دور القانون الدولي الانساني في حماية البنى التحتية الرقمية في النزاعات المسلحة

م.م أريج عباس حسن
كلية القانون–جامعة تكريت

البريد الإلكتروني Email : Areej.A.Hasan@tu.edu.iq

الكلمات المفتاحية: القانون الدولي الإنساني، البنى التحتية الرقمية، النزاعات المسلحة.

كيفية اقتباس البحث

حسن، أريج عباس ، دور القانون الدولي الانساني في حماية البنى التحتية الرقمية في النزاعات المسلحة، مجلة مركز بابل للدراسات الانسانية، تشرين الثاني ٢٠٢٦، المجلد:١٦ ،العدد:١١ .

هذا البحث من نوع الوصول المفتوح مرخص بموجب رخصة المشاع الإبداعي لحقوق التأليف والنشر (Creative Commons Attribution) تتيح فقط للآخرين تحميل البحث ومشاركته مع الآخرين بشرط نَسب العمل الأصلي للمؤلف، ودون القيام بأي تعديل أو استخدامه لأغراض تجارية.

مفهرسة في Indexed
IASJ

مسجلة في Registered
ROAD

The Role of International Humanitarian Law in Protecting Digital Infrastructure in Armed Conflicts

Areej Abbas Hasan
College of Law - Tekreet University

Keywords : International Humanitarian Law, Digital Infrastructure, Armed Conflicts.

How To Cite This Article
Hasan, Areej Abbas , The Role of International Humanitarian Law in Protecting Digital Infrastructure in Armed Conflicts,Journal Of Babylon Center For Humanities Studies, November 2026,Volume:16,Issue 11.

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Abstract

This research highlights the role of international humanitarian law in protecting digital infrastructure during armed conflicts. It adopts the descriptive approach to clarify the legal the international rules relating to the protection of civilian objects and digital infrastructure, and the analytical approach to examine legal texts in international conventions, particularly the Geneva Conventions, the Additional Protocols, and international judicial practice. It also employs the comparative approach to compare Arab and international experiences in applying international humanitarian law to cyberattacks. The study finds that traditional principles of international humanitarian law, especially the principle of distinction, are applicable to digital infrastructure when a cyberattack produces effects comparable to conventional kinetic attacks. However, this application faces difficulties, particularly the dual civilian/military use of digital infrastructure. The study recommends establishing a clear international legal framework for attributing cyberattacks and holding states responsible for non-state actors acting under their direction or effective control.

The importance of this research stems from the evolving nature of armed conflicts. With the rapid digital transformation and the emergence of cyber warfare as a tool of conflict, it has become necessary to study the applicability of traditional rules of international humanitarian law—which were developed in the context of physical conflicts—in the digital environment. The importance of this study also lies in the importance of filling the international legislative gap. The legal rules that regulate cyberattacks are still unclear or incomplete, which makes research on this topic a means of contributing to the development of a legal framework that ensures the protection of individuals and civilian infrastructure from the effects of digital warfare.

ملخص

يسلط هذا البحث الضوء على دور القانون الدولي الإنساني في حماية البنى التحتية الرقمية أثناء النزاعات المسلحة. وقد اعتمد المنهج الوصفي لبيان القواعد القانونية الدولية المتعلقة بحماية الأعيان المدنية والبنية التحتية الرقمية، والمنهج التحليلي لتحليل النصوص القانونية في الاتفاقيات الدولية، ولا سيما اتفاقيات جنيف والبروتوكولات الإضافية والممارسات القضائية الدولية، فضلًا عن المنهج المقارن لمقارنة التجارب العربية والدولية في تطبيق القانون الدولي الإنساني على الهجمات السيبرانية. وتوصلت الدراسة إلى عدد من النتائج، أبرزها أن مبادئ القانون الدولي الإنساني التقليدية، وفي مقدمتها مبدأ التمييز، قابلة للتطبيق على البنى التحتية الرقمية متى أحدث الهجوم السيبراني آثارًا تماثل آثار الهجمات الحركية التقليدية، غير أن هذا التطبيق يواجه صعوبات، أهمها ازدواجية الاستخدام المدني/العسكري. وأوصت الدراسة بوضع إطار قانوني دولي واضح لإسناد الهجمات السيبرانية وتحميل الدولة مسؤولية الجهات غير الحكومية التي تعمل بتوجيه أو سيطرة فعلية منها.

تنبع أهمية هذا البحث من تطور طبيعة النزاعات المسلحة، فمع التحول الرقمي المتسارع وظهور الحروب السيبرانية كأداة من أدوات الصراع، أصبح من الضروري دراسة مدى قابلية قواعد القانون الدولي الإنساني التقليدية –التي وُضعت في سياق النزاعات المادية – للتطبيق في البيئة الرقمية، كما تكمن أهمية هذه الدراسة من أهمية سد الفراغ التشريعي الدولي، فلا تزال القواعد القانونية التي تنظم الهجمات الإلكترونية غير واضحة أو غير مكتملة، مما يجعل البحث في هذا الموضوع وسيلة للمساهمة في وضع إطار قانوني يضمن حماية الأفراد والبنى التحتية المدنية من آثار الحرب الرقمية.

مقدمة

أصبحت البنى التحتية الرقمية في العصر الحديث أحد الأعمدة الأساسية للحياة المدنية، إذ تقوم عليها شبكات الاتصالات، والطاقة، والخدمات الصحية، والأنظمة المالية، وقواعد البيانات الحكومية، بما يجعلها عنصراً حيوياً لا غنى عنه لاستقرار المجتمعات واستمرار الخدمات الأساسية. وفي ظل النزاعات المسلحة المعاصرة، لم تعد آثار العمليات العسكرية مقتصرة على الأعيان المادية التقليدية، بل امتدت لتشمل الفضاء الرقمي وما يرتبط به من نظم وتقنيات، الأمر الذي يطرح تساؤلات قانونية وإنسانية جوهرية حول مدى كفاية قواعد القانون الدولي الإنساني في توفير الحماية اللازمة لهذه البنى أثناء النزاعات.

ويضطلع القانون الدولي الإنساني بدور محوري في حماية الأعيان المدنية خلال النزاعات المسلحة، من خلال مبادئه الأساسية، وعلى رأسها مبدأ التمييز بين الأهداف العسكرية والأعيان المدنية، ومبدأ التناسب، وواجب اتخاذ الاحتياطات اللازمة عند شن الهجمات. ومع التطور المتسارع للتقنيات الرقمية وازدياد الاعتماد على الأنظمة السيبرانية في إدارة المرافق الحيوية، بات من الضروري بحث مدى انطباق هذه المبادئ التقليدية على البنى التحتية الرقمية، ومدى قدرتها على مواكبة طبيعة الهجمات السيبرانية التي قد تُحدث آثاراً إنسانية جسيمة دون إحداث دمار مادي مباشر.

وتنبع أهمية هذا البحث من أن استهداف أو تعطيل البنية التحتية الرقمية أثناء النزاعات المسلحة يؤدي إلى نتائج إنسانية خطيرة، تتمثل في تعطيل الخدمات الأساسية، وحرمان المدنيين من الاتصال والمعلومات، وإضعاف قدرة الدول والمنظمات الإنسانية على إدارة الأزمات والاستجابة لها. كما أن هذه الهجمات تُفاقم من معاناة السكان المدنيين، وتزيد من هشاشتهم الاقتصادية والاجتماعية، وتُسهم في خلق أزمات مركّبة تمتد آثارها إلى ما بعد انتهاء النزاع، بما في ذلك إعاقة جهود إعادة الإعمار وبناء السلام.

وانطلاقاً من ذلك، يسعى هذا البحث إلى تحليل دور القانون الدولي الإنساني في حماية البنى التحتية الرقمية أثناء النزاعات المسلحة، من خلال دراسة الإطار القانوني القائم، وتقييم مدى فعاليته في مواجهة التحديات التي تفرضها العمليات السيبرانية الحديثة. كما يهدف إلى استجلاء أوجه القصور في التنظيم القانوني الحالي، وبيان الحاجة إلى تطوير قواعد قانونية أكثر وضوحاً، سواء عبر تفسير موسّع لمبادئ القانون الدولي الإنساني أو من خلال العمل على إرساء إطار دولي خاص ينظم حماية الأعيان الرقمية، ويحدد مفهوم الضرر الرقمي وآليات المساءلة القانونية.

ويخلص البحث إلى أن حماية البنية التحتية الرقمية لم تعد مسألة تقنية بحتة، بل أضحت ضرورة إنسانية وقانونية تفرض إعادة النظر في آليات تطبيق القانون الدولي الإنساني، بما يضمن صون كرامة المدنيين، واستمرارية الخدمات الحيوية، والحفاظ على الحد الأدنى من الاستقرار المجتمعي حتى في خضم النزاعات المسلحة.

الدراسات السابقة:

يتناول هذا الجزء من البحث الدراسات السابقة بحيث يتم استعراضها بحسب تسلسلها الزمني من الأحدث إلى الأقدم وكالآتي:

تناولت دراسة السيحاني وغرير (٢٠٢٥) الإجراءات القانونية لحماية المدنيين والبنى التحتية الحيوية مثل شبكات الكهرباء والاتصالات في النزاعات السيبرانية. استخدمت الدراسة تحليل قانوني لوضع الحماية القائمة تحت IHL ومدى كفايتها في مواجهة التهديدات السيبرانية. تم التوصل في نهاية الدراسة إلى أن القانون الدولي الإنساني يواجه تحديات في حماية المدنيين والبنى الحيوية بسبب تطور التكنولوجيا وعدم وضوح تعريف "الهجوم السيبراني". وأوصت الدراسة بضرورة تفسير أوسع للقواعد الحالية لتغطية الفضاء السيبراني بشكل فعال.

تتقاطع الدراسة الحالية مع الدراسة السابقة في التركيز على التحديات التطبيقية، لكن الدراسة الحالية تذهب إلى تقديم توصيات عملية أكثر تفصيلاً (اتفاقية دولية وآليات مساءلة).

هدفت دراسة Kumar et al (٢٠٢٥) إلى اقتراح إطار يعادل اتفاقيات جنيف لتنظيم الحرب السيبرانية، يهدف بشكل صريح إلى حماية المواطنين وحياتهم الرقمية والبنى التحتية أثناء النزاعات المسلحة. استخدمت الدراسة تحليلي يُحلّل مبادئ اتفاقيات جنيف القائمة ويكيّفها بإطار جديد يتناول الحرب السيبرانية. توصلت الدراسة إلى حاجة ملحّة لتطوير أطر تنظيمية إضافية تتجاوز النصوص التقليدية للتمييز والتناسب، وذلك لحماية البيانات المدنية، الشبكات الحيوية، والشبكات الفضائية، ولمنع النتائج الإنسانية الخطيرة للهجمات السيبرانية. وتم التوصية بدعوة المجتمع الدولي إلى اعتماد اتفاقية جديدة تُكمّل اتفاقيات جنيف وتوفّر آليات واضحة لمسائلة الدول والمقاتلين عن أذى البنى التحتية الرقمية.

وتعتبر هذه الدراسة السابقة أقرب إلى الدراسة الحالية، إذ كلاهما يقترحان إطارًا جديدًا ينظم حماية البنى التحتية الرقمية بوضوح عبر اتفاقية أو قواعد دولية إضافية، إلا أن الدراسة الحالية تمتاز عن الدراسة السابقة من كونها تضيف تحديد مفهوم "الضرر الرقمي" وآليات المساءلة بشكل أكثر تفصيلاً.

حاولت دراسة Biggio (٢٠٢٥) تحليل التوازن بين مبدأ الإنسانية ومبدأ الضرورة العسكرية في تطبيق قواعد القانون الدولي الإنساني على العمليات السيبرانية، مع التركيز على كيفية تفسير "الهجوم" في الفضاء السيبراني بحيث يشمل التأثيرات غير الحركية على البنية التحتية، وذلك من خلال تحليل نقدي وتفسيري يدرس الإطار القانوني للتمييز والتناسب في سياق الهجمات السيبرانية، ومقارنة بين تفسيرات مختلفة لمفهوم "الهجوم" في الفضاء الرقمي. وجدت الدراسة أن التفسير السائد لـ IHL في المجال السيبراني يفضّل الضرورة العسكرية على المبادئ الإنسانية، ما قد يُتيح للهجمات السيبرانية غير الحركية التأثير على البنى التحتية المدنية دون تقييد كافٍ. ولتعزيز حماية المدنيين، تقترح الدراسة توسيع مفهوم الهجوم بحيث يشمل فقدان الوظائف الحيوية في الشبكات أو الأنظمة.

تمتاز الدراسة الحالية عن دراسة السابقة بأنها تعتمد مقاربة أشمل لحماية البنى التحتية الرقمية، إذ لا تقتصر على تفسير مفهوم «الهجوم» السيبراني، بل تنظر إلى البنية الرقمية كعين مدنية مستقلة تستوجب حماية خاصة في إطار القانون الدولي الإنساني، وبذلك تضيف الدراسة الحالية بعداً بنيوياً وتنظيمياً أوسع مقارنة بالطرح التحليلي الجزئي الذي تبنته الدراسة السابقة.

هدفت دراسة أبو النور ومحمد، (٢٠٢٤) إلى البحث في التحديات القانونية التي يواجهها القانون الدولي الإنساني في التعامل مع الحرب السيبرانية أثناء النزاعات المسلحة. استخدمت الدراسة منهج وصفي تحليلي لتحليل المفاهيم القانونية والتحديات المرتبطة بتطبيق مبادئ القانون الدولي الإنساني في مواجهة الهجمات السيبرانية. أظهرت الدراسة أن القانون الدولي الإنساني لا يزال يواجه صعوبات في تحديد نطاق «الهجوم السيبراني» وتطبيق مبادئ مثل التمييز والتناسب في الفضاء الرقمي. اوصت الدراسة بإعادة تفسير قواعد القانون الدولي الإنساني لتتناسب مع خصائص الحرب السيبرانية وتعزيز التدريب القضائي على هذه القواعد الرقمية.

اتفقت الدراسة الحالية مع الدراسة في السابقة في تناولهما التحديات التطبيقية لمبادئ القانون الدولي الإنساني في الفضاء السيبراني، لكن الدراسة الحالية تذهب أبعد باقتراح صياغة قواعد دولية جديدة لحماية البنى التحتية الرقمية، بينما هذه السابقة تركز على الحاجة إلى تفسير موسّع للقواعد القائمة.

سعت دراسة محمد وعبد الغني (٢٠٢٣) إلى تحليل مدى انطباق أحكام القانون الدولي الإنساني على الحرب السيبرانية في النزاعات المسلحة غير الدولية، مع إبراز التحديات القانونية المرتبطة بتطبيق القانون الدولي الإنساني على الهجمات السيبرانية، استخدمت الدراسة منهج

وصف–تحليلي، يعتمد على تحليل النصوص القانونية الدولية ذات الصلة ومناقشة التحديات القانونية والتطبيقية في الفضاء السيبراني. توصلت الدراسة إلى أن الهجمات السيبرانية تُعد من أهم أدوات النزاعات المعاصرة وبأن أطر القانون الدولي الإنساني الحالية تواجه صعوبات في التطبيق على هذه العمليات بسبب تعقيد الطبيعة السيبرانية وصعوبة إسناد الهجمات. وأوصت الدراسة بضرورة تطوير آليات قانونية دولية فعّالة لتنظيم سلوك الدول والجهات المسلحة في الفضاء السيبراني، وتعزيز الامتثال لأحكام القانون الدولي الإنساني.

تشترك الدراسة الحالية مع هذه الدراسة في التركيز على تطبيق قواعد القانون الدولي الإنساني على الهجمات السيبرانية، إلا أن الدراسة الحالية تمتاز عن الدراسة السابقة في كونها تتوسع في حماية البنى التحتية الرقمية تحديداً، بينما تركّز الدراسة السابقة بشكل أوسع على التحديات القانونية وإسقاطها على النزاعات غير الدولية.

أولاً: إشكالية البحث:

تواجه البنى التحتية الرقمية في ظل النزاعات المسلحة تحديات متزايدة نتيجة تصاعد الهجمات السيبرانية التي تستهدف الأنظمة المدنية الحيوية، مما يهدد أمن المعلومات والخدمات الأساسية المرتبطة بحياة المدنيين. ورغم أن القانون الدولي الإنساني يتضمن مبادئ عامة لحماية الأعيان المدنية، إلا أن تطبيق هذه القواعد على الفضاء السيبراني ما زال يثير جدلاً واسعاً من حيث مدى كفايتها وقدرتها على مواكبة طبيعة التهديدات الرقمية الحديثة. ومن هنا تبرز الإشكالية الرئيسة في التساؤل: إلى أي مدى يُسهم القانون الدولي الإنساني في حماية البنى التحتية الرقمية أثناء النزاعات المسلحة، وما هي حدود فاعليته في مواجهة التطورات التكنولوجية والهجمات السيبرانية المعاصرة؟

وفي إطار الإجابة عن هذه الإشكالية، تعترضنا الأسئلة الفرعية الآتية:

١.ما المقصود بالبنية التحتية الرقمية؟ وما هو نطاقها القانوني في ظل القانون الدولي الإنساني؟

٢.ما مدى انطباق قواعد القانون الدولي الإنساني التقليدية، مثل مبدأ التمييز والتناسب والاحتياط على حماية البنى التحتية الرقمية أثناء النزاعات المسلحة؟

٣.هل تكفي النصوص الحالية في اتفاقيات جنيف وبروتوكولاتها الإضافية لتوفير حماية فعّالة للبنى التحتية الرقمية من الهجمات السيبرانية؟

٤.ما أبرز التحديات القانونية والتقنية التي تواجه تطبيق أحكام القانون الدولي الإنساني على العمليات السيبرانية؟

ثانياً: أهمية البحث

تنبع أهمية هذا البحث من تطور طبيعة النزاعات المسلحة، فمع التحول الرقمي المتسارع وظهور الحروب السيبرانية كأداة من أدوات الصراع، أصبح من الضروري دراسة مدى قابلية قواعد القانون الدولي الإنساني التقليدية –التي وُضعت في سياق النزاعات المادية – للتطبيق في البيئة الرقمية، كما تكمن أهمية هذه الدراسة من أهمية سد الفراغ التشريعي الدولي، فلا تزال القواعد القانونية التي تنظم الهجمات الإلكترونية غير واضحة أو غير مكتملة، مما يجعل البحث في هذا الموضوع وسيلة للمساهمة في وضع إطار قانوني يضمن حماية الأفراد والبنى التحتية المدنية من آثار الحرب الرقمية.

وتكمن أهمية هذه الدراسة أيضاً في تعزيز الحماية الإنسانية في الفضاء السيبراني، إذ تسعى الدراسة إلى إبراز كيفية امتداد مبادئ القانون الدولي الإنساني، مثل التمييز والتناسب والضرورة العسكرية، إلى الهجمات السيبرانية لضمان حماية المدنيين والأنظمة الحيوية المدنية من الأضرار الإلكترونية. وتبرز أهمية هذه الدراسة نظرًا لقلة الدراسات العربية المتخصصة في هذا المجال، إذ تساهم الدراسة في سد فجوة معرفية مهمة من خلال تحليل التفاعل بين القانون الدولي الإنساني والقانون الدولي السيبراني، واستعراض التطبيقات العملية والأمثلة الواقعية من النزاعات الحديثة.

ثالثاً: أهداف الدراسة

يتمثل الهدف الرئيسي للدراسة في بيان أي مدى يُسهم القانون الدولي الإنساني في حماية البنى التحتية الرقمية أثناء النزاعات المسلحة، كما تهدف هذه الدراسة إلى تحقيق الآتي:

١.توضيح المقصود بالبنية التحتية الرقمية؟ وما هو نطاقها القانوني في ظل القانون الدولي الإنساني.

٢.تحديد مدى انطباق قواعد القانون الدولي الإنساني التقليدية، مثل مبدأ التمييز والتناسب والاحتياط على حماية البنى التحتية الرقمية أثناء النزاعات المسلحة.

٣.بيان مدى كفاية النصوص الحالية في اتفاقيات جنيف وبروتوكولاتها الإضافية لتوفير حماية فعّالة للبنى التحتية الرقمية من الهجمات السيبرانية.

٤.الكشف عن أبرز التحديات القانونية والتقنية التي تواجه تطبيق أحكام القانون الدولي الإنساني على العمليات السيبرانية.

رابعاً: منهج الدراسة

لتحقيق أهداف هذه الدراسة حول دور القانون الدولي الإنساني في حماية البنى التحتية الرقمية أثناء النزاعات المسلحة، تم اعتماد منهج تحليلي ومقارن، يجمع بين المنهج الوصفي والمنهج النقدي، كما يلي:

١-المنهج الوصفي: والذي يعتمد على وصف القواعد القانونية الدولية المتعلقة بحماية الأعيان المدنية والبنية التحتية الرقمية في النزاعات المسلحة، مع استعراض مبادئ القانون الدولي الإنساني الأساسية، مثل التمييز، والتناسب، والضرورة العسكرية، وكيفية تطبيقها في البيئة الرقمية.

٢-المنهج التحليلي: والذي يركز على تحليل النصوص القانونية، سواء من الاتفاقيات الدولية مثل اتفاقيات جنيف والبروتوكولات الإضافية، أو من الممارسات القضائية الدولية والأحكام الصادرة عن المحاكم الدولية، لفهم مدى فعالية هذه النصوص في حماية البنية التحتية الرقمية.

٣-المنهج المقارن: والذي يتم من خلاله مقارنة التجارب العربية والدولية في تطبيق القانون الدولي الإنساني على الهجمات السيبرانية، مع دراسة الممارسات الوطنية للبلدان العربية فيما يتعلق بحماية الفضاء الرقمي أثناء النزاعات.

خامساً: هيكلية الدراسة:

سوف يتم تقسيم الدراسة إلى مبحثين وكالآتي:

المبحث الأول: ماهية البنية التحتية الرقمية

المطلب الأول: التعريف بالبنية التحتية الرقمية

المطلب الثاني: الأسس القانونية الدولية لحماية الأعيان الرقمية

المبحث الثاني: التحديات والآليات العملية لحماية البيئة الرقمية

المطلب الأول: التحديات المرتبطة بتطبيق القانون الدولي الإنساني على البنية الرقمية

المطلب الثاني: آليات حماية البنية الرقمية وتعزيز الامتثال للقانون الدولي الإنساني،

الخاتمة والنتائج والتوصيات

قائمة المصادر والمراجع.

المبحث الأول

ماهية البنية التحتية الرقمية

يقدم هذا المبحث فهم شامل لمفهوم البيئة الرقمية والبنية التحتية الرقمية التي تُشكل العمود الفقري للخدمات الحيوية في العصر الحديث، خصوصاً في ظل النزاعات المسلحة، حيث تعتبر هذه

البيئة الرقمية عنصراً حيوياً لاستمرارية الحياة الاقتصادية والاجتماعية والسياسية، إذ يعتمد عليها السكان المدنيون في الحصول على الخدمات الأساسية، والتواصل، وإدارة شؤونهم اليومية.

وعليه، سوف يتم تناول هذا المبحث من خلال مطلبين:

المطلب الأول: التعريف بالبيئة التحتية الرقمية

وتعد البنية التحتية الرقمية من الركائز الأساسية التي تدعم الأنشطة الرقمية في العصر الحديث، حيث تمثل الأساس لتطوير الاقتصاد الرقمي وتقديم الخدمات الرقمية المتنوعة، وكلمة "بنية تحتية" تعني الأساس، ويمكن تعريف البنية التّحتيّة على أنها الأنظمة المادية الأساسية التي تسهل عملية الإنتاج في القطاع الصناعي، أو الحياة في المجتمعات ().[١]

ولم تعد البنية التحتية الرقمية تُطرح اليوم بوصفها مجرد منظومة تقنية أو أدوات برمجية، بل أضحت محل نقاش قانوني متزايد، ولا سيما في إطار القانون الدولي الإنساني، بشأن مدى خضوعها لنظام الحماية المقرر للأعيان المدنية أثناء النزاعات المسلحة. فالتطور المتسارع في أنماط الحروب السيبرانية والهجمات الرقمية أفرز إشكالية جوهرية تتعلق بتحديد ما إذا كانت مكونات البنية التحتية الرقمية، وعلى رأسها البيانات الرقمية، تدخل ضمن مفهوم "الأعيان" الوارد في المادة (٥٢) من البروتوكول الإضافي الأول لعام ١٩٧٧.

وتنص المادة (١/٥٢) من البروتوكول الإضافي الأول على أن: "الأعيان المدنية هي جميع الأعيان التي ليست أهدافًا عسكرية"، وتضيف الفقرة (٢) أن الأهداف العسكرية تقتصر على "الأعيان التي تسهم إسهامًا فعالًا في العمل العسكري، والتي يحقق تدميرها أو الاستيلاء عليها ميزة عسكرية أكيد" [٢].

غير أن النص لم يضع تعريفًا صريحًا لمفهوم "العين"، الأمر الذي فتح المجال لاجتهادات فقهية وقضائية متعددة حول ما إذا كان هذا المفهوم يقتصر على الأشياء المادية الملموسة، أم يمكن أن يمتد ليشمل الكيانات غير المادية، وعلى رأسها البيانات الرقمية.

في هذا السياق، يذهب اتجاه فقهي تقليدي إلى قصر مفهوم "الأعيان" على الأشياء المادية القابلة للتدمير أو الإتلاف الفيزيائي، مستندًا إلى السياق التاريخي لنصوص القانون الدولي الإنساني، التي وُضعت أساسًا لتنظيم وسائل وأساليب الحرب التقليدية. ووفقًا لهذا الاتجاه، فإن البيانات المجردة، بصفتها كيانات غير ملموسة، لا تُعد أعيانًا بالمعنى المقصود في المادة (٥٢)، حتى وإن كانت مخزنة على وسائط مادية محمية كالأقراص الصلبة أو الخوادم[٣] .

في المقابل، يذهب اتجاه فقهي حديث، مدعوم بتطور طبيعة النزاعات المسلحة، إلى تبني تفسير وظيفي ومرن لمفهوم "العين" معتبرًا أن القيمة العملية للبيانات وتأثيرها المباشر على البنى المدنية

الحيوية (كالمستشفيات، وشبكات الكهرباء، والمياه، والمصارف) يبرر إدخالها ضمن نطاق الحماية، ولو بشكل غير مباشر. ويستند هذا الاتجاه إلى أن تعطيل البيانات أو التلاعب بها قد يُحدث آثارًا مماثلة، أو حتى أشد خطورة، من تدمير الأعيان المادية ذاتها ().[٤]

وقد انعكس هذا الجدل بوضوح في دليل تالين ٢.٠ بشأن تطبيق القانون الدولي على العمليات السيبرانية، حيث ميّز الخبراء بين البنية التحتية المادية الداعمة للفضاء السيبراني، والتي تُعد دون خلاف "أعيانًا" قابلة للحماية أو الاستهداف وفقًا لطبيعتها، وبين البيانات في حد ذاتها، التي لم يحسم الدليل اعتبارها عينًا مستقلة، مع إقرار وجود انقسام فقهي حاد حول هذه المسألة ().[٥]

وعليه، ترى الباحثة، أن البنية التحتية الرقمية، في بعدها القانوني، تطرح تحديًا حقيقيًا أمام القواعد التقليدية للقانون الدولي الإنساني، إذ إن المكونات المادية لها (كالخوادم ومراكز البيانات) تخضع دون إشكال لمفهوم الأعيان، في حين تبقى البيانات الرقمية في منطقة رمادية قانونيًا، تتأرجح بين التفسير الحرفي للنصوص والتفسير الغائي الذي يراعي طبيعة النزاعات المعاصرة وآثارها الإنسانية.

المطلب الثاني: الأسس القانونية الدولية لحماية الأعيان الرقمية.

ترتكز الأسس القانونية الدولية لحماية الأعيان الرقمية على مبادئ القانون الدولي الإنساني التي تُلزم أطراف النزاع بعدم استهداف الأعيان المدنية، إذ تُعد الأعيان الرقمية في الوقت الراهن جزءًا من تلك الأعيان التي يجب حمايتها من الهجمات خلال النزاعات المسلحة، لا سيما في ظل استخدام الفضاء السيبراني كوسيلة من وسائل القتال. ويُعزَّز هذا الإطار القانوني بمبادئ حماية الخصوصية الرقمية التي تؤكد على ضرورة تكاتف الجهود الدولية لوضع نظم قانونية متكاملة تكفل صون البيانات والمعلومات الشخصية للأفراد، وتضمن احترام حقوقهم الرقمية في مواجهة التهديدات التقنية المعاصرة[٦] .

وفي السياق القانوني الدولي، يُطرح سؤال جوهري حول تعريف "الأعيان الرقمية"؟ وما إذا كان يُنظر إليها كأعيان محمية بموجب القانون الدولي الإنساني (IHL)؟، وفيما إذا كانت البيانات الحاسوبية تُعد "أعيانًا"، أي أنها تدخل ضمن مفهوم "الأشياء المدنية" التي يحظر استهدافها في النزاعات المسلحة، خاصة إذا كان تدميرها أو تغييرها يترتب عليه تأثير على المدنيين أو العمليات المدنية؟، لذلك، من المهم أن يُثبت القانون أن الأعيان الرقمية تستوفي شروط التمايز والتمييز بين الأهداف العسكرية والمدنية حتى يكون لها الحماية القانونية[٧] .

إن استعمال العمليات السيبرانية في النزاعات المسلحة بات واقعًا لا يمكن تجاهله، ويثير تحديات كبيرة في تطبيق القانون الدولي الإنساني، فالقانون الدولي الإنساني قد تطور ليشمل حماية

المدنيين من الآثار السيبرانية التي تسببها هجمات إلكترونية تستهدف بنيتها التحتية أو الخدمات الأساسية، إلا أن المبادئ الأساسية للقانون الدولي الإنساني مثل مبدأ التمييز، ومبدأ الضرورة العسكرية، ومبدأ التناسب، تُطبق أيضًا على العمليات الرقمية، لكن التنفيذ العملي غالبًا ما يواجه تعقيدات تقنية أو غموضًا قانونيًا حول مدى إمكانيات الأضرار الرقمية وتأثيراتها على المدنيين[٨].

وتفرض القوانين الدولية على الدول التزامات واضحة عندما تعمل في فضاء النزاع المسلح بما يتعلق بالأعيان الرقمية. فوفقًا لتقارير اللجنة الدولية للصليب الأحمر (ICRC)، فعلى سبيل المثال في تقرير للهيئة الاستشارية العالمية بشأن التهديدات الرقمية أثناء النزاعات المسلحة لسنة (٢٠٢٣)، فإن الدول ملزمة "بحماية السكان المدنيين من التهديدات الرقمية"، وإيجاد ضوابط تتيح استمرارية حماية الخصوصية والبيانات الشخصية، وعدم استخدام العمليات السيبرانية بشكل ينتهك الحقوق القائمة للمدنيين. كما يشير التقرير إلى الحاجة لتطوير سياسة دولية واضحة حول "التهديدات الرقمية" تشمل تنسيقًا بين القانون الوطني والدولي لضمان عدم إساءة استخدام القدرات السيبرانية .[٩]

من أمثلة الأعيان الرقمية التي تتطلب الحماية، "التراث الرقمي الثقافي". فالأعمال الرقمية ذات القيمة الثقافية (كالوسائط الرقمية، والمخطوطات الرقمية، وأعمال الفنون الرقمية) تستحق حماية مماثلة للملكية الثقافية المادية بموجب الاتفاقيات مثل اتفاقية لاهاي لحماية الممتلكات الثقافية. ويتم التركيز على أن القوانين الحالية لا تُعرّف بوضوح ما إذا كانت هذه المواد الرقمية تُعد "الممتلكات الثقافية" ويجب أن تُعامل بنفس الامتدادات القانونية التي تُخصص للممتلكات التقليدية.

وترى الباحثة، أنه بالرغم من التقدم في الأدبيات القانونية، توجد فجوات كبيرة في الحماية القانونية للأعيان الرقمية، من بين هذه الفجوات غياب تعريف موحد للدولة بين ما يُشكّل "الشيء الرقمي" المحمي، وعدم وجود نظام دولي معترف به دوليًا لتحديد موقع الأعيان الرقمية وتحديد ملكيتها ومسؤوليات الحماية قبل وأثناء النزاعات، بالإضافة إلى التحديات التقنية مثل صعوبة تحديد الأضرار الرقمية، وإثبات الأثر، وحصر التداخل بين الأهداف المدنية والعسكرية في الهجمات الإلكترونية، كما أن بعض الدراسات تشير إلى أن الكثير من التشريعات الوطنية والدولية لم تواكب التطور التكنولوجي، مما يترك المدنيين عرضة لمخاطر قد لا تغطيها الأطر القانونية القائمة تمامًا[١٠].

المبحث الثاني

التحديات والآليات العملية لحماية البيئة الرقمية

يتناول هذا المبحث العقبات القانونية والفنية والعملية التي تحول دون التطبيق الفعّال للقواعد القانونية الدولية، كما يسلط الضوء على مجموعة من الآليات الوقائية والمراقبية التي يمكن تبنيها لتعزيز الامتثال للقانون الدولي الإنساني، بما يشمل الأطر التشريعية، نظم المراقبة والتقييم، وتدريب الأطراف المعنية على احترام القواعد القانونية في الفضاء السيبراني. ويهدف هذا المبحث إلى تقديم تصور متكامل لكيفية التوفيق بين المتطلبات القانونية وحاجات حماية البيئة الرقمية، لضمان استدامة الخدمات الرقمية الحيوية وتقليل المخاطر على المدنيين والبنية التحتية الحيوية. وعليه، ولتحديد التحديات والآليات العملية لحماية البيئة الرقمية تم تقسيم هذا المبحث إلى مطلبين:

المطلب الأول: التحديات المرتبطة بتطبيق القانون الدولي الإنساني على البيئة الرقمية

شهد العالم اليوم تحولًا رقميًا متسارعًا، مما يطرح تحديات جديدة أمام تطبيق القانون الدولي الإنساني (IHL) في النزاعات المسلحة. تتمثل أبرز هذه التحديات في صعوبة تحديد المسؤولية عن الهجمات السيبرانية، تداخل الأهداف العسكرية والمدنية في الفضاء الرقمي، تعقيد تحديد الضرر الناتج عن هذه الهجمات، وأثر تطور التقنيات على فعالية القوانين القائمة.

وسوف يتم البحث في التحديات المرتبطة بتطبيق القانون الدولي الإنساني على البنية التحتية الرقمية من خلال الفرع الآتية:

الفرع الأول: التحديات القانونية في تطبيق القانون الدولي الإنساني على الهجمات السيبرانية

تتمثل التحديات القانونية لتطبيق القانون الدولي الإنساني على الهجمات السيبرانية في عدة محاور رئيسية، أولا صعوبة تحديد ما إذا كان الهجوم السيبراني يُعد "هجومًا" بموجب القانون الدولي، خصوصًا عندما يقتصر تأثيره على التعطيل دون التسبب في أضرار مادية ملموسة، وثانيًا، تواجه المبادئ الأساسية للقانون الدولي الإنساني مثل التمييز والتناسب تحديات كبيرة نتيجة للطبيعة الافتراضية للإنترنت، وصعوبة تحديد العلاقة المباشرة بين الهجوم ومصدره. ثالثًا، يتفاقم التعقيد بسبب التطور السريع للتقنيات السيبرانية، الذي يجعل قدرة الأطر القانونية الحالية على مواكبة هذه المستجدات محدودة، مما يفرض إعادة النظر في القواعد التقليدية لضمان حماية المدنيين والبنية التحتية الحيوية في الفضاء الرقمي[١١].

كما يواجه تطبيق قواعد القانون الدولي الإنساني على الهجمات السيبرانية صعوبات قانونية متعددة، من أبرز هذه الصعوبات عدم وضوح تعريف "الهجوم" في الفضاء السيبراني، حيث

يختلف الفقهاء والدول في تفسير ما يشكل هجومًا قانونيًا في هذا السياق، فبينما يرى البعض أن الهجوم السيبراني يجب أن يؤدي إلى ضرر مادي ملموس، يقترح آخرون توسيع هذا التعريف ليشمل تعطيل الوظائف الحيوية للبنية التحتية الرقمية، حتى وإن لم ينتج عنه ضرر مادي مباشر. هذه الاختلافات تؤثر على تطبيق مبادئ التمييز والتناسب والاحتياطات، مما يخلق تحديات في تحديد الأهداف العسكرية المشروعة وحماية الأعيان المدنية () .[١٢]

وتشير اللجنة الدولية للصليب الأحمر إلى أن الهجوم السيبراني الذي يهدف إلى تعطيل شبكة حاسوبية يُعتبر هجومًا بموجب القانون الدولي الإنساني، حتى وإن لم يُنتج عنه ضرر مادي مباشر، هذا التوسع في تعريف "الهجوم" يثير تساؤلات حول مدى توافقه مع المبادئ الأساسية للقانون الدولي الإنساني، مثل التمييز والتناسب.

وتُواجه تطبيق مبادئ التمييز والتناسب في الهجمات السيبرانية صعوبات تقنية وقانونية. فالهجمات السيبرانية قد تؤثر على أنظمة مدنية حيوية، مثل شبكات الكهرباء والمياه، مما يجعل من الصعب التمييز بين الأهداف العسكرية والمدنية، وتؤكد اللجنة الدولية للصليب الأحمر على ضرورة احترام مبادئ التمييز والتناسب والاحتياطات في تنفيذ العمليات السيبرانية، إلا أن التطبيق الفعلي لهذه المبادئ يُواجه تحديات كبيرة في ظل تعقيدات الفضاء السيبراني[١٣] .

وترى الباحثة، أن غموض تعريف "الهجوم" في الفضاء السيبراني يعد من أبرز التحديات القانونية التي تواجه تطبيق القانون الدولي الإنساني. فبينما يشير البروتوكول الإضافي الأول لعام ١٩٧٧ إلى أن الهجوم هو "استخدام القوة المسلحة ضد دولة أخرى"، إلا أن هذا التعريف لا يتناسب مع طبيعة الهجمات السيبرانية التي قد لا تُنتج آثارًا مادية فورية.

الفرع الثاني: التحديات التقنية في حماية البنية التحتية للبيئة الرقمية

من الناحية التقنية، تبرز صعوبات كبيرة في تقييم الأضرار الناجمة عن الهجمات السيبرانية. فالعديد من هذه الهجمات لا تُحدث تأثيرات مادية فورية، بل تؤدي إلى تعطيل الأنظمة أو فقدان البيانات، مما يجعل قياس الأضرار وتوثيقها أمرًا معقدًا. علاوة على ذلك، فإن الطبيعة العابرة للحدود للفضاء السيبراني تجعل من الصعب تحديد المسؤولية القانونية، خاصة عندما تكون الهجمات منسوبة إلى جهات غير حكومية أو مجهولة، وعليه، فإن هذه التحديات التقنية تعيق قدرة الأطراف المتنازعة على الامتثال لقواعد القانون الدولي الإنساني، وتزيد من صعوبة حماية المدنيين والبنية التحتية الحيوية[١٤] .

ومن أبرز التحديات التقنية التي تواجه حماية البنية التحتية للبيئة الرقمية في النزاعات المسلحة الآتي:

أولاً: صعوبة تحديد عزو المسؤولية في الهجمات السيبرانية العابرة للحدود

تعد الطبيعة العابرة للحدود للهجمات السيبرانية من أبرز التحديات التقنية في حماية البنية التحتية الرقمية. فالهجمات قد تُنفّذ من دول، جماعات مسلحة غير حكومية، أو حتى أفراد، مما يجعل من الصعب تحديد الجهة المسؤولة بدقة. ويواجه القانون الدولي الإنساني تحديات كبيرة في تحديد الجهة المسؤولة عن الهجمات السيبرانية، خاصةً عندما تكون الهجمات مجهولة المصدر أو تُنفّذ من قبل جهات غير حكومية. هذا الغموض في تحديد المسؤولية يُعرّض المدنيين والبنية التحتية الحيوية لمخاطر متزايدة ().[١٥]

وتعد مسألة عزو الهجوم السيبراني إلى دولة معينة من أكثر الإشكاليات تعقيدًا في النزاعات الرقمية، غير أن صعوبة التحديد التقني لمصدر الهجوم لا تعني بالضرورة غياب الإطار القانوني للمساءلة، إذ إن القانون الدولي العام، مدعومًا باجتهادات فقهية وقضائية مستقرة، قد وضع قواعد واضحة لعزو الأفعال غير المشروعة إلى الدول، حتى عندما تُنفذ بواسطة أشخاص أو جماعات غير حكومية، إذ استقر الفقه الدولي على أن مسؤولية الدولة تقوم متى نُسب إليها فعل يشكل إخلالًا بالتزام دولي [١٦]. وقد تم تقنين هذه القاعدة في مشروع مواد لجنة القانون الدولي بشأن مسؤولية الدول عن الأفعال غير المشروعة دوليًا (٢٠٠١)، الذي يُعد اليوم مرجعًا فقهيًا وقضائيًا معتمدًا.

ولا تقتصر المسؤولية الدولية على أفعال أجهزة الدولة الرسمية، بل تمتد إلى أفعال الأفراد أو الجماعات متى ثبت وجود رابطة قانونية كافية بينهم وبين الدولة[١٧] .

وفي إسناد أفعال الجهات غير الحكومية إلى الدولة ففي معيار التوجيه أو السيطرة (Direction or Control) نصت المادة (٨) من مشروع مواد المسؤولية الدولية على أن يُنسب إلى الدولة سلوك شخص أو جماعة إذا كان ذلك السلوك يتم بتوجيه أو تحت سيطرة الدولة. وقد فسّر الفقه هذا المعيار بأنه لا يشترط السيطرة المطلقة، بل يكفي أن تمارس الدولة تأثيرًا فعليًا على النشاط غير المشروع[١٨] .

ويرى ألان بيليه أن هذا المعيار يتيح إسناد الأفعال السيبرانية التي ينفذها قراصنة يعملون لصالح الدولة، أو بتكليف غير معلن منها، متى ثبت وجود توجيه عملياتي أو دعم تقني أو استخباراتي [١٩].

وقد ميّز الفقه بين السيطرة الفعالة (Effective Control)، وهو معيار صارم ارتبط باجتهاد محكمة العدل الدولية، والسيطرة العامة أو الشاملة (Overall Control)، وهو معيار أكثر مرونة تبناه جانب من الفقه، إذ يرى أنطونيو كاسيسي أن الاكتفاء بمعيار السيطرة الفعالة قد يؤدي إلى

إفلات الدول من المسؤولية في النزاعات غير التقليدية، بما فيها النزاعات السيبرانية، حيث يتم التعهيد الرقمي للهجمات[٢٠] .

في سياق الهجمات السيبرانية، يذهب الفقه الحديث إلى أن الدعم التقني، أو توفير البنية التحتية، أو الحماية القانونية، أو التغاضي المتعمد عن أنشطة القراصنة، قد يشكل قرائن كافية لعزو السلوك إلى الدولة، إذا توافرت معها عناصر التوجيه أو الإشراف، إذ يؤكد مايكل شميت أن الطبيعة السرية للعمليات السيبرانية لا تنفي المسؤولية الدولية، بل تستدعي اعتماد منهج استدلالي يقوم على تجميع القرائن القانونية والتقنية ().[٢١]

وعليه، ترى الباحثة، أن صعوبة الإسناد التقني لا تُبرر إنكار المسؤولية القانونية، إذ إن القانون الدولي يتيح، من خلال قواعد الإسناد، تحميل الدولة المسؤولية عن الهجمات السيبرانية التي تنفذها جهات غير حكومية متى ثبت التوجيه أو السيطرة أو الإخلال بواجب العناية الواجبة. ويُعد هذا الإطار ضرورة حتمية لسد الفراغ القانوني الذي أفرزته النزاعات السيبرانية الحديثة.

ثانياً: صعوبة تقييم الأضرار الناجمة عن الهجمات السيبرانية

من التحديات التقنية الأخرى، صعوبة تقييم الأضرار الناجمة عن الهجمات السيبرانية، فالعديد من هذه الهجمات لا تُحدث تأثيرات مادية فورية، بل تؤدي إلى تعطيل الأنظمة أو فقدان البيانات، مما يجعل قياس الأضرار وتوثيقها أمرًا معقدًا. اللجنة الدولية للصليب الأحمر تُؤكد على ضرورة احترام مبادئ التمييز والتناسب والاحتياطات في تنفيذ العمليات السيبرانية، إلا أن التطبيق الفعلي لهذه المبادئ يُواجه تحديات كبيرة في ظل تعقيدات الفضاء السيبراني ().[٢٢]

ويُعد مفهوم الضرر من أكثر المفاهيم إثارة للجدل عند إسقاط قواعد القانون الدولي الإنساني على الفضاء السيبراني، إذ إن الصياغة التقليدية لهذه القواعد قامت على افتراض أن الهجوم لا يتحقق إلا إذا أسفر عن تدمير مادي ملموس للأعيان أو إزهاق للأرواح. غير أن التحول إلى النزاعات السيبرانية فرض إعادة النظر في هذا الفهم، خاصة في ظل قدرة الهجمات الرقمية على تعطيل الوظائف الحيوية للأعيان دون إحداث تلف مادي مباشر، وقد استقر الفقه التقليدي على أن الهجوم، وفق المادة (٤٩) من البروتوكول الإضافي الأول لعام ١٩٧٧، يفترض استخدام وسائل قتال تؤدي إلى إلحاق أذى مادي بالأشخاص أو الأعيان. وقد انعكس هذا الفهم في تفسير مفهوم الضرر بوصفه نتيجة مادية محسوسة، كالتدمير، أو الإتلاف، أو الإضرار الفيزيائي المباشر بالبنية محل الحماية.، ويؤكد هذا الاتجاه ما أورده كل من (ساندوز وسوينارسكي وزيمرمان) في شرحهم للبروتوكول الإضافي الأول، حيث ربطوا تحقق الهجوم بوجود أثر مادي ملموس، معتبرين أن النصوص وُضعت في سياق تاريخي لم يكن يتصور أفعالًا قتالية ذات طبيعة غير مادية[٢٣] .

إلا أن الواقع العملي للنزاعات المعاصرة أظهر أن الاقتصار على الضرر المادي يفضي إلى فجوة حماية، إذ يمكن لهجوم سيبراني أن يشل مستشفى، أو شبكة كهرباء، أو نظام مياه، عبر تعطيل البيانات أو البرمجيات، دون تدمير الأجهزة المادية ذاتها. وفي هذه الحالة، تتحقق آثار إنسانية جسيمة تماثل – بل تفوق أحيانًا – آثار التدمير الفيزيائي [٢٤].

ويرى الفقيه أنطونيو كاسيسي[٢٥] أن التفسير الحرفي الضيق لمفاهيم القانون الدولي الإنساني قد يؤدي إلى إفراغها من مضمونها الإنساني، داعيًا إلى تبني تفسير غائي يراعي الهدف الأساسي المتمثل في حماية السكان المدنيين من آثار الأعمال العدائية.

كما ذهب اتجاه فقهي حديث إلى تبني المعيار الوظيفي للضرر، بحيث لا يُشترط التدمير المادي، بل يكفي أن يؤدي الهجوم إلى تعطيل الوظيفة الأساسية للعين أو حرمان المدنيين من الانتفاع بها على نحو جوهري، ووفقًا لهذا الاتجاه، فإن تعطيل نظام رقمي يدير مرفقًا حيويًا يُعد ضررًا محظورًا إذا كانت آثار التعطيل تمس المصالح الإنسانية المحمية، إذ تؤكد هيذر هاريسون دينيس أن التركيز على الأثر الوظيفي يتفق مع فلسفة القانون الدولي الإنساني، لأن الغاية ليست حماية المادة لذاتها، بل حماية الوظيفة المدنية التي تؤديها العين[٢٦].

كما يذهب مايكل شميت [٢٧] إلى أن استبعاد الضرر غير المادي من نطاق الهجوم يفتح الباب أمام التحايل على قواعد التمييز والتناسب، إذ يمكن شن هجمات سيبرانية مدمرة وظيفيًا دون تحمل أي التزام قانوني

وبذلك، يمتد مفهوم الضرر ليشمل الضرر الرقمي الوظيفي، بما ينسجم مع مبدأ التمييز وحظر استهداف الأعيان المدنية، ويحدّ من الفراغ القانوني الذي تفرضه النزاعات السيبرانية، بالتالي يتضح مما سبق، أن حصر الضرر في التدمير المادي لم يعد كافيًا في سياق النزاعات السيبرانية، وأن تبني مفهوم أوسع يشمل تعطيل الوظائف الحيوية للأعيان الرقمية يمثل استجابة فقهية منسجمة مع الغاية الإنسانية للقانون الدولي الإنساني، دون أن يستلزم تعديلًا نصيًا مباشرًا، وإنما عبر تفسير تطوري للنصوص القائمة، فالهجمات السيبرانية في النزاعات لا تقتصر على التدمير المادي، بل يمكن أن تُحدث تعطيلًا وظيفيًا واسع النطاق يلحق ضررًا فعليًا بالسكان المدنيين، ما يستدعي تحليلها في ضوء قواعد القانون الدولي الإنساني حول التمييز والتناسب، فعلى سبيل المثال، الهجوم الذي حدث على شركة الاتصالات "Kyivstar" أوكرانيا في ١٢ ديسمبر ٢٠٢٣، حيث تعرَّضت شركة الاتصالات الأوكرانية Kyivstar لهجوم سيبراني واسع النطاق، وتسبب الهجوم في تعطيل خدمات الإنترنت والاتصالات على نطاق واسع في أنحاء

أوكرانيا، مما أثر على ملايين المستخدمين المدنيين، وأدى إلى خسائر اقتصادية تزيد على ٩٠ مليون دولار للتعافي من الأضرار [٢٨].

وايضاً هجمات قرصنة على قطاع الطاقة الأوروبي والنووي (٢٠٢٤–٢٠٢٥) فبحسب تقارير تحليلية دولية فإن جماعات قرصنة متورطة في الصراع بين روسيا وأوكرانيا وعمليات أخرى قد استهدفت شركات في القطاع النووي والطاقة في بلجيكا وأماكن أخرى في ٢٠٢٤–٢٠٢٥، بما في ذلك هجمات DDoS على مواقع شركات مرتبطة بمحطات نووية [٢٩] .

وترى الباحثة، أن هذه الأمثلة تركز على الاستهداف الرقمي للبنى التحتية الحرجة للطاقة والقطاع النووي في سياقات توتر جيوسياسي، وهو مناسب لدراسة حالة تبين تداخل العمل السيبراني مع النزاعات المسلحة أو التوترات الكبرى، بالتالي تبرز هذه الأمثلة كيف يمكن أن يستهدف الهجوم الخوادم وأنظمة الاتصالات الحيوية خلال نزاع مسلح، ويُظهر الضرر الرقمي على الخدمات المدنية الأساسية، مما يجعله مهمًا في تحليل كيفية تطبيق القانون الدولي الإنساني على الضرر غير المادي.

ثالثاً: تأثير التطور السريع للتكنولوجيا على فعالية القوانين القائمة

تُواجه القوانين القائمة تحديات كبيرة في مواكبة التطور السريع للتكنولوجيا السيبرانية. فالتقنيات الحديثة مثل الذكاء الاصطناعي وإنترنت الأشياء تُستخدم بشكل متزايد في العمليات العسكرية والمدنية، مما يزيد من تعقيد تطبيق القانون الدولي الإنساني. اللجنة الدولية للصليب الأحمر تُشير إلى أن هذه التقنيات تُتيح فرصًا جديدة للعمليات العسكرية، لكنها في الوقت نفسه تُعقّد من تطبيق المبادئ الأساسية للقانون الدولي الإنساني، مثل التمييز والتناسب[٣٠] .

رابعاً: ضعف التعاون الدولي في مجال الأمن السيبراني

من التحديات التقنية الأخرى، ضعف التعاون الدولي في مجال الأمن السيبراني. فالهجمات السيبرانية غالبًا ما تكون مجهولة المصدر، مما يجعل من الصعب تحديد الجهة المسؤولة ومحاسبتها. اللجنة الدولية للصليب الأحمر تُؤكد على ضرورة تعزيز التعاون بين الدول والمنظمات الدولية في مجال الأمن السيبراني، لتطوير آليات فعّالة لحماية البنية التحتية الرقمية وضمان الامتثال للقانون الدولي الإنساني[٣١] .

الفرع الثالث: التحديات العملية والإنسانية في حماية المدنيين

على المستوى العملي، تواجه حماية المدنيين في البيئة الرقمية تحديات متزايدة. فمع تداخل الأهداف العسكرية والمدنية في الفضاء السيبراني، يصبح من الصعب تطبيق مبدأ التمييز بين الأهداف العسكرية المحمية والأعيان المدنية. كما أن الهجمات السيبرانية قد تؤثر على الخدمات

الأساسية مثل الكهرباء والمياه والاتصالات، مما يضر بالمدنيين بشكل غير مباشر. بالإضافة إلى ذلك، فإن نقص التعاون الدولي في مجال التحقيقات السيبرانية يعرقل محاسبة الجناة وضمان العدالة للضحايا. هذه التحديات العملية تتطلب تطوير آليات قانونية وتقنية فعّالة لحماية المدنيين وضمان الامتثال لقواعد القانون الدولي الإنساني في الفضاء السيبراني[٣٢] . ومن أهم هذه التحديات:

أولاً: صعوبة الفصل بين المدنيين والأهداف العسكرية

تُعتبر التحديات العملية لحماية المدنيين في النزاعات الرقمية متشابكة مع الطبيعة المتداخلة للبنية التحتية الرقمية، حيث غالبًا ما تُستخدم نفس الشبكات والخوادم لأغراض مدنية وعسكرية معًا. وفقًا للاتفاقيات الدولية، يجب على أطراف النزاع التمييز بين الأهداف العسكرية والمدنية، لكن في الواقع، يؤدي التعقيد التقني إلى صعوبة تطبيق هذا المبدأ بدقة. وتشير اللجنة الدولية للصليب الأحمر إلى أن عدم وضوح الأهداف يُعرّض المدنيين لمخاطر متزايدة، خصوصًا عند استهداف الأنظمة الرقمية التي تعتمد عليها الخدمات الأساسية مثل الطاقة والمواصلات والخدمات الصحية [٣٣] .

ثانياً: نقص الوعي والتدريب لدى الأطراف المسلحة

تشير الدراسات إلى أن العديد من الأطراف المسلحة، خاصة غير الدول، تفتقر إلى التدريب الكافي حول تطبيق القانون الدولي الإنساني في الفضاء الرقمي، مما يزيد من احتمالية استهداف المدنيين عن غير قصد. وفقًا لدراسة للأكاديمية العربية للعلوم القانونية والسياسية، فإن غياب المعرفة القانونية والتقنية يجعل من الصعب ضمان حماية المدنيين، ويستدعي تطوير برامج تدريبية متخصصة لرفع مستوى الامتثال للقواعد الإنسانية في العمليات السيبرانية[٣٤] .

ثالثاً: التأثير الإنساني غير المباشر

لا يقتصر تهديد المدنيين على الأضرار المادية المباشرة، بل يشمل أيضًا الأضرار غير المباشرة الناتجة عن تعطيل الخدمات الحيوية مثل المياه والكهرباء والصحة الرقمية. وتشير تقارير الأمم المتحدة إلى أن الهجمات السيبرانية على البنية التحتية الحيوية تزيد من الهشاشة الاجتماعية والاقتصادية، وتحد من قدرة السكان المدنيين على تلبية احتياجاتهم الأساسية، مما يضاعف العبء الإنساني للنزاعات[٣٥] .

رابعاً: صعوبة تقديم المساعدات الإنسانية

التحديات العملية تتضمن أيضًا صعوبة وصول الفرق الإنسانية إلى المناطق المتضررة بسبب هجمات رقمية تعطل نظم التواصل والمعلومات. وتوضح اللجنة الدولية للصليب الأحمر أن

تعطيل البنية التحتية الرقمية يعوق الاستجابة الإنسانية الفعالة ويؤخر تقديم المساعدات العاجلة للمدنيين، مما يجعل حماية المدنيين أكثر تعقيدًا ويستدعي تطوير آليات تكنولوجية لضمان استمرار الخدمات الأساسية حتى أثناء النزاعات [٣٦] .

المطلب الثاني: آليات حماية البيئة الرقمية وتعزيز الامتثال للقانون الدولي الإنساني

يتناول هذا المطلب الإجراءات العملية والسياسات الوقائية التي يمكن تبنيها لتعزيز حماية البيئة الرقمية، مثل وضع أطر تشريعية وطنية ودولية، اعتماد نظم مراقبة وتقييم الأضرار الرقمية، وتطوير برامج تدريبية للقوات المسلحة والمدنيين على احترام القانون الدولي الإنساني في المجال السيبراني. وعليه، تُعد البيئة الرقمية من الأعيان المدنية الحيوية التي يحميها القانون الدولي الإنساني، ويجب اتخاذ تدابير فعّالة لضمان حمايتها خلال النزاعات المسلحة. وسوف يتم تناول هذه الآليات التي تساهم في حماية البيئة الرقمية من خلال الفروع الآتية:

الفرع الأول: وضع أطر تشريعية وطنية ودولية

تعتبر التشريعات السيبرانية مكونًا أساسيًا من مكونات البيئة التنظيمية والقانونية اللازمة لتطوير مجتمع المعلومات، كما تشكل عنصرًا هامًا لتوفير الثقة بالخدمات الإلكترونية وتأمين الحماية لمستخدمي الفضاء السيبراني [٣٧] .

وقد دخلت الدول العربية مجال تشريع الفضاء السيبراني متأخرة مقارنة بالدول الغربية، وهو ما يعكس الوضع نفسه في كثير من دول العالم الجنوبي بشكل عام، خاصة أن بناء مجتمع المعلومات في هذه الدول استغرق وقتًا أطول، في حين بدأت الدول المتقدمة مسيرتها الفعلية في هذا المجال منذ مطلع التسعينات. كما أن الاعتماد على شبكات وأنظمة الحاسوب في المعاملات التجارية والإدارية وفي القطاع العام وبين الأفراد في الدول العربية ليس بنفس المستوى الذي هو عليه في الدول الصناعية والشمالية. مع ذلك، بدأ استخدام أجهزة الحاسوب وأنظمتها يزداد تدريجيًا في الدول العربية، ما أدى إلى تنامي الحاجة إلى وضع إطار قانوني ينظم استخدام هذه الأنظمة، خاصة بعد أن بدأ القطاع الخاص والأفراد في استغلال شبكة الإنترنت للقيام بالعمليات المصرفية، وإتمام المعاملات والتعاقد عن بعد، أو حتى كتابة المدونات والمحتوى الرقمي. ومن هذا المنطلق، أصبح وضع قوانين متخصصة للفضاء السيبراني ضرورة قانونية لتنظيم التعاملات بين الأفراد والمؤسسات، بما يشمل جوانب مثل الإثبات الإلكتروني، والتعاقد الرقمي، والمراسلات الإلكترونية، ومكافحة الجرائم السيبرانية[٣٨] .

وقد دأبت بعض الدراسات[٣٩] على الإشارة إلى تأخر الدول العربية في تنظيم الفضاء السيبراني، غير أن هذا التوصيف العام لا يكفي لتحقيق المنهج المقارن الدقيق، ما لم يُدعّم بتحليل نماذج

تشريعية وطنية محددة، وبيان مدى اتساقها أو تعارضها مع الالتزامات المستقرة في القانون الدولي الإنساني، ولا سيما مبدأ التمييز وحماية الأعيان المدنية المنصوص عليهما في البروتوكول الإضافي الأول لعام ١٩٧٧، ففي التشريع الأردني كنموذج عربي حديث، اتجه المشرّع، ولا سيما من خلال قانون الجرائم الإلكترونية رقم (١٧) لسنة ٢٠٢٣ المعدل، وما تبعه من تطبيقات تشريعية وتنظيمية حتى عام ٢٠٢٥، إلى معالجة الأفعال غير المشروعة في الفضاء السيبراني من زاوية الأمن الجنائي الداخلي، مع التركيز على حماية البيانات، والأنظمة المعلوماتية، والبنى الرقمية من الاعتداء غير المشروع.

إلا أن الملاحظ فقهيًا أن هذا التنظيم ظل محصورًا في الإطار الجنائي، دون أن يتوسع لمعالجة الطبيعة القانونية للهجمات السيبرانية ذات البعد العسكري أو شبه العسكري، أو ربطها صراحةً بقواعد القانون الدولي الإنساني، رغم كون الأردن دولة طرفًا في اتفاقيات جنيف وبروتوكولاتها الإضافية، إذ يذهب جانب من الفقه[٤٠] إلى أن هذا القصور التشريعي لا يُعد مخالفة مباشرة لالتزامات الأردن الدولية، بقدر ما يُعبّر عن فجوة تنظيمية، إذ إن المشرّع لم يضع معايير قانونية داخلية تُسهم في تكييف الهجمات السيبرانية أثناء النزاعات المسلحة، أو في تحديد ما إذا كانت البنية التحتية الرقمية والبيانات تدخل ضمن نطاق "الأعيان المدنية" المحمية بموجب المادة (٥٢) من البروتوكول الإضافي الأول.

في المقابل، يُظهر الإطار التشريعي العراقي – ولا سيما مشاريع وقوانين أمن المعلومات والجرائم المعلوماتية المتداولة حتى ٢٠٢٥ – توجهًا أكثر ارتباطًا بالهاجس الأمني الوطني في ظل النزاعات المسلحة التي شهدها العراق، فقد حاول المشرّع العراقي، وفقًا لما يشير إليه الفقه، الربط بين حماية الأنظمة المعلوماتية وحماية الأمن القومي، إلا أن هذا الربط جاء دون إحالة صريحة أو ضمنية إلى قواعد القانون الدولي الإنساني، ويرى الفقيه فاضل حسين الكعبي[٤١] أن التشريع العراقي، رغم إدراكه لخطورة الفضاء السيبراني في النزاعات المسلحة، لم يصل بعد إلى مرحلة دمج قواعد التمييز والتناسب في النصوص الوطنية المتعلقة بالهجمات الرقمية، الأمر الذي يحدّ من إمكانية مساءلة الأفعال السيبرانية المسلحة وفق منظور القانون الدولي الإنساني

وبمقارنة التشريعين الأردني والعراقي مع الالتزامات المقررة في القانون الدولي الإنساني، يتبيّن أن كليهما: يفتقر إلى نصوص تُكيّف صراحةً الهجمات السيبرانية أثناء النزاعات المسلحة، ولا يُحددان بشكل واضح الوضع القانوني للبنية التحتية الرقمية أو البيانات بوصفها أعيانًا مدنية أو أهدافًا عسكرية، وهو ما يتعارض، من الناحية التحليلية، مع الاتجاه الفقهي الدولي الذي يدعو إلى مواءمة التشريعات الوطنية مع قواعد حماية الأعيان المدنية، حتى في صورتها الرقمية،

باعتبار أن آثار الهجمات السيبرانية قد تمس المصالح الإنسانية ذاتها التي يسعى القانون الدولي الإنساني إلى حمايتها[٤٢].

وعليه، ترى الباحثة، أن التشريعين الأردني والعراقي يمثلان نموذجين عربيين مختلفين في المقاربة، لكنهما يشتركان في غياب الربط الصريح بين تنظيم الفضاء السيبراني وقواعد القانون الدولي الإنساني. وهو ما يستدعي، فقهيًا وتشريعيًا، الانتقال من تنظيم تقني أو أمني داخلي إلى تنظيم قانوني تكاملي يستوعب الطبيعة الخاصة للنزاعات السيبرانية، ويُفعّل الالتزامات الدولية المتعلقة بحماية الأعيان المدنية في بعدها الرقمي.

الفرع الثاني: اعتماد نظم مراقبة وتقييم الأضرار الرقمية

تُعد نظم المراقبة والتقييم الفعّالة ضرورية لتحديد مدى تأثير العمليات السيبرانية على البيئة الرقمية، وتقييم الأضرار المحتملة التي قد تلحق بالمدنيين والبنية التحتية الحيوية، تساهم هذه النظم في اتخاذ قرارات مستنيرة بشأن حماية الأعيان المدنية وضمان الامتثال لقواعد القانون الدولي الإنساني.

وتسهم أدوات الرصد المتقدمة، مثل أنظمة الكشف عن التسلل (IDS) وتحليل البيانات الضخمة، في تحديد الأنشطة السيبرانية المشبوهة وتحليلها بشكل فعّال[٤٣] . تُمكّن هذه الأدوات الجهات المعنية من التفاعل السريع مع التهديدات المحتملة، مما يقلل من الأضرار المحتملة على البيئة الرقمية. على سبيل المثال، تُستخدم هذه الأدوات في مراقبة الشبكات الحيوية مثل شبكات الطاقة والمستشفيات للكشف عن أي نشاط غير معتاد قد يشير إلى هجوم سيبراني[٤٤] ، فالتوسع في الأنشطة الدولية في المجالات التقنية الحديثة لا يعني انتقاصًا من السيادة، شريطة أن تقوم هذه الأنشطة على مبدأ التعاون الدولي الرضائي، لا على التدخل أو الإشراف القسري[٤٥] .

وعليه، فإن نظام الرصد الدولي يجب أن يُبنى على موافقة الدول المسبقة، واحترام اختصاصها الحصري في إدارة بنيتها الرقمية، وعدم منح جهة دولية صلاحيات تنفيذية مباشرة داخل الإقليم الوطني.

وإلى جانب السيادة، تبرز خصوصية البيانات بوصفها قيدًا جوهريًا على أي نظام رصد يعتمد على الذكاء الاصطناعي، خاصة إذا كان هذا الرصد يشمل تدفقات بيانات مدنية أو معلومات شخصية. وقد أكد الفقه العربي أن حماية الخصوصية لم تعد مسألة داخلية بحتة، بل أصبحت التزامًا قانونيًا ذا بعد دولي، إذ أن استخدام التقنيات الذكية في الرصد يجب أن يخضع لمبدأ التناسب، بحيث لا يتجاوز جمع البيانات الحدّ اللازم لتحقيق الغاية الأمنية المشروعة ().[٤٦]

انطلاقًا من ذلك، يمكن تطوير آلية الرصد على أسس قانونية متوازنة، وذلك عبر: الرصد غير التدخلي يقتصر دور النظام الدولي على تحليل الأنماط العامة للهجمات السيبرانية والبيانات التقنية المجرّدة (Metadata)، دون النفاذ إلى المحتوى أو البيانات الشخصية، والإشراف الوطني حيث يتم الرصد الفعلي عبر هيئات وطنية مختصة، على أن تقوم المنظومة الدولية بدور تنسيقي وتحليلي، لا دور تنفيذي مباشر[٤٧] . بالتالي، فإن اعتماد مثل هذه الضوابط يُحقق التوازن المطلوب بين متطلبات الأمن الجماعي واحترام السيادة الوطنية، ويمنع تحول التعاون التقني إلى أداة انتهاك

ويُعتبر التعاون بين الدول والمنظمات الدولية أمرًا حيويًا في مجال رصد الأضرار الرقمية. من خلال تبادل المعلومات والخبرات، يمكن تطوير استراتيجيات مشتركة للتصدي للتهديدات السيبرانية. على سبيل المثال، تُنظم ورش عمل ومؤتمرات دولية تجمع بين الخبراء من مختلف الدول لمناقشة أحدث التوجهات في مجال الأمن السيبراني وتبادل أفضل الممارسات.

ويجب أن يتم تقييم الأضرار الرقمية وفقًا لمبادئ القانون الدولي الإنساني، مثل التناسب والتمييز. يُساعد ذلك في تحديد ما إذا كانت العمليات السيبرانية تتماشى مع القواعد القانونية الدولية، وتحديد المسؤوليات في حالة حدوث أضرار غير مبررة. على سبيل المثال، يُمكن استخدام هذه المبادئ في التحقيق في الهجمات السيبرانية التي تستهدف البنية التحتية المدنية وتقييم ما إذا كانت هذه الهجمات متناسبة مع الأهداف العسكرية المرجوة ().[٤٨]

ويُعتبر التدريب المستمر للكوادر البشرية على استخدام نظم المراقبة والتقييم أمرًا أساسيًا لضمان فعالية هذه النظم. يجب أن يشمل التدريب فهمًا عميقًا للتقنيات المستخدمة، بالإضافة إلى المعرفة بالقوانين واللوائح المتعلقة بالأمن السيبراني. على سبيل المثال، تُنظم دورات تدريبية متخصصة للمتخصصين في تكنولوجيا المعلومات والقانونيين العاملين في مجال الأمن السيبراني لتعزيز مهاراتهم وقدراتهم في هذا المجال ().[٤٩]

ويجب أن يتضمن تقييم الأضرار الرقمية تحليلًا لتأثير الهجمات السيبرانية على حقوق الإنسان، مثل الحق في الخصوصية والحق في الوصول إلى المعلومات. يساعد ذلك في ضمان أن استراتيجيات الحماية الرقمية لا تنتهك الحقوق الأساسية للأفراد. على سبيل المثال، يُمكن إجراء دراسات لتقييم كيفية تأثير الهجمات السيبرانية على حرية التعبير والوصول إلى المعلومات في مناطق النزاع[٥٠] .

وعليه، ترى الباحثة، أنه ومن خلال تنفيذ هذه الآليات، يمكن تعزيز حماية البيئة الرقمية وضمان الامتثال لقواعد القانون الدولي الإنساني، مما يسهم في تقليل الأضرار على المدنيين والبنية التحتية الحيوية خلال النزاعات المسلحة.

الخاتمة

ختامًا، يمكن القول إن القانون الدولي الإنساني يمثل الإطار الأبرز لضمان حماية البنى التحتية الرقمية خلال النزاعات المسلحة، إذ يسعى إلى تكييف مبادئه التقليدية — ولا سيما مبادئ التمييز، والتناسب، والضرورة العسكرية — لتواكب طبيعة الفضاء السيبراني ومخاطره المستجدة. ومع أن النصوص الدولية الحالية، مثل اتفاقيات جنيف والبروتوكولات الإضافية، لم تتناول صراحةً الأعيان الرقمية، إلا أن التفسيرات الحديثة والاجتهادات الفقهية والعملية الصادرة عن اللجنة الدولية للصليب الأحمر (ICRC) أكدت ضرورة إدراج البنى الرقمية ضمن نطاق الأعيان المدنية التي يجب حمايتها من الهجمات. وتبقى الحاجة ملحة اليوم لوضع أطر قانونية دولية محدثة تُعالج الثغرات التقنية والقانونية التي يثيرها المجال الرقمي، بما يضمن استمرارية الخدمات المدنية وحماية الخصوصية الرقمية والبيانات الحيوية في أوقات النزاع، ويعزز من فاعلية القانون الدولي الإنساني في مواجهة التحديات السيبرانية المستقبلية.

وفي نهاية هذا البحث تم التوصل إلى عدد من النتائج والتوصيات.

اولاً: النتائج

١.توصل البحث إلى أن البنية التحتية الرقمية لم تعد تُفهم بوصفها مجرد أدوات تقنية، بل تشمل منظومة متكاملة من العناصر المادية (كالخوادم، ومراكز البيانات، وشبكات الطاقة والاتصالات) والعناصر غير المادية (كالبرمجيات والبيانات والأنظمة التشغيلية) التي تقوم عليها الخدمات الأساسية للمجتمع المدني، وعلى الصعيد القانوني، يبيّن البحث أن البنية التحتية الرقمية، في شقها المادي، تندرج دون إشكال ضمن مفهوم الأعيان وفق المادة (٥٢) من البروتوكول الإضافي الأول لعام ١٩٧٧، في حين لا يزال توصيف البيانات الرقمية محل خلاف فقهي، بين اتجاه يربط الحماية بالطبيعة المادية، وآخر يتبنى معيار الوظيفة والأثر الإنساني. كما يخلص البحث إلى أن النطاق القانوني للبنية التحتية الرقمية في ظل القانون الدولي الإنساني غير مكتمل، ويعتمد حاليًا على التفسير الفقهي والاجتهادي أكثر من اعتماده على نصوص صريحة.

٢.اثبتت الدراسة أن مبادئ القانون الدولي الإنساني التقليدية، وعلى رأسها مبدأ التمييز، قابلة من حيث المبدأ للتطبيق على البنى التحتية الرقمية، متى ثبت أن الهجوم السيبراني يُحدث آثارًا تماثل آثار الهجمات الحركية التقليدية، غير أن التطبيق العملي لهذه المبادئ يواجه صعوبات جوهرية،

أبرزها ازدواجية الاستخدام (مدني/عسكري) للبنية التحتية الرقمية، مما يُعقّد عملية تحديد الهدف العسكري المشروع، وأن مبدأ التناسب يكتسب أهمية خاصة في الهجمات السيبرانية، نظرًا لقدرة هذه الهجمات على إحداث أضرار واسعة النطاق وغير متوقعة في الخدمات المدنية الأساسية، أما مبدأ الاحتياط، فيُعد من أكثر المبادئ قابلية للتفعيل في المجال السيبراني، لكنه يتطلب التزامًا تقنيًا وقانونيًا عاليًا من أطراف النزاع لتقدير الآثار غير المباشرة للهجمات الرقمية.

٣.إن اتفاقيات جنيف وبروتوكولاتها الإضافية لم تُصغ في الأصل لمواجهة الهجمات السيبرانية، وهو ما يجعلها غير كافية بذاتها لتوفير حماية فعّالة ومباشرة للبنى التحتية الرقمية، ومع ذلك، يتضح أن هذه النصوص تظل قابلة للتطبيق عبر التفسير التطوري والغائي، بما يسمح بمدّ الحماية إلى الأعيان الرقمية متى ترتب على استهدافها آثار إنسانية جسيمة، كما أن النصوص الحالية تؤسس حماية غير مباشرة، لكنها لا تسد الفراغ القانوني القائم، ما يستدعي تدخلًا تشريعيًا دوليًا أو إقليميًا أكثر تخصّصًا.

٤.بيّن البحث أن أبرز التحديات القانونية تتمثل في: صعوبة إسناد الهجوم السيبراني إلى دولة معينة، وغموض توصيف الضرر الرقمي وحدود اعتباره هجومًا مسلحًا، وضعف المواءمة بين التشريعات الوطنية والقواعد الدولية، كما أن التحديات التقنية، كإخفاء المصدر، وسرعة تنفيذ الهجمات، وتعقيد الأنظمة الرقمية، تُضعف من فعالية تطبيق قواعد القانون الدولي الإنساني، بالتالي، فإن استمرار هذه التحديات دون معالجة قانونية واضحة من شأنه أن يُبقي المدنيين والبنى الحيوية الرقمية في دائرة خطر قانوني غير مغطّى بالكامل.

ثانياً :التوصيات

في ضوء النتائج السابقة توصي الدراسة بالآتي:

١.توصي الدراسة بضرورة تطوير صك دولي خاص أو بروتوكول إضافي مكمّل لاتفاقيات جنيف، يُعنى بتنظيم العمليات السيبرانية أثناء النزاعات المسلحة، ويتضمن تعريفًا دقيقًا للبنية التحتية الرقمية ونطاق حمايتها، مع مراعاة طبيعتها المزدوجة (المدنية والعسكرية).

٢.تؤكد الدراسة على ضرورة توسيع مفهوم الضرر في القانون الدولي الإنساني ليشمل الضرر الرقمي غير المادي متى ترتب عليه تعطيل واسع أو طويل الأمد للخدمات الأساسية، بما يحقق حماية فعّالة للمدنيين.

٣.توصي الدراسة بوضع إطار قانوني دولي واضح لإسناد الهجمات السيبرانية، يستند إلى قرائن تقنية وقانونية مشتركة، ويُحمّل الدولة المسؤولية عن أفعال الجهات غير الحكومية التي تعمل بتوجيه أو سيطرة فعلية منها، وفق قواعد المسؤولية الدولية، بالإضافة إلى تعزيز دور القضاء

الدولي وآليات التحقيق الدولية المستقلة في فحص الانتهاكات السيبرانية الجسيمة، بما يحدّ من إفلات الفاعلين من المسؤولية القانونية.

٤.توصي الدراسة إنشاء آلية دولية للرصد السيبراني تعتمد تقنيات الذكاء الاصطناعي، على أن تُدار تحت مظلة دولية محايدة، مع وضع ضوابط قانونية صارمة تضمن احترام سيادة الدول وخصوصية البيانات وعدم إساءة استخدام المعلومات المرصودة.

٥.تؤكد الدراسة على أهمية مواءمة التشريعات الوطنية مع مبادئ القانون الدولي الإنساني في المجال السيبراني، من خلال تجريم الهجمات الرقمية التي تستهدف البنى التحتية المدنية أثناء النزاعات المسلحة، وفرض عقوبات رادعة عليها.

الهوامش

(١) غسان قاسم داود اللامي، "تحليل مكونات البنية التحتية لتكنولوجيا المعلومات: دراسة استطلاعية في بيئة عمل عراقية"، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد الخاص بمؤتمر الكلية، ٢٠١٣، ص ١٤.

(٢) المادة (٥٢) من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام ١٩٤٩، والمتعلق بحماية ضحايا المنازعات المسلحة الدولية، ١٩٧٧.

(3) International Committee of the Red Cross, Commentary on the Additional Protocols, 1987, available at: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/commentary.

(4) Heather Harrison Dinniss, Cyber Warfare and the Laws of War, Cambridge University Press, 2012, p. 11.

(5) Michael N. Schmitt, "Cyber Operations and the Jus in Bello", International Law Studies, Vol. 87, 2011, available at: https://digital-commons.usnwc.edu/ils/vol87/iss1/6.

(٦) موسى بن تغري، "الحرب السيبرانية والقانون الدولي الإنساني"، مجلة الاجتهاد القضائي، جامعة محمد خيضر – بسكرة، المجلد ١٢، العدد ٢، ٢٠٢٠، ص ١٩٩–٢١٨.

(7) Ori Pomson, "'Objects'? The Legal Status of Computer Data under International Humanitarian Law", Journal of Conflict and Security Law, Vol. 28, No. 2, 2023, pp. 349-387.

(٨) ناجي محمد أسامة الشاذلي، "الجوانب القانونية للحرب السيبرانية: دراسة في إطار القانون الدولي الإنساني"، مجلة روح القانون، جامعة طنطا، المجلد ٣٥، العدد ١٠٣، ٢٠٢٣، ص ١٢٢٦–١٢٨٦.

(٩) محمد صبحي حسن علي محمد وأمل عمرو عبد الغني، "القانون الدولي الإنساني والحرب السيبرانية في النزاعات المسلحة غير الدولية: الأطر القانونية والتحديات"، المجلة القانونية الاقتصادية، جامعة الزقازيق، المجلد ٣٥، العدد ٤٤، ٢٠٢٣، ص ٥٣٤–٥٨٤.

(١٠) عبد الكريم علوان، الوسيط في القانون الدولي العام، دار الثقافة، عمّان، ٢٠١٨، ص ٥١٧.

(١١) إسماعيل براهيمي، "الهجمات السيبرانية بين التحديات القانونية والأخلاقية والاستجابات الدولية"، مجلة المعيار، المجلد ١٥، العدد ٢، ٢٠٢٤، ص ٤٠٤.

(١٢) المعهد الدولي للقانون العسكري، "التحديات القانونية في تطبيق القانون الدولي الإنساني على الهجمات السيبرانية"، مجلة القانون الدولي الإنساني، العدد ١٥، ٢٠٢٣.

(١٣) حميد سالم الكندي، "أثر التكنولوجيا الحديثة على مبدأ التناسب في القانون الدولي الإنساني"، مجلة العلوم القانونية والسياسية، العدد ١، ٢٠٢٣، ص ٧٦.

(١٤) أحمد أجعون، المستحدث في القانون الرقمي والذكاء الاصطناعي، ج ١، دار الآفاق المغربية، الدار البيضاء، ٢٠٢٣، ص ٩١.

(١٥) سلوى يوسف عبد الهادي الإكيابي، "مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية"، المجلة الدولية للفقه والقضاء والتشريع، المجلد ٣٥، العدد ١٠١، ٢٠٢٣، ص ١٢٦٤.

(16) Ian Brownlie, Principles of Public International Law, op.cit., p. 16.

(17) Ian Brownlie, Principles of Public International Law, op.cit., p. 13.

(18) Ibid., p. 13.

(19) Alain Pellet, The Law of International Responsibility, Oxford University Press, 2010, p. 18.

(20) Antonio Cassese, International Law, Oxford University Press, 2005, p. 23.

(21) Michael N. Schmitt (General Editor), Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, pp. 26-34.

(٢٢) اللجنة الدولية للصليب الأحمر، "القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة"، ورقة موقف، جنيف، نوفمبر ٢٠١٩، https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations

(23) Yves Sandoz, Christophe Swinarski and Bruno Zimmermann, Commentary on the Additional Protocols of 1977, Martinus Nijhoff Publishers, 1987, p. 57.

(٢٤) سلوى يوسف عبد الهادي الإكيابي، مرجع سابق، ص ١٢٦٤.

(25) Antonio Cassese, International Law, op.cit., p. 10.

(26) Heather Harrison Dinniss, Cyber Warfare and the Laws of War, op.cit., p. 31.

(27) Michael N. Schmitt, "Cyber Operations and the Jus in Bello", op.cit., p. 9.

(28) "Russian Hackers Infiltrated Ukrainian Telecom Giant Months Before Cyberattack", The Record Media, retrieved June 1, 2025.

(29) "Cyber Threats Against Energy Sector Surge as Global Tensions Mount", 15 April 2025, https://www.resecurity.com/blog/article/cyber-threats-against-energy-sector-surge-global-tensions-mount

(٣٠) علاء الدين فرحات، "الحرب السيبرانية ومستقبل الأمن العالمي"، مجلة الناقد للدراسات السياسية، المجلد ٤٤، ٢٠٢٢، ص ٦٨٧.

(٣١) نسيب نجيب، "الحرب السيبرانية من منظور القانون الدولي الإنساني"، المجلة النقدية للقانون والعلوم السياسية، المجلد ٢، العدد ١، ٢٠٢١، ص ٢٢٤.

(٣٢) مركز دراسات القانون الدولي، "التحديات التقنية في حماية البيئة الرقمية"، مجلة القانون الدولي الإنساني، العدد ١٨، ٢٠٢٤، متوفر على الرابط الإلكتروني: https://unidir.org/files/2022-02/UNIDIR_International_Cooperation_Mitigate_Cyber_Operations_Critical_Infrastructure_AR.pdf

(٣٣) اللجنة الدولية للصليب الأحمر، مرجع سابق.
(34) A. Al-Shamsi, "Cyber Warfare and Civilian Protection in the Arab World", Arab Academy of Legal and Political Sciences Journal, Vol. 1, No. 2, 2021, p. 129.
(35) United Nations, Report on the Impact of Cyberattacks on Critical Infrastructure, UN Humanitarian Affairs, 2020.
(36) ICRC, Guidelines on Humanitarian Protection in Cyber Contexts, Geneva, 2022.
(٣٧) الأمم المتحدة، اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، إدارة تكنولوجيا المعلومات والاتصالات، مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية، بيروت، ٢٠١٢، متوفر على الرابط الإلكتروني: https://www.unescwa.org/sites/default/files/event/materials/Directives-Full_0.pdf اطلع عليه الاحد ٢٠٢٥/١٠/٥.
(٣٨) تهاني الظفيري، "الأمن الرقمي الدولي وحقوق الإنسان"، مجلة القانون والأعمال، جامعة الحسين الأول، العدد ١١١، ٢٠٢٤، ص ١٧٧.
(٣٩) عبد الكريم علوان، مرجع سابق، ص ٢١٩.
(٤٠) محمد عبد الحميد مهنا، القانون الدولي الإنساني، دار الجامعة الجديدة، الإسكندرية، ٢٠١٦، ص ٩٧.
(٤١) فاضل حسين الكعبي، القانون الدولي الإنساني المعاصر، دار السنهوري، بغداد، ٢٠١٩، ص ١١٤.
(42) Antonio Cassese, International Law, op.cit., p. 22.
(٤٣) مؤلف جماعي، القانون في ظل التحول الرقمي، دار السلام، الرباط، ٢٠٢٣، ص ١١٢.
(44) Mike Burgess, "Offensive Cyber and the People Who Do It", speech given to the Lowy Institute, Australian Signals Directorate, 27 March 2019, available at: www.asd.gov.au/speeches/20190327-lowy-institute-offensive-cyber-operations.htm.
(٤٥) محمد عبد الحميد مهنا، القانون الدولي العام المعاصر، دار الجامعة الجديدة، الإسكندرية، ٢٠١٧، ص ٢٢٣.
(٤٦) عبد الفتاح بيومي حجازي، حماية الحياة الخاصة في ظل ثورة المعلومات، دار الفكر الجامعي، ٢٠١٩، ص ٨١.
(٤٧) عبد الكريم علوان، مرجع سابق، ص ٢٤١.
(48) Paul M. Nakasone, Statement of General Paul M. Nakasone, Commander, United States Cyber Command, before the Senate Committee on Armed Services, 14 February 2019, available at: www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf;
(٤٩) عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مكتبة الإسكندرية، وحدة الدراسات المستقبلية، الإسكندرية، ٢٠١٦، ص ٥٥.
(50) Sergio Caltagirone, "Industrial Cyber Attacks: A Humanitarian Crisis in the Making", Humanitarian Law and Policy Blog, 3 December 2019, available at: https://blogs.icrc.org/law-and-policy/2019/12/03/industrial-cyber-attacks-crisis.

المصادر والمراجع

اولاً: الكتب

أجعون، احمد (٢٠٢٣). **المستحدث في القانون الرقمي والذكاء الاصطناعي**، ج١، دار الآفاق المغربية.

الكعبي، فاضل حسين (٢٠١٩). **القانون الدولي الإنساني المعاصر**، دار السنهوري.

حجازي، عبد الفتاح بيومي (٢٠١٩). **حماية الحياة الخاصة في ظل ثورة المعلومات**، دار الفكر الجامعي.

عبد الصادق، عادل (٢٠١٦). **أسلحة القضاء الالكتروني في ضوء القانون الدولي الإنساني**، مكتبة الاسكندرية، وحدة الدراسات المستقبلية.

علوان، عبد الكريم. (٢٠١٨). **الوسيط في القانون الدولي العام**، دار الثقافة.

مهنا، محمد عبد الحميد (٢٠١٦). **القانون الدولي الإنساني**، دار الجامعة الجديدة.

مهنا، محمد عبد الحميد (٢٠١٧). **القانون الدولي العام المعاصر**، دار الجامعة الجديدة.

مؤلف جماعي (٢٠٢٣). **القانون في ظل التحول الرقمي**، دار السلام.

ثانياً: البحوث والدوريات:

أبو النور، مصطفى السيد عبد السلام ومحمد، احمد ربيع (٢٠٢٤). مواجهة الحرب السيبرانية أثناء النزاعات المسلحة في ضوء القانون الدولي الإنساني، **مجلة كلية الشريعة والقانون بتفهنا الاشراف**، جامعة الأزهر، ٢٩(٣)، ٣٠٢٧-٣١٢٠.

الإكيابي، سلوى يوسف عبد الهادي (٢٠٢٣). مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية، **المجلة الدولية للفقه والقضاء والتشريع**، ٣٥(١٠١)، ١٢٦٤.

السيحاني، فيصل ضيف الله وغرير، احمد محمد صبحي (٢٠٢٥). آليات حماية المدنيين من الحروب السيبرانية وفقا للقانون الدولي الإنساني، **مجلة البحوث الفقهية والقانون**، ٥١(٥١)، ٣٢٢٧-٣٢٨٠.

الشاذلي، ناجى محمد اسامه (٢٠٢٣). الجوانب القانونية للحرب السيبرانية دراسة في إطار القانون الدولي الإنساني، مجلة روح القانون، ٣٥(١٠٣)، ١٢٢٦-١٢٨٦.

الظفيري، تهاني (٢٠٢٤). الأمن الرقمي الدولي وحقوق الإنسان، مجلة القانون والأعمال، العدد (١١١).

الكندي، حميد سالم (٢٠٢٣). اثر التكنولوجيا الحديثة على مبدأ التناسب في القانون الدولي الإنساني، مجلة العلوم القانونية والسياسية، (١).

اللامي، غسان قاسم داود (٢٠١٣). تحليل مكونات البنية التحلية لتكنولوجيا المعلومات، دراسة استطلاعية في بيئة عمل عراقية، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد الخاص بمؤتمر الكلية.

المعهد الدولي للقانون العسكري، (٢٠٢٣)، التحديات القانونية في تطبيق القانون الدولي الإنساني على الهجمات السيبرانية، مجلة القانون الدولي الإنساني (١٥).

براهيمي، إسماعيل (٢٠٢٤). الهجمات السيبرانية بين التحديات القانونية والأخلاقية والاستجابات الدولية، **مجلة المعيار**.15(2) .

بن تغري، موسى (٢٠٢٠). الحرب السيبرانية والقانون الدولي الإنساني، **مجلة الاجتهاد القضائي**، ١٢(٢)، ١٩٩-٢١٨.

فرحات، علاء الدين (٢٠٢٢). الحرب السيبرانية ومستقبل الأمن العالمي، مجلة الناقد للدراسات السياسية، ٤٤.
محمد، صبحي حسن علي محمد وعبد الغني، أمل عمرو (٢٠٢٣)، القانون الدولي الإنساني والحرب السيبرانية في النزاعات المسلحة غير الدولية، المجلة القانونية الاقتصادية (44)35 ..584-534
نجيب، نسيب (٢٠٢١)، الحرب السيبرانية من منظور القانون الدولي الإنساني، المجلة النقدية للقانون والعلوم السياسية(1)2 .

ثالثاً: المواقع الالكترونية:

الأمم المتحدة، اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، إدارة تكنولوجيا المعلومات والاتصالات. (٢٠١٢)، مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية. متوفر على الرابط الالكتروني: https://www.unescwa.org/sites/default/files/publications/full-pdf_0.pdf اطلع عليه الاحد ٢٠٢٥/١٠/٥.

البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام ١٩٤٩ والمتعلق بحماية ضحايا المنازعات المسلحة الدولية(1977) ، المادة ٥٢ .

اللجنة الدولية للصليب الأحمر، "القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة"، ورقة موقف، جنيف، نوفمبر ٢٠١٩ https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations.

مركز دراسات القانون الدولي، (٢٠٢٤). التحديات التقنية في حماية البيئة الرقمية، مجلة القانون الدولي الإنساني (١٨)، متوفر على الرابط الالكتروني: https://unidir.org/files/Critical_Infrastructure_AR.pdf

المراجع الأجنبية:

Al-Shamsi, A. (2021). Cyber Warfare and Civilian Protection in the Arab World, Arab Academy of Legal and Political Sciences Journal, 1(2), p129.

Antoniuk, D. (2024, January 4). *Russian hackers infiltrated Ukrainian telecom giant months before cyberattack*. The Record.

Biggio, G. (2025). Regulating non-kinetic effects of cyber operations: the 'Loss of Functionality' approach and the military necessity-humanity balance under International Humanitarian Law, Journal of Conflict and Security Law, 30(2), 241-263.

Brownlie, I. (2008). Principles of Public International Law, Oxford University Press.

Burgess, M. (2019, March 27). *Offensive cyber and the people who do it* [Speech]. Australian Signals Directorate, available at: www.asd.gov.au/speeches/20190327-lowy-institute-offensive-cyber-operations.htm.

Caltagirone, S., Industrial Cyber Attacks: A Humanitarian Crisis in the Making", Humanitarian Law and Policy Blog, 3 December 2019, available at: https://blogs.icrc.org/law-and-policy/2019/12/03/industrial-cyber-attacks-crisis.

Cassese, A. (2005). International Law, Oxford University Press, 10.

Dinniss, H. H., (2012). Cyber Warfare and the Laws of War, Cambridge University Press.

International Committee of the Red Cross. (1987). *Commentary on the Additional Protocols*, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/commentary.
International Committee of the Red Cross. (2022). *Guidelines on humanitarian protection in cyber contexts*.
Kumar, S., Niranjan, M., Nagar, G., Peddoju, S. K., & Tripathi, K. (2025). Humanizing cyber war: A Geneva Conventions-based framework for cyber warfare. *Proceedings of the 20th International Conference on Cyber Warfare and Security, 20*(1), 179–187
Nakasone, P. M. (2019, February 14). *Statement of General Paul M. Nakasone, Commander, United States Cyber Command, before the Senate Committee on Armed Services* [Testimony]. U.S. Senate Committee on Armed Services, available at: www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf;
Pellet, A. (2010). The Law of International Responsibility, Oxford University Press.
Pomson, O., (2023). The Legal Status of Computer Data under International Humanitarian Law, Open Access, Journal of Conflict and Security Law, 28(2), 349–387.
Resecurity. (2025, April 15). *Cyber threats against energy sector surge as global tensions mount*, https://www.resecurity.com/blog/article/cyber-threats-against-energy-sector-surge-global-tensions-mount.
Sandoz, Y.; Swinarski, C.; Zimmermann, B. (1987). Commentary on the Additional Protocols of 1977, Martinus Nijhoff Publishers.
Schmitt, M. N. (2011). Cyber Operations and the Jus in Bello, International Law Studies, 87(6), https://digital-commons.usnwc.
Schmitt, M. N. (General Editor), Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013.
United Nations Office for the Coordination of Humanitarian Affairs. (2020). *Report on the impact of cyberattacks on critical infrastructure*.

Sources and References

First: Books

Ajjoun, Ahmed (2023). Modern Developments in Digital Law and Artificial Intelligence, Vol. 1, Dar Al-Afaq Al-Maghribiya.
Al-Kaabi, Fadel Hussein (2019). Contemporary International Humanitarian Law, Dar Al-Sanhouri.
Hijazi, Abdel Fattah Bayoumi (2019). Protecting Privacy in the Information Revolution, Dar Al-Fikr Al-Jami'i.
Abdel Sadek, Adel (2016). Weapons of Electronic Justice in Light of International Humanitarian Law, Bibliotheca Alexandrina, Future Studies Unit.
Alwan, Abdel Karim (2018). The Intermediate in Public International Law, Dar Al-Thaqafa.
Muhanna, Mohamed Abdel Hamid (2016). International Humanitarian Law, Dar Al-Jami'a Al-Jadeeda.
Muhanna, Mohamed Abdel Hamid (2017). Contemporary Public International Law, Dar Al-Jami'a Al-Jadeeda.
Collective work (2023). Law in the Digital Age, Dar Al-Salam.

Second: Research and Periodicals:

Abu Al-Nour, Mustafa El-Sayed Abdel Salam and Mohamed, Ahmed Rabie (2024). Confronting Cyber Warfare During Armed Conflicts in Light of International Humanitarian Law, Journal of the Faculty of Sharia and Law, Tafahna Al-Ashraf, Al-Azhar University, 29(3), 3027-3120.

Al-Akyabi, Salwa Yousef Abdel-Hadi (2023). The Applicability of International Humanitarian Law to Cyber Attacks, International Journal of Jurisprudence, Judiciary and Legislation, 35(101), 1264.
Al-Sihani, Faisal Dhaifallah and Ghurair, Ahmed Mohamed Sobhi (2025). Mechanisms for Protecting Civilians from Cyber Warfare According to International Humanitarian Law, Journal of Jurisprudence and Law Research, 51(51), 3227-3280.
Al-Shazly, Naji Mohamed Osama (2023). The Legal Aspects of Cyber Warfare: A Study within the Framework of International Humanitarian Law, Journal of the Spirit of Law, 35(103), 1226-1286.
Al-Dhafeeri, Tahani (2024). International Digital Security and Human Rights, Journal of Law and Business, Issue (111.(
Al-Kindi, Hamid Salem (2023). The Impact of Modern Technology on the Principle of Proportionality in International Humanitarian Law, Journal of Legal and Political Sciences, (1.(
Al-Lami, Ghassan Qasim Dawood (2013). Analysis of the Components of the Local Infrastructure of Information Technology: An Exploratory Study in an Iraqi Work Environment, Journal of Baghdad College of Economic Sciences University, Special Issue for the College Conference.
International Institute of Military Law, (2023). Legal Challenges in Applying International Humanitarian Law to Cyber Attacks, Journal of International Humanitarian Law (15.(
Brahimi, Ismail (2024). Cyber Attacks Between Legal and Ethical Challenges and International Responses, Al-Mi'yar Journal, 15(2.(
Ben Taghri, Moussa (2020). Cyber Warfare and International Humanitarian Law, Journal of Judicial Reasoning, 12(2), 199-218.
Farhat, Alaa El-Din (2022). Cyber Warfare and the Future of Global Security, Al-Naqid Journal for Political Studies, 44.
Mohammed, Sobhi Hassan Ali Mohammed and Abdel-Ghani, Amal Amr (2023), International Humanitarian Law and Cyber Warfare in Non-International Armed Conflicts, Economic Legal Journal, 35(44), 534-584.
Najib, Nassib (2021), Cyber Warfare from the Perspective of International Humanitarian Law, Al-Naqd Journal of Law and Political Science, 2(1.(

Third: Websites:

United Nations, Economic and Social Commission for Western Asia (ESCWA), Information and Communication Technology Division. (2012), Cyber Legislation Harmonization Project to Promote a Knowledge Society in the Arab Region. Available at: https://www.unescwa.org/sites/default/files/event/materials/Directives-Full_0.pdf. Accessed Sunday, October 5, 2025.
Additional Protocol I to the Geneva Conventions of 1949 relating to the Protection of Victims of International Armed Conflicts (1977), Article 52.
ICRC, "International Humanitarian Law and Cyber Operations in Armed Conflicts," Position Paper, Geneva, November 2019 https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations.
Center for International Law Studies, (2024). Technical Challenges in Protecting the Digital Environment, Journal of International Humanitarian Law (18), available online at: https://unidir.org/files Critical_Infrastructure_AR.pdf