فيظهر في أداة الهجوم ومكان الهجوم، ففي الهجوم السيبراني الأداة تكون ذات تقنية عالية، وأيضا المكان الذي انطلق منه الهجوم لا يتطلب انتقال فاعله انتقال جسمانيا، لأنه يتم عن بعد بواسطة خطوط وشبكات الاتصال بين المهاجم ومكان الهجوم المستهدف.

ويمكن التمييز بين الحرب السيبرانية والحرب التقليدية بالنظر إلى طبيعة السلاح المستخدم، وبالتالي يمكن القول إن الحرب السيبرانية هي الحرب التي تستخدم فيها الأسلحة غير التقليدية، وفقاً للآثار المترتبة على استخدام هذا النوع من الأسلحة، والمتمثل بالتدمير واسع النطاق.(١)

كما عرفه **Hayden** المدير السابق لوكالة الأمن القومي ووكالة المخابرات المركزية بأنه: "محاولة متعمدة من دولة لتعطيل شبكات الكمبيوتر الخاصة بدولة أخري أو تدميرها "(٢).

---

(١) Martin C. Libicki: Conquest in Cyberspace: National Security and Information Warfare، New York: Cambridge University Press، ٢٠٠٧.p. ١-١٤.

(٢) Extending the Law of War to Cyberspace، (Sept. ٢٢، ٢٠١٠)، p. ٢٩.

وذهب "**Roscini** إلى القول بأن الهجمات السيبرانية هي: "تطويع الإمكانيات الإلكترونية العسكرية للتأثير على مواقع إلكترونية أخرى لتعطيلها أو تدميرها سواء كانت تقدم خدمات مدنية أو عسكرية[١] .

(١) Marco Roscini:" World Wide Warfare Jus ad bellum and the use of Cyber Force"، MPYUNL، vol. ١٤،٢٠١٠، p. ٩١.

الفرع الثاني

الآثار المترتبة على الهجمات السيبرانية

خلق انتشار الهجمات السيبرانية واختراقها كافة المجالات إلى اكتسابها القدرة على التأثير في حركات الملاحة الجوية والبحرية محدثة خللا في أنظمة الملاحة والعبث في أنظمة التوجيه المعتمدة على المواقع الجغرافية الإلكترونية وأيضاً قد تحدث تشويش على أنظمة الدفاع الجوي للدول والطائرات وإدخال التعديلات الخاطئة بمسارات أجهزة التحكم، وإصابة أنظمة المرافق العامة وتعطيلها مما يضر بأنظمة تشغيل الطاقة ومحطات توزيع الكهرباء وشبكات الاتصالات، كما تؤثر أيضا علي محطات الطاقة النووية و محطات الوقود.

ومن أهم الآثار المترتبة علي الهجمات السيبرانية ما يلي[1]:

الإضرار بالبنية التحتية للدول:

حيث تؤدي شن الهجمات السيبرانية إلى حدوث تعطل بأنظمة تشغيل المصانع للدولة المستهدفة وإرباك الأوضاع الداخلية لها وإحداث الإضرابات مستهدفه أنظمة التحكم المركزية وموارد الطاقة والتمويل والاتصالات والنقل ومرافق المياه.

إلحاق خسائر اقتصادية بالدولة المستهدفة:

نظراً لأهمية القطاع المالي والمصرفي في المجال الاقتصادي للدول فسوف يتأثر النمو الاقتصادي للدولة المستهدفة كما حدث في العديد من الهجمات السيبرانية التي أحدثت خللاً بأنظمة التحويلات بالبنوك وسرقة مبالغ مالية كبيرة

---

(١) هديب إسلام رمضان الحرب السيبرانية في ضوء القانون الدولي. "مجلة البحوث القانونية والاقتصادية، عدد ١ سنة ٢٠٢٤ ص ١٢٥.

من بعض الحسابات البنكية مما يؤدى إلى خروج المستثمرين من هذه الدولة

حدوث أضرار صحية للدولة المستهدفة:

نتيجة دخول أنظمة التكنولوجيا والتقنيات المختلفة الحديثة وأنظمة الذكاء الاصطناعي في تشخيص الحالات المرضية وإجراء العمليات الدقيقة وتحديد أنواع العلاج الأكثر فاعلية وملائمه الحالات المرضى، فأصبح هناك قاعدة بيانات ضخمة تضم الملفات المرضية للأشخاص وملفات التأمين الصحي كما تطورت المستشفيات بتعديل أنظمتها وإدخال الأنظمة الذكية فإذا تعرضت هذه المنظومة الصحية لهجمات سيبرانية ستدمر منظومة الرعاية الصحية، ومن ثم تأثر الفرد بالإصابة أو العجز أو الوفاة.

حدوث أضرار بيئية جراء الهجمات السيبرانية:

أصبح التطور التقني والتكنولوجيا وسيلة للحفاظ على البيئة وحمايتها من التلوث فعن طريق استغلال أنظمة الذكاء الاصطناعي أصبح من الممكن معرفة الأماكن المعرضة للتلوث البيئي وكذا قياس درجاته ومصدره، والتنبؤ بأماكن حدوث التلوث كما تساعد تلك الأنظمة في دقة استشعار التلوث الإشعاعي أو وجود تسرب نووي وعلية يمكن مواجهته بسرعة والسيطرة عليه، فإذا تعرضت هذه المنظومة البيئية لهجوم سيبراني، فإن من شأن ذلك الهجوم أن يؤدي إلى تدمير أنظمة الحفاظ على البيئة للدولة المستهدفة.

حدوث خسائر عسكرية للدولة المستهدفة سيبرانيا:

وهو من أكثر المجالات خطورة وحساسية لكونه هو خط الدفاع عن الدول ونظراً لاعتماد التطورات بمجال التسليح والدفاع على التقنيات الحديثة والتكنولوجيا المتطورة فتأثير الهجمات السيبرانية على المجال العسكري قد يتمثل في قطع الإشارات وموجات التواصل بين السكنات العسكرية وقادة الجيش ويؤثر على إعطاء الأوامر الخاطئة للأسلحة ذاتية التوجيه أو الطائرات ذاتية القيادة بتعديل إحداثيات الأهداف وتوجيهها لضرب أهداف داخل الدولة

نفسها؛ مما يؤدى إلى قتل العسكريين أو المدنيين على حد سواء.

تأثير الهجمات السيبرانية على سيادة الدولة المستهدفة:

نتيجة لاختراق الهجمات السيبرانية لحدود الفضاء السيبراني للدولة المستهدفة وصولا إلي إلحاق الضرر بالهدف سواء كان مدنيا أو عسكريا، فإن ذلك ينال من سيادة الدولة باعتبار أن الحفاظ علي الفضاء السيبراني من الاختراق يعد من مقومات الأمن القومي للدول، ويعد تطبيقا لذلك ما حدث في عام ٢٠٠٧ حيث قامت السلطات في استونيا بإزالة تمثال تذكاري مصنوع من البرونز في العاصمة تالين بدولة استونيا قد وضعه الاتحاد السوفيتي السابق ، وقد ثار هذا التماثل غضب الشعب في استونيا ، حيث يعتبر هذا التماثل رمز للاحتلال السوفيتي السابق الأمر الذي اضطرت معه السلطات استونيا إلى إزالته ، مما أثار غضب السلطات في روسيا من هذا التصرف ، وقامت السلطات الروسية بناءً على ذلك بهجوم سيبراني واسع ترتب عليه شلل تمام في الدولة في استونيا في البنوك ، والمواقع الحكومية ، مما أدى إلى اختراق سيادة الدولة[١]

(١) د حسام عبد الأمير خلف ، البعد الجديد - الخامس في النزاعات المسلحة - الفضاء الالكتروني ، مجلة كلية الحقوق ، جامعة النهرين ، المجلد ١٨ ، ٢٠١٦ ، ص ١٢٥.

الفرع الثالث

الهجمات السيبرانية أسلحة باعتبار سماتها ومؤثراتها

أصبحت الدول تهتم بتكنولوجيا المعلومات ودورها في الصراعات والحروب المستقبلية، وذلك استعدادًا لمواجهة ما قد 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، ولذا بات من الصعب تخيل صراع عسكري اليوم دون أن يكون لهذا الصراع أبعاد 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 الإنترنت للحماية من مئات وآلاف القراصنة المحترفين [١]

فالعمليات السيبرانية أصبحت بديلاً لتلك الحروب التقليدية التي كانت تعتمد على جيوش عسكرية وأسلحة قتالية، فعلى الرغم من أن العمليات السيبرانية تكون بدون نار أو قصف، إلا أن لها جانبًا عنيفًا 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 وبدقة عالية، كما تتميز هذه الحروب بالسرعة والدقة في تنفيذ العمليات العسكرية، وتعتبر من أدوات الحرب

---

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

الشاملة [١] ويتميز الهجوم السيبراني بأنه من الهجمات الخفية[٢] التي لا يلاحظها الضحية رغم أنها تقع أثناء وجوده على الشبكة، والسبب في ذلك تمتع فاعل الهجوم بقدرات فنية عالية تجعله ينفذ هجومه بدقة، كما في حالة إرسال الفيروسات وسرقة الأموال والبيانات الخاصة أو إتلافها والتجسس وسرقة المكالمات وغيرها من الهجمات، كما تتميز الهجمات السيبرانية بأنها عابرة للحدود(٣) ، فلم تعد هناك حدودا مرئية أو ملموسة تقف أمام نقل المعلومات بين الدول، وذلك لما تتمتع به الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات، وبالتالي فان أماكن متعددة في دول مختلفة قد تتأثر بهجمة الكترونية، فقد يكون الفاعل في دولة والهجوم يقع في دولة أخرى [٤].

وبالتالي يمكن القول أن هذه الهجمات تعد تدميرا لا يصاحبه دماء وأشلاء بالضرورة، بل يتضمن التجسس والتسلل ثم النسف، لكن لا دخان ولا أنقاض، ويتميز أطرافه بعدم الوضوح، وتكون تداعياته خطيرة.

وتعرف الأسلحة بوجه عام بأنها: أجهزة أو ذخائر أو أدوات أو مواد أو قطع

---

(١) هاني محمد خليل العزازي : النظام القانوني الدولي لمكافحة المخاطر السيبرانية، مجلة مصر المعاصرة، عدد (٥٤٩) ، يناير ٢٠٢٣ ، ص ٤٧٦.

(٢) Gary Brown، Colonel، Keira Poellet، Major: The Customary International Law of Cyberspace، Strategic Studies Quarterly، ٢٠١٢، p. ١٣٩.

(٣) Johann-Christoph Woltag: Cyber Warfare: Military Cross-border Computer Network Operations Under International Law، Intersentia، ٢٠١٤، p. ١١٢.

(٤) رعد فجر الراوي: القصور التشريعي في مواجهة الهجمات السيربانية، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد (١٠) ، العدد (٣٩)، ٢٠٢١، ص ١٩٤.

من المعدات التي تولد قدرة هجومية يمكن تطبيقها على شخص أو كائن معاد، أو هي وسيلة حرب تستخدم في العمليات القتالية، سواء بندقية أو صاروخ أو قنبلة، والتي يمكن أن تسبب إصابة أو وفاة أو تدمير الأشياء(١)

وبناء عليه فإن السلاح هو كل ما يؤدي إلى الدمار باستخدام القوة الحركية مثل القنابل والصواريخ والقذائف، إلا أن هناك أنواعا أخرى من الأسلحة مثل الغازات والعوامل الكيميائية والبيولوجية، تؤدى إلى التدمير دون استخدام القوة الحركية وعليه فإن العامل الحاسم فيما يتعلق بالأسلحة هو تحقيق الدمار والتأثير الضار على الأشخاص.

وفي هذا السياق فإن تساؤلا يطرح نفسه مفاده هل الهجوم السيبراني يعد سلاحا بالمعني المطروح سلفًا ؟

قدم البروفيسور " **Schmitt** إجابة على هذا التساؤل مفادها أنه بالرغم أن القدرة الحركية السيبرانية تتمثل في تحريك أصابع اليد علي مفتاح الكمبيوتر ليبدأ الهجوم السيبراني، إلا أن العواقب الوخيمة المترتبة على الهجوم السيبراني هي الحاسمة في وصف مثل هذا الحدث على أنه هجوم سيبراني، وقال أن النتائج العنيفة من التسبب في وفاة شخص أو إصابتهم من الهجوم السيبراني تكفي لاعتباره سلاح بالمعني المتعارف عليه في القانون الدولي (٢).

وعليه فإن تأثير القدرة السيبرانية على المنشأة التي يخدمها الحاسب المستهدف من الهجوم، يجعل هذه القدرة سلاحا سيبرانيا، وذلك مثل الهجوم

---

(١) william H. Boothby: weapons and the law of armed conflict، no. ٤، ٢٠٠٩، p. ٣٤٤.

(٢) Cyber Operations and the Jus in Bello: Key Issues، Naval War College International Law Studies، ٢٠١١، v. ٨٧، P.٩٣-٩٤.

على نظام التحكم الذي يتحكم في تشغيل منشأة للمرافق العامة، كمعمل لتكرير البترول، فإن الضرر الذي تسببه العملية السيبرانية لمصفاة البترول، يؤدي إلى اعتبار الأداة الإلكترونية سلاحا إلكترونيا .

وتختلف البنية التحتية لقدرات الأسلحة السيبرانية عن الأسلحة التقليدية فتتكون من جهاز كمبيوتر أو هاتف محمول متصل بالإنترنت وسلسلة من برمجيات فتتكون من جهاز كمبيوتر أو هاتف محمول[١] متصل بالإنترنت وسلسلة من برمجيات تقليدية، وبرمجيات خبيثة وبرامج تجسس، ولا تحتاج عملية التطوير لمعدات متخصصة أو يمكن حظرها كما هو الحال في الأسلحة النووية، والتي تحتاج إلي عمليات تخصيب اليورانيوم وخدمات لوجستية معقدة، كما تتطلب هذه الأسلحة مهارات نادرة لإنتاجها ولا تحتاج لإطلاقها سوي منصات بسيطة وغير مرئية، تتمثل في موقع إطلاق كمبيوتر، وموقع علي شبكة الإنترنت ومحرك بحث وخادم افتراضي أو مادي، كما أن هذه الأسلحة قد يستخدمها العسكريون والمدنيون، بل يتميز فيها المدني علي العسكري بخلاف الحال في استخدام الأسلحة التقليدية، كما أن هجمات الفضاء السيبراني تكون استباقية دون سابق إنذار، وأنها غير محددة المجال أو المدى وتكون أهدافها غير مأمونة، وذلك بخلاف الحرب التقليدية التي تكون أهدافها محددة ومكانها محددًا، كما أن قوات العمليات السيبرانية غير معروفة وغير مرئية.

---

(١) سامي محمد عبد العال، الدفاع الشرعي ضد الهجمات السيبرانية، المجلة المصرية للقانون الدولي – المجلد ٧٩، لسنة ٢٠٢٣م، ص ٣١.

الفرع الرابع

مدي انطباق مفهوم الحرب على الهجمات السيبرانية

إن عدم وجود نصوص محددة في القانون الدولي تنظم العمليات السيبرانية بصورة محددة، لا يعني خلو القانون الدولي من قواعد تنظم هذا النوع من العمليات، إذ يتسع القانون الدولي بقواعده التعاهدية والعرفية ليتمكن من شمول قواعد القانون الدولي لهذا النوع من العمليات، وخاصة تلك القواعد الخاصة بتنظيم استخدام الأسلحة لا سيما غير التقليدية منها(١).

فقد نظمت قواعد القانون الدولي استخدام الأسلحة بأنواعها، وذلك من خلال اتفاقية حظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أوعشوائية الأثر، وهي الاتفاقية التي تنظم استخدام أي سلاح مستحدث، أو أي نوع من الحروب الحديثة التي طرأت دون أن تجد لها تنظيما مباشرا في القانون الدولي، وهي الاتفاقية التي أكدت علي أن حق الأطراف في النزاعات المسلحة في اختيار أساليب ووسائل الحرب لا يمكن عده حقا غير محدود، إذ يحظر استخدام أسلحة تسبب أضراراً مفرطة أو آلاماً لا داعي لها(٢)

وفي هذا السياق تجدر الإشارة إلى أن الحرب في القانون الدولي العام التقليدي هي نزاع مسلح بين عسكريين من دولتين مختلفتين، فهي الوسيلة التي

---

(١) مصطفى نعوس، حقوق والتزامات الدول في الحرب المعلوماتية، بحث منشور في مجلة دراسات علوم الشريعة والقانون، مجلد ٤٠ ملحق، الجامعة الأردنية عمان ٢٠١٣، ص ٧٨٤

(٢) للاطلاع على النص الكامل للاتفاقية راجع الموقع الرسمي للجنة الدولية للصليب الأحمر.

https://www.icrc.org/ar/doc/resources/documents/misc/٦٢sd٤j.htm

تاريخ الاطلاع ٢٠/١٠/٢٠٢٤.

من خلالها تدافع الدول المتحاربة عن حقوقها ومصالحها، ولا يمكن اطلاق مصطلح الحرب إلا على النزاع المسلح بين الدول.(١)

أما بالنسبة للفقه الحديث فقد تغاضى عن بعض القواعد في تحديده لمفهوم الحرب، حيث توسع في مفهوم الحرب ليتضمن أي نزاع جماعي مسلح، حتى إذا لم تتوفر له عناصر التعريف الكلاسيكي من تمتع الجماعة المسلحة بصفة الدولة، كما أصبحت الحرب الأهلية التي تنشب داخل نفس الدولة تندرج تحت مسمى الحرب لدى هذا الفقه(٢).

وبغض النظر عن ترجيح أيا من الاتجاهين فإن العمليات السيبرانية تتماشى مع مضمون كلا الاتجاهين

وتشير اللجنة الدولية للصليب الأحمر إلي أن القانون الدولي الإنساني ينظم الهجمات السيبرانية أثناء العمليات السيبرانية.

وعلي ذلك فإن غالبية الدول والمنظمات الدولية وخبراء القانون الدولي ذهب إلي خضوع العمليات السيبرانية لقواعد القانون الدولي الإنساني، وهو ما انتهي إليه تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي التابع للأمم المتحدة، عامي ٢٠١٣ و ٢٠١٥، حيث ورد به أن أحكام القانون الدولي، وخاصة ميثاق الأمم المتحدة ينطبق على استخدام لتكنولوجيا المعلومات والاتصالات، وهو عنصر لابد منه لحفظ السلام والاستقرار وتهيئة بيئة لتكنولوجيا المعلومات

---

(١) تمارا برو استخدام الأسلحة غير التقليدية في القانون الدولي العام، دار المنهل اللبناني للطباعة والنشر بيروت ٢٠١٠، ص ٣٠

(٢) لفقير بولنوار بن الصديق، جرائم الحرب في ضوء أحكام القانون الدولي، دار الأيام للنشر والتوزيع، عمان٢٠١٧، ص ٢٢.

والاتصالات[١].

وإذا خلت النصوص والمواثيق سالفة الذكر من النص صراحة وبطريق مباشر علي تنظيم العمليات السيبرانية بين الدول فذلك ينفي عدم إمكانيه تطبيق قواعد القانون الدولي الإنساني علي الهجمات السيبرانية وذلك بالنظر إلي الأثر المترتب علي النتائج البالغة الصعوبة علي الدولة المستهدفة، ويكون الخطر أكثر تأثيرا عند تعرض المحطات النووية وأنظمة التحكم في الطائرات لهجمات سيبرانية نظرا لاعتمادها على الحواسيب وتكون الشبكات مترابطة إلى حد يجعل من الصعب الحد من آثار هجوم سيبراني ضد جزء من المنظومة دون الإضرار بأجزاء أخرى أو تعطيل المنظومة بأكملها[٢].

وبقراءة الإحصائيات الخاصة بالهجمات السيبرانية أو الإلكترونية يمكن التعرف علي مدي تأثيرها بالغ الخطورة، فعلي سبيل المثال تلك الهجمات التي استهدفت العراق خلال حرب الخليج الثانية، حيث تشير مصادر كلية الحرب الأمريكية إلى أن ضرب مولدات الطاقة الكهربائية العراقية أدى بشكل غير مباشر إلى موت ما بين ٧٠ إلى ٩٠ ألف مواطن عراقي كنتيجة مباشرة لعدم توفر الطاقة الكهربائية[٣]، وكذلك اختراق الفضاء الإلكتروني في الحرب بين جورجيا وروسيا في أغسطس ٢٠٠٨.

فالقانون الدولي لم يكن لديه أية عقبات في اعتبار استخدام الأسلحة

---

(١) وثيقة الأمم المتحدة A/٦٨/٩٨ ٢٤ حزيران – يونيو ٢٠١٣ – فقرة ١٩.

(٢) اللجنة الدولية للصليب الأحمر، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية، أسئلة وإجابات، ٢٠١٣، ص ١.

(٣) عادل عبد الصادق محمد الجخة، أثر الإرهاب الالكتروني على مبدأ استخدام القوة في العلاقات الدولية – رسالة ماجستير – كلية الإقتصاد والعلوم السياسية – جامعة القاهرة ٢٠٠٩ ص ١٨٠.

البيولوجية أو الكيميائية تقع ضمن عمليات الهجوم المسلح على الرغم من كون هذه الأسلحة غير قابلة للكشف عنها بواسطة الحواس البشرية المجردة كما أنها لا تعتبر من الأسلحة الحركية، مما يستتبع معه أن نوع الأسلحة المستخدمة في أي نزاع مسلح لا يخرجه من نطاق تطبيق قواعد القانون الدولي الإنساني(١).

كما سعي المشرع الدولي جاهدا أن يعالج القصور التشريعي المنظم للعمليات السيبرانية بشكل صريح ومفصل، حيث صدرت عدة قرارات أممية تعالج الاعتداءات بالقوة السيبرانية كما عقدت اتفاقية بودابست لمواجهة الجريمة السيبرانية عام ٢٠٠١ ، وكذلك تم إصدار دليل عن طريق تكليف حلف الناتو لعدد من فقهاء القانون الدولي سمي حينها بدليل تالين وصدر سنة ٢٠١٣.

وعليه فإن مفهوم الحرب حتى وإن كان مفهوما تقليديا فإنه ينطبق على العمليات السيبرانية، إذ أن هذه العمليات تشكل هجوما من دولة على دولة أخرى، أو هجوما من جماعة تفتقر لصفة الدولة على جماعة أو دولة، والنتائج التي تترتب على هذا النوع من العمليات هي ذات النتائج المترتبة على الحرب التقليدية أو ربما تفوقها خطورة(٢).

---

(١) مصطفي نعوس – حق الدولة في استخدام القوة في الفضاء الإلكتروني للدفاع عن النفس – مجلة الحقوق – العدد الأول – جامعة الكويت، ٢٠١٤، ص ٢٠٥.

(٢) حسين إبراهيم حسن طه ، الحرب السيبرانية في ضوء قواعد القانون الدولي، بحث منشور بمجلة كلية الحقوق – جامعة المنوفية، ص ٢١١.

المطلب الثاني

العمليات السيبرانية ومبدأ حظر استخدام القوة

إن اعتماد الدول على نمط الهجمات السيبرانية في عصرنا الحالي فرض اهتماما ملحوظا من قبل قواعد القانون الدولي المنظمة لاستعمال القوة في العلاقات الدولية، ومدى إمكانية تطبيق قواعد القانون الدولي الإنساني المتعلقة بالعمليات السيبرانية.

وقد نصت الفقرة الرابعة من المادة الثانية من ميثاق الأمم المتحدة على مبدأ حظر استخدام القوة في العلاقات الدولية، باعتباره من المبادئ الأساسية للقانون الدولي بأنه: "على جميع الأعضاء في علاقاتهم أن يتخلصوا من التهديد باستخدام أو استخدام القوة ضد سلامة الإقليم أو الاستقلال السياسي لأي دولة، أو في أي حالة أخرى تتعارض مع مبادئ الأمم المتحدة"، وبموجب هذا المبدأ، وفي غير الأحوال الاستثنائية التي أجاز فيها الميثاق اللجوء للحرب، تعد جميع الحروب التي تشنها الدول غير مشروعة.

ويدلل موقع هذه المادة من الميثاق علي مركزيتها والوصول إلى رؤية شاملة لمنظمة الأمم المتحدة في تحقيق الأمن والسلم الدوليين، من خلال عدم التهديد أو استخدام القوة [١]، كما تطور هذا المبدأ ليصبح عرفا دوليا، كما أشارت بذلك محكمة العدل الدولية في قضية الأنشطة العسكرية وشبه العسكرية ضد نيكاراجوا عام ١٩٨٦ [٢].

---

(١) رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة، المجلد ١٥ ، العدد ٢، ديسمبر ٢٠١٨، ص٣٣٩

(٢) Judgment of the international court of justice in Military and

=

غير أن هناك تفسير ضيق لمصطلح استخدام القوة الوارد في ميثاق الأمم المتحدة والذي يعني عدم مشروعية استخدام القوة المسلحة، أو التهديد باستخدامها، وآخر موسع بحيث يعتبر استخدام الدول لأساليب الضغط السياسي أو الاقتصادي استخداما للقوة المحرم اللجوء إليها بموجب الميثاق.

ويدق الأمر عند ظهور عمليات عسكرية غير تقليدية مختلفة شكلا ومضمونا عن أساليب القتال في الماضي فهل تخضع مثل هذه الأنماط الجديدة لمبدأ الحظر المنصوص عليه بموجب الميثاق؟

فالعمليات السيبرانية التي تشنها دولة ضد أخرى تعد انتهاكا لمبدأ حظر استخدام القوة إذا كانت آثارها مضاهية للآثار الناجمة عن استخدام الأسلحة التقليدية، مثل العمليات السيبرانية التي تؤدي إلي إصابة الأفراد أو موتهم أو إلحاق الضرر بالممتلكات أو تدميرها.

ومن وجهة نظري فإن الهجمات السيبرانية التي تشنها دولة علي أخري أشد خطرا وأعتي تأثيرا علي البيئة الإنسانية وما تحويه من بنية تحتية مدنية كانت أو عسكرية وعليه فإن استخدام الدول لأنماط العمليات السيبرانية واختراق الفضاء السيبراني لدولة أخري معتدي عليها أو حتي مجرد التهديد بذلك يعد استخداما للقوة المحرم اللجوء إليها بموجب الميثاق.

وتنص 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 الحالة التي تتعرض بها إلى اعتداء مسلح... ".

Paramilitary Activities in and against Nicaragua (Nicaragua V. United States)، ١٩٨٦، I.C.J. ١٤، ٩٦-٩٧.

ويرى البعض أن هناك اختلافا حول المصطلح المستخدم في المادة (٥١) وهو شرط الاعتداء المسلح لتفعيل الحق في الدفاع عن النفس، ومصطلح استخدام القوة والتهديد بها وفقا للمادة (٢/٤).

أما استخدام القوة أو التهديد بها والذي لا يرقى إلى كونه اعتداءً مسلحا، فيضع الدولة المعتدى عليها أمام خيارات قانونية أخرى، تأتي في مقدمتها الإجراء المضاد والذي يعطي الدولة المتضررة القدرة على الرد ضد الاعتداء بوسائل أخرى دون استخدام القوة[١].

ومن ناحية أخرى فإن فكرة الإجراء المضاد كخيار أمام الدولة المعتدى عليها المقررة في المادة (٢٢) من مشروع مواد مسئولية الدول عن الأفعال غير المشروعة لعام٢٠٠١ جاء مقيدا بمجموعة من الشروط أهمها شرط التناسب بين الخرق والخرق المقابل، وهذا ما أكدت عليه محكمة العدل الدولية في قضية كوسوفو عام ١٩٩٧[٢].

بينما الاحتكاكات المسلحة على الحدود - مثلا - لا ترقى إلى مرتبة الاعتداء المسلح الذي من شأنه تفعيل خيار الدفاع عن النفس وفقا للمادة (٥١)، كما بينت ذلك محكمة العدل الدولية في قضية نيكاراجوا [٣]

---

(١) Omer Elegab; the Legality of Non-forcible counter-measures in International Law، Oxford Monographs in International Law، ١٩٨٨، P. ٢٩.

(٢) (ICJ، Case Concerning Gabcikovo Nagymaros Project (Hungay Islovakia)، ١٩٩٧، Paragraph ٧١.

(٣) (ICJ، Case Concerning Military and Poramilitary Activities in and Against Nicaragua (Nicaragua V. United States)، Reports،

=

وجاء تعريف الجمعية العامة للأمم المتحدة للعدوان مشترطا الخطورة الكافية كأحد متطلبات الهجوم العسكري.

ويستفاد من جملة ما سبق أن كل اعتداء مسلح في ضوء المادة (٥١) يعد في الوقت ذاته استخداما للقوة، ولكن العكس غير صحيح، فالهجوم بالأسلحة الفتاكة كالنووي والدمار الشامل مثلا يعد استخداما للقوة وهجوما مسلحا في آن واحد، وبالتالي يتم تطبيق المادة (٥١) لأنها حققت الشرط الوارد بها.

كما أن تفعيل المادة (٥١) واللجوء إلى الدفاع عن النفس في مواجهة هجوم مسلح لا يعني - في حقيقة الواقع - أن الدولة المدافعة في حل من القيود، فهذا الفهم يناقض قواعد العرف الدولي، كما يناقض المادة (٥١) من ميثاق الأمم المتحدة التي تتطلب مجموعة من الشروط الواجب توافرها حتى يبقى التصرف متوافقا مع أحكامها وتتمثل في: أولا - الضرورة: ويقصد بها توافر الحالة التي تجبر فيها الدولة على اللجوء للدفاع عن نفسها باستخدام القوة، حيث لم يعد اللجوء إلى خيار الوسائل والطرق السلمية لفض النزاع وفقا للمادة (٣٣) من الفصل السادس من ميثاق الأمم المتحدة، كالمفاوضات والتحقيق والوساطة والتوفيق والتحكيم، أو تم اللجوء لهذه الطرق دون جدوي، ثانيا التناسب: ويعني اتخاذ الإجراءات اللازمة والضرورية لرد الاعتداء وعدم تجاوزها، وبعبارة أخرى أن لا تتجاوز الإجراءات المتخذة الهدف العام وهو تحقيق الأمن والسلم الدوليين(١).

١٩٨٦، Para، ١٩١.

(١) Micheal Newton & Larry May; Proportionality in International Law، Oxford University Press، ٢٠١٤: Arbitral Award in the Naulilaa Case ١٩٢٨، ٢ Reports of the International Arbitral Awards ١٠١١-١٠٢٨.

المطلب الثالث

خضوع العمليات السيبرانية لقواعد القانون الدولي الإنساني

القانون الدولي وضع قواعد عامة تنظم استخدام القوة في العلاقات الدولية، ومن هذه المبادئ التي يمكن الاسترشاد بها مبدأ حق المتحاربين في أساليب ووسائل القتال، وكذلك مبدأ التميز بين المقاتلين والمدنيين، وبين المنشئات المدنية والعسكرية[1]، كما يعد تحريم اللجوء إلي استخدام القوة مبدأ رئيسي من مبادئ القانون الدولي، إلا أن الواقع العملي يظهر وقوع هجمات سيبرانية من دولة علي أخري، وخضوع الهجمات السيبرانية للقانون الدولي الإنساني أو خروجها من نطاق تطبيق قواعده تتحدد بالنظر لطبيعتها والنتائج المترتبة عليها، حيث تختلف الهجمات الإلكترونية عن غيرها من الهجمات التقليدية في الوسائل والتنفيذ.

ومن الواضح بجلاء أن اتفاقيات جنيف الأربع المبرمة عام ١٩٤٩ والبرتوكولان الملحقان المضافان لها عام ١٩٧٧، تعد من المصادر الأساسية لقواعد القانون الدولي الإنساني، وهي قواعد واجبة التطبيق على كافة العمليات التي تقوم بها الأطراف أثناء النزاع المسلح، وإذا كان الأصل العام في القانون الدولي الإنساني الوارد في المادة ٣٥ من البروتوكول الإضافي الأول لعام ١٩٧٧ الملحق باتفاقيات جنيف الأربع للعام ١٩٤٩ ينص على: "حق أطراف أي نزاع مسلح في اختيار أساليب القتال ووسائله ليس حقاً لا تقيده قيود " فقواعد القانون الدولي الإنساني لم تتضمن أي دلائل محددة عن العمليات السيبرانية، وليس معنى ذلك عدم خضوع هذه العمليات لقواعد القانون الدولي الإنساني، حيث أنه يتبين من القواعد العامة التي تنظم استخدام الأسلحة

---

(١) د عادل عبد الصادق ، أسلحة الفضاء الإلكتروني في القانون الدولي الإنساني ، مكتبة الإسكندرية ، وحدة الدراسات المستقبلية ، ٢٠١٦ ، ص ٨٢

وأساليب الحرب أنها تشمل جميع التطورات ذات العلاقة، من ذلك ما تضمنه البروتوكول الإضافي الأول الملحق باتفاقيات جنيف الأربع لعام ١٩٧٧، حيث نص على أن "يلتزم أي طرف سام متعاقد عند دراسة أو تطوير أو اقتناء سلاح جديد أو إدارة للحرب أو إتباع أسلوب للحرب، بأن يتحقق مما إذا كان محظوراً في جميع الأحوال أو في بعضها بمقضي هذا الملحق أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد[١].

ومعني ذلك أنه حال شن الهجمات السيبرانية، فإنه يجب علي أطرافها التحقق من مشروعيتها من عدمه وفقاً لقواعد البروتوكول الإضافي أو أيا من قواعد القانون الدولي، كما أن اللجنة الدولية التابعة لحلف شمال الأطلسي، قامت بنشر ما يُعرف "بدليل تالين" الذي يرى بأنه يمكن تطبيق القانون الدولي الإنساني على العمليات السيبرانية، ويجب خضوع الهجمات السيبرانية لقانون النزاعات المسلحة.

كما يعد مبدأ ماتنز من أهم المبادئ التي تعالج القضايا الدولية الحديثة وغير المقننة وفقاً لأحكام القانون الدولي العام، حيث صرح فيودور ماتنز مندوب روسيا لدى مؤتمر السلام ١٨٩٩ "أنه في الحالات غير المشمولة بالأحكام، يظل السكان المتحاربون تحت حماية وسلطان مبادئ قانون الأمم كما جاءت، من التقاليد التي استقر عليها الحال بين الشعوب المتمدنة وقوانين الإنسانية ومقتضيات الضمير العام"[٢]، وذكر هذا المبدأ أيضا في ديباجة اتفاقية لاهاي المتعلقة بقوانين وأعراف الحرب القديمة البرية لعام ١٨٩٩ حيث نصت على أن: حتى تصدر مدونة بقوانين الحرب أكثر اكتمالاً، ترى الأطراف المتعاقدة من

---

(١) انظر : المادة ٣٦ من البروتوكول الإضافي الأول من اتفاقيات جنيف لعام ١٩٧٧.

(٢) Antonio Gessese "The Maetens Clouse: Haif a loaf or simily Pie in the sky?" EJIL VOL ١١١ No.١,٢٠٠٠ p١٨٧

المناسب أن تعلن أنه في الحالات التي لا تشملها هذه اللائحة التي اعتمدتها، يظل السكان المدنيون والمقاتلون تحت حماية مبادئ الأمم الناتجة عن العادات الراسخة بين الشعوب، وما يمليه الضمير العام(١).

وبالرغم من إمكانية تطبيق شرط ماتنز على العمليات السيبرانية، إلا أن الكثير من قواعد القانون الدولي الإنساني بحاجة إلي تطوير، فنجد في تطبيق مبدأ التميز، الذي يُعد الأساس لأحكام البرتوكولان الإضافيان لاتفاقيات جنيف ١٩٧٧ نصت المادة ٤٨ من البروتوكول الأول على أن: " تعمل أطراف النزاع على التميز بين السكان المدنيين والمقاتلين، وبين الأعيان المدنية والأهداف العسكرية، ومن ثم توجه عملياتها ضد الأهداف العسكرية دون غيرها وذلك من أجل تأمين احترام وحماية السكان المدنية والأعيان المدنية - إلا أن ذلك من الصعوبة بمكان تطبيقه في العمليات السيبرانية فهذه الأخيرة يمكن توجيه الهجمات السيبرانية إلى الأنظمة المدنية والبنية التحتية ما لم تكن هذه الأنظمة المدنية والبنية التحتية أهدافا عسكرية(٢).

فالغرض الذي يتم اختياره بالهجمات السيبرانية، هو الغرض الذي من المتوقع أن يسبب خطرا أقل على الأعيان المدنية والمدنيين، على أنه ومراعاة لمبدأ الضرورة العسكرية يتطلب أن يختار الهجوم الذي يتسبب بأضرار وإصابات

---

(١) وقد أشارت عدد من الاتفاقيات إلى مبدأ مارتنز منها اتفاقيات جنيف الأربع لعام ١٩٤٩ الأولى في المادة ٦٣ ، والثانية في المادة ٦٢ ، والثالثة في المادة ١٤٢ ، والرابعة في ١٥٢ ، كذلك البروتوكول الإضافي الأول ١٩٧٧ المادة الأولى فقرة ٢ ، والبروتوكول الإضافي الثاني ١٩٧٧ في ديباجته.

(٢) د شريف عبد الحميد حسن رمضان الحرب السيبرانية ومدى ملائمتها مع القانون الدولي الإنساني – مجلة كلية الشريعة والقانون بتفهنا الأشراف – دقهلية – العدد الثالث والعشرون لسنة ٢٠٢١ م الجزء الرابع ص ٣٢.

أقل، وفي حالة وجود أهداف كثيرة إلا أن إحداها يتحقق معها ميزة عسكرية أكثر من مثيلاتها، وفي هذه الحالة من حق المهاجم توجيه الهجمات السيبرانية المباشرة ضد الهدف العسكري الذي يحقق أكثر ميزة ممكنة في النزاع المسلح، ومن هذا المنطلق لابد أن ينظر إلى الهجمات السيبرانية إلى الضرر الذي يلحق بالمنشئات والبنية التحتية المهمة بالنسبة للمدنيين(١).

كما يُعد مبدأ الإنسانية ضمانة قانونية أساسية لاحترام حقوق الإنسان أثناء سير العمليات الحربية، حيث يلزم الأطراف المتنازعة الأخذ به، وهو التزام قانوني دولي في غياب الاتفاقيات الدولية التي لا يوجد بها حل لبعض الحالات(٢) ، حيث يعالج جميع أفعال الأطراف المشاركة في النزاع المسلح، فمبدأ الإنسانية يعنى الاعتراف بالحرب باعتبارها حقيقة واقعية، ويسعى في الوقت ذاته إلى وضع حدود لاحترام حقوق الإنسان، وذلك عن طريق وضع قواعد وسلوكيات للحرب تأخذ في حسبانها كلاً من الضرورة العسكرية، والضرورة الإنسانية التي تصون كرامة الإنسان، ويمكن تطبيق هذا المبدأ على الهجمات السيبرانية حيث من الممكن تطابقها مع أساليب الحرب الأخرى من حيث التسبب في الآلام والأضرار للمدنيين والعسكريين(٣).

كما أن مبدأ التناسب الذي يتمثل في التزام الأطراف المتحاربة في استعمال وسائل وطرق قتالية تتناسب مع الهدف العسكري دون أن تؤدى بطبيعتها إلى

---

(١) د مايكل شميت ، الحرب بواسطة شبكات الاتصال ، الهجوم على شبكات الكومبيوتر والقانون في الحرب ، المجلة الدولية للصليب الأحمر ٢٠٠٢ ، ص ١٣٠ .

(٢) د محمد فهاد الشلالدة ، القانون الدولي الإنساني ، منشاة المعارف ، الإسكندرية ، ٢٠٠٥ ، ص ٦٣ .

(٣) د محمود حجازي محمود ، العنف الجنسي ضد المرأة في أوقات النزاعات المسلحة ، دار النهضة العربية – القاهرة ٢٠٠٧ ص ٦٤

إحداث آثار مفرطة الضرر بالمقاتلين أو تلحق آثار عشوائية تؤثر على المدنيين(١).

كما تمثلت هذه الجهود في السعي الدؤوب لأن تظل الأنماط الجديدة من الحروب لا سيما العمليات السيبرانية، مشمولة بالضوابط ومحصورة في الحدود التي أرستها أحكام القانون الدولي الإنساني، بالرغم من عدم انتشارها حال إبرام تلك الاتفاقيات.

وخلافا لما استقر عليه غالبية الفقه ذهبت بعض الآراء إلي عدم خضوع الهجمات السيبرانية لقواعد القانون الدولي الإنساني، حيث خلت مواثيق القانون الدولي الإنساني من نص ينظم الهجوم على شبكات الحاسوب، أو يعالج قواعد تتعلق بحرب المعلومات، والقانون الدولي الإنساني المعمول به حاليا لا يتلاءم مع وسائل الحرب الإلكترونية بالإضافة إلى أن المعاهدات القائمة حاليا يرجع تاريخها إلى ما قبل وجود أو ظهور الهجمات عبر شبكات الحاسوب(٢).

كما أن هناك رأيا آخر يبرر ذلك بقوله: إن عدم انطباق المعاهدات الإنسانية على هذه الأسلحة، هو أن قواعد القانون الدولي تعالج الأساليب والوسائل الحركية بطبيعتها**kinetic** ، وحيث أن الهجوم على شبكات الحاسوب غير مادي بطبيعة الحال، فإن الهجمات عن طريق الحاسوب تقع خارج نطاق القانون الدولي الإنساني، أي أن قواعد القانون الدولي الإنساني تنطبق على النزاعات

---

(١) د مزيان جعفر ، مبدأ التناسب والأضرار الجوارية في النزاعات المسلحة ، رسالة ماجستير، كلية الحقوق ، جامعة يتزى ، وزد ، ٢٠١١ ، ص ٧ .

(٢) عمر محمود أعمر الحرب الإلكترونية في القانون الدولي الإنساني دراسات علوم الشريعة والقانون، المجلد ٤٦ عدد ٣ – ٢٠١٩ ص ١٣٦. الرابط التالي: https://journals.ju.edu jo

المسلحة ولكن الهجوم على شبكات الحاسوب ليس له الطابع المسلح(١).

ووفقا لما استقر عليه غالب الفقه فإن قواعد القانون الدولي الإنساني تنطبق عند قيام نزاع مسلح، ولا يمكن الاعتداد بقالة أن الاتفاقيات القائمة أغفلت معالجة الهجوم على شبكات الحاسوب وأخرجتها من نطاق قواعد القانون الدولي الإنساني، والدليل علي ذلك شرط مانتز الذي ينص على أنه "يظل المدنيون والمقاتلون في الحالات التي لا ينص عليها في الاتفاقيات تحت حماية وسلطان مبادئ قانون الشعوب كما استقر بها العرف ومبادئ الإنسانية وما يمليه الضمير العام(٢)".

كما أن الزعم بأن الهجوم على شبكات الحاسوب يرجع تاريخه إلى ما بعد اعتماد المواثيق الحالية ليس سليما، حيث أن هذا التبرير كان قد قدم إلى محكمة العدل الدولية لترى مدى مشروعية التهديد بالأسلحة النووية أو استخدامها، ورفضت المحكمة في رأيها الاستشاري القول بأنه نظرا لأن المبادئ والقواعد الإنسانية قد وضعت قبل اختراع الأسلحة النووية، فإن القانون الدولي الإنساني يكون غير منطبق عليها.

ويؤيد ذلك أيضا ما قررته المادة الثانية المشتركة في اتفاقيات جنيف لعام ١٩٤٩ كما ذهب البعض أيضا إلي تطبيق قواعد القانون الدولي الإنساني علي الهجمات السيبرانية بمفردها، دون أن تكون جزءاً من عمليات عسكرية باستخدام الهجوم المسلح التقليدي حيث تخضع هذه الهجمات لقواعد القانون الدولي

---

(١) مايكل ن شميث – الحرب بواسطة شبكات الإتصال : الهجوم علي شبكات الكمبيوتر "الحاسوب" والقانون في الحرب – المجلة الدولية للصليب الأحمر – ٢٠٠٢ ص ٨٩.

(٢) - Ahmed Abou-el- Wafa، current value of customory international humanitarianlaw، revue egyptienne de droit international، vol ٦٣، ٢٠٠٧، p ١٤.

الإنساني بالاستناد إلي طبيعتها، طالما استهدفت منشئآت حيوية مدنية كانت أم عسكرية[١].

وبالنسبة لتطبيق قواعد القانون الدولي الإنساني على العمليات السيبرانية التي تتم ضمن نزاع مسلح، فقد ذهب الاتجاه الغالب لتطبيق قواعد القانون الدولي الإنساني عليها حيث أن غياب معالجة نصوص القانون الدولي الإنساني للعمليات السيبرانية، أمر يبرر بعدم حدوثها حال وضع تلك النصوص، وقد ورد في تعليق اللجنة الدولية للصليب الأحمر على اتفاقية جنيف الأولى "عندما تنفذ إحدى الدول عمليات سيبرانية ضد دولة أخرى واقترن ذلك ودعمه بعمليات عسكرية أكثر تقليدية، فهذه الحالات، بمثابة نزاع مسلح دولي"[٢].

فضلا عن أن خلو قواعد القانون الدولي الإنساني من إشارات محددة لا يعني عدم خضوع هذه العمليات لقواعده، لأن قواعد القانون الدولي الإنساني العامة التي تنظم جميع أساليب الحرب ووسائلها بما فيها استخدام الأسلحة، قد أتت لتشمل كافة التطورات ذات الصلة، وهو ما تشير إليه المادة (٣٦) من البروتوكول الاضافي الأول الملحق باتفاقيات جنيف الأربع لعام ١٩٧٧ إذ نصت على أن: يلتزم أي طرف سام متعاقد عند دراسة أو تطوير أو اقتناء سلاح جديد،

---

(١) مايكل من سميت . " الحرب بواسطة شبكات الاتصال : الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب المجلة الدولية. للصليب الأحمر مختارات من أعداد ٢٠٠٢، ، من ٩٠ الرابط:

https://www.icrc.org/ar/doc/resources/documents/misc/٥x٦lsp.htm

(٢) المقريف، نورية الساعدي، الحرب السيبرانية في ضوء أحكام القانون الدولي العام. مجلة أبحاث ،٢٠٢٢، ص ١٦

أو أداة للحرب، أو اتباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظوراً في جميع الأحوال أو في بعضها بمقتضى هذا الملحق "البروتوكول".

وبالنظر إلي الرأي الاستشاري لمحكمة العدل الدولية الصادر عام ١٩٩٦ والمتعلق بمشروعية التهديد بالأسلحة النووية أو استخدامها والذي ذهبت فيه إلى القول: إن التهديد بالأسلحة النووية أو استخدامها مخالف بصورة عامة لقواعد القانون الدولي المنطبقة في أوقات النزاع المسلح وخاصة مبادئ القانون الإنساني وقواعده، وذلك بقياس استخدام الأسلحة السيبرانية على استخدام الأسلحة النووية، وبذلك يمكننا تأييد خضوع الدول عند استخدام الأسلحة السيبرانية في النزاعات المسلحة لأحكام القانون الدولي الإنساني.

المبحث الثالث

التدابير الدولية المتخذة لمواجهة الحروب السيبرانية

تمهيد وتقسيم:

من الممكن أن يرتب الهجوم السيبراني الذي يستهدف نظاماً معيناً أضرارا على أنظمة أخرى مختلفة، بغض النظر عن مكان وجود تلك الأنظمة، فالهجمات التي تشن ضد دولة واحدة من الممكن أن تؤثر على العديد من الدول الأخرى، بغض النظر عن مكان وجودها وعن كونها طرفا في النزاع [(١)].

ورغم أنه لم تظهر إلي النور بعد اتفاقية دولية تحظر استخدام الهجمات السيبرانية أو تضبطها، إلا أن هناك اهتمام دولي متزايد صوب اتخاذ خطوات عملية في مواجهة خطورة الهجمات السيبرانية.

كما أجريت مناقشات بشأن تطبيق القانون الدولي بما في ذلك القانون الدولي الإنساني، في المنظمة الاستشارية القانونية الأسيوية الأفريقية (الكو) التي أنشأت في عام ٢٠١٥ فريقا مفتوح العضوية بشأن القانون الدولي في الفضاء السيبراني.

وفي غضون عام ٢٠١٨، أنشأت الجمعية العامة للأمم المتحدة أيضاً الفريق العامل المفتوح العضوية، والذي أتاح للجمعية العامة إمكانية عقد اجتماعات تشاورية مع جميع الأطراف المعنية، وكذلك الجهود البارزة التي حققتها المنظمات الدولية والتي نتناولها خلال هذا المبحث عبر التقسيم التالي: مدي التزام العمليات السيبرانية بمبادئ القانون الدولي الإنساني في مطلب أول،

---

(١) توران جيزلو تيلمانرو دنها و سروكنو تدورمان القانون الدولي الإنساني وحماية المدنيين من آثار العمليات السيبرانية أثناء النزاعات المسلحة – المجلة الدولية للصليب الأحمر ، مجلد ١٠٢ (٩١٣) ٢٠٢٠ ص ٢٩٤ .

والذي يشمل فرعه الأول: مبدأ التمييز، وفرعه الثاني: مبدأ التناسب، وفرعه الثالث: مبدأ الاحتياط أثناء الهجوم، ثم جهود المجتمع الدولي لمواجهة الهجمات السيبرانية في مطلب ثان والذي يشمل الفرع الأول منه علي: قرارات الأمم المتحدة والفرع الثاني منه علي: الإتحاد الدولي للإتصالات والفرع الثالث منه علي: إتفاقية بودابست والفرع الرابع منه علي: مؤتمر الأمم المتحدة لمنع الجريمة والعدالة ، والفرع الخامس منه علي: منظمة حلف شمال الأطلسي "الناتو"، والفرع السادس منه علي: جامعة الدول العربية، وفي المطلب الثالث: مواجهة أحكام "دليل تالين" للعمليات السيبرانية، وذلك علي النحو التالي:

□

المطلب الأول

التزام العمليات السيبرانية بمبادئ القانون الدولي الإنساني

تمهيد وتقسيم:

قواعد القانون الدولي الإنساني لا تضفي أية مشروعية على الحرب، وإنما تتعامل معها بشكل موضوعي فمن المسلم به عدم إمكانية تفادي وقوع حرب بين البشر، وبالتالي فإن الامتثال للقانون الدولي الإنساني من جميع الأطراف المتنازعة يعد أساساً جوهرياً لتحقيق الغايات والأهداف المنوطة بالقانون، ويحكم سير العمليات العدائية عدداً من المبادئ الأساسية للقانون الدولي الإنساني: وهي مبدأ التمييز، ومبدأ التناسب ومبدأ الاحتياطات أثناء الهجوم. فهل تمتثل العمليات السيبرانية لهذه المبادئ ؟

لبحث مدى قدرة العمليات السيبرانية على الامتثال لأحكام القانون الدولي الإنساني، ينبغي في البداية الإشارة إلى أن القانون الدولي الإنساني - أو كما في الدوائر العسكرية بقانون النزاعات المسلحة - ينظم السلوك الفعلي للأعمال العدائية في ساحة القتال، وتهدف مبادئه إلى تخفيف معاناة الإنسان أثناء النزاعات المسلحة، وذلك من خلال حماية الأشخاص غير المشاركين في الأعمال العدائية، وقصر وسائل وأساليب القتال على تلك الضرورية لتحقيق الهدف المشروع من النزاع وهو حماية الأرواح المدنية والعسكرية.

من هذا المنطلق، فإن مبادئ القانون الدولي الإنساني المشار إليها - التمييز والتناسب والاحتياط أثناء الهجوم هي مبادئ تكمل بعضها البعض للوصول للموازنة بين الاعتبارات الإنسانية التي تتمثل في حماية المدنيين والاعتبارات العسكرية وهي تحقيق الهدف من النزاع المسلح، وفيما يلي نتناول هذه المبادئ من خلال ثلاثة فروع على النحو التالي: الفرع الأول: مبدأ التمييز، الفرع الثاني: مبدأ التناسب، الفرع الثالث: ومبدأ الاحتياطات أثناء الهجوم، وذلك علي النحو التالي:

الفرع الأول

مبدأ التمييز

يتطلب مبدأ التمييز بأن يميز المقاتل بين المجندين والمدنيين وبين الأهداف العسكرية والأعيان المدنية(١)، وقد رسخت المادة (٤٨) من البروتوكول الإضافي الأول لعام ١٩٧٧ الملحق باتفاقيات جنيف لعام ١٩٤٩ قاعدة عامة لحماية المدنيين والأعيان المدنية؛ حيث نصت على أن تعمل أطراف النزاع على التمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية.

وهذه القاعدة جاءت مكملة للقواعد المنصوص عليها في المادة (٥١) وعلى الأخص فقرة (٢) والمادة (٥٢) الفقرة (١) من البروتوكول الإضافي الأول، تعتبر المادة (٤٨) سالفة الذكر ذات طبيعة عرفية تكون واجبة التطبيق في أوقات النزاعات المسلحة الدولية وغير الدولية، وإذا ما ثار الشك حول طبيعة الشخص أو العين، فترجح الكفة للطابع المدني لهذا الشخص وتلك العين(٢).

وقد نصت المادة (٣/٥١) من البروتوكول الإضافي لعام ١٩٧٧ الملحق باتفاقيات جنيف الأربع لعام ١٩٤٩ على أن: يتمتع الأشخاص المدنيون بالحماية التي يوفرها هذا القسم ما لم يقوموا بدور مباشر في الأعمال العدائية وعلى مدى

---

(١) Kenneth Anderson and Mathew C. Waxman، Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can ،American University Washington College of Law، Research Paper No. ٢٠١٣-١١p١١.

(٢) جون ماري هنكرتس ولويز دوز والد - بك القانون الدولي الإنساني العرفي: المجلد الأول: القواعد اللجنة الدولية للصليب الأحمر، القاهرة، ٢٠٠٧، ص ٣، ص ٢٣.

الوقت الذي يقومون خلاله بهذا الدور، ومن هنا فإن الطبيعة غير المتماثلة للحروب اليوم وتكاثر النزاعات المسلحة غير الدولية التي تدور رحاها في المدن والتي يشترك فيها المدنيون من خلال قيامهم بأدوار مختلفة تشكل عقبة أمام أنظمة الأسلحة هذه لجهة التمييز بين المدنيين والأهداف المشروعة، لا سيما أن العبرة في التمييز هنا من خلال سلوكهم العدائي، وهو ما قد لا تتمكن الأسلحة ذاتية التشغيل من تفسيره على النحو الذي يضمن تطبيق مبدأ التمييز على النحو الواجب[١]

□

(١) UN Human Rights Council، Report of the Special Rapporteur on extrajudicial ،summary or arbitrary executions، Christof Heyns، op. cit.، para. ٦٨.

الفرع الثاني

مبدأ التناسب

إذا كان مبدأ التمييز يحظر الهجمات المباشرة ضد المدنيين، فإن مبدأ التناسب يحمي المدنيين من الضرر غير المباشر الذي يلحق بهم إذا كان هذا الضرر غير متناسب مع الميزة العسكرية المتوخاة من الهجوم، حيث نصت المادة (٥١/٥/ب) من البروتوكول الإضافي الأول لعام ١٩٧٧ الملحق باتفاقيات جنيف لعام ١٩٤٩ على أن: «تعتبر الأنواع التالية من الهجمات من بين هجمات أخرى، بمثابة هجمات عشوائية... الهجوم الذي يتوقع منه أن يسبب خسارة في أرواح المدنيين أو إصابتهم أو أضرارا بالأعيان المدنية أو أن يحدث خلطا من هذه الخسائر والأضرار، يفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة.

ويعنبر هذا المبدأ مبدأ عرفي يسري في النزاعات المسلحة الدولية وغير الدولية، إذ نصت عليه القاعدة (١٤) من القواعد العرفية التي وردت في الدراسة التي أعدتها اللجنة الدولية للصليب الأحمر وقضت بأن: «يحظر الهجوم الذي قد يتوقع منه أن يسبب بصورة عارضة خسائر في أرواح المدنيين أو إصابات بينهم، أو أضرارا بالأعيان المدنية، أو مجموعة من هذه الخسائر والأضرار، ويكون مفرطا في تجاوز ما ينتظر أن يسفر عنه من ميزة عسكرية ملموسة أو مباشرة.

أن العملية الذهنية التي تُجرى لتقييم مدى تناسب الميزة العسكرية المتوقعة والضرر المحتمل حصوله في صفوف المدنيين، تنطوي على عملية صنع قرار معقدة وقائمة على أساس كل حالة على حدة؛ حيث يجب تقييم الظروف في مجملها، وبهذا الخصوص؛ فقد أشار تقرير المقرر الخاص المعني بحالات الإعدام خارج القضاء أو إجراءات موجزة أو تعسفا المقدم إلى مجلس حقوق الإنسان، إلى أنه من المتعارف عليه على نطاق واسع بأن التناسب على حكم متميز للإنسان، وأن التفاسير القانونية لهذا المبدأ تعتمد صراحة على مفهوم «الحس السليم» و«حسن النية» و "معيار القائد العسكري المعقول".

ويري الدكتور (Sassoli) أنه على الرغم من أن عملية برمجة مدى تناسب الميزة العسكرية المتوقعة مع الأضرار العرضية في صفوف المدنيين هي عملية محيرة يصاحبها إعطاء حكم بناء على تقييم شخصي، إلا أنه قد يكون من الممكن تحديد مؤشرات ومعايير لتقييم التناسب وذلك بالتعاون بين الخبراء العسكريين والإنسانيين، لجعل الحكم أكثر موضوعية.

الفرع الثالث

مبدأ الاحتياطات أثناء الهجوم

يقضي القانون الدولي الإنساني بقيام الأطراف المتحاربة باتخاذ احتياطات مناسبة عند الهجوم من أجل تجنب أو تقليل الضرر العرضي الذي قد يسفر عنه الهجوم ويؤدي بالتالي إلى خسائر في أرواح المدنيين أو إلحاق الإصابة بهم أو الإضرار بالأعيان المدنية.

وقد نصت على هذا المبدأ المادة (٥٧) من البروتوكول الإضافي الأول لعام ١٩٧٧ الملحق باتفاقيات جنيف الأربع لعام ١٩٤٩، ويتضمن اتخاذ عددا من الإجراءات التي نصت عليها المادة (فقرة ٢ / أ و ب وج) وهي التحقق من أن الأهداف المراد مهاجمتها أهدافا عسكرية، واتخاذ جميع الاحتياطات الممكنة عند تخير وسائل وأساليب الهجوم، والامتناع عن اتخاذ القرار بشن أي هجوم لا يُراعي مبدأ التناسب، وإلغاء أو تعليق أي هجوم إن تبين أن الهدف المقصود ليس هدفًا عسكريا أو أنه مشمول بحماية خاصة أو أن الهجوم لا يراعي مبدأ التناسب، وتوجيه إنذار مسبق وبوسائل مجدية في حالة الهجمات التي تمس السكان المدنيين ما لم تحل الظروف دون ذلك.

كما يعتبر مبدأ الاحتياطات أثناء الهجوم قاعدة عرفية، ورد تفصيلها في دراسة القواعد العرفية التي أعدتها اللجنة الدولية للصليب الأحمر، وذلك في القواعد (١٥-٢١) : حيث نصت القاعدة (١٥) على أن: يتوخى الحرص الدائم في إدارة العمليات العسكرية على تفادي إصابة السكان المدنيين، والأشخاص

المدنيين، والأعيان المدنية، وتتخذ جميع الاحتياطات العملية لتجنب إيقاع خسائر في أرواح المدنيين، أو إصابتهم أو الإضرار بالأعيان المدنية بصورة عارضة، وتقليلها على أي حال إلى الحد الأدنى، كما تطبق هذه القاعدة العرفية في النزاعات المسلحة الدولية وغير الدولية على حد سواء.

ولم يرد تعريف المقصود بـ «الاحتياطات المستطاعة» في البروتوكول الإضافي الأول لعام ١٩٧٧ ، ولكن المادة (٣/١٠) من البروتوكول الثاني المعدل الملحق باتفاقية حظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر لعام ١٩٨٠، والمتعلق بحظر أو تقييد استعمال الألغام والأشراك الخداعية والنبائط الأخرى لعام ١٩٩٦ نصت على أن «الاحتياطات المستطاعة هي الاحتياطات العملية أو الممكن اتخاذها عمليا مع مراعاة جميع الظروف السائدة في ذلك الوقت، بما في ذلك الاعتبارات الإنسانية والعسكرية[١].

□

(١) Geneva Academy of International Humanitarian Law and Human Rights، op. cit.، p. ١٥.

المطلب الثاني

جهود المجتمع الدولي لمواجهة العمليات السيبرانية

تمهيد وتقسيم:

حظر ميثاق الأمم المتحدة في مادته الثانية في الفقرة الرابعة استخدام القوة في العلاقات الدولية أو التهديد بها، وأصبحت الحرب عملا غير مشروع في القانون الدولي المعاصر، ومع ذلك فإن الحرب ظاهرة موجودة - ولا يمكن إغفالها، ولهذا فإن المجتمع الدولي قام بوضع قواعد وضوابط لتقييم الحرب وسلوكيات المتحاربين، وذلك لغرض التخفيف من آثار الحرب، طالما أن المجتمع الدولي غير قادر على التخلص منها نهائياً.

وقد ارتكزت الجهود المبذولة من الدول والمنظمات الدولية على تطوير قواعد القانون الدولي، ومن الممكن أن تسهم في احتواء الهجمات السيبرانية وتضمينها من بين الأعمال العدائية التي تنطوي على استعمال القوة، ووضع معايير وتدابير لبناء الثقة للتطبيق على المستوى الدولي. وترتب على هذه الجهود ظهور ما يعرف بنظام الأمن السيبرانيCybersecurity Regime ، ويشمل كافة القواعد والمؤسسات والإجراءات الرسمية وغير الرسمية، والتي تعمل على تطوير القواعد الحاكمة للأنشطة السيبرانية، كما أنها تشمل المنظمات العالمية والإقليمية التي تلعب دوراً بارزاً في صياغة سياسات الأمن والدفاع السيبراني وحقوق الإنسان وحماية الملكية الفكرية.

وسوف أتطرق إلى جهود المجتمع الدولي في مواجهة العمليات السيبرانية من خلال تقسيم دراسة هذا المطلب إلي فرع أول حول: قرارات الأمم المتحدة، بينما يأتي الفرع الثاني حول: الإتحاد الدولي للاتصالات "I TU" ، ويأتي الفرع الثالث حول: عقد اتفاقية بودابست لمقاومة جرائم السيبرانية والاتصالات ٢٠٠١، ويأتي الفرع الرابع حول: مؤتمر الأمم المتحدة لمنع الجريمة والعدالة الجنائية، ويأتي الفرع الخامس حول: منظمة حلف شمال الأطلسي (الناتو) واخيرا الفرع السادس حول: جامعة الدول العربية، وذلك على النحو التالي:

الفرع الأول

قرارات الأمم المتحدة

ولقد أبدت الجمعية العامة للأمم المتحدة اهتماماً كبيراً بالعمليات السيبرانية، وبدأت المناقشات حول المسائل المتعلقة بأمن المعلومات عندما دعت روسيا في عام ١٩٩٨، الجمعية العامة للأمم المتحدة إلى إبرام اتفاقية دولية معنية بالهجمات السيبرانية، وهو ما دفع الجمعية العامة عام ٢٠٠٠ إلى إصدار قرار يدعو إلى دراسة التهديدات التي تصاحب استخدام المنظومات الإلكترونية لأغراض عسكرية(١).

ويعد من أبرز قرارات الجمعية العامة للأمم المتحدة التي تدعو فيها 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 العمليات السيبرانية علي البشرية، ومن تلك القرارات:

القرار رقم ٥٧ / ٢٣٩ الصادر عن الجمعية العامة للأمم المتحدة في ٢٠ كانون الأول / ديسمبر ٢٠٠٢، لإرساء مبادئ عالمية للأمن السيبراني، حيث اعتمدت فيه قراراً بشأن الأمن السيبراني والذي سلمت فيه بضرورة دعم الجهود الوطنية بتبادل المعلومات والتعاون في هذا المجال على الصعيد الوطني والإقليمي والدولي، كي يتسنى التصدي الفعال لما تتسم به هذه التهديدات السيبرانية، بصفة متزايدة من طابع عابر للحدود الوطنية، ويشهد هذا القرار على

---

(١) أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية – مفهومها والمسئولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر – مجلة المحقق الحلي للمعلومات القانونية والسياسية – جامعة بابل – كلية القانون – العدد الرابع – السنة الثامنة - ٢٠١٦ ، ص ٦٥٦

التزام العالم بإنشاء مبادئ عالمية للأمن السيبراني، ويتبلور فحوي القرار في التأكيد علي أن الأمن السيبراني للهياكل الأساسية الحيوية للمعلومات مسؤولية ملقاة على عاتق الحكومات ومجال يجب عليها أن تحمل فيه لواء الصدارة علي الصعيد الوطني.

القرار ٥٨ / ١٩٩ الصادر عن الجمعية العامة للأمم المتحدة في ٣٠ كانون الثاني / يناير ٢٠٠٤ ، بشأن إرساء ثقافة عالمية للأمن السيبراني وحماية البنية التحتية للمعلومات.

القرارين ٦٣/٥٥ و ٥٦ / ١٢١ الصادرين عن الجمعية العامة للأمم المتحدة، اللذين يضعان الإطار القانوني بشأن مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية.

القرار رقم ٤١/٦٥ والذي صادقت الجمعية العامة للأم المتحدة عليه في كانون الأول / يناير ٢٠١١ على تقرير فريق الخبراء الحكوميين في مجال المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، وتضمنت استنتاجات فريق الخبراء من بينها ما ذكرته من أن هناك دول تستحدث تكنولوجيا المعلومات والإتصال كوسائل للحرب والاستخبارات، وتلفت اللجنة الدولية في هذا الصدد انتباه الدول إلى عواقب العمليات 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 الحيوية والنووية، وتذكر اللجنة الدولية بالتزام كل الأطراف في النزاعات المسلحة باحترام قواعد القانون الدولي الإنساني إذا لجأت إلى وسائل وأساليب العمليات السيبرانية ومن هذه القواعد

مبادئ التمييز والتناسبية[١].

الفرع الثاني

الإتحاد الدولي للاتصالات: "I TU"

في سبيل الوصول إلي الحفاظ علي الأمن السيبراني باعتباره محورا جوهريا من محاور الأمن القومي للدول، أنشأ الإتحاد الدولي للاتصالات فريق متخصص معني بالبحث في الشبكات الذكية من منظور منظومة الاتصالات.

وكان من أهم أهداف الإتحاد الدولي للاتصالات عقب القمة العالمية لمجتمع المعلومات ومؤتمر المندوبين المفوضين لعام ٢٠٠٦ تحديد عوامل أمان أكثر فعالية في استعمال تكنولوجيا المعلومات والاتصالات، فقد قام المشاركين في القمة العالمية لمجتمع المعلومات، وكذلك الدول الأعضاء في الإتحاد، بتكليف الإتحاد باتخاذ خطوات ملموسة للحد من التهديدات وانعدام الأمن فيما يتصل بمجتمع المعلومات.

لذا أطلق الأمين العام للاتحاد " الدكتور حمدون !. توريه" برنامج الأمن السيبراني العالمي في غضون عام ٢٠٠٧ ليكون إطاراً للتعاون الدولي وكذلك برنامج الأمن السيبراني العالمي (GCA) لتوفير إطار يمكن من خلاله عمل تنسيق استجابة دولية للتحديات المتنامية التي يطرحها الأمن السيبراني، ويعتمد هذا البرنامج على التعاون الدولي بهدف توحيد الجهود الدولية لبناء الثقة والأمن في مجتمع المعلومات.

---

(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، الدورة٦٦ ، اللجنة الأولى، البندان ٨٧ و ١٠٦ من جدول الأعمال، بيان اللجنة الدولية للصليب الأحمر، نيويورك، ١١ تشرين الأول/ أكتوبر ٢٠١١.

وخلال مؤتمر المندوبين المفوضين لعام ٢٠١٠ ، أكدت الدول الأعضاء عمل الإتحاد على برنامج الأمن السيبراني العالمي باعتباره إطاراً للتعاون الدولي في القرار ١٣٠ الذي يكلف الأمين العام بمواصلة عرض التقدم المحرز في نطاق اختصاصه وتعزيزه وبالتحديد لاحظت الدول الأعضاء تعزيز دور الإتحاد في بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات إلى جانب المخاطر السيبرانية وسبل مواجهتها.

وقد أعدت لوائح الاتصالات الدولية كإطار تنظيمي لمعالجة القضايا الناشئة والتحديات التي تصاحب عالم الاتصالات الجديد، مرتكزة على تعزيز الكفاءة والتنمية الدوليين، وصون حق الدول في الاتصال.

ومن خلال مساعيه المسؤولة وإدراكا منه للخطر المتنامي للهجوم السيبراني اقترح الأمين العام للاتحاد الدولي للاتصالات، خمسة مبادئ توجيهية لإحلال السلام وحفظه في العالم السيبراني المعاصر وتنبثق هذه المبادئ عن تحقيق السلام السيبراني والالتزام بالقواعد الكفيلة بتحقيق الأمن في الفضاء السيبراني، وتتتمثل هذه المبادئ في ما يلي[١]:

- التزام الحكومات بإتاحة نفاذ شعبها إلى الاتصالات.
- التزام الحكومات بتأمين الحماية لشعبها في الفضاء السيبراني.
- التزام الحكومات بعدم إيواء الإرهابيين / المجرمين علي أراضيها.
- التزام كل دولة بألا تكون الطرف الذي يبدأ بشن هجوم سيبراني على غيرها من الدول.

---

(١) قرارات المؤتمر العالمي لتنمية الاتصالات لعام ٢٠١٧ (WTDC١٧) المرفوعة إلى عناية مؤتمر المندوبين المفوضين، مؤتمر المندوبين المفوضين (PP-١٨) دبي، ٢٩ أكتوبر – ١٦ نوفمبر ٢٠١٨ ، الإتحاد الدولي للاتصالات.

- التزام كل دولة بالتعاون مع غيرها من الدول ضمن إطار دولي لحفظ السلام في الفضاء السيبراني.

وفي عام ٢٠٠٨ وقع الإتحاد الدولي للإتصالات 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.

الفرع الثالث

عقد اتفاقية بودابست لمقاومة جرائم السيبرانية والإتصالات ٢٠٠١

إيمانا من الدول بمدى خطورة الجريمة السيبرانية بوصفها جريمة عابرة للحدود جاءت هذه الاتفاقية لتعالج إشكالية دولية الجريمة السيبرانية بما يساعد الدول على مكافحة هذه الجريمة وتعقب مرتكبيها والمساعدة على الاستدلال عليهم وضبطهم.

وقام بالتوقيع علي الاتفاقية ثلاثون دولة في العاصمة المجرية "بودابست" من بينها دول أعضاء من الإتحاد الأوروبي، إضافة إلى كندا اليابان، جنوب إفريقيا، أمريكا، وتعد اتفاقية بودابست محاولة جادة من المشرع الدولي لتحديد القانون واجب التطبيق على العمليات السيبرانية، ووضع قواعد قانونية حاكمة لهذا النوع من الحروب، فقد ورد في ديباجة الاتفاقية أن إبرامها جاء نتيجة للتغيرات الناجمة عن التكنولوجيا السيبرانية، وعولمة الشبكات الرقمية، حيث أدرك المشرع الدولي وأشخاص المجتمع الدولي ما قد ينجم من مخاطر عن استخدام هذه التكنولوجيا في ارتكاب أفعال تعد من قبيل الجريمة، حيث حاولت إيجاد نظام فعال للتعاون الدولي في مجال مكافحة الهجمات السيبرانية، إذ حاولت الدول الأطراف في الاتفاقية الوصول لصيغة تشريعية عامة لمكافحة الهجمات السيبرانية، والحد من آثارها[١] .

---

(١) الاتفاقية المتعلقة بالجريمة الإلكترونية، اعتمدت في ٨ نوفمبر ٢٠٠١، وفتح باب التوقيع عليها في ٢٣ نوفمبر ٢٠٠١ ، ودخلت حيز النفاذ في ١ يوليو ٢٠٠٤ للاطلاع على النص الكامل للاتفاقية راجع الموقع الرسمي لمجلس أوروبا، مجموعة المعاهدات الأوروبية

https://rm.coe.int/budapest-convention-in-arabic/١٦٨٠٧٣٩١٧٣

وتتضمن الاتفاقية التعاون والعمل المشترك ما بين الدول الأعضاء لمواجهة الهجمات السيبرانية، وقد دخلت الاتفاقية حيز التنفيذ عام ٢٠٠٤وتم الاتفاق من خلال الاتفاقية علي الالتزام بما يلي[١]:

أولا: مواصلة اعتبار الأمن السيبراني ضمن أولويات أنشطة الإتحاد.

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

ثالثا: تعيين نظام سريع وفعال للتعاون الدولي للحفاظ بشكل سريع على البيانات المخزنة على أجهزة الكمبيوتر وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة على الكمبيوتر.

ويعيب الأستاذ حسين إبراهيم حسن طه على هذه الاتفاقية عدم التفاتها إلى الهجمات السيبرانية التي تقوم بها الدول في إطار رسمي، حيث اقتصرت نصوصها علي الهجوم السيبراني الذي يشنه الأشخاص ضد بعضهم، بمعنى أن اهتمامها قد انصب على الطابع التجريمي للهجمات السيبرانية، وهو ما يتبين من عنوانها، وذلك برغم واقعية وجود العمليات السيبرانية، وسبق وقوع مثل هذه الحرب قبل توقيع الاتفاقية في حرب البلقان التي دارت على أرض يوغسلافيا السابقة، حيث استخدمت قوات حلف شمال الأطلسي العمليات السيبرانية صوب الأهداف الإلكترونية الصربية، مما يعني أن العمليات السيبرانية كانت واقعا موجودا قبل دخول الاتفاقية حيز النفاذ، وكان ذلك يوجب على المشرع

---

(١) د/ هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، دار النهضة العربية، ط ٢ ، ٢٠١١، ص ١٣٠.

الدولي أن يلتفت الى هذا النوع من الحروب من خلال هذه الاتفاقية[١].

وعلي الرغم من هذا النقد الموجه لاتفاقية بودابست إلا أن الاتفاقية الأوربية لمكافحة الجرائم السيبرانية "بودابست"، خطوة مهمة على مستوي التعاون بين الدول لوضع إطار عالمي للتعاون الدولي في مواجهة تلك الجرائم المرتبطة بالفضاء السيبراني وبرهنت علي تحقيق ذلك من خلال إعطاء حق الانضمام للاتفاقية لأي دولة دون الاقتصار على الدول الأوربية فقط.

□

(١) حسين ابراهيم حسن طه ، الحرب السيبرانية في ضوء قواعد القانون الدولي ، مرجع سابق ص ٢١٨

الفرع الرابع

مؤتمر الأمم المتحدة لمنع الجريمة والعدالة الجنائية

في دورتها الثانية عشرة في غضون شهر أبريل لعام ٢٠١٠ صاغت لجنة الأمم المتحدة لمنع الجريمة والعدالة الجنائية مجموعة من الإعلانات التي تشمل حكماً يدعو إلى إنشاء فريق خبراء حكومي دولي لبحث مشكلة الجريمة السيبرانية والاستجابات الدولية لها، وعملا بذلك، 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، وعلى الرغم من أن المؤتمر لم يتوصل إلى توافق الآراء بشأن إعداد معاهدة جديدة للجريمة السيبرانية، إلي أنه اعتبر طريقا ممهدا لإبرام اتفاقات بشأن المساعدة التقنية وبناء القدرات التي تشكل أساساً جيداً لحل الصعوبات[١].

---

(١) Draft Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World.

الفرع الخامس

منظمة حلف شمال الأطلسي (الناتو)

إقليميا اعتمد الناتو سياسته الخاصة في مجال الدفاع السيبراني في غضون عام ٢٠٠٨ من أجل حفظ وصون موارده التكنولوجية وتلك الخاصة بالدول الأعضاء(١).

كما أنشأ فريقاً للاستجابة للحوادث الحاسوبية يكفل إرسال فرق الدعم السريع إلى البلدان الأعضاء، ومركزاً للتميز من أجل الدفاع السيبراني التعاوني مقره في إستونيا ويضم خبراء يضطلعون بالبحث والتدريب في مجال الأمن السيبراني، وتضم البلدان التي ترعى هذا المركز "إستونيا ولاتفيا وليتوانيا وألمانيا وإيطاليا والجمهورية السلوفاكية وإسبانيا"، كما أعد الناتو تمارين في مجال الدفاع السيبراني حيث تقوم فرق من الدول الأعضاء بمحاولة الدفاع عن الشبكات الحاسوبية الافتراضية من الهجوم السيبراني، وتهدف هذه التمارين إلي زيادة فهم البيئة السيبرانية الدولية وتعزيز التعاون الدولي لمعالجة الحوادث التقنية، وأيضا وقع الناتو مذكرة تفاهم بشأن الأمن السيبراني مع إستونيا والولايات المتحدة والمملكة المتحدة وتركيا وسلوفاكيا.

ونتيجة لفشل حلف الناتو في مواجهة الهجمات السيبرانية على استونيا عام ٢٠٠٧ وجورجيا عام ٢٠٠٨ أنشأ الحلف وحدة للدفاع السيبراني مقرها تالين عاصمة استونيا وأصبح الفضاء السيبراني منطقة لعمليات الحلف وأن عليه أن يطور قدراته الدفاعية السيبرانية بما يشمل مساندة ودعم حلفائه الذين يتعرضون لهجمات سيبرانية وأنه حال تعرض أوروبا أو أمريكا الشمالية لهجوم سيبراني

---

(١) الدفاع ضد الهجمات السيبرانية – الناتو: https://www.nato.int/cps/en/natohq/

يعتبر هجوما ضد الجميع يلزم تكاتف الجهود لصده[١].

الفرع السادس

جامعة الدول العربية

على الصعيد العربي فقد بذلت جهود كبيرة في مكافحة الجرائم السيبرانية تبلورت في وضع اتفاقية عربية لمكافحة جرائم تقنية المعلومات، والتي انبثقت عن الاجتماع المشترك لمجلس وزراء الداخلية والعدل العرب الذي عقد بمقر الأمانة العامة لجامعة الدول العربية في عام ٢٠١٠ بهدف تعزيز التعاون بين الدول العربية في مكافحة جرائم تقنية المعلومات، والجرائم السيبرانية التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، وضرورة وضع سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات[٢].

كما سعت الدول العربية جاهدة لتقنين وتجريم الأعمال الغير مشروعة المرتكبة عبر الفضاء السيبراني بالتوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بتاريخ ٢١ / ١٢ / ٢٠١٠ لتعزيز التعاون بين الدول العربية لمكافحة الجرائم السيبرانية والحفاظ على أمنها وسلامة مجتمعاتها[٣].

---

(١) 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 الراهنة.

(٢) طلال ياسين العيسى عدي محمد عناب المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر" مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد ١٩ العدد الأول ٢٠١٩، ص ٨٥ .

(٣) 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 .

=

وألزم المجلس، الدول المصدقة على الاتفاقية موافاة الأمانة الفنية للمجلس بما اتخذته من إجراءات لموائمة تشريعاتها مع أحكام الاتفاقية.

وأكد المجلس، على أهمية تعزيز التعاون مع المنظمات والوكالات الدولية المتخصصة للحصول على المساعدات المطلوبة في بناء القدرات اللازمة لمواجهة خطر استخدام الإرهابيين لأسلحة الدمار الشامل أو مكوناتها ودعم أمن المطارات والموانئ والحدود.[1]

□

terms/٤٧٨٠

(١) د أميرة عبد العظيم محمد – المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام . مرجع سابق ص ١٣٨

المطلب الثاني

أحكام دليل تالين بشأن الحروب السيبرانية

وقد قامت جهود دولية من أجل تنظيم العمليات السيبرانية بإصدار دليل "تالين" حول القانون الدولي الذي يطبق على هذه الحرب في عام ٢٠١٢ وهو من إعداد اللجنة الدولية للخبراء بدعوة من مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي، ويقسم هذا الدليل إلى قسمين:

القسم الأول: يختص بمعالجة قانون الأمن الإلكتروني، والقسم الثاني: قانون النزاعات الإلكترونية، ويوضح دليل تالين بأن العمليات الإلكترونية قد تشكل نزاعات مسلحة، لا سيما الآثار المدمرة لتلك العمليات، والمبادرة الأكثر نجاحاً التي تضمنها هي إشارته إلى أن القانون الدولي الإنساني ينطبق على الحرب الإلكترونية، مع تحديدها للدور الذي ستلعبه قواعد القانون الدولي الإنساني.

ويعد دليل تالين هو الوثيقة الدولية الوحيدة التي تناولت العمليات السيبرانية بين الدول، وذلك من خلال خمس وتسعين قاعدة تأسست جميعها على قواعد القانون الدولي، والقانون الدولي الإنساني وقد أسس هذا الدليل عدد من المبادئ أهمها إمكانية النظر للعمليات السيبرانية على أنها نزاع مسلح، حتى لو لم تتوازي مع نزاع مسلح فعلي، بحيث يمكن الاعتداد بالعمليات السيبرانية إذا كانت قد تم شنها على سبيل الاستقلال، كما يتصور أن تكون العمليات السيبرانية دولية أو غير دولية.

كما تناول دليل تالين مبدأ الضرورة العسكرية، حيث أنه في الحالات التي يكون هناك عدة أهداف عسكرية لكي يكون هناك خيار، فالهدف الذي يقع عليه الخيار للهجوم السيبراني هو الذي يتوقع منه أن يلحق خطر أقل على المدنيين والأعيان المدنية، على أن مراعاة تطبيق مبدأ الضرورة العسكرية لابد أن يكون الذي يسبب أضرار وإصابات أقل، أما في حالة وجود أهداف عديدة وأن أحدها سوف يحقق ميزة عسكرية أكثر من غيرها هنا من حق المهاجم توجيه الهجمات

السيبرانية ضد الهدف العسكري الذي يحقق ميزة أكثر في النزاع المسلح، ومن هنا لابد من النظر إلى الضرر الذي يصيب البنية التحتية والمنشئات الحيوية بالنسبة للمدنيين بالإضافة إلى حرمانهم من الوظائف وخدمات هذه المنشئات.

ويعتبر دليل تالين نتاج مجهود فئة لا يستهان بها من فقهاء القانون الدولي والممارسين له عالجوا مسألة العمليات السيبرانية وغيرها من التحديات المتعلقة بالقانون الدولي الإنساني خلال مشروع دام مدة ثلاث سنوات ممول من قبل حلف الناتو، نجم عنه هذا الدليل للقانون الدولي المطبق في العمليات السيبرانية **Tallinn Manuel** مكون من ٢٩٢ صفحة، وقد بين الدليل بشكل واضح القوانين المنظمة لقواعد الاشتباك عن طريق الانترنت، إذ اتفقوا على أنه متى أحدثت العمليات السيبرانية **Cyber Operations** من قبل دولة ما، دمارا أو أذى، لدولة أخرى فإن ثمة نزاع مسلح دولي، بل إن البعض من هؤلاء الفقهاء والممارسين يرى بأن حدوث أي ضرر ولو بالدرجة الأدنى للضرر يمكن أن يشكل نزاعا مسلحا.

□

الخاتمة والتوصيات

تعد العمليات السيبرانية من أكبر التحديات التي يواجهها القانون الدولي الإنساني، إذ تشكل تهديدًا غير مسبوق للبنى التحتية الحيوية وللأمن القومي للدول، وفي ضوء التحولات التكنولوجية المتسارعة، أصبح من الضروري تحديث القواعد القانونية التقليدية لتتناسب مع طبيعة العمليات السيبرانية، كما تميزت العمليات السيبرانية بقدرتها على إلحاق أضرار جسيمة بتكلفة منخفضة ومن دون الحاجة إلى تدخل عسكري تقليدي، ما يجعلها وسيلة فعالة لتحقيق أهداف عسكرية أو سياسية بوسائل غير ملموسة يصعب ردعها.

توصي الدراسة بعدة إجراءات ضرورية للتعامل مع هذا النوع من النزاعات على النحو التالي:

أولاً: تحديث التشريعات الدولية الخاصة بالقانون الدولي الإنساني لتشمل نصوصًا صريحة تتعلق بالعمليات السيبرانية، خاصة في ما يتعلق بتحديد مسؤولية الفاعلين في الهجمات السيبرانية سواء أكانوا دولًا أم أفرادًا، كما ينبغي اعتبار كل شخص يقوم بهجوم سيبراني نيابة عن دولته مشاركًا فعليًا في النزاع، مما يسقط عنه الحماية المدنية في إطار القانون الدولي.

ثانيا: مراجعة الدول لتشريعاتها الداخلية بما يتوافق مع التشريعات الدولية والأممية الجديدة بشأن الالتزام بالقواعد المنظمة للفضاء السيبراني.

ثالثا: يجب أن تتضمن نصوص القانون الدولي الالتزام باحترام وضع الحياد من قبل الأطراف المتحاربة سيبرانيا، إذ لا بد من النص الصريح على حظر استخدام الفضاء السيبراني لأي دولة محايدة دون علمها في شن هجمات سيبرانية.

رابعا: ضرورة التزام كافة الدول بالتعاون في مجال أمن الفضاء السيبراني، لضمان عدم استخدام هذا الفضاء في العدوان المتبادل بين الدول، كما يضمن عدم استخدام الفضاء في شن الهجمات السيبرانية.

خامسا: يجب على الدول الالتزام باستخدام الهجمات السيبرانية على سبيل الدفاع فقط، بحيث تكون الدولة غير بادئة بالعدوان، وذلك نظرا لاتساع مدى هذه الهجمات، وفداحة الآثار المترتبة عليها للعسكريين والمدنيين.

سادسا: تعزيز التعاون الدولي بين الدول والمنظمات الأممية لتبادل الخبرات والمعلومات حول أحدث أساليب الدفاع السيبراني، ووضع إطار قانوني موحد لمنع إساءة استخدام التكنولوجيا في شن الهجمات السيبرانية. وقد يساهم هذا التعاون في رصد وتتبع الهجمات وتحديد الجهة المسؤولة عنها بشكل أدق.

ختاما: تعزيز الوعي العام والتدريب على مبادئ الأمن السيبراني لكل من المدنيين والقادة العسكريين، لضمان استعدادهم في حال تعرض البنية التحتية لهجمات سيبرانية مفاجئة.

□

النتائـــــج

توصلت من خلال هذه الدراسة إلى مجموعة من الاستنتاجات أهمها :

١-تختلف العمليات السيبرانية عن الحرب التقليدية، وتتسم بعدد من الخصائص التي تميزها، وهي خصائص نابعة من طبيعتها المتطورة غير التقليدية، كما تنبع من آثارها وطريقة القيام بها، والتي تختلف كليا عن الحروب التقليدية.

٢-برغم حداثة العمليات السيبرانية إلا إنها استطاعت أن تفرض نفسها على ساحات النزاعات الدولية، وهو الأمر الذي نتج عن مدى تنوعها وسرعة تطورها، وشدة تأثيرها، وقلة تكاليفها وعدم احتياجها لجهود أو معدات كبيرة، إذ يمكن شنها بأبسط الإمكانات وعن طريق عدد محدود من الأفراد مقارنة بالحرب التقليدية.

٣- تسعى أغلب الدول اليوم لتطوير إمكانياتها السيبرانية، ودعم قوتها العسكرية بالكفاءات والأدوات التي تمكنها من شن هذا النوع من الهجمات، حيث باتت القوة المعاصرة للدول قوة سيبرانية أكثر من كونها قوة عسكرية تقليدية.

٤-الحروب الحديثة في القرن الحادي والعشرين أصبحت تتم عبر الفضاء السيبراني للدول.

٥- الهجمات السيبرانية أصبحت تستهدف البنى التحتية الحيوية للدول وتهدد مواردها الأساسية، فلم تعد تقتصر على الجوانب العسكرية فحسب بل تطال أيضا البني الحيوية للدولة كالقطاعات المالية والمصرفية وقطاع تكنولوجيا المعلومات والنقل والطيران والكهرباء والطاقة وتعرضها لأضرار يصعب معالجتها.

٦-الدولة لسيت الطرف والفاعل الوحيد في القيام بهجمات سيبرانية، فهناك أطراف أخري غير الدول لديها إمكانية شن الهجمات السيبرانية.

٧- أصبح الفضاء السيبراني مقوما هاما من مقومات الأمن القومي للدول وحمايته وتحصينه من التعرض لاختراقات سيبرانية يعد مؤشرا فاعلا للتعبير عن صلابة الدولة وقوتها.

شكر وعرفان:

يتقدم المؤلفون بخالص الشكر لجامعة الأمير سطام بن عبد العزيز على تمويل هذا العمل البحثي من خلال المشروع رقم (PSAU/٢٠٢٤/٠٢/٣٠٦٦٢).

Acknowledgment

"The authors extend their appreciation to Prince Sattam bin Abdulaziz University for funding this research work through the project number (PSAU/٢٠٢٤/ ٠٢/٣٠٦٦٢)

المصادر والمراجع

أولا: المراجع العربية

المراجع القانونية:

احمد عبيس نعمة الفتلاوي الهجمات السيبرانية – مفهومها والمسئولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر – مجلة المحقق الحلي للمعلومات القانونية والسياسية – جامعة بابل – كلية القانون – العدد الرابع – السنة الثامنة – ٢٠١٦.

إسلام رمضان هديب، الحرب السيبرانية في ضوء القانون الدولي مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة بني سويف، ٢٠٢٤ .

١. أميرة عبد العظيم محمد – المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام ، مجلة الشريعة والقانون • العدد الخامس والثلاثون الجزء الثالث (١٤٤٢ هـ - ٢٠٢٠م .(
٢. إيهاب خليفة – كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت – دار العربي للنشر والتوزيع – القاهرة، ٢٠١٧.
٣. بقرين عبد الصمد صالح حماية المرأة أثناء النزاعات المسلحة في ضوء أحكام القانون الدولي العام، دار الفكر الجامعي، الإسكندرية، ٢٠١٧.
٤. تمارا برو، استخدام الأسلحة غير التقليدية في القانون الدولي العام، دار المنهل اللبناني للطباعة والنشر، بيروت، ٢٠١٠.
٥. توران جيزلو تيلمانرو دنها و سروكنو تدورمان القانون الدولي الإنساني وحماية المدنيين من اثار العمليات السيبرانية أثناء النزاعات المسلحة – المجلة الدولية للصليب الأحمر ، مجلد ١٠٢ (٩١٣) .٢٠٢٠.
٦. جمال بوازدية، الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية - التحديات والآفاق المستقبلية. مجلة العلوم القانونية والسياسية، جامعة الوادي الجزائر، المجلد ١٠ العدد ١ أفريل / أبريل ٢٠١٩.
٧. جون ماري هنكرتس ولويز دوز والد - بك القانون الدولي الإنساني العرفي: المجلد الأول: القواعد اللجنة الدولية للصليب الأحمر، القاهرة، ٢٠٠٧.
٨. الجيلالي دلالي و بلبشير يعقوب (٢٠٢١). رهانات الأمن السيبراني الوطني في ظل التحول الرقمي : قراءة في التأصيل المعرفي واستراتيجية المواجهة التشريعية . مجلة كلية القانون الكويتية العالمية مج ١٠،٣٧.

٩. حسين إبراهيم حسن طه ، الحرب السيبرانية في ضوء قواعد القانون الدولي، بحث منشور بمجلة كلية الحقوق – جامعة المنوفية.
١٠. حكيم غريب ، صبرينة شرقي تداعيات الحرب الإلكترونية علي العلاقات الدولية "دراسة في الهجوم الإلكتروني علي إيران" فيروس ستكنست ، دفاتر السياسة والقانون المجلد ١٢ عدد ٢ – ٢٠٢١م. ٠١٠٠٠٢٣١٥٣٠
١١. حيدر كاظم عبد علي، القواعد المتعلقة بوسائل وأساليب القتال أثناء النزاعات المسلحة غير الدولية ، مجلة المحقق الحلي للعلوم القانونية والسياسية ، العدد الثاني ، السنة الرابعة.
١٢. خليفة إيهاب – القوة الإلكترونية وأبعاد التحول في خصائص القوة – مكتبة الاسكندرية – مصر ٢٠١٤م.
١٣. رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة، المجلد ١٥، العدد (٢) ديسمبر ٢٠١٨.
١٤. رعد فجر الراوي: القصور التشريعي في مواجهة الهجمات السيربانية، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد١٠، العدد ٣٩، ٢٠٢١.
١٥. سامي محمد عبد العال، الدفاع الشرعي ضد الهجمات السيبرانية، المجلة المصرية للقانون الدولي - المجلد ٧٩ لسنة ٢٠٢٣م.
١٦. ستار عبد عودة الفهداوي، حماية المدنيين وقت الحرب في الشريعة الاسلامية والقانون الدولي العام، مركز البحوث والدراسات الإسلامية، عمان ٢٠١٧.
١٧. سعيد درويش – الحروب السيبرانية وأثرها علي حقوق الإنسان دراسة في ضوء أحكام دليل "تالين" – المجلة الجزائرية للعلوم القانونية والإقتصادية والسياسية – مجلد ٥٤ عدد ٥ – ٢٠١٧م.
١٨. سيف غانم السويدي، النطاق المادي للقانون الدولي الانساني"، مجلة جنوب الوادي للدراسات القانونية، العدد الثالث، ٢٠١٨.
١٩. شريف عبد الحميد حسن رمضان الحرب السيبرانية ومدى ملائمتها مع القانون الدولي الإنساني – مجلة كلية الشريعة والقانون بتفهنا الأشراف – دقهلية – العدد الثالث والعشرون لسنة ٢٠٢١ م الجزء الرابع.
٢٠. طلال ياسين العيسى عدي محمد عناب المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر" مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد ١٩ العدد الأول ٢٠١٩ .

٢١. عادل عبد الصادق ، أسلحة الفضاء الألكتروني في القانون الدولي الإنساني ، مكتبة الإسكندرية ، وحدة الدراسات المستقبلية ، ٢٠١٦.
٢٢. عادل عبد الصادق محمد الجخة، أثر الإرهاب الالكتروني على مبدأ استخدام القوة في العلاقات الدولية – رسالة ماجستير – كلية الإقتصاد والعلوم السياسية – جامعة القاهرة ٢٠٠٩.
٢٣. عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، وحدة الدراسات المستقبلية، قوانين وتشريعات، إصدارات مكتبة الإسكندرية، العدد ٢٣.
٢٤. عباس بدران الحرب السيبرانية، الاشتباك في عالم المعلومات، مركز دراسات الحكومة السيبرانية، بيروت، ٢٠١٠.
٢٥. عبد العزيز بن فهد بن محمد بن داود الجرائم السيبرانية : دراسة تأصيلية مقارنة مجلة الاجتهاد للدراسات القانونية والاقتصادية، جامعة تمنراست، الجزائر، المجلد ٩ ، العدد ٣، سنة ٢٠٢٠.
٢٦. عبد القادر دندن، العلاقات الدولية في عصر التكنولوجيا الرقمية، مركز الكتاب الاكاديمي، عمان ٢٠٢١.
٢٧. عصام عبد الفتاح مطر، القانون الدولي الإنساني مصادره، مبادئه أهم قواعده، دار الجامعة الجديدة، الإسكندرية، بدون طبعة ٢٠١١.
٢٨. علي حسين باكير – الحروب الإلكترونية في القرن الواحد والعشرين – مركز الجزيرة للدراسات – قطر، ٢٠١٠م.
٢٩. عمر سعد الله تطوير و تدوين القانون الدولي الإنساني، دار الغرب الإسلامي، لبنان ، ١٩٩٧.
٣٠. عمر محمود أعمر الحرب الإلكترونية في القانون الدولي الإنساني دراسات علوم الشريعة والقانون، المجلد ٤٦ عدد ٣ – ٢٠١٩ .
٣١. لفقير بولنوار بن الصديق، جرائم الحرب في ضوء أحكام القانون الدولي، دار الأيام للنشر والتوزيع، عمان٢٠١٧.
٣٢. مايكل شميت ، الحرب بواسطة شبكات الاتصال ، الهجوم على شبكات الكومبيوتر والقانون في الحرب ، المجلة الدولية للصليب الأحمر ٢٠٠٢.
٣٣. مايكل من سميت ، " الحرب بواسطة شبكات الاتصال : الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب المجلة الدولية. للصليب الأحمر مختارات من أعداد ٢٠٠٢.

٣٤. مايكل ن شميث – الحرب بواسطة شبكات الإتصال : الهجوم علي شبكات الكمبيوتر "الحاسوب" والقانون في الحرب – المجلة الدولية للصليب الأحمر – ٢٠٠٢.

٣٥. محمد المجذوب القانون الدول الإنساني وشرعية المقاومة ضد الاحتلال، القانون الدولي الإنساني- المؤتمر العلمي السنوي الكلية الحقوق، جامعة بيروت العربية، بيروت منشورات الحلبي الحقوقية، ٢٠١٠.

٣٦. محمد فهاد الشلالدة ، القانون الدولي الإنساني ، منشاة المعارف ، الإسكندرية ، ٢٠٠٥.

٣٧. محمود حجازي محمود ، العنف الجنسي ضد المرأة في أوقات النزاعات المسلحة ، دار النهضة العربية – القاهرة ٢٠٠٧.

٣٨. محمود محارب إسرائيل والحرب الإلكترونية - قراءة في كتاب حرب في الفضاء الإلكتروني اتجاهات وتأثيرات على إسرائيل، المركز العربي للأبحاث ودراسة السياسات، بيروت ٢٠١١.

٣٩. مزيان جعفر ، مبدأ التناسب والأضرار الجوارية في النزاعات المسلحة ، رسالة ماجستير، كلية الحقوق ، جامعة يتزى ، وزد ، ٢٠١١.

٤٠. مصطفى نعوس، حقوق والتزامات الدول في الحرب المعلوماتية، بحث منشور في مجلة دراسات علوم الشريعة والقانون، مجلد ٤٠ ملحق ، الجامعة الأردنية عمان ٢٠١٣.

٤١. مصطفي نعوس – حق الدولة في استخدام القوة في الفضاء الإلكتروني للدفاع عن النفس – مجلة الحقوق – العدد الأول – جامعة الكويت ٢٠١٤.

٤٢. موسى بن تغري الحرب السيبرانية والقانون الدولي الانساني، بحث منشور في مجلة الاجتهاد القضائي مجلد ١٢ عدد خاص جامعة محمد خيضر بسكرة الجزائر ٢٠٢٠.

٤٣. نبيل إدريس الجريمة السيبرانية بين المفاهيم والنصوص التشريعية - الجزائر أنموذجا مجلة القانون والمجتمع، جامعة أحمد دراية أدرار الجزائر، المجلد ٥ العدد ٢ سنة ٢٠٠٧.

٤٤. نوال أحمد بسج، القانون الدولي الإنساني وحماية المدنيين والأعيان المدينة في زمن النزاعات المسلحة، منشورات الحلبي الحقوقية، بيروت، لبنان سنة ٢٠١٠.

٤٥. هاشمي عفاف، فنيدس عبير حماية الفرق الطبية خلال النزاعات المسلحة مذكرة مكملة لمتطلبات نيل شهادة الماستر في القانون ، كلية الحقوق والعلوم السياسية ، جامعة ٠٨ ماي ١٩٤٥ قالمة.

٤٦. هاني محمد خليل العزازي : النظام القانوني الدولي لمكافحة المخاطر السيبرانية، مجلة مصر المعاصرة، عدد (٥٤٩) ، يناير ٢٠٢٣.

٤٧. هربرت لين: النزاع السبراني والقانون الدولي الإنساني، المجلة الدولية للصليب الأحمر، مجلد٩٤، ٢٠١٢.
٤٨. هشام بشير وإبراهيم عبد ربة إبراهيم، المدخل لدراسة القانون الدولي الإنساني، ط١، القاهرة: المركز القومي للإصدارات القانونية، ٢٠١٢.
٤٩. هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، دار النهضة العربية، ط ٢ ، ٢٠١١.
٥٠. يوسف بوغرارة، الأمن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري مجلة الدراسات الإفريقية وحوض النيل المركز الديمقراطي العربي، برلين ألمانيا، المجلد ١، العدد ٣.

القوانين والمواثيق الدولية:

١. وثيقة الأمم المتحدة ٦٨/٩٨ A ٢٤/حزيران – يونيو ٢٠١٣.
٢. اللجنة الدولية للصليب الأحمر، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية، أسئلة وإجابات ٢٠١٣.
٣. البروتوكول الإضافي الأول من اتفاقيات جنيف لعام ١٩٧٧.
٤. اتفاقيات جنيف الأربع لعام ١٩٤٩ الأولى في المادة ٦٣ ، والثانية في المادة ٦٢ ، والثالثة في المادة ١٤٢ ، والرابعة في ١٥٢ ، كذلك البروتوكول الإضافي الأول ١٩٧٧ المادة الأولى فقرة ٢ ، والبروتوكول الإضافي الثاني ١٩٧٧ في ديباجته .
٥. 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 الراهنة.
٦. 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/٤٧٨٠
٧. 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، الدورة٦٦ ، اللجنة الأولى، البندان ٨٧ و ١٠٦ من جدول الأعمال، بيان اللجنة الدولية للصليب الأحمر، نيويورك، ١١ تشرين الأول/ أكتوبر ٢٠١١.

٨. 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.

٩. قرارات المؤتمر العالمي لتنمية الاتصالات لعام ٢٠١٧ (١٧ WTDC) المرفوعة إلى عناية مؤتمر المندوبين المفوضين، مؤتمر المندوبين المفوضين (١٨ PP-دبي، ٢٩ أكتوبر – ١٦ نوفمبر ٢٠١٨ ، الإتحاد الدولي للإتصالات.

١٠. الإتفاقية المتعلقة بالجريمة الإلكترونية، اعتمدت في ٨ نوفمبر ٢٠٠١، وفتح باب التوقيع عليها في ٢٣ نوفمبر ٢٠٠١ ، ودخلت حيز النفاذ في ١ يوليو ٢٠٠٤ للاطلاع على النص الكامل للاتفاقية راجع الموقع الرسمي لمجلس أوروبا، مجموعة المعاهدات الأوروبية

١١. القانون رقم ٠٤-١٥ المؤرخ في ١٠ نوفمبر ٢٠٠٤ المعدل والمتمم للأمر رقم ٦٦-١٥٦ المؤرخ في ٨ يونيو ١٩٦٦، المتضمن قانون العقوبات الجريدة الرسمية، الجزائر، العدد ٧١ ، بتاريخ ١٠ نوفمبر ٢٠٠٤ ، والقانون رقم ٠٩-٠٤ المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المؤرخ في ٥ أوت أغسطس ٢٠٠٩ الجريدة الرسمية، الجزائر، العدد ٤٧، بتاريخ ١٦ أوت أغسطس ٢٠٠٩ (٣٢) .

١٢. القانون رقم ١٤ لسنة ٢٠١٤، الصادر بتاريخ ١٥/٠٩/٢٠١٤.

المواقع الإلكترونية:

https://www.icrc.org/ar/doc/resources/documents/faq/١٣٠٦٢٨-cyber-warfare-q-and-a-eng.htm

https://rm.coe.int/budapest-convention-in-arabic/١٦٨٠٧٣٩١٧٣

https://www.icrc.org/ar/doc/resources/documents/misc/٦٢sd٤j.htm

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

ثانيا: المراجع الأجنبية

١. "Cyber-Attacks and the Use of Matthew C. Waxman The Yale Journal Force: Back to the Future of Article ٢ (٤) "P٤٢٣ ٢٠١١ Vol. ٣٦ of International Law.

٢. (ICJ، Case Concerning Gabcikovo Nagymaros Project (Hungay

٣. (ICJ، Case Concerning Military and Poramilitary Activities in and Against Nicaragua (Nicaragua V. United States)، Reports، ١٩٨٦.

٤. Ahmed Abou-el- Wafa، current value of customory international humanitarianlaw، revue egyptienne de droit international، vol ٦٣، ٢٠٠٧.

٥. Antonio Gessese "The Maetens Clouse: Haif a loaf or simily Pie in the sky?" EJIL VOL ١١١ No.١,٢٠٠٠.

٦. Cameron S. D. Brown، «Investigating and Prosecuting Cyber Crime: Forensic Depende cies and Barriers to Justice»، International Journal of Cyber Criminology، Vol ٩، Issue ١، January June ٢٠١٥.

٧. Computer Network Operations Under International Law، Intersentia، ٢٠١٤.

٨. Cyber Operations and the Jus in Bello: Key Issues، Naval War College International Law Studies، ٢٠١١، v. ٨٧.

٩. Extending the Law of War to Cyberspace، (Sept. ٢٢، ٢٠١٠).

١٠. Gary Brown، Colonel، Keira Poellet، Major: The Customary International Law of Cyberspace، Strategic Studies Quarterly، ٢٠١٢.

١١. International Law، Oxford Monographs in International Law، ١٩٨٨.

١٢. Johann-Christoph Woltag: Cyber Warfare: Military Cross-border

١٣. Judgment of the international court of justice in Military and Paramilitary Activities in and against Nicaragua (Nicaragua V. United States)، ١٩٨٦، ١.C.J. ١٤، ٩٦-٩٧

١٤. Kenneth Anderson and Mathew C. Waxman، Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can ،American University Washington College of Law، Research Paper No. ٢٠١٣.

١٥. Marcelo Mendonça Teixeira، Cyberculture: From Plato to The Virtual Universe، Munich، GRIN Verlag، ٢٠١٢، https://www.grin.com/document/٢٠٠٨٣٢.

١٦. Marco Roscini:" World Wide Warfare Jus ad bellum and the use of Cyber Force"، MPYUNL، vol. ١٤،٢٠١٠.

١٧. Martin C. Libicki: Conquest in Cyberspace: National Security and Information Warfare، New York: Cambridge University Press، ٢٠٠٧.

١٨. Micheal Newton & Larry May; Proportionality in International Law، Oxford University Press، ٢٠١٤: Arbitral Award in the Naulilaa Case ١٩٢٨، ٢ Reports of the International Arbitral Awards ١٠١١-١٠٢٨.

١٩. Richard A. Kemmerer، Cyber security، University of California Santa Barbara، Department of Computer Science، ٢٠٠٣.

٢٠. Schmitt، M.N." Computer Network Attack and the Use of Force in International Law through on a Normative"، CJTL، ١٩٩٩، v.٢٧، n.٨٨٥.

٢١. The International Télécommunication Union، ITU Toolkit for CybercrimeLégislation،

٢٢. william H. Boothby: weapons and the law of armed conflict، no. ٤، ٢٠٠٩.