المسؤولية الدولية المترتبة عن الهجوم السيبراني في منظور القانون الدولي

International responsibility for the cyber attack in the perspective of international law

د/ صديقي سامية
جامعة محمد البشير الإبراهيمي برج بوعريريج (الجزائر)
Soumajawad19@gmail.com

تاريخ الاستلام: 2022/07/06 تاريخ القبول للنشر: 2023/01/06

****

ملخص:

رغم التطور الهائل للثورة المعلومات في المجتمع الدولي التي جعلته يواجه مخاطر جديدة، فقد ظهر الهجوم السيبراني التي لا تقتصر آثاره على البيانات في أجهزة الكمبيوتر و أنظمته بل تتجاوز ذلك لتقوم بتأثير بشكل مباشر على العالم الحقيقي كاختراق أنظمة الكمبيوتر للسيطرة على الحركة الجوية،و تعطيل عمل الطاقة النووية و العديد من التأثيرات الكارثية التي يكون المدنيين هم الضحايا الرئيسيين لمثل هذه الهجمات، من هنا ظهرت مسألة المسؤولية الدولية عن الأضرار الجسيمة التي نجمت عن الهجوم السيبراني في العالم الافتراضي التي من خلالها يمكن مواجهة الأخطار و الحفاظ على الأمن السيبراني **الكلمات المفتاحية:** الهجوم السيبراني ، الأمن السيبراني، الفضاء الافتراضي، المسؤولية الدولية، الأمن القومي.

Abstract:

Despite the tremendous development of the information revolution in the international community, which made it face new dangers, the cyber attack appeared that directly affected the real world, such as penetrating computer systems to control air traffic, disrupting the work of nuclear energy, and many catastrophic effects that civilians are the main victims of, from Here the issue of international responsibility for the damage caused by a cyber attack arose through which it is possible to confront the dangers and maintain cyber security.

The problem revolves around the extent of the possibility of international responsibility for the damage caused by the cyber attack.
The issue was addressed in two sections. In the first section, we address the definition of a cyber attack, and its legal adaptation in international

law. As for the second topic, we devoted it to responsibility for cyber attacks on the basis of an illegal act and risk theory.
Key words: cyber attack, cyber security, virtual space, international responsibility, national security.

مقدمة

رغم الإيجابيات المشرقة لعصر تقنية المعلومات في جميع الأصعدة وفي شتى ميادين الحياة المعاصرة، فإن هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل جملة من الانعكاسات السلبية والخطيرة جراء استخدام هذه التقنية، واستغلالها على نحو غير مشروع نتج عنه تهديدا خطيرا للأمن والاستقرار في المجتمع، ومن بينها هجوم الفضاء الإلكتروني غير محدد المجال، وغامض الأهداف باعتباره يتحرك عبر شبكات المعلومات والاتصالات المتعدية للحدود الدولية يرتكب بواسطة أسلحة إلكترونية جديدة تلائم طبيعة السياق التكنولوجي لعصر المعلومات، حيث يتم توجيهه ضد المنشآت الحيوية، أو دسها عن طريق عملاء لأجهزة الاستخبارات، تهدف الدراسة محل البحث إلى تكوين صورة واضحة المعالم حول الهجمات السيبرانية التي تحدث في العالم الافتراضي الذي يعتبر ساحة جديدة للقتال، وبيان إمكانية انطباق قواعد المسؤولية الدولية عن أضرار الهجمات السيبرانية، خصوصا و أن الفضاء السيبراني أصبح مسرحا للهجوم العسكري التي قلبت قواعد القانون الدولي رأسا على عقب.

يكمن الهدف من الموضوع محل الدراسة في تسليط الضوء على إمكانية المسؤولية الدولية عن الأضرار التي يخلفها الهجوم السيبراني في القانون الدولي ومدى انطباق قواعد المسؤولية الدولية التقليدية عليها، في ظل انتشار الهائل لهذه الهجمات في الوقت الراهن نتيجة تزايد ارتباط العالم بالفضاء الإلكتروني، الأمر الذي اتسع معه خطر تعرض البنية التحتية الكونية للمعلومات لهجوم إلكتروني، فضلا عن استخدامه من قبل أطراف فاعلة من غير الدول، خاصة الجماعات الإرهابية لتحقيق أهدافها التي تنال من الأمن القومي للدول، من هذا المنطلق تواجه الدول مخاطر كبيرة نتيجة لما تتعرض له من هجوم يمس سيادة الدولة ويهدد استقرارها ويعرض مصالحها للخطر في شتى المجالات، من هذا المنطلق نطرح الإشكالية الرئيسية التالية

ما مدى إمكانية المسؤولية الدولية عن أضرار التي يخلها الهجوم السيبراني؟.

تستدعي طبيعة موضوع محل الدراسة الاعتماد على المنهج الوصفي في توصيف ظاهرة الهجوم السيبراني من خلال عرض ما تتميز به من خصائص ومحددات، واقترن الوصف بذكر

أسباب ظهور الهجوم السيبراني، كما تم استعمال المنهج التحليلي في تحليل قواعد ومبادئ القانون الدولي في زمن السلم و النزاعات المسلحة من أجل تقييم إمكانية تطبيقها على الهجوم السيبراني، وتحليل أسس المسؤولية الدولية عن الهجوم التقليدي ومدى الاعتماد عليها في تقرير المسؤولية الدولية عن الأضرار الناجمة عن الهجوم السيبراني.

للإجابة على الإشكالية المطروحة تم معالجة موضوع محل الدراسة في مبحثين، حيث نتناول في المبحث الأول الطبيعة القانونية للهجوم السيبراني من خلال تعريفه و التكييف القانوني له في زمن السلم و الحرب، أما في المبحث الثاني تم التطرق إلى أسس المسؤولية الدولية في القانون الدولي ومدى الاستناد إليها لتقرير المسؤولية الدولية عن الهجوم السيبراني.

المبحث الأول: الطبيعة القانونية للهجوم السيبراني

إن سيناريو افتراضي لحرب المستقبل أو ما يعرف الحرب السيبرانية تكون في شكل هجمات دقيقة، ومعقدة للغاية عبر نظم وشبكات الكمبيوتر والأجهزة الذكية،التي تمس الأمن القومي للدولة و تأثر على الأمن و السلم الدولي،حيث تستهدف البنية التحتية المدنية والعسكرية للدول من محطات الطاقة والكهرباء، ونظم الاتصالات والمواصلات والأقمار الصناعية، وخدمات تحديد الموقع الجغرافي والسيارات ذاتية القيادة ،فضلا عن المفاعلات النووية والسدود والخزانات المائية،وعليه نتطرق إلى تعريف الهجوم السيبراني في المطلب الأول، أما المطلب الثاني فقد خصصناه للتكييف القانوني للهجمات السيبرانية.

المطلب الأول:تعريف الهجوم السيبراني

من المعلوم أن الاعتماد على التقنيات الذكية والحديثة وتبني نماذج الحكومات والمدن الذكية، فإنه يصبح أكثر انكشافًا و عرضة للهجمات السيبرانية، ومع تزايد الاعتماد على الإنترنت أثناء جائحة كورونا لتيسير مهام العمل والتعليم عن بعد تزايد معها نشاط القراصنة مستغلين ضعف الثقافة الأمنية بكثير من مستخدمي الإنترنت حول العالم، وهو ما يتسبب في تهديد الأمن القومي وتعريض مصالح الأفراد والدول للخطر.

لا يوجد تعريف متفق للهجمات السيبرانية بين فقهاء القانون الدولي فقد عرفها جانب من الفقه على أنها عملية استغلال متعمد لأنظمة الكوبيوتر و الشبكات المعتمدة على تكنولوجيا من خلال البرمجيات الضارة(Marshall, 2000, p. 03) ،كما عرف البعض الأخر الهجوم الإلكتروني على أنه أي تصرف إلكتروني دفاعيا كان و هجوميا يتوقع منه، و على نحو معقول التسبب بجرح أو قتل شخص أو إلحاق أضرار مادية، أو دمار يهدف المهاجم(N.Schmit, 2013, p. 92) ، أما غالبية

الفقهاء قد الهجمات السيبرانية على أنها تلك الإجراءات التي تتخذها الدولة من أجل الهجوم على النظم المعلوماتية للعدو بهدف التأثير فيها و الدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة(M.N, 1999, p. 07) .

من التعاريف السابقة يمكن القول أن هناك تشابه بين الهجوم السيبراني و الهجوم العادي في أن قائم بكلا الهجومين له دافع للقيام بالهجوم، وضحية قد تكون شخص طبيعي أو معنوي،أما الاختلاف بينهما يظهر في أداة الهجوم ومكان الهجوم، ففي الهجوم السبيراني الأداة تكون ذات تقنية عالية، وأيضا المكان الذي انطلق منه الهجوم لا يتطلب انتقال فاعله انتقال جسمانيا لأنه يتم عن بعد بواسطة خطوط وشبكات الاتصال بين المهاجم ومكان الهجوم.

لا تنفذ هجمات السيبرانية من أشخاص عاديين بل يتم تنفيذها من مجموعة من محترفي اختراق شبكات الحاسب الآلي يشكلون جيشا سيبرانيا عسكريا، يقاتل ضمن صفوف القوات العسكرية المسلحة، ولكنه يتكون من مجموعة من المبرمجين والباحثين الأمنيين ومكتشفي الثغرات ومحللي الشفرات ومطوري البرمجيات، أو كما يطلق عليهم قراصنة المعلومات، يعملون خلف شاشات وأجهزة الكمبيوتر، مسلحين ببرمجيات وفيروسات فتّاكة يمكن أن تحقق ما لم تحققه الدبابات والطائرات على أرض المعركة (خليفة، 2009، صفحة 10)، ومن دوافع ارتكاب الهجوم السيبراني ما يالي:

- انسحاب الدولة من بعض المجالات الحيوية للقطاع الخاص نتيجة تراجع دورها في ظل العولمة التي يشهدها العالم، إلى جانب ذلك تصاعدت أدوار الشركات متعدية الجنسيات العابرة للحدود،خاصة العاملة في مجال التكنولوجيا كفاعل مؤثر في الفضاء الإلكتروني، لاسيما مع امتلاكها قدرات تقنية تفوق الحكومات.

- نشوء نمط جديد من الضرر على خلفية الهجمات الإلكترونية يمكن أن تسببه دولة لأخرى، دون الحاجة للدخول المادي إلى أراضيها، ذلك أن تزايد اعتماد الدول على الأنظمة الإلكترونية في جميع منشآتها الحيوية جعل هذه الأخيرة عرضة للهجوم المزدوج، لما لها من سمات مدنية وعسكرية متداخلة، خاصة أن الثورة التكنولوجية الحديثة تمخضت عنها ثورة أخرى في المجالات العسكرية، وتطور تقنيات الحرب.

باعتبار الهجوم السيبراني نوع من الأفعال الإجرامية المستحدثة حيث أصبحت حقيقة يومية خاصة مع التطور التكنولوجي المتسارع ،والتي تسمح للمخترقين من الاختراق بسهولة سواء من الدول أو من غيرها(bendovschi, 2015, p. 03) ،و تعتبر سهولة إخفاء ومحو الدليل أو

تدميره من بين الصعوبات التي تثار في مرحلة البحث عن الأدلة عند ارتكاب الهجوم السيبراني ،فالجاني يمكنه محو الأدلة التي قد تدنيه أو يدمرها في وقت وجيز وبمجرد كبسة زر،بحيث لا تتمكن سلطات البحث والتحقيق من كشف جرمه وإقامة الدليل ضده، فهو لا يحتاج إلى جهد عضلي بل يعتمد على الذكاء الذهني المحكم، و التفكير العلمي المدروس القائم على معرفة تقنية ممتازة للحاسب الآلي ، و التعامل السليم للشبكة (مراد، 2006، صفحة 47).

لا يعترف الهجوم السيبراني بالحدود بين الدول وهو بذلك شكل جديد من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة، وهذا راجع لقدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم انعكست على طبيعة الأعمال الإجرامية التي يعمد فيها المجرمون إلى استخدام هذه التقنيات في خرقهم للقانون (خالد، 2009، صفحة 89)، وهو ما يعني أن مسرح هجوم السيبراني لم يعد محليا بل أصبح عالميا، إذ لا يتواجد الفاعل على مسرح الجريمة بل يرتكب جريمته عن بعد، ويقع الهجوم السيبراني في بيئة افتراضية تقنية لا تترك أية آثار محسوسة و يتم في الخفاء لأن الجناة يعمدون في كثير من الأحيان إلى إخفاء نشاطهم الإجرامي، كما أنه من السهل عليهم تدمير الأدلة ومحوها مما يعقد أمر كشف الجريمة و إثباتها.

من هذا المنطلق فإن الهجمات السيبرانية ميدانها الفضاء السيبراني وهي غير محدودة المجال وتكون غامضة الأهداف لأنها تتحرك عبر شبكة المعلومات والاتصالات المتعدية للحدود الدولية، فضلا عن اعتمادها على أسلحة الكترونية ذكية ومتطورة تلائم طبيعة السباق الإلكتروني لعصر المعلومات، أو يتم توجيهها ضد المنشآت الحيوية أو دسها عن طريق عملاء لأجهزة الاستخبارات.

المطلب الثاني التكييف القانوني للهجوم السيبراني

تعمل الجيوش السيبرانية في زمن السلم على تقديم الدعم المعلوماتي واللوجستي فيقومون بالتجسس على العدو عبر اختراق شبكاته لكشف أسراره، وسرقة تصميمات الأسلحة المتقدمة التي يمتلكها والخطط الإستراتيجية والاقتصادية في حالة الحرب، ونوع التسليح الذي يمتلكه ومناطق توزيعه وانتشاره،أما في زمن النزاعات المسلحة يقومون بمهمتي الهجوم والدفاع على حد سواء، فضلا عن مهمة تقديم الدعم للوحدات العسكرية المقاتلة في الميادين المختلفة، فيقومون بمهمة الهجوم عن طريق محاولة شن هجمات سيبرانية تستهدف نظم التحكم والسيطرة الخاصة بالعدو عن طريق تعطيل نظم الدفاع الجوي، ومنصات إطلاق الصواريخ،

والسيطرة على الأسلحة ذاتية التشغيل كالربوتات العسكرية، وقطع شبكات الاتصال بين الوحدات العسكرية، فضلا عن القيام بعمليات الخداع والتشويش الرقمي على أجهزة العدو.

نظرا لحساسية استخدام القوة في العلاقات الدولية، وكذلك تعقد الفضاء السيبراني الذي أصبح يشكل قلق كبير للمجتمع الدولي لخطورة الهجمات التي تشن من خلاله ،حيث تعد ظاهرة الهجمات السيبرانية من الأساليب المستحدثة والمتطورة في نفس الوقت والتي لا تزال تثير جدل لعدم وجود موقف موحد تجاهها،حيث ينطبق القانون الدولي على الهجوم السيبراني إذا اعتبر هذا الهجوم قوة وفقا لميثاق الأمم المتحدة،فالقواعد المعاصرة للقانون الدولي تحظر استخدام القوة، باستثناء حق الدول أو جماعات في الدفاع عن نفسها(Lin, 2012, p. 515) ، فقد حضرت الفقرة 04 من المادة 02 من ميثاق الأمم المتحدة لسنة 1945 على الدول اللجوء إلى الحرب، أو التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي، أو الاستقلال السياسي لأي دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة، لكن الميثاق ترك تحديد المعنى الحقيقي لهذه القاعدة القانونية لمجلس الأمن الذي يقررها تبعا للظروف المحيطة بكل حالة على حدة، وهذا واضح من نص المادة 39 من الميثاق الأمم المتحدة التي تمنح مجلس الأمن سلطة تقرير الإجراءات القهرية، وقد ورد هذا النص بصورة غير ملزمة وذلك بسبب تمتع مجلس الأمن بصلاحيات تقرير ما إذا وقع تهديد للأمن والسلم الدوليين، أو إخلال به أو كان وقع عملا من أعمال العدوان،و مصطلح القوة الوارد في الفقرة 04 من المادة 02 من الميثاق الأمم المتحدة جاءت واسعة حيث لا ينحصر فقط بالقوة العسكرية، وإنما يشمل كل أنواع التهديدات بغض النظر عن الوسيلة المستخدمة في التهديد طالما أن هناك النية العدائية، وهذه الفقرة جاءت مرنة بحيث تستوعب الهجوم السيبراني نتيجة الآثار المشابهة بالنسبة للقوة العسكرية التقليدية، لذلك فإن الكود الضار أو الفيروسات لها نفس خصائص السلاح التي يمكن أن تكون أداة للتخريب والتدمير كالسلاح الحركي،وهنا لا يهم الوسيلة المستخدمة في الهجوم سواء التقليدي و السيبراني و إنما مهم هو الأضرار التي تترتب عن الهجوم والتي تشكل خطرا على سيادة الدول و الأمن الدولي(R.Dev, 2015, p. 380) .

أصبحت مسألة أمن الفضاء السيبراني من أولويات الأمن القومي للعديد من الدول التي تعتمد بشكل كبير على التكنولوجيا والاتصالات في إدارة شؤونها الداخلية،كما أن حق الدولة المعتدى عليها في الرد على الهجوم السيبراني يجب أن لا يخرج عن أطار ميثاق الأمم المتحدة والقانون الدولي الإنساني من حيث الضرورة والتناسب، و يجب أن يستوفي رد الفعل في الدفاع

عن النفس ضد الهجمات السيبرانية التي ترتقي إلى مستوى الهجوم المسلح بمتطلبات الضرورة والتناسب الذي أشارت إليه نص المادة 51 من ميثاق الأمم المتحدة لسنة 1945، إذ تشترط هذه الأخيرة على الدول استخدام حقها في الدفاع الشرعي أن تكون قد تعرضت لاعتداء مسلح، كما لا تشير إلى استخدام نوع محدد من الأسلحة في الرد على الهجمات التي تتعرض لها الدول، مما يعني أن نوع السلاح المستخدم في الهجمات ليس له تأثير في نفي استخدام القوة، وأن ما يعتد به هو الآثار المادية لهذا السلاح على أرض الواقع، و بالتالي فإن الهجوم السيبراني هو بمثابة استخدم للقوة تبعا لنتائجه المادية ويشكل تهديدا للأمن والسلم الدوليين، ويعطي الحق للدولة التي تعرضت للهجوم بأن تطلب التعاون من دول أخرى لمواجهة هذا الهجوم.

ما يمكن قوله أن الهجوم الإلكتروني من قبيل أفعال العدوان التي يعاقب عليها القانون الدولي العام بتفعيل دور مجلس الأمن ،الذي يكيف فعل العدوان على أي تصرف غير شرعي يرتكب في حق دولة عضو في هيئة الأمم المتحدة في حال أنه ارتكب من خلال دولة تبنت هذا الهجوم أو جماعة معينة تتبع لدولة.

رغم أن اتفاقيات القانون الدولي الإنساني لم تشر على وجه الخصوص للهجوم السيبراني إلا أن القانون الدولي الإنساني بمبادئه وقواعده ينطبق بصفة عامة على أي نزاع مسلح بما فيها الحروب السيبرانية، فقد أشار شرط مارتينز وهو من المبادئ الراسخة في القانون الدولي الإنساني على أنه عند وجود حالة لا تغطيها اتفاقية دولية يظل المدنيون والمقاتلون تحت حماية وسلطة مبادئ القانون الدولي المستمد من التقاليد الراسخة، ومن مبادئ الإنسانية، وما يمليه الضمير العام (سميث، 2002، صفحة 90)، وبناء على ذلك فإن مبادئ القانون الإنساني تطبق على الهجوم السيبراني الذي يرتكب في النزاعات المسلحة من بين هذه المبادئ مبدأ الضرورة العسكرية الذي يتمحور حول فكرة مفادها أن استعمال أساليب العنف و القوة في الحرب تقف عند قهر العدو،و تحقيق الهدف من الحرب وهو هزيمته وتحقيق النصر (المجذوب و طارق، صفحة 38)،و يمنع على الطرف الفائز التمادي في الأعمال العدائية ضد الطرف الأخر في استعمال أساليب عنف ضده، ولكي يتمكن القائد العسكري أو الدولة في حد ذاتها من إثارة الضرورة العسكرية بقصد تبرير الأفعال أو الانتهاكات التي ترتكب أثناء النزعات المسلحة لابد أن تكون تصرفات طرف المحتج بالضرورة وموافقة لما هو منصوص عليه في اتفاقيات القانون الدولي الإنساني خصوصا المنظمة لسير العمليات القتالية، وعليه الضرورة الحربية هي حالة التي تكون ملحة لدرجة أنها لا تترك وقتا كافيا للأطراف المتحاربة لإختيار الوسائل المستخدمة في

أعمالها، أو هي الأحوال التي تظهر أثناء الحرب وتفرض حال قيامها ارتكاب أفعال معينة على وجه السرعة بسبب موقف أو ظروف استثنائية في ذات اللحظة.

إن اتفاقيات جنيف قد سلمت بوجود مثل هذه الضرورات الحربية التي قد تمليها ظروف القتال وجعلت منها مبررا لبعض الانتهاكات الجسيمة لأحكامها فقد نصت المادة 50 من اتفاقية جنيف الأولى المتعلقة بتحسين حال الجرحى و المرضى بالقوات المسلحة في الميدان على أن تدمير الممتلكات و الإستلاء عليها في نطاق واسع يعد انتهاكا جسيما للقانون الدولي الإنساني ما لم تبرره الضرورات الحربية (علتم، 2005، صفحة 113)،أما المادة 53 من اتفاقية جنيف الرابعة بشأن حماية الأشخاص المدنيين في وقت الحرب فقد جاءت واضحة أكثر حين بينت مشتملات الممتلكات حيث أكدت على أنه يحظر على دولة الاحتلال أن تدمر أي ممتلكات خاصة ثابتة أو منقولة تتعلق بالأفراد أو الجماعات أو بالدولة السلطات العامة أو المنظمات الاجتماعية أو التعاونية إلا إذا كانت الضرورات الحربية تقتضي حتما هذا التدمير.

من هنا فإن اللجوء إلى الهجمات السيبرانية يجب أن يكون ضروريا لتحقيق الهدف العسكري المشروع، غير أن مسالة تحديد الأهداف العسكرية في الفضاء السيبراني تثير تحديا واسعا في المجتمع الدولي باعتبار أن المنشآت المخصصة للعمل العسكري هي في نفس الوقت تخدم الهدف المدني(Michael, 2012, p. 33) ، و بالتالي يقع على عاتق المقاتل السيبراني أن يقرر بشكل قاطع أن الهجوم السيبراني يوفر ميزة عسكرية لتحقيق هدف عسكري.

يقضي مبدأ التمييز بين الأهداف المدنية و الأهداف العسكرية التمييز بين المدنيين و مقاتلين و الأهداف العسكرية و الأهداف المدنية، وأن لا تستهدف العمليات الحربية المدنيين و أولئك الأشخاص الذين أصبحوا غير قادرين على القتال، وكذا الأعيان المدنية التي بحيث يستوجب على المتحاربين الامتناع عن استهداف كل مبنى لا يشكل هدفا عسكريا كأماكن العبادة و المستشفيات و محطات لتوليد الطاقة الكهربائية و الممتلكات التي لا غنى عنها لبقاء السكان المدنيين على قيد الحياة (الزملي، 1997، صفحة 81)،وقد تم الإشارة إلى مبدأ التمييز في نص المادة 48 من برتوكول الإضافي الأول لاتفاقيات جنيف 1977 التي أكدت على ضرورة قيام أطراف النزاع بالتمييز بين السكان المدنيين و المقاتلين و بين الأعيان المدنية، و الأهداف العسكرية دون غيرها، وذلك من أجل تأمين احترام وحماية السكان المدنيين و الأعيان المدنية و تدعم هذا المبدأ بالمادة 52 من البروتوكول الإضافي الأول التي توضح بأنه لا يجوز أن تشكل الأعيان المدنية هدفا لأي هجمات أو أعمال انتقامية.

ففي إطار تطبيق مبدأ التميز على الهجمات السيبرانية أشار دليل تالين، بالرغم من عدم الزامية قواعده، بأنه لا يجوز أن تكون الأعيان المدنية هدفا للهجمات السيبرانية، فلا يجوز على سبيل المثال توجيه الهجمات السيبرانية التي من شأنها تدمير الأنظمة المدنية والبنية التحتية، ما لم تعتبر هذه الأنظمة من قبيل الأهداف العسكرية التي يجوز استهدافها وفقا للظروف السائدة.

يعد تطبيق مبدأ وجوب التمييز بين المقاتلين والمدنيين على الهجمات السيبرانية مسألة في غاية التعقيد على عكس الهجمات التقليدية إذ سيكون المهاجم في الأغلب بعيدا عن المكان المستهدف من الهجوم ولمسافة قد تتجاوز المئات من الكيلومترات، ما يعني أن التمييز بين المقاتلين والمدنيين هو أمر صعب إذا لم يكن مستحيلا، كما أن مسألة التمييز بين الأهداف المدنية والعسكرية في الهجمات السيبرانية صعبة، خاصة أن نظم الحواسيب العسكرية غالب ما تتصل بالنظم التجارية والمدنية وتعتمد عليها كليا أو جزئيا، بل وقد يكون هناك تداخل بين الاستخدامات المدنية والعسكرية بارتباطهما بشبكة واحدة ووسيط واحد هو الفضاء السيبراني ،ومن ثم يكون من المستحيل شن هجوم سيبراني على بنى تحتية عسكرية وجعل آثارها تقتصر على هدف عسكري فقط دون الإضرار بالمدنيين والمنشآت المدنية (الصادق، 2016، صفحة 96).

المبحث الثاني: أساس المسؤولية الدولية عن الأضرار التي يسببها الهجوم السيبراني

إن المسؤولية الدولية للهجوم السيبراني بالمعنى الدقيق تنبعث من القانون الدولي العرفي،و المواثيق الدولية باعتبارها تمس القيم الأساسية للمجتمع الدولي، حيث أصبحت شبكة الإنترنت تشكل قوة اجتماعية واقتصادية وسياسية مؤثرة في العالم، و يمكن أن تستخدم لزيادة حدة سباق التسلح، وقمع حركات التحرر الوطني، وحرمان الأفراد والشعوب من حقوقهم الإنسانية وحرياتهم الأساسية، كما أن المنجزات العلمية والتكنولوجية يمكن أن تعرض للأخطار الحقوق المدنية السياسية للفرد أو للجماعة، والكرامة البشرية، وتمس بكيان الدولة و استقلالها، من هذا المنطلق نتناول في المطلب الأول المسؤولية عن الهجمات السيبرانية على أساس عمل غير مشروع، أما المسؤولية عن الهجمات السيبرانية استنادا إلى نظرية المخاطر نتطرق إليها في المطلب الثاني.

المطلب الأول: المسؤولية عن الهجمات السيبرانية على أساس عمل غير مشروع

مما لا شك فيه أن المسؤولية الدولية من المواضيع المتشعبة و المهمة وهي أهم ضمانة لكفالة تطبيق القانون الدولي بسبب غياب سلطة عليا مستقلة عن الدول تمتلك السلطة الشرعية لتحديد نظام المسؤولية، و فرض احترامه كما هو الحال في القانون الوطني.

تنطوي نظرية الفعل غير مشروع على أن كل إخلال بالتزام دولي من قبل دولة ما يستوجب مسؤولية هذه الدولة سواء كان هذا الإخلال صادر من سلطتها التشريعية أو التنفيذية أو القضائية و ألحق ضررا بأحد الأجانب في شخصه أو أمواله وكان متواجدا بأراضيها، ويعتبر الفقيه أنزيلوتي أول من تبنى نظرية الفعل غير المشروع (العيشاوي ع.، 2007، صفحة 18)، و يرى أنه من حق الدولة المضرورة المطالبة بإصلاح الضرر وتقديم ضمانات للمستقبل، وأن العلاقة القانونية التي تنشأ بها الروابط بين الدولة نتيجة الإخلال بالحقوق نفس الملامح الرئيسية التي تتسم بها الروابط في قانون الإلتزمات وتظهر في أعقاب تصرف غير مشروع هو بصورة عامة انتهاك لالتزام دولي ينشأ علاقة قانونية جديدة بين الدولة صاحبة التصرف، و الدولة التي وقع الإخلال في مواجهتها فتلتزم بالتعويض و يحق للثانية أن تقتضي هذا التعويض تلك هي النتيجة الوحيدة التي يمكن أن تلصقها القواعد الدولية المعبرة عن الالتزامات المتبادلة بين الدول بالعمل المخالف للقانون، كما نجد الفقيه بول روتر يعتبر أيضا العمل غير مشروع أساس للمسؤولية الدولية بل الشرط الأهم لقيامها.

تعتبر الهجمات الدولية عمل غير مشروع وتخضع للمسؤولية الدولية على هذا الأساس إذا توفر معيار الصفة الدولية ومتمثل في صدور هذه الهجمات من قبل الدولة تخضع هذه حتى يتم إلحاقها بالمسؤولية الدولية، أما المعيار الثاني أن تكون هذه الهجمات الإلكترونية الدولية خارقة لمعاهدة أو عرف أو ميثاق دولي وبتوضيح أكثر لهذا العنصر يجب أن يترتب على هذه الهجمات الإضرار بمصالح الدولة المعتدى عليها الاقتصادية والسياسية والإستراتيجية، أو تمس بأحد المبادئ التي كرستها الأمم المتحدة من أجل حفظ السلم والأمن الدوليين والمحافظة عليهما من أي اختراق أو تدخل يضر بمصالح الدول الأساسية التي لا يجوز انتهاكها، هنا يمكن إسناد مسؤولية الدولة عن هجمات السيبرانية التي تعتبر أعمال غير مشروعة إلى نص المادة 19 من مشروع تقنين مسؤولية الدولة التي أكدت على أن عمل الدولة الذي يشكل مخالفة للالتزام الدولي يعد عملا جائرا دوليا بغض النظر عن موضوع الالتزام الذي تمت مخالفته، كانتهاك جسيم للالتزام الدولي ذي أهمية أساسية في الحفاظ على السلم والأمن الدوليين منح ذلك تلك التي تحضر العدوان.

إن إسناد المسؤولية للدولة عن الأضرار الناتجة عن الهجمات السيبرانية يمكن أن تثير مشكلة تتمثل في صعوبة تحديد ما إذا كان هذا العمل منسوبا للدولة فعلا، وهذا مرتبط بالقدرة التكنولوجية المتنامية، والتي يمكن أن يمكن الدولة منشأ التصرف أن تطمس هوية الفاعل الحقيقي (سمودي، 2018، صفحة 338)، إضافة إلى ذلك فإن عملية نسبة العمل الدولية تزداد تعقيدا في الحالة التي لا تكون الشبكات السيبرانية هي الوسط الذي تمت من خلاله هذه الهجمات، كإرسال فيروسات توضع مباشرة في أجهزة الحاسوب الخاصة بالدولة المستهدفة، أو في الحالة التي يستخدم فيها إقليم دولة أخرى لتنفيذ هذه الهجمات، كما أن التحقيقات بشأن الهجمات السيبرانية قد تجمع بين المبادئ الأساسية لعمل أجهزة الاستخبارات بوصفها عملا ماديا طبيعيا وبين الإلكتروني العابر للشبكات والحدود الدولية، لكن المحققين في أجهزة الاستخبارات الدولية قد لا يستطيعون الولوج إلى الدول الأخرى لأنه يشكل مساسا و انتهاكا بسيادتها.

يترتب على المسؤولية الدولة عن هجمات السيبرانية أضرار فقد تؤدي الهجمات السيبرانية ضد الشبكات الخاصة بالمؤسسات الأمنية و العسكرية إلى سيطرة عليها مما يؤدي إلى وقوع ضحايا في صفوف المقاتلين و المدنيين، وتهديد السلم والأمن الدوليين، مما يوحي أن الهجوم السيبراني في مجال العسكري له نفس النتائج الناجمة عن الاستخدام المادي لبقوة العسكرية و المتمثلة في انهيار البنى التحتية للدولة و قتل العسكريين و المدنيين (بدران، 2010، صفحة 111)، أما من الجانب الاقتصادي فقد يتم اختراق النظام المصرفي و إلحاق أضرار بأعمال البنوك أو أسواق المال، وتعطيل عملية التحويل المالي، كما يمكن استخدام التكنولوجيا في إعلانات المنتجات الجديدة،ومعلومات ترويجية حول المبيعات و التسويق الإلكتروني وجمع المعلومات الخاصة بخدمة العملاء، فأي هجوم سيبراني في هذا المجال سيخلف أثار سلبية وسيكون المدنيون عاطلين عن العمل وغير محميين، و ستتعطل العمليات من منطقة إلى أخرى مسببة تدهورا اقتصاديا على مستوى الدولة (سليمان، 2012، صفحة 62).

ترى اللجنة الدولية للصليب الأحمر أن أهم المعايير التي يجب الاستناد إليها في تحديد المستوى المطلوب لوصول العمليات السيبرانية إلى درجة الهجوم المسلح يتمثل في جسامة هذا التصرف أو حدته، ومدى تأثيره على الدولة المعتدى عليها، وأن يكون هناك ضررا ماديا حالا على الأفراد والممتلكات في الدولة المعتدى عليها بهجوم سيبراني، وفي سبيل ذلك قامت اللجنة بالمقارنة بين أثر الهجمات العسكرية التقليدية والهجمات السيبرانية استنادا إلى قياس نتائج الأخيرة، وفيما إذا كانت منتجة لأضرار مماثلة للهجمات العسكرية التقليدية أم لا، من هذا

المنطلق ترى اللجنة أن الأضرار الناتجة عن الهجمات السيبرانية مماثل للهجمات العسكرية التقليدية أو يفوقه كما لو حدث اعتداء سيبرانيا على شبكات الكمبيوتر الخاصة بمطار إحدى الدولة،و أدى إلى مقتل الآلاف بسبب الخلل الذي أحدثته الهجمة وأدى إلى تصادم الطائرات هبوطاً وصعودا، ففي مثل هذه الحالة تعتبر العملية السيبرانية هجوماً عسكرياً، أما تلك التصرفات التي، لا تلحق مثل هذا النوع من الضرر فتخرج حسب اللجنة من دائرة الهجوم العسكري، إلا في الحالة التي تضر فيها هذه العمليات السيبرانية بمصلحة وطنية حساسة للدولة المعتدى عليها دون أن تتصل بضرر مادي محسوس.

عليه تعتبر الهجمات الإلكترونية عمل غير مشروع ابتداء، وهو بحد ذاته ينتهك أحكام وقواعد القانون الدولي لأنه يخترق أسرار ووثائق الدول،و يستهدف مصالحها الكبرى ويختلق مشاكل وقضايا دولية معاصرة لم تكن موجودة في السابق في عهد الحروب التقليدية ولا حتى الحرب الباردة، فهذا التسابق في التسلح التقني الجديد نعتبره في غاية الخطورة والدقة والأهمية.

المطلب الثاني:المسؤولية عن الهجمات السيبرانية استنادا إلى نظرية المخاطر

جاءت نظرية المخاطر كنظرية حديثة نتيجة الانتقادات التي وجهت لنظرية الفعل غير المشروع التي أصبحت عاجزة عن مواكبة التطور التكنولوجي و العلمي، و كان نتاج هذا التطور العالم الافتراضي الذي أصبح مسرحا لإدارة شؤون الدول في شتى المجالات سواء سياسية أو اجتماعية أو اقتصادية، و تقوم نظرية المخاطر على أساس مساءلة الشخص القانوني الدولي الذي يقوم بارتكاب سلوك مخالف للقانون الدولي يكون على درجة الخطورة بحيث ينتج عنه أضرارا بالدول أخرى، فالعبرة بحدوث الضرر لأنه وحده من يرتب المسؤولية الدولية في حق الدولة التي تباشر نشاطا دوليا مشروعا، ويؤكد أنصار هذه النظرية على أن المخاطر تقوم على فكرة تحمل نتائج التي تترتب عن النشاطات الخطرة وليس على أساس الخطأ.

من أهم الاتفاقيات الدولية التي أخذت بنظرية المخاطر نجد الاتفاقيات الخاصة بالطاقة الذرية التي تلزم الدولة التي تقوم بأي نشاط ذري وقت السلم بتعويض الأضرار الناجمة عن هذه النشاط على أساس المسؤولية المطلقة المتجردة عن نسبة أي خطأ للدولة كاتفاقية باريس المتعلقة بالمسؤولية الدولية قبل الغير في ميدان الطاقة النووية لسنة 1960 التي وازنت بين المصالح بما يضمن تطوير الإستخدمات السلمية للطاقة النووية، و المسؤولية بموجب هذه الاتفاقية مطلقة تقع على عاتق المشغل القائم بإدارة المنشأة النووية فهو المسؤول عن أي

خسارة أو ضرر للأشخاص أو الممتلكات، وعما يقع خارج المنشأة و لا تنتفي المسؤولية إلا في حالة وقوع حادث إبان النزعات المسلحة أو كارثة طبيعية أو غزو وإلا عليه أن يدفع تعويض اللازم (العيشاوي ص.، 2010، صفحة 174).

إن أغلب الأضرار التي تصيب دولا أخرى تكون نتيجة أعمال غير مشروعة للدول المتسببة فيها أو عن أنشطة مشروعة وفقا لمعايير القانون الدولي،ورغم ذلك يتعذر إثبات عدم مشروعيتها أو يتعذر إثباتها بصفة عامة لذلك أقيمت المسؤولية على أساس توفر ركن الضرر و العلاقة السببية بين الضرر و بين النشاط الذي تقوم به الدولة،وعلى هذا الأساس يجب أن نبين ما إذا كانت شروط المسؤولية الموضوعية تنطبق على الفضاء السيبراني، وعليه فإن أول شرط يجب أن يتوفر هو وجود نشاط خطر باعتبار أن الهجمات السيبرانية و الأنشطة الضارة في الفضاء السيبراني تسبب ضررا عابر للحدود يمس البنية التحتية للدول و الأمن و السلم الدولي، فإن الهجمات السيبرانية و الأنشطة الضارة التي تقوم بها الدول في العالم الافتراضي. تكيف على أنها نشاطات خطرة نظرا لما يترب عليها من آثار وخيمة على الأمن القومي و الدولي.

أما الشرط الثاني وهو الضرر العابر للحدود وهنا لا يمكن أن ننكر أن الهجمات السيبرانية و الأنشطة الضارة التي تمارسها الدولة في الفضاء الإلكتروني تلحق أضرارا بالدولة ، إذ أن تبني الدول الحكومة الإلكترونية في تسيير شؤونها و اتساع نطاق مستخدمي وسائل الاتصال و تكنولوجيا المعلومات في العالم جعل قواعد البيانات القومية غير سرية مما عرضها إلى مخاطر هجمات الفضاء الإلكتروني حيث أصبحت المصالح القومية التي ترتبط بالبنية التحتية الحيوية عرضة لخطر الهجوم، التي تشمل الطاقة و الاتصالات و المصاريف و المؤسسات المالية باعتبار أن العالم الافتراضي جعل تلك المصالح مرتبطة ببعضها البعض في بيئة عمل واحدة التي تعرف بالبيئة التحتية القومية للمعلومات، و لكون الفضاء الالكتروني عابرا للحدود و سهولة الدخول إليه اتسعت دائرة الصراعات السيبرانية وزاد عدد المهاجمين وظهرت حالات الكر و الفر لتعبر عن صراع ممتد وتعبيرا وكاشفا عن ما يجري في الأرض وصراع حول امتلاك أدوات الحماية و الدفاع و تطوير القدرات الهجومية الإلكترونية وسباق حول حيازة القوة و الهيمنة و تعظيم القدرة على زيادة النفوذ و التأثر على المستويين المحلي و الدولي، مما قد ينجم عليه هجمات سيبرانية من أجل الاستحواذ على المعلومات أو سرقة الأسرار الدولة مما يعرض أمنها، و استقرارها للخطر و يزعزع نظام الحكم فيها.

إن قيام المسؤولية الموضوعية تشترط وجود علاقة سببية بين النشاط الخطر و الأضرار الناتجة عنها (حيدرة، 2014، صفحة 145)،لذا يجب إثبات أن الأضرار التي لحقت الدول ومست أمنها القومي ناتج عن الهجمات السيبرانية التي قامت بها دولة أخرى، من يمكن القول أن نظرية المخاطر يمكن أن تصلح كأساس للمسؤولية الموضوعية في عالم الخارجي، لكن لا يمكن اعتماد عليها كأساس للمسؤولية الدولة عن الهجمات السيبرانية باعتبار أن نشاط الدولة في عالم الإفتراضي ليس مشروع فهو في زمن الحرب نزاعا مسلحا وفي وقت السلم يكيف على أنه نشاط إجرامي تقوم به دولة ضد دولة أخرى من أجل تحطيم البنية التحية للدول مما يشكل تدخل في الشؤون الداخلية للدول.

من هذا الجانب يمكن القول أن مسؤولية الدولية عن الهجمات السيبرانية في سياق القواعد الدولية للقانون الدولي العام قد لا تحقق أهدافها و السبب هو صعوبة تحديد هوية المهاجم السيبراني، وبالتالي تزداد صعوبة مهمة الدولة المدعية في إثبات هوية المهاجم السيبراني، والعمل على إكمال ملاحقه قضائيا، وهذا بحد ذاته يعد عائقا أمام تحقيق أهداف القانون الدولي باعتباره ينظم قواعد المسؤولية المتعلقة بانتهاكات القانون الدولي العام و القانون الدولي الإنساني.

تعتبر أول مرة نفذت فيها الهجمات السيبرانية، كانت في حرب كوسوفو سنة 1999 ، من خلال استهداف سلاح الجو التابع لحلف الشمال الأطلسي لشبكات الهاتف في يوغسلافيا السابقة وفي النزاع المسلح ذاته، وبعد استهداف طيران حلف شمال الأطلسي للسفارة الصينية في بلغراد، قام عدد من القراصنة الصينيين وكردة فعل بمهاجمة مواقع الكترونية رسمية منتخبة تابعة للولايات المتحدة الأمريكية، وبالذات الموقع الالكتروني للبيت الأبيض نجم عنها الاستحواذ على الآلاف من البيانات الرقمية ، المصنفة آنذاك بأنها عالية السرية(W.Smith, 2002, p. 366) ، وهناك الهجوم السيبراني الذي تعرض له المفاعل النووي الأمريكي ديفيد بيس لتوليد الطاقة الكهربائية في أوهايو في 02 جوان 2003 بفعل أنظمة اختراق وتعطيل لشبكات السيطرة والتحكم الالكترونية في المفاعل نفسه(Kesler, 2011, p. 19) ، فلولا وجود وسائل الحماية في المفاعل، و مبادرتها بإطفاء المفاعل ذاتياً، لكانت الكارثة تتعدى توقف المفاعل النووي عن العمل، و لأدى إلى كارثة انفجاره ، لدرجة يصعب فيها تخيل الأضرار والخسائر البشرية الناجمة عن ذلك الهجوم.

خاتمة

ظهرت الهجمات السيبرانية نتيجة التطور الحاصل في تقنيات الحاسوب نتيجة الثورة التكنولوجية في العالم، وهو سلوك غير مشروع يهدد أمن الدول و سلامة مواطنيها وبنيتها التحية الحيوية ،و يتسبب في تعطيل استخدام الدولة لآليات الإلكترونية في إدارة شؤونها الداخلية، كما يمس بالسلم و الأمن الدوليين، مما يستلزم مساءلة الدولة التي تشن هجمات السيبرانية ضد دولة أخرى ونتج عنها أضرار لحقت بها، من خلال دراسة موضوع محل البحث تم التوصل إلى المجوعة من النتائج و الاقتراحات.

أولا- النتائج:

- تمتاز هجمات السيبرانية بقوة تدميرية لا تصاحبها دماء وأشلاء، إذ يتضمن التجسس ثم النسف، لكن لا دخان ولا غبار فيتم التدمير بوابل من الفيروسات،كما أن انتشار الفضاء الالكتروني وسع دائرة استهداف المواقع بمستوياتها كافة.

- لا تحتاج الدول إلى تخصيص ميزانيات ضخمة لإنتاج أسلحتها أسوة بالأسلحة المستخدمة في النزاعات التقليدية ذات الكلفة العالية، وأنما ذات تكلفة متدنية نسبة للأدوات اللازمة لشنها.

- تقع مسؤولية الدولة على ما تقوم به من هجمات سيبرانية تلحق أضرارا بدولة أخرى على أساس خرقها للقواعد القانون الدولي كمبدأ عدم التدخل في الشؤون الداخلية للدول، وعليه فإن النظرية العمل غير المشروع يمكن استناد عليها كأساس لقيام المسؤولية الدولية عن الهجمات السيبرانية، أما نظرية المخاطر فيتم استبعدها بسبب عدم مشروعية الهجمات السيبرانية التي تقوم بها الدولة.

- يعتبر الهجوم السيبراني استخداما للقوة نتيجة الآثار التي يخلفها مقارنة بالهجوم المسلح، وكلاهما يحقق ذات النتيجة ويمكن أن تكون نتائج الهجوم السيبراني أكثر تدميرا وخطورة لذا فهو يرتقي إلى مستوى الهجوم التقليدي.

ثانيا- الاقتراحات:

- تعزيز العمل والتعاون وتبادل المعلومات مع جميع المنظمات الدولية والإقليمية ذات الصلة فيما يتعلق بالمبادرات المتصلة بالأمن السيبراني في مجالات اختصاصاتها، مع مراعاة احتياجات مساعدة البلدان النامية.

- تعيين نظام سريع وفعال للتعاون الدولية، و الحفاظ بشكل سريع على البيانات المخزنة على أجهزة الكمبيوتر وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة على الكمبيوتر.

- اتخاذ الإجراءات من قبل الدول لضمان حمايتها من الهجمات السيبرانية من خلال تعزيز الاستثمار في الأمن الإلكتروني وحماية البنية التحتية الرقميه بها،وتدريب الكوادر الوطنية في مختلف المؤسسات على كيفية التعامل مع الهجمات السيبرانية، و مواجهتها و الحد من تداعيتها وكذا نشر الوعي السيبراني في المجتمع.

- العمل على تزويد الجيوش بتقنيات ومهارات التعامل مع التهديدات السيبرانية من خلال تدريب مهندسين المعلوماتيين العاملين في القوات المسلحة بهدف اكتساب مهارات الأمن السيبراني تؤهلهم إلى تولي مسؤوليات حماية البنية البنى التحتية الوطنية من التهديدات الهجمات السيبرانية.

قائمة المراجع:

أولا- مراجع باللغة العربية:

1- الكتب:

- إيهاب خليفة،2009، مجتمع ما بعد المعلومات،تأثير الثورة الصناعية الرابعة على الأمن القومي، العربي للنشر والتوزيع، الطبعة الأولى، القاهرة.
- خالد ممدوح إبراهيم، 2009، الجرائم المعلوماتية، دار الفكر الجامعي،مصر، الطبعة الأولى.
- شريف علتم،2005، محاضرات في القانون الدولي الإنساني، بعثة اللجنة الدولية لصليب الأحمر بالقاهرة، مصر.
- صباح العشاوي،2010،المسؤولية الدولية عن حماية البيئة، دار الخلدونية للنشر والتوزيع، الجزائر،الطبعة الأولى،.
- طارق محمد سليمان، 2012، الجريمة المعلوماتية، الجامعة الافتراضية السورية، برنامج الإجازة في الحقوق، دمشق، 2012.
- عامر الزملي،1997، مدخل للقانون الدولي الإنساني، منشورات المعهد العربي لحقوق الإنسانو اللجنة الدولية لصليب الأحمر، تونس.
- عبد الفتاح مراد،2006، شرح التحقيق الجنائي الفني و البحث الجنائي، دار الكتب و الوثائق المصرية، مصر.
- عبد العزيز العيشاوي،2007، محاضرات في المسؤولية الدولية،دار هومة للنشر والتوزيع، الجزائر.
- عباس بدران،2010 الحروب الإلكترونية (الاشتباك في العالم المتغير)، مركز دراسات الحكومات الإلكترونية، بيروت.
- عادل عبد الصادق،2016، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مكتبة الإسكندرية، وحدة الدراسات المستقبلية، مصر، 2016.

- محمد المجذوب و طارق المجذوب، القانون الدولي الإنساني، منشورات الحلبي الحقوقية، لبنان، الطبعة الأولى.

2- مقالات:

- رزق أحمد سمودي،ربيع الثاني 1440، ديسمبر 2018، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية، المجلد 15، العدد 02.

- مايك شميت، مختارات من أعداد 2002، الحرب بواسطة شبكات الاتصال(الهجوم على شبكات الكمبيوتر و القانون في الحرب)، المجلة الدولية للصليب الأحمر.

3- المداخلات:

- محمد حيدرة، المنعقد يومي 01 و 02 ديسمبر 2014، المسؤولية المدنية عن الأضرار البيئية في القانون المدني الجزائري، مداخلة مقدمة في ملتقى الوطني حول آليات الوقاية من الأخطار الطبيعية والتكنولوجية الكبرى في القانون الجزائري والقوانين المقارن ،كلية الحقوق و العلوم السياسية،جامعة حسيبة بن بوعلي،الشلف.

ثانيا- مراجع باللغة الأجنبية:

A-Overages :

- Michael N.Schmit,2013, (Tallinn manual on the international law applicable to cyber warfare), Cambridge university press, first publishes.

B- Articles :

- Andreea bendovschi,2015, cyber -attacks - trends, patterns and security counter measures, procedia economics and finance, Elsevier, Vol 28.
- Brent Kesler, 2011,the vulnerability of Nuclear Facilities to Cyber Attack, Strategic Insight Journal, Vol 10, Issue 01.
- Gervais Michael,2012,Cyber Attacks and The Laws of War, Berkeley Journal of International Law, Vol 30, Issue 02.
- Herbert Lin,2012 Cyber conflict and international humanitarian law, International review of the red cross, Vol 94,N^0 886
- Junaidu Bello Marshall, 2000, Cyber attacks (the legal response, International journal of international law) , Vol 01 , Is 02 , universal multidisciplinary research institute , India.
- Priyanka R. Dev,2015, (Use of Force and Armed Attack) Thresholds in Cyber Conflict; The Looming Definitional Gaps and the Growing Need for Formal U.N. Response), Texas International Law Journal Vol 50, Issue 2.
- Schmitt, M.N,1999,(computer network attack and the use force in international law through on normative), the Colombia journal of transitional law, Vol.27,N^0 885.
- Thomas W. Smith,2002 ,(The New Law of War: Legitimizing Hi-Tech and Infrastructural) , International Studies Quarterly, Vol 46.