العدد 4 No 4
تموز 2026 July 2026
مجلة ساوة للدراسات الانسانية
Sawah Journal of Humanities
E-ISSN 3106 - 8324 P-ISSN 3106 - 8316
مجلة محكمة تصدر عن
جامعة ساوة الاهلية

تحديات قواعد القانون الدولي في مواجهة الحرب السيبرانية

م. د فلاح مهدي عبد السادة
المديرية العامة لتربية بابل
وزارة التربية / المديرية العامة للتربية في محافظة النجف الاشرف
Falahmahdi19801980@gmail.com

ملخص :
يهتم البحث بدراسة موضوع على غاية من الاهمية، خاصة مع التطورات الحاصلة في الوضع الدولي بشكل عام، مع زيادة في استخدام الهجمات السيبرانية، وازدياد حجم المخاطر الناتجة عنها، في الوقت الذي تفتقر فيه الى تنظيم قانوني متكامل يحدد معالم تلك الظاهرة التي اخذت بالشيوع في العصر الحاضر، حتى صارت اثارها الجانبية اكثر من الاهداف المطلوب تحقيقها .ان استمرار الاثار والمخاطر التي تترتب على تلك الحرب، من دون وازع قانوني واخلاقي يردع الاطراف المتنازعة، يجعل الوضع الدولي في خطر دائم، لذلك ظهرت الحاجة الملحة لضرورة تدخل المجتمع الدولة لمعالجة بعض المخاطر الناتجة منها والحد من المخاطر المحتملة في حال تطورها، لذلك تظهر اهمية البحث من نفس المفهوم الذي تظهر فيه تلك الحروب والمسائل المعقدة التي تحتاج الى تفكيك وحل المسائل المتعلقة بها او تقييدها ببعض الالتزامات التي تنتج عنها .لذا وضعت هذه الدراسة بعض معاني ومفاهيم تلك الحرب وبيان اهم انواعها مع ذكر اهم التطبيقات التي جاءت في هذا العصر لاسيما بعد الحرب الاخيرة التي شنتها الولايات المتحدة والكيان الغاصب ضد جمهورية ايران الاسلامية وما تخللته من استخدام تقنيات الحرب السيبرانية والاضرار التي نتجت عنها، وخلصت الى الدراسة الى مجموعة من النتائج والتوصيات ... ونسأل الله التوفيق

الكلمات المفتاحية: الحرب السيبرانية، التطبيقات الدولية، الاضرار الناتجة عن الحرب السيبرانية، التحديات القانونية والقضائية .

Challenges of international law rules in the face of cyber warfare

Falah Mahdi Abdulasada
Falahmahdi19801980@gmail.com
Directorate General of Education in Babylon Governorate

Abstract:
This research addresses a highly important topic, particularly given the developments in the international landscape, including the increasing use of cyberattacks and the growing risks they pose. This occurs against a backdrop of a lack of comprehensive legal frameworks to define this phenomenon, which has become increasingly prevalent in the modern era, to the point where its side effects now outweigh its intended objectives.The continued impact and risks stemming from this type of warfare, without legal and ethical constraints to deter the conflicting parties, place the international situation in constant danger. Therefore, the urgent need for international intervention to address some of the resulting risks and mitigate potential dangers should the situation escalate, has become apparent. Thus, the importance of this research arises from the very concept of cyber warfare and the complex issues it raises, requiring analysis and resolution of related matters or the establishment of certain obligations arising from it.The importance of this research stems from the same understanding that cyber warfare and its complex issues require analysis and resolution, or at least

the establishment of certain obligations to address them. Therefore, this study outlines some meanings and concepts of cyber warfare, identifies its most important types, and mentions its most significant applications in this era, particularly after the recent war waged by the United States and the occupying entity against the Islamic Republic of Iran. This war involved the use of cyber warfare technologies and resulted in damages. The study concludes with a set of findings and recommendations. We ask God for success.
Keywords: Cyber warfare, international applications, damages resulting from cyber warfare, Legal and judicial challenges.

المقدمة :

اولا : مقدمة البحث Research Introduction :

تستند الحروب التقليدية الى قواعد قانونية تنظم وقوعها واساليب وطرق حدوثها والقيود التي تستخدم على بعض انواع من الاسلحة، الا ان الحرب السيبرانية وفق حداثة وجودها، تطرح تحديات جمّة، لذلك يوضح البحث بعض التعريفات الأساسية للحرب السيبرانية والأسلحة السيبرانية التي طُرحت حتى الآن، فضلًا عن الإطار القانوني الدولي، وتنطلق اهمية البحث من كثرة استعمال الاسلحة السيبرانية في الوقت الحاضر؛ لسهولة الاستعمال وقلة التكلفة وشدة التأثير في الخصم، مع بيان و عرض نماذج وتطبيقات لهجمات سيبرانية .

ثانيا: مشكلة البحث Research problem:

بسبب التطورات الحاصلة في اساليب ووسائل القتال، ولعدم وجود قواعد قانونية تنظم الهجمات السيبرانية بشكل صريح وخاصة في قواعد القانون الدولي الانساني التي تعتمد على اتفاقيات جنيف لعام ١٩٤٩ والبروتوكولات الملحقة بها .

لذا تبقى الحرب السيبرانية حالة معقدة، قد يتم حل جزء من مشاكلها القانونية بينما يبقى الجزء الآخر رهين الدراسات والبحوث الاكاديمية الاخرى .

يقودنا ذلك الى بيان المفاهيم والاسئلة الاتية :

ما هي الحرب او الهجمات السيبرانية ؟

كيف يمكننا تمييزها عن غيرها ؟

ما هي الاثار التي تترتب عليها ؟

هل يمكن تطبيقها عمليا على حالات من الهجمات والنزاعات في الوقت الحاضر ؟

ما هي ابرز التحديات التي تواجهها ؟

ثالثا : أهمية البحث Research Importance .

تنبع اهمية موضوع الدراسة من اهمية الهجمات السيبرانية نفسها؛ كونها احدى الوسائل الحديثة والمتطورة في مجال وسائل واساليب القتال غير التقليدية، التي باتت تشكل جزءً مهما من العمليات العسكرية في الوقت الحالي .

خاصة اذا كانت دول النزاع المسلح متباعدة في جغرافيا الارض، ان استخدام تقنيات ذات نزعة تدميرية تستهدف مراكز حيوية للدول المتنازعة بأقل جهد وتكلفة، يجعل ميدان استخدام هذه الاسلحة في اغلب النزاعات التي تدور رحاها في العالم .

رابعا : أهداف البحث Research objectives:

بيان مفهوم الحرب السيبرانية وتأثيرها على الاطراف محل النزاع بل المجتمع الدولي بشكل عام.

بيان القواعد القانونية التي تحكم هذه الهجمات .

توضيح اهم مسارات تطورها.

بيان اهم التطبيقات التي تحصل فيها .

خامسا : منهجية البحث Research Methodology ك
سيعتمد البحث على المنهج الوصفي التحليلي الذي يعتمد على تحليل النصوص القانونية والفقهية التي كتبت في الحرب السيبرانية من اجل ايجاد المعالجات القانونية اللازمة لحل اشكالية الدراسة .
المبحث الاول : مفهوم الحرب السيبرانية
تُعدّ الحرب السيبرانية ظاهرة معقدة، وتثير العديد من التساؤلات حول تعريفاتها، واختلافها عن أنواع الحروب الأخرى، ومدى توافقها مع مبادئ القانون الدولي المتعلقة بالحرب وقواعدها، ومن اجل الوصول الى حل هذه التساؤلات سنقوم ببيان مفهومها اولا، ومن ثم الحديث عن ذاتيتها وتمييزها عن غيرها .
المطلب الاول تعريف الحرب السيبرانية
تعتمد هذه المفاهيم في جزء منها على حقيقة أن الهجمات قد تختلف اختلافًا كبيرًا تبعًا للهدف النهائي، والنطاق، وأدوات الأجهزة والبرامج المستخدمة، الا انها تشترك في هدف واحد هو استغلال أنظمة وشبكات الحاسوب لتحقيق هدف عسكري مميز، الا انه وفي ذات الوقت؛ نتيجة إلى التنوع الكبير في تقنيات المعلومات، ونطاقاتها، وأهدافها، يصعب تقديم تعريف محدد لها.
هناك عدة محاولات من جانب الفقه لتعريف الحرب السيبرانية:
هناك من عرفها على انها : (أفعال تقوم بها دولة لاختراق أجهزة الكمبيوتر أو الشبكات الخاصة بدولة أخرى من اجل إحداث ضرر أو تعطيل) (Richard A. & Roberto K., 2010) .
هذا التعريف يقتصر على السلوك الذي تقوم به الدولة المنفذة والغاية التي تستهدفها من القيام بذلك العمل، وهذا التعريف هو تعريف مختصر من جانب ولا يبين او يوضح بقية الافعال، فهو وان كان يبين الهدف من الفعل الا انه لا يوضح بقية التفاصيل، كما انه يبرز الفعل كأنه صادر عن الدولة فقط، في حين ان هناك جهات او منظمات او شبكات خاصة تقوم بنفس الفعل .
ومن عرفها على انها : (عمليات تشن ضد الحاسوب او بواسطته من خلال معلومات دقيقة والهدف تحقيق اغراض مختلفة منها على سبيل المثال : اختراق نظام معين او جمع معلومات او نقلها او تشفير معلومات او تدمير اهداف معينة او اي اجراء ينطوي على تعديل البيانات والتحكم بها، او التلاعب ببياناتها وفقا لعملية دقيقة) (ربيع ، ٢٠٢٤)
التعريف المتقدم وان كان اوسع من التعريف الاول، الا انه لا يبين الجهة التي تقوم بالعمل السيبراني هل هي دولة ام جهة تابعة لها ام مجموعة افراد قاموا بالاختراق .
كذلك تم تعريفها على انها : (تلك الاجراءات التي تتخذها الاطراف في نزاع مسلح لكسب الميزة على الخصم في فضاء سايبر من خلال استخدام مختلف الادوات التكنلوجية والافراد المدربين على العمليات التقنية، والحصول على اهداف سريعة كتدمير او تعطيل انظمة الحاسوب للعدو او اختراق تلك الاجهزة للحصول على معلومات مهمة او ايقاف نشاط معين، او ما يعرف بعملية التجسس السيبراني متى ما كانت تلك العمليات في اطار نزاع مسلح يصل لمستوى الحرب) (سعود، ٢٠١٨)
ويبدو ان هذا التعريف يشتمل على الاجراءات المتخذة من اطراف النزاع ويحدد نطاق العمل والهدف المبتغى منه، فضلا عن تحديد الجهات القائمة بالفعل، لذا يتفق الباحث مع ما تقدم من تعريف وكذلك التعريف الذي اختصر تعريفها على انها : (الحرب التي تُشن في الفضاء الإلكتروني من خلال الوسائل والأساليب الإلكترونية) (Samuel Liles, J., Eric Dietz, & , Marcus Rogers, Dean L, 2012)
لقد جاء دور الفقه عقب غياب النص القانوني؛ بسبب حداثة تلك الهجمات وعدم النص عليها ضمن اتفاقيات القانون الدولي الانساني، مع مرور الوقت، تم بحث المزيد من تفاصيل هذه الظاهرة، ويمكن ملاحظة بعض أوجه التشابه في هذه التعريفات أو في تعريف المفهوم الأوسع نطاقًا مثل "حرب المعلومات"، الذي ورد في الملحق رقم (١) من (اتفاقية التعاون بين حكومات الدول الأعضاء في منظمة شنغهاي للتعاون بشأن التعاون في مجال ضمان الأمن المعلوماتي الدولي) لعام ٢٠٠٩ التي عرفت الحرب المعلوماتية جاء فيه : " المواجهة بين دولتين او اكثر في الفضاء المعلوماتي يهدف الى الاضرار بأنظمة المعلومات والعمليات والموارد والهياكل ذات الاهمية البالغة وتقويض الانظمة الاقتصادية

العدد 4 No 4
تموز 2026 July 2026
مجلة ساوة للدراسات الانسانية
Sawah Journal of Humanities
E-ISSN 3106 - 8324 P-ISSN 3106 - 8316
مجلة محكمة تصدر عن
جامعة ساوة الاهلية

والاجتماعية والتلاعب النفسي بالجماهير بهدف زعزعة استقرار المجتمع والدولة واجبار تلك الدولة على اتخاذ اجراءات وقرارات تصب في مصلحة الطرف المعارض "

المطلب الثاني خصائص الحرب السيبرانية

تمتاز الحرب السيبرانية بمجموعة خصائص نذكر منها (Stefano Mele, 2014):

أولًا: تُعدّ الحرب السيبرانية حرب تقنية برزت نتيجة التطور التكنولوجي وتعد أنظمة وشبكات الحاسوب أهدافًا مباشرة لها، وتُنفّذ معظم الهجمات السيبرانية عبرها، مع ذلك، يُمكن استخدام أنظمة وشبكات الحاسوب لاستهداف الأنظمة المادية وإلحاق أضرار مادية، بما في ذلك الوفاة والإصابة.

ثانيًا: قصر المدة الزمنية لتنفيذ الهجمات في الحرب السيبرانية بخلاف الحروب التقليدية وهذه ميزة تمتاز بها الحرب السيبرانية تمنح المتخاصمين استعمالها .

ثالثًا: اتساع الرقعة الجغرافية نظرًا لتصميم شبكات الحاسوب، وخاصة الإنترنت، قد تُوجّه أنشطة الحرب السيبرانية عبر مناطق جغرافية متعددة؛ مما يُثير إشكاليات معقدة تتعلق بقوانين الحياد.

رابعًا: ميزة التحكم عن بعد اذ قد تستخدم بعض أنشطة الحرب السيبرانية، التي تهدف إلى شنّ هجمات حركية، أجهزة وأسلحة العدو لتنفيذ الهجوم عن طريق التحكم بها عن بُعد.

خامسًا: طبيعة الحرب السيبرانية القائمة على مجهولية الفاعل في الغالب اذ تُشنّ معظم هجمات الحرب السيبرانية في وضع التخفي، أي دون الكشف عن هوية المهاجمين.

سادسا : قلة كلفة الحرب السيبرانية، اذ لا تحتاج الى ميزانية ضخمة او طلب تمويل اضافي للحرب كما تفعل الدول في الحروب التقليدية، التي تحتاج الى تكلفة عالية مثل المعدات المستخدمة ونقلها والبنى التحتية لها كالمطارات او حاملة الطائرات او الناقلات البحرية .

المطلب الثالث : الاسلحة المستعملة في الحرب السيبرانية

ان استعمال الاسلحة في الحرب السيبرانية، وفق مبدأ القوة أو التهديد باستخدامها، وكيفية إدارة العمليات العدائية، وما هي الاعتبارات والمعايير في اعتبارها اسلحة سيبرانية، وفي هذا الشأن ظهرت وجهتي نظر مختلفتين، وفقًا لوجهة النظر الاولى ان الاسلحة تُعتبر الأداة _ سواء كانت معدات مادية أو شفرة برمجية_ بناءً على قدرتها الموضوعية على إحداث ضرر أو تنفيذ هجوم، ومن أمثلة ذلك : قدرة السلاح السيبراني من احداث وثغرات أمنية، وحمولة مصممة لإحداث آثار تدميرية مادية أو رقمية (Samuel Liles, J., Eric Dietz, & , Marcus Rogers, Dean L, 2012)

في حين بينت وجهة النظر الثانية تقييم غرض المستخدم أو المطور لتحديد ما إذا كانت الأداة (أو الأدوات) المستخدمة تُعتبر سلاحًا سيبرانيًا: "جزء من معدات، أو جهاز، أو أي مجموعة من تعليمات الحاسوب، تُستخدم في نزاع بين جهات فاعلة وطنية وغير وطنية، بهدف إلحاق ضرر مادي (مباشر أو غير مباشر) بالأشياء أو الأشخاص، أو تخريب او إتلاف أنظمة المعلومات الخاصة بهدف حساس تابع للجهة المستهدفة بشكل مباشر (Mele, Stefan ٢٠١٤o) و توجد أمثلة عديدة على الأسلحة السيبرانية، من اهمها، و بصرف النظر عن المنهج أو وجهة النظر سلاح ستوكسنت (StuxNet) (Michael N. Schmidt, 2013) : هو برنامج خبيث معقد مصمم للبحث عن نظام تحكم محدد لعمليات صناعية معينة ضمن شبكة مغلقة، عند تحديد هذا النظام واختراقه، يُصمم البرنامج الخبيث لإلحاق الضرر بنوع معين من التوربينات وإحداث أضرار مادية متجاوزًا بذلك الضوابط البشرية والآلية للمصنع الصناعي المستهدف، ويُشابه هذا التأثير الناتج عن تدمير هذه التوربينات بالأسلحة التقليدية (ما يُعرف بالهجوم الحركي) خلال العمليات الحربية التقليدية، كما تشير خصائص البرمجيات الخبيثة المعقدة والمعرفة العميقة بالأنظمة المستهدفة إلى أنها برمجيات مصممة خصيصًا، أنشأها فريق متعدد التخصصات بالاعتماد على معرفة خاصة بالعمليات الصناعية التي تحكم النظام المستهدف يبدو أن البرمجيات الخبيثة طُوّرت لتتوافق مع معظم قواعد القانون الدولي(Trey Her, 2014) .

كما يمكن تقسيم الاسلحة السيبرانية الى عدة اقسام منها : الاسلحة الثابتة وتكون ذات الهجوم التلقائي مثل الاسلحة ذاتية الدفاع عن المنشآت الحيوية، والاسلحة الارضية وهذا النوع قليل جدا ويستخدم لاستهداف المناطق التي يصعب الوصول اليها ومثالها الروبوت البشري، وكذلك الاسلحة البحرية ومثالها الغواصات

العدد 4 No 4
تموز 2026 July 2026
مجلة ساوة للدراسات الانسانية
Sawah Journal of Humanities
E-ISSN 3106 - 8324 P-ISSN 3106 - 8316
مجلة محكمة تصدر عن جامعة ساوة الاهلية

والالغام المزروعة تحت الماء، و الاسلحة الجوية وهي اكثر انواع الاسلحة ومثالها الاسلحة من دون طيار (جنديل، ٢٠٢٥)

المبحث الثاني نماذج من الحروب السيبرانية وآثارها

تسبب الهجمات السيبرانية آثارا جانبية كثيرة، فهي تتعدى الهدف المرسوم لها؛ نظرا للقوة التدميرية التي تحدثها، لا تقتصر على الهدف كما اسلفنا، مما يؤدي الى انتهاك وخرق قواعد واساليب الحرب التي نظمتها المواثيق الدولية كمبدأ التناسب، ولهذه الحروب استعمالات كثيرة في الوقت الحاضر.

عليه سنناقش هذا المبحث في المطالب الاتية :

المطلب الاول : الحرب السيبرانية بين روسيا وعدد من الدول المجاورة لها

المطلب الثاني : الحرب السيبرانية بين الولايات المتحدة الامريكية والجمهورية الاسلامية في ايران

المطلب الثالث : الأضرار الجانبية والضحايا

المطلب الاول: الحرب السيبرانية بين روسيا وعدد من الدول المجاورة لها

كانت ولا تزال روسيا تمثل الجانب الدولي المناوئ للولايات المتحدة الامريكية في حروب السيطرة على العالم، ففي اعقاب تشظي وانقسام الاتحاد السوفيتي السابق برزت روسيا كدولة وريثة لذلك النظام، الا انها احتفظت بقوتها ومكانتها الدولية، خاصة كدولة اقتصادية وعسكرية ولها كيان مؤثر في الامم المتحدة، و مجلس الامن الدولي من العضوية الدائمة وحق النقض (الفيتو)، مقابل ذلك دعمت غريمتها امريكا عدد من الدول التي نشأت في اعقاب تفكك الاتحاد السوفيتي واصبحت مناوئة للحكومة الروسية مثل اوكرانيا واستونيا وليتوانيا وغيرها، لذا لم تقف روسيا مكتوفة الايدي ازاء ذلك، مما ادى الى حدوث هجمات سيبرانية قبل ان يندلع النزاع العسكري بين روسيا واوكرانيا .

اولا : هجمات الحرمان من الخدمة الموزعة في إستونيا : في عام ٢٠٠٢ حصل هجوم سيبراني على قدر عالي من الخطورة والضرر، بعد التطور الهائل في تكنلوجيا هذه الدولة وادى هذا الهجوم الى غلق مواقع حكومية وخدمات مصرفية وتم اتهام روسيا بهذا الهجوم (جنديل، ٢٠٢٥)، في عام ٢٠٠٧، تعرضت العديد من مواقع البنوك والحكومات والجامعات والصحف لهجمات "حجب الخدمة الموزعة" (James Pamment, Vladmir Sazonov, & Francesca Granelli, 2019) استمر لثلاث اسابيع حدث خلالها موجتان من الهجمات السيبرانية، ادت الى خسائر كبيرة قدرت بمليارات من عملة اليورو، اتهمت الحكومة روسيا بتدبير تلك الهجمات بصورة مباشرة او غير مباشرة الا نفي الحكومة الروسية وغموض الحدث وصعوبة تحديد الفاعلين، ادى الى ان تكون الاجراءات القانونية قضائيا غير ممكنة نظرا لصعوبة تحديد الجهة، وعدم وجود ادلة، فضلا عن عدم تبني تلك الهجمات من اي جهة كانت؛ مما جعل ان تكون اجراءات حكومية كردة فعل لتلك الهجمات كالتصريحات الحكومية او الاعلامية ، الا ان حجم الخسائر التي جاءت نتيجة تلك الهجمات وضعت المؤسسات المالية امام ضغط هائل على خوادمها نتيجةً للطلبات التي تولدها شبكات الروبوتات التي تقف وراء الهجمات، مما أدى إلى تباطؤ ملحوظ في حركة التجارة (Irawati Handayani, 2021).

ويرى الباحث انه بالرغم من امكانية حدوث تلك الحرب بين الطرفين، الا ان صعوبة تحديد الطرف القائم بها، واستعراض تلك الحرب وفق مجال التصريحات والاتهامات المتبادلة بين الطرفين، يشكل احدى التحديات التي تواجه الحرب السيبرانية وتكييفها القانوني .

ثانيا : الحرب السيبرانية بين روسيا واوكرانيا :

في عام ٢٠١٧ وفي ظل استمرار الازمة على شبه جزيرة القرم وعدد من المناطق محل النزاع، قامت روسيا بعدة هجمات سيبرانية على عدد من المواقع في اوكرانيا، وتم استخدام نوع من الفايروسات تحت اسم (بيتا)، تعرضت المواقع الاوكرانية عقب هذا الهجوم الى تعطيل في الانظمة الالكترونية لعدد من شركات ومؤسسات القطاع العام والخاص على حد سواء، في حين هاجمت اوكرانيا في العام نفسه اثناء حملة الانتخابات الرئاسية في روسيا، وتجددت عام ٢٠١٨ يوم التصويت على تلك الانتخابات مما ادى الى تعطيل عمليات المراقبة، كما تعرضت روسيا الى استهداف مباشر بهجمات سيبرانية على البنى التحية ابان بطولة كأس العالم التي اقيمت في روسيا عام ٢٠١٨، بعد عام اعلنت شركات الطاقة تعرضها

العدد 4 No 4
تموز 2026 July 2026
مجلة ساوة للدراسات الانسانية
Sawah Journal of Humanities
E-ISSN 3106 - 8324 P-ISSN 3106 - 8316
مجلة محكمة تصدر عن
جامعة ساوة الاهلية

الى هجوم سيبراني ادى الى تعطيل عدد من شبكات النقل، وكانت روسيا تتهم الولايات المتحدة الامريكية الحلف الاكبر لأوكرانيا بتمويل تلك الهجمات (عبد الواحد، ٢٠٢١).
وقد اشتدت تلك الحرب بعد ان اصبحت حربا تقليدية في عام ٢٠٢٢ مع استخدام تقنيات الحرب السيبرانية، عبر استخدام الطائرات من دون طيار والاقمار الصناعية والهجمات الالكترونية ودخول جهات من غير الدول في تلك الحرب، وقد سعت روسيا لحماية بناها التحتية وقطاعات مهمة مثل الطاقة والنقل وعملت على تأمين الدور الوقائي وعمليات الردع وتطوير قدراتها في سبيل المواجهة، الا ان اوكرانيا وبمعونة حلف شمال الاطلسي ودور الولايات المتحدة الامريكية الواضح استطاعة استهداف مواقع حيوية لروسيا اثرت بشكل كبير في استمرار الحرب (العمارات، ٢٠٢٤).

المطلب الثاني: الحرب السيبرانية بين الولايات المتحدة الامريكية والجمهورية الاسلامية في ايران
يعود تاريخ الحرب السيبرانية بين الولايات المتحدة وايران الى اكثر من عقدين من الزمن، وقد دخلت اوجها في الفترة الحالية ويتم اللجوء الى تلك الحرب؛ لأسباب عديدة منها : قلة الجهد والمال، وشدة التأثير، اذ تصل الى تدمير منشآت بأكملها او تعطيل قدراتها الانتاجية، تركز هذه الحروب على استخدام البرامج والفيروسات المدمرة، وقد شهدت الحرب التي شنتها الولايات المتحدة والكيان الصهيوني هجمات سيبرانية دعمت المجهود الحربي، وقد استخدم اطراف النزاع الفضاء السيبراني، اذ استخدمت ايران هجمات سيبرانية كأداة تأثير لتحقيق اهداف مختلفة، استهدفت المصالح الامريكية في المنطقة، كالشركات الاستثمارية وقطاع النفط والحرب النفسية، ومحاولة تعطيل القدرات العسكرية والمدنية على حد سواء (https://www.ecssr.ae/ar/research/products/infograph/٢٠٥٥٩٩/٢ ، ٢٠٢٦)
واستخدمت الولايات المتحدة هجمات سيبرانية ضد منشآت نووية ايرانية عام ٢٠١٠ (خليل، ٢٠٢٥) ، ومن ضمن ابرز الهجمات السيبرانية التي نفذتها الولايات المتحدة ضد المواقع والمنشآت الايرانية، تم استخدام فايروس ستوكسينت في هجمات ضد منشآت نووية عام ٢٠١٠، وفي ذات العام تم اصابة حوالي (٣٠٠٠٠) جهاز كمبيوتر مما ادى الى تعطيلها وفي عام ٢٠١٢ تم استهداف عدد من المنشآت النفطية واستمرت تلك الهجمات في الاعوام اللاحقة، اذ تسبب اختراق سيبراني للاعلام الايراني بنشر اعلانات عن الانتخابات الامريكية عام ٢٠١٩، في نفس العام اكتشفت الجهات المختصة في الجمهورية الاسلامية شبكات تجسس تديريها وكالة الاستخبارات الامريكية استطاعت تفكيكها، وفي العام نفسه شنت وزارة الدفاع الامريكية بواسطة طائرات مسيرة ناقلات نفط ايرانية في مضيق هرمز، وفي العام ٢٠٢٠ اقرت الحكومة الايرانية بانخفاض انتاجية الانترنيت ووسائل الاتصال الى نسب كبيرة؛ بسبب هجمات سيبرانية امريكية، في حين قامت الجهات المختصة في ايران بإحباط العديد من الهجمات منها : هجمات سيبرانية على الموانئ الايرانية وشبكات قرصنة عام (متعب، ٢٠٢١).
في الوقت ذاته لم تقف الجهات المختصة في الجمهورية الاسلامية مكتوفة الايدي امام تلك الهجمات وتداعياتها على الامن القومي الايراني بشكل خاص والمنطقة بشكل عام، ففي الوقت الذي عززت قدراتها التقنية وتعزيز الامن السيبراني، وفي اطار ذلك اسست كيان اسمته (جيش فضاء ايران السيبراني)، وقامت بتطوير قدراتها العسكرية والاعتماد في ذلك على احدث التقنيات وتشكلت عدد من التشكيلات القادرة على القيام بأي هجمات او صد الاعتداءات الموجهة لإيران ومنها : (المجلس الاعلى للسايبر، قيادة دفاع السايبر، الفاعلين المعلوماتيين) شكل هؤلاء الجيش السيبراني الذي اسس لعدد من الهجمات منها : حملة تشويش على موقع (تويتر) سابقا عام ٢٠٠٩ وفي عام ٢٠١٢ تم الهجوم السيبراني على عدد من البنوك الامريكية، ادى الى تعطيل حركتها المالية، كررت العملية عام ٢٠١٣، كما قام الفاعلين المعلوماتيين باختراق اجهزة كمبيوتر تابعة للبحرية الامريكية وبين الاعوام (٢٠١٧-٢٠١٨) اعترفت شركة مايكروسوفت بتعرضها لهجمات سيبرانية ايرانية، وفي عام ٢٠١٩ استهدف جيش الفضاء الايراني عمليات سيبرانية على عدد من الشركات الايرانية، كما اعترفت وسائل اعلام امريكية بحدوث هجوم سيبراني عام ٢٠٢٠ ادى الى التشويش على حملة ترامب الانتخابية (الميموني، تداعيات المواجهة بين ايران وامريكا، ٢٠٢٠) ، وبالرغم من حجم المعاناة التي واجهتها ايران بعد عام ١٩٧٩؛ بسبب تكثيف العقوبات الامريكية عليها، الا انها استطاعت التفوق في عدد من المجالات وتطوير قدراتها التي

العدد 4 No 4
تموز 2026 July 2026
مجلة ساوة للدراسات الانسانية
Sawah Journal of Humanities
E-ISSN 3106 - 8324 P-ISSN 3106 - 8316
مجلة محكمة تصدر عن
جامعة ساوة الاهلية

بانت بوادرها في الحرب الاخيرة (مطلك، الحروب السيبرانية بعد العام ٢٠١٠ الحرب الايرانية نموذجا، ٢٠٢٥) ، وقد استثمرت ايران قدراتها بادئ الامر بجمع المعلومات والبيانات، مما جعلها تصيب اهداف حيوية في حربها الاخيرة مع الكيان، بعد ان شنت عدة هجمات سيبرانية لبنى تحتية رقمية وصلت الى البث الاذاعي ومواقع انترنيت، وحذرت الدول المتعاونة مع الكيان من استخدام ذات الاسلوب، مع اختراق اجهزة سكانها وايصال رسائل تهديد، وقد حققت نتائج دقيقة وتحسن حجم الضربات الصاروخية مع تطور قدرتها الرقمية (القراضي، ٢٠٢٦)

المطلب الثالث: الاضرار الجانبية للحرب السيبرانية

من نتائج الحروب والنزاعات تضرر البنى التحتية للمرافق المدنية واصابة المدنيين او قتلهم، مما يؤدي الى ان كل عسكري يخلف اضرار جانبية، فاستهداف شبكات الماء وخطوط الطاقة والبنى التحتية، فضلا عن المدارس والمستشفيات، كما ان احتمالية اختراق المنظومة الالكترونية للطاقة النووية قد يتسبب في زيادة حجم الكوارث البيئية التي يصعب توقع حجم اثارها الانية والمستقبلية، كما ان هذا الامر قد يؤدي الى استغلال الجماعات الارهابية لتشديد عملياتها ضد الدول (سعيد، ٢٠١٧)
اقترح فريق خبراء تالين القاعدة ٥١ (القاعدة ١١٣ في الطبعة الثانية)، وتحديدًا فيما يتعلق بالأضرار الجانبية: "يُحظر أي هجوم إلكتروني... يُتوقع أن يتسبب في خسائر عرضية في أرواح المدنيين، أو إصابات للمدنيين، أو أضرار للأعيان المدنية، أو مزيج من ذلك، بما يتجاوز بكثير الميزة العسكرية الملموسة والمباشرة المتوقعة"، الا ان هذا المقترح تعرض للانتقاد؛ كونه يحتاج الى تقييم الأضرار المحتملة ومقارنتها بما تحقق من اهداف عسكرية على ارض الواقع والاهداف المحتملة او المباشرة التي تنتج هجمات السيبرانية، هذا الامر يتطلب معرفة عواقب الهجمات السيبرانية المباشرة وغير المباشرة، علاوة على ذلك يجب إجراء التقييم عند تصميم الهجوم وإصدار أوامره وتنفيذه، وينبغي النظر إلى الميزة العسكرية ككل، لا بالرجوع إلى جزء معين من الهجوم وتُقترح قواعد إضافية لتعزيز حماية المدنيين والحد من الأضرار الجانبية(Christopher Waters & Nils Melzer, 2011)
يمكن تقسيم الهجمات الإلكترونية إلى ثلاث مجموعات
وتشمل المجموعة الأولى الهجمات التي يمكن فيها التمييز بسهولة بين الضحايا والأهداف من جهة، والضحايا والأضرار الجانبية من جهة أخرى.
أما المجموعة الثانية : تضم الهجمات التي يصعب فيها التمييز بين الضحايا والأهداف والضحايا والأهداف الجانبية.
المجموعة الثالثة : تتضمن المجموعة الثالثة هجمات تستهدف كل شيء وكل شخص موجود في منطقة معينة.
إن احترام قواعد القانون الدولي، يفرض على القائمين على تلك الحروب اتخاذ الاحتياطات اللازمة وبذل العناية واختيار الاهداف العسكرية بدقة متناهية من اجل تقليل الاضرار الجانبية، بل وتأجيل تلك الهجمات او تعليقها في حال ادت الى ان تكون هناك اضرار جانبية بشكل مفرط مقارنة بالأهداف والنتائج العسكرية التي يمكن تحقيقها، لذلك جاء في البروتوكول الاضافي الاول الملحق باتفاقيات جنيف لعام ١٩٧٧ اشارت الى ذلك على انه : " يلغي أو يعلق أي هجوم إذا تبين أن الهدف ليس هدفا عسكريا أو أنه مشمول بحماية خاصة أو أن الهجوم قد يتوقع منه أن يحدث خسائر في أرواح المدنيين أو إلحاق الإصابة بهم. أو الأضرار بالأعيان المدنية، أو أن يحدث خلطا من هذه الخسائر والأضرار، وذلك بصفة عرضية، تفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة " (المادة (٥٧ /٢)، ١٩٧٧) واذ يثير هذا الأمر صعوبات كبيرة في الجانب العملي والتطبيقي، طالما كانت هناك نسبة كبيرة من عدم امكانية التمييز بين الأهداف المدنية والعسكرية على المواقع الالكترونية، بموجب البروتوكول الإضافي الأول، لا يُختار من بين الأهداف المكافئة إلا الهدف الذي يُشكّل أقل خطر على أرواح المدنيين وممتلكاتهم في حين جاءت الفقرة (٣) من نفس المادة " ينبغي أن يكون الهدف الواجب اختياره حين يكون الخيار ممكنا بين عدة أهداف عسكرية للحصول علي ميزة عسكرية مماثلة، هو ذلك الهدف الذي

يتوقع أن يسفر الهجوم عليه عن إحداث أقل قدر من الأخطار علي أرواح المدنيين والأعيان المدنية " (البروتوكول الاضافي الاول الملحق باتفاقيات جنيف ١٩٧٧، ١٩٧٧)
ينبغي فهم هذه الأحكام في سياق الالتزامات الأخرى التي بينتها ذات المادة من خلال ضرورة التحقق من أن الأهداف عسكرية وليست اعيان مدنية وليست خاضعة لحماية خاصة، كما يفترض التزام عام بعدم إلحاق الضرر بالسكان المدنيين، علاوة على ذلك، يستند الالتزام باختيار الأهداف المناسبة التي تُقلل من المخاطر على أرواح المدنيين وممتلكاتهم (نعمة، ٢٠١٨) ، كما توجد التزامات عامة بحماية السكان المدنيين وممتلكاتهم أثناء الحرب، وأخيرًا، من الواجبات الخاصة توخي الحذر الشديد أثناء الهجمات الإلكترونية على المنشآت التي تحتوي على مواد خطرة، كالسدود والحواجز ومحطات توليد الطاقة النووية، فضلًا عن المنشآت المجاورة لها كما توجد محظورات هامة يجب مراعاتها: أولها حظر الهجوم بهدف بث الرعب بين المدنيين؛ وثانيها حظر تدمير أو إزالة أو تعطيل أي شيء ضروري لبقاء المدنيين، ويجب قراءة هذه القواعد بالتزامن مع القواعد المتعلقة بالأهداف المشروعة، مع الأخذ في الاعتبار الأهداف غير المشروعة، كالمدنيين، والعاملين في المجال الطبي، والبنى التحتية الطبية، وأجهزة الحاسوب والشبكات الطبية، وأفراد ومنشآت الأطراف الثالثة في النزاع التي تسعى لتقديم المساعدات الإنسانية، والأشياء الضرورية لبقاء المدنيين من القواعد المثيرة للاهتمام بشكل خاص والتي تم صياغتها في دليل تالين القاعدة ٨٣ (القاعدة ١٤٣ في الطبعة الثانية) القائمة على مبدأ التمييز، والتي تنص على حظر مهاجمة الأعيان المدنية، والمادتين ٣٥ (٣) و٥٥ من البروتوكول الإضافي الأول لعام ١٩٧٧ (منيب، ٢٠٢٢) .

المبحث الثالث: تحديات ومعوقات مواجهة الحرب السيبرانية
ابرز ما يعيق تنظيم الحرب السيبرانية هو وجود قواعد القانون الدولي تعمل على تنظيم تلك الحروب على الرغم من شيوعها في الوقت الحاضر؛ مما تسببت في مشاكل عديدة اهمها عدم امكانية تحديد الطرف الذي قام بالهجوم السيبراني، فضلا عن التحديات التي تواجه التنظيم القانوني لها؛ مما يجعل الامر اكثر تعقيدا، مع اتساع وانتشار هذه الحروب، تظهر تحديات التكييف القانوني للحرب السيبرانية، فضلا عن قواعد تحديد المسؤولية، يضاف لها عدم التعاون الدولي بشكل حقيقي؛ لذلك سنناقش هذا المبحث بمطالب ثلاثة :
المطلب الاول : تحديات التكييف القانوني للحرب السيبرانية
المطلب الثاني : التحديات القضائية
المطلب الثالث : تحديات التعاون الدولي
المطلب الاول : تحديات التكييف القانوني للحرب السيبرانية
من اهم التحديات التي تواجه قواعد القانون الدولي في تكييف الحرب السيبرانية هي تكييف قواعد القانون الدولي مع تلك الهجمات وما تخلفه من تداعيات على القانون الدولي برمته، اذ يُعد تحليل هذه الحرب وبيان مفهومها أمرًا مهمًا للتعامل مع قضايا القانون الدولي الرئيسية، ولا سيما فيما يتعلق بحق اللجوء إلى الحرب، أما فيما يتعلق بحق الحرب، فإن المشاكل الأساسية تتمثل في ما إذا كان ينبغي اعتبار الحرب السيبرانية "استخدامًا للقوة" او هجومًا مسلحًا وفقًا لميثاق الأمم المتحدة، اما إذا كانت تمنح الحق في الدفاع الشرعي (Stefano Mele, 2014) .
فيما يتعلق بقانون الحرب ، تُثير الحرب السيبرانية إشكالياتٍ هامة بشأن إمكانية تطبيق قواعد القانون الدولي الإنساني القائمة في الواقع، لم تكن الحرب السيبرانية والفضاء السيبراني موجودين وقت صياغة ميثاق الأمم المتحدة، ولذا فإن مسألة ما إذا كانت القواعد الدولية الحالية قابلة للتطبيق أم أن هناك حاجة إلى قواعد دولية جديدة تكتسب أهمية بالغة ، وبالعودة الى الاتفاقيات الدولية التي نظمت قواعد الحرب واساليبها، من اتفاقية لاهاي عام ١٨٩٩ و١٩٠٧ واتفاقيات جنيف لعام ١٩٤٩ وبروتوكولاتها لعام ١٩٧٧ لم تنظم تلك المواثيق معالجة حالة الهجمات السيبرانية؛ وذلك لحداثتها، الامر الذي شكل خللا في التنظيم القانوني لها، مما ادى الى الحاجة الى تنظيمها، خاصة مع تزايد استخداماتها، الا انها تواجه مشكلة اخرى لا تقل عن عدم تنظيمها، تتمثل بصعوبة اثباتها ماديا، فضلا عن انكار فاعليها، على عكس طرق القتال

العدد 4 No 4
تموز 2026 July 2026
مجلة ساوة للدراسات الانسانية
Sawah Journal of Humanities
E-ISSN 3106 - 8324 P-ISSN 3106 - 8316
مجلة محكمة تصدر عن
جامعة ساوة الاهلية

التقليدي الذي يمكن اثبات العمليات العسكرية وعدم استطاعة الفاعلين انكارها، مع ذلك يمكن الاشارة الى عدد من القواعد التي تنطبق ولو بشكل غير صريح على الهجمات السيبرانية مثل مبدأ الامتناع عن استخدام القوة الوارد في ميثاق الامم المتحدة (المادة (٤ /٢)) ومن ثم فان استخدام تلك الهجمات هو بمثابة خرق لميثاق الامم المتحدة، كذلك تعد تلك الهجمات منتهكة لمبدأ التمييز بين المدنيين والمقاتلين؛ نظرا لشدة تأثيرها طبقا لقواعد البروتوكول الاضافي الاول لعام ١٩٧٧ اذ جاء في المادة (٤٨) منه على ان " تعمل أطراف النزاع علي التمييز 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 المدنيين والأعيان المدنية ". ، كما يمكن ان ينطبق عليها نص الفقرة (٤) من المادة (٥١) من نفس البروتوكول التي جاء فيها : " تحظر الهجمات العشوائية، وتعتبر هجمات عشوائية:
(أ) تلك التي لا توجه إلي هدف عسكري محدد.
(ب) أو تلك التي تستخدم طريقة أو وسيلة للقتال لا يمكن أن توجه إلي هدف عسكري محدد.
(ج) أو تلك التي تستخدم طريقة أو وسيلة للقتال لا يمكن حصر آثارها علي النحو الذي يتطلبه هذا اللحق "البروتوكول". ومن ثم فإن من شأنها أن تصيب، في كل حالة كهذه، الأهداف العسكرية والأشخاص المدنيين أو الأعيان المدنية دون تمييز " .

فيما يتعلق بالقانون الدولي، قامت مجموعة من الخبراء، بدعوة من مركز دولي، هو مركز التميز التابع لحلف الناتو في مجال الدفاع السيبراني التعاوني بمبادرة قيّمة لوضع دليل ينظم الحرب السيبرانية المعروف باسم (دليل تالين) لا يُعتبر وثيقة رسمية ، وإنما يعبّر فقط عن وجهة نظر الخبراء الدولي في مجال الدفاع السيبراني التعاوني، إلا أنه يُشير إلى محاولة جادة لدراسة الحرب السيبرانية استنادًا إلى القانون الدولي العرفي والاتفاقي، واقتراح قواعد سلوك واضحة ، كذلك معاهدة بودابست عام ٢٠٠١ التي اطلق عليها (الاتفاقية الاوروبية لمكافحة الجريمة المعلوماتية) مما جعلها اتفاقية قارية، وركزت على توحيد الجهود القانونية وتعزيز التعاون الدولي بين السلطات المختصة في تلك الدول وتبادل المعلومات والتنسيق الامني وحماية الحدود، ويركز التعاون الدولي على تبادل المعلومات والتنسيق بين الجهات المختصة ومساعدتها في تعقب الجريمة الالكترونية، وعلى الرغم من كونها اتفاقية قارية الا ان انضمام دول اخرى خارج قارة اوروبا اليها لاحقا كالولايات المتحدة واليابان وجنوب افريقيا عزز من اهميتها فضلا عن كونها اللبنة الاولى في سبيل الاهتمام بهكذا نوع من الجرائم، ووضعها لاطار قانوني للإجراءات اللازمة لمواجهة تلك الجرائم، وان اصطدمت ببعض العقبات والتحديات الا ان تبنيها لآليات محددة وفقا لقواعد القانون الدولي المرعية في التعاون الدولي ومنها : التعاون في تسليم المجرمين والتنسيق الامني والمعلوماتي و تعزيز الاجراءات القضائية، جعل من هذه الاتفاقية بمثابة رؤية قانونية وركيزة دولية مهمة في مجال مواجهة الجريمة الالكترونية والمعلوماتية والحد منها، مما يتطلب مزيد من الاهتمام الدولي لتطوير الادوات القانونية التي يمكنها من مواجهة التحديات المختلفة في سبيل مواجهة تلك الهجمات (الكثيري، ٢٠٢٥)

بالرغم من ذلك فان دليل تالين يفتقر الى الصفة الالزامية؛ كونه لم يصدر بقرار دولي ولا وفقا لمعاهدة دولية برعاية منظمة الامم المتحدة، بل ان محتوى الدليل يعكس الرؤية الغربية للعمليات السيبرانية، مما يقلل من فائدته العامة دوليا خاصة مع رفض عدد من الدول لمضامينه كروسيا والصين (الابيض ، ٢٠٢٥) .

المطلب الثاني: التحديات القضائية

مع تطور تكنلوجيا المعلومات ومع ازدياد النزاعات واستخدام اساليب ووسائل جديدة، كان لابد للقضاء الدولي الاستعانة بالتقنيات الحديثة في الملاحقة القضائية والتحقيق والاجراءات القانونية الاخرى، اذ ان الهدف القضاء هو تحقيق العدالة وانصاف الضحايا، ومع قيام القضاء بالأساس على الادلة المباشرة وغير المباشرة في اجراءات الاثبات، ومع استخدام تقنيات الذكاء الاصطناعي، ولما كانت المحكمة الجنائية الدولية المؤسسة القضائية الدولية التي تم انشاؤها من اجل تحقيق العدالة الجنائية وملاحقة مرتكبي اشد الجرائم خطرا، الا ان تواجه تحديات قانونية كبيرة في التعامل مع الجرائم السيبرانية، من أبرزها صعوبة

العدد 4 No 4
تموز 2026 July 2026
مجلة ساوة للدراسات الانسانية
Sawah Journal of Humanities
E-ISSN 3106 - 8324 P-ISSN 3106 - 8316
مجلة محكمة تصدر عن
جامعة ساوة الاهلية

تحديد الفاعل الحقيقي للهجوم الإلكتروني؛ بسبب استخدام وسائل وتقنيات تساعد على اخفاء معالم الجريمة، فضلا عن الطابع العابر للحدود لهذه الجرائم، الذي قد يثير مشاكل تتعلق بمسائل تبعية الاختصاص القضائي ، فضلاً عن صعوبة جمع الأدلة الرقمية واثبات العلاقة وغيرها من الاسباب التي قد تعرقل فرص نجاح القضاء الدولي في معالجتها، بالرغم من التطور الحاصل في تقنيات تلك الجرائم خاصة مع عمليات عندما استهداف المنشآت المدنية أثناء النزاعات المسلحة، في حال أدى هجوم سيبراني إلى تعطيل المرافق المدنية الى تعطيل عمل المستشفيات أو محطات الطاقة أو شبكات المياه، مما يؤدي إلى خسائر كبيرة في الارواح ، وهو ما قد يجعله يرقى إلى مستوى جرائم الحرب (جسام، ٢٠٢٦)

فهل بالإمكان الاستناد الى الادلة الرقمية في الاجراءات القضائية ؟ يمكن القول ان التطور التكنلوجي احدث امرين، الاول منهما : خلق مجموعة من الادلة الرقمية، والثاني : تغيير في وسائل الاثبات والتحقيق وعرض الادلة .

مما يؤدي الى امكانية استخدام تلك الادلة في النزاعات المسلحة، خاصة مع زيادتها في الوقت الحاضر من خلال استخدام الاقمار الصناعية ووسائل الاتصال التقنية، ومن الادلة على ذلك اعتماد المحكمة الجنائية الدولية على ادلة من تم تداولها في مواقع التواصل الاجتماعي لمقاطع مصورة منشورة لعمليات اعدام جماعية في ليبيا؛ مما ادى الى اصدار مذكرة توقيف بحق (محمود مصطفى يوسف الورفلي)، وهو احد قادة قوات حفتر المعارضة الذي اغتيل لاحقا، وقد صدرت الاجراءات عام ٢٠١٦ بناءً غلى ادلة رقمية استندت اليها المحكمة الجنائية الدولية، وهي اول قضية يتم اعتماد الادلة الرقمية في الاجراءات القانونية التي اعتمدتها المحكمة، بعد اتهامه بجرائم حرب بالاستناد الى قانون المحكمة الجنائية الدولية (Lindsay Freeman, 2018) .

الا ان الاجراءات القانونية توقفت بحق الورفلي بقرار من مجلس الامن ؛ بسبب اغتياله في النزاع الليبي من دون توقف بقية الاجراءات (قرار مجلس الامن الدولي ٠١/١١-٠١/١٧، ٢٠٢٢)

نستنتج من هذا الاجراء ما يلي :

اولا : التطور الحاصل في القضايا الجنائية الدولية من خلال الاستناد الى الادلة الرقمية .

ثانيا : امكانية الاستناد الى الادلة الرقمية في الادلة الجنائية، خاصة ان التهم المنسوبة الى الورفلي تستند الى جرائم الحرب الواردة في النظام الاساسي للمحكمة الجنائية الدولية .

ثالثا : امكانية اعتماد الادلة الرقمية خاصة مع زيادة استخدام تقنيات التكنلوجيا والذكاء الاصطناعي في اغتيال عدد من القادة المدنيين في الاعتداء الذي حصل من امريكا والكيان الصهيوني ضد ايران وعدد من الدول العربية .

بالرغم من ذلك لا يزال التحديات القضائية في هذا المجال كبيرة جدا، خاصة مع القيود التي يفرضها النظام القضائي للمحكمة الجنائية الدولية، مما يجعل الامر يحتاج الى تعديل في النظام الاساسي للمحكمة .

المطلب الثالث : تحديات التعاون الدولي

بعد انتشار تقنيات الذكاء الاصطناعي، وازدياد استخدام التكنلوجيا في النزاعات الدولية، مع عجز عدد من المواثيق الدولية الخاصة بتنظيم التقاضي الدولي ، او عدم كفاية طرق التعاون الدولي في تحقيق العدالة الجنائية، صار لزاما على المجتمع الدولي ايجاد وسائل للتعاون تعمل بشكل مؤثر لتحقيق معايير العدالة الجنائية، فالنظام القانوني يعتمد بشكل كبير على مسائل التعاون الدولي في الاجراءات القانونية الجنائية كمسألة تسليم المجرمين والمساعدة القانونية و تبادل المعلومات والخبرات، الى ان يصل الى التعاون مع المحاكم الدولية، ووفقا لنظام روما الاساسي قانون المحكمة الجنائية الدولية لعام ١٩٩٨، فأنه يعتمد على مسائل تعاون الدول في اجراءات التحقيق والمقاضاة وفق المواد (٨٦-١٠٢)، غير ان التعاون الذي اشار اليه النظام الاساسي انما يعتمد على مدى قيام الدول الأطراف بالتعاون مع المحكمة الجنائية الدولية ، من خلال سريان ولاية المحكمة عليها عند قبولها باختصاصات المحكمة وفقا لما ما جاء في النظام الاساسي للمحكمة، كما إن نظام روما الأساسي لم يغفل تعاون الدول غير الأطراف مع المحكمة الدولية الجنائية، إلا أن ذلك لا يتم الا وفق الشروط التي بينتها المادة (٨٧) من ذلك النظام، وبالرغم من الاهتمام الكبير من المحكمة بشأن التركيز على القضايا الأشد خطورة من جرائم تكون موضع الاهتمام الدولي ،

العدد 4 No 4
تموز 2026 July 2026
مجلة ساوة للدراسات الانسانية
Sawah Journal of Humanities
E-ISSN 3106 - 8324 P-ISSN 3106 - 8316
مجلة محكمة تصدر عن
جامعة ساوة الاهلية

وهو امر لا يمكن الاستهانة به في القضاء الجنائي الدولي، الا ان هذه المكانة القانونية لا يمكن لها الاستمرار مالم تسندها الدول بالتعاون المطلوب وفق نظامها الاساس (الطائي، ٢٠١٧).

في حين كان هناك استراتيجيات وطنية للأمن السيبراني، فقد اطلقت الولايات المتحدة الامريكية استراتيجية دولية للفضاء السيبراني عام ٢٠٢٤ التي ترمي للتضامن الرقمي من خلال التعاون الدولي في مجال الفضاء السيبراني وتنظيم عمل الفضاء الالكتروني من خلال احترام قواعد القانون الدولي، الا انها مع ذلك سعت لتعزيز الامن القومي الامريكي على حساب بقية الدول سواء المتحالفة معها او التي تخاصمها كروسيا والصين (خليل، ٢٠٢٥) ، كما ان هناك العديد من الدول تطلق استراتيجية وطنية لحماية امنها السيبراني ومنها العراق الذي يحاول اتخاذ التدابير اللازمة لضمان حماية امن العراق السيبراني من التهديدات المحتملة واصلاح حالات الضعف التي تحصل في بعض الاحيان؛ بسبب الابتزاز الالكتروني واساءة استخدام مواقع التواصل وصولا للتجسس الالكتروني والتدخل الخبيث والارهاب الالكتروني، وتسعى الجهات المختصة للحد من تأثيرات التهديدات السيبرانية وحماية الامن الوطني (مستشارية الامن الوطني في العراق، ٢٠٢٦) (١).

ومع عمليات خرق الانظمة القانونية الدولية بعد تفرد الولايات المتحدة الامريكية في عدد من النزاعات الدولية دون اللجوء الى الامم المتحدة، وبقرارات منفردة من الرئيس الامريكي والتغطية على انتهاكات الكيان الصهيوني لقواعد القانون الدولي خاصة في الاعتداءات الاخيرة على ايران والدول العربية، لا سيما مع استخدام تقنيات الهجمات السيبرانية التي ادت الى قتل قادة مدنيين واستخدام اسلحة محظورة في ذلك، كذلك قيام الكيان الصهيوني بعمليات اغتيال لعدد من قادة المقاومة الفلسطينية مستخدمة الطائرات المسيرة والاسلحة الموجة، وكذلك احدث عملية البيجر ضد افراد حزب الله اللبناني في اعقاب العدوان على فلسطين ولبنان عام ٢٠٢٤، مما يستدعي تغيير قواعد التعاون الدولي ووضع حد لتلك الانتهاكات و الخروقات القانونية التي ظهرت بشكل علني من دون رادع .

الاستنتاجات Conclusions:

إن انتشار التقنيات الجديدة مثل الذكاء الاصطناعي والأسلحة المتطورة، بالإضافة إلى الأسلحة المزودة بأنظمة استهداف تعتمد على الذكاء الاصطناعي سيؤدي إلى ظهور مشاكل قانونية أكثر تعقيدًا لحلها.

ان محاولات المجتمع الدولي إيجاد نهج متفق عليه للتعامل مع الحرب السيبرانية بالتوازي مع تطور التكنولوجيا، لا يزال في طور التأسيس ويفتقر الى اتفاقيات دولية تنظمه او تحل المشاكل التي تنتج عنه.

ان التطور الهائل في استخدم تقنيات الحرب السيبرانية وهجماتها تحتاج الى تدخل منظمة الامم المتحدة لمعالجة الكوارث الناتجة عنها وذلك حفاظاً على تطبيق المبادئ الأساسية المتعلقة باستخدام القوة والدفاع عن النفس ودور الأمم المتحدة في حل النزاعات الدولية.

نتج عن دراسة الحرب السيبرانية انها بحاجة الى معرفة العديد من التفاصيل منها : القانون الواجب التطبيق، و هل هناك وعي عام بالمخاطر التي تنتج عن تلك الهجمات التي تُلحق أضرارًا أكبر من الهجمات التقليدية، لا سيما إذا لم تُصمَّم بعناية للحد من الأضرار الجانبية، في ظل غياب المعايير التي تحدد ذلك .

امكانية الاستناد الى الادلة الرقمية في القضايا الجنائية الدولية الناتجة عن النزاعات المسلحة والاستناد الى الادلة الرقمية كوسائل من وسائل الاثبات والتحقيق .

المقترحات The proposals :

حث المجتمع الدولي ولا سيما منظمة الامم المتحدة من اجل وضع معايير محددة او الاتفاق على آليات للحد من المخاطر الجانبية للأضرار التي تلحقها الحروب السيبرانية .

الزام الدول التي تستخدم تقنيات الحرب السيبرانية باتخاذ الاحتياطات اللازمة لمنع حدوث اي اضرار جانبية او التقليل منها قدر الامكان .

(١) مستشارية الامن الوطني العراقي، استراتيجية الامن السيبراني، متاح على الموقع الالكتروني : تاريخ الوصول ٢٠٢٦/٦/٥.

دعوة الامم المتحدة لعقد اتفاقية دولية تحد من مخاطر وآثار الحرب السيبرانية وتعمل على حل المشاكل القانونية ومن ضمنها تحديد وسائل وآليات التعامل مع تلك الاسلحة، وتحديد القانون الواجب التطبيق، والمسؤولية الدولية الناتجة عنها .

ينبغي توخي أقصى درجات الحذر لتقليل حجم هذه الأضرار مع الالتزام بتقاليد القانون الدولي الإنساني، ان لم تتوفر قواعد قانونية لمثل تلك الحروب والنزاعات الالكترونية .

ضرورة تعديل الاجراءات القانونية في مجال المنظمات الدولية وخاصة منظومة الامم المتحدة وميثاق روما الاساسي ليتناسب والتطورات الحاصلة في مجال استخدام تقنيات الذكاء الاصطناعي وحرب السيبرانية .

المصادر والمراجع ومواقع الانترنيت .

المراجع

Nils Melzer, & Nils Melzer. (2011). Cyberwarfare and the International Law. Dalhousie Law Journa(2), p. 33.

البروتوكول الاضافي الاول الملحق باتفاقيات جنيف ١٩٧٧. (١٩٧٧). الامم المتحدة.

المادة (٥٧ /٢). (١٩٧٧).

(٢٠٢٢). قرار مجلس الامن الدولي ٠١/١١-٠١/١٧. منظمة الامم المتحدة.

دور الفضاء السيبراني في الحرب الايرانية – الامريكية. (٢ ٤، ٢٠٢٦). مركز الامارات للدراسات والبحوث الاستراتيجية.

Christopher Waters, & Nils Melzer. (2011). Cyberwarfare and the International Law. Dalhousie Law Journa, p. 33.

Irawati Handayani. (2021). Diajeng Wulan Christiant,Cyber-Attack in Estonia: a New Challenge in The Applicability of International Humanitarian Law. p. 50.

James Pamment, Vladmir Sazonov, & Francesca Granelli. (2019). cyber attacks on Estonia. p. 22.

Lindsay Freeman. (2018). Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials,. Fordham International Law Journal, pp. 229-231.

Michael N. Schmidt. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press.

Richard A., C., & Roberto K., K. (2010). Cyberwar. Harper Colins.

Samuel Liles, J., Eric Dietz, & , Marcus Rogers, Dean L. (2012). Applying Traditional Principles To Cyber Warfare.

Stefano Mele. (2014). Legal Considerations on Cyber-Weapons and Their Definition. p. 17.

Trey Her. (2014, February 1). PrEP: A Framework for Malware & Cyber Weapons, Journal of Information Warfare. (1.(

ابراهيم علي القراضي. (٢٠٢٦). تداعيات الحرب الايرانية الاسرائيلية على الامن القومي العربي. مجلة العلوم الشاملة(٣٩)، صفحة ٢٠٧١.

احمد عبيس نعمة. (٢٠١٨). الهجمات السيبرانية دراسة قانونية علمية بشأن تحديات تنظيمها المعاصر (المجلد ١). بيروت، لبنان: منشورات زين الحقوقية.

احمد علي الميموني. (٢٠٢٠). تداعيات المواجهة بين ايران و امريكا. مجلة الدراسات الايرانية(١٢)، صفحة ٢٠.

احمد علي الميموني. (٢٠٢٠). تداعيات المواجهة بين ايران وامريكا. مجلة الدراسات الايرانية(١٢)، صفحة ٢٠.
المادة (٤ /٢). (بلا تاريخ). ميثاق الامم المتحدة. منظمة الامم المتحدة.
تقى اياد خليل. (٢٠٢٥). حروب الجيل السادس واستراتيجية المواجهة : السيبرانية انموذجا كلية القانون والعلوم السياسية، العدد(٢٧). كلية القانون والعلوم السياسية، صفحة ٤١٥.
درويش سعيد. (٢٠١٧). الحروب السيبرانية وأثرها على حقوق الانسان دراسة على ضوء أحكام دليل "تالين. لمجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية(٥٤)، صفحة ١٨٩.
دنيا جواد مطلك. (٢٠٢٥). استراتيجيات الحروب السيبرانية بعد العام ٢٠١٠ الحرب الايرانية نموذجا. صفحة ١٠٢٩.
دنيا جواد مطلك. (٢٠٢٥). الحروب السيبرانية بعد العام ٢٠١٠ الحرب الايرانية نموذجا. مجلة القادسية للقانون والعلوم السياسية.
سعد عبيد الطائي. (٢٠١٧). تعاون الدول مع المحكمة الدولية الجنائية في اجراءات التحقيق والمحاكمة. كلية القانون، القانون. جامعة بابل.
سعيد مسعود الكثيري. (٢٠٢٥). الجريمة الالكترونية في ضوء اتفاقية بودابست : الاطار المفاهيمي والتصنيفي. مجلة البحوث القانونية والاقتصادية، صفحة ٩٥٠.
صلاح حيدر عبد الواحد. (٢٠٢١). حروب الفضاء الالكتروني دراسة في مفهومها وخصائصها وسبل مواجهتها. رسالة ماجستير، ٣٢. الاردن: جامعة الشرق الاوسط.
عبد المنعم منيب. (٢٠٢٢). الحرب السيبرانية والصراع بين الدول، المركز العربي للدراسات الانسانية. الرياض: المركز العربي للدراسات الانسانية.
فارس محمد العمارات. (٢٠٢٤). الامن السيبراني المفهوم وتحديات العصر (المجلد ١). عمان، الاردن: دار الخليج للنشر والتوزيع.
كاظم محمد جسام. (٢٦ ٤، ٢٠٢٦). تاريخ الاسترداد ٢٦ ٤، ٢٠٢٦، من https://altaakhi.net/2026/05/251751
كرار عباس متعب. (٢٠٢١). الحرب السيبرانية : دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة وايران، ، العدد(٤٠)، ٢٠٢١، ص٢١٠.(٤٠)، صفحة ٢١٠.
محمد الابيض . (٢٠٢٥). دليل تالين والقواعد المنطبقة على الهجمات السيبرانية. مجلة العلوم القانونية والاجتماعي، صفحة ٩٧٠.
محمد صلاح ربيع . (٢٠٢٤). الهجمات السيبرانية بين مشروعيتها كوسيلة للدفاع الشرعي وادانتها كاعتداء غير مشروع (دراسة تحليلية في ضوء القانون الدولي). مجلة الدراسات القانونية، صفحة ٤١٦٢.
مستشارية الامن الوطني في العراق. (٢٠٢٦). https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf . تاريخ الاسترداد ٥ ٥، ٢٠٢٦، من https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf
مهند عجب جنديل. (٢٠٢٥). الهجمات السيبرانية والاسلحة الذاتية في ظل التناسب. مجلة واسط للعلوم الانسانية، صفحة ٣٠١.
يحيى ياسين سعود. (٢٠١٨). الحرب السيبرانية في ضوء قواعد القانون الدولي الانساني. المجلة القانونية، صفحة ٨٤.