

الهجمات السيبرانية على الاحتلال الإسرائيلي وأثرها على القضية الفلسطينية من منظور القانون الدولي

The impact of Israeli occupation's cyberattacks on the Palestinian cause – and the rule of contemporary international humanitarian law .

أشرف محمد إبراهيم أبو صيام

كلية الدراسات العليا، الجامعة العربية الأمريكية، رام الله فلسطين،

ash.adv10@gmail.com

تاريخ النشر: 2024/06/29

تاريخ القبول: 2024/05/ 23

تاريخ الاستلام: 2023/08/ 03

Abstract:

The study of cyber-attacks on the Israeli occupation and their impact on the Palestinian cause from the perspective of international law aims to study .The main objectives of the study can be summarized as follows :studying and analyzing international humanitarian law and the possibility of having laws dealing with cyber-attacks and how to deal with them , presenting 3 cases of cyber-attacks and how to deal with them ,the Convention on Cybercrime of the Council of Europe in 2001and the possibility of adopting it as a basis for international humanitarian law , reviewing and analyzing the Tallinn Manual and examining its applicability and effectiveness in dealing with this phenomenon ,Expanding the circle of specialists in this field due to the increasing demand for experts in this field ,The study also specialized in talking about the relationship of tension between the occupation state and the Palestinian resistance ,especially after the first cyber-attack carried out by the Palestinian resistance in Gaza against Israeli targets .

ملخص:

تهدف دراسة موضوع الهجمات السيبرانية على الاحتلال الإسرائيلي وأثرها على القضية الفلسطينية من منظور القانون الدولي.

ويمكن تلخيص الأهداف الرئيسية للدراسة بالتالي: دراسة وتحليل القانون الدولي الإنساني وإمكانية وجود قوانين تتعامل مع الهجمات السيبرانية وكيفية تعامله معها، عرض 3 حالات لهجمات سيبرانية وكيفية التعامل معها، الاتفاقية المتعلقة بالجريمة الالكترونية للمجلس الأوروبي سنة 2001 وإمكانية تبنيها كأساس للقانون الدولي الإنساني، استعراض وتحليل دليل تالين وفحص مدى إمكانية تطبيقه والنجاعة في التعامل مع هذه الظاهرة، توسيع دائرة ذوي الاختصاص في هذا المجال نظرا لتزايد الطلب لخبراء في هذا المجال،

كما اختصت الدراسة في الحديث عن علاقة التوتر بين دولة الاحتلال والمقاومة الفلسطينية خاصة بعد أول هجوم إلكتروني نفذته المقاومة الفلسطينية في غزة ضد أهداف إسرائيلية. وتسعى هذه الدراسة على الإجابة على الإشكالية الرئيسية والمتمثلة في: ما هي المعايير لتحديد الهجمات السيبرانية كنزاع مسلح ام لا وخضوعها

أشرف أبو صيام: الهجمات السيبرانية على الاحتلال الاسرائيلي وأثرها على القضية الفلسطينية، من منظور القانون الدولي

This study seeks to answer the main problem :What are the criteria for identifying cyber-attacks as an armed conflict or not and subjecting them to the law of war ?The study will also delve into three important principles that must be taken into account through cyber-attacks or self-defense .

The study showed many results ,the most important of which is international humanitarian law is insufficient to deal with cyber-attacks and the United Nations lacks a comprehensive agreement between countries in this field ,but there is an agreement in this regard in the Council of Europe so that it is considered an effective and purposeful agreement ,while the Tallinn guide remained as a scientific paper without officially adopting it.

Keywords: International humanitarian law, cyberattacks, Palestinian cause.

لقانون الحرب؟ وأيضاً ستخوض الدراسة في ثلاثة مبادئ مهمة التي يجب ان تأخذ بعين الاعتبار من خلال الهجمات السيبرانية او الدفاع عن النفس.

أظهرت الدراسة العديد من النتائج وأهمها القانون الدولي الإنساني غير كافي للتعامل مع الهجمات السيبرانية وتفتقر الأمم المتحدة لاتفاقية شاملة بين الدول في هذا المجال، ولكن هنالك اتفاقية بهذا الشأن في المجلس الأوروبي بحيث تعتبر اتفاقية ناجعة وهادفة، اما دليل تالين فبقي كورقة علمية دون تبنيها بشكل رسمي.

الكلمات المفتاحية: القانون الدولي الإنساني، الهجمات السيبرانية، القضية الفلسطينية.

*المؤلف المرسل

مقدمة:

تطور التكنولوجيا وخاصة الحاسبات الإلية يعتبر من أهم الثورات في القرن العشرين ومع هذا التطور أصبح الانترنت والحاسوب والهواتف الذكية جزء لا يتجزأ من حياتنا، مع ذلك أصبحت كل وسائل الحياة الخاصة والعامة المرتبطة بالانترنت معرضة للهجمات السيبرانية لأغراض إلحاق الضرر أو كسب المال بطرق سهلة. واتي ظهور الحاسوب الالي ليسهل على الانسان والمؤسسات ويختصر له الوقت والمسافة والجهد البدني والذهني. وفي نفس الوقت استخدم الحاسوب الالي كأداة لارتكاب الجرائم الغير مشروعة. الجرائم أو الهجمات السيبرانية أتت بتحديات جديدة غير موجودة في القانون الدولي الإنساني وصعوبة وضع تعريف لها، فالتبيعة الخاصة للجريمة الالكترونية التي تمس الأنشطة الحساسة للدولة وتكون عابرة للحدود بواسطة شبكات الاتصال، كل هذا يجعلها مختلفة عن باقي الجرائم لذا نعالجها من خلال إشكالية:

ملائمة القانون القديم لتكنولوجيات السايبر الجديدة، والمعايير لتحديد الحرب السيبرانية كنزاع مسلح، ومتى تخضع الهجمات السيبرانية لقوانين الحرب، تطبيق مبدأ التمييز على الفضاء السيبراني، تطبيق مبدأ التناسب على الفضاء السيبراني، تطبيق مبدأ الاحتراز والحذر على الفضاء السيبراني، القوانين والقواعد القائمة اليوم حول العالم للتعامل مع الهجمات السيبرانية، امثلة 3 هجمات سيبرانية ونتائجها.

سأتبع في هذا البحث المنهجين الوصفي والتحليلي لضرورة تحليل النصوص القانونية والاتفاقيات، دخول عالم التكنولوجيا لحيزنا غير الكثير من عالمنا وأصبح جزء كبير من حياتنا اليومية، ولكنه جلب للعالم حروب غير تقليدية بعيدة عن البر والبحر والجو، ساحة الفضاء السيبراني. هذا الفضاء معرض كغيره لهجمات التي تؤدي الى خسائر مادية، معنوية وأيضا خسائر في الأرواح (على سبيل المثال خلال سنة 2015 تم استهداف القطاعات التالية بواسطة الهجمات السيبرانية: القطاع الحكومي 36%، القطاع المالي 26%، قطاع الاتصالات 16%، المتاجر الالكترونية 14%، قطاع الغاز والنفط 8%)¹ يستدل من هذه المعطيات ان هنالك اهداف معنوية، مالية، وجنائية من وراء هذا الهجمات، من هنا نشهد في السنوات الأخيرة تصاعد ثابت في وتيرة هذا النوع من الهجمات السيبرانية خاصة على صعيد الدول. القانون الدولي لم يكن جاهزا لمثل هذه الهجمات، والتمسنا قصور هذا القانون امام هذه الهجمات وعدم قدرته لمنح الحلول الملائمة وكيفية التعامل مع هذه المعضلة. برزت الحاجة لهذه الدراسة مع تصاعد هذه الجرائم حول العالم وضرورة حثله القانون بما يتلاءم مع التحديات الجديدة التي افرزتها هذه الانواع من الجرائم. وأبرز هذه التصريحات هي للسكرتير العام للأمم المتحدة يوم 21.1.2022 وحذر غوتيرش من ان "الفوضى الرقمية المتزايدة تفيد القوى الأكثر تدميرا وتحرم الأشخاص العاديين الفرص". غالبية دول العالم تعنى بمثل هذه الدراسات من اجل افساح المجال امامها للتعامل مع هذا النوع من الجرائم والحد من الظاهرة المقلقة،

مع ازدياد استعمالات الشبكة العنكبوتية اخذ هذا الحيز مساحة كبيرة في حياتنا حيث يبلغ اليوم عدد مستخدميها المليار وثمانمائة مليون وأصبحت عرضة للهجمات السيبرانية من كل

¹ ساره عبد العزيز، الحرب السيبرانية- التداعيات المحتملة لتصاعد الهجمات الالكترونية على الساحة الدولية، 2016 دراسة

المستقبل عبر الرابط. <https://platform.almanhal.com/details/article/100427>

أشرف أبو صيام: الهجمات السيبرانية على الاحتلال الاسرائيلي وأثرها على القضية الفلسطينية، من منظور القانون الدولي

مكان وفي كل زمان وهي غير محصنة مقابل هذه الهجمات، هذه الظاهرة أصبحت منتشرة ولا يمكن تجاهلها من حيث الاضرار التي تخلفها.

تأتي الاهمية العملية بضرورة الوقوف على تأثير الأمن السيبراني على شكل النظام العالمي الجديد الذي أخذ في التبلور والتغير، فمن المهم معرفة ألى أي درجة يُساعد اهتمام دول العالم بقضايا الأمن السيبراني، وما يصاحبه من آليات وتقنيات حديثة على تغيير بنية النظام الدولي، فهو يغير معايير وتوازنات القوة الأمر الذي قد يهدد الأمن والسلم الدوليين.

لغرض الإحاطة بهذا الموضوع قسمنا الدراسة على النحو التالي:

المبحث الأول: تعريف وخصائص وطبيعة الهجمات السيبرانية

المبحث الثاني: مدى انطباق قواعد القانون الدولي الإنساني على الهجمات السيبرانية
المبحث الثالث: أهم مبادئ القانون الدولي الإنساني المطبق على الهجمات السيبرانية حرب سيبرانية على الاحتلال

المبحث الرابع: مصادر القانون الدولي الإنساني المطبق على الهجمات السيبرانية باعتبارها نزاع مسلح، ودليل تالين

المبحث الخامس: مصادر القانون الدولي الإنساني المطبق على الهجمات السيبرانية باعتبارها نزاع مسلح، ودليل تالين.

المبحث الأول: تعريف وخصائص وطبيعة الهجمات السيبرانية

بما أن موضوع البحث في الهجمات السيبرانية يحمل في طياته العديد من المصطلحات والمعاني الجديدة رأينا من الضرورة الإشارة لبعض منها. سأتناول في المبحث 3 مطالب: المطلب الأول سيتناول تعريف الهجمات السيبرانية، اما في المطلب الثاني سأتناول خصائص الهجمات السيبرانية، اما المطلب الثالث طبيعة الهجمات السيبرانية.

المطلب الأول: مفهوم الهجمات السيبرانية

هي أشكال السلوك الغير مشروع (او ضار بالمجتمع) الذي يتم ارتكابه بواسطة الحاسوب² كما عرفها الفقيه تايدمان Tiedman. وهي أيضا تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا كما عرفها مكتب التقنية في الولايات المتحدة الامريكية.

ويمكن تعريف الحرب الالكترونية بهجمات تتم بواسطة الحاسوب وتهدف الى تعطيل او تدمير أنظمة الانترنت والممتلكات او الوظائف الحاسوبية الخاصة بالخصم ويشار الى هذا الشكل من اشكال النزاع المسلح الذي يتم عن طريق الشبكة العنكبوتية ويؤدي الى نفس الخسائر كالنزاع المسلح التقليدي الذي نعرفه، ويعرف أيضا كتصرف دفاعي او هجومي ويتوقع منه ان يتسبب في جرح او قتل شخص والحاق اضرار مادية او دمار بالهدف المهاجم او تهديدا باستخدام القوة ضد سلامة الأراضي او الاستقلال السياسي لاي دولة ولا تتفق بأي وجه مع مقاصد الأمم المتحدة.³

المطلب الثاني: من اهم خصائص الهجمات السيبرانية:

جرائم عابرة للدول: وهي نوع كأي نوع من الجرائم الأخرى التي نعرفها بشكل اعتيادي كتجارة المخدرات وتبييض الأموال وغيرها من الجرائم الجنائية، ولكن ما يميز هذه الجرائم هو توزيعها من حيث بلد المنشأ للمعتدي والبلد المجني عليها وبلد الام الحاضن لمنفذي الهجوم أي ان الجريمة تتعلق بعدة جغرافية لذلك هي احد الأنواع الجديدة من الجرائم.⁴

² انظر:

- الباحث محمود احمد عبابنة، محمد معمر الرازي، جرائم الحاسوب، ابعادها الدولية، دار الثقافة للنشر والتوزيع 2005، ص 15.

- أسامة احمد المناعسة - جلال محمد الزغي، جرائم الحاسب الآلي والانترنت، دراسة تحليلية مقارنة، دار وائل للنشر والتوزيع، 2001، ص 73.

³ أ.د عمر اعمر، الحرب الالكترونية في القانون الإنساني، دراسات، علوم الشريعة والقانون، المجلد 46، عدد 3، صفحة 134، 2019.

⁴ اسامه احمد المناعسة - جلال محمد الزغي، جرائم الحاسوب الآلي والانترنت، دراسة تحليلية مقارنة، دار وائل للنشر والتوزيع، 2001، ص 73.

أشرف أبو صيام: الهجمات السيبرانية على الاحتلال الاسرائيلي وأثرها على القضية الفلسطينية، من منظور القانون الدولي

أ. جرائم يصعب اكتشافها: هذا النوع من الجرائم ليس بالسهل اكتشافه لانه على ارض الواقع يتم اكتشاف 1% منها بعد ان تم الإبلاغ عن 10% فقط منها. وهذه الصعوبة تنتج بسبب الخصائص التالية:

1. سرعة تدمير الأدلة: فيقوم منفذ الهجوم السيبراني بتدمير الأدلة خلال ثواني.
2. عدم ترك نتائج او اثر مادي كما هو الحال في الجرائم التقليدية: النتيجة لهذه الهجمات ليست بالأحرى ان تترك خسائر واضرار جسيمة بل ممكن أيضا ان تترك اضرار بسيطة.⁵

3. النشاط الحاسوبي غير مرئي: وهو عبارة عن ذبذبات الكترونية لا ترى بالعين المرئية بحيث انها مشفرة ولا يراها المجني عليه الا بعد رؤية حدوثها او ضررها.

4. الخبرات القليلة لدى السلطات في الدول المختلفة⁶: بشكل عام الخبرات لدى الأشخاص منفذي هذه الهجمات السيبرانية يتمتعون بخبرة اكبر بكثير من مختصي الدول والاكتشاف يكون عن طريق الصدفة ليس الا.

5. التستر والتكتم على حدوث مثل هذه الهجمات: خوف المؤسسات من فضح امر انها تعرضت لهجمات سيبرانية لان هذا سيضر بالهبة والاسم امام المواطنين او العملاء للشركة، فنحن لا نعلم مدى حجم هذه الجرائم لعدم الكشف عن غالبيتها⁷.

6. النظام الالي: بشكل عام طريقة التنفيذ الالية تكون بدون ترك اثار ويصعب بشكل كبير اكتشافها.

ب. صعوبة الاثبات: الأدوات المستعملة في هذا النوع من الجرائم معقدة ويصعب اثبات القيام بالهجمات السيبرانية⁸.

ت. متطلبات هذه الهجمات هو حاسوب ومعرفة استعماله تكنولوجيا: يعتبر الحاسوب هو الأداة المركزية لارتكاب الجرائم بواسطة الضغط على بضعة ازرار يكون قد تم الهجوم السيبراني⁹.

⁵ د. محمد حماد موهج الهيتي، جرائم الحاسوب ماهيتها، موضوعها، اهم صورها والصعوبات التي تواجهها، دار المناهج للنشر والتوزيع 2006، ص 21.

⁶ محمد حماد موهج الهيتي، المرجع السابق، ص 215.

⁷ محمد حماد موهج الهيتي، المرجع السابق، ص 218.

⁸ أسامة احمد المناعسة- جلال محمد الزغبى، مرجع سابق، ص 106.

ث. جرائم مغرية للمجرمين: فهي تتسم بسرعة التنفيذ وسرعة الربح خلال مدة زمنية قد تصل لبضع ثواني¹⁰.

ج. جرائم ناعمة: خلافا للجرائم العادية فيها يقومون باستعمال القوة والمعدات في الهجمات السيبرانية استعمال العقل وريح الكثير من الأموال¹¹.

المطلب الثالث: طبيعة الهجمات السيبرانية – وسيلة وأسلوب:

الحرب التقليدية تتم بواسطة الأسلحة والمعدات الحربية مثل الطائرات والمدافع والصواريخ بحيث تتم اشتباكات داخل ساحة المعركة وأيضا تشمل الحرب التقليدية أيضا أسلحة الدمار الشامل مثل الكيماوية، والبيولوجية، والنووية. اما الحرب السيبرانية تختلف عن الحرب التقليدية في أن الهجمات لا تستعمل الأسلحة والمعدات بل تستخدم الكمبيوتر عبر شبكة الانترنت وتلحق الضرر أحيانا مماثل للحرب التقليدية او اكثر بحيث يلحق ضرر بهدف او منظومة معينة او ممتلكات تخص الخصم¹². من المهم ذكره ان الفقه قد اختلف في بيان الطبيعة القانونية للحرب السيبرانية. هنالك فارق بين الهجمات السيبرانية والجرائم الالكترونية لكل واحدة خصائصها، وهنالك اختلاف كبير بين الأسلحة الالكترونية المستعملة في الحرب او الهجمات السيبرانية.

المبحث الثاني: مدى انطباق قواعد القانون الدولي الإنساني على الهجمات السيبرانية

المطلب الأول : المعايير لتحديد الحرب السيبرانية كنزاع مسلح:

المسار المركزي لتحديد إذا كانت الهجمات السيبرانية هي نزاع مسلح ام لا؟ هو هل حدوثها تم في إطار نزاع مسلح ام انها حدثت في نفس النطاق. اما تعريف النزاع المسلح كما في اتفاقيات جنيف الأربع بأنها: ("أي اشتباك مسلح ينشب بين طرفين أو أكثر من أشخاص القانون الدولي العام")¹³ ويدخل ضمن النزاع المسلح الدولي الاحتلال الحربي، حيث عرفت اللائحة –

⁹ د. فتوح الشاذلي – عفيفي كامل عفيفي، جرائم الكمبيوتر، منشورات الحلبي الحقوقية، 2003، ص 34.

¹⁰ أسامة احمد المناعسة- جلال محمد الزغي، مرجع سابق، ص 107.

¹¹ أسامة احمد المناعسة- جلال محمد الزغي، مرجع سابق، ص 108.

¹² Kittichaisaree public international law of Cyberspace Law Governance and Technology op.cit 7 p154.

¹³ انظر : المادة الثانية من اتفاقيات جنيف الأربع .

أشرف أبو صيام: الهجمات السيبرانية على الاحتلال الاسرائيلي وأثرها على القضية الفلسطينية، من منظور القانون الدولي

الملحقة باتفاقية لاهاي ١٩٠٧ الاحتلال الحربي" عندما يصبح يعتبر الإقليم محتلاً - لسلطة الجيش المعادي، ولا يمتد الاحتلال إلى الأقاليم التي تقوم فيها هذه فعلاً خاضعاً . (السلطة وتكون قادرة على تدعيم نفوذها)"¹⁴ "كما يلحق بالنزاع المسلح الدولي حروب التحرير الوطني من أجل الاستعمار، حيث نص البروتوكول الإضافي الأول الخاص بالنزاعات المسلحة الدولية على" تتضمن الأوضاع المشار إليها في الفقرة السابقة، المنازعات المسلحة التي تناضل بها الشعوب ضد التسلط الاستعماري والاحتلال الأجنبي وضد الأنظمة العنصرية. وذلك في ممارستها لحق الشعوب في تقرير المصير. إمكانية الأكثر شيوعاً هي بأن هوية منفذ الهجوم السيبراني تبقى مجهولة لصعوبة الوصول إليه بسبب القدرة على إخفاء الأدلة بسرعة فائقة أحياناً خلال ثواني، من هنا إذا صعب تحديد هوية المنفذ فلا تطبيق للقانون الدولي الإنساني. في الحالات التي تتم فيها هجمات سيبرانية من دون علاقة مع نزاع مسلح، هل هذه الهجمات تدخل تحت تعريف النزاع المسلح أم لا؟ في هذا السياق يجب أن نفرق بين نوعين من النزاعات: نزاع مسلح دولي والذي يحدث بين دولتين، ونزاع مسلح غير دولي والذي أحد أطرافه ليست دولة.

النزاع المسلح الدولي: وهو يحدث في حال تفعيل قوة مسلحة بين دولتين¹⁵. بناء عليه فالهجمات السيبرانية ستحسب كنزاع مسلح دولي إذا كان بإمكاننا نسبها لدولة معينة وإذا أدت هذه الأفعال لنزاع مسلح ضد دولة أخرى. مسألة أسناد أفعال المهاجم في الهجمات السيبرانية لدولة أو لجهة معينة هي مسألة شائكة¹⁶، وقد أثرت إمكانية تخفيف هذه الصعوبة إلى حد ما من خلال اعتماد أو افتراض أن الدولة مسؤولة عن أي عملية إلكترونية خرجت من بنيتها التحتية، ولكن لا يوجد أساس لمثل هذا الافتراض في القانون الدولي الحالي. علاوة على ذلك، في ضوء السهولة التي يتمتع بها منفذ العملية وإمكانية إخفاء الأدلة خلال ثواني فيمكن أن يكون هذا الافتراض مصطنعاً إلى حد كبير وقد يفرض عبئاً غير معقول على الدول لأنه ممكن أن ينفذ

ويعرف الاحتلال بأنها سيطرة فعلية وذلك ليتمكن من إدارة الإقليم المحتل، فإذا لم يكن هناك مثل هذه السيطرة لا تكون بصدد احتلال حربي" انظر في ذلك د جمعة شحود شباط ، حماية المدنيين والأعيان المدنية في وقت الحرب ، رسالة دكتوراه ، كلية الحقوق ، جامعة حلب ، سوريا ، ٢٠٠٣ ، ص ٣١٩.

¹⁴ انظر : المادة ٤٢١ من اللائحة الملحقة باتفاقية لاهاي ١٩٠٧.

¹⁵ البند 1(4) للملحق (البروتوكول) الأول الإضافي إلى اتفاقيات جنيف، 1977.

¹⁶ 17 Cordula Droege, Get off My Cloud: Cyber Warfare, International Humanitarian Law 1 and The Protection of Civilians, 94(886) INTERNATIONAL REVIEW OF THE RED CROSS 533, 538(2012).

بواسطة جماعات غير تابعة للدولة من أجل إلحاق ضرر بالدولة نفسها¹⁷. هناك اتفاق واسع، بأن الهجوم على شبكات الحواسيب الذي يخلف أضرار مادية كبيرة هو بمثابة هجوم مسلح تمام كما هو الحال في استعمال قوة تقليدية في النزاع المسلح¹⁸.

النزاع المسلح الغير دولي: النزاع المسلح الغير دولي يحدث عندما يكون أحد الأطراف ليس دولة وينجم عنه نزاع في الحد الأدنى وأيضاً حد أدنى من التنظيم أي نزاعات مسلحة لجماعات مقابل دولة¹⁹، من هنا تكمن صعوبة في التعقب وراء أفراد هذه الجماعات بسبب التعقيد في التعقيب كما ذكرنا سابقاً في هذا البحث، إذاً من أجل تعريف نزاع مسلح كنزاع مسلح غير دولي يجب أن يكون أحد أطرافه ليست دولة وأن يكون نزاع مسلح بما معناه أن يكون حد أدنى من التنظيم وحد أدنى من استعمال القوة. عندما نطبق هذه التعريفات على الهجمات السيبرانية هنالك صعوبة وتكمن في الأسئلة التالية: هل المجموعات المتنازعة مقابل الدولة تتمتع بنظام أساسي أم لا؟ في حالات نادرة نجد تنظيم في المجموعات المنفذة للهجمات السيبرانية والهاكرز التي تكفي من أجل إنتاج هجمات سيبرانية ويمكن أخذها بعين الاعتبار بأنها بمثابة استعمال للقوة لفترة متتابعة ويمكن إدراجها تحت مسمى النزاع المسلح وتطبيق القانون الدولي الإنساني عليها²⁰. لذلك نرى أنه من الصعوبة أن يكون تنظيم وعلاقات هرمية خلا مجموعة الاتصال الوحيد بينها هو عبر الشبكة العنكبوتية من هنا ففعلها يمكن إدراجها تحت تصرف جنائي ليس أكثر وليس كنزاع مسلح²¹.

¹⁷ القاعدة 9 لدليل تالين - Michael N. Schmitt.

¹⁸ Cordula Droegge, Get off My Cloud: Cyber Warfare, International Humanitarian Law 1 and The Protection of Civilians, 94(886) INTERNATIONAL REVIEW OF THE RED CROSS 533, 538(2012).

¹⁹ هذا التعريف تم بواسطة المحكمة الدولية لجرائم حرب يوغسلافيا سابقاً `prosecutor v. tadic` الفقرة 70.

²⁰ ICTY, Prosecutor v. Boskoski, IT-04-82-T, Trial Chamber Judgement of July 10 2008, paras 199-203; ICTY, Prosecutor v. Limaj, IT-03-66-T, Trial Chamber Judgement of November 30, 2005, paras. 94-134; ICTY, Prosecutor v. Haradinaj, IT-04-84-T, Trial Chamber Judgement of April 3, 2008, para. 60.

²¹ القاعدة 23 الفقرة 13-15 لدليل تالين.

أشرف أبو صيام: الهجمات السيبرانية على الاحتلال الاسرائيلي وأثرها على القضية الفلسطينية، من منظور القانون الدولي

المطلب الثاني: مدى خضوع الهجمات السيبرانية لقوانين الحرب:

قوانين الحرب، على النحو المنصوص عليه في البروتوكول الإضافي الأول لاتفاقية جنيف (البروتوكول الأول)، معترف بها على نطاق واسع على أنها تعكس القانون الدولي العرفي في النزاعات المسلحة، الدولية وغير الدولية على حد سواء. القيود المفروضة على العمليات العسكرية. غالبية البنود المنصوص عليها صيغت في إطار تقييدات على عمليات عسكرية التي تعتبر "هجوم"²². في ضوء ذلك، يجب النظر إلى المبادئ الأساسية للأحكام العرفية على أنها قابلة للتطبيق ليس فقط على الهجمات ولكن أيضًا على الحرب بالمعنى الأوسع، أي العمليات العسكرية الأخرى التي يتم تنفيذها في سياق النزاع المسلح وبغرض إلحاق الضرر بالعدو.

في الوقت نفسه، يبدو أن جميع القواعد المحددة للأحكام العرفية التي تركز على الهجمات، على عكس الأنواع الأخرى من العمليات العسكرية، تنطبق بالفعل فقط على تلك العمليات الإلكترونية التي هي في طبيعة الحال "هجوم". نظرًا لأن الإطار القانوني الذي يحكم القتال يتعامل مع معظم "الهجمات"، وليس كلها، فمن المهم التأكد من العمليات الإلكترونية التي تصل فعليًا إلى مستوى الهجوم.

تُعرّف المادة 49 من البروتوكول الإضافي الأول، التي تعكس قوانين القانون الدولي الإنساني العرفي، الهجمات على أنها "أعمال عنف ضد العدو، سواء في الهجوم أو الدفاع". من الشائع الافتراض أن العنف المعني يشير إلى نتائج الهجوم وليس إلى الوسائل المستخدمة لتحقيق هذه النتائج. وفقًا لذلك، يمكن اعتبار إطلاق رمز الكمبيوتر، على الرغم من أنه لا يتضمن عنفًا جسديًا، هجومًا إذا أدى إلى نتيجة عنيفة.

ينعكس هذا الرأي في دليل تالين الذي يعرف "الهجوم السيبراني" بأنه "عملية إلكترونية، سواء كانت هجومية أو دفاعية، والتي من المحتمل بشكل معقول ومنطقي أن تؤدي إلى إصابة أو وفاة الأشخاص أو إصابة أو تدمير الأشياء"²³. المهم في الأمر هو ما إذا كانت العملية الإلكترونية التي تسبب الضرر يمكن أن ترقى إلى مستوى "الهجوم"، على الرغم من أنها لم تسبب في تدمير

²² هنالك توجيهات عديدة "للحجوم" موجودة في البنود 15، 25، 45-85 في البروتوكول الإضافي الأول

²³ دليل تالين القاعدة 30.

مادي مباشر للهدف، بل إلى أضرار أخرى، مثل تعطيل وظيفتها. من ناحية، لا معنى لهذا الادعاء بأن العمليات السيبرانية بالنسبة للعديد من الأشخاص، لن يتم اعتبارها هجوماً لمجرد أنها لا تتضمن تدميرًا ماديًا؛ من ناحية أخرى، سيكون من غير المعقول افتراض أن أي محاولة لإلحاق الضرر بنظام الكمبيوتر تعتبر هجوماً، بحيث يتم تطبيق جميع القواعد المتعلقة بالسلوك في وقت الحرب عليه.

بالتالي، يظل الخط الفاصل الدقيق بين منفذي هجمات السايبر التي تعتبر هجوماً وبين التي لا تعتبر هجوماً بعيد المنال. ومع ذلك، هناك بعض الاعتبارات التي يمكن أن تساعد في التمييز بين الحالتين: أولاً، لأنه بموجب القانون الدولي الإنساني، لا تنطبق فكرة الهجوم على الوسائل غير المادية للحرب (مثل الحرب الاقتصادية أو النفسية، مثل الانتشار الدعاية أو فرض حظر)؛²⁴ السيبرانية المكافئة لمثل هذه الأشكال من "الحرب" لا تعتبر أيضاً هجوماً. على عكس الهجمات التي لا يجب أن توجه أبداً ضد المدنيين، لا يحظر القانون الإنساني الدولي فرض حصار أو عقوبات اقتصادية على السكان المدنيين. وبناءً عليه، لا يمكن الجدل بأن العمليات السيبرانية، مثل العقوبات الاقتصادية، هي هجوم²⁵. علاوة على ذلك، تماماً مثل التدخل في عمليات البث، مثل حجب البث الإذاعي أو التلفزيوني، لا يعتبر هجوماً بموجب القانون الإنساني الدولي، وبالتالي يمكن تستخدم ضد الأنظمة الاتصالات المدنية، لذلك لا يتحول كل اضطراب في أنظمة الاتصالات الحاسوبية إلى هجوم. بالطبع، هناك أنواع من التدخل الإعلامي المستند إلى الكمبيوتر يمكن أن يكون له آثار بعيدة المدى (مثل تعطيل المؤسسات المالية)، لذلك لا يزال من الضروري توضيح متى، وإذا حدث ذلك على الإطلاق، تصبح هذه الاضطرابات هجوماً.

²⁴ MICHAEL BOTHE, KARL JOSEF PARTSCH & WALDEMAR A. SOLF, NEW RULES FOR VICTIMS OF ARMED CONFLICTS: COMMENTARY TO THE TWO 1977 PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 1949, 289 (1982).

²⁵ Cordula Droegge, Get off My Cloud: Cyber Warfare, International Humanitarian Law and The Protection of Civilians, 94(886) INTERNATIONAL REVIEW OF THE RED CROSS 533, (2010) 835.

أشرف أبو صيام: الهجمات السيبرانية على الاحتلال الاسرائيلي وأثرها على القضية الفلسطينية، من منظور القانون الدولي

ليس هناك شك في أنه من السهل نسبياً افتراض أن العمليات الإلكترونية التي تعطل عمل الأهداف في العالم الحقيقي تشكل هجوماً؛ يكون الموقف أقل وضوحاً عندما يتعلق الأمر بالعمليات التي تهدف فقط إلى تعطيل الاتصالات في الفضاء الإلكتروني.

تكمّن خصوصية الفضاء الإلكتروني بأنه لا يخضع لدولة معينة وهذا قد يؤدي لاستخدام قد يضر الإنسانية. لصعوبة التوصل لاتفاق شامل يشمل جميع الدول يقودنا الى ان الاتجاه هو بأن الدول تتفق على ما تم الاتفاق عليه حتى الان بالنسبة للقواعد التقليدية ومنها التعامل مع الهجمات السيبرانية.

هناك في هذا السياق توجهين²⁶: الاتجاه الأول وهم التوجه الأمريكي الأوروبي ويدعون فيه بأن الفضاء السيبراني الإلكتروني منطقة بلا قانون أي تقر بوجود فراغ قانوني، الفقهاء الذين يدعمون هذا التوجه يدعون بأن الفضاء السيبراني لا يخضع للقانون لان الهجمات السيبرانية ممكن التصدي لها او منعها بنفس أدوات الهجوم. يجب التنويه بأن عبارة "الحرب الإلكترونية" لم تذكر في ميثاق الأمم المتحدة، اتفاقيات جنيف ولاهي ومعاهدة حلف شمال الأطلسي. بحيث يتم استخدام المصطلحات التالية في هذه الاتفاقيات مثل "السلامة الإقليمية"، "استخدام القوة المسلحة"، "عمل من جانب القوات الجوية او البرية او البحرية" و "هجوم مسلح" وهي مصطلحات لا تنسجم مع الحرب الإلكترونية مما يضعها ظاهرياً خارج نطاق القانون الدولي. بالإضافة الى ان المادة 51 من ميثاق الأمم المتحدة بينت انه "ليس في هذا الميثاق ما يضعف او ينقص الحق الطبيعي للدول، فرادى او جماعات في الدفاع عن أنفسهم اذا اعتدت قوة مسلحة على احد أعضاء الأمم المتحدة..." كما رأينا فهذا النص يعطي الدولة الحق في الدفاع عن نفسها في مواجهة أي هجوم من قبل قوات مسلحة. اما بالنسبة للهجمات السيبرانية فلا يمكن اعتبارها هجوماً مسلحاً لأنه لا يتم استعمال قوة مسلحة.

في هذا السياق أرفق تصريحات سكرتير الأمم المتحدة²⁷ أنطونيو غوتيريش قبل عدة أيام وتحديدا يوم 21.1.2022 وورد فيها ما يلي: "بينما توفر التكنولوجيا إمكانيات غير عادية للبشرية، حذر السيد غوتيريش من أن "الفوضى الرقمية المتزايدة تفيد القوى الأكثر تدميراً

²⁶ أ.د عمر اعمر، الحرب الإلكترونية في القانون الإنساني، دراسات، علوم الشريعة والقانون، المجلد 46، عدد 3، صفحة 136، 2019.

²⁷ نشر في موقع الأمم المتحدة في هذا الرابط: <https://news.un.org/ar/story/2022/01/1092282>.

وتحرم الأشخاص العاديين من الفرص". تحدث عن الحاجة إلى شبك ما يقرب من ثلاثة مليارات شخص بالإنترنت ما زالوا محرومين منها، ومعالجة المخاطر مثل إساءة استخدام البيانات والمعلومات المضللة والجرائم الإلكترونية. "يتم استغلال معلوماتنا الشخصية للسيطرة علينا أو التلاعب بنا، وتغيير سلوكياتنا، وانتهاك حقوقنا الإنسانية، وتقويض المؤسسات الديمقراطية. فاختياراتنا تُنتزع منا دون علمنا".

دعا الأمين العام للأمم المتحدة إلى وضع أطر تنظيمية قوية لتغيير نماذج الأعمال لشركات التواصل الاجتماعي التي "تستفيد من الخوارزميات التي تعطي الأولوية للإدمان والغضب والقلق على حساب السلامة العامة".

قد اقترح إنشاء ميثاق رقمي عالمي يجمع الحكومات والقطاع الخاص والمجتمع المدني للاتفاق على المبادئ الأساسية التي يقوم عليها التعاون الرقمي العالمي. اقترح آخر هو وضع مدونة سلوك عالمية لإنهاء جائحة المعلومات المضللة والحرب على العلم، وتعزيز النزاهة في المعلومات العامة، بما في ذلك عبر الإنترنت.

كما شجع البلدان على تكثيف العمل على حظر الأسلحة الفتاكة المستقلة، أو "الروبوتات القتالة"، والبدء في النظر في أطر حوكمة جديدة للتكنولوجيا الحيوية والتكنولوجيا العصبية". هذه الرسالة خير دليل وتأكيد على عدم وجود قواعد وقوانين في القانون الدولي الإنساني من أجل التعامل مع التحديات الجديدة التي يأتي بها الفضاء السيبراني وفق ما ورد عن لسان الأمين العام لجمعية الأمم المتحدة.

أما الاتجاه الثاني: أنصار هذا التوجه يدعون بأن الفضاء الإلكتروني يجب أن يكون خاضع للقانون، ويجب تطبيق القانون الدولي الإنساني على الحرب الإلكترونية، فالمادة 39 لميثاق الأمم المتحدة يشمل سلطة تقديرية لمجلس الأمن في حال وقع هنالك تهديد للسلم والأمن الدوليين، تهديد السلم والمن الدوليين يحمل في طياته الكثير من التعريفات التي يمكنها أن تدخل تحت إطار هذا البند. أما بالنسبة للحق في الدفاع عن النفس المنصوص وفق المادة 51 لميثاق الأمم المتحدة واستخدام وسائل الكترونية أو تقليدية، اجمع الفقهاء بأن الهجمات السيبرانية تعد هجوما مسلحا إذا كانت اثاره المادية مدمرة كما هو الحال في النزاع المسلح التقليدي وبالتالي يتيح لها الحق في الدفاع عن نفسها.

المطلب الثالث: ملائمة القانون القديم لتكنولوجيات السايبر الجديدة:

أشرف أبو صيام: الهجمات السيبرانية على الاحتلال الاسرائيلي وأثرها على القضية الفلسطينية، من منظور القانون الدولي

القواعد القانونية عامة بطبيعتها وتحاول أن تنأى بنفسها. إنهم يسعون جاهدين لصياغة قواعد السلوك التي تناسب مجموعة متنوعة من المواقف، بما في ذلك تلك التي لم تُعرف بعد والتي قد تظهر في المستقبل. للوفاء بهذه المهمة، يجب أن يكون القانون واسع النطاق بما يكفي: لا يمكنه توفير قواعد محددة لمجموعة لا حصر لها من الظروف التي قد تنشأ، لذلك بدلاً من ذلك يطبق القوانين على مجموعة متنوعة من الفئات العامة، التي يحددها ويميز بعضها عن بعض، غير مقسمة، وتتطلب معالجة وتعديل مستمرين.

القوانين القائمة هي بطبيعتها عبارة عن تفاهم أو اتفاق بين أطراف ومن طبيعتها تحاول أن تكون عامه وليست خاصة، طريقة صياغة القوانين تحاول أن تكون عامة قدر الإمكان من أجل أن تلائم لحالات متنوعة، عندما تحصل تغيرات معينة في البيئة المحيطة للقانون هذا التغيير يؤدي الى تغيير أو تصحيح للقانون، سيرورة تغيير وحتلنة القانون الدولي الإنساني وفق ما يحدث من تطورات خاصة تكنولوجية ليس بالأمر السهل لأن القانون الإنساني الدولي يعبر عن تفاهمات منذ أجل بعيد أحيانا منذ أكثر من مئة سنة²⁸ وهناك صعوبة لوجود نقاط اتفاق بين كمية كبيرة من الدول حول موضوع معين وخاصة بما يتعلق بالتزاعات من خلال الهجمات السيبرانية. بنود القانون الدولي الإنساني أُعدت للحروب التقليدية والتي تستعمل فيها القوة، أما ملاءمتها للهجمات السيبرانية تلاقى صعوبة من حيث ترجمة ما يحدث على أرض الواقع. من الجدير ذكره بأن القانون الدولي الإنساني يحتوي بداخله على مبادئ كالتمييز والتناسب وتوخي الحذر وصياغتها تمت بصورة واسعة وعامة وتحتوي بمرونة واسعة نوعا ما إلا أن استعمال هذه المبادئ بكل ما يتعلق بالفضاء السيبراني تتمدد الى أوسع نطاق ولكنها غير كافية حتى تسد الحاجة الخاصة لهذه الهجمات السيبرانية. لأنه عادة القانون الدولي الإنساني يطبق على الحروب التي تستعمل فيها السلاح والقوة في العالم الحقيقي بالمقارنة مع الهجمات السيبرانية التي تحتوي على مراوغات تكنولوجية بالمُعطيات في الفضاء السيبراني مما يجعل جزء من مبادئ القانون الدولي الإنساني غير قابلة للتطبيق والفهم بسهولة مثل "النزاع المسلح"، "الهجمات"، "هدف مدني"، "هدف عسكري".

²⁸ هذه المعاهدات تشمل، خاصة، معاهدة هاج من السنوات 1899 و-1907، ومعاهدات جنيف الأربعة من سنة 1949، والبروتوكولين الإضافيين لمعاهدة جنيف من سنة 1949 وسنة 1977.

المبحث الثالث: اهم مبادئ القانون الدولي الإنساني المطبق على الهجمات السيبرانية

في هذا المبحث سنتناول 3 مبادئ التي يجب على الدول مراعاتها في الهجمات او الرد على هجمات عسكريا او بواسطة الهجمات السيبرانية. وهي مبدأ التمييز بين القوات العسكرية والمدنيين، ومبدأ التناسب لتفادي خسارة الأرواح، ومبدأ الاحتراز والحذر حتى ان كلف الامر تعيين مختصين للتأكد من صحة ودقة المعلومات.

المطلب الأول: تطبيق مبدأ التمييز بين المقاتلين والمدنيين

وفق هذا المبدأ على أطراف النزاع التمييز بين الأهداف المدنية والأهداف العسكرية، وبإمكانهم توجيه فعلهم ضد اهداف عسكرية²⁹. من هنا نستنتج بأن الهجمات السيبرانية يجب ان توجه حتما ضد اهداف عسكرية التي تعطي تقدم لطرف على اخر، كل هدف غير ذلك يعتبر هدف مدني ولا يمكنه ان يكون هدف للهجوم³⁰. حتى في حال شك بأن موقع مدني معين في الأيام العادية يعطي خدمات لمواقع عسكرية يجب الانطلاق من وجهة نظر بأنه لم يعطي الخدمات العسكرية لذلك يصبح الموقع غير قابل للهجوم³¹. الصعوبة المركزية هي في ازدواجية الاستعمال فمواقع كثيرة تستعمل للمدني والعسكري، الرأي السائد اليوم هو بأن هذه المواقع عسكرية بسبب الوظيفة التي تنفذها ويجب التطرق لها كعسكرية³². في الواقع، وفقاً لهذا الرأي، فإن الكابلات والموجهات والأقمار الصناعية، وهي أنظمة مدنية يعتمد الكثيرون عليهم، وسيتم اعتبارهم جميعاً لأغراض عسكرية، لأن لديهم أيضاً وظيفة نقل المعلومات العسكرية. عندما يتم اعتبار العديد من الأهداف في عالم الإنترنت عسكرية، إن مبدأ التمييز الذي يعتبر حجر الزاوية في حماية المدنيين من أخطار الحرب أخذ في التغير ولا قيمة له إلى حد كبير. ومن ثم، فإن أي حماية يمكن أن يوفرها القانون الدولي الإنساني ستحتاج إلى توفير بنية تحتية إلكترونية مدنية والأنظمة والخدمات المدنية التي تعتمد عليها وأن يقوم على مبادئ التناسب والحذر فقط³³.

المطلب الثاني: تطبيق مبدأ التناسب بين الضرر والميزة العسكرية الواضحة

²⁹ البند 48 للملحق (البروتوكول) الأول الإضافي الى اتفاقيات جنيف، 1977.

³⁰ البند 52(1) للملحق (البروتوكول) الأول الإضافي الى اتفاقيات جنيف، 1977.

³¹ البند 52(3) للملحق (البروتوكول) الأول الإضافي الى اتفاقيات جنيف، 1977.

³² دليل تالين، القاعدة 39 الفقرة 1.

³³ البند 51(4) للملحق (البروتوكول) الأول الإضافي الى اتفاقيات جنيف، 1977.

أشرف أبو صيام: الهجمات السيبرانية على الاحتلال الاسرائيلي وأثرها على القضية الفلسطينية، من منظور القانون الدولي

وفقاً لمبدأ التناسب، يُحظر الهجوم إذا "كان من المتوقع أن يؤدي إلى خسارة مصاحبة للحياة المدنية، والإصابات العرضية للمدنيين، والأضرار العرضية للأعيان المدنية، أو مزيج من كل هذه الأمور، والتي من شأنها أن تكون مفرطة بالنسبة إلى الميزة العسكرية الملموسة والمباشرة المتوقعة"³⁴. السؤال المركزي هو هل "الضرر" يضمن فقدان السيطرة على تأدية المهام الاعتيادية، هنا أيضاً سيكون السؤال الرئيسي هو كيفية تحديد إلى أي مدى يشمل مصطلح "الضرر" فقدان أداء المهام اليومية. وبالنظر إلى خطورة العواقب التي قد تترتب على عمل البنية التحتية المدنية، فإن الأمر مشابه من المنطقي فقط إدراج مثل هذا الضرر في حساب التناسب. من ناحية أخرى، وكما ذكرنا سابقاً، يبقى أن يتم توضيح أنواع الخلل الوظيفي المدرجة في الفئة ذات الصلة من "الضرر".

المطلب الثالث: تطبيق مبدأ الحذر والتمييز بين المنشآت العسكرية والمدنية

يُلزم القانون الدولي الإنساني الأطراف المعادية باتخاذ الاحتياطات وقت وقوع هجوم،³⁵ وضد آثار مثل هذا الهجوم.³⁶ احتياطات لحماية السكان المدنيين والأهداف المدنية³⁷. وبموجب أحكام إضافية تحدد متطلبات محددة للحذر، كما تتطلب هذه الأحكام، في جملة أمور، من يخططون للهجوم أو يقررونه أن يفعلوا كل ما في وسعهم للتأكد من أن الأهداف أهداف عسكرية، الحد من الأضرار العرضية التي تلحق بالمدنيين. كما يتعين على الأطراف المتنازعة إلغاء أو تعليق الهجوم، إذا تبين أنه ينطوي على انتهاك لمبدأ التناسب.

وفقاً لهذه الأحكام، يتعين على كل طرف في مواجهة مسلحة أن يخطط لشن هجوم إلكتروني، أن يبذل كل ما في وسعه للحصول على المعلومات اللازمة لضمان أن يكون الهدف المخطط هدفاً عسكرياً وأن الهجوم لا يفعل ذلك.

لا تسبب أضراراً لا داعي لها. قد يتطلب ذلك توظيف خبراء تقنيين يقومون قدر الإمكان، بتحليل الشبكة التي يُقصد بها أن تكون هدفاً والأنظمة المتصلة بها. في حالة عدم وجود الخبرة

³⁴ البند 51(5) (b) للملحق (البروتوكول) الأول الإضافي الى اتفاقيات جنيف، 1977.

³⁵ البند 57 للملحق (البروتوكول) الأول الإضافي الى اتفاقيات جنيف، 1977.

³⁶ البند 58 للملحق (البروتوكول) الأول الإضافي الى اتفاقيات جنيف، 1977.

³⁷ البند 58 للملحق (البروتوكول) الأول الإضافي الى اتفاقيات جنيف، 1977.

اللازمة للحصول على المعلومات وتقييمها بشكل صحيح، سيتعين على المهاجم الامتناع عن الهجوم، وفي أي حال سيكون عليه قصره على الأغراض التي لديه معلومات كافية من أجله.³⁸

في بعض الظروف، يمكن لواجب اختيار وسائل وأساليب الحرب، من وجهة نظر تسعى إلى تقليل الضرر العشوائي الذي يلحق بالمدنيين، أن يدفع أطراف النزاع لمحاولة تحقيق الهدف العسكري من خلال هجوم إلكتروني، بدلاً من اللجوء إلى المزيد. التدابير المدمرة التي تنطوي على استخدام القوة الحركية.

يتطلب واجب اتخاذ الاحتياطات ضد عواقب الهجمات، قدر الإمكان، أن تبذل أطراف النزاع المسلح جهداً للحفاظ على الفصل بين الأهداف العسكرية والأهداف المدنية والمدنيين، وتنفيذ احتياطات إضافية لحماية المدنيين والأهداف المدنية تحت السيطرة العسكرية. في ضوء ذلك، سيُطلب من أطراف النزاع من حيث المبدأ بذل كل ما في وسعهم للفصل بين البنى التحتية الإلكترونية المدنية والعسكرية. ولكن من الناحية العملية، فإن البنى التحتية السيبرانية المدنية والعسكرية متشابكة بشدة لدرجة أن الجهد المبذول للفصل بينهما غير عملي.

قد يكون الطموح العملي هو أن تبذل أطراف المواجهة كل ما في وسعها لاتخاذ الاحتياطات بحيث تظل البنى التحتية المدنية الحيوية محمية قدر الإمكان من آثار الهجوم السيبراني. يتم ذلك، على سبيل المثال، من خلال ضمان تخزين البيانات الحيوية بشكل آمن ونسخ احتياطي فعال، وكذلك من خلال تقديم المساعدة السريعة في إصلاح الأنظمة المدنية المتضررة.

المبحث الرابع: حرب سيبرانية على الاحتلال

في إطار ما يسمى بالحروب الجديدة وتراجع الحروب العسكرية التقليدية، يواجه الاحتلال الإسرائيلي حرباً جديدة، تختلف هذه المرة عن سابقتها من الحروب

المطلب الأول: الهجمات السيبرانية وجه آخر لنزاع الأدمغة بين المقاومة والاحتلال

³⁸ Droege الهامش السابق رقم 16.

أشرف أبو صيام: الهجمات السيبرانية على الاحتلال الاسرائيلي وأثرها على القضية الفلسطينية، من منظور القانون الدولي

بعيداً عن المواجهة العسكرية تدور بين المقاومة والاحتلال رعى معركة أخرى في الغرف المغلقة، وخلف شاشات ذكية، وعبر أجهزة حوسبة متطورة، تعتمد على الأدمغة، ولم يكن غريباً على المقاومة التي تعمل بصمت على تطوير قدراتها في مواجهة الاحتلال أن يستحوذ مجال صراع "الأمن السيبراني على اهتمامها كأحد أبرز أشكال الصراع المتطور، التي يمكن أن تحقق أهدافاً تستغني أو تخفف فيها المقاومة من دفع فاتورة المعركة بالدم. وفعلياً خلال السنوات الأخيرة، تعرض كيان الاحتلال إلى هجمات سيبرانية عديدة، أجبرته على الاعتراف بها رسمياً بعد أن توسعت وبانت مؤثرة، في تطور مهم بعدما كان يتعرض لهجمات مماثلة يتكلم عليها سابقاً، لكن كثرة هذه الهجمات وتضاعفها، وتحقيق عدد من أهدافها، دفع الاحتلال للإعلان عنها وسط وقوعه في حرج كبير في أوساط الجمهور الصهيوني الداخلي، واستهدفت الهجمات السيبرانية عدداً كبيراً من المرافق الصهيونية لكون الاحتلال يعتمد على التكنولوجيا المتطورة في كل محاور أعماله العسكرية والأمنية والاقتصادية، وتعرضت محطات توليد الطاقة، وشركة الكهرباء، والحسابات المصرفية والشركات الائتمانية والبنوك، لهجوم سيبراني خلال السنوات الماضية، كان الهدف تعطيلها والتأثير على الكيان الصهيوني في أي مواجهة قادمة، عدا عن أهداف أخرى متمثلة بالحصول على معلومات أمنية تستهدف مواقع ومراكز الجيش وقادته. وتحت وطأة إدراك خطورة هذا المجال، وتأثير بعض الضربات التي نفذتها المقاومة، جعل الاحتلال خبراء هذا المجال في المقاومة هدفاً للاغتيال.

المطلب الثاني: جيش القدس الإلكتروني جهة جديدة في وجه الاحتلال

على الرغم من فارق القوة العسكرية بين المقاومة والاحتلال، فإن المقاومة لم تترك وسيلة في الميدان أو في الفضاء الإلكتروني إلا واستخدمتها. وخلال الأعوام الماضية - في ظل استراتيجيتها صنع جبهات متعددة في مواجهة العدو - فعلت المقاومة سلاح "الساير" الإلكتروني، ليكون جبهة عمل متقدمة ومؤثرة في الاحتلال، ولعد الحرب على غزة عام 2014، بادر الشهيد جمعة الطحله، القائد في كتائب القسام، الجناح العسكري لحركة "حماس"، إلى إنشاء "جيش القدس الإلكتروني" وتشكيله، كسلاح إلكتروني للكتائب في مواجهة العدو. واستطاع هذا السلاح، خلال وقت قصير، تجاوز كل العقبات، وبات مؤثراً في مختلف الأوقات، وخصوصاً خلال المعارك والمواجهات، وهو الجيش المسؤول عن أغلبية الهجمات الإلكترونية التي أعلنها جيش الاحتلال خلال الأعوام الماضية، فإن "جيش القدس الإلكتروني" هو عمل فريد وعجيب للمقاومة

الفلسطينية، إذ استطاعت كتائب القسام تجاوز كل العقبات التي يضعها الاحتلال، وأسست جيشاً إلكترونيًا ممتداً لها يعمل من قطاع غزة، على رغم سيطرة الاحتلال على الطيف الكهرومغناطيسي الإلكتروني للقطاع المحاصر. كما يمتلك الجيش الإلكتروني للقسام امتدادات ومجموعات عمل متعدّدة في دول عربية وإسلامية تناصر القضية الفلسطينية، وفي الوقت الذي تعيش المقاومة الفلسطينية حصاراً خانقاً يمنع إمدادها بالعدة والعتاد والخبرات، وفي ظل وجود طاقات عربية وإسلامية تريد الجهاد والمشاركة في تحرير فلسطين، فإنّ المقاومة أتاحت عبر "جيش القدس الإلكتروني" الفرصة أمام أصحاب العقول والتخصصات الإلكترونية للمشاركة في مواجهة العدو، وهو الأمر الذي عزّز قدراتها وقوتها في مواجهة الاحتلال وما يميز "جيش القدس الإلكتروني" أنّه استطاع تنفيذ هجمات إلكترونية كبيرة جداً على "دولة" الاحتلال من داخل قطاع غزة، خلال الأعوام الماضية، على رغم سيطرة الاحتلال على شبكة "الإنترنت" في قطاع غزة، ولم يتمكّن الاحتلال من إيقاف هذه الهجمات أو إبطال تأثيرها، على رغم استنفاره وحدات "الأمن السيبراني، استطاعت المقاومة، عبر هذا السلاح الإلكتروني، إلحاق الضرر عدة مرات بعمل منظومة "القبة الحديدية" والتأثير فيها والتشويش عليها، وهو ما منح مزيداً من القوة للضربات الصاروخية التي وجهتها المقاومة إلى الاحتلال خلال معركة "سيف القدس" عام 2021، إذ عطّلت كتائب القسام جزءاً من عمل "القبة الحديدية" إلكترونياً عبر سلاح "الساير"، بالتزامن مع إغراق مدينة عسقلان بأكثر من 130 صاروخاً، وهو ما تسبب بأضرار واسعة في المدينة.

المطلب الثالث: تعزيز الدفاع والهجوم

في السابع من أبريل 2013 شنت مجموعة قراصنة على الإنترنت أولى الهجمات السيبرانية ضد المواقع الإسرائيلية، وفتحت بذلك حرباً إلكترونية لا تزال مستمرة ضد الاحتلال وأمام هذه الهجمات الإلكترونية، أوصت هيئة السايبر الاسرائيلية الحكومة والأجهزة الأمنية بضرورة تعزيز أنظمة الدفاع السيبراني للمشاريع ومنشآت البنى التحتية الحيوية والحوسبة الأمنية لمختلف المؤسسات والوزارات وكبرى الشركات المدنية لتفادي خسائر في الاقتصاد وشلل الحياة العامة، وترى هيئة السايبر ضرورة أن تتحضر إسرائيل لبناء جيش إلكتروني وقوة هجومية إلى جانب

أشرف أبو صيام: الهجمات السيبرانية على الاحتلال الاسرائيلي وأثرها على القضية الفلسطينية، من منظور القانون الدولي

القوة الدفاعية، على أن يكون هذا الجيش الإلكتروني البوصلة لرصد الهجمات السيبرانية وإحباطها والتقليل من تداعياتها على المنشآت والمؤسسات الإسرائيلية³⁹.

المبحث الخامس: مصادر القانون الدولي الإنساني المطبق على الهجمات السيبرانية باعتبارها نزاع مسلح، ودليل تالين

هناك عدة توجهات حول العالم في كيفية التعامل مع الهجمات السيبرانية ولكن من خلال هذا البحث بإمكاننا الاستنتاج بأن هذه القواعد غير كافية. سنتطرق لبعض منها وما مدى فعاليتها:

المطلب الأول: مصادر القانون الدولي الإنساني المطبق على الهجمات السيبرانية باعتبارها نزاع مسلح

اتفاقية مجلس أوروبا بشأن الجريمة الإلكترونية، المعروفة باتفاقية بودابست سنة 2001⁴⁰، تعتبر هذه الاتفاقية أكثر تفاهم على الصعيد الدولي بشأن الجريمة الإلكترونية بين الدول التابعة لمجلس أوروبا والدول التي انضمت للاتفاقية بحيث تشمل هذه الاتفاقية بنود عدة من أجل التعامل مع التحديات الناتجة عن آثار الجرائم الإلكترونية وذلك بعد التطورات التكنولوجية العديدة التي أوجبت تبني تصور جديد بالمعاهدات والاتفاقيات ضمن هذا المجال. وتشمل هذه الاتفاقية ما يلي: التدابير الواجب اتخاذها على الصعيد الوطني بكل ما يتعلق بالجرائم الإلكترونية، إبراز البيانات وأماكن تخزين بيانات الحواسيب المعتمدة، الولاية القضائية، التعاون الدولي بهذا الشأن، المساعدة المتبادلة المستعجلة بحفظ البيانات، شبكة على مدار الساعة 7 أيام في الأسبوع للمساعدات والتشاورات والقرارات الطارئة⁴¹ بحيث تساعد في التصرف السريع ومحاولة انقاذ الأدلة قبل اخفائها عن طريق المجرمين. ويمكننا القول بأن بنود هذه الاتفاقية وبعد الخوض في تفاصيلها تحتوي على تصور شمولي للتعامل مع التحديات المنبثقة من التعامل مع الجرائم الإلكترونية ودول مجلس أوروبا تطالب بتبني هذه الاتفاقية في هيئة الأمم المتحدة للعالم عامة والعمل وفق مبادئها.

³⁹ <https://www.aljazeera.net/politics/3/5/2023>

⁴⁰ الاتفاقية الأوروبية

⁴¹ الاتفاقية المتعلقة بالجريمة الإلكترونية، مجلس أوروبا، مجموعة المعاهدات الأوروبية رقم 185، بودابست، 23.11.2011.

إن اتفاقية مجلس أوروبا بشأن الجريمة الإلكترونية، المعروفة باسم اتفاقية بودابست، هي وثيقة دولية مُلزِمة تعمل كإطار عمل للتعاون الدولي بين الدول الأطراف في هذه المعاهدة. ويعمل مجلس أوروبا على وضع بروتوكول إضافي ثاني للاتفاقية من شأنه أن يعالج تعزيز التعاون والكشف عن الأدلة الإلكترونية⁴². وتحتوي أحدث مسوِّدة لنسخ البروتوكول الإضافي الثاني على أحكام تتعلق ببيانات تسجيل اسم النطاق. ظهرت هذه النسخ لأول مرة في نسخة نوفمبر / تشرين الثاني 2020 للبروتوكول، وتم تأكيدها في نسخة أبريل / نيسان 2021، التي وافقت فيها اللجنة العامة لصياغة البروتوكول لمجلس أوروبا على استخدامها في المشاورات مع الهيئات ذات الصلة لمجلس أوروبا وأصحاب المصلحة. وترد الأحكام ذات الصلة في المادة 6 من البروتوكول، على النحو المبين أدناه، وتُستكمل بأجزاء ذات صلة في المذكرة التوضيحية الواردة في نفس النسخة

المطلب الثاني دليل تالين⁴³ بشأن القانون الدولي المطبق على الحروب السيبرانية:

وهو عبارة عن مقترح لكيفية التعامل مع الجرائم الإلكترونية وهي ورقة مقترحة من قبل مجموعة خبراء دوليين وعلى رأسهم المحرر العام Michael N. Schmitt⁴⁴ وبدعوة من مركز تالين التابع لحلف الناتو التعاوني الإلكتروني للتميز، من قبل مجموعة دولية تضم حوالي عشرين خبيراً ويضم 7 فصول و 12 قسماً و 95 قاعدة. ويشمل هذا الدليل قسمين: الأول يعالج قانون الأمن الإلكتروني والثاني قانون النزاعات الإلكترونية، ويشمل المبادئ التالية: سلطة القضاء والرقابة، مسؤولية الدولة، استخدام القوة، الدفاع عن النفس، تصرفات المنظمات الحكومية الدولية، قانون النزاعات المسلحة السيبرانية، سير العمليات العدائية، الهجمات، وسائل الحرب واساليبها، إدارة الهجمات، الاحتياطات، الغدر، الاستخدام غير السليم والتجسس، الحصار والمناطق، بعض فئات الأشخاص والاعيان والانشطة، الصحفيين، المنشآت التي تحتوي على قوى خطرة، الاعيان التي لا غنى عنها لبقاء السكان المدنيين، الممتلكات الثقافية، البيئة

⁴² نشر على الموقع الإلكتروني: <https://www.icann.org>

⁴³ تمت ترجمة دليل تالين من اللغة الإنجليزية للغة العربية بواسطة علي محمد كاظم الموسوي وتحت اشراف أ.د حيدر أدهم الطائي، 2017.

⁴⁴ مايكل إن. شميث باحث في القانون الدولي الأمريكي متخصص في القانون الدولي الإنساني، واستخدام قضايا القوة والقانون الدولي الساري على الفضاء الإلكتروني.

أشرف أبو صيام: الهجمات السيبرانية على الاحتلال الاسرائيلي وأثرها على القضية الفلسطينية، من منظور القانون الدولي

الطبيعية، المحفوظات والاتصالات الدبلوماسية، العقوبات الجماعية، المساعدة الإنسانية، الاحتلال، الحياد. ويتمسك هذا الدليل بالتقسيم التقليدي للنزاعات المسلحة الدولية والنزاعات المسلحة غير الدولية، ويقر بأن العمليات الإلكترونية وحدها قد تشكل نزاعات مسلحة تبعا للظروف، وقد اعتبر الهجوم الإلكتروني بمثابة استخدام للقوة إذا كان أثر هذا الهجوم عند مقارنته بالاستخدام الفعلي للقوة مساويا له، أو قريبا منه⁴⁵، ففي هذه الحالة يجب إخضاع هذا النوع من الهجمات لقانون النزاعات المسلحة، بحيث يتم إخضاع أطراف النزاع للاتفاقيات الدولية التي تنظم هذه النزاعات، لاسيما الآثار المدمرة لتلك العمليات⁴⁶، ويقدم الدليل في هذا الصدد تعريفاً "للهجوم السيبراني" بموجب القانون الدولي الإنساني بوصفه "عملية إلكترونية سواء هجومية أو دفاعية يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الأضرار بأعيان أو تدميرها كما يعدّ توقف أحد الأعيان عن العمل قد يشكل ضرراً مادياً"⁴⁷، وتتمثل وجهة نظر اللجنة الدولية في أنه إذا تعطل أحد الأعيان فليس من المهم كيفية حدوث ذلك، سواء بوسائل حركية أو عملية إلكترونية⁴⁸، وهذه القضية مهمة للغاية في الممارسة العملية، حيث إنّ أي عملية إلكترونية تستهدف تعطيل شبكة مدنية خلاف ذلك لن يشملها الحظر الذي يفرضه القانون الدولي

من هنا فعلى هذا النحو، كان هذا هو الجهد الأول لتحليل هذا الموضوع بشكل شامل وموثوق وإلضفاء قدر من الوضوح على القضايا القانونية المعقدة المرتبطة بالحرب السيبرانية. يعتبر هذا الدليل حتى اللحظة ورقة بحثية غير ملزمة للدول والسبب الرئيسي هو تباعد وجهات النظر بين الدول وصعوبة الحصول على انضمام غالبية الدول إن لم يكن معظمها من أجل اتفاقية أو معاهدة شاملة لمعالجة التحديات الناتجة عن الحروب السيبرانية.

⁴⁵ المادة 69 من دليل تالين.

⁴⁶ المادة 80 من دليل تالين.

⁴⁷ المادة 92 من دليل تالين.

⁴⁸ Decision on the Defence motion for interlocutory appeal, paras. 120, 124.49

الخاتمة:

مع دخولنا في عصر هذا النوع الجديد من الحروب فإن الخطورة المتعلقة بوسائل القتال الجديدة وأساليبه تكمن في انتقاء 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 أن لا تتعدى هذا الغرض فتصل الى الاعمال الوحشية، كما ان الهجمات السيبرانية ممكن ان تستهدف القطاعات الاقتصادية والأجنبية وغيرها في إطار نزاع مسلح. ورغم ذلك فقد تم التوصل لعدد من النتائج التي تجيب على التساؤل الرئيسي للدراسة وما نتج عنه من تساؤلات فرعية والوقوف على مدى صحة فروض الدراسة:

1- القانون الدولي الإنساني غير كافٍ للتعامل مع الهجمات السيبرانية وتفتقر الأمم المتحدة لاتفاقية شاملة بين الدول في هذا المجال، ولكن هنالك اتفاقية بهذا الشأن في المجلس الأوروبي بحيث تعتبر اتفاقية ناجعة وهادفة، اما دليل تالين فبقي كورقة علمية دون تبنيها بشكل رسمي.

2- إن الاحتلال الاسرائيلي ينظر الى الهجمات الالكترونية المتواصلة أنها جبهة جديدة فتحت عليه لا تقل ضراوة عن الجبهات القتالية الأخرى.

3- أن الهجمات السيبرانية يجب ان توجه حتما ضد اهداف عسكرية التي تعطي تقدم لطرف على اخر، كل هدف غير ذلك يعتبر هدف مدني ولا يمكنه ان يكون هدف للهجوم.

4- أن تطبيق مبدأ التمييز بين المقاتلين على الهجمات السيبرانية للأغراض العسكرية لا سيما الهجومية هي مسألة في غاية التعقيد بالقدر الذي يمكن تصوره، أن يكون المهاجم في أغلب الأحيان بعيداً عن المكان المستهدف من الهجوم والتي قد تصل أحياناً لمسافة تتجاوز الالاف الكيلومترات.

5- يجب الوقوف على تأثير الأمن السيبراني على شكل النظام العالمي الجديد الذي أخذ في التبلور والتغير، فمن المهم معرفة ألى أي درجة يُساعد اهتمام دول العالم بقضايا الأمن السيبراني، وما يصاحبه من آليات وتقنيات حديثة على تغيير بنية النظام الدولي، فهو يغير معايير وتوازنات القوة الأمر الذي قد يهدد الأمن والسلم الدوليين.

أشرف أبو صيام: الهجمات السيبرانية على الاحتلال الاسرائيلي وأثرها على القضية الفلسطينية، من منظور القانون الدولي

قائمة المراجع:

1. ساره عبد العزيز، الحرب السيبرانية- التداعيات المحتملة لتصاعد الهجمات الالكترونية على الساحة الدولية، 2016 دراسة المستقبل عبر الرابط <https://platform.almanhal.com/details/article/100427>.
 2. الباحث محمود احمد عابنة، محمد معمر الرازقي، جرائم الحاسوب، ابعادها الدولية، دار الثقافة للنشر والتوزيع 2005، ص 15.
 3. أسامة احمد المناعسة – جلال محمد الزغبى، جرائم الحاسب الالى والانترنت، دراسة تحليلية مقارنة، دار وائل للنشر والتوزيع، 2001، ص 73.
 4. أ.د عمر اعمر، الحرب الالكترونية في القانون الإنساني، دراسات، علوم الشريعة والقانون، المجلد 46، عدد 3، صفحة 134، 2019.
 5. د. محمد حماد موهج الهيتي، جرائم الحاسوب ماهيتها، موضوعها، اهم صورها والصعوبات التي تواجهها، دار المناهج للنشر والتوزيع 2006، ص 21.
 6. د. فتوح الشاذلي – عفيفي كامل عفيفي، جرائم الكمبيوتر، منشورات الحلبي الحقوقية، 2003، ص 34.
- اتفاقيات معاهدات وتشريعات دولية:**
1. اتفاقيات جنيف الأربعة 1949 وبروتوكولاتها الوال والثاني..
 2. الاتفاقية المتعلقة بالجريمة الالكترونية، مجلس أوروبا، مجموعة المعاهدات الأوروبية رقم 185، بودابست، 23.11.2011.
 3. اتفاقية لاهاي 1907.
 4. معاهدة هاج 1899، 1907.
- تشريعات مقترحة لم تنطبق:**
1. دليل تالين.
- مصادر اجنبية:**
- أ. الإنجليزية:

1. Kittichaisaree public international law of Cyberspace Law Governance and Technology op .cit 7 p154.

2. Cordula Droegé، Get off My Cloud: Cyber Warfare، International Humanitarian Law 1 and The Protection of Civilians،

94(886) INTERNATIONAL REVIEW OF THE RED CROSS 533، 538(2012).

3. ICTY، Prosecutor v. Boskoski، IT-04-82-T، Trial Chamber Judgement of July 10 2008، paras 199-203; ICTY، Prosecutor v. Limaj، IT-03-66-T، Trial Chamber Judgement of November 30، 2005، paras. 94-134; ICTY، Prosecutor v. Haradinaj، IT-04-84-T، Trial Chamber Judgement of April 3، 2008، para. 60.

4. 'INTERNATIONAL COMMITTEE OF THE RED CROSS، CUSTOMARY INTERNATIONAL HUMANITARIAN LAW Vol. I، Rules، (Jean-Marie Henckaerts and Louise Doswald-Beck eds.، 2005).

5. MICHAEL BOTHE، KARL JOSEF PARTSCH & WALDEMAR A. SOLF، NEW RULES FOR VICTIMS OF ARMED CONFLICTS: COMMENTARY TO THE TWO 1977 PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 1949، 289 (1982).

6. Cordula Droege، Get off My Cloud: Cyber Warfare، International Humanitarian Law and The Protection of Civilians، 94(886) INTERNATIONAL REVIEW OF THE RED CROSS 533، .)2102(835.

7. Decision on the Defence motion for interlocutory appeal، paras. 120، 124.43.

8. Tikk Eneken، Kaska Kadri & Vihul Liis، International Cyber Incidents: Legal Consideration (2010).

مواقع الكترونية:

1. <https://www.icann.org/ar/blogs/details/feedback-on-the-second-additional-protocol-to-the-convention-on-cybercrime-ends-early-may-23-4-2021-ar>.

2. <https://news.un.org/ar/>

3. <https://platform.almanhal.com/details/article/100427>.

4. <https://www.aljazeera.net/politics/3/5/2023>

5. www.almayadeen.net/artical/7/3/2023

6. <https://palinfo.com.20/20/2022/196233>