القضية الافتراضية
مسابقة المحكمة الصورية العربية بدورتها الثامنة 2022

المحكمة: العدل الدولية

المدّعية الأولى: دولة نجمستان

المدّعية الثانية: دولة بدرستان

المدّعى عليها: دولة حذرستان

الموضوع: هجمات سيبرانية.

إعداد / د. إيلي مسعود خطار – الجمهورية اللبنانية

القسم الأوّل - في الوقائع:

في العام 2016، قامت دولة حذرستان بالعديد من العمليات العسكرية في أراضي إقليم رغد الخاضع لسيادة دولة نجمستان الواقعة على حدودها الشرقية، بسبب خلافات تاريخية، ذلك أنّ حذرستان تعتبر الإقليم المذكور مسلوخا عنها بدون وجه حق، كما وبسبب مخاوف جديدة بسبب إقدام دولة نجمستان على إنشاء وكالة فضاء في الإقليم المذكور ما أثار ريبتها من الأهداف المبيّتة.

إنّ ما عزّز مخاوف دولة حذرستان، هو التعاون المشترك بين دولة بدرستان الواقعة على حدودها الشمالية الشرقية ودولة نجمستان، بحيث تقوم هذه الأخيرة بتجهيز ومكننة وكالة الفضاء وتأمين حماية منشآتها وشبكة أمن نظمها، في حين تعمل دولة بدرستان على توفير التمويل اللازم لذلك.

حُدّدت الأهداف المشتركة لهذا التعاون في بيان مشترك صدر عن كل من دولة نجمستان ودولة بدرستان بتشجيع وإعداد جيل جديد من روّاد الفضاء بهدف إرسالهم في مهمّات فضائية، جمع المعلومات العلمية لأبحاث الفضاء المستقبلية، العمل مع المتاحف ومراكز العلوم في كلا الدولتين لتعليم التكنولوجيا والهندسة والتدريب العملي في منشآت وكالة الفضاء وإرساء شراكة فضاء ناجحة طويلة الأمد.

أعربت حذرستان عن معلومات لديها تفيد أنّ أعمال تجسّس استخباراتية تقع في منزلة العدوان تنوي دولة نجمستان القيام بها ضدّها تحت ستار المشروع الفضائي، من خلال العمل على تطوير وإطلاق أقمار اصطناعية بهدف الاستطلاع والاتّصال والاستهداف والعدوان، رغم تأكيد نجمستان على سلمية مشروعها الفضائي، وعلى كونه حقا مشروعا لها، ذلك أنّ كل الدول تتمتع بالحرية في استخدام الفضاء وفقا للقانون الدولي، وهي لا تستهدف من مشروعها المذكور سوى الأبحاث العلمية والتدريب واستخدام الأقمار الصناعية للإنذار المبكر وإدارة الاتّصال الفعّال للأزمات وغيرها من الأنشطة السلمية ولكن ليس للعدوان.

بتاريخ 2017/9/2 وبصورة مفاجئة، تعرّضت دولة نجمستان لسلسلة هجمات سيبرانية قوية تشكّل ما يعرف بجريمة الاختراق أو ما يعرف بجريمة الدخول غير المشروع أدّت الى اختراق أنظمتها وإلحاق أقصى الأضرار بها من خلال التشويش الإلكتروني والهجوم على الحواسيب العسكرية وإعاقة وظائفها واستغلال ضعف شبكاتها وتدمير أجهزتها، مستهدفة بشكل أساسي وكالة الفضاء ومصارف ووزارات وصحف وشركات كهرباء ونظم المترو وأهداف مدنية، واستمرت هذه الحرب لمدة سبعة ايام.

كان الهدف من الهجوم السيبراني شلّ عمل دولة نجمستان بصورة عامة وشلّ عمل مشروعها الفضائي بشكل خاص بحيث تمّ اختيار التوقيت المناسب بدقّة.

وبالفعل، انطلق الهجوم عشية يوم العطلة الرسمية لدولة نجمستان احتفالًا بالذكرى السنوية للاستقلال بحيث كانت معظم المكاتب الحكومية خالية، ممّا سمح للهجوم السيبراني في الانتشار بدون أي تدخل لصدّه، فتمّ التغلغل إلى نظم وكالة الفضاء والسيطرة عليها والتحكّم بها عن بعد، الأمر الذي مكّن المهاجمين من إرسال معلومات خاطئة إلى غرفة التحكّم لجعلها تبدو وكأنها تعمل بشكل طبيعي، ما تسبّب بكارثة كبيرة جرّاء الهجمات السيبرانية أدّت إلى شلّ عمل كافة المرافق المستهدفة وتعطّلها.

في 10 / 9 / 2017 ذكرت حكومة نجمستان أنّ الهجوم قد توقّف، وصرّحت أنّ الوضع تحت السيطرة الكاملة لجهاز الأمن السيبراني، الذي يعمل على استعادة البيانات المفقودة.

في 25 / 11 / 2017 صرّح الجهاز المذكور أنّ بحوزته دلائل على تورّط دولة حذرستان.

بدورها سارعت حذرستان إلى نفي أي دور أو مسؤولية لها عن الهجمات، ووصفت مزاعم نجمستان بأنّها اتّهامات واهية لا أساس لها.

اعتبرت دولة نجمستان أنّه بحسب قواعد القانون الدولي الانساني وقانون النزاعات المسلّحة، يعود لكل دولة الحق بالرد على الهجمات التي توجّه ضدها بكل الوسائل المشروعة، وقد دعمت رأيها مستندة الى تجربة الولايات المتحدة الأميركية عقب هجمات الحادي عشر من أيلول عام 2001 في إطار ممارسة حق الدفاع المشروع، واستندت على قرار مجلس الأمن رقم 1368 الصادر بتاريخ 2001/9/12 والذي أعرب عن تصميمه على مكافحة التهديدات للسلام والأمن الدوليين الناجمة عن أعمال الإرهاب والاعتراف بحق الدفاع عن النفس الفردي والجماعي.

وعليه، شنّت دولة نجمستان بتاريخ 2017/12/20 هجوما" عسكريا" تقليديا" محدودا" ضد دولة حذرستان ردّا" على الهجوم السيبراني مستهدفة المقارّ الحكومية والعسكرية والمدنية، رغم إدراكها لصعوبة معرفة هوية المهاجم وموقعه الجغرافي، ما يجعل عملية نسبة الفعل الضار المتمثل بالهجوم السيبراني لدولة حذرستان أمرا" صعبا" للغاية.

القسم الثاني – في القانون والطلبات:

بتاريخ 2018/2/5 تقدّمت دولة نجمستان بدعوى لدى محكمة العدل الدولية ضد دولة حذرستان مستندة إلى ما يلي:

- القانون الدولي الإنساني الذي ينظم سلوك الدول، الجماعات والأفراد وينطبق في السلم والنزاع، ويطبق على الهجمات السيبرانية التي تشكّل تهديدا للأمن والسلم الدوليين، وتؤدّي إلى إلحاق دمار كبير في الركائز الأساسية داخل الدولة، وتؤثّر على شعبها والبنية الاقتصادية والأمنية الطبيعية الخاصة بها.

- ميثاق الأمم المتحدة لعام 1945 الذي يحدّد أنه يجوز استخدام القوة المسلّحة في حالة الدفاع الشرعي عن النفس (المادة 51) وفي حالة وقوع عمل عدواني يبرّر تدخل مجلس الأمن استنادا" إلى الفصل السابع من الميثاق.

- " دليل تالين " الذي يشير إلى إمكانية تطبيق القانون الدولي الإنساني والذي يعتبر أنّ الهجوم السيبراني يعتبر بمثابة استخدام للقوة، الأمر الذي يحتّم إخضاعه لقانون النزاعات المسلّحة.

وخلصت إلى المطالبة بإعلان مسؤولية دولة حذرستان عن الهجمات السيبرانية، وبالتالي إلزامها بالتعويض عليها عن الأضرار المادية والمعنوية الفادحة التي لحقت بها وما نتج عنها من فسخ التعاون المشترك بينها وبين دولة بدرستان، وتوقف العمل في مختلف المرافق لا سيّما في وكالة الفضاء وتهديد استمراريتها.

بالمقابل، قدّمت دولة حذرستان دفاعها طالبة رد الدعوى لعدم القانونية ولعدم الثبوت مستندة إلى ما يلي:

- مبدأ تحريم استخدام القوة وحق اللجوء إلى الحرب في القانون الدولي.

- نص ميثاق الأمم المتحدة لجهة امتناع أعضاء المنظمة جميعا" في علاقاتهم الدولية عن التهديد باستعمال القوة أو استعمالها ضد سلامة الأراضي أو الاستقلال السياسي لأيّة دولة أو أي وجه آخر لا يتفق ومقاصد الأمم المتحدة. **(الفقرة الرابعة من المادة الثانية من ميثاق الأمم المتحدة لعام 1945)**

- في حال التسليم جدلا" بانتهاك أحكام المادة المذكورة، فإنّ العدوان الذي لا يصل لدرجة القوة لا يفعّل حق الدفاع الشرعي للدولة الضحية.

- يعود الحق للدولة في الدفاع عن نفسها عندما تواجه هجوما" مسلّحا"، في حين لا يعتبر الهجوم السيبراني نزاعا" مسلّحا" لأنه لا يتضمّن استعمالا" للقوّة المسلّحة.

- انّ تطبيق القواعد الأساسية للقانون الدولي الإنساني لا يتماشى مع مستجدات العصر، لأنه وضع أساسا للتعامل مع النزاعات المسلّحة التقليدية ولا ينطبق على الهجمات السيبرانية.

-انّ القانون الدولي الإنساني لا يتلاءم مع وسائل وأساليب الهجمات السيبرانية، بالإضافة إلى أنّ المعاهدات القائمة يرجع تاريخها إلى ما قبل وجود أو ظهور هذه الهجمات، بحيث أنّ عبارة الهجوم السيبراني لم ترد في ميثاق الأمم المتحدة واتفاقيات جنيف ولاهاي ومعاهدة حلف شمال الأطلسي.
- عدم مراعاة دولة نجمستان للقواعد المتعلقة بالاستهداف وأهمّها مبادىء التمييز، التناسب والضرورة العسكرية، كما عجزها عن إثبات ضلوع حذرستان او مسؤوليتها عن الهجمات السيبرانية، وعجزها أيضا " عن اثبات أنّ الهجمات السيبرانية كانت موجهة نحو أهداف مدنية.

- عدم سلوك دولة نجمستان الطرق الديبلوماسية والسياسية أوّلا" لاجبار دولة حذرستان التي يُزعم انطلاق الهجمات السيبرانية من إقليمها على ردعها ومحاسبة من نفّذها وإيقافها، إنما لجأت مباشرة إلى الحرب العسكرية التقليدية.

- وخلصت إلى المطالبة بإعلان عدم صلاحية محكمة العدل الدولية لبت النزاع لأنها غير مسؤولة عن الهجوم السيبراني كونه من تدبير مجموعات إجرامية تعمل من خلال شبكة الإنترنت المظلم (Dark Web) بحيث يمكن للمهاجم استعمال تكنولوجيا اتّصال مجهول الهوية والتشفير لإخفاء هويته، وبالتالي استحالة توجيه الاتهام إليها أو إلى أيّة دولة من الدول، ما يجعل الصلاحية معقودة للمحكمة الجنائية الدولية.

بدورها تقدمت دولة بدرستان من المحكمة ذاتها بدعوى ضد كل من دولة حذرستان ونجمستان مدلية ومستندة إلى ما يلي:

- أنّ المسؤولية مشتركة على عاتق كل من دولة نجمستان شريكتها، ودولة حذرستان، الأولى كونها تعهدت في اتفاق التعاون المشترك فيما بينهما على تجهيز وكالة الفضاء ومكننتها وتأمين الأمن وحماية المنشآت، خاصة أنّ وكالة الفضاء تقع ضمن أراضيها، في حين أثبتت الهجمات السيبرانية هشاشة نظام الدفاع والأمن السيبراني وسهولة اختراقه، والثانية، كونها مسؤولة عن الهجمات السيبرانية التي حصلت.

- في سبيل تبيان عدم جدوى الحروب المتبادلة بين كل من حذرستان ونجمستان، أثارت بدرستان في دعواها إشكالية قانونية جديدة انطلاقا" من عدم تبني دولة حذرستان للهجوم السيبراني رغم إقرارها بحصوله وهي التالية:

مسألة الهجوم السيبراني من قبل مدنيين أو جماعات مسلّحة منظمة غير منتمية للدولة يشير إلى تساؤل مهم وهو هل من الممكن تطبيق القواعد ذاتها التي تطبق على تفعيل حق الدفاع الشرعي فيما بين الدول على تلك الهجمات التي توجّه من قبل أشخاص غير منتمين للدولة ، سواء في إطار نزاع مسلّح دولي أم نزاع مسلّح غير دولي تتعدى آثاره على الدول الأخرى غير الطرف في النزاع، ذلك أنّ مسألة الدفاع الشرعي وانتهاك القواعد المتعلقة بحظر استخدام القوة في العلاقات الدولية تطبق فقط على الدول وليس على الأشخاص غير المنتمين للدولة بأي صلة من الذين يقومون بتنفيذ الهجمات ضد الدول الأخرى، بالإضافة إلى أنّ الدول ترغب في اللجوء الى أدوات الهجوم السيبراني واستخدام المنظّمات، الجماعات والأفراد غير التابعين لها في الأصل من أجل توجيه الهجمات السيبرانية ضد الدول الأخرى وذلك بغية التنصّل من المسؤولية الدولية التي يمكن أن تترتب عليها إذا ما تمّ نسبة تصرّفات هؤلاء إلى الدولة.

- وخلصت إلى المطالبة بأنّها تكبّدت خسائر فادحة لا تعوّض جرّاء إلحاق أقصى الأضرار باستثمارها في وكالة الفضاء ما يستوجب التعويض عليها عن كافة الأضرار اللاحقة بها بالتكافل والتضامن فيما بين حذرستان ونجمستان وفسخ اتفاق التعاون مع هذه الأخيرة على كامل مسؤوليتها.

كذلك ردّت دولة نجمستان على الإشكالية المطروحة من قبل بدرستان مدلية بما يلي:

- وجود حق الدفاع الشرعي وحق الرد على الهجمات السيبرانية التي توجّه من الجهات الفاعلة من غير الدول، مستندة إلى ممارسة الدول أعقاب هجمات الحادي عشر من أيلول عام 2001 التي وفّرت دعما" قويا" لوجود الحق في الدفاع والرد على الهجمات الفاعلة من غير الدول حتى لو لم تكن لهذه الهجمات ايّة علاقة بالدولة، معزّزة موقفها بقرار مجلس الأمن المذكور سابقا" حول الحق في الدفاع الشرعي والرد ضد منفّذي هجمات الحادي عشر من أيلول، بحيث أنّ للدولة التي تواجه الهجمات السيبرانية او خطر التعرّض لها تستطيع أن ترد على هذه الهجمات حتى لو كانت توجه من قبل أشخاص لا ينتمون إلى الدولة مثل المدنيين المشاركين مباشرة في الهجوم السيبراني أو الجماعات المسلّحة المنظمة غير المنتمية إلى الدولة، ويكون هذا الرد مشروعا" طالما كان موافقا" لقانون حق اللجوء إلى الحرب.

- أنّ دولة حذرستان تتحمل المسؤولية الدولية ليس فقط في حالة نسبة تصرّف المشارك المباشر لها بل تتحمل هذه المسؤولية لأنها لم تتخذ التدابير اللازمة لمواجهة المشارك المباشر في الهجمات السيبرانية ومنعه من تنفيذ الهجوم.

- لا يمكن التسليم بأنّ تصرفات المشارك في الهجوم السيبراني التي تشكّل انتهاكا" للقانون الدولي والتي لا يمكن أن تنسب إلى دولة، تبقى بدون عواقب، ومن دون الخضوع لأيّة مسؤولية بموجب القانون الدولي.

- إنّ ضرورة إخضاع أي عمل عدائي تحت المسؤولية الدولية يتطلّب البحث عن عدّة معايير أخرى تلزم الدول بمنع الضرر العابر للحدود من إقليمها ضد الدول الأخرى، بحيث تكون المسؤولية الدولية لحذرستان عن الهجمات السيبرانية ثابتة من خلال الإخلال بواجب فرض احترام القانون الدولي الإنساني ومن خلال الإخلال بواجب منع حصول الضرر وواجب القمع بعد حصول الضرر، ومن هذا المنطلق يكون من حق دولة نجمستان الدفاع السيبراني.

- التأكيد على اختصاص محكمة العدل الدولية كون دولة حذرستان مسؤولة عن الهجمات السيبرانية كدولة من جهة، ومن جهة أخرى، وعلى سبيل الاستطراد، لأنه لا يمكن اعتبار اختصاص المحكمة الجنائية

الدولية متوفرا" فيما خصّ الجرائم الدولية المرتكبة عن بعد، الأمر الذي يخالف أحكام نظام روما الأساسي للمحكمة الجنائية الدولية.

بدورها ردّت دولة حذرستان معتبرة ما يلي:

- أنّ التصرّف الوحيد الذي ينسب إلى الدولة على الصعيد الدولي هو تصرّف أجهزتها الحكومية أو الأشخاص الذين تصرّفوا بموجب تعليمات من أجهزتها أو بإيعاز منها أو تحت رقابتها، أو بصفتهم وكلاء للدولة. وتتحمل الدولة المسؤولية القانونية الدولية عن الهجمات السيبرانية التي تنسب إليها والتي تشكّل خرقا" لالتزام دولي. والحق في اتخاذ التدابير المضادة أو الدفاع الشرعي من قبل الدولة الضحية ضد الهجمات السيبرانية يستلزم قبل كل شيء أن يتم إثبات وجود الهجوم السيبراني، وأن يتم نسبة هذا الهجوم السيبراني إلى دولة، الأمر غير الثابت.

2- الأسباب الموجبة:

إنّ السباق غير التقليدي نحو الهجمات السيبرانية يتزايد بسبب المميزات العديدة لهذه الهجمات كسرعة الأداء، فاعلية التدمير، صعوبة الكشف عن القائم بهذه الهجمات.

من هذا المنطلق، يكتسب الأمن السيبراني أهمية كبيرة كونه يحمي من سرقة البيانات الحسّاسة، معلومات التعريف الشخصية، المعلومات الصحّية، الملكية الفكرية، أنظمة المعلومات الحكومية والصناعية وغيرها.

يمثل الأمن السيبراني قضية دولية يصعب على مختلف حكومات العالم وكبرى الشركات التصدّي لها بمفردها، الأمر الذي يتطلّب التعاون مع مختلف الجهات الحكومية والخاصة في سبيل إرساء قواعد راسخة.

يهدف الأمن السيبراني إلى حماية واستعادة أنظمة الكمبيوتر والشبكات والأجهزة والبرامج من أي نوع من أنواع الهجمات السيبرانية الخطيرة والمتطورة والتي يعتمد فيها المهاجمون أساليب مدعومة بالذكاء الاصطناعي والتعلّم الآلي لإطلاق هذه الهجمات بهدف التحايل على ضوابط الأمان، وبالتالي اختراق الأنظمة الآمنة بدون أي تدخل بشري، وتشكّل هذه الهجمات السيبرانية ذعرا" عالميا"، لذلك تسعى الحكومات في جميع أنحاء العالم إلى زيادة جميع الموارد المتاحة من أجل تأمين الأمن السيبراني.

من هذا المنطلق تمّ اقتراح موضوع القضية الافتراضية لهذا العام خاصة أنّ ما نعيشه اليوم من اعتماد أكثر فأكثر على الوسائل الالكترونية لتأمين التواصل والعمل والتعلّم عن بعد بسبب جائحة كورونا، والاستعدادات الدولية لإطلاق تقنية ال 5G وما تشكّله من تحديات وما قد تتسبّب به ربما من ثغرات في مجال الأمن السيبراني، كلها عوامل ومواضيع تجعل من موضوع الأمن السيبراني يستحوذ على اهتمام الطلاب وجيل الشباب كونه مرتبطا بحاضرهم ومستقبلهم ولتعزيز خبراتهم وتمرّسهم في القانون الدولي الإنساني والمعاهدات والمواثيق الدولية ذات الصلة، والانكباب على دراسة الإشكاليات القانونية التي نتجت عن الثورة

الرقمية لجهة مدى انطباق القانون الدولي بما في ذلك قانون النزاعات المسلّحة والقانون الدولي الإنساني على الهجمات السيبرانية، وعلى مبدأ عدم وجود فراغ قانوني، في حين أنّ بعض المنظمات الدولية مثل اللجنة الدولية للصليب الأحمر وبعض الدول مثل الولايات المتحدة الأمريكية وأستراليا تعتبر أن القانون الدولي القائم كافي لتنظيم الهجمات السيبرانية.

3- بعض المراجع والمصادر:

1- دليل تالين باللغة العربية.
2- قواعد ومبادىء القانون الدولي الإنساني.
3- شرط مارتنز، اتفاقية لاهاي (البند الرابع).
4- د. شيخة حسن الهلالي، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة الشارقة، 2020 م.
5- رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام/ مجلة الشارقة، 2018.
6- د. يحي ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة الدولية للدراسات.
7- علم الدين بانقه، مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي، المعهد العربي للتخطيط.
8- بسمة فايد، الحروب السيبرانية: ترسانات رقمية وتهديدات دولية.
9- رزق أحمد، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلّة الشارقة.
10- خالد وليد محمود، الهجمات عبر الانترنت: ساحة الصراع الإلكتروني للجريمة، المركز العربي للأبحاث والدراسات السياسية.

11- ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟ اللجنة الدولية للصليب الأحمر https://www.icrc.org/ara/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm2013.

12- مايكل شميت، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر، 2002، ص 97.

13- احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية، منشورات زين الحقوقية، بيروت 2018، ص.56.

14- توريه، حمدون إ.، (2011)، الاستجابة الدولية للحرب السيبرانية، البحث عن الأمن السيبراني، الناشر الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، ص. 89.

15- عبد الصادق، عادل، مؤتمر حروب الفضاء السيبراني، الفضاء الإلكتروني وأسلحة الانتشار الشامل بين الردع وسباق التسلح 2015/5/15، متاح على الرابط التالي:
https://seconf.wordpress.com/2015/05/15/

16- عبد الصادق، عادل، (2009)، الإرهاب الإلكتروني، القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والاستراتيجية - الأهرام، القاهرة، ص. 130-140.

17- جرائم الحاسوب الإلكتروني في التشريع المقارن، تأليف د. هدى حامد قشقوش، أستاذ القانون الجنائي في كلية الحقوق – جامعة عين شمس، سنة 1992 (البحث الحاصل على جائزة أفضل البحوث الممتازة في جامعة عين شمس– 21 .)

18- إرشادات الاسكوا للتشريعات السيبرانية، بيروت 2012

19- فيما خصّ معرفة المهاجم وموقعه الجغرافي الذي يجعل عملية نسبة الفعل الضار المتمثل بالهجوم السيبراني أمرا" صعبا" للغاية:

Russell Buchan and Nicholas Tsagourias, Special Issue: Non-State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issue of Evidence, Journal of Conflict and Security Law, Oxford University Press, 2016, Vol. 21, No. 3, P 378

20- علي محمود كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، المؤسسة الحديثة للكتاب، الطبعة الاولى، سنة 2019

(21)
Schmitt, M., (2013), Tallinn Manual on the International Law Applicable to Cyber Warfare, (1st Edition) Cambridge University press, first publishes, p.92.

(22)
Baylon, C., (2017), Lessons from Stuxnet and the Realm of Cyber and Nuclear Security: Implications for Ethics in Cyber Warfare. In: Mariarosaria, Taddeo and Glorioso, Ludovica (Volume 134), Ethics and Policies for Cyber Operations.

(pp.213-230), Switzerland, A NATO Cooperative Cyber Defense Centre of Excellence Initiative. Page 27

(23)

Schindler, D. (1982). International Humanitarian Law and Internationalized Internal Armed Conflicts, International Review of the Red Cross, 22(230), P. 255-264.

(24)

Kelsey, J., (2008) Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare, Michigan Law Review, Volume 106, Issue 7, (p. 1427- 1452), P. 1437.

(25)

Cordula Droege, conseillère juridique au CICR, Pas de vide juridique dans le cyberspace, CICR Comité international de la Croix- Rouge: https://www.icrc.org/.../interview/.../cyber-warfare-interview-2011-0...

3- بعض الاتفاقيات الدولية:

- اتفاقيات جنيف المؤرخة في 12 أغسطس/آب 1949 المتعلقة بحماية ضحايا النزاعات المسلّحة الدولية.
- الاتفاقية الخاصة باحترام قوانين وأعراف الحرب البرية لعام 1907.
- اتفاقية لاهاي الخاصة باحترام قوانين وأعراف الحرب البرية لعام 1907.
- إعلان سان بطرسبورغ بغية حظر استعمال قذائف معينة في زمن الحرب، 1868.
- ميثاق الأمم المتحدة لعام 1945.
- النظام الاساسي لمحكمة العدل الدولية 1945.
- العهد الدولي الخاص بالحقوق المدنية والسياسية لعام 1966.
- نظام روما الاساسي للمحكمة الجنائية الدولية لعام 1998.
- مبدأ الضرورة العسكرية في المواد 2/54 و1/62 و3/71 و4/67 في البروتوكول الإضافي الأول الملحق باتفاقيات جنيف المؤرخة في 12 أغسطس/آب 1949 والمتعلق بحماية ضحايا النزاعات المسلّحة الدولية.
- الرأي الاستشاري لمحكمة العدل الدولية لعام 1966 والخاص بشأن شرعية التهديد او استخدام الاسلحة النووية.
- شريف عتلم ومحمد ماهر عبد الواحد، موسوعة اتفاقيات القانون الدولي الانساني، النصوص الرسمية للاتفاقيات والدول المصادقة عليها، إصدار بعثة اللجنة الدولية للصليب الاحمر في القاهرة، الطبعة السابعة، 2007.

4- في بعض السوابق:

أ – سورية:

في السادس من شهر أيلول من العام 2007 تعرّضت الدفاعات الجوية السورية في مدينة دير الزور لهجوم سيبراني من قبل إسرائيل أدّى الى تعطيل هذه الدفاعات لتمكين الطائرات الإسرائيلية من قصف هذا الموقع من دون الكشف عن الهجوم وتعقيبه.

ب – جورجيا:

في شهر آب من العام 2008 بدأت الحرب بين جورجيا وروسيا على خلفية إعلان استقلال بلدة أوسيتيا الجنوبية من جورجيا، وقد سبقت الحرب التقليدية بين هذه الدولتين بيوم واحد هجمات سيبرانية واسعة ضربت البنية التحتية الجورجية على الإنترنت، وقد تسبّبت هذه الهجمات بقطع التواصل بين الحكومة الجورجية ومواطنيها فضلا" عن قطع التواصل مع الدول الأخرى في العالم، واستمرت هذه الحالة حتى نهاية النزاع مع روسيا.

ج – جمهورية استونيا:

في العام 2007 تعرّضت استونيا المعروفة بتطورها التكنولوجي واعتمادها بشكل أساسي على الإنترنت وشبكات الحاسوب في الحياة اليومية، إلى هجوم سيبراني من روسيا الاتحادية استهدف البنية التحتية والمواقع الحكومية والجامعات والمستشفيات . ويعتبر هذا الهجوم أبرز مثال على مشاركة متطوّعين غير عسكريين في هجمات من هذا القبيل والذين شاركوا بصورة مباشرة في هذه الهجمات كميليشيات أو أفراد متفرقين وعلى انفراد.

د –إيران:

تعرّضت إيران لهجوم سيبراني لمدة تسعة أشهر من نهاية عام 2009 وبداية العام 2010 وقد تمّ هذا الهجوم للتسلل في أنظمة السيطرة المستخدمة في أهم المنشآت النووية الإيرانية (نطنز و بوشهر)

5- دليل المصطلحات:

- القانون الدولي الإنساني:

هو مجموعة من القواعد التي ترمي إلى الحد من آثار النزاعات المسلحة لدوافع إنسانية. ويحمي هذا القانون الأشخاص الذين لا يشاركون في الأعمال القتالية أو كفوا عن المشاركة فيها، كما أنه يفرض قيوداً على الوسائل والأساليب المستعملة في الحرب. ويُعرف القانون الدولي الإنساني أيضا "بقانون الحرب".

- محكمة العدل الدولية:

لمحكمة العدل الدولية نشاط قضائي واسع، فتفصل طبقا لأحكام القانون الدولي في النزاعات القانونية التي تنشأ بين الدول، كما تمارس وظيفة استشارية من خلال إصدار الفتاوى للجهات التي تحال إليها من هيئات الأمم المتحدة ووكالاتها المتخصصة.

- المحكمة الجنائية الدولية:

تختص بمحاكمة الأفراد المتهمين بجرائم الإبادة الجماعية والجرائم ضد الإنسانية وجرائم الحرب وجرائم الاعتداء.

تسعى إلى وضع حد للثقافة العالمية المتمثلة في الإفلات من العقوبة وهى أول هيئة قضائية دولية تحظى بولاية عالمية، وبزمن غير محدد، لمحاكمة مجرمي الحرب ومرتكبي الفظائع بحق الإنسانية وجرائم إبادة الجنس البشري.

- قانون النزاعات المسلّحة:

قانون النزاعات المسلّحة هو فرع من القانون الدولي، وهو القانون الذي وافقت الدول على التزامه في تعاملاتها مع الدول الأخرى، كما أنه ينطبق على سير الأعمال العدائية داخل الدولة.

- مبدأ الضرورة العسكرية:

استخدام القوة التي تنطوي على عمليات سيبرانية تقوم بها الدولة في ممارسة حقها في الدفاع عن النفس ينبغي أن تكون ضرورية ومتناسبة. هذا المبدأ يتضمنه التمهيد الخاص بإعلان سان بطرسبرغ للعام 1868، والذي يقر بأنّ « الهدف الشرعي الوحيد الذي يمكن للدول السعي لتحقيقه أثناء الحرب هو إضعاف القوة العسكرية للعدو»، هذا المبدأ يجيز القوة المعقولة الضرورية والشرعية في أثناء القتال لإجبار العدو على الاستسلام. أمّا النشاطات التي تتضح عدم ضرورتها عسكريًا، فهي محظورة.

- مبدأ التمييز:

وجوب التمييز بوضوح بين المقاتلين وغير المقاتلين. بحيث يجوز مهاجمة المقاتلين ما لم يكونوا قد توقفوا عن المشاركة في القتال. يتمتع المدنيون بالحماية من الهجوم، ولكنهم يفقدون تلك الحماية متى قاموا بدور مباشر في الأعمال العدوانية، وطوال فترة مشاركتهم فيها.

- مبدأ التناسب:

تحظّر الهجمات السيبرانية التي من شأنها أن تسبّب أضرارا" أو إصابات في أرواح المدنيين أو الإضرار بأهداف مدنية، والتي من شأنها أن تكون مفرطة بالنسبة للميزة العسكرية الملموسة والمباشرة المتوقعة من ذلك الهجوم. ينبغي عند مهاجمة الأهداف العسكرية تجنب إصابة المدنيين والأعيان المدنية بأضرار عارضة أو جانبية إلى أقصى حد ممكن. كما يجب ألا تكون الأضرار العارضة شديدة بالقياس إلى الميزة العسكرية المباشرة والملموسة المتوقعة من العمليات. إنّ المبالغة في استخدام القوة انتهاك شديد لقانون النزاعات المسلّحة.

- دليل تالين بشأن القانون الدولي المطبّق على الحروب السيبرانية:

تمّت كتابته من قبل مجموعة من الخبراء برئاسة مايكل سميث بتكليف من منظمة حلف شمال الأطلسي، والذي يقترح تطبيق القانون الدولي على النزاعات الإلكترونية. ظهر هذا المشروع في عام 2013، وتم تعديل الدليل ونشره في شباط 2017 تحت اسم Tallinn 2.0، وتتناول الدراسة الجديدة الخيارات التي يقدمها القانون الدولي للدول ضحايا الهجمات السيبرانية .

- الهجمات السيبرانية:

هى عمليات سيبرانية سواء كانت هجومية او دفاعية، وتهدف للتسبب بالإصابة أو وفاة الأشخاص أو الإضرار أو تدمير الأهداف. هي تلك العمليات المعلوماتية التي تستخدم الفضاء السيبراني، بقصد التسبب بأضرار في المعلومات المخزّنة وقد تصل إلى التدمير الكلي. تهدف إلى تغيير أو تعطيل أو تدمير أو سرقة أو الحصول على اختراق او استخدام غير مصرّح به، وتستهدف عادة أنظمة معلومات الكمبيوتر أو البنية التحتية أو شبكات الكمبيوتر أو أجهزة الكمبيوتر الشخصية. يمكن استخدام الهجوم السيبراني من قِبل دول أو أفراد أو مجموعات أو منظمات أو حتى عصابات.

يمكن أن تتراوح الهجمات السيبرانية بين تثبيت برامج تجسسّ على جهاز كمبيوتر شخصي ومحاولة تدمير البنية التحتية لدول بأكملها.

- الحرب السيبرانية:

هى إجراء عسكري يتضمن استخدام الطاقة الكهرومغناطيسية للتحكم في المجال الذي يتميز باستخدام الإلكترونيات والطيف الكهرومغناطيسى لاستخدام بيانات التبادل عبر الأنظمة الشبكية والبنى التحتية المرتبطة بها.

- الجريمة السيبرانية:

بطريقة مباشرة أو غير كل فعل أو امتناع من شأنه الإعتداء على الأموال المادية أو المعنوية يكون ناتجا، مباشرة عن الإستخدام غير المشروع لتقنية المعلومات.

- الدفاع السيبراني:

اعتماد الوسائل والأساليب للمحافظة على البنية التحتية السيبرانية أو للتقليل من حجم الآثار المادية وغير المادية التي سوف تسبّبها الهجمات السيبرانية بأقصى سرعة ممكنة.

- الأمن السيبراني:

ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية التي تهدف عادةً إلى الوصول إلى المعلومات الحسّاسة أو تغييرها أو إتلافها أو ابتزاز المال من المستخدمين أو مقاطعة العمليات التجارية، وتهديد مصالح الدول وأمنها الاستراتيجي.

- جريمة الاختراق:

هى كل سلوك غير قانوني يتم باستخدام الأجهزة الإلكترونية، ينتج عنها حصول المجرم على فوائد مادية أو معنوية مع تحميل الضحية خسارة مقابلة وغالبا ما يكون هدف هذه الجرائم هو القرصنة من أجل سرقة أو إتلاف المعلومات.

- الانترنت المظلم (Dark Web):

يعتبر جزءاً مهماً من منظومة الإنترنت. حيث يسمح بإصدار المواقع الإلكترونية ونشر المعلومات بدون الكشف عن هوية الناشر أو موقعه. ويمكن الوصول الى الإنترنت المظلم من خلال خدمات معينة مثل خدمة Torيستخدم العديد من مستخدمي الإنترنت نظام تور (Tor) وخدمات مماثلة كطريقة لتوفير حرية التعبير عن الرأي والارتباط والوصول إلى المعلومات وحق الخصوصية.

- التشفير:

التعمية أو التشفير تكون بشكل نص بسيط عند التخزين على وسائط التخزين المختلفة أو عند نقلها على شبكات نص مجرّد بحيث تصبح غير مقروءة لأحد باستثناء من يملك معرفة خاصة أو مفتاح خاص لإعادة تحويل النص المشفّر إلى نص مقروء. عملية الفك هذه تتم عن طريق ما يدعى مفتاح التشفير. نتيجة عملية التشفير تصبح المعلومات مشفّرة وغير متاحة لأي أحد لأغراض سرّية عسكرية أو سياسية أو أمنية.