**المراجعات القانونية لتعريف الأسلحة السيبرانية**

[**العدد 117 - تموز 2021**](https://www.lebarmy.gov.lb/ar/content/117-d)

**المراجعات القانونية لتعريف الأسلحة السيبرانية**  
إعداد: العقيد الركن البحري علي حمية  
ضابط في الجيش اللبناني

**المقدمة**

أثار مراسل نيويورك تايمز David Sanger ضجة كبيرة داخل مجتمع القانون السيبراني حين أعلن في حزيران 2012 أن حزمة برامج ضارة ذات تعقيد غير مسبوق استهدفت وبشكلٍ فعال برنامج الأبحاث النووية الإيرانية، كما تم اكتشاف البرنامج الذي عُرف لاحقًا باسم Stuxnet على العديد من أنظمة الكمبيوتر خارج إيران لكنه لم يسبب أي ضرر لها، وفي مقابلة مع السيد Sanger أشارت الصحيفة إلى أن البرنامج الضار كان جزءًا من خطة أميركية وعملية إلكترونية سرية، وقد استرعى التأكيد أن دولة ما استخدمت هجومًا إلكترونيًا لدعم أهدافها الوطنية انتباه العاملين على القانون الإلكتروني داخل الحكومات وخارجها.

ما جعل Stuxnet مثيرًا للاهتمام هو أن الوظيفة الأساسية له سهلة الفهم والتصنيف، فقد أُدخل في الأنظمة المستهدفة بهدف إحداث ضرر مادي للعتاد، كما أن التحليل القانوني له ذو فائدة كبيرة عند تقييم الأنشطة السيبرانية، فالنقص الواضح في التأثيرات المادية أو الجسدية هو سمة العمليات السيبرانية بينما آثار Stuxnet كانت كارثية على إيران وبرنامجها النووي وأدت إلى تعقيد التحليل القانوني السيبراني في سياق العمليات العسكرية.

تشير مصطلحات الحرب الإلكترونية ضمنًا إلى استخدام الأسلحة السيبرانية في هذه الحروب، لكن عدم اليقين في تحديد هذا المصطلح يؤدي إلى عدم يقين متساوٍ في تحديد الأسلحة السيبرانية، وارتباك كبير حول متى يكون استخدام سلاح إلكتروني بمثابة هجوم يؤدي إلى حالة من الحرب الإلكترونية، لذلك بدأ العمل على تعريف السلاح السيبراني بشكلٍ قانوني واستنباط أحكامه القانونية ثم استخدام ذلك لاكتساب فهم أفضل للحرب والأسلحة الإلكترونية.

الغرض من هذه المقالة هو تسليط الضوء على تأثير القانون السيبراني في العمليات العسكرية وترجمة المناقشات الأكاديمية والنظرية إلى مشورة قانونية ملموسة، كما تسلّط الأمثلة الفعلية للقدرات والعمليات السيبرانية التي حدثت في الآونة الأخيرة الضوء على القضايا التي تنطوي عليها عمليات الفضاء السيبراني، بهدف تحليلها في ظل النظام القانوني المتعلق بالأسلحة ووسائل الحرب وأساليبها. تخلص هذه المقالة إلى أن التعامل مع جميع التقنيات السيبرانية على أنها أسلحة هو استنتاج غير عملي وفي غير محله، والتقييم الذي يركّز على كيفية استخدام القدرة السيبرانية لا سيما الهدف الأساسي لاستخدامها يكون أكثر دقة لتحديد ماهيتها (أسلحة أم لا) ويتوافق مع القانون الدولي بشكلٍ أكثر فعالية وموضوعية.

ما لا تعالجه هذه المقالة هو مناقشة الفرق بين العمليات السيبرانية التي ترعاها الدولة والجرائم الإلكترونية، فالتمييز بين استخدامات الدولة للفضاء السيبراني وعمليات الجماعات الإجرامية باستخدام هذا الفضاء من خلال فحص التفاصيل الفنية للحوادث الإلكترونية معقد للغاية، ولا يمكن تحديد ذلك إلا من خلال فهم دوافع الطرف المسؤول عن العملية الإلكترونية وتقييمها.

**أولًا: ما هو التجسس الإلكتروني؟**

التجسس الإلكتروني هو شكل من أشكال الهجوم الإلكتروني الذي يهدف إلى سرقة بيانات سرية أو حساسة أو ملكية فكرية للحصول على ميزة لشركةٍ أو كيان حكومي منافس، وبحسب قاموس ميريام Merriam Webster التجسس هو «استخدام الجواسيس بهدف الحصول على معلومات مهمة حول خطط وأنشطة خاصة بحكومةٍ أجنبية أو شركة منافسة»[[1]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftn1" \o ").

في عالم الإنترنت، الجواسيس هم جيوش من المتسللين من أنحاء العالم كافة يستخدمون الحرب والوسائل الإلكترونية لتحقيق مكاسب اقتصادية أو سياسية أو عسكرية. هؤلاء المجرمون الإلكترونيون ذوو القيمة العالية لديهم المعرفة والقدرة التقنية لاختراق البنى التحتية الحكومية كما الأنظمة المالية والعقارية أو موارد المرافق كالمطارات والموانئ وغيرها، وقد استطاعوا التأثير في نتائج الانتخابات السياسية في عدة دول (اتهام الولايات المتحدة الأميركية روسيا بالتدخل في نتائج الانتخابات التي أدت إلى فوز ترامب)، وأحدثوا الفوضى الدولية كما وساعدوا الشركات على النجاح أو الفشل. يستخدم العديد من هؤلاء المهاجمين التهديدات المستمرة المتقدمة APTs) Advance Persistent Threats)[[2]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftn2" \o ") كطريقة عمل للدخول خلسة إلى الشبكات أو الأنظمة للشركات والدول والبقاء لسنواتٍ من دون أن يكتشفهم أحد.

تنص المادة 29 من اتفاقية لاهاي للعام 1907 على أنه لا يمكن اعتبار الفرد جاسوسًا لمصلحة دولة معينة إلا إذا حصل أو سعى للحصول على معلومات في منطقة عمليات العدو وذلك بتصرفه سرًا وبقصد إبلاغ الطرف المعادي بها، وبالتالي فإن الجنود غير المتخفين الذين يتوغلون في منطقة عمليات جيش معاد للحصول على معلومات عسكرية أو استخباراتية لا يُعَدون جواسيس، كما لا يُعد جواسيس الجنود أو المدنيوين التابعون لدولةٍ معينة والذين يقومون بمهامهم علانية أو يكونون مكلفين بتسليم رسائل موجهة إما لجيشهم أو لجيش العدو.

تنص المادة 46 (2) من البروتوكول الإضافي الأول للعام 1977 على أنه لا يُعد منخرطًا في التجسس أفراد القوات المسلحة لطرفٍ في نزاع معين ويقوم بتكليفٍ من ذلك الطرف وفي إقليم يسيطر عليه الخصم بجمع معلومات أو محاولة جمعها بالزي الرسمي لقوات بلاده المسلحة[[3]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftn3" \o ").

**ثانيًا: دليل تالين Tallinn Manual**

نشرت مجموعة من الخبراء القانونيين والعسكريين دليلًا يعرف بـدليل تالين وهو وثيقة غير ملزمة للدول، وساهمت فيها اللجنة الدولية للصليب الأحمر بصفة مراقب. تشير هذه الوثيقة إلى أن القانون الدولي الإنساني ينطبق على الحرب السيبرانية كما هي الحال مع الحروب التقليدية ويحدد الدور الذي ستؤديه قواعد القانون الدولي الإنساني في هذا المجال.

بالنسبة للمستشارين القانونيين وصانعي السياسات والقادة العسكريين المهتمين بالقانون الدولي من حيث صلته بالأسلحة الإلكترونية، فإن دليل تالين يمثّل نقطة انطلاق مهمة لتحليل كيفية تطبيق القانون الدولي الإنساني على العمليات والأسلحة السيبرانية. يتناول دليل تالين للعام 2017 مسألة مراجعة الأسلحة السيبرانية، بالإضافة إلى العديد من القضايا الحيوية الأخرى ذات الصلة بهذا المجال في ما يقرب 600 صفحة من القواعد والتعليمات المرتبطة بالقانون الدولي العام.

لتقدير أهمية دليل تالين في المجال السيبراني من الضروري تقديم السياق التاريخي لهذا الدليل وبإيجاز؛ ففي العام 2009، دعا مركز التعاون للدفاع السيبراني التابع لحلف الناتو NATO Cooperative Cyber Defence Centre of Excellence وهو مؤسسة شهيرة للبحث والتدريب الدفاعي عبر الإنترنت في مدينة تالين بإستونيا مجموعة من الخبراء السيبرانيين المستقلين لإعداد دليل حول القانون الدولي الذي يجب أن يحكم الأنشطة الإلكترونية في أثناء الحروب أسوة بالأنشطة التقليدية. جمع هذا المشروع مجموعة متميزة من القادة العسكريين والباحثين والممارسين في القانون الدولي - مجموعة الخبراء الدوليين - لدراسة كيفية تطبيق القواعد القانونية المرتبطة بالحرب الإلكترونية وتوضيحها، وفي العام 2013 نُشرت النسخة الأولى من دليل تالين للقانون الدولي وأصبح المرجع الوحيد في هذا المجال وبنتيجة النجاح الذي حققه الدليل الأول بدأ المركز المذكور أعلاه CCD COE مشروع متابعة لتوسيع نطاق التغطية بدليلٍ محدث ومطور ليشمل القانون الدولي الذي يحكم الأنشطة الإلكترونية خلال وقت السلم.

شاركت مجموعة ثانية من الخبراء السيبرانيين أكثر تنوعًا وأدى عملهم إلى إنشاء النسخة الثانية المحدثة من دليل تالين في شباط 2017 وتعميمها. شمل الدليل الموسع بشكلٍ كبير مواد من دليل تالين الأول وأخرى لتغطية الأطر القانونية للقوى المتورطة في الأنشطة والحوادث الإلكترونية في وقت السلم، وقد احتوى الدليل على 154 قاعدة أهمها القاعدة 110 المتعلقة بعملية مراجعة الأسلحة بموجب القانون الدولي الإنساني. يقدّم التعليق التفصيلي لكل قاعدة بعض الأفكار المهمة في ما يتعلق بالأساس القانوني وتبرير القواعد وسياقها، كما أنه يقدّم أيضًا تبريرًا لآثار عملية تطبيق القواعد في السياق السيبراني لناحية النتائج الميدانية للسلاح والعواقب القانونية المترتبة عليها. هذا المستوى من الدخول في التفاصيل مفيد بشكلٍ خاص للمستشارين القانونيين والأكاديميين، بالإضافة إلى ذلك يوضح الدليل تبريرات الخبراء لشرح القواعد القانونية ومواقفهم منها عند التوصل إلى اتفاق، كذلك الأمر عندما لا يتمكنون من التوصل إلى توافق في الآراء بشأن قضية معينة، إضافة إلى إبراز أسباب عدم التوافق بهدف فهم السياق القانوني للتوافق أو عدمه.

**في مراجعة الأسلحة تنص القاعدة 110 في دليل تالين على ما يأتي:**

• يُطلب من جميع الدول ضمان امتثال وسائل الحرب الإلكترونية التي تحصل عليها أو التي تستخدمها لقواعد قانون النزاع المسلح الملزمة.

• يُطلب من الدول الأطراف في البروتوكول الإضافي الأول دراسة وسائل الحرب الإلكترونية وطرقها لتحديد ما إذا كان استخدامها، في بعض أو جميع الظروف، محظورًا بموجب ذلك البروتوكول أو بموجب أي قاعدة أخرى من قواعد القانون الدولي.

هناك ما لا يقل عن ست نقاط يجب الإضاءة عليها في ما يتعلق بالقاعدة 110:

1- يجب قراءة القاعدة 110 من دليل تالين من منظور فتوى محكمة العدل الدولية بشأن الأسلحة النووية، فقد أكدت هذه المحكمة فكرة أن القانون الدولي الإنساني ينطبق على الأسلحة الجديدة كما القديمة. على الرغم من اختراع الأسلحة السيبرانية بعد ظهور غالبية مبادئ القانون الدولي الإنساني وقواعده إلا أنه من الخطأ استنتاج أن القانون الدولي الإنساني لا ينطبق عليها، بالإضافة إلى ذلك وكما لاحظت محكمة العدل الدولية سيكون من غير المتوافق مع الطابع الإنساني الجوهري للمبادئ القانونية في القانون الدولي الإنساني بكامله الاعتقاد أن هذا القانون لا ينطبق على الأسلحة الجديدة. وبالمحصلة يُطبَّق القانون الدولي الإنساني على جميع أشكال الحرب الإلكترونية أو التقليدية وعلى كل أنواع الأسلحة الموجودة في الماضي والحاضر والتي يمكن اختراعها في المستقبل.

2- تعزيزًا للنقطة أعلاها، فإن تصنيف أي عتاد مستخدم في الحرب أو السلم كسلاحٍ إلكتروني يعني أيضًا أن هذا السلاح وفي أي وقت من الأوقات يجب أن يمتثل للقانون الدولي الإنساني.

3- الفقرة الفرعية (أ) تعكس القانون الدولي العرفي وتنبع من واجب عام للامتثال للقانون الدولي الإنساني. الفقرة الفرعية (ب) مشتقة من المادة 36، فالالتزامات المبينة في هذه الفقرة لا تقتصر على القانون الدولي الإنساني ولكنها تمتد لتشمل القانون الدولي بأكمله، فهي أوسع وأشمل بكثيرٍ من تلك الواردة في الفقرة الفرعية (أ).

4- الفقرة الفرعية (ب) لا تحدد ولا تتطلب منهجية معينة لإجراء مراجعة للأسلحة السيبرانية، لذلك فإن الدول ليست ملزمة بنشر مراجعات أسلحتها على الملأ وهذا الأمر يُعد وثيق الصلة بشكلٍ خاص في سياق الأسلحة السيبرانية بسبب الطبيعة السرية للغاية لهذه الأسلحة. كما هو الحال في جميع عمليات استعراض الأسلحة وفق القانون الدولي الإنساني، فإنه يجب تحديد شرعية السلاح السيبراني بالرجوع إلى استخدامه الطبيعي والمتوقع وقت التقييم.

5- إذا استلمت دولة ما سلاحًا إلكترونيًا من دولة أخرى لاستخدامه في عملياتها السيبرانية المستقبلية، فإن حقيقة أن الدولة الموردة للسلاح قد أجرت مراجعة لا تعفي الدولة الحائزة من التزاماتها في ما يتعلق بذلك السلاح السيبراني. يجوز للدولة المقتنية النظر في المراجعة التي أجرتها الدولة الموردة، ويجب عليها الوفاء بالتزاماتها بموجب القانون الدولي الإنساني.

6- في ما يتعلق بما يجب مراجعته، بالنسبة إلى الدول الأطراف في البروتوكول الإضافي الأول، للإجابة عن سؤال ما الذي يشكل على وجه التحديد أسلحة أو وسائل أو طريقة إلكترونية، يمكن القول إن كل الدول بغض النظر عما إذا كانت قد صدّقت على البروتوكول الإضافي الأول أم لا، فهي مطالبة بإجراء تقييم منهجي لشرعية الأسلحة والوسائل والأساليب الجديدة التي تملكها. ينبع هذا الالتزام منطقيًا من واجب عام متعارف عليه هو الامتثال للقانون الدولي الإنساني وحقيقة أن الدول ممنوعة من استخدام أسلحة أو وسائل أو أساليب حرب غير مشروعة وتتنافى مع شرعة حقوق الإنسان.

**ثالثًا: التجسس والعمليات السيبرانية**

من أولى القضايا التي تواجه العمليات السيبرانية التمييز بينها وبين التجسس. وفي حين أن هناك اتفاقية Gentleman’s Agreement طويلة الأمد بين الدول لتجاهل التجسس في القانون الدولي، إلا أن تحديد الإجراءات الإلكترونية التي تشكل تجسسًا يمثل تحديًا حقيقيًا بسبب أوجه التشابه بين التجسس الإلكتروني والهجوم الإلكتروني في ساحة العمليات ويبدو أن خبراء الإنترنت وصناع السياسات عازمون على استبعاد التجسس من الاعتبار نفسه الذي تحظى به العمليات الإلكترونية[[4]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftn4" \o ").

غالبًا ما تكون تقنيات التجسس الإلكتروني والهجوم الإلكتروني متطابقة، وعادة ما يكون التجسس شرطًا ضروريًا للهجوم، فهناك قدرة ضئيلة أو معدومة على التمييز بين التقنيات الإلكترونية المستخدمة في التجسس وتلك المستخدمة في الهجوم الإلكتروني، ففي الأخيرة وبمجرد أن يسيطر الخصم على جهاز الكمبيوتر يمكنه أن يفعل ما يريد كسرقة المعلومات (أحد أنواع التجسس)، أو تعطيل النظام أو تدميره.

التجسس السيبراني ليس مجرد نسخ للمعلومات من نظام ما فهو يتطلب عادة شكلًا من أشكال المناورة الإلكترونية التي تجعل من الممكن سرقة المعلومات المستهدفة، وقد تفرض إجراء يجب اتخاذه بهدف تعطيل النظام للوصول إلى المعلومات، فعلى سبيل المثال يمكن تنفيذ عملية لإضعاف التشفير أو تعطيل القدرة الإلكترونية للهدف لإجباره على استخدام نظام بديل يؤمّن وصولًا أسهل إلى قاعدة بياناته وفك تشفيره، وبمجرد اختراق النظام يمكن للمالك الجديد له اتخاذ أي إجراء من معالجة البيانات وسرقتها إلى تدمير البرنامج وفي بعض الحالات تدمير الأجهزة فعليًا، ولا يمكن للضحية معرفة ما إذا كان المستخدم غير المصرح له يهدف إلى التجسس أو تعطيل النظام أو تدميره.

غالبًا ما يكون الاختلاف الوحيد بين العمليات التي تهدف إلى جمع المعلومات الاستخبارية (التجسس) وتلك المصممة لإيصال التأثيرات الإلكترونية (التعطيل أو التدمير) هو النية الكامنة خلف هذا الإجراء، فالأولى تتم بقصد جمع المعلومات وبطرقٍ متعددة، بينما الثانية لدعم التخطيط العملياتي أو تنفيذ العمليات العسكرية التقليدية. بعض الدعم يكون مباشرًا كجمع المعلومات حول التمركز المسبق لقوى العدو أو الإمدادات الاستراتيجية التي يستخدمها في حقل المعركة، الدعم الآخر غير مباشر كتدريب جيوش الدول الشريكة أو الدعم المتبادل مع الدول الصديقة. معظم أنشطة الدعم غير مثيرة للجدل من منظور قانوني على الرغم من أنه قد يتم إجراؤها في الخفاء ضمن الدولة ومن دون موافقتها وبشكلٍ مشابه للتجسس[[5]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftn5" \o ").

هذا الانقسام في أنشطة الفضاء الإلكتروني يجعل تقديم المشورة القانونية للقادة العسكريين أكثر تحديًا مما هو عليه في العمليات العسكرية التقليدية، فالنشاط الإلكتروني غير مثير للجدل عندما يكون الهدف الأساسي هو جمع المعلومات أو الوصول إليها، بينما يمكن تعريف النشاط الذي يُجرى لغرضٍ آخر غير جمع المعلومات الاستخبارية على أنه هجوم بـسلاحٍ يتطلب تحليلًا شاملًا تشارك فيه كل فروع الدولة. قد يؤمّن تعريف السلاح الإلكتروني أساسًا لتحديدٍ موضوعي لطبيعة الأنشطة في الفضاء السيبراني.

**رابعًا: تحديات قانون العمليات السيبرانية**

تُعرِّف وزارة الدفاع الأميركية الفضاء الإلكتروني بأنه مجال من صنع الإنسان[[6]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftn6" \o ")، وتعتبر أن عملياته العسكرية تمزج بين قضايا الجغرافيا والسيادة والقانون والحقوق المدنية بطرقٍ تتخطى الحدود القانونية التقليدية ويجب مقاربتها بطريقةٍ مختلفة.

يرتاح المحللون القانونيون العسكريون لمناقشة مفاهيم الحرب في مجالات الحرب البرية أو الحرب الجوية أو الحرب البحرية، ولكن لا يبدو أن الاستخدام الشائع لتلك المفاهيم قد انتقل إلى الحرب الإلكترونية على الرغم من استخدام مصطلحَي الحرب والهجوم في سياق إلكتروني على نطاق واسع في العمليات العسكرية، فعلى سبيل المثال، يستخدم مصطلح الحرب الإلكترونية لوصف استخدام المجال السيبراني والهجمات الإلكترونية لإجراء عمليات عسكرية، تتراوح من الهجوم السيبراني ضد المواقع اللوجستية إلى تنفيذ الهجمات العسكرية العنيفة.

بسبب طبيعتها قد يكون من الصعب تصنيف عمليات الفضاء الإلكتروني ضمن نطاق العمليات العسكرية، ولا يزال السؤال الأساسي حول متى تُنتهك المادة 51 أو المادة 2(4) من ميثاق الأمم المتحدة، فالمجتمع الدولي يواصل تحليل الحوادث السيبرانية على أساس كل حالة على حدة مع التركيز على ما إذا كان النشاط الإلكتروني يشكل استخدامًا محظورًا للقوة بموجب المادة 2(4) أو هجومًا مسلحًا من شأنه أن يولد الحق في ممارسة الدفاع عن النفس على النحو المنصوص عليه في المادة 51.

بالاعتماد على دليل تالين Tallinn Manual ومع الهجوم السيبراني المعروف باسم Stuxnet كمثالٍ رئيسي، من السهل التمييز بين العمليات الإلكترونية الموازية لـهجومٍ مسلح بموجب المادة 51 من ميثاق الأمم المتحدة وتلك التي لا توازي الهجوم المسلح، وقد يكون السؤال الأكثر أهمية، هل تشكل هذه العمليات استخدامًا للقوة بموجب المادة 2(4) من ميثاق الأمم المتحدة أم لا؟

التحليل الأكثر اكتمالًا لتحديد طبيعة العمليات السيبرانية كهجومٍ هو اختبار أجراه أحد الباحثين وهو البروفيسور شميت مكون من ست نقاط، والذي يحاول من خلاله تصنيف الحالات عند اعتبار استخدام الفضاء الإلكتروني كاستخدامٍ للقوة بموجب المادة 2(4)، هذا الاختبار يأخذ بعين الاعتبار عناصر الخطورة الفورية والمباشرة والغزوية والقابلية للقياس والشرعية. عند تطبيق هذه المعايير لتحديد قانونية الهجوم، يأخذ البروفيسور شميت في الاعتبار عواقب الهجمات الإلكترونية لتقييم اعتبارها مساوية لهجومٍ تقليدي مسلح[[7]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftn7" \o ").

هناك مجموعة من العمليات السيبرانية لا ترقى إلى مستوى الهجوم المسلح، ولا تعتبر استخدامًا للقوة بموجب القانون الدولي، كما لا يمكن اعتبارها تدخلًا في قدرة الدولة على ممارسة سيادتها، لكنها تشكل خرقًا للسلام، وتكون هذه العمليات قسرية وغير مرحب بها وقد تكون موضوع اعتراض دبلوماسي وتخضع لإجراءاتٍ من قبل مجلس الأمن الدولي. بالنسبة إلى هذه الإجراءات السيبرانية ومن أجل تطوير أساس قانوني يشرّع العمليات العسكرية السيبرانية يجب الاقتناع أن هناك مجموعة فرعية من أنشطة الحرب الإلكترونية لا تُعد هجمات سيبرانية ولا تشكل شكلًا من أشكال الحرب وتتوافق مع القانون الدولي. يُطبق هذا المنطق على التجسس الإلكتروني، على الرغم من أنه عند فحص التقنيات الفعلية المستخدمة، فإن التمييز بينه وبين العمليات الإلكترونية ليس واضحًا ويشكل معضلة يجب النظر فيها.

يؤدي الفشل في الوصف الدقيق لما هو سلاح إلكتروني وما ليس سلاحًا إلكترونيًا إلى زيادة صعوبة تحديد الدول التي تلتزم بالقانون الدولي وما يجب أن تفعله لضمان امتثال أنشطتها الإلكترونية لقانون الحرب. يساعد النهج العقلاني لتحليل الحرب السيبرانية في توضيح القواعد القانونية بطريقةٍ تدعم العمليات العسكرية في الفضاء الإلكتروني. ويشمل ذلك تحليل الآلية والتقنيات المستخدمة في بعض الحوادث السيبرانية، والتي تسلط الضوء على صعوبة تطبيق التفاصيل الأكاديمية النظرية في العمليات السيبرانية الحقيقية.

**خامسًا: أمثلة على الهجمات السيبرانية**

تُعد أنظمة التحكم واكتساب البيانات Supervisory Control and Data Acquisition (SCAD A)A[[8]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftn8" \o ") مجالًا أساسيًا للاعورار الوطني السيبراني، فهي تتحكم بأنظمة المرافق والنقل والتصنيع وتديرها. من بين المخاطر المحدقة بها أنه قد يتم التلاعب بهذه الأنظمة للتدخل في عمل القطاعات (توزيع الكهرباء، الوقود، التشغيل السليم للقطارات والموانئ البحرية، تصنيع الآلات الثقيلة...)، وقد أدى الاعتراف بالتهديد الذي تتعرض له هذه الأنظمة إلى قيام الولايات المتحدة الأميركية إلى إنشاء فريق الاستجابة للطوارئ السيبرانية لأنظمة التحكم الصناعي (ICS-CERT)[[9]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftn9" \o ") تحت إشراف وزارة الأمن الداخلي لتعزيز الدفاع عن هذه الأنظمة كون تفاصيل أي عمليات سيبرانية فعلية تصنف سرية فإن الأمثلة أدناها هي عمليات إلكترونية مفتوحة المصدر ومتاحة للجميع ويمكن الاستدلال منها على كيفية استخدام قدرة إلكترونية في هجوم إلكتروني.

**Stuxnet:** هو الاسم الذي يطلق على جزء متطور من رمز كمبيوتري Code يهدف إلى الانتشار عن طريق استخدام ميزة التشغيل التلقائي Auto Run ضمن الشبكة العنكبوتية، وصُمم ليكون قادرًا على القيام بوظائف متعددة، فبمجرد تثبيته يحدد النظام المضيف ويطور خرائط الشبكة المضيفة ويوزع نسخًا عنها كما لديه القدرة على الإبلاغ عما وجده.

في الحالة الإيرانية، أُدخل البرنامج إلى نظام تشغيل أجهزة الطرد المركزي لمعالجة اليورانيوم، وتسببت البرمجيات الخبيثة في تسريع هذه الأجهزة التي تدور بسرعةٍ تفوق سرعة الصوت أو إبطائها، وهذه التغييرات المفاجئة في السرعة أدت إلى تعطيلها، وبالتوازي كان مكون آخر من البرنامج يتسبب في قيام برنامج المراقبة الإلكتروني الإيراني بالإبلاغ عن أن أجهزة الطرد المركزي تعمل بشكلٍ صحيح ما منع اكتشاف المشكلة حتى فوات الأوان[[10]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftn10" \o ").

يُعد Stuxnet أشهر البرامج التي تم وصفها كسلاحٍ إلكتروني استُخدم في هجوم إلكتروني ومن تصميمه كان يهدف إلى التسبب في هذا الضرر، وبالتالي فهو يلبي معظم تعريفات السلاح خاصة النية من استخدامه، ولكن هناك صعوبة في التصنيف القانوني له كسلاحٍ، فالأسلحة العادية القانونية ليست ذاتية التناسخ وغير قادرة على الانتشار المستقل والتشغيل التلقائي Auto Run.

**ZeuS Trojan:** هو الاسم الذي يطلق على عائلة من برامج تعد فيروسات ضارة تعطل وظائف نظام الكمبيوتر برمّته، صُمم فيروس ZeuS Trojan لاعتراض المعاملات المصرفية بين المصارف فهو ينتشر بشكلٍ شائع وسريع من خلال استخدام التصيد الاحتيالي Phishing وقد ينتشر أيضًا عن طريق اختراق مواقع الويب بصورةٍ سرية وإحداث ثغرات أمنية في برنامج التصفح الخاص بالمستخدم[[11]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftn11" \o ").

على سبيل المثال لدى اختراق جهاز كمبيوتر في أحد مواقع البنوك يقوم البرنامج بالتعرف على معلومات تسجيل الدخول الخاصة بالبنك واعتراضها وينتقل إليه من دون تنبيه المستخدم إلى وجود مشكلة ثم يرسل المعلومات إلى خادم تحكّم قد يكون موجودًا في أي مكان في العالم ولديه القدرة على تحليل المعلومات المحصلة والخروج بخلاصاتٍ مفيدة. لا يقوم خادم التحكّم بجمع بيانات البنك فقط ولكن يمكنه أيضًا إرسال التحديثات وإصدار الأوامر وتثبيت برامج إضافية إذا اختار المجرم ذلك.

مُنح البرنامج القدرة على تلقي التحديثات Updates لمنع الاكتشاف من برامج مكافحة الفيروسات، كما يمكنه أيضًا استخدام البيانات المسروقة لاستغلال النظام المستهدف بشكلٍ أكبر، لذلك إذا حدث أن النظام المصاب كان نظام التحكم الصناعي فقد يكون ZeuS Trojan قادرًا على التحكم في نظام SCADA الأساسي أو إتلافه والتأثير سلبًا في الخدمات أو على نظام الدولة برمته.

**Poison Ivy RAT:** أداة الوصول عن بُعد Remote Access Tool هو تطبيق برمجي يسمح للمستخدم بالتفاعل عن بُعد كما لو كان لديه وصول فعلي إلى نظام كومبيتري مستهدف وهو مشابه لفيروس ZeuS Trojan ولكنه يتميز عنه بأن له قابلية تطبيق أوسع كأداة وصول عن بُعد للأغراض العامة إضافة إلى أنه متاح مجانًا على الإنترنت. تم تصميمه ونشره بطريقةٍ مشابهة لـ ZeuS Trojan ويستخدم للسيطرة على جهاز كمبيوتر مستهدف بالكامل[[12]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftn12" \o ").

**LOIC) Low Orbit Ion Cannon):** هو برنامج متوافر مجانًا على الإنترنت يسمح لأي كمبيوتر المشاركة في هجوم شائع جدًا يدعى DDSo) distributed denial of service ). يعمل من خلال ملء النطاق الترددي المتاح للنظام المستهدف وإعاقة قدرته على الاستجابة الفورية والسريعة، ويمكن اعتباره أداة هجوم إلكترونية من الممكن فحصها لمعرفة ما إذا كانت تتوافق مع المفهوم التقليدي للسلاح وكيف يمكن التعامل معها بموجب قانون الحرب[[13]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftn13" \o ").

الهجوم باستخدام هذا البرنامج يشبه إقدام مجموعة من الأشخاص على الاتصال برقمٍ معين في الوقت نفسه ما يؤدي إلى تعريض خط الهاتف لطلباتٍ مفرطة وعدم القدرة على التعامل مع جميعها وبالتالي فشل الاتصال. من الصعب في هذه الحالة تحديد ما يمكن اعتباره سلاح الهواتف المتصلة وبالتالي صعوبة كبيرة لتحديد العامل الذي يمكن وصفه بأنه سلاح سواء عادي أو إلكتروني.

يمكن اعتبار فيروسات LOIC و Poison Ivy أدوات هجوم محمولة بكودٍ كومبيوتري ومن الممكن فحصها لتحديد ماهيتها وما هي قادرة على فعله، وباستخدام المعلومات المتوافرة يمكن إجراء تحليل لمعرفة إذا كانت تتوافق مع المفهوم التقليدي للسلاح وكيف يمكن التعامل معًا واستخدامها بموجب قانون الحرب لكن عمليات الفضاء الإلكتروني التي يكون فيها العامل الأساسي عاملًا بشريًا ذكيًا يتمتع بفهمٍ بديهي لكيفية عمل النظام المستهدف هي الأكثر إشكالية، ففي هذه الحالات من الصعب جدًا العثور على ذلك العامل ليكون موضوع مراجعة قانونية لتحديد شرعيته من عدمها.

**Sarah Palin Email Hack:** هو مثال جيد على الطبيعة الإشكالية لعمليات الفضاء الإلكتروني، حيث قام أحد الشبان الأميركيين القلقين من انتخاب السيدة سارة بالين Sarah Palin لمنصب نائب الرئيس في الانتخابات الرئاسية الأميركية في العام 2008 بقرصنة بريدها الإلكتروني الشخصي من جهازه الشخصي باستخدام خدمة إنترنت تسمى C tunnel ساعدته على إخفاء نشاطه عن أعين المراقبة الإلكترونية، واعتقد بذلك أنه يقوّض فرصها للوصول إلى هدفها من خلال إصدار ما افترض أنه سيكون المحتوى المثير للجدل في بريدها الإلكتروني الشخصي ثم قام بنشر محتويات هذا البريد على موقع الإنترنت Four Chanel[[14]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftn14" \o ").

إذا كان هذا الإجراء قد اتُخذ من قبل جهة أجنبية بغرض التأثير في الانتخابات الرئاسية الأميركية أو بطريقةٍ فردية، فقد يُعد انتهاكًا لسيادة الولايات المتحدة وبالتالي انتهاكًا للقانون الدولي، ولكن هنا يبرز السؤال أين السلاح الإلكتروني في هذه الحالة طالما أن المخترق لم يستخدم أي برامج ضارة بل اعتمد في بحثه على مصدر مفتوح أمام الجميع لاختراق حساب السيدة سارة بالين.

**HB Gary Hack**: شركة كبيرة للأمن السيبراني أعلن رئيسها التنفيذي Greg Hoglund في العام 2011 أن أرباح شركته قد تراجعت وأنه حصل على أسماء أعضاء مجموعة قراصنة هاجمت الشركة ولكن تعذّر عليه تقديم الأسماء إلى السلطات القانونية كونه فشل في اتباع قاعدة حماية أساسية تقول إنه قبل الادعاء على المجموعة يجب عليه التأكد من أن أنظمة الكمبيوتر في الشركة آمنة ومحصنة ضد الهجمات الإلكترونية[[15]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftn15" \o ").

انتهك الرئيس التنفيذي للشركة اثنين من المبادئ الأساسية لأمان الشبكة فقد استخدم كلمات مرور الشركة لإدارة حسابه الشخصي، كما كان لديه حساب على خادمها يستخدمه لتخزين النسخ الاحتياطية المهمة، لذا فإن اختراق حسابه يعني أن البريد الإلكتروني للشركة بالكامل قد تم اختراقه. كما أن الخادم نفسه كان يعمل بإصدارٍ قديم غير ميوّم من برنامج الحماية Linux وفيه ثغرة سمحت للمتسللين Hakers بدخول الموقع، وقد اعتمد هذا الهجوم على الحرفة اليدوية والهندسة مسلطًا الضوء على عدم وجود سلاح إلكتروني واضح في هجوم مدمر اقتصاديًا ضد الشركة.

**سادسًا: إشكالية مراجعة أسلحة الحرب السيبرانية**

تخضع عمليات تخطيط الحروب سواء التقليدية منها أم السيبرانية لمراجعاتٍ قانونية متعددة قبل خوضها، حيث يشارك المستشارون القانونيون في مراحل تطوير العمليات ومراجعة الأسلحة لضمان عدم وجود تأثير سلبي في السكان المدنيين أو معاناة لا داعي لها للمدنيين أو المقاتلين كما الامتثال لقانون الحرب.

تتألف المراجعة التي تقيّم شرعية العملية الهجومية السيبرانية والتي من الهدف Target المقترح، القدرة Capability المقترحة والتقنيات Techniques المخطط لها لتحقيق التأثير المطلوب في الهدف لتأمين شرعية العمليات العسكرية والعمليات الإلكترونية.

من خلال فهم الطبيعة المعقدة للعمليات السيبرانية يمكن فهم سبب أهمية حل مشكلات تعريف السلاح السيبراني وقدرة الجيوش على العمل في الفضاء الإلكتروني. إن تسمية أي قدرة على أنها سلاح لها آثار قانونية وسياسية، ولا يمكن استخدامها من قبل الجيوش حتى تخضع لمراجعةٍ قانونية كجزءٍ من عملية الشراء، فالقدرات السيبرانية تواجه تحديات بسبب الاختلاف بين الأسلحة التقليدية والقدرات الإلكترونية.

يتم تطوير العديد من البرمجيات وهذا ما يعطي تعريف السلاح السيبراني معنى موسعًا للغاية، فقد لا يكون هناك ما يكفي من القانونيين لمراجعتها جميعًا وقد يصبح البرنامج قديمًا في أثناء عملية المراجعة كون البرامج تخضع للتغيير المستمر. من ناحية أخرى قد يكون من الصعب صياغة اختبار موضوعي لتحديد متى تحتاج القدرة أي السلاح التي تمت مراجعتها مسبقًا إلى مراجعة قانونية جديدة.

تنص اتفاقية لاهاي الرابعة ولا سيما المادة 22 من اللوائح الملحقة بها على أن حق المتحاربين في تبنّي وسائل لإيذاء العدو هو حق محدود وليس مطلقًا كما تقنّن المادة 36 من البروتوكول الإضافي الأول للعام 1977 الملحق باتفاقيات جنيف للعام 1949 مطلب إجراء مراجعات قانونية للأسلحة الجديدة كافة. لذلك ونظرًا لأن شراء السلاح واستخدامه يعتمدان على خضوعه للمراجعة القانونية فمن الأهمية بمكان اختيار التعريف المناسب للأسلحة السيبرانية، فقد يؤدي التعريف الخاطئ إلى الإخفاق في الامتثال للمعايير القانونية الدولية، بالمقابل يمكن أن يشمل التعريف الواسع للغاية الأدوات والتقنيات المستخدمة في التجسس وإخضاعها لتدقيقٍ عميق من شأنه تعطيل العمليات الحيوية للأمن القومي للدولة وجعلها عرضة لهجماتٍ دامية[[16]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftn16" \o ").

بسبب عدم إمكانية وضع قواعد تجيب بوضوحٍ على كل الأمور التي لا يمكن السيطرة عليها في الفضاء الإلكتروني، فإن التركيز ينصبّ على الإجابة على سؤال: ما هو السلاح السيبراني؟ حيث أن إجراء أي نوع من أنواع الحرب بالمعنى العسكري يعني وجود أسلحة قادرة على شن هجوم. إذا كان مصطلح الحرب البرية أو الجوية سيتوسع ليشمل مفهوم الحرب الإلكترونية فإنه يجب افتراض وجود أسلحة إلكترونية إلى جانب الأسلحة التقليدية.

**سابعًا: مقاربات تطبيق القانون على تعاريف الأسلحة السيبرانية**

تنص المادة 36 من البروتوكول الإضافي الأول لاتفاقية جنيف للعام 1949على ما يأتي:

عند دراسة سلاح جديد أو تطويره أو اقتنائه أو تبنّيه أو أي وسيلة أو طريقة حرب، يكون الطرف المتعاقد السامي ملزمًا بتحديد ما إذا كان استخدامه في بعض أو كل الظروف محظورًا بموجب هذا البروتوكول، أو من قبل أي قاعدة أخرى من قواعد القانون الدولي.

تتعلق مسألة المراجعة بالأساليب والوسائل أي الأسلحة، فعلى سبيل المثال يمكننا النظر إلى تقنية DDoS أي منع الوصول إلى موقع إلكتروني وتحليلها كأسلوبٍ من أساليب الحرب بشكلٍ عام لتحديد قدرتها على التمييز بين الأهداف المدنية والعسكرية لتجنب أي معاناة غير ضرورية للسكان المدنيين أو العسكريين. من الواضح أنه يمكن استخدام هذه التقنية بطريقةٍ تتوافق مع القانون الدولي من خلال استهداف المواقع الإلكترونية العسكرية فقط، بالمقابل فإن الهجوم الإلكتروني Stuxnet الذي شُن ضد البرنامج النووي الإيراني قد فشل في التمييز بين الأهداف العسكرية والمدنية، لذلك وجب مراجعة الأساليب لتحديد شرعية الهجمات الإلكترونية وفق القانون الدولي.

يُعرّف السلاح على أنه أداة تستخدم في سياق الأعمال العدائية، هذا التعريف غير كافٍ لأنه يمكن استخدام أي وسيلة في الأعمال العدائية كما اقترن تحديد السلاح بحالة الأعمال العدائية، ومن هنا يمكن استعراض التعاريف الآتية:

• إن أوضح نقطة لتحديد ما يشكل سلاحًا إلكترونيًا هو تعريف السلاح بطريقةٍ موضوعية تؤدي الغرض منها، فموقع Dictionary.com العالمي يعرّف السلاح عل أنه «أي أداة أو جهاز يستخدم في القتال كالسيف، البندقية، المدفع....»، وبالنسبة إلى موقع ويكيبيديا وعلى الرغم من عدم الركون إليه بشكلٍ رسمي فإنه يعرّف السلاح على أنه «أداة تستخدم بهدف إحداث ضرر جسدي أو عقلي للكائنات الحية أو الهياكل أو الأنظمة الاصطناعية»، كما تعرّف الموسوعة البريطانية Encyclopedia Britannica السلاح على أنه «أداة تُستخدم في القتال بغرض قتل أو إصابة أو هزيمة العدو»[[17]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftn17" \o ").

• عرّف الجيش الأميركي الأسلحة على أنها الأدوات والأجهزة «التي لها تأثير مقصود يتمثل في إصابة أو تدمير أو تعطيل أفراد أو عتاد أو ممتلكات العدو»، كما أن البحرية الأميركية عرّفت الأسلحة على أنها «أجهزة والمكونات المطلوبة لعملياتها بقصد إصابة أو إتلاف أو تدمير أو تعطيل الأفراد أو الممتلكات[[18]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftn18" \o ").

• فتح سلاح الجو الأميركي آفاقًا جديدة من خلال تعريف الأسلحة على أنها «أجهزة مصممة لقتل الأشخاص أو إصابتهم أو إعاقتهم أو تدمير الممتلكات أو المواد أو إلحاق الضرر بها أو تعطيلها مؤقتًا»، كما عرّف القدرة الإلكترونية أو القدرة السيبرانية على أنها «أي جهاز أو برنامج يهدف إلى تعطيل أو تدمير أنظمة الكمبيوتر أو البيانات أو الأنشطة أو القدرات المعادية» ويمضي تعريف القدرة الإلكترونية إلى استبعاد أي «جهاز أو برنامج يهدف إلى توفير الوصول إلى نظام كمبيوتر معاد لاستغلال البيانات فقط» لذلك فإن القليل من الأسلحة الإلكترونية تلبي تعريفات الأسلحة والباقي هو مجرد برامج أو تقنيات توفر الوصول إلى نظام كمبيوتر الخصم بهدف الحصول على المعلومات أو مراجعة البيانات[[19]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftn19" \o ").

على الرغم من أن التعريفات أعلاها غير كافية، إلا أن هناك موضوعًا مشتركًا قد يؤدي النظر فيه إلى تعريف عام للسلاح على أنه «جهاز مصمم لإحداث ضرر وهو النية المرجوة من هذا الاستخدام والتي تعد جانبًا مهمًا في أي تعريف تقني، فعادة ما تحصل الجيوش على أعتدة خطرة بطبيعتها ويمكن أن تسبب ضررًا كبيرًا للعدو ولكنها لا تعد أسلحة كالجرافات (حصل أحد جنود الجيش الأميركي على وسام الشرف لقتله جنديَين صينيَين بعدة الحفر بعد نفاد الذخيرة في أثناء مشاركته في القتال خلال الحرب الكورية)، وهي لا تخضع لمراجعة الأسلحة كما باقي الأعتدة لأنه لا يتم الحصول عليها بقصد استخدامها كأسلحةٍ، كما أنها متاحة للاستخدام حتى في المواقف غير القتالية.

يمكن تطبيق المعيار أعلاه على القدرات الإلكترونية، وهناك جانبان لهذا التحليل الأول تأكيد وجود جهاز أو سلاح في عمليات الفضاء الإلكتروني لتحليله وتحديد شرعية استخدامه من عدمه، والثاني هو تحديد تأثيرات أي أضرار هذا السلاح بهدف الحد من الأضرار الجانبية أو أي معاناة غير ضرورية.

إن السلاح في العملية الإلكترونية هو البرمجيات غير الملموسة والتي تخضع لتغييراتٍ متكررة وفق الإصدارات المختلفة، لذلك من غير المنطقي استنتاج أن كل البرامج هي أسلحة، ومن غير العملي أيضًا تقديم مراجعة قانونية جديدة في كل مرة يتم فيها تطوير البرنامج. البديل هو توافر عتبة موضوعية لحجم التغيير في هذه البرمجيات الذي يتطلب مراجعة جديدة.

تبرز فئة أخرى من القدرات الإلكترونية التي تتحدى التعريف بموجب القواعد التقليدية وهي command line tactics. هذه الإجراءات ليست برامج ولكنها نمط أو سلسلة من الأوامر تؤدي إلى نتيجة ذات صلة بالعمليات تتمثل بالوصول غير المصرح به إلى نظام الكمبيوتر، فيكون حذف ملف أو التلاعب بالبيانات جزءًا مهمًا من حملة عسكرية من دون أن يكون هناك سلاحٌ متورط[[20]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftn20" \o ").

تتمثل الخطوة التالية في تحديد التأثيرات المقصودة والمباشرة لاستخدام السلاح الإلكتروني ومقارنة تلك الآثار مع آثار الأسلحة التقليدية، فغالبًا ما يتم احتواء التأثيرات المقصودة والمباشرة للعمليات الإلكترونية بالكامل في الفضاء الإلكتروني وهنا يُطرح السؤال: إلى أي مدى ينبغي تطوير القواعد التي تحكم الآثار المادية التقليدية للأسلحة السيبرانية؟

يُعد تعريف دليل تالين الأقرب إلى الواقع فيشير إلى أن الأسلحة السيبرانية هي الوسائل الإلكترونية للحرب التي يتم تصميمها واستخدامها والتي يمكن أن تسبب إما إصابة أو وفاة الأشخاص، أو إتلاف أو تدمير الأشياء، أي أنه يجب التسبب بخسائر لوصف عملية إلكترونية على أنها هجوم إلكتروني. كما يعرّف الدليل الهجوم السيبراني على أنه «عملية إلكترونية يمكن أن تسبب إصابة الأشخاص أو موتهم أو إتلاف أو تدمير الأشياء». من المهم ملاحظة أن دليل تالين يستبعد صراحة تدمير البيانات من تعريف الهجوم ما لم يكن هناك اتصال مباشر بينها وبين الموت. أي أنه يستثني التقنيات التي تسمح بالتلاعب بالبيانات من التصنيف كأسلحةٍ. من ناحية أخرى فإن تعريف الدليل للسلاح مبالغ فيه حيث أنه يشمل كل الوسائل التي يمكن استخدامها لإحداث تلف معين حتى من دون نية استخدام هذه الوسائل في أي أمر يتجاوز التجسس أو التلاعب بالبيانات[[21]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftn21" \o ").

**ثامنًا: التعريف المقترح للأسلحة السيبرانية**

إن تعريف القدرة الإلكترونية على أنها «سلاح يُعد سيفًا ذا حدين ومشكلة حقيقية» لأنه يضع معيارًا بعيد المنال من حيث كمية المراجعات القانونية فالقدرات السيبرانية التي يتم تطويرها أو الحصول عليها يجب أن تُراجَع للتأكد من شرعيتها بموجب قانون النزاعات المسلحة والقانون المحلي والقانون الدولي قبل استخدامها في نزاع أو عملية عسكرية. يتطلب هذا الأمر مراجعة قانونية جديدة في كل مرة تُغير فيها برنامج الكمبيوتر ليكون بمثابة قدرة. نظرًا لأن هذا يمكن أن يحدث عشرات المرات في أثناء سير العملية، فإن المطلب غير عملي ويشكل عائقًا أمام قدرة القائد على توظيف قوة عسكرية فعالة في الوقت المناسب في الفضاء الإلكتروني لتحقيق أهداف عمليته.

على النقيض من ذلك، غالبًا ما يتم إجراء العمليات الإلكترونية التي لا تشكل هجومًا بموجب القانون الدولي من دون استخدام أي شيء يمكن تعريفه على أنه سلاح. وهذا من شأنه أن يلغي الحاجة إلى سلسلة من المراجعات القانونية لكنها لن تلغي متطلبات المراجعة القانونية التشغيلية operational التي يجب أن توائم بين القدرة المستخدمة capability ونتائج العملية المخطط لها بما يضمن الامتثال للقانون الدولي.

في حين أنه ليس هناك تعريف واحد ومحدد للسلاح فإن هذا المصطلح رائج بدرجةٍ كافية في الاستخدام وفي كيفية معاملته بموجب القانون الدولي، فالسلاح «شيء مصمم بغرضٍ أساسي هو القتل أو التشويه أو الإصابة أو الإضرار أو التدمير». هذا التعريف المناسب للأسلحة التقليدية يمكن استخدامه أيضًا كتعريفٍ للأسلحة السيبرانية لضمان الامتثال للقانون الدولي، لا سيما في حالة عدم وجود إرشادات واضحة في العمليات الخاصة بالإنترنت فربما يكون من المنطقي مواءمة التعريفات ذات الصلة بالعمليات السيبرانية مع التعاريف المستخدمة في العمليات العسكرية التقليدية.

بالمحصلة التعريف المقترح يوفر تعريفًا منطقيًا للهجوم الإلكتروني، والذي يمكن وصفه بعد ذلك بأنه عملية إلكترونية تستخدم سلاحًا إلكترونيًا. وبشكلٍ أكثر تحديدًا يمكن تعريف الهجوم الإلكتروني على أنه «عملية تستخدم الوسائل الإلكترونية بغرض القتل أو التشويه أو الإصابة أو التدمير»، وهذا من شأنه أن يوضح متى تنطبق قوانين الحرب على العمليات الإلكترونية ويفتح النقاش حول القضايا المحيطة بالعمليات الإلكترونية التي لا ترقى إلى مستوى استخدام القوة، والتي تشكل الغالبية العظمى من العمليات السيبرانية التي تجري حاليًا ويتم القيام بذلك من دون وجود قواعد متماسكة للتحكم في السلوك.

على الرغم من وجود مزايا لتعريف السلاح السيبراني، إلا أن هناك عيوبًا محتملة أيضًا لهذا التعريف. من شأن التحديد الأكثر صرامة للأسلحة السيبرانية أن يغني عن الحاجة إلى معظم المراجعات القانونية قبل التخطيط العملياتي. على الرغم من أن المراجعة القانونية تبقى مطلوبة قبل استخدام أي تقنية إلكترونية في عملية تتصدى للانتهاكات المحتملة للقانون الدولي، فإن إجراء المراجعة القانونية اللاحقة يؤدي إلى إهدار الوقت والموارد في تطوير هذه التقنية، ويمكن معالجة هذا الأمر من خلال المراجعة الواعية لأساليب الحرب الإلكترونية ومراجعة شرعية توزيع القدرات السيبرانية الضارة ووقف التوزيع العشوائي وغير المنضبط واعتباره غير قانوني.

يكشف التحليل المعمق للتعريف المقترح للأسلحة السيبرانية عن نتيجة مثيرة للفضول هي أن الإنترنت يُعد المنطقة الوحيدة للعمليات العسكرية التي يمكن أن تتسبب فيها الدولة بشكلٍ مباشر في ضرر مادي كبير للخصم أو العدو من دون استخدام سلاح، وستظل المراجعة القانونية التشغيلية تتناول مخاوف القانون الدولي سواء كانت تلك المخاوف ناتجة عن الوسائل المستخدمة أو الطريقة المعتمدة أو التناسب في الاستخدام بين الوسائل والهدف، وتبقى النية وتأثير العملية هو الذي سيحكم شرعيتها، فالفضاء الإلكتروني فريد بما يكفي لتبرير هذه النتيجة إلى حد ما.

**الخاتمة**

على الرغم من أن مصطلح السلاح السيبراني أصبح جزءًا من الثقافة العامة ومتداولًا أكثر من الأسلحة التقليدية وبديلًا عنها، فلم يكن هناك إجماع حقيقي أو توافق على تعريفه الصحيح. تم استخدام المصطلح لتعريف مجموعات من رموز كمبيوترية تؤدي إلى تأثيرات مختلفة تبدأ من إبطاء المواقع الإلكترونية إلى تدمير منشآت الطاقة النووية كما في الحالة الإيرانية. هذه المجموعة الواسعة من الاحتمالات تجعل من الصعب السيطرة على العمليات الإلكترونية لضمان الامتثال للقانون الدولي والمعايير الإنسانية.

يجب أن يكون هناك أساس للتحليل القانوني للعمليات العسكرية في الفضاء الإلكتروني التي هي دون مستوى استخدام القوة كذلك عدم اعتبارها على أنها تجسس، كون الإطار الحالي للتجسس السيبراني وبموجب القانون الدولي غير محدد أو متوافق على عدم تحديده، أضف إلى ذلك أن الخلط بين العمليات الإلكترونية غير التجسسية والهجوم الإلكتروني يعرقلان تحليل امتثال العمليات الإلكترونية العسكرية لقانون الحرب. يجب أن تكون الخطوة الأولى في هذه العملية هي تطوير تعريفات عملية للهجوم الإلكتروني والسلاح السيبراني.

على الرغم من أن الحاجة إلى تعريف واضح، فإن بعض التعريفات التي اقتُرحت غير عملية في سياق العمليات الإلكترونية. يجب أن يكون تعريف السلاح السيبراني منطقيًا وقابلًا للاستخدام من قبل مشغلي الإنترنت ومستشاريهم القانونيين. تقصر معظم التعريفات المنطقية التي استُعرض معظمها عن الهدف المتمثل في أن تكون مفيدة للمشغلين، لأن هذه التعريفات إما غامضة للغاية أو واسعة للغاية وقد تتطلب التعريفات شديدة الغموض مراجعات قانونية لكل شيء يستخدمه الجيش كسلاحٍ سيبراني، كما تتطلب مراجعات لإصداراته المتكررة من البرامج وهذا ما يُعد مستحيلًا من الناحية التشغيلية.

يجب ربط تعريف الأسلحة السيبرانية بتعريف الأسلحة التقليدية بحيث يتناول الأشياء التي يكون استخدامها الأساسي بمثابة سلاح بهدف القتل أو التدمير أو التشويه فقط. هذا من شأنه أن يسمح باستخدام المعايير الدولية ويتوافق مع النهج المتبع في دليل تالين. ستلبّي هذه التعريفات احتياجات المشغلين العسكريين وتوفر لهم إرشادات أوضح وتستمر في توافر حماية فعالة للمدنيين من العمليات الإلكترونية التي قد تكون غير قانونية بموجب القانون الدولي.

**المراجع**

1- <https://www.vmware.com/topics/glossary/content/cyber-espionage>.

2- https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2\_rul\_rule107

3- US Bugged Merkel’s Phone from 2002 Until 2013, Report Claims, BBC (Oct 2013), http://www.bbc.co.uk/news/ world-europe-24690055.

4- Dictionary of Military and Asspciated Terms, JOINT PUB. 1-02, at 73 (2013) (as amended through Feb. 15, 2013).

5- Michael N. Schmitt, International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed, <http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf>

6- Michael N. Schmitt, Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework (1999)

7- Industrial Control Systems Cyber Emergency Response Team. http:// ics-cert.us-cert.gov/content/frequently-asked-questions.

8- David E. Sanger, Obama Order Sped Up Wave of Cyberattacks Against Iran, N.Y. TIMES,) June 1, 2012).

9- Kevin Stevens & Don Jackson, ZeuS Banking Trojan Report, DELL SECUREWORKS (Mar. 11, 2010), <http://www.secureworks.com/cyber-threat-intelligence/threats/zeus/>

10- Roger A. Grimes, Danger, Remote Access Trojans, Security Admin, Sept. 2002, available at http://technet.microsoft.com/en-us/library/dd632947.aspx.

11- LOIC, SOURCE FORGE, <http://sourceforge.net/projects/loic>.

12- Kim Zetter, Palin E-Mail Hacker Says It Was Easy, WIRED (Sep.2008), http://www.wired.com/ threatlevel/2008/09/palin-e-mail-ha/.

13-<http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgaryhack/>

14- Protocol Additional to the Geneva Conventions, Aug. 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977

15- Weapon, DICTIONARY.COM, <http://dictionary.reference.com/browse/weapon>.

16- US DEP’T OF THE NAVY: Implementation and Operation of the Defense. Acquisition System and the Joint Capabilities Integration and security system of the Navy Instruction (2011).

17- US DEP’T OF THE AIR FORCE, Air Force Instruction, Legal Reviews Of Weapons And Cyber Capabilities (2011).

18- Command Line, WEBOPEDIA, <http://www.webopedia.com/TERM/C/command_line.html>.

19- TALLINN MANUAL on The International Law Applicable To Cyber Warfare (Michael N. Schmitt 2013).

[[1]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftnref1" \o ")-     .https://www.vmware.com/topics/glossary/content/cyber-espionage

[[2]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftnref2" \o ")-     التهديد المستمر المتقدم (APT) هو عامل تهديد خفي يستخدم تقنيات قرصنة سرية ومتطورة للوصول إلى نظام ما، عادة ترعاه دولة أو مجموعة ترعاها الدولة، ويكتسب وصولًا غير مصرح به إلى شبكة كمبيوتر ويبقى غير مكتشف لفترةٍ طويلة، بمجرد أن يتمكن المهاجم من الوصول إلى الشبكة وعادة عن طريق التصيّد الاحتيالي أو تثبيت البرامج الضارة يمكنه عرض ملفات الشركة والمحادثات والبيانات والمواد الحساسة الأخرى. في الآونة الأخيرة يشير المصطلح أيضًا إلى الجماعات التي ترعاها غير الدول والتي تقوم بعمليات تدخل واسعة النطاق ضد أهداف ذات قيمة عالية (HVT).

[3]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftnref3" \o ")-    .https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2\_rul\_rule107

[[4]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftnref4" \o ")-     (US Bugged Merkel’s Phone from 2002 Until 2013, Report Claims, BBC (Oct 2013

.http://www.bbc.co.uk/news/ world-europe-24690055

[[5]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftnref5" \o ")-     DICTIONARY OF MILITARY AND ASSOCIATED TERMS, JOINT PUB. 1-02, at 73 (2013) (as amended

through Feb. 15, 2013).3

[[6]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftnref6" \o ")-     DICTIONARY OF MILITARY AND ASSOCIATED TERMS, JOINT PUB. 1-02, at 73 (2013) (as amended

.(through Feb. 15, 2013

[[7]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftnref7" \o ")-     Michael N. Schmitt, Computer Network Attack and Use of Force in International Law: Thoughts on a

.(Normative Framework (1999

[[8]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftnref8" \o ")-   هو نظام مكون من برامج وأجهزة تسمح للمنظومات الصناعية بالتحكم في العمليات الصناعية محليًا أو من أماكن بعيدة، مراقبة البيانات وجمعها ومعالجتها، التفاعل المباشر مع الأجهزة عبر المستشعرات وغير ذلك وتسجيل الأحداث في السجلات.

[[9]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftnref9" \o ")-     Industrial Control Systems Cyber Emergency Response Team.

http:// ics-cert.uscert.gov/content/frequently-asked-questions.

[[10]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftnref10" \o ")-    .(David E. Sanger, Obama Order Sped Up Wave of Cyberattacks Against Iran, N.Y. TIMES,(June 1, 2012

[[11]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftnref11" \o ")-  (11,2010.Kevin Stevens & Don Jackson, ZeuS Banking Trojan Report, DELL SECUREWORKS (Mar

.http://www.secureworks.com/cyber-threat-intelligence/threats/zeus/

[[12]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftnref12" \o ")-  Roger A. Grimes, Danger, Remote Access Trojans, SECURITY ADMIN

 Sept. 2002, available at http://technet.microsoft.com/en-us/library/dd632947.aspx

[[13]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftnref13" \o ")-    .LOIC, SOURCEFORGE, http://sourceforge.net/projects/loic

[[14]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftnref14" \o ")-  .(2008 .Kim Zetter, Palin E-Mail Hacker Says It Was Easy, WIRED (Sep

http://www.wired.com/ threatlevel/2008/09/palin-e-mail-ha/

[[15]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftnref15" \o ")-    http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgaryhack/

[[16]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftnref16" \o ")-  Protocol Additional to the Geneva Conventions, Aug. 12, 1949, and Relating to the Protection of Victims of

.International Armed Conflicts (Protocol I), June 8, 1977

[[17]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftnref17" \o ")-    .Weapon, DICTIONARY.COM, http://dictionary.reference.com/browse/weapon

[[18]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftnref18" \o ")-  DEP’T OF THE NAVY IMPLEMENTATION AND OPERATION OF THE DEF. ACQUISITION SYSTEM AND THE JOINT CAPABILITIES INTEGRATION AND DEV. SYSTEM SEC. OF THE NAVY

.INSTRUCTION 2011

[[19]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftnref19" \o ")-  DEP’T OF THE AIR FORCE, AIR FORCE INSTRUCTION, LEGAL REVIEWS OF WEAPONS AND CYBER CAPABILITIES (2011).1

[[20]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftnref20" \o ")-    .Command Line, WEBOPEDIA, http://www.webopedia.com/TERM/C/command\_line.html

[[21]](file:///\\\\192.168.137.98\\d$\\DATA\\Website-Content\\%D9%85%D9%86%D8%B4%D9%88%D8%B1%D8%A7%D8%AA\\%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A\\Defense\\117\\defence-117%20finale\\New%20folder%20(4)\\ar\\ar2.rtf" \l "_ftnref21" \o ")-  TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N

.(Schmitt 2013

**Legal Reviews of the Definition of Cyber Weapons**  
  
Cyber attacks have become a regular feature of the media landscape. Thanks in great part to the investigations carried out by different U.S. entities following Russian interference in the 2016 U.S. elections – which included mounted cyber attacks – episodes of "hacks", "infiltrations" and "assaults" are now reported on a regular basis.   
Of course, the fact that cyber attacks are more reported these days does not mean they did not exist before as objects of academic inquiry or even as matters for policy debate. However, what constitutes a "cyber attack" is not yet resolved. Despite some understandings reached as informed by "real life events", what is a cyber attack very much remains a contested matter.   
As noted above, events of a nature that may amount to a “cyber attack” have been mostly addressed by the domestic law – or domestic institutions – in the country where they happened. However, it is the occurrence of episodes of this nature between states that puts in jeopardy the type of “friendly relations” needed for a peaceful and “orderly” international community of states.   
A case in point is that related to Stuxnet. In June 2012, author and New York Times reporter David Sanger reported that a malware package of “unprecedented complexity” had targeted the Iranian nuclear research program. The malware, which came to be known as Stuxnet, was then discovered on many computer systems outside Iran. However, it did not appear to do any damage to these other systems.   
Mr. Sanger’s latest book, published in 2018, was “The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age”. In an interview with the New York Times to discuss his latest publication, the author and reporter offered the contention that the Stuxnet malware had been part of a U.S. planned and led covert cyber operation.   
The assertion that a nation state may had used a “cyber attack” in support of its national objectives had already picked the attention of cyber-law commentators, both in and out of government. In 2014, Gary D. Brown and Andrew O. Metcalf, two U.S. Army officers with extensive knowledge and experience on cyber space and cyber command issues, provided some elements of legal analysis about Stuxnet and cyber warfare in general.   
In their legal review published in the Journal of National Security Law and Policy, the two authors explained that even if the terms “cyber attack” or “cyber warfare” implied the employment of cyber weapons, there was still great perplexity surrounding the matter. More concretely, the threshold needed for the use of such weapons to amount to a “cyber attack” that created a state of “cyber warfare” had yet to be established. For these two U.S. army officers, defining what constitutes a “cyber weapon” could help gain a better understanding of cyber war.   
The purpose of this paper is to highlight the difficulty in transforming these broad topics into practical legal advice for commanders in the “theatre of operations”. In line with (recent) literature published on the topic, the article concludes that just as not all cyber attacks amount to cyber warfare, not all cyber techniques constitute “weapons”. The paper argues instead that an assessment focusing on the usages of a given capability in a context provides a better lens to addressing the many unresolved features comprehended within the field of cyber operations.

**Examens juridiques de la définition des cyber-armes**

Les cyberattaques sont devenues un élément régulier du contexte médiatique. Grâce en grande partie aux enquêtes menées par différentes entités américaines à la suite de l'ingérence russe dans les élections américaines de 2016 - qui comprenaient des cyberattaques montées - des épisodes de "hacks", d'"infiltrations" et d'"agressions" sont désormais régulièrement rapportés.   
Bien sûr, le fait que les cyberattaques soient davantage rapportées de nos jours ne signifie pas qu'elles n'existaient pas auparavant en tant qu'objets d'enquête académique ou même en tant que sujets de débat politique. Cependant, la question de savoir ce qui constitue une "cyberattaque" n'est pas encore résolue. Malgré certaines interprétations fondées sur des "événements réels", la définition d'une cyberattaque reste très contestée.   
Comme indiqué plus haut, les événements susceptibles de constituer une "cyberattaque" ont été principalement traités par le droit interne - ou les institutions nationales - du pays où ils se sont produits. Cependant, c'est la survenue d'épisodes de cette nature entre Etats qui met en péril le type de "relations amicales" nécessaires à une communauté internationale d'Etats pacifique et "ordonnée".   
Un exemple concret est celui lié à Stuxnet. En juin 2012, David Sanger, auteur et journaliste au New York Times, a rapporté qu'un logiciel malveillant d'une "complexité sans précédent" avait ciblé le programme de recherche nucléaire iranien. Ce logiciel malveillant, connu sous le nom de Stuxnet, a ensuite été découvert sur de nombreux systèmes informatiques en dehors de l'Iran. Toutefois, il ne semble pas avoir causé de dommages à ces autres systèmes.   
Le dernier livre de M. Sanger, publié en 2018, était "L’arme parfaite : Guerre, sabotage et peur à l'ère cybernétique". Dans une interview avec le New York Times pour discuter de sa dernière publication, l'auteur et journaliste a offert l'affirmation que le logiciel malveillant Stuxnet avait fait partie d'une cyberopération secrète planifiée et dirigée par les États-Unis.   
L'affirmation selon laquelle un État-nation peut avoir utilisé une "cyberattaque" pour soutenir ses objectifs nationaux avait déjà attiré l'attention des commentateurs du droit de la cybernétique, tant à l'intérieur qu'à l'extérieur du gouvernement. En 2014, Gary D. Brown et Andrew O. Metcalf, deux officiers de l'armée américaine ayant une connaissance et une expérience approfondies des questions de cyberespace et de cybercommande, ont fourni quelques éléments d'analyse juridique sur Stuxnet et la cyberguerre en général.   
Dans leur analyse juridique publiée dans le journal du droit et de la politique de sécurité nationale, les deux auteurs expliquent que même si les termes "cyberattaque" ou "cyberguerre" impliquent l'emploi de cyberarmes, la perplexité reste grande en la matière. Plus concrètement, le seuil nécessaire pour que l'utilisation de telles armes équivaille à une "cyberattaque" créant un état de "cyberguerre" reste à établir. Pour ces deux officiers de l'armée américaine, définir ce qui constitue une "cyberarme" pourrait aider à mieux comprendre la cyberguerre.   
L'objectif de cet article est de souligner la difficulté de transformer ces vastes sujets en conseils juridiques pratiques pour les commandants sur le "théâtre des opérations". Conformément à la littérature (récente) publiée sur le sujet, l'article conclut que, de même que toutes les cyberattaques ne constituent pas une cyberguerre, toutes les cybertechniques ne constituent pas des "armes". L'article soutient plutôt qu'une évaluation axée sur les usages d'une capacité donnée dans un contexte donné constitue une meilleure optique pour aborder les nombreuses caractéristiques non résolues comprises dans le domaine des cyberopérations.