
ماعت للسلام والتنمية وحقوق الإنسان
Maat For Peace, Development, and Human Rights
التهديدات السيبرانية
وأثرها على حماية البنى
التحتية والخدمات الحيوية

تمهيد

تصاعد الاهتمام الدولي بالعلاقة بين الامن والتكنولوجيا نتيجة بعدين هامين اما الاول فيتعلق بالتقدم التكنولوجي والانتشار السريع لتكنولوجيا الاتصال والمعلومات عالميا ودخولها في كافة مجالات الحياة وفي عمل المرافق الحيوية من خلال تطبيقاتها المتعددة ، واما الثاني فيتعلق بامكانية استخدام ذلك التقدم وما نتج عنه من ادوات واليات جديدة كوسيلة وكوسيط لتهديد عمل المرافق الحيوية والبنية التحتية الكونية للمعلومات وذلك من جراء تخطيها للحدود السيادية للدول مما جعلها بيئة خصبة للاستخدام غير السلمي من جانب كافة الفاعليين على تنوعاتهم المختلفة والذين تراوحوا ما بين استخدام الدول الى الفاعليين من غير الدول، وظهر ذلك في استخدم الفضاء الالكتروني كساحة للحرب الباردة والحرب النفسية وحرب الافكار او من خلال استخدامه لشن الحروب والارهاب بين الدول او استخدام الافراد او الجماعات الارهابية او القراصنة اوالجريمة المنظمة وذلك على نحو يؤثر في الطبيعة المدنية او السلمية للفضاء الالكتروني.

ومع تحول الفضاء الإلكتروني الي مجال جديد للتفاعلات الدولية وهو ما جعل منه ساحة يتم توظيفه في الاستخدامات المدنية والعسكرية علي حد سواء ،وقد ظهرت الهجمات السيبرانية عبر نمطين الأول يتعلق بالقوة الناعمة في الصراع عبر الفضاء الإلكتروني باستخدام حروب الافكار والعمليات النفسية. أما النمط الآخر فهو مرتبط بالقوة الصلبة باستخدام الفيروسات والهجمات الالكترونية كنشاط عدائي.وفي هذا السياق أصبح الفضاء الألكتروني مجالا للصراعات بين كل أنواع اللاعبين سواء من الدول او من غير الدول. وتبلورت الحروب السيبرانية في خصائص مغايرة للحروب التقليدية، من حيث طبيعة الأنشطة والفواعل والإنعكاسات علي بنية الأمن العالمي وكذلك في فرص الاستجابه لتلك التهديدات الجديدة. فضلا عن أن تلك الهجمات أصبحت تمثل تهديدا حرجا لعمل منظمات المجتمع المدني والمدافعين عن حقوق الإنسان.

وبالتالي تخضع تهديدات الأمن السيبراني في ضوء التطورات التكنولوجية الأخيرة وتحديات الأمن السيبراني لضوابط وقواعد القانون الدولي، اذ يعتبر الأمن السيبراني من أهم الأسلحة الأساسية التي تسعى الدول لامتلاكها وحمايتها من أي اختراق لضمان المعلومات العسكرية. كما أنه على الرغم من تطور وسائل الحرب وأساليبها عما كانت عليه عند صياغة اتفاقيات جنيف عام 1949، ولكن لا يزال القانون الدولي الإنساني منطبقا على كافة الأنشطة التي تقوم بها الأطراف أثناء النزاع المسلح وينبغي احترامه. ولا يمكن مع ذلك استبعاد حقيقة مؤداها أنه قد تكون ثمة حاجة إلى تطوير القانون لضمان توفيره الحماية الكافية للسكان المدنيين لمواكبة تطور التكنولوجيا السيبرانية أو كلما اتضح تأثيرها الإنساني بشكل أفضل. وينبغي للدول أن تقرر هذا الأمر بنفسها.

ومن هنا اهتمت مؤسسة ماعت للسلام والتنمية وحقوق الانسان بتقديم هذه الورقة البحثية حول تأثير التهديدات السيبرانية للبنى التحتية والخدمات الحيوية للدول. من خلال عدة محاور:

أولا: ماهية الهجمات السيبرانية وأنواعها

تميل العديد من الدراسات والتقارير إلى تعريف الهجمة الإلكترونية أو السيبرانية على أنها محاولة ضارة ومتعمدة من قبل جهة ما قد تكون دولة أو مؤسسة أو مجموعة أفراد أو فرد وذلك لاختراق كافة المؤسسات التي تعتمد على أنظمة الأنترنت في عملها بهدف الوصول إلى البيانات الخاصة بها وأصبتها بإضرار مادية واسعة النطاق عن طريق إغلاق أو إتلاف أجزاء منها لتعطيلها والتأثير على جودة الخدمة التي تقدمها، أو استخراج البيانات والمعلومات منها بهدف سرقتها، ناهيك عن عمليات التلاعب بالبيانات لتقويض الثقة في عمل هذه المؤسسات[1].

وتشير تقديرات الأمم المتحدة إلي أن بعض الهجمات الإلكترونية ساهمت في تحقيق ضرر محقق لأجزاء رئيسية من البنية التحتية الخدمية الخاصة بالمؤسسات الحكومية في بعض الدول بما في ذلك من التأثير على إمدادات الكهرباء والمياه والمستشفيات، هذا فضلا عن قواعد البيانات في المؤسسات المالية والوزارات الحكومية[2]. ومع تمدد الأعمال العدائية الإلكترونية إلى البنية التحتية المعلوماتية للدول لتحقيق أغراض متداخلة(سياسية واقتصادية وإجرامية وغيرها) حمل مفهوم الحرب الإلكترونية أبعادا جديدة، وصار البعض يفضل مصطلح الحرب السيبرانية كتعبير عن ذلك التوجه الجديد الذي يعبر عن تلك الأنشطة العدائية الإلكتروني منها الهجمات الإلكترونية والإرهاب الإلكتروني وغيرهما. [3] .

وبناءا على ذلك يمكن تقسيم الهجمات الإلكترونية إلى أنواع عديدة، وذلك طبقا للوسيلة المستخدمة في الاختراق الإلكتروني أو الهدف النهائي للعملية، إذ يتم استخدام البرامج الضارة والفيروسات لإلحاق الضرر بشبكة الأنترنت التي تعمل على تشغيل الخدمات المختلفة ويعتبر برنامج حصان طروادة أحد أبرز الأمثلة الخاصة بهذا الأمر وتسبب هذه الهجمات في تعطيل شبكة الأنترنت أو التحكم فيها عن بعد، علاوة علي ذلك تقوم بعض الجهات على إرسال رسائل بريد إلكتروني لخداع الجهة المستهدفة من أجل سرقة المعلومات الخاص بها أو التحكم بها وتعرف هذه التقنية بعملية التصيد الإلكتروني وغالبا ما يتم استخدمها ضد المدافعين عن حقوق الإنسان ونشطاء المجتمع المدني، وفى هذا الإطار تحاول بعض الجهات استخدام القوة الغاشمة لمحاولة إيقاف تشغيل بعض الخدمات عبر الإنترنت أو تعطيلها فيما يعرف بهجوم حجب الخدمات، على الجانب الأخر تنجح بعض الجهات في إقحام نفسها سرا ما بين مستخدمي الخدمة ونظام الويب وتعرف هذه التقنية باسم الرجل في المنتصف وفى غمرة ذلك يستغل منفذي الهجمات الإلكترونية الثغرات الموجودة في أنظمة الأنترنت القائمة على إدارة بعض الخدمات للدخول إليها والسيطرة على البيانات الخاصة بها من أجل التحكم فيها وتحقيق أهدافها وذلك من خلال هجمات يطلق عليها هجمات الحقن أو الهجمات دون الانتظار[4].

[1] التعرف على الهجمات الالكترونية وكيفية الدفاع ضدها، الخدمات والاستشارات، https://ibm.co/2YUxKHM
[2] استخدام المرتزقة كوسيلة لانتهاك حقوق الإنسان وإعاقة ممارسة حق الشعوب في تقرير المصير ، الأمم المتحدة الجمعية العامة ، يوليو 2020، https://bit.ly/3vgL8BJ
[3] - أنماط الحرب السيبرانية وتداعياتها على الامن العالمي، السياسة الدولية، الرابط، http://www.siyassa.org.eg/News/12072.aspx
[4] ما معنى الهجمات الالكترونية واشهر الهجمات السيبرانية، مؤسسة غائم لتقنية الحاسب الآلي ، https://bit.ly/3p7nvud

ثانيا: الهجمات السيبرانية والقانون الدولي الانساني

إن اللجوء المتزايد للدول في استخدام الفضاء الإلكتروني لشن هجمات سيبرانية في أثناء النزاعات المسلحة، 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، حينها لم يكن للهجمات السيبرانية عند إبرامها أي وجود يُذكر، ما يعني أنها لم تقنن بأحكام خاصة تنظّم استعمالها من الناحية القانونية. [5]

وعلى ضوء أحكام قانون الحرب كان تطوير وسائل وأساليب قتال جديدة متوقعا. فالمادة 36 من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف نصت على ***«يلتزم أي طرف سام متعاقد عند دراسة سلاح جديد أو تطويره أو اقتنائه أو أداة حرب أو اتباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظورا في الأحوال كافة أو في بعضها بمقتضى هذا الملحق البروتوكول أو أي قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها ذلك الطرف السامي المتعاقد»***. وبالتالي تضع هذه المادة الإطار العام المنظم لاستخدام وسائل وأساليب قتال جديدة في النزاعات المسلحة.[6]. كما تبين أحكام هذه المادة أنه على ضوء قانون الحرب، يتعين على الدول التي تقتني أسلحة حديثة أو تطورها تتبّع أسلوب قتال جديد، وأن تحدد مشروعية استعمالها. كما يفيد هذا النص ضمنيا أن كل قواعد قانون الحرب تكون قابلة للتطبيق على وسائل القتال الحديثة وأساليبها، ففي حال غياب النص الخاص يطبّق النص العام، هذا من حيث المبدأ.

ايضا استنادا إلى مبادئ القانون الدولي الإنساني، فإن شرط مارتنز هو وسيلة فعالة لمواجهة التطورات التقنية التي تعرفها وسائل القتال وأساليبه، إذ ورد لأول مرة في اتفاقية لاهاي الثانية لعام 1899 والذي ينص على: «أنه في الحالة التي لا تنطبق فيها معاهدة أو قانون عرفي، فإن المدنيين والعسكريين يتمتعون بحماية مبادئ القانون الدولي المشتقة من العرف المستقر، ومن المبادئ الإنسانية، وما يمليه الضمير العام». وقياسًا على هذا المغزى، أمكن تحريم الأسلحة البغيضة للضمير العام. [7].

<u>كما يمكن القول أن الهجمات الالكترونية كأحد الاسلحة الحديثة في الحروب ينطبق عليها عدد من المبادئ الحاكمة في القانون الدولي الانساني وخاصة</u>

- **<u>مبدأ التمييز</u>** الذي يتطلب وفق نص المادة 48 من البروتوكول الإضافي الأول لعام 1977 أن تميز أطراف النزاع المسلح في الأوقات كافة بين الأشخاص المدنيين والأعيان المدنية من جهة، والمقاتلين والأهداف العسكرية من جهة أخرى.

[5] - حسن فياض، الهجمات السيبرانية من منظور القانون الدولي الإنساني، مجلة الدفاع الوطني، 2020، الرابط، https://bit.ly/3bHUG2J
[6] - راجع المادة 36 من البروتوكول الإضافي الأول لاتفاقيات جينيف 1977، الرابط،
https://www.icrc.org/ar/doc/resources/documents/misc/5ntccf.htm
[7] - صلاح جبير البصيصي، دور محكمة العدل الدولية في تطوير مبادئ القانون الدولي الإنساني، الرابط، https://bit.ly/3xXrYIQ

- ما نصت عليه الفقرة 2 المادة 51 من البروتوكول نفسه بأنه «لا يجوز أن يكون السكان المدنيون بوصفهم هذا، وكذلك الأشخاص المدنيون محلا للهجوم وتحظر أعمال العنف أو التهديد به الرامية أساسا إلى بث الذعر في صفوف السكان المدنيين».
- ما ورد في المادة 52 من البروتوكول عينه:«لا تكون الأعيان المدنية محلا للهجوم أو لهجمات الردع»، فضلا عن المادة 55 من البروتوكول الأول أيضا الذي يحظر استخدام وسائل القتال وأساليبه التي يقصد بها أو يتوقع منها أن تسبب أضرارا بالغة واسعة الانتشار وطويلة الأمد بالبيئة الطبيعية ومن ثم تضر بصحة السكان أو بقائهم، وتحظر هجمات الردع ضد البيئة الطبيعية. كما توفر المادة 56 منه الحماية للأشغال الهندسية والمنشآت التي تضم قوى خطرة.

- ما أكدت محكمة العدل الدوليةعليه في رأيها استشاري في العام 1966 على أن القانون الدولي الإنساني يقوم على مبدأين جوهريين، **يقضي الأول** بأنه يجب على الدول ألا تجعل من المدنيين هدفا للهجوم، **أما المبدأ الثاني** فيقضي بتحريم استعمال الأسلحة التي من شأنها أن تسبب آلاما لا مبرر لها، وهذا المبدأ قد نصت عليه أيضا لائحة لاهاي المتعلقة بقوانين الحرب البرية وأعرافها لعام 1907 «على أن حق الأطراف المتحاربين في اختيار وسائل القتال وأساليبه ليس بالحق غير المحدود". وبالتالي نظرًا لإلزامية هذه القواعد نرى أنها تنطبق بالكامل على الهجمات السيبرانية. [8]

ثالثا: تأثير تصعد الهجمات الالكترونية ضد البنية التحتية للدول

ظهرت العلاقة ما بين الفضاء الإلكتروني والأمن الدولي مع التوسع في تبني الحكومات الإلكترونية من جانب العديد من الدول، واتساع نطاق مستخدمي وسائل الاتصال وتكنولوجيا المعلومات في العالم، ومن ثم تصبح قواعد البيانات القومية في حالة انكشاف خارجي، مما يعرضها لخطر التعرض لهجمات الفضاء الإلكتروني إلى جانب الدعاية والمعلومات المضللة ونشر الشائعات أو الدعوة لإعمال تحريضية أو دعم المعارضة الداخلية للنظم الحاكمة و تقديم الدعم المادي والمعنوي عبر الفضاء الإلكتروني.

ايضا أصبحت المصالح القومية التي ترتبط بالبنية التحتية الحيوية عرضة لخطر الهجوم، والتي تشمل الطاقة والاتصالات والنقل والخدمات الحكومية والتجارة الإلكترونية والمصارف والمؤسسات المالية، حيث جعل الفضاء الإلكتروني من تلك المصالح مرتبطة يبعضها البعض في بيئة عمل واحدة والتي تعرف بالبنية التحتية القومية للمعلومات وارتباطها بالبنية التحتية الكونية للمعلومات، واصبح يتعلق الامن العالمي بمدى قدرة المجتمع الدولي على اتخاذ إجراءات للحماية ضد التعرض للأعمال العدائية والاستخدام السيئ للفضاء الالكتروني. [9]

ولقد تزايدت الهجمات الإلكترونية ضد البنى التحتية الحيوية للدول بشكل كبير في السنوات الأخيرة، وهذا أسفر عن تداعيات كارثية على بعض الحقوق الاقتصادية والمدنية، إذ تعتبر البنية التحتية المفتاح الرئيسي لتطوير الخدمات في المجتمعات، وبالتالي يعني إعاقتها عن عملها تهديدا لجملة من الحقوق المرتبطة بحياة المواطنين. كما ظهرت عدد من المحددات الجديدة للأمن العالمي نتيجة عدد من المتغيرات لعل اهمها ما يتعلق بعملية تزايد ارتباط

[8] - حسن فياض، الهجمات السيبرانية من منظور القانون الدولي الإنساني، مجلة الدفاع الوطني، 2020، الرابط، https://bit.ly/3bHUG2J
[9] - الهجمات السيبرانية: أنماط وتحديات جديدة للأمن العالمي، الموسوعة الجزائرية، الرابط، https://bit.ly/2J3GFua

البنية التحتية الكونية للمعلومات بالفضاء الالكتروني بما يجعلها عرضة للهجمات الالكترونية، وبخاصة مع اتساع حركة الفاعلين في استخدامها من غير الدول.

فعلى سبيل المثال قوضت تلك الهجمات من الحق في الحصول على الرعاية الطبية والصحية إضافة إلي الحق في الحصول على خدمات المياه النظيفة والصرف الصحي فضلا عن الحصول على الكهرباء إضافة إلي تعطيل الحق في التنمية، ناهيك عن الحقوق السياسية والمدنية المرتبطة بالحصول على المعلومات. فنجد مثلا أن المستشفيات وأماكن الرعاية الطبية أصبحت أكثر الأماكن تعرضا للهجمات الإلكترونية بالآونة الأخيرة، حيث يستخدم المهاجمون برامج الفدية لاستهداف المستشفيات ومؤسسات الرعاية الصحية في جميع أنحاء أوروبا كذا بالولايات المتحدة الأمريكية نظرا لاعتمادها على شبكة الأنترنت في كل أعمالها، وتشير التقديرات إلي زيادة الهجمات الإلكترونية على المستشفيات في خضم انتشار وباء كوفيد-19. [10] فلقد شهد شهر سبتمبر 2020 أول حالة وفاة بشرية جراء هجوم الفدية فقد تسبب الهجوم في تعطل أنظمة تكنولوجيا المعلومات في مستشفى جامعة دوسلدورف الألمانية، ما تسبب في وفاة امرأة بعد أن نُقلت إلى مدينة أخرى على بعد 20 ميلا لتلقي العلاج، وبعد أن عجز المستشفى عن استقبال أي حالاتٍ طارئة. وقد أفادت بعض التقارير بأن ذلك الهجوم لم يكن يستهدف المستشفى نفسها، وإنما جامعة هاينريش هاينه(Heinrich Heine) التي كانت مخاطبة بتقديم الفدية [11]. ايضا في مايو 2017 ضرب هجومًا الإلكتروني خدمة الصحة الوطنية في إنجلترا مما أدى إلى منع الموظفين من استخدام أجهزة الكمبيوتر الخاصة بهم وإجبار بعض المستشفيات على تحويل المرضى إلي مستشفيات أخري[12].

ومع انتشار جانحة كوفيد 19 زاد استهداف الأنظمة الصحية على مستوى العالم ففي أكتوبر 2020 حذر مكتب التحقيقات الفدرالي من موجة وشيكة من الهجمات الإلكترونية على المستشفيات وسط جائحة كورونا مع إشارة بطريقة غير مباشرة إلي إمكانية تورط الحكومة الروسية بالأمر[13]، كما وصلت بعض الهجمات الإلكترونية إلي أنظمة الخدمة الصحية الأيرلندية، واستهداف هيئة الخدمات الصحية الأيرلندية وعملت على تشفير بيانات المرضى وذلك في شهر مايو 2021 ، وفى هذا الشأن أدى الهجوم إلى إصابة بعض المستشفيات بالشلل، ما أدى إلى إلغاء الخدمات الاستشارية لمرضى السرطان، وتعطيل أنظمة الأشعة والتشخيص ويطلق مرتكبو الهجوم على أنفسهم اسم كونتي لوكر[14]، وفي يونيو 2021 استهدفت برمجيات الفدية شبكة تكنولوجيا المعلومات الخاصة بالنظام الصحي في جورجيا، وهو ما اضطرهم إلى إغلاق أنظمة تكنولوجيا المعلومات للحد من الآثار المحتملة للهجوم ليتحول النظام الصحي إلى طرق التشغيل الاحتياطية، ومنها التوثيق الورقي لمدة أسبوع على الأقل منذ شن الهجوم[15].

وعلى صعيد أخر أدي الهجمات على محطات المياه والكهرباء إلي تعطل الخدمات ناهيك عن تسمم المياه في بعض الأحيان، فعلى سبيل الذكر وفى يناير 2021 حاولت أحدى الهجمات الإلكترونية تسميم محطة لمعالجة المياه

[10] Microsoft. Cyberattacks targeting health care must stop . https://bit.ly/3vf3brW November 2020

[11] - الامن السيبراني في 2020 بين الفرص والتحديات والحماية، الموسوعة الجزائرية ، 2021، الرابط، https://bit.ly/3yGFWu8

[12] Massive ransomware cyber-attack hits nearly 100 countries around the world ،theguardian،https://bit.ly/3vf4sil

[13] الـFBI تحذر من موجة وشيكة من الهجمات الإلكترونية على المستشفيات، روسيا اليوم ، أكتوبر 2020 ، https://bit.ly/3mSBVLS

[14] قراصنة يهاجمون هيئة الخدمات الصحية الأيرلندية ويطلبون 20 مليون دولار فدية، الشرق ، مايو 2021 ، https://bit.ly/2YPQY0G

[15] مخاطر متزايدة دلالات تصاعد هجمات الفدية عالمياً، مركز المستقبل للأبحاث والدراسات، يوليو 2021 ، https://bit.ly/3DJzYIE

تخدم أجزاء من منطقة خليج سان فرانسيسكو في الولايات المتحدة الأمريكية[16]، بينما فى نوفمبر 2017 أصبح وضع شبكة الكهرباء في الولايات المتحدة مثيراً للقلق بشكل متزايد بعد أن تم اختراق العديد من محطات الكهرباء بما ساهم في انقطاع الكهرباء عن المصانع وأماكن العمل والمنازل، وفى السياق ذاته انقطاع التيار الكهربائي بالكامل في أوكرانيا ما بين العامين 2015 إلي 2016 وفى أحد الهجمات أشارت التقديرات إلي قيام (فريق ساندورم) الروسي إلي اختراق محطات الكهرباء في أوكرانيا بعد الصراع على جبهة القرم وهذا ساهم في قطع لكهرباء عن كافة أنحاء البلاد وتضرر نحو ربع مليون مواطن أوكراني[17]. وفى ذات الإطار تعرضت الولايات المتحدة في 7 مايو 2021 لهجوم استهدف أحد أكبر خطوط أنابيب البنزين والسولار التي تمد الساحل الشرقي بالوقود من خلال شبكة يبلغ طولها 5500 ميل، ما أسفر عن إغلاقه وتوقفه عن العمل وهذا انعكس بالسلب على حياة المواطنين بالساحل[18]، وفى يوليو 2021 تأثرت 200 شركة أمريكية بعمليات للاختراق الإلكتروني وهذا أثر على تقديم الخدمات للمواطنين[19].

➢ التهديدات السيبرانية في المنطقة العربية

ايضا تعرضت المنطقة العربية عبر المجال السيبراني الى حروب نفسية حيث مارست قوى خارجية التدخل "سيبرنيا" للتاثير على الامن والاستقرار سواء عبر تغذية النزاعات الطائفية مثل الدور الذي تلعبة ايران في تغذية حسابات على شبكات التواصل الاجتماعي لدعم الشيعة في دور الخليج وتحريضهم سياسيا او عبر توظيف المجال السيبراني لتعزيز الرقابة والتجسس على دول المنطقة من قبل قوى اقليمية مثل اسرائيل وايران وتركيا او عبر التجسس من قوى دولية اخري[20] . حيث تعرضت بعض القطاعات الصناعية والهيئات الحكومية في المنطقة للهجوم الإلكتروني مما أثر على مستوى الخدمة العامة المقدمة للمواطنين أو يقوض من الثقة العامة للمؤسسات الحكومية، فعلى سبيل المثال تعرّضت شركة أرامكو السعودية لهجمات إلكترونية متزايدة عبر برمجيات خبيثة ويضر هذا الأمر من اقتصاد المملكة العربية السعودية وينعكس بالسلب على الحقوق الاقتصادية للمواطنين السعوديين[21].

ايضا أثر المجال السيبراني كذلك على العلاقات البينية بين الدول العربية حيث شهدت العلاقة بين قطر وجيرانها توترا اثر تصريحات نسبت الى امير قطر وادعاء قطر بان موقع وكالة الابناء القطرية تم اختراقة في مايو 2017 وهو ما كان من شأنه بأن اتهمت قطر الامارات بالوقوف خلف القرصنة بينما نفت الاخيرة تلك ألاتهامات. واتجاه قطر لتعزيز امنها الالكتروني بالتعاون مع امريكا وتركيا ، وكان لتلك الازمة انعكاس في تطور الازمة بين قطر ودول الرباعي العربي وهي مصر والسعودية والامارات والبحرين بفرض مقاطعة،وكان من ضمن آلياتها حجب المواقع الالكترونية الممولة والموجهة من قبل قطر والداعمة للارهاب.

وشهدت المنطقة العربية ايضا ما يعرف بنمو ظاهرة الجيوش الالكترونية والتي لا تعني ان لها اية ابعاد عسكرية بل انها عبارة عن كتائب تحاول التأثير المتبادل في الاخر عبر توظيف الفضاء السيبراني في الصراع بين الفاعلين .الى

[16] مركز استخباراتي: قرصان يحاول تسميم مياه الشرب إلكترونيا في أمريكا، الوطن ، يونيو 2021 ، https://bit.ly/3lM6jIL
[17] القرصنة الإلكترونية تهدد شبكات الكهرباء العالمية، الروية، نوفمبر 2017 ، https://bit.ly/3BRo9PW
[18] مخاطر متزايدة دلالات تصاعد هجمات الفدية عالمياً مرجع سابق ذكره
[19] تقرير هجوم إلكتروني روسي يخترق أكثر من 200 شركة أمريكية، الدستور ، يوليو 2021 ، https://bit.ly/3DM0ilj
[20] - الامن السيبراني في 2020 بين الفرص والتحديات والحماية، الموسوعة الجزائرية ، 2021، الرابط، https://bit.ly/3yGFWu8
[21] رويترز أرامكو" تتعرَّض لهجمات إلكترونية متزايدة عبر برمجيات خبيثة، الشرق ، فبراير 2020 ، https://bit.ly/3DOrEqW

جانب تزايد تعرض المنطقة الى الهجمات والقرصنة الالكترونية وبخاصة في الخليج العربي وهو الامر الذي دفع تلك الدول الى زيادة الانفاق و الاستثمار في الامن السيبراني وبتشكيل هيئات وطنية للامن السيبراني مثل قيام السعودية في شهر نوفمبر 2017 ناهيك عن وجود المركز الاقليمي للامن السيبراني في سلطنة عمان بدعم من الاتحاد الدولي للاتصالات[22]. كما شهد عام 2020 تزايد استهداف دول الشرق الأوسط :فقد استهدفت برمجية طلب الفدية ثانوس (Thanos)مؤسساتٍ حكومية عدة في منطقة الشرق الأوسط وشمال إفريقيا في شهر يوليو 2020، في مثال بارز على توظيف أدوات مسح البيانات في شن هجمات سيبرانية غامضة. كما استخدم القراصنة المعروفون باسم (MoleRAT)رسائل التصيد الاحتيالي ذات الصلة بالشرق الأوسط للتجسس على عدد من المسؤولين الحكوميين البارزين في الأراضي الفلسطينية والإمارات وتركيا[23]. .

ولقد قدرت تقارير دولية أنه من المتوقع أن تصل تكلفة الخسائر المرافقة للهجمات السيبرانية على البنى التحتية إلى ما يصل لـ 265 مليار دولار بحلول عام 2031. وخاصة في ظل ارتفاع معدل هجمات برامج الفدية الرئيسية والهجمات الالكترونية الخبيثة التي تحدث تغييرات عدة في التكنولوجيا التشغيلية تحتاج هذه الصناعة إلى إيجاد حلول آمنة من الفشل للحفاظ على الإنتاجية العالية لهذه البنى بشكل آمن و فعال. وقد زادت تعقيدات الهجمات وأصبحت أكثر شراسة، كما أصبحت طلبات برامج الفدية الآن خيالية فمن المتوقع أن تتجاوز تكلفة برامج الفدية كمحصلة لعمليات الرضوخ و الدفع. [24]

- **التهديدات السيبرانية في ظل الجائحة**

ايضا جسد المشهد العالمي لتفشي فيروس كورونا (كوفيد-19) هشاشة النظام الاقتصادي العالمي وضعف البنى التحتية لمرافق ومؤسسات الأنظمة الصحية عبر مختلف دول العالم، فضلا عن ضعف الاستجابة السريعة لمكافحة ذلك الكوفيد والعجز عن منع تفشيه وانتشاره، الأمر الذي كان له تداعياته الخطيرة وآثاره المدمرة على الاقتصاد العالمي والأمن القومي الاقتصادي والصحي للدول. فكان لـ(كوفيد-19) تأثيره الخطير على الظاهرة الإجرامية من خلال انحسار بعض الجرائم التقليدية وزيادة كبيرة في معدل ارتكاب الجرائم السيبرانية خاصة جرائم الإرهاب السيبراني على مراكز البنى التحتية للدول والمؤسسات والمرافق وخاصة الصحية منها.

حيث تزايد ارتكاب الجرائم السيبرانية في فترة تفشي كوفيد -19 وتطور وسائل ارتكابها نتيجة سياسة الإغلاق العالمي والتحول إلى نظام العمل عن بُعد، الذي فرض استخدام الاختصارات الأمنية مع إشراف أقل وضوابط تقنية أقل والعديد من نقاط الضعف في منظومة الأمن السيبراني يستغلها المجرم السيبراني لتكثيف هجماته على مختلف المواقع، بنى تحتية أو شركات أو مواقع لأفراد. وذلك بغرض التجسس السيبراني الاقتصادي لسرقة بيانات لقاح (كوفيد-19) من قبل بعض الدول أو المنظمات، والتي يمكن أن تشمل البيانات المتعلقة بمقترحات البحث، وتطوير الأدوية، والمخطوطات، واختبار الفيروسات، والتجارب السريرية، وتصنيع الأدوية، والتي تقدر بالمليارات من

[22] - الهجمات السيبرانية: أنماط وتحديات جديدة للأمن العالمي، الموسوعة الجزائرية، الرابط، https://bit.ly/2J3GFua
[23] - الامن السيبراني في 2020 بين الفرص والتحديات والحماية، الموسوعة الجزائرية ، 2021، الرابط، https://bit.ly/3yGFWu8
[24] - 265 مليار دولار خسائر البنى التحتية جراء الهجمات السيبرانية، بوابة اخبار اليوم ، 31 اغسطس 2021، الرابط، https://bit.ly/3bPe9ie

الدولارات لقيمتها العلمية ولحقوق ملكيتها الفكرية، خاصة مع تزايد الاستثمارات العالمية في القطاع الصحي، الأمر الذي أضر بالاقتصاد العالمي والأمن القومي الاقتصادي للدول.[25]

وبالتالي وطبقا لما ذكر أعلاه تؤثر الهجمات الإلكترونية على جملة من الحقوق الاقتصادية والاجتماعية ويعتبر أبرزها الحق في حصول المواطنين على الخدمة العامة من خلال الدولة، هذا بالإضافة إلي الحق في الرعاية الصحية والحصول على الخدمات المائية النظيفة والرعاية الصحية، الجدير بالذكر أن كل هذه الحقوق مصانه بموجب مواد العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية[26].

- **الهجمات السيبرانية والفضاء المدني وحقوق الانسان**

تواجه منظمات حقوق الإنسان والمجتمع المدني بالإضافة إلى النشطاء الحقوقيين مجموعة متزايدة من الهجمات الإلكترونية من هجمات للتصيد الإلكتروني وهجمات لرفض الخدمة وذلك بهدف ممارسة الانتقام منهم بسبب أعمالهم الحقوقية أو إجبارهم على السكوت عن الانتهاكات الحقوقية المختلفة، وهذا يضر جملة من الحقوق المدنية والسياسية المنصوص عليها في العهد الدولي الخاص بالحقوق السياسية والمدنية والتي من بينها الحق في تكوين الجمعيات المنصوص عليه في المادة 22 من العهد سابق الذكر، هذا بالإضافة إلي الاعتداء على الحق في الخصوصية وحرية الرأي والتعبير.

وفى هذا الصدد تعرض الموقع الإلكتروني لمنظمة الشبكة السورية لحقوق الإنسان في أكتوبر 2021 لهجمات إلكترونية مجهولة المصدر ما أدى لتوقفه عن العمل لعدة ساعات ويعتبر هذا الأمر استمرار لسياسات التخوين والعنصرية التي تواجها المنظمة التي توثق انتهاكات حقوق الإنسان في سوريا من كافة الفئات، الجدير بالذكر أن بعض التقديرات تشير إلي تورط مجموعات تابعة للحكومة الروسية في هذا الأمر[27]، و في 17 يونيو 2019 تم إجراء عدد من المحاولات لاختراق حسابات وسائل التواصل الاجتماعي والبريد الإلكتروني لمنظمة حقوق الإنسان PROMEDEHUM[28] وهي منظمة مجتمع مدني بارزة في فنزويلا.

وفى العام 2018 ومع بداية الانتخابات الرئاسية في أذربيجان قامت الحكومة بمساعدة مجموعات تابعة لها بتقويض عمل منظمات المجتمع المدني المعارضة لها على الأنترنت عبر سلسلة من الهجمات الإلكترونية، إذ تعرضت بعض مواقع المنظمات الحقوقية إلي هجمات الحرمان المباشر للخدمة ليس هذا فحسب بل تعرضت بعض المواقع الإعلامية المعارضة إلي الاختراق الإلكتروني وإزالة كافة المعلومات المتاحة عليها، كما تم اختراق الحساب الشخصي على الفيس بوك للمعارض الحقوقي الأذربيجاني جميل حسنلي مع حذف كافة متابعيه[29]،وفي فيتنام خضعت منظمات المجتمع المدني والنشطاء لعمليات استحواذ على الحسابات الإلكترونية الخاصة بهم، وذلك من خلال استخدام

[25] - الجرائم السيبرانية في زمن كورونا واثارها على الامن القومي الاقتصادي، الرابط، https://bit.ly/3urMBFZ
[26] لعهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية، مكتبة منسونا ، http://bit.ly/3aI7gKs
[27] الشبكة السورية لحقوق الإنسان تتعرض لهجمات إلكترونية، شبكة أرام الإعلامية ، https://bit.ly/3n1oI3r
[28] https://bit.ly/30mnKan. Frontlinedefenders. CYBER ATTACKS AGAINST HUMAN RIGHTS ORGANISATION PROMEDEHUM
[29] https://bit.ly/3BPHyAP،February 2018،meydan، Azerbaijan's authoritarianism goes digital

هجمات الإلكترونية معتمدة على رواب مزيفة و محملة بالبرامج الضارة والتي تنتهك الأمان الرقمي لمستخدم الإنترنت للوصول إلى معلومات حساباتهم الخاصة[30].

بناءا عليه يمكن القول أن متطلبات توافر الأمن الإلكتروني الدولي ضد الهجمات والتهديدات السيبرانية تتمثل في التأكد من سلامة الدفاعات الإلكترونية، وعدم تعرضها لأي خلل فني طارئ، وألا تعالج هذه المسألة منفصلة عن غيرها وإنما ضمن ترسانة شاملة للدفاع تشكل إطارا رادعا لأي حرب استباقية، وهو ما يفرض على المجتمع الدولي التركيز على العلاقة بين الأمن الإلكتروني وبقضايا التنمية الاقتصادية والاجتماعية والاستقرار السياسي، وصياغة إستراتيجية دولية لمواجهة تصاعد الأخطار الإلكترونية ، وأهمية تعاون كافة الفاعلين في مجتمع المعلومات العالمي لترسيخ ثقافة عالمية لأمن الفضاء الإلكتروني،وأهمية الموازنة بين اعتبارات الأمن وحرية استخدام الفضاء الإلكتروني وما بين الاحتكار العالمي للتكنولوجيا والعمل على انتقالها في دول العالم.

من ثم تؤكد **مؤسسة ماعت للسلام والتنمية وحقوق الانسان** أنه لا يمكن لأي دولة أو مؤسسة على مستوى العالم أن تحقق الأمن السيبراني بنسبة 100%، لأننا في عالم صراع التقنيات فلم يعد من الملائم القول بأن تقنية اليوم يمكن اختراقها بتقنية الغد، بل سادت حقيقة أن العالم في كل ثانية في تقنية جديدة، تخترق وتقوض ما سبقها من تقنيات، ولكن يمكن تقليل مخاطر التهديد والهجمات السيبرانية بشكل كبير إلى المستوى الذي يسمح بالاستمرار في الاستفادة من الفرص الهائلة التي توفرها التكنولوجيا الرقمية. كما اظهرت ايضا جائحة كورونا أنه على جميع دول العالم أن تدرك وحدة المصير المشترك على هذا الكوكب، وأنها لن تنجو بمفردها في ظل فرض سياسة العزلة والفردية وضعف الشراكات العالمية، وأنه لا سبيل أمامها لحل تلك الأزمات والجوائح سوى أنويلتقي الجميع حول مائدة المفاوضات المستديرة، لتسريع الخروج من الأزمة لتعزيز التعاون الدولي وإعادة ضبط الشراكات العالمية، لتسهل التعافي وإعادة بناء النظم الاجتماعية والاقتصادية والصحية بطرق شاملة ومستدامة وتساعد في الاستعداد للمخاطر والأوبئة في المستقبل وبما يحقق مصلحة جميع الدول.

كما تؤكد المؤسسة أن إبرام الاتفاقية في هذا الشأن في المستقبل سيعني تحريك المسؤولية الجنائية الفردية عن دعم أي مجموعات مسلحة يمكن أن تستخدم الوسائل الإلكترونية للأغراض غير العسكرية تجاه دول أخرى أو تدريبها أو تمويلها وبالتالي يجب على الدول الوصول إلى حل وسط من أجل اتخاذ مثل هذه التدابير لحماية وصولها الآمن إلى الفضاء السيبراني والخدمات التي يمنحها.

[30] Ccessnow . Vietnam under review at the Human Rights Council: Cyber attacks on civil society a key concern. https://bit.ly/3FLBv2C

ومن ثم توصي بـــــــــــ

1- أهمية الحاجة إلى فتح الطريق أمام التعاون المثمر بين الحكومات والأفراد والشركات العاملة في تكنولوجيا الاتصال والمعلومات لكي يتم تعزيز دور الفضاء الإلكتروني في النمو الاقتصادي وتحسين حياة المواطنين وحرية الرأي والتعبير وتعزيز التسامح بين الثقافات ،

2- الحاجة إلى بذل جهود دولية عاجلة ومتكاتفة لمواجهة تهديدات أمن الفضاء الإلكتروني بإمكانية العمل على حل الصراعات على أرض الواقع لمنع انتقالها إليه.

3- العمل على توافق القوانين المتعلقة بالصراع الإلكتروني مع القانون الدولي وأهمية المبادرات الدولية لحماية الفضاء الإلكتروني فضلا عن البحث والتطوير في مجال الدفاعات ضد الأخطار الإلكترونية وتعزيز أشكال التعاون الدولي في سبيل مكافحتها من أجل تعزيز أمن الفضاء الإلكتروني باعتباره مرفقا دوليا وتراثا مشتركا للإنسانية.

4- ضرورة اتخاذ تدابير جديدة بشأن مراجعة دورية للأمن السيبراني للبعد الدولي المرتبط بأصول التشفير، فالأصول المشفرة بطبيعتها عابرة للحدود في تطبيقاتها وبنيتها التحتية، فضلاً عن سرعة تطور تلك الأصول المشفرة وتعقيدها،

5- يجب أن يكون هناك تقييم مستمر للتشريعات الصادرة للتحقق من إمكانية تطبيقها بشكل فعال على هذا النوع من الأصول أو كونها بحاجة إلى تعديلات أو إرشادات.

6- يجب اتخاذ تدابير لتعزيز قدرة أجهزة العدالة الجنائية في التحقيقات الرقمية، والتأكد من أن لديهم الأدوات والتقنيات والمهارات المناسبة والذكاء الاصطناعي والبيانات الضخمة والحوسبة عالية الأداء في السياسة الأمنية، كل ذلك يمثل أولية جوهرية لتحقيق الأمن السيبراني، ومن ثم مكافحة الجرائم السيبرانية.

7- ضرورة الاستثمار في مجال الأمن السيبراني وعقد شراكات دولية مع الدول الرائدة والمتطورة في هذا المجال لمشاركة معلومات التهديد السيبراني لتحديد معالم التطور العالمي للفضاء السيبراني ولإنشاء مراكز جديدة للابتكار السيبراني لإيجاد نظام كامل لحماية الأمن السيبراني ولرفع القدرة على مكافحة الجرائم السيبرانية.

8- لابد أن تعمل الدول على زيادة الإنفاق على تنمية القدرات في مجال الدفاع السيبراني، وتخصيص موارد في الميزانية العامة للدولة، أو في ميزانيتها المعنية بالأمن والدفاع، إلى جانب تشكيل مجالس تُعنى بوضع السياسات المتعلقة بالأمن السيبراني بوصفه رافدًا من روافد الأمن القومي .