
بسم الله الرحمن الرحيم

مجلة جامعة الملك عبدالعزيز: الآداب والعلوم الإنسانية، م ٣٣ ع ١ ص ص: ١ – ٥٦٥ (٢٠٢٥م)
ردمد ٠٩٨٩ – ١٣١٩
رقم الإيداع ١٤/٠٢٩٤

مجـــــلة
جامعة الملك عبد العزيز
الآداب والعلوم الإنسانية

المجلد ٣٣ العدد ١

٢٠٢٥ م

مَركز النشر العلمّي
جَامعَة الملك عبدالعزيز
ص ب: ٨٠٢٠٠ – جدة: ٢١٥٨٩

http://spc.kau.edu.sa

مجلة جامعة الملك عبدالعزيز: الآداب والعلوم الإنسانية، م ٣٣ ع ١ ص ص: ١ – ٥٦٥ (٢٠٢٥م)
ردمد ٠٩٨٩ – ١٣١٩
رقم الإيداع ١٤/٠٢٩٤

المحتويات

القسم العربي

الصفحة

مجلة جامعة الملك عبدالعزيز: الآداب والعلوم الإنسانية، م ٣٣ ع ١ ص ص: ١ – ٥٦٥ (٢٠٢٥م)
ردمد ٠٩٨٩ – ١٣١٩
رقم الإيداع ١٤/٠٢٩٤

القسم الإنجليزي
المستخلص العربي

مجلة جامعة الملك عبدالعزيز: الآداب والعلوم الإنسانية، م ٣٣ ع ١ ص ص: ٤٣٩ – ٤٥٧ (٢٠٢٥م)
DOI: 10.4197/Art.33-1 - 16

الهجمات السيبرانية الحربية كفتيل للحروب المستحدثة في ظل النزاع المسلح وفق دليل تالين

راويه بوالانوار

طالبة دكتوراه، قسم القانون العام، كلية الحقوق، جامعة الإخوة منتوري قسنطينة ١، قسنطينة، الجزائر
rawiya.boulanouar@doc.umc.edu.dz

المستخلص:

تتناول هذه الورقة البحثية بالدراسة والتحليل موضوع الهجمات السيبرانية الحربية التي تشكل أحد أهم التحديات التي تواجه البشرية في زمن الثورة الصناعية الرابعة، وبالاعتماد على المنهج الوصفي والتحليلي تهدف هذه الدراسة إلى تقديم تحليل معمق للهجمات السيبرانية الحربية وفق دليل تالين، وكيف ساهمت في إفراز تغيرات جذرية طرأت على بنية الحرب الكلاسيكية، وذلك بتحويلها إلى حرب مستحدثة تتدعم باستخدام القوة الالكترونية الناعمة كأسلحة مثل الفيروسات وبرامج التجسس وقرصنة المعلومات العسكرية والإستراتجية، كما خلصت هذه الدراسة إلى نتيجة مفادها أن تأثير الهجمات السيبرانية الحربية لا يختلف عن تأثير الأسلحة التقليدية في النزاع المسلح.

الكلمات المفتاحية: الهجمات السيبرانية الحربية، التهديد الرقمي، الحروب المستحدثة، الأمن العالمي، دليل تالين.

مقدمــة

شهد العالم تطورا في المخاطر الأمنية مع تطور مراحل النضج التكنولوجي، والانتقال من مرحلة النمو السريع إلى مرحلة الاستعمال المكثف، حيث أصبحت قضية أمن الفضاء الالكتروني تلقى اهتماما متصاعدا على أجندة الأمن العالمي، في ظل تنامي التحديات والتهديدات الجديدة المندرجة على سلم أولويات قضايا

المجتمع الدولي والتي من بينها الهجمات السيبرانية بشكل عام والهجمات السيبرانية الحربية بشكل خاص، هاته الأخيرة التي تتصل بالفضاء الالكتروني الذي شكل تحولا جذريا في خصائص ومهددات الأمن العالمي.

تتجلى أهمية موضوع الهجمات السيبرانية الحربية في كونها أصبحت وسيلة للتهديدات الأمنية والصراعات التي تحصل في الفضاء الالكتروني، وهو الأمر الذي جعل من أمن الفضاء الإلكتروني يلقى اهتمامًا متصاعدًا على أجندة الأمن الدولي، وذلك في محاولة لمواجهة تصاعد التهديدات الإلكترونية ودورها في التأثير على الطابع السلمي للفضاء الإلكتروني، وفي محاولة أخرى لدفع الجهود الدولية لمنع عسكرة المجال الالكتروني[1].

كما تهدف هذه الدراسة إلى معرفة طبيعة الهجمات السيبرانية الحربية وفق دليل تالين بإعتبارها تشكل تهديدات وتحديات أمنية جديدة غير تقليدية ضمن النزاع المسلح، في ظل الأنماط والتحديات المتنوعة لها.

وهو ما يدفعنا لطرح **الإشكالية** الآتية:

ما مدى ملائمة القواعد القانونية التقليدية الخاصة باستخدام القوة مع طبيعة الهجمات السيبرانية الحربية كفتيل للحروب المستحدثة وفق دليل تالين؟

كما تتفرع على هذه الاشكاليه الرئيسية تساؤلات فرعية هي كالتالي:

- ما المقصود بالهجمات السيبرانية الحربية؟

- فيما تتمثل الطبيعة القانونية للهجمات السيبرانيه الحربية؟

- هل يعتبر دليل تالين آلية لتكييف وتطبيق المبادئ الأساسية للقانون الدولي الإنساني على الحروب السيبرانية المستحدثة القائمة على الهجمات السيبرانية الحربية؟

- هل ترتب الهجمات السيبرانية الحربية المسؤولية؟

(5) عادل عبد الصادق، الهجمات السيبرانية- أنماط وتحديات جديدة للأمن العالمي-، المركز العربي لأبحاث الفضاء الالكتروني، رابط الدخول: https://accronline.com/article، تاريخ الدخول: ٢٠٢٤/٠١/٢٠، ساعة الاطلاع: ١٠:٠٠.

وللتصدي للإشكالية المطروحة أعلاه والتساؤلات الفرعية المشتقه عنها نتناولها وفق محورين الأول حول الهجمات السيبرانية الحربية (قراءة في المفهوم)، والمحور الثاني بخصوص تحديد طبيعة الهجمات السيبرانية الحربية وفق دليل تالين.

المحور الأول: الهجمات السيبرانية الحربية (قراءة في المفهوم)

لم تكن الهجمات السيبرانية بصفة عامة معروفة إلا في وقت قريب، ما يشكل إحدى أهم التحديات الراهنة التي يواجهها المختصون في القانون الدولي العام، وما يزيد في اتساع التحدي الذي يواجهه المختصون في القانون الدولي العام والإنساني على وجه الخصوص، إنما يتجسد في الغموض الذي اكتنف مفهوم الهجمات السيبرانية وعدم الاتفاق على تعريف محدد[2]، والى جانبها الهجمات السيبرانية الحربية بصفة خاصة موضوع ورقتنا البحثية كأحد الهجمات المنبثقة عن الهجمات السيبرانية.

أولا: مفهوم الهجمات السيبرانية الحربية

٠١- تعريف الهجمات السيبرانية الحربية

في حقيقة الأمر لا يوجد هناك تعريف خاص بالهجمات السيبرانية الحربية بالتحديد، إلا أننا نجد بالمقابل العديد من التعريفات المقدمة بشان الهجمات السيبرانية بشكل عام، وعليه سوف نعرض البعض من هذه التعريفات لنستنتج من خلالها تعريف حول الهجمات السيبرانية الحربية.

- عرف مايكل شميت الهجمات السيبرانية على أنها"مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نُظم المعلومات المعادية بهدف التأثير والإضرار بها، وفي الوقت نفسه للدفاع عن نُظم المعلومات الخاصة بالدولة المهاجمة[3].

أما جونيدو مارشال فيعرفها بأنها عملية الاستغلال المتعمد لأنظمة الكمبيوتر والشبكات المعتمدة على التكنولوجيا من خلال البرامج الضارة[4].

---

(2) أحمد عبيس نعمة الفتلاوي، "الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، ***مجلة المحقق الحلي للعلوم القانونية و السياسية***، جامعة بابل، المجلد ٨، العدد ٤، ٢٠١٦، ص ٦١٣.

(3) Michael N Schmitt, computer network attack and the use of force in international law Thoughts on a normative framework, Columbia journal of transnational law, 1998-1999, p890.

(4) Junaidu Bello Marshall, Cyber-attacks: the legal response, International journal of international law, Vol 01, No 02, universal multidisciplinary research institute, India, P 03.

كما تعرف الهجمات السيبرانية على أنها فعل يقوض من قدرات الشبكة المعلوماتية من خلال استغلال احد نقاط الضعف ما يمنح المهاجم القدرة على التلاعب بالنظام، وتتعدد ما بين الأساليب الممنهجه أو العشوائية فقد تستخدم من طرف الرسميين كأساليب ضغط أو بشكل عشوائي من طرف محترفين للنفع الذاتي، أو هجمات منظمة من طرف جماعات مارقة[5].

بالنسبة لدليل تالين فلقد عرف الهجمات السيبرانية بأنها "عمليات سيبرانية سواء كانت هجومية أو دفاعية، والتي يهدف من خلالها بصورة معقولة التسبب بالإصابة أو وفاة الأشخاص أو الإضرار أو تدمير الأعيان (الأهداف)[6].

وعليه من خلال التعاريف التي عرضناها سابقا حول الهجمات السيبرانية بشكل عام يمكننا القول **إن:**

الهجمات السيبرانية الحربية هي هجمات الكترونية معادية في سياق نزاع مسلح، تقوم بها إحدى الدول على أجهزة الكمبيوتر والشبكات للدولة المعادية في محاولة لتعطيل الاتصالات وأجزاء أخرى من البنية التحتية لهذه الأخيرة، كآلية لإلحاق ضرر(تغيير أو تعطيل برامج أو تدمير معطيات أو سرقة معلومات سرية أو اختراق أنظمة التحكم والأوامر أو تعطيل الدفاعات. ..الخ)، بغرض تحقيق أهداف عسكرية.

٠٢- خصائص الهجمات السيبرانية الحربية

تتميز الهجمات السيبرانية الحربية بمجموعة من الخصائص نوجزها فيما يلي:

أ- هي بمثابة تهديدات يواجهها أمن الفضاء السيبراني والأمن القومي للدول، فهي مرتبطة بالاستخدامات غير السلميه للفضاء السيبراني الأكثر تطورا وتعقيدا وخطورة[7].

ب- تستهدف أنظمة معلومات الكمبيوتر أو البنية التحتية أو شبكات الكمبيوتر للدولة المعادية.

---

(5) عنترة بن مرزوق، حرشاوي محي الدين، ***الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية***، مجلة دفاتر السيادة والقانون، جامعة قاصدي مرباح، ورقلة، العدد ١٧، ٢٠١٧، ص ٦٦.

(6) القاعدة ٣٠ من دليل تالين بشأن القانون الدولي المطبق على الحروب السيبرانية لعام ٢٠١٣.

(7) ماجد عزيز إسكندر، التوظيف السياسي للهجمات السيبرانية ومخاطرها على الأمن القومي، مركز الإمارات للبحوث والدراسات الإستراتجية، ٢٠٢٣، أبو ظبي، ص ص ٧-٩.

ت– المهاجم هو دولة أو عملية تحاول الوصول إلى البيانات أو الوظائف أو المناطق المحظورة الأخرى في نظام الدولة المعادية دون الحصول على إذن.

ث– يتم استخدام الهجوم السيبراني الحربي من قِبل دولة [8]في سياق نزاع مسلح تحت ظل قيادة عسكرية، مما ينتج معه احتمالية شن حرب سيبرانية دفاعية أو تقليدية.

ج – تتم في عالم افتراضي قائم على استخدام بيانات رقمية، ووسائل اتصال تعمل الكترونيا[9].

ح – تعمل على اختراق مواقع الكترونية حساسة، عادة ما تقوم بوظائف تصنف بأنها ذات أولوية، كأنظمة حماية محطات الطاقة النووية أو الكهربائية أو المطارات ووسائل النقل الأخرى...الخ.

خ– تعد الهجمات السيبرانية الحربية بمثابة قوة مرنة يتم استخدامها داخل الفضاء الالكتروني في سياق نزاع مسلح.

د– تعتبر من احدث الأسلحة الرقمية المستعملة في إصابة أهداف إستراتجية يصعب الوصول لها عبر الفضاء السيبراني[10].

هـ– تتخذ الهجمات السيبرانية الحربية عدة أشكال، تساهم في إختراق الأنظمة الدفاعية والبيانات من خلال استغلال نقاط الضعف من بينها نذكر هجمات **DRIVE-BY**، هجمات رفض الخدمة وهجمات رفض الخدمة الموزعة (كلا النوعين الأخيرين من الهجمات يغمران الخادم أو تطبيق الويب بهدف مقاطعة الخدمات، ونظرًا لأن الخادم يتم غمره بمزيد من حزم **TCP/UDP"** أكثر مما يمكنه معالجتها، فقد يتعطل وقد تتلف البيانات، وقد يتم توجيه الموارد بشكل خاطئ أو حتى استنفادها لدرجة شل النظام)[11]، برامج القنابل المنطقية.

---

(8) سامي محمد بونيف، دور الاستراتجيات الإستباقية في مواجهة الهجمات السيبرانية– الردع السيبراني أنموذجا–، ***المجلة الجزائرية للحقوق والعلوم السياسية***، المجلد ٤، العدد ٠٧، ٢٠١٩، ص ١٢٤.

(9) أحمد عبيس نعمة الفتلاوي، المرجع السابق، ص ٦١٥.

(10) عادل عبد الصادق، أسلحة الفضاء الالكتروني في ضوء القانون الدولي الإنساني، وحدة الدراسات المستقبلية، الإسكندرية، ٢٠١٦، ص٦١.

(11) نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني–التهديد المتصاعد لأمن الدول–، ***مجلة مركز بابل للدراسات الإنسانية***، جامعة بابل، العراق، المجلد ٨، العدد ٦، ٢٠١٨، ص ١٢٥.

و- وسيلة من وسائل القتال الجديدة وأساليبه، ينتفي فيها عنصر المواجهة المباشرة والتقدير البشري الذي يصاحبها.

ر- يمكن أن تستهدف الهجمات السيبرانية الحربية القطاعات الاقتصادية، الأمنية، الزراعية، الصناعية وغيرها من القطاعات التابعة للدولة في إطار نزاع مسلح.

م- التغلب على العامل الجغرافي حيث يختفي معها الأثر ولا يؤثر على اختيار الجهة المستهدف الهجوم عليها[12].

٠٣- تمييز الهجمات السيبرانية الحربية عن الجرائم السيبرانية

تختلف الهجمات السيبرانية الحربية عن الجرائم السيبرانية المرتكبة في الفضاء السيبراني بالإستناد على معايير التمييز التالية:

أ- **المصدر:** الهجمات السيبرانية الحربية تكون صادرة عن الدولة أو إحدى مؤسساتها الحكومية بهدف إضعاف الوظيفة التي تقوم بها أجهزة الحاسوب المستهدفة للدولة المعادية في إطار نزاع مسلح، أما الجرائم السيبرانية فتصدر غالبا عن أفراد أو قراصنة متخصصين يتجاوزون مساحة النزاع المسلح (حالة سلم).

ب- **القواعد القانونية المطبقة:** القواعد القانونية المطبقة على الهجمات السيبرانية الحربية هي قواعد القانون الدولي العام(تحديدا قواعد اللجوء إلى القوة)، بينما تطبق على الجرائم السيبرانية قواعد قانونية مغايرة.

ج- **الباعث:** الباعث على الهجمات السيبرانية الحربية هو إضعاف وظيفة شبكات الحاسوب في دولة أخرى لتحقيق أهداف سياسية، أمنية أو عسكرية أو اقتصادية...الخ، أما الجرائم السيبرانية فالباعث منها الربح المادي أو الرغبة في الإنتقام.

د- **الأضرار المحتملة:** بالنسبة للأضرار المحتملة للهجمات السيبرانية الحربية، فهي تهدف إلى إلحاق ضرر شامل سواء للأشخاص أو الممتلكات في الدولة الأخرى فهي تعد أضرار واسعة، أما بالنسبة للأضرار المحتملة للجرائم السيبرانية فينحصر ضررها في أشخاص معينين فقط بالإضافة إلى الذمة المالية لهؤلاء الأشخاص كأقصى تقدير.

(12) وسام محمود عرفان، سبل مكافحة الهجمات السيبرانية دوليا، مجلة الدراسات القانونية والإقتصاديه، المجلد ١٠، العدد ٠٣، ٢٠٢٤، ص ٢٩٩١.

٤- التحديات التي تطرحها الهجمات السيبرانية الحربية و سبل مواجهتها

أ- التحديات التي تطرحها الهجمات السيبرانية الحربية

تشكل الهجمات السيبرانية الحربية تهديدا حقيقيا لأمن الدول وسلامتها، خاصة مع التطور المتصاعد للتكنولوجيا التي يصاحبها الإستخدام اللاشرعي، مما يوحي الى إمكانية ظهور تحديات وتهديدات جديدة في المستقبل تساهم في التأثير وخلق توتر في العلاقات بين الدول، ومن بين هذه التهديدات نذكر مثلا:

* الهجمات السيبرانية الحربية المدعومة بالذكاء الإصطناعي:يعد الذكاء الاصطناعي تقنية سريعة التطور ويمكن استخدامها لإنشاء هجمات سيبرانية أكثر تعقيدا وقوة، مما يجعل من الصعب اكتشافها والتصدي لها، حيث يمكن استخدام الذكاء الاصطناعي لإنشاء برامج ضارة أكثر ذكاء يمكنها التهرب من تقنيات الأمان التقليدية، كما يمكن أيضا استخدام الذكاء الاصطناعي لإنشاء هجمات تستهدف البنية التحتية الحيوية، مثل شبكات الطاقة أو نظم النقل[13].

* عسكرة الفضاء السيبراني:وذلك سعيا لدرء تهديداته مما أدى إلى بروز اتجاهات في هذا الإطار، مثل التطور في مجال سياسات الدفاع والأمن الإلكتروني، وتصاعد القدرات في سباق التسلح السيبراني، وتبني سياسات دفاعية سيبرانية لدي الأجهزة المعنية بالدفاع والأمن في الدول، وتزايد الاستثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة[14].

* دخول العالم في سباق التسلح السيبراني.

ب- سبل مواجهة الهجمات السيبرانية الحربية.

تتعدد وتتنوع سبل مواجهة الهجمات السيبرانية الحربية نذكر من بينها على سبيل المثال:

- سبل المواجهة ذات الطابع التقني للهجمات السيبرانية: نذكر من بينها:

* جدران الحماية: تعد من أقوى السبل الوقائية ضد الهجمات السيبرانية الحربية الماسة بأنظمة الكمبيوتر والشبكات، والتي تعرف أيضا باسم الجدران النارية.

---

(13) أحمد عنتر، تقنيات الأمن السيبراني والتحديات المستقبليه، رابط الدخول: https://www.aljazeera.net/tech/2023/12/4، تاريخ الاطلاع: ٢٠٢٤/١٠/٢١، ساعة الاطلاع: ١٠:٠٠.

(14) عادل عبد الصادق، أنماط الحرب السيبرانية و تداعياتها على الأمن العالمي، مجلة السياسة الدولية، رابط الدخول: https://www.siyassa.org.eg، تاريخ الاطلاع: ٢٠١٤/١٠/٢١، ساعة الاطلاع: ١١:٠٠.

* أنظمة كشف التسلل: تتألف هذه الأنظمة من عدة مكونات هي جهاز استشعار ينبه على وقوع الأحداث ولوحة تحكم لمراقبة الأحداث والتنبيهات والتحكم بأجهزة الاستشعار في قاعدة البيانات، وتكون أنظمة كشف التسلل مصنفه بالإعتماد على نوع وموقع أجهزة الإستشعاروالمنهجيات المستخدمة على المحرك(15).

– إدماج الفضاء السيبراني ضمن الأمن القومي للدول، وذلك عبر تحديث الجيوش وتدشين وحدات متخصصة في الحروب السيبرانيه، وإقامة هيئات وطنية للأمن والدفاع السيبراني والقيام بالتدريب، وإجراء المناورات لتعزيز الدفاعات السيبرانيه، والعمل على تعزيز التعاون الدولي في مجالات تأمين الفضاء السيبراني، والقيام بمشروعات وطنية للأمن السيبراني(16).

– تحديث القدرات الدفاعية والهجومية، حيث سعت الدول إلى تحديث النشاط الدفاعي لمواجهة مخاطر الهجمات السيبرانية الحربيه الناتجة عن الحرب السيبرانية، والاستثمار في البنية التحتية المعلوماتية وتأمينها، وتحديث القدرات العسكرية، ورفع كفاءة الجاهزية لمثل هذه الهجمات عن طريق التدريب، والمشاركة الدولية في حماية البنية المعلوماتية والاستثمار في رفع القدرات البشرية داخل الأجهزة الوطنية المعنية، وهنا يتعلق التوجه الأخطر بنقل تلك القدرات من الدفاع إلى الهجوم عن طريق استخدام تلك الهجمات في إطار إدارة الصراع والتوتر مع دول أخرى(17).

ثانيا: نماذج تطبيقية عن هجمات سيبرانية حربية

في ظل تزايد الهجمات السيبرانية الحربية على مستوى الفضاء السيبراني بما يكرس ما يمكن أن نصطلح عليه بالاختراق الأمني اللامصرح، فلقد أعلن المنتدى الاقتصادي العالمي أن الهجمات السيبرانية بصفة عامة تشكل خامس أكبر الأخطار العالمية إلى جانب أسلحة الدمار الشامل والتغير المناخي، وهذا نظرا لانتشارها الكبير فضلا عن آثارها الهائلة التي تصيب الدول وكذا الأفراد على حد سواء(18)، لذلك يطرح لنا الواقع العديد من الهجمات السيبرانية الحربية التي وقعت في ظل الصراع الروسي الاوكراني، فمنذ بداية الأزمة الروسية الاوكرانية استخدم طرفي الصراع الأمن الإلكتروني كتكتيك هجومي أو ردعي لتغيير ميزان الحرب،

(15) محمد الصغير كاوجة، الهجمات السيبرانية بين الواقع وسبل المواجهة، مجلة الرسالة للدراسات الإعلامية، المجلد ٠٦، العدد ٠٣، ٢٠٢٢، ص ١١٦.

(16) عادل عبد الصادق، أنماط الحرب السيبرانية و تداعياتها على الأمن العالمي، مرجع سابق.

(17) عادل عبد الصادق، المرجع نفسه.

(18) رابح منزر، سعيد درويش، الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول، مجلة صوت القانون، جامعة الجيلالي بونعامة، خميس مليانة، المجلد ٨، العدد ٠١، ٢٠٢١، ص ٥٣٩.

فلقد نجحت موسكو مبدئيا في توظيف استراتيجيتها السيبرانية(هجمات سيبرانية حربية) لتمهيد الطريق لقواتها العسكرية لتنفيذ مهامهم الخاصة في إخراج منظومة الدفاع الجوي الأوكرانية من الخدمة، فلقد تجسدت ملامح الإستراتجية السيبرانية الروسية ضد أوكرانيا في العديد من المحاولات لاختراق الشبكة الإلكترونية الأوكرانية، والسعي لإخراجها من الخدمة نذكر منها:

٠١ – هجوم DDoS الروسي ضد أوكرانيا

شنت روسيا بتاريخ: ٢٠٢٢/٠٢/١٥ هجوما كبيرا (DDoS)[19] على أوكرانيا، مما نتج عنه تدمير مواقع وزارة الدفاع والجيش وأكبر بنكين في أوكرانيا وهما(برايفيت بنك و أوشاد بنك)، حيث وصف هذا الهجوم بأنه أكبر هجوم من نوعه في تاريخ البلاد، وهذا حسب تصريح مسؤولي الحكومة الأوكرانية الذين أشاروا إلى أن روسيا كانت وراءه على الرغم من وجود مخاوف من أن هجوم الحرمان من الخدمة يمكن أن يكون غطاءاً لهجمات أكثر خطورة مستقبلا .

هنا يشكل الفضاء السيبراني الفضاء الخامس للحروب بعد الفضاءات البري والجوي والبحري والفضائي[20].

٠٢– تعطيل الأقمار الصناعية الأوكرانية

استبقت القوات العسكرية الروسية المشاركة في العملية الخاصة في أوكرانيا هجومها الشامل بريًا وبحريًا وجويًا بتعطيل شبكة اتصالات الأقمار الصناعية، وهو الأمر الذي أدى إلى إعاقة الدفاعات الأوكرانية في كييف، وقد كان الهجوم الذي طال شركة الأقمار الصناعية الأوكرانية **Viasat** من أخطر عمليات الهجوم الإلكتروني في الحرب، إذ أدى إلى تعطيل الاتصالات العسكرية الأوكرانية مما تسبب في قطع المعلومات بين أفرع الجيش الأوكراني المختلفة[21].

مما تعكسه لنا استراتجية روسيا السيبرانية في حربها ضد أوكرانيا أنها توجه هجمات سيبرانية حربية إلى البنية التحتية لتكنولوجيا المعلومات الأوكرانية، ما دفع بحكومة هذه الأخيرة في كييف للبحث عن متطوعين قادرين على صد هجمات القراصنة الروس والتحضير لهجماتهم الخاصة على البنية التحتية لتكنولوجيا المعلومات

---

(19) هجوم DDoS والذي نعني به حرمان الموزع من الخدمة كبير.

(20) ساعد بوقرص، الأمن السيبراني"مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتجيات خاصة"، مجلة الأبحاث في الحماية الاجتماعية، المجلد ٣، العدد ٠١، ٢٠٢٢، ص ٦٣.

(21) كيف استخدمت روسيا الهجمات الالكترونية في حربها ضد أوكرانيا، رابط الدخول: https://alqaheranews.net، تاريخ الاطلاع: ٢٠٢٤/٠١/٢٣، ساعة الاطلاع:٨:٣٠.

الروسية المهمة، وهو ما جعل هذه الحرب الفريدة من نوعها ولأول مرة تأخذ ساحتين للقتال ساحة الواقع وساحة الفضاء السيبراني، لأن الهجمات السيبرانية الحربية لها تأثير في الحرب الفعلية على الأرض، فتعطيل أو اختراق بيانات وزارات الدفاع لكلا الطرفين قد يغير شيئا من الحرب لمصلحة أحدهما[22].

المحور الثاني: طبيعة الهجمات السيبرانية الحربية وفق دليل تالين

نحن نعلم أن القانون الدولي الإنساني لا يتناول الهجمات السيبرانية الحربية بشكل خاص(فلقد بلورت قواعد القانون الدولي الإنساني في وقت لم تكن فيه الهجمات السيبرانية بشكل عام موجودة بعدُ)، والتي تقع خارج نطاق النزاعات المسلحة لإعتبار أن قواعد القانون الدولي الإنساني تتناول فقط النزعات ذات الطابع التقليدي، بالمقابل فإننا نجد أن الهجمات السيبرانية الحربية تتم عبر شبكة الحاسوب، لأنها هجمات تتميز بأنها بمثابة فتيل حرب حديثة مدعمة بالتكنولوجيا.

أولا: التعريف بدليل تالين

أعدت لجنة من الخبراء في حلف شمال الأطلسي الناتو دليلاً باسم **دليل تالين** صدر في عام ٢٠١٣ وخاص بالقوانين الدولية المطبقة في حالة نشوب حروب إلكترونية وتنظيم قواعد الاشتباك عبر الإنترنت، ويشير دليل تالين إلى أن القانون الدولي الإنساني ينطبق على الحرب الالكترونية (ولا يعني ذلك أن القانون الدولي الإنساني ينطبق على كافة العمليات الإلكترونية أو كل ما يطلق عليه "هجمات سيبرانية" في اللغة الشائعة، فالقانون الدولي الإنساني لا ينظم العمليات الإلكترونية التي تقع خارج سياق النزاع المسلح)، ويحدد الدور الذي ستلعبه قواعد القانون الدولي الإنساني في هذا المجال، كما يتميز هذا الدليل بأنه وثيقة غير ملزمة أعدتها لجنة الخبراء[23]، ويتبنى هذا الدليل مفهومين أساسين، يتعلق المفهوم الأول باستخدام وسائل وأساليب الحرب السيبرانية، أما المفهوم الثاني يتعلق بالعمل على مراجعة قانونية لتحديد الوصف التقني وطبيعة الأهداف والآثار على الأهداف والدقة ونطاق الآثار المقصودة في حالة استخدام الحرب الالكترونية[24].

يثير دليل تالين رؤىٍ مثيرة للاهتمام في هذا الصدد، فهو يتمسك على سبيل المثال بالثنائية التقليدية للنزاعات المسلحة الدولية والنزاعات المسلحة غير الدولية، ويقر بأن العمليات الإلكترونية وحدها قد تشكل نزاعات

(22) رابط الدخول: https://www.almayadeen.net/news/politics، تاريخ الدخول: ٢٠٢٣/٠١/١٠، ساعة الاطلاع: ١١:٠٠.

(23) إيهاب خليفة، القوة الالكترونية كيف يمكن أن تدير الدول شؤونها في عصر الانترنت "الولايات المتحدة الأمريكية نموذجا"، العربي للنشر والتوزيع، د ذ ب ن، ٢٠١٧، ص ١٦٦.

(24) عادل عبد الصادق، الفضاء الالكتروني والعلاقات الدولية(دراسة في النظرية والتطبيق)، المركز العربي لأبحاث الفضاء الالكتروني، د ذ ب ن، ٢٠١٦، ص ٥١٦.

مسلحة تبعاً للظروف، لا سيما الآثار المدمرة لتلك العمليات، 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 الإضرار بأعيان أو تدميرها، ويكمن صلب الموضوع مع ذلك في التفاصيل أي ما ينبغي أن يُفهم على أنه "ضرر" في العالم الالكتروني[25].

ثانيا: تحديد طبيعة الهجمات السيبرانية الحربية وسيرها كنزاع مسلح وفق دليل تالين

٠١- شروط معاصرة القواعد التقليدية لطبيعة الهجمات السيبرانية الحربية كنزاع مسلح

نص دليل تالين على أن العمليات السيبرانية التي تنفد في سياق نزاع مسلح تخضع لقانون النزاعات المسلحة[26]، كما اعتبر دليل تالين أن الهجمات الالكترونية وحدها قد تشكل نزاعات مسلحة تبعا للظروف، لا سيما الآثار المدمرة لتلك العمليات، حيث عرف دليل تالين الهجوم الالكتروني بموجب القانون الدولي الإنساني بوصفه عملية الكترونية سواء هجومية أو دفاعية، يتوقع أن تتسبب في إصابة آو قتل أشخاص أو الإضرار بأعيان أو تدميرها[27]، عليه وفق دليل تالين فالهجمات السيبرانية التي تتم في الفضاء السيبراني ذات الضرر المحدث والمؤثر تشكل في مضمونها **نزاعا مسلحا.**

كما أكد دليل تالين أنه من أجل استيفاء شرط حصول الضرر أن تصنف الهجمات على شبكات الحاسوب على أنها اشتراك مباشر في العمليات العدائية عندما ترقى إلى مفهوم الهجمات المباشرة الواردة في القانون الدولي الإنساني، بحيث تؤدي إلى الإصابة أو الموت أو إلحاق الضرر أو الدمار للأشخاص والأعيان المدنية من الهجمات المباشرة[28].

من المفارقات نجد أن قواعد القانون الدولي الإنساني لا تتناول ما يمكن أن نصطلح عليه بالبيانات الرقمية في الفضاء السيبراني وكيفية حمايتها في ظل النزاع المسلح، في حال تم إستهدافها بهجمات سيبرانية حربية، غير أننا نجد بالمقابل ردا إيضاحيا ضمن التقرير الذي أصدره فريق الخبراء الحكوميين عام ٢٠١٣ (دليل

---

(25) اللجنة الدولية للصليب الأحمر، ما هي القيود التي يفرضها دليل الحرب على الهجمات السيبرانية(الأسئلة الشائعة)، رابط الدخول:https://www.icrc.org ، تاريخ الاطلاع: ٢٠٢٤/٠٢/١١، ساعة الاطلاع: ٨:٢٢.

(٢٦) ، مرجع سابق. القاعدة ٢٠ من دليل تالين بشأن القانون الدولي المطبق على الحروب السيبرانية

(٢٧) إيهاب خليفة، المرجع السابق، ص ١٦٦.

(28) أزهر عبد الأمير الفتلاوي، العمليات العدائية طبقا لقواعد القانون الدولي الإنساني، المركز العربي للدراسات والبحوث العلمية، د ذ ب ن، ٢٠١٨، ص ١٧٧.

تالين) والمعتمد بتوافق الآراء والذي يؤكد أن استخدام الدول لتكنولوجيا المعلومات يخضع للقانون الدولي، أي ما نفهمه هنا أن الهجمات السيبرانية الحربية التي تتعمد إحدى الدول شنها ضد الدولة المعادية في سياق نزاع مسلح والمؤدية بالنتيجة إلى إحداث أضرار جسيمة متنوعة تتعدى مساحة الفضاء السيبراني فهي تخضع لقواعد القانون الدولي الإنساني وفق ما نص عليه دليل تالين.

ومن بين ميزات المطابقة والمقاربة والمسائل الثابتة بين قواعد القانون الدولي الإنساني ودليل تالين، هي أن حماية المدنيين والأعيان المدنية في سياق أي نزاع سواء كان مسلح تقليدي أو سيبراني من المسائل الثابتة الغير قابلة للتغيير أو التجاوز.

٠٢- التدابير المضادة والمشروطة للدولة المتعرضة لهجوم سيبراني حربي

في إطار السبل القانونية المتاحة لرد الدولة المتعرضة لهجوم سيبراني حربي دفاعا عن النفس، يعطي دليل تالين للدولة التي تتعرض لهجوم سيبراني حربي(فعل دولي غير مشروع) الحق في شن حرب هجومية الكترونية مضادة على الدولة الأخرى، كما أجاز الدليل أيضا إمكانية استخدام القوة العسكرية الحقيقية التقليدية في حال تم هجوم الكتروني على دولة ما، وأدى هذا الهجوم إلى الخسائر بالأرواح البشرية[29]، إذ يفيد هذا الترخيص الذي يبيحه دليل تالين كدفاع عن النفس ضد هجومات الكترونية بإمكانية مواجهتها باستخدام القوة التقليدية العسكرية التي تتجاوز الفضاء السيبراني، حيث نص ميثاق هيئة الأمم المتحدة في ما قبل على انه لا يوجد وفق مضمونه ما ينقص أو يضعف الحق الطبيعي للدول،بشكل فردي أو جماعي في الدفاع عن النفس في الحالة التي تتعرض فيها هذه الدول لإعتداء مسلح[30]، لكن مع عدم التمييع في استخدام القوة الدفاعية وتقييدها بالشروط التي تضمنتها قواعد العرف الدولي وهي (الضرورة، التناسب، الفورية)[31]، وهي الشروط التي أوردها دليل تالين ضمن القاعدتين ١٤ و١٥ منه، وفي سياق متصل أكد دليل تالين على إمكانية ممارسة حق الدفاع على النفس ضد هجوم سيبراني يصل إلى مستوى النزاع المسلح

(٢٩) عادل عبد الصادق، المرجع السابق، ص ٥١٦. -

(٣٠) المادة ٥١ من ميثاق الأمم المتحدة لعام ١٩٤٥.

(31) ولقد أكدت على هذه الشروط محكمة العدل الدولية في قرارها في قضية نيكاراغوا عام ١٩٨٦ ورأيها الاستشاري في قضية الأسلحة النووية عام ١٩٩٦، لمزيد من التفاصيل راجع: رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الالكترونية في ضوء قواعد القانون الدولي، مجلة جامعة الشارقة للعلوم القانونية، المجلد ١٥، العدد ٠٢، ٢٠١٨، ص ٣٤٢.

تتعرض له الدولة في إطار جماعي وبناء على طلب من الدولة الضحية[32]، فلقد صرح رئيس قسم الحرب الالكترونية الصينية(داي كوينجمن) عام ٢٠٠٣ بضرورة تهيأ الصين لحرب سيبرانية تتضمن سلسلة هجمات الكترونية، وهو ما يدعوها إلى الإعداد و التنسيق في العمليات العسكرية لصد الهجمات السيبرانية المضادة.
إلى جانب الشروط التي يجب على الدولة التي تعرضت لهجوم سيبراني مراعاتها في موقفها الدفاعي على النفس (الضرورة، التناسب، الفورية)، لابد لها من شرط التبليغ الفوري عن مجمل التدابير المتخذة من قبلها لمجلس الأمن الأممي[33].

فضلا عن هذا يحضر دليل تالين المساس ببعض **الأهداف المحصنة** في ظل تدابير الاقتصاص المضادة وهي(السكان المدنيين والأطراف المدنيين، الأعيان المدنية، الأعيان الثقافية وأماكن العبادة، الأماكن التي لا غنى عنها لبقاء السكان المدنيين، البيئة الطبيعية، السدود، الجسور ومحطات توليد الكهرباء النووية)[34]، إذ تشكل هذه الأهداف المحظورة إحدى الالتزامات المتعهد بها من قبل الدول الأطراف في البروتوكول الأول لإتفاقيات جنيف الأربعة لعام ١٩٤٩، إلى جانب هذا أيضا يحضر دليل تالين انتهاج سبل الهجمات السيبرانية العشوائية الغير موجهة نحو هدف مشروع، إذ من شانها إلحاق الأذى بالأهداف المحصنة من دون أي تمييز[35]، وهو ما استنكره البروتوكول الأول لعام ١٩٧٧ لاتفاقيات جنيف الأربعة ١٩٤٩ بعدم جواز استعمال وسائل وطرق قتال من شانها إن تؤدي إلى هجمات عشوائية وهذا في ظل المقاربة التقليدية، كما يفرض دليل تالين بعض الشروط والاحتياطات الواجب مراعاتها اتجاه الأهداف المحصنة من الهجوم السيبراني والمتمثلة في الرعاية المستمرة والتحقق من الأهداف، اختيار الوسائل والأساليب المستعملة.

إلى جانب المحظورات التي يفرضها دليل تالين والمتعلقة بالهجمات السيبرانية الحربية، ضرورة تجنب **الهجمات الذعريـة** التي يكون الغرض الأساسي منها بث الذعر بين السكان المدنيين[36].

---

(32) القاعدة ١٦ من دليل تالين بشأن القانون الدولي المطبق على الحروب السيبرانية لعام ٢٠١٣، مصدر سابق.
(33) المصدر نفسه، القاعدة ١٦.
(34) المصدر نفسه، القاعدة ٤٧.
(35) المصدر نفسه، القاعدة ٤٩.
(36) القاعدة ٣٦ من دليل تالين بشأن القانون الدولي المطبق على الحروب السيبرانية، مصدر سابق.

٠٣- المسؤولية الناشئة عن الهجمات السيبرانية الحربية

نحن نعلم أن مسؤولية الدول لا تثار إلا في حالة انتهاك هذه الأخيرة لقواعد وأحكام القانون الدولي، فإذا كانت المسؤولية بنوعيها(الدولية والجنائية) تثبت في حق الدول المنتهكة لأحكام القانون الدولي الإنساني في سياق نزاع مسلح تقليدي،فهي كذلك تثبت في حق هذه الدول في سياق هجوم سيبراني حربي، إذ تعد هذه الأخيرة من بين أهم التطورات الحديثة التي طرأت على العلاقات الدولية مؤخرا، فالدولة التي تقوم بفعل من شأنه إحداث ضرر أو تتسبب في إحداثه لدولة أخرى أو عدة دول في سياق نزاع مسلح، تتحمل تبعات المسؤولية الدولية على هذا الفعل غير المشروع دوليا.

أ- المسؤولية القانونية للدولة المعتدية سيبرانيا

تتحمل الدولة المعتدية سيبرانيا في نزاع مسلح المسؤولية القانونية الكاملة عن العمليات السيبرانية التي تنسب لها، والتي تشكل خرقا لالتزام دولي[37]، باعتبارأن الدول شخص من أشخاص القانون الدولي، حيث يفرض هذا الأخير على هذه الدول التزامات ويرتب لها حقوق،وعليه فالهجمات المثبته و الصادرة عن دولة اتجاه دولة أخرى في سياق نزاع مسلح مخلفة بذلك أضرارا تتعدى الهدف العسكري المشروع حسب ما أورده البروتوكول الإضافي الأول عام ١٩٩٧ والملحق باتفاقيات جنيف ١٩٤٩[38]، تضع هذه الدولة في قفص المسؤولية الدولية في حال توفر الشروط القانونية التالية:

- **صدور فعل غير مشروع دوليا:** المتمثل في توجيه هجمات سيبرانية حربية من طرف دولة ضد دولة أخرى معادية في سياق نزاع مسلح، مما يشكل انتهاكا ومخالفة لقواعد وأحكام القانون الدولي مولدا بذلك معه المسؤولية الدولية.

- **نسبة الفعل غير المشروع للدولة:** لكي تتحقق أركان المسؤولية الدولية لا بد من نسبة هذا الفعل إلى دولة ما، أي انتفاء جهل مصدر هذه الهجمات وفق ما بينته القاعدة ٤٦ من دليل تالين لعام ٢٠١٣، فلا يمكن تصور مسؤولية دولية بدون وجود فاعل حقيقي يتحمل تبعات فعله غير المشروع دوليا.

---

(37) المصدر نفسه، القاعدة ٦.

(38) فلقد نص البروتوكول الأول ضمن الفقرة الثانية من المادة ٥٢ على اقتصار الهجمات على الأهداف العسكرية فحسب، والتي تساهم مساهمة فعالة في العمل العسكري، وبالموازاة ينطبق هذا الأمر على مدلول الهجمات السيبرانية الحربية.

– **الضرر:** يعتبر عامل الضرر أهم عنصر من عناصر المسؤولية الدولية فبوجوده تتحقق هذه المسؤولية وبانتفائه تنعدم ولا يذكر لها وجود، وفي حالة الهجمات السيبرانية الحربية نجد أن الضرر يتحقق بمجرد توجيه تلك الهجمات المستهدفة للبنى التحتية للدولة المعادية مما قد يخلف أضرار بالغة وكبيرة.

ب– **المسؤولية القانونية الجنائية للقادة والرؤساء**

يقدم لنا دليل تالين ترخيصا بإمكانية محاسبة ومحاكمة القادة والرؤساء في ظل الهجمات السيبرانية الحربية، لأنهم يتحملون المسؤولية الجنائية الناتجة عن إصدارهم أوامر بالعمليات السيبرانية التي تشكل جرائم حرب، وفي الوقت نفسه يتحمل القادة هذه المسؤولية في حال علمهم بظروف ارتكاب هذه الهجمات التي تشكل جرائم حرب من طرف رؤسائهم، في حالة فشلهم في الحيلولة دون ارتكابها بموجب تدابير معقولة ومتاحة.

خـاتمة

أظهر الواقع تنوع الهجمات السيبرانية الحربية في النزاع المسلح، من خلال توظيف هذه الهجمات لأجل دعم المجهود الحربي الأرضي، وفي الإتجاه المعاكس نجد هناك العديد من المحاولات المستمرة لتطوير أساليب هذه الهجمات لتتوافق مع أي تحديثات أمنية يقوم بها خبراء الأمن السيبراني، فلقد ساهمت الهجمات السيبرانية الحربية بخصائصها في إفراز نوع مستحدث من الحروب الرقمية في العصر الحالي تشكل بطبيعتها تهديدا فعليا لأمن وسلامة الدول، لذلك يعد دليل تالين أول وثيقة ومحاولـة أعدتها مجموعـة من الخبراء تتناول في مضمونها التكييف القانوني لهذه الهجمات وكيفية سيرها في إطار نزاع مسلح تقليدي على الرغم من أن دليل تالين وثيقة غير ملزمة قانونيا غير أنه يبقى الوثيقة الوحيدة حاليا المستأنس بها في ظل هذه الهجمات، وعليه توصلنا **<u>للنتائج</u>** التالية:

– أدت التطورات التكنولوجية والمعلوماتية الحديثة إلى إفراز ثورة في مجال التسلح السيبراني في سياق النزاع المسلح بين الدول، الذي يعتمد بشكل كبير على الهجمات السيبرانية الحربية، مما يشير إلى زيادة الاعتماد على الفضاء السيبراني المعسكر وهو ما يؤدي معه في اغلب الأحيان إلى مواجهة عسكرية تقليدية في العالم الواقعي.

– تطرح الهجمات السيبرانية الحربية بإعتبارها وسيلة مستحدثة من وسائل القتال الجديدة وأساليبه تحديات قانونية وعملية، في ما يخص ضمان استخدامها على نحو يمتثل لقواعد القانون الدولي الإنساني القائمة وإيلاء الاعتبار الواجب للتداعيات الإنسانية المتوقعة جراء استخدامها.

المراجـع

المراجع العربية

أحمد عنتر، تقنيات الأمن السيبراني والتحديات المستقبليه، رابط الدخول: https://www.aljazeera.net/tech/2023/12/4.

البروتوكول الإضافي الأول لاتفاقية جنيف المتعلق بحماية ضحايا النزاعات المسلحة الدولية عام ١٩٧٧.

بوقرص ساعد، (٢٠٢٢)، "الأمن السيبراني مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتجيات خاصة"، مجلة الأبحاث في الحماية الاجتماعية، المجلد ٣، (العدد ٠١)، (٦٣).

بونيف سامي محمد، (٢٠١٩)، "دورالاستراتجيات الإستباقية في مواجهة الهجمات السيبرانية الردع السيبراني أنموذجا"، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد ٤، (العدد ٠٧)، (١٢٤).

خليفة إيهاب، (٢٠١٧)، القوة الالكترونية كيف يمكن أن تدير الدول شؤونها في عصر الانترنت"الولايات المتحدة الأمريكية نموذجا"، د ذ ب ن، العربي للنشر والتوزيع.

دليل تالين بشأن القانون الدولي المطبق على الحروب السيبرانية عام ٢٠١٣.

سمودي رزق أحمد، (٢٠١٨)، "حق الدفاع عن النفس نتيجة الهجمات الالكترونية في ضوء قواعد القانون الدولي العام"، مجلة جامعة الشارقة للعلوم القانونية، المجلد ١٥، (العدد ٠٢)، (١٦٦).

شلوش نورة، (٢٠١٨)، "القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول"، مجلة مركز بابل للدراسات الإنسانية، جامعة بابل، العراق، المجلد ٨، (العدد ٦)، (١٢٥).

عبد الصادق عادل، (٢٠١٦)، أسلحة الفضاء الالكتروني في ضوء القانون الدولي الإنساني، الإسكندرية، وحدة الدراسات المستقبلية.

عبد الصادق عادل، (٢٠١٦)، الفضاء الالكتروني والعلاقات الدولية"دراسة في النظرية والتطبيق، د ذ ب ن، المركز العربي لأبحاث الفضاء الالكتروني.

عبد الصادق عادل، أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي، مجلة السياسة الدولية، رابط الدخول: https://www.siyassa.org.eg.

عبد الصادق عادل، الهجمات السيبرانية– أنماط وتحديات جديدة للأمن العالمي–، المركز العربي لأبحاث الفضاء الالكتروني، رابط الدخول: https://accronline.com/article.

عبيس أحمد، الفتلاوي نعمة، (٢٠١٦)، "الهجمات السيبرانية"مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل (كلية القانون)، المجلد ٨، (العدد ٤)، (٦١٣).

الفتلاوي أزهر عبد الأمير، (٢٠١٨)، العمليات العدائية طبقا لقواعد القانون الدولي الإنساني، المركز العربي للدراسات والبحوث العلمية.

كاوجة محمد الصغير، (٢٠٢٢)، "الهجمات السيبرانية بين الواقع وسبل المواجهة"، مجلة الرسالة للدراسات الإعلامية، المجلد ٠٦، (العدد ٠٣)، (١١٦).

كيف استخدمت روسيا الهجمات الالكترونية في حربها ضد أوكرانيا، رابط الدخول: https://alqaheranews.net .

اللجنة الدولية للصليب الأحمر، ما هي القيود التي يفرضها دليل الحرب على الهجمات السيبرانية(الأسئلة الشائعة)، رابط الدخول: https://www.icrc.org

محمود عرفان وسام، (٢٠٢٤)، سبل مكافحة الهجمات السيبرانية دوليا، مجلة الدراسات القانونية والإقتصاديه، المجلد ١٠، (العدد ٠٣)، (٢٩٩١).

بن مرزوق عنترة، حرشاوي محي الدين، (٢٠١٧)"الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية"، مجلة دفاتر السيادة والقانون، جامعة قاصدي مرباح، ورقلة، (العدد ١٧)، (٦٦).

منزر رابح، درويش سعيد، (٢٠٢١)، "الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول"، مجلة صوت القانون، جامعة الجيلالي بونعامة، خميس مليانة، المجلد 8، (العدد ٠١)، (٥٣٩).

ميثاق الأمم المتحدة لعام ١٩٤٥. https://www.almayadeen.net/news/politics

المراجع الأجنبية

Junaidu Bello Marshall,Cyber attacks:the legal response, International journal of international law, Vol 01, universal multidisciplinary research institute,India, (No 02).

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

المراجع العربية بالحروف اللاتينية

Aḥmad ʻAntar, Tiqniyāt al-amn alsybrāny wa-al-taḥaddiyāt almstqblyh, rābṭ alwlwj: https://www.aljazeera.net/tech/2023/12/4.

Albrwtwkwl al-iḍāfī al-Awwal lātfāqyh Jinīf al-mutaʻalliq bi-ḥimāyat Ḍaḥāyā al-nizāʻāt al-musallaḥah al-Dawlīyah ʻām 1977.

Bwqrṣ Sāʻid, (2022), "al-amn alsybrāny Makhāṭir wa-tahdīdāt wa-taḥaddiyāt tṭṭlb mumārasāt wa-tawṣiyāt wāstrātjyāt khāṣṣah", Majallat al-Abḥāth fī al-Ḥimāyah al-ijtimāʻīyah, al-mujallad 3, (al-ʻadad 01), (63).

Būnīf Sāmī Muḥammad, (2019), "dwrālāstrātjyāt al’stbāqyh fī muwājahat alhjmāt alsybrānyh al-radʻ alsybrāny anmūdhajan", al-Majallah al-Jazā’irīyah lil-Ḥuqūq wa-al-ʻUlūm al-siyāsīyah, al-mujallad 4, (al-ʻadad 07), (124).

Khalīfah Īhāb, (2017), al-qūwah al-iliktrūnīyah Kayfa yumkinu an tdyr al-Duwal shu’ūnahsa fī ʻaṣr al-Intarnit "al-Wilāyāt al-Muttaḥidah al-Amrīkīyah namūdhajan", D Dh b N, al-ʻArabī lil-Nashr wa-al-Tawzīʻ.

Dalīl tālyn bi-sha’n al-qānūn al-dawlī al-muṭabbaq ʻalá al-ḥurūb alsybrānyh ʻām 2013.

Smwdy Rizq Aḥmad, (2018), "Ḥaqq al-Difāʻ ʻan al-nafs Natījat alhjmāt al-iliktrūnīyah fī ḍaw’ Qawāʻid al-qānūn al-dawlī al-ʻāmm", Majallat Jāmiʻat al-Shāriqah lil-ʻUlūm al-qānūnīyah, al-mujallad 15, (al-ʻadad 02), (166).

Shlwsh Nūrah, (2018), "al-Qarṣanah al-iliktrūnīyah fī al-faḍā’ alsybrāny" al-tahdīd almṭṣāʻd li-amn al-Duwal ", Majallat Markaz Bābil lil-Dirāsāt al-Insānīyah, Jāmiʻat Bābil, al-ʻIrāq, al-mujallad 8, (al-ʻadad 6), (125).

ʻAbd al-Ṣādiq ʻĀdil, (2016), asliḥat al-faḍā’ al-iliktrūnī fī ḍaw’ al-qānūn al-dawlī al-insānī, al-Iskandarīyah, Waḥdat al-Dirāsāt al-mustaqbalīyah.

ʻAbd al-Ṣādiq ʻĀdil, (2016), al-faḍā’ al-iliktrūnī wa-al-ʻalāqāt al-Dawlīyah "dirāsah fī al-naẓarīyah wa-al-taṭbīq, D Dh b N, al-Markaz al-ʻArabī li-Abḥāth al-faḍā’ al-iliktrūnī.

‘Abd al-Ṣādiq ‘Ādil, Anmāṭ al-ḥarb alsybrānyh wa tdā‘yāthā ‘alá al-amn al-‘Ālamī, Majallat al-siyāsah al-Dawlīyah, rābṭ alwlwj: https://www.siyassa.org.eg.

‘Abd al-Ṣādiq ‘Ādil, alhjmāt alsybrānyt-Anmāṭ wa-taḥaddiyāt jadīdah lil-amn al‘ālmy-, al-Markaz al-‘Arabī li-Abḥāth al-faḍā’ al-iliktrūnī, rābṭ alwlwj: https://accronline.com/article.

‘Bys Aḥmad, al-Fatlāwī Ni‘mah, (2016), "alhjmāt alsybrānyh" mafhūmuhā wa al-Mas’ūlīyah al-Dawlīyah al-nāshi’ah ‘anhā fī ḍaw’ al-tanẓīm al-dawlī al-mu‘āṣir ", Majallat al-muḥaqqiq al-Ḥillī lil-‘Ulūm al-qānūnīyah wa-al-siyāsīyah, Jāmi‘at Bābil (Kullīyat al-qānūn), al-mujallad 8, (al-‘adad 4), (613).

al-Fatlāwī Azhar ‘Abd al-Amīr, (2018), al-‘amalīyāt al-‘adā’īyah ṭibqan li-qawā‘id al-qānūn al-dawlī al-insānī, al-Markaz al-‘Arabī lil-Dirāsāt wa-al-Buḥūth al-‘Ilmīyah.

Kāwjh Muḥammad al-Ṣaghīr, (2022), "alhjmāt alsybrānyh bayna al-wāqi‘ wa-subul al-muwājahah", Majallat al-Risālah lil-Dirāsāt al-I‘lāmīyah, al-mujallad 06, (al-‘adad 03), (116).

Kayfa astkhdmt Rūsiyā alhjmāt al-iliktrūnīyah fī ḥrbhā ḍidda awkrānyā, rābṭ alwlwj: https://alqaheranews.net.

al-Lajnah al-Dawlīyah lil-Ṣalīb al-Aḥmar, mā hiya al-quyūd allatī yfrḍhā Dalīl al-ḥarb ‘alá alhjmāt alsybrānyh (al-as’ilah al-shā’i‘ah), rābṭ alwlwj: https://.www.icrc.org.

Maḥmūd ‘Irfān Wisām, (2024), Subul Mukāfaḥat alhjmāt alsybrānyh dawlīyan, Majallat al-Dirāsāt al-qānūnīyah wāl’qtṣādyh, al-mujallad 10, (al-‘adad 03), (2991).

Ibn Marzūq ‘Antarah, ḥrshāwy Muḥyī al-Dīn, (2017) "al-amn alsybrāny kb‘d jadīd fī al-siyāsah al-difā‘īyah al-Jazā’irīyah", Majallat Dafātir al-siyādah wa-al-qānūn, Jāmi‘at qāṣdy mrbāḥ, Warqalah, (al‘dd17), (66).

Mnzr Rābiḥ, Darwīsh Sa‘īd, (2021), "al-ṭabī‘ah al-qānūnīyah llhjmāt alsybrānyh allatī taqa‘u bayna al-Duwal", Majallat Ṣawt al-qānūn, Jāmi‘at al-Jīlālī bwn‘āmh, Khamīs mlyānh, al-mujallad 8, (al-‘adad 01), (539).

Mīthāq al-Umam al-Muttaḥidah li-‘ām 1945. https://www.almayadeen.net/news/politics

مجلة جامعة الملك عبدالعزيز: الآداب والعلوم الإنسانية، م ٣٣ ع ١ ص ص: ٤٣٩ – ٤٥٧ (٢٠٢٥م)
DOI: 10.4197/Art.33-1 - 16

Cyber Warfare attacks as a Catalyst for Emerging wars in the Context of Armed conflict according to the Tallinne Manual

Rawiya Boulanoair

Department of LAW, Faculty of LAW, University of Brothers Montori Constantine 1., Constantine, Algeria

rawiya.boulanouar@doc.umc.edu.dz

Abstract

The current paper examines and analyses the topic of cyber warfare attacks which is considered as one of the most significant challenges that faces humanity in the era of the Fourth Industrial Revolution. Through a descriptive comparative analysis, this study aims to provide an in-depth analysis of the cyber warfare attacks using Tallinn Manual, and how they contributed to radical changes in the structure of the classical warfare over transforming it into a modern war supported by the use of soft electronic power as weapons such as viruses spyware, and hacking of military and strategic information. We concluded that that the effect of war cyberattacks is different from the conventional weapons in armed conflict.

Keywords: Cyber warfare attacks, Digital threat, Global security, Modernized warfare, Tallinn.

IN THE NAME OF ALLAH,
THE MERCIFUL,
THE MERCY-GIVING

JKAU/ Arts and Humanities, Vol. **33** No. **1**, 565 Pages (2025)
ISSN: 1319-0989
Legal Deposit 14/0294

Journal of
KING ABDULAZIZ UNIVERSITY
Arts and Humanities

Volume 33 Number 1
2025

Scientific Publishing Center
King Abdulaziz University
P.O. Box 80200, Jeddah 21589
http://spc.kau.edu.sa

Editorial Board

JKAU/ Arts and Humanities, Vol. **33** No. **1**, 565 Pages (2025)
ISSN: 1319-0989
Legal Deposit 14/0294

Contents

English Articles

Arabic Articles - English Abstracts