★★★★★★★★★★★

العدالة الجنائية الدولية وسؤال الفعالية

La justice pénale internationale et la question de l'efficacité

★★★★★★★★★★★

المدير المسؤول:

✍ د. حكيم التوزاني (أستاذ القانون الدولي العام والعلوم السياسية)

رئيس التحرير:

✍ د. عبد الحميد اليعقوبي (أستاذ القانون الخاص)

★★★★★★★★★★★

تنسيق العدد:

✍ د. حكيم التوزاني (أستاذ القانون الدولي العام والعلوم السياسية)

✍ د. محمد بن التاجر (أستاذ القانون الخاص)

★★★★★★★★★★★

العدد الأول: 2024

تخلي هيئة تحرير والنشر مسؤوليتها عن أي انتهاك لحقوق الملكية الفكرية
لا تعبر الآراء الواردة في هذا المؤلف بالضرورة عن رأي إدارة التحرير والنشر
لا يسمح بإعادة إصدار هذا الكتاب أو أي جزء منه أو تخزينه في نطاق استعادة المعلومات أو نقله بأي شكل من الأشكال دون إذن خطي مسبق من الناشر
جميع الحقوق محفوظة للمجلة الدولية لتدبير الأزمات وتسوية النزاعات©

معلومات عن المجلة الدولية لتدبير الأزمات وتسوية النزاعات

✍ المجلة الدولية لتدبير الأزمات وتسوية النزاعات

✍ مدير المجلة: د. حكيم غزواني

(أستاذ القانون الدولي العام والعلوم السياسية- جامعة ابن زهر بأكادير- المملكة المغربية الشريفة)

✍ رئيس التحرير: د. عبد الحميد البعقوبي

(أستاذ القانون الخاص- جامعة ابن زهر بأكادير- المملكة المغربية الشريفة)

✍ تنسيق العدد: د. حكيم غزواني / د. محمد بن الناجر

✍ العدد الأول: 2024

✍ الحقوق: © جميع الحقوق محفوظة للمجلة الدولية لتدبير الأزمات وتسوية النزاعات

✍ الإيداع القانوني:(2024PE0029 (dépôt légal

✍ International Standard Serial Number:3009-5530 (ISSN)

✍ ملف الصحافة رقم: 2024/106 ص.

✍ البريد الالكتروني:rigcrc@gmail.com

✍ موقع المجلة الالكتروني: www.rigcrc.com

✍ رقم هاتف المدير المسؤول: 677977793 212+

✍ مطبعة:SO-ME-PRINT/ أكادير-المغرب

✍ الهاتف / الفاكس: 05.28.22.79.88

✍ المحمول: 06.74.80.68.58

✍ العنوان: قرب كلية العلوم، حي الداخلة، أكادير، المملكة المغربية

✍ الناشر: مركز الدراسات والأبحاث القانونية والقضائية والاجتماعية

(المضيق- المملكة المغربية)

اللجنة العلمية:

أساتذة القانون الدولي العام، والعلاقات الدولية، والقانون الدستوري والعلوم السياسية والإدارية والاقتصادية

ت	الاسم	المؤسسة	ت	الاسم	المؤسسة
1	د. رحيم الطوم	(جامعة ابن زهر بأكادير)	21	د. زكرياء أقنوش	(جامعة المولى اسماعيل بمكناس)
2	د. عبد القادر لشقر	(جامعة سيدي محمد بن عبد الله بفاس)	22	د. إبراهيم الزيتوني	(جامعة ابن زهر بأكادير)
3	د. فؤاد أعلوان	(جامعة سيدي محمد بن عبد الله بفاس)	23	د. عبد الهادي الحرفاوي	(جامعة ابن زهر بأكادير)
4	د. محمد الكيحل	(جامعة محمد الخامس الرباط)	24	د. بدر زاهر الأزرق	(جامعة الحسن الثاني بالدار البيضاء)
5	د. أحمد بودراع	(جامعة محمد الخامس الرباط)	25	د. وديع الهامل	(جامعة سيدي محمد بن عبد الله بفاس)
6	د. محمد المكليف	(جامعة محمد الخامس الرباط)	26	دة. زهرة الهياض	(جامعة محمد الخامس الرباط)
7	د. رضا فلاح	(جامعة ابن زهر بأكادير)	27	د. عبد العزيز دحماني	(جامعة محمد الخامس الرباط)
8	د. المصطفى منار	(جامعة محمد الخامس الرباط)	28	د. حسن رحيمي	(جامعة ابن زهر بأكادير)
9	د. محمد بنطلحة الدكالي	(جامعة القاضي عياض بمراكش)	29	د. محمد بن التاجر	(جامعة ابن زهر بأكادير)
10	د. نور الدين السوسي	(جامعة ابن زهر بأكادير)	30	د. عبد الرحيم خالص	(جامعة ابن زهر بأكادير)
11	د. الحسين شكراني	(جامعة القاضي عياض بمراكش)	31	د. أبو بكر شنيبة	(جامعة ابن زهر بأكادير)
12	د. جمال كدوري	(جامعة سيدي محمد بن عبد الله بفاس)	32	د. عبد المولى موسعيد	(جامعة الحسن الثاني بالدار البيضاء)
13	دة. وفاء الفيلالي	(جامعة محمد الخامس الرباط)	33	دة. نادية جامع	(جامعة ابن طفيل بالقنيطرة)
14	د. محمد همام	(جامعة ابن زهر بأكادير)	34	د. محمد الغواطي	(جامعة محمد الخامس الرباط)
15	د. حكيم التوزاني	(جامعة ابن زهر بأكادير)	35	د. الحسن تراوري	مدرسة العليا سبيل النور
16	د. عبد الكريم الحبيكي	(جامعة ابن زهر بأكادير)	36	دة. إكرام عدناني	(جامعة ابن زهر بأكادير)
17	د. عبد الحكيم أبو اللوز	(جامعة ابن زهر بأكادير)	37	د. رشيد كديرة	(جامعة ابن زهر بأكادير)
18	د. جواد الرباع	(جامعة ابن زهر بأكادير)	38	د. خالد يايموت	(جامعة سيدي محمد بن عبد الله بفاس)
19	د. يوسف عنتار	(جامعة محمد الأول بوجدة)	39	د. عبد المجيد بوكير	(جامعة سيدي محمد بن عبد الله بفاس)
20	د. محمد بويوتش	(جامعة محمد الأول بوجدة)	40	د. عبد الحميد اليعقوبي	(جامعة ابن زهر بأكادير)

✍ هيئة التحرير:

ر.ث	الاسم		الصفة
1)	د. حكيم الثوزاني	:	باحث في القانون العام والعلوم السياسية
2)	د. عبد الحميد البعقوبي	:	رئيس مركز الدراسات والأبحاث القانونية والقضائية والاجتماعية
3)	د. محمد بن الناجر	:	أستاذ القانون الخاص بجامعة ابن زهر بأكادير
4)	د. منير أوخليفا	:	عضو مركز الدراسات والأبحاث القانونية والقضائية والاجتماعية
5)	د. عبد الهادي الحرفاوي	:	أستاذ القانون الخاص بجامعة ابن زهر بأكادير
6)	د. أبو بكر شيبة	:	عضو مركز الدراسات والأبحاث القانونية والقضائية والاجتماعية

التعريف بالمجلة

"المجلة الدولية لتدبير الأزمات وتسوية النزاعات" : مجلة محكّمة نصف سنوية ذات الولوج المفتوح، متخصصة دولية ومرخصة تصدر عن مركز الدراسات والأبحاث القانونية والقضائية والاجتماعية. وتهتم المجلة بنشر الأبحاث القانونية والسياسية والفقهية والقضائية والاجتماعية الأصيلة والقيمة التي تتوافر فيها مقومات البحث العلمي من حيث توافر عنصر الأصالة والإبداع، ووضوح الهدف والمنهج، ودقة التوثيق، التي من شأنها أن تعطي اقتراحات لتخفيف الصراعات وتسوية النزاعات وإدارة الأزمات العابرة للحدود.

تهدف المجلة إلى نشر المعرفة والوعي في القضايا القانونية والسياسية والفقهية والقضائية والاجتماعية الدولية بشتى فروعها وتخصصاتها المتنوعة عربيا ودوليا. وهي مجلة مستقلة عن التيارات الدينية والحزبية والسياسية ولا تهدف إلى تحقيق الربح. تصدر بصيغتيها الالكترونية والورقية.

الأهداف والنطاق

تتطلع المجلة الدولية لتدبير الأزمات وتسوية النزاعات إلى تحقيق معايير النشر العلمي وتحقيق الذيوع والانتشار. تهدف هذه المجلة لأن تكون مجلة متميزة ورائدة تخدمة كل من يهتم بالعلوم القانونية والاجتماعية والاقتصادية من باحثين أو قانونيين أو اعضاء الهيئات التدريسية؛ بتقديم كل ما هو جديد ورائد في هذه المجالات. كما تهدف المجلة بأن تكون بوابة قانونية في متناول كل باحث قانوني بدون قيد أو شرط؛ ذلك أنها مجلة قانونية متاحة للجميع للاطلاع والمشاركة الفكرية بكل أنواعها حيث أنها تتبع سياسة الوصول الحر المفتوح.

كما وتهدف المجلة لأن تكون متميزة بالمادة العلمية التي تقدمها ملتزمين أن تكون جميع الأبحاث العلمية والتقارير البحثية أو تقارير المؤتمرات والندوات المنشورة فيها تتسم بالأصالة والعمق والحداثة واتباع القواعد العلمية الدقيقة للبحث العلمي والتزام اخلاقيات البحث.

الرسالة

تسعى المجلة لتحقيق ما يلي:

- لا تهدف إلى الربح، وإنما لنشر المعرفة وتقاسم الخبرات الأكاديمية.
- تشجيع نشر الأعمال العلمية بجميع صورها : الأبحاث والدراسات والكتب والرسائل والأطروحات الجامعية. وأشغال المؤتمرات والندوات ...
- تشجيع البحث القانوني والمساهمة الجادة في إثراء الفكر القانوني من خلال نشر القواعد القانونية والآراء الفقهية والاجتهادات القضائية.
- الانفتاح على المجالات البينية والاستراتيجية.
- تهدف إلى نشر البحوث العلمية الأصلية باللغات العربية والإنجليزية والفرنسية والإسبانية.
- إبراز جهود الباحثين من خلال نشر الإنتاج العلمي الخاص في مجال القانون والعلاقات الدولية وحقوق الإنسان. وعلم الاجتماع والاقتصاد.
- توثيق الروابط الفكرية ونشر الثقافة العلمية بين الباحثين لتحقيق التواصل العلمي المستمر.
- الارتقاء بمستوى البحث العلمي بالمؤسسات الأكاديمية ومراكز البحث المختلفة وتطويره باستخدام الأساليب والوسائل العلمية.
- العمل على حفظ حقوق الملكية الفكرية لنتاج الباحثين في مجالات أشتغال المجلة.

أخلاقيات النشر

تتبنى **المجلة الدولية لتدبير الأزمات وتسوية النزاعات** المعايير الدولية الخاصة بالمؤلفين الصادرة عن لجنة أخلاقيات النشر ***COPE*** فيما يتعلق بتصميم وإدارة عملية تحكيم ونشر المجلة والتعامل مع القضايا الأخرى ذات الصلة.

مسؤولية الباحث:

- الالتزام بمبادئ ومعايير أخلاقيات البحث والنشر.
- تقديم أبحاث أصلية خالصة وتوفير قائمة بالمراجع التي تمّ الرُّجوع إليها في البحث.
- الالتزام بكتابة البحث وفقًا لقواعد المجلة الدولية لتدبير الأزمات وتسوية النزاعات.
- عدم تقديم عمل نُشِر مسبقًا في مجلّات أخرى. إلا في حالة إجراء تعديلات جوهرية داخل البحث أو في العنوان، كما يجب عليه عدم تقديم عمله إلى أكثر من مجلّةٍ في وقتٍ واحدٍ؛ إذ يُعدُّ ذلك منافيًا لأخلاقيّات النّشر العالمية.
- يمكن نشرُ بحثه في المجلّات الأخرى بعد تلقّي الرّفض الرّسميّ منَ المجلّة أو في حال موافقة المجلّة رسميًّا على طلب سَحْبِ البحث المقدّم.
- أن يذكر إسهام الآخرين في البحث بشكل صحيح وترتيب أسماء الباحثين حسب ما جاء بالبحث على أن تكون الأسماء مذكورة بالتسلسل حسب الإسهام العلمي لكلّ منهم في البحث.
- الالتزام بقواعد الاقتباس والتوثيق وأخلاقيّات النّشر.
- ضمان أصالة أبحاثه واستيفائها للمعايير المِهْنيّة لأخلاقيات البحث.
- الابتعاد عن جميع أنواع السلوك غير الأخلاقي مثل الانتحال والافتعال والتزوير.
- إذا اكتشف خطأً فادحًا في بحثه المنشور يجب عليه إبلاغ هيئة التحرير بالمجلة بحذف الخطأ أو تصويبه.
- مراجعة بحثه وفقًا لمقترحات المحكمين، وفي حال عدم موافقة الباحث على الأخذ بالتعديلات المقترحة؛ يجب عليه تقديم تبريرٍ منطقيٍّ بذلك، وفي حالة عدم تقديم أسباب مقنعة تحتفظ المجلة بالحق في رفض النشر.

مسؤولية المحكم:

تُعدُّ عمليّة تحكيم الأبحاث العلمية مرحلةً أساسية من مراحل النّشر العلميّ، لذا يجب على المحكم:

- الالتزام بمعايير لجنة أخلاقيات النشر العالمية للمحكمين عند تحكيم البحوث.
- إعلام مدير التحرير حال عدم استعداده لتحكيم البحث المقدم وينسحب من عملية التحكيم.
- النّأيُ بنفسه عنِ المصالح الشّخصيّة؛ كأن يستخدم معلومات حصل عليها من البحث الذي تم تحكيمه لمصلحته الشخصية.
- ألا يقبل المحكم بتحكيم البحوث التي يكون فيها تضارب مصالح نتيجة لعلاقات تنافسية أو غيرها مع المؤلف.
- التأكد من خُلوّ الأبحاث منَ الانتحال أوِ السّرقة الأدبيّة كما يجب على المحكم أن يعلم رئيس التحرير بأي تشابه بين البحث الذي تم تحكيمه وأي أعمال أخرى منشورة يعرفها .
- الالتزام بمعايير السريّة المتعلقة بعملية التحكيم فيجب عليه معاملة الأبحاث التي تسلمها للتحكيم كوثائق سرية. ويجب عليه عدم الكشف عنها أو مناقشتها مع الآخرين باستثناء ما يأذن به مدير المجلة أورئيس التحرير.
- تحرّي الموضوعيّة في الأحكام والنّتائج الصّادرة عن عمليّة التّحكيم.
- التعبير عن رأيه بنزاهة ووضوح مع ذكر الحجج الداعمة.
- الالتزام بالوقت المخصّص لعمليّة التّحكيم.

وعليه، يتم تحليل وتقييم الأوراق العلمية على اعتبار كل حالة على حدة مع مراعاة مناسبة وجودة وأصالة الورقة المقدمة. وبشكل عام، يمكن تقييم ما يلي في عملية التحكيم:

- بنية الورقة العلمية المقدمة ومدى ملاءمتها لإرشادات النشر.
- الغرض والهدف من الورقة العلمية.
- طريقة استخدام الانتقالات بين الفقرات في الورقة العلمية.
- المقدمة والخاتمة.
- المراجع المقدمة لدعم المحتوى.
- القواعد النحوية وعلامات الترقيم والإملاء.

- السرقة الأدبية.
- ملاءمة الورقة العلمية لحاجة المجتمع العلمي.
- يقرر المحكمون قبول أو رفض ورقة علمية، ويُعتبرون عنصرا رئيسيا في عملية تحكيم الأقران. ويُطلب من جميع المحكمين لدى المجلة تحكيم الأوراق المرسلة إليهم بشكل مفصل وإبداء تعليقاتهم بحيادية، وهو ما من شأنه أن يرفع من جودة المجلة.

- مسئولية هيئة التحرير

- يتولّى مدير تحرير المجلة بالتعاون مع هيئة التحرير مسئولية اختيار المحكّمين المناسبين وَفْقا لموضوع البحث واختصاص المحكّم بسرّية تامة.
- يتحمل مدير التحرير مسؤولية التصرف النهائي في جميع عمليات التقديم للنشر.
- يستند قرار النشر أو عدم النشر على تقارير المحكّمين وملاحظاتهم والقيمة العلمية للبحث وأصالته وصلته بمجال تخصص المجلة.

ويجب على المحررين:

- التأكد من الحفاظ على سرّية عمليّة التّحكيم والمعلومات الواردة من المحكمين.
- التأكد من أن الأبحاث المقدمة للتحكيم تتفق مع أخلاقيات النشر العلمي ومبادئه.
- عدم التمييز ضد المؤلفين على أساس الجنس، الأصل، الاعتقاد الديني، المواطنة أو الانتماء السياسي للمؤلف.
- معالجة شكاوى المؤلفين والاحتفاظ بأية مستندات ذات صلة بالشكاوى.
- التأكد من مراجعة الأبحاث بطريقة سرية.

قرار و حقوق النشر

-تؤول حقوق النشر للمجلة.

-البحوث المنشورة لا تمثل رأي المجلة، بل تمثل رأي الباحث نفسه، ولا تتحمل إدارة المجلة أي مسؤولية قانونية ترد على هذه البحوث.

-المجلة لها القرار في نشر المقال أو عدم نشره مع التعليل لصاحب المقال.

فهرس المحتويات

فهرس المحتويات 1

المسؤولية الجنائية الدولية لمرتكبي المخالفات عن الحرب السيبرانية 3

دة. زهرة الهياض

موقع العدالة الجنائية الدولية في المنهج التكاملي لتسوية النزاعات المسلحة الداخلية 46

د. خالد الوردي

تكريس مبدأ استقلال القضاء الدولي الجنائي في ظل نظام روما الأساسي 115

دة. عائشة عبد الحميد

تأثير تمويل المحكمة الجنائية الدولية على فعالية العدالة الجنائية الدولية 129

هشام الميموني

أزمة العدالة الجنائية الدولية: دراسة قانونية وسياسية 153

د. محمد حومالك

فعالية المحكمة الجنائية الدولية في حماية حقوق الضحايا بعد ربع قرن من اعتماد نظام روما الأساسي 182

دة. مريم أكري

مسار العدالة في تحقيقات المحكمة الجنائية الدولية في شأن الجرائم الإسرائيلية في فلسطين 221

د. هشام بولنوار

القضاء الجنائي الدولي وحماية الأقليات: أية فاعلية؟ 256

د. فؤاد أعلوان

د. عبد الحكيم أشفاي

قراءة استقصائية لمدى فاعلية العدالة الدولية في ظل الواقع الدولي المعاصر 278

د. هاشم علوي عبدالله مقيبل

✍ **علاقة مجلس الأمن الدولي بالمحكمة الجنائية الدولية: مقاربة على ضوء مفهوم "الفوضى" في نظريات العلاقات الدولية** **303**

د. حمدي أتراس

✍ **علاقة مجلس الأمن بالمحكمة الجنائية الدولية من خلال آليات تحريك الدعوى ضد الجرائم الدولية بين جدلية الاستقلالية والتبعية** **332**

د. المصطفى بوكرين

✍ **إشكالية تنفيذ أوامر القبض الصادرة عن المحكمة الجنائية الدولية** **365**

سمير الشمالي (تحت إشراف الأستاذة زهرة الهياض)

✍ *LA COOPERATION ENTRE LES ÉTATS MEMBRES COMME FACTEUR CLE POUR L'EFFICACITE DE LA JUSTICE PENALE INTERNATIONALE* *387*

KHADIJA BENCHHIBA

JAMAL MOHAMMED

د. زهرة الهياض، "المسؤولية الجنائية الدولية لمرتكبي المخالفات عن الحرب السيبرانية"،
المجلة الدولية لتدبير الأزمات وتسوية النزاعات، المملكة المغربية، العدد الأول، 2024، (ص.3 ← ص.45)

المسؤولية الجنائية الدولية لمرتكبي المخالفات عن الحرب السيبرانية

د.ة. زهرة الهياض

أستاذة القانون الدولي العام والعلاقات الدولية / جامعة محمد الخامس بالرباط (المملكة المغربية)

الملخص:

أصبح الهجوم السيبراني اليوم جزءا لا يتجزأ من حروب العصر الراهن التي تدور رحاها في ساحة "هجينية" يتداخل فيها العالم المادي مع العالم الافتراضي ناهيك عن ما تخلفه م تكلفة مادية وبشرية لا يستهان بها. واذا كان من المسلم به ان الفضاء السيبراني ليس خلوا من أي قانون، وان الأسلحة الجديدة يجب أن تكون قادرة على أن تُستخدم وفقاً لقواعد القانون الدولي الإنساني بمعناه الواسع، الا ان صعوبات تنشأ بخصوص تفسير وتطبيق هذه القواعد على التكنولوجيات الجديدة للحرب لاسيما وان الممارسة اثبتت بان الدول تلجأ الى هذه الهجمات بمعزل عن النزاع المسلح باستثناء ما افرزته في السنتين الأخيرتين الحرب الروسية –الأوكرانية. هي صعوبات تخلق الشك في خضوع الحرب السيبرانية لقواعد القانون الدولي الإنساني وبالتالي تعذر إمكانية محاسبة الجهات التي تخطط أو تنفذ الهجمات الالكترونية بعد التمكن من تحديد هويتها.

كلمات مفتاحية: الحرب السيبرانية، الهجوم السيبراني، القانون الدولي الإنساني، دليل تالين، المسؤولية الجنائية الدولية

Résumé:

Aujourd'hui, les cyberattaques font désormais partie intégrante des guerres d'aujourd'hui qui se déroulent dans une arène « hybride » où le monde physique se superpose au monde virtuel, sans parler du coût matériel et humain important. S'il est reconnu que le cyberespace n'est pas anarchique et que les nouvelles armes doivent pouvoir être utilisées conformément aux règles du droit international humanitaire au sens large, néanmoins des difficultés se posent quant à l'interprétation et à l'application de ces règles aux nouvelles technologies de guerre, d'autant plus que la pratique a montré que les États ont recours à ces attaques indépendamment du conflit armé, à l'exception de ce qui a émergé surtout ces deux dernières années de la guerre russo-ukrainienne. Ces difficultés font douter que la cyberguerre soit soumise aux règles du droit international humanitaire et qu'il soit donc impossible de demander des comptes à ceux qui planifient ou mènent des cyberattaques.

مقدمة

أدى ظهور الانترنيت منذ ستينيات القرن الماضي الى الترابط الشديد بين دول العالم من خلال بنية أساسية لتبادل أيسر واقل تكلفة للمعلومات والبيانات المتعلقة بكل نواحي الحياة الإنسانية بشكل يتخطى الحدود المادية التقليدية للدولة. إن الدوافع الأكثر شيوعا وراء العمليات السيبرانية الإجرامية كالهجمات هي سرقة الأسرار التجارية وتفاصيل بطاقات الائتمان والهويات والملكية الفكرية. في بعض الحالات، يؤدي التجسس السيبراني إلى زعزعة استقرار الدبلوماسية ويؤثر على سيادة الدولة. تخلق من العمليات تحديات جديدة للمهنيين في مجال تكنولوجيا المعلومات وأمن البيانات على مستوى العالم وكذلك لأولئك الذين يستخدمون هذه المعلومات، بما في ذلك السكان المدنيون والحكومات والعسكريون. انه الوجه الآخر أو بالأحرى الخبيث للتكنولوجيا الحديثة. فعلى الرغم من الفوائد التي تقدمها التكنولوجيا الرقمية في الوقت الراهن، فإنها تتسبب في عواقب تؤثر على حياة الناس في كل الأوقات بسبب التهديدات القائمة والمحتملة في الفضاء السيبراني والتي تتزايد بفعل تغيير طبيعة الحدود لما يسمى المجال الجوي والبري والبحري. لقد فرض الفضاء الافتراضي نفسه كبعد استراتيجي للصراع وكمجال خامس جديد للنزاع بين الدول وتوجيه ضربات عسكرية كجزء من الغزو ووسيلة قتال مبتكرة لمهاجمة البنية التحتية لتكنولوجيا المعلومات في إقليم الخصم مما يهدد الأمن القومي للدولة بل الامن والسلم الدوليين. بسبب استخدام برمجيات تخريبية خبيثة اثناء العمليات السيبرانية، تحدث خسائر مادية كتعطيل عمل المؤسسات وتدمير البنية التحتية الحيوية من اتلاف أشياء او نظم واصول مادية او افتراضية مرتبطة بالاقتصاد الوطني والصحة العامة. كما توقع هذه العمليات إصابات ووفيات على إثر تعطيل خدمات اساسية يحرم منها السكان المدنيون او يعرضهم لمخاطر صحية. تشير التقديرات إلى أن أكثر من 100 دولة قد طوّرت- أو

تعمل على تطوير- قدرات عسكرية سيبرانية، لكن عددا ضئيلا منها يقرّ علناً باستخدام وسائل سيبرانية لدعم عملياتها العسكرية ولشل قدرات الدولة العدو.

من هنا تبرز أهمية هذه الدراسة. فاذا كان الاستخدام الخبيث للفضاء السيبراني في سياق نزاع مسلح يساهم في ارتكاب أفعال يحظرها قانون النزاعات المسلحة وتستوجب ملاحقة جزائية من القضاء الجنائي الدولي، كما لو حدثت اثناء حرب تقليدية تتواجه فيها الجيوش النظامية، يُطرح السؤال حول تقرير المسؤولية الجنائية عن عواقب الهجمات الالكترونية. تقتضي الإجابة على هذا السؤال من جهة، تبني مقاربة قانونية وإنسانية لإبراز بعض الإشكاليات القانونية والإنسانية التي يثيرها استعمال وسائل واساليب حرب جديدة؛ ومن جهة ثانية اعتماد المنهج التحليلي الاستنباطي لتفكيك مضامين قواعد القانون الدولي الإنساني ولاستكشاف مدى قابلية هذا الفرع القانوني في صيغته الحالية– الذي يشار إليه أيضاً باسم قوانين الحرب أو قانون النزاعات المسلحة – للتطبيق على العمليات العسكرية السيبرانية بهدف تفادي آثارها الخطيرة على المدنيين والممتلكات المدنية والتي قد تتجاوز بتأثيرها وأبعادها الأهداف العسكرية للأطراف المتعادية. واذا استعصى الإدلاء بجواب مقنع، فهذا يعني ان ثمة حاجة الى وضع نهج تفسيري تطوري للبنية المعيارية للقانون الدولي الإنساني ليستوعب التطورات الحاصلة والمفاهيم الجديدة[1]، وربما حتى اقتراح تعديل على النظام المؤسس للقضاء الجنائي الدولي.

تتمثل خطة الدراسة في مبحثين اثنين، يخصص الأول لمعالجة مخاطر العمليات السيبرانية التي تنفذ في سياق نزاع مسلح وعواقبها المحتملة على الصعيد الإنساني والأخلاقي مع

1 نشير الى ان الحرب السيبرانية واثارها لم تبق دون اهتمام: في سنة 2013 أصدر فريق الخبراء الحكوميين تقريراً اعتُمد بتوافق الآراء يؤكد أن استخدام الدول لتكنولوجيا المعلومات يخضع للقانون الدولي. وظلت مسألة كيفية تطبيق القانون مفتوحة. لمتابعة النتائج التي توصل إليها فريق الخبراء الحكوميين أُنشأ فريق عمل جديد في الأمم المتحدة سنة 2019 مفتوح العضوية لجميع الدول الأعضاء خلص الى القول أن القانون الدولي ينطبق على الحرب الإلكترونية؛ لكنه هو الآخر لم يتمكن من التوصل إلى اتفاق حول كيفية تنفيذ ذلك، فانشأ فريق عامل جديد في الأمم المتحدة للفترة الممتدة من 2021 إلى 2025.

التوقف عند مسألة تكييفها في القانون الدولي وبصفة خاصة القانون الدولي الإنساني. فهل يستقيم الرأي القائل بعدم وجود فراغ قانوني يحكم استخدام الفضاء السيبراني في الحروب المسماة "حروب الجيل الخامس" وهو ما يعني شمولها بهذا القانون او أنه يبقى قانونا ضعيفا يحتاج اما تطويره بتوسيع نطاق المعايير الموجودة مسبقا أو الاستعاضة عنه بمعاهدات أخرى تعالج بشكل محدد استغلال التكنولوجيا في الحروب الحديثة. يروم المبحث الثاني، مقاربة النقطة المتعلقة بالمساءلة القانونية أي استجلاء موقف القضاء الجنائي الدولي ومدى قدرته على تكييف العمليات الالكترونية ذات اضرار مادية ومؤثرة على السكان الآمنين. باعتبارها مركزا للعدالة الدولية، يجدر بنا هنا توضيح دور المحكمة الجنائية الدولية الجهد الذي تبذله هذه الهيئة لإدماج العمليات السيبرانية في شكل هجمات عدوانية في نظامها الأساسي.

المبحث الأول : مخاطر الرقمنة في النزاعات المسلحة المعاصرة

في عالم يزيد اتصالا اكثر فاكثر في جميع الميادين بفضل فضائل الذكاء الاصطناعي تُبتكر وتتطور أدوات تستخدم لارتكاب جرائم دولية خطيرة في جميع الأوقات في السلم والحرب على السواء. يلاحظ اليوم لجوء الدول والجهات الفاعلة الأخرى بشكل متزايد إلى العمليات في الفضاء الإلكتروني. ويمكن إساءة استخدام هذه الوسيلة الجديدة والمتنامية للدبلوماسية والحرب لارتكاب أو تسهيل جرائم الحرب والجرائم ضد الإنسانية والإبادة الجماعية، وحتى العدوان من دولة إلى دولة ضد دولة أخرى .

المطلب الاول: أوجه تأثير التكنولوجيا الحديثة على سير العمليات العدائية

قبل التطرق الى مظاهر تأثير التكنولوجيا الحديثة على النزاعات الحديثة وكيف تفسح المجال اليوم لاستعمالها كوسيلة مستحدثة لشن وإدارة الحرب عبر الفضاء الافتراضي، يجدر تعريف الحرب السيبرانية التي تعالجها هذه الدراسة وتحديد بعض المصطلحات الأخرى القريبة او المتداخلة مع هذا المصطلح.

الفقرة الأولى: تعريف الحرب السيبرانية وتمييزها عن مصطلحات اخرى

إن كلمة "سيبرانية" مشتقة من الكلمة اللاتينية(kybernetes) "Cyber" تنطوي على معنى التخيل والافتراض. تستخدم لوصف الفضاء الذي يضم الشبكات العنكبوتية المحوسبة، ومنظومات الاتصال والمعلومات وأنظمة التحكم عن بعد. ومنها اشتقت صفة السيبريانية (Cybernetics) التي يقصد بها علم التحكم الأتوماتيكي بما يفيد القياد والتوجيه. ارتباطا بأهداف هذه الدراسة، فان الحرب السيبرانية تشير الى المواقف التي تعدّ جزءا من سياق نزاع مسلح متخذة شكل هجمات الكترونية. فالعمليات السيبريانية التي تشن ضد أو عبر حاسوب أو نظام حاسوبي مستهدفة تحقيق أغراض مختلفة كاختراق وجمع أو نقل أو تدمير أو نقل او تغيير او تشفير البيانات او التلاعب بها او تدمير الحواسيب التي تتحكم في هذه الأخيرة1، ليست

1 قد تكون العملية في سياق سيبراني هدفها التجسس. في حين كان التجسس التقليدي يستلزم نوعا من التفاعل المادي المباشر مع الدولة المستهدفة، يمكن إجراء التجسس السيبراني من طرف الدولة عبر وسيلة رقمية للاستحواذ السري على معلومات استخباراتية سرية من جهات فاعلة أخرى دون أن يغادر الجاني دولته الأصلية. انظر، أميرة عبد العظيم، محمد عبد الجواد: المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد 35 الجزء الثالث سنة 2020 ص 378.

جميعها حربا إلكترونية(سيبرانية)[1]. فهي سواء كانت هجومية او دفاعية قد تتحول الى هجوم سيبراني وتوصف بانها حرب سيبرانية، عندما تُحدث تأثيرات مكافئة للنزاع المسلح التقليدي أو تقع في سياق نزاع مسلح بغرض التسبب بإصابة او وفاة اشخاص او الحاق اضرار بالأعيان المدنية والمنشآت التي تشتمل على قوى خطرة عن طريق تدمير أو تعطيل" شبكات الكومبيوتر[2].

يفيد التعريف البسيط للهجوم الإلكتروني، بأنه الهجوم الذى ينطلق من كمبيوتر ضد موقع على الانترنت، أنظمة كمبيوتر أو حاسوب شخصي بهدف الإضرار بسرية أو سلامة الكمبيوتر أو المعلومات المخزنة عليه. يذهب البعض في تعريف الهجمات الإلكترونية/السيبرانية، بأنها أي شكل من الاعتداء يقوم بها أفراد أو منظمات تستهدف نظم معلومات حاسوبية، بنية تحتية، شبكات كمبيوتر، أجهزة حاسب شخصية، وذلك من خلال وسائل مختلفة من الأعمال الخبيثة، وعادتاً ما تصدر من مصدر مجهول، بغرض السرقة أو تدمير أهداف محددة[3].

على الرغم من أن عددا من المحللين والخبراء يوقنون أن الهجمات السيبرانية لها أضرار اقتصادية ومادية جسيمة وواسعة النطاق، وتؤثر على حياة وسلامة السكان المدنيين، فانه لم

1 -إن المثال الوحيد المعروف علنا للحرب السيبرانية هو دودة"Stuxnet" ، التي أنشأتها إسرائيل والولايات المتحدة بشكل مشترك والتي ألحقت أضرارا ب 1000 جهاز طرد مركزي في منشأة نووية إيرانية. وبالمقارنة، في عام 2012، بدأت إيران هجوما إلكترونيا يزعم أنه ألحق أضرارا ب 30 ألف جهاز كمبيوتر في شركة النفط السعودية أرامكو، لكنه لم يؤثر بشكل مباشر على البنية التحتية المادية لشركة أرامكو. يعتبر محللون إنه من خلال هاتين الحالتين اي هجوم "ستوكسنت" و "أرامكو"، من المحتمل أن يكمن التمييز المهم بين ما هو عمل من أعمال الحرب وما هو ليس كذلك.

2 -CICR, Le droit international humanitaire et les défis des conflits armés contemporains Réengagement en faveur de la protection dans les conflits armés à l'occasion du 70e anniversaire des Conventions de Genève), 33e CONFÉRENCE INTERNATIONALE DE LA CROIX-ROUGE ET DU CROISSANT-ROUGE, Genève, Suisse, 9-12 décembre (2019),(33IC/19/9.7), P. (25) (41).

3 شريف نسيم فلتة بخيت، دليل "تالين" :الهجمات الإلكترونية وحظر استخدام القوة في القانون الدولي، المركز العربي لأبحاث الفضاء الإلكتروني، متاح على الرابط: https://accronline.com/print_article.aspx?id=28958

يتم توقيع أي وثيقة دولية تعطي تعريفا شاملا للحرب السيبرانية، وتنص على أحكام واضحة تنظمها. ولا يزال هناك جدل كبير حول ما إذا كان أي حادث إلكتروني حتى الآن يشكل عملا من أعمال الحرب الإلكترونية، لان مصطلح "الحرب السيبرانية " بنفسه غامض بعض الشيء. بل ان "توماس ريد"، في كتابه "الحرب الإلكترونية لن تحدث"، يجادل بأنه حتى الآن لا يوجد فعل معروف لـ "الحرب الإلكترونية"، عندما يتم تعريف الحرب بشكل صحيح. لا شك ان هناك محاولات فكرية من طرف باحثين ومبادرات مختلفة لمعاهد علمية لتعريف الحرب السيبرانية، لكن لم يجر اتفاق دولي على معنى قانوني محدد لعبارات تُتداول في هذا المجال ك" الهجمات السيبرانية" او العمليات السيبرانية" او هجمات على شبكات الحواسيب. فهي كلها عبارات تستعمل في سياقات مختلفة وبمعان مختلفة وفي حالات يومية أي ليس لها دائما علاقة بنزاع مسلح[1].

إن التعريف الأكثر استشهادا به، هو ذاك الذي قدمه "ريتشارد كلارك وروبرت نيك" سنة 2010 واصفا من خلاله الحرب السيبرانية بانها "إجراءات من قبل الدولة القومية لاختراق أجهزة الكمبيوتر أو الشبكات الخاصة بدولة أخرى"[2]. من هنا يمكن تمييز الحرب السيبرانية عن الحرب التقليدية /الحركية باعتبار ان الأولى تعتمد أسلحة الكترونية تتمثل في هجمات منفذة في فضاء افتراضي عبر شبكات المعلومات والاتصالات متجاوزة حدود الدول المتعارف عليها، بينما

1 كوردولا دروغيه، ما من فراغ قانوني في الفضاء السيبراني، مقابلة مع المستشارة القانونية في اللجنة الدولية للصليب الأحمر. متاح على الموقع الرسمي للجنة الدولية للصليب الأحمر.

2 هناك فئتان او شكلين للعملية السيبرانية: الأول، الاستغلال السيبراني، وهو عمل غير مدمر عادة ما يكون سريا يسعى إلى الحصول على معلومات من شأنها أن تظل سرية لولا الاختراق. والثاني، هو الهجوم السيبراني. هذا عمل مدمر متعمد يهدف إلى تغيير أو تعطيل أو خداع أو إضعاف أو تدمير أنظمة أو شبكات الكمبيوتر الخاصة بالخصم أو المعلومات الموجودة في هذه الأنظمة أو الشبكات سواء كانت سرية أم لا. ريتشارد كلارك، روبرت نيك، حرب الفضاء الالكتروني: التهديد التالي للأمن القومي وكيفية التعامل معه. مركز الامارات للدراسات والبحوث الاستراتيجية، أبو ظبي، طبعة أولى ،2012 ص 48 متاح على الموقع، www.noor-book.com/uqnwj6

الثانية (حرب تقليدية) تعتمد على انخراط وتحركات الجيوش النظامية في ميدان قتال طبيعي أي محدد.

الفقرة الثانية: مظاهر استخدام الفضاء السيبراني كوسيلة حرب تؤثر في سير العمليات العدائية

يخلق الفضاء السيبراني ساحة معركة فريدة في قانون النزاعات المسلحة تمتاز بتوجيه الهجمات على الأهداف بدقة باتخاذ القرارات بسرعة أكبر بكثير من أي وقت مضى في التاريخ. فمن ناحية، هناك دول قد بدأت منذ سنوات بإنشاء وحدات داخل قواتها النظامية متخصصة في المحافظة على الامن السيبراني حيث طورت كل من الولايات المتحدة الامريكية وإسرائيل وروسيا وحدات متخصصة تحت مسمى القيادة القتالية السيبرانية، وانشات الصين عام 2015 "الجيش الصيني الأزرق". من ناحية أخرى، يسمح نفس الفضاء بإمكانية تنسيق الأفراد والجماعات المشاركة في الهجمات السيبرانية بمشاركة معلومات في الوقت المناسب. بعدما كانت الهجمات المسلحة تشن عن طريق وسائل وطرق تقليدية، تشمل البر والبحر والجو والفضاء، برزت هجمات من نوع آخر تحدث خارج المجال المادي وذات بعد جديد يتجاوز حدود الحرب التقليدية. في ساحة معركة افتراضية، يستخدم فيها رمز الكمبيوتر أو الحواسيب كأسلحة سيبرانية، يمكن أن تكون مدمرة مثل الذخائر التقليدية فتسبب أضرارا جانبية كبيرة، بما في ذلك الخسائر في صفوف المدنيين. وعند اختراق خدمة الإنترنت بواسطة برمجيات خبيثة وضارة مصممة على شكل فيروسات وديدان ورموز وشفرات لإلحاق الضرر بالعدو، من الصعب جداً التنبؤ بانها ستضر بنظم معينة فقط، لا بمجموعة واسعة منها.

تشير معظم الادبيات الى الحرب الالكترونية والى الدور المؤثر الذي تلعبه أنظمة المعلومات التي تُحشد لها فرق الدفاع والهجوم السيبراني مما جعل هذا الفضاء يدخل ضمن التشكيلات الأمنية والعسكرية للدول. فمع الإنترنت والفضاء السيبراني، اتخذت حرب

المعلومات هذه بعدا جديدا تماما لكسب الحرب. وكما ان التجربة بينت التجربة بانه من الضروري دائما إتقان المعلومات استراتيجيا وتشغيليا أي "تسليح المعلومات" أو استخدامها كسلاح لدعم النزاع الدائر فوق الأرض وأيضا للتأثير على الخصم قادة ومدنيين.

من السمات الرئيسية الأخرى التكنولوجيا الرقمية العسكرية، استعمال لأنظمة الأسلحة التي يتم التحكم فيها عن بعد كالطائرات بدون طيار التي تسمح للمقاتلين بالتغيب المادي عن منطقة العمليات القتالية. هذه التكنولوجيا الجديدة، شأنها شأن بعض أوجه التقدم الأخرى في التكنولوجيا العسكرية، يمكن أن تساعد المتحاربين أي مستخدميها من البشر على تشغيل هذه الأسلحة وتوجيه هجماتهم بدقة أكبر ضد الأهداف العسكرية، وبالتالي تقليل الخسائر في صفوف المدنيين والأضرار التي تلحق بالأعيان المدنية. لكن الدراسات أظهرت أن الحرب السيبرانية تتميز باستخدام أسلحة فتاكة ذات قدرة تدميرية واسعة النطاق تتجاوز ما قد تحدثه الأسلحة التقليدية التي حظرت أو قيدت استخدامها اتفاقية الأمم المتحدة لسنة 1980[1] بناء على خطورتها على المقاتلين والمدنيين[2].

أظهرت الأبحاث أيضا بان أنظمة الأسلحة التي يتم التحكم فيها عن بُعد تنطوي على مخاطر كبيرة: إن فصل الشخص، خاصة عن طريق المسافة (سواء كانت جسدية أو عاطفية) عن خصم محتمل يجعل الاستهداف أسهل والإيذاء أكثر احتمالا. يواجه التشغيل المسؤول لمثل هذا النظام تحديات كالقدرة المحدودة للمشغل على معالجة كمية كبيرة من البيانات، بما في

1 تنص اتفاقية الأمم المتحدة بشان أسلحة تقليدية معينة 1980 على حظر أو تقييد استعمال بعض أنواع الأسلحة ال تقليدية لأنها تعارض مع قاعدتين عرفيتين عامتين للقانون الدولي الإنساني هما :حظر استعمال الأسلحة العشوائية الأثر، وحظر استعمال الأسلحة التي تسبب معاناة لا مبرر لها أو إصابات مفرطة. وهي بهذا تحمي المدنيين من آثار الأسلحة المستخدمة في النزاعات المسلحة، وأيضا المقاتلين من المعاناة المفرطة التي قد تلحق بهم على نحو يتجاوز ما هو ضروري لتحقيق هدف عسكري مشروع.

2 اذا كان مبرر حظر او تقييد بعض أنواع الأسلحة التقليدية هو ان استخدامها ينتهك مبدأي التناسب والتمييز، فتحصيل حاصل ان يشمل الهجمات السيبرانية كسلاح حربي خطير يجب ان يخضع لنفس الاحكام.

ذلك البيانات المتناقضة في وقت معين ("الحمل الزائد للمعلومات")، والإشراف على أكثر من نظام واحد في وقت واحد، مما يؤدي إلى تساؤلات حول قدرة المشغل على الامتثال الكامل لقواعد القانون الإنساني الدولي ذات الصلة في تلك الظروف. كما ان استخدام أسلحة آلية أو ذاتية التشغيل ك "الروبوتات" بناء على كلمة مرور مثل بنادق الحراسة الآلية، والذخائر المزودة بأجهزة الاستشعار، وبعض الألغام الأرضية المضادة للمركبات، تعجز على التمييز بين المدني والمقاتل وبين مقاتل جريح أو عاجز من مهاجم أو أشخاص غير قادرين على فهم أو الاستجابة لتحذير شفهي صادر من النظام الذي يتحكم فيها، وبالتالي تطرح مشكلات متعددة عويصة ذات جوانب أخلاقية-انسانية وقانونية[1]. كما تثير كثير من الأسئلة الصعبة التي تحاول اللجنة الدولية بمعية خبراء حكوميين وغير حكوميين إيجاد تفسيرات لها في قواعد القانون الدولي الإنساني. كذلك على المستوى الإعلامي، يجب التحكم في المعلومات المتعلقة بالحرب، من أجل السيطرة على صورة الأطراف المعنية، والتأثير على الرأي العام، وتعبئته، وفي حالات لتجنيد المواطنين (مقاتلين سيبرانيين و/ أو المنشقين عبر الإنترنت وتحريضهم بشكل مباشر أو غير مباشر على القيام بأعمال انتقامية أو دعم للصراعات الحقيقية.

لا شك ان القانون الدولي الإنساني لن يطبق على جميع أنواع العمليات السيبرانية التي توصف بانها جريمة أو تجسس سيبراني أو غير ذلك[2]. لكن في نفس الوقت، الفضاء الإلكتروني ليس منطقة "خالية من القانون". فنظرًا لقدرتها كسلاح او كأسلوب للقتال يساهم في دعم الأسلحة المستخدمة في البيئات الأخرى، وعلى تحقيق ميزة عسكرية داعمة للعمليات العدائية التقليدية في سياق نزاع مسلح، فان الحرب السيبرانية تنطبق عليها قوانين الحرب وقابلة لأن يشملها القانون الدولي الإنساني عندما تنفذ في سياق نزاع مسلح. ليس هناك شك ان تنتج

1 بقراءة المادة 52 من البروتوكول الأول لعام 1977، يتبين ان العمل العسكري يجب ان يوجه الى الأهداف العسكرية.

2 يزخر الواقع وممارسة الدول بنماذج كثيرة للحرب والتجسس والهجمات السيبرانية. لمزيد من التفصيل انظر، نورية الساعدي المقريف "الحرب السيبرانية في ضوء احكام القانون الدولي العام، المجلد السابع عدد 2 دجنبر 2022 ص 11.

الأسلحة السيبرانية نفس تأثيرات الاستخبارات والتحييد والخداع التي تنتجها الوسائل التقليدية التي تخضع لإجراءات الاستهداف التي تنفذها اطراف النزاع. من تمّ، لايمكن الحديث عن الحماية دون الحديث عن الأسلحة خاصة وانها تشهد اليوم تطورا كبيرا[1].

عند اثارة الحديث عن استعمال الفضاء الالكتروني في سياق نزاع مسلح يتم التركيز بشكل كبير جدا على النزاع الروسي الاوكراني الذي شهد سلسلة من الهجمات الالكترونية التي زعزعت استقرار الفضاء الالكتروني وهددت الاستخدام الآمن والموثوق للتكنولوجيا. مع بداية الصراع، تم نشر ستة أنواع مختلفة من البرامج الضارة ضد المؤسسات العامة القطاعات الحيوية في أوكرانيا لمسح البيانات مما تسبب في تعطيل الخدمات الحيوية للسكان المدنيين. فتأثير الهجمات لا يقتصر على سرقة بيانات النظام الحاسوبي أو أجهزة الكومبيوتر المستهدفة بل تكون الغاية منها هي التأثير في العالم الواقعي من خلال العبث بالنظم الحاسوبية واختراق نظم مراقبة الحركة الجوية او نظم التدفق عبر انابيب النفط أو المحطات النووية لدولة العدو[2]. بهذه الوسائل، يمكن تدمير مجموعة متنوعة من "الأهداف" في العالم الحقيقي أو تغييرها أو تعطيلها، مثل الصناعات أو البنى التحتية أو الاتصالات السلكية واللاسلكية أو الأنظمة المالية. على الرغم من طابعها غير الحركي، فإن وسائل القتال هذه تخلق نتيجة "عنيفة" على سبيل المثال، على صحة الإنسان.

1 - أشار القانون الدولي الإنساني الى الأسلحة فحظر او قيد أسلحة استعمالها لثلاثة اومور: اما بسبب اثارها او حظرها او قيدها بأسمائها كالأسلحة التقليدية واسلحة الدمار الشامل(كيماوية، بيولوجية ونووية).

2 شهد النزاع الروسي –الاوكراني سلسلة من الهجمات الالكترونية زعزعت استقرار الفضاء الالكتروني وهددت الاستخدام الامن والموثوق للتكنولوجيا. مع بداية الصراع، تم نشر ستة أنواع مختلفة من البرامج الضارة ضد المؤسسات العامة القطاعات الحيوية في أوكرانيا لمسح البيانات مما تسبب في تعطيل الخدمات الحيوية للسكان المدنيين. فتأثير الهجمات لا يقتصر على سرقة بيانات النظام الحاسوبي أو أجهزة الكومبيوتر المستهدفة بل تكون الغاية منها هي التأثير في العالم الواقعي من خلال العبث بالنظم الحاسوبية واختراق نظم مراقبة الحركة الجوية او نظم التدفق عبر انابيب النفط أو المحطات النووية لدولة العدو.

هذا الاستنتاج هو ملاحظة مهمة في سياق الحرب السيبرانية، مما يشير إلى أن استخدام أسلحة محددة أثناء الأعمال العدائية المسلحة يجب أن ينطوي على تأثير مماثل للأدوات التقليدية للقتال مثل التدمير المادي أو الإصابة الضارة[1]. فهذا النوع الجديد من الاسلحة قد لا يخلف تأثيرا "دمويا" مثل القصف بالمدافع والقنابل والمتفجرات، لكن التحكم في أنظمة الطيران او اطلاق اشعاعات من محطات نووية او مواد "بالغة السّميّة" من محطات كيميائية او تلويث المياه العذبة او تسميمها تكون ذات نتائج كارثية. وبما ان القانون الدولي الإنساني حظر او قيد استعمال أنواع معينة من الأسلحة التقليدية armes conventionnelles بهدف حماية المدنيين من آثارها العشوائية وتجنيب المقاتلين إصابات مفرطة لا تخدم أي غرض عسكري؛ فلا يستساغ اذن ان لا تخضع العمليات السيبرانية - التي توصف بانها هجمات خلال حرب حركية، وتنتج اثارا عنيفة- لمبادئ قانون الحرب(jus in bello). والمبادئ الأساسية التي يرتكن اليها القانون الدولي الإنساني وهي مبدأ الإنسانية والتمييز والتناسب. فمن البديهي أن التسبب في انقطاع الكهرباء عن مستشفى وبالتالي التسبب في وفاة الناس لا يختلف عن إلقاء قنبلة. ومثاله أيضا، تسبب هجوم سيبراني في اغلاق شبكة وطنية لتوليد الطاقة لم يكن ممكنا اغلاقها الا من خلال قصف عسكري او غيره من اشكال الهجوم المسلح المادي.

في ضوء التقدم الهائل في القدرات السيبرانية المستخدمة لتوجيه ضربات عسكرية للدولة العدو خلال النزاع المسلح، ليس هناك شك بان القانون الدولي الإنساني ينطبق على العمليات السيبرانية مع استبعاد تلك الخارجة عن سياقات النزاعات. ذلك أن ميلاد هذا الفرع من القانون الدولي جاء اساسا لتلبية مقاصد محددة. أولها على الاطلاق، أنسنة الحرب وجعلها اقل ألما ومعاناة من جهة أولى، إعمالا بمبدأ "عدم إحداث آلام لا مبرر لها" الموثق في أحد اقدم

1 حامد محمد علي البلداوي، مواجهة الحرب السيبرانية في قواعد القانون الدولي الإنساني، مجلة الجامعة العراقية، عدد 57 مجلد 2 ص 375-376.

صكوك القانون الدولي الانساني [1]. من ناحية اخرى، يعد احتراما والتزاما بمبدأ تقييد حرية الأطراف المتحاربة في اختيار وسائل واساليب القتال. هذه قاعدة أساسية في قانون النزاعات المسلحة[2]، وهو واضح بخصوص بشأنها. غني عن البيان انه قانون سيحدّ من العمليات السيبرانية أثناء النزاعات المسلحة تماماً مثلما يحدّ من استخدام أي أسلحة ووسائل وأساليب حرب أخرى أثناء نزاع مسلح، جديدة كانت أم قديمة. هذا ما أكدته محكمة العدل الدولية معتبرة ان مبادئ وقواعد القانون الدولي الإنساني المنطبق في النزاع المسلح تنطبق على جميع اشكال الحروب وعلى جميع أنواع الأسلحة. كما ان هذا الموقف القضائي مؤطر بالمادة 36 من البروتوكول الأول الملحق باتفاقيات جنيف الأربعة[3]. تلزم هذه المادة الدول الأطراف بأن تجري استعراضات قانونية للأسلحة وان تحدد ما اذا كان او اتباع أسلوب جديد في الحرب او استخدام سلاح تقوم بدراسته او تطويره او اقتناءه يمتثل لقواعد القانون الدولي الإنساني. على الرغم من ان "وسائل الحرب" لا تجد لها تعريفا في القانون الدولي الإنساني، الا انها "أشياء" تستخدم لشن هجمات لتحقيق ميزة عسكرية وتؤدي الى تبعات عنيفة بإلحاق إصابات وأذى بالمدنيين وللتدمير المادي للأعيان او الممتلكات[4].

1 بخصوص هذه المبادئ راجع مضامين إعلانات صدرت في القرن 19 لا سيما اعلان سان بترسبورغ لعام 1868 وإعلان بروكسيل 1874 المعتمدة في ذلك العهد من طرف الدول الاوربية الكبرى الى جانب روسيا القيصرية.

2 عمر محمود المخزومي، القانون الدولي الإنساني في ضوء المحكمة الجنائية الدولية، دار الثقافة للنشر والتوزيع، عمان، طبعة أولى 2008 ص 28.

3 انظر الراي الاستشاري لمحكمة العدل الدولية حول مشروعية استعمال او التهديد باستعمال الأسلحة النووية، 8 يوليوز 1996، تقارير محكمة العدل الدولية، 1996، 226، فقرة 86.

4 - حسب المادة 36 من البروتوكول، تجري الدولة الطرف المنتجة للسلاح هذه المراجعة القانونية في مرحلة تصميم السلاح اي قبل الدخول في مرحلة الإنتاج وبعد ذلك في مرحلة تطويره التكنولوجي. وتجري الدولة المقتنية للسلاح المراجعة والاستعراض في مرحلة دراسة السلاح. وتشير المادة 84 من البروتوكول الأول ان تتبادل الأطراف السامية المتعاقدة اللوائح ذات الصلة بوضع الية دائمة لإجراء مراجعات للأسلحة الجديدة وطبعا الأسلحة السيبرانية مشمولة بالمادتين معا.

انها مسألة استحضرها " **دليل تالين**" المتعلق بالقانون الدولي المنطبق على الحرب السيبرانية[1]. رغم كونه صكا غير ملزم واقل شمولا، يعتبر هذا الدليل إنجازا مهنيا مهمّا يعالج المشاكل القانونية للأمن السيبراني في نطاق النزاعات المسلحة التي ركز عليها عمدا (الدولية وغير الدولية). إن "دليل تالين" عبارة عن توجيهات هدفها تطويع قانون المنازعات المسلحة ليشمل الحرب بوسائل الكترونية[2]. فهو يناشد الدول بان لا تتصرف في الفضاء السيبراني وكأن ثمة فراغ قانوني يجعله مستبعدا من القواعد والمبادئ القانونية التي تنطبق على الفضاءات المادية. تشير هذه الوثيقة الى ان انتهاك مبدأ عدم استخدام القوة يحدث أيضا إذا تسبب هجوم إلكتروني في أضرار شخصية أو أضرارا في الممتلكات وانه ينتهك سيادة الدولة التي هي أساس النظام القانوني الدولي[3]. لهذا يجوز الرد على الهجمات الالكترونية بأسلحة الحرب الحقيقية[4]. وفيما يتعلق بقانون الحرب، يشرح الدليل المبادئ والقواعد الهامة التي تنطبق على الحرب السيبرانية، ولكنه يدعو أيضا الى بذل المزيد من الجهود لوضع معايير أفضل الممارسات لإجراء العمليات العسكرية، وحل مشاكل الأمن السيبراني وتحسين مستوى التعاون الدولي في هذا المجال. فبالنسبة للبعض الذي يجادل في مسالة اخضاع الحرب السيبرانية للقانون الدولي الإنساني رغم الخسائر التي تتسبب فيها، ويطالب باعتماد اتفاقية جديدة او بروتوكول ضابط لهذا النوع من الحرب، فان المنطق يقتضي إعمال مقتضيات القانون الدولي الإنساني بمعناه الواسع

1 صدر دليل تالين في نسخة أولى سنة 2013 تتكون من سبعة فصول ويتضمن 95 قاعدة قانونية وضعتها لجنة خبراء قانونيين بارزين كانوا يجتمعون في"تالين" بإستونيا. في سنة 2016، تم اصدار نسخة ثانية مستحدثة حيث تم رفع سقف البنود الى 154 من قواعد القانون الدولي.

2 اللجنة الدولية للخبراء التي أعدته كان بدعوة من مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي (الناتو) تكلفت به مطابع جامعة كمبريدج 2013.

3-كثيرة هي الدول التي تتمسك بمبدأ السيادة كما حددته محكمة العدل الدولية سنة 1949 في قضية "مضيق كورفو" حيث شددت على مبدأ مساواة الدول المستقلة في السيادة التي تعني عدم الاعتداء على الحدود الإقليمية للدولة مستطردة بانه أساس العلاقات الدولية.

4 رغدة البهي، مجال حرب: كيف استجاب حلف شمال الأطلسي للدفاع السيبراني، كراسات استراتيجية، مركز الاهرام للدراسات الاستراتيجية، العدد 334 المجلد(31) مارس، 2022 ص 27.

(قانون جنيف وقانون الحرب) في انتظار حسم نهائي للنقاش الدائر اليوم في منتديات دولية بين الدول والخبراء والأقران بخصوص هذه المسألة. كما ان المنطق يقتضي الالتزام بميثاق منظمة الأمم المتحدة الذي يحظر الحرب العدوانية التي تعتدي على استقلال وسيادة دولة عضو. بموجب قانون مسوغات الحرب، لا يسمح بالعمليات العسكرية عبر الحدود بسبب الحظر الذي يفرضه ميثاق الأمم المتحدة فيما بين الدول الملزمة بهذا الحظر إما بالتصديق على المعاهدة الدولية أو بالقانون الدولي العرفي[1].

المطلب الثاني: التحديات في حماية البنية المدنية الأساسية من الهجمات السيبرانية

ليس هناك شك ان حماية المدنيين في الأوضاع الاستثنائية (نزاع مسلح) هي سبب وجود القانون الدولي الإنساني. سبقت الإشارة غير ما مرة ان العمليات السيبرانية اصبحت تشكل جزءا من النزاعات المسلحة اليوم بسبب استعمالها كنوع من أسلحة او أساليب القتال مخلفة خسائر مادية وعواقب إنسانية قد تصل الى إزهاق أرواح سكان آمنين. على مدى السنوات الأخيرة، شاركت اللجنة الدولية للصليب الأحمر باعتبارها حارسا للقانون الدولي الإنساني وحريصة على تذكير اطراف النزاع بالتزاماتها بموجب هذا القانون في حوار ثنائي وسرّي مع عدد من الدول بشأن التكلفة البشرية المحتملة للحرب السيبرانية وبشأن التحديات التي تطرحها استعمالها كوسيلة حرب. كما ان المنظمة لا تتخلّف في التنقيب عن سبل الاستجابة المستمرة ومواجهة نوع مستجد من «التسلح المعلوماتي»، ببلورة أنشطة حمائية جديدة،

1 رغم ان استخدام القوة غير معرف في الميثاق الا انه يتطلب الهجوم المسلح ويمتد التهديد بحظر استخدام القوة ليشمل العمليات السيبرانية. انظر المادة الثانية من ميثاق الأمم المتحدة فقرة رابعة.

تتناسب مع أشكال التسلح الجديدة فضلًا عن التفكير والعمل المستمرَّين على تطوير وتطبيق القانون الدولي الإنساني وسياسات العمل الإنساني وبرامج العمل الإنساني والمعايير العملياتية..

الفقرة الأولى: تهديد او تدمير البنى الأساسية والحيوية لبقاء السكان المدنيين

في قانون سير العمليات العدائية تُتداول مفاهيم قانونية مثل -"المدنيون" والاعيان او الممتلكات المدنية" والسكان المدنيين"- تستدعي تطبيق قواعد قانونية مختلفة لكن لها نفس الغاية أي الحماية[1]. لغرض هذه الدراسة، يجب ان يفهم بان تضرر المدنيين من العمليات السيبرانية يتحقق أيضا من خلال الاعتداء على البنية الأساسية المدنية سواء كانت العملية هجومية أو دفاعية. هذا ما يحدث اليوم في اول حرب اليكترونية حقيقية (روسيا ضد أوكرانيا) على حد تعبير اكبر مسؤولي التحول الرقمي في اوكرانيا "فيكتور زورا" مؤكدا بان الهجمات الحركية تتم بالتنسيق مع الهجمات السيبرانية وان اغلبها موجهة ومنظمة ضد المدنيين. انها أكثر الطرق احتمالا لتأثير العمليات السيبرانية على السكان المدنيين. في القانون الدولي الإنساني تتأسس الحماية على مبدأين جوهريين لا محيد عنهما هما: مبدأ الضرورة العسكرية ومبدأ المتطلبات الإنسانية. فإذا كانت الضرورة العسكرية تقتضي تحقيق ميزة عسكرية باستخدام الدولة وسائل وطرق تتيح لها تحقيق هذه الغاية، فإن المتطلبات الإنسانية تحتم على المتحاربين الساعين إلى تحقيق التقدم العسكري، مراعاة القواعد والمبادئ الإنسانية التي تمنع الاعتداء على الأشخاص غير المقاتلين[2]. انه حظر يجسد مبدأ حصانة المدنيين الذي تمت الإشارة اليه

1- جاء تعريف المدني في المادة 50:" المدني هو أي شخص لا ينتمي إلى فئة من فئات الأشخاص المشار إليهم في المادة 4 من اتفاقية جنيف الثالثة والمادة 43 من هذا البروتوكول. وإذا أثير الشك حول شخص فإنه يعتبر مدنيا". لا تسقط الحماية المقررة للمدنيين الا في حالات ووفق شروط محددة في قانون النزاعات المسلحة.

2 انظر، زهرة الهياض، القواعد الأساسية لحماية ضحايا النزاعات المسلحة منشورات وزارة الثقافة ،مطبعة دار المناهل ،لمغرب السنة 2012 ص 29.

لأول مرة في مدونة "فرانسيس ليبر"[1]، وأكد عليه الدبلوماسي والمسؤول العسكري "دي مارتينز" في القرن التاسع عشر. واستنادا الى "دليل تالين" تحظى الممتلكات والأشخاص المدنيون بالحماية وبالتالي اتفق أغلب الخبراء المساهمين في صياغته أنه علاوة على الضرر المادي، فإن توقف أحد الأعيان عن العمل قد يشكل ضرراً أيضاً.

يشير تعبير «العواقب الإنسانية» إلى موجات النزوح والموت والاختفاء وخسارة الممتلكات أو تدميرها وضياع مصادر الدخل، والأذى أو الضرر الجسدي والعقلي/النفسي والاجتماعي، والوصم وتشتت أفراد الأسرة، أو الحرمان من الحصول على الخدمات (التعليم، الصحة، المأوى، الغذاء).

في أوقات النزاع المسلح، قد يميل المتحاربون مهاجمة "عين" مدنية مثل شبكة مدنية مصرفية او كهربائية او اتصالات بهدف تدميرها او فقط احداث اختلال وظيفي في نظامها لتعطيلها مما يحرم المستفيدين من خدماتها لمدة قد تطول او تكون قصيرة. لإضعاف الخصم أو لتقويض معنوياته، قد يتم اختراق شبكة الكهرباء في أراضيه من خلال هجوم سيبراني لقطع الكهرباء عن المناطق المأهولة بالسكان وعرقلة كل جهد لتجنب إعادتها بسرعة. انها عملية تترك تبعات خطيرة لأنها ستمس لامحالة قطاعات أخرى ولو ان البعض سيدخلها في خانة الأضرار "العرضية"les dommages collatéraux. فالعواقب الإنسانية التي تتسبب فيها التحديات الرقمية تشمل أيضًا ظهور أو تفاقم الاحتياجات إلى المساعدات الإنسانية كالمأوى والغذاء والمواد الأخرى والرعاية الطبية والدعم النفسي والنفسي-الاجتماعي، والدعم الاقتصادي والحصول على الخدمات والحصول على المعلومات المناسبة على المستوى المحلي وفي الوقت المناسب، والدعم والمشورة القانونيَّين والوصول إلى الإنترنت. فلنتصور أن لدى الدول النووية

1 راجع - Yves sandoz ; commentaires des protocoles addionnels du 8 juin 1977 aux conventions de Genève de 1949 ,CICR Genève 1986 P 595.

التسع أكثر من 13 ألف قنبلة نووية، وليست نظم القيادة والسيطرة بكل منها بمنأى عن الخطأ البشري والهجمات السيبرانية. وقوة العديد من هذه الرؤوس الحربية أشد بكثير من القنبلتين اللتين أُسقطتا في عام 1945، وتسببتا في مقتل أكثر من 100 ألف إنسان، من بينهم 1,924 فردًا من الأطباء وأطقم التمريض في هيروشيما التي كانت تبلغ 2,080 فردًا آنذاك. وإذا كان مقررًا أن تنفجر أسلحة نووية في منطقة مأهولة بالسكان أو بالقرب منها في وقتنا الحاضر، فقد أظهرت دراسات أجرتها اللجنة الدولية والأمم المتحدة أنه لا توجد حكومة وطنية أو منظمة دولية لديها القدرة على الاستجابة للاحتياجات الإنسانية الهائلة التي ستنجم عن ذلك. فأعداد الذين سيحتاجون إلى العلاج ستكون ضخمة، ومن المحتمل أن تدمر معظم المرافق الطبية المحلية، وستُزهق العديد من الأرواح في لمح البصر[1]. من شأن هذه الحوادث، أن تؤدي إلى تفاقم ضعف السكان المدنيين في المناطق المتضررة من النزاع [2]، كالمرضى في المستشفيات في حال تعرض قطاع الرعاية الصحية للهجوم. لقد كانت جائحة كوفيد-19 كإحدى حالات الطوارئ القاسية التي أثرت على جميع دول العالم، بمثابة تذكير قوي بأن حماية القطاع الطبي أصبحت أكثر أهمية من أي وقت مضى. في هذا السياق تجدر الإشارة الى الهجمات السيبرانية التي ترقى بموجب القانون الدولي الإنساني الى هجوم، تشكل فعلا انتهاكات لقواعد هذا القانون اذا وجهت لمنشآت مدنية من بنيات صحية (مستشفيات او وسائل النقل الطبي) وشبكات المياه الصالحة للشرب ومحطات توليد الكهرباء والسدود ...الخ. ما لم تستخدم لأغراض عسكرية تجعلها هدفا للهجوم. وحتى لو كان هذا صحيحا، تلتزم الأطراف المتحاربة باتخاذ العناية اللازمة لتفادي انفلات قوى

1 يلزم للدول ان تستأنس برأي محكمة العدل الدولية إزاء استعمال أسلحة أو متفجرات نووية حيث اعتبرت" بانها ضرر أعظم مما لا يمكن تجنبه لتحقيق اهداف عسكرية مشروعة". انظر، زهرة الهياض، القواعد الأساسية لحماية ضحايا النزاعات المسلحة، مرجع سابق ص 261.

2 - سنة 2015 تم تنفيذ هجوم إلكتروني لأول مرة غرب أوكرانيا باستعمال برنامج خبيث BlackEnergy تسبب في انقطاع الطاقة والتيار الكهربائي عن بُعد عن ما يقرب من 225 ألف مستهلك حيث قامت البرمجيات الخبيثة بفصل المحطات الكهربائية الفرعية. هناك مخاوف انه إذا تمكنت الجهات الفاعلة الخبيثة من تعطيل أنظمة الكهرباء في بلد ما، فإن ذلك سيؤثر على الأنظمة الأخرى ابتداء من الخدمات المصرفية الى أنظمة التحكم في حركة المرور. أن قطعة من البرامج الضارة الموجهة إلى نظام واحد يمكن أن تؤثر.

خطرة سترتب خسائر فادحة في صفوف السكان المسالمين وإلا سيوقع هذا الدولة في الحظر المتعلق بالهجمات العشوائية[1].

ان الترابط بين الشبكات المدنية والعسكرية يجعل معظم الشبكات العسكرية تعتمد على البنية الأساسية السيبرانية المدنية. وعندما تمتد الحرب إلى الفضاء الإلكتروني بتنفيذ هجوم سيبراني، فليس مستبعدا ان لا يحترم منفذ هذا الهجوم مبدأ التمييز والتناسب بسبب طمس الخط الفاصل ليس فقط بين الأهداف العسكرية والاهداف المدنية لكن أيضا بين المدنيين والجنود. تساهم الوسائل الرقمية في حروب هذا العصر في انخراط عدد متزايد من المدنيين في الصراعات المسلحة. هي مشاركة تكتسي أهمية خاصة لأن استخدام الخبرات المدنية أمر ضروري. قد يكون هؤلاء المدنيون أعضاء في القوات المسلحة النظامية ولكن أيضا من جهات فاعلة غير حكومية، أو يكونون فقط "متسللين "نظرًا لوجودهم على مسافة ما من الأعمال العدائية المادية، بما في ذلك حتى من خارج البلدان التي تشهد حربًا[2]، وبالتالي قد يتم استهدافهم وفقا للقواعد العامة للمشاركة في العمليات العدائية. لقد وصلت ظاهرة القراصنة المدنيين الذين يقومون بعمليات الكترونية في سياق النزاعات المسلحة إلى أبعاد غير مسبوقة لأنها تلحق الضرر بالسكان المدنيين، إما عن طريق استهداف الأعيان المدنية بشكل مباشر أو إلحاق الضرر بها بشكل عرضي. بوجود بنية تحتية "مزدوجة الاستخدام" أي فضاء إلكتروني واحد فقط تتقاسمه القوات المسلحة مع المستخدمين المدنيين، مثل الخوادم، يصبح الخط الفاصل بين المدنيين والعسكريين أقل وضوحا في الفضاء الإلكتروني، مما يجعل هؤلاء المتسللين او

1 راجع التعليقات على البروتوكول الاضافيين سنة 1977، الفقرة 1962.

2 ناشطين او محترفي الامن السيبراني او "قراصنة وطنيين" كما يحدث في النزاع الدولي الروسي-الاوكراني حيث قدمت مجموعة من المتسللين نفسها على أنها "مجتمع عالمي لتكنولوجيا المعلومات" سيقوم "بمساعدة أوكرانيا على الفوز من خلال شل الاقتصادات المعتدية، وعرقلة الخدمات المالية والبنية التحتية والحكومية الحيوية". وإرهاق كبار دافعي الضرائب.....الخ

"القراصنة" انفسهم عرضة للهجوم من الخصم كأهداف عسكرية[1]. وإذا كان القانون الدولي الإنساني لا يجيز مهاجمة المدنيين ما لم يشاركوا بشكل مباشر في الأعمال العدائية لانهم مدنيين يستمرون في التمتع بحماية القانون الدولي الإنساني من الهجوم المباشر عليهم. اما اذا قاموا بشن هجمات إلكترونية ضد أهداف عسكرية أو مدنية قد ترقى إلى مستوى "المشاركة المباشرة في الأعمال العدائية"[2]؛ فيحتمل ان يفقدوا الحماية المقررة لهم في القانون الدولي الإنساني، لان العدو لن يتوانى في استهدافهم لإرغامهم على الكف عن دعم العمليات العدائية[3].

اذا كان القانون الدولي الإنساني لا يشير الى حظر "للقرصنة" في حد ذاتها، ولا الى قيام المدنيين بعمليات إلكترونية ضد الأصول العسكرية، فهو يلزم الجميع دولا وفاعلين غير حكوميين بمراعاة ما يسمى "اعتبارات إنسانية أولية" بشأن حماية المدنيين في سياق النزاع المسلح بغض النظر عن أسباب النزاع[4] ثم من وجهة نظر قانونية، فقد تعهدت جميع الدول بعدم "السماح عن علم باستخدام أراضيها لارتكاب أفعال غير مشروعة دوليًا باستخدام تكنولوجيا المعلومات والاتصالات. ورغم صياغته كالتزام سياسي، فإن هذا المعيار يعكس التزام الدول ببذل "العناية الواجبة" بموجب القانون الدولي، بما في ذلك ما يتعلق بالقراصنة المدنيين الذين يعملون من أراضيها. يجب على أي دولة ملتزمة بسيادة القانون أو "النظام الدولي القائم على القواعد" ألا تتجاهل ما يقوم به الأشخاص الموجودون على أراضيها من عمليات إلكترونية تتعارض مع الالتزامات القانونية الدولية للدولة، بما في ذلك القانون الإنساني الدولي حتى لو

1 هناك خطر تحديد او تتبع مكان وجودهم فيتعرضون للهجوم بالرصاص او الصواريخ او طائرات مسيرة او بعمليات سيبرانية.

2 حسب فقهاء القانون الدولي يحتفظ المدنيون بالحماية لصفتهم المدنية ويوصون بان يتم التعامل مع كل حالة وفق لنوع المشاركة ودرجة خطورة المشاركة في تنفيذ عملية سيبرانية وما انتجته من اضرار.

3 كما أنهم يظلون خاضعين لعمليات إنفاذ القانون وقد يتعرضون للمقاضاة الجنائية تبعاً لما إذا كانت أنشطتهم تنتهك مجموعة أخرى من القوانين ويعتبرون مجرمين أو "إرهابيين" يجب محاكمتهم.

4 انظر حكم محكمة العدل الدولية في قضية نيكاراغوا ضد الولايات المتحدة الامريكية وموقفها من المادة الثالثة المشتركة ومكانة "الاعتبارات الإنسانية الأولية".

كانت موجهة ضد خصم[1]. فعلى الدولة "بذل العناية" لمنع هذا السلوك وما يشبهه لان فيه انتهاك لحماية البيانات المدنية الأساسية سواء المتعلقة بالأشخاص الطبيعيين أو المتعلقة ببنيات الرعاية الصحية والمنشآت الطبية. لن يكون موقف الدولة هنا سوى ترجمة صريحة للمادة الأولى المشتركة بين اتفاقيات جنيف الأربع والبروتوكول الإضافي الأول التي تتعهد الدولة الطرف في الاتفاقيات او البروتوكول باحترام وضمان احترام القانون الدولي الإنساني.

الفقرة الثانية: تهديدات الحرب السيبرانية للعمل الإنساني (المساعدة والحماية)

يمكن للتحول الرقمي الكبير في عالمنا المعاصر، لاسيما وسائل التواصل الاجتماعي، أن تحسِّن حياة الأفراد والمجتمعات المتضررة من الحرب والعنف ويؤدي إلى تحسين المسائل الطبية والإنسانية وتيسير جهود المنظمات الإنسانية التي تعمل على حماية الأشخاص المتأثرين بالنزاع ومساعدتهم. كما يؤدي استخدام تكنولوجيات الاتصال أو تحديد الموقع الجغرافي إلى تسهيل تحديد الاحتياجات، وإعادة إنشاء الروابط العائلية بعد الأزمة، أو تتبع تحركات السكان حتى في المناطق النائية. لكن في حالات أخرى، يسفر استعمال الانترنيت وما يتيحه من تقنيات رقمية عن مخاطر رقمية تعرّض الأشخاص الى مواقف محرجة او خطيرة يتأذى فيها الافراد اما جسديًّا أو نفسيًّا أو اجتماعيًّا أو اقتصاديًّا أو تتسبب في ظهور نقاط ضعف جديدة أو تضاعف بشكل رهيب نقاط ضعف موجودة. بالإضافة الى استهداف الهجمات السيبرانية البنية التحتية التي لا غنى عنها لإنقاذ الأرواح، وأنظمة الاتصالات، واستغلال البيانات الشخصية، والمراقبة الرقمية، والتنميط الرقمي (profilage)، والاستخدام غير المسؤول للتقنيات الناشئة، والانتشار الضار للمعلومات على المنصات الرقمية، وما إلى ذلك[2] ؛ ومن العواقب الإنسانية الأخرى احتمال

1 منعا للاستخدام المزدوج للبنية العسكرية والمدنية يجب ان تهتدي الدول بالمادة 58 من البروتوكول الأول لعام 1977 فتقصل "قدر المستطاع" بين الشبكات العسكرية والمدنية والبنية التحتية السيبرانية .

2 تستخدم اللجنة الدولية مفاهيم «المعلومات المغلوطة والمعلومات المضللة وخطاب الكراهية» للإشارة إلى أبرز أنواع المعلومات «المُسلَّحة» كمصطلح عام يمكن أن يشمل، على سبيل المثال لا الحصر: المعلومات المغلوطة، والمعلومات المضللة، وخطاب الكراهية، بالإضافة إلى

استعمال بيانات الافراد الشخصية لأغراض أخرى غير الأغراض الإنسانية[1]. في نزاعات اليوم ومنذ اول هجوم سيبراني، تعرضت له دولة إستونيا، اصبح مرجحا بان توجه هجمات الكترونية الى البيانات الرقمية التي تكون مخزنة في حواسيب العاملين في المجال الإنساني وقاعدة بيانات المنظمات الإنسانية كاللجنة الدولية للصليب الأحمر الراعي الأول للقانون الدولي الانساني[2]. يحدث هذا رغم ان المنظمات الإنسانية التي تتصف بكونها إنسانية وغير متحيزة بطبيعتها (كاللجنة الدولية للصليب الأحمر)، وانها حصلت على تفويض دولي صريح بموجب اتفاقيات جنيف الأربعة وبرتوكوليها الاضافيين لتقديم خدماتها في أوضاع النزاع المسلح[3]. هكذا لا تقتصر التبعات العنيفة والوخيمة للهجمات الالكترونية على المدنيين فقط، انما توجه بشكل متعمد للمنظمات الإنسانية التي تؤمن المساعدة والحماية للمتضررين من النزاعات المسلحة[4]. بالنظر الى التسهيلات التي تستفيد منها المنظمات الإنسانية في عصر التقدم التكنولوجي لدعم البرامج

عمليات التأثير المعلوماتي، والمعلومات الملغومة والدعاية الموجَّهة. وهذه المعلومات يمكن أن تُتداول من خلال الوسائل الرقمية (عبر الإنترنت) وغير الرقمية (غير المتصلة بالإنترنت). ومع أن هذه الظواهر موجودة دائمًا، إلا أن مظاهرها على الإنترنت أفضت إلى مجموعة جديدة من التحديات والأضرار المحتملة.

1 في سنة 2022 تعرضت حواسيب اللجنة الدولية للصليب الأحمر من خلال شركة خارجية في سويسرا تتعامل معها هذه المنظمة الانسانية لهجوم الكتروني أثر على بيانات شخصية تتعلق بما يزيد عن 515000 شخص من الأشخاص المعرضين للخطر بشكل خاص بما في ذلك اولك الذين انفصلوا عن اسرهم بسبب النزاع او الكوارث او الهجرة او الاحتجاز وهي بيانات توصلت بها اللجنة من حوالي 60 جمعية وطنية للصليب الأحمر والهلال الأحمر.؛Pirater les données des personnes les plus vulnérables au monde est un affront a l'humanité disponible sur https://www.ifrc.org /

2 في شهر شتنبر 2022 تعرضت لعملية القرصنة الخوادم والحواسيب التي تتضمن بيانات شخصية تخص أكثر من 515,000 شخص حول العالم. وشعر موظفو اللجنة الدولية للصليب الأحمر بالحرج بوصف اللجنة منظمة إنسانية تخضع للمساءلة أمام شركائها والناس الذين تخدمهم.

3 على إثر الهجوم الالكتروني الذي اخترق قاعدة بيانات الضحايا والأشخاص الموجودة لدى اللجنة الدولية للصليب الأحمر، اضطرت المنظمة تجميد العديد من برامجها كبرنامج إعادة الروابط العائلية الذي تديره مع المكونات الأخرى في الحركة الدولية للصليب الأحمر والهلال الأحمر.

4 لمزيد من معلومات حول افراد الخدمات الطبية بمفهوم قانون جنيف أنظر، زهرة الهياض، القواعد الأساسية لحماية..."، مرجع سابق ص 374-388.

الإنسانية، مثلاً عن طريق تسجيل المعلومات واستخدامها لتوجيه وتكييف الاستجابات أو عن طريق تيسير التواصل بين الموظفين العاملين في المجال الإنساني والمدنيين المتضررين من النزاع أو العنف يزيد اعتماد المنظمات الانسانية والنظم التي تصمّمها على الرقمنة والاتصال بالإنترنت. لكنها في نفس الوقت تكون معرضة بشكل خاص للهجمات السيبرانية لافتقارها إلى الحماية في غالب الأحيان مما يؤثر على قدرتها على توفير الحماية والمساعدة أثناء حالات الطوارئ الإنسانية[1]. يتعاظم خطر الهجمات الإلكترونية أكبر، وأكثر جسامة عندما تكون العمليات العسكرية التي تتواجه فيها الأطراف المتحاربة باستعمال الأسلحة والأساليب الحربية المعروفة، مدعومة بهذه الهجمات؛ فيتضاعف حجم الأضرار التي تصيب نظم الرعاية الصحية والبنية التحتية للمياه والطاقة، أو المستشفيات جراء القصف في العالم المادي. في كثير من الأحيان، تتعثر الخدمات حيث تعمل جزئياً فقط أو لا تعمل على الإطلاق كأن يعرض الهجوم البنية التحتية الرقمية المستخدمة للتنسيق بين الأطباء والأسرة والعلاج للخطر، مما يجبر الاطقم الطبية على إلغاء مئات العمليات والإجراءات الأخرى ويعرقل قبول المرضى الجدد. بالإضافة الى هذا، بات استهداف البيانات حقيقة إذ يمكن اتلافها أو حذفها اثناء نزاع مسلح دون عواقب قانونية مادام أن قواعد القانون الإنساني الدولي لا تتطرق إلى حماية البيانات على نحو صريح". انه مثال اخر على خرق مبدأ التمييز ولقواعد القانون الدولي الإنساني التي توفر حماية الوحدات الطبية ووسائل النقل الطبي على غرار أعيان اخرى مثل والممتلكات الثقافية والمنشآت الحيوية والمنشآت التي تحتوي قوى خطرة. انها حماية تمتد لتشمل البيانات الرقمية اللازمة لتشغيلها. لهذا يفصح الخبراء القانونيون والدول عن آراء متباينة بشأن كيفية تطبيق القانون الإنساني الدولي في هذه الحالة. من الأمثلة الحية التي نسوقها في هذا الصدد، ما يروج

1 فعندما تتعرض الحواسيب أو الشبكات التابعة لدولة ما لهجوم أو اختراق أو إعاقة، قد يجعل هذا الأمر المدنيين عرضة لخطر الحرمان من الاحتياجات الأساسية مثل مياه الشرب والرعاية الطبية والكهرباء. وإذا تعطلت أنظمة تحديد المواقع GPS عن العمل، قد تحدث إصابات في صفوف المدنيين من خلال تعطيل عمليات إقلاع مروحيات الإنقاذ وتوصيل مواد الإغاثة....الخ

من اخبار عن الانتهاكات التي تحدث في الحرب الروسية-الأوكرانية في الميدان كما في افضاء الافتراضي. اعلنت "مؤسسة السلام الإلكتروني" أن معظم الهجمات السيبرانية التي كانت أوكرانيا ضحية لها استهدفت أهدافاً عسكرية ومؤسسات عامة ووسائل إعلام، إلا أن المدنيين تضرروا أيضاً بقصد أو بغير قصد[1].

في ضوء هذه الحقائق الجديدة التي حفزتها الثورة الرقمية، مثل الهجمات السيبرانية التي تؤثر على المنظمات غير الحكومية الدولية وتستهدف بنيتها الرقمية، هناك دعوات لتحديث القانون الدولي الإنساني والتفكير في الحماية التي توفرها قواعدها الحالية[2]. على مستوى اخر، تبحث اللجنة الدولية للصليب الأحمر كيفية استجابة الإطار الحالي للقانون الدولي الإنساني للتحديات التي يفرضها التقدم التكنولوجي والتكيف معها[3]. على صعيد آخر ولمواجهة ظاهرة التسليح التي تهددها، وضعت اللجنة الدولية للصليب الأحمر «الدليل العملي بشأن المعلومات المغلوطة والمضللة وخطاب الكراهية» كمورد إرشادي يُعتمد لمعالجة بعض التحديات الرقمية

1 يوجد مقر هذه المنظمة غير الحكومية في جنيف وهي تقوم من موقعها على الانترنيت بتجميع الأدلة لتقييم ما إذا كانت البلدان تحترم المعاهدات الدولية التي وقعت عليها، من اجل تحديد الثغرات القائمة في القانون الدولي. كما تراقب الهجمات السيبرانية التي تنفذ في سياق الحرب الروسية –الأوكرانية.

2 تجدر الإشارة الى انه بمبادرة وجهد اللجنة الدولية للصليب الأحمر، يجري تحديث لاتفاقيات جنيف منذ سنة 2011 لجعلها تتماشى مع ما يحصل من تطورات في مجال التسلح وظهور إشكاليات في مجال الحماية. طبعا حافظت اللجنة الدولية على التعليقات السابقة الصادرة سنة1952 وسنة 1965 لكنها جندت خبراء عبر العالم ومحامون وأكاديميين قادة عسكريين، قضاة محاكم، هيئات التحكيم، منظمات دولية أخرى حكومية وغير حكومية لبلورة تعليقات جديدة تستجيب للمستجدات الطارئة.

3 انها مسالة لم تغب عن اهتمام اللجنة حيث طالبت الدول الأطراف في اتفاقيات جنيف أثناء المؤتمر الدولي الثامن والعشرين للصليب الأحمر والهلال الأحمر المنعقد عام 2003 بأن تخضع جميع الأسلحة الجديدة ووسائل وأساليب الحرب الجديدة "لاستعراض دقيق ومتعدد التخصصات" وذلك لضمان ألا يتخطى تطور التكنولوجيا الحماية القانونية المكفولة. ويُعَد استخدام العمليات السيبرانية أثناء النزاعات المسلحة مثالاً جيدًا على هذا التطور التكنولوجي السريع ; CICR ;. quelles limites le droit de la guerre impose t' il aux cyberattaques accessible sur htpps//www.org

التي تواجه العمل الإنساني في الميدان[1]. وفي عام 2020 اطلقت المنظمة مشروعا لوضع "شارة رقمية" تشير إلى البنية التحتية وبيانات الجهات الفاعلة المحمية التي لها الحق في استخدام الشارات المميزة من أجل تسهيل تحديدها ومنع استهدافها عن طريق الخطأ أو وقوعها ضحايا للأضرار العرضية الناجمة عن العمليات السيبرانية[2]. في نظر اللجنة لم يكن تحديد القانون الدولي الانساني للقواعد الأساسية التي تحد من آثار النزاعات المسلحة على المدنيين دون جدوى. فلا يجوز لأحد يشارك في الحرب أن يتجاوزها. بالنسبة للجنة الدولية للصليب الأحمر، فإنه من المهم أن تفسر الدول القانون القائم على نحو يكفل للمدنيين والبنى التحتية المدنية التمتع بنفس مستوى الحماية الذي تمتعوا به في الماضي. وتظل نفس الحماية قائمة في وجه الأسلحة الإلكترونية التي تخضع لنفس الضوابط التي تتحكم الوسائل الحربية التقليدية. وفي الحالات التي لا تشملها قواعد القانون الدولي الإنساني القائمة، يظل المدنيون والمقاتلون محميين بما يسمى "شرط مارتنز"، أي أنهم يظلون تحت حماية وسلطة مبادئ القانون الدولي المستمدة من الأعراف الراسخة، ومن مبادئ الإنسانية و ما يمليه الضمير العام[3].

1 لمزيد معلومات انظر محرر الإنساني، وجهة نظر إنسانية: مفاهيم أساسية في الحروب الرقمية، مجلة "الإنساني" العدد 70 11 غشت 2023

2 اللجنة الدولية للصليب الأحمر، دراسة عن استخدام الشارات: مسائل تشغيلية وتجارية ومسائل أخرى غير تشغيلية؛ جنيف سويسرا2013. متاح على الرابط :

https:// www.icrc.org/ar/publication/ study-the use-the emblèms

3 يرتبط «مبدأ مارتينز" باسم القائد العسكري والدبلوماسي الروسي" فريدريك فرومهولد دي مارتينز" الذي اقترحه على الوفود المجتمعة في مؤتمرات السلام بلاهاي 1899-1907، فتقرر ادراجه في ديباجة اتفاقية قوانين واعراف الحرب البرية 1899 واتفاقيات جنيف الإنسانية .

المبحث الثاني: المسؤولية الجنائية الدولية عن الهجمات السيبرانية والفضاء الجنائي الدولي

في هذا المبحث تعالج مسألة ما إذا كان ارتكاب عمليات سيبرانية عدائية يرتب مسؤولية جنائية يتحملها الأفراد في السياق السيبراني بسبب الاثار التي تخلفها. تبين نماذج تطبيقية كثيرة ان الدول والجهات الفاعلة الأخرى تلجأ بشكل متزايد إلى العمليات في الفضاء الإلكتروني لارتكاب أو تسهيل جرائم الحرب والجرائم ضد الإنسانية والإبادة الجماعية، وحتى العدوان من دولة ضد دولة أخرى. وكلها جرائم تدخل في الولاية الموضوعية للنظام الأساسي للمحكمة الجنائية الدولية. إن أول من أثار فكرة تشكيل ولاية قضائية عالمية لإنزال العقاب على مرتكبي الجرائم الأكثر إهانة لجوهر الإنسانية، هو غوستاف موينييه، أحد مؤسسي اللجنة الدولية للصليب الأحمر عام 1872[1]، إذ أن فكرة الردع الجنائي للمخالفات الجسيمة لقواعد الحرب التي ستكرسها فيما بعد مقتضيات اتفاقيات جنيف ولاهاي، كانت موازية لنشوء وتبلور هذه الأخيرة.

غير أن معالم العدالة الجنائية الدولية تبلورت عبر مراحل ومحطات، من المحاكم الجنائية الدولية المؤقتة-محكمة نورومبرغ وطوكيو، ثم محكمة يوغوسلافيا ورواندا-ثم المحاكم الجنائية الدولية الخاصة المشتركة –سيراليون ولبنان-، وصولا إلى مؤتمر روما لعام 1998 الذي أنشأ محكمة جنائية دولية دائمة لها سلطة التحقيق والمتابعة بشكل دائم في الجرائم التي تقع ضمن ولايتها، وهي جرائم الحرب، والجرائم ضد الإنسانية، وجريمة الإبادة الجماعية، وجريمة العدوان[2].

1 William Bourdon ; la cour pénale international : le statut de Rome ; éditions de seuil ; mai 2000 ; p14-15

2 انظر المادة 5 من نظام روما الأساسي.

حددت اتفاقية روما تعريفا دقيقا لمعنى هذه الجرائم حيث نصت على الأفعال التي تشكل جريمة من الجرائم التي تقع ضمن اختصاص المحكمة[1]، وغني عن البيان أنه عند صياغة هذه الاتفاقية المؤسسة لم تشهد الحروب استخدام الهجمات السيبرانية، كما ان هذه المسألة لم تُطرح في أروقة مؤتمر روما. ان الهجمات السيبرانية خاصة في إطار النزاع المسلح ظهرت كخطر جديد، وكسلاح حربي مبتكر يثير مخاوف كبيرة خاصة بعد تصاعد الادعاءات باستخدام الهجمات الالكترونية في النزاع الروسي الأوكراني كسابقة من نوعها. مما يطرح أسئلة حول سبل تطبيق نظام روما على الهجمات السيبرانية (المطلب الأول)، على ضوء البحث في تحديات وحدود تطبيق نظام روما الأساسي على الهجمات السيبرانية (المطلب الثاني).

بما ان هناك أصوات أو حتى اتفاق العديد من الدول على أن الفضاء السيبراني لا ينبغي أن يكون بمنأى عن التنظيم، بمعنى أن للقانون الدولي دورا رئيسيا يؤديه، وأن العدالة الجنائية الدولية ايضا، مطالبة بمسايرة هذا التطور الهائل فان الأسلحة السيبرانية التي تستعمل كوسيلة او أسلوب لارتكاب مثل هذه الجرائم يجب ان تكون محكومة أيضا بالقانون. صحيح أن النظام الأساسي للمحكمة الجنائية الدولية لعام 1998 لا يحتوي على أحكام محددة بشأن الجرائم الإلكترونية، إلا أن الجرائم الإلكترونية تقع ضمن نطاق العديد من الجرائم الدولية كما تم تعريفها بالفعل. ذلك ان الحدود لم تبق مادية وانما أصبحت حدودا رقمية تسمح للعمليات السيبرانية في شكل "هجوم" ان يكون له تأثير عميق على حياة المدنيين وعواقب فورية على البنية التحتية الحيوية مثل المرافق الطبية أو أنظمة التحكم في إنتاج الطاقة كما سبق توضيح ذلك في المبحث الأول من هذه الدراسة.

1 انظر المواد من 6 إلى 8 من نظام روما الأساسي.

المطلب الأول: سبل تطبيق نظام روما على الهجمات السيبرانية في سياق نزاع مسلح

إن غياب حكم واضح بشأن الهجمات السيبرانية في نظام روما الأساسي للمحكمة الجنائية الدولية، يثير السؤال حول إمكانية وصف الهجمات السيبرانية كجريمة على ضوء نظام روما(فقرة اولى)، ثم سبل تكييف الهجمات السيبرانية مع مقتضيات نظام روما الأساسي (فقرة ثانية).

الفقرة الأولى: الهجوم السيبراني كجريمة في ضوء نظام روما

من البديهيات أن عدم توقع الهجمات السيبرانية لا ينبغي أن يمنع الدول الأطراف في نظام روما الأساسي من الاعتراف بحقيقة التهديد اليوم، إذ يجب أن تخضع الإجراءات السيبرانية التي تستخدم لأغراض هجومية تلحق أضرار جسيمة بالبنية التحتية العامة أو الخاصة لدولة أخرى للملاحقة الجنائية أمام المحكمة الجنائية الدولية[1]. يجب أن تكون هذه الهجمات على درجة كافية من الخطورة لتقع ضمن ولاية المحكمة الجنائية الدولية بسبب عتبة الخطورة بموجب نظام التكامل المنصوص عليه من نظام روما الأساسي[2]. بوصفها مركزا لنظام العدالة الدولي الذي تلعب فيه كل من الدول والمجتمع المدني والمنظمات الدولية دورها، يمكن للمحكمة الجنائية الدولية أن تقدم العديد من المساهمات من خلال إجراءاتها الخاصة لضمان المساءلة القانونية بردع الجناة. من جهتها شددت اللجنة الدولية للصليب الأحمر على أن الهجمات

Ambassador David Scheffer; Amending the Rome Statute to Cover Cyber warfare as Aggression 1 international criminal law forum ; see the link : https://iccforum.com/cyberwar

2 استنادا الى المادة 17 (1) (د) من نظام روما التي تشير الى شرط التكامل لا تتدخل المحكمة اذا كانت الدولة التي لها ولاية على الدعوى قد شرعت في التحقيق او في حالة تقاعس هذه الدولة او عدم رغبتها في اجراء تحقيق ومقاضاة من ارتكب الفعل المحظور.

السيبرانية يجب أن تحترم المبادئ الأساسية للتمييز والتناسب المرعية في القانون الدولي الإنساني الناظم للحروب التقليدية، ويجب أن توجه فقط إلى الأهداف العسكرية [1].

بالعودة إلى معجم بعض المرافعات أمام المحكمة الجنائية الدولية، قد يكون القضاة قادرين على تفسير نظام روما الأساسي على أنه يغطي الهجمات السيبرانية والحرب السيبرانية، إذ أن العمليات السيبرانية هي في الأساس حديثة، لكنها وسيلة مؤثرة للغاية للاعتداء على الحكومات، المؤسسات الدولية، وانتهاك سيادة البلد وسلامته الإقليمية. فهي ذات وقع شديد الخطورة تضاهي ما يحدث في العالم المادي ولا ينبغي صرف النظر عنها. في هدا الصدد تجدر الإشارة الى مبادرة "مركز حقوق الانسان" التابع لجامعة "بيركلاي" Berkeley الذي وجه طلبا الى المدعي العام للمحكمة لإجراء تحقيق في الأفعال التي ارتكبها متسللون لدعم القوات الروسية في حربها ضد اوكرانيا[2].

كما يذهب رأي آخر في نفس الاتجاه، حيث اعتبر أنه من الممكن أن تشكل العمليات السيبرانية جرائم حرب بموجب اختصاص المحكمة الجنائية الدولية دون الحاجة إلى تعديل نظام روما الأساسي، إذا ما ارتكبت في سياق نزاع مسلح بالاقتران مع الهجمات الحركية التقليدية، كما تنطوي على أركان الجرائم المدرجة في المادة 8 من نظام روما الأساسي، وارتكبت في إقليم دولة طرف أو على يد أحد رعايا دولة طرف، وتنطوي على درجة الخطورة الواردة في

1 عملت اللجنة الدولية في البداية مع معهدين للبحث هما: مركز الثقة السيبرانية في معهد زيوريخ ومختبر الفيزياء التطبيقية في جامعة جونز هوبكين لا يجاد طرق تقنية للإبلاغ عن البنية التحتية والبيانات الرقمية للجهات الفاعلة المحمية. من المزايا الرئيسية لوضع شعار رقمي، أن هذه العلامة الجديدة يمكن إدراجها ضمن "الشعارات المميزة" أو "الإشارات المميزة" المعترف بها دوليا وسياسيا منذ زمن مثل الإشارة الضوئية وإشارة الراديو وتحديد الهوية . لمزيد من الوضوح، انظر المرفق الأول للبروتوكول الإضافي الأول لعام 1977.

2 اخترق هؤلاء البنية التحتية لأوكرانيا وهاجموا منشآت ومحطات نووية واخترقوا حسابات " الفايسبوك" لجنود اوكرانيين توهم السكان بان القوات الأوكرانية قد استسلمت.

نظام روما[1]. إذ لا يوجد في العناصر التي تستهدف جرائم الحرب بموجب المادة 8 ما يمنع تطبيقها على العمليات السيبرانية، وبالتالي، ليست هناك حاجة لتعديل نظام روما الأساسي لمحاكمتها أمام المحكمة. ولا تتعلق التحديات الرئيسية بتعريف الجرائم أو بقواعد القانون الإنساني الدولي المقابلة لها، بل بالعقبات التقنية المعروفة جيدا التي تحول دون تحديد هوية الجناة وجمع الأدلة، مشيرا إلى أن الدائرة التمهيدية في قضية "نتاغاندا" حددت مؤشرات معينة من أجل إثبات وجود شرط الصلة فيما يتعلق بجرائم الحرب، أبرزها هي إمكانية القول إن الفعل يخدم الهدف النهائي لحملة عسكرية التي تجعل من الممكن إثبات أن القانون الدولي الإنساني ينطبق على العمليات السيبرانية، ويمكن ارتكاب جرائم حرب محتملة في حالة انتهاكها[2].

غني عن البيان أن العملية السيبرانية التي تسبب تأثيرا مشابها لسلاح تقليدي يمكن أن تشكل "استخداما للقوة"، وبالتالي انتهاكا للمادة الثانية من ميثاق الأمم المتحدة وقد تشكل انتهاكا واضحا، إذا كان كافيا "الطابع والتأثير والحجم". غير أنه لم يحدث أي انتهاك حتى الآن قد يفي بهذا الاختبار الصارم. ونتيجة لذلك، لم يتم بعد تحديد ما يعنيه الانتهاك "الواضح" لميثاق الأمم المتحدة في سياق العمليات السيبرانية لان هناك افتقار للتوافق في الآراء. توصل أعضاء اللجنة الاستشارية بشأن تطبيق نظام روما الأساسي على الحرب السيبرانية إلى استنتاجات مختلفة بشأن ما يمكن أن يشكل انتهاكا "واضحا". فالبعض منهم اتخذ موقفا بناء على "نهج الآثار" مؤداه أن العمليات السيبرانية التي تؤدي إلى فقدان أو إصابة الحياة بشرية هي وحدها التي ستصل إلى مستوى الانتهاك "الواضح"؛ أو أنها التي تنطوي على تدمير مادي واسع النطاق يصل إلى مستوى الانتهاك الواضح. وهناك فريق اخر، يعتبر أنصاره أن إحداث العجز، دون

1 Marco Roscini; Cyber Operations Can Constitute War Crimes Under the ICC Jurisdiction Without Need to Amend the Rome Statute; international criminal law forum ; see the link : https://iccforum.com/cyberwar

2 - Marco Roscini; op.cit.

تدمير مادي، يمكن أن يكون كافيا[1]. يظهر من هذه الآراء ان هناك، اختلافات كبيرة بين الخبراء بشأن هذه المسألة. لكن من زاوية المحكمة الجنائية الدولية[2]، وعلى ضوء ما حدث ويحدث في سياق الحرب الروسية الأوكرانية من هجمات الكترونية كان لها آثار بعيدة المدى بسبب البرامج الضارة القادمة من الجانبين معا، أعلن المدعي العام الحالي للمحكمة الجنائية الدولية "كريم خان" عن عزم مكتبه فتح التحقيق، على الرغم من عدم تخصيص أي حكم من أحكام نظام روما الأساسي للجرائم الإلكترونية[3].

الفقرة الثانية: مسوغات تكييف الهجمات السيبرانية وفق قواعد نظام روما

يفترض نموذج التكييف القانوني عن طريق القياس الذي اقترحه "ريسينجر Reisinger" أنه في سياق مشكلة قانونية، من الضروري التمييز بين إطار واقعي وإطار معياري. إن المفهوم القانوني الأكثر وضوحا، أي المفهوم الذي يلعب دورا في عملية تفسير وتطبيق القانون، هو الحجة عن طريق القياس.

1- Oona A. Hathaway; To What Extent and Under What Conditions Might Cyber Operations or Cyber warfare Constitute Crimes Specified in the Rome Statute?; international criminal law forum ; see the link : https://iccforum.com/cyberwar

2 - KARIM A.A. KHAN KC ; Technology Will Not Exceed Our Humanity ; digital front lines ; see the link : https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/

3 - استضاف مكتب المدعي العام سنة يناير 2024 مؤتمرا رائدا شارك فيه اكثر من 100 مشارك بما في ذلك 12 شركة متخصصة في الامن السيبراني للنظر بعناية في الجرائم السيبرانية في سياق القانون الجنائي الدولي. دار النقاش حول احدث التهديدات الرقمية وتأثير الجرائم السيبرانية على حقوق الانسان والعدالة والمساءلة واستخدام الذكاء الاصطناعي بغرض التمويه والتضليل وإبراز الدور الذي بإمكان المحكمة الجنائية الدولية ان تلعبه في مكافحة هذا النوع من الجرائم. خرج المؤتمر بخلاصات ستساهم في صياغة سياسة عامة تتعلق بالجرائم الالكترونية على حد تعبير المدعي العام " كريم خان" الذي اطلق مكتبه منصة Project harmony لدمج بياناته في السحابة ولتعزيز سلامتها وتعزيز الامن الرقمي، ولان المحكمة بنفسها شهدت اختراق نظامها من طرف قراصنة ربما بسبب إصدارها مذكرة اعتقال ضد الرئيس الروسي "فلاديمير بوتين" بتهمة الإبعاد القسري لأطفال اوكرانيين. راجع الموقع الرسمي للمحكمة الجنائية الدولية.

على مستوى التشريعات الوطنية يُخوّل القاضي سلطة تقديرية في هذا الإطار. لكن على المستوى الجنائي يجعل مبدأ الشرعية سلطة القاضي ضيقة لان هذا الأخير مطالب بالتفسير الضيق لمقتضيات النص القانون[1]. انه نفس التوجه الذي يتبناه النظام الأساسي للمحكمة الجنائية الدولية حيث نص صراحة على إلزامية التأويل الدقيق وعدم التوسع في القياس على مقتضياته[2]. بان نص على ان لا يسال الشخص جنائيا بموجب نظام روما ما لم يشكل السلوك المعني وقت وقوعه جريمة تدخل في اختصاص المحكمة[3].

في نفس الإطار يشير أحد الباحثين أن السلوك في الفضاء السيبراني قد يقع ضمن اختصاص المحكمة إما لأنه يشكل وسيلة جديدة لارتكاب جريمة سبق إدراجها في النظام الأساسي[4]، أو لأنه يحرض على ارتكاب هذه الجريمة أو ييسرها اذ يجب على أساس عوامل كمية ونوعية كدرجة الخطورة أي تستوفي المعيار الوارد في المادة17 من النظام الأساسي للمحكمة بما في ذلك، على سبيل المثال لا الحصر، حجم الجرائم وطبيعتها وطريقة ارتكابها وعن تأثيرها. وقد طبق مكتب المدعي العام والدائرة التمهيدية هذه العوامل لتقييم خطورة الحالات والقضايا على السواء

كما أن هناك طريقتين يمكن من خلالهما إدراج العمليات السيبرانية في القائمة المحددة لأعمال العدوان المذكورة في المادة 8 مكررا. أولا، لكون القائمة غير حصرية؛ وبالتالي فهي تسمح للمحكمة الجنائية الدولية بإيجاد استخدامات أخرى للقوة المسلحة تشكل عملا عدوانيا. ثانيا،

1 انظر، Manuel Atienza ; L'analogie en droit ; Revue interdisciplinaire d'études juridiques 1988/2 (Volume 21),pages 33-56 , https://www.cairn.info/revue-interdisciplinaire-d-etudes-juridiques-1988-2-page-33.htm

2 الفقرة الثانية من المادة 22:" يؤول تعريف الجريمة تأويلاً دقيقاً ولا يجوز توسيع نطاقه عن طريق القياس، وفي حالة الغموض يفسر التعريف لصالح الشخص محل التحقيق أو المقاضاة أو الإدانة."

3 فقرة 1 من المادة 22 من نظام روما.

يمكن تفسير العديد من الأفعال الواردة في القائمة على أنها تنطبق على العمليات السيبرانية. ومن ثم فمن الواضح أن جريمة العدوان على النحو المحدد في نظام روما الأساسي يمكن أن تنطبق على العمليات السيبرانية، قد تنشأ عندما تكون العملية السيبرانية جزءا من حرب عدوانية أوسع؛ أو قد تنشأ عندما تكون العملية السيبرانية حدثا قائما بذاته.

في هذا السياق يتحدث أحد الخبراء في القانون الجنائي الدولي عن إمكانية التكييف الواسع لبعض المكونات القانونية للجرائم المنصوص عليها في القواعد الدولية تبعا لظروف اجتماعية جديدة[1*]، حيث أن عملية التكييف التطوري الذي تقوم به المحاكم، لاسيما توسيع نطاق المكونات القانونية لجريمة كفعل جرمي من أجل الحكم على سلوك لم يعتبر جرميا في السابق، متماشية مع القواعد الجنائية التي تحدد "جوهر الجريمة" خاصة إذا كان يسهل للمعنيين تكهنها بشكل منطقي. بمعنى آخر، أنه حتى لو تبين أن عملية توسيع النطاق المذكورة تضر بمصلحة المتّهم، إلا أنه كان بإمكان هذا الأخير توقّعها منطقيا بسبب توافقها مع المبادئ العامة للقانون الجنائي[2].

قد يستفاد من هذا الرأي وجود إمكانية لدى المدعي العام باستحداث فعل جرمي جديد، إذا توافرت الشروط التي سبق ذكرها، وبالتالي يمكن تجريم الهجمات السيبرانية إذا تماشت مع قواعد الجريمة، وكان بالإمكان توقعها. لكن من جهة ثانية، قد يكون في ذلك تنافي مع مبدأ الشرعية. فلا يجوز أن تستحدث المحاكم جريمة جنائية جديدة عن طريق مكونات قانونية جديدة -فعل جرمي جديد أو قصد جنائي جديد-، فهي لا تستطيع إلاّ تكييف الأحكام التي تتناول الجرائم الجنائية مع الظروف الاجتماعية المتبدّلة، خاصة عن طريق توسيع نطاق الفعل

1 -مستندا في ذلك إلى بعض السوابق القضائية للمحكمة الأوربية لحقوق الإنسان التي قضت أنه لا يمكن تفسير الاتفاقية الأوروبية على أنّها "تحظّر التوضيح التدريجي لقواعد المسؤولية الجنائية عن طريق التفسير القضائي من قضية إلى أخرى، ما لم يكن التطور الناجم عن ذلك منسجما مع جوهر الجريمة ويمكن توقّعه بشكل معقول- انظر انطونيو كاسيزي، مرجع سابق، ص85

2 أنطونيو كاسيزي وآخرون، القانون الجنائي الدولي، ترجمة مكتبة صادرون للنشر، الطبعة الأولى 2015، ص86

الجرمي أو ربما خفض عتبة العنصر المعنوي، من القصد إلى الاستهتار، أو من الاستهتار إلى الإهمال المذنب. ان التكييف لمبحوث عنه لإخضاع هذا النوع الجديد من الأفعال الخطيرة. فيجب ان يكون متوافقًا مع المبادئ العامة أ يكون مقبولا على خلفية انه تفسير لمقتضيات قائمة، وليس ذلك التفسير الذي يُحدث مقتضيات جديدة، فيسود شعور بان المحكمة تقوم بدور الهيئة التشريعية، أو أنها تتصرف بشكل شأنه ينتهك مبدأ الشرعية الذي يقوم عليها القانون الجنائي الدولي.

سبق ان أكّدت المحاكم الجنائية الوطنية والدولية مرارا وتكرارا على إجازة اللّجوء إلى المبادئ العامة للقانون الجنائي الدولي أو للعدالة الجنائية لتحديد ما إذا كانت قاعدة دولية تغطّي مسألة معينة في النزاع. ومن المؤكد أن هذه المعضلة لطالما طرحت ضمن إطار "التفسير" وليس التطبيق القائم على "القياس". إذ لا يكون هذا اللجوء إلى المبادئ من أجل ابتكار فئات جديدة من السلوك الإجرامي بل من أجل تفسير قواعد قائمة. إنما التمسك بخلاف ذلك يعني انحرافًا جديا عن مسار مبدأ الشرعية، يتناقض ومتطلبات القانون الجنائي الدولي[1].

المطلب الثاني: حدود تكييف الهجمات السيبرانية مع النظام الأساسي لمحكمة الجنائية الدولية

إن عملية تكييف الهجمات السيبرانية، في ظل غياب حكم بشأنها يبدو نوعا من "العدالة الموضوعية" التي عرف القرن العشرين التخلي عنها وتكريس مبدأ "الشرعية الصارمة". يرجع ذلك إلى عاملين اثنين،: أولهما، مصادقة الدول على عدد من المعاهدات المهمة حول حقوق

1 أنطونيو كاسيزي، مرجع سابق، ص91

الإنسان التي جعلت من مبدأ الشرعية ركيزة قانونية. أما العامل الثاني، فهو توسع شبكة القانون الجنائي الدولي تدريجيا، عن طريق عدد من المعاهدات التي تُجرم سلوك الفرد[1].

يتطلب البحث في المسألة ضرورة استيعاب مبدأ الشرعية في نظام روما علما انها مسالة تطرح العديد من الإشكاليات النظرية والعملية وتقف عائقا أمام تكيف مقتضيات روما مع مستجدات جرائم الحرب (فقرة اولى)، ثم السبل الممكنة من خلالها مواجهة الهجمات السيبرانية عبر القضاء الجنائي الدولي(فقرة ثانية).

الفقرة الأولى: الاحتكام الى مبدأ الشرعية

تعود الظروف التاريخية التي أنتجت مبدأ شرعية الجرائم والعقوبات، لكون ما يطلق عليه العدالة الموضوعية أدى إلى تعسف القضاة، فأصبح الوضع السائد ينطوي على إهدار لحقوق الأفراد وحرياتهم وايقاع الحيف وعدم المساواة وعدم استقرار لمراكزهم القانونية[2]. يعود الفضل الأكبر في صياغة هذا المبدأ إلى الفقيه الإيطالي "بكاريا" سنة 1764، ثم تواتر فيما بعد، حيث نص عليه إعلان حقوق الإنسان الأمريكي 1776[3]، والإعلان الفرنسي لحقوق الإنسان والمواطن 1789، ثم الإعلان العالمي لحقوق الانسان 1948، والاتفاقية الدولية للحقوق المدنية والسياسية 1966، وأصبح تأخذ به أغلب التشريعات الحديثة العربية والأجنبية[4].

1 نفس المرجع، ص77_79

2 علي عبد القادر القهوجي، مبدأ شرعية الجرائم والعقوبات في القانون الدولي الجنائي، مجلة كلية القانون الكويتية العالمية، دون بيانات العدد، ص 72، الرابط: https://shorturl.at/BR568

3- اعلان حقوق ولاية فرجينيا واحد من اول إعلانات حقوق الانسان غير القابلة للتنازل وحق مقاومة الطغيان وضعت بعناية توماس جيفرسون وجورج ماسون الذي كان احد اكبر مالكي الأرض وأيضا نائبا في الجمعية النيابية لولاية فيلادلفيا.

4 نفس المرجع، ص 71.

لقد قد نص النظام الأساسي للمحكمة الجنائية الدولية صراحة على مبدأ الشرعية الصارمة حيث لا يجوز أن يتحمل الفرد المسؤولية الجنائية بموجب اتفاقية روما إلا إذا كان سلوكه، وقت حصوله، يعتبر جريمة تقع ضمن اختصاص المحكمة[1].

أما معنى هذا المبدأ، فينصرف إلى عدم جواز اعتبار أي فعل من الأفعال جريمة بموجب نظام روما الأساسي، ما لم يكن قد نص على اعتباره كذلك بموجب النظام، مهما كان هذا الفعل خطيراً أو قبيحاً. وأيضا أن توكل مهمة حصر الجرائم وتحديد عقوباتها إلى السلطة التشريعية، فهي الجهة الوحيدة التي يعهد إليها بيان الأفعال التي تُعد جرائم وهي التي تقرّر الجزاء الجنائي، ويتفرّع على ذلك أن تقتصر مهمة القضاء على تطبيق القواعد الجنائية[2]. والجهة التي لها سلطة التشريع، وإحداث مقتضيات جديدة في اتفاقية روما هي جمعية الدول الأطراف[3]. في الواقع اتفقت اللجنة التحضيرية لعام 1996 على الحاجة إلى حكم يعترف بمبدأ عدم ارتكاب جريمة، مستطردة أن" الجرائم التي تدخل في اختصاص المحكمة ينبغي تعريفها بوضوح وبمراعاة الدقة والخصوصية المطلوبة للقانون الجنائي وفقا لمبدأ الشرعية[4].

هناك اتجاه اخر يرى في هذا المبدأ عقبة أمام حق المجتمع وواجبه في مواجهة الأفعال الخطرة اجتماعيا، والتي تلازم التطور الاجتماعي ولا يستطيع القاضي تجريمها[5]. بالإضافة الى

1 تنص الفقرة 1 من المادة 22 من نظام روما: " لا يسأل الشخص جنائياً بموجب هذا النظام الأساسي ما لم يشكل السلوك المعني وقت وقوعه، جريمة تدخل في اختصاص المحكمة."

2 طلال العيسى، مبدأ الشرعية في نظام روما الأساسي لعام 1988، مجلة اتحاد الجامعات العربية، المجلد 12، العدد 1، ص122، الرابط: https://shorturl.at/fklyD

3 انظر المادتين 9 و112 من نظام روما الأساسي.

4- Mark Klamberg, Jonas Nilsson and Antonio Angotti; Commentary on the Law of the International Criminal Court: The Statute; Volume1; Torkel Opsahl Academic EPublisher Brussels; Second Edition; 2023; P713 ; see the link : https://shorturl.at/cdelI

5 علي عبد القادر القهوجي، مرجع سابق، ص74

هذا غالبا ما يكون القانون الجنائي الدولي اكثر غموضا مقارنة بالقانون الجنائي الوطني. هذه مشكلة كانت في قلب الإجراءات في محكمة "نورمبرغ"، حيث لم يتم تعريف الجرائم الدولية بشكل شامل، مما دفع قضاة المحكمة إلى تحديد العديد من أركان الجرائم بأنفسهم، وبسبب موقفهم هذا، تعرضت هذه المحكمة لانتقادات شديدة منها إنشاءها مفهوم جديد لمبدأ الشرعية حيث خلص قضاتها إلى اعتباره "مبدأ أخلاقي"، يسمح بمعاقبة الأفعال التي لم تكن محظورة وقت السلوك في الحالات التي يكون فيها " غير عادل" عدم معاقبة الأفعال.

في حين أن الأمر مختلف في المحكمة الجنائية الدائمة الدولية، حيث تلعب أركان الجرائم دورا مهما في تحقيق أهداف المادة 22. انها تعرف الجرائم التي تدخل في اختصاص المحكمة. ولاحظت الولايات المتحدة في اللجنة التحضيرية الحاجة إلى عنصر الجرائم: لقد اعتبرت أن تحديد أركان الجرائم مسالة تتفق مع "الحاجة إلى تعريف الجرائم بالوضوح والدقة والخصوصية التي تتطلبها الولاية القضائية. كما شددت اليابان أيضا خلال مؤتمر روما على الحاجة إلى أركان الجرائم.

اسفرت هذه المواقف عن جعل تعريفات الجرائم تدخل في نطاق الولاية القضائية للمحكمة على وجه الدقة، من خلال تحديد الأفعال التي تشكل الركن المادي لكل جريمة.

من خلال ما سبق، يتضح أن اللجوء إلى التكييف من أجل تجريم الهجمات السيبرانية إن كان يضمن حقوق الضحايا، والتصدي له يبقى ضروريا من أجل الحد من الآثار الوخيمة للحرب السيبرانية. كما أنه يندرج ضمن الحد من الإفلات من العقاب كهدف تأسست من أجله المحكمة الجنائية الدولية، رغم انه يبقى في تماس مع إرادة الدول الأطراف في نظام روما، ومع بمبدأ الشرعية الصارمة التي كرسها. وقد تقف الدول الأطراف موقف رافضا لخطوة كهذه.

بالإضافة إلى ذلك وفي سياق حماية حقوق المتهم، فإن حظر القياس يرتبط بشكل وثيق مع مبدأ آخر يتعلق بمصلحة المتهم، وهو مبدأ تبناه نظام روما الأساسي. في قضية "فليك ورفاقه" تمسكت محكمة عسكرية أمريكية منعقدة في "نورمبرغ" بالمعيار التالي: "إذا كان من الممكن الوصول إلى استنتاجين معقولين انطلاقًا من دليل موثوق، الأول يدين المتهم والثاني يحكم عليه بالبراءة، يتم اعتماد الاستنتاج الثاني"[1].

تجدر الإشارة إلى أن مبدأ الشرعية هنا كعقبة أمام تجريم الهجمات السيبرانية يقتصر على قواعد النظام الأساسي للمحكمة الجنائية الدولية بحد ذاته، وليس القانون الجنائي الدولي العام [2]. حيث لا تؤثر هذه المادة على تكييف أي سلوك على أنه سلوك إجرامي بموجب القانون الدولي، شريطة ألا تعتبر في حكم ذلك بالنسبة لاتفاقية روما[3].

أما العقبة الأخيرة المرتبطة بمبدأ الشرعية أيضا، تتعلق بحالة القيام بتعديل في نظام روما، وإدراج الهجمات السيبرانية ضمن الأفعال التي تشكل ركنا ماديا لجريمة الحرب حيث أنه لا يمكن تطبيقها بأثر رجعي. إذ لم تكتف اللجنة التحضيرية بتناول الحاجة إلى حكم بشأن مبدأ عدم الشرعية في وقت مبكر من إعداد النظام الأساسي للمحكمة الجنائية الدولية فحسب، بل تناولت أيضا على وجه التحديد الحاجة إلى حكم بشأن عدم الأثر الرجعي، الذي يعتبر أيضا أساسيا لنظام قانوني جنائي، حيث لا يمكن اعتبار سلوك معين غير قانوني إلا إذا كان هذا

1 -هذا يفيد أنه في حالة ما تم التوصل إلى أن فعلا مجرّما بموجب نظام روما قد ينصرف إلى الهجمات السيبرانية، فإن احتمالية هذا التفسير تطرح معها نقيضها، أي أنها قد لا تنصرف إلى ذلك أيضا، وهو الاحتمال الغالب نظرا لأنه عند صياغة اتفاقية روما لم تكن هذه الهجمات مطروحة، وبالتالي يبقى التفسير الأخير هو الأصلح للمتهم أنطونيو كاسيزي، مرجع سابق، ص 94

2 نفس المرجع، ص78

3- الفقرة الثالثة من المادة 22:" 3- لا تؤثر هذه المادة على تكييف أي سلوك على أنه سلوك إجرامي بموجب القانون الدولي خارج إطار هذا النظام الأساسي."

السلوك المحدد محظورا وقت حدوث السلوك[1]. أما بالنظر إلى كيفية إجراء العمليات السيبرانية فالأمر يزداد تعقيدا، حتى مع وجود معلومات شبه كاملة، قد يكون من الصعب تحديد مسؤولية الدولة. إذ أن معرفة موقع وهوية الشبكات والأنظمة المستخدمة لإطلاق أو تسهيل الأنشطة الخبيثة ليست سوى جزء من التحقيق؛ والخطوة الحاسمة هي ضرورة تحديد نية وهوية أولئك الذين يقومون بها. ولسوء الحظ، نادرا ما يكون تحليل المسؤولية عن العمليات التي تحتوي على معلومات شبه مثالية. إذ يتطلب ذلك الوقت والمهارات العالية للوصول إلى ذلك.

hgفقرة hgثانية: حلول لمواجهة الهجمات السيبرانية وضمان المساءلة عن أثارها الوخيمة

خلال بروز قضية "بيغاسوس" التي سلطت الضوء على استخدام تخريب الكمبيوتر كسلاح دبلوماسي جديد اعتبر الباحثين في الأمن السيبراني أن الوقت قد حان لعقد "اتفاقية للفضاء السيبراني"[2]. ومن الأهمية بما كان الترويج لاعتماد اتفاقية جنيف الرقمية لحماية الفضاء الإلكتروني لان العالم اليوم في حاجة اليها[3].

تجدر الإشارة الى ان دولة هولندا استضافت المؤتمر العالمي للفضاء السيبراني لعام 2015، حضرت اليه اطراف متعددة من أصحاب المصلحة هو الأحدث في سلسلة من الجهود الرامية إلى رسم خريطة طريق او بالأحرى إرساء قواعد لتجنب الصراع السيبراني. في البداية

1- هذا ما أكدته أيضا دائرة الاستئناف للمحكمة الجنائية الدولية في قضية علي "محمد علي عبد الرحمن"، حيث ذكرت أنه يتعين على المحكمة عند تفسير الفقرة الأولى من المادة 22 أن تنظر إلى ما هو أبعد من النظام الأساسي وأن تأخذ في الاعتبار تقييم ما إذا كان " الشخص العاقل كان يتوقع، في تلك اللحظة من الزمن، أن يجد نفسه أو نفسها في مواجهة الجرائم المنسوبة إليه.1

2- Ivan Kwiatkowski; « Projet Pegasus » : « La communauté internationale doit se concerter pour élaborer les normes technologiques de demain »; le monde 19 septembre 2021 à 17h00; le lien: https://shorturl.at/vwNZ2

3- Bernard Ourghanlian; Promouvoir une Convention de Genève du numérique pour protéger le cyberespace en temps de paix; microsoft; Publié le 23 janvier 2018; le lien: https://experiences.microsoft.fr/articles/cybersecurite/cyberespace/

يستند الالتزام بهذه السلوكيات أو "القواعد" إلى نهج طوعي، ولكن مع مرور الوقت، كما يعتقد بعض الخبراء يمكن أن تصبح هذه القواعد جزءا لا يتجزأ من القانون الدولي العرفي[1]. كما حدث لكثير من ممارسات الدول التي تواتر عليها الاستعمال حتى استقرت قناعة بأهمية احترامها. فمثلما انتظر العالم طويلا تبني اتفاقية جنيف الرابعة وبروتوكولاتها الاضافية لتحمي المدنيين من وسائل وبعض أساليب القتال المذمومة في أوقات الحرب، فقد آن الأوان إلى استصدار اتفاقية جنيف الرقمية تلزم الحكومات بحماية المدنيين من هجمات سيبرانية للدول القومية في أوقات السلم. ومثلما اعترفت اتفاقية جنيف الرابعة بأن حماية المدنيين تتطلب مشاركة نشطة من الصليب الأحمر الدولي، فإن الحماية من الهجمات الإلكترونية للدول القومية تتطلب مساعدة نشطة من شركات التكنولوجيا، لان هذا القطاع يلعب دورا فريدا كأول المستجيبين للإنترنت، وبالتالي يجب الالتزام بالعمل الجماعي الذي سيجعل الإنترنت مكانا أكثر أمانا مع التأكيد على دور سويسرا الرقمية المحايدة التي تساعد العملاء في كل مكان وتحتفظ بثقة العالم[2]. رغم كونه مطلبا معقولا، فان تحقيقه يتطلب إرادة سياسية والتزاما قويا من القادة في جميع أنحاء العالم[3]. هذا نموذج دولة إلى دولة تتفاوض فيه البلدان على المعاهدات، لكن المشكلة فيما يخص الهجمات الالكترونية هي أن الفضاء الإلكتروني كان له تقليديا أصحاب مصلحة آخرون، بما في ذلك الشركات الخاصة. اما بالنسبة لنظام روما، فبإمكان الدول التفاعل بطريقة إيجابية مع الاقتراح الذي يقدمه بعض الخبراء في القانون الدولي الجنائي والقانون الدولي الإنساني وهو الذي يقضي بإدخال تعديل على نظام روما مادام انه هو بنفسه يجيز هذه الخطوة. ففي كل خمس سنوات يُعقد مؤتمر لمراجعة عمل المحكمة ونظامها الأساسي

1 - JOSEPH S. NYE, JR; Les normes internationales au sein du cyberespace; project-syndicate; publié: 11-mai-2015; le lien: https://shorturl.at/ktuJM

2- Brad Smith; The need for a Digital Geneva Convention; Microsoft; Feb 14, 2017; link: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

3 - مع ذلك، فقد تم بالفعل وضع بعض الأسس الهامة وتوفر نقطة انطلاق لإنشاء إطار قانوني دولي فعال.

ويمكن لأي دولة طرف في نظام روما الأساسي أو الجمعية العامة للأمم المتحدة أن تقترح تعديلات على النظام الأساسي يتم اعتمادها بأغلبية ثلثي الدول الأطراف الحاضرة والمشاركة في التصويت. كما يمكن لأي دولة طرف في نظام روما الأساسي أن تقترح تعديلات على النظام الأساسي في أي وقت. ويتم إرسال الاقتراح إلى الأمين العام للأمم المتحدة، الذي ينقله إلى جميع الدول الأطراف، حيث يصبح ملزما إذا تم اعتماده للدول التي تقبله[1] . بطبيعة الحال، يبدو ان مجرد تعديل جملة أو جملتين في بعض بنود نظام روما الأساسي سيكون أفضل بكثير من الاضطرار إلى إنشاء محكمة جديدة تمامًا، الا انه من الناحية العملية تعتبر عملية تعديل مقتضيات النظام معقدة.

انه الأمر الذي يزيد المسالة تعقيدا حيث يلزم في هذا الإطار تعاون الدول من أجل إحداث مقتضيات كفيلة بقمع الهجمات السيبرانية مادامت تشكل خطرا يهدد الجميع دولا، أفرادا، وشركات؛ وان الأمر يتعلق بنزاع مسلح بين الدول قادرة على استخدام سلاح قوي قد يتوفر عليه الجميع على قدم المساواة في ظل انتشار الأجهزة الإلكترونية بشكل واسع النطاق حول العالم. من السبل او الاستراتيجيات التي قد يعوّل عليها هي ان تجتمع منظمات المجتمع المدني المعنية والمدافعة عن حقوق الإنسان على المستوى المحلي والدولي في اطار تحالف دولي وتمارس الضغط كسلاح لكسب المعارك في مكافحة الإفلات من العقاب عن جريمة الحرب السيبرانية[2].

1 تنص الفقرة الأولى من المادة 122: " يصبح أي تعديل على المادة 5 من هذا النظام الأساسي نافذاً بالنسبة إلى الدول الأطراف التي تقبل التعديل , وذلك بعد سنة واحدة من إيداع صكوك التصديق أو القبول الخاصة بها , وفي حالة الدولة الطرف التي لا تقبل التعديل , يكون على المحكمة ألا تمارس اختصاصها فيما يتعلق بجريمة مشمولة بالتعديل عندما يرتكب هذه الجريمة مواطنون من تلك الدولة أو ترتكب الجريمة في إقليمها."

2 - ان الشواغل الإنسانية المرتبطة بالحرب السيبرانية تشغل منذ فترة اللجنة الدولية للصليب الأحمر تماما كما شغلتها كثيرا أنواع أخرى الأسلحة كانت تظهر بشكل مستمر كالأسلحة النووية والأسلحة الخفيفة والالغام المضادة للأفراد... الخ ذلك ان قلق المنظمة متزايد بسبب ترابط الفضاء الالكتروني وعدم قدرة الطرف المهاجم على التمييز دائما بين أنظمة الحواسيب العسكرية والمدنية ولصعوبة تقييم التأثيرات على غير المباشرة على شبكات الحاسوب المدنية.

خلاصة الدراسة:

إن الحرب السيبرانية/الالكترونية أصبحت حقيقة قائمة ولا يمكن مع ذلك استبعاد انها ذات تكلفة مادية وبشرية ملموسة رغم ان دولا تمتنع حتى الآن عن وصف كل العمليات السيبرانية المقترنة بأعمال عدائية بأنها نزاع مسلح دولي أو غير دولي. ثم ان اغلب الهجمات تحدث تحت عتبة استخدام القوة أي تقع فيما يسمى" المنطقة الرمادية" كما في حالة نشر فيروس "ستوكسنت" لزعزعة نظام عمل المنشآت النووية الإيرانية. حتى دليل "تالين" الذي اعتمدته الدول قد لا يجد قبولا عالميا على محتواه، ليس فقط لأنه قانون غير ملزم، بل أيضا لأنه يعكس وجهة نظر غربية خالصة بسبب عدد الخبراء الفنيين والمراقبين المشاركين في صياغته ذلك ان معظمهم ينحدر من الولايات المتحدة الامريكية وأروبا الغربية. على الرغم من كل هذه المعيقات، فان القانون الدولي الإنساني لا يزال منطبقًا على كافة الأنشطة التي تقوم بها الأطراف أثناء النزاع. مع ذلك هناك حاجة إلى تطوير القواعد القانونية الموجودة لمواكبة تطور التكنولوجيا السيبرانية لتقليص تأثيرها غير المحمود ولضمان توفيرها الحماية الكافية للأعيان المدنية وللسكان المدنيين. من جهة أولى، لا ينبغي أن يكون الفضاء السيبراني بمنأى عن التنظيم، لأن للقانون الدولي دورا رئيسيا يؤديه. وبما أن الحرب السيبرانية تتقاطع مع النزاع المسلح، فمن الأهمية بما كان الالتزام بقواعد القانون الدولي الإنساني اثناء العمليات السيبرانية التي ترتكب اثناء نزاع مسلح سواء كان بين دول او بين دول وجماعات معارضة مسلحة ومنظمة طالما ينظر اليها "كوسيلة او كأسلوب" حرب. من جهة ثانية، إذا كان مقبولا ان ينطبق القانون الدولي الإنساني على هذا النوع الجديد من السلاح كما هو الحال لأي تقنية جديدة، فعلى القضاء الجنائي الدولي- باعتباره مكملا للقضاء الجنائي الوطني لمحاكمة وزجر كل الأفعال التي يعتبرها القانون الدولي شديدة الخطورة بما فيها الهجمات السيبرانية في سياق نزاع مسلح او التي تؤدي بنفسها الى نزاع مسلح متسببة في الايذاء والضرر- ان يدخلها في دائرة اجتهاده. يتوجب على

محكمة روما ان تحول تركيزها من الحرب التقليدية نحو العالم الافتراضي الذي ترتكب فيه انتهاكات حقوق الانسان بواسطة عمليات الكترونية تساهم في تحقيق ميزات عسكرية على حساب المبادئ الأساسية للقانون الدولي الانساني او حتى بإهدارها. وينبغي لمكتب المدعي العام أيضا أن يلعب دورا داعما أو تنسيقيا، ليس فقط في التحقيق من أجل الملاحقة القضائية أمام المحكمة الجنائية الدولية، ولكن أيضا في دعم الدول والمنظمات الأخرى وتشجيع التعاون بين كل هذه الاطراف والتعاون وتعزيز الشراكات ليس فقط مع الدول ولكن أيضا مع الشركات. انه مطلب مشروع يخدم حماية ضحايا النزاعات والعاملين في المجال الإنساني ويحتمل ان يحد من التداعيات الخطيرة للحرب السيبرانية واثارها التي لا تقتصر على الأنظمة والحواسيب المستهدفة بالهجوم، إنما تتعداها الى العالم الحقيقي. على أي حال، فإن العمليات السيبرانية ستشكل حتما تحديات صعبة لتصنيف النزاعات بالنسبة للدول في المستقبل. ففيما يتعلق بالنزاعات المسلحة الدولية، من المرجح أن يكون إسناد العمليات السيبرانية التي تنفذها جهات فاعلة من غير الدول أكثر إشكالية من إسناد الأفعال الحركية إلى الدول في الماضي. ففي سياق نزاع مسلح غير دولي، سيزداد تعقيد التوصيف كجماعة مسلحة منظمة مع تطور هياكل التنظيم الافتراضي ووسائله وانتشاره. أن التهديدات السيبرانية هي مشاكل عالمية وتحتاج إلى تنسيق عالمي يشمل الجميع أصحاب المصلحة: فالدول مطالبة بالتعاون وحشد الجهود الكافية والاستثمار في البحث لتطوير تقنيات لتحديد مصدر التهديدات السيبرانية ومنعها. اما وسيلتها نحو تحقيق هذا المسعى، فتتمثل في تعزيز الحوارات بين الحكومات والقطاع الخاص بشأن التدابير الأمنية في الفضاء السيبراني بالعمل على وضع معاهدة أو مجموعة معاهدات بشأن أمن الفضاء الحاسوبي تكون بمثابة نموذج عالمي لأمن الفضاء الحاسوبي وصياغة تشريعات جرائم الفضاء الحاسوبي تكون قابلة للتطبيق وقابلة للتنفيذ المتبادل مع التدابير التشريعية الوطنية والإقليمية القائمة.