الحروب الالكترونية وإستراتيجية التصدي لها كتهديد جديد للسلم والأمن الدولي "منظمة حلف شمال الأطلسي نموذجا"

بقلم /.فاروق حمودة
طالب دكتوراه - كلية الحقوق سعيد حمدين- جامعة الجزائر 1

ملخص:
تهدف هذه الدراسة إلى معرفة حجم المكانة التي بات يحتلها الفضاء الالكتروني على الساحة الدولية، حيث أصبح هذا الأخير ، حلبة لخوض الحروب الالكترونية، التي ازدادت حدتها أكثر مع ارتفاع وتيرة التقدم التكنولوجي والتقني والالكتروني، وهو ما سهل المجال لإمكانية الاعتداء على أية دولة أو منظمة في وقت قصير وبتكلفة قليلة، وذلك عن طريق استخدام الانترنت ووسائل الاتصال الالكتروني.
لذلك ومن منطلق هذه الأهمية البالغة لهذا الفضاء، ارتأينا تسليط الضوء على منظمة حلف شمال الأطلسي "الناتو"، باعتبارها نموذج لهذا الموضوع الهام من جهة، وكذا باعتبارها منظمة أمنية إقليمية تستند إلى مبدأ التضامن الجماعي لحماية دولها الأعضاء من جهة أخرى، وهو ما جعلها تتخذ جملة من القواعد والتدابير، التي صيغت في إطار إستراتيجية حماية فضائها الالكتروني باعتباره بات تهديدا مباشرا لسلامة وأمن دولها الأعضاء.
الكلمات الدالة: الأسلحة الالكترونية- استراتيجيات الأمن- دليل " تالين"- منظمة حلف شمال الأطلسي- العولمة التقنية والتكنولوجية.

Résumé:

Cette étude vise à mesurer le poids de l'électronique à l'échelle internationale. Ce domaine devient une scène aux guerres qui ne cessent de s'intensifier surtout avec les avancées technologiques, en ce qui rend facile à tout pays de menacer, en utilisant l'Internet et les moyens électroniques de communication, n'importe quel pays ou organisation en peu de temps et avec des charges faibles. C'est pourquoi, nous concentrons notre étude sur l'OTAN qui nous en est, d'une part, un échantillon et d'autre part, une organisation chargée de la sécurité régionale qui mise sur la solidarité pour protéger ses Etats membres et met au point une stratégie de lutte pour protéger son espace électronique en prenant les précautions nécessaires.

مقدمة:

تعتبر الحروب الالكترونية[1] (ELECTRONICWARFARE)، إحدى أهم الوسائل الحديثة التي عاصرها الإنسان في خضم التطورات التي شهدتها الساحة العالمية[2] ، فهي تعتبر بمثابة امتداد للحروب التقليدية، القائمة على الاشتباك المباشر والمواجهة بين الأطراف المتحاربة، بواسطة مختلف الأسلحة، التي تؤدي إلى تبعات إنسانية وخيمة، تلحق بالأعيان المدنية، والسكان المدنيين.

هذا ولا يختلف اثنان، أن حجم الأضرار البليغة التي باتت تلحقها الحروب القائمة عبر الفضاء الالكتروني، على الإدارات الحكومية، والأعمال، والاقتصاد تضاهي وتفوق حجم الحروب التقليدية، وهو ما أدى بفقهاء القانون الدولي، إلى طرح مفهوم الدفاع الشرعي عن النفس، الذي نصت عليه المادة (51) من ميثاق هيئة الأمم المتحدة لعام 1945 ، والتي أجازت بموجبه للدول فرادى وجماعات، حق استخدام القوة

المسلحة، لمواجهة أي اعتداء، أو عدوان مسلح، يهدد كيانها الإقليمي أو استقلالها السياسي[3] ، لذلك فالدول تستطيع أن تمارس هذا الحق سواءا منفردة، أو من خلال جماعات، تتفق على المساعدة المتبادلة إذا ما تعرضت إحداها لأي هجوم أو عدوان[4] ، كما هو عليه الحال، في إطار معاهدة "واشنطن"، المعقودة بتاريخ :04 افريل 1949 ، والتي أعلنت عن ميلاد منظمة حلف شمال الأطلسي (NORTH ATLANTIC ORGANISATION TREATY)، أو ما يعرف بحلف الناتو، كمنظمة أمنية إقليمية، تعنى بمهمة ضمان أمن وحرية مواطني كل الدول الأعضاء في الحلف، استنادا لمبدأ التضامن الجماعي، الذي جاءت به المادة الخامسة (05) من معاهدة الحلف في نصها التالي:"تتفق الدول الأطراف في الحلف، على اعتبار أي هجوم مسلح على اروبا و أمريكا الشمالية، ضد دولة أو عدة دول أخرى، هجوما موجها ضدها جميعا، وبالتالي يحق لهم سواءا فرادى أو جماعات التدخل الفوري لنجدة الحليف"[5].

ومع تحول الفضاء الالكتروني العالمي (CYBER SPACE)، إلى حلبة لخوض معارك حقيقية في عالم افتراضي، يعتمد على كل ما هو جديد من صيحات التكنولوجيا الرقمية والاتصالات الحديثة، أولت منظمة حلف شمال الأطلسي، بالغ اهتمامها لهاته الحروب الرقمية الجديدة، باعتبارها عتبة تهديد جديد تمس برخاء وامن واستقرار الدول والأفراد في المنطقة الأطلسية ككل، مثلها مثل الحروب التقليدية، الأمر الذي فرض على الحلف، تطوير أساليب الدفاع والهجوم في الفضاء الالكتروني، بما في ذلك استخدام القوة المسلحة للتصدي لأية هجمات أو اختراقات الكترونية، تهدف إلى تعطيل البنى المعلوماتية، وإلحاق إصابات عرضية في صفوف الأعيان المدنية والسكان المدنيين، فإلى أين وصلت جهود منظمة حلف شمال الأطلسي للتصدي للحروب الالكترونية، وهل استدعى الأمر فعلا

حتمية استخدام القوة العسكرية المسلحة لردع هاته الحروب في إستراتيجية الحلف؟

وللإجابة على هذه التساؤلات، ارتأينا تقسيم هذه الورقة البحثية إلى مبحثين، ندرس في المبحث الأول: الحروب الالكترونية كتهديد جديد للمجال الأمني، أما المبحث الثاني، نتناول فيه جهود منظمة حلف شمال الأطلسي لمجابهة هذه الحروب الالكترونية.

المبحث الأول: الحروب الالكترونية كتهديد جديد للمجال الأمني

إن تقييم مشروعية الحروب الالكترونية في منظور القانون الدولي الإنساني، يستدعي قبل بادئ ذي بدء، التطرق لمفهوم وتعريف هاته الحروب، حتى نتمكن من حصر الأضرار المادية والمعنوية التي قد تتبعها للرقي بها إلى مستوى الحروب المسلحة التقليدية.

المطلب الأول: الحروب الالكترونية "المفهوم الاصطلاحي"

تعرف الحروب الالكترونية بأنها: "حروب تخيلية أو افتراضية (VIRUTAL REALITY)، ذات طبيعة غير ملموسة تحاكي الواقع بشكل شبه تام، وهي حرب بلا دماء، تتلخص أدوات الصراع فيها على المواجهة الالكترونية والبرمجيات التقنية، وجنود من برامج التخريب المحوسبة، وطلقات من لوحات المفاتيح ونقرات المبرمجين، في بيئة اصطناعية، تحاول ما أمكن الوصول إلى صورة حقيقية لملامح الحياة المادية الملموسة"[6].

كما تعرف هذه الحروب كذلك بأنها: "الحروب التي تستهدف المعلومات، وهي تعبير عن الاعتداءات التي تطال مواقع البيانات الموجودة على الانترنت، وتحاول الاستيلاء على معطياتها، بين أطراف متناقضة الأهداف، ومتعارضة المصالح، ومختلفة المواقف"[7].

كما ربط دليل "تالين"، بشأن تطبيق القانون الدولي الإنساني في الفضاء الالكتروني، الذي أعده نخبة من الخبراء العسكريين والقانونيين لمنظمة حلف شمال الأطلسي سنة 2008 ،الحرب الالكترونية بحجم الآثار

المدمرة التي يمكن أن تتسبب فيها تلك الحروب، فعرف هذه الأخيرة بأنها: "كل عملية الكترونية، سواءا كانت هجومية، أو دفاعية، يتوقع أن تتسبب في إصابة، أو قتل أشخاص، أو الإضرار بأعيان، أو تدميرها"[8].

والملاحظ أن كل هذه التعريفات، ترى في الحروب الالكترونية، بأنها استخدام العنف، وممارسة الأنشطة التخريبية، أو التهديد باستخدامها، في الفضاء الالكتروني، من اجل تعزيز أهداف سياسية، أو اقتصادية، أو اجتماعية، أو إيديولوجية، وهو ما يعكس بحق، اعتبار الباحث الهندي في مجال الانترنت"ASHISH PANDEY"، هذه الأعمال بمثابة جرائم الكترونية، تستدعي تحرك المجتمع الدولي كافة، من أجل ملاحقة المجرمين عندما يقع الهجوم على دولة معينة[9].

المطلب الثاني: مخاطر الحروب الالكترونية على المجال الأمني

إن تواتر وتنظيم سيناريوهات الحروب الالكترونية عبر الفضاء الالكتروني، واستهداف المحتوى ألمعلوماتي للأهداف العسكرية، والسياسية والاقتصادية والمالية، يجعل السكان المدنيين عرضة لخطر الحرمان من الاحتياجات الأساسية للحياة، مثل مياه الشرب، الرعاية والإغاثة الطبية، الكهرباء، وخطوط الملاحة البرية، والبحرية، و الجوية، والبنوك، والبورصة وغيرها، فتعطيل مثل هذه المجالات، سيؤدي إلى نتائج مادية خطيرة، وإصابات في صفوف السكان المدنيين، وهو ما جعل الدكتور سلطان محمد سيد يقول: "لا يجب أن ننادي اليوم فقط بمهاجمة أسلحة الدمار الشامل، بل يجب أن نرفع أصواتنا لمحاربة أسلحة التعطيل الشامل" ،فتعطيل المنظومة الالكترونية، سيؤدي لا محالة، إلى تعطيل شامل للعديد من مجالات الحياة الضرورية، مما يؤدي إلى تضرر صحة وحياة الآلاف من الناس[10]، لذلك دعت اللجنة الدولية للصليب الأحمر، على لسان مستشارها القانوني الدكتور "جيزيل لوران"، أن الحروب الالكترونية اليوم، لها قواعد وحدود، وتحظى بنفس القدر من الاهتمام الذي ينطبق على استخدام البنادق والمدفعية والصورايخ[11].

المطلب الثالث: الحروب الالكترونية في منظور القانون الدولي الإنساني

تتسلح الحروب الالكترونية، بالعديد من الوسائل والأدوات التقنية والرقمية، التي يتم توظيفها في الصراعات الافتراضية الدائرة عبر الفضاء الالكتروني، في صورة مشابهة لتلك الحروب التقليدية التي تندلع على ارض الواقع، لذلك فان تقييم مشروعية هذه الأسلحة الجديدة المستخدمة أثناء النزاعات المسلحة، يقتضي التعرف عليها، لإدراجها ضمن خانة الأسلحة المحرمة دوليا، وفقا لما جاءت به قواعد و نصوص اتفاقيات القانون الدولي الإنساني.

هذا ويجدر التنويه في هذا الصدد، بأن الأسلحة المستخدمة في الحروب الالكترونية، تتغير وتتطور باستمرار، مواكبة في ذلك حجم التطور التكنولوجي والتقني الذي بلغه العلم، وعليه فان إعداد وحصر قائمة مسبقة بهذه الأسلحة يعتبر ضربا من الخيال، لذلك سنتولى عرض نماذج عن هاته الأسلحة المستخدمة في الحروب الالكترونية، للتعرف على موقف القانون الدولي الإنساني منها.

أولا: بعض نماذج الأسلحة الالكترونية:

1- **التجسس المعلوماتي: (SPYWARE INFORMATION)**

يعتبر من أشهر وأقدم أسلحة الحروب الالكترونية، فهو يقوم على التنصت، والتجسس على المعلومات الصادرة عن أجهزة الحواسيب، والأقمار الصناعية والهواتف المحمولة، وغيرها من وسائل التجسس المعلوماتي[12].

2-الاختراق الالكتروني: (PENTRATION MAIL)

وهو عبارة عن إنشاء نظام، أو برنامج الكتروني، يهدف إلى الدخول إلى قلب معلومات الخصم لاستغلالها وتدميرها، قصد التفوق عليه، وإحداث ميزة أكيدة في المجال الأمني أو العسكري أو الاقتصادي أو السياسي.

3- زرع الفيروسات التقنية في البيئة المعلوماتية:

وهي عبارة عن برامج الكترونية مدمرة، تهدف إلى إحداث فوضى في أنظمة التشغيل الخاصة بالخصم، بغية كبح تدفق ووصول المعلومات إليه، وافقداه لكامل مخزونه الرقمي.

4-**القرصنة الالكترونية: (ELECTRONIC PIRACY)**

وهي من أضخم الأسلحة الالكترونية المستخدمة عبر الفضاء الرقمي، فهي تعتمد على تجنيد كم هائل من التقنيين المؤهلين، الذين يطلق عليهم اسم "الهاكرز"(HACKERS)، للتعامل مع الحاسوب بخبرة عالية جدا، تمكنهم من التغلغل لاقتحام وسائل ونظم الاتصال والتكنولوجيا، من حواسيب، وهواتف وموجات الكترونية، وألياف ضوئية.

5- **الأقمار الصناعية: (SATILITTES)**

وهي أسلحة ذات دلالات استحواذية، هدفها السيطرة على اكبر قدر ممكن من المعلومات، فهي قادرة على التقاط ملايين الصور وإرسالها إلى القاعدة المعلوماتية الموجودة على الأرض، لذلك فالأقمار الصناعية تعتبر من أكفء الوسائل وأكثرها تعقيدا في حسم المعارك والحروب الالكترونية، فهي قادرة على توجيه الصورايخ والقاذفات النارية صوب أهدافها على الأرض[13].

6- **الخداع الالكتروني:**

وهو كذلك من أهم وسائل تأمين الحروب الالكترونية، حيث يشتمل هذا السلاح الرقمي على عدة وسائل أهمها: التقليد الصوتي، التشويش الالكتروني، التضليل المعلوماتي، الخداع ونشر الشائعات، انتحال الشخصيات افتراضيا، الابتزاز الالكتروني، وغيرها من أساليب الخداع الرقمي[14].

ثانيا: موقف القانون الدولي الإنساني من الأسلحة الالكترونية

إن الحديث عن الأسلحة المستخدمة في الحروب الالكترونية، باعتبارها أسلحة جديدة تستعمل أثناء النزاعات المسلحة، ويحتمل أن

تكون لها تبعات إنسانية وخيمة، يستدعي التذكير أولا، بالحماية الخاصة التي يوفرها القانون الدولي الإنساني للممتلكات و الأشخاص الذين لا يشتركون في الحروب، من خلال اتفاقيات جنيف الأربع المعقودة بتاريخ 1949/08/12 ، وكذا البروتوكولين الاضافين الملحقين بها المعقودين بتاريخ 1977/06/08. [15]

وإذا كانت وثائق واتفاقيات هذا القانون، لم تحمل بين ثنياها في صورة واضحة وصريحة اعتبار هذه الأسلحة الالكترونية، كوسيلة من وسائل القتال المستخدمة أثناء الحروب والنزاعات المسلحة، فان تحليل نص المادة 36/فقرة 01 من البروتوكول الإضافي الأول الخاص بالنزاعات المسلحة الدولية لعام 1977 يستنتج منها حظر هذا النوع من الأسلحة، باعتبار أن المادة ألزمت جميع الدول الأطراف في اتفاقيات القانون الدولي الإنساني، التحقق عند دراسة أو تطوير أو اقتناء أي سلاح جديد، أو أداة للحرب، ما إذا كان ذلك السلاح محظورا بموجب هذا البروتوكول، أو أية قاعدة أخرى من قواعد القانون الدولي[16].

فالحظر الذي نصت عليه الفقرة الأولى من هذه المادة (36)، ينصرف إلى جميع الأسلحة التي لها تأثير مباشر على صحة وحياة الأشخاص المحميين بموجب القانون الدولي الإنساني، كالأسلحة الكيميائية، والبيولوجية، والنووية، وحتى الأسلحة الالكترونية، لما قد تسببه من قتل للمدنيين، وإصابات وأضرار عارضة في صفوف الأعيان والممتلكات[17]، هذا وقد طالبت الدول الأطراف في اتفاقيات جنيف الأربع لعام 1949 ، أثناء المؤتمر الدولي الثامن والعشرين 28 للصليب والهلال الأحمر، المنعقد في جنيف بسويسرا سنة 2003 ، بأن تخضع جميع الأسلحة الجديدة، لاستعراض دقيق ومتعدد التخصصات، وذلك لضمان بأن لا يتخطى تطور التكنولوجيا الحماية القانونية المكفولة بموجب قواعد واتفاقيات القانون الدولي الإنساني[18].

فالأسلحة الالكترونية اليوم، يمكن اعتبارها كأسلحة قتال جديدة إلى جانب الأسلحة التقليدية، الأمر الذي يستدعي ايلاء كامل الاعتبار لها في إطار استراتيجيات ومفاهيم الأمن الخاصة بالدول والمنظمات الدولية، على غرار ما هو عليه الحال مع منظمة حلف شمال الأطلسي، التي ارتأينا بأن تكون كنموذج لهذا الموضوع الهام والشائك.

المبحث الثاني: منظمة حلف شمال الأطلسي وجهود مجابهة الحروب الالكترونية

إن إضافة الفضاء الالكتروني كساحة قتال جديد إلى جانب ساحات القتال الأخرى في البر والبحر والجو، استوجب معه الأمر دمج الحروب القائمة فيه، في استراتيجيات ومفاهيم الأمن[19]، خاصة في ظل اختلاف البيئة الإستراتيجية في الفضاء الالكتروني عن المفهوم التقليدي لها في نظرية الأمن، القائم على التهديدات التقليدية، حيث يختلف الزمان والمسافة والمساحة في الفضاء الالكتروني عن المفاهيم التقليدية، إذ انه بإمكان العدو شن هجمات على الخصم بسرعة البرق وإلحاق أضرار جسيمة به مع الصعوبة بمكان تحديد هوية المهاجم، وكمثال على ذلك فقد شهدت الدول الأعضاء في منظمة حلف شمال الأطلسي، هذه الهجمات في العديد من المرات، كانت أكثرها حدة، تلك الهجمات التي استهدفت كل من "استونيا"سنة 2007 ، و"جورجيا" سنة 2008 ، بواسطة فيروس "ستاكنيست"[20]، والتي أجبرت الحلف على وضع شبكة محكمة من القواعد والتدابير لحماية فضاءه الالكتروني، باعتبار أن إعاقة أو اختراق هذا الفضاء، بات يشكل تهديدا صارخا لسلامة و أمن الدول الأعضاء.

المطلب الأول: التدابير القانونية

يعتبر دليل "تالين" للقانون الدولي الإنساني المطبق على الحروب الالكترونية، احد أهم القوانين التي سنها حلف شمال الأطلسي لتنظيم قواعد الاشتباك وحالة الحرب عبر الفضاء الالكتروني، فهو مكون من 95 مادة، تولى إعدادها جملة من الخبراء القانونيين والعسكريين للحلف،

بمدينة "تالين" باستونيا سنة 2008 ، ويقر هذا الدليل، بأن الحروب الالكترونية تشكل في حد ذاتها نزاعات مسلحة تبعا للظروف التي قد تتبعها، لا سيما حجم الآثار المدمرة لتلك العمليات، كما يعطي هذا الدليل، الدول التي تتعرض لهجوم الكتروني، حق شن حرب الكترونية مضادة على الدولة المعتدية، بالإضافة إلى إمكانية استخدام القوة المسلحة للدفاع الشرعي عن النفس تطبيقا لما جاءت به المادة (51) من ميثاق هيئة الأمم المتحدة، إذا ما تسبب هذا الهجوم في قتل أرواح، أو الإضرار بأعيان أو ممتلكات أو تدميرها.

كما يشترط هذا الدليل، بأن لا تكون الإصابات العرضية والأضرار المحتملة في صفوف السكان المدنيين مفرطة، مقارنة بالميزة العسكرية المباشرة والملموسة المتوقعة من الحروب الالكترونية، فإذا لم تستوف هذه الشروط، فلا يمكن بأي حال من الأحوال شن الهجوم عبر الفضاء الالكتروني[21].

ورغم أن هذا الدليل غير ملزم من الناحية العملية، إلا انه ساهم وبشكل كبير في إثراء النقاش حول هذا الموضوع المثير للجدل، خاصة وأن موضوع الحروب الالكترونية، يتفاعل مباشرة مع المواضيع التي ينظمها القانون الدولي الإنساني، فهاته الأخيرة قد تشكل في حد ذاتها نزاعات مسلحة تبعا للآثار المدمرة التي قد تتبعها[22].

المطلب الثاني: التدابير المؤسسية

أولا: إنشاء مركز الامتياز للدفاع ضد الهجمات الالكترونية: (NATO.CCD.COE)

يعتبر مركز الامتياز للدفاع ضد الهجمات الالكترونية، الذي اعتمد سنة 2008 ، من قبل مجلس شمال الأطلسي (N.A.C)، فاعل رئيسي في مجال التعاون بين الدول الأعضاء في الحلف والدول الشريكة للدفاع ضد أية هجمات الكترونية، ويقدم المركز في هذا الشأن، خدمات هامة في

مجال الاستشارة، والتعليم، والتدريب، والبحث في المواضيع ذات الصلة بالفضاء الالكتروني[23].

هذا ويعمل مركز الامتياز للدفاع ضد الهجمات الالكترونية، بالتنسيق مع مراكز ومدارس أخرى تابعة للحلف، تتولى كذلك مهمة الدفاع ضد أية مهاجمة أو اختراق لبرامج وأنظمة المعلومات التابعة للحلف، وكأمثلة عن ذلك نجد: مدرسة أنظمة المعلومات والاتصالات الكائنة ب"لاتينا" بايطاليا، ومدرسة "اوبرمرغو" بألمانيا، وكلية الدفاع التابعة لحلف شمال الأطلسي الكائن مقرها بمدينة روما الايطالية[24].

ثانيا: استحداث لجنة الدفاع ضد الهجمات الالكترونية:

تعتبر لجنة الدفاع ضد الهجمات الالكترونية، أحد أهم اللجان التي أنشأها مجلس شمال الأطلسي (N.A.C)، مؤخرا في شهر افريل سنة 2014 ،لتعوض بذلك اللجنة السياسية للتخطيطات والدفاع ضد الهجمات الالكترونية، وتتولى هذه اللجنة مهام التنظيم والمراقبة وإعداد البرامج المتعلقة بكبح أي هجوم أو اختراق الكتروني لأنظمة وبرامج الحلف[25].

المطلب الثالث: التدابير العملية

الاعتراف بالفضاء الالكتروني كمجال جديد ينبغي الدفاع عنه بشكل خاص إلى جانب المجالات الأخرى (البر، البحر، والجو)، ولذلك تم تفعيل نص المادة الخامسة 05 من معاهدة الحلف، باعتبارها حجر الأساس في مواجهة أي هجوم أو عدوان الكتروني، للتصدي لأية جهات خارجية يثبت ضلوعها في هجمات من هذا النوع ضد الدول الأعضاء في الحلف[26].

بناء نظام دفاعي وديناميي فعال وشامل، مثل إعداد مخطط الدفاع ضد الهجمات الالكترونية، الذي صادق عليه رؤساء الدول الأعضاء في الحلف بالإجماع، خلال قمة حلف شمال الأطلسي الأخيرة المنعقدة "بويلز""بلاد الغال"، بين 03 و05 سبتمبر 2014 ، والقائم على تضامن

الدول الأعضاء لاستثمار الإمكانيات والقدرات لتطوير الدفاع الالكتروني وإدماجه ضمن المخططات المدنية المستعجلة للحلف[27].

ترقية وتوسيع نشاطات التحسيس، والتعليم، والتدريب، وتكثيف المناورات والتمارين التطبيقية، لمواكبة التطورات الجديدة الحاصلة في المجال الالكتروني.

إقامة شبكة واسعة للشراكة والتعاون مع مختلف الدول المنظمات الدولية الأخرى، وكذا القطاع الخاص (l'indestré)، باعتباره فاعل هام في هذا الميدان.

بلورة وتطوير سياسة الردع ضد أي هجوم الكتروني، بما في ذلك إمكانية استخدام القوة العسكرية المسلحة، للرد المباشر على كل هجوم الكتروني يتسبب في إلحاق أضرار بالغة ومباشرة بالأشخاص المدنيين والأعيان المدنية الأخرى[28].

خاتمة:

ختاما لهذه الورقة البحثية، نستخلص بأن الحروب الالكترونية القائمة اليوم، تعتبر أحد أهم افرازت العولمة التقنية والتكنولوجية التي يشهدها العالم في القرن الواحد والعشرين، فالأسلحة الرقمية المستعملة فيها، لا تبعث لا دخان ولا صوت ولكنها تدمر بصمت وتتجسس بخبث، مهددة بذلك الأمن القومي ومراكز القوى والقرار في الدول والمنظمات الدولية التي باتت مجبرة على تحسين وتمتين امن معلوماتها القومي والوطني، سواءا منه العسكري، أو السياسي، أو ألاقتصادي أو الاجتماعي ، وذلك لدرء الانكشاف الأمني الذي قد يجبرها على دفع ضريبة التكنولوجيا، ولا ربما انهيار منظومتها الأمنية ككل في ظل احتدام الحروب الالكترونية عبر الفضاء الرقمي الخالي من منظومة قانونية دولية تدير هذه الحروب وتحدد كيفيات الدفاع والهجوم بين الوحدات الالكترونية المهاجمة سواءا كانت بشرية أو مادية.

وأمام هذا الشلل والفراغ القانوني الدولي الذي يحكم وينظم هاته الحروب، حاول القانون الدولي الإنساني التدخل لتنظيم حالة الحروب الالكترونية أثناء النزاعات المسلحة، غير أن الإشكالات المثيرة للجدل في هذا الشأن تتعلق بكيفيات تطبيق هذا القانون على الدول والأطراف من غير الدول في الفضاء الالكتروني هذا من جهة، ومن جهة أخرى صعوبة تحديد العدو الذي يقوم بالهجوم الالكتروني، لذلك يجب على الدول والمنظمات الدولية التريث قليلا قبل الحزم باستخدام القوة العسكرية المسلحة في حالة تعرضها لهجوم الكتروني يتسبب في قتل أرواح أو الإضرار بأشخاص أو ممتلكات، وما عليها سوى الانحياز لقواعد المسؤولية الدولية في هذا الشأن للمطالبة بجبر الضرر والتعويض.

الهوامش:

(1) للحروب الإلكترونية تسميات عديدة في عالمنا المعاصر منها الحرب المعلوماتية (information warfare) حرب الفضاء الالكتروني (space war) حرب السايبر (cyber war) حر ب الهاكرز(war hackers) الحرب الرقمية (digital war) حرب الانترنت (internet war) وغيرها راجع في ذلك : **جعلود وليد غسان سعيد**، دور الحرب الالكترونية في الصراع العربي الاسرائيلي، اطروحة تخرج لنيل شهادة الماجستير في التخطيط والتنمية السياسية ، جامعة النجاح الوطنية، نابلس، فلسطين، 2013، ص76.

(2) **د/ فردوس أحمد**، الحروب الالكترونية متاح على الموقع الالكتروني: http//www.isecur1ty.org

(3) **د/ علوي مصطفى**، الأمن الإقليمي....بين الأمن الوطني والأمن العالمي، مجلة مفاهيم الأسس العلمية للمعرفة، العدد الرابع، السنة الأولى، المركز الدولي للدراسات المستقبلية والإستراتيجية، مصر، أبريل 2005، ص31.

(4) **د/ بوزنادة معمر**،المنظمات الإقليمية ونظام الأمن الجماعي، بدون طبعة، ديوان المطبوعات الجامعية، بن عكنون، الجزائر،1992، ص92.

(5) **د/ ممدوح منصور** ، سياسيات التحالف الدولي، دراسة في أصول نظرية التحالف الدولي ودور الأحلاف العسكرية في توازن القوى واستقرار الأنساق الدولية، بدون طبعة، مكتبة مدبولي، الإسكندرية، مصر،1997، ص336.

(6) **د/ مساعد كمال**، الحرب الافتراضية وسيناريوهات محاكاة الواقع، مجلة الجيش اللبناني، يوليو، 2006 متاح على الموقع الالكتروني التالي: http//www.lebaramy.gov.lb/article.asp.in = araid=11575.

(7) **جعلود وليد غسان سعيد**، مرجع سابق، ص82.

(8) **ما هي القيود التي يفرضها لقانون الحرب على الهجمات السيبرانية ؟**، على الموقع الالكتروني:- www.icrc./ara/rousourcs/doucuments/faq/130628-cyber-warfare-q-and-a-eng-htm

(9)**د/سلطان محمد سيد**، قضايا قانونية في أمن المعلومات وحماية البيئة الالكترونية، بدون طبعة ، دار ناشري للنشر الالكتروني، جانفي،2012، ص31.

(10)المرجع نفسه، ص 34.

(11) **ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية ؟**، مرجع سابق.

(12) **جعلود وليد غسان سعيد**، مرجع سابق، ص 99-100.

(13) **حرب الفضاء والاقمار الصناعية "صراع استراتيجي جديد"**، متاح على الموقع الالكتروني التالي: http//www.annbaa.org/nbanews/69/022.htm

(14) **كاخيا اسماعيل**، "الحرب اللكترونية"، مجلة الدفاع .....2012/11/20 متاح على الموقع الالكتروني:
http :www.arabdefencejournal.com/article.php !categoryID=9oarticleID=552

(15) **كالسهوفن فريتس و تسغفلد ليزابيث**، ضوابط تحكم خوض الحرب (مدخل للقانون الدولي الإنساني)، ترجمة: **عبد العليم أحمد**، اللجنة الدولية للصليب الأحمر، بدون طبعة ، جنيف، جوان 2004، ص 15.

(16) **د/عتلم شريف ود/عبد الواحد محمد ماهر**، موسوعة اتفاقيات القانون الدولي الإنساني النصوص الرسمية للاتفاقيات والدول المصدقة والموقعة، الطبعة السادسة، القاهرة،2005، ص283.

(17) **د/ سعد الله عمر**، ملخص محاضرات في القانون الدولي الإنساني ألقيت على طلبة الماجستير تخصص القانون الدولي والعلاقات الدولية، كلية الحقوق بن عكنون، الجزائر، 2012/2011، ص20.

(18) **ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية ؟**، مرجع سابق.

(19) **د/ محارب محمود**، إسرائيل والحرب الإلكترونية قراءة في كتاب، حرب في الفضاء الإلكتروني اتجاهات وتأثيرات على إسرائيل، المركز العربي للأبحاث ودراسة السياسيات، الدوحة، قطر، ص08.

(20) **Enrico bendetto cossidente**, legal aspects of cyber and cyber-related issue affecting nato, nato legal gazette issue 35, December, 2014, p11.

(21) الحرب الالكترونية تنسف منطق الحرب التقليدية، متاح على الموقع الالكتروني: http//www.arab.co.uk/p=27010

(22) **Enrico bendetto cossidente**,op.cit,p15.

(23) **Rocisini Marco**, cyber operations and use of force in international law, oxford university press, 2014, p58.

(24) Organisation du traité de l'atlantique nord, guide du sommet du payes del'otan au pays de galles 4/5 septembre 2014 , division diplomatique de l'otan, octobre 2014,p102.

(25) jens stoltenberg, rapport annuel 2014 du secrétaie générale, division diplomatique public de l'otan ; bruxelles, Belgique, 2015, p15.

(26) F.lorentine.j.m.de Boer, Examining the Threshold of "Armed Attack" in light of Collective Self-Defence against Cyber Attacks: NATO's Enhanced Cyber Defense, nato legal gazette, issue 35, December, 2014,p29.

(27) Organisation du traité de l'atlantique nord, guide du sommet du payes de l'otan au pays de galles 4/5 septembre 2014 , op.cit, p102-103.

(28) Ibid.p103.

1- باللغة العربية:.

أولا: الكتب:

1- **د/ ممدوح منصور** ، سياسيات التحالف الدولي، دراسة في أصول نظرية التحالف الدولي ودور الأحلاف العسكرية في توازن القوى واستقرار الأنساق الدولية، بدون طبعة، مكتبة مدبولي، الإسكندرية، مصر،1997.

2- **د/ بوزنادة معمر**،المنظمات الإقليمية ونظام الأمن الجماعي، بدون طبعة، ديوان المطبوعات الجامعية، بن عكنون، الجزائر،1992.

3- **كالسهوفن فريتس و تسغفلد ليزابيث**، ضوابط تحكم خوض الحرب (مدخل للقانون الدولي الإنساني)، ترجمة: **عبد العليم أحمد**، اللجنة الدولية للصليب الأحمر، بدون طبعة ، جنيف، جوان 2004.

4- **د/عتلم شريف ود/عبد الواحد محمد ماهر**، موسوعة اتفاقيات القانون الدولي الإنساني النصوص الرسمية للاتفاقيات والدول المصدقة والموقعة، الطبعة السادسة، القاهرة،2005.

5- **د/سلطان محمد سيد**، قضايا قانونية في أمن المعلومات وحماية البيئة الالكترونية، بدون طبعة ، دار ناشري للنشر الالكتروني، جانفي،2012.

6- **د/ سعد الله عمر**، ملخص محاضرات في القانون الدولي الإنساني ألقيت على طلبة الماجستير تخصص القانون الدولي والعلاقات الدولية، كلية الحقوق بن عكنون، الجزائر، 2012/2011.

7- **د/ محارب محمود،** إسرائيل والحرب الإلكترونية قراءة في كتاب، حرب في الفضاء الإلكتروني اتجاهات وتأثيرات على إسرائيل، المركز العربي للأبحاث ودراسة السياسيات، الدوحة، قطر.بدون سنة نشر.

ثانيا: المقالات العلمية :

1- **د/ علوي مصطفى،** الأمن الإقليمي....بين الأمن الوطني والأمن العالمي، مجلة مفاهيم الأسس العلمية للمعرفة، العدد الرابع، السنة الأولى، المركز الدولي للدراسات المستقبلية الإستراتيجية، مصر، أبريل 2005.

2- **د/ فردوس أحمد،** الحروب الالكترونية متاح على الموقع الالكتروني: http//www.isecur1ty.org

3- **د/ مساعد كمال،** الحرب الافتراضية وسيناريوهات محاكاة الواقع، مجلة الجيش اللبناني، يوليو، 2006 متاح على الموقع الالكتروني التالي: http//www.lebaramy.gov.lb/article.asp.in = araid=11575.

4- **ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية ؟،** على الموقع الالكتروني: www.icrc./ara/rousourcs/doucuments/faq/130628-cyber-warfare-q-and-a-eng-htm

5- **كاخيا إسماعيل، "**الحرب الإلكترونية"، مجلة الدفاع اللبناني2012/11/20 متاح على الموقع الالكتروني: http :www.arabdefencejournal.com/article.php !categoryID=9oarticleID=552

6- **حرب الفضاء والأقمار الصناعية "صراع استراتيجي جديد"،** متاح على الموقع الالكتروني التالي: http//www.annbaa.org/nbanews/69/022.htm

7- **الحرب الالكترونية تنسف منطق الحرب التقليدية،** متاح على الموقع الالكتروني: http//www.arab.co.uk/p=27010

ثالثا: الرسائل والمذكرات الجامعية:

1- **جعلود وليد غسان سعيد**، دور الحرب الالكترونية في الصراع العربي الإسرائيلي، أطروحة تخرج لنيل شهادة الماجستير في التخطيط والتنمية السياسية ، جامعة النجاح الوطنية، نابلس، فلسطين، 2013.

2- باللغة الأجنبية:

1-les livres :

1- **jens stoltenberg**, rapport annuel 2014 du secrétaie générale, division diplomatique public de l'otan ; bruxelles, Belgique, 2015.

2- **Organisation du traité de l'atlantique nord, guide du sommet du payes del'otan au pays de galles** 4/5 septembre 2014 , division diplomatique de l'otan, octobre 2014.

2-les articles :

1- **F.lorentine.j.m.de Boer**, Examining the Threshold of "Armed Attack" in light of Collective Self-Defense against Cyber Attacks: NATO's Enhanced Cyber Defense, nato legal gazette, issue 35, December, 2014.

2- **Enrico bendetto cossidente**, legal aspects of cyber and cyber-related issue affecting nato, nato legal gazette issue 35, December, 2014.

3- **Rocisini Marco**, cyber operations and use of force in international law, oxford university press, 2014.