ISSN: 1812-0512 (Print) 2790-346X (online)

Wasit Journal for Human Sciences

Available online at: https://wjfh.uowasit.edu.iq

# Cyber-attacks and autonomous weapons under the principle of proportionality

*** Corresponding Author**
Muhannad Ajab Jandal
College of Law / University of Wasit

Email:
mjandel@uowasit.edu.iq

**Keywords**: Cyber-attacks, autonomous weapons, proportionality principle, artificial intelligence

Article history:
Received: 2025-01-29
Accepted: 2025-03-23
Availablonline: 2025-05-01

**ABSTRACT**

The digital world has produced a new type of danger, with cyber-attacks and the use of autonomous weapons becoming a reality in contemporary armed conflicts. With the new arms race in which countries arm themselves for cyberspace battles, many countries are not only conducting cyber espionage, cyber reconnaissance and investigation missions; they have also created cyber offensive capabilities, developed national strategies, and engaged in cyber-attacks at a frightening pace. The same is true for autonomous weapons, which are nothing more than machines with tremendous artificial intelligence, some of which even resemble humans in their design, and have the ability to determine their targets automatically. All a person has to do is operate them and then leave them to work by themselves. These weapons are undoubtedly the future of wars, as countries no longer need to sacrifice their human soldiers, nor spend huge sums of money on soldiers' salaries and equipment, and perhaps compensation after their death on the battlefields. Such dangerous operations had to be viewed through the lens of international humanitarian law. It is a type of war, and whenever wars exist, international humanitarian law exists to protect individuals from them in accordance with the principles in effect in this regard, including the principle of proportionality.


DOI: https://doi.org/10.31185/wjfh.Vol21.Iss2.892

# الهجمات السيبرانية والأسلحة الذّاتيّة في ظلِّ مبدأ التناسُب

م.د مهند عجب جنديل
كلية القانون / جامعة واسط

**المُستخلص**

أنتج العالم الرقمي نوعًا جديدًا من الخطر أصبحت معه الهجمات السيبرانية ، واستخدام "الأسلحة ذاتيّة التشغيلِ" حقيقة واقعة في النزاعات المسلحة المعاصرة؛ فمع سباق التسلح الجديد الذي تقوم فيه الدول بتسليح نفسها من أجل معارك الفضاء الإلكتروني؛ أصبحت العديد من الدول لا تقوم فقط بالتجسس السيبرانيّ، او الاستطلاع السيبراني ومهام الاستقصاء؛ بل إنَّها خلقت قدرات هجومية سيبرانية، وطورت استراتيجيات وطنية، وانخرطت في الهجمات السيبرانية بوتيرة مخيفة، وكذلك الأمر بالنسبة "للأسلحة ذاتيّة التشغيل" فهي لا تعدو كونها مجرد آلات ذات ذكاء اصطناعي هائل، حتى أن بعضها يشبه البشر بتصميمه، ولها القدرة على أن تحدد أهدافها ذاتياً، فكل ما يقوم به الإنسان مجرد تشغيلها ثم تترك لتعمل بنفسها، إن هذه الأسلحة من دون أدنى شك تعد مستقبل الحروب، فلم تعد الدول بحاجة للتضحية بجنودها البشر، ولا ان تنفق أموال هائلة على رواتب وتجهيزات الجنود، وربما تعويضات بعد موتهم في ساحات القتال، فمثل هذه العمليات الخطيرة كان لابد من النظر إليها بمنظار "القانون الدولي الإنساني"؛ فهي نوع من "الحروب" ومتى ما وجدت الحروب وجد القانون الدوليّ الإنسانيّ لحماية الأفراد منها وفق المبادئ المعمول بها في هذا الشأن ومنها مبدأ "التناسب".

**الكلمات المفتاحية:** الهجمات السيبرانية ، الأسلحة الذاتية ، مبدأُ "التناسُب"، ذكاء اصطناعي.

**المقدمة**

**أولاً: موضوع البحث**

منذ نهاية الحرب العالمية الثانية ونشوء منظمة الأمم المتحدة وتحريمها اللجوء للحرب في صلب ميثاقها، أصبح العالم يعيش إلى حد ما بسلام، ولكن هذا السلام لم يكن إلا ظاهريا فقط ، فقد لجأت الدول الى جيل جديد من الحروب، وهذه الحروب ليست حروباً واضحة المعالم ؛ بل يكتنفها كثير من الغموض، وكانت على نوعين: النوع الأول: هو ما يعرف بالهجمات او الحروب السيبرانية، فبعد التطور الكبير الذي رافق ظهور أجهزة الكمبيوتر وسهولة الوصول إلى الانترنيت، وصيرورة هذا الأخير جزءا من حياة الشعوب والعالم وذا فائدة كبيرة لها، إلا أن المشكلة ظهرت من جراء ذلك؛ فقد ربطت الدول كل ما يتعلق بسير أمورها اليومية بهذه الأجهزة، فأدى ذلك إلى ظهور وسيلة بسيطة وسهلة للهجوم على هذه الدول، وذلك من خلال ما يسمى بالهجمات الالكترونية، وهذه الوسيلة لا تحتاج إلا إلى تمويل بسيط، وربما يتم الهجوم على أكثر الدول قوة من دولة نائية لا تمتلك أي قدر من الامكانيات؛ فمثل هذه الهجمات قد تؤدي لتفعيل او تعطيل أنظمة نووية شديدة الخطورة، أو قد تؤدي لإحداث خلل في أنظمة الدفاع، فمثل هذه العمليات الخطيرة كان لابد من النظر اليها بمنظار "القانون الدّولي الإنسانيّ"؛ فهي نوع من الحروب ومتى ما وجدت الحروب وجد "القانون الدّوليّ الإنسانيّ" لحماية الأفراد منها وفق المبادئ المعمول بها في هذا الشأن ومنها مبدأُ التناسُب.

أما النوع الثاني من هذه الحروب، فهو الأسلحة الذاتية التي لا تعدو كونها مجرد آلات ذات ذكاء اصطناعي هائل، حتى أن بعضها يشبه البشر بتصميمه، ولها القدرة في أن تحدد أهدافها ذاتياً، فكل ما يقوم به الإنسان مجرد تشغيلها ثم تترك لتعمل بنفسها، إن هذه الأسلحة من دون أدنى شك تعد مستقبل الحروب، فلم تعد الدول بحاجة للتضحية بجنودها

البشر، ولا أن تنفق أموالا هائلة على رواتب وتجهيزات الجنود، وربما تعويضات بعد موتهم في ساحات القتال، فهذا الأمر يجعل من السهل جدا فهم سبب تتسابق الدول على صنع وتطوير هذه الأسلحة، وهنا يظهر دور القانون الدولي الإنساني ليحكم على شرعية وجود هذه الأسلحة في أرض المعركة، ومدى قدرتها على الالتزام بآلياته التي فرضها على الدول.

ثانياً: أهمية البّحث :

تكمن أهمية هذا البحث في مدى الخطورة التي أخذت تشكلها "الهجمات السيبرانية" و"الأسلحة الذاتية" ، وازدياد التطور التكنلوجي في استخدامها, وما تشكله من أضرار بمصالح الدول وبنيتها التحتية وعدم تمييزها بين الأهداف المدنيّة والعسكريّة, واتساع رقعه اضرارها دون رادع ، ولابد من إخضاعها لقواعد ومبادئ "القانون الدّوليّ الإنسانيّ" ومنها مبدأُ "التناسُب".

ثالثاً : مشكلة البحث

تكمن مشكلة البحث في الخطورة الشديدة للحروب السيبرانية، والأسلحة الذاتية، فهي تعد ثورة في مجال العلم والتقدم التكنلوجي، وللأسف استغلت بصورة مضرة لحياة الناس وكرامتهم، كذلك فإنَّ أغلب قواعد القانون الدولي الإنساني ومبادئه، ومن ضمنها مبدأ التناسب، وضعت قبل ظهور هذا النوع من الأسلحة؛ لذا كان لا بد من إيضاح وجهة نظر القانون الدولي الإنساني فيها، وما مدى انطباق مبدأ التناسُب عليها ؟، وينطلق البحث من تساؤل رئيس يتمثل بـ: ( إلى أي مدى يمكن إعمال مبدأ التناسُب في القانون الدولي الإنساني على الهجمات السيبرانية والأسلحة الذاتية )، وتتفرع عن هذا التساؤل الرئيس أسئلة فرعية:

- هل يمكن وصف الهجمات السيبرانية هجوماً مسلحاً وفقاً للمبادئ التي أقرها ميثاق الأمم المتحدة .
- مدى شرعية الهجمات السيبرانية في "القانون الدّوليّ الإنسانيّ".
- مدى شرعية استخدام الأسلحة الذاتية في "القانون الدّوليّ الإنسانيّ" .

رابعاً : منهجية البّحث :

اعتمدنا في هذا البحث على "المنهج الوصفي" في وصف موضوعات هذه الدراسة لغموضها وقلة ما مكتوب عنها، واعتمدنا كذلك على "المنهج التحليلي" في تحليل نصوص قواعد "القانون الدّوليّ الإنسانيّ"، وآراء الفقهاء لمعالجة المسائل المهمة المتعلقة بموضوع البحث.

خامساً :هيكلية البحث:

قسمنا الموضوع على مبحثين، تناولنا في المبحث الأول "الهجمات السيبرانية" في ظل مبدأ "التناسُب"، في المطلب الأول منه تطرقنا لمفهوم "الهجمات السيبرانية" ، وفي المطلب الثاني بحثنا في مدى انطباق مبدأ "التناسُب" على "الهجمات السيبرانية"، أما المبحث الثاني فقد خصصناه لبحث موضوع "الأسلحة الذاتية" في ظل مبدأ "التناسب"، في المطلب الأول منه تناولنا مفهوم الأسلحة الذاتيّة، أما المطلب الثاني فقد خصصناه لبحث مدى انطباق مبدأ "التناسُب" على "الأسلحة الذاتيّة" .

**المبحث الأول**

**التناسب في الهجمات السيبرانية**

أنتج العالم الرقمي نوعًا جديدًا من الخطر الذي أصبحت معه الهجمات السيبرانية حقيقة واقعة في النزاعات المسلحة المعاصرة؛ فمع سباق التسلح الجديد الذي تقوم فيه الدول بتسليح نفسها من أجل معارك الفضاء الإلكتروني ,Schreier (2015, p.10)؛ أصبحت العديد من الدول لا تقوم فقط بالتجسس السيبراني، او الاستطلاع السيبراني ومهام الاستقصاء؛ بل إنَّها خلقت قدرات هجومية سيبرانية، وطورت استراتيجيات وطنية، وانخرطت في الهجمات السيبرانية بوتيرة مخيفة، إذ أنشأت العديد من البلدان فروعاً لوحداتها الإلكترونية داخل جيوشها، وعلى سبيل المثال لا الحصر؛ فإنَّ الولايات المتحدة الأمريكية تمتلك" القيادة السيبرانية الأمريكيّة"، ولدى جيش التحرير الشعبي الصيني قسم سيبراني يسمى "Blue Team" ، أي الفريق الأزرق، وكذلك النرويج لديها " Cyberforsvaret " ويعني" الدفاع السيبراني "، وبدأت وزارة الدفاع في المملكة المتحدة بتجنيد أفراد لوحدة الكترونية جديدة (Khan,2017, p2).

سنوضح في هذا المبحث مفهوم "الهجمات السيبرانية"، وبيان مدى انطباق مبدأ "التناسُب" عليها وذلك في مطلب مستقل لكلٍ منهما.

**المطلب الأول**

**مَفهوم الهجمات السيبرانية**

**سنتعرف على مفهوم الهجمات السيبرانية من خلال الفروع الآتية:**

**الفرع الأول : تعريف "الهجمات السيبرانية":**

بالرغم من الاستخدام الشائع لمصطلح الهجمات السيبرانية؛ إلا أنَّهُ لا يوجد إلى الآن تعريف ثابت لتحديد مفهومها ؛ وسبب ذلك أنَّ الكثير من العواقب المحتملة لهذهِ الهجمات لم تحدث إلى الآن؛ مما يعني صعوبة وضع تعريف جامع مانع لها، إذ تكهن المحللون حول العواقب المحتملة للهجوم السيبراني؛ فوضعوا سيناريوهات تتراوح بين كونه فيروسا يخترق السجلات المالية، أو يعطل سوق الأسهم فيها، إلى رسالة خاطئة قد تتسبب في إغلاق مفاعل نووي أو فتح سد، إلى تعتيم نظام التحكم في الحركة الجوية الذي ينتج عنه تعطل طائرة، وتوقعوا حدوث أضرار اقتصادية أو مادية شديدة وواسعة النطاق؛ لكن لم يحدث أي من هذه الآثار حتى الآن ، ومع ذلك فإنَّ العديد من الحوادث السيبرانية تحدث بانتظام ، كما سبق الإشارة إليها في الفرع الأول الخاص بالتطور التاريخي للهجمات السيبرانية(Hathaway,2012,p.822).

ومع ذلك؛ فإنَّ هنالك العديد من التعاريف التي حاولت فهم نطاق التهديد الذي تشكله" الهجمات السيبرانية"؛ ومنها التعريف الذي يذهب الى أن الهجوم السيبراني يعني " هجوم عبر الانترنت يقوم على التسلل الى المواقع الالكترونية غير مرخص بالدخول اليها يهدف الى تعطيل او اتلاف البيانات المتفرة فيها او الاستحواذ عليها ، وهي عبارة عن سلسلة هجمات الكترونية تقوم بها دولة ضد أخرى "( عطا ، 2022، ص 668)، ومن التعاريف المهمة "للهجمات السيبرانية" التعريف الوارد في دليل" تالين" إذ عرف" الهجمات السيبرانية" : "هي عملية سيبرانية هجومية أو دفاعية يتوقع أن تتسبب في ايقاع ضحايا في صفوف الأشخاص سواء إصابةً أو قتلاً أو إلحاق الأذى بالأعيان سواء إضراراً أو تدميرا" ، ودليل تالين هو دليل لدراسات تداعيات الحروب و"الهجمات السيبرانية" والقواعد المعيارية المنظمة لها، أصدره مجموعة من

الخبراء العسكريين والقانونيين بمشاركة " اللجنة الدّوليّة للصليب الأحمر"(الحديثي، 2021 ، ص 21 ). كذلك يمكن أن تعرف الهجمات السيبرانية على أنها " عمليّات تعطيل او رفض او اضعاف او اتلاف المعلومات الموجودة في شبكات او اجهزة الكومبيوتر" (علام ،2023، ص 456) .

كما تُعرَّف بأنَّها: " عمل عدائي يستخدم الكمبيوتر أو الشبكات أو الأنظمة ذاتُ الصّلة، بهدف تعطيّل أو تدميرِ الأنظمة السيبرانية الحرجة أو الأصول أو الوظائف "، ولا تقتصر التأثيرات المقصودة للهجوم السيبراني بالضرورة على أنظمة الكمبيوتر أو البيانات المستهدفة نفسها؛ فالهجمات على أنظمة الكمبيوتر قد تهدف، مثلاً : تهدف إلى تحطيم أو تدمير البنية التحتية (Hathaway, 2012,823) .

ونلاحظ أن التعريفات أعلاه واسعه ولم تبيّن الغرض من هذه الهجمات، هل لغرض الرد على هجوم مماثل يحدث في نطاق نزاع عسكري من عدمه ؟ او لأغراض سياسية ؟ او لأغراض تتعلق بالأمن الوطني ؟

وكذلك ورد تعريف للهجمات السيبرانية من قبل (ريتشارد كلارك)*[1] الذي عرفها بأنها" : "أفعال دولة قوميّة لأختراقِ أجّهزة الكمبيوتر، أو الشّبكات في دولة أُخرى لأغراض التسبّب في الضرر أو التعطيل"
( Mazanec, 2023,P.530)،

وبالمثل عرَّف( مايكل هايدن)*[2] الحرب السيبرانية بأنها :"محاولة متعمدة لتعطيل أو تدمير شبكات الكمبيوتر في دولة أخرى ".(Hathaway, 2012,823 ).

وأهم ما لاحظناه على تعريفي" كلارك، ومايكل " أنَّهما لم يُميزا بين الهجوم السيبراني والحرب السيبرانية؛ إذ جعلا من المفهومين سواء، في حين أنَّ للحرب السيبرانية مفهوما آخر؛ إذ تُعرَّف بأنَّها" :" صراع يستخدم هجمات معادية أو غير قانونية على أجهزة الكمبيوتر والشبكات في محاولة لتعطيل الاتصالات وغيرها من البنى التحتية كآلية لإلحاق الضرر الاقتصادي أو اضطراب الدفاعات " (Schreier, 2015, p.10).

وتأسيساً على ما تقدم فإنَّ الهجوم السيبراني يحمل مفهومل أوسع من مفهوم الحرب السيبرانية؛ إذ يُشترط في الحرب السيبرانية أن تكون آثارها معادلة لآثار النزاعات المسلحة، أو أن تحدث عملياتها في سياق نزاع مسلح؛ بينما لا يشترط ذلك في الهجوم السيبراني، فضلاً عن ذلك؛ فإن تعريف" كلارك" قد ضيّق من نطاق "الهجمات السيبرانية" ؛ فهو يقصر التعريف على الهجمات التي ترتكبها الدول، ومن ثمَّ يستبعد تمامًا الهجمات التي تنفذها جهات أخرى من غير الدول، كالجماعات المسلحة غير الحكومية.

لذا فإننا مع تعريف الهجوم السيبراني الذي يذهب إلى أن تعريف الهجوم السيبراني بأنَّه : "أي إجراء يُتخذ لتقويض وظائف شبكة الكمبيوتر لأغراض سياسية أو لأغراض الأمن الوطني " (Schreier, 2015, p.17).

والعنصر الأخير في هذا التعريف؛ هو أهم ما يُميز الهجوم السيبراني عن الجرائم الالكترونية؛ إذ إنَّ غرض الهجوم السيبراني إما سياسي أو للحفاظ على الأمن الوطني، وإنَّ أي هجوم سيبراني لا يتم تنفيذه وفقاً لهذا الغرض يكون مجرد

*خبير أمني أمريكي؛ أصبح في عهد الرئيس كلنتون منسقا قوميا أول للأمن وبقي في منصبه حتى عام2003 .
* جنرال متقاعد في سلاح الجو الأمريكي، ومدير وكالة الأمن القومي ووكالة المخابرات المركزية السابق.

جريمة إلكترونية، كما هو الحال في معظم حالات الاحتيال عبر الإنترنت، أو سرقة الهويات والبيانات أو قرصنة الملكية **الفكرية.**

**الفرع الثاني : التطور التاريخي للهجمات السيبرانية وأنواعها**

**سنقسم هذا الفرع على فقرتين كالآتي :**

**أولاً: التطور التاريخي للهجمات السيبرانية:**

عندما ظهر الإنترنت لأول مرة قبل نصف قرن، لم يكن الأمن في المخطط التفصيلي لهذا الاكتشاف، وكان التركيز الفني يقتصر على كيفية جعل مخطط الشبكات يعمل؛ لكن بعد مدة وجيزة أصبح من السهل أن نرى كيف كان تجاهل الأمان خطأً هائلاً ؛ إذ جلبت ثورة الحواسيب والإنترنت معها إمكانية سوء الاستخدام، وقد أدى تزايد الاندفاع والاستخدام للإنترنت، الحديث إلى ظهور العديد من الهجمات السيبرانية (Warner,2012,p.785).

أول هذه الهجمات كانت عام(1982)، نفذته "الولايات المتّحدةُ الامريكيّة "ضد "الاتحاد السوفيتيّ" من خلال نقل البرامج المستخدمة لتشغيل مضخات خطوط الأنابيب والتوربينات إلى الاتحاد السوفيتي، والتي صممت لتتسبب في تعطيل سرعات المضخة وإعدادات الصمام؛ وكانت النتيجة ظهور انفجار كبير وحريق غير نووي تم رؤيته من الفضاء، وقد نُسب لهذا الهجوم الفضل في المساعدة في إنهاء" الحرب الباردة" بين "الولايات المتحدة" و"الاتحاد السوفيتي" ( Schreier, 2015, p.107) .

أما الهجوم الآخر؛ فقد كان في عام(1991) ؛ عندما استخدمت الولايات المتحدة الامريكية وسائل وأساليب الحرب السيبرانية أثناء الحرب على العراق؛ إذ طالت هذه الهجمات أنظمة القيادة والتحكم ومرافق الاتصالات والعناصر الرئيسة في البنية التحتية الوطنية، مثل الشبكات الكهربائية الحرجة، كما استخدمت الولايات المتحدة أيضًا أنظمة الاتصالات والأقمار الصناعية واسعة النطاق لدعم العملية؛ وقد وصفَ" لميريل ماكبيك"، رئيس أركان القوات الجوية الأمريكية، حرب الخليج بأنّها "الحرب الأولى في عصر الفضاء" (jon,1991,p 10).

وتُعد حرب كوسوفو عام (1999) أول حرب سيبرانية واسعة النطاق؛ إذ بدأت بقيام طائرات الناتو بقصف صربيا، لتبدأ بعد ذلك مجاميع القراصنة الموالية للصرب أو المعادين للغرب، بمهاجمة البنية التحتية للإنترنت في الناتو؛ إذ تعرضت جميع أجهزة الكمبيوتر التابعة لحلفِ "الناتو" ، والولايات المتحدة، والمملكة المتحدة للهجوم السيبراني خلال الحرب، كما تم تشويش موقع" البيت الأبيض"، على الرغم من أنَّ" الولايات المتحدة" ادعت أنَّ هذه الهجمات لم تؤثر على مجمل الحرب؛ فقد اعترفت المملكة المتحدة بأنها فقدت بعض المعلومات لقاعدة بيانات واحدة على الأقل (Geers,2008,p.15)، وفي مايو( 1999 )، قصف الناتو عن طريق الخطأ السفارة الصينية في بلغراد؛ مما أدى إلى موجة من "الهجمات السيبرانية" من الصين ضد مواقع الحكومة الأمريكيّة (Schreier, 2015, p.107) .

والهجوم الآخر كان على شكل حرب سيبرانية غير معلنة بين إسرائيل وفلسطين؛ بدأت عام (2000) ، في إثر اختطاف ثلاثة جنود إسرائيليين؛ إذ قام قراصنة إسرائيليون مراهقون بشن هجوم سيبراني متواصل على مواقع للسلطة الوطنية الفلسطينية وحماس وإيران؛ مما أثار بوادر حرب سيبرانية تصاعدت بشكل سريع؛ إذ كان رد المهاجمين المؤيدين لفلسطين سريعًا ومتنوعًا؛ فقد تم ضرب مواقع الكترونية لإسرائيل رفيعة المستوى كموقعي وزارة الخارجية، ومعلومات

جيش الدفاع الإسرائيلي، ومواقع لمكتب رئيس الوزراء الإسرائيلي، وبنك إسرائيل، وبورصة تل أبيب(Geers,2008,p.15).

وفي عام (2002) حصل هجوم سيبراني ضار جداً على إستونيا؛ في وقت أصبحت فيه هذه الدولة أعجوبة؛ بوصفها واحدة من أكثر الدول المتقدمة إلكترونيًا؛ إذ حولت الحكومة الإستونية عملياتها منذ عام (2002) إلى المجال الافتراضي؛ لكن الهجوم السيبراني الأخير عليها أدى إلى انسداد شبكة الإنترنت فيها، وإغلاق مواقع الإلكترونية حكومية، ثم بدأت شبكات الروبوت بعد مدة بمهاجمة مواقع وخوادم خاصة، تم في إثرها إغلاق البنوك في إستونيا، مما أثر على الخدمات المصرفية الدولية، وتم اتهام الكرملين الروسي بالوقوف وراء هذه الهجمات، كما أرسلت كل من" الولايات المتحدّة" وحلفِ "الناتو" فرقاً لخبراء في أمن الكمبيوتر لمساعدة السلطات الإستونية على التعامل مع الموجة الهائلة من الهجمات التي شلت المواقع الحكومية والصناعية والمصرفية للبلاد، فضلا عن توقف وسائل الإعلام(Schreier, 2015, p.109).

وقامت إسرائيل في عام( 2002) بتنفيذ هجوم مختلط على موقع يُعتقد بأنَّهُ "موقع نووي" في منطقة ( دير الزور) السورية؛ إذ تمت العملية باستخدام القنابل الدقيقة التقليدية والهجوم الإلكتروني لتشويش الرادارات السورية؛ فيما أكدت مصادر أوربية أنَّ شبكة الدفاع الجوي السوري قد تم تعطيلها بواسطة مفتاح داخلي سري تم تنشيطه من قبل الإسرائيليين؛ وعلى أي حال؛ فإنَّ الهجوم المختلط حقق نتائجه؛ إذ أدى هذا الهجوم إلى عجز القوات الدفاعية عن المقاومة؛ مما ساعد السلاح التقليدي على اتمام مهامه دون مقاومة تُذكر (Schreier, 2015, p.111) .

وتُعد الهجمات السيبرانية الروسية ضد جورجيا في عام( 2009) أول مثال على "الهجمات السيبرانية" التي تزامنت بشكل مباشر مع نزاع مسلح بري وبحري وجوي، وربما يكون أفضل نموذج على كيفية استخدام هذه الهجمات في المعارك الحديثة؛ إذ بدأت روسيا الحرب ضد جورجيا مستخدمة هجمات سيبرانية منسقة للغاية على مواقع للحكومة الجورجية وغيرها من المواقع ذات القيمة الاستراتيجية؛ بما في ذلك السفارات الأمريكية والبريطانية، لقد قطعت الهجمات السيبرانية اتصال جورجيا بالعالم؛ مما أدى إلى تأخير أي رد دولي على الصراع، كما أربكت الدفاعات الجورجية بطريقة جعلت أي اتصال لهذه الدفاعات شبه مستحيل (Schreier, 2015, p.112).

وكذلك في عام( 2009) حصل هجوم سيبراني ضد مواقع حكومية وتجارية في كلٍ من الولايات المتحدة وكوريا الجنوبية؛ وقد تزامن الهجوم مع إطلاق صاروخ من كوريا الشمالية بمناسبة الذكرى الخامسة عشرة لوفاة زعيم كوريا الشمالية الأسبق؛ مما ولد شكاً في وقوف كوريا الشمالية وراء الهجمات(Schreier, 2015, p.113) .

وأكثر" الهجمات السيبرانية" حداثة؛ هو الهجوم الذي حصل ضد المفاعلات النووية الإيرانية في عام (2009) بإستخدام برنامج(Stuxnet) (لين ، 2012، ص 519)، وهو برنامج متطور يهاجم ويعطل أجهزة الطرد المركزي النووية، ويتميز بذكاء شديد؛ لدرجة أنه يخفي الضرر الذي يحدث عن المشغلين والمشرفين، وهذا ما حصل في هذا الهجوم؛ إذ تسبب في إتلاف سلسلة من أجهزة الطرد المركزي، وأخرج برنامج تطوير الأسلحة النووية عن الخدمة ولم يكتشف المشغلون والمشرفون ذلك إلا في وقت متأخر جدًا(Allhoff, 2013,p.25) .

ومن الهجمات السيبرانية الحديثة أيضاً ما حدث في عام( 2012 )، عندما اتهمت اللجنة الوطنية الديمقراطية للحزب الديمقراطي الامريكي المخابرات الروسية باختراق خادم للولايات المتحدة وحذف عدد كبير من الرسائل الالكترونية الخاصة بمرشح الحزب الجمهوري للرئاسة دونالد ترامب (Nakashima,2018, p.33).

وكان آخر الهجمات السيبرانية ما حدث في ايلول (2024) من قيام الكيان الصهيوني باختراق أمني كبير لعناصر حزب الله من خلال أجهزة الاتصالات اللاسلكية التي يستخدمونها في الاتصال ، وخلف الهجوم عشرات الشهداء ومئات الجرحى، لمزيد من التفاصيل حول هذا الموضوع ينظر الموقع الالكتروني ( https://arabic.cnn.com/middleeast/article/2024/09/17 / - ).

من كل ذلك نلاحظ أن الهجمات السيبرانية قد مرت بمراحل تطور سريعة ، وأخذت تشكل أضراراً بالبنى التحتية للدول ، وكذلك من الممكن أن تحدث بمثابة الرد على هجوم مسلح قد يحدث من الدول، او لأغراض سياسية او تتعلق بالأمن الوطني .

ثانياً : تطور الأساليب التقنية في الهجمات السيبرانية وأنواعها .

إن الأساليب التقنية في الهجمات السيبرانية شهدت تطورًا ملحوظًا في السنوات الأخيرة؛ مما أدى إلى زيادة تعقيد هذه الهجمات وصعوبة اكتشافها والتصدي لها. تتضمن هذه التطورات استخدام تقنيات متقدمة مثل الذكاء الاصطناعي والتعلم الآلي، فضلا عن استهداف البنية التحتية الحيوية والاعتماد على هجمات سلسلة التوريد.

1. استخدام الذكاء الاصطناعي والتعلم الآلي:

أصبح المهاجمون يستغلون تقنيات "الذكاء الاصطناعي" والتعلم الآلي لتحسين فعالية هذه الهجمات، على سبيل المثال، يمكن استخدام "خوارزميات التعلم الآلي" لتحليل سلوك المستخدمين، وتحديد أفضل الطرق لتنفيذ هجمات التصيد الاحتيالي، كما يمكن استخدام "الذكاء الاصطناعي" لتطوير برامج خبيثة قادرة على التكيّف مع بيئات مختلفة، وتجاوز أنظمة الكشف التقليدية (Raineri, 2021,P. 222).

2. استهداف "البنية التحتية" الحيوية:

أصبحت "الهجمات السيبرانية" تستهدف بشكل متزايد البنية التحتية الحيوية، مثل شبكات الكهرباء والمياه والأنظمة الصحية، كما يمكن أن تؤدي هذه "الهجمات" إلى تعطيل الخدمات الأساسية، والتسبب في أضرار جسيمة، فمثلاً هجوم "Stuxnet" الذي استهدف منشآت نووية في إيران يُعد من أبرز الأمثلة على هذا النوع من الهجمات ( Gao P. 35 , 2017 ).

3. **هجمات سلسلة التوريد:**

تتضمن هجمات سلسلة التوريد استهداف الموردين أو الشركاء في سلسلة التوريد للوصول إلى الهدف النهائي. يمكن أن تكون هذه الهجمات فعالة للغاية، إذ يستغل المهاجمون الثقة بين الشركات وموردیها. من الأمثلة البارزة على ذلك هجوم "SolarWinds" الذي أثر على العديد من المؤسسات الحكومية والخاصة (Kanno, 2020, P.115).

4. هجمات الفدية المتقدمة:

تطورت هجمات الفدية لتصبح أكثر تعقيدًا، إذ يقوم المهاجمون بتشفير بيانات الضحايا والمطالبة بفدية لإعادتها. بالإضافة إلى ذلك، بدأ المهاجمون في تهديد الضحايا بنشر البيانات المسروقة إذا لم يتم دفع الفدية، مما يزيد من الضغط على الضحايا للاستجابة لمطالبهم(Khan, 2018,P.400).

وعليه فإن استخدام الأساليب التقنية الحريثة في الهجمات السيبرانية، يطرح تحديات قانونية جدية لم يُحسم أمرها بالكامل في القانون الدولي، إذ إن هناك حاجة ماسة لتطوير اتفاقيات دولية جديدة، مثل اتفاقية شاملة للأمن السيبراني، تحدد المسؤوليات القانونية للدول والجهات الفاعلة غير الحكومية، وتعزز آليات إسناد الهجمات، والرد عليها ضمن إطار القانون الدولي.

أما فيما يتعلق بأنواع الهجمات تختلف الهجمات الإلكترونية اختلافًا كبيراً في طبيعتها وحجمها ونطاقها، تبعاً لاختلاف أنواعها، ومن أبرز هذه الأنواع:

1- هجمات الحرمان من الخدمات (DDoS): وهي أكثر أشكال الهجمات السيبرانية انتشاراً في السنوات الأخيرة، إذ يستخدم المهاجم في هكذا نوع من الهجمات فايروسًا للسيطرة على عدد كبير من أجهزة الكمبيوتر؛ ويسبب الهجوم بزيادة هائلة في عدد الزيارات على موقع الشبكة التي تؤدي إلى توقفها، وقد وقع هجوم (DDoS) الأبرز في إستونيا عام( 2007) ، وكانت عواقبه تهدد الحياة تقريبًا؛ بسبب إغلاقه خط الطوارئ وعدم تمكن المواطنين من طلب سيارة إسعاف، أو تسبب في إبقاء شاحنة إطفاء خارج الخدمة لمدة ساعة، كما نفذت روسيا هجوماً من هذا النوع على جورجيا في صيف(2009) ، عندما وجدت البلاد نفسها غير قادرة على التواصل مع العالم الخارجي(Khan, 2017, p.5) .

2- هجمات تقويض أنظمة التشغيل والتحكم : هذه الهجمات أكثر خطورة من هجمات (DDoS)؛ لأن هذا النوع من الهجمات يهدف إلى تقويض أنظمة التحكم، وتستخدم كود كمبيوتر ضارا أو برامج ضارة مثل الديدان، والفايروسات، وأحصنة طروادة؛ لاختراق أنظمة تشغيل الكمبيوتر، ولا تدمر هذه الهجمات نظام تشغيل الكمبيوتر؛ بدلاً من ذلك تؤدي إلى ظهور نظام الكمبيوتر على أنه يعمل بشكل طبيعي، حتى مع فشله، ومن الامثلة على هذا النوع من الهجمات فيروس(Stuxnet) الذي هاجم المفاعلات النووية الايرانية؛ مما أدى إلى تراجع برنامجها النووي( Khan, 2017, p.6) .

3- التسلل إلى شبكة كمبيوتر آمنة : يقوم هذا النوع من الهجمات على مجرد اختراق مهاجم لشبكة كمبيوتر آمنة، دون أن يدمر عادةً شبكة الكمبيوتر، أو البنية التحتية التي يسيطر عليها؛ ومن أمثلته الهجوم الذي نفذته الولايات المتحدة في عام( 2003) ، قبل وقت قصير من غزو العراق، إذ تسللت إلى نظام البريد الإلكتروني التابع لوزارة الدفاع العراقية للاتصال بالضباط العراقيين وتوجيه تعليمات الاستسلام السلمي (Hathaway,2012, p.839)..

الفرع الثالث : آثار الهجمات السيبرانية

للهجمات السيبرانية مزايا وعيوب نبحثها بالنقاط الآتية :

أولاً: مزايا الهجمات السيبرانية

لم تتطرق الكتب العلمية ولا الوثائق ذات الصلة إلى مزايا هذه الهجمات، ومع ذلك فقد لاحظنا أنَّ الهجمات السيبرانية توفر فوائد معدودة لكنَّها جديرة بالذكر، وأهمها؛ إنَّها تجعل من الصراعات المستقبلية أقصر أمدا، وأقل ضرراً على حياة الإنسان، مما قد يسهل الانتعاش الاقتصادي والدبلوماسي بعد الحرب (Schreier, 2015, p.103)، كما يمكن استخدام هذه الهجمات في المسائل التي يكون فيها الحد من الضرر الماديّ للهجوم التقليدي مصدر قلق؛ وكمثال على ذلك فإنَّ الهجوم السيبراني الإسرائيلي على سوريا في عام( 2002)، إذ ساعد هذا الهجوم التقليدي على إتمام مهامه دون تدمير واسع النطاق للممتلكات أو خسائر في الأرواح على أي من الجانبين.

كما يمكن شن الهجمات السيبرانية من مواقع بعيدة آمنة (Schreier, 2015,p.113)، فالهجمات السيبرانية لا تتطلب تقابل جيشين، أو هجوم مادي كما هي الحال في النزاع التقليدي.

**ثانياً : عيوب الهجمات السيبرانية**

1- تؤثر على نظام الكمبيوتر أو الشبكة المستهدفة؛ فيؤدي إلى توقفها عن العمل مسببةً عواقب اقتصادية كبيرة؛ خصوصاً وأنَّ أغلب التعاملات أصبحت تُدار عبر الانترنت والوسائل التكنلوجية الأخرى.

2- تؤدي إلى فقدان ثقة مستخدمي الإنترنت عند استخدامهم للموارد عبر الإنترنت لأداء مهام معينة؛ مثل تقديم الإقرارات الضريبية عبر الإنترنت، أو حتى التسوق عبر الإنترنت، وفي حال حصول تجنب واسع النطاق عن هذه الأنشطة عبر الإنترنت، فقد تؤدي إلى شل التجارة الإلكترونية (Kesan,2011,p.445).

3- مشكلة الإسناد؛ إذ تتميز الهجمات السيبرانية بمجهولية فاعلها, وأنَّ أكثر الهجمات السيبرانية تأثيراً لم يُعرف فاعلها الأصلي لحد الآن؛ كما هو الحال في هجوم إستونيا عام(2007)، والهجوم على المفاعلات النووية الإيرانية في عام( 2008 ) الذي اتُهِمت به الولايات المتحدة وإسرائيل ، لكن لم يتم إثبات ذلك لغاية الآن، وسبب ذلك يعود إلى قدرة المهاجمين السيبرانيين على إخفاء هويتهم، وعدم الكشف عنها(Khan, 2017, p.10).

**المطلب الثاني**

**مدى انطباق مبدأ التناسُب على الهجمات السيبرانية**

قبل أن نتطرق لِمدى انطباق مبدأُ التناسُب على الهجمات السيبرانية؛ سنحاول معرفة ما إذا كان الهجوم السيبراني يصل إلى درجة" استخدام القوة" أو حتى "هجوم مسلح" لكي ينطبق عليه مبدأ التناسب، فقد كان للتباين بين النزاع التقليدي( الحركي )، والنزاع السيبراني(الالكتروني) آثار واسعة من جهة تصورنا للنزاع، فقواعد "النزاعات المسلحة"، والقواعد المنظمة "لاستخدام القوة" في العلاقات الدولية التي يتضمنها "ميثاق الأمم المتحدة "وُضِعَت لتتلاءم مع النزاع التقليدي "الحركي"؛ وعلى الرغم من أن المبادئ الرئيسة لهذه القواعد ما زالت صالحة للتطبيق؛ ولكن كيفية تطبيقها على الهجوم السيبراني في أي حالة مُعيَّنة أمر يشوبه ـ على أحسن تقدير ـ الغموض في الوقت الحاضر، فالمعتقدات البديهية للقادة( ومستشاريهم القانونيين) صُقِلت في بيئات النزاع التقليدي وما عدا قلة من المتخصصين لا يوجد لديهم على نطاق واسع فهم للهجوم السيبراني داخل أوساط قادة القوات المسلحة اليوم (هنكرتس، 2005، 523).

الفرع الأول:" الهجوم السيبرانيّ بوصفه "هجوماً مُسلحاً:"

سنحاول هنا توضح مدى إمكانية وصف" الهجمات السيبرانية" هجوماً مسلحاً؛ وذلك لأن العديد من مبادئ القانون الدولي الإنساني، وأبرزها مبدأ التناسب، تنطبق فقط على حالات الهجوم المسلح .

بالرجوع إلى ميثاق الأمم المتحدة لعام( 1945) ، نجده يتضمن ـ بهذا الصدد ـ على مصطلحين مختلفين يشيران للهجمات المسلحة، إذ تشير الفقرة (4) من المادة (2) الى مصطلح (استخدام القوة )، والآخر ( الاعتداء المسلح ) بموجب المادة (51) من الميثاق، وبالرغم من عدم وجود تعريف محدد لمصطلح( استخدام القوة)؛ إلا أنَّنا نلاحظ أنَّه واسع؛ إذ يشمل فئة واسعة من مجموعة الأعمال العدوانية، من الأقل تدميراً إلى الأكثر تدميراً، أما( الاعتداء المسلح)؛ فإنَّه يدلُ على الأعمال العدوانية الأقوى أو الأكثر تدميراً وضرراً من (استخدام القوة)؛ لِذا فإن" استخدام القوة "يصف شيئاً أقل من( هجوم مسلح)، ومن ثمَّ يمكن أن تكون الدولة ضحية لهجوم يشكل" استخدامًا للقوة"، إلا أنه ليس شديدًا بما يكفي ليكون( هجوماً مسلحًا)(Kesan,2011,p.114).

ويبدو واضحاً أنَّ الهجوم السيبراني قد يشكل في بعض حالاته( هجوماً مسلحاً)، وهذا ما لاحظناه في الهجوم السيبراني على إستونيا عام (2012) ؛ فقد كان خطيراً للغاية لدرجة أن( جاك ايفيكسو)، وزير الدفاع الإستوني حينها فكر في التذرع بالمادة (5) من اتفاقية حلف شمال الأطلسي( الناتو) لعام (1949)، التي تنص "على أن الهجوم على دولة حليفة واحدة يُعد هجوماً عليهم جميعاً"، ومن ثمَّ فإنَّ الحلف مُلزم بمهاجمة المعتدي؛ في الوقت الذي اشتبه فيه أنَّ روسيا تقف وراء هذه الهجمات، لكن تدخل حلف شمال الأطلس اقتصر على إرسال فرقًا من خبراء أمن الكمبيوتر لمساعدة السلطات الإستونية على التعامل مع الموجة الهائلة من الهجمات السيبرانية( Scott,2009,p.193).

لذا ذهب بعض الباحثين، ونحن نؤيدهم، إلى أنَّ الهجوم السيبراني يمكن أن يعد هجوماً مسلحاً؛ إذا كان السلاح السيبراني قد استخدم ضد ممتلكات أو أشخاص دولة، من قبل دولة أجنبية كانت على علم بالجهة التي قامت بالهجوم، وأن تكون هذه الجهة تحت سيطرتها القانونية؛ مما يدل على رضا الدولة المعنية باستخدام السلاح السيبراني ضد الدولة المتضررة (Kesan,2011,p.517).

كما يشير( دايفيد غراهام) إلى أنَّ الهجوم السيبراني قد يصل إلى درجة هجوم مسلح يوجب تحمل الدولة مصدر الهجوم للمسؤولية الدولية (Graham,2010,p.93)، بينما يرى( سكوت شاكلفورد) أن الهجوم السيبراني يؤدي إلى آثار كارثية موازية تمامًا للهجوم التقليدي؛ مما يعني أنَّه يؤيد ضمناً إمكانية اعتبار الهجوم السيبراني
سلاحاً حربياً، ويؤيد ذلك ما ذهبت إليه( إين إرجما)، رئيس البرلمان الإستوني السابقة والحاصلة على دكتوراه في الفيزياء النووية، إذ قالت" :عندما أنظر إلى الانفجار النووي والانفجار الذي حدث في بلدنا في مايو، أرى نفس الشيء ... كما هو الحال مع الإشعاع النووي، إذ يمكن للحرب السيبرانية تدمير دولة حديثة دون إراقة الدم"(Scott,2009,p.194).

وإذا أخذنا بالحسبان ما توصلنا إليه من أنَّ الهجوم السيبراني يُشكل استخداماً للقوة، وقد يصل في بعض الحالات إلى حد الهجوم المسلح، فإننا نرى أنهُ قد يصل إلى مستوى نزاع دولي في حال تبادل هذه الهجمات بين بلدين أو أكثر؛ مما يستوجب تطبيق قواعد "القانون الدولي الإنساني" عليه؛ لأن المادة (2) المشتركة في" اتفاقيات جنيف" الاربعة لعام( 1949) ، اعتبرت الاعتداءات الفعلية بين بلدين أو أكثر بحكم الحرب حتى وإن لم تُعلن الدول عن وجود حالة حرب.

الفرع الثاني: تطبيق مبدأ "التناسُب" على" الهجمات السيبرانية"

مبدأُ "التناسُب" من المبادئ المهمة التي تمثل "القانون الدولي الإنساني"، وهو مبدأ ذو شمولية تتسع لجميع "النّزاعات المسلحة الدوليّة وغير الدولية"، التي تستخدم مختلف الأسلحة فيها بالعادة، ومبدأُ التناسُب ذو طبيعة ميدانية عملية، والذي يحظر" شن هجوم مسلح، قد يؤدي إلى خسائر جانبية في أرواحِ المدنيين وممتلكاتهم، أو بالأعيان المدنيّة والبنى التحتية" . ولا بد من الإشارة الى أنه تم اعتماد هذا المبدأ في المواد (51) و (57) من "البروتوكول الإضافيّ الملحق باتفاقياتِ جنيف لعام 1977".

وفي إطار خصوصية" الهجمات السيبرانية" عندما تكون سلاح أو أداة عسكرية في إطار "النزاعات المسلحة"، نجد أن هنالك صعوبة في تطبيق هذا المبدأ ؛ تتمثل بعدم إمكانية التمييز بين" الفضاءِ السيبرانيّ" المُستخدم للأغراض المدنيّة أو من قبل المدنيين، وبين "الفضاءِ السيبرانيّ" المُستخدم للأغراض العسكريّة عندما تستخدمه أطراف النزاعات المسلحة، ولأن مبدأ "التناسُب" يتضمن إجراء نوع من الموازنة بين المعاناة أو التدمير، وبين الميزة العسكرية المبتغاة؛ لأننا أمام فقدان معايير واضحة لتقييم ما هو مقبول من درجة المعاناة الإنسانية المقبولة عند تعطيل بعض المنشآت المدنية التي توفر أو تضمن استمرار تقديم الخدمات الأساسية للمدنيين، كالكهرباء والاتصالات والخدمات الطبية مثلا، التي سوف يكون لتوقفها أو تدميرها أثر حقيقي للهجمات السيبرانية التي يترتب على القيام بها إيقاف تلك الخدمات المرتبطة بالجانب الإنساني( الحديثي، 2021 ، ص 132).

وبالرغم من تلك الصعوبات في تطبيق مبدأ التناسُب وفقا لما ينبغي في إطار ارتكاب هجمات سيبرانية، إلا أننا نجد أن دليل( تالين )المطبق في حالة الحروب و"الهجمات السيبرانية"، قد أشار إلى تطبيق مبدأ "التناسُب" من حيث "منع القيام بهجمات سيبرانية يترتب عليها خسائر بين أرواح المدنيين أو إصابات أو أضرار تصيب الأعيان المدنيّة، والتي يكون فيها نوع من المغالاة والإفراط غير المبرر، لا يتناسب مع غاية تحقيق الميزة العسكرية التي يراد الحصول عليها أو تحصيلها باستخدام هجمات سيبرانية"( شميت، 2002 ، ص107 ) .

ينطبق مبدأُ التناسُب الوارد في المادتين (51) و(57) من البروتوكول الإضافيّ الأول لاتفاقيات جنيف لعام (1949) ، على حالات الهجوم المسلح، وإن مفهوم الهجوم المسلح، كما مر بنا، لم يعد قاصراً على إطلاق القوة الحركية؛ فقد يُحدِث الهجوم السيبراني آثاراً ضارة على دولة ما بشكل مواز للأثر الذي يُحدِثهُ الهجوم المسلح التقليدي، أو يزيد عنه، وإنَّ هذا الأثر الضار هو الذي يحدد نوع الهجوم أكثر من الهجوم ذاته.

يتطلب مبدأُ التناسُب عدة أمور يجب مراعاتها في الهجوم؛ أولها : معيار الرعاية الدائمة أو المتواصلة كما عبرت عنها المادة (57) من البروتوكول الإضافي الأول، التي جاءت بعنوان (الاحتياطات في الهجوم)؛ فالفقرة الأولى من هذه المادة تفرض شرطًا قانونيًا عامًا على العمليات العسكرية، الشرط القانوني هو ممارسة الرعاية الدائمة، بالرغم من أنَّ هذا المصطلح غير معرَّف سواء في المادة (57) ، أو في تعليق" اللجنة الدوليّة للصليب الأحمر" ، أو بصورة عامة في خطاب الاعتماد؛ إلا أن التطبيق دقيق هذا المبدأ في العمليات العسكرية يُشير على الأقل إلى أن القائد لا يمكنه تجاهل الآثار على السكان المدنيين.

وإذا ما عكسنا ذلك على العمليات السيبرانية ؛ فإنَّ الرعاية المتواصلة تتطلب من قائد الهجوم السيبراني الحفاظ على الوعي بالموقف في جميع الأوقات، بما في ذلك جميع مراحل العملية، لكن هذا صعب جداً، نظراً لأن كل عملية إلكترونية تقريبًا ستعمل على اجتياز "البُنيّة التحتيّة السيبرانية المدنية"، أو التأثير عليها، أو استخدامها أو إتلافها.

من التطبيقات المعاصرة لهذا المعيار الهجوم ببرنامج (Stuxnet) سيئ السمعة عام (2009) الذي سبقت الإشارة اليه، إذ من الواضح أنَّ الهجوم كان يستهدف المنشآت النووية الإيرانية، لكن التقارير تُظهر أنه انتشر أوسع من ذلك بكثير، إذ إنه انتشر أوسع مما كانت تعتزم الولايات المتحدة وإسرائيل؛ وبهذا فإن الانتشار غير المقصود للفايروس خرق على الأقل معيار الرعاية الدائمة؛ لِذا يجب على القادة وجميع الأشخاص الذين يقومون بالعمليات السيبرانية أن يعترفوا ويقبلوا بالالتزام القانوني الخاص بممارسة العناية المستمره في جميع العمليّات العسكرية، بما في ذلك العمليات السيبرانية (Jensen, 2012,p.203).

أما الأمر الثاني: فهو معيار الآثار غير المباشرة للهجوم، ونعني به "الإضرار أو الخسائر التي تُصيب المدنيين أو الأعيانِ المدنيّة"، أو حدوث الخلط في هذه الخسائر والأضرار، وقد أشارت إليه المادة (51/5/ب) من البروتوكول الإضافي الأول لاتفاقيات جنيف لعام (1949) ، التي تنص : "من بين هجمات أخرى، تعدَّ الأنواع الآتية من الهجمات بمثابة هجمات عشوائية ... ب – الهجوم الذي يمكن أن يتوقع منه أن يسبب خسارة في أرواح المدنيين أو إصابة بهم أو أضراراً بالأعيان المدنية، أو أن يحدث خلطاً من هذه الخسائر والأضرار، يفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة" ( وقد أشارت إلى هذه الآثار أيضاً مقدمة "اتفاقيّة حَظر أو تقييّد استعمال أسلحة تقليدية معينة يمكن وصفها بأنها مفرطه الضّرر أو عشوائيّة الأثر لعام (1980)" والمعدلة في عام (1996) .

ابتداءً؛ يحظر القانون الدولي الإنساني بشكل عام جعل المدنيين أهدافًا للهجوم، ولكن بعض الهجمات على الأهداف العسكرية قد تؤدي إلى اصابات أو خسائر في أرواح المدنيين؛ لذا فإنَّ مبدأ التناسُب يمنع القادة من الإقدام على هجوم إذا توقعوا أن الوفاة والإصابة والأضرار التي يُسببها هذا الهجوم مفرطة وتفوق الميزة العسكريّة الملموسة والمباشرة المتوقعة.

وإذا ما نظرنا إلى الهجمات السيبرانية سنجد أنها تملك القدرة على التسبب بخسائر وأضرار في أرواح المدنيين أو ممتلكاتهم، كما أن الغالبية العظمى من العمليات السيبرانية المعروفة نتج عنها ضرر في الأعيان المدنية؛ بما في ذلك الكابلات والخوادم وأجهزة التوجيه التي تتألف من أغراض مدنية، يملكها ويديرها مدنيون؛ وإن أي ضرر يلحق بعناصر البنية التحتية للإنترنت سيعد ضرراً مدنيًا يتعارض مع مبدأ التناسب.

وبالرغم من أن واضعي البروتوكول الإضافيّ الأول لعام (1977 ، لم يتوقعوا الحرب السيبرانية، إلا أنَّهم أدركوا أن التقدم الإلكتروني في التكنولوجيا سيؤثر على الطريقة التي ستخوض بها الحروب وتأثيراتها المحتملة على المدنيين، ويمكن أن نلمس ذلك في تعليق اللجنة الدولية للصليب الأحمر، إذ لاحظت أنه: " أشير أيضًا إلى أن الوسائل الإلكترونية الحديثة أتاحت تحديد الأهداف العسكرية، لكنها لم تقدم معلومات عن وجود عناصر مدنية داخل هذه الأهداف أو بالقرب منها"، وبالرغم من أن هذا ليس صحيحاً تمامًا في الحرب السيبرانية، إلا أن هذه الفكرة تؤثر بالتأكيد على تطبيق مبدأ "التناسُب" على الهجمات السيبرانية(Jensen, 2012,p.204).

يُثير هذا المعيار مسألتين غاية في الأهمية؛ تدور المسألة الأولى حول كيفية تحديد الضرر عند استخدام أدوات الإنترنت لشن هجوم؛ هناك عدة طرق في تحديد ما يعادل الضرر في المجال السيبراني، أدقها نهج الوظائف؛ ومفاده أن الضرر يشمل أي انقطاع خطير في الوظائف، كأن يؤدي إلى استبدال أجزاء أو إعادة تحميل أنظمة البرامج، على سبيل المثال، إذا أغلق هجوم إلكتروني منفذ اتصال لكنه ترك بقية الكمبيوتر دون تأثر، فسيظل الكمبيوتر قيد التشغيل؛ ولكن وظيفته الفعلية قد تتأثر بشدة، ويبدو أن هذا النهج هو الأفضل في تطبيق مبدأ "التناسُب" على" الهجوم السيبراني"، إذ يأخذ في الاعتبار الجوانب الفريدة للعمليات الإلكترونية (Jensen, 2012,p.204).

المسألة الثانية : والأهم؛ تتمثل في طريقة قياس التأثيرات غير المباشرة في الحرب الإلكترونية، إذ تُعرَّف التأثيرات غير المباشرة بأنَّها: "النتائج المتأخرة أو البعيدة من الدرجة الثانية فصاعداً، والتي تنشأ من خلال أحداث أو آليات وسيطة"، في المجال السيبرانيّ، ستشمل هذه الاثار، الاضرار التي لم تكن مقصودة من الهجوم، كما لو تم الهجوم على نظام كمبيوتر عسكري سيؤدي إلى إيقاف تشغيل النظام، ثم تنتشر البرامج الضارة أيضًا إلى الأنظمة المدنية وتغلقها أيضًا؛ بسبب الروابط بين الانظمة العسكرية والمدنية ، وهذا ما حصل في هجوم ( Stuxnet ) داخل ايران ( Jensen, 2012,p.208).

لذا فإنَّ مبدأ التناسُب يفرض على القائد في هجوم سيراني أن يؤسس قراره بناءً على ما توقعه من الآثار، على ضوء المعلومات التي كانت لديه في ذلك الوقت، ومثال ذلك ما حصل أثناء الهجمات الأمريكية على العراق عام( 2003)، إذ فكر المهاجمون الإلكترونيون" للولايات المتحّدة" في مهاجمة "الحسّابات الماليّة " للرئيس العراقي المخلوع (صدام حسين) في محاولة للضغط عليه، ومع ذلك، تم إلغاء الهجمات عندما تقرر أن الهجمات قد تؤثر على النظام المصرفي الأوروبي وستكون لها تداعيات وآثار سلبية(Markoff,2009,p.33) .

أخيراً فإن مبدأ التناسُب يحظر شن هجوم يمكن وصفه عشوائيًا، وذلك في حال عدم قدرة المهاجم على تحديد مدى تأثير الهجوم أثناء التحضير لهجوم عبر الإنترنت، أما إذا كان المُهاجم غير قادر على جمع معلومات كافية عن طبيعة النظام المستهدف المقترح، فينبغي أن يقتصر الهجوم على تلك الأجزاء فقط من النظام التي لديه معلومات كافية للتحقق من حالتها كأهداف قانونية.

## المبحث الثاني

## "التناسُب" في استخدامِ الأسلحة الذّاتيّة

**سنتناول هذا المبحث في مطلبين: الأول نتحدث فيه عن مفهوم الأسلحة الذاتية، والثاني سنتناول فيه مدى انطباق مبدأ "التناسُب" على الأسلحة الذاتية.**

### المطلب الأول

### مفهوم الأسلحة الذّاتيّة

**سنحاول توضيح مفهوم الأسلحة الذاتية من خلال الفروع الآتية:**

**الفرع الأول: تعريف الأسلحة الذّاتيّة:**

في الكتب العلمية والوثائق الحكومية الرسمية، لا يوجد تعريف مقبول عالميا لتحديد معنى الأسلحة الذاتية، ومع ذلك ولأجل التوصل إلى تعريف مقبول فإنه لا بد من بيان معنى "الذاتية" ، فلا يمكن أن يفهم هذا المصطلح بالمعنى الفلسفي والأخلاقي بأنه الإرادة الحرة للفرد، فحتى الروبوتات المستقلة لا يمكنها العمل إلا في حدود الإمكانيات المبرمجة عليها عن طريق الخوارزميات، فلا يوجد نظام مستقل تماما، ولا بد وعند نقطة معينة أن يشارك الإنسان في صنع خوارزمية القرار ( Geiss,2015,p.6 ) ؛ فالأسلحة الذاتية وإن كانت تحمل هذه التسمية إلا أنها ليست مستقلة بالمعنى الحقيقي والكامل لهذه التسمية.

بعد بيان معنى الذاتية سنتطرق إلى التعريفات التي وضعت لهذا النوع من الأسلحة:

حسب التوجيه الصادر وزارة الدفاع الأمريكية(dodd,3000,09) فإن السلاح الذاتي هو السلاح الذي بإمكانه تحديد الأهداف والاشتباك معها دون تدخل إضافي من قبل العامل البشري (البصيصي ، 2023، ص 18).

ووفقا لمقرر الأمم المتحدة المعني بحالات الإعدام تعسفا تشير الأسلحة الذاتيّه إلى أنظمة الأسلحة الإلية التي يمكنها بمجرد تفعيلها تحديد الأهداف والاشتباك معها دون تدخل إضافي من البشر والعنصر المهم هو أن السلاح لديه خيار مستقل فيما يتعلق باختيار الهدف واستعمال القوة المميتة(Heyns,2013,p.83) .

وقد اقترحت" اللجنة الدوليّة للصليب الأحمر" أن" الأسلحة الذاتيه"، "هو مصطلح شامل من شأنه أن يضم أي نوع من أنواع الأسلحة سواء كانت تعمل في الجو أو على البر أو في البحر بتلقائية، وهذا يدل على أنه سلاح يمكنه أن يختار أي يبحث ويكشف ويحدد ويتعقب، ويهاجم أي يستخدم القوة ضد العدو أو يضر أو يدمر أهدافاً دون تدخل البشر، أي بعد التشغيل الأوليّ، تقوم منظومة السلاح بنفسها باستخدام أجهزة الاستشعار والبرمجة بعملية الاستهداف والعمليات التي عادة ما يتحكم بها البشر" (Righetti,2018,p.26). .

ومن بين التعاريف التي وردت نحن نميل إلى تعريف اللجنة الدوليّة للصليبِ الأحمر, ونرى أنه الأقرب للصحة لأنه قام بتعريف آلية عمل هذه الأسلحة ومعنى الذاتية فيها.

الفرع الثاني –التطور التاريخي للأسلحة الذاتية:

شهدت نهاية القرن التاسع عشر الجهود الأولى لتطوير ما يعرف بالأنظمة غير المأهولة التي تعد الخطوة الأولى للأسلحة الذاتية، فقد قام المخترع نيكولا تيسلا بتطوير النظام(UMS) لأول مرة, وذلك بصنعه لقارب يعمل عن بعد, ولكن اختراعه هذا لم يدخل في الخدمة أبدا.

ثم شملت التطورات صناعة ما يسمى (kattering bug ) وهي طائرة بلا طيار كانت قادرة على حمل المتفجرات، وقد تم تطويرها في أعقاب الحرب الثانية، وبعد ذلك بنصف قرن وبعد ابتكار نظام تحديد المواقع الذي لعب دوراً في تطوير مجال الاتصالات( GPS) العالمي وتطوير الأجهزة التي يتم تشغيلها عن بعد؛ فأحدث ذلك طفرة نوعية في عالم الأسلحة الذاتية, وقد تم استخدام أول طائرة بلا طيار حديثة في عام (1982) خلال عمليات وادي البقاع في لبنان, وقد نشرها الجيش الإسرائيلي لأغراض المخابرات والاستعمال للخداع، ثم تسارعت بعد ذلك وتيرة صنع الطائرات بلا طيار أو ما يعرف (DRON) ، وقد تسابقت الدول في الإنفاق للحصول على أكبر عدد منها( Wagner, 2014,p.1365_1377).

الفرع الثالث : مدى شرعية استخدام الأسلحة الذاتية :

تُثير مسألة شرعية استخدام "الأسلحة ذاتية" التشغيل في "القانون الدولي الإنساني"، نقاشًا واسعًا بين الباحثين والخبراء القانونيين، نظرًا للتحديات القانونية والأخلاقية التي تطرحها هذه التكنولوجيا المتقدمة، ويعد السلاح حديثاً من وجهة نظرنا في حالتين: الأولى: درجة تطوره وخصائصه التدميرية الناتجة عن استخدامه في الهجوم أو الدفاع، والثانية : في حالة عدم وجود قواعد قانونية تنظم استخدام هذه الأسلحة .

وهناك مبادئ مطبقة في القانون الدولي الإنساني تثبت عدم شرعية الأسلحة "ذاتية التشغيل" نذكر منها :

المبدأ الأول: المعاناة المفرطة أو الآلام التي لا مبرر لها

تعود جذور هذا المعيار إلى إعلان سان بطرسبيرج، إذ جاء في ديباجته "حظر الأسلحة التي من شأنها أن تفاقم – دون أي داع – آلام الرجال"، وكذلك نص على هذا المبدأ في مشروع إعلان "بروكسل " سنة ١٨٧٤، ثم تأكد هذا المبدأ من خلال لائحة "لاهاي" القوانين وأعراف الحرب البرية سنة ١٨٩٩ ، إذ نصت على "حظر استعمال أسلحة، أو قذائف أو مواد من شأنها أن تتسبب في معاناة غير ضرورية"، وقد ورد ذات النص في المادة (5/23) من لائحة "لاهاي لقوانين وأعرف الحرب البرية سنة ١٩٠٧" إذ استبدلت كلمة "المعاناة المفرطة" بكلمة "إصابات وآلام لا مبرر لها " ( محمد عبد العال الخضرى, 2023 ص 469).

وقد منح "البرتوكول الإضافي الأول الملحق باتفاقيات جنيف لسنة ١٩٧٧"، هذا المبدأ مرتبة "القاعدة الأساسية" المستقلة بذاتها، إذ نصت المادة (2/35) من البرتوكول على: " يحظر استخدام الأسلحة والقذائف والمواد ووسائل القتال التي من شأنها إحداث إصابات وآلام لا مبرر لها ".("البروتكول الاضافي الاول المحلق باتفاقيات جنيف1977 " ).

وبالنظر إلى الترادف في صياغة نص المادة (5/23) من "لائحة لاهاى" ، والمادة (2/35) من "البرتوكول الاضافي لاتفاقيات جنيف 1977" نجد أن صياغة نص المادة الأخيرة عام وشامل، إذ لا يتحدد مفهوم وأساليب الحرب على بعض أنواع من الأسلحة؛ بل يتسع مفهومها ليشمل كل ما من شأنه أن يتسبب في "آلام لا مبرر لها"، بغض النظر عن طابعه أو نوعه، والتي من بينها الأسلحة "ذاتية التشغيل" .

وكذلك المادة (36) من "البروتوكول الإضافي الأول لعام(1977) الملحق باتفاقيات جنيف لعام (1949)" ، ألزمت أي طرف سامي مُتعاقد عند دراسته أو تطويره أو اقتنائه لسلاح أو وسيلة حرب أن يتحقق مما إذا كان ذلك محظوراً بمقتضى هذا البروتوكول، أو أي قاعدة أخرى من قواعد "القانون الدّوليّ الإنسانيّ".

عند النظر في هذه المادة نجد أن تعبير (سلاح) الوارد فيها واضح جدا ويقصد به "أي قدرة هجومية يمكن تطبيقها على هدف عسكري ،" وحسب" اللجنة الدولية للصليب الأحمر" والدول التي تجري مراجعات لهذا البروتوكول، فإن هذا التعبير يُقصد به" كل أنواع الأسلحة سواءً أكانت مضادة للأفراد أو العتاد أو كانت أسلحة قاتلة أو غير قاتلة" ، إلا أن المشكلة تكمن بوجود بعض الدول ومنها ألمانيا قد أضافت تحفظات لإعفاء أنواع معينة من الأسلحة من نطاق تطبيق المادة (36) فهي تقصر نص المادة مدار البحث على الأسلحة التقليدية؛ أما الأسلحة ذات الاستخدام المزدوج فإنها لا تخضع للمراجعة (McClelland,2003,p.404).

وهنا تكمن مشكلة الأسلحة الذاتية؛ إذ يمكن عدها ببساطة من الأسلحة ذات الاستخدام المزدوج فكما يمكن استخدامها للقتال، يمكن استخدامها لتفكيك القنابل وإنقاذ حياة الجنود، أو يمكن استخدامها لمجرد جمع المعلومات.

وهناك من يرى أن مشكلة شرعية الأسلحة الذاتية لا تكون بنص المادة (36) من" البرتوكول الإضافي الأول لعام (1977)" ، إنما تكون في قواعد ومعايير" القانون الدولي الإنساني" لمن يمكن أن يكون مقاتلا، فهناك شروط تتعلق بالقدرة العقلية، فلا يجوز تجنيد أصحاب الخلل العقلي؛ وذلك من أجل حماية حقوق الطرف المقاتل مما قد يحدثه صاحب الخلل العقل ، فمثل هؤلاء لا يمكن محاسبتهم أو الانتصاف منهم، وهذا الأمر يطبق على الأسلحة الذاتية, فمهما بلغت من درجة عالية بذكائها الصناعي فإنها لا يمكن أن تمتلك مثل قدرات العقل البشري الكامل(Chengeta,2016,p. 24) .

ونحن نؤيد الرأي الذي يذهب الى تطبيق مبدأ "المعاناة المفرطة أو الآلام التي لا مبرر لها" على الأسلحة ذاتية التشغيل عند تطوير أو اقتناء او اعتماد سلاح جديد، أو ابتكار أساليب ووسائل جديدة للحرب، وذلك إعمالاً لنص المادة (٣٦) من البرتوكول الإضافي الأول، الذي يلزم أي طرف عند دراسة أو تطوير اساليب جديدة للحرب، بالتأكد فيما إذا كانت هذه الأسلحة او الأساليب "محظورة في جميع الأحوال أو بعضها بمقتضى هذا البرتوكول"، أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها.

ونود أن نؤكد ـ وكما ذهب البعض وبحق( Weeramantry, C. G. Ed. (1999 ) ـ أن معيار أو مبدأ حظر الأسلحة وخصوصا الأسلحة ذاتية الاستخدام، التي تتسبب بمعاناه مفرطة أو آلام لا مبرو منها، يعد من "المبادئ العامة للقانون المعترف بها من جانب الأمم المتمدنة " .

**المبدأ الثاني : عشوائية الاثر**

من الجدير بالذكر بداية أن قواعد "القانون الدولي الإنساني" لم تضع تعريفاً جامعاً مانعاً للأسلحة عشوائية الأثر، إلا أنها ذكرت الحالات التي يمكن من خلالها معرفة كون "السلاح عشوائي الأثر"، ومن ثمَّ لا يجوز استخدامه ، ومن الواضح أن وهذا المبدأ هدفه حماية المدنيين من كوارث وإضرار الحرب، بالأخص "الأسلحة ذاتية التشغيل " التي تفتقد لعنصر التمييز بين "المدنيين والمقاتلين"، إذ تم تأكيد هذا المبدأ في المادة (٤٨) من "البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لسنة ١٩٧٧" ، التي نصت على: "يعمل أطراف النزاع على التمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية، ومن ثم توجه العمليات العسكرية ضد الأهداف العسكرية دون غيرها، وذلك من أجل تأمين وحماية السكان المدنيين والأعيان المدنية" ( محمد عبد العال الخضرى, 2023 ص 475).

وقد نصت المادة (٥١) من البروتوكول ذاته على: "يتمتع الأشخاص المدنيون بحماية عامة ضد الأخطار الناجمة عن العمليات العسكرية، ويجب لإضفاء فعالية على هذه الحماية مراعاة القواعد التالية دومًا، بالإضافة إلى القواعد الدولية الأخرى القابلة للتطبيق " ، إذ "لا يجوز أن يكون السكان المدنيون بوصفهم هذا محلاً للهجوم، وتحظر أعمال العنف والتهديد الرامية أساساً إلى بث الرعب بين السكان المدنيين" ، ومن أجل الحماية التي يقررها البرتوكول نص على بعض القواعد الخاصة بتحديد الأشخاص المدنيين والأعيان المدنية، نصّ فى المادة (٥٠) من "البروتوكول الإضافي الأول" على الآتي: " المدنى هو أى شخص لا ينتمي إلى فئة من الفئات المشار إليها فى البنود الأول والثاني والثالث والسادس

من الفقرة (أ) من المادة ٤ من الاتفاقية الثالثة والمادة (٤٣) من هذا الملحق البرتوكول، وإذا ثار الشك حول ما إذا كان شخص ما مدنياً أم غير مدنى فإن ذلك الشخص يعد مدنيا، يندرج في السكان المدنيين كافة الأشخاص المدنيين. لا يُجرد السكان المدنيين من صفتهم المدنية وجود أفراد بينهم لا يسرى عليهم تعريف المدينين"، و" لا يجوز استخدام المدنيين بوصفهم دروع، لمنع أو درء الهجوم على أهداف عسكرية أو لدرء الهجمات الموجهة ضد السكان المدنيين، أو استخدامهم كغطاء عسكرى لتغطية تحركات المقاتلين في تنفيذ أهدافهم العسكرية" . ( Kalshoven, F 1985, P.247 ) .

وقد أكدت "محكمة العدل الدولية" في رأيها الاستشارى بشأن الأسلحة النووية أنه " لا ينبغي للدول أبداً أن تجعل المدنيين هدفا للهجوم، ومن ثمَّ لا ينبغي لها أن تستخدم الأسلحة غير القادرة على التمييز بين الأهداف المدنية والعسكرية" (Smis, 1998, P. 78)

ويؤكد جانب فقهي أن هذه المبدأ لا يعد قاعدة عرفية فحسب، بل هي قاعدة من "القواعد الآمرة فى القانون الدولي الإنساني"( Hayashi, N. 2010, P. 87).

نظرًا للتحديات القانونية والأخلاقية المرتبطة بالأسلحة ذاتية التشغيل، يتعين على المجتمع الدولي العمل على تطوير إطار قانوني ينظم استخدامها، بما يضمن احترام المبادئ الأساسية "للقانون الدولي الإنساني" و"حماية المدنيين خلال النزاعات المسلحة".

**الفرع الرابع –آثار الأسلحة الذاتية :**

**سنبحث هذا الفرع في فقرتين :**

**أولاً: – مزايا الأسلحة الذاتية**

سنتطرق بداية على مزايا الأسلحة الذاتية؛ إذ يقدم المدافعون عن أنظمة الأسلحة الذاتية حججهم من الجانب العسكري ومن الجانب الأخلاقيّ.

فمن الجانب العسكري يرى المدافعون عنها أنها أداة لمضاعفة القوة العسكرية، كما أنها بإمكانها أن تقلل الخسائر البشرية في المعركة؛ إذ عن طريق استعمالها يمكن ازاحة عدد كبير من الجنود عن ساحة المعارك الخطيرة . كما تقدم وزارة الدفاع الأمريكية أسبابا أخرى للدفاع عن هذه الأسلحة، فهي تعد أكثر ملاءمة للمهام الخطرة أو القذرة، وتعطي مثالا على المهام الخطرة بالتخلص من الألغام المتفجرة، والمهام القذرة مثل المهام التي تتطلب تعرض البشر للمواد الإشعاعية الضارة.

إضافة إلى ذلك أظهرت وزارة الدفاع الأمريكية أهمية هذه الأسلحة ، وذلك عن طريق تقليل النفقات الحربية، فقد صرحت بأن أي جندي في أفغانستان يكلف البانتاغون حوالي (850) ألف دولار سنويا ، بالمقابل فإن( روبوت تالون) وهو عبارة عن عربة صغيرة يمكن تجهيزها بالأسلحة تكلف (230) ألف دولار فقط .إضافة إلى ذلك فإن هذه الأسلحة لا يمكن أن تتعرض للإجهاد البدني أو التعب أو الإرهاق عكس البشر تماما.

إما من الجانب الأخلاقيّ؛ فيرى المدافعون أن مثل هذه الأسلحة ستكون سببا في إبعاد البشر عن مناطق القتال الشديدة، ومن ثمَّ التقليل من الخسائر البشرية، كما يضيفون أن هذه الأسلحة لا ترتكب الجرائم التي قد يقوم بها الجنود كالاعتداءات الجنسية ، او الاعتداءآت بدافع الحقد والكراهية والمزاجية وغيرها(Etzioni, 2018, p.260).

**ثانياً: سلبيات الأسلحة الذاتية:**

أما عن سلبيات هذه الأسلحة؛ فيقدم تقرير هيومن رايتس ووتش لعام(2012) سردا مفصلا للإضرار التي قد تسببها الأسلحة الذاتية ، إذ يقدم التقرير الحجج الآتية:

1- أن إدخال مثل هذه الآلات للحرب واستبدال الوجود البشري بها، يكون من شأنه القضاء على أي فرصة لإظهار الرحمة أثناء المعركة، والتي يمكن أن تكون وسيلة لتقليل عدد القتلى.

2- أن وجود مثل هذه الأسلحة يمكن أن يقدم تسهيلا لأصحاب السلطة لخوض الصراعات دون المخاطرة بأوطانهم او الجنود البشر.

3- هنالك من يرى أنه لا يمكن مساءلة هذه الأسلحة ذات الذكاء الصناعي ، فليس من الممكن تحميل السلاح أو الروبوت مسؤولية أفعاله، فإذا ما حدثت حالات وفاة أو إصابة غير ضرورية بين المدنين فليس من الواضح من الذي يمكن مساءلته أو معاقبته.

4-ويرى العلماء أن مثل هذه الأسلحة قد لا تتوافق مع قواعد "القانون الدوليّ الإنسانيّ" ، فمبدأ التمييز بين المقاتلين وغير المقاتلين قد لا يكون متوافرا عند هذه الأسلحة، فعلى الرغم من أن هذه الآلات ستكون قادرة على اكتشاف البشر إلا أن أنظمتهم الحسية ليس باستطاعتها التمييز بين "المقاتل وغير المقاتل"، أو معرفة المقاتلين الجرحى، أو الذين استسلموا.

5- بالإضافة إلى ما سبق، فإن هذه الأسلحة ستتعارض مع كرامة الإنسان، فمثل هذه الآلات غير الحية لا يمكنها فهم قيمة الحياة أو احترامها، وعلى الرغم من ذلك يمكنها إزالة هذه الحياة بكل بساطة (Sharkey,2019.p.79).

الفرع الخامس : أنواع الأسلحة الذّاتيّة:

قبل البدء ببيان بعض أنواع الأسلحه الذاتيّة الموجودة حاليا، لا بد من الإشارة إلى أن هناك عددا قليلا نسبيا من المعلومات المتاحة للعامة لتقييم مدى الاستقلال الذي تتمتع به هذه الأسلحة، في اختيار أهدافها وأنواعها كالآتي:

1- أنظمة الأسلحة الثابتة : يعد هذا النوع هو صاحب أعلى مستوى من الاستقلال، وتشمل هذه الأنظمة الأسلحة الدفاعية للسفن، وأنظمة المدافع الثابتة ( تسمى عادة بنادق الح راسة)، وتستخدم العديد من البلدان حاليا أسلحة ذاتية للدفاع عن السفن، أو المنشآت الأرضية ضد الصواريخ، وقذائف الهاون، والطائرات ، والقوارب عالية السرعة، فهذه الأسلحة تقوم باختيار الهدف ثم الهجوم تلقائيا (Chavannes,2020,p.65). وحسب وزارة الدفاع الأمريكية فإنه لا يمكن لهذا النوع اختيار البشر كهدف ولكنه على الرغم من ذلك يمكنه مهاجمة المركبات المأهولة (Chavannes,2020,p.65 )، ومن أمثلتها صواريخ كاونتر.

2-أنظمة الأسلحة الأرضية :غالبا ما يستخدم هذا النوع لغرض الوصول إلى المناطق التي يصعب الولوج إليها، أو شديدة الخطورة على البشر، وتستخدم عادة في التخلص من القنابل، ولكن هذا النوع من الأسلحة نسبية الاستقلال فيه ضئيلة جدا، إذ يرى العلماء أنه لا بد من تحسين أنظمة الملاحة في التضاريس المعقدة لهذا النوع قبل أن يصبح سلاحا مستقلا تماما، وهناك من يرى أن التقدم التكنولوجي المتسارع سيجعل من هذا النوع مستقبل الحروب القادمة( Chavannes,2020,p.70 )، ومن أمثلة هذا النوع "أثينا" التي تكون عبارة عن دبابة صغيرة تعمل على الأرض وتحت الماء، وأيضاً الروبوت البشري " أطلس".

3-أنظمة الأسلحه الجويّة :خلال السنوات القليلة الماضية تم استخدام أسلحة الطائرات من دون طيار لتنفيذ بعض الهجمات ، ومن الأمثلة على ذلك قيام الطائرة (MQ8.Reaper )او الحاصدة التي تم استخدامها لقتل الجنرال قاسم سليماني وأبي مهدي المهندس على أرض العراق بتاريخ (2020/1/3) ، وتتميز هذه الطائرة بإمكانياتها العالية في تنفيذ الهجوم؛ نظراً لمعدات الرصد الخاصة بها، وذخائرها الموجهة بالليزر ، وكذلك تم استعمال الطائرات من دون طيار في الهجوم على منشآت نفط آرامكو السعودية بتاريخ(19/9/14). ويوجد الآن عدد كبير من الطائرات التي تم تسليحها أو ما زالت قيد التطوير ويقدر أن حوالي (20) دولة طورت أو اكتسبت هذه القدرة على الرغم من أن قليلا منها فقط استخدمتها في النزاعات المسلحة. وعلى الرغم من أن هذا النوع مستقل بشكل كبير من ناحية وظائف الإقلاع، والهبوط، والملاحة، وتحديد الأهداف؛ إلا أن قرار الهجوم ما زال يحتفظ به عامل بشري، وقد تم تطوير هذا النوع في البداية لأغراض الاستطلاع والاستخبارات وتم تكييفها لاحقا لحمل الأسلحة وتنفيذ الهجمات (Chavannes,2020,p.72)، ويتم الآن صنع جيل جديد من هذه الأسلحة يكون أكثر استقلالية ويستخدم للقتال ومن أمثلتها طائرة (MQ9.Reaper).

4- أنظمة الأسلحة البحرية : يتم كذلك صنع أسلحة بحرية ذاتية من مختلف الأحجام والوظائف, وهناك نوعان رئيسان: الأول هو المركبات السطحية غير المأهولة التي تقوم بهجمات الحروب السطحية، والثاني المركبات غير المأهولة تحت الماء التي تستخدم بالحرب ضد الغواصات وزرع الألغام؛ ولهذا النوع أهمية خاصة؛ إذ يمكنه أن يعمل تحت الماء لوقت طويل ودون أي تفاعل بشري، وذلك بسبب صعوبة الاتصالات تحت الماء(Connor,2013,p.24).

**المطلب الثاني**

**مدى انطباق مبدأ "التناسُب" على الأسلحة الذاتية**

سبق وأن بينا بأن مبدأ التناسُب يتطلب اتخاذ كل الاحتياطات اللازمة عند اختيار وسائل القتال لتجنب أية أضرار وخسائر في أرواح المدنيين او الإضرار بممتلكاتهم بشكل عرضي، أي إن هذا المبدأ يقوم بموازنة الآثار المتوقعة من استعمال سلاح ما وبين تحقيق الهدف العسكري المنشود(البصيصي ، 2023، ص 18)، وقد أشارت لهذا المبدأ الفقرة ( 5 / ب ) من المادة (51) من البروتوكول الإضافي الأول العام 1977 بالقول: " ..... والهجوم الذي يمكن يتوقع منه أن يسبب خسارة في أرواح المدنيين أو إصابتهم أو أضراراً بالأعيان المدنية، أو أن يحدث خلط من هذه الخسائر

والأضرار ، يفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة مباشرة " وكذلك ورد مبدأ التناسُب في المادة (36) من البروتوكول الإضافي الأول لعام 1977، وتم تأكيده في المادة(57) منه .

وإن "مبدأ التناسب" عامل حاسم في أي قرار يتم اتخاذه أثناء النزاع المسلح، فهو بمثابة خط الدفاع الأخير بالنسبة للمدنيين، والأعيان التي لا تعد أهدافًا عسكرية ، ومما تجب الإشارة إليه أن "التناسب" يتجاوز نطاق "القانون الدولي الإنساني" في أهميته ، على الرغم من أنه لا ينطبق بذات الطريقة في جميع المجالات، إلا أنه يحوي دائما على فكرة مشتركة تبرز التوازن بين العناصر التي – إذا تغيرت – يجب أن تعطى جميعها نفس النتيجة، فالتناسب موجود في جميع " فروع القانون الدولي العام"، على سبيل المثال، يطبق التناسب على قانون الاستثمار الدولي والتحكيم، وترسيم الحدود البحرية، و"القانون الجنائي الدولي"، وإن كان التناسب مبدأ عاما من مبادئ "القانون الدولي الإنساني"، إلا أنه يعمل بوصفه أداة لسد الثغرات في القانون الدولي التقليدي والعرفي، أو بوصفه وسيلة لتفسير قواعد أخرى للقانون الدولي، أو لدعم الاستدلال القانوني, فضلاً عن أنه يمكن أن يكون بمثابة أساس للنظام القانوني الدولي أو بوصفه "وسيلة لتعزيز طابعه المنهجي"( Newton, M,2018 P. 860. ).

وقد أصدرت "محكمة العدل الدولية" قرارات عدّة تناولت "مبدأ التناسب في القانون الدولي"، من أبرز هذه القرارات الفتوى الاستشارية الصادرة عام 1996 بشأن "مشروعية التهديد بالأسلحة النووية أو استخدامها" في هذه الفتوى، أكدت المحكمة " أهمية مبدأ التناسب، مشيرة إلى أن "استخدام القوة يجب أن يكون متناسبًا مع الهدف العسكري المشروع، وألا يسبب أضرارًا مفرطة للمدنيين أو البيئة "، كما شددت المحكمة على" ضرورة التمييز بين المقاتلين والمدنيين، وأن أي استخدام للقوة يجب أن يلتزم بقواعد القانون الدولي الإنساني" (عصام الدين محمد إبراهيم، (2020)، ص 100 ).

فضلاً عن ذلك، تناولت المحكمة مبدأ التناسب في قضايا أخرى، مثل "قضية الجدار العازل في الأراضي الفلسطينية المحتلة عام 2004"، إذ أشارت إلى " أن بناء الجدار وتأثيراته على حياة الفلسطينيين يجب أن يكون متناسبًا مع الاحتياجات الأمنية المعلنة" (زامونه،، 2022 ، ص 45) .

تُظهر هذه القرارات التزام محكمة العدل الدولية بتطبيق "مبدأ التناسب" بوصفه جزءا أساسيا من القانون الدولي، لضمان أن تكون الأعمال العسكرية والإجراءات الأخرى متوافقة مع المعايير الإنسانية والقانونية.

بعبارة أخرى يحظر المبدأ الهجمات على الأهداف العسكرية إذا كان الضرر المدني الذي يمكن التنبؤ به للهجوم يفوق ميزته العسكرية المتوقعة (Ghasemi,2014,p.21).

إن مبدأ التناسُب يحتم على القائد العسكري أن يواصل مرافقة ما إذا كان الهجوم لا يزال ضمن القيود الموجودة في قاعدة التناسب، فإذا ما اتضح للقائد أن الهجوم لا يحترم مبدأ التناسُب فيلزم عندئذ بإلغائه إن أمكن، فضلاً عن أن هنالك العديد من المسائل التي تحتاج إلى تقييم في الهجوم، فهنالك الميزة العسكرية، والأعيان المدنية، فضلا عن مدى توافر المعلومات الاستخباراتية الضرورية، كذلك الأضرار الجانبية المتوقعة من الهجوم ، أو حتى مسألة الطقس الذي قد يكون عاملا مهما في الهجوم(Kwik,2024,p.14).

فما مدى إمكانية الأسلحة الذاتية على القيام بهذه الحسابات؟

بالنظر إلى تعقيد وصعوبة الحسابات التي يجب إجراؤها قبل تقرير الهجوم، يبدو من الواضح جدا أن من المستحيل برمجة آلة لإجراء هذه الحسابات، خاصة في بيئة ديناميكية، وحتى لو افترضنا أنه في يوم من الأيام تمكن المبرمجون من صنع آلات قادرة على تحقيق ذلك ، وخلق أنظمة يمكنها تطبيق مبدأ التناسُب حتى في المناطق ذات الكثافة المدنية ، مع ذلك يبدو أن الأمر صعب المنال؛ وذلك بسبب العدد الكبير من المتغيرات التي يستوجب على الأسلحة الذاتية تفسيرها في وقت واحد؛ فمثل هذا الأمر يتطلب إلى العقلانية والموضوعية في التقييم, ويحتاج حتماً لعقل بشري فريد.

وبتطبيق مبدأ "التناسب" على " الأسلحة ذاتية التشغيل " ، فإنه من الصعب إعماله بالشكل الذي تضمن احترام حقوق المدنيين، وكذلك العسكريين أثناء "النزاعات المسلحة"، وذلك بسبب احتمالية وقوع خطأ في التوجيه والرقابة، وبحكم أنها أسلحة "ذاتية التشغيل" دون تدخل عنصر بشري، فضلا عن أنها تفتقد لعنصري التمييز والإدراك، ومن جهة أخرى أن "الأسلحة ذاتية التشغيل " تتصف في كثير من الأحيان بالعشوائية، الأمر الذي يؤدي إلى أضرار واسعة غير متناسبة مع "الضرورة العسكرية".

فالحرب فن وليست علما يمكن اختزاله بخوارزميات رياضية، فمبدأ التناسُب يتجاوز كثيراً برمجة هذه الأسلحة وعمله بصورة ذاتية .

**الخاتمة:**

**أولاً: النتائج:**

بعد استكمال دراسة هذا البحث، توصلنا إلى جملة من النتائج نوجزها فيما يلي:

1- إن ظهور "الهجمات السيبرانية" هو أحدث جزء في تطور الحرب واستمرارية التغيرات في الحرب الناجمة عن التغيرات التكنولوجية، ولا شك أن هذه التغييرات تتحدى تأطير استخدامِ القوة، وكذلك الجوانب الأخرى ذات الصلة في القانون الدّوليّ الإنسانيّ.

2-إن مبادئ القانون الدولي الإنساني ومنها مبدأ التناسُب هي مبادئ تتمتع بصفة الشمولية والعمومية، وقابليتها للتطبيق على الهجمات السيبرانية مع مراعاة خصوصية تلك الهجمات بوصفها سلاحا جديدا ومتطورا، قد دخل حديثا في ميدان النزاعات المسلحة الدولية وغير الدولية.

3- أصبحت الدول تدرك أنَّ" الهجمات السيبرانية" قد تشكل" استخداماً للقوة" يصل إلى درجة الهجوم المسلح، إذا كان حجم الهجوم وآثاره واسع النطاق بما فيه الكفاية.

4- يصعب على القائم بهجوم سيبراني تطبيق مبدأ التناسُب جميع معاييره؛ كون الممتلكات والأعيان العسكرية والمدنية في المجال الالكتروني مترابطة إلى درجة كبيرة جداً.

5- على الرغم من نبذ أغلب الدول لا سيما المتقدمة منها للهجمات السيبرانية؛ إلا أنَّ هذه الدول ذاتها مستمرة بتطوير أدواتها السيبرانية، بحيث أصبحت متهمة بأكثر الهجمات السيرانيّة خطورة.

6- إن الأسلحة الذاتية التي بدأت بالظهور بعد الحرب العالمية الثانية تقريبا تعد أفضل طريقة لتجنيب الجنود خطر الحروب ، ومع ذلك فإنها تعد خطراً قائما بحد ذاته؛ إذ يمكن أن يصبح حق الحياة مرهون بيد آلة لا تملك من العقل إلا ما برمجت عليه.

7- إن هذه الأسلحة ومهما بلغت درجة تطورها وامكانياتها تعجز عن القيام بأداء متطلبات التناسب التي يجب على القائد الحربي مراعاتها أثناء التخطيط للهجوم.

**ثانياً: المقترحات**

أما المقترحات التي ترشد إليها الدراسة فهي:

1- مع عدم وجود قواعد واضحة تحكم" الأسلحة الذاتية والهجمات السيبرانية"؛ نرى ضرورة أن تأخذ الدول بالحسبان أنَّ ممارستها الدقيقة في تكييف قواعد قانون النزاعات المسلحة وتطبيقه على ما ينشأ من نزاعات مسلحة تستخدم فيها "الأسلحة الذاتية"، أو "الهجمات السيبرانية"، سينتج قواعد مهمة تحكم العمليات السيبرانية، أو استخدام الأسلحة أثناء النزاعات المسلحة. ضرورة إدخال تعديلات جوهريه كي تتسع الاتفاقيات الدولية للهجمات السيبرانية، ومنها ميثاق الأمم المتحدة فيما يتعلق باعتبار الهجمات السيبرانية اعتداء يعطي الحق باعتماد الاستثناء أو التصريح باستخدام القوة دفاعا عن النفس أو تدابير الأمن الجماعي من خلال مجلس الأمن الدولي، وينص على ذلك صراحة. وكذلك تعديل النصوص الحاكمة في اتفاقيات جنيف الأربعة لعام 1949 والبروتوكولين الإضافيين الملحقين بها، لعام 1977، وكذلك أحكام اتفاقيات لاهاي إلى حين التوصل إلى اتفاقيات دولية ملزمة في إطار القانون الدولي الإنساني يشمل بشكل واضح وصريح الهجمات السيبرانية.

2- ضرورة توجيه الإرادة الدولية لوضع قواعد جديدة قد تكون على شكل بروتوكول جديد ( رابع) أو اتفاقية مستقلة، تضع قواعد جديدة تعالج مشاكل الاستخدام السيء لهذه الأسلحة والهجمات.

3- على الدول أن تتخذ الاحتياطات اللازمة لحماية سكانها المدنيين والأعيان والممتلكات المدنية من الأخطار الناجمة عن العمليات السيبرانية وأهم هذه الاحتياطات:

أ- وضع الخوادم وغيرها من معدات الإنترنت العسكرية بعيدا عن المناطق المدنية.

ب- للدول أن تنشئ بنية تحتية سيبرانية أساسية تقوم عليها اتصالاتها الإلكترونية السيرانيّة ، وتفصلها فعليا عن البنية التحتية المدنية.

4-وضع قواعد صارمة على الدول بما يتعلق بعملها على برمجة هذه الأسلحة والتأكيد على ضرورة عدم منحها الاستقلال الكامل فلا بد+ ن يبقى قرار الهجوم بيد عامل بشري.

المصادر

اولاً : المصادر العربية :

.610-678 :)8( والسياسية، 4.

1.احمد عطا حسين. (2022). وسائل حماية التجارة الالكترونية من مخاطر الهجمات السيبرانيه .*مجلة واسط للعلوم الإنسانية*.(52)*18*، https://doi.org/10.31185/.Vol18.Iss52.338

2. الحديثي، (2021)التفصيل الشامل لتطور القواعد القانونية الخاصة بالحرب السيبرانية ،ط1 مصر : منشورات المجموعة العلمية للطباعة والنشروالتوزيع.
3. صلاح جبير البصيصي, & حازم فارس حبيب. (2023). استجابة اتفاقيات جنيف الأربع لعام 1949 بشأن استخدام أنظمة أسلحة الذكاء الاصطناعي في النزاعات المسلحة. مجلة رسالة الحقوق، ١٥(٥).
4.علام ، ايمان احمد ،(2023)، الهجمات السيبرانية واستخدام القوة المسلحة في القانون الدولي العام ، بحث منشور في مجلة الدراسات القانونية والاقتصادية ، المجلد /9، العدد /4، مصر .
5.عصام الدين محمد إبراهيم. (2020). التعليق على فتوى محكمة العدل الدولية في مدى مشروعية التهديد باستخدام الأسلحة النووية عام 1996م .*مجلة العلوم الإقتصادية و الإدارية و القانونية*–114 ,(13)*4* , 100.
6.الفتلاوي، أ. ( 2016 )، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق للعلوم القانونية
7.الفتلاوي، أ.( 2018 ) الهجمات السيبرانية، دراسة قانونية تحليلية. )ط 1(. بيروت: منشورات زين الحقوقية.
8.لين ، هربرت ،(2012) ، النزاع السيبراني والقانون الدولي ، المجلة الدولية للصليب الاحمر ، المجلد /94، العدد/ 886.
9.زامونه & ,د. عبد الحكيم ضو. (2022). الْإِعْتِرَافُ الْأَمْرِيْكِي بِالْقُدْسِ عَاصِمَة لِإِسْرَائِيل مُبَرِّرَاتِه وَتَبَعَاتِه.
10. هنكرتس ، ماري، ولويز دوزوالد بك(2005) ، القانون الدولي الإنساني العرفي، المجلد الأول :القواعد، اللجنة الدولية للصليب الاحمر ، مطابع جامعة كامبردج، كامبردج.
**11**.محمد عبدالعال الخضرى, س & ,.سامى. (2023). الوضع القانوني لاستخدام الروبوتات العسكرية في ضوء قواعد القانون الدولى الإنسانى Light Legal Status Of The Use Of Military Robots In Of The Rules Of International Humanitarian Law.*مجلة كلية الشريعة و القانون بطنطا* 509–440 ,(3)*38*.

**ثانياً : المصادر باللغة الانكليزية :**

1–Allhoff, F., Evans, N. G., & Henschke, A. (2013). *Routledge handbook of ethics and war: Just war theory in the 21st century*. Routledge.
2–Chavannes, E., Klonowska, K., & Sweijs, T. (2020). Governing autonomous weapon systems. *The Hague: The Hague Centre For Strategic Studies*.
3–Chengeta, T. (2016). Are Autonomous Weapons Systems the Subject of Article 36 of Additional Protocol I to the Geneva Conventions. *UC Davis J. Int'l L. & Pol'y*, *23*, 65.
4–Connor, W. (2013). Underwater Drones Are Multiplying Fast. *Wall Street Journal*, *24*.
5–Converse, B. D. Cyber Power and Operational Art.

6-Etzioni, A., & Etzioni, A. (2018). Pros and cons of autonomous weapons systems (with Oren Etzioni). *Happiness is the Wrong Metric: A Liberal Communitarian Response to Populism*, 253-263.
7-Geers, K. (2008). Cyberspace and the changing nature of warfare. *SC magazine*, *27*.
8-Gao, S., Ye, Q., Luo, L., Pan, Z., Yan, Y., & Zheng, H. (2017). Recursive Orthogonal Label Regression: A Framework for Semisupervised Dimension Reduction. *Computing in Science & Engineering*, *19*(4), 30-43.
9-Geiss, R. (2015). *The international-law dimension of autonomous weapons systems*. Friedrich-Ebert-Stiftung, International Policy Analysis.
10-Ghasemi, A. H. (2014). *Semi-autonomous weapon systems in international humanitarian law: A study of the new decision-making and responsibility issue in international humanitarian law relating to semi-autonomous weapon systems* (Doctoral dissertation, Lund University, Faculty of Law).
11-Graham, D. E. (2010). Cyber threats and the law of war. *J. Nat'l Sec. L. & Pol'y*, *4*, 87.
12-Hathaway, O. A., Crootof, R., Levitz, P., & Nix, H. (2012). The law of cyber-attack. *Calif. L. Rev.*,
13-Heyns, C. (2013). Extrajudicial, summary or arbitrary executions. *Security Issues in the Greater Middle East*, 183.
14-Hayashi, N. (2010). Requirements of military necessity in international humanitarian law and international criminal law. *BU Int'l LJ*, *28*, 39.
15-Jensen, E. T. (2012). Cyber attacks: Proportionality and precautions in attack.
16-Kesan, J. P., & Hayes, C. M. (2011). Mitigative counterstriking: Self-defense and deterrence in cyberspace. *Harv. JL & Tech.*, *25*, 429.
17-Khan, A., Ullah, M., Rehman, F., & Ghani, A. (2017). Cyber Attacks in International Law: From Atomic War to Computer War. *Available at SSRN 3064787*.
18-Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future generation computer systems*, *82*, 395-411.
19-Kalshoven, F. (1985). *Arms, armaments and international law*. Martinus Nijhoff.
20-Kwik, J. (2024). AWS and Targeting. In *Lawfully Using Autonomous Weapon Technologies* (pp. 227-273). The Hague: TMC Asser Press.
21-Kanno, A., Dat, P. T., Yamamoto, N., Kawanishi, T., Iwasawa, N., Iwaki, N., ... & Kashima, K. (2020). High-speed railway communication system using linear-cell-based radio-over-fiber network and its field trial in 90-GHz bands. *Journal of lightwave technology*, *38*(1), 112-122.
22-Markoff, J., & Shanker, T. (2009). Halted'03 Iraq plan illustrates US fear of cyberwar risk. *The New York Times*, *2*, 2009.
23-McClelland, J. (2003). The review of weapons in accordance with Article 36 of Additional Protocol I. *International Review of the Red Cross*, *85*(850), 397-420.
24-Nakashima, E., & Harris, S. (2018). How the Russians hacked the DNC and passed its emails to WikiLeaks. *The Washington Post*, *13*.
25-Righetti, L., Sharkey, N., Arkin, R., Ansell, D., Sassoli, M., Heyns, C., ... & Lee, P. (2014, March). Autonomous weapon systems: technical, military, legal and humanitarian aspects. In *Expert Meeting, International Committee of the Red Cross*.

26-Raineri, M., Monica, R., & Bianco, C. G. L. (2021). A real-time 3d reconstruction of staircases for rehabilitative exoskeletons. *IEEE Transactions on Medical Robotics and Bionics*, *3*(1), 220-229.
27-Shackelford, S. J. (2009). From nuclear war to net war: analogizing cyber attacks in international law. *Berkeley J. Int'l Law*, *27*, 192.
28-Sharkey, A. (2019). Autonomous weapons systems, killer robots and human dignity. *Ethics and Information Technology*, *21*(2), 75-87.
29-Smis, S., & Van der Borght, K. (1998). The advisory Opinion on the Legality of the Threat or use of nuclear Weapons. Ga. J. Int'l & Comp. L., 27, 345.
30-Trux, J. (1991). Desert Storm: a space-age war. *New Scientist*, *131*, 30-4.
31-Wagner, M. (2014). The dehumanization of international humanitarian law: legal, ethical, and political implications of autonomous weapon systems. *Vand. J. Transnat'l L.*, *47*, 1371.
32-Warner, M. (2012). Cybersecurity: A pre-history. *Intelligence and National Security*, *27*(5), 781-799.
33-Weeramantry, C. G. (Ed.). (1999). *Nuclear weapons and scientific responsibility*. Martinus Nijhoff Publishers.
34-Whyte, C., & Mazanec, B. (2023). *Understanding cyber-warfare: Politics, policy and strategy*. Routledge.