**الهجمات السيبرانية من منظور القانون الدولي الإنساني**

[**العدد 114 - تشرين الأول 2020**](https://www.lebarmy.gov.lb/ar/content/114-d)

**الهجمات السيبرانية من منظور القانون الدولي الإنساني**
إعداد: الرائد حسن فياض
ضابط في الجيش اللبناني

**المقدمة**

لقد كان للحرب نصيبها الوافر من التطور التكنولوجي، إذ شهد العالم نوعًا جديدًا من سباق التسلح، الذي تحوّل إلى عنوان في العلاقات الدولية، ومقياس يقاس به توازن الردع بين الدول. لم يعد سباق التسلح اصطلاحًا عسكريًا يقوم على تكديس الطائرات أو المدافع أو الدبابات أو أسلحة الدمار الشامل فقط، بل يقوم على استحداث برامج إلكترونية مُعدة لأغراضٍ عسكرية وتطويرها تُعرف اختصارًا بالسايبر Cyber.

وقد انبثقت عن سباق التسلح نزاعات مسلحة دولية أو غير دولية كثيرة، ويرعاها القانون الدولي الإنساني، الذي صُمّم للتعامل مع أشخاص القانون الدولي التقليديين وغير التقليديين التي تستخدم وسائل وأساليب قتال تقليدية. كما أنه يجمع بين فكرتَين مختلفتَين في طبيعتهما، إحداهما قانونية والثانية أخلاقية لا سيما الإنسانية التي وجدت طريقها في هذا القانون. يتكون القانون المذكور من الأحكام القانونية الدولية كافة، سواء في التشريعات أو القوانين العامة التي تكفل احترام الفرد وتعزز رفاهه، ويهدف بدوره إلى وضع قواعد منظمة للعمليات العسكرية، وتخفيف الأضرار الناجمة عنها إلى أقصى حد تتيحه الضرورات العسكرية، من خلال تحديد حقوق المتحاربين في إدارة العمليات وتقييد اختيار وسائل القتال وأساليبها الواردة في اتفاقيات لاهاي. كما يستهدف قانون جنيف، المتجسد في اتفاقيات جنيف الأربعة لعام 1949 وبروتوكولَيها لعام 1977، حماية العسكريين العاجزين عن القتال، والأشخاص الذين لا يشتركون في العمليات الحربية.

شهد العالم عدة أجيال من الحروب لغاية تاريخه، ولكل جيل سماته من حيث أنواع الأسلحة المستخدمة، وطبيعة الخطط والتكتيكات والاستراتيجيات، وميادين المعارك وغيرها، بدءًا من الجيل الأول الذي كان يعتمد على حشد الجيوش واستخدام الأسلحة والمدافع البدائية، مرورًا بالجيل الثاني الذي يعتمد على القوة النارية من خلال حشد أكبر عدد من الجنود واستخدام المدرعات والأسلحة الآلية. ظهر الجيل الثالث من الحروب إبان الحرب العالمية الثانية (1939-1945)، إذ تميّز بالتطوّر الكبير للمدرعات والاعتماد على القوات الجوية وسرعة الحركة والمفاجأة. أما الجيل الرابع من الحروب، فيقوم على ضرب العدو من الداخل من خلال عمليات التمرد والتشجيع على الحروب الأهلية والطائفية، ليصبح المجتمع هو السلاح المستخدم لتدمير نفسه، إلى أن وصلنا إلى الجيلَين الخامس والسادس اللذين يجمعان بين الوسائل والأساليب التقليدية وغير التقليدية كحروب المعلومات والحروب السيبرانية وغيرها[[1]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn1%22%20%5Co%20%22).

تتحول الهجمات السيبرانية بشكلٍ سريع إلى نموذج جديد من الحرب الحديثة، ظهرت علنًا لأول مرة في النزاع المسلح الدولي لعام 2008 بين جورجيا وروسيا، كما استُخدمت في النزاع المسلح الدولي بين روسيا وأوكرانيا[[2]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn2%22%20%5Co%20%22)، وأيضًا في أثناء النزاعات المسلحة الدولية وغير الدولية في أفغانستان والعراق وليبيا وسوريا.

فالاستعمال المتزايد للهجمات السيبرانية في النزاعات المسلحة التي وقعت في السنوات العشرة الأخيرة، وفي ضوء معطيات مؤكدة بأن تهديدًا ستتسبب به هذه الهجمات على صعيد السلم والأمن الدوليَين، وبمستوى لا يقل جسامة عن أخطر التهديدات المعروفة دوليًا، طرح تحديات على مختلف الصعد ومنها القانونية، وبالتالي شكّل تحديًا لبعض أحكام القانون الدولي العام عمومًا والقانون الدولي الإنساني خصوصًا.

فاللجوء المتزايد للدول في استخدام الفضاء الإلكتروني لشن هجمات سيبرانية في أثناء النزاعات المسلحة، يطرح الإشكالية الأساسية حول كيفية التعامل مع الهجمات السيبرانية من منظور القانون الدولي الإنساني. إن الإشكالية القانونية التي يثيرها هذا النوع الجديد من الحروب تتلخص في الإجابة عن عدة أسئلة منها ما يتعلق بتحديد مفهوم الهجمات السيبرانية الذي سوف نتطرق إليه في المطلب الأول، والطبيعة القانونية للهجمات السيبرانية في القانون الدولي الإنساني ومدى إمكانية تطبيق قواعد القانون الدولي الإنساني ومبادئه على هذا النوع الجديد من الحروب في المطلب الثاني.

**المطلب الأول: مفهوم الهجمات السيبرانية**

تختلف الحرب السيبرانية عن الحرب التقليدية، إذ تنطوي الأخيرة على استخدام الجيوش النظامية مع إعلان مسبق للحرب وميدان قتال محدد، بينما تكون الأولى غامضة وغير محددة الأهداف كونها تتحرك عبر شبكة المعلومات الإلكترونية[[3]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn3%22%20%5Co%20%22).

ومن أجل الوقوف على مفهوم الهجمات السيبرانية، سنتطرق أولًا إلى تعريفها لغويًا، ثم إلى مصدر كلمة السيبرانية اصطلاحًا في ضوء الاجتهادات الفقهية والممارسات الدولية.

أول من أطـلق هذه التسـمية عالم الرياضيات نــوربرت وينــر Norbert Weiner في العام 1948، في أثناء دراسته لموضوع القيادة والسيطرة والاتصال في عالم الحيوان، فضلًا عن حقل الهندسة الميكانيكية. ترجع السيبرانية إلى المصطلح اللاتينـي kybernetes، ويعني القيادة أو التحكم عن بُعد[[4]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn4%22%20%5Co%20%22). وقد ورد هذا المصطلح في قاموس المورد إذ يعرّفها بالقول: السيبرانية هي علم الضبط ومصدرها، وهو مصدر يتطابق مع مفهوم الهجمات السيبرانية، أي ضبط الأشياء عن بُعد والسيطرة عليها[[5]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn5%22%20%5Co%20%22). وهي عملية انتقال أوامر شفهية أو غير مرئية إلى حقيقة واقعة مادية.

أما من حيث المعنى الاصطلاحي للهجمات السيبرانية: فهي مجموعة من الأنشطة الإلكترونية التي تتخذ من طرف سواء أكان تابعًا لدولةٍ أم يعمل لحسابها بصورةٍ مستقلة عنها في الدولة (أ)، ضد نُظم إلكترونية تابعة لطرف (ب) في دولة أخرى، يُراد منها التغلغل إلى تلك النُظم بهدف السيطرة على قوّتها الإلكترونية ومن ثم التحكم بها عن بُعد، لأجل إحداث أكبر قدر ممكن من الأضرار.

ووفق دليل تالين المطبّق على الحرب السيبرانية في العام 2013، الذي أعدّته مجموعة من الخبراء في القانون الدولي الإنساني أبرزهم الأستاذ مايكل شيمت بالتعاون مع حلف شمال الأطلسي، وبدعمٍ من فريق مؤلف من خبراء السيبرانية، واللجنة الدولية للصليب الأحمر والقيادة السيبرانية الأميركية الذين شاركوا في المداولات كافة، عرّف الهجمات السيبرانية بأنها: «عمليات سيبرانية، سواء أكانت هجومية أم دفاعية، والتي يهدف من خلالها بصورةٍ معقولة التسبب بالإصابة أو وفاة الأشخاص أو الأضرار أو تدمير الأعيان الأهداف». ووفق هذا التعريف الوارد في الدليل المذكور أعلاه، فقد اتفق معظم الفقهاء القانونيين على أنه قد يتحقق الضرر أيضًا بتوقف أحد الأعيان عن العمل، علاوة على الضرر المادي، وليس من المهم كيف يحدث ذلك.

كما عرّفها مايكل شميت على أنها: «مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نُظم المعلومات المعادية بهدف التأثير والإضرار بها، وفي الوقت نفسه للدفاع عن نُظم المعلومات الخاصة بالدولة المهاجمة»[[6]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn6%22%20%5Co%20%22).

واستنادًا إلى التعاريف السابقة، هناك ثلاثة معايير مجتمعة تشكل نواة معيار الضرر:

١- أضرار واسعة النطاق.

٢- أن تكون طويلة الأمد أي آثارها تستغرق فترة زمنية.

٣- أن تكون بغرضٍ، أي عملية استخدام هذا السلاح أو هذه الوسيلة من أجل أن يكون واسع النطاق وطويل الأمد.

تتميز الهجمات السيبرانية بأنها تتم بواسطة شخص أو أكثر باستخدام جهاز كمبيوتر مزوّد بعددٍ كبير من الفيروسات، ويتم إرسالها إلى الهدف المراد إلحاق الضرر به، ويمكن أن يكون الضرر ماديًا أو معنويًا. وعليه، فإن الهجمات السيبرانية ليست سلاحًا تقليديًا، ولا ترقى لأن تكون سلاح دمار شامل وذلك نظرًا للأضرار الناتجة عنها. ونظرًا لأهميتها في النزاعات المسلحة، والأضرار المتوقعة من جرائها، عُقدت مباحثات بين أميركا وروسيا لوضع قيود لاستخدام هذا النوع من الأسلحة، إذ نادت أميركا بتقييده، بينما كانت روسيا مع حظره، وبالنهاية لم يتم التوصل إلى قواعد مشتركة.

أما من منظور القانون الدولي الإنساني فتثير الهجمات السيبرانية التساؤل الآتي: «هل هي وسيلة أم أسلوب قتال؟».

قبل شرح الهجمات السيبرانية، لا بد من الإضاءة على معنى الهجوم في العمليات السيبرانية إذا استُخدمت لأغراضٍ عسكرية. عرّف البروتوكول الإضافي الأول لعام 1977 الملحق باتفاقيات جنيف الأربعة لعام 1949 في الفقرة ١ من المادة 49 بأن: «الهجوم هو أعمال العنف الهجومية أو الدفاعية ضد الخصم».

لقد كان هذا التعريف كافيًا في عصر كانت فيه الهجمات تُنفّذ بالوسائل التقليدية، لأن هذه الوسائل عنيفة بطبيعتها. أما العمليات السيبرانية معقّدة كونها تفي بالغاية العسكرية المطلوبة من دون التسبب بآثارٍ مدمرة أو ضارة أحيانًا.

بعد نقاش طويل في تعريف الهجوم في سياق العمليات السيبرانية، انقسم خبراء القانون الدولي الإنساني بين مؤيد لنهجٍ يقصر نطاق الهجمات على العمليات العسكرية التي تؤدي إلى أضرار وإصابة[[7]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn7%22%20%5Co%20%22)، إذ يركّز هؤلاء على المعنى الواضح للنص، وبين مؤيد لمفهومٍ أوسع للهجمات لبعض العمليات غير المدمرة أو غير الضارة[[8]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn8%22%20%5Co%20%22). ويتبين لنا أن للنهجَين نقاط قوة ونقاط ضعف، ولم يستطع أي منهما الحصول على الدعم الكلي أو الإجماع من قبل الخبراء الدوليين. لكن تم التوصل بين الفريقَين إلى قاعدة مفادها: «إن العملية السيبرانية، سواء في الهجوم أو في الدفاع، التي يُتوقع منها أن تسبب إصابة أو وفاة للأشخاص أو إلحاق الضرر أو تدمير الأشياء، تعد بمثابة هجوم». طبعًا الحد الأدنى من الضرر أو التدمير لا يفي بهذا المفهوم.

وفي الإطار عينه، رأى بعض الخبراء أنه نظرًا لعدم وجود ممارسات دولية بشأن الاعتماد على تعريف موحد «للهجوم» في العمليات السيبرانية، فإن القانون الحالي يقصر المصطلح على الأذى الجسدي الذي يلحق بالأشخاص والضرر الذي يلحق بالأشياء المادية. فبالنسبة لهم، تعد العملية السيبرانية بمثابة هجوم تتطلب إصلاحًا للبنية السيبرانية المستهدفة بهذه العملية[[9]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn9%22%20%5Co%20%22).

فمن خلال قراءة التعاريف السابقة، وللتمييز سواء أكانت الهجمات السيبرانية وسيلة أم أسلوب قتال، يجب معرفة الهدف من استخدامها. ففي العام 2007، قام العدو الإسرائيلي بواسطة سلاحه الجوي بهجومٍ على موقع سوري يُشتبه بأنه مفاعل نووي، والذي تزامن معه قيام العدو الإسرائيلي بهجماتٍ سيبرانية على أجهزة الرادار والاتصال في وزارة الدفاع وباقي منظومات الاتصال في المطارات العسكرية والمدنية، أدت إلى تعطيلها عن العمل بالكامل. ففي هذه الحالة، يعد الهجوم السيبراني أسلوب قتال لأنه يدخل ضمن الخطط العسكرية، وساعدت في تحسين أداء العمليات العسكرية التقليدية وتوافر الدعم اللازم في إنجازها[[10]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn10%22%20%5Co%20%22).

في المقابل، قد تكون الهجمات السيبرانية وسيلة قتال من خلال استخدامها بذاتها، للتسلل إلى أنظمة إلكترونية معدّة لحماية سير عمل منشآت حيوية أو لتنظيمها، كمحطات توليد الطاقة النووية أو السدود أو وسائل نقل كالمطارات، بهدف تطويعها والسيطرة عليها، لتدمير ذاتها بذاتها من خلال تغذيتها بمعلوماتٍ خاطئة لأجهزة التحكم والحماية الإلكترونية. والمثال على ذلك ما تعرضت له محطة نطانز لتوليد الطاقة النووية الإيرانية من هجوم سيبراني من قبل الولايات المتحدة الأميركية في العام 2011، باستخدام برنامج stuxnet الذي عطّل العمليات الحساسة وألحق أضرارًا جزئية في عمليات تخصيب اليورانيوم[[11]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn11%22%20%5Co%20%22).

فالتمييز بين أن تكون الهجمات السيبرانية وسيلة أو أسلوب قتال، برأينا يعتمد على الهدف من استخدامها والنتيجة المتوقعة منها، فإذا تسببت بشكلٍ مباشر أو غير مباشر بقتلٍ أو جرح أو تدمير أو تعطيل كلي أو جزئي، تعد وسيلة قتال، أما إذا استُخدمت كجزءٍ من مخطط عسكري فتعد أسلوب قتال. وخلاصة ما تقدّم، يتبين أنها وسيلة وأسلوب قتال في الوقت نفسه، وفق الهدف من استعمالها.

عرف العالم مع ظهور هذا النوع الجديد من الحروب عدة نماذج، سوف نذكر بعضًا منها وثّقها بعض المختصين في هذا المجال:

في العام 2007، تعرضت أستونيا، إحدى جمهوريات الاتحاد السوفياتي السابق، إلى هجمات سيبرانية متلاحقة أدت إلى التعطيل الكامل لشبكات الاتصال فيها، شملت مواقع رسمية حساسة لرئيس الوزراء ورئيس البرلمان والوزراء الأستونيين. وقد وجّهت أستونيا الاتهام إلى روسيا الاتحادية باعتبار أن الهجمة السيبرانية التي قامت بها الأخيرة ليست إلا عملية انتقامية لما قامت به أستونيا بنقل نصب تذكاري يخلّد الجيش الروسي من العاصمة تالين إلى مكان مجهول[[12]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn12%22%20%5Co%20%22).

والمثال الآخر على الهجمات السيبرانية هو النزاع الروسي الجورجي في العام 2008، والذي أدى إلى تعطل نظام الاتصال الإلكتروني(IT) للقوات الجورجية بالكامل قبل بدء العمليات القتالية بيومٍ واحد، وبخاصةٍ في إقليم أوسيتيا عقب إعلان انفصاله عن جورجيا[[13]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn13%22%20%5Co%20%22)، ما أضعف وسائل الدفاع الجوية الجورجية، فضلًا عن تعرّض وسائل الإعلام والبنى التحتية وأهمها قطاع المواصلات لهجماتٍ سيبرانية أيضًا.

قد يتم إطلاق هذا النوع من الهجمات السيبرانية بعيدًا عن ساحات القتال، ما يثير مخاوف عن الحدود العملية والمعيارية لتصنيف نزاع على أنه نزاع مسلح. فالقدرة على إخفاء نقطة انطلاق أو أصل الهجمة السيبرانية يعقد خيارات الرد لأولئك المستهدفين، فضلًا عن أنها يمكن أن تؤدي إلى آثار مدمرة أو ضارة بالسكان المدنيين.

وبالتالي، فإن رسم خط واضح يفصل بين الحالات التي تمثّل نزاعًا مسلحًا والحالات التي لا تمثّله لم تكن بالمهمة اليسيرة على الإطلاق في الحروب التقليدية، فكيف يمكن أن تكون عليه في هذا النوع الجديد من الحروب وبخاصةٍ في استعمال الهجمات السيبرانية، لأن هذه المسائل تؤثّر تأثيرًا كبيرًا على إمكانية تطبيق القانون الدولي الإنساني، وتؤدي إلى مزيد من الصعوبة في تصنيف النزاعات.

تخضع العمليات السيبرانية المستخدمة خلال النزاع المسلح إلى القانون المطبّق على النزاعات المسلحة الدولية أو غير الدولية[[14]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn14%22%20%5Co%20%22). هذا يطرح السؤال الآتي: هل يمكن في أي نوع من النزاعات المسلحة أن تقتصر العمليات على التبادل السيبراني فقط؟

النزاع المسلح الدولي هو نزاع مسلح بين دولتَين أو أكثر، إذ يتطلب اللجوء إلى القوة المسلحة بين الدول[[15]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn15%22%20%5Co%20%22). فقد اقترحت المحكمة الجنائية الدولية ليوغوسلافيا السابقة تعريفًا عامًا للنزاعات المسلحة الدولية في قضية تاديتش، وقالت المحكمة إن «النزاع المسلح يوجد حيثما يكون هناك لجوء للقوة المسلحة بين الدول»، من دون الإشارة إلى متطلبات أخرى لتصنيف النزاع[[16]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn16%22%20%5Co%20%22). وقد أيد هذا الرأي جان بكتيه قائلًا: «إن أي خلاف ينشب بين دولتَين ويُفضي إلى تدخّل القوات المسلحة هو نزاع مسلح بالمعنى المقصود، حتى لو لم يعترف أحد الطرفَين بحالة الحرب. ولا يعوّل في هذا الصدد على المدة التي تستمر خلالها النزاعات أو عدد القتلى[[17]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn17%22%20%5Co%20%22)».

لا يوجد أساس منطقي أو قانوني لوجوب تمييز العمليات التقليدية والعمليات السيبرانية، في ما يتعلق ببدء نزاع مسلح دولي، في الحالة التي تتسبب الأخيرة فيها بعواقب مماثلة للنزاع المسلح. من الواضح أن العمليات السيبرانية لن تشكّل جميعها حالة من اللجوء إلى القوة المسلحة. ولكي تكون هناك قوة مسلحة، يجب أن تكون هناك أعمال قتالية[[18]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn18%22%20%5Co%20%22). المشكلة الأساسية تكمن في الوضع الذي لا تؤدي فيه الأنشطة السيبرانية إلى أضرار جسيمة غير مدمرة وغير ضارة. فقد أثار ذلك جدلًا واسعًا، إلا أنه يبدو، وفق تعريف الهجوم في القانون الدولي الإنساني، أن أي عملية سيبرانية ترقى لمستوى الهجوم، تعد تجاوزًا لعتبة الأعمال العدائية، علمًا أنه لغاية اليوم لم يتوصل الخبراء الدوليون إلى اتفاق بشأن مقدار الضرر أو الإصابة المطلوبَين من الهجمات السيبرانية لبدء نزاع مسلح دولي. ووفق اتفاقيات جنيف الأربعة المؤرخة في 12 آب 1949، النزاع المسلح الدولي هو «أي خلاف نشأ بين دولتَين ويؤدي إلى تدخّل القوات المسلحة فهو نزاع مسلح....لا يهم كم من الوقت يستمر النزاع أو حدة العنف. ومع ذلك، هناك بعض الخبراء تبنوا موقفًا أكثر تقييدًا يستلزم نطاقًا أوسع، أو مدة أطول أو حدة أشد».

من الصعب التكهن أي المقاربات سوف تحدد العمليات السيبرانية المطلوبة لتصنيف النزاع على أنه نزاع مسلح دولي. فمن جهة، إن الخيار الأول مفضّل من قبل الدول، لتوسيع حماية القانون الدولي الإنساني للأشخاص والأشياء التي يُحتمل أن تتأثر بالنزاع السيبراني. ومن جهة أخرى، فإن الموقف الأخير له فائدة الحد من الحالات التي توصف فيها العمليات السيبرانية بأنها نزاع مسلح دولي، وبالتالي تُجنّب عدم الاستقرار بين الدول، الذي يصاحب هذه التوصيفات.

أما بالنسبة لانطلاق العمليات السيبرانية في النزاع المسلح غير الدولي، بين جماعة مسلحة من غير الدول والقوات النظامية التابعة لدولةٍ ما، هو أمر في غاية التعقيد. على عكس النزاع المسلح الدولي، هناك عاملان واقعيان لتصنيف حالة عنف على أنها نزاع مسلح غير دولي وفق المادة الثالثة المشتركة:

أولًا: أن تظهر الأطراف المشاركة مستوىً معيّنًا من التنظيم.

ثانيًا: أن يصل العنف إلى مستوى معيّن من الحدة[[19]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn19%22%20%5Co%20%22).

لا يشمل النزاع المسلح غير الدولي الاضطرابات والتوترات الداخلية كأعمال الشغب وأعمال عنف متفرقة أو أي أعمال أخرى مشابهة، وبالتالي الأحداث السيبرانية المتفرقة، بما في ذلك تلك التي تسبب أضرارًا مادية وإصابة لا تصنف على أنها نزاع مسلح غير دولي[[20]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn20%22%20%5Co%20%22).

ونرى أنه يوجد عدة عوامل يمكن على أساسها تقييم معيار التنظيم، وفق ما أعلنته المحكمة الجنائية الدولية ليوغوسلافيا السابقة، إذ تتضمن هذه العوامل الإرشادية وجود هيكل للقيادة وقواعد وآليات تأديبية داخل الجماعة؛ وقدرة الجماعة على الحصول على الأسلحة والمعدات العسكرية والمجندين والتدريب العسكري؛ وقدرتها على تخطيط العمليات العسكرية وتنسيقها وتنفيذها، بما في ذلك تحركات القوات وتوافر الدعم اللوجستي لها؛ وقدرتها على وضع استراتيجية عسكرية موحدة والتفاوض وإبرام الاتفاقات مثل اتفاقات وقف إطلاق النار أو اتفاقات السلام[[21]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn21%22%20%5Co%20%22).

يتمثل المعيار الثاني لتحديد وجود نزاع مسلح دولي في حدة أعمال العنف. ولتقييمه يجب دراسة الأحداث الدائرة على أرض الواقع. فقدّمت المحكمة الجنائية ليوغوسلافيا السابقة أيضًا عوامل إرشادية لتقييم هذا المعيار منها: «عدد المواجهات الفردية ومدتها وحدّتها، نوع الأسلحة والمعدات العسكرية الأخرى المستخدمة وعدد الذخائر التي أُطلقت وعيارها، عدد الأفراد وأنواع القوات المشاركة في القتال، حجم الخسائر البشرية، حجم الدمار المادي وعدد المدنيين الفارين من منطقة القتال».

فالمجموعة المسلحة من غير الدول التي هي طرف من أطراف النزاع المسلح غير الدولي، يمكن أن تنخرط مستقبلًا في الأعمال العدائية التي تتكون بالكامل من العمليات السيبرانية التي تفي بمعيار الشدة، لكن لتصنيفها بأنها نزاع مسلح غير دولي يتعيّن على هذه المجموعة تلبية المعيار الثاني وهو التنظيم. كانت محكمة يوغوسلافيا السابقة قد أعلنت في قضية تاديتش وهي قضية في النزاع، على أن النزاع المسلح لكي يصنف غير دولي يجب توافر معيارَي العنف وهيكل القيادة لهذه المجموعة. لذلك، فإن العمليات السيبرانية الفردية أو التي تنفّذها مجموعة غير منظمة من المقرصنين لا يمكن أن تعد نزاعًا مسلحًا غير دولي. فقد ارتأى الخبراء الدوليون أن فشل أعضاء المجموعة من الاجتماع جسديًا، لا يعني أن هذه المجموعة غير منظمة، ففي الواقع يجب أن يعمل أعضاء الجماعة جنبًا إلى جنب، من خلال استهداف أهداف معينة يتم تحديدها على موقع المجموعة على الشبكة الإلكترونية، لكن في رأيهم هذا لا يكفي لتلبية متطلبات التنظيم. فيجب أن تعمل الجماعة بشكلٍ تعاوني لغرضٍ مشترك، وأن تخضع لتعليمات قيادة موحدة، وتحترم أحكام القانون الدولي الإنساني[[22]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn22%22%20%5Co%20%22).

وفي إطار موضوعنا، ومع ظهور الهجمات السيبرانية سواء كوسيلةٍ أو كأسلوبٍ جديد في ساحات القتال، يبرز تحدٍّ جديد يتمثل في معرفة حدود استعمال وسائل القتال وأساليبه الذي وضعه القانون الدولي الإنساني، سواء في القانون الدولي الاتفاقي أو القانون الدولي العرفي. فضلًا عن أن الهجمات السيبرانية العابرة للحدود وغير العابرة لها، إذا ما نُفّذت في أثناء نزاع مسلح يجب أن تتفق مع مبادئ القانون الدولي الإنساني في الحرب، ما أثار جدلًا قانونيًا بشأن شرعية الهجمات السيبرانية بموجب القانون السالف الذكر. لذلك سوف نبحث في المطلب الثاني عن الطبيعة القانونية للهجمات السيبرانية.

**المطلب الثاني: الطبيعة القانونية للهجمات السيبرانية**

معلوم أن القانون الدولي الإنساني هو قانون وُلد من رحم الحروب، فهو على موعد مع التطوّر كلما تطوّرت وسائل القتال وأساليبه. لذا ترتب الفجوة التكنولوجية والتقنية المتزايدة يومًا بعد يوم بين دول العالم تحديات على مختلف الصعد وبخاصةٍ على صعيد القانون الدولي الإنساني، من حيث الطبيعة القانونية للهجمات السيبرانية في هذا القانون، ومدى إمكانية تطبيق مبادئه وقواعده على هذا الشكل الجديد من الحروب. وبعبارةٍ أخرى، في ظل وجود فراغ قانوني وعدم وجود قواعد قانونية محددة تُنظّم الهجمات السيبرانية، يُثار التساؤل عن القواعد الواجبة التطبيق.

إن اللجوء المتزايد للدول في استخدام الفضاء الإلكتروني لشن هجمات سيبرانية في أثناء النزاعات المسلحة، جعل مبادئ القانون الدولي الإنساني وقواعده أمام اختبار حقيقي ومعقد حول إمكانية تطبيق قواعده على هذا النوع الجديد من الحروب، ذلك لأن الفترة التي جرى فيها تقنين قواعد قانونية ذات الصلة بوسائل القتال وأساليبه، لا سيما اتفاقيات لاهاي لعام 1899-1907، واتفاقيات جنيف الأربعة لعام 1949 والبروتوكولان الإضافيان لعام 1977، حينها لم يكن للهجمات السيبرانية عند إبرامها أي وجود يُذكر، ما يعني أنها لم تُقنّن بأحكامٍ خاصة تنظّم استعمالها من الناحية القانونية.

وعلى ضوء أحكام قانون الحرب، كان تطوير وسائل وأساليب قتال جديدة متوقعًا. فالمادة 36 من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف نصت على ما يأتي: «يلتزم أي طرف سامٍ متعاقد، عند دراسة سلاح جديد أو تطويره أو اقتنائه أو أداة حرب أو اتّباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظورًا في الأحوال كافة أو في بعضها بمقتضى هذا الملحق البروتوكول أو أي قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها ذلك الطرف السامي المتعاقد». وبالتالي، تضع هذه المادة الإطار العام الناظم لاستخدام وسائل وأساليب قتال جديدة في النزاعات المسلحة.

وتبين أحكام هذه المادة أنه على ضوء قانون الحرب، يتعيّن على الدول التي تقتني أسلحة حديثة أو تطوّرها تتبّع أسلوب قتال جديد، وأن تحدد مشروعية استعمالها. كما يفيد هذا النص ضمنيًا أن كل قواعد قانون الحرب تكون قابلة للتطبيق على وسائل القتال الحديثة وأساليبها، ففي حال غياب النص الخاص يطبّق النص العام، هذا من حيث المبدأ.

وفي المقابل، فإن المادة 36 من البروتوكول الإضافي الأول لا تحرّم تطوير، أو اقتناء أسلحة حديثة أو حتى حيازة أسلحة أو اعتماد أساليب جديدة غير منظمة بقواعد القانون الدولي الإنساني، ومن هذا المنطلق فإن أحكام هذه المادة لا توقف حق الدول في ذلك، وإنما تنص على ضرورة المراجعة القانونية عند اقتناء أسلحة من نوع جديد أو تطويرها أو أسلوب حديث أو ما يعرف بالمطابقة القانونية مع قواعد القانون الدولي وذلك قبل استعمالها، ومن ثم لا يعد هذا النص قانونًا جديدًا ولكنه يقنّن القاعدة القانونية العرفية في التزام الدول بتطبيق معاهدة أو قاعدة عرفية بنيّةٍ حسنة[[23]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn23%22%20%5Co%20%22)، والمقصود هنا بصفةٍ خاصة القواعد الدولية لتنظيم العمليات العدائية.

واستنادًا إلى مبادئ القانون الدولي الإنساني، فإن شرط مارتنز la clause de Martens هو وسيلة فعالة لمواجهة التطورات التقنية التي تعرفها وسائل القتال وأساليبه، إذ ورد لأول مرة في اتفاقية لاهاي الثانية لعام 1899 والذي ينص على: «أنه في الحالة التي لا تنطبق فيها معاهدة أو قانون عرفي، فإن المدنيين والعسكريين يتمتعون بحماية مبادئ القانون الدولي المشتقة من العرف المستقر، ومن المبادئ الإنسانية، وما يمليه الضمير العام». وقياسًا على هذا المغزى، أمكن تحريم الأسلحة البغيضة للضمير العام[[24]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn24%22%20%5Co%20%22).

كما تطرح وسائل القتال الجديدة وأساليبه تحديات قانونية وعملية في ما يخص ضمان استخدامها على نحو يمتثل لقواعد القانون الدولي الإنساني القائمة وإيلاء الاعتبار الواجب للتداعيات الإنسانية المتوقعة جراء استخدامها.

فحق الأطراف في اختيار وسائل الحرب وأساليبها حق مقيد باحترام مبادئ النزاعات المسلحة وقوانينها وأعرافها، ويحظّر القانون الدولي الإنساني استخدام وسائل الحرب وأساليبها التي تعد عشوائية الأثر أو تسبب ضررًا زائدًا أو آلامًا لا لزوم لها. وعليه، فإن هذه المنظومة القانونية السابقة الذكر تشكّل القيود والحدود لاستعمال وسائل الحرب وأساليبها[[25]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn25%22%20%5Co%20%22).

مع دخولنا في عصر هذا النوع الجديد من الحروب، فإن الخطورة المتعلقة بوسائل القتال الجديدة وأساليبه تكمن في انتفاء عنصر المواجهة المباشرة والتقدير البشري الذي يصاحبها، ويجب أن تبقى الأعمال العدائية ضمن الغرض المطلوب من الحرب ألا وهو قهر قوات العدو وإجبارها على التسليم، وبذلك فإن الوسائل والأساليب المستعملة يجب ألا تتعدى هذا الغرض فتصل إلى الأعمال الوحشية.

كما يمكن أن تستهدف الهجمات السيبرانية القطاعات الاقتصادية، الأمنية، الزراعية، الصناعية وغيرها من القطاعات.... في إطار نزاع مسلح. في السابق، نجحت عدة هجمات في قطع إمدادات خدمات أساسية للسكان المدنيين، إذ طالت هذه الهجمات السيبرانية قطاع الخدمات الصحية المحمي بموجب القانون الدولي الإنساني، فضلًا عن الأعيان المدنية مثل الأعيان التي لا غنى عنها لبقاء السكان المدنيين على قيد الحياة، والأعيان التي تضم قوى خطرة وغيرها المحمية أيضًا بموجب قانون الحرب.

فقد أفرد القانون الدولي الإنساني مجموعة من القواعد التي تهدف إلى الحد من آثار النزاعات المسلحة سواء أكانت دولية أم غير دولية، إذ تضمن مبادئ وقواعد أساسية تحكم اختيار وسائل القتال وأساليبه. إذ انبثقت مبادئ القانون الدولي الإنساني من فكرة مفادها أن هذه المبادئ لا تمنع الأعمال القتالية في النزاعات المسلحة، إنما وُجدت لتقييد وسائل القتال وأساليبه في هذه النزاعات. ولهذه الأسباب هناك إقرار بضرورة قبول مستوى معيّن من العنف والخسارة في الأرواح والدمار من جانب الأطراف المتحاربة كافة كنتيجةٍ طبيعية لمباشرة الأعمال العدائية. وهي تمثّل أبسط الأسس الإنسانية التي تنطبق في كل زمان ومكان، كما أنها تقدّم الحل باستقراء الحالات غير المتوقعة وتسهم في سد ثغرات القانون. وعليه، يقوم القانون الدولي الإنساني على المبادئ التي تحكم سير العمليات العدائية وهي التمييز، التناسب والاحتياطات.

يتطلب مبدأ التمييز وفق نص المادة 48 من البروتوكول الإضافي الأول لعام 1977 أن تميز أطراف النزاع المسلح في الأوقات كافة بين الأشخاص المدنيين والأعيان المدنية من جهة، والمقاتلين والأهداف العسكرية من جهة أخرى، فضلًا عما نصت عليه الفقرة 2 المادة 51 من البروتوكول نفسه: «لا يجوز أن يكون السكان المدنيون بوصفهم هذا، وكذلك الأشخاص المدنيون محلًا للهجوم وتُحظّر أعمال العنف أو التهديد به الرامية أساسًا إلى بث الذعر في صفوف السكان المدنيين». كما ورد في المادة 52 من البروتوكول عينه:«لا تكون الأعيان المدنية محلًا للهجوم أو لهجمات الردع»، فضلًا عن المادة 55 من البروتوكول الأول أيضًا الذي يُحظّر استخدام وسائل القتال وأساليبه التي يُقصد بها أو يُتوقع منها أن تسبب أضرارًا بالغة واسعة الانتشار وطويلة الأمد بالبيئة الطبيعية ومن ثم تضر بصحة السكان أو بقائهم، وتُحظّر هجمات الردع ضد البيئة الطبيعية. كما توفر المادة 56 منه الحماية للأشغال الهندسية والمنشآت التي تضم قوى خطرة. لقد ورد مبدأ التمييز في العديد من أحكام القانون الدولي الإنساني والقانون الدولي العرفي، اللذين يوفران إرشادات حول كيفية شن الهجمات، بالإضافة إلى مبدأَي الضرورة والتناسب. وفي هذا السياق أكدت محكمة العدل الدولية في رأي استشاري في العام 1966 على أن القانون الدولي الإنساني يقوم على مبدأَين جوهريَين، يقضي الأول بأنه يجب على الدول ألا تجعل من المدنيين هدفًا للهجوم، أما المبدأ الثاني فيقضي بتحريم استعمال الأسلحة التي من شأنها أن تسبب آلامًا لا مبرر لها، وهذا المبدأ قد نصت عليه أيضًا لائحة لاهاي المتعلقة بقوانين الحرب البرية وأعرافها لعام 1907 «على أن حق الأطراف المتحاربين في اختيار وسائل القتال وأساليبه ليس بالحق غير المحدود[[26]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn26%22%20%5Co%20%22)». وبالتالي نظرًا لإلزامية هذه القواعد، نرى أنها تنطبق بالكامل على الهجمات السيبرانية.

وربطًا بمبدأ  التمييز هناك فضاء سيبراني واحد فقط تتقاسمه القوات  المسلحة مع المستخدمين المدنيين وكل شيء متشابك ومترابط. وتبرز التحديات في ضمان توجيه هذا النوع من الهجمات السيبرانية ضد المقاتلين والأهداف العسكرية، وبالتالي تحييد المدنيين أو الأعيان المدنية المحميين بموجب القانون الدولي الإنساني، كما يجب على الدول المشاركة في النزاع المسلح أن تكون حذرة عند استخدام الهجمات السيبرانية، مع العلم أن الخصائص التقنية التي تتمتع بها الهجمات السيبرانية تمنحها القدرة على أن تُضبط بدقةٍ كبيرة لتصيب أهدافًا عسكرية بعينها فقط[[27]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn27%22%20%5Co%20%22).

فالقاعدة هي أنه لا يجوز مهاجمة السكان المدنيين إلا في حال مشاركتهم مشاركة مباشرة في الأعمال العدائية وعلى مدى الوقت الذي يقومون خلاله بهذا الدور[[28]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn28%22%20%5Co%20%22)، أي أن المدنيين يشاركون مشاركة مباشرة في الأعمال العدائية عندما يقومون بأعمالٍ محددة كجزءٍ من سير الأعمال العدائية بين الأطراف في نزاع مسلح. فالقراصنة يظلون مشمولين بالحماية بموجب القانون الدولي الإنساني ما لم يقوموا بدورٍ مباشر في العمليات العدائية. شمولهم بالحماية لا يعني إعفاءهم من المساءلة الجنائية عما قد ارتكبوه. أما في حال شارك هؤلاء القراصنة مباشرة في الأعمال العدائية، وقاموا بهجماتٍ سيبرانية دعمًا لطرفٍ في النزاع على حساب طرف آخر، فإنهم يخسرون هذه الحماية المكفولة لهم ضد الهجوم المباشر في أثناء تنفيذ الهجوم السيبراني[[29]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn29%22%20%5Co%20%22).

وفي إطار تطبيق مبدأ التمييز على الهجمات السيبرانية فقد أشار دليل تالين، على الرغم من عدم إلزامية قواعده، بأنه لا يجوز أن تكون الأعيان المدنية هدفًا للهجمات السيبرانية، فلا يجوز على سبيل المثال توجيه الهجمات السيبرانية التي من شأنها تدمير الأنظمة المدنية والبنية التحتية، ما لم تعد هذه الأنظمة من قبيل الأهداف العسكرية التي يجوز استهدافها وفق الظروف السائدة[[30]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn30%22%20%5Co%20%22).

وبناءً على ما تقدّم من معطيات، فإن تطبيق مبدأ التمييز بين المقاتلين والمدنيين على الهجمات السيبرانية هو أمر في غاية التعقيد، إذ إن المهاجم في الأغلب يكون بعيدًا عن مكان الهجوم ولمسافةٍ تتجاوز المئات من الكيلومترات، ما يجعل التأكد من الالتزام به أمرًا غاية في الصعوبة.

ويلحق بمبادئ القانون الدولي الإنساني، مبدأ حظر الهجمات العشوائية، إذ نصت المادة 51 في الفقرة ٤ من البروتوكول الإضافي الأول، بأن الهجمات العشوائية هي تلك الهجمات التي لا توجه إلى هدف عسكري محدد، أو التي تستخدم طريقة أو وسيلة للقتال لا يمكن أن توجه إلى هدف عسكري محدد، أو التي تستخدم طريقة أو وسيلة للقتال تترتب عليها آثار لا يمكن أن تقتصر على النحو المطلوب بموجب القانون الإنساني الدولي. وبالتالي، من شأنها أن تصيب الأهداف العسكرية والأشخاص المدنيين أو المنشآت المدنية من دون تمييز[[31]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn31%22%20%5Co%20%22).

أما في ما خص مبدأ التناسب، وهو ذو طابع ميداني عملاني، ومفاده أنه من المحظور شن هجوم من المحتمل أن يسبب خسائر عرضية في أرواح المدنيين أو إلحاق الضرر بهم، و/أو الإضرار بالأعيان المدنية والتي يمكن أن تكون مفرطة في ما يتعلق بالميزة العسكرية الملموسة والمباشرة المتوقعة.

ففي حال كان الهجوم السيبراني موجهًا إلى هدف عسكري بحت، يكون هدفًا مشروعًا. ولكن القلق الذي يراود الخبراء جميعًا في هذا المجال يكمن في أن الفضاء السيبراني يتميز بالارتباط بين نُظم الحواسيب. ويتألف هذا الفضاء من عدد لا يحصى من نُظم الحواسيب المتصلة بعضها ببعض في أرجاء العالم. وغالبًا ما يبدو أن نُظم الحواسيب العسكرية تتصل بالنُظم التجارية والمدنية وتعتمد عليها كليًا أو جزئيًا. وبالتالي, قد يكون من المستحيل شن هجوم سيبراني على بنية تحتية عسكرية وجعل الآثار تقتصر على هدف عسكري فحسب. وهذا ما أكده الخبيران في القانون الدولي الإنساني ركس Rex و شين Shin بقولهما: «إذا تم توجيه هجمات سيبرانية ضد بنى تحتية تُستخدم للاستعمال المزدوج المدني- العسكري وعن بُعد، فلا يبدو أن الميزة العسكرية الملموسة والمباشرة ستكون واضحة، ما يجعل تطبيق مبدأ التناسب في أثناء الهجمات السيبرانية أمرًا معقدًا عمليًا. من المسلّم به أن أيًا من الأعيان المدنية التي تُستخدم لأغراضٍ عسكرية تصبح هدفًا عسكريًا، وبالتالي لا تتوافر لها الحماية بموجب القانون الدولي الإنساني.

وتكمن المعضلة بوجود العديد من البنى التحتية الإلكترونية الحالية ذات استخدام مزدوج بطبيعتها، ولن يتغير هذا في المستقبل. على سبيل المثال، يمكن مد شبكة الاتصالات العسكرية جزئيًا عبر الكابلات مع وسائط أخرى تُستخدم أيضًا لحركة المرور المدنية. غالبًا ما تعتمد الأسلحة على البيانات الناتجة عن نظام تحديد المواقع العالمي GPS، والذي يخدم أغراضًا مدنية مثل الملاحة. كما أنه تم استخدام وسائل التواصل الاجتماعي مثل Facebook و Twitter على نطاق واسع خلال النزاعات الأخيرة لنقل معلومات مهمة عسكريًا. كما تتجه الجيوش بشكلٍ متزايد إلى المعدات الجاهزة مثل أنظمة الكمبيوتر التجارية لقواتها، ما يجعل من المصانع التي تنتجها أهدافًا عسكرية.

كانت هذه الحقيقة مصدر دراسة مكثفة من قبل فريق الخبراء الدولي، الذي خلص إلى أن «الأشياء والمنشآت كافة ذات الاستخدام المزدوج هي أهداف عسكرية، من دون قيد أو شرط». تنبع أي حماية للجوانب المدنية للبنية التحتية الإلكترونية ثنائية الاستخدام المستهدفة من تطبيق مبدأ التناسب وشرط اتخاذ الاحتياطات في أثناء الهجوم. وأشار الخبراء على وجه الخصوص، إلى أن «الهجوم على منشأة إلكترونية أو على أجزاء كبيرة منها، قد يتعارض بالقدر نفسه مع مبدأ التناسب.

يتزايد الاعتماد العسكري على البنية التحتية الإلكترونية المدنية، وذلك للحفاظ على القوات التابعة لدولةٍ ما وقدراتها العسكرية في مواجهة تراجع الميزانيات. سيكون من الصعب تمويل صيانة شبكات إلكترونية منفصلة أو شراء منتجات مصممة خصيصًا للأغراض العسكرية. هذا الواقع سيضع الدول أمام معضلة. فمن ناحية، سيرغبون في حرمان أعدائهم من استخدام البنية التحتية الإلكترونية ذات الاستخدام المزدوج، ومن ناحية أخرى، سترغب الدول في تحصين البنية التحتية الإلكترونية التي يعتمد عليها سكانها المدنيون وأنشطتها[[32]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn32%22%20%5Co%20%22).

ضمن سياق التحليل، سوف نتطرق إلى مبدأ الضرورة العسكرية الذي يرتبط مباشرة بمبدأ التناسب. فالجيوش تقاتل وفق خطط مدروسة وموافق عليها من القيادات العسكرية الأعلى، لكن في بعض الظروف الطارئة في أثناء النزاع المسلح، يضطر فيها القائد إلى اتخاذ قرار مباشر وفي وقت ضيق، كما أنه قد تواجهه ضرورات عسكرية حربية تكون مؤثّرة في قراره.

تلك ضرورات عسكرية قد تمليها على القائد ظروف القتال ومتطلبات تحقيق مهمته، فهل يُقدِم على تنفيذ قراره أم يحجم عنه؟

إن اتفاقيات جنيف ذات الصلة قد سلّمت بوجود مثل هذه الضرورات الحربية التي قد تمليها ظروف القتال، وجعلت منها مبررًا لبعض الانتهاكات لأحكامها. فقد نصت المواد 51و50و17 من الاتفاقيات الأولى والثانية والثالثة والرابعة بالتوالي على أن تدمير الممتلكات أو الاستيلاء عليها على نطاق واسع يعد انتهاكًا جسيمًا لهذه الاتفاقيات ما لم تبرره الضرورات الحربية.

وعلى الرغم من غموض فكرة الضرورة، فإنها بالغة الأهمية في مجال القانون بصفةٍ عامة وفي مجال القانون الدولي الإنساني بصفةٍ خاصة، وغاية ما في الأمر أنه يجب أن تقدّر هذه الضرورة بقدرها، وبالتالي لا يجوز بأي حال من الأحوال أن تُتخذ كستارٍ لخرق قوانين الحرب وأعرافها، فهي بهذا تخرج من إطار القدر المقدّر لها، فلا يجوز مهاجمة الأهداف المدنية سواء كانت مدنًا مأهولة بالسكان أو أعيانًا مدنية. فلا يوجد ضرورة ملحّة إلى ذلك، كما أن فكرة الضرورة المقصودة يُعنى بها عدم تجاوز مقتضيات الحرب، وهي تحقيق النصر وإضعاف قدرة العدو بالطرق والأساليب التي لا تخالف حكمًا في قوانين الحرب، سواء كان هذا الحكم بمقتضى قاعدة عرفية أو قاعدة تعاهدية، وفي إطار قيام الدولة بردّ العدوان أو المحافظة على كيانها.

وبناء على ما تقدّم، يُفهم أن مبدأ الضرورة العسكرية يتيح مهاجمة الأهداف العسكرية كخيارٍ ضروري بالمرتبة الأولى، إلا أن ذلك لا يمنع كضرورةٍ من مهاجمة الأعيان المدنية إذا كانت تُسهم بطريقةٍ مباشرة في تحقيق ميزة عسكرية أكيدة. وعدم تحديد معايير منظمة لاستخدام تكنولوجيا المعلومات للأغراض العسكرية الهجومية، سيعني إمكانية اللجوء إلى استخدامها بداعي الضرورة العسكرية، وهو ما نجده جليًا في تصريحات متبادلة بين الولايات المتحدة الأميركية وروسيا.

وفي ما يتعلق بمبدأ الضرورة العسكرية، أشار دليل تالين، إلى أنه في الحالات التي يكون فيها الخيار ممكنًا بين عدة أهداف عسكرية للحصول على ميزة عسكرية مماثلة، فالهدف الذي يتم اختياره للهجوم السيبراني، هو ذلك الهدف الذي يُتوقع منه أن يسبب أقل خطر على المدنيين والأعيان المدنية[[33]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn33%22%20%5Co%20%22).

من المسلّم به، أن المتحكمين بهذا النظام الجديد من الهجمات السيبرانية بعيدون عن ساحات القتال، ويعملون تحت قيادة مسؤولة وفق التراتبية العسكرية، تبدأ بالتخطيط للهجمة إلى إعطاء الأمر وأخيرًا بتنفيذها. من هنا نطرح التساؤل الآتي: على من تقع المسؤولية الجنائية عن الانتهاكات الجسيمة لقوانين الحرب؟

البشر وحدهم مخاطبون بالقواعد القانونية، مهما تطورت وسائل القتال وأساليبه سيبقى الإنسان الأول والأخير المسؤول عن توجيهها واستخدامها. ومهما تطور الذكاء الاصطناعي في المستقبل، فسيكون هناك دائمًا إنسان في نقطة البداية. فالإنسان مخاطب بالقانون أما الآلة أو الوسيلة فهي غير مخاطبة به.

سابقًا، كانت الدولة هي الوحيدة التي تتحمل المسؤولية عن الجرائم الدولية المرتكبة من قبل الأفراد الممثلين للسلطة في الدولة، ولكن بسبب فظاعة الجرائم التي يرتكبها هؤلاء الأفراد باسم الدولة في حق الإنسان وكرامته، أصبح الشخص الطبيعي من أشخاص القانون الدولي الإنساني، يتمتع بحقوقه ويتحمل التزاماته، وفي مقدمتها المسؤولية الجنائية الدولية الفردية[[34]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn34%22%20%5Co%20%22). وتبعًا لذلك، تكلّلت الجهود الفقهية في أواخر القرن الماضي بإنشاء المحكمة الجنائية الدولية ومهمتها النظر في الجرائم التي يرتكبها الأشخاص الطبيعيون.

إن المقصود بالمسؤولية هي مسؤولية الرؤساء والقادة عن الأعمال المخالفة لقوانين الحرب عمومًا واتفاقيات جنيف خصوصًا. وقد قسّمها الفقه إلى نوعَين من المسؤولية: مسؤولية القائد عن أعمال مرؤوسيه والمسؤولية الفردية المنصوص عنهما تباعًا في المادتَين 25 و 28 من نظام روما الأساسي. وفي ما يتعلق بالمسؤولية الجنائية الناتجة عن تعطيل وسائل الاتصال المدنية في أثناء نزاع مسلح، فإنها من حيث المبدأ، تخضع للأحكام العامة للمسؤولية الجنائية كما نصّها القانون الدولي الإنساني والذي يهدف إلى ضبط تصرفات المقاتلين وتقييد وسائل القتال وأساليبه[[35]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftn35%22%20%5Co%20%22).

إلا أن سُنّة الإنسان كما القانون، هي التطوّر الدائم، لذا ما علينا إلا أن ننتظر ونواكب ما قد يستجد من تطورات ميدانية وقانونية لنبني على الشيء مقتضاه.

**الخاتمة**

مع تطور التكنولوجيا في وسائل القتال وأساليبه، وبخاصةٍ المستعملة في النموذج الجديد من الحروب كالحرب السيبرانية، التي حلت في صدارة الدراسات القانونية المتخصصة، مقارنة مع القضايا الدولية الأخرى المهددة للسلم والأمن الدوليَين، برزت تحديات كبيرة على صعيد القانون الدولي عمومًا وعلى صعيد القانون الدولي الإنساني خصوصًا، بما أنه ذلك القانون الذي يُنظّم وسائل القتال وأساليبه خلال النزاعات المسلحة.

بعد بيان مفهوم الهجمات السيبرانية في النظام القانوني الدولي، لا يزال غير متفق عليه دوليًا، ما يستدعي تعاون الجهود الفقهية لتحديده لأنه سوف يكون الركيزة الأساسية لأي اتفاقية تقنّن استخدامه مستقبلًا أو تنظّمه. أما أبرز المعضلات التي تؤخّر الجهود الدولية من تقنين هذا النوع الجديد من وسائل القتال وأساليبه، هو انعدام الثقة بين الدول، وبخاصةٍ بين الولايات المتحدة الأميركية وروسيا، الأمر الذي سبب تأخير عقد العديد من الاتفاقيات سابقًا، منها اتفاقية حظر الأسلحة البيولوجية لعام١٩٧٢ واتفاقية حظر الأسلحة الكيميائية لعام١٩٩٣. بناء على ما تقدّم، تؤيد روسيا حظر هذا النوع الجديد من وسائل القتال وأساليبه، بينما تنادي الولايات المتحدة الأميركية بتقييدها.

إلا أن إبرام الاتفاقية في هذا الشأن في المستقبل، سيعني تحريك المسؤولية الجنائية الفردية عن دعم أي مجموعات مسلحة يمكن أن تستخدم الوسائل الإلكترونية للأغراض غير العسكرية تجاه دول أخرى أو تدريبها أو تمويلها.

فمن خلال هذه المقالة، ونظرًا لأن الأنشطة السيبرانية أصبحت مركزية أكثر من أي وقت مضى في تنظيم المجتمعات الحديثة، من المرجح أن تتكيّف هذه الأنشطة مع القانون من خلال تقنينها في اتفاقية خاصة لمنحه حماية أكبر لهذه المجتمعات، إذ ستفرض التزامات على الدول للتصرف بصفتها مسؤولة عن حماية الفضاء السيبراني، وتقليل النقطة التي تنتهك فيها العمليات الإلكترونية الحظر المفروض على استخدام القوة، والسماح للدول بالرد بقوةٍ على بعض العمليات السيبرانية غير المدمرة، وتعزيز حماية البنية التحتية السيبرانية والبيانات والأنشطة خلال النزاعات المسلحة. من الواضح أن هذه التحولات لن تكون خالية من التكلفة، فقد تكون باهظة الثمن، وتؤثّر في انتهاك الخصوصية، وتمتد إلى العمليات الميدانية، وتحرم القادة في ميدان القتال من بعض الخيارات التي كانت متاحة سابقًا. في النهاية، وعلى الرغم من ذلك، تعكس الاتفاقية المصالح الوطنية. لذا، سوف تجد الدول في آخر المطاف أنه من مصلحتها اتخاذ مثل هذه التدابير لحماية وصولها الآمن إلى الفضاء السيبراني والخدمات التي يمنحها.

**المراجع العربية:**

- مقال للدكتور أحمد علو، موقع الجيش اللبناني، آذار 2019، العدد 405.

- أحمد عبيس الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل – كلية القانون العدد الرابع، السنة الثامنة، 2016.

- جون – ماري هنكرتس ولويز دوزوالد – بك، "القانون الدولي الإنساني العرفي"، المجلد الأول، القواعد، اللجنة الدولية للصليب الأحمر، مطبعة برنت رايت للإعلان والدعاية، القاهرة، 2007.

- مايكل شميدت، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر والقانون في الحرب، المجلة الدولية للصليب الأحمر، 2002.

- أشرف عبد العزيز الزيات، المسؤولية الدولية لرؤساء الدول، دار النهضة العربية القاهرة، ط1.

- لويز دوسولد– بك وآنا نويتن: "الأسلحة الحديثة والقانون الدولي الإنساني"، ندوة علمية حول القانون الدولي الإنساني: الواقع والطموح، اللجنة الدولية للصليب الأحمر، جامعة دمشق كلية الحقوق، 2000.

- بيتر ماورير، القانون الدولي الإنساني، إجابات على أسئلتك، حقوق الطبع محفوظة للجنة الدولية للصليب الأحمر، كانون الأول 2014.

- الرأي الاستشاري لمحكمة العدل الدولية لعام 1966 والخاص بشأن شرعية التهديد أو استخدام الأسلحة النووية.

- اللجنة الدولية للصليب الأحمر، الحرب السيبرانية: القانون الدولي الإنساني يوفر طبقة إضافية من الحماية، 10 أيلول 2019.

- اللجنة الدولية للصليب الأحمر، دليل تفسيري لمفهوم المشاركة المباشرة بالأعمال العدائية، آذار 2010.

- مايكل شميدت، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر والقانون في الحرب، المجلة الدولية للصليب الأحمر، 2002.

- منير البعلبكي، "المورد: قاموس إنكليزي-عربي"، دار العلم للملايين، بيروت، 2004.

- شريف عتلم ومحمد ماهر عبد الواحد، "موسوعة اتفاقيات القانون الدولي الإنساني، النصوص الرسمية للاتفاقيات والدول المصادقة عليها"، إصدار بعثة اللجنة الدولية للصليب الأحمر بالقاهرة، الطبعة السابعة، 2007.

**المراجع الأجنبية:**

- Schmitt, Michael N., The Law of Cyber Warfare: Quo Vadis? (September 4, 2013). 25 Stanford Law & Policy Review, (Available at SSRN: https://ssrn.com/abstract=2320755

- Philip Levitz, The law of cyber attack, 2012, vol.37, issue 4.

- Michael N Schmitt, computer network attack and the use of force in international law: Thoughts on a normative framework,Columbia journal of transnational law, 1998-1999.

- Michael N. Schmitt, Wired Warfare: Computer Network Attack and International Law, supra note 73, at 365-99 (2002). The authorhas since moderated his views to accord with the functionality approach set forth in the Tallinn manual.

- Knut Dörmann, Applicability of the Additional Protocols to Computer Network Attacks, INT’L COMM. OF THE RED CROSS (Nov.19,2004), http://www.icrc.org/eng/resources/documents/misc/68lg92.htm.

- Michael N.Schmidt, the law of cyber warfare, STANFORD LAW & POLICY REVIEW, Vol. 25:269.

- Thomas Rid and peter Mcburney, cyber – weapons, Routledge publisher, The RUSI Journal, February 2012.

- Micheal Gervais, “Cyber Attacks and the law of warfare’’, Berkeley Journal of international law, vol:30,Issue.2, article 6,2012.

- Scott J.Shackelford, Änalogizind Cyber: from Nuclear War to Net war Attacks in international law”, university of Cambridge, Dept of politicos and international Studies, Cambridge,UK,205.

- Jonathan A.OPHARD, “Cyber warfare and the crime of aggression: the Need for individual Accountability on tomorrow Battlefield, Duke law and technology review.

- Gorman S.Dreazen & Y.Cole, “Insurgents Hack U.S Drones”, Wall Street journal, 17 December 2009.

- discussion of the subject of characterization of cyber warfare in Michael N.Schmitt, Classification of Cyber Conflict, 89 INT’L L. STUD. 233 (2013).

- Prosecutor v. Tadić, Case No. IT-94-1-I, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction,  70 (Int’l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

- Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment  131-40.

- (Intl’l Crim. Trib. for the Former Yugoslavia July 15, 1999). See also Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v.Serb. & Montenegro.), 2007 I.C.J. 108, 404 (Feb. 26); Prosecutor v. Lubanga, Case No.ICC-01/0401/06, Decision on Confirmation of Charges, 211 (Jan. 29, 2007),http://www.icccpi.int/iccdocs/doc/doc266175.pdf. On the internationalization of a non international armed conflict, see Tadić, Decision on Defence Motion, supra note 77,  76.

- J.Pictet, commentary on the Geneva Convention for the Amelioration of the condition of the wounded and Sick in Armed Forces in the field, ICRC, Geneva, 1952.

- Tallinn Manual, supra note 2, at 74. See also Int’l comm. of the red cross,interpretive guidance on the notion of direct participation in hostilities underinternational humanitarian law 43 (Nils Melzer ed).s

- SassoliM."Transnational Armed Groups and International Humanitarian Law", program on Humanitarian policy and conflict Research, Harvard University, Occasional paper Series, Winter 2006, number 6.

- TALLINN MANUAL

- Prosecutor v RamushHaradinaj, IdrizBalajBrahimaj (Trial judgment), IT-04-84-T (3 April 2008) para 49.

- Schmit Michael N, Classification of Cyber Conflict, supra note 76, at 246; see also INT’LCOMM. OF THE RED CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO

- THE GENEVA CONVENTIONS OF 12 AUGUST 1949, 4470 (Yves Sandoz et al.eds., 1987)[hereinafter Additional Protocols Commentary] (referring to the requirement in Additional protocol I.

- Protocol II, supra note 85, art. 1(1). It is unclear whether the implementation requirement applies beyond Additional Protocol II to all non-international armed conflicts).

- Michael N.Schmidt, the law of cyber warfare, STANFORD LAW & POLICY REVIEW, Vol. 25:269.

[[1]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref1%22%20%5Co%20%22)-     مقال للدكتور أحمد علو، موقع الجيش اللبناني، مجلة الجيش، آذار 2019، العدد 405، 5/8/2020.

[[2]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref2%22%20%5Co%20%22)- Schmitt, Michael N., The Law of Cyber Warfare: Quo Vadis? (September 4, 2013). 25 Stanford Law

& Policy Review, p 270, (Available at SSRN: [https://ssrn.com/abstract=2320755](https://ssrn.com/abstract%3D2320755)).

[[3]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref3%22%20%5Co%20%22)-     Philip Levitz, The law of cyber attack, 2012, vol.37, issue 4,p 890

[[4]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref4%22%20%5Co%20%22)-     أحمد عبيس الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل – كلية القانون العدد الرابع، السنة الثامنة، 2016، ص 614.

[[5]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref5%22%20%5Co%20%22)-     منير البعلبكي، «المورد: قاموس إنكليزي-عربي»، دار العلم للملايين، بيروت، 2004، ص 243.

[[6]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref6%22%20%5Co%20%22)-     Michael N Schmitt, computer network attack and the use of force in international law: Thoughts on a normative

framework,Columbia journal of transnational law, 1998-1999, p890.

[[7]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref7%22%20%5Co%20%22)-     The lead article advocating this view is Michael N. Schmitt, Wired Warfare: Computer Network Attack and

International Law, supra note 73, at 365-99 (2002). The author has since moderated his views to accord with

the functionality approach set forth in the Tallinn Manual.

[[8]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref8%22%20%5Co%20%22)-     The lead article advocating this view is Knut Dörmann, Applicability of the Additional Protocols to Computer

Network Attacks, INT’L COMM. OF THE RED CROSS (Nov. 19,2004), http://www.icrc.org/eng/resources/

documents/misc/68lg92.htm.

[[9]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref9%22%20%5Co%20%22)-     Michael N.Schmidt, the law of cyber warfare, STANFORD LAW & POLICY REVIEW, Vol. 25:269,p.295

[[10]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref10%22%20%5Co%20%22)-    Thomas Rid and peter Mcburney,  cyber – weapons , Routledge publisher, The RUSI Journal, February 2012, p6

[[11]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref11%22%20%5Co%20%22)-    ,Micheal Gervais, “Cyber Attacks and the law of warfare’’, Berkeley Journal of international law, vol:30

Issue.2 article 6, 2012, p.46.

[[12]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref12%22%20%5Co%20%22)-    Scott J.Shackelford, Änalogizind Cyber: from Nuclear War to Net war Attacks in international

law”, university of Cambridge, Dept of politicos and international Studies, Cambridge,UK, 205.

[[13]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref13%22%20%5Co%20%22)-    Jonathan A.OPHARD, “Cyber warfare and the crime of aggression: the Need for individual Accountability on

tomorrow Battlefield, Duke law and technology” review, p3.

[[14]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref14%22%20%5Co%20%22)-    See discussion of the subject of characterization of cyber warfare in Michael N.Schmitt, Classification of Cyber

Conflict, 89 INT’L L. STUD. 233 (2013).

[[15]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref15%22%20%5Co%20%22)-    Prosecutor v. Tadić, Case No. IT-94-1-I, Decision on the Defence Motion for Interlocutory Appeal on

Jurisdiction, 70 (Int’l Crim. Trib. for the Former Yugoslavia Oct. 2,1995).

[[16]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref16%22%20%5Co%20%22)16- Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment 131-40, 145 (Intl’l Crim. Trib. for

the Former Yugoslavia July 15, 1999). See also Application of theConvention on the Prevention and Punishment of the Crime of Genocide (Bosn. &Herz. v.Serb. & Montenegro.), 2007 I.C.J. 108, 404 (Feb. 26); Prosecutor v. Lubanga, Case No.ICC-01/0401/06, Decision on Confirmation of Charges, 211 (Jan. 29, 2007), http://www.icccpi.int/iccdocs/doc/doc266175.pdf. On the internationalization of a noninternationalarmed conflict, see Tadić, Decision on Defence Motion, supra note 77, 76.

[[17]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref17%22%20%5Co%20%22)-    J.Pictet, commentary on the Geneva Convention for the Amelioration of the condition of the wounded and Sick

in Armed Forces in the field, ICRC, Geneva, 1952, p.3.

[[18]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref18%22%20%5Co%20%22)-    Tallinn Manual, supra note 2, at 74. See also Int’l comm. of the red cross,interpretive guidance on the notion of direct participation in hostilities underinternational humanitarian law 43 (Nils Melzer ed).s

[[19]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref19%22%20%5Co%20%22)-    أنظر: ICTY, The prosecutor V.DuskoTadic ، أنظر أيضًا

SassoliM.”Transnational Armed Groups and International Humanitarian Law”, program on Humanitarian policy

and conflict Research, Harvard University, Occasional paper Series, Winter 2006, number 6, p.9.

[[20]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref20%22%20%5Co%20%22)-    TALLINN MANUAL, supra note 2, at 77

[[21]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref21%22%20%5Co%20%22)-    Prosecutor v RamushHaradinaj, IdrizBalajBrahimaj (Trial judgment), IT-04-84-T (3 April 2008) para 49

[[22]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref22%22%20%5Co%20%22)- See Schmitt, Classification of Cyber Conflict, supra note 76, at 246; see also INT’LCOMM. OF THE RED

CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA

CONVENTIONS OF 12 AUGUST 1949, 4470 (Yves Sandoz et al. eds., 1987) [hereinafter Additional Protocols

Commentary] (referring to the requirement in Additional Protocol II, supra note 85, art. 1(1). It is unclear whether the implementation requirementapplies beyond Additional Protocol II to all non-international armed conflicts).

[[23]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref23%22%20%5Co%20%22)-    لويس دوسولد– بك وآنا نويتن: «الأسلحة الحديثة والقانون الدولي الإنساني»، المرجع السابق، ص 152.

[[24]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref24%22%20%5Co%20%22)-    لويز دوسولد– بك وآنا نويتن: "الأسلحة الحديثة والقانون الدولي الإنساني"، ندوة علمية حول القانون الدولي الإنساني: الواقع والطموح، اللجنة الدولية للصليب الأحمر، جامعة دمشق كلية الحقوق، 2000، ص 158.

[[25]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref25%22%20%5Co%20%22)-    بيتر ماورير، القانون الدولي الإنساني، إجابات على أسئلتك، حقوق الطبع محفوظة للجنة الدولية للصليب الأحمر، كانون الأول 2014، ص 50.

[[26]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref26%22%20%5Co%20%22)-    الرأي الاستشاري لمحكمة العدل الدولية لعام 1966 والخاص بشأن شرعية التهديد أو استخدام الأسلحة النووية.

[[27]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref27%22%20%5Co%20%22)-    اللجنة الدولية للصليب الأحمر، الحرب السيبرانية: القانون الدولي الإنساني يوفر طبقة إضافية من الحماية، 10 أيلول 2019.

[[28]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref28%22%20%5Co%20%22)-    اللجنة الدولية للصليب الأحمر، دليل تفسيري لمفهوم المشاركة المباشرة بالأعمال العدائية، آذار 2010، ص 20.

[[29]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref29%22%20%5Co%20%22)-    اللجنة الدولية للصليب الأحمر، الحرب السيبرانية: القانون الدولي الإنساني يوفر طبقة إضافية من الحماية، 10 أيلول 2019.

[[30]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref30%22%20%5Co%20%22)-    مايكل شميدت، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر والقانون في الحرب، المجلة الدولية للصليب الأحمر، 2002، ص 105.

[[31]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref31%22%20%5Co%20%22)-    الفقرة (4) من المادة (51) من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لسنة 1977.

[[32]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref32%22%20%5Co%20%22)-    Michael N.Schmidt, the law of cyber warfare, STANFORD LAW & POLICY REVIEW, Vol. 25:269,p.29

[[33]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref33%22%20%5Co%20%22)-    مايكل شميدت، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر والقانون في الحرب، المجلة الدولية للصليب الأحمر، 2002، ص 130.

[[34]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref34%22%20%5Co%20%22)-    أشرف عبد العزيز الزيات، المسؤولية الدولية لرؤساء الدول، دار النهضة العربية القاهرة، ط1، ص2.

[[35]](https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%85%D9%86-%D9%85%D9%86%D8%B8%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A%22%20%5Cl%20%22_ftnref35%22%20%5Co%20%22)-    أحمد عبيس الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل – كلية القانون العدد الرابع، السنة الثامنة، 2016، ص 642.

**Cyber attacks under the pespective of the international humanitarian law**

The world has witnessed a new arms race which is based on inventing and developing electronic software intended for military purposes briefly known as Cyber. The cyber attacks quickly became the new model of the modern wars which combine the traditional and nontraditional means and methods such as data-collection wars and Cyber wars. The excessive usage of the cyberattacks during the armed conflicts presents new challenges at various levels especially the legal one. Therefore, it presents a challenge to some provisions of the International Law (IL) generally and to the International Humanitarian Law (IHL) specifically.

This article entitled "The Cyber attacks from the perspective of IHL" discusses the excessive utilization of the electronic space in launching cyberattacks during the armed conflicts. The legal problem that is raised by this kind of modern wars is illustrated in answering several questions related to the definition of the concept of the cyber attacks and its legal nature in the IHL and to what extent the IHL rules can be applied on such kind of wars.

Eventually, as we concluded that the concept of cyber attacks is still debatable and needs in-depth research which calls for international concerted efforts to define it since it is going to be the essential foundation for any agreement that would limit or regulate its future use with the confirmation of the flexibility of the current IHL regulations and its applicability on these attacks and handling its effects.

In order to answer this questioning we divided this article into two sections:

Section one: the concept of the cyber attacks

Section two: legal nature of the cyber attacks in the IHL.

**Les cyberattaques du point de vue du droit international humanitaire**

Le monde a vu récemment un nouveau style et cours d’armement celui de l’évolution et de nouveauté électronique conçu pour des objectifs militaires: c’est le cyberespace. Le cyberattaque c’est le nouveau système de guerre qui unit entre le style et le droit public en général et le droit international humanitaire plus specialement.
Mon article intitulée “les cyberattaques du point de vue du droit international humanitaire”. Utilisé le cyberespace pour des cyberattaques lors des conflicts. Ma problématique juridique est les réponses sur des questions nombreuses premièrement définir le concept du cyberattaque, la nature juridique des cyberattaques et jusqu’à quel degré est-il possible d’appliquer les principes et les règles du droit international humanitaire sur ce type de guerre.
On a conclu qu’on cherche jusqu’à maintenant à definir le concept du cyberattaque. Ce qui demande une action internationale car celle-ci sera la base de n’importe quelle convention.
Mon article se divise en deux:
        1. Définir le concept du cyberattaque.
        2. La nature juridique des cyberattaques en droit international humanitaire.