

الحروب السيبرانية في ظل القانون الدولي الإنساني

Cyber wars under international humanitarian law



دحماني عبد القادر^{*1}

¹ كلية الحقوق / جامعة الجزائر 1 ، (الجزائر)

ab.dahmani@univ-alger.dz

تاريخ الإرسال: 2025/03/11 تاريخ القبول: 2025/05/05 تاريخ النشر: 2025/06/01

ملخص:

أصبح انطباق قواعد القانون الدولي الإنساني على الحروب السيبرانية من أهم القضايا التي تطرح وتشغل بال المنظمات والمهتمين بهذا المجال، بسبب التطور التكنولوجي والتوسع في استعمال الفضاء السيبراني لتنفيذ الكثير من العمليات العدائية قصد السيطرة وتعطيل البنية التحتية للدول أو الجماعات المسلحة المنظمة في سياق نزاع مسلح.

الأمر الذي دفعنا إلى البحث في مجال شرعية استعمال الفضاء السيبراني في النزاع، وتكييف ذلك مع قواعد القانون الدولي الإنساني، وإبراز استراتيجية المجتمع الدولي في التعامل مع هذا النوع من الحروب.

الكلمات المفتاحية: الحرب؛ السيبرانية؛ القانون؛ الدولي؛ الإنساني.

Abstract:

The applicability of the rules of international humanitarian law (IHL) to cyber warfare is one of the most pressing issues that have become a concern for organizations and those interested in this field, due to technological advancements and the increasing use of cyberspace to carry out many hostile operations aimed at controlling or disrupting the infrastructure of states or organized armed groups in the context of armed conflicts.

This has prompted us to examine the legitimacy of this type of warfare, adapt it to the rules of international humanitarian law, and highlight the international community's strategy in dealing with such warfare.

Key words: Warfare; Cyber; Law; International; Humanitarian.

مقدمة:

أدى التطور السريع في تكنولوجيا المعلومات إلى ظهور حروب بنمط جديد، قائمة على المعلوماتية التي قد لا تنظمها صراحة معاهدات القانون الدولي الإنساني، وأن هذه التكنولوجيا، كما هو الحال مع جميع منظومات الأسلحة، يجب أن تكون قابلة للاستخدام وفقا للقانون الدولي الإنساني، ولا سيما قواعده المتعلقة بسير الأعمال العدائية. والأمر متروك في المقام الأول لكل دولة تقوم بتطوير هذه التكنولوجيا الجديدة للحرب لضمان ذلك.

وعملا بالبروتوكول الإضافي الأول، يقع على عاتق كل دولة طرف التزام بتحديد ما إذا كان القانون الدولي يحظر في أي ظرف من الظروف أو جميع الظروف استخدام سلاح أو وسيلة أو أسلوب حرب جديد، تقوم بدراسته أو تطويره أو حيازته أو اعتماده. ويعد النظر في مشروعية الأسلحة الجديدة، بما في ذلك التكنولوجيات الجديدة للحرب، خطوة حاسمة بالنسبة للدول لإنفاذ القانون الدولي الإنساني، وبشكل أكثر تحديدا، فهي وسيلة لضمان قدرة القوات المسلحة لدولة ما على القيام بأعمال عدائية وفقا لالتزاماتها الدولية وعدم استخدام أسلحة جديدة قبل الأوان في ظل ظروف لا تضمن احترام القانون الدولي الإنساني.

لكن على الرغم من هذا الالتزام القانوني والعدد الكبير من الدول التي تطور أو تحوز منظومات أسلحة جديدة كل عام، لم يشر سوى عدد قليل من الدول إلى أن لديها إجراءات قائمة لإجراء استعراض قانوني للأسلحة الجديدة.

وفي حين أنه لا جدال في أن الأسلحة الجديدة يجب أن تكون قابلة للاستخدام وفقا لقواعد القانون الدولي الإنساني التي تحكم سير الأعمال العدائية، فإن تطبيق هذه القواعد وتفسيرها على التكنولوجيات الجديدة للحرب قد يشكلان صعوبات بسبب خصائصها، والظروف المتوخاة والمتوقعة لاستخدامها وعواقبها الإنسانية المتوقعة. وفي نهاية المطاف، قد تثير هذه الصعوبات تساؤلات حول ما إذا كانت القواعد المعمول بها واضحة بما فيه الكفاية، أو ما إذا كان من الضروري توضيح القانون الدولي الإنساني أو وضع قواعد جديدة للتغلب على هذه الصعوبات.

فيصبح من الضروري مناقشة إشكالية أساسية متعلقة بما مدى مشروعية الحروب السيبرانية؟ وهل بإمكان القانون الدولي الإنساني ضبطها؟

وللإجابة على هذه الإشكالية يتطلب منا الأمر التطرق للموضوع وفق مبحثين، الأول يتعلق بالإطار العام للحروب السيبرانية، والذي يتفرع إلى مطلب أول حول ماهية الحروب السيبرانية أما الثاني فنتناول فيه الطبيعة القانونية لهذا النوع من الحروب، ونخصص المبحث الثاني لتكييف الحروب السيبرانية،

الذي يتفرع بدوره إلى مطلبين، الأول يتعلق بمشروعية الهجمات السيبرانية، والثاني نتطرق فيه لاستراتيجية المجتمع الدولي لمواجهة الحروب السيبرانية.

المبحث الأول

الإطار العام للحروب السيبرانية

شكلت ظاهرة الحروب السيبرانية في الفترة المعاصرة تحدياً جديداً لدى المجتمع الدولي بسبب استغلال الفضاء الافتراضي الذي يتجاوز كل الحواجز الجغرافية والسياسية، مما سهل العمل التدميري والتخريبي للبنية التحتية وتعطيل تشغيل الخدمات الأساسية أثناء الأعمال العدائية، فأصبح الوضع يحتاج إلى تبيان لهذا النوع من الحروب ووسائلها المستعملة وطبيعتها، لذلك نتطرق إلى ماهية الحروب السيبرانية في المطلب الأول، وإلى طبيعتها في المطلب الثاني.

المطلب الأول: ماهية الحروب السيبرانية

أضحى الفضاء الإلكتروني في الفترة المعاصرة من الأهمية بمكان لدى المجتمع الدولي وتحول الأمر إلى تسابق لاستغلاله علمياً وتكنولوجياً في المجالات المدنية ليتم بعدها التوجه إلى المجال العسكري، وبذلك سادت ظاهرة الحروب السيبرانية أثناء العمليات العدائية، مما صار يهدد السلم والأمن الدوليين، وعليه يستوجب التطرق إلى مفهوم الحروب السيبرانية، ثم تبيان خصائص هذا النوع من الحروب.

الفرع الأول: مفهوم الحروب السيبرانية

لقد حاول الكثير من الدارسين التطرق إلى مفهوم الهجمات السيبرانية خاصة المهتمون بالقانون الدولي الإنساني لمعرفة أبعاد هذه الظاهرة وانعكاساتها على العلاقات الدولية والمخاطر التي قد تنتجها. حيث تعتبر الهجمات السيبرانية ثورة جديدة في عالم تكنولوجيا المعلومات تستهدف عمل الحواسيب والمعلومات التي بحوزتها، ومختلف البرامج والشبكات المصممة والمستغلة من طرف فئة معينة، وتكون مفصولة عن شبكات الأنترنت العامة.⁽¹⁾

تعتبر الحروب السيبرانية كبديل للحروب التقليدية المادية فهي حرب علمية أساسها الفضاء الإلكتروني وتهدف إلى تدمير البنية المعلوماتية العسكرية والاقتصادية وإضعاف شبكات التواصل باختلاف أنواعها ودرجة أهميتها، وتخريب كل وسائل الإمدادات وبالتالي عرقلة الاستراتيجيات العسكرية.⁽²⁾

¹ - كاخيا إبراهيم، الحرب الإلكترونية، مجلة الدفاع العربية، بيروت، 2010، ص 23.

² - حكيم غريب: تداعيات الحرب الإلكترونية على العلاقات الدولية: دراسة في الهجوم الإلكتروني على إيران، دفا تر السياسة والقانون، المجلد 1، العدد 2، 2020، ص 96.

السيبرانية من المصطلحات الحديثة الاستعمال وإن كان يستعمل مصطلح **Cybernetics** من قبل عالم الرياضيات الأمريكي "نوربرت وينر" **Norbert Wiener** «عام 1948 كإشارة إلى " آليات التنظيم الذاتي " كما استخدم هذا المصطلح السيبرانية في قاموس المورد كدلالة على الضبط، أي ضبط الأشياء عن بعد والتمكن من تسييرها.⁽¹⁾

وأصبحت القواميس المتخصصة في المجالات الأمنية تستعمل مصطلح السيبرانية كدلالة على العمل عبر الفضاء الإلكتروني الذي يسعى إلى السيطرة على المواقع والبنى الإلكترونية للإضرار بها أو تدميرها كلياً.⁽²⁾

أما اصطلاحاً فتم تداول المصطلح من طرف الفقه والمنظمات الدولية بكيفية متقاربة حيث يرى الفقيه فيورتنس **Fuertes** بأنها "هجوم عبر الأنترنت على المواقع الإلكترونية هدفها تعطيل أو إتلاف البيانات أو الاستحواذ عليها"، فيما يعتقد شميت **schmitt** بأنها مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات لدى دولة أخرى للإضرار بها مع العمل على وضع احتياطات والدفاع عن معلومات تلك الدولة المهاجمة.⁽³⁾

ويرى ماركو روسيني بأنها تلك العمليات التي تهدف إلى تطويع الإمكانيات الإلكترونية العسكرية قصد التأثير في مواقع إلكترونية أخرى لتعطيلها أو تدميرها سواء كانت تقدم خدمات مدنية أو عسكرية.⁽⁴⁾

أوهي امتداد للحروب التقليدية والمادية إذ يتألف جندها من المدنيين والعسكريين في آن واحد، كما أنها حرب أدمغة بالدرجة الأولى، كونها تستهدف في المقام الأول تدمير البنية العلمية والمعلوماتية للهدف، وتأخذ أشكالاً عدة، كشكل الاتصالات بين الجيوش وقاداتها، وإضعاف شبكات النقل والإمدادات اللوجستية وضرب المعلومات الاقتصادية، والعبث بالمحتوى التقني والرقمي وغيرها.⁽⁵⁾

¹ - منير البعلبكي : المورد قاموس إنكليزي عربي دار العلم للملايين، بيروت 2004، ص 243.

² - Richard Kissel – Glossary of Information Security Terms, National Institute of Standards and technology, U.S Department of Commerce. 2013, P 31.

³ - أحمد عبيس نعمة: الهجمات السيبرانية، دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط1، منشورات زين الحقوقية، بيروت، لبنان، 2018، ص16.

⁴ - أحمد عبيس نعمة الفتلاوي: الهجمات السيبرانية، مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد4، السنة 8، 2016، ص 616.

⁵ - حكيم غريب: مرجع سابق، ص96.

كما استخدمت اللجنة الدولية للصليب الأحمر مصطلح الحرب السيبرانية⁽¹⁾، في مختلف وثائقها التي تتعلق بطبيعة الحروب الجديدة وخاصة المتعلقة بالفضاء الإلكتروني وما يرتبط به من عمليات، ومما ذكر في الموضوع أنه على مدى السنوات العديدة الماضية، كان الاهتمام بالقضايا القانونية الناتجة عن احتمال سيرا أعمال العدائية في الفضاء السيبراني. ليفتح الفضاء الإلكتروني مجالا جديدا محتملا للقتال الحربي، وهو مسرح حرب من صنع الإنسان، بالإضافة إلى المسارح الطبيعية في الأرض والجو والبحر والفضاء الخارجي وهو مترابط مع كل منها. إنها مساحة افتراضية توفر الترابط في جميع أنحاء العالم بغض النظر عن الحدود. في حين أن هذه الميزات ذات فائدة كبيرة في وقت السلم، فإن الترابط يعني أيضا أن كل ما له واجهة مع الإنترنت يمكن استهدافه من أي مكان في العالم. ويعني الترابط أيضا أن آثار الهجوم قد يكون لها تداعيات على أنظمة أخرى مختلفة بالنظر إلى أن الشبكات العسكرية تعتمد في كثير من الحالات على البنية التحتية التجارية.

وبالرجوع إلى "دليل تالين"⁽²⁾ بشأن القانون الدولي المطبق على الحروب السيبرانية، فإنه أورد تعريفا في القاعدة (30)⁽³⁾ حول الهجمات السيبرانية بمختلف حالاتها التي يراد بها إحداث أضرار بالأشخاص الطبيعيين بمختلف فئاتهم، وكذا الأعيان المدنية المحددة في قواعد القانون الدولي الإنساني. ويعتبر "دليل تالين" من أهم النصوص التي تناولت الحروب السيبرانية حيث تم إعداده من طرف مجموعة من الخبراء الدوليين في المجال، وكان ذلك بدعوة من منظمة حلف شمال الأطلسي (NATO) ويتكون الدليل من 95 قاعدة مستمدة من أحكام القانون الدولي بصفة عامة وقواعد القانون الدولي الإنساني بصفة خاصة، تم اللجوء إلى هذه الطريقة لضبط قواعد متعلقة بالحروب السيبرانية من طرف منظمة حلف شمال الأطلسي بسبب الاختلافات التي ظهرت بعد التوسع في استغلال الفضاء الإلكتروني.

¹ - Document prepared by the International Committee of the Red Cross, 31st INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT Geneva, Switzerland 28 November – 1 December 2011, p 36

² - مجموعة من الخبراء الدوليين: دليل تالين بشأن القانون الدولي المطبق على الحروب السيبرانية، بدعوة من قبل الناتو. 2013

³ - مفاده أن "الهجمات السيبرانية هي عمليات سيبرانية، سواء كانت هجومية أو دفاعية، والتي يهدف من خلالها بصورة معقولة التسبب بالإصابة أو وفاة الأشخاص أو الأضرار أو تدمير الأعيان"

الفرع الثاني: خصائص الحروب السيبرانية

لهذا النوع من الحروب مجموعة من الخصائص تجعلها تختلف عن الحروب التقليدية التي تعتمد على الجيوش والمعدات الحربية المخصصة للدفاع أو الهجوم على الأهداف العسكرية المادية ونذكر منها:

(1)- انخفاض التكلفة: لا تحتاج الحروب السيبرانية إلى المعدات الحربية والجيوش المدربة والمجهزة التي تتطلب الإمكانات المادية من جهة ووقوع الضحايا والخسائر البشرية.

(2)- إخلاء المسؤولية المباشرة: نظرا لطبيعة الهجمات السيبرانية فإنه يصعب تحديد المسؤولية عن الجرائم المرتكبة وإثبات الطرف المتورط في الهجمات بسبب احتمالية استخدام وكلاء لشن الهجوم من مكان آخر لا ينتهي للمجال الجغرافي للدولة مصدر القرار.

لقد قامت إستونيا في 26 أبريل 2007 بنقل نصب تذكاري للجيش الأحمر من وسط مدينة تالين إلى مقبرة خارج المدينة، فوقعت احتجاجات شعبية داخلية، وخارجية من روسيا، ونتيجة لهذا القرار وقع هجوم سيبراني على المواقع الحكومية الإستونية وبعض البنى التحتية فوجه الاتهام حينها إلى روسيا لكن في سبتمبر 2007 اعترفت إستونيا بأنها لا تستطيع أن تجزم بأن موسكو هي المسؤولة فعلا عن الهجمات السيبرانية التي تعرضت لها.

(3)- تغير الأهداف: الأهداف العسكرية التقليدية المتعلقة بالثكنات والآليات الحربية ومختلف الوسائل المستعملة من طرف الجيوش غير تلك الأهداف الجديدة في الحروب السيبرانية التي أضحت تستهدف البنك المتنوع من الأهداف كالبنية التحتية المدنية، وشبكة المعلومات التي تتوفر على كل المعطيات المتعلقة بالحياة والمصالح الحيوية، كالبحوث العلمية وشبكات المياه والكهرباء والمواصلات حيث باتت كل المعاملات الحكومية متصلة بهذه الشبكات.

(4)- حرب هلامية الشكل: متنوعة ومتطورة مرتبطة بالمجالات التقنية الأكثر تطورا، وتأخذ عدة أشكال وتستهدف بنك المعلومات بما يتماشى والحياة المعاصرة للدول، التي أصبحت تعتمد بالدرجة الأولى على الحكومات الإلكترونية التي تستمد استراتيجيتها في التسيير على المعطيات والبرمجيات وفقا للبنك المعلوماتي.

(5)- توسع بنك الأهداف المتاحة أمام الهجمات الإلكترونية، كما وقع في إيران التي أعلنت في نوفمبر 2010 بأن أجهزة الطرد المركزي في البرنامج النووي الإيراني قد أصيب بدودة حاسوبية واتهمت الولايات المتحدة بالوقوف وراء الهجوم، ليكشف بعدها الصحفي الأمريكي "ريتشارد إنجل" بأن دودة الكمبيوتر

Stuxnet تم إنشاؤها من قبل الاستخبارات الأمريكية والإسرائيلية، ولم تؤكد أو تنفي الولايات المتحدة ذلك.⁽¹⁾

المطلب الثاني: طبيعة الحروب السيبرانية

يعتبر الفضاء الإلكتروني الآن ساحة معركة جديدة، كما يقع في المجالات الإقليمية للدول، وقد توصف في كثير من الأحيان الهجمات السيبرانية الحكومية على أنها حرب إلكترونية.² نظرا لارتباط هذه الحرب بأنشطة عسكرية في سياق نزاع مسلح، باستخدام الوسائل والأساليب الرقمية في الفضاء السيبراني. ويشمل كلا من الأنشطة الهجومية والدفاعية للبنى التحتية لتكنولوجيا المعلومات، أما في حالة عدم وجود نزاع مسلح بين دولتين، يعتبر أي هجوم إلكتروني بينهما قد وقع في وقت السلم وبالتالي لا يعد من الأعمال الحربية السيبرانية.

فالهجوم السيبراني يتعلق بأي هجوم إلكتروني من دولة أو برعايتها أو نيابة عنها ويتم إطلاقه ضد وسط تكنولوجيا معلوماتي أو نحو البنية التحتية لدولة أخرى. كما يمكن أن يكون مرتكب هذه الأفعال من وكلاء الدولة بحكم القانون أو بحكم الأمر الواقع.⁽³⁾

حيث نجد مختلف دول العالم حاليا أصبحت مهتمة بتطوير قدراتها في المجال السيبراني، بل وضعت استراتيجيات وخصصت ميزانيات للبحث والتكوين ولم تصبح من الأمور السرية، لكن بالمقابل لم تعلن أية دولة حتى الآن مسؤوليتها علنا عن أي هجوم سيبراني، وعلى مدى العقد الماضي، لوحظ في كثير من الأحيان أن العديد من الهجمات الإلكترونية الحكومية قد نفذت من قبل مجموعات من الأفراد ذوي الدوافع المختلفة الذين يتصرفون بأجر من الدولة أو بمبادرة منهم، دون أن يتم إدانة أفعالهم غير القانونية ضد دولة أخرى من قبل البلد الذي تنطلق منه الهجمات. الأفراد والكيانات المتورطة في الهجمات الإلكترونية ضد الدول الأخرى تعود في كثير من الأحيان لأسباب وطنية في الأساس، يتم تنفيذ الهجمات بهدف الادعاء أو الاحتجاج على القرارات السياسية لدولة أخرى.

ومن أهم النصوص التي يمكن العودة إليها للنظر في طبيعة الحروب السيبرانية ما جاء في قواعد دليل تالين 2013 المتعلق بشأن القانون الدولي المطبق على الحروب السيبرانية، حيث يحتوي هذا الدليل على 95 قاعدة مستمدة من أحكام القانون الدولي العام، وكذا قواعد القانون الدولي الإنساني.

¹ -Richard Engel ; Iran's nuclear negotiator says U.S. involved in cyberattack

Iran's nuclear says U.S. involved in cyberattack

² - Voir Scott J Shackelford et Richard B Andres, « State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem » (2010) 42:1 Geo J Intl L 971 à la p 974

³ - Evelyn AKOTO, Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ? : Première partie, Revue de droit d'Ottawa, Volume 46, n° 1, 2014- 2015.

ويتضح ذلك من خلال التركيز على النزاعات المسلحة الدولية وغير الدولية، وتم العمل على تكييف الهجوم السيبراني لقواعد القانون الدولي الإنساني على أنه عمل إلكتروني هجومي أو دفاعي القصد منه إحداث أضرار بالأشخاص الطبيعية بالقتل والإصابات أو بتدمير الأعيان المدنية، وهذا ما يعتبر في نظر القانون الدولي الإنساني جرائم يتابع ويعاقب عليها كل منتهك لها. كما أكد نفس الدليل في القاعدة 20 منه على تطبيق القانون الدولي الإنساني كلما تمت العمليات السيبرانية في سياق نزاع مسلح، وخضوعها للقيود الجغرافية التي تفرضها قواعد القانون الدولي الإنساني المعنية بالتطبيق في هذا المجال. وبذلك اعتبرت كالحروب التقليدية تخضع لقواعد القانون الدولي الإنساني.

المبحث الثاني

تكييف الحروب السيبرانية

أصبح من الضروري التطرق إلى مآل الحروب السيبرانية التي صارت تستهدف القدرات والبنى التحتية للطرف المعادي أثناء نشوب الأعمال العدائية، وقد تحدث أضرارا مختلفة سواء تعلق الأمر بالأهداف العسكرية أو حتى المدنية المحمية وفقا للقانون الدولي الإنساني، لذا يتطلب الأمر التطرق لتكييف هذه الأعمال والبحث في مشروعيتها، ودور المجتمع الدولي أمام ذلك. وعليه نخصص المطلب الأول لمشروعية الهجمات السيبرانية، والمطلب الثاني حول استراتيجية المجتمع الدولي.

المطلب الأول: مشروعية الهجمات السيبرانية

إن قواعد القانون الدولي الإنساني سواء العرفية منها أو الاتفاقية ظهرت وتطورت نتيجة للظروف غير المستقرة التي عرفت المجتمعات عبر مراحل تاريخية مختلفة والانتهاكات للقيم الإنسانية حيث تنوعت وسائل وأساليب القتال، وفي كل فترة ظهرت القواعد بما يتناسب والتحديات المرحلية التي تضبط وتواجه الجوانب الانتقامية خلال الأعمال العدائية.

لكن تظهر أحيانا تحديات بسبب التقنيات الحربية الجديدة المستعملة وأصبح من الضروري دراسة مدى تلاؤم الهجمات السيبرانية مع قواعد القانون الدولي الإنساني، فبدأ التساؤل عن القواعد الواجبة التطبيق.

إن اعتماد الدول على استخدام الفضاء الإلكتروني والقيام بالهجمات السيبرانية أثناء الأعمال العدائية، جعل مبادئ القانون الدولي الإنساني وقواعده أمام اختبار حقيقي ومعقد حول إمكانية تطبيق قواعده على هذا النوع الجديد من الحروب، ذلك لأن الفترة التي جرى فيها تقنين قواعد قانونية ذات

الصلة بوسائل القتال وأساليبه، لا سيما اتفاقيات لاهاي لعام 1899-1907، واتفاقيات جنيف الأربعة لعام 1949 والبروتوكولان الإضافيان لعام 1977، لم تأخذ بعين الاعتبار الهجمات السيبرانية، لكن هذا لا يعني خلو القانون الدولي الإنساني من القواعد التي تضبط الوسائل الحربية الجديدة مهما كان نوعها. حيث يعتبر شرط مارتينز من الركائز الأساسية للقانون الدولي الإنساني الذي يركز في الحماية على ما استقر عليه العرف ومبادئ الإنسانية، وما يفرضه الضمير العام، وأخذ بنفس المبدأ البروتوكول الأول لاتفاقيات جنيف 1977 في المادة الأولى الفقرة الثانية.

وتم التركيز بصفة أكثر وضوح من خلال المادة 36 من نفس البروتوكول على انطباق قواعد هذه الاتفاقية الدولية على كل سلاح جديد تم تطويره واستعماله في الحرب من طرف سام متعاقد.⁽¹⁾ وفي هذا المجال دعت اللجنة الدولية للصليب الأحمر في كانون الثاني/يناير 2020 خبراء من مختلف أنحاء العالم لتبادل معارفهم بشأن القضايا العملية لتنفيذ القانون الدولي الإنساني في العمليات السيبرانية العسكرية.⁽²⁾ وكان من بين المشاركين خبراء من ذوي الخبرة في تطوير واستخدام العمليات السيبرانية العسكرية، وخبرة في العمل مع شركات تكنولوجيا المعلومات العالمية وشركات استخبارات التهديدات السيبرانية، فضلا عن المحامين والأكاديميين. وحلل الخبراء سير العمليات السيبرانية العسكرية، مع التركيز على كيفية فهم القوات المسلحة وتقييم مخاطر الأضرار المدنية وما هي التدابير التي قد تكون فعالة ومناسبة لتجنب هذه المخاطر أو التخفيف من حدتها.

وقدمت المناقشات الثرية صورة ثاقبة للطرق التي تنظر بها القوات المسلحة في تطبيق القانون الدولي الإنساني عند إجراء العمليات السيبرانية والمخاطر التي يمكن أن تنطوي عليها هذه العمليات على السكان المدنيين، وما تمخضت عنه المناقشات هو أن الدول بحاجة إلى استثمار الوقت والموارد لتطوير أدوات وعمليات لتقييم مخاطر الأضرار العرضية للمدنيين وتدابير للحد من هذه المخاطر.

تستخدم اليوم في النزاعات المسلحة العمليات السيبرانية بشكل متزايد لدعم العمليات الحربية. وقد اعترفت عدة دول علنا اهتمامها بتطوير إمكاناتها في هذا المجال، ويقوم كثيرون آخرون بتطوير القدرات السيبرانية العسكرية وكذلك المذاهب والسياسات التي تهدف إلى وضع مناهج ومبادئ وطنية للاستخدامات العسكرية للفضاء السيبراني. وبالتوازي مع ذلك، أدت الحوادث السيبرانية التي لا توجد بها صلات بالنزاعات المسلحة أو التي لها صلات غير واضحة بالنزاعات المسلحة إلى إلحاق أضرار بالخدمات المدنية وتعطيلها. وشملت هذه الحوادث عمليات سيبرانية ضد المستشفيات والبنية التحتية للمياه

¹ - المادة 36 من البروتوكول الإضافي الأول لاتفاقيات جنيف 1977.

² - Ewan Lawson, military adviser on cyber, and Kubo Macák, legal adviser, ICRC. The full report is "Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts: ICRC Expert Meeting 21–22 January 2020 – Geneva

والكهرباء والمنشآت النووية والبتروكيماوية. وهي تقدم تحذيرا مخيفا بشأن الأثر الإنساني المحتمل للعمليات السيبرانية العسكرية في النزاعات المسلحة المعاصرة والمستقبلية.

فالقانون الدولي الإنساني يتضمن القواعد المتعلقة بتسيير الأعمال العدائية وكذا القواعد التي تحمي الأشخاص الخاضعين لسلطة الطرف الخصم، فالقانون المتعلق بتسيير العمليات العدائية جاء مع اتفاقيات لاهاي بينما القانون الذي يعمل على حماية الضحايا فيسمى بقانون جنيف، وتطور بصورة منفصلة في اتفاقيات جنيف ثم وقع ترابط بينهما في البروتوكولين الإضافيين 1977 في مجموعة قانونية واحدة، حيث تم العمل على إزالة التمييز وجعل القانون الدولي الإنساني واحدا سواء انبثق عن اتفاقيات لاهاي أو جنيف.

فالقانون الدولي الإنساني يرتبط بمجموعة من المبادئ الأساسية التي هي عبارة تطور وتسلسل بداية من القواعد العرفية إلى غاية ظهور مختلف الاتفاقيات المطورة لقواعد القانون الدولي الإنساني، وما لا شك فيه فإن النزاعات الحربية التي تستعمل الهجومات البيولوجية أو الكيميائية تخضع للقانون الدولي الإنساني، على الرغم من أنها أسلحة غير تقليدية، فالعبرة بالأثر الذي تحدثه الوسائل الحربية من دمار وانتهاك للحدود التي ضببتها قواعد الحماية وخاصة ما تعلق بالمبادئ الأساسية.

هذه المبادئ تبين بأن الحماية المتعلقة بالأفراد غير المشتركين في الأعمال العدائية كمبدأ التمييز الذي يهدف إلى حماية السكان المدنيين والأعيان المدنية ويميز بين المقاتلين وغير المقاتلين.⁽¹⁾

تعتمد الهجمات السيبرانية على فضاء واحد تشترك فيه القوات المسلحة وكل ما هو معتبر من الأهداف العسكرية مع المدنيين والأعيان المدنية، ومن الصعب التقيد باستهداف ما هو عسكري بعيدا عن كل ما هو مدني، ويجب أن تؤخذ بعين الاعتبار حماية كل هدف غير عسكري، حتى لا تحدث التجاوزات وبالتالي الجرائم التي يحضرها ويعاقب عليها القانون الدولي الإنساني، وبذلك فإن مبدأ التمييز في الهجمات السيبرانية ينطبق كما هو الحال في النزاعات المسلحة العسكرية المنصوص عليها في قواعد القانون الدولي الإنساني.

كما أن قواعد القانون الدولي الإنساني تحضر الهجمات العشوائية التي توجه ضد أهداف عسكرية دون الأخذ بعين الاعتبار المدنيين والأعيان المدنية، مهما كانت وسيلة الاعتداء التي لا يمكن التحكم في آثارها من أضرار للمدنيين والأعيان المدنية وفقا لما جاء في قواعد الحماية الإنسانية.⁽²⁾

¹ - المادة 48 من البروتوكول الإضافي الأول 1977.

² - المادة 51 الفقرة 4/ج من البروتوكول الإضافي الأول 1977.

ولعل من أهم التحديات التي قد تواجه الحرب السيبرانية هو أنها تعتمد بالأساس على فضاء إلكتروني مشترك يستخدم من العسكريين والمدنيين، فهذا الترابط يشكل تحديات رئيسية من أجل النجاح في توجيه الهجمات ضد الأهداف العسكرية فقط، دون إحداث أضرار بالمدنيين والأعيان المدنية. وفي نفس الوقت يقع على عاتق الدول الالتزام بتجنب وقوع إصابات عرضية على المدنيين، ويؤخذ بعين الاعتبار ذلك أثناء التخطيط للهجوم قبل تنفيذه، وهذا ما يفرض على الأطراف أثناء الهجوم أو الدفاع ضوابطاً جد دقيقة ومهمة، تفادياً للوقوع في الانتهاكات المخلة بالالتزامات الدولية والمجربة في الاتفاقيات والأعراف الدولية.

أما في حالة مشاركة المدنيين في العمليات السيبرانية العدائية فإنهم يفقدون الحماية من الهجمات خلال فترة مشاركتهم هذه، وعليه فإن العمليات السيبرانية أثناء النزاع المسلح تخضع لقواعد القانون الدولي الإنساني.

المطلب الثاني: استراتيجية المجتمع الدولي لمواجهة الحروب السيبرانية

تعتبر الهجمات السيبرانية من المخاطر الخارجية على الدول من منظور عسكري واستخباراتي، ونتيجة لتطور قدرات بعض الدول في هذا المجال يصبح من الضروري وضع استراتيجية دولية مبنية على التعاون وتبادل الخبرات لتطوير القدرات اللازمة للدول تفادياً وتجنباً للتهديدات المختلفة التي تشكل خطراً على السلم والأمن الدوليين، نتيجة لامتلاك بعض الدول التقنية السيبرانية المؤهلة للقيام بالهجوم.

فيصبح من الصواب اتخاذ التدابير المناسبة لحث الدول على وقف التصرفات غير المشروعة بموجب أحكام القانون الدولي، خاصة عندما يتحول الأمر إلى انتهاكات صارخة لقواعد القانون الدولي الإنساني. وعليه نتطرق لجهود الأمم المتحدة لمواجهة الهجمات السيبرانية، والتعاون الدولي للتصدي لها.

الفرع الأول: جهود الأمم المتحدة لمواجهة الهجمات السيبرانية

يشكل ميثاق الأمم المتحدة النظام الأساسي للعلاقات الدولية ويعتمد على مبادئ أساسية ومنها عدم استعمال القوة في العلاقات الدولية وبالتالي فإن الهجمات السيبرانية يدخل ضمن العدوان الذي قد يوجه ضد الدول قصد الإضرار ببنيتها التحتية وأجهزتها الاستراتيجية ويكون ذلك من الأسباب الرئيسية لزرع البلبلة وعدم الاستقرار وتهديد السلم والأمن الدوليين.¹ وعلى نفس المنوال ذهب

¹ - المادة 2 الفقرة 3 من ميثاق الأمم المتحدة.

مجموعة الخبراء الدوليين من خلال "دليل تالين" على أن الهجمات السيبرانية التي تعتمد على التهديد أو اعتماد القوة ضد الاستقلال السياسي للدول يعتبر عمل غير شرعي.⁽¹⁾

وجاء في قرار الأمم المتحدة أنه من مصلحة الدول الاتجاه نحو استخدام تكنولوجيا المعلومات والاتصالات في الأغراض السلمية ومنع نشوب النزاعات انطلاقاً من هذا الاستخدام، وفي نفس الوقت تعرب عن قلقها من استخدام هذه التكنولوجيا بما يضر بأمن الدول في الجوانب المدنية والعسكرية، وبالتالي يصبح ذلك مما يعمل على عدم صون الاستقرار والأمن الدوليين.⁽²⁾

وانطلاقاً من الاستنتاجات التي توصل إليها فريق الخبراء الحكوميين في التقريرين لعام 2013 و2015 بأن القانون الدولي وميثاق الأمم المتحدة تنطبق أحكامهما على النزاع السيبراني وهي أساسية لضمان صون السلام والأمن في المجتمع الدولي.

فصدر عن الجمعية العامة للأمم المتحدة عدة قرارات ومنها القرار رقم (95 / 45) بتاريخ 14 / 12 / 1990 حول المعطيات الحساسة المتعلقة بكل المعلومات التي تؤدي إلى العنصرية والتمييز بشكل عام بين البشر كتلك المعلومات المرتبط بالعرق والمعتقد واللون والآراء السياسية.⁽³⁾

ومن الخطوات الهامة تلك التوصيات التي قدمها خبراء الأمن السيبراني من خمس عشرة دولة إلى مجلس الأمن الدولي، وهي خطوة لبناء قواعد دولية قد تساهم في الأمن والاستقرار ومن هذه التوصيات⁽⁴⁾:

(1)- تبادل المعلومات بشأن التشريعات الوطنية وتكنولوجيا المعلومات والاتصالات الأمنية.

(2)- بناء الثقة والاستقرار واخذ تدابير للحد من المخاطر وتبادل وجهات النظر باستخدام تكنولوجيا المعلومات والاتصالات أثناء النزاع المسلح.

(3)- تكتيف الحوار بين الدول.

(4)- وضع تدابير مناسبة لدعم القدرات في البلدان النامية.

وأثناء المناقشة رفيعة المستوى التي عقدها مجلس الأمن الدولي حول: "صون السلام والأمن الدوليين: التصدي للتهديدات المتطورة في الفضاء السيبراني" بتاريخ 20 جوان 2024 أكد فيها الأمين

¹ - القاعدة 10 القسم الأول، من الفصل الثاني، دليل تالين، مرجع سابق.

² - قرار الجمعية العامة للأمم المتحدة حول الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي A/RES/ 73/266

³ - محروس نصار غايب، الجريمة المعلوماتية، مجلة التقني، مج 24، الإصدار 9، العراق، 2011، ص 118.

⁴ - UN. Secretary General, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security, 4, U.N.Doc .A/65/20(July. 30,2010).

العام للأمم المتحدة "أنطونيو غوتيريش" على أهمية التعاون الدولي من أجل التصدي للتهديدات في الفضاء السيبراني والجرائم السيبرانية، وتسليح الأدوات الرقمية، وهذا بناء على التطورات السريعة في التكنولوجيا الرقمية وأثارها الاقتصادية والاجتماعية على المجتمعات في جميع أنحاء العالم.⁽¹⁾

وأكدت "نينا إيفياني- أجوفو" نائبة رئيس فريق خبراء الأمن السيبراني التابع للاتحاد الإفريقي في نفس الجلسة على أهمية تعزيز الأمن السيبراني للحفاظ على السلام والأمن الدوليين.

وهو التقرير نفسه الذي نشره المعهد الملكي للشؤون الدولية البريطاني "تشاتام هاوس" أن أفريقيا شهدت موجة من الهجمات السيبرانية عام 2023 ضد أنظمة مفوضية الاتحاد الإفريقي وأنظمة بيانات الحكومة الكينية والبنية التحتية للانتخابات النيجيرية وغيرها.

كما طالبت أغلبية الوفود المشاركة من مجلس الأمن أن يضع معايير وأطر دولية لتحديد مسؤولية الدول لنشاطها في الفضاء السيبراني، ووضع نظم للجزاء الدولي، ونفس الاتجاه عبرت عنه كوريا وسلفوانيا وسويسرا، ودعت دول أخرى كالجزائر وموزامبيق وسيراليون إلى بناء القدرات ونقل التكنولوجيا في البلدان النامية لتطوير التعاون الدولي والاستثمار في الأمن الجماعي.

الفرع الثاني: التعاون الدولي في التصدي للهجمات السيبرانية

يعتبر التعاون الدولي في المجال الأمني ضرورة ملحة واستراتيجية لمواجهة التحديات المتعلقة بالهجمات السيبرانية ضد أمن واستقرار الدول، حيث أصبحت أساليب الحرب ووسائلها تعتمد على تكنولوجيا المعلومات وتستخدم في سياق نزاع مسلح، انطلاقاً من الهجمات والعمليات التي ترتكب ضد أو بواسطة شبكات الحواسيب وأنظمة البيانات بين الدول أو الجماعات المسلحة المنظمة في سياق النزاعات أو الأعمال الردعية المتبادلة.

وبذلك فإن الهجمات السيبرانية تعتبر ضمن أبرز المخاطر التي تحيط بالدول نتيجة استهدافها للأنظمة العسكرية والبنية التحتية الحيوية للدول فضلاً عن الشبكات الذكية وشبكات المراقبة وحياسة البيانات التي تسمح لها بالدفاع عن نفسها.

وأكثر الأمور أهمية هو العمل على تكثيف الجهود الدولية للتعاون الأمني خاصة في ظل ضعف بعض أجهزة العدالة الجزائية، فيمكن الاستفادة من الجوانب التقنية والتكنولوجية التي تتمتع بها بعض الدول للتمكن من مواجهة الجرائم بالاستناد على الجوانب التشريعية والفنية.⁽²⁾

¹ -<https://news.un.org/ar/Story/1024/06/1131931>.

² - أحمد سعد محمد الحسيني: الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية ، أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، 2012 ، ص 279.

ففي هذا السياق ينبغي التأكيد على أهمية التعاون بين الدول والمنظمات الدولية والإقليمية بسبب مختلف التهديدات السيبرانية، وعلى الرغم من بعض الاختلافات الواقعة بين السياسات الوطنية والاتفاقيات الدولية حول المبادرات المتعلقة بالأمن السيبراني لكنها متفقة على البعد الدولي للفضاء السيبراني.

الأمر الذي أكدت عليه الجمعية العامة في العديد من قراراتها في هذا المجال على تحسين قدرات الدول على التعاون والعمل الجماعي من أجل تعزيز استخدام تكنولوجيا المعلومات للأغراض السلمية. وتم فتح المجال لمكتب شؤون نزع السلاح بالأمانة العامة للأمم المتحدة من أجل التعاون مع المنظمات

الإقليمية ذات الصلة، كالاتحاد الأوروبي والاتحاد الأفريقي ومنظمة الدول الأمريكية ومنظمة الأمن والتعاون في أوروبا والمنتدى الإقليمي لرابطة أمم جنوب شرق آسيا لعقد مشاورات مع أعضاء فريق الخبراء الحكوميين في مجال التعاون لدراسة التطورات الحاصلة في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي.

ينبغي على الدول ألا تسمح لدولة أخرى أو أية جهة فاعلة باستخدام إقليمها في تكنولوجيا المعلومات والاتصالات للقيام بارتكاب أفعال غير مشروعة وفقا للاتفاقيات والعرف الدوليين، ويكون على الدولة المتضررة إخطار الدولة التي صدر من أراضيها هذا النشاط لتقوم بتوضيح الأمر والتعاون للتدخل وتوقيف هذه الأفعال، ولا يعني ذلك بأن الدولة الثالثة التي استخدم إقليمها مسؤولة عن تلك الأعمال.

ويجب على الدول ألا تستخدم وكلاء عنها للقيام بهجمات سيبرانية وأن تحرص في نفس الوقت على ضمان عدم استخدام إقليمها من قبل جهات أخرى.

ومن المبادرات كذلك نذكر مشروع اتفاقية الاتحاد الأفريقي بشأن إنشاء إطار قانوني للأمن السيبراني في إفريقيا، وتعتبر اتفاقية "مالابو"⁽¹⁾ اتفاقية طموحة لأمن المعلومات على مستوى القارة، وعلى الرغم من أن دول الاتحاد الأفريقي تواجه تحديات كبيرة فيما يتعلق بالأمن السيبراني بسبب الاختلافات الكبيرة في المجالات السياسية والثقافية والاجتماعية، برزت فكرة أهمية التعاون في مجال

¹ - صيغت هذه الاتفاقية في 2011 واعتمدت في عام 2014 وبدأ سريانها في 8 يونيو 2023 ، بعد أن صادقت عليها 15 دولة من أصل 55 دولة في الاتحاد الأفريقي.

الأمن السيبراني من خلال قمة الاتحاد الأفريقي واعتماد موقف موحد وهو العمل على تطبيق القانون الدولي في الفضاء السيبراني، فقاد العملية مجلس السلام والأمن التابع للاتحاد الأفريقي.⁽¹⁾ كما قام الاتحاد الأوروبي بوضع وثيقة سياسية شاملة تعبر عن وجهة نظر جميع الدول الأعضاء من خلال نشر بياننا مشتركا يتعلق بالاستراتيجية المتعلقة بالأمن السيبراني للاتحاد الأوروبي. من خلال إبرام اتفاقية بودابست بشأن الجريمة السيبرانية المحررة في 23 نوفمبر 2001 من أجل تحقيق وحدة بين الأعضاء وتعزيز التعاون بين الأطراف، لاتباع سياسية جنائية مشتركة لحماية المجتمع من الجرائم الحاسوبية، ولحماية المصالح المشروعة في استخدام تكنولوجيا المعلومات، وتوفير الترتيبات اللازمة للتعاون الدولي السريع.⁽²⁾

إن المعاهدات المتعددة الأطراف أكثر الوسائل العملية لموائمة النظم القانونية الوطنية بما يصبو إليه النظام الدولي ولإمالة الغموض المتعلق بالقانون الدولي في سياق الأمن السيبراني ويعتبر بذلك التعاون الدولي هو حجر الزاوية لمواجهة مخاطر الحروب السيبرانية.

خاتمة:

نتيجة للتطور التكنولوجي السريع الذي عرفه عصرنا، لاسيما جانب الاتصال والمعلومات جعل النزاعات والأعمال العدائية يطفئ عليها استعمال الفضاء السيبراني وما يصحبه من تطور تقني للقيام بهجمات سيبرانية هدفها التعطيل والتخريب أو التدمير، أو التحكم بشكل ضار في البنية التحتية لتكنولوجيا المعلومات الخاصة بالهدف، مما فرض على المنظمات الدولية وكل المهتمين بهذا المجال التفكير حول مدى انطباق القانون الدولي الإنساني والمخاطر التي قد يشكلها على السلم والأمن الدوليين. فمن خلا هذه الدراسة تبين ما يلي:

- (1)- لا يوجد اتفاق وتقارب حول مفهوم الحروب السيبرانية لعدم جدية الدول الفاعلة المتحكمة والمؤثرة والمستغلة لقدراتها السيبرانية، التي تأمل على بقاء إمكانية السيطرة على هذا الفضاء في نزاعاتها الدولية.
- (2)- أنه لا يوجد فراغ في القانون الدولي الإنساني المنظم للنزاعات المسلحة الدولية وغير الدولية سواء المنبثق من الاتفاقيات الدولية المعنية، أو تلك المتعلقة بالعرف الدولي، لكن هذا لا يعني تجاهل الوسائل الحربية الجديدة فعلى المجتمع الدولي العمل على مراجعة وتحديث بعض القواعد بما يتناسب والوضع.

¹ - نينا إيفياني أجوفو، افريقيا أمام تحدي كسب رهان الأمن السيبراني، صحيفة العرب، على الموقع الإلكتروني التالي:

www.alarab.co.uk

² - CETS 185 - Convention on Cybercrime Budapest, 23.XI.2001.

- (3)- ضرورة وضع معايير وقواعد ومبادئ للسلوك المسؤول من جانب الدول فى استخدام تكنولوجيا المعلومات والاتصالات للحد من المخاطر التى تهدد الاستقرار على الصعيد الدولى.
- (4)- ينبغى الفصل بين الهجمات السيبرانية فى إطار الأعمال العدائية الحربية التى تقوم بها الدول، ويحكمها القانون الدولى الإنسانى، والهجمات السيبرانية الأخرى الإجرامية المحظورة التى تخضع للقانون الجنائى الوطنى.
- (5)- القانون الدولى الإنسانى لا يطبق إلا فى حالة نشوب نزاع مسلح ويعتمد على مبادئ قانونية دولية راسخة كمبدأ الإنسانية والضرورة والتناسب والتمييز، وهو ما يجب احترامه لدى استخدام الدول لتكنولوجيا المعلومات والاتصالات فى النزاعات السيبرانية.
- (6)- لا يمكن توجيه الاتهام إلى أية دولة بمجرد انطلاق الهجوم السيبرانى من إقليمها أو من بنيتها التحتية لتكنولوجيا المعلومات والاتصالات، فهذا لا يكون كافياً فى حد ذاته لينسب الفعل إلى تلك الدولة، بل ينبغى الاعتماد على الأدلة التقنية والقانونية.
- والذى يجب أن تتضمن تلخيصاً لما ورد فى متن البحث، مع التركيز على سرد جملة النتائج المتوصل إليها، وتقديم الاقتراحات والتوصيات المهمة وذات الصلة.

قائمة المصادر والمراجع:

باللغة العربية:

أولاً/ الكتب:

1- أحمد عبيس نعمة: الهجمات السيبرانية، دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط1، منشورات زين الحقوقية، بيروت، لبنان، 2018.

2- منير البعلبكي: المورد قاموس إنكليزي عربي، دار العلم للملايين، بيروت 2004.

ثانياً/ أطروحات الدكتوراه:

- أحمد سعد محمد الحسيني: الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، 2012.

ثالثاً/ البحوث والمقالات العلمية:

(1)- كاخيا إبراهيم، الحرب الإلكترونية، مجلة الدفاع العربية، بيروت، 2010.

(2)- محروس نصار غايب، الجريمة المعلوماتية، مجلة التقني، مج 24، الإصدار 9، العراق، 2011.

(3)- أحمد عبيس نعمة الفتلاوي: الهجمات السيبرانية، مفهومها والمسؤولية الدولية الناشئة عنها فى ضوء التنظيم الدولى المعاصر، مجلة المحقق الحلى للعلوم القانونية والسياسية، العدد4، السنة 8، 2016.

(4)- حكيم غريب : تداعيات الحرب الإلكترونية على العلاقات الدولية: دراسة في الهجوم الإلكتروني على إيران، دفاتر السياسة والقانون، المجلد 1، العدد 2، 2020.

(5)- ميشال شميت ومجموعة من الخبراء: دليل تالين، بشأن القانون المطبق على الحروب السيبرانية، بدعوة من الناتو، 2013.

رابعاً/ النصوص الدولية:

أ/ المواثيق الدولية:

(1)- ميثاق الأمم المتحدة .

(2)- البروتوكول الإضافي الأول 1977 لاتفاقيات جنيف 1949 .

ب/ القرارات الدولية:

- قرار الجمعية العامة للأمم المتحدة حول الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي A/RES/ 73/266

خامساً/ المواقع الإلكترونية:

نينا إيفياني أجوفو ، افريقيا أمام تحدي كسب رهان الأمن السيبراني، صحيفة العرب، على الموقع الإلكتروني التالي:
www.alarab.co.uk

باللغة الأجنبية:

- 1)- Secretary General, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security, 4, U.N.Doc .A/65/20(July. 30,2010.
- 2)- Scott J Shackelford et Richard B Andres, « State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem » (2010).
- 3)- Evelyne AKOTO, Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ? : Première partie, Revue de droit d'Ottawa, Volume 46, n° 1, 2014- 2015.
- 4)- Ewan Lawson, military adviser on cyber, and Kubo Macák, legal adviser, ICRC. The full report is "Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts: ICRC Expert Meeting 21–22 January 2020 – Geneva
- 5)- Richard Kissel – Glossary of Information Security Terms, National Institute of Standards and technology, U.S Department of Commerce. 2013,
- 6)- Document prepared by the International Committee of the Red Cross, 31st INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT Geneva, Switzerland 28 November – 1 December 2011.
- 7)- <https://news.un.org/ar/Story/1024/06/1131931>.
- 8)- Iran's nuclear says U.S. involved in cyberattack
- 9)- CETS 185 - Convention on Cybercrime Budapest, 23.XI.2001.