الوضع القانوني للحرب الالكترونية

The Legal status of Cyberwar

الباحث/ أنيس بوقيدر[1]

[1]جامعة الجزائر 3 ، anisboukider16@gmail.com

تاريخ الإرسال22/ 12/ 2019 *تاريخ القبول: 10/ 02/ 2020* *تاريخ النشر: 30/ 05/ 2020*

ملخص:

تركز هذه الورقة على دراسة الوضع القانوني للحرب الالكترونية، وذلك من خلال اسقاط قوانين الحرب الحركية على الحرب الالكترونية، واختبار فاعلية الاليات القانونية التقليدية في تحقيق الامن المعلوماتي والحد من انتشار الحروب الالكترونية والتخفيف من حدتها.

تقتضي الدراسة تحديد مفهوم الحرب الالكترونية وإبراز خصوصياته وتمييزه عن المفاهيم ذات الصلة به على غرار النزاع السبراني ، ثم اسقاط قوانين الحروب التقليدية على الحرب الالكترونية، ليتم في الاخير استنتاج أهم معيقات الاسقاط القانوني ومن أبرزها قلة الجهود المعرفية التي تزاوج بين الجوانب التقنية المعلوماتية والتشريعية، بحكم أن تقنين الحرب الالكترونية يقتضي دراية ومعرفة تقنية واسعة بتكنولوجيات الاتصال بشقيها المادي والناعم (البرمجيات).

كلمات مفتاحية: الحرب .الالكترونية.، قانون .الحرب.، الوضع. القانوني.، الفضاء .السبراني.

Abstract:

This paper focuses on studying the legal status of the cyber war through the application of the conventional warfare's laws on the cyber war, in order to achieve information security.

This study aims at defining cyber war and its characteristics, as well as distinguishing it from other terms such as cyber conflict, then analyzing the application of the laws of conventional warfare on the cyber war. The objective of this paper is to draw conclusions about the obstacles found in the field of legislation concerning the cyber war.
Keywords: *cyberwar; legal status; law of war; cyberspace.*

1- المؤلف المرسل : أنيس بوقيدر ، **الإيميل :** anisboukider16@gmail.com

مقدمة :

تعتبر الضوابط والتشريعات القانونية من الاليات الفعالة للحد من الحروب ومراقبتها وتقليل نسبة حدوثها، حيث عمدت الجماعة الدولية منذ نهاية الحرب العالمية الثانية استصدار لوائح ونصوص قانونية مختصة بالحروب التقليدية على غرار القانون الدولي الإنساني، بالإضافة الى ابرام المعاهدات لتفادي الانزلاق الى مواجهة عالمية ثالثة.

أما على الجانب النووي فقد برزت مجموعة من الجهود القانونية الدولية لمنع حدوث حرب نووية مدمرة، ولعل أبرزها اتفاقية حظر انتشار الأسلحة النووية NPT ، ومختلف الاتفاقيات الجزئية المصاحبة لها، بحيث تمثل كلها اطر قانونية وتشريعية عالمية ذات طابع الزامي.

لا تقل الحروب الالكترونية خطرا عن سابقيها فغالبا ما تستهدف الفيروسات والبرامج الخبيثة الاخرى البنى التحتية الحساسة للدولة والأنظمة المالية والصحية فتصيبها بالشلل والعطب وهو مايشكل تهديدا مباشرا للأمن القومي للدول المستهدفة، وعليه تهدف الدراسة الى محاولة اسقاط قوانين الحرب التقليدية والنووية على الحروب الالكترونية لإيجاد أرضية قانونية من شأنها كبح حدة انتشار لحروب الالكترونية والتقليل من اثارها المدمرة، وعليه فإن

الإشكالية البحثية للدراسة تتمحور حول **مدى إمكانية اسقاط قوانين الحرب التقليدية على الحرب الالكترونية**، ويكمن الهدف منها في إيجاد ضوابط قانونية لهذا النوع من الحروب.

لقد تم الاعتماد في سياق البحث على المنهج الوصفي التحليلي لفهم خلفيات الأطر القانونية للحرب التقليدية ومحاولة اسقاطها على الحرب الالكترونية، و هو ما يستدعي التركيز على المحاور التالية:

- مفهوم الحرب الالكترونية والنزاع السبراني وخصوصياتهما.
- مواطن الاختلاف بين الحرب الالكترونية والحروب التقليدية.
- اسقاط قوانين الحرب التقليدية على الحرب الالكترونية (قانون الصراع المسلح – قانون الحرب – قانون اللجوء الى الحرب)
- معيقات التشريع للحرب الالكترونية.

1. إطار مفاهيمي حول الحرب الالكترونية والنزاع في الفضاء السبراني:

1.1. تعريف الحرب الالكترونية

قبل الشروع في تعريف الحرب الالكترونية وجب تحديد مفهوم الفضاء السبراني كونه المجال الذي يحتضن هذا النوع من الحروب، ويشير الى تلك البيئة الافتراضية التي يتم فيها نقل المعلومات الرقمية عبر شبكات الحاسوب، وتحتضن مختلف التفاعلات الصراعية والتعاونية ذات الطابع الرقمي والمعلوماتي.[1]

و تشير الحرب الالكترونية الى تلك العمليات الهجومية والدفاعية على مستوى الفضاء السبراني، وتستهدف في شقها الهجومي تعجيز العدو و إصابته بالعطب عن طريق تدمير نظم الحاسوب و شبكات الاتصال و قواعد البيانات الخاصة به، و بنيته الأساسية و مؤسساته الاستراتيجية و ذلك باستخدام مختلف الأسلحة المعلوماتية والالكترونية كفيروسات و ديدان الحاسوب (Worms)، و برامج التجسّس و القنابل المثبّتة في مواقع محدّدة، أما على الجانب الدفاعي

فتعمل على حماية الذات و القوات الصديقة من العمليات المماثلة الصادرة عن العدو عن طريق منظومات الدفاع الالكترونية و برامج المنع و الوقاية، أي منع العدو من الوصول الى القواعد المعلوماتية الحساسة[2]

حدد خبراء الحرب الالكترونية وفي مقدمتهم جيفري كار Jeffery Carr مجموعة من المعايير التي تحدد معالم الحرب الالكترونية أو الاعمال العدوانية التي ترتقي لدرجة الحرب acte de guerre [3]:

- الهجمات السبرانية ضد المواقع الحكومية أو الشبكات المدنية حتى دون ارفاقها بالقوة العسكرية.
- الهجمات السبرانية ضد المواقع الحكومية أو الشبكات المدنية التي تكون متبوعة بضربات عسكرية.
- الهجمات الالكترونية التي تستهدف البنى التحتية الهامة والحيوية.
- أعمال التجسس الالكتروني.

2.1. تعريف النزاع في الفضاء السبراني:

يشير النزاع في الفضاء السبراني الى الممارسات ذات الطابع الصراعي على مستوى الفضاء السبراني، والتي تصدر عن اطراف ما بغرض تحقيق ميزة على خصومهم ضمن هذا المجال وذلك بالاعتماد على الأدوات التقنية المختلفة والأسلحة المعلوماتية وتقنيات تستند أساسا على ابداع وتحكم العقل البشري.[4] .

- اركان النزاع السبراني:

- الأدوات والتقنيات التي تتطلب المهارة في الاستعمال والتحكم، وهو ما يبرز مجددا أهمية العامل الإنساني في احداث الفارق في هذا النوع من الحروب وحسمها.

- العمليات الهجومية والتي يقصد بها جميع الممارسات والأنشطة التي تستهدف اختراق أنظمة العدو بغرض الجوسسة او الاتلاف.
- الفواعل: وهي جميع الأطراف المشاركة في النزاع السبراني باختلاف صفاتهم (افراد – جماعات – دول..)
- الدوافع: فهناك من يهاجم لغرض الحصول على المال بحيث يحتضن الفضاء السبراني قدرا كبيرا من المعاملات التجارية، وبالتالي فإنه يمثل أرضية خصبة للسطو على الأموال بطريقة غير شرعية سوآءا بالابتزاز او النهب أو التحايل أو قرصنة بطاقات الائتمان وبيانات الولوج الى الحسابات المصرفية او الاسرار التجارية او مختلف المشاريع الاقتصادية[5]

كما يمكن أن تتخذ دوافع النزاع السبراني طابعا سياسيا من خلال توجيه رسالة سياسية معينة، على غرار ما حدث في الهجوم الالكتروني على استونيا، أو عسكريا، كتلك التي تشنها الجيوش الالكترونية للدول او قراصنتها المعتمدين وتسعى من خلال ذلك الى تحقيق أهداف استراتيجية، أو شخصيا بدافع اثبات الذات ورفع التحدي من خلال اختراق أعتى أنظمة الدفاع والحماية الالكترونية أو ابراز الجانب المهاري وفرض الذات.

2. مواطن الاختلاف بين الحرب الالكترونية والحروب التقليدية :

2.1. ميدان المواجهة او حقل المعركة :

يتسم حقل المعركة في الحروب التقليدية بوضوح المعالم والحدود والفواعل أيضا، بحكم ان المتخاصمين هم جيوش عسكرية او مقاتلين معلومين لدى بعضهم البعض، أما مجال الصدام في الفضاء السبراني فإنه يتسم بالافتراضية (غير ملموس) والشمول (لا يعترف بالحدود المادية) وينتشر فيه المدنيين الذين قد يشكلون أحيانا جزءا من الصراع (فواعل)، بالإضافة الى صعوبة تحديد هوية المتصارعين، وهو ما يضفي نوعا من التعقيد والغموض

على حروب ونزاعات الفضاء السبراني، وما يترتب عن ذلك لاحقا من صعوبة في تحديد وملاحقة مجرمي هذا النوع من الحروب ومحاسبتهم.

2.2 تحديد المسؤوليات:

على عكس الحروب التقليدية فإنه يصعب في الفضاء السبراني اسناد مسؤوليات الهجمات الالكترونية الى جهات حكومية نظرا لتعذّر التأكد والاحاطة بالمعلومات التالية [6]

- الة الهجوم وصاحبها.
- الموقع الجغرافي للآلة التي قامت بالهجوم.
- الفرد الجالس أمام لوحة مفاتيح الالة التي نفذت الهجوم.
- البلد الذي يندرج تحت اختصاصه الجهة المنفذة للهجوم.
- الكيان او المؤسسة التي تتبنى وترعى سلوك الجهة المبادرة بالهجوم.

3.2 الاختلاف في قدرات الفواعل:

يستمد الهجوم الالكتروني قوته من مهارة وعدد الفواعل المشاركة فيه، فالضربة الصادرة من فرد تلقى تكوينا تنقيا عاليا ضمن جيوش الكترونية تكون أشد حدة عن تلك الناجمة عن هاكر « Hacker » هاوي بالرغم من موهبته ومهارته، كما أن العمل ضمن فرق او مجموعات يكون أكثر نجاعة، أما الحروب التقليدية فإنها تعتمد على تعداد الجيوش وقوة الأسلحة وكثرتها، وتكتسي فواعلها صفة الجنود الذين ينخرطون بصفة مباشرة في الحرب ويمتلكون مؤهلات قتالية وعسكرية مادية وجسدية، على عكس القراصنة والمحاربين الالكترونيين الذين يستندون أكثر على المؤهلات المعرفية والتقنية. [7]

4.2 البعد المتعلق بالمسافات والحدود الوطنية :

في الحرب التقليدية قد تكون المسافات طويلة، واجتيازها امرا لابد منه لاختراق الحدود الوطنية لدولة ما، ويكون ذلك ملاحظا وملموسا مما يسمح

بإتباعه بالإجراءات القانونية اللازمة من طرف المجتمع الدولي، أو الدفاع الشرعي من طرف الدولة المستهدفة، أما في النزاع السبراني فلا وجود لعامل المسافة او الحدود الوطنية المادية، بحيث يكون الولوج الى نطاق الدولة المستهدفة اكثر سهولة من خلال الشبكة، وهو ما يوحي بتراجع مفهوم السيادة بمعناه التقليدي الصلب في الحروب السبرانية.[8]

5.2 مسائل الاسناد والوكالة:

يصعب في الحروب الالكترونية اسناد الهجمات الالكترونية ذات الطابع العسكري لجهة معينة، أو اثبات الوكالة عليها من طرف دولة معينة نظرا لصعوبة تتبع مصدر الهجمة وميزة التخفي وإمكانية التمويه التي تشوب هذا النوع من الحروب (إمكانية تغيير العنوان الالكتروني للمستخدم adress IP)، وبالتالي صعوبة تحديد المعايير اللازمة التي تفيد بتورط دولة ما في هجمات الكترونية ضد دول أخرى، والتي لا يمكن ان تتحقق بدون توفر شرطين أساسيين لإثبات ذلك وهما الاسناد والوكالة.

الاسناد: يقتضي ضرورة التأكد من إسناد مرتكب الهجوم الالكتروني الى الدولة، من خلال التحقق من ان هذه الأخيرة تسيطر سيطرة تامة على مرتكبي الجرائم الالكترونية ويقعون تحت سيادتها.

الوكالة: أي أن توكل الدولة أطرافا خاصة للقيام بعمليات عدوانية على مستوى الفضاء السبراني.

3. إسقاط قوانين الحروب التقليدية على الحرب الالكترونية:

لقد تعرضت العديد من الدول لهجمات الكترونية مست شبكاتها الحيوية وهددت امنها القومي بصفة مباشرة، وهو ما أدى الى فتح نقاش دولي حول مدى إمكانية تطبيق قانون النزاع المسلح على الحرب الالكترونية، خاصة بعد الهجمات السبرانية الروسية على جورجيا واستونيا، وعليه، ظهرت الحاجة الى الضوابط القانونية التي جسدتها العديد من المبادرات والأفكار التي لازالت في

طور النقاش ومن أهمها ابرام المعاهدات الدولية، على غرارالمعاهدات الخاصة بالأسلحة النووية ومكافحتها [9] مثل معاهدات حظر انتشار الأسلحة النووية NPT والمناطق الخالية من التجارب والتفجيرات النووية على كمعاهدة انتركتيكا[10]

1.3 اسقاط اليات الرقابة القانونية للأسلحة النووية على الأسلحة الالكترونية:

يكمن المشكل في تطبيق الرقابة القانونية على الأسلحة الالكترونية في عناصر أساسية غير مطروحة في مسألة الأسلحة النووية:

العنصر الأول:

حدة تأثير الهجمات الالكترونية التي لا تتناسب مع نظيرتها النووية، فبالرغم من الخسائر التي قد تنجم عن الهجمات الالكترونية التي تستهدف المحطات النووية والمصانع الكيماوية وأنظمة المرور، فإنها لاتصل حدة ومقدار الدمار التي تسببه الأسلحة النووية رغم انهما يمكن أن يحققا نفس الأهداف الاستراتيجية كإلحاق الشلل بالعدو.

العنصر الثاني

ويتعلق بإمكانية تفعيل اليات المراقبة والردع، فبالرغم من أن بعض الدول ممن تسعى الى تطوير الأسلحة النووية ترفض التعاون مع المنظمة الدولية للطاقة الذرية IAEA على غرار إيران، بل وأن بعضها لم توقع حتى على معاهدة حظر انتشار الأسلحة النووية NPT في شاكلة إسرائيل، إلا أنه من الممكن مراقبة ومتابعة مراحل تصنيع السلاح النووي، وتخصيب اليورانيوم بحكم أن الوكالات الدولية الخاصة والمختصة بمراقبة هذا النوع من الأنشطة على غرار فريق دعم الطوارئ النووية الأمريكي NEST يسهل عليه اكتشاف أماكن المفاعلات النووية والاشعاعات المنبعثة منها، وبالتالي اكتشاف الأنشطة

التي تجري داخلها، وهو ما يسهل من اتخاذ الإجراءات اللازمة لعرقلتها او إيقافها، إن توفرت الإرادة السياسية الدولية لذلك..[11]

العنصر الثالث:

يعتبر اختلاف وجهات النظر الدولية تجاه كيفيات مواجهة الجرائم والحروب السبرانية عائقا كبيرا في سبيل تبني أطر قانونية عالمية موحدة، ففي هذا الصدد تختلف مقاربات القوى العظمى وتصوراتها لطبيعة التدابير القانونية الواجب اتخاذها، بحيث تتبنى روسيا الاتحادية خيار ابرام المعاهدات الدولية على غرار مسائل الشأن النووي، في حين تفضل الولايات المتحدة الامريكية إشراك أجهزة إنفاذ القانون الدولي التي ترى فيها الالية المناسبة للتعاون بشكل أفضل للقبض على مجرمي الانترنيت.

2.3 اسقاط قانون الصراع المسلح LOAC (القانون الدولي الإنساني) على الحرب الالكترونية:

يعد تطبيق قانون الصراع المسلح على الحروب السبرانية من الاليات المقترحة للحد من حدة هذه الحروب وتقليل حدوثها، بحيث يمكن ان يكون ذلك من خلال اتفاق دولي جديد يتناول بشكل حصري الهجمات الالكترونية التي ترعاها الدولة، وهو ما قد يرجح الطرح الروسي على حساب الطرح الأمريكي، ويترافق ذلك مع إنشاء الية لمتابعة هذه الهجمات الالكترونية في شاكلة هيئة دائمة للاستجابة لحالات الطوارئ.

ينبع اقتراح هذه الالية من إدراك مفاده ان الخسائر الناجمة عن الهجمات الالكترونية لا تقل في حدتها عن مخلفات الحرب التقليدية وقد تصل في بعض الأحيان الى حجم خسائر الحرب النووية، ومنه فقد كان لزاما على الدول اعتماد تعريف جامع للحرب الالكترونية وتحديد الأطراف الفاعلة فيها من جهة، ورصد اليات المكافحة والردع ذات الطابع القانوني، ومحاولة تكييفها مع اللوائح السارية المفعول كالقانون الدولي الإنساني (قانون الحرب)، خاصة بعد الهجمات

الالكترونية على جورجيا التي مثّلت الدافع الرئيسي لبداية الجهود الدولية للتقليل من إمكانية حدوث الحروب السبرانية.

غير أن المباشرة في تطبيق الأطر القانونية على الحروب السبرانية يقتضي أولا الإجابة على مجموعة من المسائل المتعلقة بطبيعة الهجمات الالكترونية حول ما إذا كانت ترتقي لمستوى الحرب، ام انها ممارسات منعزلة عن ارادات الدول، ومن أهم هذه الأسئلة نجد:

هل تتوافق الهجمات الالكترونية مع النزاع المسلح؟ هل يمكن إثبات تورط الدول بطابعها الرسمي في الهجمات الالكترونية؟ هل هناك نية مسبّقة لإحداث ضرر من جرّاء هجمة الكترونية؟

ماهي طبيعة المخلفات والاضرار التي يمكن ان تنجر عن الهجمات الالكترونية (نقدية – بشرية – مادية..) [12]

هل يعبّر تصرف فرد معين عن موقف دولته أو يمثلها بالضرورة؟

هل يمكن أن ترتقي ممارساته الى ممارسات دولة؟

هل بإمكان الدولة ذاتها أن تثني فردا يقطن أراضيها أو يحمل جنسيتها عن القيام بأعمال الكترونية عدائية ضد دولة أخرى؟

لحد الساعة لم يتم التوصل الى الإجابة القطعية عن الأسئلة المطروحة، أو إيجاد السبل والاليات التقنية المناسبة لذلك، وكل ما يتم الاعتماد عليه هو افتراضات تستند الى سياقات تنفيذ الهجمات الالكترونية ونوعيتها أو حجمها مثلما تم ذكره سابقا، وهو ما يضفي نوعا من الضبابية واللايقين حول دور الدولة في هذه الهجمات، مما يضعف فرضيتا الاسناد أو الوكالة الى حين التوصل الى اكتشافات تقنية من شأنها التتبع الدقيق لأثر الهجمة والهدف منها وتحديد هوية المهاجم.

إن استخدام مصطلح الحرب الالكترونية يقتضي قانونا اثبات تورط الدول فيها، وعلى هذا الأساس تحاول الدراسة التركيز على هجمات الكترونية

التي من المفترض أن تكون الدول قد تورطت فيها بشكل رسمي بناءا على سياقات معينة، وخصوصا السياق السياسي، غير ذلك، فإنه لا يمكن إسناد الهجمات التي تتولاها الكيانات والأشخاص الى الدولة دون أدلّة قطعية، الا اذا فوضت هذه الأخيرة (الدولة) بشكل مباشر وصريح جزءا من مهامها ووظائفها الى كيان خاص، غير ذلك فإنه يتعذّر تحميل دولة معينة مسؤولية جرائم وهجمات الكترونية بصفة رسمية،[13] حتى ولو تم التعرف على منفذي هذه الهجمات والتأكد من كونهم يحملون جنسيتها ويقيمون في ترابها، وذلك لعدم توفر معيار السيطرة الكاملة والفعالة على ممارسات مواطنيها الموجبة للمتابعة القانونية، ففي ظل حروب الفضاء السبراني الغير مقيدة يسهل على جميع الفواعل والكيانات سوآءا كانوا أفرادا أو جماعات او قراصنة محترفين الولوج الى أي نظام معلوماتي حتى ولو كان تابعا لدولة أجنبية قريبة كانت أم بعيدة، إضافة الى الطبيعة المعقدة للفضاء السبراني الذي زادته خاصية الاتصال الشبكي العالمي تعقيدا، فإنه بذلك يصعب على الدولة ان لم نقل يستحيل عليها مراقبة الممارسات الالكترونية لمواطنيها، وهو ما يقودنا الى الجزم بغياب الأدلة الكافية لا ثبات تورط الدولة، و ما يدفع الى معالجة قضايا الهجمات الالكترونية بمنطق الافتراض والسياقية.

كل هذه المعطيات التي تفرضها خصوصية الهجمات الالكترونية تدفع بالدول الى التعاطي معها بمنطق الافتراض والسياقية، خاصة في ظل غياب الأدلة الكافية عن مصدر هذه الهجمات الالكترونية وعدم وجود قاعدة معرفية متينة بشأنها، وفيما يلي بعض الهجمات الالكترونية التي استهدفت بعض الدول والتي من المفترض أن دولا أخرى تقف ورائها بالنظر الى المعايير السالفة الذكر [14]

قيرغيزستان: في 18 يناير من عام 2009 تم استهداف ثلاثة من أصل اربع مزوّدي خدمات الانترنيت في قيرغيزستان عديدة لتصبح غير قادرة على

استيعابها فتتعطل، وهو ما حال دون وصول الانترنيت الى معظم سكان البلد، وقد تزامن هذا الهجوم مع المحاولات المتكررة للحكومة الروسية بإجبار رئيس قيرغيزستان على إغلاق قاعدة ماناس الجوية امام حركة المرور الأمريكية.

كوريا الجنوبية: في 4 يوليو من عام 2009 أسفر هجوم DDOS عن تعطيل جل مواقع الويب الحكومية والتجارة لكوريا الجنوبية، وقد قامت هذه الأخير باتهام جارته الشمالية استنادا الى سياق التوتر السياسي والاختلاف الأيديولوجي والعداء بينهما.

3.3 إسقاط قوانين الحرب التقليدية (jus ad bellum) and (jus in bello) على الحرب الالكترونية

تنقسم قوانين الحرب التقليدية بحكم الاختصاص الى فرعين أساسيين وجب التفريق بينهما، واسقاط كل منهما على الحروب السبرانية أو النزاع في الفضاء السبراني.

يتمثل الفرع الأول من قوانين الحرب في قانون اللجوء الى الحرب (jus ad bellum)، ويختص بتحديد المعايير التي تخوّل الدول اللجوء الى الحرب واستعمال القوة المسلحة، فهو ينظم مسائل ما قبل الحرب أي: متى يمكن لدولة ما اللجوء الى استعمال القوة المسلحة ودخول الحرب.

أما الفرع الثاني المتمثل في قانون الحرب (jus in bello) فإنه يختص في مسائل تنظيم استعمال القوة المسلحة اثناء الحرب، وكلا الفرعين مدرجين في المادة 38 من النظام الأساسي للمحكمة الجنائية الدولية. [15]

أ - قانون اللجوء الى الحرب (jus ad bellum) والحرب السبرانية:

يشكل ميثاق الأمم المتحدة المصدر الرئيسي لقانون اللجوء الى الحرب jus ad bellum والذي يحظر في مادته (2-4) بشكل صريح على كل الأطراف الموقعة على الميثاق استعمال القوة المسلحة في العلاقات الدولية الا في حالتين اثنتين: حالة التفويض من مجلس الامن الدولي تحت طائلة البند

السابع من ميثاق الأمم المتحدة (الحل العسكري القسري بعد فشل الحل السلمي الذي ينص عليه البند السادس)، أو في حالة الدفاع الشرعي عن النفس التي تخوّل الطرف المعتدى عليه استعمال القوة الشرعية، وهو ما يندرج في إطار نظرية الحرب العادلة. (16)

تعترض مجموعة من التحديات عملية اسقاط قواعد قانون اللجوء الى الحرب على النزاع او الحرب في الفضاء السبراني، وذلك نظرا لمجموعة من العوامل أهمها:

- مسألة التحيين الزمني للقانون، بحيث ان الفترة التي شرعت فيها القواعد القانونية الخاصة ب jus ad bellum لم تكن موجهة للنزاعات والحروب السبرانية، والتي لم تكن موجودة أصلا آنذاك، أو على الأقل لم تكن بنفس الحدة التي هي عليها الان.
- مسألة الفواعل: بحيث ان النصوص والقواعد القانونية الخاصة بقانون اللجوء الى الحرب jus ad bellum تحدد معايير استعمال القوة بين الدول كفواعل رئيسية ووحيدة، خاصة وأن الفترة التي حرر فيها الميثاق لم تعرف بروز فواعل من غير الدول، في حين ان عددا كبيرا من الهجمات العدوانية السبرانية يصدر عن أفراد وكيانات ومؤسسات ليست بمستوى الدولة، ناهيك عن صعوبة اسناد هذه الاعمال لدولة ما أو اثبات الوكالة عليها.
- مسألة تحديد المفاهيم والتعريفات: على الرغم من أن ميثاق الأمم المتحدة المنظم للحروب في شاكلة jus ad bellum جاء لتحديد معايير استعمال القوة التقليدية بين الدول، إلا أنه وفي نفس المجال لم يحدد أو يفصل بين مفاهيم (استخدام القوة) و (التهديد باستخدام القوة) و(الهجوم المسلح)، واكتف المجتمع الدولي في ذلك بالرجوع الى العرف الدولي، ومع غياب

تعاريف محددة للمفاهيم سالفة الذكر في الحرب التقليدية فإنها حتما تغيب في الحرب السبرانية وهي الأكثر تعقيدا وغموضا مقارنة بسابقتها. (17)

- مسألة انتقال تضارب وتناقضات بعض قواعد القانون الدولي بخصوص الحرب التقليدية الى الحرب السبرانية: فمثلا تحظر المادة 2 من ميثاق الأمم المتحدة في فقرتها الرابعة جميع اشكال استخدامات القوة التي قد تضر بالأشخاص او الممتلكات إلا في حالة الدفاع الشرعي عن النفس، في حين تجيز المادة 4 أفعالا وممارسات في شاكلة عقوبات اقتصادية وهي إجراءات تضر مباشرة بالأشخاص والممتلكات، هذا التناقض يتنقل بصفة الية ومباشرة الى مسائل الحروب والنزاعات السبرانية في حال قمنا بعملية الاسقاط، ويمكن شرح ذلك في المثال التالي.

ب- قانون الحرب (jus in bello) والحرب الالكترونية:

يستند قانون الحرب jus in bello أو القانون الدولي الإنساني في جزء كبير منه على أحكام **اتفاقيات جنيف** ونظائرها العرفية، وينظر هذا القانون أساسا في المسائل العسكرية البحتة أثناء الحرب، وبالضبط في كيفية استعمال القوة المسلحة استنادا على معايير الضرورة العسكرية، التمييز، التناسب. (18)

يقوم معيار الضرورة العسكرية على مبدأ أساسي مفاده أن المقصود والهدف من العمليات العسكرية يجب ان يكون عسكريا، وعليه فإن الحرب او استعمال القوة المسلحة حسب هذا المبدأ لا تكون شرعية الا إذا صدرت عن جهات عسكرية تجاه أهداف عسكرية، سوآءا كانت جيوش أو كيانات انخرطت في خوض غمار الحرب والعمليات المسلحة، بحيث تكون المواجهة بين جيشين نظاميين، أو جيش نظامي وجماعة مسلحة (حرب لا تماثلية)، ويمنع فيها استعمال أي شكل من أشكال القوة ضد أهداف غير عسكرية. (19)

أما معيار التمييز في قانون الحرب jus in bello فيركز على ضرورة تفادي الأهداف المدنية في العمليات العسكرية، والحرص على أن تكون موجهة ضد

أهداف متماثل الصفة (أي مسلحة كالجيوش أو الجماعات المسلحة) ذات طابع عسكري. (20)

في حين يركز معيار التناسب على حجم ومقدار الخسائر والاضرار الناجمة عن العمليات العسكرية في حال رد الفعل، والتي يجب ان تكون متناسبة مع الخسائر التي تم تكبّدها من جراء الضربة العدوانية، و تتناسب أيضا مع الميزة العسكرية المتوقعة. (21)

بالنظر لما سبق، هل تنطبق القواعد القانونية ل jus in bello على طبيعة الحرب السبرانية؟

فيما يخص مبدأ الضرورة العسكرية والتمييز فإنه يصعب التحقق منهما أو تحقيقهما في سياق الحرب السبرانية، بحيث يجب أن يؤدي الهجوم على نظام معلوماتي معادي الى إتلاف اهداف عسكرية بحتة، على غرار نظم المعلومات الخاصة بالجيوش او الصناعات العسكرية، وهو ما جسده الهجوم الالكتروني stuxnet ، غير أن هذه العملية تعتبر فريدة من نوعها و من الصعب تكرارها في تجارب أخرى، بحيث يصعب تحقيق ميزات عسكرية من خلال هجمات الكترونية دون التعرض او المساس بقطاعات مالية او اقتصادية أو إتلاف معلومات أو بيانات شخصية لمرتادي مواقع التواصل الاجتماعي .

كما أن الجيوش الالكترونية تمارس عملياتها العسكرية عبر شبكات اتصالات تستخدم أساسا للأغراض السلمية، وتكون أهدافها ذات طابع مدني كشبكات توليد الكهرباء أو أنظمة المرور والاتصالات التابعة للخصم أو العدو، وهو ما يدفعنا للاستنتاج انه من الصعب الحفاظ على الطابع العسكري البحت لعمليات الفضاء الالكتروني وأهدافها، و بالتالي صعوبة تحقيق معيار التمييز بين ما هو عسكري ومدني، نظرا لخاصية الاتصال الشبكي المعقدة وكذا تعدد الفواعل على مستوى الفضاء السبراني، وبالتالي، فإن إسقاط نصوص وقواعد قانون الحرب على الحروب السبرانية لايزال بعيد المنال وصعب التحقيق

ويحتاج الى دراسات معمقة في المجالات التقنية وجهودا كبيرة لموائمتها مع الضوابط التشريعية للقانون الدولي.

أما معيار التناسب في حروب الفضاء السبراني فإن تحقيقه يقتضي التأكد من أن الضربة الالكترونية الموجه ضد هدف ما لا تفوق الميزة العسكرية المتوقعة، وتتناسب في حجم الخسائر مع نظيرتها في العمليات العسكرية التقليدية، على سبيل المثال، يجب تقييم الاضرار الناجمة عن مهاجمة محطة كهرباء، بحيث يجب على القائد العسكري أن يمتلك معلومات استخباراتية كافية عن تلك المحطة ليتأكد من أن مهاجمتها ليؤدي الى مضاعفات خارجة عن نطاق الأهداف العسكرية المسطرة.

بالرغم من اختلاف طبيعة حقل المعركة (Battle Field) والفواعل وكذا الأسلحة المستعملة، فإن الغايات الاستراتيجية وتبعات الحروب السبرانية ورهاناتها لا تختلف كثيرا عن الحروب التقليدية، وهو ما دفع ببروز العديد من محاولات الاسقاط القانوني التي اصطدمت بمجموعة من التحديات أهمها معايير التناسب، التمييز والضرورة العسكرية.

4. معيقات التشريع للحرب الالكترونية:

تواجه عملية اسقاط الأطر القانونية ذات الطابع التقليدي الخاص بالحرب المسلحة على الحرب الالكترونية مجموعة من العوائق والتحديات يمكن تلخيصها فيما يلي:

- صعوبة اسقاط قواعد قانونية على مواضيع ومسائل ذات طابع تقني على غرار صناعة وإنتاج البرمجيات، بحيث يصعب على المشرّع ذو الاختصاص القانوني ان يسن تشريعات دون دراية بالمجالات التقنية أو بمعزل عن تقنيين واختصاصيين في تكنولوجيات الحاسوب والكمبيوتر، وبالتالي فإن أي قاعدة قانونية تستدعي في صياغتها المزاوجة بين التشريع

والتقنية تفترض على من يتولى التشريع فهم عبارات واليات ذات طابع تقني بحت [22].

- الديناميكية السريعة والمستمرة لمسائل الفضاء السبراني نظرا لطبيعته المعقدة التي تتسم بالاتصال الشبكي بين مختلف الفواعل وفي مختلف أنحاء العالم. [23]
- صعوبة التوفيق بين ثوابت السيادة الوطنية ومقتضيات الرقابة الدولية، خاصة اذا علمنا ان العمليات العدوانية والاجرامية على مستوى الفضاء السبراني تحمل خاصية شمولية عابرة للحدود والقوميات.
- اختلاف الرؤى الدولية حول كيفية التنسيق الأمني بين الدول، وكذا اختلاف تصوراتها لطبيعة السياسات التي يجب انتهاجها لمواجهة التهديدات السبرانية.
- نقص الثقافة المعلوماتية لدى العديد من الدول، فقد بدأت معظمها في اصدار التشريعات والضوابط القانونية في أواخر التسعينات مما يترك المجال مفتوحا لتنامي الممارسات العدوانية في الفضاء السبراني.
- قلة المعرفة والاجتهادات في مجال التشريعات السبرانية، فالمعارف التقنية والتحكم بمسائل ومواضيع الامن المعلوماتي تساعد على صياغة قواعد قانونية وتؤسس لها، خاصة في ظل تعدد الاختصاصات القانونية ضمن هذا الفضاء (المعاملات الالكترونية- التجارة الالكترونية – حماية البيانات الخاصة – الجرائم السبرانية – حرية التعبير – حماية حقوق الملكية الفردية – مكافحة الإرهاب السبراني – التحقيق الجنائي – التحكيم عبر شبكة الانترنيت – الضوابط المهنية والأخلاقية على شبكة الانترنيت – المحتوى غير المشروع).

خاتمة

تختلف الحرب الالكترونية في طبيعتها عن الحرب التقليدية، لكنهما لا يختلفان في الغايات والتبعات، ومنه برزت الحاجة الى تقنين الحرب الالكترونية من أجل تحقيق الامن والسلم في الفضاء السبراني والعالم الواقعي بحكم ان مخرجاتها ونتائجها تنعكس بصفة مباشرة على الامن القومي للدول.

ان الاختلافات البنيوية بين الحروب التقليدية والحرب الالكترونية إضافة الى خصوصية هذه الأخيرة، يجعل من الصعب اسقاط قوانين الصراع المسلح والقانون الدولي الإنساني (قانون الحرب) على الحرب الالكترونية كمحاولة لإضفاء الطابع القانوني على هذا النوع من الحروب لتقييدها وإدارتها أو الحد من انتشارها، وذلك لما يشوبها من صعوبات في تحديد المسؤوليات عن الهجمات العدوانية الالكترونية وتعذّر اسنادها او اثبات الوكالة عليها لدول أو جهات معينة، وبالتالي استحالة المتابعة القانونية للأعمال العدوانية ذات الطابع المعلوماتي.

وعليه، وبالنظر لما تقدم، اهتدت الدراسة الى ضرورة مضاعفة الجهود المعرفية التي تزاوج بين الجوانب التقنية والقانونية في سبيل إيجاد ضوابط تشريعية وقانونية خاصة بطبيعة الحرب الالكترونية لتحقيق الامن السبراني وتخفيف حدة وتبعات هذا النوع الجديد من الحروب.

الهامش:

1- Andress, Jason And Winterfeld ,Steve, (2011), Cyber Warfare Techniques, Tactics and Tools, for security practitioners, Syngress imprint of ELSEVIER, first edition.

2- سلامة، صفات أمين، (2005)، أسلحة حروب المستقبل بين الخيال والواقع، مجلّة الدراسات الاستراتيجي، مركز الإمارات للدراسات والبحوث الاستراتيجية، ع 112

3- Carr, Jeffrey, (2009) Inside cyber warfare, O'Reilly media,Inc.,1005 Gravenstein Highway NorthSebastopol, first edition

4 - Mness, Ryan C, and Valeriano، Brandon, The Impact of Cyber Conflict on International Interactions, Armed Forces & Society, reprints and permission: sagepub.com/journalspermission.nav.

5- lin, Herb,(2017), fundamentals of cyber conflicts, Stanford University, cs 203

6- روبينسون، إيزابيل، ونول،إيلين ، (2012)،النزاع السبراني والقانون الدولي الإنساني، المجلة الدولية للصليب الأحمر- مجلد 94 ،886 ص.

7- Stimpson, Maj R.T, (2014) CYBERWARFARE WILL NOT REPLACE CONVENTIONAL WARFARE, canadian forces college, exercise solo flight, JCSP 41 – PCEMI 41

8- روبينسون ،إيزابيل ، مرجع سابق.

9- Carr, Jeffery, op, cite.

10-T.Richelson, Jeffrey, (2009) Defusing Armageddon: Inside NEST, America's Secret Nuclear 12-Bomb Squad, New York : W.W. norton & company.

11- HUGHES ,Dr Rex, Towards a Global Regime for Cyber Warfare, Cyber Security Project, Chatham House, London.

12-J. SHACKELFORD, Scott, (2010), State Responsibility for Cyber Attacks: Competing Standards for Growing Problem, Conference on Cyber Conflict Proceedings, University of Cambridge, Cambridge, UK.

13-SANG-HUN, CHOE and MARKOFF, JOHN (2009) *Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea, the new york Times,* TECHNOLOGY, https://www.nytimes.com/2009/07/09/technology/09cyber.html Visited on 20 11 2018

14- Halpin, Edward, Trevorrow, Philippa, David Webb and Wright ,Steve Cyberwar, (2006), Netwar and the Revolution in Military Affairs, Editorial matter and selection ©

15- TAŞDEMİR, Fatma, ALBAYRAK, Gökhan,(2017) The Law of Cyber Warfare In Terms of Jus Ad Bellum and Jus In Bello: Application of International Law to the Unknown?Journal of law, Vol 3 (2)
16- Kilovaty, Ido, Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare, American University National Security Law Brief, Vol. 5, No. 1.
17- counsel, General, (2016), of Department of defense law of war manuel USA, Law of war: Description of Changes ,1600 defense pentagon washington D C 2030 – 1 1600.
18- غـايس، روبـين ، (2006) هياكـل النزاعـات غـي المتكافئة،المجلـة الدوليـة للصـليب الأحمر، المجلد 88- العدد 864.
19- غايس، روبين، المرجع نفسه.
20- غايس، روبين، المرجع نفسه.
21- حـرب، وسـيم ، (15-14 مـارس)، ورشـة عمـل حـول إرشـادات الإسـكوا لتنسـيق التشريعات السبرانية في المنطقة العربية ، الاسكوا، هيئة الأمم المتحدة.
22- حرب، وسيم ، المرجع نفسه.
23- Ángel Mendoza, Miguel,(2017), Challenges and implications of the enactment of laws relating to cybersecurity,in : https://www.welivesecurity.com/2017/03/13/challenges-implications-cybersecurity-legislation/