كلية الحقوق والعلوم السياسية والإدارية
الفرع الثاني

الإطار القانوني للهجمات الإلكترونية في الحرب السيبرانية

رسالة لنيل دبلوم الدراسات العليا في القانون الجزائي

إعداد
ماريا كركي

المقدمة :

نتيجة الخسائر المادية والبشرية الفادحة التي خلفتهما الحربين العالميتين، بدأت الدول بتقييم الأساليب والأسلحة والأدوات التي استخدمتها في النزاعات والحروب التقليدية التي شاركت فيها والسعي الى تبني مفهوم جديد للحروب كبديل عن الحرب التقليدية، وذلك عن طريق محاولة تطوير أسلحة متطورة من أجل الحدّ من الخسائر التي يمكن أن تلحق بها في النزاعات المستقبلية، والتوصل الى تحقيق أهدافها المرجوّة دون تعريض جيشها وأرضها الى أي مخاطر او خسائر يمكن ان تلحق بهم، وتوصلت بالفعل الى هذا الهدف في العقد الأخير، حيث انخفضت نسبة إستخدام الدول للأسلحة الحركية التقليدية، بفضل ظهور أسلحة غير تقليدية فريدة من نوعها تسمح لها بتحقيق مزايا عسكرية على الخصوم دون تحمل المخاطر التي كانت تتحملها في السابق، وذلك بفضل الإستغلال السيئ للتكنولوجيا الذي يتمثل الجانب السلبي منه بإضعاف الخصوصية وظهور جرائم جديدة متعلقة بالحاسب الآلي والإنترنت، هذه الأسلحة تسمح بإستهداف المرافق الحيوية والبنى التحتية للخصم وإحداث أضرار جسيمة بالأرواح والأعيان العسكرية والمدنية دون حتى اللجوء الى أي اشتباك مادي، مما جعل من الفضاء السيبراني ساحة فعلية لخوض معركة غير محسوسة أو حركية ولا تتطلب اي تكلفة أو قوات عسكرية أو أسلحة مادية تقليدية برية كانت أم بحرية أم جوية، بل كل ما نحن بحاجة اليه لإخضاع الطرف الآخر هو حاسوب متصل بالإنترنت أو حتى هاتف محمول من أجل التأثير على موازين القوّة لدى الخصم كالسيطرة على محطات الطاقة النووية أو محطات الكهرباء والبنى التحتية المدنية والعسكرية للخصم والحصول على المعلومات السرية الخاصة به من أجل تحقيق مزايا عسكرية أو سياسية أو أمنية، فكافة هذه الأهداف السابقة تتحقق من خلال " الحرب السيبرانية (CyberWarfare) والهجمات السيبرانية (CyberAttacks)" اللذان يساهمان في إلغاء الحدود بين الدول وتشكيل ساحة جديدة للصراع الدولي سواء كنا في زمن السلم أم الحرب، مما جعل من هذه الهجمات مصدر تهديد فعلي للأمن القومي للدول وللمؤسسات والمنشآت العامة والخاصة، والأفراد.

هذا التطور الهائل في مجال التكنولوجيا والمعلومات والاتصالات دفع بالمجرمين الى إستغلال شبكة الإنترنت من أجل تسهيل أعمالهم الإجرامية والتواصل بين بعضهم البعض، وإستهداف الضحية بأسهل طريقة ممكنة، مما أدى الى ظهور نوع جديد من المجرمين وهو المجرم المعلوماتي الذي يختلف في تكوينه وأهدافه وأساليبه عن المجرم التقليدي وأكثر منه ذكاءً و دهاءً.

أطلق على الحرب السيبرانية إسم "حرب الجيل الرابع" أو "الحرب اللاتماثلية Asymmetric Warfare" التي تتوافر فيها أحدث أنواع الاسلحة الفريدة من نوعها، التي تلزم الجندي ليس فقط بحمل السلاح وإنما التمتع بمهارات وإمتيازات إلكترونية من أجل التصدي الى الهجوم الموجه ضده، فقد إعتبر Richard Clarke أن الحرب السيبرانية هي مجموعة الإجراءات المتخذة من قبل الدولة لإختراق أجهزة الكمبيوتر الخاصة بالعدو، وأن من يتولى الحرب هنا ليس قائداً عسكرياً وإنما أشخاص ذو كفاءة عالية يعتمدون على تكنولوجيا المعلومات من أجل إلحاق الأضرار بالطرف الآخر، وهذه الحرب تتضمن : الهجوم السيبراني(السيطرة على معلومات الخصم وإلحاق الأضرار به)، الحماية الإلكترونية Electronic Defense Operation(الإجراءات الوقائية للتصدي للهجوم) والدعم الإلكتروني Electronic Support Operation(هي عملية مكملة لعمليتي الهجوم والدفاع)، سوف نكتفي في بحثنا الحالي الى التطرق الى الهجمات السيبرانية التي تتصدر قائمة الإستراتجيات في الحرب السيبرانية، من خلال تتضمن إستراتجية

عسكرة التكنولوجيا Technology Militarization Strategy لهذه الهجمات، بمعنى آخر أن الهجمات هي جزء أساسي في الحرب السيبرانية.

حداثة الهجمات السيبرانية وطبيعتها الخاصة والغامضة دفعت بالمجتمع الدولي الى البحث والتحليل في كافة معطياتها الغير مفهومة وكيفية الحدّ من آثارها الخطيرة، خاصةً أن هذه الجرائم ترتكب بكبسة زر، فالمهاجم(CyberActor) يستطيع تدمير وإتلاف النظم المعلوماتية للطرف الآخر دون أي مجهود يذكر وأيضاً التسلل اليها وإختراقها والسيطرة عليها وإلحاق الأضرار بها عن طريق الحصول على معلومات الطرف الآخر العسكرية والإقتصادية، المالية وحتى الشخصية، مما وضع القانون الدولي الإنساني أمام إختبار حقيقي وجدّي حول كيفية التصّدي لها والحدّ من سلبياتها الخطيرة، وخاصةً أن هذا القانون يفتقر الى نصوص تنظمها، كونها في الأصل جديدة على الساحة الدولية من جهة، ولقلة الأبحاث والإتفاقيات والإجتهادات القضائية والفقهية الدولية بشأنها من جهة أخرى، مما يستدعي التحرك لمواجهة هذه التهديدات السيبرانية في ظل صعوبات وتعقيدات كثيرة ومخاوف إنسانية واضحة حول المخاطر التي يمكن أن تلحقها بالدول والأفراد، خاصةً في حال إرتقت هذه الهجمات الى مستوى النزاع المسلح، والتي تؤدي في حال حصولها الى نتائج كارثية (كالتصادم بين الطائرات والقطارات والتعرض للأنظمة الخاصة بالمستشفيات وشبكات المياه والطاقة..الخ)، تفوق الآثار الناجمة عن أسلحة الدمار الشامل في بعض الأحيان، مما يؤدي الى تداعيات خطيرة على المجتمع الدولي ككل.

هذه التحديات لم يألفها المجتمع المحلي والدولي في السابق، فوقفت الدول مكتوفة الأيدي حائرةً حول الأساليب والمعطيات التي يمكن تبنيها لمحاربة الجرائم الناتجة عن التطورات التكنولوجية، وكيفية توفير الحماية القانونية اللاّزمة للدول والأفراد في ظل الصفة العابرة للحدود لهذه الهجمات، بمعنى آخر أسقطت الحدود الجغرافية بين الدول ووضعت السيادة الوطنية على المحك، فالعالم لم يعرف من قبل إنترنت الأشياء(IOT-Internet Of Things) والحواجز المتسلسلة والتهديدات السيبرانية المستحدثة التي سرعَت في تكوين ما يسمى بالجرائم السيبرانية التي تنفذ غالباً في الفضاء السيبراني، ومن بينها الهجمات السيبرانية.

أهمية البحث :

تعتبر الهجمات السيبرانية في العصر الراهن من أخطر وأهم التحديات الدولية التي تفرض على الدول ضرورة بذل جهود استثنائية في إطار تعزيز التعاون بينها من كافة النواحي القانونية والتقنية والقضائية والفنية، بغية تنظيمها والحدّ من مخاطرها وآثارها الخطيرة، محاولين التوصل الى حلول تنظمية دولية في إطار الهجمات السيبرانية ووضع إطار قانوني ناظم لها والعقوبات المناسبة عن طريق تكييف هذه الهجمات ضمن قواعد القانون الدولي، مع الإعتراف للدولة المعتدى عليها بحقوق التصدي للإعتداءات السيبرانية التي من الممكن أن تتعرض لها ضمن قيود معينة، مع التشديد على ضرورة توفيرالحماية المدنيين والأعيان المحمية من ويلات الهجمات السيبرانية في حال إرتقائها الى مستوى النزاع المسلح بالإضافة الى مساعدة بعض الدول على تطوير قدراتها المحلية المحدودة (خاصةً الدول النامية) بهدف تسلحها سيبرنياً وتقنياً، كي تستطيع مواجهة هذه المستجدات الطارئة.

أما على الصعيد المحلي لا بدّ من إلقاء الضوء على الأدوار والجهود التي تقوم بها كل من الدولة والقطاع الخاص والمجتمع المدني في السعي الى مواجهة الهجمات السيبرانية عبر نشر الثقافة والوعي السيبراني،

كلٌ منهم وفق قدراته المادية والفنية والتقنية التي يمتلكها مع التشديد على ضرورة بذل المزيد من الجهود المحلية بغية تأمين سلامة المعلومات في الفضاء السيبراني .

منهجية البحث :

سوف نعتمد على عدة مناهج نظراً للأبعاد المهمة التي يحملها الموضوع كالتالي :

في البدء سوف نلجأ الى المنهج الموضوعي من أجل البحث في موضوع الهجمات السيبرانية دون تحيز الى الإتجاهات والآراء الأخرى، سوف نلجأ أيضاً الى كل من المنهج الإستقرائي(التأصيلي) من أجل تحليل كافة التفاصيل المتعلقة بموضوعنا هذا وصولاً الى تكونين حقائق ونتائج عامة، والمنهج التحليلي (الإستنباطي) من أجل تطبيق القواعد العامة على الحالات الفردية.

إشكالية البحث :

إن عدداً من التساؤلات سوف تثار لدى تحليلنا وبحثنا في موضوع الدراسة الحالي :

- ما هي الهجمات السيبرانية ؟ كيف نشأت ؟ وما هي أبرز خصائصها ؟

- هل يمكن تكييف الهجمات السيبرانية ضمن أحكام القانون الدولي الإنساني والقواعد الدولية والعرفية ذات صلة بسير العمليات العدائية ؟ وما هي القيود والشروط المتوافرة في هذا الإطار ؟

- الى أي مدى تُسأل الدولة المعتدية جنائياً ومدنياً عن الإنتهاكات الفاضحة للأحكام القانون الدولي الإنساني؟ وما هي الحقوق الدولية المعترف بها للدولة المعتدى عليها سيبرانياً للدفاع عن نفسها بوجه الدولة المعتدية ؟

- كيف تتم محاسبة المشارك المباشر دولياً ووطنياً عن مخالفته للإلتزامات المفروضة عليه عند مشاركته المباشرة في الهجوم السيبراني ؟

- الى أي مدى تعتبر السبل والجهود الدولية القانونية والتقنية المبذولة كافية من أجل الحّد من الهجمات السيبرانية ؟ وما هي الحلول المنتجة التي تساهم بنظرنا في الحفاظ على السلم والأمن الدوليين ؟

- ما مدى فعالية الدور الذي يقوم به المشّرع الوطني في هذا المجال ؟ وما هي الصعوبات والعراقيل القانونية والقضائية والفنية التي تعترض الأهداف الأساسية التي يسعى اليها ؟ ومن هي الجهات التي يستعين بها كداعم أساسي لا غنى عنها لمكافحة الهجمات السيبرانية؟

خطة البحث :

كافة الأسباب السابق ذكرها أعلاه، دفعتنا الى إختيار موضوع الدراسة الحالي وتقسيم بحثنا الى قسمين : القسم الأول يتناول مفهوم الهجمات السيبرانية والقسم الثاني نحو اتحاد دولي للتعامل مع الهجمات الإلكترونية وتأمين الفضاء السيبراني.

سوف نقسم القسم الأول الى بابين، في الباب الأول سوف نتناول ماهية الهجمات السيبرانية، أما في الباب الثاني سوف نناقش المسؤولية عن الهجمات السيبرانية من منظار القانون الدولية، كذلك الأمر بالنسبة الى

القسم الثاني، ففي الباب الأول منه سوف نعالج الإطار القانوني والتقني للإستخدام السليم للمعلومات وفي الباب الثاني دور المشرّع الوطني في مكافحة الهجمات الإلكترونية.

القسم الاول : مفهوم الهجمات السيبرانية

قديماً كان النظام التقليدي يعتمد على القوة العسكرية لمواجهة الدول أو احتلالها والسيطرة عليها وإخضاعها بالقوة لنهب ثرواتها الطبيعة وتسخير مواطنيها لمصلحتها الذاتية، هذا الهجوم كان يكلف الدولة الكثير من الخسائر المادية والبشرية فضلاً عن الوقت والجهد، وذلك بهدف التأثيرعلى قرارات الدولة المعادية من الناحيتين المادية والمعنوية وإستنزاف طاقاتها، فالفوز في الحرب لم يعد يعتمد في عصرنا الحالي على من يمتلك السلاح الأقوى أو من يستطيع ان يشل النظام الاقتصادي والمالي والمصرفي للطرف اللآخر بل وبكبسة زر واحدة أصبح المهاجم يستطيع ان يكبد دولة بأكملها خسائر بشرية ومادية تفوق ميزانيات أكبر الدول، فالحقيقة التي لا يمكن إنكارها أننا نعيش في ظل عصر إستثنائي تحكمه شبكة الإنترنت في كافة إتجاهاته، فالتطور السريع في وسائل الاتصال وتقنية المعلومات أدى الى ظهور أنماط جديدة من الجرائم عن طريق سوء إستغلال التكنولوجيا، فظهرت الجرائم التي تهدف الى إختراق المعلومات السرية المتعلقة إما بقطاع عام ام عسكري ام اقتصادي والإحتيال الإلكتروني والتجسس الإلكتروني والجرائم المنظمة والهجمات الالكترونية وغيرها من الجرائم التي تتم في الفضاء الإلكتروني .

فالنظام المعلوماتي الآني أصبح يحتل مكانة عالمية كبرى لم يسبق لها مثيل وبعد أن كانت الدولة بحاجة الى شن حرب على دولة أخرى من أجل الحصول على مواردها او التأثير على نظامها الإقتصادي والعسكري والثقافي أصبحت الحروب تتم من وراء شاشة الحاسوب وبالتالي لم يعد مفهوم القوة مرتبط بحجم الجيوش وطبيعة موارد الدولة المعتدى عليها بل بالتقنيات و الوسائل الالكترونية المتطورة و على هذا الأساس تصنف الدول المتقدمة التي تمتلك الجيوش الإلكترونية، فمجرمي اليوم هم من يتمتعون بدهاء وذكاء إلكتروني لم يسبق له مثيل ومختلف عن المجرمون التقليديون، فهم قادرون على إرتكاب جرائم تحتاج الى كثير من التفكير والتخطيط والتحضير فضلاً عن دراية أساسية بالتكنولوجيا وما تتطلبه الجرائم الالكترونية من مقدرة وكفاءة ومكر في تنفيذها لدرجة أنه أطلق على جرائمهم : جرائم الأذكياء.

اعتبرت الهجمات السيبرانية المعضلة المهمة الظاهرة في الفضاء السيبراني التي تفرض ضرورة إيجاد حل قانوني لها نظراً لمخاطرها وآثارها الجسيمة ولكن إختلفت الآراء الفقهية والتحليلات القانونية بغية الوصول الى تعريف قانوني موحّد للهجمات السيبرانية.

الباب الأول : ماهية الهجمات السيبرانية

أدى الاعتماد المتزايد على شبكة الإنترنت في كافة الامورالإقتصادية والعسكرية والأمنية والثقافية الى ظهور جرائم وتهديدات جديدة لم تكن في الحسبان في التعامل الدولي، فإنتقلت ساحة المعركة من الحيز المادي الى الحيز الافتراضي، الذي يعتبر أرضاً خصباً للمواجهة بين الدول دون المخاطرة والدخول في حرب عسكرية مادية، بعد أن كانت النزاعات المسلحة تتم على الأرض أو الجو أو البحر أصبحت بفضل كل هذه التقنيات تتم بأسلوب إلكتروني، وأصبح الاعتماد العالمي على التكنولوجيا الرقمية أساسي وأصبحت الهجمات السيبرانية إحدى الأساليب الضرورية لإلحاق الضرر بالخصم دون ان يتطلب أي وقت او جهد، يمكن للدولة أن تشل نظام مصرفي أو امني أو عسكري لدولة أخرى دون أن تدخل في حرب حقيقة مع هذه الأخيرة، بمعنى آخر أصبحت الحرب الإفتراضية بديل عن الحرب المادية في العقد الاخير، فهذه الجرائم

المستحدثة دفعتنا الى إختيار الهجمات السيبرانية موضوع الدراسة الحالي من أجل وضع النقاط على الحروف في مسألة تعتبر من أهم وأصعب التهديدات التي تواجه الدول في العصر الحالي، فسوف نسعى في هذا الباب إزالة الإلتباس عن مفهوم الهجمات السيبرانية في الفصل الأول، موضحين الخصائص التي تميز الهجمات السيبرانية وخاصةً تحديد ماهية المعلومات التي يستهدفها هذا الهجوم وطبيعتها القانونية بالإضافة الى إلقاء الضوء على صفات المجرم المعلوماتي في الفصل الثاني.

الفصل الاول : خصائص الهجمات السبرانية

كثرت التعريفات التي عالجت مفهوم الهجمات السيبرانية كونها من الجرائم الجديدة التي ظهرت في الفضاء السيبراني وأصبحت تحتل مركز أساسي في النظام الدولي المعاصر نظراً الى خصائصها المتميزة التي تمكن الدول والأفراد على حدٍّ سواء من توجيه هجمات ضد أهداف معينة ضمن مسافات بعيدة جداً، فتعتبر الهجمات السيبرانية من المواضيع الحديثة على الساحة الدولية التي لا تزال دون أي تنظيم قانوني لها، فلا يزال الفقهاء والخبراء القانونيون يحاولون البحث في إطارها من أجل الكشف عن كافة جوانبها الغامضة وأثارها ونتائجها السلبية وكيفية الحدّ منهم، لذلك لا نجد تعريف واضح لها نستطيع الإستناد عليه في أبحاثنا بل مجموعة من المحاولات الغير منتجة، لذلك سوف نحاول في هذا الفصل التوصل الى مجموعة من النتائج التي تساعد في وضع إطار قانوني واضح للهجمات السيبرانية من خلال تعريف متكامل وشامل لكافة جوانبها مع تبيان الفروقات التي تتميز بها عن غيرها من الجرائم السيبرانية المشابهة لها (المبحث الأول)بالإضافة الى نشأة هذه الهجمات مع أمثلة عنها(المبحث الثاني).

المبحث الأول : التكييف القانوني للهجمات السيبرانية

في المبحث الحالي سوف نحاول تحديد الإطار القانوني للهجمات السيبرانية عبر إلقاء الضوء على التعاريف الفقهية والقانونية المختلفة لغةً وإصطلاحاً في الفرع الأول، وتوضيح أبرز صفات المجرم المعلوماتي في الفرع الثاني.

الفرع الأول : السيبرانية لغةً وإصطلاحاً

لا بدّ أن نشير في البدء أن التنظيم الدولي يفتقر قانونياً الى أي تعريف موحد معترف به ومتفق عليه في موضوع الهجمات السيبرانية، لذلك سوف نحاول قدر المستطاع في هذا الفرع توضيح هذا المفهوم والسعي الى التوصل الى تعريف جديد يعالج كافة الجوانب الغامضة التي تكتنفه.

- مفهوم السيبرانية في اللغة :

ان كلمة سايبر تشتق من الكلمة اليونانية(kybernetes) التي تعني القيادة والتحكم عن بعد وقد إستخدم هذا المصطلح لأول مرة باللغة الانكليزية من قبل عالم الرياضيات (Norbert wiener) في كتابه بعنوان (cybernetics :or, control and communication in the animal and the machine) الصادر عام ١٩٤٨ وهو علم الدراسة والتحكم بالآليات في الأنظمة الحيوانية، البشرية

والحاسوبية[1]، عند الاطلاع على القواميس العربية نجد ان قاموس المورد عرف كلمة سايبر بانها (بادئة "أ" كومبيوتري -cybertalk) أي عصري جداً وعرف كلمة -cybernation - بأنها (السبرنة : الضبط الأوتوماتي لعملية ما،عن طريق استخدام الكومبيوتر)، كما عرفت كلمة (cybernetics) و هي مصدر كلمة سايبر بأنها (السبرنة أي علم الضبط) كما عرف مصطلح الفضاء السيبراني بأنه (الفضاء الكومبيوتري : عالم الإتصالات المستخدمة للكومبيوتر وبخاصة الإنترنت)[2].

قاموس المصطلحات العسكرية الاميريكية عرف كلمة سايبر" بأنها أي فعل يستخدم عن طريق شبكات إلكترونية بهدف السيطرة أو تعطيل لبرامج الكترونية أخرى " [3].

اما سبب اخيارنا لمصطلح السايبر يعود الى إستخدامه في شتى الوثائق والمنشورات الصادرة عن الأمم المتحدة باللغة العربية ومقالات اللجنة الدولية للصليب الأحمر، و دليل تالين وايضاً استخدمت مصطلح السيبرانية أهم المنصات الدولية المعينة التي نذكر منها على سبيل المثال لا الحصر :

- إرشادات الإسكوا للتشريعات السيبرانية

- مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية (بيروت، ٢٠١٢) .

- دليل الأمن السيبراني للبلدان النامية (الاتحاد الدولي للاتصالات، ٢٠٠٦) .

- الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية : توصيات سياسية، اللجنة الإقتصادية والسياسية لغربي أسيا (إسكوا)، الأمم المتحدة، نيويورك,٢٠١٥

- أللقاء السنوي للمختصين في أمن وسلامة الفضاء السيبراني، جامعة الدول العربية، بيروت، ٢٠١٢-٢٠١٦.

- دليل تالين بشأن القانون الدولي المطبق على الحروب السيبرانية لعام ٢٠١٧

- الاستراتجية الوطنية اللبنانية للأمن السيبراني، ٢٠٢٢

اذاً لكافة الأسباب المذكورة أعلاه قررنا أن نستخدم هذا المصطلح في دراستنا الحالية .

- مفهوم السيبرانية اصطلاحاً :

يعتبر مفهوم الهجوم السيبراني من المواضيع الحديثة نسبياً مما دفع الفقهاء وعلماء القانون السعي الى توضيح هذا المفهوم عبر تعاريف مختلفة نوعاً ما، وضعت في سبيل ازالة الغموض والالتباس، لذلك سوف نستعرض مختلف هذه التعاريف في هذا المبحث ولكن لا بدَ قبل البدء، توضيح سبب إختيارنا لتعبير الهجمات السيبرانية في هذه الدراسة (cyber attacks) : إستخدم (James A.lewis) مفهوم الفضاء السيبراني للدلالة على العمليات السيبرانية التي تتم فيها الذي اعتبر:" أننا يمكننا مواجهة المخاطر الناشئة

[1] علي محمد كاظم الموسوي، "المشاركة المباشرة في الهجمات السيبرانية"، المؤسسة الحديثة للكتاب، الطبعة الأولى ٢٠١٩، ص ٢١

[2] رمزي منير البعلبكي، المورد الحديث، دار العلم للملايين، بيروت، ٢٠١٩، ص ٣٠٧

3 U.S . Departement of Defense , Dictionary of Military and Associated Terms , joint Publication 02,Nov.8.2010,as amended through Feb.15, 2012

عن العمليات السيبرانية عبر أنظمة إلكترونية مخصصة لهذا الغرض"، وبعد العودة الى مفهوم الفضاء السيبراني نرى أنه من المفاهيم الواسعة النطاق التي كثرت التعاريف بشأنه، ولكن يمكن القول أنه بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكونة من مجموعة من الأجهزة الرقمية وأنظمة الشبكات والبرمجيات والمستخدمين سواء مشغلين او مستعملين ومسألة تحديد مفهوم الفضاء السيبراني هي مسألة نسبية تتوقف على طبيعة إدراك وفهم كل من الدولة والهيئات كلٌ حسب رؤيته وإستراتجيته وقدرته على إستغلال المزايا المتاحة ومواجهة المخاطر الكامنة في هذا الفضاء " [٤]، اذاً نستنتج انه يتكون من جانبين:

الجانب التقني : يتكون من أجهزة الكمبيوتر والشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكم .

- الجانب البشري :هم مستخدموا العناصر المذكورة أعلاه في الجانب التقني .

مع الإشارة الى أنه من غير الموفق أن نستخدم مفهوم الفضاء السيبراني للدلالة على الهجمات السيبرانية وذلك لأن العمليات غير المشروعة التي تتم في الفضاء السيبراني ليست عبارة فقط عن هجمات سيبرانية بل أيضاً هناك العديد من التهديدات التي تمس بالأمن السيبراني ونذكر منها على سبيل المثال لا الحصر : التجسس السيبراني، الإستطلاع الالكتروني، الجرائم السيبرانية، الإرهاب السيبراني .

إستخدم مفهوم الحرب السيبرانية (Cyber warfare) في بعض الأبحاث ويعود الهدف وراء إستخدام هذا التعبير الى أسباب إيديولوجية أمنية وعسكرية[٥]، يمكن أن نعتبر أنها نوع من أنواع حرب المعلومات، الغاية منها إحداث خلل في أنظمة المعلومات للخصم أي أنه يقصد منها توظيف أجهزة الحاسب وكل ما يتعلق بتكنولوجيا المعلومات لمواجهة شبكات الإنترنت ذات الصلة بمصادر المعلومات المدنية والعسكرية للخصم ولكن إستخدام مثل هكذا تعبير خاصةً في عصرنا الحالي ليس بالأهمية خاصةً بعد أن شددت المؤسسات الدولية على إستخدام "مصطلح النزاع المسلح بدلاً من مصطلح الحرب " بحيث تم إستخدامه وللمرةَ الاولى في إتفاقيات جنيف الأربعة الموقعة في ١٢ اب عام ١٩٤٩ وهذا ما أكده (Michael Gervais) ان مصطلح الحرب السيبرانية ليس بالمصطلح المناسب لكونه مصطلح عام لا يميز بين آثار إستخدام السيبرانية كوسيلة أم كطريقة قتالية، هذا ما أيده (Thomas Rid و Peter Mcburney) المختصان في القانون الدولي الإنساني عبر التركيز على مصطلح الهجمات السيبرانية أكثر من الحرب السيبرانية [٦]، وذلك كون هذه الأخيرة تعتبر أوسع نطاق من الهجمات السيبرانية .

للهجمات السيبرانية العديد من التعاريف تبعاً لوجهات النظر التي يتبناها أصحابها : بحسب Michael N Schmitt" الهجمات السيبرانية هي تلك الاجراءات التي تتخذها الدولة من أجل الهجوم على نظم المعلومات للعدو بهدف التأثير و الإضرار فيها، والدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة " ،اذاً بالنسبة ل Schmitt التركيز على النتائج والأهداف أساسي لبيان تأثير هذا الهجوم على أنظمة الحاسوب

[٤] اسماعيل زروقة , " الفضاء السيبراني والتحول في مفاهيم القوة و الصراع "، طبعة ٢٠١٩ ، مجلة العلوم القانونية والسياسية، المجلد ١٠ ، العدد ٠١ ، ص ١٠١٧-١٠١٨

[٥] اسماعيل زروقة، مرجع سابق، ص ١٠١٧

[٦] احمد عبيس نعمة الفتلاوي، "الهجمات السيبرانية : دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر"، الطبعة الأولى، منشورات زين الحقوقية، ٢٠١٨، بيرو ت-لبنان ص ١٥

والمعلومات المخزنة التي تكون معرضة للتلف أو الفقدان أو التسريب بسبب هذا الهجوم [٧]، أما Marco Roscini عرفها بأنها " تطويع الإمكانيات التقنية من أجل التأثير على المواقع الإلكترونية الأخرى أو تعطيلها او تدميرها سواء تقدم الخدمات المدنية أم العسكرية " [٨].

لذلك وبحسب Schmitt "الهجوم السيبراني هو كل هجوم يتم من قبل دولة معتدية ضد دولة معتدى عليها بهدف تدمير أو تعطيل النظم الإلكترونية للدولة المعتدى عليها ولعل أشهرها هو نقل الفيروسات الى شبكة الكمبيوتر الخاصة بالخصم لتدمير البيانات والبرامج و تغييرها "[٩]، هنالك تعريف اخر Schmitt الوارد في *دليل تالين* هو الأهم في توضيح مفهوم الهجمات، بحيث نصت المادة ٣٠ منه : " الهجوم السيبراني هو أي تصرف إلكتروني دفاعياً كان أم هجومياً يتوقع منه وعلى نحو معقول في التسبب بجرح أو وفاة أشخاص او إلحاق الأضرار أو تدمير الأعيان(الأهداف) "، وهذا ما نؤيده في الأصل في هذا التعريف أنه يبنى على تلك النتائج التي تتسبب بها هذه الهجمات ومن خلال هذا التعريف يمكن التمييز بين الهجمات السيبرانية وغيرها من الأفعال المقاربة لها .

وبمعنى آخر الهجوم السيبراني هو ذلك الهجوم التي تقوم به الدول فقط آي ان الهجوم الذي يقوم به الأفراد لا يعد هجوم سيبراني بحسب تعريفه.

اما Fuertes عرّف "الهجوم السيبراني أنه هجوم عبر الإنترنت يقوم على التسلل الى مواقع إلكترونية غير مرخص بالدخول اليها، بهدف تعطيل أو إتلاف البيانات المتوفرة فيها أو الإستحواذ عليها وهي عبارة عن سلسلة هجمات إلكترونية تقوم بها دولة ضد أخرى " [١٠] و Shin الذي ذهب بالقول "أن الهجمات هي إستخدام اللطيف الإلكتروني أو الكهرومغناطيسي لتخزين وتعديل تبادل البيانات وجهاً لوجه مع أنظمة تحكم في البني التحتية المرتبطة بها" [١١].

المادة ٤٩ من البروتوكول الإضافي الأول لسنة ١٩٧٧ :" تعني "الهجمات" أعمال العنف الهجومية والدفاعية ضد الخصم وتنطبق أحكام هذا اللحق "البروتوكول" المتعلقة بالهجمات على كافة الهجمات في أي إقليم تشن منه بما في ذلك الإقليم الوطني لأحد أطراف النزاع والواقع تحت سيطرة الخصم ".

كذلك Zimet & Barry عرفا الهجوم بأنه : " مجموعة من العمليات القائمة على الحرب الإلكترونية والخداع النفسي فضلاً عن إستهداف شبكة تواصل العدو العسكرية وعملياته الأمنية والإلكترونية" [١٢] .

---

[٧] Michael N.Schmitt , computer Network Attack and the Use of Force in International Law : Thoughts on a Normative Framework , Columbia Journal of Transnational Law , 1998-99, Vol.37, p 890.

[٨] Marco Roscini, World Wide Warfare –Jus ad Bellum and the use of CyberForce , Max Planck yearbook of United Nations Law,2010,Vol. 14 .p91

[9] Michael N.Schmitt,Ibid,p7

[١٠] Michael S.Fuertes , "cyber warfare ,Unjust Actions in a Just war" , Florida International University , Full 2013,p.1.

[١١] Shin.Beomchul,op.cit.p.105.

[١٢] Zimet.E and C.L Barry " Military services Overview , Cyber power and National Security" .National Defense University Press, Washington,DC,USA,2009.P.291.

بدورها القيادة الإستراتيجية الأمريكية U.S. Strategic Command عام ٢٠٠٧ عرفت الهجمات السيبرانية بأنها " تطويع عمليات نظام الكومبيوتر بهدف منع الخصوم من الإستخدام الفعّال لها، فضلاً عن التسلل الى أنظمة المعلومات وشبكات الإتصال بهدف جمع وحيازة وتحليل البيانات التي تحتويها" [١٣]، كذلك Johan Sigholm إعتبر: " أن هذه الهجمات هي جزء من العمليات السيبرانية التي تعمل على توظيف إمكانيات الفضاء السيبراني والإستخدام العدائي له من الدولة والجهات غير الحكومية الفاعلة في النزاعات والتي تعمل نيابة عنها من أجل التسبب بالضرر، الدمار أو سقوط الضحايا لتحقيق أهداف عسكرية أو سياسية" [١٤] ، أما Matthew C. Waxman اعتبر أن " الهجمات السيبرانية هي الجهود الرامية الى تغيير، تعطيل أو تدمير أنظمة الحاسوب او الشبكات او المعلومات او البرامج الموجودة عليهما، والأضرار التي تسببها هذه الهجمات يمكن أن تصيب شبكة الحاسوب أو المرافق المادية او الأشخاص وتتراوح أضرار الهجمات السيبرانية من القرصنة الخبيثة وتشويه مواقع الإنترنت الى الدمار واسع النطاق على البنية التحتية العسكرية والمدنية المرتبطة بهذه الشبكات " [١٥].

لا بدّ ان نشير أن هناك اتجاهين للهجمات السيبرانية : *الإتجاه الضيق* الذي تبنته الولايات المتحدة الامريكية الذي يركز على موضوع الهجوم وهو ما ورد في معجم الإستخدامات الأمريكية الذي نشرته هيئة الأركان المشتركة عام ٢٠١١ الذي عرّف الهجوم السيبراني انه " نشاط عدائي بإستخدام الكمبيوتر او الشبكات أو الأنظمة ذات الصلة بهدف تعطيل او تدمير أنظمة الخصم السيبرانية الحرجة أو ممتلكاته أو وظائفه، ان النتائج المرجوة من الهجوم السيبراني لا تقتصر بالضرورة على أنظمة كمبيوترية مستهدفة أو البيانات نفسها وإن تفعيل او تأثير الهجوم السيبراني قد يفصل زمنياً او مكانياً عن النشاط السيبراني " [١٦]، أما *الإتجاه الواسع* الذي تبنته منظمة شنغهاي للتعاون ينص على ان " نشر المعلومات الضارة للأنظمة الإجتماعية والسياسية والإقتصادية فضلاً عن المجالات الروحية والأخلاقية والثقافية للدول الأخرى بوصفها أيضاً من التهديدات الرئيسية للأمن السيبراني" [١٧]، نضيف ما نصت عليه المنظمة من الإتجاهات الحديثة على الساحة الدولية.

بعد إلقاء الضوء على معظم تعاريف الفقهاء نستنتج أن الهجمات السيبرانية هي مجموعة من الأعمال غير المباحة التي تهدف الى التسلل الى مواقع إلكترونية سواء كانت هذه الاخيرة حكومية أم لا بهدف تعطيل او تدمير او إتلاف او تسريب المعلومات المخزنة او الإستحواذ عليها بصورة غير شرعية، مع التشديد انه ليس بالضرورة هذه الهجمات ان تكون موجهة من دولة ضد اخرى بل يمكن ان يوجهها الأفراد ضد دولة أم ضد شركة ام مؤسسة ام ان توجهها دولة بنفسها الى شركة أم مؤسسة غير حكومية، بحسب رأينا أن الهجوم الموجه من دولة الى مؤسسة حكومية لدولة أخرى هو هجوم موجه الى الدولة نفسها طالما أن

---

[١٣] احمد عبيس نعمة الفتلاوي، مرجع سابق، ص ١٨

[١٤] علي محمد كاظم الموسوي، مرجع سابق، ص ٢٤.

[١٥] علي كاظم الموسوي، مرجع سابق، ص ٢٥

[١٦] James E.Cartwright , “Memorandum for Chiefs of the Military Serve , commanders of the Combattant Commands,Dirs, of the Joint staff Directories on joint Terminology for cyberspace operations” , Washington, 2018 ,p5, available on : https://info.publicintelligence.net/DoD-JointCyberTerms.pdf

[١٧] Shanhai Cooperation Agreement,Annex I , p, 203.

المؤسسة هي حكومية فضلاً على أنه من الضروري أن نخرج من نطاق بعض التعاريف الآنف ذكرها التي تحصر الهجمات السيبرانية بنطاق الدولة .

اذاً فواعل الهجمات السيبرانة:

- الدول: لديها قدرة كبيرة على تنفيذ الهجمات طالما أنها تملك القدرة والقوة السيبرانية والوسائل الضرورية لتنفيذ هذا الهجوم .

-أفراد طبيعيون : الذين لديهم المام بالتكنولوجيا ويمتلكون الوسائل المتاحة لتنفيذ هذه الهجمات

- الشركات المتعددة الجنسيات : هذه الشركات تمتلك البيانات العملاقة التي تؤثر في اقتصاديات الدول و في ثقافة مجتمعاتها بحيث أنها تمتلك موارد للقوة تفوق قدرة بعض الدول ولا ينقصها سوى الشرعية لممارسة أعمالها فهي تعتبر أرض خصبة للهجمات السيبرانية سواء كانت المعتدي ام المعتدى عليها .

- المنظمات الإجرامية : هذه المنظمات تقوم بعمليات القرصنة السيبرانة وإختراق الحسابات المصرفية وتحويل الاموال وتبيضها فضلاً عن السوق السوداء على الإنترنت لتجارة المخدرات والأسلحة والإتجار بالبشر.

- الجماعات الارهابية : تستغل هذه الجماعات الفضاء السيبراني في عمليات التجنيد والتعبئة والدعاية وجلب الأموال والمتطوعين وتوجيه الهجمات السيبرانية ضد الشركات والمؤسسات الحكومية وغير الحكومية والمنشات السيبرانية لبعض الدول واستهداف البنية التحتية المعلوماتية للدول وللمصارف بهدف تحقيق إمتيازات غير مشروعة وأرباح خيالية وإحداث أضرار مادية ومعنوية [١٨] .

في الفرع الثاني من هذا المبحث سوف نبين أبرز الخصائص المميزة للمهاجم السيبراني التي تجعله مختلفاً عن المجرم التقليدي.

الفرع الثاني : سمات مرتكب الهجوم السيبراني

يتميز المجرم المعلوماتي بعدة صفات مختلفة عن سائر المجرمين التقليدين سوف نبينها تباعاً.

ينتمي المجرم المعلوماتي الى فئة خاصة من المجرمين إنطلاقاً من الوسط الإجتماعي الراقي الذي نشأ فيه وحصوله على درجة معينة من العلم والمعرفة وإنتسابه الى طبقة خاصة بالمجتمع التي تسمى بذوي الياقات البيضاء التي عرفت على أنها : " جريمة يرتكبها فرد من ذوي الطبقات الاجتماعية العليا وله مكانة مرموقة في نطاق مهنته " [١٩] وتشمل الجرائم المرتكبة من قبلهم كالإحتيال والرشوة والتجارة من الداخل والإختلاس والجرائم الالكترونية وإنتهاك حقوق الطبع، وغالباً تجمع الجاني بالمجني عليه علاقة وظيفية سواء كان هذا الأخير شخص طبيعي أم معنوي، تارةً تكون الغاية لدى الجاني استهداف شخص طبيعي بقصد ايقاعه في إحدى الجرائم المذكورة أعلاه او الإستلاء على معلومات خاصة به عن طريق هجمات سيبرانية يوجهها

---

[١٨] اسماعيل زروقة، مرجع سابق، ص ١٠٢٠-١٠٢١

[١٩] - فاديا بيضون : " : نظرية جرائم ذوي الياقات البيضاء عام ١٩٣٩ لأدوين سذرلاند "، مجلة محكمة، ٢٠٢١، لبنان ، متوفرة على الرابط التالي : www.mahkama.net

اليه، وتارةً أخرى يكون الهدف هو إستهداف شخص معنوي كشركة ام مؤسسة اقتصادية أم اجتماعية أم مالية أم مرفق عام ام احدى المصارف العامة والخاصة التي تكون عرضة للهجمات السيبرانية والجرائم الالكترونية الأكثر شهرة في عصرنا الحالي .

بالعودة الى خصائص شخصية المجرم السيبراني نستخلصها بأربع صفات أساسية على الشكل التالي :

١. المهارة :

أن المجرم المعلوماتي يمتلك المهارة والقدرة والخبرة المكتسبة في مجالات التكنولوجيا والمعلومات، فالذكاء أساسي في جرائم المعلومات، أن يكون على قدر كبير من العلم ولديه خبرة معينة يكتسبها عن طريق التعليم والدراسة المتخصصة في المجال، فيستطيع الدخول الى البرامج الغير مرخصة ويقوم ببرمجة فيروسات أو برامج معينة من شأنها أن تلحق الأضرار بالمعلومات المتوافرة أو إتلافها أو الإستحواذ عليها، بحيث يكون على بيّنة حول طريقة عمل هذا الفيروس، فأنواع البرمجيات الخبيثة والفيروسات الإلكترونية كثيرة وجميعها تهدف الى إلحاق الأضرار بالمجني عليه وكل منها وفقاً للهدف الذي وضعت من أجله، لذلك نعتبر الذكاء والمعرفة والمهارات اللاّزمة من أبرز الخصائص المطلوبة في الجاني لتنفيذ نشاطه السيبراني.

٢. المعرفة :

إن المسار الجرمي يمر بعدة مراحل قبل الوصول الى النتيجة المرجوة وهي تنفيذ الجريمة ولكن ينبغي على الجاني التعرف على كافة الظروف التي تحيط بالجريمة أو بأرضيتها وذلك من أجل التأكد أن نسبة النجاح أعلى بكثير من نسبة الفشل وهذا الأمر مشترك بين الجرائم التقليدية والمستحدثة، فالتأكد من التفاصيل أمرُ أساسيُ، فيبدأ النشاط السيبراني والهجوم في التفكير والتصميم على ارتكاب الجرم ثم الإنتقال الى المرحلة التحضيرية التي تسبق التنفيذ من أجل التأكد أن كافة التفاصيل جاهزة، فالمهاجم السيبراني يتأكد أن البرنامج الخبيث الذي يريد استخدامه جاهزاً وكافة الأمور الأساسية أيضاً لضمان نجاح العملية عبر التحضير الدقيق للأرضية الإفتراضية كي لا يواجه أشياء غير متوقعة [٢٠].

٣. الوسيلة :

الوسيلة هي الأسلوب المستخدم من قبل الفاعل لتنفيذ الجريمة وهي التي يحصل عليها من مصادر خارجية وذلك بهدف مساعدته على إرتكاب الجرم وأحياناً المتدخل يمده بالوسائل اللازمة، التي تكون إما عادية موجودة في أي مكان أو تكون مبتكرة (أي من صنع الفاعل) وخاصةً في مجال الهجمات التي تكون عبارة عن برمجيات خبيثة وفيروسات صممها الفاعل أم شخصُ آخر بالإتفاق معه، ونشير أن الوسائل المطلوبة للتلاعب بأنظمة الحاسبات الالية تتميز نسبياً بالبساطة وبسهولة الحصول عليها [٢١] وهنالك شرطُ آخر لنجاح الهجوم وهو أن تكون الأنظمة المعلوماتية مألوفة من الفاعل وذلك من أجل تسهيل عملية إرتكاب النشاط السيبراني، فكلما كان نظام الحاسب الذي يحتوي على المعلومات المستهدفة غير مألوف كانت الوسائل أكثر صعوبة في الحصول عليها لإقتصارها على عدد قليل من الأفراد اللذين هم عادةً القائمون على تشغيل النظام وذلك على عكس الأنظمة الشائعة الإستعمال [٢٢] .

---

[٢٠] نائلة قورة، مرجع سابق، ص ٥٧-٥٨

[٢١] شيخة حسين الزهراني، مرجع سابق، ص ٧٩

[٢٢] طارق ابراهيم الدسوقي، مرجع سابق، ص ١٧١

إضافة الى ما تقدم أعلاه، الأفراد يختلفون فيما بينهم في قدر ما يتمتعون من ذكاء ولكن نريد أن نأكد أن غالباً المجرم المعلوماتي يتمتع بذكاء ودهاء كافي لإرتكاب الجرائم السيبرانية، فمنهم العباقرة النابغون اللذين يمثلون فئة ضئيلة من المجرمين ومنهم متوسطي الذكاء وهم الكثرة الغالبة، أما بالنسبة الى أنواع الذكاء نميز بين الذكاء العملي والذكاء الفكري والذكاء الفني وغالباً المجرم المعلوماتي تنطبق عليه الأنواع الثلاثة وجميعها مرتبطة ارتباطاً وثيقاً بالذكاء الإصطناعي وبالوسيلة المستخدمة في إرتكاب الجريمة السيبرانية [٢٣]، فالذكاء الاصطناعي يرتبط بمجموعة من الإمكانيات والقدرات التي توفر للشخص أفضل الطرق من أجل إرتكاب الجرم السيبراني عن طريق إتاحة مواقع خاصة ومميزة في التصور والتخيل والتطبيق والمساعدة في التحليل والتأصيل وإبتكار مواقع خاصة من أجل مساعدة المجرم في توسيع آفاقه وإمكانياته الفعلية في عرض الصورالإجرامية وشرح كيفية إرتكاب الجرائم وغيرها من الأساليب المستحدثة .

٤.السلطة :

هي الحقوق أو المزايا التي يتمتع بها المجرم السيبراني والتي تمكنه من إرتكاب جريمته [٢٤]، فبعض الأشخاص يتمتعون بصفة رسمية تساعدهم في تجاوز الصلاحيات المعطاة لهم، ان هذه الصفة لا يمكنها أن تكون سبباً لإعفاء صاحبها من المسؤولية الجنائية في حال إرتكابه لجرائم دولية تشكل إنتهاكات للقانون الدولي الانساني، والهدف الأساسي الذي نسعى اليه هو الحؤول دون إفلات المجرم من العقاب سواء كان الفاعل قد ارتكب الجرم عن سبق تصور وتصميم وإما عن تقصير أو اهمال وقلة احتراز، فالمجرمين المعلوماتيين لديهم سلطة مباشرة أم غير مباشرة في الحصول على ما يريدونه وهذه السلطة تسمح لهم بالدخول الى النظام الذي يحتوي على المعلومات والذي يمّكن الفاعل من فتح الملفات او قراءتها وكتابتها ومحوها أو تعديل محتواها[٢٥]، فهؤلاء المجرمين يتولون وظائف مهمة تسمح لهم بالولوج الى الأماكن غير المرخص بها للكافة أو الوصول الى معلومات حساسة خاصة بالعملاء أو الدخول الى أنظمة الحاسبات الآلية مع إمكانية فتح ملفات معينة.

أما في إطار الهجمات السيبرانية نحن أمام قادة عسكريين جرى تحت قيادتهم تنفيذ هجمات جسيمة إعتبرت كإنتهاكات للقانون الدولي الإنساني، فهذا الأخير نظم ووضع قيود وشروط لأي نشاط سيبراني سواء قد إرتكب من قبل جهة مدنية أم عسكرية، مع التشديد على ضرورة تطبيق القانون للحؤول دون التهرب من العقاب ومحاكمة أي شخص متهم بمخالفة قواعد القانون الدولي الانساني، وهذا ما أكدته المادتين السابعة من النظام الأساسي للمحكمة الجنائية الدولية ليوغوسلافيا السابقة والمادة السادسة من النظام الأساسي للمحكمة الجنائية الدولية الخاصة برواندا ووفق هاتين الماديتن : "يتحمل أي شخص خطط أو حرّض أو أمر أو إرتكب أو ساعد أو شارك بطريقة أخرى في التخطيط أو الإعداد لجريمة أو تنفيذها بموجب الإختصاص القضائي للمحكمتين سواء كان هذا الشخص موظفاً حكومياً أو قائداً عسكرياً أو تابعاً لها، المسؤولية الفردية من الجرائم وتجوز محاكمته" [٢٦].

---

[٢٣] سامية شينار، مرجع سابق، ص ١

[٢٤] شيخة حسين الزهراني، مرجع سابق، ص ٨٠

[٢٥] طارق ابراهيم الدسوقي، مرجع سابق، ص ١٧٢

[٢٦] المادة السابعة (فقرة ١) من النظام الأساسي للمحكمة الجنائية الدولية ليوغوسلافيا السابقة والمادة السادسة(فقرة ١) من النظام الأساسي للمحكمة الجنائية الدولية الخاصة برواندا

أيضاً في حالة الأشخاص ذوي المناصب العليا، سواء كان رئيس دولة أو حكومة أو موظفاً مدنياً مهماً فان منصبهم لا يعفيهم من تحمل المسؤولية الجنائية ولا تخفف عقوبتهم [٢٧]، وأخيراً يتحمل المسؤول أو القائد مسؤولية تسمى بالمسؤولية التقصيرية عن جريمة إرتكبها أحد مرؤوسيه وذلك في حال من كان في منصب أعلى على علم أو كانت لديه أسباب ليعلم أن أحد مرؤوسيه على وشك إرتكاب مثل هذه الأعمال أو إرتكبها وفشل في إتخاذ الإجراءات الضرورية والمعقولة لمنع وقوع مثل هذه الأعمال أو معاقبة مرتكبيها [٢٨].

وبالرغم من أن القانون وجب على القادة العسكريين منع الإنتهاكات للإتفاقيات وخاصة للبروتوكول الإضافي الأول وإبلاغها الى السلطات المختصة، بالنسبة لتلك المرتكبة من قبل القوات المسلحة اللذين يعملون تحت إمرتهم وغيرهم ممن يعملون تحت إشرافهم والتأكد أن كافة العناصر على بيّنة من الإلتزامات المفروضة عليهم والمنصوص عنها في هذا البروتوكول الإضافي الأول [٢٩].

كذلك لا يعفى قيام أي مرؤوس بإنتهاك الإتفاقيات من المسؤولية الجنائية أو التأديبية حسب الأحوال اذا علموا أو كانت لديهم معلومات تتيح لهم في تلك الظروف أو يخلصوا الى أنه كان يرتكب أو أنه في سبيله لإرتكاب مثل هذا الإنتهاك ولم يتخذوا كل ما في وسعهم من إجراءات مستطاعة لمنع أو قمع هذا الإنتهاك [٣٠]، وفي إطار الهجمات السيبرانية وجب على القادة الالتزام بالقوانين المفروضة المختصة بتنظيم العمليات في الفضاء السيبراني ولا يعفى من العقاب ومن المسؤولية الجنائية الدولية وفقاً للأحكام المفروضة أعلاه، في حال ثبت أنه تخلف عن معاقبة الأفراد اللذين إرتكبوا انتهاكات للقانون الدولي الانساني أو بسبب تقصيره لم يتخذ الإجراءات اللازمة للحؤول دون وقوع مثل هكذا جرم بعلمه او بسبب تقصيره وإهماله ولا يعفى من العقاب أياً كانت رتبته أو مركزه سواء كان هو من يرتكب هذه الجرائم أو بالاشتراك مع آخرون .

أما الحالة الأخرى التي نريد التطرق اليها في إطار معالجة الجرائم المعلوماتية المرتكبة من قبل الرؤساء والقادة في حال قدم العون أو حرّض أو ساعد بأي شكل آخر لغرض تسيير ارتكاب إنتهاكات للقانون الدولي الانساني او ساهم بأي طريقة في قيام جماعة من الأشخاص يعملون بقصد مشترك لإرتكاب الجريمة[٣١] ولكن من أجل تطبيق مبدأ العدالة لا يسأل الرئيس عن الجرائم التي إرتكبها المرؤوس الاّ اذا كان على علم بإرتكابها أو تجاهل إرتكابها [٣٢].

---

[٢٧] المادة السابعة (فقرة ٢) من النظام الأساسي للمحكمة الجنائية الدولية ليوغوسلافيا السابقة والمادة السادسة(فقرة ٢) من النظام الأساسي للمحكمة الجنائية الدولية الخاصة برواندا

[٢٨] المادة السابعة (فقرة ٣) من النظام الأساسي للمحكمة الجنائية الدولية ليوغوسلافيا السابقة والمادة السادسة(فقرة ٣) من النظام الأساسي للمحكمة الجنائية الدولية الخاصة برواندا

[٢٩] المادة ٨٧ من البروتوكول الاضافي الأول

[٣٠] المادة ٨٦ من البروتوكول الاضافي الأول

[٣١] المادة ٢٥ من نظام روما الأساسي

[٣٢] خلفان كريم : " الأسس القانونية لتراجع نظام الحصانة القضائية الجنائية لكبار المسؤولين في القانون الدولي المعاصر"، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، كلية الحقوق – جامعة مولود معمري، ص ٢٢٠

المبحث الثاني : في محاولة تحديد مراحل تطور الهجمات السيبرانية

إن تحديد المسار التاريخي للهجمات السيبرانية أمرٌ أساسيُ في توضيح أبرز المراحل التي مرت بها وصولاً الى الوضع الحالي في الفرع الأول من هذا المبحث، محاولين تحديد الخصائص المميزة للهجوم بإعتباره جريمة عابرة للحدود في الفرع الثاني .

الفرع الأول : نشأة الهجمات السيبرانية ونماذج عنها

تتأثر نشأة الهجمات السيبرانية من جهة بإستحداث أجهزة الكومبيوتر في منتصف الخمسينيات من القرن الماضي كأداة لمعالجة وحفظ المعلومات رقمياً ودخول الحاسوب في عمل المؤسسات الشركات وكافة الأمور الحياتية للأفراد وظهور الشبكة العنكبوتية من جهة اخرى أحدثا انقلاباً كبيراً في حياة البشرية من خلال التواصل ونقل المعلومات بسرعة فائقة .

في الأربعينيات من القرن الماضي كان إستخدام الحواسيب مقتصر على المؤسسات العسكرية والمؤسسات الكبرى ولكن في نطاق ضيق، ففي البدء تم إستحداث الحاسوب وذلك من أجل تسيير وتسهيل عمل المؤسسات العامة والخاصة ومن أجل الإحتفاظ بالمعلومات بطريقة جديدة يمكن الرجوع اليها في أي لحظة.

في الخمسينيات بدأت الدراسات تشير الى ظهور الجرائم السيبرانية بحيث أشار (دون باركر) الى أول حالة موثقة لجريمة إرتكبت بواسطة الحاسوب تعود الى عام ١٩٥٨ بحيث شهد هذا العام العديد من الجرائم التي رصدها معهد (ستانفورد) الدولي للأبحاث في أميريكا وصنفها الى أربع جرائم (العبث أو التخريب الموجه الى الحاسوب، سرقة المعلومات أو الممتلكات، الإحتيال أو الغش المالي، الإستخدام غير المصرح به لخدمات الحاسوب)، اما بالنسبة للإنترنت ترجح أصوله التاريخية الى عام ١٩٦٢على يد العلماء العاملين في المشروعات المتطورة في الولايات المتحدة الامريكية، وهذا المشروع لديه هدفاً استراتجياً وهو إرسال تعليمات التصويب من خلال مركز التحكم الى قواعد الصواريخ حتى لو بعد ، وتدمير جزء من شبكات الإتصال نتيجة تعرضها لهجوم، وقد عُرفت هذه الوكالة فيما بعد بإسم وكالة الأبحاث والمشروعات الدفاعية لوزارة الدفاع الامريكية.[٣٣]

مرحلة السبعينيات (خاصةً عام ١٩٧٣) تمثل الإنطلاقة الحقيقية للبحوث في مجال الحاسوب والإنترنت، عبر ربط الحاسبات الآلية المختلفة والتي تستخدم بروتوكول مشترك للاتصال IP/TCP، هذا البروتوكول هو القاعدة المعيارية المحددة للإتصال عبرالإنترنت بحيث يقوم بتقسيم المعلومات المراد إرسالها من حاسوب عبر الإنترنت الى حزم ثم إعادة تجميعها من جديد في حاسوب آخر في الجهة المرسل اليها – هذا البروتوكول يسمح للإنترنت بتحويل الحزم الخاصة بالبيانات كي تصل الى المرسل اليه بسرعة فائقة[٣٤]، أما لناحية التشريع، أعتبر المشرع الفرنسي في الصدارة عن طريق سنَ قانون حماية الحريات المعلوماتية عام ١٩٧٨، اما في فلوريدا صدر أول قانون جرائم الحاسوب في الولايات المتحدة في العام نفسه.

---

[٣٣] اسامة ابو الحسن مجاهد، " خصوصية التعاقد عبر الانترنت "، طبعة ٢٠٠٠، دار النهضة العربية، ص ٣

[٣٤] مصطفى السيد مصطفى عبد العال، " دليلك الشامل الى شبكة الانترنت "، الطبعة الثالثة، دار الكتب العلمية للنشر والتوزيع، القاهرة، ص ١٤ .

فترة السبعينيات تمثلت الفترة الحقيقية لإنطلاقة الدراسات والبحوث في مجال الحاسوب، من أبرز هذه الدراسات على سبيل المثال لا الحصر[٣٥] :

- دراسة مكتب أبحاث إساءة استخدام الحاسوب في استراليا التابع لمعهد (كلوفيد) للتقنية بدأت عام ١٩٧٥ وإنتهت عام ١٩٨٥ والتي رصدت ١٥٠ حالة .

- دراسة معهد ستانفورد العلمي للأبحاث في اميريكا(SRI) عام ١٩٧١ والتي رصدت ١٦٠٠ حالة إساءة إستخدام الحاسوب وكذلك إستبيان المعهد ذاته في عام ١٩٧٩ الذي وصل الى ٧٢ مدعي عام للتحضير لمناقشة مشروع قانون الجريمة الاقتصادية وحيث أفاد أربعون منهم بوصول ٢٢٤ جريمة متصلة بالحاسوب الى علمهم، منها ١٩٠ جريمة حركت الدعوى على مرتكبيها و ١٧٦ جريمة قضت المحاكم فيها بالإدانة .

في مرحلة الثمانينات ترسخت مبادئ السياسة التشريعية في مجال الجرائم الإلكترونية وبدأت المناداة بضرورة سنّ قوانين لحماية مستخدمي الحاسوب وتجريم الأفعال التي ترتكب بواسطة الإنترنت والتي تلحق أضرار مادية ومعنوية مما دفع المشرع الإنكليزي بإقرار قانون حماية البيانات عام ١٩٨٤ والتي تعتبر سابقة من نوعها .

على أثر تنامي ظاهرة إختراق شبكات الحاسوب الذي عرّف بإصطلاح (Hacking) بدأت الدول بتحصين أمنها السيبراني وتحقيق قفزات نوعية في المجال الأمني والعسكري في مطلع التسعينيات من القرن المنصرم حتى أطلق البعض عليها مصطلح الحرب السيبرانية الباردة (Cyber cold war) أو سباق التسلح السيبراني (Cyber arms race) [٣٦]، وظهرت في العقد الأخير أبعاد جديدة في طرائق القتال وأسلوب الجيوش في التصدي للخصم لا سيما في المجالين العسكري والأمني، فدخلت أساليب جديدة على الساحة الدولية ومنها الهجمات السيبرانية : (John Arquila)جون اركويلا وديفيد رونفيلد (David Ronfeld) أول من بحثا في مسالة الهجمات السيبرانية عام ١٩٩٧ في كتابهم " الحرب السيبرانية قادمة : "Cyber war is coming”، اذ أشارا فيه الى أنظمة الإتصال الالكترونية ودورها في النزاعات المسلحة مستقبلاً . [٣٧]

ايضاً مرحلة التسعينات كانت بداية لحرب الهاكر العظمى بين كل من فريقين من الهاكرز المحترفين (LOD MOD –) فكان هدف المجموعة الدخول الى اجهزة الحاسب الالي للآخرين والعبث فيها وهكذا بدأت جرائم الإستلاء على المعلومات الشخصية والحكومية .

اذاً ان الإتجاه الحالي على الصعيد الدولي يجمع أن نجاح الحروب التي تشن او سوف تشن مستقبلاً سوف يفوز بها الفريق الذي يتقن المعلوماتية بأحدث صورها، فالقوة السيبرانية هي من أهم مصادر الحماية المعلوماتية في العصر الحالي، مما سارعت الدول المتقدمة الى زيادة نشاطاتها وتكثيف جهودها في الفضاء السيبراني وخاصةً ان البنى التحتية الحيوية لعمل الدولة كالكهرباء والمياه والمواصلات وشبكات القيادة

---

[٣٥] هشام محمد فريد رستم، "جرائم الحاسوب كصورة من صور الجرائم الاقتصادية "، ١٩٩٥، مجلة الدراسات القانونية، كلية الحقوق - جامعة أسيوط، العدد ١٧ , ص ٢٠٤.

[٣٦] احمد عبيس نعمة الفتلاوي، مرجع سابق، ص ٢٨

[٣٧] احمد عبيس نعمة الفتلاوي، مرجع سابق، ص ٢٤

والتحكم العسكرية كلها تعتمد على هذا الفضاء بحيث أنها تعتبر هدفاً للدولة المهاجمة ضد الخصوم وقد تكون هدفاً لهجوم الخصوم عليها .[٣٨]

كثيرةُ هي الأمثلة التي سجلها التاريخ عن الهجمات السيبرانية التي من الممكن ان تكون مرافقة للحروب التقليدية، مساندة لها أم مستقلة عنها وقد تكون عابرة للحدود الوطنية ام لا، نلخصها كالتالي:

سنبدأها من العام ١٩٨٢ مع الهجوم الأمريكي ضد منظومة التحكم العالية صناعياً في أنبوب نفط (Chelyabinsk) التابع للإتحاد السوفياتي السابق الذي أدى الى إنفجار كبير طال ثلاثة كيلومترات من الأنبوب وأدى الى خسائر بالغة في الأرواح وفي الماديات والمثال الآخر الهجمات السيبرانية المرافقة للحروب التقليدية هي حالة إستهداف حلف الشمال الأطلسي لشبكات الهاتف في يوغوسلافيا سابقاً وذلك في إطار حرب كوسوفو عام ١٩٩٩.[٣٩]

الهجمات السيبرانية في إطار الحرب التقليدية :

- النزاع السوري - الاسرائيلي :

عام ٢٠٠٧ تعرضت الدفاعات الجوية السورية التي يشتبه أنها منشأة نووية في منطقة دير الزورالى هجوم سيبراني ألحق بها خسائر فادحة .

- الحرب بين جورجيا وروسيا عام ٢٠٠٨ :

على خلفية إعلان إستقلال بلدة اوسيتيا الجنوبية من جورجيا الاّ أن سبقت الحرب التقليدية بينهما هجمات سيبرانية واسعة ضربت البنى التحتية الجورجية الإلكترونية التي تسببت هذه الهجمات بقطع التواصل بين الحكومة الجورجية ومواطنيها، فضلاً عن قطع التواصل مع دول العالم وإستمرت هذه الحالة حتى إنتهاء النزاع الروسي- الجورجي.

أما بالنسبة الى الهجمات بين الدول خارج إطار الحرب التقليدية نذكر منها [٤٠] :

الهجمات السيبرانية الصينية على الولايات المتحدة الامريكية :

- حادثة تيتاين راين (Titan Rain) عام ٢٠٠٣ التي أدت لى استخراج بيانات حساسة من منظمات تشمل وكالة الناسا NASA, lockhead Martin وSANDIA National Labratoires و مكتب التحقيقات الفيديرالي فضلاً عن وزارة الدفاع الاميريكية،على أثر ذلك إتهمت الحكومية الأمريكية الصين بتوليها قيادة هذه الهجمات .

- المكتب الاميريكي لإدارة شؤون الموظفين تعرض عام ٢٠١٥ الى هجمات سيبرانية أدت الى إستخراج ٢١,٥ مليون سجل خاص بموظفي حكومة الولايات المتحدة التي عزيت الى الصين.

---

[٣٨] علي محمد كاظم الموسوي، مرجع سابق، ص٣٣

[٣٩] احمد عبيس نعمة الفتلاوي ، مرجع سابق، ص ٦٢٣

[٤٠] بودرو بنجامين: " تهديدات مجهولة المصدر – نحو مسائلة دولية في الفضاء الالكتروني " , مؤسسةRAND ، سانتا مونيكا، كاليفورنيا , ٢٠١٧ , ص ٧ , مقال متوفرعلى الرابط التالي : https://www.rand.org/pubs/research_reports/RR2081.html

- إختراق الأنظمة الإلكترونية في البيت الأبيض عام ٢٠١٤ حيث اتهم فيها الرئيس الأميريكي روسيا بهذه الهجمات السيبرانية .

- قرصنة حساب SONY pictures في الولايات المتحدة الاميريكية عام ٢٠١٤ وسرقة بياناته وتسريبها وتعطيل أعماله، حيث عزاها الرئيس الأميريكي الى جهات حكومية فاعلة كورية .

-تعرضت قناة TV5 monde الفرنسية الي هجمات سيبرانية متتالية أدت الى تعطل أعمالها لمدة ١٨ ساعة عام ٢٠١٥ التي عزته القناة الى مجموعة القرصنة الروسية APT28.

- المكتب الامريكي لإدارة شؤون الموظفين : تعرض عام ٢٠١٥ الى هجمات سيبرانية أدت الى إستخراج ٢١,٥ مليون سجل خاص بموظفي حكومة الولايات المتحدة التي عزيت الى الصين.

- تعرضت شركة أرامكو السعودية الى إتلاف وتدمير أكثر من ٣٥٠٠٠ كومبيوتر بين عام ٢٠١٢ و ٢٠١٦ بحيث تبنت جهات ايرانية هذا الهجوم .

- عام ٢٠١٦ تم سرقة أكثر من ٨١ مليون دولار من حساب البنك المركزي في بنغلادش لدى البنك الإحتياطي الفديرالي في نيويورك بإستخدام نظام جمعية الإتصالات السلكية واللاسلكية بين المصارف على مستوى العالم في الميدان المالي المصرفي SWIFT .

- هجوم Stuxnetعلى ايران لمدة ٩ أشهر : نهاية عام ٢٠٠٩ وبداية عام ٢٠١٠ تم هذا الهجوم بهدف التسلل في أنظمة السيطرة المستخدمة في أهم المنشآت النووية الإيرانية، عن طريق فايروس يسمى Stuxnet صمم لكي يستهدف نظم التحكم والسيطرة SCADA أو PLCs ولكي ينتشر بصورة سريعة ومن دون التسبب بأضرار للمنشآت الأخرى والأشخاص اللذين لم يتم برمجته على ذلك، تم نشره بعد ذلك من خلال (USB Flash Drive) في الحاسبات وعند دخوله لأي حاسبة يبدأ في البحث عن أنواع محددة من أنظمة التحكم وهي Siemens PCS7 , WinCC, Step 7 , Siemens S 7 PLCs : لكي يهاجمها، ففي حالة عدم الكشف عن أي من هذه الأنظمة يصبح غير فعال الاّ في حالة نقل الفايروس للغير وهو يحتوي على ٣ وحدات او أجزاء :

١. الوحدة التي تنفذ كافة الأعمال التخريبية الخبيثة

٢. الوحدة التي تنسخ الفايروس تلقائياً وتعمل على إنتشاره

٣. الوحدة التي تكون مسؤولة عن إخفاء الملفات والعمليات الخبيثة بواسطة (Rootkit) وتعمل هذه الوحدات المكونة لهذا الفايروس كلها وفق نظام يعرف (Zero-Day).

يعمل هذا الفايروس على مرحلتين، الأولى : مرحلة السيطرة على نظام التحكم الموجود في أجهزة القيادة والسيطرة في المنشأة والمرحلة الثانية : إستخدام الحواسيب المربوطة بهذه الأنظمة للدخول في نظام SCADA اعتبر من أشهر الهجمات الطويلة الأمد، ينبغي الذكر أن ايران بعد هذا الهجوم قامت بتغيير

ما يقارب ١٠٪ من أجهزة الطرد المركزية في محطة نطنز(Natanz Nuclear Facility)من أصل ٩٠٠٠ جهاز وجميع الشلالات في أجهزة الطرد المركزية [٤١].

- عام ٢٠٠٧ تعرضت استونيا الى هجوم سيبراني مستقل بذاته موجه من روسيا الإتحادية بحيث استخدمت فيه هذه الاخيرة هجمات الحرمان او الإنكار من الخدمة (DDOS -Services Distributed Denial of) عن طريق إغراق المواقع الالكترونية بسيل من البيانات غير اللازمة التي يتم إرسالها من قبل المخترقين والقراصنة لمهاجمة شبكة الانترنت عن بعد، بإرسال تلك البيانات الى مواقع بشكل كثيف يسبب في تعطيل عمل النظام او يسبب زخماً في تلك المواقع، الذي يؤدي الى صعوبة وصول المستخدمين لها والى زيادة حركة مرور البيانات في الانترنت من ٢٠٠٠٠حزمة الى أكثر من ٤ ملايين حزمة في الثانية الواحدة وقد كانت المواقع الحكومية، الصحف والجامعات، المصارف، خدمات الإطفاء والإسعاف ضحية لهذه الهجمات المنسقة بهدف اسقاط الحكومة الاستونية وشلها، إستمرت هذه الهجمات الى عدة اسابيع وتسببت بأعمال شغب وإضطرابات جماعية أدت الى الأضرار في الممتلكات وقتل شخص وإصابة أكثر من ١٥٠شخص ويعتبر هذا الهجوم أبرز مثال على مشاركة متطوعون غير عسكريين في هجمات من هذا القبيل والذين شاركوا كميليشيات أو أفراد [٤٢] .

أخيراً تم إستهداف القطاع الصحي والنقل والبنية التحتية للإتصالات في جميع أنحاء العام من خلال ما يسمى وانكراي رانسوموار عام ٢٠١٧ مما دفع روسيا الى إلقاء اللوم على الولايات المتحدة لإبتكارها برمجية Exploit القادرة على تفعيل برامج وانكراي رانسوموار (سوف يتم تفصيله لاحقاً).

إنتهينا من تبيان نشأة الهجمات السيبرانية في الفرع الأول سوف ننتقل الى توضيح أبرز خصائص الهجوم السيبراني بإعتباره جريمة سيبرانية عابررة للحدود في الفرع الثاني.

الفرع الثاني: الهجوم السيبراني جريمة عابرة للحدود

نتيجة التقدم العلمي الذي شهده العالم، زاد إنتشار وتوسع الجرائم المنظمة العابرة للحدود وخاصةً الإلكترونية والإفتراضية منها، هذه الأخيرة أصبحت الشغل الشاغل لدى الدول وذلك بسبب مخاطرها المحدقة كالتجسس الالكتروني وسرقة البيانات المالية والشخصية وإستخدامها في أعمال إجرامية، الإبتزاز الإلكتروني والهجمات التي تحصل في الفضاء السيبراني والتي تعتبر موضوع بحثنا الحالي وغيرها من الجرائم .

مرتكبوا هذه الجرائم يستغلون أجهزة الكمبيوتر عبر برامج خبيثة تؤدي الى إتلاف هذه الأجهزة أو ايقافها عن العمل والحصول على المعلومات التي بداخلها أو حذفها أو سرقتها وأحياناً منع الشركة التي تقدم خدمة برمجية معينة من الوصول الى عملائها أو ايقاف الخدمات التي تقدمها .

عرّف المؤتمر العاشر للأمم المتحدة لمنع الجريمة ومعاملة المجرمين عام ٢٠٠٠ الجريمة المنظمة : " يقصد بتعبير جماعة إجرامية منظمة ذات هيكل تنظيمي مؤلف من ثلاث أشخاص أو أكثر موجودة لفترة من

---

[٤١] Michael Gervais : CyberAttacks and the Laws of War , Berkeley journal of International .Law,vol30, issue2,Article 6, 2012, p46

[٤٢] علي كاظم الموسوي، مرجع سابق، ص ٣٥-٣٦

الزمن وتعمل بصورة متضافرة بهدف إرتكاب واحدة أو أكثر من الجرائم الخطيرة أو الأفعال المجرمة وفقاً لهذه الاتفاقية من أجل الحصول بشكل مباشر أو غير مباشر على منفعة مالية أو منفعة مادية أخرى "، كذلك اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام ٢٠٠٠ التي تسمى أيضاً بإتفاقية *باليرمو* عرفت الجريمة المنظمة العابرة للحدود في المادة (المادة ٢ (أ))، "الجماعة الإجرامية المنظمة" باستخدام المعايير الأربعة التالية:

١ -جماعة ذات هيكل تنظيمي، مؤلفة من ثلاثة أشخاص أو أكثر؛

٢ -موجودة لفترة من الزمن؛

٣ -تعمل بصورة متضافرة بهدف ارتكاب واحدة أو أكثر من الجرائم الخطيرة؛

٤- تحصل، بشكل مباشر أو غير مباشر، على منفعة مالية أو منفعة مادية أخرى.

ولكن ما علاقة الجريمة المنظمة العابرة للحدود بالهجمات السيبرانية ؟ وكيف يمكن تكييف هذه الهجمات في ظل التعريف الوارد أعلاه ؟

بعد معالجتنا للهجمات السيبرانية يمكن أن تستنتج وجود نوعان منها :

النوع الأول هي مجموعة الهجمات السيبرانية التي يتم تنفيذها من قبل فرد أم عدة أفراد وذلك من أجل إحداث خلل أم ضرر في أنظمة المعلومات التابعة للخصم أو من أجل الحصول على البيانات التي تحتويها بقصد اتلافها أو تدميرها أم استخدامها في أساليب ملتوية أو الحصول على منفعة معينة، بمعنى آخر أن هذه الهجمات ليس بالضرورة أن يكون لها آي هدف في إلحاق أضرار مادية جسيمة في الأرواح والممتلكات أي انه ليس بالضرورة أن ترتقي الى مستوى النزاع المسلح، أما النوع الثاني هي الهجمات التي تلحق أضرار في جسيمة في البنى التحتية للدولة أو في المؤسسات العامة والخاصة وتؤدي الى وفيات وخسائر مادية خطيرة أي أنها تعتبر بمثابة هجوم مسلح، فيمكن تطبيق التعريف الوارد أعلاه على النوع الأول من الهجمات وسوف نبين اسبابه كالتالي :

١. ان الجريمة المنظمة هي جريمة عابرة للحدود: أي أنها تتخطى حدود الدولة الواحدة وتتأثر بها الدول معينة بهذه الجريمة، أما بالنسبة للهجمات السيبرانية تكون هي جريمة عابرة للحدود الوطنية وذلك مثلاً عند وجود كل جاني في بلد مختلف عن الآخر ولكن جميعهم خططوا للهجوم نفسه مما يأدي الى إعتبار أن كل دولة مختصة للنظر بهذا الجرم وذلك بسبب إنطلاق الهجوم منها أم تحقق النتيجة فيها، فالهجوم لم يبقى محصوراً ضمن دولة واحدة بل تخطى الحدود مما يتوافق هذا الأمر مع الخاصية الأولى للجريمة المنظمة .

٢.لناحية تعدد الجناة : سواء في الجريمة المنظمة أم في الهجمات السيبرانية فان تعدد الجناة يعني أن مجموعة من المجرمين إتفقوا على إرتكاب جريمة معينة ولم ينفرد اي منهم في إرتكابها، فمن الصعب تصور جريمة منظمة إرتكبت من قبل شخص واحد والأمر نفسه بالنسبة للهجوم السيبراني في بعض الحالات وذلك عندما يقرر مجموعة من الهاكرز مثلاً على توجيه هجمات سيبرانية الى جهة معينة أو توجيه بعض عناصر القوات المسلحة هجوم سيبراني الى دولة معادية متجاوزين بذلك الصلاحيات المعطاة لهم وخالفوا قواعد القانون الدولي الانساني وذلك مقابل المال، مما يعتبر الشرط الثاني محققاً .

٣.التخطيط الجرمي : يعتبر التخطيط من أهم الوسائل لإرتكاب الجرائم المنظمة العابرة للحدود كما الهجمات السيبرانية وذلك عن طريق تحديد الوسائل اللازمة لإرتكاب الجرم كتحضيرالبرمجيات والفيروسات الخبيثة أي تهيئة الأرضية لحسن ارتكاب الجرم وفي حال تعدد الجناة يكون لكل منهم دوره في هذا التخطيط عبر توزيع الأدوار فيما بينهم .

٤. الغاية من ارتكاب الجرم : بالنسبة الى الجرائم المنظمة يكون الربح المادي هو الهدف الأساسي من وراءه أما بالنسبة الى الهجمات السيبرانية قد لا يكون الهدف دائماً هو تحقيق غاية مادية ام مالية بل أحياناً يكون من أجل الحاق أضرار بالخصم عن طريق الحصول على معلومات مهمة بهدف التصرف بها بأي شكل كان أو إستهداف مرافق عامة للدولة وغيرها من الغايات التي تختلف بإختلاف الباعث .

اذاً يمكننا أن نستنتج من ما تقدم أن الهجمات السيبرانية كي تعد جريمة منظمة عابرة للحدود لا بدّ من توافر شروط معينة (تعدد الجناة , تحقيق ربح مادي, أن يتخطى الجرم حدود الدولة الواحدة، التخطيط الجرمي، الإستعانة بوسائل العنف والفساد للوصول الى الهدف) وذلك لأن ليس أي هجوم سيبراني يوجه هو جريمة منظمة بل في حالات كثيرة لا يمكن إعتباره كذلك ومن أجل تصنيف عما اذا كان الهجوم السيبراني هو جريمة منظمة أم لا، لا بدّ من العودة الى الخصائص المميزة لكل من الجريمتين والتأكد من توافرهم في الحالة المستجدة أي بمعنى أخر إن تكييف الهجمات السيبرانية كجريمة منظمة عابرة للحدود وجب تحليل كل حالة على حدة والتأكد من توافر كافة الشروط اللازمة.

لقد إنتهينا في الفصل الأول من الباب الحالي سوف ننتقل الى البحث في ماهية المعلومات الإلكترونية المعتدى عليها سيبرانياً في الفصل الثاني.

الفصل الثاني : الإعتداء على المعلومات

سبق وفصلنا بالشكل الصحيح ماهية الهجمات السيبرانية التي يستخدمها المهاجم للحصول على المعلومات المخزنة داخل الحاسب الآلي من أجل إتلافها او تدميرها ام إستخدامها بالشكل الذي يلحق الاضرار بالبنى التحتية للفضاء السيبراني، اذاً هذه الهجمات ترتكب في مجال المعالجة الالكترونية للبيانات، فالهدف الأساسي لدى المهاجم ليس الحاسوب كقيمة مادية من أجل إلحاق أضرارمادية به بل على المعلومات المتوافرة ضمنه باعتبارها هي محل الإعتداء، ومن أجل تحديد التكييف القانوني الصحيح للهجوم السيبراني لا بدً من التطرق الى ماهية المعلومات التي يقع عليها هذا الاعتداء ومدى أهميتها في المبحث الأول من هذا الفصل،والتطبيق العملي لهذه الهجمات في المبحث الثاني.

المبحث الأول : ماهية المعلومات

في هذا المبحث سوف نلقي الضوء على ماهية المعلومات التي من الممكن الإعتداء عليها سيبرانياً والى أي مدى يمكن حمايتها قانوناً من أي إعتداء يلحق الأضرار بها، ففي الفرع الأول سوف نحدد ماهية هذه المعلومات وفي الفرع الثاني سف نبين كيفية حماية هذه المعلومات من المخاطر .

الفرع الأول : تحديد المعلومات المعتدى عليها سيبرانياً

تعتبر المعلومات أنها مجموعة من الرموز أو الحقائق أو المفاهيم او التعليمات التي تصلح لأن تكون محلاً لتبادل او إتصال او للتفسيروالتأويل او للمعالجة سواء بواسطة الأفراد او الانظمة الإلكترونية وهي تتميز بالمرونة بحيث يمكن تغييرها، وتجزئتها وجمعها أو نقلها بوسائل أو أشكال مختلفة [٤٣] أو انها تلك البيانات التي تمت معالجتها لتحقيق هدف معين أو لإستعمال محدد لأغراض إتخاذ القرارات، أي تلك التي أصبح لها قيمة بعد تحليلها وتفسيرها أو تجميعها في شكل معين، والتي يمكن تداولها وتسجيلها ونشرها وتوزيعها في صورة رسمية في أي شكل، فالمعلومات هي مجموعة من البيانات التي تختص بمجال علمي معين وتهدف الى زيادة المعرفة لدى الإنسان، فهي معرفة مكتسبة من خلال البحث أو القراءة وما شابه ذلك من وسائل إكتساب المعلومات والحصول عليها.

أربعة ركائز أساسية للمعلومة كالتالي :

- من حيث النوع : تختلف المعلومة من حيث النوع فقد تكون نوع من الأوامر او الإرشادات، تتمثل في رسم هندسي أو ذات طبيعة فنية او أدبية او علمية وفي هذا الصدد نعتبر ان تكنولوجيا المعلومات من أهم الأنواع في المعلومات وعرفت على أنها "التقنيات الإلكترونية والرقمية التي تستخدم في تخزين ومعالجة و تناقل وبث نتائج عمليات تحليل وتصنيف وإستخلاص المعلومات وتوجيه الإفادة منها من قبل المستفيدين بأيسر السبل مع السرعة و الدقة "، المعلومات في هذه الحالة والتي تتخذ شكل برامج للحاسب الالي " Software " تعطي التعليمات اللازمة لتشغيل الحاسب لقيامه بالعمليات المطلوبة منه، هذه البرامج إعتبرت وسيلة مهمة لإرتكاب الجرائم المعلوماتية . [٤٤]

من الخصائص التكميلية للمعلومات التي تساعد في الوقوف على طبيعتها والتعرف على نوع الحماية اللازمة لها يمكن تلخيصها كالتالي [٤٥]:

- مدى إتاحة المعلومة : اي مدى يمكن ان تكون المعلومة متاحة للجميع أم أنها محصورة بمجموعة من الأفراد، نشير أيضاً ان المعلومة وان كانت غير متاحة للجميع وتم نشرها عبر الإنترنت فان هذا الحصر يتم ايضاً ويخصص فقط للأفراد المسموح لهم بالولوج الى الصفحة المخصصة عبر وضعهم لكلمة السر وهكذا تكون المعلومة غير مخصصة للجميع سواء كانت منشورة عبرالإنترنت أم في مجلة معينة تهتم بموضوع معين يختص بفئة معينة .

- حيازة المعلومة : بتحديد مالكها وحائزها ومن يسيطرعليها

---

[٤٣] شيخة حسين الزهراني " مواجهة القانون الدولي للهجوم الالكتروني (السيبراني)" , طبعة ٢٠٢١, " دار النهضة العربية, ص ٤٩

[٤٤] نائلة عادل محمد فريد القورة , مرجع سابق , ص ٦
https://elearn.univ-oran1.dz/pluginfile.php/73801/course/overviewfiles/%D8%A7%D9%84%D8%AF%D8%B1%D8%B3%20%D8%A7%D9%84%D8%A7%D9%88%D9%84.docx?forcedownload=1

[٤٥] " طارق ابراهيم الدسوقي عطية :" الاحتلال و أثره على حقوق الانسان، دراسة تطبيقية على الاحتلال الأميريكي - البريطاني للعراق" طبعة ٢٠٠٥، دار النهضة العربية، مصر، ص ٥٨-٥٩

- قيمة المعلومة من حيث الزمان : وذلك من خلال تحديد ما اذا كان للمعلومة قيمة في وقت معين وهل تتناقص القيمة أو تنتهي مع الوقت .

- الأثر التي تتمع به المعلومة ويتوقف ذلك على تحديد التأثير الذي يحدثه معرفة المعلومة أو حيازتها أو إستعمالها .

- المكان التي توجد فيه المعلومة

- الوسائل أو الأساليب التي يتم إتخاذها لحماية المعلومة

- مقدار ما تتمتع به المعلومة من الصحة والمصداقية

في الفرع الثاني من هذا المبحث سوف نحدد أهمية توفير الحماية القانونية للمعلومات الإلكترونية.

الفرع الثاني : شروط توفير الحماية القانونية للمعلومات الإلكترونية

لا بدَ أن تتوافر في المعلومات شروط معينة كي تحميها النصوص القانونية وعلى هذا الأساس سوف نستعرض هذه الشروط فيما يلي :

- أن تكون المعلومة محددة بذاتها :

الإعتداء في الهجوم السيبراني لا بد أن يكون واقعاً على معلومة محددة ومبتكرة بذاتها وغير متاحة للجميع، فالمعلومة التي تكون متاحة للعامة لا يمكن ان تكون بحسب رأينا محل اعتداء أي أنها غير منسوبة لشخص معين أم فئة ام طائفة محددة بل يمكن للجميع الحصول عليها افتراضياً ام مادياَ، فتكون محصورة بموضوع معين ومبتكرة الإستلاء عليها قد يلحق الأضرار بمالكها وإذا كانت غير محددة لا يمكن أن تكون حقيقية وخاصة المعلومات التي تتخذ شكل التعليمات في مجال تكنولوجيا الحاسبات الالية، فالمعلومات هنا تتخذ شكل برامج للحاسب الالي والتي تتضاعف نسبة التعرض لهذه البرامج من خلال الجرائم المعلوماتية التي يتم التلاعب بها وتغييرها مما يحتم حمايتها قانوناً، بالنسبة الى خصائص المعلومات يمكن تحديدها وفقاً للآتي:[٤٦]

- سرية المعلومة :

المعلومة كي تكون محمية قانوناً يجب أن تكون سرية وغير متاحة للكل والمساس بها يشكل اعتداءً قانونياً أي أنها تعود لشخص أو لمجموعة معينة من الأشخاص إستأثروا بها ومن حيث طبيعتها تستمد خاصية السرية، فالمعلومة التي يتم نشرها والتي تتعلق بحقيقة معينة متاحة للجمهور دون أي تحديد لا يمكن أن تعتبر أن الحصول عليها يشكل اعتداءً، بل إن المعلومات الموجودة في بطاقة الإئتمان ام تعود لمؤسسة معينة (تشدد هذه الأخيرة في ابقائها سرية) او أي معلومة يتم الكشف عنها يؤدي الى إلحاق الضرر بصاحبها (أن تكون ملك لهذا الأخير و يريد ابقائها سرية)عبر إظهارها للعلن أم الإستحواذ عليها او إتلافها او الحاق الضرر بها وهنا تظهر صفة الاستئثار بالمعلومة.

[٤٦] طارق ابراهيم الدسوقي، مرجع سابق، ص ٤٤

ولكن ما هي الطبيعة القانونية للمعلومات وخصوصاً تلك التي يقع عليها الاعتداء السيبراني؟

إعتبر الفقه الفرنسي من خلال كل من Pierre Catalaو Michel Vivant أن المعلومة هي من قبيل المال للحيازة بوجود علاقة قانونية قائمة وهي علاقة المالك بالشيئ الذي يملكه، بسبب علاقة التبني التي تربط بينهما عبر استنادهم الى حجتين الأولى : هي أن فكرة الشيئ أو المال الذي يغلب عليه الطابع المعنوي وان صفة محل الحق يجوز ان تستند الى مال معنوي بحيث يكون هذا المال من قبيل الأموال الاقتصادية، وانه جدير بالحماية القانونية، أما الحجة الثانية هي ان كل الاشياء المملوكة ملكية معنوية ترتكز على الإقرار بأن للمعلومة قيمة عندما نكون بصدد براءة اختراع أو علامات أو رسومات أو نماذج ،يعترف بحق المؤلف والفرد الذي يقدم للجماعة معلومة خاصته او فكرة أو شكل معين ويجب أن يعامل على انها مالاً وتصبح محلاً للحق، فلا يوجد ما يسمى بالملكية المعنوية بدون الإعتراف بالقيمة المعلوماتية [٤٧]، إذاً أن المعلومة التي لا بدَ أن تتمتع بالحماية القانونية خاصةً تلك التي يقدمها الفرد الى العلن بشرط أن تكون خاصته، مبتكرة، مميزة وخاصة، هذا الذي يجعل أي إعتداء يقع عليها معاقب عليه قانونياً وفقاً للنصوص المرعية الإجراء.

في إطار المعلومات التي تعتبر محل إعتداء في الهجمات السيبرانية هي منوعة وكثيرة، فالفاعل هنا يريد الإستلاء على معلومات أو بيانات تخص الغير دون إذنه وذلك بهدف إلحاق الأضرار به أو بالمنشأة التي ينتمي اليها أو بهدف إتلافها أو إخراجها الى العلن بعد ان كان المجني عليه يريد إبقائها سرية وحتى بالسعي الى تحقيق الأرباح من هذه المعلومات بطريقة غير شرعية أو حتى بالحصول على المعلومات الإقتصادية أو المالية المملوكة من قبل مرفق عام أم خاص وإلحاق الأضرار به وبالمستهلكين التابعين له، فالحصول على المعلومات السرية والشخصية الخاصة[٤٨] وإفشاءها أمر محرم دولياً، مثلاًعندما يريد الحصول على بيانات معينة بمرضى إحدى المستشفيات دون إذن صريح من المريض ومن المستشفى يعتبر فعلاً محظوراً، وذلك عن طريق توجيه هجوم سيبراني الى قاعدة المعلومات الإلكترونية الخاصة بالمستشفى للحصول عليها وأحياناً يكون الهجوم مفتك ويؤدي الى وفات مئات المرضى والأمر نفسه بالنسبة مثلاً الى إستهداف المواقع الالكترونية للمصارف، فالمهاجم هنا يستطيع تعطيل المرافق العامة و لبنوك وحتى يصل الأمر الى التحكم بالمنشآت العسكرية وإطلاق صواريخ الى هدف معين وإلحاق خسائر فادحة في الأموال والاشخاص، فحماية المعلومات أمرُ اساسيُ و ضروريُ في أي قانون محلي ودولي.

سوف ننتقل الى المبحث الثاني من أجل تبيان التطبيق العملي للهجمات السيبرانية.

---

[٤٧] عبد الله حسين علي محمود : " سرقة المعلومات المخزنة في الحاسب الالي "، الطبعة الاولى، ٢٠٠٠، دار النهضة العربية، ص ١٦٩-١٧٠-١٧١

[48] Article 9/1 states: Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

المبحث الثاني : التأطير العملي للهجمات السيبرانية

في المبحث الحالي سوف نبين الأشكال والأنواع المختلفة للفيروسات والبرمجيات الخبيثة المستخدمة في إطار الهجمات السيبرانية(الفرع الأول) ومحاولين تحديد مصدر هذه الهجمات (الفرع الثاني) .

الفرع الأول : البرمجيات والفيروسات الخبيثة

تختلف طرائق الهجمات السيبرانية بإختلاف هدف المهاجم منها، بعد أن اصبحت هذه الهجمات في هذا الزمن معقدة وخطيرة الى حدَ ما، لا تقل أهمية من القدرة العسكرية وحتى النووية للدول، بحيث يمكنها إختراق المنشآت والقاذفات النووية والقواعد العسكرية وتعطيلها أو التحكم بها، وكانت معظم هذه الهجمات سابقاً تشن سابقاً من قبل أشخاص أو مبرمجين لأهداف شخصية، ولكن في العقدين الاخرين دخلت المنظمات الأمنية و الحكومية الى الساحة وأخذت تنفق الملايين لتطوير قدراتها وبناء جيوش ألكترونية للدفاع عن منشآتها وشن هجمات مضادة نحو الدولة المعتدية، ففي هذا الفرع سوف نبين أبرز الأساليب و الطرائق السيبرانية، على الشكل التالي :

البرمجيات الخبيثة (Malware) :

هو مصطلح شامل لمجموعة متنوعة من التهديدات السيبرانية، وهي عبارة عن برمجيات يتم برمجتها لإستهداف وظائف الحاسوب وتدميره وسرقة بياناته أو إستهداف نظم الحماية فيه، فهي تسبب بطئ في عمل الجهاز بشكل غير اعتيادي و قبل الغوص في التفاصيل لا بد من توضيح المعنى , كلمة "البرمجيات الخبيثة (malicious) " هي اختصار لكلمة مال- (mal) المشتقة من الكلمة اللاتينية "mallus"تعني سيء- مهاجمة أو تدمير أو تغيير أو إتلاف الجهاز المضيف الذي تعمل عليه أو الشبكة التي يتصل بها هذا الجهاز، والمالوار هي برمجيات خطيرة تسبب زيادة في إستخدام المعالج بشكل مبالغ فيه، مما يسبب مشاكل في الإتصال بالإنترنت وتوقف مفاجئ لبعض البرامج[٤٩] .

هي على أنواع كثيرة : البرامج الموقوتة ,Ransomware, spyware , adware , viruses .

سوف يتم تفصيل كافة هذه الأنواع بالتفصيل، كالتالي :

*البرامج الموقوتة : تعرف بإسم الشفرة الموقوتة وهي نوع من أنواع البرامج الخبيثة صغيرة الحجم يتم إدخالها بطريقة غير قانونية وإخفائها مع البرامج الأخرى وهذه الأخيرة ليست ملفاً متكاملاً وإنما هي شفرة توضع ضمن مجموعة من الملفات وذلك عن طريق تقسيمها الى أجزاء متفرقة كي لا يمكن التعرف اليها،

[٤٩] روان زيدان : " البرمجيات الخبيثة: الدودة، وحصان طروادة، والبوت والفرق بينها" ،مقال منشور على موقع ناسا بالعربي، ٢٠١٧، ص ١ ، متوفر على الرابط التالي :

https://nasainarabic.net/main/articles/view/malicious-software-worms-trojans-and-bots-oh-my

فهي تتجمع فيما بينها بحسب الأمر المعطي لها في الزمان والمكان المعينين، هذه البرامج تستخدم لتدمير المعلومات والبيانات وتغيير برامج ومعلومات نظام الحاسوب.[٥٠]

-Ransomware أو برامج الفدية : هي عبارة عن هجوم إلكتروني يُستخدم لإبتزاز المستخدم وتحريضه على دفع المال، كان المجرمون في البداية يستخدمون رانسوم وير كوسيلة إبتزاز لجني الأموال من الأفراد الذين يريدون إسترداد معلوماتهم الشخصية، واليوم يستخدم المجرمون رانسوم وير كوسيلة إبتزاز لجني الأموال من الشركات التي تريد إسترداد معلوماتها الحساسة، بحيث أن هذا الهجوم يمنع المستخدم من الدخول الى معلوماته الشخصية أو النظام بمختلف أنواعه دون دفع ما يسمى " بالفدية "، وهنالك عدة طرق لإصابة الهاتف او الحاسوب ولكن من أكثر الطرق الشائعة : السبام (Spam) او ما يعرف أيضاً بإسم (Malspam) الذي يعمد الى إرسال بعض البرمجيات الخبيثة إلى المستخدم عبر البريد الإلكتروني، وربما يحتوي هذا الأخيرعلى بعض المرفقات المصابة مثل ملفات PDF على سبيل المثال، أو حتى ملفات Word الكتابية أو روابط خبيثة تحتوي على فيروس الفدية[٥١] .

لكن كيف يعمل رانسوموير ؟

- يقوم المستخدم بإستلام رسالة عبر البريد الالكتروني او إعلان في موقع مجاني لمشاهدة شيء فبمجرد النقر على الرابط او المرفق لتلك الرسالة يبدأ الهجوم فيتم تنزيل البرمجيات الخبيثة في جهاز الضحية عن طريق جهاز يسمى Crypto-Ransomware معين .

- يحصل كل ذلك بشكل خفي والمستخدم لا يعلم بشيء ويتم تشفير الملفات، وبعد الانتهاء من ذلك تظهر للمستخدم رسالة في المتصفح او على سطح المكتب تطلب منه استخدام متصفح التور للدفع بعملة البتكوين او غيرها وتحدد المهلة الممنوحة للضحية قبل حذف الملفات او نشرها للعلن (ان كانت سرية).

من أثاره :
- قفل الجهاز ومنع المستخدم من الدخول اليه حتى دفع الفدية المطلوبة.

- التحكم بجهاز الضحية عن بعد وجعله جهاز زومبي وإستخدامه في هذه الحالة للولوج الى أجهزة أخرى، (zombie computer) .

- يستهدف الشركات و الأفراد على حدَ سواء ويلحق بهم أضرار جسيمة.

- يستهدف المهاجمون البيانات على أساس أنها ثمينة و صاحبها سوف يدفع الأموال في سبيل استردادها أو دفع ما يسمى بالفدية .

---

[٥٠] عمار عباس الحسيني , مرجع سابق , ص ١٤٤- ١٤٢

[٥١] مقال بعنوان : "ما هو فيروس دفع الفِدية Ransomware؟ كيفية إزالته؟ أنواع برمجيات رانسوم وير ٢٠٢٢؟! " متوافر على الرابط التالي :

https://mohamedovic.com/ransomware/

* Adware :

برامج ادوير هي برامج معدة خصيصاً لعرض إعلانات إجبارية على الحاسوب أم الهواتف الذكية وتتم توجيه هذه الهجمات من خلال هذه الأخيرة والغرض منها هي إما تحقيق الربح المالي للمهاجم الذي وجه الإعلانات أو تسويق خدمات مزيفة ومهما كانت الطريقة المستخدمة في هذا الهجوم يبقى الهدف الأساسي منها جني الأرباح غير المشروعة.

* Viruses :

الفايروس هو برنامج مصمم يهدف الى إحداث أكبر عدد ممكن من الضرر للنظام بعد ربطه بالبرامج الاخرى، لديه القدرة على تكرار نفسه وكأنه يتكاثر ذاتياً وله القدرة على إستهداف البرامج الأخرى في الحاسب ومواقع أخرى في الذاكرة بهدف تدميرها، يعمد المهاجم الى تحديد الزمان و المكان الذي سوف ينتشر بها وغالباً يعطى الفيروس الوقت الكافي للإنتشار دون لفت الإنتباه .

بعد أن ينشط الفيروس يقوم بعدة أنشطة تخريبية حسب الغرض من إنشاءه، فهنالك من يقوم بعرض رسالة تحذيرية عن إمتلاء الذاكرة وهناك أنواع أخرى تقوم بحذف أو تعديل بعض الملفات وهناك من يقوم بتكرار ونسخ نفسه حتى يشل الجهازتماما أما الأنواع الأشد فتكاً تقوم بمسح كافة المعلومات الخاصة بالضحية، من خصائص هذه الفيروسات أنها سريعة الانتشار، قدرتها التدميرية وخاصية الإختفاء التي تتميز بها .[٥٢] الفيروسيات هي على ستة أنواع[٥٣] :

١- فيروسات تعمل عند بدء التشغيل Virus Sector Boot : يتميز هذا النوع أنه مرتبط بالبرامج المختصة بالتشغيل، يقوم هذا النوع من الفيروسات بالتسلل إلى القطاع الخاص ببرنامج الإقلاع على القرص Sector Boot وإتالف محتوياته والعبث بها، ما يؤدي إلى تعطل عملية الاقلاع الخاصة بالجهاز.

٢- فيروس الملفات File Infector Virus : يهاجم هذا النوع نظام التشغيل، وأي برامج أخرى موجودة على الكمبيوتر، وغيرها ويعمل على العب بمحتويات الملفات التي تنتهي بامتداد.exe, sys com, bin

٣- المايكروفايروسMicro-virus : تصيب البرامج التطبيقية مثل مايكروسوفت ورد وواكسيل وهذه الفيروسات من أكثر الأنواع التي تصيب التطبيقات.

---

[٥٢] عمار عباس الحسيني " جرائم الحاسوب والإنترنت (الجرائم المعلوماتية)، الطبعة الأولى، منشورات زين الحقوقية، ٢٠١٧ , ص ١٤٠-١٤٢

[53] https://e3arabi.com/technology/%D8%A3%D9%86%D9%88%D8%A7%D8%B9-%D9%81%D9%8A%D8%B1%D9%88%D8%B3%D8%A7%D8%AA-%D8%A7%D9%84%D9%83%D9%85%D8%A8%D9%8A%D9%88%D8%AA%D8%B1/

٤- فيروس الروتكيت Rootkit virus : ما يميز هذا الفيروس أنّه يُصيب جهاز الحاسوب ويقوم بالسيطرة والتحكم دون علم مستخدم الجهاز به، وتتمحور طريقة عمله بأن الهاكر يقوم بالوصول إلى ملفات(Log File) ، أي ملفات السجلات وذلك للتجسس على نشاطات مستخدم الجهاز، ويقوم مباشرة بتعديل إعدادات النظام الأساسية؛ عن طريق إدخال برامج أساسية على الجهاز لفرض السيطرة على نظام التشغيل، فتعمل إمّا على تعطيله أو تعديل الوظائف والبرامج الأساسية في الجهاز، إلا أنّه يصعب إكتشافه من قبل البرامج المضادة للفيروسات.

٥-.فيروس التنفيذ المباشر Direct Action Virus : هو الفيروس الذي يبقى في ذاكرة الحاسوب دون أن يؤثر عليه ويسمى بالفيروس لغير مقيم.

٦- الفيروس المتحول Polymorphic Virus : هو فيروس متعدد الأشكال يقوم بتغيير نفسه وتغييرالكود الخاص به بشكل مستمر من أجل التمويه، وعلى تشفير محتوياته حتى لا يتم معرفته واكتشافه من خلال البرامج المضادة للفيروسات، لذلك يصعب إزالته، وإذا تم اكتشافه من قبل هذه البرامج فيقوم بتغيير شكله وتغيير الكود الخاص به، وكذلك يغير من شكل الكود دون المساس بوظائف وصفات البرنامج الاساسية.

٧- برامج الدودة Worms

برامج الدودة هي البرامج التي تستفيد من الثغرات الموجودة في نظام تشغيل الحاسوب للإنتقال من كومبيوتر الى آخر، مما يؤدي الى إختلال الشبكة بالكامل والتسبب في النهاية بآثار مدمرة بفضل الوصلات التي تربط الشبكات ببعضها البعض، يمكنهم الإنتقال من حاسوب الى آخر عبر التكاثر، ومن أهداف هذه البرامج شغل أكبر عدد ممكن من سعة الشبكة و من ثم تقليل أو خفض كفاءتها، هذه الديدان تصيب مرفقات البريد الالكتروني والتنزيلات التلقائية عند زيارة بعض المواقع الإنترنت والتسلل عبرالثغرات الأمنية في أنظمة التشغيل أو برامج الحماية كما أنها تتيح للمهاجم ان يستخدم الكمبيوتر المصاب لمهاجمة مواقع الإنترنت او إرسال بريد الكتروني أو تنزيل برامج ضارة به .

*برامج التجسس : Spyware

برامج التجسس هي عبارة عن الدخول الغير مصرح به الى الحاسوب العائد الى شركة ما ام فرد والهدف منها إلحاق الأضرار بهذه المعلومات اما بقصد إتلافها و تدميرها أو تسريبها مثلاً الى شركة منافسة، فالهدف والوسيلة غير مشروعين، وأيضاً عبر إلتقاط المعلومات الخاصة بالحسابات المصرفية والإئتمانية وسرقة هوية العملاء الشخصية وتوظيفها لأغراض غير قانونية والسعي الى مراقبة حسابات العملاء ومحاولة سرقة كلمة المرور ومعلومات تسجيل الدخول، وأهم نوع ما يسمى بحصان طروادة Trojan horse، هذا النوع من برامج التجسس يتنكر على أنه برنامج شرعي عن طريق ظهورإشارة على أنها تحديث ل flash player , java وغيرهم وذلك بهدف التجسس على المستخدمين أو سرقة البيانات الحساسة للأفراد أو الشركات، وسمي بحصان طروادة نظراً لطريقة دخوله، فهو يستخدم الهندسة الإجتماعية لإخفاء التعليمات الضارة البرمجية داخل البرامج الشرعية، فهو لا يعمل من تلقاء نفسه أو يتكاثر كالفيروسات الأخرى وإنما لا بدّ تحميل ملف قابل للتنفيذ exe وتثبيت برنامج حصان طروادة الضار.

من آثار هذا البرنامج : إمكانية إنتقاله من جهاز الى آخر والتجسس على معلومات حساسة للمستخدمين، وأخيراً لا يتأثر الجهاز ويكمل عمله بشكل طبيعي حتى يقوم المستخدم بتصرف معين يظهر بهذا الفيروس

الى العلن مثلاً : يكون الهدف هو إختراق والتجسس على حساب مصرفي يعود لأحد المستخدمين، ينتظر حصان طروادة حتى يدخل العميل الى الحساب المصرف الكترونياً كي يقوم باختراقه.

التصيد أو الخداع الإلكتروني : Phishing

هجمات التصيد الاحتيالي : هي رسائل إلكترونية تصل الى المستخدمين تدفعهم الى إجراء تصرف معين : اما مشاركة معلوماتهم الشخصية اما تنزيل برامج ضارة فيتم ارسال هذه الهجمات عبر البريد الإكتروني وتطلب من المستخدمين النقر على الرابط وإدخال بياناتهم الشخصية كالإسم الثلاثي، رقم الهوية، رقم البطاقة المصرفية .. ، من أجل الاستلاء على الأموال الموجودة داخلها أو القيام بعمليات إحتيالية شرائية مما يصعب على المستخدمين التمييز بين واجهات المواقع الحقيقية من الواجهات المزيفة، وتجدرالاشارة الى أن رسائل التصيد الاحتيالي غالباً ما تذهب الى قسم الرسائل الالكترونية غير المرغوب بها (Spam Junk or).

-هجمات الحرمان من الخدمة (DDoS _ Distributed Denial of Service) :

الهدف الأساسي للفاعل في هذا النوع من الهجوم هو حجب الخدمة فلا يكون الهدف مثل البرمجيات الضارة الأخرى كسرقة المعلومات الشخصية أو الخرق والتجسس وإنما يتم هذا الهجوم عبر إرسال كميات كبيرة من البيانات الى الشبكة المستهدفة (اي اجراء الكثير من طلبات الاتصال)، تخضع موارد الشبكة عامةً الى حدود معينة من الطلبات التي تؤدي الى ايقاف الخدمة متى تجاوز عدد الطلبات القدرة التي يمكن للشبكة أن تستوعبها، أي تتجاوز قدرة الويب على حل ومعالجة كافة الطلبات المرسلة، مما يؤدي الى عدم الاستجابة للطلبات الحقيقية للزبائن، مما يؤدي الى خسارة كبيرة للمؤسسة ومنعها من العمل بشكل صحيح .

عند إرسال عدد كبير للغاية من الطلبات إلى المورد الضحية، سيقوم المجرم الإلكتروني غالبًا بإنشاء "شبكة زومبي" من الحواسيب التي أصابها ويسيطر على إجراءات كل حاسوب مصاب في شبكة الزومبي، يمكن أن يكون حجم الضرر الذي يلحقه الهجوم بموارد شبكة الضحية هائلاً.[٥٤] ويكون الحل في حال الإصابة هو إستخدام برمجيات الجدار الناري الخاص كتطبيقاتWeb Application Firewall أو شراء أنظمة حماية مخصصة تكون عبارة عن Hardware يتم ربطه بالشبكة،وإستخدام أنظمة توزيع الضغط Load Balancer Cluster وأخيراً شراء خدمة الحماية من هجمات DDoS المتوفرة على الإنترنت .

- هجوم الوسيط أو الرجل في الوسط (Man in the Middle) :

هذا النوع من الهجوم يتم من خلال مهاجمًا يدخل نفسه بين طرفين يتواصلان مع بعضهما البعض، حيث أن هجمات الرجل في الوسط هي في الأساس هجمات تنصت، أي يتظاهر على أنه مشارك شرعي في هذه العملية، يتيح ذلك للمهاجم إعتراض المعلومات والبيانات من أي طرف أثناء إرسال روابط ضارة أو معلومات أخرى إلى كل من المشاركين الشرعيين بطريقة قد لا يتم اكتشافها إلا بعد فوات الأوان، في هجوم الرجل في الوسط، يتلاعب المشارك الأوسط بالمحادثة بين المستخدم الأول والثاني، حيث يعمل على سرقة المعلومات السرية وإلحاق الضرر، مثلاً في حال أرسل للمستخدم بريداً إلكترونياً تبين أنه من البنك الذي يتعامل معه، يطلب منه أن يدخل الى الرابط المرفق و تسجيل معلومات خاصة، فللوهلة الأولى يتضح للمستخدم أنه الحساب الرسمي

---

[٥٤] مقال بعنوان : " ما هي هجمات DDoS؟ " , ص ١ , متوافرعلى الرابط التالي :
https://me.kaspersky.com/resource-center/threats/ddos-attacks

للبنك (لان المهاجم أنشأ حساباً وهمياً للبنك)، ففي هذه الحالة يتم تسليم المهاجم المعلومات الخاصة وبالتالي تمت المهمة بنجاح، وهذه المعلومات التي حصل عليها المهاجم يمكن أن يستخدمها لاحقاً في الموقع الحقيقي للبنك للوصول الى معلومات الضحية و نكون في هذه الحالة أمام : إعتراض البيانات، الحالة الثانية هي سرقة المعلومات من خلال انتحال عنوانIP ، يمكن للمهاجم أن يخدعك للاعتقاد بأنك تتفاعل مع موقع ويب أو مع شخص ما وهو ليس كذلك، وربما يمنح المهاجم إمكانية الوصول إلى المعلومات التي لم تشاركها وجني الأموال عندما يستخدم الطريقة نفسها في الحالة الأولى للدخول الى الحساب الأساسي للعميل والقيام بعمليات شرائية أم سحب او تحويل أموال منه.

هناك أربعة أنواع من هجوم الوسيط [٥٥] : إنتحال عنوان IP ، إنتحال DNS ، إنتحال HTTPS ،إختطاف SS

- هجمات حقن قواعد البيانات SQL Injection :

يعتمد على إرسال المهاجم جمل نصية برمجية الى قواعد البيانات من خلال التطبيقات وصفحات المواقع الإلكترونية المتصلة بها وبالتالي تسمح للمهاجم بحقن كود غريب في قواعد البيانات وذلك للتغيير في الكواد البرمجية، بعبارة أخرى ان المهاجم يستهدف القواعد الخاصة بالضحية عبر اختراقها وحقن كود معين يؤدي الى تغيير في النظام الخاص بها، ومن أجل تجنب هجمات حقن قواعد البيانات يجب على المبرمج القيام بعمليات الفلترة للمدخلات التي سوف يتعامل معها النظام كمثال على ذلك: أن يتم التأكد من مدخلات المستخدم عن طريق تحديد نوع البيانات المدخلة إضافة الى إستخدام الجدار الناري المخصص للحماية من هذه الهجمات [٥٦].

أخيراً بعد معالجة مفصلة في هذا الفرع لأنواع الهجمات الالكترونية وأهميتها وأسلوبها في إختراق وتجاوز الأنظمة وقواعد البيانات المعقدة لا بدَ من التوضيح أن أساليب الوقاية والحماية كثيرةٌ وعلى الأفراد والشركات والمؤسسات العامة والخاصة الإلتزام بالتحديث الدوري للبرامج والتطبيقات الموجودة على الأجهزة.

سوف ننتقل الى الفرع الثاني من هذا المبحث في محاولة تحديد مصدر الهجمات السيبرانية .

الفرع الثاني : في محاولة تحديد مصدر الهجمات السيبرانية

تتميز الهجمات السيبرانية بطبيعة خاصة لناحية خصائصها الفريدة من نوعها، فبيئة الهجمات السيبرانية بيئة غير تقليدية تقع خارج الإطار الواقعي الملموس، فهو واقعاً افتراضياً يجعل الأمر معقداً نوعاً ما وخاصةً على الأجهزة المختصة في القيام بإجراءات التحقيق والملاحقة [٥٧] ، بالإضافة الى ذلك نحن أمام مجموعة من الخصائص التي تميز الهجوم السيبراني عن غيره من الجرائم لناحية أسلوب إرتكاب الجرم وصفته العابرة للحدود (في أغلب الأحيان) وصعوبة اثباته وغيرها من الصفات التي سوف نتطرق اليها في هذا الفرع ونضيف أن هذه الخصائص تجعلنا غير قادرين على تحديد هوية الفاعل من أجل معاقبته بل يكون من

---

[٥٥] مقال بعنوان : " ما هو هجوم الوسيط أو الرجل في الوسط Man-In-The-Middle Attack؟ " ، ١٣-٣-٢٠٢٢

[٥٦] قيصر بهاء، مرجع سابق، ص ١٦

[٥٧] رعد فجر فتيح الراوي : " القصور التشريعية في مواجهة الهجمات السيبرانية "، مجلة كلية الحقوق والعلوم السياسية في جامعة الأنبار العراقية، المجلد ١٠، العدد ٣٩ ، ٢٠٢١، ص ١٩٤.

الصعب معرفة مصدر الهجوم على الأقل في اللحظات الأولى لوقوع الاعتداء، فالمهاجم يتقن فن إخفاء هويته وتنفيذ الهجوم دون أن يترك وراءه أي دليل يمكن من خلاله الكشف عن هويته لذلك سوف نبين الأسباب التي تدفعنا الى تبني موقف واضح لناحية صعوبة تحديد مصدر الهجمات السيبرانية[٥٨] :

١. هي متعددة الأهداف : ان الأهداف لتنفيذ الهجمات السيبرانية ليست بالضرورة أن تكون دائماً عسكرية بل يمكن أن تتعداها كي تكون ثقافية ودينية واجتماعية وإقتصادية وشخصية .

٢. صعوبة تحديد الجهة المنفذة للهجوم : ان صعوبة تحيد هوية منفذ الهجوم تسمح بالتلاعب والتمويه فيما يتعلق بمصدر ومكان إرتكابه، بالرغم من التطورات التي وصلت اليها التكنولوجيا في عملية التتبع ولكن عملية التمويه والإخفاء التي يستخدمها المهاجم تجعل من إمكانية معرفة المصدر شبه مستحيلاً وخاصةً أن معظم الدول التي تقف وراء هذه الهجمات لا تتبناها كالهجمات الصينية المتكررة على الولايات المتحدة الأميريكية وتلك التي تقوم بها هذه الاخيرة على المفاعل النووي الايراني عام ٢٠١٥.

٣. إمكانية أن يكون الفاعل من غير الدول :

تجعل هذه الهجمات إمكانية إرتكابها سهلة جداً طالما أنها ليست بحاجة لأي معدات أو جيوش مجهّزة بل كل ما تحتاج اليه جهاز حاسوب متصل بالإنترنت فليس بالضرورة أن يكون الفاعل من الدول بل يمكن أن يكون أي شخص طبيعي أم معنوي، فأي فرد أو منظمة حكومية أم غير حكومية وحتى الشركات والمؤسسات العامة أو الخاصة يمكن أن تنفذ هجوماً سيبرانياً دون أن يكون هذا الأمر حكراً على الدولة .

٤. إختلاف طبيعتها عن الحروب التقليدية : كررنا كثيراً أن الهجمات السيبرانية يتم تنفيذها في الفضاء السيبراني وهو فضاءاً افتراضياً لا يعرف حدود زمنية أو مكانية، وهو خال تماماً من أي تكتيكات عسكرية ام استخدام للوسائل والأسلحة التقليدية التي تستخدم في أي حرب تقليدية بل هدفها الأساسي هو السعي الى ضرب القلب الاستراتيجي للهياكل الالكترونية الخاصة بالخصم إلحاق الأضرار به، فالحرب التقليدية تشكل تحدياً عسكرياً فقط مع وجود تحديات للقوة من حيث الكم والكيف ونكون أمام إعلان مسبق للحرب، على أن تكون هذه الأخيرة محددة زمنياً وجغرافياً مع وجود قوات نظامية وأطرافها محددين، أما الهجمات السيبرانية تكون غير محددة المجال أو المدى وأطرافها غير معروفون وغير محصورة ضمن دولة معينة (في معظم الاوقات)سواء كانت هدفاً للحرب أم مشاركة فيها وليس بالضرورة أن تكون الدولة هي الهدف , حتى الترسانة السيبرانية غير تقليدية ((CyberWeapons) ومختلفة عن تلك المتعارف عليها، أيضاً فالأسلحة السيبرانية المستخدمة تشكل خطراً ضئيلاً على حياة الانسان مقارنةً مع الحرب التقليدية، فالمهاجم والمدافع لا يتعرضون لأي خطر يمكن أن يسلب منهم حياتهم وهذا ما يميز الهجمات السيبرانية .

٥. تنوع الأدوات المستخدمة : ان الأدوات المستخدمة في تنفيذ الهجمات السيبرانية مختلفة كلياً عن تلك التقليدية وغير محددة بالأسلحة التقليدية المعروفة بل مختلفة في طبيعتها وتركيبتها ويمكن اختصارها على الشكل التالي :

- البرمجيات والفيروسات الخبيثة بكافة أنواعها وأشكالها .

[٥٨] عادل عبد الصادق :"أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني "، مكتبة الإسكندرية، وحدة الدراسات المستقبلية، مصر، ٢٠١٦، ص١٤٠

- الشبكات : وهي عبارة عن مجموعة من الحواسيب مرتبطة ببعضها البعض من خلال خطوط اتصال تسمح للمستخدمين من مشاركة البيانات فيما بينها.

- الأسلحة الإلكترونية المستخدمة التي لا تحتاج سوى لمنصات بسيطة غير مرئية تتمثل بموقع إطلاق وكمبيوتر ثابت او محمول او هاتف محمول وموقع على شبكة الانترنت ومحرك للبحث وشبكة إجتماعية وخادم افتراضي أو مادي، فهذه الأسلحة يمكن لأياً كان (على إلمام بكيفية تصنيعها) تطويرها وإستخدامها كالقراصنة والدول والسياسيين او المجرمين الإلكترونيين، منافسين ودول متصارعة ولها الخصائص التالية:

- سلاح غير قاتل وغير مرئي (الاَّ في حالة الأسلحة السيبرانية المستخدمة في النزاع المسلح) .

- الطابع الإنتشاري : كالفيروسات التي تستنسخ نفسها دون توقف وامكانية إستهداف دول كثيرة في لحظة واحدة وقدرتها على التنقل ضمن الشبكة الواحدة .

- تكلفة الإنتاج : مقارنةً مع التكلفة العالية لصناعة الأسلحة التقليدية , فقد يمكن تشكيل قوات للفضاء السيبراني بتكلفة اقل من تلك المخصصة للأسلحة التقليدية (فصناعة الفيروسات و البرمجيات الخبيثة تكلفتها أقل بكثير من تلك الأسلحة التقليدية) ولكن يجب أن نشير أن الدول المتقدمة تلجأ في الوقت الحالي الى تصنيع ترسانة أسلحة الكترونية تفوق قيمتها المبلغ المخصص لصناعة دبابة أو طائرة عسكرية مما يعني أن الدول أصبحت تخصص ميزانيات ضخمة للأسلحة السيبرانية .

- السرية والغموض : يكتنف الأسلحة السيبرانية نوع من الغموض والسرية لناحية معرفة كيفية صناعتها وتكلفتها بدقة، فتسعى الدول المتقدمة الى إخفاء حقيقية صناعة الأسلحة السيبرانية وتكلفتها العالية مما يشوب هذا الموضوع نوع من السرية لناحية الأبحاث والجهود التي تقوم بها الدول من أجل تميزها عن الدول الأخرى .

اذاً نستنتج، لكافة الأسباب الموضحة أعلاه أن إمكانية تحديد مصدر الهجمات السيبرانية أمرُ صعبٌ نسبياً وذلك بسبب الطبيعة الخاصة التي تكتنف هذا من النوع من النشاطات الخبيثة وهذا ما يؤكد لنا ضرورة التعاون بين الدول من أجل تطوير برمجيات خاصة تساهم في الكشف عن هذه الهجمات ومحاسبة من يقف وراءها وهذا ما نسعى اليه في هذه الدراسة.

لقد إنتهينا من معالجة الإطار القانوني للهجمات السيبرانية في الباب الأول من هذا القسم، سوف ننتقل الى توضيح كيفية تكييف الهجمات السيبرانية ضمن أحكام القانون الدولي الإنساني في الباب الثاني.

الباب الثاني : المسؤولية عن الهجمات السيبرانية من منظار القانون الدولي

في إطار ما يشهده العالم اليوم من تحديات سيبرانية جديدة ظهرت مؤخراً على الساحة الدولة، بات المدنيون والأعيان المدنية المحمية في خطر تام، فرضت هذه التحديات واقعاً جديداً يتمثل في ضرورة تكييف الهجمات السيبرانية في ظل القانون الدولي الانساني الذي يهدف الى ضبط سير العمليات العدائية وخضوعها لقواعد هذا القانون، بالرغم من عدم وجود نص صريح يتناول موضوع هذه الهجمات لكن هذا لا يعني عدم خضوعها للقواعد والأحكام الموضوعة من قبل قانون لاهاي حول تنظيم وسائل الحرب بل يبقى المتحاربون خاضعون لمبادئ القانون الدولي الانساني وملزمون بالتقيد بالأنظمة المعمول بها عند

اختيارهم للوسائل والأساليب من أجل ابقاء المدنيين خارج هذا النزاع، ولكن هذا القانون ايضاَ اعترف للدولة المعتدى عليها بحقين الأول في ممارسة حقها في الدفاع الشرعي عند تعرضها للإعتداء، أما الثاني هو حقها في توجيه تدابير مضادة بوجه الدولة المعتدية مع وضعه بعض الشروط الواجب توافرها مع واجب الالتزام بمبادئ معينة تحكم سير الأعمال العدائية، فالجهة التي لم تلتزم بهذه المبادئ تعتبر مسؤولة دولياً عن الانتهاكات التي قامت بها مما يعرضها للمسؤولية الدولية وكذلك الأمر بالنسبة للمشارك المباشر الذي يلقى على عاتقه واجب الالتزام بالأحكام التي فرضها القانون الدولي الانساني بحيث يتعرض للمساءلة الدولية في حال لم يلتزم بها، فالدول ملزمة بالإلتزام بمبادئ كل من القانون الدولي الانساني والقانون الدولي العرفي ووجب عليها الالتزام بهذه المبادئ تحت طائلة المسؤولية الدولية، ففي الفصل الأول سوف نوضح امكانية تكييف الهجمات السيبرانية ضمن تطبيقات القانون الدولي الانساني وفي الفصل الثاني سوف نحدد مسؤولية المشارك المباشر عن الهجمات السيبرانية في حال مخالفته للقواعد المعمول بها دولياً .

الفصل الأول : مدى تطبيق القانون الدولي الإنساني على الهجمات السيبرانية

الهجمات السيبرانية هي نوع وأسلوب جديد وعصري من أساليب الحرب بين الاطراف المضادة، بحيث تتميز عن الاسلحة التقليدية بفقدانها للصفة الحركية التي ترافق النزاعات العدائية التقليدية، فضلاً عن نشأتها بطريقة مختلفة نوعاً ما مما أدى الى وضع الدول أمام تهديد جديد يزيد من المعاناة البشرية، فالقانون الدولي الإنساني هو إطارقانوني ناظم للنزاعات المسلحة ومن ضمنها الهجمات السيبرانية التي وضعته أمام معضلة منفردة بذاتها وإختبار حقيقي وجدي حول أمكانية تطبيق قواعده على هذا النوع الجديد من التحديات.

ان القانون الدولي الانساني هو مجموعة من القواعد التي تهدف الى الحدّ من اثار النزاعات المسلحة , بحيث يحمي الاشخاص اللذين لا يشاركون أو اللذين يكفون عن المشاركة في الأعمال العدائية , ايضاً هو مجموعة من القواعد الدولية ذكرت في المعاهدات او الاتفاقيات التي تساهم قدر الامكان في وضع قيود معينة لاعتبارات انسانية بحته بهدف حماية الاشخاص والأموال بطريقة جدية، وبموجب هذا القانون سواء كنّا أمام نزاع دولي أو غير دولي هنالك ضمانات أساسية للأشخاص اللذين لا ينخرطون في الأعمال العدائية وهذا ما أكده البروتوكول الاضافي الأول المتعلق بحماية ضحايا المنازعات الدولية المسلحة عام ١٩٧٧ ويقتضي التنويه الى أن قانون الحرب لم يتضمن أي قواعد صريحة بشأن العمليات التي تحدث في الفضاء السيبراني , فالهدف الأسمى لهذا القانون هو حماية المدنين من ويلات الحرب لذلك نعتبر أن الاستخدام السيئ للفضاء السيبراني وتعريض الاشخاص والممتلكات للخطر أو إلحاق الأضرار بهم يحتم إدراج كافة هذه الأعمال المشبوهة ضمن أحكام القانون الدولي الانساني إنطلاقاً من خضوع الوسائل المستخدمة في الحرب السيبرانية لنفس القواعد التي تحكم سير الأعمال العدائية بالأسلحة التقليدية [٥٩] وهذا ما أكدته ايضاً محكمة العدل الدولية أن هذا القانون وضع بطرق تجعله قابلاً للتطبيق على كافة أشكال وأنواع الأسلحة بما فيها الأشكال والأنواع المستقبلية " وكذلك ديباجة البروتوكول الاضافي الثاني لعام ١٩٧٧ التي أكدت أنه:" في ظل غياب قاعدة معينة في القانون الاتفاقي يظل المدنيين تحت حماية وسلطان مبادئ القانون الدولي كما استقربها العرف ومبادئ الانسانية وما يمليه الضمير العام "، ولكن هل يمكننا إضفاء الشرعية القانونية على العمليات السيبرانية وخصوصاً الهجمات منها ؟

[59] Vladimir Szoke-Pellet, "Les cyberattaques étatiques et la notion d’agression en droit international ", op. it, p. 8.

سوف نبين في هذا الباب إمكانية تطبيق القانون الدولي الانساني على الحالات التي تدخل ضمن إطار الهجمات السيبرانية عند حصولها ضمن نزاع دولي مسلح ام غير مسلح وكيف نستطيع تطبيق هذا القانون على هذا النوع من الأعمال (في المبحث الأول) وتوضيح مسؤولية المشارك المباشر (في المبحث الثاني)

المبحث الأول : إمكانية تكييف الهجمات السيبرانية ضمن قواعد القانون الدولي الإنساني

المستجدات السيبرانية المستحدثة على الساحة الدولة طرحت اشكالية مهمة في إمكانية اعتبار الهجمات السيبرانية جزء من النزاع المسلح(الفرع الأول) مع التدابير التي من الممكن أن تلجأ اليها الدولة المعتدى عليها (الفرع الثاني)، مما يدفعنا الى التعمق في هذه المفاهيم في هذا المبحث.

الفرع الأول : مدى مشروعية اللّجوء الى الهجمات السيبرانية في حالة النزاع المسلح

فالقانون الدولي الانساني هو مجموعة من القواعد القانونية النى تسعى الى الحد من اثار النزاعات المسلحة لأسباب انسانية وبالتالي ان مجال انطباق القانون الدولي الانساني هو النزاع المسلح [٦٠] ولكن بالرغم من النقاشات الجارية في مسألة انطباق القانون الدولي الانساني على الهجمات السيبرانية الاّ أننا يمكننا التوصل الى انطباق قواعد هذا القانون على الهجمات التي تحدث في سياق نزاع مسلح وذلك بعد أن توصل الى هذه النتيجة فريق العمل الذي أنشأته الجمعية العامة للأمم المتحدة الى جانب خبراء حكوميين في انطباق أحكام القانون الدولي و لا سيما ميثاق الأمم المتحدة على الهجمات السيبرانية مع ضرورة احترام مبادئ الانسانية (الضرورة والتناسب و التمييز ..) بالإضافة الى إنطباق القواعد العامة لقانون لاهاي تلك الخاصة لقانون جينيف لحماية الفئات الضعيفة والأعيان المدنية أثناء النزاعات المسلحة، فينطبق القانون الدولي الانساني على هذه الهجمات التي تشكل جزء من أي نزاع مسلح عند استخدام الوسائل التقليدية للحرب وتكون متصلة به، كما ينطبق على العمليات السيبرانية التي تصل في حد ذاتها الى مستوى النزاع المسلح من حيث الأثار الناجمة عنها في ظل غياب العمليات الحركية [٦١]، وهذا ما أكدته المادة ٣٦ من البروتوكول الاضافي الأول فيما يختص بالأسلحة الجديدة التي نصت : " يلتزم أي طرف سام متعاقد عند دراسة أو تطوير أو اقتناء السلاح جديد أو أداة للحرب أو اتباع أسلوب الحرب أن تتحقق فيما اذا كان ذلك محظوراً في جميع الأحوال أو في بعضها بمقتضى هذا الملحق أو اي معاهدة أخرى من قواعد القانون الدولي الانساني التي يلتزم بها الطرف السامي المتعاقد "، مما يؤكد تطبيق قواعد القانون الدولي الانساني على الهجمات السيبرانية مع مراعاة مبادئ الحرب، فيحق للأطراف اختيار أساليب ووسائل القتال مع التقيد بالقيود المفروضة (المادة ٣٥ من البروتوكول الاضافي الأول) .

أما بالنسبة الى دليل تالين فالمادة ٢٠ منه نصت على ما يلي : " العمليات السيبرانية التي تنفذ في سياق النزاع المسلح تخضع لقانون النزاعات المسلحة "، مما يؤكد وجوب الإلتزام بقانون الحرب عند اللجوء الى الهجمات السيبرانية في حالة النزاع المسلح كأي حرب قائمة ، فالعبرة هي في النتائج التي تحققها الهجمات السيبرانية و ليس الوسيلة المستخدمة، فالمادة ٤٩ من البروتوكول الإضافي الأول " كل عملية حربية في البرّ أم في البحر أم في الجو قد تصيب المدنيين وتنطبق أحكامه على كافة الهجمات في اي اقليم تشن فيه"،

---

[٦٠] دخلافي سفيان: " تكييف الهجمات السيبرانية في ضوء أحكام القانون الدولي "، المجلة الأكاديمية للبحث القانوني، المجلد ١٣ , العدد ٠٢، ٢٠٢٢، ص ٣١٥

[٦١] يحي ياسين سعود : " الحرب السيبرانية في ضوء القانون الدولي الانساني " ، المجلة القانونية، المجلد ٤، العدد ٤ – كلية الحقوق – جامعة القاهرة –مصر، ص ٨٥

ومن صور إستخدام العمليات السيبرانية أثناء النزاعات المسلحة : عمليات التجسس وتحديد الأهداف وقطع نظم الاتصالات الخاصة بالعدو أو تضليلها أو التشويش عليها وتعطيل محطات الرادار والمنشآت النووية والهجمات التي تستهدف البنى التحتية [٦٢]، وتجدر الإشارة الى أن القانون الدولي الانساني لا يضفي الشرعية على أي عمل من الأعمال العدوان أو أي استخدام للقوة الذي يتعارض مع ميثاق الأمم المتحدة وهذا ما أكدته المادة الثانية من ديباجة البروتوكول الاضافي الأول لسنة ١٩٧٧ و لكن السؤال الذي يطرح لماذا يعتبر الهجوم السيبراني بمثابة هجوم مسلح في بعض الحالات ؟

ان الضرر الذي تلحقه الهجمات السيبرانية يعتبر جسيماً وخطيراً انطلاقاً من آثاره الضحمة المتمثلة بالوفيات والإصابات في صفوف المدنيين، والمس بالبنى التحتية للمواطنين عن طريق تعطيل الأجهزة التي تتحكم بالقطاعات العامة للدولة، مثلاً التحكم في محطات المياه والسدود وما ينتج عنها من فيضانات في المناطق المأهولة بالسكان، والمساهمة في حدوث كوارث انسانية خطيرة دليل كافي لاعتبار الهجوم السيبراني قوة وعدوان، لذلك أحياناً يكون الدمار الذي تلحقه الهجمات السيبرانية أكبر بكثير من تلك التي تلحقه الحروب التقليدية مما يحتم ضرورة إلتزام الفرقاء بالمبادئ الخاصة بالقانون الدولي الانساني، و يجب أن نشير الى ماهية بعض المصطلحات قبل الدخول في الحالات التطبيقية [٦٣] :

- النزاع المسلح الدولي : اعتبرت المادة الثانية المشتركة لإتفاقيات جينيف الأربعة والمادة الأولى- الفقرة الرابعة من البروتوكول الاضافي الأول : نكون أمام نزاع مسلح دولي في حالات ثلاثة :

١. حالة استعمال القوة المسلحة في العلاقات بين الدول

٢. حالة الاحتلال.

٣. حالة قيام مقاومة مسلحة من طرف حركات التحرير .

- النزاع المسلح غير الدولي : نستنتج من تعريف المادة الثالثة (الفقرة الأولى) المتركة لاتفاقيات جينيف الأربعة ما يلي :

" هو كل نزاع لا تكون أطرافه كلها دول هو نزاع مسلح غير الدولي.

- ان النزاع المسلح غير الدولي هو الذي يتم في اقليم دولة واحدة .

- أن تبلغ النزاعات درجة من العنف , فتتجاوز مجرد الاضطرابات و أعمال الشغب و المظاهرات مع الأخذ بعين الاعتبار طبيعة الجهاز الذي تلجأ اليه الدولة لضبط الوضع .

- أن تكون الجماعات المسلحة طرفاً في النزاعات على درجة من التنظيم اي توافر هيكلية معينة لها .

سوف نبين بعض الحالات التطبيقة للهجمات السيبرانية في حالتي النزاع المسلح الدولي و غير الدولي .

في اطار النزاع المسلح الدولي : حرب كوسوفو عام ١٩٩٩[٦٤] :

---

[٦٢] دخلافي سفيان، مرجع سابق، ص ٣١٧

[٦٣] فتيحة بشور : " مفهوم القانون الدولي الجنائي "، مجلة المعارف العلمية ٢٠١٢، العدد ١٢، ص ٢٢-٢٨

[٦٤] ابراهيم طلال محمد الحاج : " الهجمات السيبرانية على شبكات الحاسوب في ضوء القانون الدولي الانساني "، جامعة دمشق – كلية الحقوق (قسم القانون الدولي)، دمشق-سوريا، ص ٨٤-٨٥

على اثر سيطرة دولة كل من الجبل الأسود و صربيا على كوسوفو، نشب نزاع مسلح بين جماعة متمردة تسمى بجيش تحرير كوسوفو والقوات المسلحة اليوغوسلافية وكانت أول حرب واسعة النطاق على الإنترنت مما دفع بقوات حلف الشمال الأطلسي الى توجيه هجمات سيبرانية الى يوغوسلافيا السابقة التي أدت الى استهداف شبكة الاتصالات وتعطيلها وتعطل النظام الخاص بالكمبيوتر للدفاع الجوي التي كانت مهمتها استهداف طائرات حلف الاطلسي بالصواريخ، و في النزاع المسلح نفسه تم استهداف السفارة الصينية في بلغارد، عندما عمد قراصنة صينيين الى مهاجمة المواقع الالكترونية الرسمية التابعة للولايات المتحدة الأميريكية الذي أدى الى الاستحواذ على الالاف البيانات الرقمية المصنفة بأنها عالية السرية [٦٥] .

فالنزاع الحاصل أعلاه هو ذات صفة دولية وخاضع لقواعد القانون الدولي الانساني لناحية النتائج التي أدت الى الحاق أضرار جسيمة بالأرواح والأعيان المحمية نتيجة القصف الأميركي وتوقف محطات الطاقة الكهربائية لأيام عن العمل بالنسبة الى الهجمات الموجهة من حلف الشمال الأطلسي على يوغوسلافيا السابقة، بالنسبة لهجوم الهاكرز الصينيين على الموقع الخاص بالولايات المتحدة الأمريكية الذي لم يلحق أي اضرار جسيمة بالارواح والممتلكات بل كان الهدف هو الحصول على المعلومات السرية لا يمكننا أن ندرجها ضمن النزاع المسلح الدولي.

- في اطار نزاع مسلح غير دولي :

من المتفق عليه أن الهجمات السيبرانية التي تتم خارج نزاع مسلح حركي ليس من الشرط أن تخضع لقواعد القانون الدولي الانساني الاّ في حال ارتقاءها الى النزاع المسلح نتيجة الأضرار التي تلحقها وتسببها من أضرار مادية في الأرواح والممتلكات وكان بالإمكان أن ننسب هذه الهجمات الى جهة معينة، سوف نذكر بعض الهجمات السيبرانية بين الصين و الولايات المتحدة الأمريكية.

عام ٢٠٠٧ ذكر الخبير الأميريكي Paul Strasmann أن الاف الأجهزة في الولايات المتحدة حاولت المخابرات الصينية الاستلاء عليها و التجسس و سرقة بياناتها للحصول على وثائق سرية حكومية أمريكية من خلال ما يسمى ب GhostNet الاّ ان الصين نفت هذا الأمر وفي عام ٢٠١٧ حاول ثلاث موظفين صينيين من شركة Guang Zhou Bo Yu Information Technology Company Limited في اختراق شركات اميريكية و محاولة المخابرات الصينية باختراق أجهزة الكمبيوتر الخاصة بهيئات عسكرية اميريكية وسرقة معلومات عن نظام صواريخ باتريوت (Patriot Missile System) ،فكافة هذه الأفعال لم ترتقي الى مستوى النزاع المسلح.

إذاً أن القانون الدولي الانساني وأحكامه وضعت من أجل حماية المدنيين من ويلات الحرب كما وقلنا سابقاً، فأن اللجوء الى الهجمات السيبرانية في حال النزاع المسلح يكون جائزاً ولكن ضمن شروط وقيود معينة وأهمها عدم التعرض للمدنيين والممتلكات المحمية من الخطر، بمعنى آخرلا تكون هذه الهجمات سبباً للوفيات والأضرار التي تلحق بالمنشات الحيوية والبنى التحتية، وأن خلو الإتفافيات الدولية من أي ذكر للهجمات السيبرانية لا يعني بالضرورة إباحة استخدامها دون أي قيد او شرط , فالأشكال الحديثة لهجمات الفضاء السيبراني وحرب المعلومات التي لم يتم تضمينها في استخدامات الأسلحة التقليدية وفي الإتفاقيات

[٦٥] أحمد عيسى نعمة فتلاوي، مرجع سابق، ص ٣٠-٣١

الدولية ترتبط بالقانون الدولي الانساني وتخضع له كأي سلاح جديد عندما يتم إستخدامه في النزاع المسلح [٦٦] تطبيقاً لمبدأ مارتنز .

سوف ننتقل الى الفرع الثاني من أجل التطرق الى أهم المبادئ التي ترعى سير العمليات العدائية.

الفرع الثاني : المبادئ الدولية التي تحكم سير العمليات العدائية

ان العمليات القتالية التي تحصل في الفضاء السيبراني لا تقل خطورةعن الحروب التقليدية من حيث التهديد التي تنطوي عليه، نظراً لأهمية هذه الهجمات تسعى الحكومات جاهدةً الى وضع الامن السيبراني في صميم استراتجيات أمنها القومي ولكن كأي حرب حقيقية كي لا تبقى دون أي قيود تنظمها , سعى القانون الدولي الانساني في هذا الإطار الى مجموعة من المبادئ والسلوكيات(مبدأ سلوكيات الحرب – Jus in Bello) التي تلزم أطراف النزاع على الالتزام بها ، فقد يرتكز القانون الدولي الانساني على مجموعة من المبادئ الأساسية التي تحكم سير العمليات العدائية على الشكل التالي :

١. مبدأ الضرورة العسكرية : نعني بهذا المبدأ أن يتم إستهداف فقط الأهداف العسكرية الضرورية التي تحقق ميزة مهمة للخصم فالقانون الدولي الانساني الذي يهدف الى حماية ضحايا النزاعات المسلحة وضع قيود على حرية الأطراف المتحاربة في استخدام الأسلحة والمعدات أثناء القتال وخاصة بالنسبة الى الأسلحة التي تصيب بلا تمييز او تلك التي لا يمكن السيطرة عليها من حيث اثارها التي تصيب المدنيين و الأعيان . [٦٧]

عدة صكوك وإتفاقيات دولية تطرقت الى مبدأ الضررورة العسكرية نذكر منها[٦٨] :

- إعلان بيترسبورع لعام ١٨٦٨ الذي نصَ على " ضرورات الحرب يجب أن تخضع لمتطلبات انسانية " .

- إتفاقية لاهاي بشأن الحرب البرية لعام ١٩٠٧ و خاصة المادة ٢٣ (الفقرة ٢/ز) أنه " يمنع بالخصوص..تدمير ممتلكات العدو او حجزها الاَ اذا كانت ضرورات الحرب تقتضي حتماً هذا التدمير أو الحجز "، فضلاً عن المواد (٤٣-٥٤-٢٣).

كذلك نصت المادة ٣٧ من البروتوكول الاضافي الأول اللاحق على " يحظر قتل الخصم أو إصابته او أسره باللجوء الى الغدر و يعتبر قبيل الغدر تلك الافعال التي تستثيرثقة الخصم مع تعمد خيانة هذه الثقة ودفع الخصم الى الإعتقاد بان له الحق وان عليه التزاماً ويمنح الحماية طبقاً لقواعد القانون الدولي الإنساني التي تطبق في النزاعات المسلحة، (المواد ٥٢, ٢/٥٤ , ١/٦٢ , ٣/٧١ , ٤/٦٧ لعام ضحايا النزاعات المسلحة الدولية) .

---

[٦٦] محمد دهام مسعف : " مشروعية استخدام الهجمات السيبرانية في النزاعات الدولية والمسؤولية الدولية عنها " التي تصدر عن جامعة بغداد- عدد خاص لبحوث المدرسيين مع طلبة الدراسات العليا، الجزء الرابع، المجلد ٣٦، كانون الأول ٢٠٢١، ص ٦٨٢-٦٨١

[٦٧] جان بكتيه :" مبادئ القانون الدولي الانساني: تطوره ومبادئه"،دراسات في القانون الدولي الانساني، تقديم / مفيد شهاب دار المستقبل العربي، اصدارات اللجنة الدولية للصليب الاحمر، الطبعة الثانية – القاهرة، ٢٠٠٩ ص ٥٣ .

[٦٨] احمد عباس نعمه فتلاوي، مرجع سابق، ص ٥٤ .

- المادة ٥٢ الفقرة الثانية من البروتوكول الإضافي الاول التي قضت : " تقتصر الهجمات على الأهداف العسكرية وتنحصر الاهداف العسكرية فيما يتعلق بالأعيان على تلك التي تسهم مساهمة فعالة في العمل العسكري سواء كان ذلك بطبيعتها ام بموقعها ام بغايتها ام بإستخدامها والتي يحقق تدميرها التام أو الجزئي او الإستلاء عليها او تعطيلها في الظروف السائدة ميزة عسكرية أكيدة .

- المادة ٥١ من البروتوكول الإضافي الاول لعام ١٩٧٧ الذي يؤكد عدم جواز استعمال وسائل وطرق قتال من شأنها أن تؤدي الى هجمات عشوائية ومن بينها :

* تلك التي لا توجه الى هدف عسكري محدد

* تلك التي لا تستخدم طريقة او وسيلة قتال لا يمكن حصر آثارها على النحو الذي يتطلبه هذا الملحق " البروتوكول" ومن ثم فان من شأنها ان تصيب في كل حالة لهذه الاهداف العسكرية والأشخاص المدنيين او الأعيان المدنية دون تمييز .

اذاً من قراءة المواد السابقة ان مبدأ الضرورة العسكرية ينتج مهاجمة الأهداف العسكرية كخيار ضروري بالمرتبة الاولى الاَ أن ذلك لا يمنع من ضرورة مهاجمة اعيان مدنية كانت تسهم بطريقة غير مباشرة في تحقيق ميزة عسكرية اكيدة وقد تم تحديد شروط معينة في القانون الدولي الانساني يمكن بموجبها اللجوء لمبدأ الضرورة العسكرية وفق ما يلي[٦٩] :

- ان يكون هذا التجاوز مؤقتاً ومرتبطاً بمدة قيام هذه الضرورة

- ان يكون على أهداف محددة

- ان يكون الغرض منها تحقيق ميزة عسكرية أكيدة

- ان يتم مراعاة قواعد القانون الدولي الانساني

أيضاً نصّ دليل تالين في المادة ١٤ منه بشأن الضرورة العسكرية والتناسب :" إستخدام القوة التي تنطوي على عمليات سيبرانية تقوم بها الدولة في ممارسة حقها في الدفاع ينبغي أن تكون ضرورية ومتناسبة "، اذاً اعتبر خبراء دليل تالين انه من الضروري ان تكون العمليات القتالية متناسبة وضرورية كذلك شدد عندما يكون هنالك خياراً ممكناً بين عدة اهداف عسكرية من اجل الحصول على ميزة عسكرية مماثلة فلا بدّ من ان نختار الهدف الذي يتوقع منه أن يسبب خطر أقل على المدنيين والأعيان المدنية، اما في حالة وجود العديد من الاهداف الاّ أن اهدافاً تحقق ميزة عسكرية اكثر من مثيلاتها، في هذه الحالة من حق المهاجم توجيه هجمات سيبرانية مباشرة ضد الهدف العسكري الذي يحقق أكثر ميزة عسكرية ممكنة في اطار نزاع مسلح، ففي الحرب التقليدية يكون من الأمكن ان نميز بين الاهداف العسكرية والمدنية ولكن الامر ليس بالسهل في اطار الهجمات السيبرانية وهذا ما أكده " ريكس هاجس " مدير شبكة الابتكار السيبراني في جامعة كامبردج : " ان الهجمات الرقمية تنشئ تحدياً واضحاً أمام تطبيق مبدأ الضرورة العسكرية و لحل هذه المعضلة لا بدّ من تضافر الجهود بين خبراء القانون الدوليين و مهندس الصناعات الالكترونية لتحديد ما اذا يمكن وصف بهدف ..." .

اما السؤال الذي يطرح هنا: هل تجاوز مبدأ الضرورة يؤدي الى اعتبار الفعل بمثابة جريمة ؟

---

[69] نور امين موصلي، مرجع سابق، ص ٥٣

ان تجاوز مبدأ الضرورة يؤدي الى إعتباره جريمة حرب وفقاً للنظام الاساسي للمحكمة الجنائية الدولية والتطبيق الاحدث للمبدأ العرفي الذي يقضي بحظر إستعمال الأسلحة التي من شانها ان تتسبب في احداث آلام غير مبررة وفقاً للمادة ١/٣ من النظام الاساسي للمحكمة الجنائية الدولية المعنية فيما يخص الاشخاص الذين يعتبرون مسؤولين عن الانتهاكات الجسيمة للقانون الدولي الانساني المقترفة في أراضي يوغوسلافيا السابقة منذ سنة ١٩٩١ والذي إعتمد بموجب القرار ٨٢٧ الذي اتخذه مجلس الامن في ٢٥ ايار ١٩٩٣، ولكن ما هو الحال بالنسبة الى هذه المخالفات في اطار الهجمات السيبرانية ؟

نطبق في اطار الهجمات السيبرانية أحكام القانون الدولي الانساني، لكن معيار التمييز بين الأهداف العسكرية والمدنية غير مطبق في العمليات السيبرانية وذلك لأنه الممكن أن تستهدف منشآت تقدم خدمة للمجال العسكري وفي الوقت نفسه للمدنيين، ففي هذه الحالة التي ذكرناها لا نجد أي قانون او تشريع او توصية تنظمه فلا بدّ ان تتضافر الجهود من أجل حله[٧٠] .

٢. مبدأ التناسب

يعدّ مبدأ التناسب من المبادئ المهمة الواجبة التطبيق في النزاعات المسلحة , فقد يرمي الى تحقيق الموازنة بين الهدف العسكري المرجو من العمليات الحربية وبين عدم إلحاق أضرار مفرطة بالخصم، بتعبير آخر ان الميزة العسكرية التي تحصل عليها من عملية معينة يجب ان تفوق الضرر الذي قد يلحق بالمدنيين والأعيان المدنية نتيجة هذا الاجراء، فقد شددت القاعدة ١٤ من دراسة اللجنة الدولية للصليب الاحمر للقانون العرفي الصادر في ١٤ تموز ٢٠٠٥ :" يحظر الهجوم الذي قد يتوقع منه أن يسبب بصورة عارضة خسائر في ارواح المدنيين او اصابات بينهم أو اضراراً بالأعيان المدنية او مجموعة من هذه الخسائر والأضرار ويكون مفرطاً في تجاوز ما ينتظر أن يسفر عنه من ميزة عسكرية ملموسة ومباشرة، اذاً موضع تطبيق هذا المبدأ هو المدنيين، الأعيان المدنية والأعيان المزدوجة[٧١]، فيطبق هذا المبدأ في أي وقت من الممكن ان يتضرر المدنيون جراء الهجمات وطالما لا يشارك هؤلاء في العمل العدائي، أي بمعنى اخر فان المقاتلين و المدنيين الذين يشاركون مباشرةً في العمل العدائي في وقت قيامهم بهذه الأعمال لا يتمتعون بمزايا هذا المبدأ.[٧٢]

وفق ما جاء ايضاً في قواعد القانون الدولي الانساني ان مبدأ التناسب في الهجوم مقنن في المادة ٥١(٥/ب) من البروتوكول الإضافي الأول بحيث أصبح مقبولا من كافة الدول كمبدأ عام من القانون الدولي المتعلق بالنزاعات المسلحة (القاعدة الرابعة عشر من دراسة اللجنة الدولية للصليب الأحمر ذكرت مضمون ما جاء في المادة ٥١ من البروتوكول الاضافي الأول لعام ١٩٧٧)، كذلك أكدت المادة ٥٧(ب-٢) من البروتوكول نفسه : " يلغى او يعلق اي هجوم اذا تبين أن الهدف المقصود ليس هدفاً عسكرياً او أنه مشمول بحمايةٍ خاصةٍ".

أيضاً المادة الثامنة (٢/ب) من النظام الأساسي للمحكمة الجنائية الدولية نصت على ما يلي : " ان تعمد شن هجوم مع العلم بان مثل هكذا هجوم سيسبب خسائر عرضية في أرواح المدنيين وإصابات بين صفوفهم أو اضراراً بالأعيان المدنية ويكون افراطه واضحاً بالقياس الى مجمل الميزة العسكرية المتوقعة والملموسة و

---

70 هنري ميرو متنز : " مبدأ الالام التي لا مبرر لها " دار المستقبل العربي، الطبعة الأولى عام ٢٠٠٠، ص ٢٤٣

71 دليل تالين، مرجع سابق، المادة ٥١ (التعليق الثاني والثالث)

٧٢ علي محمد كاظم الموسوي، مرجع سابق، ص ١٦٨

المباشرة، يشكل جريمة حرب في النزاعات المسلحة الدولية "، ان القانون الدولي الإنساني يحظر المعاناة التي لا تتم عن الصلة السببية المباشرة بفائدة عسكرية ملموسة ولا تتناسب معها، و هذا ما أكدته المادة الثامنة (٤/٢) من قانون المحكمة الجنائية الدولية "ان تعمد شن هجوم مع العلم بان هذا الهجوم سيسفر عن احداث ضرر واسع النطاق وطويل الاجل وشديد للبيئة الطبيعية يكون إفراطه واضحاً بالقياس الى مجمل المكاسب العسكرية المتوقعة الملموسة والمباشرة ".[٧٣]

الاّ ان التوتر او الإنزعاج او الخوف لا تعتبر اضراراً جسيمةً لأنها لا تشكل خسارة في أرواح المدنيين او اضراراً تلحق بالأعيان المدنية، اما في اطارالهجمات السيبرانية كثيرةٌ هي الإنتهاكات بسبب صعوبة التمييز بين الشبكات العسكرية والمدنية وهذا ما أكده Shinn في هذا المجال عند سؤاله اذ كان بالإمكان تأكيد احترام مبدأ التناسب قبل التخطيط لإستخدام وسائل او طرائق سيبرانية مفيدة لأغراض هجومية، فإعتبر أنه يمكن تطبيق مبدأ التناسب على الهجمات السيبرانية ولكن علينا ان نسأل فيما اذا كانت هذه الهجمات يمكن عدّها عدواناً لا يختلف عن الهجوم الذي قد تتعرض له أكان بالصواريخ او الهجمات السيبرانية وعدها مبرراً للردّ باستخدام القوة المسلحة المناسبة مما دفع ركس الى الاتفاق مع ما أكده شين في اعتبار انه اذا تم توجيه هجمات سيبرانية ضدّ بنى تحتية ثنائية الاستعمال (مدنية و عسكرية) وعن بعد فلا يبدو ان المنفعة العسكرية ستكون واضحة ما يجعل من تطبيق مبدأ التناسب في اثناء الهجمات السيبرانية أمراً في غاية الصعوبة ".[٧٤]

اذاً من الصعب التحكم بالهجمات السيبرانية أثناء التخطيط أم بعد التنفيذ لصعوبة ضبط الأثار التي من الممكن حدوثها مما يشكل اقرار ضمني في عدم إمكانية تطبيق هذا المبدأ بالشكل الصحيح الاّ بعد تطوير الأنظمة القانونية من أجل الوصول الى هذه الأهداف أعلاه .

٣.مبدأي الحياد و التمييز

نصت المادة ٣٧ من دليل تالين أنه ينبغي على جميع الأطراف المتنازعة توجيه الهجمات السيبرانية على من فقد الحماية من الهجمات المباشرة (المقاتل أو المدني الذي شارك في الأعمال العدائية وفقد الحماية على أثرها و لم يستعيدها) دون توجيهها للمدني المسالم عبر تطبيق مبدأ التمييز بين المقاتلين وغير المقاتلين، وكذلك الأمر يطبق لناحية التمييز بين الأعيان المدنية والعسكرية[٧٥]، إضافةً الى مبدأ حظر الهجمات العشوائية : أي هي تلك الهجمات التي لا يمكن أن توجه الى هدف عسكري معين أو تلك التي لا تكون اثارها محصورة بفترة النزاع المسلح فقط (أي تلك التي تصيب أهدافاً شرعية فضلاً عن المدنيين و الأعيان المدنية دون اي تمييز)، أما بالنسبة الى مبدأ الحياد يعرف على أنه : " حق معترف به للدولة في أن يكون لها علاقات مع الأطراف المتنازعة مع الإلتزام بعدم مساعدة أحد الأطراف المتنازعة ومنع الدول المحايدة في إستخدام اراضيها من قبل أحد أطراف النزاع [٧٦] ولكن من العقبات التي تواجه تطبيق هذا المبدأ في

---

[٧٣] https://ar,guide-humanitarian-law.org

[74] أحمد عباس معمه فتلاوي , مرجع سابق , ص ٦١

[٧٥] دليل تالين بشان القانون الدولي المطبق على الحروب السيبرانية، المادة ٣٧ اعتبرت أنه : "لا يجوز ان تكون الأعيان المدنية هدفاً للهجمات السيبرانية، الحواسيب، شبكات الحاسوب والبنية التحتية السيبرانية أن تكون هدفاً للهجمات اذا كانت أهدافاً عسكري".

[٧٦] مصطفى نعوس :" حقوق و التزامات الدول في الحرب المعلوماتية " , مجلة دراسات لعلوم الشريعة والقانون، المجلد ٤٠، ملحق ١، ٢٠١٣، ص ٧٨٨، متوفرة على الرابط التالي : www.mohamah.net

مسألة الهجمات السيبرانية أن المهاجم يمكن أن يستخدم أراضي الدولة المحايدة في توجيه هجوم سيبراني لدولة أخرى مما يؤكد أن هذه الدولة أصبحت غير محايدة وخاصة في حال فشلت الدولة عن منع استخدام أراضيها في هذه الحالة يحق للدولة المتضررة أن تتخذ كافة الخطوات اللازمة لمنع و مواجهة هذا الهجوم.[٧٧]

٤. مبدأ مارتنز

يعود تسمية هذا المبدأ الى "فيودور مارتنز" احد مندوبي روسيا في مؤتمر السلام عام ١٨٩٩ الذي لا يزال يطبق حتى يومنا هذا وأصبح جزء لا يتجزأ من القانون الدولي العرفي الذي صرح فيه :" أنه في الحالات غير المشمولة بالأحكام يظل السكان المتحاربون تحت حماية وسلطان مبادئ قانون الأمم كما جاءت، من التقاليد التي إستقر عليها الحل بين الشعوب المتمدنة وقوانين الإنسانية ومقتضيات الضمير العام" . شّكل هذا المبدأ ثورة في قدرته على سدّ الفراغ الذي يعتقد البعض أنه موجود في القانون الدولي لذلك أعيد إستخدامه في الإتفاقيات التالية :

- إتفاقية لاهاي الثانية المتعلقة بقوانين و أعراف الحرب البرية لعام١٨٩٩

- إتفاقية لاهاي الرابعة لعام ١٩٠٧

- ملحق اتفاقيات جنيف الأربعة ١٩٤٩

- إتفاقية حظر بعض الأسلحة التقليدية ١٩٨٠ :التي نصت على أنه : " في الحالات التي لا تتناولها هذه الإتفاقية والبروتوكولات المرفقة بها او الإتفاقيات الدولية الاخرى يتوجب على السكان المدنيون والمقاتلون متمتعين في كل الأوقات بحماية وسلطان المبادئ القانون الدولي المستمدة من الأعراف المستقرة ومن مبادئ الانسانية وما يمليه الضمير العام ".

البروتوكولان الأول والثاني لعام ١٩٧٧ :

المادة الأولى (الفقرة الثانية) من البروتوكول الأول وإتفاقية لاهاي الثانية المتعلقة بقوانين واعراف الحرب البرية لعام ١٨٩٩ نصت على: "حتى تصدر مدونة الحرب أكثر اكتمالاً، ترى الأطراف المتعاقدة من المناسب أنه في الحالات التي لا تشملها هذه اللائحة التي اعتمدتها، يظل السكان المدنيون والمقاتلون تحت حماية مبادئ الأمم الناتجة عن العادات الراسخة بين الشعوب المتحضرة وقوانين الإنسانية وما يمليه الضمير العام"، نلخص ما جاء في الملحق الخاص باتفاقيات جنيف الأربع والمادة الأولى (الفقرة الثانية) من البروتوكول الإضافي الأول لسنة ١٩٧٧ على الشكل التالي : " في حالة عدم وجود قاعدة قانونية معينة في القانون التعاهدي يظل المتحاربون في حمى وسلطة القانون العرفي ومبادئ الانسانية وما يمليه الضمير العام "[٧٨].

---

[٧٧] دليل تالين بشان القانون الدولي المطبق على الحروب السيبرانية، القاعدة٤٢ : " يحظر استخدام وسائل وأساليب الحرب السيبرانية التي من شأنها أن تسبب أضرار زائدة وآلاماً لا مبرر لها" .

[٧٨] Https://icrc.org/ar/doc/resources/documents/misc/62sd4j.htm

اذاً نستنتج من الاتفاقيات السابق ذكرها أن لمبدأ مارتنز ثلاث ركائز أساسية :

أ- العادات الراسخة بين الشعوب: و يقصد بها الأفعال المتكررة الراسخة بين الشعوب المتحضرة التي استقر التعامل الدولي على الأخذ بها على مرّ العصور فاكتسبت قوةّ العرف الدولي .

ب- أحكام الضمير العام : اشترط مبدأ مارتنز أن يتضمن تعبيراً عن المشاعر العامة القوية المتصلة بالسلوك الانساني , حيث عّرف هذا المبدأ الضمير العام أنه الشعور العام الدولي الذي يتمثل بمجموعة القرارات والإعلانات الدولية المقدمة من شخصيات ومؤسسات مؤهلة لتقييم القانون الدولي في حال كان هو بالفعل يراعي الشعور العام الدولي، لذلك فالشعوب والمقاتلون يتمتعون بحماية وسلطان القانون الدولي عامةً والعرفي خاصةً .

ج- القوانين الانسانية : هي مجموعة من القواعد الرامية الى الحدّ من اثار النزاعات المسلحة لدوافع انسانية من خلال تقييد حق اختيارالوسائل والأساليب المستعملة في الحرب، فشرط مارتنز أشار الى المبادئ او القوانين الإنسانية كجزء من القانون الدولي التي يشار اليه في حال عدم وجود نص قانوني صريح [٧٩]، كذلك أعطي لهذا المبدأ سلطة مهمة حسب ما اشارت اليه محكمة العدل الدولية في رأيها الاستشاري لعام ١٩٩٦ المختص بشرعية التهديد وإستعمال الأسلحة النووية التي اعتبرت :" يمنح شرط مارتنز سلطة معالجة مبادئ القانون الدولي الانساني و ما يمليه الضمير العام بوصفهما مبادئ من القانون الدولي تركاً المحتوى الدقيق للمعيار الذي سيلزمه مبادئ القانون الدولي على ضوء الظروف المتغيرة بما في ذلك التغيرات في وسائل الحرب ومستويات مظهر المجتمع الدولي وتسامحه " . [٨٠]

كذلك شيميت Schmitt عند معالجته للهجمات السيبرانية اعتبر ان مبدأ مارتنز هو المبدأ الأكثر قرباً لكونه يطبق على الحالات الغير منظمة في الإتفاقيات الدولية ولا ذلك يعتبر ممكناً الاّ باللجوء الى القانون الدولي الإنساني العرفي وهذا ما أكدته المادة ٣٨ من النظام الأساسي لمحكمة العدل الدولية .[٨١]

الاّ ان عبارتي "مبادئ الانسانية وما يمليه الضمير العام " التي توحي للقارئ أنها قواعد غير ملزمة، هل هي بالفعل كذلك ؟

يمكننا الإجابة على هذه الإشكالية وفق ما ورد في حكم الولايات المتحدة الامريكية العسكرية في قضية (كروب) عام ١٩٤٨ التي أشارت في حكمها "أن شرط مارتنز اكثر من مجرد إعلان وردع وإنما هو شرط عام يجعل القادات مستقرة بين الأمم المتحضرة وقوانين الانسانية، وما يمليه الضمير العام جزءاً من المقاييس القانونية التي يجب تطبيقها اذا لم تعطي أحكام الإتفاقيات حلول للحالات المحددة "، إذاً مبدأ مارتنز يحتل أهمية كبرى على الصعيد الدولي لإنطباقه على النزاعات الدولية المسلحة وغير الدولية في ظل عدم وجود اتفاقية دولية تنظم الحالات المستحدثة لذلك يبرز أهمية شرط مارتنز في اعتباره جزءاً لا يتجزأ من

---

[٧٩] أيات محمد سعود :" دراسات و أبحاث قانونية ، العدد ٥٨١٠ في ٩-٣-٢٠١٨ على الموقع :
https://www.ahewar.org/debat/show.art.asp?aid=591797

[80] أحمد عبيس نعمه فتلاوي، مرجع سابق، ص ٦٣

[٨١] Michael N.Schmmitt :" wired warfare : computer network attack and jus in Bello" , International Review of the Red Cross ,2022, p369-370

القانون الدولي الانساني وذلك بهدف استقراء الحالات غير المتوقعة ويسهم في سدّ ثغرات القانون ويساعد في تطوره مستقبلياً عبر تبيان المسار الذي ينبغي اتباعه .

٥. مبدأ الانسانية :

يطبق هذا المبدأ حصراً على المقاتلين والجماعات المسلحة والمدنيين المشاركين في العمليات العدائية ويتضمن ضرورة عدم التسبب بمعاناه لا جدوى منها أو غير مبررة وهو من المبادئ الأساسية الواجبة التطبيق في إطار الهجمات السيبرانية ويؤكد خبراء تالين على أن هذا المبدأ يطبق في النزاعات المسلحة الدولية وغير الدولية.

لقد إنتهينا من تبيان كيفية المبادئ الإنسانية التي ترعى سير العمليات العدائية السيبرانية سوف ننتقل الى توضيح كيفية التصدي للهجمات السيبرانية ميدانياً.

المبحث الثاني : كيفية التصدي ميدانياً للهجمات السيبرانية

في هذا المبحث سوف نبين الحقوق المعترف بها للدولة المعتدى عليها في دفع الإعتداء السيبراني الموجه ضدها من خلال ممارسة حقها في الدفاع الشرعي (الفرع الأول) وتوجيه تدابير مضادة(الفرع الثاني) .

الفرع الأول : شروط ممارسة حق الدفاع الشرعي

تضمنت المادة الثانية (الفقرة الثالثة) من ميثاق الأمم المتحدة على ما يلي :" يلتزم دول الأعضاء بضرورة فض المنازعات بالوسائل السليمة على وجه لا يجعل السلم والأمن الدولي عرضة للخطر "، ومفاد هذه الإتفاقية ضرورة حل النزاعات بالطرق السلمية دون اللجوء الى العنف، بمعنى آخر أنه يحّرم اللجوء الى القوة أو التهديد بإستخدامها في العلاقات الدولية، وهذا ما أكدته المادة الثانية (الفقرة الرابعة) من ميثاق الأمم المتحدة :" يمتنع اعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد بإستعمال القوة أو إستخدامها ضد سلامة الأراضي أو الإستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة"، فلا يمكن لأي دولة أن تلجأ الى القوة أو التهديد من أجل تسوية النزاعات والمشاكل الدولية بل الإلتزام بالأحكام الخاصة بهذا الميثاق، يعتبر هذا المبدأ من القواعد الآمرة التي يمنع مخالفتها وإن إستخدام تعبير القوة يغطي" كل الصور مثل العدوان المباشر وغير المباشر والحرب ووسائل إستخدام القوة المسلحة التي تعتبر اقل من الحرب وكذلك صورة وسائل المساعدة الذاتية المسلحة، كذلك منع التهديد بإستخدام القوة وليس الإستخدام الفعلي لها" [٨٢]، ولكن الى أي مدى يمكن تكييف الهجمات السيبرانية كإستخدام للقوة في القانون الدولي؟ وهل يحق للدولة المعتدى عليها سيبرانياً أن تلجأ الى ممارسة حقها في الدفاع الشرعي والرد على ما تتعرض له من هجمات؟ لهذا الحق قيود وشروط معينة سوف نتطرق اليها في هذا الفرع لتوضيح أهمية هذا الموضوع ودقته دوليا وفقاً للآراء الفقهية المختلفة.

١ . الرأي الضيق لمفهوم القوة (المعيار القائم على الوسيلة) Instrument-Based

[٨٢] عبد العزيز رمضان على الخطابي : الدفاع الوقائي في القانون الدولي العام " , ط٢٠١١دار الجامعة الجديدة , الاسكندرية – مصر –, ص ٩٦

اعتبر كل من Christopher DeLucaو Oonss Hathaway ان مفهوم القوة هو عبارة عن القوة المسلحة وفقاً للأفعال المشار اليها في المادة الثانية (الفقرة الرابعة) من ميثاق الأمم المتحدة، التي اعتبرت أن الأفعال المختصة بالقوة هي كالعدوان المسلح، والغزو والهجوم المسلح الذي يوجه الى الدولة المعادية أي أن الهجمات التي لا تستخدم الأسلحة التقليدية لا تعتبر هجوماً مسلحاً وإستخداماً للقوة، فالعبرة في النتائج التي تحدثها هذه الهجمات من خسائر مادية وبشرية جسيمة كي تعتبر خاضعة للمادة المذكورة أعلاه وبالنظر الى أصحاب هذا الرأي أن الأثار الاقتصادية والسياسية وغيرها التي لا ينتج عنها خسائر في الأرواح والممتلكات تعتبر غير خاضعة لأحكام المادة الثانية – فقرة رابعة من الميثاق، برأينا أن أشكال إستخدام القوة المسلحة فضلاً عن أي شكل أخر يترتب عليه التأثير وإنتهاك واضح للأمن القومي لدولة أخرى تعتبر إستخداماً للقوة وإنتهاك للمبدأ المذكور .

٢. وفق Milam Sahovic أن العديد من الإعتداءات لا تتضمن العنصر الحركي المطلوب في الحرب التقليدية نذكر منها : الحصار الجوي والبحري والضغوط الاقتصادية وقطع العلاقات الاقتصادية والخطوط الحديدية و البحرية و البرية والهجمات البيولوجية والجرثومية والأمراض المفتعلة واي امرٌ آخرٌ من شأنه أن يعرض الدولة الضحية للضغط، فالأدوات العسكرية والاقتصادية والدبلوماسية والإستخباراتية والإديولوجية والعلمية والتكنولوجية جميعها وسائل وأشكال متعددة لإستخدام القوة، فمعيار الجسامة في الهجمات السيبرانية غير ضروري كي نعتبر هذا الفعل هو إستخدام للقوة بل أي هجمة تؤدي الى تعطيل أنظمة الحاسب الرئيسية للدولة والتسبب في شل مفاصل الدولة أو حدوث أضرار اقتصادية دون أن تؤدي الى خسائر مادية يمكن اعتبارها استخدام للقوة وفقاً للمادة ٤/٢ من الميثاق[٨٣] ، مما يحتم إدراج الهجمات السيبرانية ضمن المادة ٣٩ من الميثاق التي تنص على ما يلي :

" يقرر مجلس الأمن ما اذا كان قد وقع تهديد للسلم او اخلال به او كان ما وقع عملاً من أعمال العدوان ويقدم في ذلك توصياته أن يقرر ما يجب اتخاذه من تدابير طبقاً لأحكام المادتين ٤١ و٤٢ لحفظ السلم و الأمن الدولي أو اعادته الى نصابه "، وفق هذه المادة يعود لمجلس الأمن وفقاً لأحكام هذه المادة تكييف أي تصرف أو فعل صادر على أحد دول الأعضاء في الأمم أو اذا كان هذا الأخير يعرض سلامة هذه الدول للخطر، مما يحتم ادراج الهجمات السيبرانية ونتائجها ضمن هذا البند وذلك بهدف الحدّ منها ولحماية الدول الاضعف تقنياً وإلكترونياً، فالمادة ٤١ تضمنت تحديداً إجراءات وتدابير خاصة لقمع العدوان من خلال وسائل لا تشمل القوة المسلحة حيث نصت: " لمجلس الأمن أن يقرر ما يجب اتخاذه من تدابير التي لا يتطلب استخدام القوات المسلحة لتنفيذ قراراته وله ان يطلب الى أعضاء الأمم المتحدة تطبيق هذه التدابير ويجوز ان يكون من بينها وفق الصلات الاقتصادية والمواصلات الحديدية والبحرية والجوية والبرية واللاسلكية وغيرها من وسائل الموصلات وقفاً جزئياً أو كلياً وقطع العلاقات الدبوماسية " ، كذلك المادة ٤٢ من ميثاق الأمم المتحدة التي نصت : " اذا راى مجلس الأمن أن التدابير المنصوص عليها في المادة ٤١ لا تفي بالغرض أو تثبت أنها لم تف به له أن يتخذ بطريق القوات البحرية والجوية والبرية من الأعمال ما يلزم لحفظ الأمن الدولي و السلم أو لاعادته الى نصابه و يجوز أن تتناول هذه الأعمال والمظاهرات والحصر والعمليات الأخرى بطريق القوات البحرية والجوية والبرية التابعة لأعضاء الأمم المتحدة ".

---

[٨٣] شريف نسيم قلته بخيت : " دليل تالين : الهجمات الالكترونية و حظر استخدام القوة في القانون الدولي " , بحث منشور على الموقع الرسمي للمركز العربي لأبحاث الفضاء الالكتروني في ٢٥-١١-٢٠١٧ , ص ١

أكد دليل تالين للقانون الدولي المطبق على الحرب السيبرانية ما تقدم في المادة العاشرة من الفصل الثاني : " العملية السيبرانية التي تتضمن التهديد أو إستخدام القوة ضد سلامة الأراضي أم الإستقلال السياسي لأي دولة أي تلك(العملية السيبرانية) التي لا تتفق بأي وجه آخر مع مقاصد الأمم تعتبر غير شرعية "، كذلك المادة ١١ من الفصل نفسه التي عرفت استخدام القوة: " تشكل العملية السيبرانية إستخداماً للقوة عندما يكون حجمها وآثارها قابلة للمقارنة مع العمليات غير السيبرانية التي تصل لمستوى إستخدام القوة "، أما المادة ١٢ من الفصل نفسه عرفت التهديد بإستخدام القوة في العمليات السيبرانية : " العملية السيبرانية أو التهديد بالعملية السيبرانية يشكل تهديداً غير شرعي باستخدام القوة عندما يكون العمل المهدد به في حال تنفيذه سوف يعتبر استخدام غير شرعي " .

٣.معيار التماثل مع الهجمات التقليدية Analogous to Instrument

أي الهجمات التي تحدث آثار مماثلة لتلك التي تسببها الحرب التقليدية كي نعتبر أن هذه الهجمات هي إستخدام للقوة ومفعلّة لممارسة حق الدفاع الشرعي من قبل الدولة الضحية [٨٤].

4.معيار عواقب الهجوم Conseqences-Based

يركز هذا المعيار على الأثار التدميرية في الأرواح والأعيان المحمية دون بالضرورة أن تتساوى مع تلك التي تسببها الهجمات التقليدية.

5.معيار الحجم والأثار أو معيار شيميت : نصت المادة ١١ من دليل تالين : " تشكل العملية السيبرانية إستخداماً للقوة عندما يكون حجمها وآثارها قابلة للمقارنة مع العمليات غير السيبرانية التي تصل لمستوى استخدام القوة " وخلاصة هذه المادة أننا من أجل تصنيف اذا كانت العملية تصل الى مستوى استخدام القوة،لا بدّ تحليل اذا كانت بحجم و تأثير العمليات غير السيبرانية أي التقليدية .

كذلك المادة ٤٢ من ميثاق الأمم المتحدة التي نصت : " اذا رأى مجلس الأمن أن التدابير المنصوص عليها في المادة ٤١ لا تفي بالغرض أو تثبت أنها لم تف به له أن يتخذ بطريق القوات البحرية والجوية والبرية من الأعمال ما يلزم لحفظ الأمن الدولي والسلم أو لاعادته الى نصابه ويجوز أن تتناول هذه الأعمال والمظاهرات والحصر والعمليات الأخرى بطريق القوات البحرية والجوية والبرية التابعة لأعضاء الأمم المتحدة ".

إنطلاقاً من هاتين المادتين نشير أن القوة لا تشمل فقط القوة المسلحة بل ايضاً إجراءات وتدابير لقمع العدوان من خلال وسائل جديدة مستخدمة من قبل الدولة المعتدية، اذاً كما أشرنا أن هناك إستثناءاً على مبدأ عدم جواز اللجوء الى القوة في العلاقات الدولية وهو مبدأ الدفاع الشرعي وهذا ما أكدته المادة ٥١ من ميثاق الأمم المتحدة التي نصت : " ليس في هذا الميثاق ما يضعف أو ينقص الحق الطبيعي للدول فرادى أو جماعات في الدفاع عن أنفسهم اذا اعتدت قوة مسلحة على أحد أعضاء الأمم المتحدة وذلك أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدوليين والتدابير التي اتخذها الأعضاء إستعمالاً لحق الدفاع عن النفس تبلغ الى المجلس فوراً ولا تؤثر تلك التدابير بأية حال فيما للمجلس بمقتضى مسؤولياته وسلطته المستمرة من أحكام هذا الميثاق من الحق أن يتخذ في أي وقت ما يرى ضرورة لاتخاذه من الأعمال لحفظ السلم والأمن الدولي أو اعادته الى نصابه "، كذلك المادة الثانية من بروتوكول جينيف للعام ١٩٢٤ التي

[٨٤] علي محمد كاظم الموسوي، مرجع سابق، ص ٤٤

جاء فيها : " الدول الموقعة قد اتفقت على أنها سوف لا تلجأ للحرب وسيلة لفض النزاعات بأي حال الاّ في حالة قيام العدوان ".

الاّ أننا أمام استثنائين فقط يجيز فيهما القانون الدولي إستخدام القوة وهما : حالة الدفاع الشرعي وحالة وقوع عمل عدواني يبرر تدخل قوى الأمن (الفصل السابع من الميثاق) .

اذاً لقيام حالة الدفاع الشرعي يجب أن نكون أمام حالة عدوان منشأة له وشروطه أربعة [٨٥]:

الشرط الأول : أن يكون العدوان مسلحاً

١. أي أن يكون ذا صفة عسكرية : يجب أن يكون العدوان بقوات مسلحة عسكرية برية أو بحرية أو جوية على حسب ما ورد في في المادة ٥١ من الميثاق :" اذا اعتدت قوة مسلحة" و أن يكون بدأ فعلاً ضد الدولة بغض النظر عما اذا كان العدوان المسلح تم بإستخدام قوات نظامية كالجيش أو غير نظامية كالعصابات المسلحة والجماعات والتنظيمات الارهابية سواء تم على الدولة نفسها أم على رعاياها المتواجدين في دولة أجنبية .

٢. أن يكون الهجوم المسلح على درجة كبيرة من الجسامة

فالحوادث البسيطة التي يمكن حلها بالطرق السلمية لإقتضاء الدولة المعتدى عليها كحصولها على تعويض أو الاعتذار، وللتحقق من هذا الشرط يتعين تحديد عدد وحجم القوات القائمة بالعدوان ومدى تسلحها وفعالية تلك الأسلحة.

٣. أن يتواجد القصد العدواني في الدولة المعتدية

هو الركن المعنوي لجريمة العدوان، فلا بدّ أن يكون التصرف الصادر عن الدولة تم عن قصد وعمد بالتعدي أما اذا كان عن طريق الخطأ فهنا لا تستطيع أن تستخدم حق الدفاع وانما يمكنها أن تطالب بالتعويض، مثلاً ان تقوم الدولة المعتدية بتدريبات عسكرية وعن طريق الخطأ تلحق بالدولة المعتدية أضرار معينة .

الشرط الثاني : أن يكون العدوان حالاً ومباشراً : في حال كانت حالة العدوان على وشك الوقوع ولم تبدأ بعد ولكن نحن أمام أفعال تدل على أنه بصدد وجود عدوان قريب وفي حال قد وقع بالفعل ولكن لم ينته بعد عندئذ يمكن قيام حق الدفاع الشرعي أما في انتهى فتنتفي عنه صفة الحال .

الشرط الثالث : أن يعتبر العدوان غير مشروع

نعني به أن الدولة المعتدى عليها لها أن تحتج بالدفاع الشرعي عن نفسها وذلك بوجه أي خطر غير مشروع تتعرض له والدولة المعتدية هنا لا يحق لها أن ترد على هذا الدفاع عملاً بقاعدة "لا دفاع ضد دفاع" أي أنه لا يحق لها ان تحتج أن الخطر غير مشروع الذي تتعرض له .

الشرط الرابع : أن يكون العدوان ماساً بأحد الحقوق الأساسية للدولة

[٨٥] العمري رقار منية : " الدفاع الشرعي في القانون العام " –جامعة الأخوة منتوري، كلية الحقوق والعلوم السياسية، رسالة ماجستير، الجزائر، عام ٢٠١١، ص ١٢٠

بموجب المادة الثانية (الفقرة الرابعة) من ميثاق الأمم المتحدة للدولة الحق بسلامة أراضيها وإقليميها الجوي وحق تقرير المصير وإستقالها السياسي وان اي إعتداء يقع عليها غير مشروع يرتب حق الدفاع الشرعي.

الشروط القانونية للدفاع الشرعي[٨٦] :

.1 إلزامية الدفاع : أن لا نكون أمام أي طريقة سلمية يمكنها أن تؤدي الى درء العدوان وأن لا تكون الدولة أمام خيار آخر لدفع العدوان عنها سوى القوة المسلحة .

٢. أن يوجه فقط الى الدولة المعتدية : لا بدَ أن توجه الدول المعتدى عليها الدفاع بوجه بوجه الدولة المعتدية دون المحايدة لأنه في حال وجهت تدابير الدفاع الشرعي الى دولة محايدة قصداً أم عن طريق الخطأ نكون أمام جريمة دولية .

٣.أن يكون مؤقت : وفق ما جاء في المادة ٥١ من الميثاق التي إعتبرت أنه من الضروري توقف الدفاع الشرعي عند إتخاذ مجلس الأمن التدابير الإجراءات اللازمة لحفظ السلم والأمن الدوليين وإعادتهما الى نصابهما .

٤. أن يكون متناسباً مع العدوان : بمعنى آخر أن تكون الوسيلة المستخدمة من قبل الدولة المعتدى عليها متناسبة من حيث القوة والجسامة مع الوسيلة المستخدمة من قبل الدولة المعتدية وذلك عبر الردّ فقط في حدود القدر الكافي لصدّ العدوان دون أي تجاوز .

تكييف الهجمات السيبرانية وفقاً للمادة ٥١ من ميثاق الأمم المتحدة :

نصت المادة ١٣ من دليل تالين : " يجوز للدولة التي تكون هدفاً للعمليات السيبرانية التي تصل لمستوى الهجوم المسلح أن تمارس حقها الطبيعي في الدفاع عن النفس وتعتبر العملية السيبرانية هجوماً مسلحاً بالإعتماد على حجمها وآثارها " أي عند تساوي الهجوم السيبراني بالهجوم المسلح وإستخدام القوة المسلحة و ترتب عليه النتائج ذاتها المترتبة على استخدام القوة المسلحة مهنا يحق للدولة أن تمارس حقها الطبيعي في الدفاع كما يمكن وبناءً على طلب من الدولة الضحية وضمن نطاق هذا الطلب أن يكون لها الحق في الدفاع الجماعي ضد العملية السيبرانية التي تصل لمستوى الهجوم المسلح [٨٧]، على أن تبلغ الدولة مجلس الأمن التابع للأمم المتحدة فوراً عن تدابيرهذا الدفاع وفقاً للمادة ٥١ من الميثاق [٨٨].

وفقاً لدليل تالين يعطى للدولة الحق بتفعيل المادة ٥١ من الميثاق بتوافر مجموعة من الشروط :

١. الحدة أو شدة الدمار Severity

لكي يعتبر التصرف الصادر في العمليات السيبرانية بمثابة هجوم مسلح لا بدّ أن يرتقي الى مستوى جسامة أو حدة مطلوبة من الدولة المعتدية، فجوهر هذا المعيار يتمثل في الضرر المادي الذي يلحق بالأفراد أو الممتلكات في الدولة المعتدى عليها سيبرانياً، فالعمليات السيبرانية ترتقي الى مستوى الهجوم المسلح عندما يقع ضرراً جسيماً يحتم تصنيف العملية السيبرانية بالهجوم المسلح ولكن المشكلة هنا بالنسبة الى الهجمات

---

[٨٦] سليمان عبدالله سلمان :" المقدمات الأساسية في القانون الدولي الانساني " , ديوان المطبوعات الجامعية , الجزائر , ص ١٥٧

[٨٧] دليل تالين، مرجع سابق، المادة ١٦

[٨٨] دليل تالين، مرجع سابق، المادة ١٧

السيبرانية التي لا ترتقي الى مستوى النزاع المسلح أي الهجمات التي لا تتسبب أضرار في الأرواح والممتلكات، فالسؤال هنا ما هو المستوى المطلوب في حدة الضرر كي نبدأ بالحديث عن هجوم سيبراني يرتقي الى مستوى الهجوم المسلح؟، الأضرارالمادية الواقعة على الأفراد أو الممتلكات تحتم اعتبار هذه العملية الالكترونية بمثابة هجوم عسكري كالإعتداء على شبكات الكمبيوتر الخاصة بمطار العاصمة في الدولة الذي أدى خسائر كبيرة في الأرواح نتيجة تصادم الطائرات هبوطاً وصعوداً، ولكن هناك أضرار تلحق بالأفراد أو الممتلكات وتعتبر أضرار غير جسيمة ولا تشكل هجمة سيبرانية وهذا ما عبرت عنه محكمة العدل الدولية في قضية نيكارغوا عندما فرقت بين الأعمال الأكثر خطورة والأقل خطورة بحيث الأعمال الأقل خطورة لا تجيز للدولة الحق في الدفاع وفقاً للمادة ٥١ من الميثاق وإنما إجراءات أخرى يمكن أن تلجأ اليها كالتدبير المضاد [٨٩]، لكن لا بدّ أن يستقر الفقه على معيار معين لمعرفة ما الذي يعتبر جسيم وما الذي يعتبر أقل جسامة .

ثانياً : الضرر" الأني " أو الحال Immediacy

وفقاً للمادة ١٥ من دليل تالين حول الوشاكة أو الآنية نصت :" الحق في استخدام الدفاع عن النفي ينشأ في حالة حدوث هجوم مسلح أو وشك الوقوع من ناحية أخرى يكون هذا الدفاع محل شرط الفورية "، اذاً ينشأ حق الدفاع في حال وقع الهجوم المسلح أو اذا كان على وشيك الوقوع على أراضيها وإمتناعها عن القيام بالأمورااللازمة لتجنب وقوع الضرر من خلال تواصلها بالدولة منشأ الإعتداء للتراجع عن هذا التصرف مما يؤدي الى نفي شرط الضرر الأني وبالتالي لا يمكن أن يرتقي الى كونه استخداماً للقوة طالما أن الدولة المستهدفة فرطت بنافذة زمنية كانت تستطيع أن تستغلها لدرء الضرر عنها : فالخطر الاني أو الحال هو الذي سوف يقع لا محالة دون أي قدرة للدولة المعتدى عليها ولا بأي طريقة على تفاديه.

ثالثاً : أن يكون أثر الهجوم مباشراً Directness

نعني بهذا الشرط أن الأثر الناتج عن الضرر لا بد أن يكون مباشراً، أي أن نكون أمام علاقة سببية مباشرة بين التصرف والنتيجة مثلاً : وجود عمليات الكترونية وجهت الى سوق الأسهم في دولة ما مما أدى الى إنكماشٍ إقتصاديٍ بطيءٍ، وهو نتيجة مباشرة للعملية الإلكترونية ولكنه خرج بشكله النهائي بعد فترة طويلة من الزمن، ولكن ممكنٍ أن نكون أمام نتيجة مختلفة مفادها أن إقتصاد تلك الدولة كان أصلاً ضعيفاً، فالعملية الإلكترونية هنا لم تكن هي السبب الحقيقي والمباشر لوقوع الضرر ويشار الى أنه وبالرغم أن الشرط الآني والشرط المباشر متمايزين الى أنهما في غلب الأحيان متلازمان، فالهجوم الحال غير المباشر من الممكن تصوره ولكن هجوم غير حال ومباشر من الصعب تصوره كأن تعتقد مثلاً دولة ما مثلاً أن الهجوم تم على شبكة معلوماتية هي مدمرة أصلاً، فهذه الأخيرة هي مدمرة أصلاً ولا تستطيع أن تحدث ضرراً اضافياً ولا يرقى التصرف الى عتبة الهجوم العسكري[٩٠].

رابعاً : أن يكون الهجوم بهدف الإعتداء

يتمثل هذا الشرط بالنية العدائية المتوافرة في الهجوم السيبراني(الركن المعنوي لجريمة العدوان) ، فلا بدّ أن تكون نية الدولة المعتدية ممنهجة نحو تحقيق أهداف عدائية في الدولة المعتدى عليها اي هدف الحاق

[89] International Court of Justice – Nicraragua Judgment, op,cit p191

[٩٠] رزق أحمد سمودي، مرجع سابق، ص ٣٥٤-٣٥٥

الأضرار في مصالح هذه الأخيرة ولكن النقاش الذي يطرح هنا هو امكانية اثبات النية العدائية من وراء اي تصرف تقوم به الدولة المعتدية، فإثبات النوايا هي عمليةُ معقدةُ وصعبةُ وغيرأكيدةٌ، فكيف يمكننا اثبات أن النية هي نية عدائية ؟

إن عملية إثبات النية العدائية ومدى توافرها لا تتم الاّ من خلال عملية قضائية وبقرار قضائي ولكن أن هذه العملية صعبة لعدم وجود اختصاص قضائي دولي الزامي في مسألة الهجمات السيبرانية، لذلك اعتمد دليل تالين على نظرية مفادها أن شرط العدائية الوارد في المادة ٥١ من الميثاق يمكن أن يوضح من خلال استهداف الدولة مصدر الهجوم شبكات الكترونية محمية ومؤمنة كالإعتداء على الشبكات الخاصة بوزارة الدفاع في دولة ما كونها هي من أكثر الشبكات المحمية من الدولة، فهنالك علاقة أساسية قائمة بين درجة الحماية للشبكة الالكترونية المستهدفة وشرط العدائية [٩١].

خامساً : إسناد التصرف بالدولة Invasiveness

إنطلاقاً من مبدأ السيادة، إن كل دولة تحدد وبحرية تامة قراراتها ولكن وبالمقابل يفرض عليها واجب الالتزام بالموجبات الدولية المفروضة عليها، وفي حال خلت بها يترتب عليها مسؤولية دولية معينة، بحيث عرفت هذه المسؤولية " أنها عملية اسناد فعل الى أحد اشخاص القانون الدولي سواء كان هذا الفعل يحظره القانون الدولي أم لا ما دام قد ترتب عليه ضرر لأحد أشخاص القانون الدولي، الأمر الذي يقتضي توقيع جزاء دولي معين سواء كان هذا الجزاء ذات طبيعة عقابية أم كان ذات طبيعة غير عقابية "[٩٢]، اما بالنسبة الى الهجمات السيبرانية، هناك الكثير من الصعوبات التي تعترض اثبات أن التصرف صادر عن الدولة المعتدية كالتالي :

١. صعوبة اثبات هوية الفاعل الحقيقي وخاصة اذا كان يمثل الدولة أم لا .

٢. صعوبة اثبات أن الهجمات السيبرانية تمت على أراضي الدولة المعتدية ووجهت الى أراضي الدولة المعتدى عليها وخاصة في الحالة التي تستخدم فيها اقليم دولة ثالثة أي أن الدولة التي وجهت هجمات ضد دولة ب من خلال أراضي دولة ج و دون علم الدولة ب، وخاصة في حال قامت مجموعات تابعة للدولة ولكنها تجاوزت الصلاحيات المعطاة لها او خالفت التعليمات مما يعتبر التصرف صادر عن الدولة وتتحمل المسؤولية الدولية .

سادساً : وضع نتائج الهجمات السيبرانية أو القدرة على قياسها Measurability of effects

لا بدّ أن تكون الدولة قادرة على تحديد الأضرار التي تسببت بها الهجمات السيبرانية أو لديها الأدوات الكافية لقياس هذه الأضرار، فالأضرار الغير خطرة أو عرضية أو ثبت مثلاً أن تكون في الأساس المنشآت التي تعرضت للهجمات هي في الأصل هشة وضعيفة، فالهجوم هنا لم يكن سوى دافع جديد أدى الى إنهيارها مما فقد كانت هذه المنشات قد تعرضت قبل الهجوم الى أضرار كثيرة اضعف قوتها وأتى الهجوم ليسارع دمارها، فهل تترتب المسؤولية الدولية ؟ يمكن أن نعتبر تارةً أن الدولة المعتدية مسؤولةً عن الأضرار بقدر الضرر التي ألحقته الهجمات في حال كان هناك إمكانية لقياس الضرر الذي الحق بالمنشأة

[٩١] رزق أحمد سمودي، مرجع سابق، ص ٣٥٥-٣٥٦

[٩٢] شيخة حسين الزهراني، مرجع سابق، ص ١٣٠

ويمكن تارةً أخرى أن ننفي المسؤولية الدولية في هذا الإطار وذلك لأن المنشات هي في الأصل متضررة والهجوم لم يكن سوى عامل اضافي سّرع إنهيارها .

انطلاقاً من النية العدائية المتوافرة لدى الدولة المعتدية وان كانت المنشآت هي في الأصل متضررة فتترتب المسؤولية الدولية كون أن الدولة المعتدية لم تكن تعلم بأن المنشأة متضررة بل كانت تهدف من هذا الهجوم الحاق الأضرار بها، فقد قامت بعمل غير مشروع وغيرمباح دولياً وخشيةً من الحؤول دون توقيع العقاب بحقها ننظرالى أهمية انعقاد المسؤولية الدولية كي نتمكن من محاسبتها وفرض العقاب اللازم[٩٣].

سابعاً : الطابع العسكري للهجمات السيبرانية Military Character

كلما كان هنالك ترابط بين هذه الهجمات والحرب التقليدية كلما كان هنالك إمكانية إعتبار أن هذا الهجوم هو استخدام للقوة وفق المعنى المنصوص عنه في دليل تالين.

سوف ننتقل الى توضيح الحق الثاني المعطى للدولة الضحية في رد الإعتداء عنها وهي التدابير المضادة في الفرع الثاني من هذا المبحث .

الفرع الثاني : التدابير المضادة

التدابير المضادة هي عبارة عن إجراءات ضرورية ومتناسبة تتخذها الدولة الضحية للرد على إنتهاك الدولة المخالفة للقانون الدولي مع ضرورة وجود شروط معينة من حيث الشكل والمضمون ويكون الهدف حث الدولة المخالفة على الامتثال للقانون الدولي، فهي في الأصل غير قانونية لولا تصرف الدولة المخالفة، أيضاً عرفها معهد القانون الدولي في دورته العادية لعام ١٩٣٤على أنها " تدابير قسرية إستثنائية من وجهة القواعد الاعتيادية للقانون الدولي تتخذها دولة علة أثر فعل غير مشروع ضار بها صادر عن دولة اخرى لحمل الاخيرة على احترام القانون عن طريق الأضرار بها، فهي العمل اللاحق الذي يتخذ بناءً على عمل غير مشروع " [٩٤]، فهي تدابير سلمية غير مصحوبة باستعمال القوة العسكرية بسبب عدم تنفيذ إلتزام دولي تجاه الدولة قامت بانتهاك التزاماتها ويخضع تقدير هذه الالتزامات للدولة المتضررة شرط أن تكون متناسبة وحجم الإنتهاك المذكور وأن تكون مؤقتة ومع ذلك يجب ان لا تؤثر التدابير المضادة في حظر اللجوء الى القوة وغيرها من الإلتزامات بموجب القواعد الآمرة للقانون الدولي" .[٩٥]

أيضاً قررت المادة التاسعة من دليل تالين على أنه : " يجوز للدولة التي أصيبت بفعل غير مشروع دولياً اللجوء الى إتخاذ التدابير المضادة المتناسبة بما في ذلك التدابير المضادة السيبرانية ضد الدولة المسؤولة " ، تعليقاً على القاعدة أعلاه في حال توقف الفعل غير المشروع دولياً لا يحق للدولة المتضررة الشروع او الإستمرار في إتخاذ التدابير المضادة بما في ذلك السيبرانية منها، ولا يمكن اللجوء الى هذه التدابير الاّ بعد مطالبة الدولة المعنية بوقف فعلها غير المشروع دولياً و لكن للدولة الضحية الحق في اتخاذ تدابير مضادة ضرورية للحفاظ على حقوقها حتى قبل وقوع الضرر، اما الشرط الأهم : كي يحق للدولة الضحية اللجوء الى التدابير المضادة لا بدَ أن تتحقق مسؤولية الدولة وفقاً للمادة السادسة من دليل تالين التي نصت " تتحمل

---

[٩٣] شيخة حسين الزهراني، مرجع سابق، ص ١٣٧-١٣٨

[٩٤] محمد حتحاني : التدابير المضادة في القانون الدولي(حالة الدول) "إشراف حامدو الهاشمي، جامعة الجزائر-كلية الحقوق بن عنكون، رسالة ماجستير، الجزائر، عام ٢٠١٠ , ص٨

[٩٥] اياد يونس محمد الصقيلي : " الحظر الدولي في القانون الدولي العام : دراسة قانونية "، طبعة ٢٠١٤، دار الفكر الجامعي، الاسكندرية، مصر، ص٦٨

الدولة المسؤولية القانونية الدولية للعمليات السيبرانية التي تنسب اليها والتي تشكل خرقاً لالتزام دولي "، أما خصائص التدابير المضادة هي كالتالي :

١. شكل من أشكال المساعدة الذاتية : يحق للدولة ان تتخذ بنفسها التدابير والإجراءات اللازمة التي تراها مناسبة عندما تتعرض لأي نوع من أنواع الأعمال غير المباحة دولياً كي تحث الدولة المعتدية إحترام إلتزاماتها التي خلت بها وان يكون هدف هذه التدابير إستعادة العلاقة القانونية بينها وبين الدولة الضحية بعد تأثرها بسبب الفعل غير المشروع دولياً .

٢. هي تدابير إنفرادية : تتخذها الدولة بناءً على تقديرها الذاتي لمشروعية الأعمال التي ترتكب بحقها لذا تعتبر في المقام الاول نظام فردي بسبب عدم وجود سلطة دولية لتنفيذ احكام القانون الدولي وتنفي لها نظام الفردية .

٣.عدم مشروعية التدابير المضادة في الأصل : هذه التدابير هي غير مشروعة في أصلها أي في ذاتها في حال لم ينظر الى الاحوال المحيطة بها، بل هي تصبح مشروعة عندما تكون موجهة الى الدولة المعتدية، تقوم هذه الاخيرة بأعمال وهجمات غير مشروعة بحق الدولة الضحية فتعمد هذه الاخيرة الى توجيه تدابير مضادة بهدف الدفاع عن مصالحها أولاً ومن أجل حث الدولة المعتدية الى تحمل مسؤوليتها الدولية، لذلك الدولة الضحية في حال قامت بهذه الأعمال دون أي هجوم شن عليها تترتب مسؤوليتها طالما ان هذه الأفعال هي غير قانونية في الأصل.[٩٦]

٤. إستثنائية التدابير المضادة : هذا النوع من التدابير تشكل استثناءاً عن القاعدة المعترف بها دولياً والتي تلزم الدول بحل الخلافات بالطريقة السلمية بشكل يحفظ العلاقات بين المتنازعين، وفي هذا الإستثناء تبرر الأفعال غير المشروعة في الأصل، أيضاً المادة ٢٢ من ميثاق الامم المتحدة نصت على :" يجب على أطراف أي نزاع من شان إستمراره ان يفرض حفظ السلم والأمن الدولي للخطر ان يلتمسوا حله بادئ ذي بدء بطريق المفاوضة والتحقيق والوساطة والتحكيم والتسوية القضائية وغيرها .. " , لهذا السبب يعد التدبير المضاد هو استثناءاً للقاعدة اعلاه التي تلزم الأطراف حل الخلافات بالطرق السلمية .

٥. الطبيعة المؤقتة للتدابير المضادة : ان الطبيعة المؤقتة لهذه التدابير هي أساسية بحيث انها لا تهدف في الاصل للعقاب وإنما لحث الدولة المعتدية التي خلت بإلتزاماتها جبر الدولة الضحية عن الأضرار التي لحقت بها وهذا ما نصت عليه المادة ٤٩ من النصوص المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً لعام ٢٠٠١ : " بالنظر الى طابعها المؤقت، يجب أن تتخذ هذه التدابير بطريقة تنتج استئناف الوفاء بالالتزامات عند حصول الامتثال، في حال حصوله "، كذلك الدولة التي تلجأ إلى التدابير المضادة استناداً إلى تقديرها الفردي للموقف إنما تفعل ذلك على مسؤوليتها وقد تتحمل مسؤولية تصرفها غير المشروع في حال كان التقدير خاطئ ، وفي هذه الحالة لا يوجد فرق بين التدابير المضادة والظروف الأخرى المنافية لعدم المشروعية.[٩٧]

٦. الصفة العلاجية للتدابيرالمضادة : ان هذه التدابير ليست تدابير عسكرية وانما سلمية ترمي الى وقف العمل غير المشروع دولياً في حال كان لا يزال سارياً، فلا تعتبر من أعمال الإنتقام العسكرية والدفاع

---

[٩٦] عابدين عبد الحميد حسن قنديل : " التدابير المضادة في النظام القانوني الدولي، دراسة نظرية وتطبيقية "،إشراف سمعان بطرس فرجالله، رسالة دكتوراه – جامعة القاهرة، كلية الاقتصاد والعلوم السياسية، سنة ٢٠٠٦ ص٤٢

[97] النصوص المتعلقة بمسؤولية الدول عن الافعال غير المشروعة دولياً لعام ٢٠٠١، المادة ٤٩، التعليق الثالث

الشرعي بل أعمال تهدف الى امتثال الدولة المعتدية للالتزامات الدولية وهذا ما اكدته القاعدة التاسعة من دليل تالين التي اعتبرت انه يمنع على الدولة الضحية الإستمرار في التدابير المضادة في حال امتثلت الدولة المعتدية للالتزامات الدولية وإستعادة العلاقات مجراها، فقد تستمر التدابير المضادة حتى يحين الوقت الذي تتوقف فيه الدولة المسؤولة عن الفعل غير المشروع من خلال الامتثال الكامل لالتزاماتها وفقاً للمادة ٣/٥٣ من مواد لجنة القانون الدولي بشأن مسؤولية الدولة عن الافعال غير المشروعة دولياً ٢٠٠١ ، لهذه التدابير طابعاً غير عقابياً (المادة ٤٩ من مواد لجنة القانون الدولي بشان مسؤولية الدولة عن الأفعال غير المشروعة دولياً ٢٠٠١)، فقد لا يتصور في العلاقات الدولية ان يكون الهدف من هذه التدابير توقيع العقاب على الدولة المعتدى عليها[٩٨] .

* مدى مشروعية اللجوء الى التدابير المضادة :

القاعدة التاسعة من دليل تالين والمواد ٤٩ الى ٥٣ من النصوص المتعلقة بمسؤولية الدول عن الأفعال الغير مشروعة دولياً لعام ٢٠٠١ ، كذلك توصية الجمعية العمومية للأمم المتحدة جميعها تحدثت عن مشروعية اللجوء الى التدابير المضادة استثنائياً عبر إعتبار ان القواعد المذكورة أعلاه هي قواعد ملزمة، فنشير عند إعترافنا للصفة الشرعية للتدابير المضادة نرتكز على الإطار الذي رسمته لجنة القانون الدولي التابعة للأمم المتحدة في دورتها السادسة والأربعون في كلا المادتين ١١ و ١٤ من مشروع مدونة الجرائم المخلة بسَلم الانسانية و أمنها حيث نصت المادة ١١ منه على : " ما دامت الدولة ارتكبت فعلاً غير مشروع دولياً لتطلبها كما تحملها على الوفاء بالتزاماتها بموجب المواد ١٠/٦ مكرر من هذا المشروع مع عدم الاخلال بالشروط و القيود المبينة في المواد ١٢-١٣-١٤[٩٩]، و في لم نعترف بهذه الصفة أنطلاقاً من أن هذه التدابير لا تعتبر من الجزاءات القانونية كون ان هذه الأخيرة لها وظيفة رادعة والهدف منها إحترام القانون وتدعيمه بينما التدابير المضادة تعتبر فقط كوسيلة ضغط على الدولة المعتدية للعودة عن المخالفات التي ارتكبتها فضلاً على أنها تفتقر للمركزية التي تعتبر من أهم الخصائص الجوهرية للجزاء القانوني كونها تقع هذه التدابير ضمن اطار القانون الدولي العام اي في اطار النظام القانوني اللامركزي[١٠٠], فضلاً عن عدم تحقيقها الإستقرار دولياً .

نؤيد الرأي الداعم للصفة الشرعية للتدابير المضادة ولكن ضمن قيود واضحة المعالم بالنسبة للإجراءات التي تقوم بها الدولة المعتدى عليها وخاصةً في حال توقفت الدولة المعتدية المخالفات التي تقوم بها مع وجوب تطبيق فعلي للمادة ٣٤ من مشروع المسؤولية الدولية لعام ٢٠٠١ التي نصت : " أن يكون الجبر الكامل للخسارة الناجمة عن الفعل غير المشروع دولياً عن طريق الجبر والتعويض والترضية، بإحداها أو بالجمع بينهما وفقاً لأحكام الفصل الثاني "، فضلاً عن التشدد في تطبيق المادة ٥٥ من المشروع عبر تحديد الشروط المتعلقة باللجوء الى هذه التدابير كالتالي[101]:

١. دعوة الدولة المتضررة للدولة المسؤولة وفقاً للمادة ٤٤ من المشروع نفسه الوفاء بإلتزاماتها المقررة الدولية وفق المادتين ٣٤ و ٥٢ منه .

---

98 سعيد سالم جويلي، مرجع سابق، ص ١٠٩

99. حولية لجنة القانون الدولي، ٢٠٠١ – المجلد الثاني – الجزء الثاني ص ١٢٨ لغاية ١٣٩ .

١٠٠ عابدين عبد الحميد حسن قنديل، مرجع سابق، ص٢٩

١٠١ عماد حسن محمد ابراهيم : " التدابير المضادة ومدى مشروعيتها في مواجهة الهجمات السيبرانية المعادية في القانون الدولي العام "، مجلة البحوث القانونية والاقتصادية، المقال رقم ٣، المجلد ٥٤، العدد ٣ ، ٢٠٢١ ، ص ٢٣٢

٢. جبر الطرف المضرور

٣. إخطار الدولة المسؤولة بالتدابير المضادة والإلتزام بالتفاوض معها .

سيبرانياً : ان هذه الفقرة تدور حول امكانية اعتماد الدولة المتضررة سيبرانياً حق اللجوء الى التدابير المضادة كنوع من أنواع دفع هذه الأضرار وحصولها على الجبر المناسب، ولكن عندما نتحدث عن أفعال سيبرانية غير مشروعة ومسألة توجيه تدابير مضادة للدولة المسؤولة لا بدّ أن نأخذ بعين الإعتبار الأمور التالية :

- تحقق اسناد العمل غير المشروع للدولة :

ان التحقق من شرط الإسناد في العمليات الالكترونية المخالفة صعبة نوعاً ما، طالما انه قد تم اللجوء اليها من أجل تضليل المتضرر وعدم تمكينه من التعرف على هوية الجناة، اذاً لا بد للدولة المتضررة التي تلجأ الى التدابير المضادة كنوع من الرد على الهجمات التي تتعرض اليها أن تتوخى الحيطة والحذر تتأكد أولاً من هوية الجناة قبل القيام بأي تصرف كي لا تصبح هي المذنبة، والتدابير المضادة لا تستخدم الاّ من قبل دولة ضحية ضد دولة معتدية لذلك لا يمكن لدولة أن توجه تدابير مضادة ضد شركة ما وجهت اليها هجمات سيبرانية ولا ضد جماعات غير منظمة وجهت الى الدولة هجمات سيبرانية، فالتريث في تحديد هوية الدولة المسؤولة أمر اساسي : أحياناً تعتقد الدولة المتضررة أن الفاعل هو دولة ما ولكن ما لبث أن يتبين أنها مخطئة مما يؤدي الى إلقاء المسؤولية الدولية عليها، ولكن بسبب الطبيعة الخاصة للهجمات السيبرانية يصعب على الدولة أكتشاف هوية الفاعل الاّ في حال إمتلكت التقنيات اللازمة، اذاً يجب أن نفهم حدود الإسناد في القانون الدولي لكي توجه التدابير المضادة الى الجهة الصح، عموماً ان إسناد فعل غير مشروع الى الدولة يتوقف على [١٠٢]:

- تصرفات أجهزة الدولة

- تصرفات الأشخاص أو الكيانات التي تمارس بعض الاختصاصات السلطة الحكومية

- تصرفات الاجهزة التي توضع تحت تصرف الدولة او تحت رقابتها

- التصرفات التي يتم القيام بها بناءً على توجيهات الدولة او تحت رقابتها

- التصرفات التي يتم القيام بها في غياب السلطات الرسمية او في حال عدم قيامها بمهامها

- تصرفات الحركات التمردية وغير التمردية

- تقديم العون لارتكاب فعل غير مشروع

في هذه الحالات السبع يعتبر التصرف الصادر عن هذه الجهات كأنه صادر عن الدولة نفسها و بالتالي يحّتم إسناد الفعل غير المشروع لها وتحقق شروط التدابير المضادة عند تحقق شرط الإسناد وبموجب قواعد المسؤولية الدولية، اما النشاطات الإلكترونية التي يكون مصدرها اشخاصُ طبيعيون أو معنويون او هيئات

[١٠٢] محمد حتحاتي، مرجع سابق، ص ٣٧

غير حكومية ولكنهم يتمتعون بقدر من السلطة بموجب نظام او قانون فان اعمالهم فيما يتعلق بهذه السلطة تعزي للدولة ذاتها و ان تجاوز اؤلئك السلطات المخولة لهم [١٠٣].

إذاً التدابير المضادة تشكل حجر الأساس في نظام تسوية النزاعات الدولية بحيث أنها يمكن أن تسدا لفراغ الناجم عن احجام الدول في رفع نزاعاتها للقضاء الدولي وامتناع الحلول الدبلوماسية وعجز المنظمات الدولية التعامل مع القضايا الدولية بسبب تضارب المصالح، فالدفع بعدم تنفيذ الإلتزامات الدولية في مواجهة الدول المسؤولة عن فعل غير مشروع دولياً يمكن أن يشكل دعامة رئيسية لفرض احترام القانون .

لقد إنتهينا من معالجة الفصل الأول من هذا القسم سوف ننتقل الى تحديد مسؤولية المشارك المباشر عن التصرفات غير المشروعة التي تصدر عنه على الصعيدين الدولي والمحلي.

الفصل الثاني: مسؤولية المشارك المباشر دولياً عن الهجمات السيبرانية

بعد التطورات التكنولوجية والتقنية الحديثة وظهور أسلحة جديدة فتاكة من شانها ان تحدث اضراراً كبيرة بالمدنيين كان لا بدّ من حماية هؤلاء من الأخطار الناجمة من العمليات العسكرية وكانت سنة ١٩٤٩ سنة مفصلية في هذا الصدد، فالقانون الدولي الانساني لم يقر الحماية للمدنيين الاّ مؤخراً، فالإتفاقيات الرئيسة التي عقدت قبل عام ١٩٤٩كانت تقوم فقط بتنظيم سير العمليات العدائية ومصير الجرحى والمقاتلين وأسرى الحرب الاّ ان اتفاقية جينيف الرابعة نظمت بنداً اساسياً تحديداً للمدنيين من أجل حمايتهم من الأعمال العدائية، مع تضاعف هذه الحماية في حالات معينة مثلما في الأراضي المحتلة وأثناء عمليات الاعتقال أو الاجلاء في ما يتعلق بفئات معينة من الاشخاص الذين يعتبرون الأضعف مثل الأطفال والمرضى والجرحى والمحتجزين، وخاصةً في البروتوكول الإضافي الأول : المادة ٤٨ حتى ٥٦ و البروتوكول الإضافي الثاني من المواد ١٣ حتى ١٨، فعززت هذه الحماية الممنوحة للمدنيين في البروتوكول الأول أثناء النزاعات المسلحة والبروتوكول الثاني الذي إعتبر ان هذه الحماية لا بدّ ان يتمتع بها المدنيون اثناء النزاعات المسلحة وغير المسلحة ونشير أن من أهم المبادئ في القانون الدولي الانساني هو مبدأ " التمييز بين المقاتلين والمدنيين " وتسري أحكام المادة ٤٩ من البروتوكول الإضافي الأول لسنة ١٩٧٧ على عملية حربية في البر كانت أم في الجو أم في البحر قد تصيب السكان المدنيين أو الأفراد المدنيين أو الأعيان المدنية على البر، كما تنطبق على كافة الهجمات الموجهة من البحر أو من الجو ضدّ أهداف على البر ولكنها لا تمس بطريقة أخرى قواعد القانون الدولي التي تطبق على النزاع المسلح في البحر أو في الجو، فالحماية ممنوحة ليست فقط للمدنيين وإنما ايضاً للمقاتل الذي اصبح عاجزاً عن القتال أو خرج من صفوف المقاتلين فيكون له الحق بالحماية التي يعطيها القانون الدولي الانساني وهذا ما اشارت اليه المادة ٤٨ من البروتوكول الإضافي الاول لعام ١٩٧٧ بالقول :" يعمل أطراف النزاع على التمييز بين السكان المدنيين والمقاتلين وبين الأهداف العسكرية والأعيان المدنية ومن ثم توجيه عملياتها ضد الأهداف العسكرية دون غيرها وذلك من أجل تأمين إحترام وحماية السكان المدنيين والأعيان المدنية" [١٠٤]وأيضاً المادة ٥١(الفقرة الثانية) من البروتوكول الاضافي نفسه بالقول :" لا يجوز أن يكون السكان المدنيون بوصفهم هذا محلاً للهجوم وتحظر أعمال العنف او التهديد به الرامية الى بث الذعر بين السكان المدنيين ،

عماد حسن محمد ابراهيم، مرجع سابق، ص 103٢٣٥

١٠٤ اللجنة الدولية للصليب الأحمر "الملحقان" البروتوكولان الاضافيان الى اتفاقية جينيف المعقودة في ١٢ اب ١٩٤٩- جينيف سوسيرا- الطبعة الرابعة، ١٩٩٧ ص ٤٠.

اما المدني الذي يشارك مشاركة مباشرة قي العمليات العدائية يفقد الحماية الممنوحة له ضمن مدة معينة من الهجمات ويصبح هدفاً شرعياً للقوات المسلحة المعادية ويستعيدها ضمن شروط معينة سوف نشرحها في هذا الفصل ولكن تترتب على هذه المشاركة مسؤولية دولية ووطنية بسبب الإنتهاكات المستمرة للقوانين الدولية والوطنية، فضلاً عن مسؤولية جنائية دولية مترتبة على الدولة التي ينتمي اليها أو الدولة التي يقوم المشارك المباشر بقيادة العمليات العدائية على أراضيها في حال ثبوت دعم هذه الدولة لأعمال المشارك المباشر او ثبوت قصور هذه الدولة بالقيام بواجباتها في منع الضرر الذي يلحق بالدول الاخرى من جراء تصرفاته [١٠٥] ، لذلك وإستناداً الى ما تقدم لا بدّ من طرح الأسئلة التالية : الى أي مدى يمكن للمشارك المباشرفي العمليات العدائية استعادة الحماية الممنوحة له من قبل القانون الدولي الانساني ؟ و ما هي العواقب المترتبة جرّاء هذه الاستعادة ؟

في المبحث الاول سوف نتطرق الى مبدأ المشاركة المباشرة في العمليات العدائية اما في المبحث الثاني سنبين المسوؤلية الجنائية الدولية المترتبة على المشارك المباشر.

المبحث الأول : مبدأ المشاركة المباشرة في العمليات العدائية

سوف نبين في هذا المبحث مفهوم المشاركة المباشرة في العمليات العدائية وفقاً للتعريفات المختلفة و الآراء الفقهية التي ناقشت هذا المبدأ الخاص بالمدنيين في الفرع الأول، أما في الفرع الثاني سوف نبين شروط فقدان الحماية المعطاة للمدنيين و أوجه إستعادتها.

الفرع الأول : الإطار النظري

بصدد تعريف الأعمال العدائية لقد اطلعنا على التعريف الوارد الدليل التفسيري لمفهوم المشاركة المباشرة في العمليات العدائية للجنة الدولية للصليب الأحمر الصادر في الأول من كانون الأول لعام ٢٠١٥ الذي اعتبر :" ان الأعمال العدائية تشير الى اللجوء الجماعي لأطراف النزاع الى وسائل وطرق من شأنها اصابة العدو" أما المشاركة فاعتبرها أنها "بمثابة مساهمة الفرد في العمليات العدائية الدائرة بين أطراف النزاع اذ على وفق نوعية ودرجة هذه المساهمة يمكن وصف المشاركة في نزاع على أنها مشاركة مباشرة أم غير مباشرة " [١٠٦]، ايضاً القاعدة ٢٥ من دليل تالين إعتبرت أن :" قانون النزاعات المسلحة لا يمنع أي فئة من المشاركة في العمليات السيبرانية"، بمعنى آخر أنه يحق لكافة الفئات المشاركة ولكن يختلف العقاب المفروض بإختلاف كل منها وطبيعة النزاع المسلح القائم"، نشير بالإضافة الى أن اهم مبدأ بين مبادئ القانون الدولي الانساني والعقيدة الأسمى بين عقائده الإنسانية هو مبدأ التمييز بين المدنيين والمقاتلين التي أقرته المادة ٤٨ من البروتوكول الاضافي الأول الخاص بإتفاقيات جينيف لحماية ضحايا النزاعات المسلحة الدولية:اذاً نحن أمام فئتين : فئة المدنيين والمقاتلين وفئة الأعيان المدنية والعسكرية .

عرفت المادة ٥٠ من البروتوكول الاضافي الأول كالتالي : " المدني هو أي شخص لا ينتمي إلى فئة من فئات الأشخاص المشار إليها في البنود الأول والثاني والثالث والسادس من الفقرة (أ) من المادة الرابعة من الاتفاقية الثالثة والمادة ٤٣ من هذا اللحق "البروتوكول"، وإذا ثار الشك حول ما إذا كان شخص ما مدنياً أم غير مدني فإن ذلك الشخص يعد مدنياً وأيضاً :

---

[105] علي محمد كاظم الموسوي، مرجع سابق، ص ١٧٩

[106] الدليل التفسيري، مرجع سابق، ص ٤٢

- يندرج في السكان المدنيين كافة الأشخاص المدنيين .

-لا يجرد السكان المدنيون من صفتهم المدنية وجود أفراد بينهم لا يسري عليهم تعريف المدنيين.

ان فئات الاشخاص التي لا ينتمي اليها المدني هي على الشكل التالي:

١- أفراد القوات المسلحة لاحد أطراف النزاع و الميليشيات و الوحدات المتطوعة التي تشكل جزءاً من هذه القوات المسلحة .

٢- أفراد الميليشيات الأخرى والوحدات المتطوعة الاخرى ممن منهم أعضاء حركات المقاومة المنظمة اللذين ينتمون الى احد اطراف النزاع ويعملون داخل اقليمهم او خارجه حتى لو كان هذا الاقليم محتلاً على ان تتوافر أربعة شروط :

- ان يقودها شخص مسؤول عن مرؤوسيه

- ان يكون لها شارة مميزة محددة يمكن تمييزها عن بعد

- ان يحمل الاسلحة مهراً

- ان يلتزم في عملياتها بقوانين الحرب و عاداتها

٣- أفراد القوات المسلحة النظامية اللذين يطبقون ولاءهم لحكومة او سلطة لا تعترف بها الدولة الحاجزة

٤- سكان الأراضي غير المحتلة اللذين يحملون السلاح من تلقاء أنفسهم عند أقتراب العدو لمقاومة القوات الغازية دون ان يتوافر لهم الوقت لتشكيل وحدات مسلحة نظامية، شريطة ان يحملوا السلاح جهراً وان يراعوا قوانين الحرب وعاداتها ويعرفون مصطلح الهبة الجماعية .

اذاً فهذا المدني الغير مشارك في الأعمال العدائية يمنع ان يكون هدفاً للهجمات المباشرة وهذا المبدأ هو جزءاً من قواعد القانون الدولي العرفي فهو ملزم للكافة ولأي طرف يخوض نزاع مسلح دولي ام غير دولي وهذا ما جاء في القاعدة الأولى من القانون الدولي الإنساني :" يميز اطراف النزاع في جميع الأوقات بين المدنيين والمقاتلين وتوجه الهجمات الى المقاتلين فحسب ولا يجوز ان توجه للمدنيين[١٠٧]، كذلك القاعدة السادسة من القانون نفسه :" يتمتع المدنيون بالحماية من الهجوم ما لم يقوموا بدوراً مباشراً في الأعمال العدائية وطوال الوقت اللذين يقومون فيه بهذا الدور، ايضاً تكرس الدول هذه القاعدة كإحدى قواعد القانون الدولي العرفي المطبقة في النزاعات المسلحة الدولية وغير الدولية " [١٠٨].

[١٠٧] علاء الدين بو مرعي : "مبدأ التمييز والأساليب والوسائل الحربية الحديثة – دراسة على ضوء مبادئ القانون الدولي الانساني"، المركز الاستشاري للدراسات والتوثيق، العدد ٣٢ ,٢٠٢٣

[١٠٨] جون ماري هنكرتس و لويز دوزولدك :" القانون الدولي الانساني العرفي – اللجنة الدولية للصليب الاحمر – القاعدة ٧٨، ص ١٨

بالإضافة إعتبر نظام المحكمة الجنائية الدولية ان " تعمد توجيه هجمات ضد السكان المدنيين لا يشاركون مباشرةً في الاعمال الحربية يعتبر انتهاك للقوانين والاعراف السارية في القانون الدولي وجريمة حرب "[١٠٩], وأخيراً كرست المادة ٥١ من البروتوكول الإضافي الأول جميع ما تقدم على الشكل التالي :

١. يتمتع السكان المدنيون والأشخاص المدنيون بحماية عامة ضد الأخطار الناجمة عن العمليات العسكرية ويجب، لإضفاء فعالية على هذه الحماية مراعاة القواعد التالية دوماً بالإضافة إلى القواعد الدولية الأخرى القابلة للتطبيق.

٢. لا يجوز أن يكون السكان المدنيون بوصفهم هذا وكذا الأشخاص المدنيون محلاً للهجوم. وتحظر أعمال العنف أو التهديد به الرامية أساساً إلى بث الذعر بين السكان المدنيين.

٣. يتمتع الأشخاص المدنيون بالحماية التي يوفرها هذا القسم ما لم يقوموا بدور مباشر في الأعمال العدائية وعلى مدى الوقت الذي يقومون خلاله بهذا الدور.

٤. تحظر الهجمات العشوائية، وتعتبر هجمات عشوائية :

أ) تلك التي لا توجه إلى هدف عسكري محدد،

ب) أو تلك التي تستخدم طريقة أو وسيلة للقتال لا يمكن أن توجه إلى هدف عسكري محدد،

ج) أو تلك التي تستخدم طريقة أو وسيلة للقتال لا يمكن حصر آثارها على النحو الذي يتطلبه هذا اللحق "البروتوكول"، ومن ثم فإن من شأنها أن تصيب، في كل حالة كهذه، الأهداف العسكرية والأشخاص المدنيين أو الأعيان المدنية دون تمييز. .

٥. تعتبر الأنواع التالية من الهجمات، من بين هجمات أخرى، بمثابة هجمات عشوائية :

أ) الهجوم قصفاً بالقنابل، أياً كانت الطرق والوسائل، الذي يعالج عدداً من الأهداف العسكرية الواضحة التباعد والتميز بعضها عن البعض الآخر والواقعة في مدينة أو بلدة أو قرية أو منطقة أخرى تضم تركزاً من المدنيين أو الأعيان المدنية، على أنها هدف عسكري واحد.

ب) والهجوم الذي يمكن أن يتوقع منه أن يسبب خسارة في أرواح المدنيين أو إصابة بهم أو أضراراً بالأعيان المدنية، أو أن يحدث خلطاً من هذه الخسائر والأضرار، يفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة.

٦. تحظر هجمات الردع ضد السكان المدنيين أو الأشخاص المدنيين.

٧. لا يجوز التوسل بوجود السكان المدنيين أو الأشخاص المدنيين أو تحركاتهم في حماية نقاط أو مناطق معينة ضد العمليات العسكرية ولاسيما في محاولة درء الهجوم عن الأهداف العسكرية أو تغطية أو تحبيذ أو إعاقة العمليات العسكرية، ولا يجوز أن يوجه أطراف النزاع تحركات السكان المدنيين أو الأشخاص المدنيين بقصد محاولة درء الهجمات عن الأهداف العسكرية أو تغطية العمليات العسكرية.

٨. لا يعفي خرق هذه المحظورات أطراف النزاع من التزاماتهم القانونية حيال السكان المدنيين والأشخاص المدنيين بما في ذلك الالتزام باتخاذ الإجراءات الوقائية المنصوص عليها في المادة ٥٧ " .

---

[109] النظام الاساسي للمحكمة الجنائية الدولية – المادة ٨(الفقرة ١ و ٢) , ٢٠٠٢

اخيراً تحمي اتفاقيات جينيف الاربعة على وجه التحديد الأشخاص الذين لا يشاركون في الأعمال العدائية (المدنيون, وعمال الصحة, وعمال الإغاثة) والأشخاص الذين توقفوا عن المشاركة في الأعمال العدائية من قبيل الجرحى، والمرضى، والجنود الناجين من السفن الغارقة، وأسرى الحرب والصحفيون دون أي تمييز مجحف يتأسس على العنصر، أو اللون، أو الجنس، أو اللغة، أو الدين، أو العقيدة، أو الرأي السياسي أو غير السياسي، أو الانتماء الوطني أو الاجتماعي، أو الثروة، أو المولد أو أي وضع آخر، أو أية معايير أخرى مماثلة .[١١٠]

فئة المقاتلين :

مفهوم المقاتل في القانون الدولي الانساني ضمن إطار النزاعات المسلحة الدولية وغير الدولية معرض اهتمام كبير لدى الفقهاء، كذلك هنالك حماية خاصة له، فالمقاتل هو الشخص المخول بموجب ضوابط معينة بحمل السلاح وإستخدام القوة ضدّ الخصم على أن يكون العدو هدفاً عسكرياً، كما وعرفت المادة الثالثة من قواعد القانون الدولي الانساني العرفي المقاتل :"المقاتلين هم جميع أفراد القوات المسلحة لطرف في النزاع ما عدا افراد الخدمات الطبية والدينية " وهم الاشخاص اللذين يقومون بدوراً مباشراً في العمليات العدائية عبر إستخدام سلاح او نظام أسلحة لا غنى عنه، كذلك أكدت المادة ٤٣ من البروتوكول الاضافي الاول : " تتكون القوات المسلحة لأي طرف في النزاع من جميع أفراد قواته المسلحة والمجموعات والوحدات النظامية التي تكون تحت قيادة مسؤولة أمام ذلك الطرف عن سلوك مرؤوسيها".

أما بالنسبة الى صفات المقاتل فحددت بأربعة على الشكل التالي [١١١]:

١- المشاركة في العمليات الحربية : ترتكز هذه المشاركة على قيام المقاتل بالمشاركة في اعمال الدفاع و الهجوم ضد الخصم فضلاً عن تدمير المواقع الخاصة بالعدو، فهي أعمال ممنوعة في اصلها الاّ في حال ارتكابها في وقت الحرب .

٢- الإستهداف من قبل الخصم : يعتبر المقاتل هدفاً أساسياً للخصم، فقد يكون عرضى للقتل أو الجرح أو الوقوع في الأسر سواء براً بحراً او جواً سواء كانوا في المواقع العسكرية او في الغواصات او في الطائرات البحرية وغيرها من وسائل النقل.

٣. إعفاءه عن الاعمال العدائية المسموحة في الحرب : الاّ أنه يحاكم عن الأفعال التي ارتكبها والتي تعتبر قانوناً بمثابة جرائم حرب .

٤.التمتع بوضع الاسير : في حال وقع في قبضة العدو يعتبر بمثابة أسير ويستفيد من الحماية الممنوحة المنصوص عنها في اتفاقية جينيف الثالثة .

الاّ أن فئة المقاتلين تنقسم الى عدة أقسام على الشكل التالي :

---

[١١٠] اتفاقيات جينيف و بروتوكولاتها الأربعة لعام ١٩٤٩ . مقال تم نشره على الموقع الرسمي للجنة الدولية للصليب الاحمر في ١ كانون الثاني ٢٠١٤ , متوفر على الرابط التالي :
https://www.icrc.org/ar/document/geneva-conventions-1949-additional-protocols

[111] شيخة حسين الزهراني، مرجع سابق، ص ١٦٢-١٦٣

١- أفراد القوات المسلحة لأحد أطراف النزاع والمليشيات والوحدات الأخرى التي تشكل جزء من هذه القوات و فقاً لما يلي :

- أفراد القوات المسلحة النظامية : هم العسكريون الذين يرتدون الزي العسكري ويحترفون وظائفهم سواء كانت قتالية أم لا وذلك ضمن تنظيمات عسكرية خاصة يناط بها مهام الدفاع الوطني واحترامهم ليبدأ التمييز وهذا ما أكدته المادة ٤٣ من البروتوكول الاضافي الأول : " يغطي تعريف القوات المسلحة هذا، في جوهره، جميع الأشخاص الذين يقاتلون بالأصالة عن طرف في نزاع ويتبعون قيادته، ونتيجة لذلك، فالمقاتل هو أي شخص يشارك، تحت قيادة مسؤولة، في أعمال عدائية في نزاع مسلح بالأصالة عن طرف في نزاع , كما تطبّق الشروط المفروضة على القوات المسلحة على المجموعات المسلحة بصفتها هذه. وبالتالي فإنّ أفراد مثل هذه القوات المسلحة هم عرضة للهجمات".

- أيضاً يدخل ضمن اطار القوات المسلحة : المليشيات والوحدات المتطوعة التي عرفت على أنها "الوحدات الاحتياطية من الجيش الذين أنهوا خدمتهم العسكرية ونظراً لخبرتهم العسكرية وتمرسهم السابق في صفوف القوات المسلحة يبقون ضمن دائرة الاحتياط في حال طلب منهم الحضور للإنضمام في الظروف الحرجة لمدة محددة ويخضعون للقانون الوطني للدولة ولكن لا يعترف لهم وفق للقانون الدولي الانساني الاَ من خلال إعتبارهم أسرى حرب في حال وقعوا في الأسر".[١١٢]

وفق ما أكدته لائحة لاهاي في اعتبار أن قوانين الحرب لا تنطبق فقط على الجيوش وإنما أيضاً على الميليشيات والقوات المسلحة التي تتوفر فيها أربعة شروط :

- أن يكون على رأسها شخص مسؤول عن مرؤوسيه
- أن تكون لها شارة مميزة ثابتة يمكن التعرف عليها عن بعد
- أن تحمل الأسلحة علناً
- أن تلتزم في عملياتها بقوانين الحرب وأعرافها

مع إعتبار هذه اللائحة ان هذه الميليشيات والقوات المسلحة تشكل جزءاً من الجيش ثم عادت وأكدت المادة ٤ من اتفاقية جنيف الثالثة هذا الأمر، مع إضافة حركات المقاومة المنظمة، فالمادة ٤٣ المذكورة أعلاه تشترط أن يكون لهذه الجماعات نوع من الإنضباط والتنظيم الداخلي بالاضافة الى الشروط الأربعة لكي تصنف كقوات مسلحة، بمعنى أخر أي جماعة تتوافر فيها الشروط المذكورة أعلاه تعتبر قوات مسلحة يستفيد أعضاؤها من مقاتلين مؤهلين لوضع أسير الحرب .[١١٣]

2. الهبة الجماعية :

هم مجموعة من المواطنين ضمن أراضي غير محتلة يحملون السلاح للدفاع عن أنفسهم بصورة عفوية وباختيارهم الشخصي عند اقتراب العدو،لم يتم تنظيمهم ضمن جماعات منظمة مسلحة ولكنهم يعاملون كأسرى حرب في حال وقوعهم في أيدي العدو، هذه الفئة من المدنيين تحمل السلاح بشكل ظاهر وعفوياً اما بناءً على طلب حكومتهم بشرط أن لا يتم ضمن أراضي محتلة وباحترام قانون الحرب وأعرافه وهذا ما

---

[112] علي محمد كاظم الموسوي، مرجع سابق، ص ٥٨

[١١٣] https://ihl-databases.icrc.org/ar/customary-ihl/v1/rule4

نصت عليه المادة ٦/١٣ من اتفاقية جينيف الأولى لعام ١٩٤٩: "سكان الأراضي غير المحتلة الذين يحملون السلاح من تلقاء نفسهم عند اقتراب العدو لمقاومة القوات الغازية دون ان يتوفر لهم الوقت لتشكيل وحدات مسلحة نظامية شريطة ان يحملوا السلاح جهراً و ان يراعوا قوانين الحرب و عاداتها " .

سيبرانياً :

ان الاشخاص المنظور اليهم كأهداف شرعية للهجوم السيبراني وفق دليل تالين ذكروا في المادة ٣٤ منه على الشكل التالي :

" يجوز ان يتم استهداف الاشخاص الاتيين بالهجمات السيبرانية كالتالي :

١. أعضاء القوات المسلحة

٢. أعضاء الجماعات المسلحة المنظمة

٣. المدنيون اللذين يشاركون مشاركة مباشرة في العمليات العدائية

٤. في نزاع مسلح دولي، المشاركون في الهبة الجماعية

اذاً نستنتج وفق للمادة أعلاه أن المدنيون يصبحون أهداف سيبرانية في حال مشاركتهم مشاركة مباشرة في العمليات العدائية وهذا ما أكدته المادة ٣٥ من دليل تالين :" يتمتع الأشخاص المدنيون بالحماية من الهجوم لحين مشاركتهم المباشرة في العمل العدائي (ويفقدون هذه الحماية على مدى هذا الوقت أي وقت مشاركتهم المباشرة في الأعمال العدائية)."

كذلك هذه المشاركة لا تتم الاّ وفق عمليات محددة عدائية تتصف بالواقعية، فضلاً عن عناصر اساسية لا بدَ من توافرها على الشكل التالي :

١. الوصول الى حدّ حصول الضرر :

يجب أن يكون من شأن العمل ان يؤثر سلباً في العمليات العسكرية أو في القدرة العسكرية لأحد أطراف النزاع او على نحو اخر ان يحدث الموت او الإصابة او التدمير للأشخاص المحميين أو الأعيان المحمية من الهجمات المباشرة ." [١١٤]

استناداً الى ما تقدم لكي تكون هذه المشاركة سبباً في فقدان المدني للحماية الممنوحة في القانون الدولي الانساني لا بدّ ان تكون هذه المشاركة تلحق الاضرار بالخصم أو تنقص من قدرته العسكرية، اذاً في حال لم يسبب العمل العدائي الاضرار اللازمة لكي يصل لحد حصول الضرر يجب أن يوجه الى الاشخاص و الاعيان المحمية كبناء سياج او اقامة الحواجز في الطرق ورفض المدني التعاون مع طرف في النزاع بصفة مخبر او مراقب وحتى اعتقال ونفي الاشخاص اللذين يكون لهم تاثير خطرعلى الامن والصحة العامة، ايضاً قيام المدنيين بالعمل في المصانع العسكرية لإنتاج السلاح وتطوير وصناعة الاسلحة كالعبوات الناسفة، فكافة هذه الافعال السابقة تخرج من اطار التصرفات التي تصل الى حد حصول الضرر وفق ما جاء في الدليل التفسيري للجنة الدولية للصليب الاحمر، فهل من الضروري ان يسبب العمل العدائي ضرراً كي يصل الى حد حصول الضرر ؟

---

[114] الدليل التفسيري، مرجع سابق، ص ٤٦

" ان العمل العدائي المحدد لكي يصل الى حدّ حصول الضرر المطلوب لا يستوجب ان يسبب الضرر فعلاً او بصورة مادية بل يكفي ان يكون من شان الفعل ان يسبب الضرر الذي يصل للحدّ المطلوب، أي بوجود احتمال موضوعي بان ينتج من العمل هذا الضرر: ولهذا يجب ان يستند تحديد الحد المطلوب الى الضرر المحتمل الذي قد يتوقع على النحو المعقول ان ينتج عن عمل يرتكب في الظروف السائدة."[١١٥]

كذلك وفقاً للدليل التفسيري المذكور أعلاه، ان الأعمال التي تعد من قبيل المشاركة المباشرة في العمليات العدائية هي على الشكل التالي :" الحاق الموت او الاصابة او الدمار للاشخاص المحميين او الاعيان المحمية من الهجمات المباشرة يصل الى حد حصول الضرر ولكن هنالك الكثير من الاعمال لا بدّ ان تدخل ضمن الأعمال العدائية ولكن غير متوافرة في هذه المادة كالترحيل القسري وإختطاف المدنيين ... فلا بد ان تعتبر ان كافة الأفعال التي تلحق اضراراً بالاعيان المدنية من جهة وبالمدنيين من جهة اخرى ان تعد ضمن العمليات العدائية بهدف التركيز على الأعمال التي تصل الى حد حصول الضرر اياً كانت.

اما في إطار الهجمات السيبرانية فحد حصول الضرر هنا مختلفاً نوعاً ما ومتأرجحاً بين الدليل التفسيري للجنة الدولية للصليب الاحمر وبين دليل تالين، فالرأي الأول يعتمد على الإحتمال الموضوعي بإحداث الضرر فليس بالضرورة ان يسبب الضرر فعلاً بل يكفي ان يكون من شأن الفعل ان يسبب الضرر الذي يصل للحد المطلوب اي بوجود احتمال موضوعي في هذا الصدد، اما دليل تالين اعتبر انه لا بدّ من اعتماد ما يسمى بالقصد بدلاً من الاحتمال الموضوعي بإحداث الضرر اي انه للوصول الى حد حصول الضرريجب ووفق دليل تالين ان يكون من شان الفعل او الافعال المرتبطة ببعضها بسلسلة وثيقة قصد الضرر او تحقيقه بصورة فعلية عن طريق التاثير سلباً في العمليات العسكرية للعدو او قدرته العسكرية او الحاق الموت او الايذاء البدني او الدمار المادي للاشخاص والاعيان المحمية من الهجمات."[١١٦]

فتصرف المدني القصدي الذي يسبب الضرر للعمليات العسكرية او القدرة العسكرية للخصم او قد احدث الاضرار بالاشخاص ام الاعيان المحمية كاف لاعتبار فعله كمشاركة مباشرة في الحرب السيبرانية , هنا الارادة كانت متجهة الى احداث الضرر بالاشخاص ام بالاعيان دون بالضرورة ان نكون امام احتمال موضوعي بتحقق الضرر المقصود احداثه، ان اتجاه دليل تالين في هذا المجال شيئاً من المبالغة لانه سوف يوسع دائرة الحالات التي من الممكن اعتبارها في اطار المشاركة المباشرة في الهجمات السيبرانية على حساب الحالات التي من الممكن اعتبارها كمشاركة مباشرة في العمليات العدائية التقليدية، ايضاً نجد فكرة معينة بهذا الشان : "أنه في حال كان الفعل يسبب ضرراً مطلوباً لاعتباره بمثابة مشاركة مباشرة في الحرب حتى و لو لم يكن الفاعل قاصداً ذلك.."، فهنا تم القاء المسؤولية نفسها على الفاعل سواء كان قاصداً احداث الضرر ام لا وهذا غير منطقي ان نكون امام مساواة غير عادلة."[١١٧]

فالتشويش الالكتروني والهجوم على الحواسيب العسكرية هي تصرفات تصل الى حدّ حصول الضرر في اطار الهجمات السيبرانية، كذلك استغلال الحواسيب لتنفيذ هجمة معينة ضد مواقع عسكرية وتطوير فيروسات معينة تستخدم لأغراض الحروب السيبرانية فضلاً عن تدمير واتلاف معلومات اساسية تستخدم

---

115 الدليل التفسيري، مرجع سابق، ص ٤٧

116 دليل تالين، القاعدة رقم ٣٥، التعليق الرابع

117 علي محمد كاظم الموسوي , مرجع سابق , ص ٧٧

في المستشفيات و المنظمات الانسانية [١١٨]، ففي هذه الحالة هل يمكننا أن هذه الأعمال من شأنها أن تؤدي الى اعتبار الفعل قد وصل الى حدّ حصول الضرر؟

سوف نحدد في البدء الفرق بين إتلاف وتدمير المعلومات : ان إتلاف المعلومات يتم عن طريق اختراق شبكات الخصم و الوصول الى البيانات والمعلومات الخاصة به والتعديل بها دون علمه، أما تدمير المعلومات تتم عن طريق إجراء مسح كامل للأصول والمعلومات المهمة الموجودة على شبكات الخصم .

نميز في هذه الحالة بين حالتين :

الحالة الأولى: هي الهجمات الموجهة ضد الأهداف العسكرية التي تصل الى حد حصول الضررالمطلوب .

الحالة الثانية : بالنسبة الى الاعيان المحمية، جاء رأي اللجنة الدولية للصليب الاحمر ان الهجمات السيبرانية الموجهة ضد المعلومات في البروتوكولين الإضافيين : اقتصر النص على الفكرة القائلة ان لفظة عين او اعيان تنطق فقط على تلك التي من الممكن رؤيتها او لمسها visible et tangible وفي حال أدت هذه الأضرار الى التسبب بالعجز الوظيفي لهذه الحواسيب والشبكات فنكون اذاً امام هجوم سيبراني، أما بالنسبة الى خبراء تالين أكدوا أنه لا بدّ من إعتبار ان البيانات المخزنة من قبيل الأعيان المحمية كون ذلك يخالف المواد ٤٨ و ٥١ من البروتوكول الإضافي الأول بشأن الحماية العامة التي يتمتع بها المدنيون والأعيان المحمية من آثارالقتال.[١١٩]

برأينا ان صور النزاعات التقليدية تغيرت في عصرنا الحالي وان تدمير المعلومات المخزنة والرقمية المتعلقة بالمدنيين يكون لها أثر كبير في اعتبار هذا العمل بمثابة هجوم فعلي، فالمفهوم المتبني من قبل اللجنة الدولية للصليب الاحمر قد اصبح قديماً نوعاً ما و لا بدّ من تطويره لكي يتماشى مع الحروب الحديثة من حيث الشكل و النوع اخذين بعين الاعتبار ان اكثرية الهجمات السيبرانية قد تصل الى حد حصول الضرر المطلوب.

٢. العلاقة السببية المباشرة في إطار العمليات العدائية عامة والسيبرانية خاصةً

يجب ان يكون هنالك علاقة سببية مباشرة بين عمل عدائي معين يقوم به الشخص والضررالمحتمل الناتج عن هذا العمل او عن عملية عسكرية منسقة، على أن يشكل هذا العمل جزءاً لا يتجزأ منها [١٢٠]، بمعنى آخر ان يكون هذا الضرر نتيجة للعمل العدائي الذي يستتبع مشاركة مباشرة تؤدي حتماً الى فقدان الحماية من الهجمات المباشرة، يعني ضمناً من الممكن ان يكون هنالك مشاركة مباشرة وغير مباشرة في العمليات العدائية لا تؤدي الى فقدان الحماية، الاّ أن هذا الدليل اعتبر أنه يجب إلحاق الضرر المقصود بخطوة مسببة واحدة (دون تحديد ما هي الخطوات المعتبرة مسببة او مفهوم هذه الخطوة)، أيضاً اعتبر انه من المفترض أن يكون هنالك علاقة وثيقة بما يكفي بين العمل والضرر الناتج عنه لإعتبار اذا كانت المشاركة هي مباشرة ام لا، فالمشاركة غير المباشرة التي تظهر عادةً عن طريق بعض الانشطة التي تعرف بدعم الجمهور الحربي والانشطة المساندة للحرب لا تعتبر مشاركة مباشرة في العمليات العدائية على الرغم من تأثيرها

---

[١١٨] Collin Allan : " Direct Participation in Hostilities From Cyberspace" , Virginia Journal of International Law, Vol. 54, No. 1, 2013 p 183-184

[١١٩] دليل تالين، مرجع سابق، القاعدة ٣٠، التعليق السادس والعاشر
القاعدة رقم 38 ، التعليق الرابع والخامس

[١٢٠] الدليل التفسيري، مرجع سابق، ص ٥٠

الضخم على مباشرة تحقيق النصر في الحرب، وانظمة ال General War Effort ترتبط بالمساهمة في الهزيمة العسكرية للعدو كالعمل في مصانع الاسلحة والذخيرة، اما الانشطة المساندة للحرب (War Sustaining Activities) هي التي تعمل على المجهود الحربي والعمليات العسكرية من خلال دعم الادوات السياسية والاقتصادية والاعلامية كالشائعات السياسية والتمويل الاقتصادي [١٢١]، وان العلاقة السببية المباشرة التي يجب تحقيقها لاعتبار العمل العدائي على انه مشاركة مباشرة لا يتحقق بالنسبة لهذه الحالات لعدم وجود السببية المباشرة ولإفتقار الأعمال العدائية للتحديد المطلوب[١٢٢] ومثلاً فرض عقوبات اقتصادية على طرف في نزاع مسلح او حرمانه من أصوله المالية أو تزويد خصمه بسلع وخدمات (كهرباء , وقود..) او البحوث والتصاميم العلمية وانتاج الاسلحة والتجهيزات ونقلها، فجيمع هذه الاعمال المذكورة تعتبر مشاركة غير مباشرة تؤدي الى أثرغير مباشرعلى القدرة العسكرية .[١٢٣]

وفق الدليل التفسيري من المفترض وجود قرب السبب بالضرر(اي فورية تحقق الضرر على أساس الفعل) والذي يختلف عن مفهوم القرب الزمني والقرب الجغرافي، بالنسبة الى هذه النقطة التي اشار اليها اعتبر أن مفهوم القرب الزمني هو اشارة الى التوقيت التي تأخذه الأسلحة المستخدمة بين أطراف النزاع للتنفيذ (في حال كانت بعيدة كالالغام والأجهزة الموقوتة او الافخاخ المتفجرة) اما القرب الجغرافي يعرّف على أنه الأسلحة الموجهة عن بعد [١٢٤]كالهجمات السيبرانية والطائرات بلا طيار والقذائف الموجهة عن بعد[١٢٥].

نضيف أن تدريب الأشخاص خصيصاً من أجل تنفيذ عمل معين مسبقاً هو بمثابة تصرف يستوفي العلاقة السببية المباشرة، ونقل المقاتلين غير الشرعيين الى المناطق التي تجري فيها العمليات العدائية او تجنيد هؤلاء الاشخاص لاستخدامهم في العمليات العدائية مستقبلاً لا يستوفي عنصر العلاقة السببية المباشرة اما في اطار الهجمات السيبرانية : لم يشير الدليل التفسيري الى معيار الخطوة المسببة الواحدة وذلك كما و قلنا سابقاً انه يستخدم القصد بدلاً من الاحتمال الموضوعي بالاضافة الى إمكانية إحداث الضرر بمجموعة من الافعال التي تنطوي تحت عملية جماعية لاحداث الضرر بالخصم، اما بالنسبة الى القرب الزمني والجغرافي لا أهمية له سواء كان الفعل يرتكب عن قرب ام عن بعد طالما ان النتيجة نفسها و اغلبية الهجمات السيبرانية تنفذ عن بعد و هي معقدة و طويلة نوعاً ما.[١٢٦]

ايضاً نذكر أن الاعمال التحضيرية في الهجمات السيبرانية تعتبر مشاركة مباشرة في العمليات العدائية كتطوير اسلحة سيبرانية وفيروسات معينة لتنفيذها على أهداف محددة مسبقاً، وان كانت سوف تستخدم مستقبلاً، فلا تستوفي في هذه الحالة العلاقة السببية في الهجمات السيبرانية : مثلاً ففي حالة قيام مدني ببرمجة فيروس وتقديمه للقوات المسلحة من دون معرفة استخداماته، اما في حال كان المدني قد استخدم من قبل القوات المسلحة لبرمجة هذا الفيروس فتستوفي اذاً العلاقة السببية هنا .[١٢٧]

---

[١٢١] Maiyin Akveld :" crossing Digital borders :Direct participation in cyber hostilities" , master's Thesis, Amesterdam University p 7 , 2016

[١٢٢] علي محمد كاظم الموسوي، مرجع سابق، ص ٨٢

[١٢٣] الدليل التفسيري، مرجع سابق، ص٥١-٥٣

[١٢٥] الدليل التفسيري، مرجع سابق، ص ٥٥

[١٢٦] الدليل التفسيري، مرجع سابق، ص ٥٣

[١٢٧] Emily Crowdford: "Virtual Battlegrounds: Direct Participation in Cyber Warfare" , Sydney Law School, master's Thesis, The University of Sydney ,2012,p14-17

٣ – الإرتباط بالعمل الحربي في إطار العمليات العدائية

يجب من اجل تلبية شرط الارتباط بالعمل الحربي ان يكون العمل مصمماً خصيصاً للتسبب مباشرة بالحدّ المطلوب لحصول الضرر دعماً لطرف في النزاع وعلى حساب الطرف الآخر . [١٢٨]

لكي يرقى عمل معين الى المشاركة المباشرة في العمليات العدائية يجب الاّ يكون فقط من المحتمل موضوعاَ ان يلحق الضرر بل يجب ان يكون ايضاً مصمماً خصيصاَ لإلحاق الضرر دعماً لطرف في النزاع وعلى حساب الطرف الاخر وهذا ما نعنيه بالإرتباط الحربي، علاوةً عن ذلك ان هذا المعيار يصعب توافره في النزاعات المعاصرة التي قد يمتاز أحياناً بضبابية فيما يختص بأطراف النزاع [١٢٩]، كذلك بجب التمييز بين شرط " الإرتباط بالعمل الحربي من شرط العلاقة العامة التي يشير الى العمل المعني وسير العمليات العدائية بين أطراف النزاع المسلح" .[١٣٠]

اذاً لا بدّ ان يكون الفعل قد صمم خصيصاً لإلحاق الضرر بالخصم ودعماً للطرف الآخر فمثلاً : قيام شخص مدني في زمن النزاع العرقي (غالباً ما يكون نزاع غير دولي) بمصادقة شخص آخر من الطائفة العرقية الخصم والقيام بفعل يتسبب بموت هذا الشخص من دون سابقة قصد ومن دون ان يكون الفعل قد صمم خصيصاً لدعم الطرف الاخر في النزاع على حساب الطرف الآخر مما يؤدي الى اعتباره مشاركة مباشرة في العمليات العدائية ولكن نقل المقاتلين والأسلحة لمناطق النزاع لا تشكل مشاركة مباشرة وأنما جريمة حرب او جريمة ضد الانسانية كون ان هذا الفعل لم يصمم خصيصاً لالحاق الضرر بالخصم على دعماً للطرف الاخر ولكن مرتكب هذه الجريمة يتمتع بالحماية من الهجمات المباشرة ولا يمكن إستهدافه وإيقافه عن أفعاله الاّ وفق التشريع الداخلي بينما الشخص الذي يتسبب بموت فرداً من الفريق الآخر يفقد الحماية من الهجمات المباشرة وهذا امر غير منطقي وغير مقبول [١٣١].

ايضاً انتقد مايكل شيميت الصياغة المتوافرة في الدليل التفسيري معتبراً ان شرط العلاقة بالعمل الحربي يتوافر عندما يكون من شأن الفعل ان يدعم طرفاً في النزاع وعلى حساب الطرف الآخر باعتبار انه من الممكن قيام أحد الأطراف باعمال تؤدي الحاق الضرر بكافة اطراف النزاع دون اي منفعة لاي طرف اخر في النزاع، فضلاً عن ان هنالك امكانية ان يكون الفعل يدعم طرفاً دون ان يسبب ضرراً مباشراً فورياً للطرف الاخر ولا يسبب أي ضرر، كذلك إتجه شيميت الى إعتبار أنه من الممكن تعديل صياغة العنصر الاخير على هذا النحو :" لدعم طرف في النزاع او على حساب (بضرر) الطرف الاخر " اي بتوافر احدى هاتين الشروط وليس كلاهما، على الشكل التالي : "in support of a party to the conflict and to the detriment of another".[١٣٢]

أما في سياق الهجمات السيبرانية، ان دليل تالين اختلف عن الدليل التفسيري في رأيه لناحية عنصرالارتباط بالعمل الحربي وإعتبر انه لكي نعتبر أن عملاً ما هو مشاركة مباشرة في الحرب السيبرانية يجب ان يستوفي العمل عنصر الارتباط بالعمل الحربي أي أن يكون الفعل متصلاً مباشرةً بالعمليات العدائية

---

[١٢٨] الدليل التفسيري، مرجع سابق، ص ٥٨

[١٢٩] الدليل التفسيري، مرجع سابق، ص٥٩

[١٣٠] نادر اسكندر دياب "تطور مفهوم المشاركة المباشرة في العمليات العدائية في القانون الدولي الانساني "، مؤسسة عامل وجامعة الحكمة، ٢٠١١ ص ٢٠

[١٣١] علي محمد كاظم الموسوي، مرجع سابق، ص ٩٠

[١٣٢] Michael N Schimitt : "Deconstructing Direct Participation in Hostilities" , op ,cit p 736

الجاري[133]، بمعنى اخر والى جانب العناصر الضرورية الأخرى اذا كان هناك ارتباط مباشر بين الفعل الذي يأتيه المدني و العمليات العدائية يمكن اعتباره مشاركة مباشرة سيبرانية، فهذا الرأي هو الأقرب الى رأي المحاكم الجنائية الدولية(رواندا ويوغوسلافيا) بشأن إرتباط الأفعال بصورة مباشرة ووثيقة مع العمليات العدائية.[١٣٤]

فالأفعال وان لم تلحق ضرراً للطرف الاخر ولكن تلحق منفعة لأحد الأطراف تعتبر مشاركة مباشرة، فوجود علاقة مباشرة بين العمل الذي يقوم به المدني والعمليات العدائية القائمة بين الطرفين حول قيام مثلاً مدني ببرمجة نوع معين من الفيروسات المخصصة لهجوم محدد[١٣٥] او القيام بتوجيه هجمة سيبرانية بهدف السيطرة على طائرة من دون طيار وتوجيهها نحو مناطق النزاع (وان لم يتسبب المهاجم بأية أضرار فهي تعدّ مرتبطة بالعمل الحربي في هذا الإطار) .[١٣٦]

سوف ننتقل تباعاً الى تبيان شروط فقدان الحماية المقدمة دولياً للمقاتل والمدنيين من الهجمات المباشرة وأوجه إستعادتها في الفرع الثاني من هذا المبحث.

الفرع الثاني : شروط فقدان الحماية المقدمة دولياً للمقاتل و المدنيين

يعدّ مبدأ التمييز حجر الزاوية بلا منازع لأحكام القانون الدولي الانساني الرامي الى حماية السكان المدنيين من اثار العمليات العدائية وبموجبه يتعين على أطراف النزاع المسلح في جميع الأحوال على التمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والعسكرية ومن ثم توجه عملياتها ضد الأهداف العسكرية دون غيرها [١٣٧]، بمعنى آخر تقتصر الهجمات المباشرة ضد اللذين يشاركون بصورة مباشرة في العمليات العدائية دون المدنيين، فهذه الفئة الأخيرة تتمتع بحصانة مهمة لناحية الحماية من الأخطار الناتجة عن النزاعات المباشرة، الاّ أن هناك استثنائين على هذه القاعدة يفقد خلالها المدني الحماية الممنوحة له دولياً كالتالي :

١. حالة مشاركة المدني في العمل العدائي بصورة عفوية ومتقطعة ومتكررة .

٢. حالة عدم اعتباره في الأساس من قبيل المدنيين نتيجة اندماجه في الجماعات المسلحة [١٣٨].

ان هذه النتيجة هي من أخطر وأدق النتائج للمشاركة المباشرة في العمليات العدائية لذلك لا بدّ من التأكد من هذه المشاركة قبل حرمان المدني الموجود في حالة الشك الحماية الممنوحة له في القانون الدولي الانساني، وبناءً عليه سوف نقسم هذا المبحث الى جزئين :

---

133 دليل تالين، القاعدة رقم ٣٥، التعليق الرابع

١٣٤ وفق هذه المحاكم لا بدّ من توافر الصلة بين الافعال التي ارتكبها الفاعل مع الصراع القائم تحت طائلة المسؤولية (ICTR Prosecutor.v.Rutaganda Appeal Chamber)

١٣٥ David trurns : Cyberwarefare and the Notion of Direct Participation in Hostilities , Journal of conflict & Security law , Oxford University , Press, 2012,Vol, p 295-296

١٣٦ Willem van poll " direct participation in hostilities : A Cyberspace Oddity?, Master thesis, Faculty of law , University of Amsterdam, 2013 p 65

١٣٧ المادة ٤٨ من البروتوكول الاضافي الأول والقاعدتان الاولى والسابعة من قواعد القانون الدولي الانساني العرفي.

١٣٨ على محمد كاظم الموسوي، مرجع سابق، ص ١١٧

- الجزء الأول : فقدان المدني للحماية على أثر المشاركة المباشرة في العمليات العدائية

- الجزء الثاني : فقدان المقاتل للحماية على أثر المشاركة المباشرة في العمليات العدائية

في الجزء الأول : نحن أمام عدة نظريات في هذا النطاق :

- نظرية اللجنة الدولية للصليب الأحمر

- نظرية خبراء دليل تالين (المعارضين للرأي الأول).

وفق أصحاب النظرية الأولى يفقد المدني الحماية من الهجمات المباشرة طوال مدة كل عمل من الأعمال المحددة التي ترتقي الى المشاركة المباشرة في العمليات العدائية وتسمى هذه النظرية بنظرية الباب الدوار التي استخدمت هذه العبارة لاول مرة عام ١٩٩٠ من قبل Hays Parks في بحثه الموسوم بالحرب الجوية وقانون الحرب (Air War and the Law of War) [١٣٩]،أي أن المدني يفقد الحماية ويستعيدها بالتوازي مع فترات انخراطه في العمل الذي يشكل مشاركة مباشرة في العمل العدائي أي طوال وقت مساهمته في الأعمال العدائية بصورة مباشرة وبغض النظر عن الفترات المتعددة التي يقوم بها المدني بالمشاركة المباشرة في العمل العدائي[١٤٠]، بينما أفراد الجماعات المسلحة المنظمة المنتمية الى طرف من غير الدول لا يعودون أشخاصاً مدنيين ويفقدون الحماية من الهجمات المباشرة على مدى الوقت الذي يستمرون في الوظيفة القتالية[١٤١]، وبرر فقهاء اللجنة الدولية للصليب الأحمر هذا الإتجاه باعتبار أن المدني الذي قام بعمل محدد يصل لمفهوم المشاركة المباشرة يفقد الحماية حتى انتهاء هذا العمل فيستعيدها بانتهاء كل عمل، أما رأي الفقه الأمريكي يرفض نظرية الباب الدوار كون أن تكرار المدني لمشاركته المباشرة في العمليات العدائية بصورة مستمرة هذا من شأنه أن جعل منه فاقداً للحماية من الهجمات بصورة مستمرة[١٤٢].

فالهدف الأساسي من هذه النظرية الى جانب حماية المدنيين من الهجمات المباشرة هو معاملة كل فعل على حدة و بصورة مستقلة بشأن تحديد النطاق الزمني لفقدان الحماية اي عدم معاملة الأفعال أنها مرتبطة ببعضها البعض .

اما خبراء تالين إعتبروا أنه في إطار الهجمات السيبرانية يكون من الصعب تحديد الفاعل الذي قام بتنفيذ الهجوم وهذا الأخير يتم الكشف عنه بعد انتهاؤه حينها يكون الفاعل قد استعاد الحماية الممنوحة له وفق نظرية الباب الدوار، مايكل شيميت يعتبر أن أفضل طريقة لاحتساب فترة فقدان الحماية هي حالة اعتبار أي مدني يشارك بصورة مباشرة في العمل العدائي هدفاً عسكرياً بالنسبة للقوات المعادية ومن الممكن استهدافه خلال الفترات التي تتخلل فيما بين الأعمال العدائية التي تأتيها الى أن يتم التأكد وبصورة لا لبس فيها أن هذا المدني انسحب من تنفيذ العمليات العدائية ولن يشارك فيما بعد الاّ أن هذا الإتجاه يخالف نظرية الانفصال التي نعتبرها الأفضل حتى الان .

فخصوصية هذه الهجمات وطبيعتها المعقدة نوعاً ما تجعل من الصعب تطبيق النظرية الأولى.

---

[١٣٩] على محمد كاظم الموسوي، مرجع سابق، ص ١٢٠-١٢١

[١٤٠] الدليل التفسيري، مرجع سابق، ص ٧٠

[١٤٢] USA ,American department of Defense Law of War Manual , office of General consul department of Defense , june 2015, p 230-231

- نظرية فك الإرتباط أو نظرية الإنفصال من الأعمال العدائية(Detach from Hostilities) :

تعتبر هذه النظرية ان المدني الذي يقوم بالمشاركة المباشرة في العمل العدائي لمرة واحدة او بصورة متقطعة ثم يقوم بعد ذلك بفصل نفسه (بالإنفصال) عن هذه الأنشطة، يعتبر مدنياً ويتمتع بالحماية من الهجمات المباشرة من الوقت الذي يقوم فيه بالإنفصال عن العمل العدائي الذي يعتبر من قبيل المشاركة المباشرة ولا يجوز أن يتم مهاجمته في ما بعد عن العمل العدائي الذي قام به في السابق وإنفصل عن اتيانه [١٤٣]، فالمدني الذي يقوم بعدة أعمال عدائية متقطعة ويعود ويستفيد من الحماية الممنوحة له بعد انتهاء كل عمل عدائي وفق ما إعتبر Bill Boothby ، الاّ أنه يعد أمراً غير مقبول منطقياً وقانونياً، فهو بمثابة دعم غير مباشر لهذا المدني لتشجيعه على القيام بأعمال عدائية مع شرط غير مرئي وهو تنفيذ الفعل بصورة متقطعة، ففترات الراحة بين كل عمل وآخر ليست سوى فترات تحضيرية للعمل العدائي القادم، ففي هذه الحالة لا بدّ من حرمانه من الحماية الممنوحة له دولياً وإستعادتها لا تكون الاّ لمرّة واحدة فقط، أما المدني الذي تكون مشاركته المباشرة متقطعة ومستمرة لا يستفيد من الحماية الممنوحة له [١٤٤].

- الجزء الثاني : فقدان المقاتل للحماية من الهجمات المباشرة

ان أعضاء القوات المسلحة النظامية يفقدون الحماية المعطاة للمدنيين وذلك بسبب مشاركتهم المباشرة في النزاعات وهذا ما أكدته نظرية الدليل التفسيري للجنة الدولية للصليب الأحمر التي تسمى بنظرية " الاستمرار بالمهام القتالية " ويذهب أصحاب هذه النظرية الى انه " لا يعود اعضاء الجماعات المسلحة المنظمة التابعة لأحد أطراف النزاع اشخاصاً مدنيين طوال المدة التي يظلون فيعا أعضاء في هذه الجماعات بموجب استمرارهم في الوظيفة القتالية التي يقومون بها [١٤٥]، وهذه النظرية مطبقة بشكل أكيد على الجماعات المسلحة المنظمة لأن من شأنها أن توفر لأعضاء هذه الجماعات ميزة ميدانية أكيدة التابعين للدول التي من الممكن مهاجمتها في أي وقت [١٤٦] .

فالأعمال التي يقوم بها أفراد القوات المسلحة هي منظمة ومستمرة مما يفقدهم صفتهم كمدنيين الاّ في حال تأكيد أحدهم انه لم يقوم بدور مباشر في الأعمال العدائية وعلى مدى الوقت الذي يقوم يقوم خلاله بهذا الدور، هذه النظرية تتخطى الأشخاص اللذين يستطيعون المشاركة المباشرة في أي وقت طلب منهم ذلك (نعني بالجملة الأخيرة أن ثمة عسكريون يظلون تحت راية الإحتياط وذلك بعد خروجهم من الخدمة الفعلية لمدة معينة، فطوال المدة المذكورة يمكن إستدعائهم في أي وقت للمشاركة في الأعمال العدائية ومن واجبهم تلبية النداء) .

فالقوات المسلحة يمنع عليها إستهداف سوى الجماعات المنظمة التي تقوم بدور قتالي بينما هذه الأخيرة يحق لها استهداف من تشاء من القوات المسلحة التابعة للدولة، فأصبحت هذه النظرية عرضة لإنتقادات كثيرة[١٤٧]

---

[١٤٣] علي محمد كاظم الموسوي، مرجع سابق، ص ١٢٦

[١٤٤] اسامة صبري محمد :" فقدان المدنيين الحق في الحماية من الهجمات المباشرة" جامعة الأنبار للعلوم القانونية و السياسية , ٢٠١٢, العدد السادس ص ١٦٢

[١٤٥] الدليل التفسيري، مرجع سابق، ص ٧١

[١٤٦] الدليل التفسيري، مرجع سابق، ص ٧٢

[١٤٧] NostBakken , Ase Tordahl :" Consequences Under International Humanitarian Law of Civilians who take a direct part in hostilities " University of Bergen , Faculty of Law – Norwegian , Master thesis , 2011,p 23

بشأن توجهاتها الغريبة نوعاً ما، فكيف يمكننا التمييز بين أفراد القوات المسلحة المسموح لهم المشاركة في جميع الأوقات وبين الأفراد اللذين يمكن مشاركتهم في بعض الحالات ؟

ان فكرة التمييز بين الأفراد تعتبر صعبة ومعقدة نوعاً ما مما يدفعنا للإعتبار أن امكانية تحديد النطاق الزمني لفقدان الحماية الممنوحة لأعضاء الجماعات المسلحة أمر غير مجدي وفق هذه النظرية المذكورة أعلاه والتمييز بين المقاتلين ايضاً مرفوضاً لمعارضته مبادئ القانون الدولي الانساني .

فقدان المقاتلين للحماية وفق النظرية العضوية :

تقف النظرية العضوية على قدر من المساواة بين أطراف النزاع عبر تحديد النطاق الزمني لفقدان الحماية فهي تعامل القوات المسلحة والجماعات المعارضة المسلحة بشكل صحيح وفق القانون الدولي الانساني دون تمييز، فعضوية الفرد في القوات والجماعات المسلحة تجعل منه هدفاً مشروعاً للهجمات المباشرة بغض النظر عن مشاركته المباشرة في العمليات العدائية، فاستمرار الفرد بعضويته في الجماعة المسلحة يعدّ بحدّ ذاته تصرفاً دالاً على مشاركته المباشرة في العمليات العدائية .[١٤٨]

الاّ أن هذه النظرية تسمح باستهداف جميع أعضاء القوات والجماعات المسلحة في أي وقت وفي كافة الظروف وهو أمر غير مقبول دولياً مما دفعهم الى إعادة صياغتها وفق ما يسمى "بالنظرية العضوية المحدودة " الي تسمح بمراعاة مسألتين اساسيتين : الأولى هي التأكد من أن تحديد الأشخاص وإنتمائهم للجماعة والقوات المسلحة قد تم بصورة دقيقة وواضحة والثانية هي أن هذه النظرية تعرضت للانتقاد وبالتالي فقدان الحماية على أولئك المحاربين اللذين يتولون المهام يتولون المهام القتالية والمشاركة المباشرة والمستمرة في العمليات العدائية بخلاف الطباخين والموظفين الاداريين[١٤٩] ،أيضاً يجب أن يكون للمقاتل الحق والوظيفة في المشاركة المباشرة في العمل العدائي[١٥٠]، وأن توجه الهجمات المباشرة وفق هذه النظرية ضد من يقوم بتخطيط وقيادة العمليات العدائية وان كان دون سلاح [١٥١].

أما في إطار الهجمات السيبرانية اعتبرت القاعدة ٣٤ من دليل تالين :

" يجوز أن يتم استهداف الأشخاص الآتين بالهجمات السيبرانية كالتالي :

أ- أعضاء القوات المسلحة

ب- أعضاء الجماعات المسلحة المنظمة

ج- المدنيون اللذين يشاركون مباشرةً في العمليات العدائية

د- في نزاع مسلح دولي المشاركون في الهبة الجماعية . "

أما بالنسبة الى النطاق الزمني لفقدان الحماية بالنسبة للجماعات المسلحة المنظمة اختلف خبراء تالين في البدء عندما دعموا رأي الدليل التفسيري معتبرين أن فقدان الحماية من الهجمات السيبرانية المباشرة يكون على أساس استمرار العضو بالمهام القتالية ثم عادوا وإعتبروا أنه لا بدّ الأخذ بالنظرية العضوية وذلك

---

[١٤٨] ICRC, Report DPH 2005, op, cit p48

[149] IBID , P64

[١٥٠] ICRC, Report DPH 2005, op, cit 165

[151] IBID , P٨٣

بالاستناد الى عضوية الفرد في القوات او الجماعات المسلحة التي تجعله هدفا للهجمات المباشرة و فقدان الحماية، برأينا النظرية العضوية المقيدة او المحدودة هي المعيار الأساس والحاسم للتحديد بسبب امكانية المشاركة المباشرة في العمليات العدائية في أي وقت وذلك لسبب بسيط ان العضو في القوات المسلحة للدولة الذي تعرض للاصابة جعلته غير قادر على القيام بأي عمل مسلح وهو غير قادرعلى المشاركة في اي وقت في العمليات العدائية في هذه الحالة يستفيد من الحماية من الهجمات المباشرة و ان بقي عضواً في القوات المسلحة او الجماعات المنظمة .

اذاً نستخلص ان فقدان الحماية من الهجمات المباشرة تتوقف على استطاعة العضو بحكم وظيفته، عضويته، إنتمائه وحتى موقعه الجغرافي من المشاركة المباشرة في العمليات العدائية وذلك وفق أسس واقعية ومعقولة [١٥٢].

لقد انتهينا من معالجة شروط فقدان الحماية المقدمة دولياً للمدني والمقاتل من الهجمات المباشرة على حد سواء، سوف ننتقل الى معالجة أوجه استعادة هذه الحماية .

استعادة الحماية المقدمة دولياً للمدني أو للمقاتل :

إن استعادة الحماية من الهجمات المباشرة امراً معقولاً في القانون الدولي الانساني بالنسبة للمدني ام المقاتل ولكن ضمن حالات محددة حصراً وعلى أثر هذه الاستعادة يبقى هذا المدني مسوؤلاً عن الأفعال التي قام بها والتي تشكل انتهاكات مهمة للقانون الدولي الإنساني والقانون الوطني، بمعنى آخر هذه الإستعادة لا تشكل سبب اعفاء للعقوبة المترتبة في هذه الحالة، وعلى هذا الأساس إعتبرت المادة ٤١ من البروتوكول الاضافي الأول عن حماية العدو العاجز عن القتال (التي تشكل احدى حالات استعادة الحماية من الهجمات المباشرة) التي نصت على ما يلي :" لا يجوز ان يكون الشخص العاجز عن القتال أو الذي يعترف بأنه كذلك لما يحيط به من ظروف محلاً للهجوم، فيعد الشخص عاجزاً عن القتال اذا :

- وقع في قبضة الخصم

- فقد الوعي وأصبح عاجزاً على نحو اخر بسبب جروح أو مرض ومن ثم غير قادر على الدفاع عن نفسه- شريطة أن يحجم في اي من هذه الحالات عن أي عمل عدائي والاّ يحاول الفرار " .

اذاً العاجزعن القتال يتمتع بكامل حقوقه ويستعيد الحماية من الهجمات المباشرة التي فقدها جرّاء مشاركته المباشرة ولكن هذه الحالة تطبق على المدني أو على المقاتل الموجود في قبضة الخصم والتي قيدت حريته وأصبح عاجز عن القتال بسبب حالة الحبس البدني، ايضاً الفرد الذي إستسلم وأصبح غير قادر على الدفاع عن نفسه بسبب مرض أم جرح .

فالفرد ام المقاتل وضمن الشروط التي ذكرت أعلاه يظل متمتعاً بكامل حقوقه المكفولة في القانون الدولي الانساني لناحية الإلتزام بقاعدة بقائه على قيد الحياة وحمايته في عدم التسبب بإصابات أو القتل المتعمد او إلحاق الاضرار به، فجميع هذه الحالات تعتبر محظورات قانونية وبناءً عليه نصت المادة ٨٥ في الفقرتين الثانية والثالثة على الشكل التالي :

[١٥٢] علي محمد كاظم الموسوي، مرجع سابق، ص ١٤١

٢ ." تعد الأعمال التي كيّفت على أنها انتهاكات جسيمة في الاتفاقيات بمثابة انتهاكات جسيمة كذلك بالنسبة لهذا اللحق "البروتوكول" الذي إعتبر أنه إذا اقترفت ضد أشخاص هم في قبضة الخصم وتشملهم حماية المواد ٤٤، ٤٥ و٧٣ من هذا اللحق "البروتوكول"، أو اقترفت ضد الجرحى أو المرضى أو المنكوبين في البحار الذين ينتمون إلى الخصم ويحميهم هذا اللحق "البروتوكول"، أو اقترفت ضد أفراد الخدمات الطبية أو الهيئات الدينية، أو ضد الوحدات الطبية أو وسائط النقل الطبي التي يسيطر عليها الخصم ويحميها هذا البروتوكول".

٣. تعد الأعمال التالية، فضلاً على الانتهاكات الجسيمة المحددة من المادة ١١، بمثابة انتهاكات جسيمة لهذا اللحق "البروتوكول" إذا اقترفت عن عمد، مخالفة للنصوص الخاصة بها في هذا اللحق "البروتوكول"، وسببت وفاة أو أذى بالغاً بالجسد أو بالصحة :

أ) جعل السكان المدنيين أو الأفراد المدنيين هدفاً للهجوم،

ب) شن هجوم عشوائي، يصيب السكان المدنيين أو الأعيان المدنية عن معرفة بأن مثل هذا الهجوم يسبب خسائر بالغة في الأرواح، أو إصابات بالأشخاص المدنيين أو أضراراً للأعيان المدنية كما جاء في الفقرة الثانية "١" ثالثاً من المادة ٥٧،

ج) شن هجوم على الأشغال الهندسية أو المنشآت التي تحوي قوى خطرة عن معرفة بأن مثل هذا الهجوم يسبب خسائر بالغة في الأرواح، أو إصابات بالأشخاص المدنيين، أو أضراراً للأعيان المدنية كما جاء في الفقرة الثانية " أ " ثالثاً من المادة ٥٧،

د) اتخاذ المواقع المجردة من وسائل الدفاع، أو المناطق المنزوعة السلاح هدفاً للهجوم،

هـ) اتخاذ شخص ما هدفاً للهجوم، عن معرفة بأنه عاجز عن القتال،"

ايضاً المادة ٤٦ و ٤٧ من دليل تالين حول الاقتصاص الحربي بحيث نصت المادة ٤٦ منه :" يحظر الاقتصاص الحربي عن طريق العمليات السيبرانية ضد :

أ- أسرى الحرب

ب- المسنين المعقلين، المدنيين في الأراضي المحتلة أو في يد أحد الخصوم في النزاع وكذلك ممتلكاتهم.

ج- اولئك العاجزين عن القتال

د- الموظفين الطبيين، المرافقين، المركبات والمعدات.

في الحالات التي لا يحظرها القانون الدولي، يخضع الإقتصاص الحربي لشروط صارمة ."

كذلك المادة ٤٧ من الدليل نفسه :

" يحظر البروتوكول الاضافي الأول , الدول الأطراف من اتخاذ السكان المدنيين , الأفراد المدنيين , الأعيان المدنية , الأعيان الثقافية و أمكان العبادة , الأعيان التي لا غنى عنها لبقاء السكان المدنيين , البيئة الطبيعية و السدود , الجسور و محطات توليد الكهرباء النووية هدفاً للهجوم السيبراني عن طريق الانتقام " .

كافة هذه الانتهاكات المذكورة أعلاه تعتبر جرائم حرب، ونكرر الصور التي نصت عنها المادة ٤١ من البروتوكول الإضافي الأول التي ذكرت أعلاه ومفادها أن افصاح الشخص بكامل ارادته عن عدم قدرته على الدفاع عن نفسه بسبب حالته الصحية وسلم نفسه للعدو بشكل واضح وبصورة غير مشروطة (وليس الوقوع القهري في قبضة الخصم) وبالمقابل وجب على الخصم قبول هذا الإستسلام وعدم رفضه، أما في

إطار الهجمات السيبرانية فكرة الإستسلام تتم وفق حالات وصور مختلفة، فالخصم الذي يريد الإستسلام يستطيع أن يعبر عنه على سبيل المثال لا الحصر:

- إرسال رسالة الكترونية الى قوات الخصم للتعبير من خلالها عن نيته بالاستسلام وتعد هذه الرسالة كافية لاعتبار هذه القوات عاجزة عن القتال بشرط ان لا تقوم بعد اعلانها عن استسلامها بقيادة عمليات عدائية سيبرانية ضد الخصم الذي وافق على إستسلام المشارك المباشر في الهجمات السيبرانية [١٥٣]، كذلك إعتبر خبراء تالين أن الخداع (الحالة الأولى من حالات إستعادة الحماية) بهدف إعتقاد الخصم بأن المشارك المباشر يريد فعلاً الإستسلام بقصد خيانة الثقة التي منحها الخصم للمشارك المباشر يعد عملاً محظوراً وهذا ما أكدته المادة ٦٠ من دليل تالين على انه :

" في إطار سير العمليات العدائية التي تنطوي على عمليات سيبرانية يحظر قتل أو جرح العدو باللجوء الى الغدر، التصرفات التي تكسب ثقة الخصم بهدف جعله يعتقد بأنه يستحق الحماية (القيام بالتصرف الذي ينطوي على الغدر) أو أن (على الخصم)واجب منح الحماية بموجب قانون النزاعات المسلحة وذلك بقصد خيانة هذه الثقة تشكل الغدر "، اما الحالة الثانية من حالات استعادة الحماية هي حالة المرض او الجرح التي تجعل المشارك المباشر لا يستطيع الدفاع عن نفسه ولكن شريطة التوقف عن القيام بالعمليات العدائية وعدم الهروب فيتمتع اذاً بالحصانة من الهجمات المباشرة أو كان ضمن وضعية الإستعداد لإطلاق النار نحو الخصم او في حال كان في حالة اطلاق النار ولم يتوقف، ففي هذه الأحوال التي ذكرناها ليس بالضروري أن تلتزم القوات التابعة للخصم في الامتناع عن الهجمات المباشرة أما في الاحوال الأخرى فالعاجز عن القتال يعتبر محمياً بموجب القانون من الهجمات المباشرة والنتائج المنبثقة عنها .

في إطار العمليات السيبرانية، ينص التعليق الثالث على القاعدة ٣٤ من دليل تالين أن المشارك المباشر العاجز عن القتال الذي لا يقوم بأية عمليات عدائية ولا يحاول الهروب محمي من الهجمات المباشرة وذلك لأنه من الممكن أن يشارك في العمليات العدائية ويفقد على أثرها الحماية الممنوحه له قانوناً .

لقد إنتهينا من معالجة شروط فقدان الحماية التي يقدمها القانون الدولي الانساني للمدني والمقاتل بسبب مشاركتهم في الهجمات العدائية سوف ننتقل في المبحث الثاني من هذا الفصل لتوضيح مفهوم المسؤولية الجنائية الدولية المفروضة على المشارك المباشر.

المبحث الثاني : المسؤولية الجنائية الدولية المترتبة على المشارك المباشر

يعتبر المشارك المباشر في العمليات العدائية مسؤولاً عن الإنتهاكات المهمة للقانون الوطني والدولي التي إرتكبها وتترتب عليه مسؤولية جنائية دولية تارةً عندما تكون مخالفة للقواعد الدولية ومسؤولية محلية عند مخالفته للقواعد المحلية، سوف نبين هذه النتائج في هذا المبحث، محددين ماهية المسؤولية الدولية في الفرع الأول والحالات إسناد تصرفات هذا المشارك الى الدولة في الفرع الثاني .

الفرع الأول : مدلول المسؤولية الدولية

القانون الدولي "منح" أفراد القوات المسلحة حق المشاركة المباشرة في العمليات العدائية دون مقاضاة أفرادهم عن مشاركتهم فيها وكذلك المشاركين في الهبة الجماعية طالما أن هؤلاء التزموا بقانون الحرب

[١٥٣] دليل تالين، مرجع سابق، القاعدة رقم ٦٠، التعليق السادس

وشتى الإلتزامات التي فرضها القانون الدولي الانساني على هؤلاء، فكل من لا يتمتع بالإمتيازات الممنوحة للمقاتلين وبوضع أسير الحرب لا يملك الحصانة من المقاضاة المحلية لأعمال الحرب المشروعة [١٥٤]، ونعني بأفراد هذه الفئة : المدنيون المشاركون مباشرةً في النزاع المسلح غير الدولي والجماعات المسلحة الفاعلة في النزاعات المسلحة الدولية التي لا تنتمي الى أي طرف من الأطراف المتنازعة في النزاع الدولي ،المرتزقة والجواسيس، اذاً يجوز معاقبة أفراد الفئة المذكورة أعلاه عن مشاركتهم المباشرة في العمليات العدائية وفرض عقوبات مناسبة بحقهم الى الحد الذي يعاقب فيه القانون المحلي أنشطتهم أو عضويتهم أو نتيجة الضرر الذي تسببوا به (نذكر مثلاً الخيانة أو الحرق عمداً أو القتل...الخ) [١٥٥].

فالمقاتلين يتمتعون بحصانة من المقاضاة للأعمال التي تشكل جرائم بموجب القانون الجنائي لأطراف النزاع بالرغم من توافقها مع القانون الدولي الانساني وهذا ما يسمى بإمتيازات المقاتل[١٥٦] وينطبق كل ما تقدم على العمليات السيبرانية غير المشروعة التي تتم في الفضاء السيبراني والتي تشكل إنتهاكات فاضحة للقوانين المحلية والدولية .

المدني أيضاً المشارك في العمليات العدائية يجب أن يحترم القواعد الخاصة بالقانون الدولي الإنساني التي تنظم سير العمليات العدائية وان كان قد لا يتمتع بالحماية من المقاضاة المحلية لا يحق له انتهاك قواعد أساسية وجب القانون احترامها في اطار سير العمليات العدائية، فالمسؤولية المفروضة هي على نوعين : مسؤولية جنائية دولية ومسؤولية جنائية محلية بالنسبة الى المسؤولية الأولى تتحقق نتيجة الإنتهاكات المرتكبة للقواعد الدولية التي فرض القانون الدولي إحترامها والتي تحظرالقيام بأنواع معينة من السلوكيات العدائية(كجرائم حرب أم جرائم ضد الانسانية والابادة الجماعية أم جرائم العدوان وغيرها من الجرائم)، فيخضع مرتكب احدى الجرائم المذكورة أعلاه للمساءلة أمام المحاكم الجنائية الدولية عن الجريمة أم الجرائم التي ارتكبها أثناء سير العمليات العدائية سواء كان من أفراد القوات النظامية ام مدنياً ام احد افراد الجماعات المسلحة، فالصفة هنا لا قيمة لها بل تفرض المسؤولية الجنائية الدولية ام المحلية على مرتكب الفعل سواء كان فاعلاً أم شريكاً ام مساهماً أم متدخلاً .[١٥٧]

أما بالنسبة للمسؤولية الجنائية المحلية : يتم معاقبة الفاعل الذي لا يتمتع بالحصانة من المقاضاة كونه لا تنطبق عليه صفة المقاتل الشرعي.

في اطار الهجمات السيبرانية نواجه صعوبات معينة في هذا الاطار لناحية الطبيعة الخاصة لهذه الهجمات وصعوبة تحديد مكان الفاعل فضلاً عن العراقيل التي تواجه عملية التحقيق والمحاكمة خاصةً بالنسبة للمجرم الذي يرتكب الجريمة السيبرانية في اطار القانون الدولي الإنساني والقانون الدولي الجنائي[١٥٨] وعند مناقشتنا للمساءلة الدولية نتيجة مشاركة المشارك المباشر في العمليات العدائية لا بدّ أن نتحدث عن كيفية تطبيق هذه المساءلة أمام المحاكم الجنائية الدولية، ففي هذا النطاق سوف نلقي الضوء أولاً على الجرائم التي تدخل ضمن اختصاص هذه المحكمة التي ذكرتها، حيث نصت المادة الخامسة من نظام روما الأساسي

---

[154] ICRC, Report DPH,2006,op,cit, p80

[155] ICRC ,Report DPH , 2004,op, cit, P17

[156] ICRC ,Report DPH , 2010,op,cit ,p17

[١٥٧] أنطونيو كاسيزي " القانون الدولي الجنائي "، الطبعة الأولى باللغة العربية، مكتبة صادر للناشرون، ٢٠١٥، بيروت، ص٣٥-٣٦

[١٥٨] علي محمد كاظم الموسوي، مرجع سابق، ص ١٩٩

للمحكمة الجنائية الدولية لعام ١٩٩٨ وفقاً لما يلي : "يقتصر إختصاص المحكمة على اشدّ الجرائم خطورة على الشكل التالي :

أ- جريمة الابادة الجماعية

ب- جرائم ضد الانسانية

ج- جرائم الحرب

د-جريمة العدوان

من خلال النظر في الجرائم التي تدخل ضمن إختصاص المحكمة الجنائية الدولية نستنتج أنها ذكرت على سبيل الحصر لا المثال دون أن تتضمن أي بند يشير الى الجرائم الإلكترونية أم السيبرانية التي تنفذ عن بعد و لكن ما ورد في مقدمة نظام روما الأساسي كافٍ للاتفاق على ضرورة معالجة الجرائم حسب ما وردت : " التي تثير قلق المجتمع الدولي بأسره وأنه يجب ضمان مقاضاة مرتكبيها على نحو فعّال من خلال تدابير تتخذ على الصعيد الوطني والدولي من خلال تعزيز التعاون الدولي وعقدّ العزم على ضرورة وضع حدّ لحالات الافلات من العقاب و على الإسهام بالتالي في منع هذه الجرائم .." [١٥٩].

اما بالنسبة الى للصلاحية الاقليمية للمحكمة الجنائية الدولية نشير أن المادة ١٢ من نظام روما الاساسي ذكرت الشروط المسبقة لممارسة هذا الإختصاص في الفقرة الثانية منها بالنسبة الى الجرائم التي : تقع في إقليم أحد الأطراف أو أن يكون الشخص مرتكب الجريمة أحد رعاياها (دون تحديد المفهوم الدقيق لعبارة الاقليم سواء كان الإقليم التي ترتكب فيه الجريمة او الغقليم التي تقع فيه آثارها)، وعلى المستوى الوطني ينبغي القول بانه لا يوجد في ممارسات الدول ما يشير الى الإختصاص القضائي الإقليمي بالنسبة للجرائم السيبرانية ولكن يوجد بعض الممارسات التي تشير له بشأن الجرائم التي تقع عن بعد او من خلال الإنترنت [١٦٠] يذكر مثلاً القضية التي رفعت على شركة Yahoo عام ٢٠٠٢ من قبل بعض الجمعيات الفرنسية بسبب عرض بعض الرموز النازية وبيعها في فرنسا على الإنترنت وطالما أن الفعل والآثارالضارة وقعت في فرنسا يعود للقضاء الفرنسي الصلاحية الإقليمية للنظر في هذه القضية بالرغم من خصوصيتها [١٦١] .

نشير بالذكر أن الهجمات السيبرانية التي تعرضت لها استونيا عام ٢٠٠٧، يعود الحق للسلطات القضائية الاستونية في متابعة القضية و محاسبة الفاعلين بعد التأكد من هويتهم وخاصةً أنه في اطار الهجمات السيبرانية يختلف الأمر نوعاً ما بالنسبة للصلاحية الاقليمية، فنصت القاعدة الثانية من دليل تالين على ما يلي :

"من دون الإخلال بالإلتزامات الدولية الأخرى المعمول بها يجوز للدولة ان تمارس ولايتها القضائية على:

أ- الأشخاص المتورطين في الأنشطة السيبرانية على أقليميها

---

[١٥٩] جزء من مقدمة نظام روما الاساسي للمحكمة الجنائية الدولية لعام ١٩٩٨

[١٦٠] علي محمد كاظم الموسوي، مرجع سابق، ص ٢٠٣

[161] Elissa.A.Okoniewski :" The french Challenge to Free Expression on the internet ", American University International Law review,2002,article 6, p311

ب- البنية التحتية السيبرانية الواقعة على أراضيها

ت- خارج أراضيها وفق القانون الدولي " .

كذلك نص التعليق الثاني الوارد على هذه القاعدة الى أن الدولة تمارس ولايتها القضائية على أساس الوجود المادي أو القانوني للشخص أو الأعيان في إقليمها وأيضاً التعليق السادس اعتبر أن أن هنالك صورتين للولاية الإقليمية وخاصةً في الفضاء السيبراني : فالصورة الأولى هي الولاية الإقليمية الذاتية والصورة الثانية هي الولاية الإقليمية الموضوعية، ما نعنية في الولاية الأولى هي حق الدولة في النظر في الحوادث والجرائم التي تبدأ على أقليميها ولو إنتهت على إقليم دولة أخرى أما الصورة الثانية نعني بها حق الدولة النظر في الجرائم التي لها تأثيرات على إقليميها بالرغم من حدوثها أو إبتدائها خارج هذا الإقليم [١٦٢] .

ومن الصور الأخرى للولاية الإقليمية وفق دليل تالين : جنسية الفاعل، جنسية الضحية، إمكانية تهديد الأمن القومي للدولة، إنتهاك قاعدة عالمية للقانون الدولي (الصلاحية القضائية العالمية)[١٦٣].

بعد أن انتهينا من معالجة الصلاحية الإقليمية للمحكمة الجنائية الدولية بالنظر للجرائم المرتكبة عن بعد،سوف ننتقل الى معالجة أصول تحقيق ومحاكمة المشارك المباشر في الهجمات السيبرانية عن الجرائم المرتكبة . فيعتبر الفاعل مسؤولاً عن الإرتكاب المادي للجريمة او الإمتناع عن سلوك يسبب ضرراً معيناً سواء بمفرده أو بالاشتراك مع جناة اخرين لكن اثبات وقوع الفعل وتقدير الضرر ومكان ارتكاب الفعل وهوية الفاعلين صعباً نوعاً ما وذلك لأن معظم الهجمات السيبرانية تنفذ عن بعد وفي معظم الحالات لا يمكننا التأكد من هوية الفاعل ومن التفاصيل اللازمة للقضية كون ان العملية تنفذ عن طريق حاسوب موجود في دولة معينة يستهدف حاسوب او مجموعة من الحواسيب الموجودة في الدولة ذاتها ام في دولة أخرى أو حتى عند استهدافه لمجموعة من الحواسيب يمكن ان يكون أمام حالة وجود كل حاسوب في دولة معينة، فيلزم على المحكمة الناظرة في هذه القضية أن تتأكد من كافة المعطيات ان أمكن ذلك قبل النطق بأي حكم.

عند التثبت من كافة الشروط اللازمة للسير بالقضية تبدأ عملية التحقيق والمحاكمة، ففي حال تعرفت المحكمة الى هوية الفاعل ومكانه وأثبتت أنه ارتكب الفعل في اطار النزاع أكثر من جريمة أو إنتهاك فلا بدّ للمحكمة أن تأخذ بالفعل اوالانتهاك الأشدّ ليتسنى الفرصة للقضاء من التحقق والمحاكمة بدقة كافية وأن يتم ترك الانتهاكات التي تكون أقل شدّة للقضاء الوطني[١٦٤]، فالمحكمة الجنائية الدولية الخاصة بيوغوسلافيا السابقة وضعت بعض المعايير للمحاكمة السليمة أمام المحكمة الجنائية الدولية على الشكل التالي :

- خطورة الجريمة

-أعداد الضحايا، مدة الجرائم، نطاق التدمير، وظيفة الشخص المشتبه به ودوره، سواء كان من أجهزة الدولة أو من القوات النظامية أو من الكيانات التي تمارس بعض اختصاصات السلطة الحكومية أو له صفة سياسية معينة [١٦٥]، فتحديد عناصر المسؤولية الجنائية الفردية من أهم المساهمات الي أدخلها النظام الأساسي للمحكمة الجنائية الدولية ليوغوسلافيا السابقة و خاصةً المادة السابعة منه .

---

[١٦٢] دليل تالين، مرجع سابق، القاعدة الثانية، التعليق السادس

[١٦٣] دليل تالين، مرجع سابق، القاعدة الثانية، التعليق الثامن

[١٦٤] علي محمد كاظم الموسوي، مرجع سابق، ص ٢٠٦-٢٠٧

[١٦٥] Fausto Bukar :" The International Tribunal for the Former Yugoslavia ", The united Nations

اذاً هذه الشروط والمعايير السابق ذكرها تطبق ايضاً على العمليات السيبرانية وعلى المشارك المباشر ولكن الفرق أنه في إطار الهجمات والجرائم السيبرانية نكون امام صعوبة في الإثبات والتحقيق وايضاً لناحية تطبيق المعايير التطبيقية التي وضعت في إطار العمليات العدائية التقليدية على الهجمات السيبرانية مثلاً الهجمات السيبرانية التي تهدف الى التحكم بالقواعد الخاصة بطائرة مدنية (بالاتفاق مع قائد الطائرة) بهدف تغيير مسارها بشكل قسري يؤدي هذا الأمر الى موت مئات الأشخاص المدنيين الذي لا ذنب لهم فضلاً عن أضرار مادية بسبب خروجها عن مسارها الطبيعي، فالمسؤولية هنا تنقسم بمقدار مشاركة كل جهة في تحقق النتيجة، كذلك على الدول بموجب أحكام القانون الدولي الانساني أن تلتزم بالبحث عن الأشخاص اللذين يزعم ارتكابهم أو أقروا بارتكاب جرائم تعنيف ذكرت على أنها مخالفات خطيرة لاتفاقيات جينيف لعام ١٩٤٩ و البروتوكولات الأربعة وتقديم هؤلاء الأشخاص للمحاكمة بغض النظر عن جنسيتهم ويجوز للدول عوضاً عن ذلك وبما يتماشى دائماً مع مبادئ القانون الوطني والدولي ذات صلة بتسليم هؤلاء المتهمين الى دولة أخرى لمحاكمتهم بشرط أن تقدم الدول قضية ظاهرة الوجاهة [١٦٦] .

وهذا ما جاء في المادة ٤٩ الفقرة الثانية من إتفاقية جينيف الأولى والمادة ٥٠ الفقرة الثانية من اتفاقية جينيف الثانية و المادة ١٢٩ من اتفاقية جينيف الثالثة و المادة ١٤٦ الفقرة الثانية من اتفاقية جينيف الرابعة : " وكذلك اتخاذ جميع التدابير اللازمة لقمع جميع الأفعال المخالفة لأحكام الاتفاقية، ان الدول يجوز لها أن تتخذ طائفة واسعة من التدابير اللازمة لمنع تكرارها " [١٦٧].

ففي إطار الهجمات السيبرانية يتم الفعل غير المشروع عند انطلاق التصرف الالكتروني الهجومي من الحاسوب أو من مركزه المنشأ بهدف اتلاف أو تدمير المعلومات أو السيطرة على المنشأت المستخدمة او بهدف التسبب بإصابة او وفاة أشخاص نتيجة هذه الهجمات، أما لناحية الفعل المادي يعتبر متحققاً لحظة انطلاقه من الحاسوب نحو المنشأة التي يريد إستهدافها وإن لم تتحقق النتيجة المرجوة طالما أنه كان من الواضح ان المتهم يريد إرتكاب الفعل أو أنه كان يدرك أن من شأن تصرفه او إمتناعه سوف يحقق النتيجة المرجوة وفقاً للسير العادي للأحداث أي أنه يتم التركيز على النية والإرادة الجرمية، أما بالنسبة للمحاولة : في الجرائم التقليدية المحاولة الجرمية معاقب عليها، فهل هو الأمر نفسه في اطار الهجمات السيبرانية ؟

لا بدَ الحديث عن حالتين بالنسبة لهذا الموضوع :

١. في حال التثبت من وقائع وظروف الهجوم السيبراني :

إثبات المسؤولية الجنائية الفردية عن ارتكاب الهجمات السيبرانية والقصد الجنائي يكمن في اثباتهما بعض الصعوبات العملية، فالمحكمة في هكذا نوع من الجرائم يجب ان تتأكد بشكل أكيد أن الجريمة قد ارتكبت بالفعل من قبل شخص أصبحت هويته معروفة ومن حاسوب معين وضمن نقطة معينة من العالم .

٢. في حال عدم التثبت من وقائع وظروف الهجوم السيبراني :

في حال لم يتم التثبت من وقائع الهجوم وخاصةً عندما يتم توجيه هجمات سيبرانية عن طريق حواسيب في دولة أ مثلاً الى دولة ب، أو في حال توجيه هجمات سيبرانية من خلال حواسيب موجودة في دولة أ ولكن

Audiovisual library of international law , p2

[١٦٦] الدليل التفسيري، مرجع سابق، ص ٢٧٦

[١٦٧] اللجنة الدولية للصليب الاحمر، التعليق على اتفاقية جينيف الأولى الخاصة بتحسين حالة المرضى والجرحى في القوات المسلحة في الميدان، مطبعة كامبردج، الطبعة الثانية لعام ٢٠١٦، المادة ٤٩

تمت السيطرة عليها من خلال اشخاص موجودين في دولة ب ضد دولة ج ,ففي هذه الحالة الفاعلين الحقيقين ليسوا موجودين في الدولة مكان انطلاق الفعل الجرمي ، فعلى المحكمة التثبت من وقائع و ظروف كل هجوم لترتب المسؤولية الجنائية الصحيحة على الفاعلين.

المساعدة في إطار الهجمات السيبرانية :
ان المساعدة في إرتكاب جريمة ما تكمن في امداد الفاعل باي وسيلة لاتمام العمل الجرمي، فيعد شريكاً في الجريمة من أعطى الفاعل اي سلاح أو الة أو أداة او اي شيئ اخر يقصد من خلاله معاونة الفاعل على ارتكاب الجريمة بأي صورة كانت مع علمه بالأمر، وهذا ما أكدته المادة ٢٥ (الفقرة ٢- ج) من نظام روما الاساسي التي نصت : " يسأل جنائياً ويكون عرضة للعقاب عن أية جريمة تدخل في اختصاص المحكمة الشخص الذي يقوم بتقديم العون او المساعدة باي شكل اخر لغرض تسيير ارتكاب هذه الجريمة أو الشروع في ارتكابها بما في ذلك توفير وسائل ارتكابها "، من الأمثلة على المساعدة وتقديم العون في تنفيذ الهجمات السيبرانية عندما يقوم بمساعدة الفاعل على تهيئة الحاسوب وامداده بالبرامج اللازمة التي تساعده على توجيه هجمات معينة أو مثلاً من يقوم بتصميم وتهيئة تفاصيل الأسلحة السيبرانية لكي تكون جاهزة عند توجيه الهجوم مع علمه المسبق بأن الأعمال التي يقوم بها تساعد على ارتكاب الهجوم وليس بالضرورة أن يكون هنالك إتفاق مسبق مع الفاعل على ارتكاب الجريمة وإنما يكفي أن يكون الشريك عالماً بإرتكاب الفاعل للجريمة وأن يساعده في الأعمال المجهزة أو المسهلة أو المتممة لإرتكابها [١٦٨].

اخيراً سوف نوضح في الفرع الثاني من هذا الفصل إمكانية إسناد تصرفات المشارك المباشر للدولة وفق القواعد المعمول بها محلياً ودولياً.

الفرع الثاني: إمكانية إسناد تصرفات المشارك المباشر للدولة

إن إمكانية اعتبار تصرفات المشارك المباشر منسوبة للدولة في حال كان لا ينتمي الى أحد أجهزتها أو الكيانات التي تمارس بعض إختصاصات الحكومة تطرح سؤال مهم، وهو هل يمكننا بالفعل إسناد تصرفات المشارك المباشر للدولة وان كان لا ينتمي اليها ؟

نحن أمام شرطين :

الشرط الأول : في حل كان الشخص أو مجموعة الأشخاص يتصرفون في الواقع بناءً على تعليمات الدولة أو بتوجيهاتها أو تحت رقابتها .

الشرط الثاني : إمكانية اعتبار الفعل الذي يقوم به الشخص أو مجموعة من الأشخاص بمثابة إنتهاكاً للقانون الدولي .

إعتبرت المادة الثامنة من مشروع المسؤولية الدولية أن المشارك المباشر وإن لم ينتمي الى أحد اجهزة الدولة او مؤسساتها فقد يكفي أن يتصرف ضمن التوجيهات أو التعليمات التي يتلقاها من الدولة لإسناد التصرفات التي يقوم بها لهذه الأخيرة، نحن هنا أمام الحالة التي تقوم فيه أجهزة الدولة لاستكمال أعمالها بتجنيد أو تحريض أشخاصاً عاديين مدنيين أو مجموعات من الاشخاص للعمل كمساعدين مع بقائهم خارج الهيكل الرسمي للدولة، على سبيل المثال : تعين أفراد أو مجموعات عاديين مساعدين في قوات الشرطة أو القوات المسلحة أو ارسالهم الى البلدان المجاورة مع اعطائهم تعليمات خاصة لتنفيذ مهام معينة بالرغم أنهم

[١٦٨] محمود محمود مصطفى : " شرح قانون العقوبات-القسم العام "، الطبعة الثامنة، دار النهضة العربية، ١٩٦٩، ص٣٣٣

غير مفوضين تفويضاً محدداً من الدولة ولا يشكلون جزءاً من قواتها المسلحة [١٦٩]، وتتوقف كل حالة على وقائعها الذاتية، فالمصطلحات الثلاثة : " التوجيه والرقابة والتعليمات " الواردة في المادة ٨ منفصلة ويتعين على صاحب العلاقة أن يثبت أياً منها [١٧٠].

بالنسبة الى نوعي السيطرة : السيطرة الفعالة والسيطرة الكاملة : فالأولى تطبق أحكامها محكمة العدل الدولية : تعني أن تكون للدولة رقابة فعلية وفعالة على عملية محددة لكي تنسب هذه العملية فقط اليها، اذ لا تنسب تصرفات وانتهاكات المشارك المباشر في هذه الحالة الى الدولة الاّ اذا كانت هي التي وجهت أو راقبت العملية المحددة وكانت التصرفات موضوع الشكوى تشكل جزءاً لا يتجزأ من هذه العملية [١٧١]، يطبق فقط على الجماعات والأفراد غير المنظمة ولا تطبق على المنظمة، فلا بدَ أن تبسط الدولة سيطرتها على كل عملية عدائية لكي تنسب المسؤولية لهذه الأخيرة وتتحمل مسؤوليتها الدولية، فضلاً عن التزام هؤلاء الأفراد أو الجماعات بالتوجيهات التي تصدرها الدولة وفرض رقابتها على العملية المعينة التي يقوموا بها ولا يمتد هذا المعيار لكي يشمل التصرفات التي لا تكون مرتبطة بالدولة الاّ ارتباطاً هامشياً أو عرضياً بعملية ما والتي أفلتت من توجيه الدولة ورقابتها [١٧٢] .

اذاً السيطرة التي تمارسها الدولة يجب أن تكون فعالة وكاملة ولكن ضمن عملية واحدة ومحددة لكي تنسب المسؤولية اليها وبسبب ضعف هذا النوع من السيطرة وهشاشته وقلة وضوحه دفع الأمر الى تبني الإتجاه التي ذهبت اليه المحكمة الجنائية الدولية ليوغوسلافيا السابقة (معيار السيطرة الكاملة) التي نستخلص شروطه على الشكل التالي :

١- لا تطبق الاّ على الجماعات المنظمة فقط ولا يشمل تلك الغير منظمة والأفراد .

٢- تحديد التوجهات والتخطيط العام للعمليات التي تقوم بها الجماعات المنظمة بالاضافة الى التمويل والدعم المادي والمعنوي.

في اطار الهجمات السيبرانية نميز بين عدّة حالات :

الحالة الأولى : قيام الجماعات المنظمة بناءً على تعليمات الدولة بتنفيذ هجمات ضدّ هدف معين، وفقاً لمعيار السيطرة الفعلية تعتبر الدولة مسؤولة عن تصرفات هذه الجماعات المنظمة وذلك بسبب اعطاءها تعليمات خاصة بكيفية تنفيذ الهجمات نحو هدف معين محدد بذاته، ولكن نشير أن الدولة لا تكون مسؤولة وفقاً لهذا المعيار عن تصرفات الجماعات المنظمة في حال لم تزود هذه الأخيرة بأية تعليمات أو توجيهات خاصة بتنفيذ الهجوم، ايضاً تسأل دولياً عن تصرفات الأفراد والجماعات المنظمة أو غير المنظمة التي تقوم بهجمات سيبيرانية ضمن تعليمات معينة لتوجيه هجوم معين وذلك من أجل التخلص من المسؤولية الدولية أي كمنفذ غير شرعي للهروب من العقاب والرقابة هنا تصبح أكثر من مجرد تحريض أو ابداء الدعم المعنوي الى المشاركين مباشرةً في الهجوم السيبراني[173].

---

[١٦٩] مشروع المسؤولية الدولية عن الأفعال غير المشروعة دولياً، مرجع سابق، المادة الثامنة، التعليق الثاني

[١٧٠] المرجع سابق، المادة الثامنة، التعليق السابع

[١٧١] علي محمد كاظم الموسوي، مرجع سابق، ص ٢٢٩-٢٣٠

[١٧٢] مشروع المسؤولية الدولية عن الأفعال غير المشروعة دولياً، مرجع سابق، المادة الثامنة، التعليق الثالث

[١٧٣] دليل تالين، مرجع سابق، القاعدة السادسة، التعليق الحادي عشر

- الحالة الثانية: اقدام الجماعات المنظمة على استخدام أسلحة ووسائل سيبرانية مقدمة من الدولة في اطار الهجمات السيبرانية التي توجه ضدّ أهداف عامة بعلم الدولة، ففي هذه الحالة تسأل الدولة سيبرانياً ودولياً عن المخالفات التي وجهت ضدّ أهداف ومرافق عامة والتي أدت الى خسائر مادية أو بشرية وحتى معنوية والتي اعتبرت انتهاكات دولية تجاوزت من خلاله هذه الجماعات الحدود الموضوعة لها دولياُ [١٧٤]، نطبق في هذه الحالة معيار السيطرة الكاملة طالما أن الدولة لم تحدد هدفاً معيناً للجماعات المنظمة وهذا ما أشار اليه خبراء تالين .

- الحالة الثالثة : حالة عدم امكانية نسبة تصرفات المشارك المباشر في الهجوم السيبراني للدولة

اختلفت الاراء حول امكانية توجيه هجمات مضادة ضد المشارك المباشر في الحالة التي لا يمكننا اسناد تصرف هذا الاخير للدولة، هل للدول الحق في الدفاع عند تضررها من هجوم سيبراني قام به فرداً أو جماعة غير منظمة عندما يعتبر من الصعب اسناد هذا الهجوم للدولة ؟

نحن أمام عدة آراء في هذه المسألة المطروحة أعلاه :

* رأي محكمة العدل الدولية : أعتبرت المحكمة أنه من غير الممكن ممارسة حق الدفاع الشرعي في العلاقات الدولية بناءً على وجود هجوم مسلح قام به فرداً أو جماعة غير منظمة، فالحق في الدفاع يكون فيما بين الدول فقط [١٧٥] .

*الرأي الراجح في الفقه : هو امكانية توجيه الدولة المتضررة تدابير مضادة أو ممارسة حقها في الدفاع الشرعي عن نفسها بوجه المشارك المباشر ان كان من غير الدول وذلك بسبب عدم امكانية اسناد تصرفاته أو الهجوم السيبراني الذي قام به للدولة وهذا ما أكده Nicholas Tsagourias في كتابه الشهير : " Cyberattacks Self Defense and the Problem of Attribution " الذي اعتبر من خلاله أن الهجمات الفاعلة من غير الدول يتوافر فيها بعض مقومات الشخصية القانونية التي يترتب عليها تحمل هذه الجهات المسؤولية الدولية عن أفعالهم بحيث يكون لهؤلاء السلطة الفاعلة والسيطرة على أجزاء من الأقاليم كي تتأهل لحمل المسؤولية الدولية , فقد يكون كافياً عند توافر هذه الشروط الى اعتبار هذه الجماعات شخصاً من أشخاص القانون العام [١٧٦] .

نشير أيضاً أن غالبية الدول في عصرنا الحالي تلجأ الى اتخاذ تدابير مضادة في اطار دفاعها وذلك عند تعرضها لهجمات سيبرانية من قبل افراد أم جماعات غير منظمة عندما يتعذر على الدولة أن تمنع الضرر الناتج عن الأفعال غير المشروعة التي تقوم بها هذه الجماعات أو حتى أن تتحكم بأعمالها ومنعها أو قبولها الضمني أو العلني لهذه الأفعال، فالدولة أحياناً هي من تقوم بايواء هذه الجماعات المسلحة الغير منظمة من أجل تنفيذ المخططات التي تريدها دون أن ينسب أي عمل لها وذلك بهدف الهروب من العقاب الدولي.

من أبرز الأمثلة هي حالة قيام الولايات المتحدة الأمريكية بشن هجومات واسعة النطاق ضد التنظيمات و الجماعات المسلحة غير النظامية في العراق و سوريا أفغانستان و غيرها من البلدان خاصةً بعد أحداث

---

[١٧٤] علي محمد كاظم الموسوي، مرجع سابق، ص ٢٣١

[١٧٥] فتوى محكمة العدل الدولية بشأن الأثار القانونية النشئة عن تشييد جدار في الأرض الفلسطينية المحتلة لعام ٢٠٠٤، الفقرة ١٣٩، ص٦٩

[١٧٦] علي محمد كاظم الموسوي، مرجع سابق، ص ٢٣٣-٢٣٤

الحادي عشر من سبتمبر , فقد اعتبر رئيس الولايات المتحدة أن دولته تمارس حقها في الدفاع بوجه الأعمال الارهابية التي قام بها تنظيم القاعدة وان لم تكن تعتبركقوات نظامية تابعة للدولة وإنما يحق للولايات المتحدة ممارسة حقها في الدفاع على أكمل وجه [١٧٧].

ختاماً، لهذا يجب أن نشير أننا من خلال دراستنا هذه توصلنا الى توضيح المفاهيم المتعددة لمسألة الهجمات السيبرانية على ضوء الإتفاقيات والمعاهدات الدولية والآراء الفقهية المختلفة والوصول الى تعريف موحدّ متفق عليه للهجمات السيبرانية، مع ضرورة توفير الحماية القانونية للمعلومات الإلكترونية من أي تهديد سيبراني، ويلاحظ أننا توصلنا الى تكييف مسأل الهجمات السيبرانية الغير منظمة دولياً ضمن أحكام القانون الدولي الإنساني شأنها شأن اي سلاح جديد لم يتم معالجته سابقاً، مع الإعتراف بحق الدولة المعتدى عليها سيبرانياً دفع التهديدات والهجمات التي تتعرض لها عن طريق ممارسة حقها في الدفاع الشرعي أو التدابير المضادة، مع إحترام المبادئ الدولية التي ترعى سير العمليات العدائية السيبرانية من أجل حماية المدنيين من الآثار السلبية الخطيرة التي يمكن أن تلحق بهم جرّاء هذه العمليات، سوف ننتقل تباعاً الى القسم الثاني من بحثنا في القسم الأول الى الإمكانيات الدولية والإقليمية والمحلية القانونية والتقنية لضمان الإستخدام للمعلومات في الفضاء السيبراني،بالإضافة الى دور المشرع الوطني في وضع حدّ للهجمات السيبرانية عبر تطوير القوانين القائمة في القسم الثاني .

القسم الثاني : نحو إتحاد دولي للتعامل مع الهجمات الإلكترونية وتأمين الفضاء السيبراني

فرضت التهديدات الالكترونية تحديات أمنية سيبرانية جديدة على الساحة الدولية خاصةً مع ظهور الأسلحة السيبرانية والكيميائية والنووية والبيولوجية وغيرها مما أدى الى تبلور ضرورة الحد من هذه التهديدات عن طريق اعتبار ان الفضاء الإلكتروني يجب أن يظل شأنه شأن غيره من المجالات التي يمارس فيها الانسان نشاطه محكوماً بالقواعد العامة التي تحقق صالح المجموعة الدولية والمحلية [١٧٨]، فقد أصبح هذا الفضاء مرفقاً دولياً لممارسة الدولة كافة التكتيكات والخطط الالكترونية من أجل تدمير الطرف الأخر وتحقيق مزايا نوعية في هذا المجال خاصةً مع سعي هذه الأخيرة الى تطوير أسلحة الكترونية جديدة تنفرد بها عن الدول الأخرى.

إزاء كافة هذه الإستخدامات غير المشروعة وتصاعد حجم الأخطار الإلكترونية وغياب المحاسبة والعقاب ومحاولة الفاعلين الى تطوير اسلحة غير مملوكة من الدول الأخرى لممارسة سيطرتهم الدائمة على الساحة الدولية من خلال إمتلاكهم أجهزة الحاسبات والمعلومات والشبكات الإلكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة على تعزيز الصراع الالكتروني وتطوير القدرات الهجومية والدفاعية للدولة (عبر فرض أليات جديدة للهيمنة الاقتصادية والثقافية والعسكرية والاجتماعية والقدرة على احتكار عمليات

---

[١٧٧] Presidential Address to the Nation (11 September 2001) available at: http:// georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010911-16.html4 (accessed 18 June 2012).

[١٧٨] عادل عبد الصادق : اسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني " , وحدة الدراسات المستقبلية- مكتبة الاسكندرية-مصر , ٢٠١٦,ص ٩

تدفق المعلومات وإنتقال هذه الهيمنة من الدول الى الشركات الكبرى) مما أدى الى فرض عالماً جديداً تحكمه القوى الكبرى.

هذه التطورات الكثيرة دفعت بالمشرع الدولي السعي الى التوصل الى إتفاقيات وبروتوكولات جديدة لتنظيم عملية الهجمات السيبرانية بين الدول عبر وضع أحكام متطورة تراعي الانتقال النوعي في الفضاء السيبراني وهذا ما سوف نحاول بحثه في الباب الأول من هذا القسم من خلال تأمين الفضاء السيبراني عبر تفسير كافة السبل والإمكانيات القانونية والتقنية التي تساعد الدول والشركات والمؤسسات والأفراد على حماية مصالحهم و معلوماتهم الخاصة مع تحديد الدورالذي يلعبه المشرع الدولي من أجل وضع حد لهذه الهجمات (الفصل الأول)، كذلك الأمر بالنسبة الآليات التقنية المتطورة في الحدّ من الهجمات السيبرانية (الفصل الثاني) وفي الباب الثاني تفسير امكانية المشرع المحلي في تطوير الأنظمة والأحكام السائدة كي تتماشى مع التطورات الحديثة وأبرز المعوقات الوطنية التي تحول دون تحقيق هذا الهدف (الفصل الأول), مع تبيان اهمية التعاون والتدريب المحلي على مواجهة الهجمات السيبرانية واالحد من آثارها (الفصل الثاني) .

الباب الأول : الإمكانيات القانونية والتقنية لضمان الإستخدام السليم للمعلومات في الفضاء السيبراني

أصبح الفضاء السيبراني مجالاً خطراً بالنسبة للدول النامية تحديداً على اثر تعرضها المستمر للهجمات السيبرانية و حرمانها من استخدام الانترنت في بعض الأحوال و ذلك لأسباب سياسية و اقتصادية و غيرها , كذلك الأمر بالنسبة للشركات الصغيرة و المتوسطة التي تستهدف دائماً في بياناتها ومعلوماتها وأموالها فضلاً عن الخسائر التي تلحق بعملائها مما يؤثر على ثقتهم بها وتحد من قوتها الموجودة أما الأفراد اللذين يتعرضون لهجمات سيبرانية تفقدهم معلوماتهم الشخصية و أموالهم و ممتلكاتهم , و لكافة هذه الاسباب أعلاه اصبح من الضروري الوصول منطقة الكترونية أمنة عبر الاستخدام السليم للفضاء السيبراني.

فكافة الأهداف التي نطمح الوصول اليها دولياً ومحلياً لا جدوى لها دون وجود آليات تشريعية وتقنية تحمي الدول والشركات والأفراد من نتائج الاستخدام غير السليم للفضاء السيبراني، ففي هذا الباب سوف نبحث في دور المشرع الدولي في تطوير تشريعات جديدة تتماشى مع المستجدات السيبرانية وتفعيل التعاون مع الدول الأخرى وكيف يستطيع التفوق على كافة العراقيل الدولية التي يمكن أن تواجهه سواء كانت قانونية أم قضائية أم تقنية (الفصل الأول) مع تبيان كافة الأساليب التقنية التي من شأنها الحد من الهجمات السيبرانية وحماية أنظمة الشركات والمؤسسات العامة (الفصل الثاني).

الفصل الأول : الآليات القانونية للحدّ من الهجمات السيبرانية

أن الطريقة الفضلى للحدّ ومواجهة جريمة أو سلوك معين مخالف للقانون هي إخضاعه لمبدأ التجريم والعقاب وهذا المبدأ نفسه يمكن تطبيقه على موضوع الهجمات السيبرانية , فهذه الأفعال لا يمكن محاربتها سوى بتنظيم أحكامها قانوناً و الأعتراف بها كجريمة مخالفة للقانون مكتملة العناصر والأركان، فدور القانون يتمثل في اخضاع المخالفين لأحكامه عبر تجريم أفعالهم ومعاقبتهم مهما تطورت الأفعال الجرمية والاساليب الملتوية المستخدمة من قبلهم، فيبقى قادراً على مواجهة كافة التطورات الإجرامية من أجل المحافظة على حقوق ومصالح الأفراد والجماعات، ولكن هذا الأمر لا يتحقق دون سنّ المشرع لقوانين جديدة تتلائم مع المستجدات الجرمية على أن يكون هذا الأخير جاهزاً من كافة النواحي القانونية و الفنية و التقنية للقيام بهذا الأمر (فلا يمكننا تصور مشرع يريد سنّ قوانين جديدة تتلائم مع الجرائم المعلوماتية و هو لا يتمتع بأدني المؤهلات التقنية و القانونية اللازمة للقيام بهذا الأمر)، بالإضافة الى ذلك لا يمكن التوصل الى بيئة سيبرانية صحية دون التشديد على ضرورة التكاتف والتضامن والتعاون بين كافة الدول والأجهزة والمنظمات من أجل التوصل الى هذا الهدف وهذا ما سوف نوضحة في الفصل الحالي، ففي المبحث الأول سوف نبين أهمية التعاون بين الدول في المجالين القضائي والشرطي، أما في المبحث الثاني سوف نلقي الضوء على الواقع التشريعي والقضائي السيبراني المحلي.

المبحث الأول : مظاهر التعاون الدولي في إطار الهجمات السيبرانية

لا جدوى لأي إتفاقية أو معاهدة أو أي مجهود يبذل في حال لم نكن أمام تعاون دولي وإقليمي جدّي من أجل التصدي للهجمات السيبرانية، فالكثير من البلدان النامية وإن أنضمت أو وقعت على أي إتفاقية دولية لا تستطيع مواجهة التهديدات السيبرانية بمفردها، بل يمكنها ذلك بمساعدة الدول والمنظمات الدولية والإقليمية، فالتعاون الدولي يمكن الدول الضعيفة تكنولوجياً من مواجهة اي تهديد يمكن أن يمس بها، والمساعدة التي نناقشها هنا هي المساعدة القضائية (الفرع الاول)، والمساعدة الشرطية (الفرع الثاني) .

الفرع الأول : التعاون القضائي الدولي

على أثر الإنتهاكات الكثيرة للقانون الدولي الانساني وبهدف توقيع العقاب على مرتكبيها، أصبح القضاء الدولي الجنائي الدائم يختص بملاحقة مرتكبي الجرائم الخطرة التي من شأنها أن تهدد السلم والأمن والاستقرار الدوليين للحؤول دون افلات هؤلاء من العقاب [١٧٩]، وبالفعل قامت الولايات المتحدة بتشكيل لجنة خاصة لوضع تصور لاعداد مشروع نظام أساسي لهذه المحكمة و فعلاًبفضل الجهود والمحاولات التي قامت بها هذه اللجنة أدت الى اقرار النظام الأساسي للمحكمة الجنائية الدولية عام ١٩٩٨ الى حين دخوله

[١٧٩] منى بو معزه : " دور القضاء الدولي لجنائي في تطبيق القانون الدولي الانساني "، جامعة باجي مختلر عنابة، كلية الحقوق، ٢٠٠٩، ص ٦٨

الى حيزّ التنفيذ عام ٢٠٠٢، فيتم التوازن بين ضرورة معاقبة الجرائم الأكثر خطورة والتي تشكل مخالفات فاضحة لقواعد القانون الدولي الانساني مع امكانية التعاون بين الأجهزة القضائية الدولية وبين الأجهزة الوطنية لتحقيق العدالة، يجب أن نشير الى نقطتين في هذا الإطار :

الأولى أن الدولة ملزمة بالحدود الاقليمية الموضوعة لها والتي تمارس سيادتها عليها فلا يمكنها أن تتعداها من أجل تطبيق الاجراءات اللازمة على المجرمين، فلا يمكنها مباشرة الإجراءات خارج نطاق حدودها، أما النقطة الثانية هي أن الاجراءات الجزائية تطبق ضمن حدود كل دولة وفي حال كان الهدف أن تطبق خارج هذه الحدود فيجب احترام مبدأ الاقليمية بين الدول لذلك نلجأ الى الأجهزة القضائية الدولية لحل هذه المعضلة من خلال التعاون بين السلطات القضائية، ومن هنا نعتبر أن الجرائم السيبرانية التي ترتكب في الفضاء السيبراني تتعدى اثارها حدود الدولة الواحدة واحياناً ترتكب من قبل عدة أشخاص كل منهم موجود في بلد معين.

فلا نستطيع أن نعالج هكذا نوع من النشاطات على الصعيد المحلي كون أن السلطات المحلية لا يمكنها أن تتجاوز حدود وظيفتها في تقديمهم للمحاكمة وتوقيع العقاب عليهم من تلقاء نفسها، مما يحتم ضرورة التعاون بين الدول المختصة في المعاينة وضبط الأقراص الصلبة التي توجد عليها معلومات معينة أو تفتيش الوحدات الظرفية في حال الإتصال عن بعد أو القبض على المشتبه بهم والتحقيق معهم وسماع الشهود أو اللجوء الى الانابة القضائية أو تقديم المعلومات التي يمكن أن تساهم في تحقيق بالجرائم , فكل ذلك لن يتحقق الاّ بمساعدة الدول الأخرى من أجل الإسراع في إجراءات الملاحقة وتوقيع العقاب [١٨٠].

من أبرز صور المساعدة القضائية هي الانابة (أو الاستنابة) القضائية و نعني بهذه الأخيرة :" طلب اتخاذ اجراء قضائي من بين اجراءات الدعوى الجزائية تتقدم به الدولة الطالبة الى الدولة المطلوب منها لضرورة الفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة و يتعذر عليها القيام به بنفسها " [١٨١].

فالغاية هي استفادة الدولة الطالبة من الامكانيات العامة للدولة المطلوب منها والتي لا تمتلكها وبعبارة أخرى أن الانابة القضائية وسيلة قانونية يتم اللجوء اليها من طرف القاضي من أجل اجراء تحقيق خارج دائرة اختصاصه لسماع الشهود أو الانتقال للمعاينة بسبب تعذره انتقاله أو بسبب تكلفة المصاريف وفق الأدلة الموجودة في الخارج [١٨٢].

اذاً هي انتداب جهة قضائية تنظر في الدعوى المرفوعة أمامها لجهة قضائية أخرى توجد في دائرة اختصاصها موطن الشاهد المراد سماعه أو الوثيقة المراد التحقيق فيها أو العقار المراد معاينته وتفويضها للقيام بالاجراء المطلوب وتحرير محضر بذلك وإرساله بعد سماعه، فهي عمل بمقتضاه تفوض المحكمة محكمة أخرى للقيام مكانها بعض اجراءات التحقيق أو الاجراءات القضائية الأخرى التي يقتضيها الفصل في الدعوى المرفوعة أمامها والتي تعذرعليها مباشرتها بسبب بعد المسافة [١٨٣] .

---

[١٨٠] جميل عبد الباقي الصغير : " الجوانب الاجرائية للجرائم المتعلقة بالانترنت "، ط٢٠٠١، دار النهضة العربية، مصر،ص ٧٩

[١٨١] شيخة حسين الزهراني، مرجع سابق، ص ١٩١

[١٨٢] كمال سمية : " الانابة القضائية " جامعة تسلمان – مجلة الدراسات القانونية والسياسية – العدد ٢، ٢٠٠٥، ص ١

[١٨٣] كمال سمية، مرجع سابق، ص ٢

أن القواعد والاجراءات أعلاه هي مثالية للجرائم التقليدية ولكن في مجال الجرائم المعلوماتية نرى وجود قصور واضحة على مستوى التعاون الدولي بالنسبة الى اجراءات التفتيش ونقل المعلومات وتبادلها بين الدول، وبهدف الحدّ من المشاكل السابق ذكرها اقر وزراء المجلس الأوروبي في ١١ سبتمبر ١٩٩٥ التوصية رقم ١٣/ ٩٥ المتعلقة بمشاكل الاجراءات الجنائية المرتبطة بتكنولوجيا المعلومات و التي حثت هذه التوصية الدول الأعضاء على مراجعة قوانين الاجراءات الجزائية على ضوء المبادئ التي وضعتها و هي [١٨٤]:

- تفتيش الأنظمة المعلوماتية و ضبط البيانات
- الرقابة الفنية و التقنية من أجل التحقيق الجنائي
- الالتزام بالتعاون مع السلطات التحقيق
- الجراءات و الوسائل الفنية التقنية لمعالجة الدليل الالكتروني

والمساعدة القضائية تشمل تبادل المعلومات بين الدول عبر تقديم كافة الوثائق والمعلومات بشأن مجرمون مثلاً أو أفراد مشتبه بهم متواجدين على اراضي الدولة المطلوب منها من أجل التأكد اذا كان لديهم سوابق جرمية أم لا، أحياناً يتم نقل الإجراءات بناءً على طلب يقدم من الدولة الى دولة أخرى ولمصلحتها مع ضرورة توافر شروط معينة كالتالي [١٨٥] :

١. أن يكون الجرم يشكل جريمة في قانون كل من الدولتين الطالبة والمطلوب منها

٢. يجوز لأي طرف متعاقد أن يطلب من اي طرف اخر أن يتخذ الإجراءات الجزائية في اي حالة من الحالات التالية :

- اذا كان الشخص المتهم خاضعاً أو ستخضع لحكم تقييد الحرية في الدولة الطالبة .
- اذا كانت الإجراءات المطلوب إتخاذها مقررة في قانون الدولة المطلوب اليها عن ذات الجرم .
- ان يكون الإجراء المطلوب اتخاذه يؤدي الى الوصول للحقيقة كأن تكون أدلة الجريمة الموجودة بالدولة المطلوب اليها .
- اذا كان تنفيذ الحكم في الدولة المطلوب اليها تحقق من اعادة تأهيل المجرم اجتماعياً .
- اذا كان حضور الشخص المتهم في الجلسة لا يمكن ضمان حضوره في الدولة الطالبة بينما يتحقق ضمان حضوره في الدولة المطلوب اليها .

---

[١٨٤] سليمان أحمد فاضل : " المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية "، طبعة ٢٠٠٧، دار النهضة العربية، ص ٤٢٤-٤٢٥

[١٨٥] غانم مرضي الشمري : " الجرائم المعلوماتية (ماهيتها – خصائصها _ كيفية التصدي لها قانوناً)" ،دار الثقافة – الأردن – ط ٢٠١٦، ص ٩٩-١٠٠

الاّ أن الانابة القضائية غالباً ما تواجه بالرفض وذلك في المجالات السياسية والعسكرية والضريبية أو في أحوال أخرى ترفضها الدول اذا كانت تمس بسيادة الدولة أو نظامها العام وبرأينا المشكلة الأهم التي تواجه الإنابة القضائية في جرائم الإنترنت أن هذه الأخيرة ترتكب بسرعة قياسية مما يحتم مواجهتها ضمن السرعة نفسها التي لا تتوافر في إجراءات التعاون القضائي التي تتصف بالشكليات الكثيرة والبطء.

لذلك فان مكافحة هكذا نوع من الجرائم وخاصة الهجمات السيبرانية لا تتم الاّ من خلال الترخيص لسلطات الدولة المطلوب اليها تقديم المساعدة عن طريق التفتيش في النظام المعلوماتي وأن تضبط فيه البيانات المراد إرسالها الى الدولة الطالبة مع مراعاة القواعد المعمول بها في تبادل المعلوماتية كي لا تشكل فرصة للمتهم بالتشكيك في الإجراءات [١٨٦].

ايضاً من صور المساعدة القضائية تسليم المجرمين للعدالة :

نعني بهذا المفهوم أنه " إجراء تعاون دولي تقوم بمقتضاه دولة تسمى بالدولة المطلوب اليها بتسليم شخص يوجد في إقليمها الى دولة أخرى تسمى بالدولة الطالبة بهدف ملاحقته عن جريمة إتهم بإرتكابها أو لأجل

تنفيذ حكم جنائي صدر ضده " [١٨٧]، فالهدف الأسمى في هكذا نوع من التعاون هو منع إفلات المجرم من العقاب وذلك في حال وجوده على اراضي دولة لا تسمح قوانينها بمحاكمته فيرتكب الجريمة ويحتمي على أراضيها بهدف عدم ملاحقته ومعاقبته أو بحالة أخرى هو صدورحكم قضائي بالادانة ولكن لم ينفذ بعد نتيجة فراره الى دولة أخرى، ففي هاتين الحالتين يكون نظام تسليم المتهمين هو الحل على ان تتم هذه الإجراءات وفق شكليات معينة تقوم بها الدولة طالبة التسليم وتلك المطلوب منها مع ضرورة توافر الشروط الأساسية في هذا المجال على الشكل التالي :

١. إزدواجية الجرم :

نعني بهذا التعبير أن يكون الفعل معاقب عليه في كلا الدولتين الطالبة والمطلوب منها التسليم والسبب في ذلك أنه من غير المنطقي أن تطلب دولة من دولة أخرى أن تقيم دعوى جزائية أم ملاحقة جنائية ضد فعل ارتكبه شخص موجود على أراضيها وهو في الأصل غير مجرم في قانونها، هذا ما أكدته معاهدة الأمم المتحدة النموذجية بشأن تسليم المجرمين لعام ١٩٩٠ في الفقرة الأولى من المادة الثانية على أنه : " الجرائم الجائز التسليم بشأنها هي لأغراض هذه المعاهدة : جرائم يعاقب عليها قانون كلا الطرفين بالسجن أو شكل آخر من الحرمان من الحرية لمدة لا تقل عن سنة واحدة أو سنتين او بعقوبة اشد " [١٨٨] .

٢. الشروط الخاصة بالشخص المطلوب تسليمه :

- لا يجوز الشخص المطلوب تسليمه أن يكون من رعايا الدولة المطلوب منها هذا الأمر .

- لا يجوز تسليم من تم منحه حق اللجوء السياسي .

---

[١٨٦] سلمان احمد فاضل، مرجع سابق، ص ٤٢٧

[١٨٧] سليمان عبد المنعم سليمان : " الجوانب الاشكالية في النظام القانوني لتسليم المجرمين "، طبعة ٢٠١٥، دار المطبوعات الجامعية، الاسكندرية، مصر ص ٣٢-٣٣

[١٨٨] المعاهدة الأمم المتحدة النموذجية بشأن تسليم المجرمين لعام ١٩٩٠، متوفرة على الرابط التالي : https://www.un.org/arabic/documents/instruments/docs_subj_ar.asp?sub=33

- في حال قد تمت محاكمة الشخص عن الجريمة المطلوب تسليمه بشأنها و قد برأ منها او كان قيد التحقيق أو المحاكمة .

٣. الشروط الخاصة بالجريمة موضوع التسليم :

- ان تكون الجريمة موضوع التسليم مدرجة ضمن القائمة التي تحدد الجرائم المتفق عليهم حصراً بين الدولتين من خلال إتفاقية معقودة بينهم .

- أن يتم تحديد في النظام الداخلي للدول أو في الاتفاقيات أو المعاهدات الثنائية أو المتعددة الأطراف الحد الأدنى للعقوبة المقررة للجرائم التي يمكن أن يتم التسليم لأجلها ومدى جسامة الجريمة [١٨٩] .

<u>علي الصعيد السيبراني :</u>

نواجه معوقات كثيرة في هذا المجال لناحية تسليم المجرمين على الشكل التالي :

- تحديد هوية الشخص مرتكب الفعل السيبراني :

ان تحديد هوية الشخص بالشكل الدقيق أمر صعب في الهجمات السيبرانية كونها تنفذ عن بعد ومن قبل مجرم ذكي يستطيع اخفاء هويته بسهولة .

- اعتبار الهجمات السيبرانية من الجرائم العابرة للحدود :

يستطيع الفاعل أن يرتكب عدة جرائم في بلدان مختلفة ويفر الى دولة أخرى أو أن يرتكب فعل جرمي في بلد معين تتعدى آثاره السلبية أكثر من دولة، فالعمل السيبراني لم يعد مقتصراً على دولة معينة بل أصبحت تختص به اكثر من دولة ووفق نظام تسليم المجرمين أصبح بإمكان الدولة التي وجد المجرم على أراضيها أن تلقي القبض عليه بعد التأكد من هويته وأن تكون فعالة في هذا النطاق عبر البحث عن المتهم الحقيقي وتتحرى عنه في حالة الشك وعن مكان تواجده وإدانته طبقاً لقانونها الداخلي إنطلاقاً من الإتفاقيات المعقودة، فضلاً عن تطبيق قاعدة " التسليم أو المحاكمة "، فالدولة التي تمتنع عن تسليم المتهم وجب عليها القيام بكافة الإجراءات الجزائية اللازمة مع محاكمته لذلك نعتبر أن نظام تسليم المجرمين هو من أهم الأطر الأساسية في مجال الحد من الجرائم السيبرانية ومكافحتها كي لا يظن المجرم أن الإنتقال من دولة الى أخرى هو الحل الأنسب للإفلات من العقاب .

لقد إنتهينا من توضيح سبل التعاون القضائي بين الدول من أجل مواجهة الهجمات السيبرانية، سوف ننتقل الى الفرع الثاني من هذا المبحث من أجل تحديد أوجه التعاون الشرطي بين الدول .

---

[١٨٩] غانم مرضي الشمري، مرجع سابق، ص ١٠٩

الفرع الثاني : التعاون الشرّطي الدولي

من أهم مظاهر التعاون الشرطي الدولي هو جهاز الأنتربول لمكافحة الجرائم الخطرة ولجعل العالم أكثر أماناً فهي المنظمة الوحيدة المتخصصة في مكافحة الجرائم الدولية ومطاردة المجرمين الدوليين ومن أهدافها إقامة وتنمية النظم التي من شأنها أن تساهم على نحو فعال في منع جرائم القانون العام ومكافحتها وتأكيد المعونة المتبادلة وتشجيعها على أوسع نطاق بين سلطات الشرطة الجنائية في حدود القوانين القائمة في البلاد المختلفة و بروح الإعلان العالمي لحقوق الانسان [١٩٠]، وتعزيز التعاون الشرطي بينه وبين أجهزة الشرطة التابعة الدول الأعضاء عبر ربط شبكات الإتصال والمعلومات وتبادل المعلومات والبيانات والقدرات لملاحقةالمجرمين وإنزال العقاب بهم وبما أن الغتصالات الشرطية تحتاج الى اتصالات خاصة تحقق لها السرعة المطلوبة لذا حاولت المنظمة و العديد من الدول الى تطوير نظم الإتصال حتى يتم الوصول وتعقب المجرمين بمجرد خروجهم من الدولة التي إرتكبت فيها الجريمة[١٩١].

نلخص مظاهر التعاون الشرطي على الشكل التالي[١٩٢] :

- توحيد إجراءات التسليم بين الدول

- تجميع البيانات وتبادل المعلومات

- تسيير خدمات التحقيق لضبط وملاحقة المجرمين الهاربين وتسليمهم الى الدولة التي تطلب تسليمهم .

- انشاء وتطوير النظم القادرة بفعالية في الوقاية والعقاب .

- تقديم الخبرات والدورات الفنية لأجهزة الشرطة التابعة للدول بهدف تطوير قدراتها عبر الاستعانة بخبراء دوليين و مختصين .

- تزويد شرطة الدول الأطراف بكتيبات ارشادية حول جرائم الانترنت و كيفية التعامل معها و التحقيق فيها .

- دور المكاتب المركزية الوطنية التابعة للشرطة الدولية الموجودة ضمن أراضي الدول الأطراف من أجل مساعدة الشرطة المحلية على تجميع البيانات المتعلقة بالجرم والمجرم .

سوف نوضح كل إجراء مذكور أعلاه :

١. لناحية توحيد إجراءات التسليم بين الدول : من المتعارف عليه أن إجراءات تسليم المتهمين تختلف بين الدول وكل دولة تضع الشروط والقيود التي تراها مناسبة من أجل تسليمها لمتهمين وجدوا على أراضيها وإن إختلاف شروط التسليم بين الدول يؤدي في معظم الأحيان الى عدم معاقبة الفاعل مما يدفعنا اى الإعتبار أن توحيد شروط تسليم المتهمين بين الدول من أهم مظاهر التعاون الشرطي الذي يؤدي الى تحقيق العدالة في نهاية المطاف .

---

[١٩٠] https://arab-ency.com.sy/ency/details/6575/19

[١٩١] سليمان أحمد فضل، مرجع سابق، ص ٤١٤ ، أنظر أيضاً شيخة حسين الزهراني، مرجع سابق، ص ١٨٠

[١٩٢] سليمان أحمد فضل، مرجع سابق، ص ٤١٤، أنظر أيضاً شيخة حسين الزهراني، مرجع سابق، ص ١٨١-١٨٢

٢. تجميع البيانات وتبادل المعلومات : أحياناً تمتلك دولة وقع الجرم على أراضيها لمعلومات مهمة تساعد الجهاز القضائي في دولةٍ أخرى الكشف عن تفاصيل متعلقة بالدعوى (في حال تواجد الفاعل على أراضيها)، مما يعتبر إجراء تبادل المعلومات بين الدول أمرٌ ضروريٌ في التوصل الى الحقيقة .

٣. تسيير خدمات التحقيق لضبط وملاحقة المجرمين الهاربين وتسليمهم الى الدولة التي تطلب تسليمهم : أن مساعدة الدول لبعضها البعض في ملاحقة المجرمين الفارين أمرٌ أساسيٌ في إنزال العقاب بالمجرم .

٤. انشاء وتطوير النظم القادرة بفعالية في الوقاية والعقاب : عن طريق تعديل القوانين التقليدية كي تتماشى مع الجرائم المستحدثة .

٥.خضوع رجال الشرطة لدورات تدريبية بهدف تطوير قدراتهم الفنية أمرٌ مهمٌ في منع إفلات المجرم من العقاب .

من أجل احترام السيادة الوطنية للدول فان أجهزة الانتربول لا تلقي من تلقاء نفسها على المجرم لأن هذا الأمر منوط بالسلطات المحلية، فهي تساعد هذه الأخيرة ولا تأخذ مكانها، وقيام عمليات شرطية دولية مشتركة بين أجهزة أكثر من دولة في تعقب المجرمين اللذين يفرون من بلد الى أخر .

هذا في اطار الجرائم عامةً أما في اطار الهجمات السيبرانية، فمظاهر التعاون الشرطي مختلقاً نوعاً ما و هذا ما سوف نوضحه (الولايات المتحدة الأمريكية نموذجاً).

لا شك أن منظمة الأنتربول تهدف الى ملاحقة المجرمون بغض النظر عن نوع الجريمة المرتكبة وضمنها مرتكبوا الهجمات السيبرانية ايضاً ومن أجل تطوير مظاهر التعاون الشرطي في مجال مكافحة هذه الهجمات و أهمها : شرطة الويب الدولية أو ما يسمى بال web Police التي أنشأت عام ١٩٨٦ في الولايات المتحدة الأميريكية التي تهدف الى ملاحقة المجرمين و تلقي الشكاوى من الأفراد وتضم أكثر من منظمة للحدّ من الهجمات السيبرانية، أيضاً نذكر الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة ٢٠١٠ التي نصت في المادة ٣٢ منها على ما يلي :

"على جميع دول الأطراف تبادل المساعدة فيما بينها بأقصى مدى ممكن لغايات التحقيق أو لجمع الادلة الإلكترونية في الجرائم.

يتم تقديم طلب المساعدة الثنائية والإتصالات المتعلقة بها بشكل خطي ويجوز لكل دولة طرف في الحالات الطارئة أن تقدم هذا الطلب بشكل عاجل بما في ذلك الفاكس أو البريد الإلكتروني.."

كذلك نصت المادة ٣٧ من هذه الإتفاقية :" لأي دولة طرف أن تطلب من دولة أخرى طرف الحصول على الحفظ العاجل للمعلومات المخزنة على تقنية المعلومات التي تقع ضمن إقليمها بخصوص ما تود الدولة الطرف الطالبة للمساعدة المتبادلة للبحث وضبط وتأمين وكشف المعلومات.

وأيضاً نذكر الجهات التالية :

1. CyberDivisions FBI[193] :

[١٩٣] https://fbi.gov/investigate/cyber

يهدف هذا الجهاز ضمن ال FBI الى الحدّ من الأفعال غير المشروعة التي ترتكب على الانترنت وخاصةً الهجمات السيبرانية التي تهدد أمن الدولة الأميريكية واقتصادها والتقصي عن المجرمون والتحقيق مع المشتبه بهم في ارتكاب الجرائم الالكترونية، من أهدافها ايضاً هي تغيير تفكير كل مجرم يظن أنه يستطيع ارتكاب جرائم سيبرانية أم توجيه هجمات الكترونية ضمن الأراضي الأميركية و لكن كيف يعمل هذا الجهاز؟

بفضل المعرفة و التطور العلمي و التكنولوجي أصبح بإمكان هذا الجهاز الذي يمتلك الوسائل المتطورة التي من شأنها الكشف عن هوية المجرم المعني ببرامج خبيثة أو فيروسات أو اي نشاط آخر يريد من خلاله توجيه هجمات سيبرانية داخل الدولة أم خارجها وبالتعاون مع منظمات دولية وأجهزة الدول الأخرى وكل ذلك بفضل وجود ٥٦ مكتب ضمن اراضي الولايات المتحدة مهمتهم الاستجابة لأي خطر سيبراني ووضع حد له و ذلك بفضل السرعة التي تمتلكها هذه الأجهزة في التخلص من المشكلة بغضون ساعات قليلة و بالتنسق مع أجهزة دولية اساسية وهذا ما يعزز التعاون الشرطي بين الدول التي تجتمع على هدف واحد وهو تحقيق الأمن والسلم الدوليين.

أيضاً تمتلك ما يسمى IC3 (Internet Crime Complain Center) الذي يهدف الى تلقي الشكاوى والتقارير من العامة بشأن أعمال غير مشروعة والإستجابة الى هذه الشكاوى بسرعة قصوى من أجل حماية الضحية وأموالها من أي خطر محدق يمكن أن تتعرض له ما يهمنا في هذا النطاق أن هذه الأجهزة تنجح في التحكم بالهجمات السيبرانية بفضل التطور التي تمتلكه.

هذا الجهاز يتضمن أيضاً ما يسمى ب CyWatch 24/7 وهو الخط الساخن على مدار الأسبوع و طوال اليوم و الذي يستطيع من خلاله تتبع الحوادث السيبرانية التي من الممكن أن تحصل خارج الدولة أم داخلها ومعالجتها بالشكل الوافي والدقيق مع وجود فريق عمل من المختصين اللذين يستطيعون الكشف عن أي محاولة توجيه الهجوم السيبراني لأي جهة كانت وتحديد مكان المجرم وهويته وتلقي القبض عليه ومحاولة توجيه الهجوم قدر الامكان و هذه هي الخبرات التي نرغب تطبيقها في عالمنا الحالي ومشاركتها مع الدول النامية التي لا تمتلك هذه الخبرات، فتسعى هذه الدولة دائماً الى توفير المساعدة التقنية لرفع قدرات العدالة الجزائية لدى حكومات الدول الأخرى ومساعدة أجهزة الشرطة فيها ومسوؤلي الادعاء العام والقضاة كي يصبحوا أكثر فعالية في مكافحة الهجمات السيبرانية.

بالإضافة الى أهمية البرنامج الدولي للمساعدة والتدريب على التحقيق الجزائي (ICITAP) الذي يعمل على توفير مساعدات لأجهزة الشرطة في البلدان النامية في مختلف انحاء العالم و تهدف المساعدة التي يقدمها البرنامج الى تعزيز القدرات التحقيقية لدى أجهزة الشرطة في البلدان الناشئة [١٩٤].

٢. المركز الدولي لمنع الجريمة ICPC (The International Center for the Prevention Of Crime)[١٩٥] :

يهدف هذا المركز الى تنفيذ وتطوير سياسات علمية وفعالة في منع الجريمة عبر برامج ومشاريع مصممة خصيصاً للحدّ من الجريمة والإنحراف في المجتمعات والمدن والوحدات الجغرافية الأخرى وتعزيز الشعور

[١٩٤] شيخة حسين الزهراني، مرجع سابق، ص ٢٢٦

[١٩٥] الموقع الرسمي للمركز الدولي لمنع الجريمة : https://cipc-icpc.org

بالأمان بشكل أكثر تحديداً تعمل على النهج الذي يرمي الى دعم التعاون بين مختلف الجهات من أجل منع الجريمة وخاصةً تلك المستحدثة .

يضم هذا المركز عدد لا يستهان به من المختصين والمسؤولين وأصحاب الإختصاص اللذين يعملون في مجالات عديدة وخاصةً تلك المتعلقة بالوقاية عبر وضع ضوابط قانونية وعملية خاصةً لكل نوع جرمي وضمن أهداف هذا المركز السعي الى حماية الضحية وتوفير الوقاية والحماية من أي خطر محدق يمكن أن يمس بها، كما أنه يعزز هذه القدرات بمشاركتها مع الدول البحاجة لها والتي تفتقدها لمساعدتها على في مواجهة الهجمات السيبرانية التي تستغل ضعف قدراتها في مواجهتها .

على الصعيد الأوروبي :

- جهاز اليوروبول :

يجمع هذا الجهاز ٢٧ دولة أوروبية، ومن أجل الحد من الهجمات السيبرانية أنشأ قناة معلومات بينه وبين هذه الدول، وفي العام ٢٠١٣ تم إنشاء المركز الأوروبي لمكافحة الجرائم الإلكترونية (EC3) لتسهيل التعاون العملي بين خدمات إنفاذ القانون والمجتمع والقطاع الخاص وفي العام ٢٠١٩ قام هذا الجهاز بتعيدل إستراتجيته ٢٠٢٠+ من أجل إستعابها عدد أكبر من الأفعال المتمثلة بهجمات سيبرانية، كما أن هذا الجهاز أتاح لسلطات الشرطة من العمل مع الأجهزة الأخرى الاجنبية بشكل مباشر من أجل توفير تبادل للمعلومات بشكل أسرع وأسهل وخاصةً في مجال التحري عن المجرمين الذين يشتبه بتورطهم بهجمات سيبرانية على الأراضي الفرنسية.

نذكر أيضاً أنه عام ٢٠٢٠ ارسلت وحدة الجرائم الإلكترونية في في الأنتربول رسالة تحذيرية الى أكثر من ١٩٤ دولة من أجل تنبيهها من وقوع هجوم سيبراني محتمل مرتبط بالترويج غير القانوني للقاحات كوفيد-١٩ عن طريق سيطرة بعض المهاجمين على مواقع طبية توفر هذا اللقاح بشكلٍ غير شرعي .

نشير أيضاً تم إنشاء جهاز الأنتربول للإبتكار CMII عام ٢٠١٥ في سنغافورة من أجل تحسين القدرات الفنية لخدمات التحقيق وتطوير القدرات عبر الوطنية .

التعاون الدولي في مجال التدريب على الحد من الهجمات السيبرانية :

من أجل مواجهة الجرائم السيبرانية لا بدّ من وجود تعاون وتنسيق دوليين ليس فقط في مجال المساعدات القضائية وتسليم المجرمين وإنما ايضاً في مجال تدريب ومساعدة رجال شرطة الدول النامية، وهذا ما اكدته الاتفاقيات الدولية التي دعت الى ضرورة وجود تعاون بين الدول في مجال التدريب و نقل الخبرات فيما بينها و خاصةً الجريمة المنظمة عبر الوطنية لسنة ٢٠٠٠ , وكذلك الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود و ايضاً اتفاقية عمان للتعاون العلمي بين المعاهد القضائية العربية من أجل توفير التدريب والتأهيل لأعضاء الهيئات القضائية العربية عام ١٩٩٧، نذكر ايضاً المؤتمر الدولي الأول لقانون الانترنت الذي عقد في مصر عام ٢٠٠٥ الذي دعى الى ضرورة التعاون بين الدول لمواجهة المستجدات الحديثة من أجل تبادل الخبرات و طرح المواضيع و المشاكل التي تعترض التعاون المشترك و الموضوعات الحيوية .

لا بد من القاء الضوء على مجموعة من الصعوبات التي تعترض هذا التعاون عامةً و تتلخص بتنوع النظم الاجرائية التي لا تسمح في بعض الدول على القيام بتطبيق مع تعلمه الأفراد اللذين خضعوا للتدريب بشكل عملي في اجراءات التحقيق والمحاكمة بسبب عدم مواكبة القضاء لهذه التطورات وخاصةً في حال كانت

السلطات القضائية لدى الدولة ترفض الأخذ بأي دليل خلافاً لما تقرره قوانينها وان كان الدليل الذي تم الحصول عليه من مرجع قضائي وبشكل مشروع.

أيضاً غياب قنوات اتصال بين الدول للحصول على المعلومات والبيانات الخاصة بالجريمة وهذا يعني عدم القدرة على جمع الادلة والوصول للحقيقة و أخيراً التجريم المزدوج و أهميته في تسليم المجرمين يعتبر عقبة في الوصول الى الحقيقة قي الجرائم السيبرانية و ذلك لأن معظم الدول لا تجرم هذه الأفعال مما يعيق تنفيذ البنود الخاصة بالاتفاقيات الدولية .

سوف تنتقل الى التطرق الى أبرز الاتفاقيات الدولية في مجال الجرائم السيبرانية عامةً والهجمات السيبرانية خاصةً في المبحث الثاني التي تسعى الى وضع حدّ لهذه الافة الخطيرة.

المبحث الثاني : الجهود الدولية الإستثنائية في حماية الفضاء السيبراني

ان تزايد مخاطر الهجمات السيبرانية والنتائج السلبية الخطيرة التي تحققها إستيقظت الدول حول الواقع الأليم والخطير الذي يهددها، كثيرةُ هي الجهود الدولية التي تسعت مراراً وتكراراً لتنظيم الهجمات السيبرانية ووضع حدّ لها الاّ أننا لا نزال نواجه ضعف قانوني في هذا المجال، مما دفع بالأجهزة الدولية والإقليمية الى محاولة تنظيم هذه المسألة قدر المستطاع من أجل وضع حدّ شبه نهائي لها وهذا ما سوف نبينه في هذا المبحث، في الفرع الأول منه سوف نبين أبرز الإتفاقيات والمعاهدات الدولية وفي الفرع الثاني سوف نعالج دور المنظمات الحكومية وغير الحكومية .

الفرع الأول : الإتفاقيات والمعاهدات الدولية

سعت بعض الجهات الدولية والاقليمية الى محاولة وضع خارطة تنظيم للهجمات السيبرانية لعلها تساهم في نوعاً ما في السيطرة على هذا التهديد المتنامي وعلى هذا الأساس فان التعاون الدولي هو الحل من خلال وجود معاهدات واتفاقيات مهمة تحاول أقصى جهدها في الحدّ من المخاطر التي تهدد الأمن الدولي والسلام العالمي وأهمها إتفاقية " بودابست" لمكافحة جرائم الانترنت لعام ٢٠٠١ وأيضاً الجهود التي تبذلها الأمم المتحدة بكافة أجهزتها والمحاولات الاقليمية، انطلاقاً من ما تقدم سوف نبين تباعاً أبرز الجهود الدولية والاقليمية في اطار الحدّ من الهجمات السيبرانية.

* دور الأمم المتحدة :

تحاول الأمم المتحدة بكافة أجهزتها ,و ادواتها الى تأمين سلامة الفضاء السيبرانية و حمايته من النشاطات السيبرانية التي تعرضه لمخاطر جسيمة، من خلال الجمعية العامة ومجلس الأمن ومكتب مكافحة الارهاب التابع للأمم المتحدة في مختلف المفاوضات لايجاد توافق في الاراء من أجل وضع معايير توفر الحماية لشبكات الإنترنت.

القرارات الصادرة عن الجمعية العامة للأمم المتحدة تلخص على الشكل التالي[١٩٦] :

- القرار رقم ٥٧/٢٣٩ لعام ٢٠٠٢ المتعلق بإرساء ثقافة عالمية للأمن الفضاء السيبراني وحماية الهياكل ألأساسية الحيوية للمعلومات .

- القرارين رقم ٥٥/٦٣ و ٥٦/١٢١ اللذين يضعان الاطار القانوني بشأن مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية.

- القرار رقم ١٧٣/١٨٧ المتعلق بمكافحة استخدام تكنولوجيا المعلومات والإتصالات لأغراض جرمية .

- القرار رقم ١٧٣/٧٤ المتعلق بتعزيز المساعدة التقنية وبناء القدرات لتدعيم التدابير الوطنية والتعاون الدولي في مجال مكافحة الجريمة السيبرانية بما يسمح بتبادل العلومات .

- القرار ١٢١/٤٥ العام ١٩٩٠، وكذلك نشر دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها في العام١٩٩٤ .

- القرار239/ ٥٧ المتعلق بإنشاء ثقافة أمنية عالمية للفضاء الحاسوبي .

- القرار رقم ٥٨/ ١٩٩ بشأن انشاء ثقافة عالمية للأمن السيبراني .

- قرار لجنة مكافحة المخدرات ٥/٤٨ حول تقرير التعاون الدولي .

- القرار رقم ٧٢/٨٤ المختص بالإستراتجية العالمية لمكافحة الارهاب .

- القرارت الصادرة عن مجلس الأمن لعام ٢٠١٧ من أجل الحدّ من الهجمات الإرهابية على الهياكل المهمة التابعة للدول وحمايتها والحدّ من أخطارها وذلك عن طريق تبادل المعلومات والخبرات بين القطاعات العامة و الخاصة عبر التدريب المشترك و ذلك بهدف تأمين الفضاء السيبراني [١٩٧].

- التوصيات والمبادئ التوجيهية للهيئة الدولية لمراقبة المحددات (INCB) التي نشرت العام ٢٠٠٥ توصيات للحد من إنتشار المبيعات غير المشرّعة [١٩٨].

- المؤتمر الثالث عشر للأمم المتحدة لمنع الجريمة والعدالة الجنائية عام ٢٠١٥ في دولة قطر .

- المؤتمر الثاني عشر للأمم المتحدة لعام ٢٠١٠ الذي عقد في البرازيل

- مكتب الامم المتحدة لمكافحة الارهاب :

---

[١٩٦] نور أمين موصلي، مرجع سابق، ص ٢٢

[197] Sc.RES.2341.UN.Docs.NO/S/RES/2341(2017) , Available at : https://un.docs.org/ar/S/RES

[١٩٨] خلف فاروق : " الاليات القانونية لمكافحة الجريمة المعلوماتية "، مجلة الحقوق والحريات، العدد ٢، عام ٢٠١٥، ص ٥-٦

يسعى هذا المكتب الى تعزيز قدرات الدول في مواجهة الإرهاب الالكتروني ومنع إتاحة الفرص للإرهابيين في استخدام التطورات التكنولوجية للسيطرة على البنى التحتية الحيوية والسعي الى كشف هويتهم ومعاقبتهم كي لا تكون وسائل التواصل الاجتماعي سبب ايجابي في تنامي قدراتهم الارهابية، فالتقنيات الحديثة لا بدّ أن تكون سبب إصلاح النظم القديمة القائمة و ليس تنامي الاثار السلبية التي من الممكن أن تنشأ عنها .

* إتفاقية بودابست لمكافحة جرائم الإنترنت :

تعتبر هذه المعاهدة من أولى المعاهدات التي سعت الى مكافحة جرائم الانترنت عبر وضع أسس وأطر قانونية تنظيمية لها والتي تمت في بودابست عاصمة المجر في ٢٠٠١/١١/٢٣، وقعت على هذه الاتفاقية ٢٦ دولة اوروبية إضافة الى الولايات المتحدة الأمريكية وكندا واليابان وجنوب أفريقيا، التي شكلت خطوة جيدة في مجال التعاون الدولي ضدّ الجرائم التي ترتكب على الانترنت ولكن بالطبع هي غير كافية وتعرف هذه الاتفاقية بأنها : أول معاهدة دولية تسعى لمعالجة جرائم الكمبيوتر (الجرائم الالكترونية) من خلال مواءمة القوانين الوطنية وتحسين تقنيات التحقيق وزيادة التعاون بين الدول [١٩٩] وهي تتضمن ٤٨ مادة على أربعة فصول كالتالي[٢٠٠]:

- الفصل الأول : تعريفات خاصة بعض التعريفات الفنية .

- الفصل الثاني : يتضمن الإجراءات اللازم إتخاذها على المستوى المحلي لكل دولة وتتضمن قسمين :

القسم الأول الذي يتعلق بالنصوص الجنائية الموضوعية المختصة بالجرائم ضد الخصوصية وسلامة و تواجد معلومات الحاسب وشمل وصفاً لأنواع متعددة من الجرائم والجرائم المتصلة بالحاسب شاملة استخدام الكمبيوتر في التزوير والأفعال الاحتيالية، يتضمن ايضاً هذا القسم الجرائم المتعلقة بالمحتوى والمضمون والجرائم المتصلة بالتعدي على حقوق المؤلف .

أما القسم الثاني يختص بالقانون الاجرائي فيما يتصل بالاجراءات الجنائية شاملة الحفاظ على المعلومات المخزنة و الأوامر الخاصة بتسليم الأدلة و يتضمن كذلك تفتيش و ضبط بيانات الحاسب المخزنة .

الفصل الثالث : متعلق بمسائل التعاون الدولي و تسليم الجناه والمساندة المشتركة و التعاون في التحريات و جميع بيانات المرور و الحركة الخاصة بالبيانات .

الفصل الرابع : يتعلق بالانضمام و الانسحاب من تعديل المعاهدة و فض النزاعات و التشاور بين الأعضاء .

ولكن كيف يمكننا تطبيق قواعد هذه الإتفاقية على موضوع الهجمات السيبرانية ؟

من أجل الإجابة على هذا السؤال،سوف نقسم هذا الموضوع الى قسمان :

١. التدابير التشريعية الموضوعية

٢. التدابير التشريعية الإجرائية

---

[199] Budapest Convention on Cybercrime , available on : https://ar.wiki5.ru/wiki/convention_on_cybercrime

[٢٠٠] هلالي عبدالله أحمد : " الجوانب الموضوعية والإجرائية للجرائم المعلوماتية – على ضوء اتفاقية بودابست ٢٠٠١" ط٢٠٠١، دار النهضة العربية العربية، مصر، ص ٣٠

في التدابير التشريعية الموضوعية : تحتوي هذه الإتفاقية على بنود ومواد تضم الجرائم التي ترتكب بواسطة الإنترنت : كالجرائم التي تتعرض لخصوصية وسلامة البيانات مثل النفاذ الشرعي والإعتراض غير الشرعي وتشويه البيانات وسلامة النظام ،فضلاً عن تنظيم ومراقبة إستخدام البيانات الشخصية المنزلة في المجال الإلكتروني المعلوماتي، والإعتراض غير القانوني للبيانات الشخصية والمتداولة بين الحواسيب في التوصية رقم ٠٤/٩٠ .

المادة الثانية من هذه الإتفاقية نصت على ما يلي :

" تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق: النفاذ الكامل أو الجزئي إلى نظام كومبيوتر. يجوز لطرف أن يستلزم أن تُرتكب الجريمة عن طريق مخالفة التدابير الأمنية، بنِية الحصول على بيانات الكومبيوتر أو بأي نية غير صادقة أخرى، أو في ارتباط بنظام كومبيوتر متصل بنظام حاسوبي آخر " ، أي أن أي دخول الى غير قانوني ومتعمد الى نظام الكمبيوتر أو جزء منه دون أي حق ولأي سببٍ كان بعرض مرتكبها الى المسائلة القانونية .

المادة الثالثة :

" تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق الاعتراض باستخدام وسائل فنية، للإرسال غير العمومي لبيانات الكومبيوتر إلى أو من أو داخل نظام كومبيوتر، بما في ذلك الانبعاثات الكهرومغناطيسية الصادرة عن نظام كومبيوتر يحمل هذه البيانات.." .

المادة الرابعة التي تعطي لحق في محاسبة من يتعرض للبيانات :

" تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً: إتلاف بيانات حاسوبية، حذفها، إفسادها، تعديلها أو تدميرها. .٢ يجوز لدولة طرف أن تحتفظ بحقها في أن تستلزم أن تتسبب الأفعال المشار إليها في الفقرة ١ في ضرر جسيم" .

المادة الخامسة :

بالنسبة الى التدخل المتعمد في الأنظمة في: " تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق: الإعاقة الخطيرة لاشتغال نظام الكومبيوتر عن طريق إدخال بيانات حاسوبية، إرسالها، إتلافها، حذفها، إفسادها، تغييرها أو تدميرها".

وأخيراً *المادة السادسة* التي حرمّت إساءة إستخدام الأجهزة على الشكل التالي :

: " تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا إرتكبت عمداً ودون أي وجه حق:

.١عملية إنتاج، بيع، شراء بغرض الاستخدام، إستيراد، توزيع أو إتاحة بأي طريقة أخرى :

-جهاز، بما في ذلك برنامج كومبيوتر، تم تصميمه أو ملاءمته مبدئيا، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من ٢ إلى ٥؛

- كلمة سر خاصة بكومبيوتر، أو رمز الولوج، أو بيانات مماثلة يمكن بواسطتها النفاذ بشكل كامل أو جزئي إلى نظام كومبيوتر، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من ٢ إلى ٥؛

- حيازة إحدى المواد المشار إليها في الفقرة أ (١) أو (٢) أعلاه، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من ٢ إلى ٥.

كذلك التزوير المتعمد باستخدام جياز الكمبيوتر (المادة ٧) و الإحتيال المتعمد باستخدام الكمبيوتر(المادة ٨) والجرائم المرتبطة بحق المؤلف، فجميع هذه الجرائم المذكورة أعلاه يمكن أن تكون كأدوات يستخدمها المهاجم في هجومه السيبراني، مما يحتم تطبيقها على بحثنا هذا .

٢. التدابير التشريعية الإجرائية :

تعطى الحق للدولة في ملاحقة الجرائم المنصوص عنها في مواد هذه الإتفاقية و مرتكبها وهذا ما أكدته المادة ١١ :

" ١.تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً: المساعدة أو التحريض على ارتكاب أي من الجرائم المنصوص عليها في المواد من ٢ إلى ١٠ من هذه الاتفاقية، وذلك بنِية ارتكاب جريمة من هذا القبيل

٢.تمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً: محاولة ارتكاب أي جريمة من الجرائم المنصوص عليها في المواد من ٣ إلى ٥، ٧، ٨ و٩ (أ) و(ج) من هذه الاتفاقية.

٣. يجوز لكل دولة طرف الاحتفاظ بالحق في عدم تطبيق الفقرة ٢ من هذه المادة كلياً أو جزئياً " .

وكذلك المادة ١٣ التي أعطت الحق للدولة في فرض العقوبات المناسبة :

"١. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير للتأكد من أن الجرائم المنصوص عليها في المواد من ٢ إلى ١١ مُعاقب عليها بعقوبات فعالة، متناسبة ورادعة، بما في ذلك العقوبات السالبة للحرية.

٢. تضمن كل دولة طرف مساءلة الأشخاص الإعتباريين وفقا للمادة ١٢ وإخضاعهم لعقوبات أو تدابير فعالة، متناسبة ورادعة، سواء كانت عقوبات أو تدابير جنائية أو غير جنائية، بما في ذلك العقوبات المالي."

نضيف أن للدولة الحق في إتخاذ تدابير تشريعية مناسبة في لإقرار السلطات والإجراءات المنصوص عليها في هذا القسم لأغراض التحقيقات والدعاوى الجنائية المحددة (المادة ١٤) ،والدور الأهم التي تقوم به هو التعجيل في حفظ البيانات المخزنة :

" ١.إتخاذ تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة من الأمر أو الحصول على الحفظ المعجل لبيانات كومبيوتر محددة، بما في ذلك بيانات الحركة المُخزنة بواسطة نظام الكومبيوتر، خاصة في حال وجود أسس للاعتقاد أن تلك البيانات معرضة بشكل خاص للضياع أو التعديل.

٢. في حال تفعيل دولة طرف للفقرة ١ أعلاه عبر توجيه أمر إلى شخص من أجل حفظ بيانات كومبيوتر محددة ومخزنة توجد بحوزته أو تحت سيطرته، تعتمد الدولة الطرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإلزام ذلك الشخص بحفظ بيانات الكومبيوتر المعنية والإبقاء على سلامتها لأطول مدة زمنية ضرورية على ألا تتجاوز تسعين يوماً، من أجل تمكين السلطات المختصة من التماس الكشف عنها. ويجوز للدولة الطرف التنصيص على تجديد هذا الأمر لاحقا" .

مفاد هذه المواد أنه في حال كنا أمام هجوم سيبراني وتعرفنا على هوية الفاعل وعلمنا أن هنالك ثمة معلومات موجودة على حاسوب الفاعل نخشى ضياعها يمكن للدولة أن تتخذ كافة الإجراءات اللازمة للمحافظة عليها وهي من أهم الأتفاقيات التي يمكن تطبيقها على بحثنا هذا وذلك لتناولها لكافة الجوانب الخاصة بالهجوم السيبراني، ما يجعلنا قادرين على معاقبة المجرم دولياً ومحلياً.

لكن هذه المعاهدة لا تتمتع بالقوة الكافية لمحاربة النشاطات غير المشروعة التي ترتكب في الفضاء السيبراني وذلك لعدة أسباب :

- تم المصادقة عليها من قبل عدد قليل من الدول هذا غير دقيق في فرض الحماية الازمة على الفضاء السيبراني .

- افتقارها لمواد تعنى خاصة و تحديداً بالهجمات السيبرانية اي أنها لم تتطرق الى هذا الموضوع بالرغم من امكانية تطبيق موادها في حالات كثيرة .

- الصفة غير الإلزامية لمواد هذه الاتفاقية وهذا يعني أن لا شيئ يلزم الدول تطبيق قواعدها طالما أنها تخلو من أي مواد عقابية للمخالفات .

يجب أن نشير أن المفاوضات المتعلقة بإبرام البروتوكول الثاني لإتفاقية بودابست بدأت عام ٢٠١٧ والهدف منه تحسين العلاقات الدولية بين أكثر من ٦٧ دولة موقعة على هذه الإتفاقية من أجل :

- تسهيل الحصول على الأدلة الإلكترونية بين الدول الموقعة

- التعاون الدولي بين أجهزة إنفاذ القانون والسلطات القضائية والتركي على المساعدة القانونية المتبادلة.

- تسهيل عملية تبادل المعلومات بين الأجهزة المختصة.

** دليل تالين بشأن القانون الدولي المطبق على الحروب السيبرانية*

دليل تالين هو عبارة عن وثيقة غير ملزمة تطبق القانون الدولي الحالي على الحرب الالكترونية اي أنه لا يعتبر وثيقة رسمية بل هو نتيجة مجموعة دراسات و أبحاث قام بها خبراء مركز التميز للدفاع السيبراني

التابع لمنظمة حلف الشمال الأطلسي الناتو (CCD-COE) وهو منظمة عسكرية دولية مقره في تالين [٢٠١] , الاّ أن الأراء والأفكار الواردة في هذا الدليل لا تمثل سوى أصحابها و لا تمثل أراء CCD-COE من الناتو بل هو نتاج أراء شخصية من الخبراء الدوليين .

أهمية هذا الدليل : يجب أن نشير أن الحروب والهجمات السيبرانية لم تكن منظمة قبل هذا الدليل، فقد ناقش كافة الجوانب المحيطة بها من تعريف هذه الهجمات ، فقد تم وضعه على نسختين : الأولى التي تعنى بالهجمات السيبرانية النادرة والأكثر خطورة والتي كانت على مستوى استعمال القوة والثانية سعت الى بناء اطار قانوني للهجمات السيبرانية التي لا تصل الى عتبة استعمال القوة [٢٠٢]، فهذا الدليل حاول وضع أطر قانونية للحرب الالكترونية مع مبادئ توجيهية موجهة الى الحكومات و الجيوش و لوكالات الاستخبارات وغيرهم من الجهات متى ارتكبت أفعال اعتبرت كانتهاكات للقانون الدولي الانساني في الفضاء السيبراني، الاّ أن هذا الدليل لا يمكن اعتباره دليلاّ حول الأمن السيبراني لأن هذا المصطلح يستخدم للحدّ من تجسس الانترنت وسرقة الملكية الفكرية، كما أنه لا يعالج مثل هذه الأمور لأن تطبيق القانون الدولي على استخدامات القوة والنزاع المسلح يلعب دوراّ ضئيلاّ أو معدوماّ في القيام بذلك [٢٠٣].

قسم هذا الدليل الى عدة فصول على الشكل التالي :

الفصل الأول :الدول والفضاء السيبراني :في هذا الفصل ناقش سلطة القضاء بالنظر الى الهجمات السيبرانية ومسؤولية الدولة عن العمليات السيبرانية التي توجه من البنى التحتية السيبرانية الحكومية أو من أجهزة الدولة.

الفصل الثاني : إستخدام القوة : نظم كافة الجوانب المحيطة بمبدأ إستخدام القوة في العلاقات الدولية ودفاع الدولة الضحية عن الهجمات التي تتعرض لها والقيود والشروط المنظمة لهذا الحق .

الفصل الثالث : قانون النزاعات المسلحة السيبرانية : ناقش هذا الدليل كافة الأمور المختصة بالنزاعات المسلحة السيبرانية و المسؤولية الجنائية للقادة والرؤساء .

الفصل الرابع : سير العمليات العدائية : تعريف الهجمات السيبرانية والقيود المفروضة عليها لناحية حماية المدنيين غير المشاركين في العمليات العدائية والأعيان المحمية والقيود الواردة على وسائل الحرب وأساليبها ومنع الغدرالإستخدام غير السليم للشعارات والتجسس.

الفصل الخامس : الفئات (الأشخاص) والأعيان والأنشطة المحمية : كأفراد الخدمات الطبية والدينية وموظفي الأمم المتحدة والمنشآت والعتاد ووالوحدات والمركبات والأشخاص المحتجزين والأطفال والصفحيين والأعيان التي لا غنى عنها لبقء السكان المدنيين على قيد الحياة والممتلكات الثقافية والطبيعية وتسهيل مرور المساعدات الإنسانية.

الفصل السادس : تنظيم وإحترام النظام العام وسلامة الفئات المتمتعين بالحماية في الأراضي المحتلة .

الفصل السابع : تنظيم العمليات السيبرانية في الأراضي المحايدة

---

[٢٠١] شيخة حسين الزهراني , مرجع سابق ,ص ١٩٩

[٢٠٢] بشار خليل :" ما هي الحرب السيبرانية ؟ - مستقبل مخيف للصراع الرقمي " ، الجمعية العلمية السورية للمعلوماتية، عدد ١٥٤، آب ٢٠٢٠، ص ٣

[٢٠٣] شيخة حسين الزهراني، مرجع سابق، ص٢٠١

- يجب أن نشير أن كافة هذه الفصول المذكورة أعلاه تم التطرق اليها في دراستنا هذه -

برأينا ان دليل تالين يشكل آلية مهمة لتوافق المبادئ الأساسية للقانون الدولي الانساني مع الحروب السيبرانية من خلال مناشدته للدول للاستجابة لمقرراته والإستعداد للهجمات السيبرانية والالتزام بمبادئ القانون الدولي المختص بتنظيم الحروب السيبرانية ونبرر ذلك أهمية اعتبار أننا يمكننا تطبيق على الهجمات والحروب السيبرانية أحكام ميثاق الأمم المتحدة و في ظل للعمليات السيبرانية غير المشروعة التي ترتكب كل يوم في الفضاء السيبراني والتي تكبد الدول والأفراد خسائر فادحة كأضرارجسيمة ووفيات وخسائر مادية، وضع دليل تالين للحدّ منها مجموعة من الاجراءات التي تتلاءم مع مبادئ القانون الدولي الانساني.

من إيجابيات هذا الدليل أن البنود المذكورة هي من أجل تنظيم المسؤوليات والحقوق للدولة الضحية و للجاني على حد سواء والواجبات التي يلزم المهاجم الالتزام بها في أي عملية سيبرانية وجميع ما تقدم يهدف الى تأمين السلام و الأمن في الفضاء السيبراني.

من أهم السيئات التي شابت هذا الدليل أن أحكامه لا تزال على شكل تمنيات وتوصيات دون أن يكون لها اي صفة الزامية و عقابية للدول , بمعنى اخر أن الدولة التي ترتكب مخالفات و انتهاكات للقانون الدولي الانساني تتحمل مسؤوليتها الجزائية بشأن مخالفتها متى كانت هذه الأفعال معتمدة من قبل نظام روما الأساسي الذي قنن هذه الجرائم و هي : جريمة الابادة الجماعية، الجرائم ضذ الانسانية وجرائم الحرب وجريمة العدوان.

اذاً حددت على سبيل الحصر هذه الجرائم وإن أي جرم يرتكب خارج هذا النطاق هذا النظام لا يعتبر جرماً دولياً انطلاقاً من مبدأ الشرعية، ونعود بالتالي الى العرف الدولي لتجريم هذا الفعل، مما يصبح الفضاء السيبراني ارضاً خصبةً لارتكاب الجرائم طالما أن المجرم سيظل دون عقاب، ولكن يجب أن نشير الى المادة ١٢٣من نظام روما الأساسي التي أعطت الحق للدول في اقتراح وتعديل واضافة جرائم جديدة للجرائم المنصوص عنها في المادة ٥ من هذا النظام، مع حق الأمين العام للأمم المتحدة للنظر في أي تعديل يمكن أن يطرق على هذه المادة.

اذاً بالنظر الى كل ما تقدم لا بدّ من اجراء بعض التعديلات للمادة الخامسة من نظام الأساسي للمحكمة الجنائية الدولية و ذلك من أجل تجريم الجرائم العابرة للحدود و الحد من الهجمات السيبرانية مع الحفاظ على مبدأ السيادة الوطنية والنظر اليها بمنظور غير تقليدي.

الفرع الثاني : دور المنظمات الحكومية وغير الحكومية

يشير مصطلح منظمة حكومية دولية الى :" كيان يتم انشاؤه بموجب معاهدة، تضم دولتين أو أكثر للعمل بحسن نية بشأن القضايا ذات الاهتمام المشترك " وكثيرة هي الأهداف لهذخ المنظمات، فهي تساهم قدر الإمكان في صياغة القوانين والقواعد القانونية والتمثيل في النزاعات والمطالبات والتعامل مع القضايا الاجرائية القضائية التي تتناول الحق في محاكمات عادلة وسريعة للمحاكم الدولية، وايضاً تعمل هذه المنظمات كمستشار للمؤسسات العامة و الخاصة في التفاوض و صياغة الاتفاقيات مع الدول و المنظمات الحكومية الدولية الأخرى[٢٠٤].

[٢٠٤] https://almrsal.com/post/1021654

مما يسعنا القول في موضوعنا هذا أن المنظمات الحكومية تحاول قدر الإمكان في ايجاد الحلول الفعالة والدقيقة للمشاكل الدولية والجرائم الجديدة التي تعرض الدول للخطر والتي تستمد كامل أموالها و نفقاتها من الحكومة لتمويل المشاريع و الأبحاث و التدريبات للتصدي للهجمات السيبرانية، ان المنظمات الحكومية تنقسم الى منظمات حكومية وطنية و هي مؤسسات تنشأها الحكومة و تقوم بادارتها و دعمها من أجل القيام بمهمات محددة و الى منظمات حكومية دولية تعود نشأتها الى فكرة المؤتمر الدولي الاّ أنها في الحقيقة ليست سوى امتداد لهذه المؤتمرات الاّ أن هذه المنظمات حصلت على ادارة وهيكل ذاتي منفصل عن الدول الأعضاء [٢٠٥].

هذه المنظمات الدولية نشأت بإتفاقية بين عدة دول أي أن أعضاؤها من الدول تكون اما عالمية (كالأمم المتحدة أو منظمة الصحة العالمية) أو اقليمية (كالاتحاد الأوروبي و مجلس التعاون الخليجي..) التي سوف نطرق لدور كل منها في هذا الفرع .

على الصعيد الدولي :

نذكر الجمعية الدولية لأمن أنظمة المعلومات ISSA -Information Systems Security Association هي منظمة دولية غير ربحية تعمل على حماية أمن الفضاء الإلكتروني، تم تأسيسها عام ١٩٢٧ ومقرها في جنيف تحت رعاية منظمة العمل الدولية (ILO) وتهدف الى مساعدة الأعضاء في مواجهة التحديات وتطوير الأنظمة السيبرانية من خلال برامج التعاون والبحث وإنتاج المعلومات ونقلها من خلال مبادئ التوجيهية المهنية وخدمات الدعم لتمكين اعضائها تحقيق الأمن السيبراني ومواجهة المخاطر السيبرانية.

على الصعيد الإقليمي :

١. جهود الاتحاد الأوروبي :

سعت وكالة تطبيق القانون الأوروبية التي تعنى بمكافحة الجرائم والارهاب في دول الاتحاد الأوروبي عن انشاءها قوة خاصة لمحاربة الهجمات السيبرانية في دول الاتحاد كما في دول أخرى و الهدف هو انخاذ التدابير اللازمة في مواجهة التهديدات الرئيسية على الإنترنت كالبرمجيات الخبيثة التي تستهدف القطاعات المالية ومكافحة عمليات الاحتيال المعلوماتية والمواقع التي تتبع الممنوعات والتابع لليوروبول [٢٠٦].

أما بالنسبة للجهود التي يقوم بها المجلس الأوروبي تتلخص في صبغ الطابع الدولي لجرائم الكمبيوتر منذ العام ١٩٧٦ و لكن اصدرت التوصية رقم ١٣/٩٨ في ١١-٩-١٩٩٥ المختصة بتكنولوجيا المعلومات ولتشجيع الدول لمراجعة قوانين الاجراءات الجزائية الوطنية لكي تتلائم مع التطور الحاصل [٢٠٧] .

من أبرز التوصيات التي جاء بها المجلس [٢٠٨] :

---

[٢٠٥] جميل عودة :" المنظمات الحكومية والغير حكومية "،مقال متوفرعلى الرابط التالي : www.siironline.org

[٢٠٦] خلف فاروق , مرجع سابق , ص ١٣

[٢٠٧] مدحت عبد الحليم رمضان : "جرائم الاعتاء على الاشخاص والإنترنت"، ط ٢٠٠٠ ، دار النهضة العربية، ص ٨٠ وما بعدها

[٢٠٨] طارق ابراهيم الدسوقي، مرجع سابق، ص ٣١٩

- أن يوضح قانون الاجراءات الجزائية أن الاجراءات الخاصة بالوثائق التقليدية تنطبق بشأن المعلومات الموجودة بأجهزة الكمبيوتر .

- أن توضح القوانين اجراءات اجهزة الكمبيوتر وضبط المعلومات الموجودة فيها ومراقبة المعلومات أثناء انتقالها .

- تطوير وتوحيد أنظمة التعامل مع الأدلة الالكترونية حتى يتم الإعتراف بها بين الدول المختلفة ويتعين ايضاً تطبيق النصوص الاجرائية الخاصة بالأدلة التطبيقية على الأدلة الالكترونية .

-يجب تشكيل وحدات خاصة لمكافحة جرائم الكمبيوتر واعداد برامج خاصة لتأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تكنولوجيا المعلومات .

- السماح باتصال الجهات القائمة على التحقيق بجهة أجنبية لجمع أدلة معينة ويتعين عتدئذ أن تسمح السلطة الأخيرة باجراءات التفتيش و الضبط و اجراء تسجيلات للتعاملات الجارية و تحديد مصدرها , ايضاً عام ١٩٩٦ أنشأت اللجنة الأوروبية لمشاكل الجريمة CDPC لجنة خبراء التعامل مع الجريمة السيبرانية و التي عملت بين سنة ١٩٩٧ و ٢٠٠٠ على الاتفاقية التي تم التصديق عليها عام ٢٠١٠ من قبل ٣٠ دولة و هي الأولى من نوعها التي تسعى الى معالجة جرائم الانترنت عبر التنسيق بين القوانين الوطنية و قوانين الدول الأخرى.

من أهم أهدافها [٢٠٩] :

- توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الالكترونية .

- توفير الاجراءات القانونية اللازمة للتحري و ملاحقة الجرائم المرتكبة الكترونياً .

- جمع معلومات عن حركة البيانات و عن امكان وجود تدخل في محتواها .

- تتضمن المبادئ العامة المتعلقة بالتعاون الدولي في : تسليم المجرمين , المساعدة الدولية المتبادلة , اعطاء المعلومات بصورة الية و انشاء الولاية القضائية على اي جريمة .

الجهود العربية :

كثرت في الأونة الأخيرة الجهود العربية في مكافحة النشاطات والهجمات السيبرانية ، عن طريق سن قوانين نموذجية جديدة اطلعت عليها الأمانة العامة لمجلس وزراء العدل العرب بالقوانين العربية الاسترشادية الخاصة بمكافحة الهجمات الالكترونية و منها[٢١٠] :

- قانون الامارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها :

---

[٢٠٩] خلف فاروق، مرجع سابق، ص ١٣-١٤٦

[٢١٠] القوانين العربية النموذجية، متوفرة على الرابط التالي : www.protectionproject.org

ما يتضمنه هذا القانون يعتبر سابقة قانونية جيدة وخطوة عربية ممتازة في مجال مكافحة الهجمات الالكترونية وتأمين سلامة الفضاء السيبراني، فمواد هذا القانون تحدد المعاني الواضحة لكل مصطلح كالبيانات و النظام المعلوماتي والبرنامج المعلوماتي في المادة الأولى منه وتحديد عقاب كل جريمة الكترونية ترتكب للحد من الابتزاز الالكتروني و الاحتيال و الارهاب و الدخول غير المصرح و الهجمات السيبرانية (المادة ٧) خاصة " كل من أعاق او شوش أو عطل عمداً و بأي وسيلة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الالي و ما في حكمها الوصول الى الخدمة أوالدخول الى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات , يعاقب بالحبس و الغرامة أو باحدى هاتين العقوبتين "، ايضاً " اذا كان الفعل ضار يوجه الى أحد الأفراد والمؤسسات أو المرافق العامة بهدف إلحاق الأضرار المادية والمعنوية به يعاقب بالحبس و الغرامة "، اذاً نحن نحتاج في وطننا العربي الى هكذا نوع من القوانين المتقدمة للحدّ من الجرائم الالكترونية والهجمات السيبرانية خاصةً.[٢١١]

- القانون العربي الاسترشادي للاثبات بالتقنيات الحديثة[٢١٢] :

أقره مجلس وزراء العدل العرب بالقرار رقم ٧٧١/د٢٤) تاريخ ٢٠٠٨/١١/٢٧يحتوي على سبعة فصول و ٢٤ مادة و الفصل الخامس من المادة ٢٣ الى ٣٢ و ما يليها تحتوي على الجرائم و العقوبات الخاصة بالجرائم الالكترونية .

- القرار رقم ٢٢٩ لسنة ١٩٩٦ الصادر عن مجلس وزراء العدل العرب الذي عني في الباب التاسع منه على الاعتداء على حقوق الأشخاص في المعالجات الالكترونية و خاصة ما نصت عليه المادة ٤٦٤ منه على عقاب من يقوم بعرقلة عمل النظام الخاص بالمعالجة الالية للمعلومات و افسادها أو تغيير المعلومات التي تتضمنها و تزويرها أو محاولة سرقتها .

- دور مجلس التعاون الخليجي :

يسعى أعضاء هذا المجلس الى جعل منطقة الخليج " منطقة الكترونية أمنة " لتشجيع الشركات على اقامة أعمالها في دول المجلس و ذلك من خلال خطة عمل تساهم في تحصين الشبكات الوطنية لدول الخليج عن طريق الاجراءات التالية :

- تحسين أمن نظام أسماء النطاقات (DNS) في دول مجلس التعاون .

- التركيز على سلامة الشبكة الوطنية .

- توطيد التعاون لمعالجة الجرائم السيبرانية .

-اعداد خطط تعاونية لتحقيق اثار هجمات الحرمان من الخدمة .

- تعزيز البنية التحتية الحساسة .

-حماية الأنظمة الحكومية و تحصينها .

---

[٢١١] www.mohamad.net

[٢١٢] خلف فاروق، مرجع سابق، ص١٥

و قد كررت هذه الأهداف في مؤتمر الأمن السيبراني الخليجي الثاني الذي عقد عام ٢١٩ في الكويت من اجل تحديد سياسات واضحة لصدّ الهجمات السيبرانية وتسخير كافة القدرات التكنولوجية وتأهيل الموارد البشرية وتحسين قدرة التعامل مع قضايا الأمن السيبراني للحد من المخاطر السيبرانية المحدقة عبر تحديد خريطة عمل متكاملة تتطلب مجهوداً جاداً ومكثفاً و ذلك من أجل مواجهة الهجمات السيبرانية.

اذاً سعت هذه الجهود أعلاه الى وضع أسس وأطر قانونية للحد من الهجمات السيبرانية والجرائم الالكترونية و لكن برأينا ان كافة هذه المحاولات غير كافية وغير مجدية في وضع نظام قانوني كامل متكامل، يعالج من العمق الهجمات السيبرانية لا أن تظل الأمور حبر على ورق دون اي تحرك جدّي يذكر .

أما بالنسبة الى المنظمات غير الحكومية :

غالباً ما تكون هذه المنظمات ضحية الهجمات السيبرانية و ذلك من أجل منعها من القيام بنشاطاتها غير الربحية , فضلاً عن اضعاف قدرتها على العمل و الحاق الأضرار بها , فالدور الذي تلعبه في مجال الحد من الهجمات السيبرانية ضعيف نسبياً بالاضافة الى الصعوبات التي تعترضها في مجال تعزيز قدراتها الدفاعية و لكن لماذا هذه المنظمات هي الاكثر عرضة لأن تكون هدفاً للهجمات ؟

اعتبرت المنظمات غير الحكومية أكثر الأجهزة تعرضاً للهجمات السيبرانية و ذلك بسبب احتفاظها بالبيانات و السجلات الشخصية للأفراد و العملاء و اللاجئين و المرضى و غيرهم من الفئات من أجل سرقة ملايين الدولارات من التبرعات و اجراء عمليات النصب و الاحتيال و حملات التضليل, مما يضعف قدرة هذه المنظمات التي هي في الأصل لا تستهدف الربح في أعمالها مما أضعف دورها في مساعدة الأفراد و المؤسسات في مجال الحد من الهجمات السيبرانية مقارنةَ مع المنظمات الحكومية التي ترتكز في تمويلها على الدول مما يعتبر من السهل التصدي للهجمات السيبرانية التي تعتبر تكلفتها باهظة لكن لا شيئ يمنعها من ذلك.

على الصعيد الدولي :

- الجمعية الدولية لأمن أنظمة المعلومات (ISSA – (Information systems security Association هي منظمة دولية غير ربحية تعمل على حماية أمن الفضاء الإلكتروني، تم تأسيسها عام ١٩٢٧ ومقرها في جنيف تحت رعاية منظمة العمل الدولية (ILO) وتهدف الى مساعدة الاعضاء في مواجهة التحديات وتطوير الأنظمة السيبرانية من خلال برامج التعاون والبحث وانتاج المعلومات ونقلها من خلال مبادئ التوجيهية المهنية وخدمات الدعم لتمكين اعضائها تحقيق الأمن السيبراني ومواجهة المخاطر السيبرانية.

-منتدى فرق الاستجابة للحوادث والأمن (FIRST) وفريقAfricaCERT ، في إنشاء أول فريق وطني للاستجابة للطوارئ الحاسوبية (CERT-GH) في غانا ومكنت أعضاء هذا الفريق من تلقي التدريب والوصول إلى شبكات مراقبة التهديدات السيبرانية العالمية. ومكّنت المعلومات التي تم تلقيها من خلال

المشاركة في هذه الشبكات فريق CERT-GH من تحديد مشغلي الشبكات ومساعدتهم على التعافي من العديد من حوادث الأمن السيبراني الخطيرة[٢١٣].

الدور الذي تلعبه هذه المنظمات في الحدّ من الهجمات السيبرانية نذكر :

- مساندة الدول التي تعرضت لهجمات سيبرانية خطيرة أدت الى نتائج خطيرة على الصعيد الاقتصادي و الاجتماعي و المالي الى النهوض من جديد و ذلك عن طريق تسخير المعطيات المتوافرة لديها .

- اخضاع العاملين في القطاعي العام و الخاص الى دورات تدريبية مكثفة مجانية أم شبة مجانية في كيفية حماية أنظم المعلومات من الأخطار السيبرانية .

سوف ننتقل الى الفصل الثاني من هذا الباب من أجل إلقاء الضوء على أبرز الآليات التقنية الأساسية التي تساهم في صدّ الهجمات السيبرانية قبل تعرضها للمعلومات أو محاولة حصر الآثار السلبية في حال تمكنت من الدخول الى أنظمة الحاسوب بهدف إلحاق الأضرار بها .

الفصل الثاني : الآليات التقنية الأساسية لحماية المعلومات

استغل المجرمون ثورة الاتصالات في ارتكاب الجرائم السيبرانية كجرائم التجسس الالكتروني و سرقة المعلومات و الاحتيال الالكتروني و اختراق الأنظمة الخاصة بالدول و بالمؤسسات الخاصة و الهجمات السيبرانية التي تعتبر من أخطر الجرائم التي من الممكن أن تتعرض لها الدول و اثارها الخطيرة التي فرضت أمر واقع أليم في ضرورة التصدي و حماية المواطنين من الخطر الذي يلاحقهم , فبات التأمين الفني و التقني ضد هذه الجرائم أمر أساسي و هاذا ما سوف نوضحه في هذا الفصل في اعتمادنا على الاليات التقنية التي تهدف الى التصدي للإعتداءات الالكترونية من خلال برامج خاصة، فضلاً عن عن تأمينات خاصة تعنى بحماية المنشأة من الأخطار التي يمكن أن تلحق بها وخاصةً أننا أمام أخطار كثيرة تعرض حياتنا وممتلكاتنا ومعلوماتنا الشخصية للخطر مما يحتم التحرك بأسرع وقت لدرءها وهذا ما سوف نفسره في هذا الفصل من آليات تقنية مهمة تحقق هذا الهدف .

المبحث الأول : الوسائل التقنية والفنية

في المبحث الحالي تكمن مهمتنا في تحديد أبرز الوسائل التقنية التي تؤمن الحماية الضرورية لأجهزة المستخدم عبر منع الهجمات السيبرانية وسائر التهديدات الخطرة التي تحاول إستهداف الأنظمة والإضرار بها عن طريق الجدار الناري والشبكة الإفتراضية (الفرع الأول) وبرامج الكشف عن الفيروسات(الفرع الثاني).

الفرع الأول : الجدار الناري والشبكة الإفتراضية

[٢١٣] https://africacenter.org/ar/spotlight/ar-ghana-multistakeholder-cyber-security/

نعني بالأليات التقنية :" نوع من المواجهة ترتكز على التقنية الرقمية التي تساهم في رسم سياسة وقائية تحد من وقوع الهجوم السيبراني او التهديدات السيبراني الأخرى من ناحية و تقديم معالجة ناجحة لأثارها اذا كانت في طور الشروع أو أنها قد وقعت بالفعل من ناحية اخرى [٢١٤]، كما وذكرنا سابقاً أن إستمرارية أي نظام أو مؤسسة ترتكز على الحفاظ على خصوصيتها و لكن من الممكن ان تكون عرضة لأي خطر يمكن أن يمس بها و يلحق الاضرار بالفرد أو المؤسسة لذلك بوجود المعلومات لا بدّ وجود الحماية المقدمة لها من اجل تحقيق التوازن المطلوب بين خصوصية المعلومات والتقدم العلمي والتكنولوجي، ويظهر دور الجدار الناري وأهميته في تقديم الحماية المطلوبة كي لا يتسلل المجرمون من الثغرات التي من الممكن أن تشوب الاتظمة الخاصة بالمعلومات.

الجدران النارية هي عبارة عن أجهزة تقوم بمسح المعلومات التي تصل من شبكة الانترنت وتقوم بتحليلها و التدقيق فيها والتأكد منها وعندما تجد اي شك في المعلومات التي تصل اليها لمحاولة الدخول أو الاختراق الى المناطق المؤمنة فانها تقوم بمنع هذه المحاولة وطردها خارج الشبكة أما اذا كانت المعلومات عادية آمنة فان الجهاز يسمح لها بالمرور والدخول على أجهزة الحاسبات الالية "[٢١٥]. وفي حال أردنا تبسيط الأمور، الجدار الناري هو أشبه بفلتر يقوم بتصفية جميع الإتصلات التي تتم على الشبكة ليسمح للإتصلات الآمنة بالمرور ويحظر تلك الضارة، فهو يفحص هذه الإتصالات وقبل أن يسمح بدخولها الى الأنظمة الخاصة يتأكد أنها أمنة وذلك لتامين الجهاز من الهجمات الضارة ويحمي البيانات من التجسس ومن الفيروسات والبرمجيات الخبيثة .

ينقسم جدارالحماية الى قسمين[٢١٦] :

القسم الأول : برامج جدار الحماية (Software FireWalls) : هي برامج يتم تنصيبها على جهاز الكمبيوتر لتأمين الشبكة، كبرامج Online Armor و Comodo FireWalls .

القسم الثاني : أدوات جدار الحماية (Hardware FireWalls) : هي أدوات خارجية يتم توصيلها على الشبكة لتأمينها .

ما هي إيجابيات وسلبيات كل نوع من هذه الأنواع المذكورة أعلاه ؟

برامج Software FireWalls تحتاج الى أن يتم تنصيبها و إعدادها على جهاز المستخدم فضلاً على إستهلاكها جزء مهم من ذاكرة الوصول العشوائية RAM ومن وحدة المعالجة المركزية CPU ، بينما Hardware FireWalls لا تحتاج الى هذا الأمر ولا تستهلك جزءاً من RAM أو CPU .

كما وتحدثنا سابقاً عن فيروس الفدية Ransomware الذي يهدف الى الوصول الى المعلومات الشخصية للمستخدم من أجل ابتزازه بها وتحريضه على دفع المال من أجل استردادها، فهذا الجدار الناري يمنع هذا الفيروس بالإضافة الى من المهاجم من التسلل الى هذه المواقع ولكن هذه العملية هي دقيقة نوعاً ما ولا بدّ

---

[٢١٤] شيخة حسين الزهراني، مرجع سابق، ص ٢٥١

[٢١٥] أيمن عبد الحفيظ : " الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية "، ط ٢٠٠٥، دار النهضة العربية، مصر، ص ١٥٨

[216] أحمد عباس :" شرح الجدار الناري وأنواعه وتفعيله على موقعك للحصول على حماية كاملة " ، موقع ووردبريس بالعربية ، ٩ آذار ٢٠٢١

من ضبطها بالشكل الجيد لأنه في حال قد تم ضبط جهاز الجدار الناري بدرجة حساسية عالية وأكثر من اللازم فان ذلك سوف يتسبب ببطئ التعامل وأحياناً منع المعلومات الآمنة من الوصول.

أما بالنسبة الى أنواع الجدران النارية هي على الشكل التالي :

١. Proxy Firewalls

نعني بهذا النوع أنه وسيط بين الشبكات الداخلية والخارجية والإنترنت وتعرف بإسم جدار الحماية الوسيط ولكن عملياً كيف تساهم في حماية المعلومات الخاصة ؟

في حال مثلاً اردنا أن نبحث عن مصطلح معين على جوجل، بوجود ال Proxy Firewalls سوف يقوم بالحصول على هذا الطلب وإعادة توجيهه على أساس أنه صادر من التطبيق نفسه وليس من الجهاز الخاص وهكذا لا يستطيع جوجل التعرف على معلومات المستخدم الخاصة وعلى موقعه الجغرافي او جمع أي معلومات خاصة بل سوف يظن أن يتعامل مع المستخدم نفسه ولكن يكون مع هذا التطبيق وهكذا يكون هو الوسيط بين المستخدم والإنترنت[٢١٧].

٢. Next Generation FireWalls (NGFW)

هو الأساس التي ترتكز عليه غالبية الشركات العامة و الخاصة و المؤسسات و غيرها في حماية معلوماتها و قد اعتبر الأفضل بين أنواع الجدران النارية على الاطلاق، فهو يقوم بالتأكد من كافة الإتصالات الصادرة والواردة من خلال تقنيات حديثة تسمى IPS التي تمنع الفيروسات والهجمات السيبرانية ويتأكد أن البريد الإلكتروني للموظفين خالٍ من أي رابط أو مرجع ضار قد يؤثر على الشبكة، فهو قادر على إكتشاف ومنع هذه الأعمال المعقدة من خلال فرض سياسات الأمان على كافة المستويات وذلك من خلال حظر البرامج الضارة قبل دخولها الى الشبكة وهذا الأمرلم يكن ممكناً من قبل وبالتالي فهو يختلف عن الجدار الناري التقليدي في أنه خيار منخفض للشركات التي تحاول أن تحسين أمان أجهزتها من خلال إستخدام الوعي بالتطبيقات والخدمات الخاصة بفحص أنظمة الحماية، فضلاً على أنها مجهزة بشكل أفضل للتعامل مع التهديدات المستمرة المتقدمة (APTS) [٢١٨] ومن أبرز أهداف هذا النوع من الجدار الناري :

- يساهم في تعزيز الوعي التطبيقي
- يمنع انظمة التسلل المتكاملة IPSES
- يتأكد من هوية المتسلل بشكل دقيق و حديث
- يستطيع استخدام مصادر ذكاء خارجية في تحليل الوضع القائم

يجب أن نشير أن الجدار الناري التقليدي و NGFW يساهمان في حماية أنظمة المؤسسة ومعلوماتها من أي خطر وقدرتهم على إجراء فحص كامل للحزم وترجمة عنوان الشبكة والمنفذ ويمكن لهما ايضاً إعداد اتصالات VPN ولكن أهم الإختلافات بينهما أن NGFW يقوم بفحص عميق للحزم وترجمة عنوان الشبكة

[217] https://upar.net/firewall-for-wordpress/

[218] Casey Clark : " Next Generation FireWall-, TechTarget,p1-2 , available on : www.techtarget.com

والمنفذ فضلاً في انه يساهم في الامكانية في التصرف بناءً على البيانات المقدمة من خدمات وإستخبارات التهديدات الحديثة المقدمة وفق برامج خاصة بالذكاء الإصطناعي وأخيراً يعمل على توسيع وظيفة الجدار الحماية التقليدية لدعم NAT ,PAT,VPN، حيث يتصرف جدار الحماية كجهاز توجيه وفقاً للمعطيات التي يحصل عليها .

٣. Packet Filtering Firewalls

ان هذا النوع من الجدار الناري هو الأقدم على الإطلاق فيتحكم في تدقيق البيانات من والى الشبكة، ويستقبل المعلومات الصادرة من الاتصال ويتأكد أنها تتلاءم مع مجموعة القواعد المحددة مسبقاً الخاصة بالتصفية ومن عنوان ال IPالخاص بالإتصال، ففي حال كانت تطابق هذه القواعد يستقبلها والاّ سوف يتم رفض هذا الإتصال.

تتمثل فوائد هذا النوع أنه سريع رخيص وفعاّل وليس له أي تاثير على السرعة مقارنةً مع أنواع أخرى من الحماية بل يوفر حماية ممتازة وسرعة قصوى بقبول الاتصال أو رفضه بناءً للمواصفات التالية :

- عنوان ال IP أو IP Adress : أي العنوان الذي يتم ارسال الإتصال منه

- هدف ال IP Adress أي السبب الذي يجعل هذا العنوان يصل الى جهاز المستخدم

-البروتوكالات الخاصة بالتطبيق لنقل البيانات (TCP , UDP , ICMP)

- الإتجاه : وارد أم صادر

ان ما يميز هذا النوع من الجدار عن ال Proxy Firewalls ان هذا الأخير يقوم بتوجيه الإتصال الى الجهاز الخاص بالحماية للتأكد أنه آمن قبل وصوله الى المستخدم، وبناءً على المعطيات المقدمة من المستهدف يتصرف بالبقول او بالرفض كي لا تكون معلومات المستخدم في الواجهة ومن أشهر تطبيقات برامج الجدران النارية " برنامج ZoneAlarm الذي يعتبر تطبيق مهم في ضبط ورصد كافة محاولات اختراق الأجهزة وقيامه بإعطاء اشارة عند حدوث أي اعتداء، ومن ابرز ايجابيات هذا التطبيق انه يقوم بفحص مرفقات البريد الإلكتروني عبر التأكد من خلوها من اي فيروس وفي حال تبين له انه يحتوي على احدى الفيروسات فيقوم بطرده أو مسحه وكما أن هذا البرنامج يتيح للمستخدم فرصة تفحص الملفات ثم يقرر تشغيلها أم لا[٢١٩].

4. Circuit –Level Gateway :

يحتوي هذا النوع من الجدران النارية على بوابات تقوم بفحص بروتوكول TCP الذي يستخدم في نفل البيانات عبر الشبكات والتأكد من مطابقتها للمعايير الأمنية الخاصة

٥. Stateful Inspection FireWalls :

[٢١٩] ايمن عبد الحفيظ، مرجع سابق، ص ١٦٠

يساهم هذا النوع من الجدران النارية الى مراقبة حركة المرور الصادرة والواردة وتصفيتها بشكل تلقائي بناءً على القواعد الأمنية المعدة مسبقاً من قبل المستخدم (يراقب الإتصال من اللحظات الأولى حتى أغلاق الموقع بالكامل) عبر فحص TCP ، ولكن من سلبياته أنه يستهلك جزء كبير من موارد الجهاز الاساسية، مما يسبب بطئ في نقل البيانات والمعلومات، وهو بحاجة بشكل دائم الى تحديث.

بعد أن وضحنا مفهوم الجدار الناري وأنواعه وأهميته في تحقيق الأمن السيبراني للأفراد والمؤسسات نشير أنه من المحبذ إستخدام أكثر من جدار ناري في الوقت نفسه وذلك من أجل التصدي لكافة الهجمات والفيروسات وملئ الثغرات التي من الممكن تسلل المجرمون من خلالها.

لقد إنتهينا من تبيان أهمية الجدار الناري في التصدي للهجمات السيبرانية سوف نعالج في القسم الثاني من هذا الفرع دور الشبكة الإفتراضية .

*الشبكة الافتراضية Virtual Private Network (VPN) [٢٢٠]

هذه الشبكة تعتبر بمثابة شبكة بيانات تستخدم البنية التحتية لشبكات الإتصال السلكية واللاسلكية العامة مع المحافظة على خصوصيتها باستخدام بروتوكول خاص وهدفها الأساسي هو إعطاء الشركات القدرات المتاحة لخطوط الاتصال المؤجرة leased Lines أو الخطوط بشكل ايسر وأدق وسميّت على أنها افتراضية لأنها تنشأ عند الحاجة اليها وتخدم عدد من المستخدمين ومغلقة عليهم وكأنها أنشات خصيصاً لهؤلاء وبتكاليف منخفضة وهي على عدة أنواع :

١. عبر شبكة الانترنت Site to Site :

تعد هذه الشبكة كأنها نفق داخل شبكة الانترنت لا تسمح بالمرور منه الاّ لأطراف هذه الشبكة و يتم تشفير البيانات و النوع الثاني هي دون الحاجة للجوء الى الانترنت.

٢. MPLS - Multi Protocol Layer Switching :

تعتمد فقط على البنية التحتية – السنترلات العامة المتاحة بكل منطقة، تتميز هذه الشبكة أنها تسمح اتصال عدة مواقع بشكل آمن وبسرعة عالية وان كانت بعيدة جغرافياً عن بعضها البعض و ذلك بهدف تحقيق الأعمال بشكل دقيق ونقل المعلومات بشكل اسرع وأسهل بكافة أشكالها، كما يمكن مثلا في حال افتتحت الشركة فروع عديدة لها يمكن إضافة هذه الأخيرة للشبكة طالما أنها تعتمد في الإتصال على البنية التحتية العامة للإتصالات.

[٢٢٠] أحمد أمين أبو سعده:" الشبكة الفتراضية الخاصة VPN للربط بين المؤسسات المتخصصة "، مجلة العربية للدراسات المعلوماتية – العدد ١، ٢٠١٢، ص ١١٧

اما سيبرانياً فان هذه المعلومات التي تنقل عبر هذه الشبكة هي مشفرة و سرية للغاية و ذلك باستخدام أكواد و مفاتيح سرية تبلغ لأصحاب العلاقة و الموظفين , أي أنه يصعب على أي طرف ثالث الدخول و الحصول على هذه المعلومات .

عملياً تتم الحماية على الشكل التالي :

تقوم بوابة الاتصال Gateway بعملية تفشير للبيانات Encryption قبل ارسالها ثم تقوم بفك هذا التفشير Decryption عند الطرف المرسل اليه [٢٢١] ثم يقوم العميل بادخال كلمة السر التي تكون مرسلة اليه اصلاً من قبل الشركة للسماح له بالدخول .

ان هذه الشبكة الافتراضية الخاصة تؤمن حماية ممتازة للمعلومات الحساسة وتقلل نسبة تعرضها لأي هجوم سيبراني بنسبة ٨٠٪ تقريباً وذلك طالما أن هذه الشبكة تتأكد أن كلمة السر هي صحيحة قبل أن تسمح للعميل بالدخول والتصفح داخل شبكة الانترنت بصورة آمنة لا يتم اختراقها أو التسلل اليها والمهاجم يفشل من توجيه أي هجوم او الحصول على أية معلومة .

3. L2TP VPN :

ترمز L2TP إلى Layer to Tunneling Protocol إلى نفق طورته ميكروسوفت، ان أساس هذا النوع من الشبكات الإفتراضية أن L2TP مرتبطة ببروتوكول حماية VPN آخر لتأمين الإتصال أو بعبارة أخرى أن L2TP هو نفق بين L2TP وشبكة VPN أخرى مثل IPsec (البروتوكول الذي يركز على تشفير البيانات وتأمين الإتصال عبر تلك الأنفاق)، لا يوفّر أيّ تشفير بل هو بروتوكول VPN نفقي يقوم بإنشاء قاعدة اتصالٍ بين المستخدم وبين خادم أو سرفر الVPN .

٤. IPsec أو Internet Protocol Security :

هو نوع من أنواع ال VPN يستخدم من أجل تأمين الإتصال بالإنترنت عبر شبكات IP من أجل التحقق أن البيانات قد تم تشفيرها ويعمل من خلال وضعيتان هما وضعية النفق Tunneling Mode و وضعية النقل Transport Mode وكلاهما لحماية انتقال البيانات بين شبكتين مختلفتين، ومن حسنات هذا النوع أنه يسمح إستخدامه مع أنواع أخرى من الشبكات الإفتراضية فهي وسيلة أو أداة هي عادة ما تكون روتر أو تطبيق حماية متعدد الأغراض من خلال هذا الروتر أو جهاز الحماية متعدد الأغراض، يتم تشفيير البيانات وخلق نفق VPN .

٥. Hybrid VPN :

يجمع هذا النوع بين MPLS وجميع أنواع الشبكات الإفترضية المعتمدة على IPsec وذلك من أجل تأمين الإتصال بالموقع الرئيسي عن بعد عن طريق إستخدام النوعين المذكورين أعلاه من أجل تأمين حماية قصوى للشركات الأ أنها باهظة الثمن .

عملياً كثيرةُ هي الشبكات الإفتراضية[٢٢٢] نذكر منها :

---

[٢٢١] أحمد أمين أبو سعده، مرجع سابق، ص ١٢٠

[٢٢٢] أحمد حسن : " أفضل ٩ خدمات VPN: موثوقة وآمنة وسريعة " ، موقع vpn Mentor ،١٣-٦-٢٠٢٣

CyberGhos , PrivateVPN , ProtonVPN ,PIA(Private Internet Access) , AtlasVPN , NordVPN , OVPN , Hotspot Shield , StealthVPN

إستعرضنا أبرز أنواع ال VPN ، سوف نتوسع بإحداها التي تصدرت هذه القائمة أعلاه وهي ExpressVPN

١. ExpressVPN :

تعد من أفضل شبكة افتراضية خاصة شاملة اختبرتها، فهي تأتي بسرعات مذهلة وحماية قوية، ويرجع ذلك بجزء كبير إلى بروتوكول Lightway الحصري الخاص بها، فهو أوسع ويستهلك موارد أقل مقارنة بالبروتوكولات الأخرى، ومن خصائص هذه الشبكة :

- سهلة الإستخدام والتثبيت

- الإنقسام النفقي ونعني به أن هذه الشبكة تسمح بإختيار التطبيقات التي تستخدم خاصية VPN وتلك التي لا تستخدمها

- الحماية من الهجمات والتهديدات السيبرانية فهي توفر حماية ضد تسريباتDNS وعنوان IP و.WebRTC

- عند إنقطاع الإنترنت ستعمل خاصية Network Lock على قفل الشبكة خوفاً من المساس بمعلومات المستخدم

- تستخدم ExpressVPN تشفير AES بمفتاح ٢٥٦-بت مع مفتاح تجزئة SHA512 وتشفير RSA بمفتاح ٤٠٩٦-بت. هذه التوليفة تجعل من الصعب على أمهر المخترقين إمكانية الوصول إلى بيانات المستخدم.

- يتضمن هذا النوع من ال VPN تقنية TrustedServer عبرتحديث كافة خوادم ExpressVPN تلقائيًا، مما يقلل من مخاطرالتعرض للبيانات الحماية بشكل كبير.

لقد انتهينا من معالجة الاليات التقنية اللازمة للحد من الهجمات السيبرانية عبر حماية الأصول و الموارد الخاصة بالأنظمة المعلوماتية مع امكانية التحكم بهذه البيانات و تبادلها دون أن يؤثر هذا الأمر على سرعة التواصل بين الشركات و المؤسسات بل هي تساهم في تحقيق الأمن السيبراني بغية الحد من المخاطر المحتملة و من أجل توفير حماية كاملة سوف نبين في المبحث الثاني كيفية التصدي للاعتداءات الالكترونية من خلال استخدام برامج خاصة للكشف عن الفيروسات .

الفرع الثاني: برامج الكشف عن الفيروسات ومضاداتها

عرفت برامج مكافحة الفيروسات على أنها مجموعة البرامج التي صممت خصيصاً للكشف عن الفيروسات و ازالتها من أجهزة الحاسوب بالاضافة الى قدراتها على حماية ألأجهزة من مجموعة التهديدات كبرامج التجسس و برامج أحصنة الطروادة و غيرها من الفيروسات الخبيثة، هذه البرامج تقوم بفحص اي ملف قد يشتبه أنه خبيث ثم تقوم بازالته و تنظيف الجهاز منه، وبعض الأجهزة التي تتصل بالانترنت يمكن أن تتعرض لأي خطر عبر دخولها الى أحد المواقع، فهذه البرامج تتأكد أنه من الممكن الدخول الى هذه المواقع لخلوها من أي خطر يمكن أن يعرض معلومات المستخدم للخطر و في حال تبين أن هذا الموقع غير امنة اي غير مطابقة للمواصفات المطلوبة لا يسمح للمستخدم بالدخول اليها عبر تنبيهه من خلال اشارة معينة،أيضاً هذه البرامج ليست مخصصة فقط لأجهزة الكمبيوتر بل يمكن تثبيتها أيضاً أي جهاز ذكي آخر.

إن أفضل برامج الكشف عن الفيروسات لعام ٢٠٢٣ هي كالتالي :

- Panda Security, Bitfender, Webroot Security, Norton Mobile Security, McAfee Mobile Security, AVG AntiVirus, Trend Micro Mobile Security , Sophos Intercept X, SurfShark Antivirus, AvastFree Antivirus .

سوف نتوسع في نوعين من هذه اللائحة هما AvastFree Antivirus و Norton Mobile Security على الشكل التالي [223]:

أ- AvastFree Antivirus :

يساهم هذا البرنامج في الكشف عن كافة البرمجيات الخبيثة كأحصنة الطروادة والفيروسات والبرامج الدعائية الخبيثة وهجمات التصيد والتصدي للمواقع غير الآمنة عن طريق إجراء فحوصات ذكية للثغرات التي يمكن من خلالها المهاجم التسلل الى أنظمة الضحية، كما يساعد في توجيه تنبيهات الى المستخدم بوجود ملفات مشبوهة قبل فتحها أو ثغرات معينة أو نقاط ضعف يصعب العثور عليها وتحليل الملفات والتأكد أنها خالية من اي فيروس وتسمى هذه الميزة CyberCapture .

من ميزات هذا التطبيق :

- التصفح الآمن للبريد الإلكتروني

- الإتصال بشبكة ال WiFi بطريقة سليمة وآمنة ومنع المتسللين إختراق الشبكة والوصول الى الملفات الشخصية .

- إرسال تنبيهات الى المستخدم في حال تم التعرض لأحد كلمات السر الخاصة به .

- الحماية من كافة الفيروسات والديدان

- التأثير الضئيل على عمل الجهاز

ب- برنامج Norton Mobile Security :

[223] Alex Macfarland: " 10 best Antivirus for MAC" , UNITE,AL, October 2023

يعتبر هذا البرنامج من أهم البرامج المضادة للفيروسات لسببٍ أساسيٍ أنه في حال إشتبه المستخدم بوجود خطرٍ ما يهدد جهازه يوفر له كانت الإمكانيات التقنية المتاحة عن طريق الإستجابة لمؤشرات الإنتباه، فضلاً عن عرض للمخاطر التي يكتشفها الجهاز في الوقت الفعلي بواسطة Norton SONAR وعرض للثغرات التي يمكن إستغلالها بوجه المستخدم ومحاولة التصدي لها عبر معالجتها، ويستطيع المهاجم في أي وقت الضغط على liveUpdate (ميزة موجودة في النافذة الرئيسية لهذا البرنامج) من أجل معرفة أية تفاصيل.

هذه الفيروسات تنتقل الى الحاسوب من خلال عدة طرق :عندما يحمل المستخدم مثلاً ملفات معينة غير امنة من مواقع على شبكة الانترنت و خاصةً اذا كان جهازه لا يحتوي على اي برامج يكشف هذه البرمجيات الخبيثة , ايضاً في حال قد أرسل له ملفات معينة هي في الأصل غير سليمة و تحتوي على فيروس معين، كذلك في حال كان هذا الحاسوب مرتبط بالشبكات المحلية الخاصة بالشركة مثلاً و قد انتقل هذا الفيروس الى الشبكة الأساسية ثم حكماً انتقل الى الأجهزة المرتبطة بها، فالأقراص الصلبة و المدمجة و الرسائل التي تصل الى البريد الالكتروني و غيرها من الحالات التي من الممكن أن تحتوي على فيروسات معينة تساهم في مسح أو تعطيل عمل البرامج التي تهدد أيضاً سلامة و أمن أجهزة الحاسب الالي.

تعتبر مضادات الفيروسات بمثابة رقيب على أي ملف يتم استخدامه في النظم المعلوماتية أو غيرها , فتقوم هذه الأجهزة كما و وضحنا اعلاه بفحص الملفات للتأكد من خلوها من الفروسات قبل استخدامها [٢٢٤], الاّ أن هذه البرامج هي على أنواع [٢٢٥]:

١. البرامج المستقلة : هي البرامج التي توضع مثلاً على Flash Memory ثم وضع هذه الأخيرة على أي جهاز للكشف عن احتمالية وجود فيروسات .

.2 البرامج الأساسية : هي البرامج التي تكون في الأصل موجودة بشكل دائم على نظام جهاز المستخدم للقيام بتحديث تلقائي ويومي للكشف عن اي أمر مشبوه ويمكن تثبيته على اي جهاز سواء كان كومبيوتر، هاتف، تابلت.. و يعتبر هذا النوع من البرامج الأقوى والأفضل لناحية تحديثه الدائم لجهاز المستخدم .

٣. برامج حماية المساحة التخزينية : وهي البرامج التي صممت خصيصاً لتكون قاعدة بيانات اونلاين، فهي لا تحتاج أن تثبت على اي جهاز بل المستخدم في حال اراد التأكد من خلو الملف من اي أمر ضار يرفع الملف اليه وسوف يقوم هذا البرنامج بعملية الكشف يبين للمستخدم وجود أو عدم وجود فيروس بالملف موضوع الكشف .

ما هي سلبيات وايجابيات هذه البرامج ؟

السلبيات[٢٢٦] :

١. تساهم في غلق المنافذ والمعابر الموجودة في الجهاز الحاسب الالي التي تمكن المخترقين من الوصول الى البيانات والمعلومات وبالتالي الوصول الى اهدافهم .

٢. ليس لديها القدرة الكاملة في توفير الحماية اللازمة للأجهزة الالكترونية والحاسب الالي .

---

[٢٢٤] شيخة حسين الزهراني، مرجع سابق، ص ٢٥٨

[٢٢٥] https://Techgena.com/antivirus-definition/

[٢٢٦] شيخة حسين الزهراني، مرجع سابق، ص ٢٥٩

٣. تقليص في أداء الجهاز، أي أن الجهاز الذي يحتوي برامج خاصة لمكافحة الفيروسات يصبح أكثر بطءً و صعوبة في استخدامه مما يدفع بالمستخدمين ازالة هذه البرامج خوفاً من فقدان الأداء الضروري وصعوبة الإستخدام .

٤. كشفت الدراسات الحديثة أن عدد البرامج المضادة للفيروسات لا تحصى مقارنةً بالخدمة الجيدة التي تقدمها , فعدد ضئيل جداً الذي يساهم فعلاً في مكافحة الفيروسات إضافةً الى جعل الأجهزة أكثر عرضة للبرامج الضارة [٢٢٧].

الايجابيات :

١. تساهم هذه البرامج في حماية الأجهزة من الفيروسات والديدان وتجنب الاصابة بها .

٢. في حال كان المستخدم يريد التأكد ان كان ملف ما يريد استخدامه مشوب بامر خطير ام لا يستطيع القيام بذلك من خلال برامج حماية المساحة التخزينية .

٣. إمكانية التعرف على الفيروسات التي تتسلل الى الأجهزة بشطل خفي ويعمل تحت مسمى أنها تقوم بعمل معين ولكنها في الحقيقة تهدف الى التجسس على الجهاز والحصول على المعلومات الخاصة بالمستخدم لتستهدف اتلافه وتدميره ومسح البيانات عنه.

٤. تساهم في الحد من الهجوم السيبراني الذي يهدف منه تخريب أجهزة الحاسوب .

اذاً ان هذه البرامج الضارة للفيروسات مهمة في التعرف على البرامج الخبيثة و كشفها و منعها من الحاق الأضرار بأجهزة المستخدم و لكنها لا تمنع من الهجمات السيبرانية التي يقوم بها مجموعة المخترقين و الهاكرز , كما لا تؤمن الحماية الكاملة ولذلك برأينا ليست الخيار الافضل التي يمكن اللجوء للتخلص من الهجمات بل كثيرةُ هي الأدوات التي تحدثنا عنها سابقاً تؤمن الحماية الافضل للأجهزة و تمنه من تعرض المستخدم لأي خطر, سوف نوضح في المبحث التالي دور التأمينات الداخلية والخارجية المطبقة في حماية المنشات من الهجمات السيبرانية.

المبحث الثاني : الأدوات التأمينية لمواجهة المخاطر السيبرانية

كثيرةُ هي الأدوات والأساليب المستخدمة في التصدي الى الهجمات السيبرانية : تقنياً، قانونياُ وميدانياً ،ولكن لماذا الإجراءات الميدانية تساهم في الحد من الهجمات السيبرانية تحمي المنشآت؟ ففي هذا المبحث سوف نبين في الفرع الأول منه كافة التأمينات الداخلية والخارجية التي تساهم في حماية المنشآت من الهجمات السيبرانية، وفي الفرع الثاني سوف نوضح أهمية التأمين السيبراني في مساعدة الشركات والمؤسسات على تخطي الآثار السلبية التي لحقت بها جرّاء هذه الهجمات.

الفرع الأول : التأمينات الميدانية الخاصة بالمنشآت

[٢٢٧] https://aljazeera.net/tech/2019/3/13

ان التأمين المادي هو عبارة عن " مجموعة من الاجراءات المادية المصصمة لسلامة الموظفين ومنع وصول غير المأذون له للمعدات والوثائق وللحماية من الكوارث التي يمكن أن تتعرض لها المنشاة [٢٢٨] ولكن الأهم من كل ما سبق يهدف الى حماية المعلومات والبيانات الحساسة التابعة للشركة من أي هجوم أو خطر يمكن أن تتعرض له مما يؤدي الى خسائر وأضرار جسيمة وذلك لأنه من الصعب معرفة وقت إرتكاب الجرائم يحتم أن تكون المؤسسات والشركات على استعداد دائم للتصدي لأي خطر يمكن أن يمس بها ومن بين هذه الأخطار : الهجمات السيبرانية التي تؤدي في حال مست بالمعلومات المراد حمايتها الى خسائر بالملايين فضلاً عن المساس بسمعة الشركة، فمبدأ التأمين هو على نوعين : الأول هو التأمين الخارجي للمنشأة موضوع التأمين والثاني هو التأمين الداخلي والهدف واحد وان إختلفت أنواع التأمين وهو حماية الأجهزة الالكترونية وملحقاتها من أي خطر محدق يمكن أن يمس بالمعلومات ويساهم في إتلافها أم تخريبها أم العبث بمحتوياتها وهذا ما سوف نوضحه في هذا المبحث مما يدفعنا الى طرح السؤال التالي: كيف يمكن للتأمينات المادية الداخلية والخارجية للمنشأة أن تؤدي الى توفير الحماية من الهجمات السيبرانية؟

-التأمين المادي الخارجي للمنشأة :

مجموعة الاجراءات المتخذة من أجل تعزيز الأمن المادي لديها خارج المنشاة المتمثلة بمجموعة مستويات أمنية مطبقة وهذه الأخيرة تطبق تبعاً لأهمية المعلومات والبيانات الموجودة على الأجهزة الالكترونية المراد تأمينها وطبيعة عمل المنشأة، لتبدأ مستويات التأمين من المستوى الأدنى الى المستوى الأعلى : كالأسوار والحواجز المادية التي تهدف الى منع الغير من الدخول عن طريق تحديد النطاق الجغرافي للمنشاة و من أجل منع أياً كان من التسلل و الدخول اليها , فهذه الحواجز المادية هي تساهم في اعاقة الأنشطة الخارجية التي يقيمها البعض من أجل الدخول للمنشاة بالقوة على أن تكون هذه الحواجز بسيطة (كالعوارض ذات القضبان للنوافذ والأقفال الأمنية المتطورة ونظام أساسي للإنذار، الى المستوى الأعلى عن طريق اقامة سياج مقاوم للاختراق كالأسلاك الشائكة وتفعيل أنظمة متقدمة للاقتحام، فضلاً عن كاميرات مراقبة، الإضاءة القوية وحراس مسلحون ومدربون تدريباً عالياً وخطط للطوارئ [٢٢٩]، فضلاً عن البوابات الإلكترونية وإستخدام أجهزة الكشف عن الأسلحة قبل الدخول الفرد للمنشاة، فهذه الإجراءات جميعها أعلاه تهدف الى حماية المعلومات والبيانات من خطر دخول أياً كان بهدف استهدافها والحاق الأضرار بها والعبث بمحتوياتها أو احراقها أو اي عمل أخر من شأنه أن يعرض الشركة خسائر كبيرة كانت بغنى عنه، وكلما كنا أمام اجراءات مشددة كلما كانت المعلومات المراد حمايتها مهمة وضروري ابقاءها سرية والتصدي لأي هجوم يمكن أن تتعرض له .

- التأمين المادي الداخلي للمنشأة :

هي الاجراءات الداخلية المتخذة والمكملة للإجراءات الخارجية لمواجهة أي خطر ويمكن تحديدها على الشكل التالي [٢٣٠] : الكاميرات وشاشات الرصد وأجهزة نقل الصور وذلك للتأكد أن كل على ما يرام دون وجود اي حركة غير مألوفة داخل المنشأة، نضيف عن أهمية مراقبة الاتصالات التي يجريها الموظفون من

---

[٢٢٨] شيخة حسين الزهراني، مرجع سابق، ص٢٦٠

[٢٢٩] أيمن عبد الحفيظ، مرجع سابق، ص ١١٧

[٢٣٠] أيمن عبد الحفيظ، مرجع سابق، ص ١٤٠

أجل التأكد أنها تدور ضمن مجراها الطبيعي دون اي تشويش عليها وتأمين على هذه الأجهزة من خلال الكشف عن أي أجهزة تنصت يمكن أن توضع في الأجهزة الخاصة بالمنشاة، بالإضافة الى التأمين على وضع الكوابل الخارجية ومعدات الهواتف وذلك عن طريق دفنها داخل حفرة عميقة لحمايتها بحيث لا يقل عمقها عن ١٨ بوصة مع عدم وضع أي علامات تدل على وجودها او ادخالها ضمن مبنى خاص مجهز لها وسري للغاية .

- الإجراءات الداخلية المطبقة على العاملين في المنشاة : تتمثل في التأكد أن كافة العاملين على المام بالتهديدات السيبرانية وكيفية التصدي لها وفي حال تبين أن أحدهم ليس على دراية بهذا الموضوع تجبره الشركة على المشاركة في الدورات التدريبية المخصصة للموظفين .

- ابقاء المعلومات السرية والمهمة خارج متناول الجميع بل غالباً يجب أن تكون محصورة بموظفين محددين على أن يتم تصنيف هؤلاء وفقاً لدرجة سرية البيانات التي تنقسم الى بيانات عادية وسرية جداً وسريةللغاية وبيانات محظور الإطلاع عليها .

اذاً وباختصار ان التصدي لأي تهديد سيبراني لا يتم الاّ عن طريق حماية الفضاء السيبراني عبر برمجيات وأنظمة سيبرانية حديثة تساهم في حماية الأجهزة من جهة وتأمينات مادية داخلية وخارجية تحمي بيانات الشركات وتحافظ على أمنها وتمنع أي شخص غير مرخص له من الدخول الى المعلومات السرية المراد حمايتها وان كان من العاملين في الشركة وذلك لأن بعض الموظفين وطمعاً بالمال يفشون معلومات سرية الى الشركة المنافسة والحاق الأضرار بالمعلومات والبيانات وإتلافها أو تخريبها في حال طلب منهم ذلك .

اذاً من أجل تحقيق حماية قصوى من التهديدات السيبرانية لا بدّ من التأمين الفني والتقني والتامين المادي الداخلي والخارجي، وفي ظل عقد تأمين سيبراني يساهم قدر الامكان في حماية المنشأة وهذا ما سوف نوضحه في الفرع الأخير من هذا المبحث.

الفرع الثاني : عقد التأمين السيبراني

ان عقد التأمين السيبراني(CyberInsurrance) هو من العقود التجارية الإجمالية الذي يقوم على جانبين : فني وقانوني، فالجانب الأول هو قائم على اساس الإجراءات الفنية التي من الممكن إتخاذها من أجل الحدّ من المخاطر السيبرانية، أما الجانب القانوني يقوم على أساس أن شخص ما، سواء كان هذا الشخص طبيعي أو المعنوي يخشى التعرض لخطر ما، فيسعى الى تأمين نفسه وممتلكاته ضد هذا الخطر من خلال عقد تأمين يلتزم المؤمن بدفع التعويض المناسب في حال تعرضه للخطر المنصوص عنه في العقد،هذا الأخير يتوجه الى أدوات التكنولوجيا والإنترنت وشبكات الإتصال والإحتيال عن طريقة إساءة استخدام البيانات، والمسؤولية تنشأ عن طريق تخريب البيانات وإتلافها أو تسريبها سواء كانت متعلقة بالأفراد او الجماعات او الحكومات بإستثناء الاخطاء التي تقع من الشركة أو من أفرادها [٢٣١]، فالمخاطرالسيبرانية صنفت على أنها الخطر الأكبر الذي يواجه الشركات على مستوى العالم وفق مقياس Allianz لعام ٢٠٢٠ ولكن ما نعني بالمخاطر السيبرانية ؟

[٢٣١] محمد سعيد اسماعيل، مرجع سابق، ص ٢١٠

قامت مجموعة من كبار مسؤولي المخاطر في شركات التأمين (CRO Forum, 2014) بتعريف المخاطر السيبرانية بأنها : " أية مخاطر تنشأ عن استخدام البيانات الإلكترونية ونقلها، بما في ذلك أدوات التكنولوجيا مثل الإنترنت وشبكات الاتصالات"، أيضاً جمعية جنيف (٢٠١٦)، (وهي مؤسسة فكرية دولية في مجال التأمين تضم في عضويتها عددًا كبيرًا من الشركات التأمينية، إقترحت تعريف للمخاطر السيبرانية أنها عبارة عن "أي خطر ينشأ عن استخدام تكنولوجيا المعلومات والاتصالات التي تهدد السرية أو سلامة البيانات أو الخدمات"[٢٣٢].

ظهر التأمين السيبراني في أواخر التسعينيات نتيجة الاعتماد المتزايد على التكنولوجيا وزيادة التهديدات السيبرانية. في البداية، كان يستهدف خروقات البيانات والهجمات الحاسوبية، ولكن مع مرور الوقت، أصبح يشمل مجموعة واسعة من الجرائم السيبرانية، بما في ذلك برامج الفدية والابتزاز السيبراني وهجمات الهندسة الاجتماعية وفشل الأنظمة وانقطاع الأعمال بسبب حوادث الأمن السيبراني، ففقدان البيانات الإلكترونية أو اختراقها أو سرقتها تأثيرات سلبيية على الأعمال التجارية، بما في ذلك خسارة العملاء والإيرادات. قد يكون أصحاب الأعمال والشركات يعتبروا مسؤولين عن الأضرار الناجمة عن سرقة بيانات الطرف الثالث، نذكر مثلاً أنه عام ٢٠١١ تعرضت شركة Sony الى هجمات سيبرانية أدت الى الكشف عن معلومات ٧٧ مليون حساب لمستخدمي PlayStation، مما أدى الى إنقطاع الخدمة لمدة ٢٣ يوماً و تكبدت الشركة حينئذٍ خسائر تفوق قيمتها ١٧١ مليون دولار أمريكي، وشركة التأمين الخاصة بالشركة تتحمل فقط الخسائر المادية دون السيبرانية، فأصبحث الشركة مسؤولة تجاه الغير عن هذه الأضرار المادية والمعنوية التي ألحقت بهم ،إنطلاقاً من عدم وجود أي عقد تأمين سيبراني يمّكن شركة التأمين من تحمل التكاليف المتعلقة بالأضرار السيبرانية التي ألحق بالشركة.

من هنا تظهر أهمية التأمين السيبراني ذلك للأسباب التالية[٢٣٣] :

١. الحماية من المخاطر والهجمات السيبرانية .

٢. توفير الحماية المالية والتعويض عن النفقات: ويشمل نفقات التحقيقات وخدمات مراقبة الائتمان والمسؤوليات القانونية المحتملة، التكاليف المرتبطة بانتهاكات البيانات، بالإضافة إلى ذلك، تقديم تعويضات عن انقطاع الأعمال وخسارة الإيرادات وعن الأضرار التي تلحق بالمؤسسة المؤمنة نتيجة الخسائر التي تتحملها الشركة رداً على حادث الكتروني وعادةً ما يشمل السرقة و الاحتيال والتحقيق الجنائي وانقطاع الاعمال والانترنت أو فقدان معلومات، والأضرار التي تلحقها الشركة المؤمنة بالشركات الأخرى نتيجة الهجمات السيبرانية مما يقع على شركة التأمين تغطية هذه الخسائر والتعويض للغير عن الأضرار التي ألحقت بهم.

٣. تأمين الدعم القانوني المناسب : تساهم شركة التأمين في دفع تكاليف المستشار القانوني، والامتثال القانوني للوائح والدعاوى القضائية المحتملة الناجمة عن انتهاكات البيانات أو انتهاكات الخصوصية للشركة المتضررة.

---

[232] OECD: "Enhancing the Role of Insurance in Cyber Risk Management, OECD Publishing ", Paris,2017

[٢٣٣] Kinza Yasar : " CyberInsurance" , TechTarget, September 2023,p1

.4 توفير راحة البال والشعور بالأمان للشركة المؤمنة : يساهم عقد التأمين السيبراني في تركيز الشركات على عملياتها التجارية الأساسية دون الحاجة إلى القلق المستمر بشأن العواقب المحتملة نتيج الهجوم السيبراني.

٥. الإستعداد الإستباقي للهجمات السيبرانية : مما يعزز ثقة العملاء والمصالح بالشركة وتجعلها متميزة بين الشركات الأخرى.

أما بالنسبة الى الجهات البحاجة للتأمين السيبراني هم كالتالي[٢٣٤] :

١.المؤسسات بكافة أشكالها و أنواعها و خاصةً تلك التي تقوم بإنشاء البيانات الإلكترونية وتخزينها وإدارتها عبر الإنترنت - مثل جهات اتصال العملاء والمبيعات ومعلومات تحديد الهوية الشخصية وأرقام بطاقات الائتمان - يحق لها الاستفادة من التأمين السيبراني.

٢. مقدمي الرعاية الصحية إنطلاقاً من طبيعة المعلومات الحساسة التي يحتفظون بها .

.3 المؤسسات المالية والمصارف : يساعد التأمين السيبراني هذه الجهات وعملائها من التعافي من الأضرار المالية التي لحقت بها .

٤.المؤسسات التعليمية : تتعرض المدارس والجامعات والمهنيات الى الهجمات السيبرانية بسبب إحتواءها على عدد لا يستهان به من المعلومات الشخصية للطلبة.

.5 الشركات المتعددة الجنسيات : نظراً لإراداتها المرتفعة والمعلومات الضخمة التي تحتفظ بها عن عملائها.

٦. المنظمات الحكومية وغير الحكومية : التي تعتبر من أهم الوكالات والمنظمات التي تتعرض للهجمات السيبرانية بإستمرار .

عقد التأمين يتميز بثلاثة أركان[٢٣٥] :

١. التراضي بين الفرقاء : ان عقد التأمين السيبراني كاي عقد لا بدّ لتحققه تلاقي الايجاب و القبول بين فرقائه فضلاً عن أهلية التعاقد و عدم وجود اي عيب من عيوب الرضى و توافر كافة الاجراءات الشكلية اللازمة لقيامه.

٢. سبب أو محل عقد التأمين السيبراني : ان محل عقد التأمين هو الخطر الذي يرغب المؤمن له أن يظل بعيداً عن المعلومات المراد حمايتها , فالخطر هو القصد الجنائي او الخطأ الواقع على المعلومات الذي يسبب ضرراً للمؤمن له ,و لكن ما هي أنواع المعلومات محل التأمين السيبراني ؟

١. المعلومات الشخصية : تعرّف على أنها معلومات مهمة مرتبطة بشخص محدد و معروف الهوية أو يمكننا تحديد هويته مباشرة أو بطريقة غير مباشرة و كل وسيلة من شأنها أن تجعلنا نتعرف على هوية الشخص عبر الاسم أو العنوان , عنوان البريد الالكتروني , رقم الهاتف , بطاقة التعريف ..الخ .

---

234 Ibid,p2

٢٣٥ بغدادي شامبي : " تأمين الخطر السيبراني "، مجلة هيرودوت للعلوم الانسانية والاجتماعية، المجلد ٧، العدد ٢٥، ٢٠٠٥، ص ٢٤٨-٢٤٩

٢.المعلومات الاستراتجية الخاصة بالمؤسسة : هي المعلومات الخاصة بالعقود المكتبية مع الشركاء لاطلاق خدمة جديدة أو عرض جديد أو العقود الخاصة مع مزودي الخدمة الحاصلة عليها الشركة أو خطة العمل الجديدة التي يريد اصحابها أبقاءها سرية أو المعلومات الخاصة بالمناقصات و اي معلومة خاصة بالعملاء يريد ابقاءها سرية ومن شأن تسريبها أو التداول بها في العلن الى الحاق الأضرار المادية و المعنوية بالشركة و خاصةً الأعمال التي من شأنها أن تنتهك سرية المعلومات الخاصة بالزبائن و عمال المؤسسة مما يؤثر سلباً على سمعة الشركة و مكانتها لدى غيرها و لكن سوف نوضح نقطة مهمة و هي أن هذه الشركة هي ضحية و مسؤولة في الوقت نفسه تجاه العملاء اللذين سرقت معلوماتهم الشخصية و استخدمت مثلاً في أعمال منافية للقانون و الحقت بهم اضرار سواء كانت مادية أم معنوية مما يقع على الشركة واجب تبرير و تعويض عن الضرر الذي لحق بهم و في حال كانت الشركة مؤمنة لدى أحد شركات التأمين السيبراني يقع على هذه الأخيرة التعويض على العملاء و الشركة انطلاقاً من عقد التأمين الموقع بينهما و مساعدة الشركة للتخلص من هذه الكارثة و لملمت جراحها لاعادة البدء من جديد

إنطلاقاً من ما تقدم، ما هي السلبيات والإيجابيات لعقد التأمين السيبراني في إطار الهجمات السيبرانية ؟

.من أبرز سلبيات عقود التأمين في إطار الهجمات السيبرانية أنها تستبعد الخسائر المالية نتيجة هذه الهجمات التي تلحق بالقطاع العام وذلك لإعتقاد شركات التأمين أن المرافق العامة والحكومية تمتلك الأموال اللازمة لتخطي هذه الخسائر والعودة الى العمل بشكل طبيعي، إضافةً الى أن شركات التأمين لا تتبنى الخسائر السيبرانية التي تلحق بالشركات والمؤسسات بنسبة ١٠٠٪ وخاصةً في حال كانت هذه الخسائر كارثية، من السلبيات ايضاً أن تكلفة بوليصة التأمين في الهجمات السيبرانية تعتمد على كثير من العوامل أهمها حجم العمل والإيرادات السنوية وطبيعة المعلومات المرد حمايتها وأهمية هذه المعلومات ومدى خطورة التعرض اليها، فغالباً تكون تكلفة هذه البوليصة مرتفعة نسبياً مما يصعب على الشركات المتوسطة والصغيرة تحمل التكاليف الباهظة لعقد التأمين السيبراني .

أما من أيجابيات هذا العقد أنه مصمم لمســاعدة الشركات على التخفيف من الأضرار والأثار المدمرة المحتملة للجرائم، على أن تحمي المؤمن من نوعين من الضرر :الأول هو الضرر الذي يلحق بالشركة نتيجة الهجمات السيبرانية أما الثاني يتمثل بالأضرار المعنوية التي تلحقها هذه الهجمات بالشركة اي عندما تمس بسمعة الشركة ومكانتها (أي الاضرار المعنوية)" [٢٣٦] .

لماذا في البلدان النامية لا تزال فكرة التأمين السيبراني غريبة نوعاً ما ؟

السبب يعود الى ضعف الثقافة التأمينية لدى الشركات الخاصة الصغيرة و المتوسطة أما الشركات الكبرى غالباً ما يكون لديها فروعُ عدة حول العالم مما يحتم حماية مصالحها من خلال العقود التأمينية و لكن يجب أن نشير أن الأنظمة القانونية فارغة من أي مادة تشير الى عقد التأمين السيبراني بل نجد فقط عقود التأمين التقليدية مما يحتم ضرورة تطور المشرع لهذه النصوص أي سن قوانين ومراسيم جديدة تتوافق مع هذه التطورات السيبرانية[٢٣٧] و تضمين بنود خاصة بالتامينات السيبرانية وتنظيمها وتهيئة الأرضية المحلية كي تتماشى مع الجرائم المستحدثة وخفض تكاليف التامين كي تتمكن الشركات الصغيرة ذات الرأسمال المحدود من حماية مصالحها.

---

[٢٣٦] محمد سعيد اسماعيل، مرجع سابق، ص -٢٠٨-٢٢٢

[٢٣٧] بغدادي شامبي، مرجع سابق، ص ٢٥٤-٢٥٥

أما بالنسبة للأحوال التي لا تعترف شركة التأمين بالأضرار و ترفض التعويض كالتالي[٢٣٨] :

- ألخطاء البشرية (أي أخطاء الموظفين) .

- استبعاد سياسات تغطية فشل الطاقة او المرافق او الميكانكية والاتصالات السلكية واللاسلكية .

- قيود تغطية الاغلاق الطوعي : تطبق هذه التغطية فقط على الحالات المتعلقة بالإغلاق الطوعي بسبب انتشار أحد البرامج الضارة او للحد من الضرر المنتشر .

اذا برأينا أن التأمين السيبراني ضروري للشركات والمرافق العامة على حد سواء وذلك من أجل حماية أنظمتها ومعلوماتها من أي تهديد جديد يمكن أن تتعرض له الاّ أن هذا الأمر لا بدّ أن يرافقه تشريعات سيبرانية تساهم قدر الامكان في مواكبة الحداثة والسعي الدائم الى معاقبة المهاجم وهذا ما سوف نتطرق اليه في الباب الثاني من هذا القسم .

الباب الثانى : دور المشرّع الوطنى فى مكافحة الهجمات الالكترونية

لا يوجد اختلاف على أن تطور التكنولوجيا والاعلام والاتصالات وظهور الشبكة العنكبوتية والتقدم السريع للبرامج المعلوماتية و الأجهزة الجديدة أدت الى تقديم خدمات وإحداث اثار جانبية في نمط الحياة ولكن أدى الى ظهور جرائم جديدة مما دفع بالمشرع الوطني والدولي الى البدء بالبحث عن كيفية القضاء على هذه الجرائم وسبل تجريمها للحد منها ومن اجل الحفاظ على حقوق ومصالح الأفراد المادية منها والمعنوية، فهذا التطور لم يمر مرور الكرام بل حمل معه اثار خطيرة وتهديدات جدية دفعت بالقوى العظمى الى البدء بتعديل قوانينها القديمة التي عالجت الجرائم التقليدية، فهذه النصوص الجنائية القديمة لا تستطيع مواجهة التطورات الحديثة والأساليب المتقدمة في ارتكاب الجرائم في حال لم تتطور هذه أيضاً لمواكبة هذه المستجدات , فالمشرع يلعب دوراً مهماً في الحد من الجرائم السيبرانية عن طريق سن قوانين جديدة متطورة تستطيع أن تفهم الطبيعة المعقدة لهذه الجرائم وتتماشى معها انطلاقاً من وجود هدفاً واحداً وهو حماية الأفراد من المخاطر التي تحملها هذه الجرائم، مما يدفعنا الى طرح الإشكالية التالية : الى أي مدى يمكن للمحاولات القانونية المستمرة الدولية والمحلية في التوصل الى مكافحة الجرائم السيبرانية ؟ وما هي أبرز العراقيل التي تعترض الدول في مجال الحد من هذه الجرائم وما هي سبل الحل ؟

لقد خصصنا هذا الباب من البحث لتسليط الضوء على أبرز المحاولات القانونية للمشرع الوطني في إطار الحد من الهجوم السيبراني (في الفصل الأول) والصعوبات المحلية في مجال التعاون والتدريب على مكافحته وسبل الحل (الفصل الثاني) .

الفصل الأول : المحاولات القانونية المحلية

لقد عالجنا السبل والإمكانيات القانونية المتاحة للتخلص من الهجمات السيبرانية وكيف الإتفاقيات الدولية والقرارات الصادرة عن الأجهزة الدولية سعت بكامل قواها الى تنظيم مسألة الهجمات السيبرانية ووضع

[٢٣٨] بغدادي شامبي، مرجع سابق، ص٢٢١

أطر قانونية لها اضافة الى الدور المهم التي تمارسه المنظمات الحكومية و غير الحكومية في هذا المجال و كما و قلنا سابقاً أننا لا زلنا نواجه فراغ قانوني شاسع دولياً ومحلياً في ظل عدم مواكبة الدول النامية خاصةً لهذه التطورات و ضرورة تجريم الهجمات السيبرانية المخالفة لقواعد القانون الدولي الانساني انطلاقاً من المبدأ القائل أن " لا جريمة و لا عقوبة دون نص "، مما يترتب مواكبة المبادئ القانونية للمستجدات الجرمية من أجل الحد منها وتنظيم أطرها .

اما محلياً فالمشرع الوطني لم يواكب تطور الجرائم الحديثة في البلاد والخطر المحدق الذي تهدد به وخاصةً أن النصوص الجنائية التقليدية لا تستطيع أن تجرم و تعاقب هذه الجرائم الجديدة بالنظر الى الطبيعة الخاصة التي تمر بها كونها هادئة في أغلب الأوقات اي أنها لا تتسم بالعنف وهي جريمة فنية لا يتخلف عنها أثار مادية ملموسة كتلك التي تخلفها الجرائم التقليدية كالسرقة والقتل والايذاء وغيرها، الاّ في حال تطورت هذه الهجمات للحدّ التي أصبحت فيه قوة وعدوان يؤديان الى أضرار خطيرة وجسيمة في الأرواح والممتلكات .

فالقانون هو نتيجة وجود ظاهرة في المجتمع تحتاج من المشرع أن يواكبها ويعالجها حتى يحمي المجتمع من الأثار السلبية التي تنشأ عن تلك الظاهرة [٢٣٩]، انطلاقاً من ما تقدم سوف نعالج في هذا الفصل أبرز المحاولات القانونية في اطار الحد من الهجمات السيبرانية .

المبحث الأول : الأنظمة القانونية المحلية

لا شك أن النصوص القانونية تساهم في الحدّ من الجرائم داخل دولة معينة وذلك بسبب أغراضها المتمثلة بالردع العام والردع الخاص وهذا المبدأ نفسه يطبق على الهجمات السيبرانية،لذلك سوف نحاول في هذا المبحث تفسير الدور الذي تقوم به الأنظمة والأطر القانونية في التصدي للهجمات السيبرانية وتنظيم أطرها القانونية (الفرع الأول) ، وحق الدولة في قطع الإنترنت عن أراضيها ضمن قيود معينة في الفرع الثاني.

الفرع الأول : الإطار التشريعي الوطني

عملاً بمبدأ لا عقوبة ولا جريمة دون نص، لا يجوز للقاضي اللجوء الى قصد اخر غير نصوص القانون لتجريم سلوك لم يرد به نص على تجريمه ولا تستطيع فرض عقوبة أخرى غير العقوبة المفروضة قانوناً [٢٤٠]، و مفاد هذا النص أن القاضي ملزم بتجريم الأفعال الموجودة في النص القانوني والالتزام بالعقوبة المقررة ايضاً، فلا يستطيع أن يتناول أفعال لم ينص القانون على أنها محرمة أو بعبارة أخرى لم ترد ضمن نص قانوني قد جرمها، وأي فعل آخر لم يحدده المشرع يعتبر قانوناً غير معاقب عليه الاّ بوجود نص في القانون وهذا ما يسمى بمبدأ الشرعية.

فالمشرع اوكل وحده بتحديد الجرائم والعقوبات الملاءمة لها ومهما كان الفعل خطيراً أو جسيماً طالما أنه لم يتم ادراجه ضمن نص قانوني لا يمكن تجريمه وفق ما جاء في المادة الأولى- الفقرة الأولى من قانون العقوبات : "لا تفرض عقوبة ولا تدبير احترازي أو اصلاحي من أجل جرم لم يكن القانون قد نص عليه حين إقترافه"، الاّ أن التجريم و العقوبة هم أدوات ردع فعّالة في الحد من الجرائم : فالردع هو التهديد باستخدام القوة او السلطة لاقناع شخص بالامتثال لارادة الطرف الذي يهدد بها و يتكون من ركنين : ركن

---

[٢٣٩] شيخة حسين الزهراني، مرجع سابق، ص ٢٤٧

[٢٤٠] على جبار شلال : " المبادئ العامة في قانون العقوبات "، الطبعة الثانية، مكتب زاكي للطباعة، بغداد، ٢٠١٠ و ص ٢١

مادي الذي ينطوي على تأمين كافة مقتضيات القدرة على انزال العقاب و اخر معنوي يهدف الى التأثير النفسي في الشخص من خلال اقتاعه بجدوى الانصياع لطرف الذي يمثل السلطة [٢٤١] و لكن ما يهمنا هو امكانية خضوع الهجمات السيبرانية لمبدأ التجريم و العقاب ,و الى اي مدى يمكن معاقبة المهاجم عن الفعل الذي ارتكبه ؟

ان الهجمات السيبرانية لم يتناولها المشرع الوطني في القوانين المحلية اي لم ينص على تجريمها مع العقوبة المناسبة لها, فنحن أمام واقع أليم و فراغ قانوني كبير يهدد مجتمعنا ومؤسساتنا العامة والخاصة، فالمشرع وحده له الحق في تجديد الأفعال المعاقب عليها والجزاءات المفروضة عليها عبر تعديل المواد القانونية الموجودة أو إستحداث نصوص جديدة ضمن شروط وإجراءات معينة وهذه التعديلات التي يمكن أن يقوم بها المشرع إنطلاقاً من وجود تهديدات وجرائم مستحدثة تمس بمصالح الأفراد وحقوقهم ومن أجل حماية هذه المصالح والمحافظة على التوازن في المجتمع .

نحن أما عدة إحتمالات بشأن الدور الذي يلعبه مبدأ لتجريم والعقاب في الحد من الهجمات السيبرانية :

الإحتمال الأول : لا جدوى من نظرية الردع في مجال الهجمات السيبرانية لعدة اسباب :

- صعوبة تحديد هوية الفاعل : ان الهجمات السيبرانية التي تنفذ عن بعد مما يعتبر من الصعب الكشف عن هوية الفاعل لانزال العقاب به و خاصةً اذا كان المجرم متواجد في بلداً أخر و نجح فعلاً في اخفاء هويته مما يعتبر مستحيلاً تطبيق مبدأ التجريم و العقاب.

- ضعف القوانين وغيابها في التطرق الى الحرب السيبرانية ومعاقبتها تجعل من البلاد أرضية خصبة لارتكاب هذه الأخيرة دون اي حسيب أو رقيب بل يحفذ المجرمين الى ارتكاب المزيد طالما ان القوانين التي تهدف في الأصل الى معاقبة هذه الافعال غير موجودة فلا جدوى من نظرية الردع على صعيد الفضاء السيبراني و ان طبيعة العمليات السيبرانية تقوض الدور المحتمل للردع و تجعله عديم الفائدة انطلاقاً من الخصائص الخاصة بالهجمات السيبرانية .

الإحتمال الثاني المؤيد لدورالردع في الحد من الهجمات السيبرانية :

لا يمكن لأحد أن يلغي الدور الاساسي الذي يلعبه مبدأ الشرعية في تجريم الأفعال الخطيرة ومعاقبتها، فدون عقوبة يعتبر المجتمع ملاذ امن للمجرمين في تطوير أفعالهم الجرمية وخاصةً السيبرانية منها، مما يستتبع ضرورة مواكبة التشريع الوطني للجرائم الجديدة المستحدثة إنطلاقاً من الخسائر الضخمة التي تلحق بالأفراد جرآء هذه الهجمات وحاجة هؤلاء الى إسترداد حقوقهم المادية والمعنوية .

الإحتمال الثالث هو اللجوء الى الردع ضمن شروط معينة :

اي أن الردع وحده غير كاف لتطبيقه على العمليات في الفضاء السيبراني بل يجب اعتبار ان الردع في عصر المعلومات يختلف عنه في الحروب التقليدية و لا بدّ لحسن التطبيق أن نستخدم الردع في المقومات العسكرية والاقتصادية والاستخباراتية والقانونية كي تتحقق أهدافه التي وضعت من أجله، فالأهداف متمثلة في جبر الطرف المتضرر سواء كان الضرر الذي لحق به هو مادي أم معنوي ومعاقبة الفاعل بعقوبة

[٢٤١] علي جبار شلال، مرجع سابق، ص ٢٥

متناسبة مع الضرر الذي لحق به،فالشروط يمكن تلخيصها بتوافر الركنين المادي والمعنوي على الشكل التالي :

- البحث في كافة التفاصيل المحيطة بالهجوم : هوية الفاعل الحقيقي وإن كان يشاركه شخصُ آخر في هذا التنفيذ (شريك، متدخل، محرض) ، الحاسوب الذي إنطلق منه الهجوم، مكان إرتكابه

- التأكد أن الهجوم الذي قام به الفاعل هو السبب وراء الأضرار التي لحقت بالضحية

- إنطباق النص القانوني السيبراني على الهجوم الذي قام به الفاعل (الركن القانوني)

- التأكد أن الفاعل قام بتنفيذ هذا الهجوم بكامل إرادته(أي علمه بأن الهجوم الذي قام به سوف يلحق الأضرار بالضحية وإرادته المتجهة الى تنفيذه) (الركن المعنوي) .

برأينا أننا أمام ظواهر خطيرة من الصعب التعامل معها الاّ أن لا شيئ يلغي الدور الجوهري التي تلعبه العقوبة في وضع حد لها وان كانت شخصية المجرم مجهولة، فالعقوبة لها دور وقائي ومبدأ الشرعية هو فكرة تحذير المشرع بموجب قواعد قانونية معينة للأفراد الذين يظنون أنه يمكنهم القيام بفعل جرمي مماثل على نحو يختلف مع القواعد تحت طائلة توقيع العقاب.

إنطلاقاً من ما تقدم نشدد فقط على ضرورة وضع للهجمات السيبرانية وان كنا أمام جرائم جديدة ومختلفة، فتجريمها أمرلا بدّ منه على أن تكون العقوبة متناسبة مع الجرم المرتكب و ان كانت شخصية الجاني المعلوماتي مختلفة عن شخصية الجاني التقليدي الاّ أنه من المفترض أن يأخذ المشرع بعين الإعتبار كافة الظروف المحيطة بالهجوم , فتطبيق مبدا الشرعية يؤدي الى تحقيق المصلحة الاجتماعية عن طريق تحقيق العدالة الفردية أي أنه يوفر الحماية للأفراد من أي اعتداء يمكن أن يتعرضوا له نتيجة هذه الجرائم التي تنال من حقوقهم و معلوماتهم الشخصية و يعطي الضمانة للأفراد أن القانون يساهم قدر الإمكان في توفير الأمان والطمأنينة وراحة البال بوجه أي شخص يحاول التعدي على مصالح يحميها القانون، ولأجل كافة الأسباب المبينة أعلاه نرى أنه من الضروري جداً على المشرع اللبناني تنظيم مسالة الحرب والهجمات السيبرانية ضمن قانون العقوبات وبشكلٍ واضحٍ بما يتماشى مع المعاهدات والإتفاقيات الدولية التي تحاول تجريم هذه الأفعال وتنظيم أطرها، نضيف أن ما نراه متوفراً محلياً وجود بعض الجهود الخجولة دون أي تطور يذكر .

سوف ننتقل الى حق الدولة في اللجوء الى بعض الإجراءات الاستثنائية لحماية وجودها وهذا ما سوف نتطرق اليه في الفرع الثاني من هذا المبحث .

الفرع الثاني : حق الدولة في قطع الإتصال بالإنترنت

بحجة الحفاظ على الامن القومي والحدّ من الثغرات الأمنية الاقتصادية، تتجه الدول الى اللجوء الى واحدة من أسوأ الحلول هي سياسة قطع الاتصال بالانترنت على البلد بكاملها اما عن منطقة معينة، المبدأ العام وفقاً لأحكام القانون الدولي : يحق للدولة في حالات استثنائية طارئة تهدد وجودها في ممارسة بعض الصلاحيات الموكلة اليها من أجل حماية المواطنين من الخطر الذي يهدد وجودها، فيعطى لها الحق في هذه الأحوال الطارئة أن يلجأ الى قطع الانترنت كي تفوت على المعتدين فرصة استغلال الانترنت في تقويض اركان الدولة أو نشر الاسرار العسكرية أو بث الفتن والذعر والشائعات بين السكان، اذاً لكي تصل الدولة الى

مرحلة القيام ببعض الصلاحيات الاستثنائية لا بد أن يتوافر في الخطر مجموعة من المواصفات كي يحق للدولة أن تمارس هذه الصلاحيات :

١. أن يكون الخطر حال وآني : يجب أن يكون الضرر آني مما يحتم على الدولة أن تتخذ اجراءات سريعة في تفادي حصول أضرار جسيمة في الارواح و الممتلكات .

٢.ان يكون من شأن الضرر أن يلحق اضرار جسيمة في اركان الدولة و مواطنيها أو بمعنى أخر تهدد حياة كالنزاع المسلح او الاضطرابات المدنية و كان من الضروري اللجوء الى قطع الانترنت من أجل تفادي الأخطار التي تهدد أو البلاد و كيان الدولة و وجودها (كالطوارئ الارهابية أو كارثة طبيعية شديدة مثل فيضانات أو زلازل و غيرها) .

٣. الطابع المؤقت لهذا التدبير : و ذلك أن تلتزم الدولة بالقيام بمجموعة هذه الاجراءات التي تتزامن مع الوضع الطارئ الى حين انتهائه و هذا يعني أن الدولة ملزمة بايقاف هذه الاجراءات الاستثنائية فور انتهاء هذا الوضع.

٤. الالتزام بمبدأ التناسب : أي ان تكون ردة فعل الدولةمتناسبة مع الخطرالحاصل دون وجود أي وسيلة فعالة مماثلة للاستجابة لمتطلبات الوضع المستجد أو بمعنى أخر لا يوجد اي وسيلة أخرى اقل تقييداً للحقوق المعنية و هذا ما أكدته المادة الرابعة من الفقرة الاولى من العهد الخاص بالحقوق المدنية و السياسية .

٥. أن يتم الاعلان عم حالة الطوارئ العامة رسمياً لكي يسمح و يبرر التقييد الحاصل و خاصة تدبير قطع الانترنت عن البلاد من خلال الاعلان عن حالة الطوارئ مع توضيح صادر عن الدولة لماذا قد لجأت الى هذا التدبير دون غيره من الوسائل الأخرى بالرغم من تأثيرها الخطير على حرية التعبير و المساس بالمبادئ الديمقراطية .

- مدى فعالية تدبير قطع الانترنت لمجابهة الهجمات السيبرانية :

في الواقع و بنظرنا الشخصي ان لجوء الدولة الى قطع الاتصال بالانترنت على أراضيها بالرغم من أن هذا الحق مكرس لها , لا تفي بالغرض بل هي سياسة خطيرة و سيئة تمس بحقوق التعبير ومبادئ الديمقراطية و التاثير على الشركات و الأفراد التي ترتبط أعمالهم بالانترنت مما يؤدي الى انهيار اقتصادي في البلاد و شلل القطاعات العامة المالية والاقتصادية والاجتماعية وخاصةً أن بعض المهم تعتمد بشكل اساسي على الشبكة العنكبوتية مما يؤدي الى أضرار جسيمة بمصالح هذه الاخيرة، أيضاً تؤدي الى تأثير قوي على التدفق الحر للمعلومات، فآلية قطع الإتصال تؤدي الى منع الوصول الى المواقع الشرعية المفيدة كما في ذلك المواقع العلمية والطبية غيرها والمساس أيضاَ بانتهاك حرية الانسان والتعبير عن رأيه الشخصي، فلجوء الدولة الى الى قطع الاتصال بالانترنت لمواجهة الهجوم السيبراني لا يؤدي الى الحد منه وذلك لناحية طبيعة هذه الهجمات التي يمكنه أن تستقر في الأجهزة بشكل خفي كي تحقق غايتها دون ان تعلم الضحية أصلاً أنها تتعرض لهجوم السيبراني، أما في حالة مساس الهجمات السيبرانية في وجود الدولة وكيانها اي عند تعرض البنى التحتية للدولة ووجود حالة الضرورة فوجب على هذه الأخيرة في حال أرادت اتخاذ مثل هذا التدبير يجب أن يتم ضمن شروط خاصة من حيث المدة والهدف ولكن وجب تحصين الأمن السيبراني في البلاد كي لا تضطر أن تلجأ الى مثل هذا التدبير.

أحياناً تلجأ الدولة لقطع الانترنت وذلك من أجل اسكات الشعب وتقييد حريته في التعبير او للقيام بعمل غير مشروع و التستر عنه من خلال قطع الاتصال بالانترنت او ارتكاب جرائم خطيرة بحق المواطنين و لمنع الاعلام الدولي من الكشف عنها كي لا تتعرض الدولة للمساءلة الدولية مثلاً : لجات السعودية الى قطع الانترنت عن بلدة العوامية التي تشهد احتجاجات كثيرة , بحيث اعتبر البعض ان قطع الانترنت عنها يعتبر بمثابة حصار تمارسه الدولة بحقها و ذلك من اجل صم الاذان عن مطالبات سكان البلدة في الوصول للمعلومات و اتمام أعمالهم عن طريق الانترنت[٢٤٢] , مما دفع بالأمم المتحدة الى اتهام السعودية بانتهاك حقوق الانسان بحرمانهم من حقهم في الاتصال بالإنترنت وإعتبرت "ان الحكومات التي تلجأ الى قطع الانترنت أو تعطيله جزئياً ينتهك حرية الانسان و كذلك الأمر في البحرين بسبب المظاهرات في منطقة الدراز دفع الأمر بالدولة الى قطع الإنترنت عن الدولة بكاملها من أجل إخمادها.

نستنتج أن أسلوب قطع الانترنت عن البلاد من أجل الحد من تأثير الهجمات غير مفضل بل من يجب أن تلجأ الدولة عن طريق مختلف في التصدي للاعتداءات التي تتعرض لها وخاصةً أن المهاجم يستطيع العودة الى الهجمات السيبرانية بعد انتهاء الدولة من قطع الانترنت ولا يمكن أن تظل الانترنت غير متوافرة في البلاد حتى اشعار آخر بل وجب عليها أن تجد حلول أخرى تؤدي الغرض نفسه الذي يؤديه اسلوب قطع الانترنت عن البلاد وخاصةً أنه مرفوض دولياً لمساسه بحق الوصول الى المعلومات فضلاً عن نتائج خطيرة على الاقتصاد المالي و التعرض لمصالح الأفراد و الحاق الاضرار بها مما يحتم علينا في المبحث التالي توضيح كيفية مواكبة القوانين القائمة لتطور الجرائم الجديدة .

المبحث الثاني : تقييم الواقع التشريعي والقضائي السيبراني في لبنان

يخلو القانون اللبناني من أي تنظيم لمسألة الحرب السيبرانية، فالهجمات المرتكبة في الفضاء السيبراني المحلي غير معاقب عليها إنطلاقاً من غياب التجريم الضروري لهذه الأفعال مما يدفعنا الى القاء الضوء على الواقع السيبراني المحلي في الفرع الأول من هذا المبحث وتوضيح كافة المعوقات القضائية التي تحول دون تحقيق العدالة السيبرانية للمتضررين في الفرع الثاني .

الفرع الأول : القصور التشريعية في معالجة الهجمات السيبرانية

القانون هو الجزاء الرادع لحماية المجتمعات من مخاطر الجرائم المستحدثة التي أصبحت تأخذ طابعاً دولياً، بحيث اختلفت طرائق و اساليب ارتكاب الجرائم و أصبحت تلحق أضرار جسيمة مادية و جسدية و معنوية في الشركات و المؤسسات العامة و الأفراد على حد سواء, مما فرضت هذه الظاهرة واقع يحتم التحرك لمواجهة هذه الظواهر الاجرامية التي تشكل خطراً على استقرار و أمن المجتمعات و لكن كيف يمكننا معالجتها في ظل وجود قانون قديم نسبياً لم يتناولها بتة, ففرض على المشرع ضرورة طرح قوانين و تشريعات جديدة تحد من هذه الجرائم المستحدثة ولكن لماذا دائماً ننظر الى تحديث القوانين كمعالجة سريعة للمشاكل المستجدة ؟

---

[٢٤٢] مقال بعنوان : " كيف تستخدم الدول قطع الانترنت لصالحها ؟"، منشور على موقع : https://www.noonpost.com/

في الواقع قانون العقوبات الوطني يبين لنا أن المشرع لم يطور النصوص و الأحكام القانونية كي تتماشى مع الوضع السيبراني الراهن، فالمجتمع في تطور مستمر و اصبحت الجرائم ترتكب بكبسة زر , فالمجرم يستخدم عند تنفيذ هذه الجرائم معطيات العلم الحديث و التي تجعلها مميزة عن الجرائم التقليدية من حيث نوع الجرم المرتكب و صعوبة الكشف عن هوية الفاعل الذي يعتمد على الذكاء و بالطبع صعوبة اثباتها , فهذه التطورات جميعها تفرض على المشرع ضرورة مواكبة الأساليب المستحدثة عبر خلق اليات قانونية و تقنية حديثة لفرض سلطان القانون و معاقبة سوء استخدام التكنولوجيا و المشرع هو الذي يقوم بهذا الدور في الحد من الجرائم عبر تطوير المستمر للقوانين القائمة , فالمجتمعات في تقدم مستمر مما يغير أسلوب ارتكاب الجرائم فضلاً عن خلق ظواهر اجرامية لم تكن بالحسبان مما يحتم على ذلك التفكير في ضبط عمل و نشاط النقنية المستخدمة بتشريعات خاصة على مستوى قوانين الدول و الاتفاقيات الدولية , فالهدف هو التفكير في كيفية توفير الحماية القانونية للبيانات و المعلومات و الامان السيبراني.

انطلاقاً من ما تقدم أعلاه سوف نوضح اسباب ضرورة مواكبة المشرع المحلي للتطورات السيبرانية[٢٤٣]:

١. الدور الجوهري في الحد من الجرائم : يلعب المشرع دوراً اساسياً في الحد من الجرائم عبر تشريع أحكام جديدة تواكب التطورات التي تفرضها هذه الأخيرة , فلا يمكن توفير الحماية القانونية للأفراد ف ظل قانون قديم لم يواكب الجرائم التي تفرض نفسها على الساحة الدولية و المحلية .

٢. ظهور أنواع جديدة من المجرمين : تحدثنا سابقاً عن صورة المجرم المعلوماتي التي تختلف كلياً عن تلك المعارف عليها للمجرمين التقليديين مما وجب على المشرع الأخذ بعن الاعتبار هذه التطورات .

٣.لناحية الملاحقة والتحقيق والمحاكمة : التي تزال في بلادنا دون أي تطور يذكر من أجل التغيرات الجذرية التي طرأت فجأة مما يجعلنا أكيدين أنه لا بد من تطوير التشريعات الجنائية قائمة لناحية التحقيق و المحاكمة كي تتماشى مع الطبيعة الخاصة للجرائم السيبرانية التي تتخطى حدود البلاد مما يجبر المشرع على تحديث القوانين من جهة والتأكيد على ضرورة تفعيل التعاون مع البلدان الأخرى للحد منها كون أن دولة وحدها لا تستطيع القيام بهذا الأمر فضلاً عن المساعدة القانونية و الفنية المتبادلة التي لا تزال تتسم بالبطئ و غياب الفعالية اللازمة، فالمشرع هو بصدد تجريمه لسلوك ما يضع في حساباته مصالح المجتمع محاولاً حمايتها بلغة العقوبة، فالجريمة المعلوماتية هي ضرب من ضروب السلوك الذي يأتيه الجاني يعتدي به على مصالح محمية [٢٤٤]، فكيف يمكن توقيع العقوبة على فعل لم ينص القانون على تجريمه , فتكون النتيجة أن المجرم يظل دون عقاب عملاً بقاعدة لا عقوبة و لا جريمة الاّ بنص في القانون، اذاً كي نحارب هذه الجرائم يجب توفير الحماية اللازمة لصالح الأفراد عبر وسائل التجريم والعقاب وبهدف تحقيق العدالة ايضاً، فالضحية التي الحقت أضرار جسيمة بها، سواء كانت معنوية ام مادية تنتظر من المشرع أن يعوض عليها عن طريقة معاقبة المجرم و اتخاذ التدابير اللازمة لاسترداد حقها أخيراً، فالقوانين المحلية مشّرعة منذ عقود طويلة و لم تواكب التطورات و المتغيرات مما حتمّ المعالجة التشريعية للجرائم الالكترونية التي اعتبرت من المواضيع المهمة في الأونة الأخيرة عبر ادخال سلسلة من التعديلات الخاصة على القوانين القائمة أو استحداث قوانين جديدة، كي تكون رادعاً لكل من سمح نفسه استخدام التكنولوجية

---

[٢٤٣] عدي محمد علي الشوابكة : " معوقات مكافحة الجرائم الالكترونية في المجتمع الاردني من نظر ذوي الاختصاص " , جامعة مؤتة، كلية العلوم الاجتماعية، أطروحة دكتوراه، ٢٠٢٢, ص ٣٣٥-٣٣٦

[٢٤٤] محروس نصار غايب : " الجريمة المعلوماتية " وجامعة الأنبار، المعهد التقني ,٢٠١٠، ص ٥-٦، متوافرة على الرابط التالي : https://www.iasj.net/iasj/download/5cd8d60110b50ba7

بطريقة خاطئة, مما يجعل من تطور المنظومة القانونية القائمة هي الحل للحؤول دون افلات المجرمين من العقاب , الاّ أنه بالرغم من هذه التحديات السيبرانية استطاعنا في الاونة الأخيرة الى وضع خارطة الطريق المتمثلة بالانجازات (في حال اردنا تسميتها هكذا) على الشكل التالي[٢٤٥] :

١. عام ٢٠٠٦ تم تأسيس مكتب مكافحة جرائم الملكية الفكرية و جرائم المعلوماتية في الشرطة القضائية في قوى الأمن الداخلي مختص بالتحقيق في كافة الخروقات و الاعتداءات السيبرانية و الجرائم المتعلقة بتكنولوجيا المعلومات.

٢.عام ٢٠١٠ تم انشاء لجنة وطنية لوضع تصور وطني حول الأمن السيبراني و مكافحة الجريمة السيبرانية تضم ممثلين عن الجهات الحكومية الأساسية و عن الأجهزة الأمنية .

٣.عام ٢٠١٨ تم صدق مجلس النواب اللبناني على القانون رقم ٨١ (قانون المعاملات الالكترونية) لناحية توضيح كيفية التعاطي مع الأدلة الرقمية و ضرورة المحافظة عليها .

٤.عام ٢٠١٩ تم وضع " الاستراتجية الوطنية اللبنانية للأمن السيبراني ", نحو عام ٢٠٢٢ يهدف لبنان الى أن يكون لديه قضاء سيبراني أكثر أماناً و استقراراً سواء في داخل الوطن او في التبادلات الدولية , مؤكدة على مسؤولية الدولة عن الأمن السيبراني .

٥. السعي الى تطوير البنى التحتية للاتصالات و المعلومات و ذلك من خلال الدور الذي تلعبه وزارة الاتصالات اللبنانية الى جانب هيئة أوجيرو و القطاع الخليوي و أيضاً التعاون مع الاتحاد الدولي للاتصالات من أجل تحقيق الأمن السيبراني .

٦.محاولة تطوير القطاع المصرفي من خلال الالتزام بالمعايير الدولية المصرفية من أجل احباط الهجمات السيبرانيةعن طريق :

- تحديث خارطة الطريق التي وضعها مصرف لبنان عن طريق اعداد ومتابعة سياسات امن المخاطر، اطلاق وتقييم برامج التوعية الأمنية .

-التشديد على أهمية الامن السيبراني المبني على الدفاع في العمق : حلول أمنية متعددة التقنيات يعطي البنى التحتية لأمن الشبكة و النقاط النهائية التي يمكن أن تجعل عملية الترقب والوقاية أولوية السلطات المختصة التي يتعامل مع أمن نظم المعلومات عبر انشاء " منصة الاستخبارات للتهديدات السيبرانية CIT و تهدف هذه المنصة الى تلقي البيانات بصورة متواصلة من كافة المصادر المحلية، وعمل هذه المنصة كنواة الفريق الوطني استجابة لطوارئ المعلوماتية CERT LB الذي يتم انشاؤه في كنف الوكالة الوطنية للأمن السيبراني و نظم المعلومات و يجب على فريق الاستجابة الوطني توفير تلقيمات البيانات و التنبيهات و الانذارات المبكرة و ما الى ذلك الى كافة مراكز خدمات امن المعلومات المحلية SOSs, فضلاً عن التنسيق مع كافة الأجهزة الوطنية المكلفة تطبيق القانون بالتعاون مع الجهات الدولية [٢٤٦].

---

[٢٤٥] الاستراتجية الوطنية اللبنانية للأمن السيبراني لعام ٢٠١٩ ، ص ١١ ، متوافرة على الرابط التالي :
http://studies.gov.lb/getattachment/Sectors/Information-Communications-Technology-Media/2019/It-19-2/It-19-2Ar.pdf

[٢٤٦] المرجع السابق، ص ٣٢

بعد أن انتهينا من توضيح الأسباب الجوهرية التي تستدعي تحديث القوانين القديمة لمواكبة تطور الجرائم الجديدة وكيفية ترجمة الحلول على أرض الواقع، سوف نبين أهم المعوقات القضائية الوطنية التي تعترض سير العدالية الجزائية في مسألة الحرب السيبرانية في الفرع الثاني من هذا المبحث.

الفرع الثاني : المعوقات القضائية

تتميز الجرائم السيبرانية و خاصةً الهجمات منها بالخصوصية التي تفرض أهمية تطوير أساليب التحقيق و جمع الأدلة و المحاكمة خاصةً أن هذه الأجراءات لا تزال تمارس ضمن طابعها التقليدي مما يتطلب الأمر ضرورة تطويرها كي تتلاءم مع هذه الخصوصية , ففي هذا المبحث سوف نبين ابرز المعوقات القضائية الوطنية التي تحّد من تحول دون توقيع العقاب على المجرم المعلوماتي وأبرز الحلول المتطورة التي تنقذ الموقف

أ - المعوقات القضائية تتمثل في الاجراءات الجزائية القديمة التي لم تواكب التطورات الجرمية وغياب دور المشرع في تحديث القوانين القائمة، فأي دعوى جزائية يجب أن تمر بعدة مراحل من أجل التوصل للنتيجة المرجوة و الأمر نفسه مطبق بالنسبة الى الدعوى الجزائية في الهجمات السيبرانية من أجل محاكمة المجرم وتوقيع العقاب عليه، فثلاث سلطات تقوم بمهام الملاحقة والتحقيق والمحاكمة في لبنان بحيث تتولى السلطة الأولى اقامة الدعوى وملاحقة المجرم, ثم تحال الدعوى الى سلطة ثانية ليحقق فيها ثم بدورها تحيل الملف الى سلطة ثالثة تتولى المحاكمة والحكم [٢٤٧]، أما اجراءات البحث والتحري في الهجمات السيبرانية لا تزال في وطننا هي الأساليب التقليدية للبحث والتحري في المعاينة والضبط والتفتيش والمراقبة والخبرة، فهذه الأساليب يعتبر من الصعب تطبيقها على الجرائم السيبرانية لناحية أسلوب ومكان إرتكاب الجرم , فهي دون جدوى في حال لم تواكب التطورات كون أن الجرائم ترتكب في الفضاء السيبراني و عن بعد بل هناك إجراءات وتقنيات حديثة تفي بالغرض وهي الإرشاد الجنائي والمراقبة الالكترونية والاختراق والترصّد الالكتروني[٢٤٨] و غيرها من الوسائل المتاحة :

- الإرشاد الجنائي : قيام رجال الشرطة بتجميع المعلومات والتقصي والكشف عن جرائم الانترنت من خلال دخول العناصر أو الغير للعالم الافتراضي بأسماء مستعارة بقصد البحث والتحري عن الجرائم ومرتكبيها وتقديمهم للمحاكمة .

---

[٢٤٧] رلى صفير : " الدعوى الجزائية وأبرز مراحلها "، مجلة الجيش اللبناني، العدد ٢١٣ ، ٢٠٠٣- متوفرة عبر الرابط التالي :
https://www.lebarmy.gov.lb/ar/taxonomy/term/317#:~:text=%D8%A7%D9%84%D8%AF%D8%B9%D9%88%D9%89%20%D8%A7%D9%84%D8%AC%D8%B2%D8%A7%D8%A6%D9%8A%D8%A9%20%D9%88%D8%A3%D8%A8%D8%B1%D8%B2%20%D9%85%D8%B1%D8%A7%D8%AD%D9%84%D9%87%D8%A7&text=%D8%A7%D9%84%D9%85%D9%84%D8%A7%D8%AD%D9%82%D8%A9%20%D9%85%D9%86%20%D8%A3%D8%AC%D9%84%20%D8%A7%D9%84%D8%B9%D9%82%D8%A7%D8%A8%20%D8%A7%D8%AA%D8%AE%D8%B0%D8%AA,%D8%B4%D8%B9%D8%A8%D9%87%D8%A7%20%D9%88%D8%A3%D8%B1%D8%A7%D8%B6%D9%8A%D9%87%D8%A7%2C%20%D8%AA%D9%85%D8%A7%D8%B1%D8%B3%D9%87%D8%A7...

[٢٤٨] غزالي لخضر : " التحريات المستحدثة في جرائم التكنولوجيا الحديثة " ،مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد الخامس، العدد الأول – ٢٠٢٠- ص ٩٧٤

- المراقبة الإلكترونية : عن طريق مراقبة الاتصالات باستخدام التقنية الإلكترونية لجمع المعلومات والبيانات التي تتم عن طريق الإنترنت كمراسلات البريد الالكتروني والترصد لإستعمال بطاقات الهوية الإلكترونية.

- الاختراق والترصد الإلكتروني : عن طريق دخول عناصر الشرطة الى داخل المواقع الاجرامية وترصدها لحين قيام المجرمين بأعمالهم الاجرامية، هذه التقنيات الحديثة في عملية الملاحقة نادراً ما تستخدم في بلادنا ولكن وبفضل خضوع رجال الشرطة الى دورات تدريبية أصبحوا استخدامها أسهل من الفترات الماضية.

- لناحية اجراءات الملاحقة : نشبر أيضاً أنه في مرحلة معاينة مسرح الجريمة يكون الأمر مختلفاً نوعاً ما بالنسبة الى الجرائم المعلوماتية مما يجب مراعاة ارشادات فنية معينة كتصوير الحاسوب و اثبات التوصيلات و عدم نقل مادة المعلوماتية من مسرح الجريمة، أما بالنسبة الى التفتيش لا بد من البحث في كافة المكونات المادية للحاسوب بطريقة معينة طالما انه لا يرد على مكونات مادية محسوسة مع الأخذ بعين الاعتبار الاجراءات الخاصة للتفتيش بطريقة تراعي امكانية اتلافها , فيتم تفتيش نظام الحاسوب او جزء منه أو المعلومات المخزنة فيه و وسائط التخزين و التفتيش في البيئة الرقمية , أما لناحية ضبط الادلة يتمثل هذا الاجراء في ضبط المكونات المادية لأنظمة الحاسوب و ضبط المكونات و البرمجيات و المعطيات التي تربط الحواسيب و ما يتصل بها من معدات مستعملة في الشبكة كجهاز المودم و وسائل تخزين البيانات و المعطيات , بالنسبة للخبرة لا بدّ من تكليف خبيراً مختصاً في المعلوماتية كي يتمكن من اجراء تحقيقات و استقصاءات معينة والأمر نفسه بالنسبة الى مرحلة الاستجواب التي تحتم الجهة الموكلة بالاستجواب أن تكون على دراية بالأمر ومتأقلمة مع هذا النوع من الجرائم وأيضاً بالنسبة للشهود.

ب- الفراغ القانوني المحلي في مسألة الهجمات السيبرانية

- لناحية اجراءات التحقيق والمحاكمة والتشريع : تحدثنا مراراً وتكرارً عن هذه المسالة ولكن ما يختص في هذا الفصل هو صعوبة الأمر وإنعكاسه على قضاة الحكم في التطرق الى هذه الجرائم المعقدة بحيث يعتبروا غير قادرين على التأقلم مع المفردات الخاصة بالجريمة المعلوماتية وذلك بسبب غياب التشريع في هذه الجرائم بالرغم من التحسن الذي لوحظ في الاونة الاخيرة لقضاة حولوا البحث في هذه الأخيرة، وهذا الإطار بين عامين ٢٠١٨ و ٢٠١٩ في اطار مشروع "Cybersouth "الذي ينظمه مجلس أوروبا سعت وزارة العدل الى تدريب حوالي ٢٠ قاضياً على طرق مواجهة جرائم الانترنت [٢٤٩]ولكننا لا زلنا بعيدين كل البعد عن الوضع الجيد التي توصلت اليه الدول المتقدمة في معاقبة الهجمات والتحكم بها، فالقاضي الوطني الذي لم يتمرس في هكذا نوع من الجرائم أن يعرض عليه واقع جديد وخاصةً أن المشرع اللبناني لم ينظم الهجمات السيبرانية حتى الآن فيصبح مكتوف الأيدي في غمكانية تكييف الجرائم المستحدثة ضمن نظام قانوني قديم .

فالصعوبة تكمن من المراحل الأولى للمحاكمة وذلك بسبب صعوبة تكيف رجال الأمن مع نوعية المجرمين الجديدة و كيفية التعامل معهم، أيضاً في مراحل التفتيش والبحث والتحري وجمع الأدلة وغيرها من اساليب الملاحقة وصولاً الى مرحلة التحقيق التي تلزم الجهة المخولة للتحقيق مع المشتبه بهم أن تكون على اطلاع كبير في كافة جوانب هذا الهجوم خاصةً في حال كان من الضروري القيام ببعض الأعمال الإجرائية خارج

[٢٤٩] الاستراتجية الوطنية اللبنانية للأمن السيبراني لعام ٢٠١٩ ،مرجع سابق، ص ١١ ,١٢

اقليم الدولة استكمالاً للتحقيق مما يحتم خضوع القضاة المنوطة بالتحقيق الى تدريبات مكثفة للحصول على المعلومات الكافية حول هذه الهجمات وكيفية التعامل معها بهدف تحقيق السرعة والفعالية في اجراءات الملاحقة، أما لناحية المحاكمة فيأتي هنا دور المشرع في تطويرالقوانين كي يستطيع القاضي مواكبة الجرائم الحديثة وفرض عقوبة مناسبة لكل جرم سيبراني .

لقد انتهينا من هذا الفصل محددين دور المشرع المحلي في الحد من الهجمات السيبرانية عن طريق تشريع قوانين جديدة أو تطوير القوانين القائمة أذا كان من الممكن القيام بذلك، واضعين حلول لكل معضلة يمكن أن تعترض سير العدالة من أجل تحقيق الامن والسلام في الفضاء السيبراني، سوف نحدد في الفصل الأخير من هذا البحث أهمية التدريب والتعاون في مجال مكافحة الهجمات السيبرانية .

الفصل الثاني : الصعوبات المحلية في مجال التعاون والتدريب وسبل الحل

يجد لبنان نفسه في خضم معركة سيبرانية قائمة نتيجة التقدم التكنولوجي والتقني في العالم و لا يستطيع الاعتماد على امكانياته السيبرانية المتواضعة دون اللجوء الى تعاون دولي و محلي في مجال التوصل الى الحد من الهجمات والتهديدات السيبرانية المتنامية بالاضافة الى تهيئة الأرضية السيبرانية الوطنية كي تعتبر البلاد قادرة على الدفاع عن نظم المعلومات بقوة، ولكن المحاولات الخجولة في هذا المجال غير كافية للتصدي والردع.

فنقاط الضعف كثيرةٌ مقارنةً مع نقاط القوة التي تمتلكها الدولة والقطاع الخاص معاً، والصعوبات التي تعترض تحقيق الأمن السيبراني في البلاد كثيرة لناحية ضعف المبادرات والجهود في مجال التدريب التقني والفني بالاضافة الى غياب التعاون بين القطاعين العام والخاص وذلك بسبب تحمل هذا الأخير المصاعب الموجهة اليه من القطاع العام التي تفوق قدرة تحمله في بعض الأحيان او لضعف الإمكانيات المتوافرة لديه في مجال التصدي للهجمات فضلاً عن ضعف التعاون بين المؤسسات والإدارات المحلية كون أن كل منها يعتمد على تأمين سيبراني مختلف عن تلك المتبعة في المؤسسة الأخرى.

اذاً كي تكون الدولة قادرة على مواجهة التهديدات والأنشطة السيبرانية الخبيثة لا بدّ من تعزيز التعاون بين القطاعات من جهة ووضع استراتجية متطورة في مجال تدريب الموظفين وتحسين قدراتهم السيبرانية من جهة أخرى، وهذا ما سوف نوضحه في هذا الفصل محددين الصعوبات المحلية في مجالي التعاون والتدريب وسبل الحل، ففي المبحث الأول سوف نوضح الرؤية السيبرانية المقترحة للبنان وفي المبحث الثاني سنبرز أهمية التدريب والوعي على مواجهة تهديدات المهاجمين .

المبحث الأول : الرؤية المحلية المقترحة

تعاني الدولة من صعوباتٍ كثيرةٍ تقوض أمكانياتها المتواضعة في التصدي لأي تهديدات سيبرانية محتملة، فمؤسساتها ومرافقها وشركاتها غير قادرة على مواجهة هجمات سيبرانية، ولا يمكننا التغلب على الصعوبات المحلية سوى بالتعاون والتكاتف بين الأجهزة العامة والخاصة،وهذا ما سوف نوضحه في المبحث الحالي، ففي الفرع الأول سوف نعالج التعاون السيبراني بين الدولة والقطاع الخاص، وفي الفرع الثاني سوف نبين كيفية بناء ثقة الدول الأخرى بالمنتجات السيبرانية اللبنانية.

الفرع الأول : التعاون السيبراني بين الدولة والقطاع الخاص

ان كيانات القطاع الخاص تكون غالباً أهدافاً للهجمات والعمليات السيبرانية المعادية ويعتقد أم أكثر من ٧٠٪ من الهجمات السيبرانية توجه ضد القطاعات الخاصة سواء كانت الصناعية أم الصحية أم الخدماتية، المعلوماتية والمالية، أيضا إعتبر البعض أن ثمة صلة مهمة أخرى هي أن أدوات ومكونات الفضاء السيبراني يجري تطويرها وبناؤها وتشغيلها وإمتلاكها من قبل كيانات او شركات للقطاع الخاص تقدم سلعاً وخدمات متصلة بتكنولوجيا المعلومات [٢٥٠] .

ففي بعض الأحيان يكون القطاع الخاص هو منفذاً للعمليات السيبرانية الهجومية وذلك بسبب إمتلاكه للوسائل والطرق الكافية لتنفيذ مثل هكذا هجوم وذلك بالإتفاق مع القطاع العام المحلي أو أحد الأجهزة الخارجية، بمعنى أخر ان القطاع الخاص يمكن أن يتعاون مع الدولة من أجل مواجهة هجمات سيبرانية موجهة من مصدر خارجي أم أن يعقد صفقة مع طرف داخلي أم خارجي من أجل تنفيذ هجوم سيبراني ضد مصلحة البلاد ومقابل مبلغ معين أو ميزة معينة .

أحياناً قد يكون التعاون بين القطاعين العام والخاص ضرورياً من أجل تسيير العمليات السيبرانية الدفاعية ضد الخصوم : كتعاون كيان مسالم يقدم خدمات الإنترنت لإطلاق هجوم سيبراني عبر شبكة الإنترنت الى العدو وقد يسمح أحياناً للقطاع الخاص في المشاركة مع القوات العسكرية مثلاً من أجل الرد على هجوم سيبراني وذلك بسبب إمتلاكه للوسائل والتقنيات المتطورة اللازمة لمواجهة مثل هكذا هجوم، مما يسمح له بتنفيذ هذا الهجوم انطلاقاً من أسباب معينة، ففي الولايات المتحدة الأمركية تستخدم القطاعات العامة والخاصة البنى التحتية بدرجة كبيرة و جزء كبير من المراسلات العسكرية الأميركية تنتقل عبر شبكات مملوكة للقطاع الخاص ويجري تشغيلها في معظمها لمنفعة مستخدمين مدنيين [٢٥١] وكذلك الأمر بالنسبة شبكات الكهرباء، الطاقة والمياه وغيرها مما يجعل البنى التحتية عرضة للعمليات العدائية .

في أغلب الأوقات يساند القطاع الخاص المرافق العامة والعسكرية خاصةً في مجال التصدي للهجمات السيبرانية ويحتاج القطاع العام خاصةً في بلادنا الى المساعدة التقنية والعلمية الضرورية وذلك لأن النظم المالية والاقتصادية والعسكرية ليست جاهزة بعد للتعامل مع الهجمات السيبرانية، وخاصةُ أن العمل

---

[٢٥٠] هربرت لين : " النزاع السيبراني والقانون الدولي الانساني "، مختارات من المجلة الدولية للصليب الأحمر، مجلد ٩٤، ٢٠١٢، ص ٥٢٧-٥٢٨

[٢٥١] هربرت لين، مرجع سابق، ص ٥٢٨

المشترك بين القطاعين العام والخاص هو الحل الأنسب، فان زيادة تبادل المعلومات بشأن التهديدات والهجمات والاستجابات بينهما يؤدي الى تعزيز القدرة على الردع والإستجابة بشكل أكبر [٢٥٢] .

الاّ أننا نواجه حواجز كبيرة تعيق عملية التعاون بين هاذين القطاعين يتمثل في قوانين حماية البيانات والمعلومات الخاصة بالعملاء التي يمنع ان يتم الكشف عنها للقطاع الخاص مما يصعب العملية وذلك لأن إتخاذ الوضعية الدفاعية الكافية في الفضاء السيبراني يستلزم ان يتحقق القطاع الخاص من هوية المستخدمين، ولكن على نحو أخر يجعل السلوكيات والتصرفات التي تصدر عن شخص مجهول أمراً مستحيلاً، وخاصةً أولئك المجرمون اللذين يحاولون الوصول الى أرقام بطاقات الائتمان واختراق المواقع الالكترونية الخاصة بالبنوك للكشف عن هوية العملاء وسرقة أموالهم، ومن المتفق عليه عالمياً أنه وجب على الأجهزة الرقابية والبنوك المركزية أن تضع بروتوكولات وممارسات لتبادل المعلومات من شأنها العمل بفعالية في ظل هذه القيود ومن الممكن أيضاً تخفيض الحواجز القائمة من خلال نموذج متفق عليه عالمياً لتبادل المعلومات وزيادة إستخدام منصات المعلومات المشتركة وتوسيع الشبكات التي تحظى بالثقة، وذلك في إطار تطوير التعاون بين القطاعين .

وعلى نحو آخر نشير أن القطاع الخاص هو المستهدف ولا بدّ من منحه كافة الوسائل اللاّزمة لحماية نفسه من الهجمات الخطيرة التي تضعف وجوده وكيانه وهذه الوسائل يمكن توفيرها من خلال تعاونه مع الدولة من جهة والمنظمات الدولية من جهة أخرى من أجل مساعدته على بناء قدراته في مجال الأمن السيبراني، وخاصةً المؤسسات الصغيرة والمتوسطة التي تحتاج الى مساندة حقيقية بسبب وجود عدد كبير من المؤسسات العامة غير قادرة على مواجهة مخاطر الهجمات السيبرانية لأسباب مادية بحتة .

أما بالنسبة الى كيفية تعزيز التعاون بين القطاعين تتمثل في :

- تطوير الشراكات بينهما عن طريق اعتبار هذا التعاون كوسيلة مناسبة لمعالجة التهديدات الأمنية التقليدية وغير التقليدية، ومن المساعدات التي يمكن أن تقدمها الدولة للقطاع الخاص هي الحوافز المالية من أجل تطوير قدراتها في مجال الأمن السيبراني كي تصبح قادرة على مواجهة المخاطر السيبرانية المحتملة و في عام ٢٠١٨ نشر المنتدى الإقتصادي العالميWEF دليل المرونة السيبرانية للتعاون بين القطاعين العام والخاص :هو عبارة عن أداة تهدف لتقديم إرشادات للتعاون بين القطاعين العام والخاص داخل الدول حول اعداد سياسية الأمن السيبراني، يتطرق القسم من الدليل، على وجه الخصوص، إلى الحاجة لتأسيس إطار عمل وطني واضح للحوكمة السيبرانية، بما في ذلك الأدوار والمسؤوليات والقدرات المتوقعة من القطاعين الحكومي والخاص[٢٥٣].

---

[٢٥٢] جنيفر اليوت و نايجل جنكينسون : " المخاطر السيبرانية...التهديد الجديد للاستقرار المالي " مقال منشور على موقع مجلة IMF في ٧-١٢-٢٠٢٠, متوفرة على الرابط التالي :
https://www.imf.org/ar/Blogs/Articles/2020/12/07/blog-cyber-risk-is-the-new-threat-to-financial-stability

[٢٥٣] ميليسا هاثاواي : " إدارة الخطر السيبراني الوطني" , مقال منشور على موقع potomacinstitute , متوفر على الرابط التالي : https://potomacinstitute.org/images/CRI/Managing-National-Cyber-Risks_FINAL-Arabic.pdf

- التواصل المستمر بين القطاعين العام والخاص : يجب على الحكومة أن تكون شفافة بشأن التهديدات السيبرانية التي يمكن أن تتعرض لها كي يتسنى على الشركات المختصة تطوير الحلول التي تناسب هذه التهديدات وذلك من خلال اتباع النهج الوقائي الذي يساهم في توفير الوقت الذي يحتاجونه لمعالجة أي مشاكل محتملة قبل أن تقع مشكلة حقيقية .

- تعزيز الثقة بين القطاعين وذلك لأن الحكومة سوف تتردد في الكشف عن معلومات حساسة متعلقة بأمن البلاد داخل القطاع الخاص ولكن لا يوجد طريق للتخلص من هذه التهديدات سوى الحصول على المساندة من القطاع الخاص وخاصةً الشركات السيبرانية المختصة، فضلا عن إستفادة كل من القطاعين بشكل كبير من هذا التعاون في مجال أمن المعلومات .

- تعرف الحكومة على القضايا الفريدة التي يواجهها القطاع الخاص كما أن هذا الأخير سوف يتمكن من الوصول الى معلومات مفصلة (التي تعطيه اياها الحكومة) التي تساعده في كيفية تقوية شبكاته[٢٥٤] .

- فقدان القطاع العام الى إطار تنظيمي في مجال الأمن السيبراني بالإضافة الى النقص في الخبرات والتقنيات وضعف الأقسام الخاصة بتكنولوجيا المعلومات الموجودة لديه دفعه الى الاعتماد كلياً على القطاعات الخاصة من أجل توفير وتأمين خدمات تكنولوجيا المعلومات مما اضعف هذا التعاون وخاصةً أن القطاع الخاص لم ينجح في تسليم المشاريع الذي طلبها منه القطاع العام، فنجد أن المسؤوليات الملقاة على عاتق القطاع الخاص متمثلة بالأمور التالية :

- حماية الأصول والبيانات الرقمية التي تحتفظ بها القطاعات المختلفة.

-الحفاظ على الخدمات التي تقوم بتقديمها الشركات والمؤسسات وتوفير المستوى المناسب من الأمان في المنتجات التي تقوم ببيعها الى المستهلكين .

- العمل مع الوكالة الوطنية للأمن السيبراني ونظم المعلومات على تسهيل عملية نقل المعرفة المكتسبة لديها الى القطاع العام .

- دمج معايير الأمن في اختيار المنتجات والخدمات الرقمية في عمليات العامة [٢٥٥].

اذاً لقد وضحنا أهمية التعاون بين القطاعين العام والخاص في مكافحة الهجمات السيبرانية وكيف يكملان بعضهما البعض من أجل درء المخاطر التي تهددهما من أجل التوصل الى تحقيق الأمن والإستقرار السيبراني.

سوف ننتقل الى المبحث الثاني من أجل تحديد كيفية بناء ثقة الشركات والمؤسسات المحلية والخارجية بالخدمات السيبرانية المحلية .

---

[٢٥٤] Rizwan Virani :" The Fight Against Cyberthreaths requires a public- private partnership, here's how to get it done " , available on : www.securitymagazine.com

[٢٥٥] الاستراتجية الوطنية اللبنانية للأمن السيبراني لعام ٢٠١٩، مرجع سابق، ص ٣١

الفرع الثاني : منهجية بناء الثقة بالخدمات السيبرانية المحلية

ان الشركات التي تقدم منتجات وخدمات الأمن السيبراني نادرة جداً مما يلقي على عاتق الدولة ضرورة ملحة في تطوير بيئة مؤاتية رقمية تعمل على الترويج على المستوى الدولي والمحلي للمنتجات والخدمات الرقمية، مما يحفز ضرورة وجود تعاون جدي بين دوائر الصناعة والحكومة والتي تتمثل في مساعدتها على تنمية قدراتها السيبرانية، في ظل إرتفاع التكاليف السيبرانية لتأمين المؤسسات والشركات الصغيرة والمتوسطة، فالدولة تتجه في بعض الأحيان الى الشركات الخارجية من أجل حصولها على المنتجات السيبرانية بدلاً من انتاجها محلياً وتصديرها للخارج وخاصةً أن في لبنان كافة المؤهلات والكفاءات العلمية اللاّزمة للقيام بهكذا توجه، فلا بدّ من تطوير وتعزيز المنتجات الوطنية من منتجات وخدمات وحلول أمنية سيبرانية وذلك بالتضامن مع الوزارات والإدارات المختلفة(الاتصالات، الاقتصاد، الداخلية، الدفاع، الشؤون الخارجية، مكتب وزير الدولة لشؤون التنمية الادارية..الخ). ففي لبنان الكثير من الشركات لديها القدرة على تطوير الحاجات السيبرانية وإنتاجها، فيبقى فقط من أجل تنمية هذه الصناعة تعزيز التعاون بين القطاعين وتمويل الدولة لمشاريع انتاج الخدمات السيبرانية، مما يجعل الدولة قادرة على التخلي عن المساعدة الخارجية وخاصة أن حصولها على المنتجات السيبرانية من الخارج أمرُ باهظُ نسبياً والإعتماد على الصناعة الوطنية الأقل كلفة [٢٥٦] .

من الأهداف أيضاً لهذا التعاون هو مساعدة المؤسسات الصناعية الجديدة التي تعمل في مجال تطوير و صناعة الأمن السيبراني على الانطلاق لتصبح قادرة على منافسة الشركات المهمة، كذلك الأمر بالنسبة للمؤسسات التي لا تستطيع تحمل تكاليف الأمن السيبراني من أجل حماية نظم معلوماتها، تتلقى المساعدة المالية من الدولة، واخضاع الموظفين من الشركات والمؤسسات الى دورات تدريبية بالتعاون مع المؤسسات الأكاديمية التي تعنى بشؤون الأمن السيبراني سواء كانت محلية أم خارجية وذلك بغية سدّ الإحتياجات السيبرانية في القطاعين العام والخاص، خاصةً أن القطاع العام بحاجة الى مساندة الشركات الخاصة وتزويدها بالتقنيات اللازمة للنهوض السيبراني .

ايضاً التسويق للمنتجات اللبنانية السيبرانية من أجل تعزيز من قدرتها التنافسية في الخارج وفي الوقت نفسه دعم الشركات اللبنانية السيبرانية كي تتميز اقليمياً ودولياً ومساعدة الشركات اللبنانية عن طريق تطوير إجراءات التصدير للحلول المقدمة منها ووضع خطة عمل جدية تساهم في تحسين وتشجيع منتجات الأمن السيبراني المحلية، ايضاً شراء المعدات السيبرانية الخاصة الضرورية من أجل الكشف عن التهديدات والهجمات السيبرانية والعمل مع المؤسسات المختصة على تطوير منتجات محلية منافسة .

- التعاون مع دوائر الصناعة المحلية أمرُ أساسيُ وضروريُ من أجل الحفاظ على بيئةٍ سيبرانيةٍ أمنةٍ عبر اتخاذ تدابير الوقاية المطلوبة فضلاً عن مساعدة المؤسسات الصناعية السيبرانية على تطوير إمكانياتها وقدرتها التنافسية على مواجهة الشركات الكبرى وخاصة أن هنالك شركات غير قادرة على حماية أنظمة معلوماتها الأساسية وتحصين امكانياتها من أجل مقاومة الهجمات السيبرانية التي يمكن أن تتعرض لها وذلك بسبب التكاليف الباهظة لنظم الأمن السيبراني ولكن مع مساعدة الدولة تصبح قادرة أن تمارس نشاطها المعتاد بأمان، بل تصبح أنظمتها هدفاً ضعيفاً للمهاجمين السيبرانين من خلال منظومة الدفاع الإستباقي،

[٢٥٦] الاستراتجية الوطنية اللبنانية للأمن السيبراني لعام ٢٠١٩، مرجع سابق، ص ٢٩

فقدرات الردع موثوقة ومقنعة وكل ذلك لا جدوى منه الاّ بوجود تعاون حقيقي وبنّاء عبر تحديث القوانين القائمة من جهة وإنشاء آليات تعاون مشتركة لادارة الأزمات من جهة أخرى ، مما يؤدي الى نهوض الدولة والقطاع الصناعي معاً، فأهمية أخضاع المواطنين والموطفين في القطاعات العامة والخاصة للتدريب أمرُ ضروريُ على مواجهة الهجمات السيبرانية وهذا ما سوف نوضحه في المبحث اللاحق .

المبحث الثاني : أهمية التوعية والتدريب

إن أي سياسة سيبرانية لا تتمع بالقوة اللازمة في حال لم يتم تأهيل الموظفين وتدريبهم على إكتشاف التهديدات السيبرانية والتعامل معها بالطريقة المناسبة من أجل حماية الأنظمة الإلكترونية من أي إعتداء يمكن أن يلحق الأضرار بها وعلى هذا الأساسي سوف نبين في المبحث الحالي ضرورة إخضاع الموظفين والعاملين وسائر الأفراد لتدريبات سيبرانية مكثفة من أجل تكييفهم مع الهجمات السيبرانية (الفرع الأول)، فضلاً عن طرق أخرى لنشر الوعي السيبراني(الفرع الثاني) .

الفرع الأول: بناء القدرات والمساعدة الفنية السيبرانية

يعدّ التدريب جزءاً مهماً في إطار التنمية السيبرانية الإدارية في الكثير من المؤسسات العامة والخاصة وأهم الأدوات الأساسية الفعاّلة لرفع مستوى كفاءة وأداء وإنتاجية الموظفين، وذلك من خلال إخضاعهم لدورات تدريبية تهدف الى تطوير قدراتهم في الكشف عن الجرائم السيرانية التي نفذت او تلك التي لا تزال في طور التنفيذ من خلال فريق متخصص في الأمن السيبراني قادر على الإستجابة بسرعة مع أي حدثٍ أمنيٍ طارئٍ بالإضافة الى تدريب الموظفين الموجودين كي يصبحوا قادرين على إلمام بالظواهر المستحدثة وقدرتهم على مواجهتهم لها، هذا بالنسبة الى الشركات والمؤسسات الخاصة.

بالنسبة الى عناصر الضابطة العدلية ورجال التحقيق يكون الهدف هو إخضاعهم لدورات خاصة من أجل تطوير قدراتهم في التعامل مع الجرائم الحديثة عن طريق إكتسابهم خبرة فنية في هذا المجال مع مراعاة كافة العناصر الشخصية للمتدرب من حيث مستواه العلمي وقدرته الذهنية والنفسية ومدى إستعابه وإستعداده لإكتساب معلومات وخبرات جديدة من خلال منهج تدريبي مهّم لمواجهة الهجمات السيبرانية الذي يختلف

كثيراً عن تلك المتعارف عليها قديماً، على أن يشتمل هذا المنهج، مجموعة من العناصر كالتالي : بيان المخاطر والتهديدات ونقاط ضعف المؤسسة، الأماكن التي يمكن أن تتم من خلالها إختراق شبكة المعلومات وأجهزة الحاسب الآلي، الثغرات الفنية التي يمكن أن يستغلها المهاجم، تحديد ماهية التعابيرالخاصة بالهجمات السيبرانية وأنماط إرتكاب الجرائم السيبرانية، الصفات التي يتميز بها المجرم المعلوماتي والدافع وراء إرتكاب هذه الجرائم [٢٥٧]، لكن لماذا نشددّ على ضرورة إخضاع الموظفين العاملين في القطاع العام أم الخاص الى دورات تدريبية في مجال الهجمات السيبرانية؟

[٢٥٧] عبدالله العازمي، مرجع سابق، ص ٦٠٤-٦٠٥

يجب أن نشير أنه من أهم المعوقات التي تحول دون تحقيق العدالة في مجال الهجمات السيبرانية يعود الى أسباب متعلقة بالملاحقة والتحقيق الجنائي، فنقص المهارة المطلوبة الفنية لملاحقة هذه الجرائم وطريقة التعامل مع الأدلة المعلوماتية التي تختلف كثيراً عن تلك التقليدية مع طريقة المحافظة عليها، والتحقيق في هذه الجرائم وخاصةً في إستخدام الحاسب الآلي وشبكة الإنترنت فضلاً عن غياب شبه كلي للخبرة المطلوبة في مجال التحقيق في جرائم المعلوماتية وقلة البرامج والأدوات الفنية المتخصصة للمساعدة في عملية التحقيق الجنائي، وعدم المام الموظفين المولجين بالتحقيق كيفية التعامل مع نوعية المجرمين المعلوماتيين، وكيفية استخدام جهاز الحاسب الألي والخوف من إستخدامه .

فكافة هذه الأسباب أعلاه تحتم خضوع العاملين في الوحدات الخاصة بجرائم المعلوماتية للتدريبات المكثفة وتأهيلهم وفق أهم وأحدث البرامج التي تستخدم في هذا المجال وحتى التعاون مع فريق أجنبي مختص من أجل تطوير مهارات البحث والملاحقة والتحقيق في الجرائم المعلوماتية، وهنا يبرز دور القطاع الخاص والمنظمات الحكومية وغير الحكومية الى جانب الدولة في تخصيص مبالغ معينة للدورات التدريبية للموظفين من أجل التوصل الى السيطرة على النقص في عدد الخبراء المختصين بالأمن السيبراني وخاصةً أن بلادنا تفتقد للكثير من التدريبات الخاصة للموظفين وهؤلاء بعيدين كل البعد عن الحال الذي وصلت اليه الدول المتقدمة في مجال توافر المهارات والقدرات البشرية على السيطرة والتعامل مع الهجمات السيبرانية وتحقيق السلام في الفضاء السيبراني.

من ناحية أخرى نشير مثلاً أن المدارس والجامعات من أهم الأهداف السيبرانية الموضوعة من قبل المهاجمين وذلك للأسباب التالية :

١. لم ينفق القطاع التربية والتعليم النفقات الضرورية على الأمن السيبراني داخل المدارس والثانويات والجامعات على النحو الذي قامت به الشركات الكبرى .

٢. المعلومات الشخصية الضخمة العائدة للطلبة التي المخزنة ألكترونياً والتي تكون عرضة للهجمات السيبرانية، ومن هذه المعلومات : الهوية الشخصية،أرقام بطاقات الإئتمان العائدة للطلبة والمدرسين،عنوان السكن، المعلومات الشخصية العائدة لأهالي التلاميذ،أرقام الهواتف ،البريد الإلكتروني...إلخ.

٣. يعتبر هذا القطاع الأكثر عرضى لهجمات التصيد الإحتيالي بسبب الثغرات الكثيرة المتوافرة داخل الأنظمة الإلكترونية والنقاط الضعف البشرية،كون أن الموظفين غير مؤهلين للتعامل مع التهديدات السيبرانية .

٤. تخزين المعلومات على عدة أجهزة بدلاً من جهاز مركزي واحد.

ما يهمنا هو الدور الذي يقوم به التدريب المهني للموظفين في القطاع التربوي على التصدي للهجمات السيبرانية ولماذا يعتبر عاملاً مهماً في فشل الهجوم السيبرانية؟

إن الموظفين الغير مؤهلين للتعامل مع أجهزة الكمبيوتر والتكنولوجيا يساهمون في تنامي الهجمات السيبرانية وتحقيق المهاجمون نجاحات مهمة في هذا الإطار للأسباب التالية :

أ- غياب التدريب المهني والأمني عن القطاع التربوي :أشارات الدراسات أن ٥٦٪ من الموظفين لا يحصلون على أي تدريب مهني طوال فترة عملهم .

ب- صعوبة التعامل مع التهديدات السيبرانية التي تواجه الموظفين الذين غالباً يقدمون المساعدة عن طريق الخطأ للمهاجم من خلال القيام ببعض الأعمال الغير مناسبة التي تسهل على المهاجم الدخول الى الأنظمة السرية.

ج- غياب السياسات الأمنية الصارمة التي تضعف إمكانية تعرضها للهجمات السيبرانية.

إنطلاقاً من الأسباب المبينة أعلاه، يجب التركيز على الجانب البشري من خلال خلق ثقافة أمن المعلومات لديهم عن طريق خضوعهم لدورات تدريبية، فالموظفين لا يستطيعون التصدي للتهديدات السيبرانية الاّ في حال كانوا على إلمام بها وإن أي موظف سياسات أمن المعلومات يعرض مؤسسته الى خطر الهجمات السيبرانية .

من أجل التوصل الى هذه الأهداف أعلاه والى جانب تطوير القدرات الفنية تبرز أهمية نشر الثقافة السيبرانية من أجل توعية المواطنين ايضاً على المخاطر السيبرانية التي من الممكن أن يتعرضوا لها وتفقدهم معلوماتهم و بياناتهم الشخصية وأموالهم في الفرع الثاني من هذا المبحث .

الفرع الثاني : التعاون بين الدولة والمجتمع المدني حول نشر الثقافة السيبرانية

قبل البحث في مسألة التعاون بين الدولة والمجتمع المدني حول نشر الثقافة السيبرانية سوف نوضح بدايةً بعض المفاهيم المتعلقة بهذا الموضوع .

الثقافة السيبرانية أم الرقمية هي آلية عمل تكنولوجيا المعلومات والإنترنت في تشكيل الطريقة التي يتفاعل بها مع هذه التكنولوجيا وإستخدامها في حياتهم العملية والشخصية، اذ تشمل الطرق والتقنيات والوسائط الجديدة التي يمكن استخدامها لأداء المهام المطلوبة " [٢٥٨]، أيضاً عرّف جينان بادج المحلل الرئيسي في شركة Forrester Research، ثقافة الأمن السيبراني بأنها " بيئة عمل يكون فيها كل شخص متحمسًا للأمن السيبراني ومتحمسًا لجعله أفضل؛ ويساعد الناس على فهم أهمية الأمن السيبراني؛ ويرون أنفسهم

جزءًا من الحل" ، والى جانب الدور التي تقوم به الدولة في محاولة منها للحدّ من الهجمات السيبرانية يبرز دور المجتمع المدني الى جانبها عن طريق نشر الثقافة والوعي السيبراني، ولكن لماذا ننظر الى الثقافة السيبرانية كمحطة أساسية في مجال مواجهة الهجمات السيبرانية ؟

ان الوعي الأمني والمعرفة بالتهديدات السيبرانية يمكن أن تقلص نسبة تعرض الأفراد والشركات والمؤسسات للهجمات والمخاطر السيبرانية، فالوعي والثقافة أهم عاملين في رحلة الحدّ من الهجمات السيبرانية، فيكونوا الأفراد على دراية بالمخاطر التي من الممكن التعرض لها وأبرز الحلول التي من الممكن اللجوء اليها للحد من الهجوم الذي يكون في طور الشروع او الذي لا يزال ينفذ، فموضوع الوعي هو من أهم المسائل المتعلقة بالأمن السيبراني وجزءاً اساسياً من الإستراتجية الموضوعة من قبل الدولة ولكن أحياناً لا تستطيع الدولة مواجهة المخاطر بمفردها بل تحتاج الى المجتمع المدني كداعماً اساسياً لها في عملية نشر الثقافة والوعي لدى الأفراد بالتحديد كي بصبحوا أكثر قدرة على مواجهة هذه الهجمات والتعرف

[٢٥٨] مقال منشور على الموقع التالي : www.islamonline.net

اليها، فالمواطنون عندما يتسلحون بالعلم والوعي والثقافة يستطيعون التعرف الى أي نشاط غريب يمكن أن يواجههم وكيفية حماية أنفسهم منه.

بالعودة الى دور المجتمع المدني في مساعدة الدولة على نشر الثقافة والوعي السيبراني من خلال :

- تفعيل التعاون بين وزارة التربية والتعليم العالي والجهات الفاعلة ذات الصلة في مؤسسات القطاع الخاص و النقابات العمالية من أجل القيام بدورات تدريبية مستمرة ومهمة من أجل تثقيف الموظفين حول ماهية الهجمات السيبرانية وكيفية التعامل معها .

- تطوير أساليب المشاركة بين الدولة والمؤسسات التعليمية (المدارس والجامعات والمهنيات الرسمية والخاصة) من أجل إدخال الأمن السيبراني ضمن المناهج التعليمية وإجراء أنشطة مبتكرة ومحفزة تساعد قدر الإمكان توضيح الأفكار السيبرانية الغامضة وإقامة مباريات أكاديمية في هذا المجال .

- التعاون مع الجهات المختصة من أجل تطوير قدرات الموظفين في الادارات العامة لناحية التأقلم مع المفاهيم المختصة بالهجمات السيبرانية من أجل تحقيق الأمن السيبراني كي تصبح متناسبة مع تلك الموجودة في القطاع الخاص.

- سعي النقابات العمالية الى التعاون مع الدولة من أجل الحصول على التمويل اللازم والضروري للقيام بدورات تدريبية للطلاب والعاملين في الجمعيات والنقابات وغيرها فيما يختص بالاستثمار الامن لتكنولوجيا المعلومات والإتصالات وخدماتها وفي الإستفادة من خبرة المختصين في مجال الأمن السيبراني .

- دور المجتمع المدني الى جانب الدولة في رفع مستوى الوعي السيبراني وتجنب المخاطر السيبرانية وتقليل أثارها وإصدار تنبيهات للثغرات التي يمكن أن تشوب أجهزتنا عبر إطلاق حملات وبرامج توعوية بالتعاون مع المراكز الإرشادية .

- تعليم المواطنين حول كيفية حماية أنفسهم من الهجمات السيبرانية بأقل كلفة ممكنة و بطريقة مبسطة و سهلة جداً(عن طريق مثلاً نشر فيديوهات مخصصة لشرح كيفية تحميل برامج الأمن السيبراني او برامج مختصة لمكافحة البرمجيات الضارة و الفيروسات) و يستطيع الكافة استخدامها.

- تضمين شرح مفصل للطلبة حول مخاطر ارسال المعلومات شخصية للغير دون التأكد من هوية هذا الأخير لتجنب الاصابة باي فيروس و لتجنب التعرض للابتزاز الإلكتروني .

- تشجيع الشباب للإحتراف في مجال الأمن السيبراني عن طريق إدخال هذا الإختصاص ضمن البرامج التعليمية الجامعية الذي يؤدي تلقائياً الى رفع القدرات الرقمية الوطنية .

-المناقشة مع الدولة حول امكانية الحصول على التمويل اللازم لتأسيس مراكز ومؤسسات معنية بالأمن السيبراني (أي إمكانية تصنيع خدمات سيبرانية محلية للتخلي عن استرادها من الخارج والبدء بتصديرها).

-التقييم المستمر للجهود التي تبذل في سبيل تنفيذ وتطوير ممارسات الأمن السيبراني من خلال تسليط الضوء على السلبيات التي تظهر.

من أهم العراقيل التي تواجه الجهات المختصة في نشر الوعي السيبراني، يمكن تحديدها من خلال نقطتين :

١. التكلفة المالية المرتفعة التي الضرورية من أجل تطوير ممارسات الأمن السيبراني

٢. عدم رغبة بعض القيادات الجامعية والثانوية في تطويرالمناهج الدراسية كي تتضمن الأمن السيبرانية وذلك على إعتبار أن هذه الممارسات هي فنية لا دخل لهم بها

اذاً التعاون بين الدولة و المجتمع المدني أمر ضروري في الحفاظ على بيئة سيبرانية صحية عن طريق نشر الوعي والثقافة في المجتمع للتوصل الى تحقيق أهداف الأمن السيبراني وحماية الشركات والمؤسسات و الأفراد من مخاطر الهجمات السيبرانية وهذه الأهداف لا تتم دون وجود تعاون حقيقي وجدّي مع كافة الجهات داخل الدولة الواحدة .

الخاتمة :

توصلنا في دراستنا هذه أننا أمام سباق غير تقليدي دفع بالدول الى إمتلاك وتطوير الأسلحة السيبرانية بسبب سرعة أداءها وتكلفتها المنخفضة مقارنةً مع الأسلحة القديمة التقليدية وفعاليتها في التدميرن مما أدى الى ظهور مفهوم الهجوم السيبراني الذي شكل تحدياً دولياً هاماً لناحية الإشكاليات الخطرة التي يطرحها والتي حاولنا جاهدين الإجابة عنها في هذة الدراسة انطلاقاً من الأهمية التي أصبح يوليها المجتمع والفقه الدوليين لها، فالتطور التكنولوجي قدم الكثير من الإجابيات للبشرية في مختلف المجالات ولكن اعتبر عاملاً أساسياً في توسيع نطاق التهديدات والويلات والأخطار وظهور ما يسمى بالجرائم المستحدثة مما دفع بالدول والأفراد الى اللجوء لهذه الهجمات في وقت السلم أم الحرب، مستغلين بالتالي غياب القواعد القانونية المنظمة لها والفراغ القانوني القائم، ففي خاتمتنا هذه سوف نتطرق الى النتائج المنبثقة عن الحالات الحديثة الغير منظمة دولياً ووطنياً والتي تعتبر نقلة نوعية في هذا النطاق، بالإضافة الى أبرز المقترحات آملين أن تتطبق عملياً وأن لا تبقى فقط حبرعلى ورق لا جدوى منها.

في ظل غياب تعريف موحدّ للهجمات السيبرانية متفق عليه دولياً، سعينا في هذه الدراسة التوصل الى تعريف مقترح على الشكل التالي : " الهجمات السيبرانية هي أعمال عدائية هجومية كانت أم دفاعية، تستخدم الفضاء السيبراني من أجل الحصول على المعلومات الهامة المخزنة في شبكات الحاسوب أو في المنشآت المرتبطة بها، بهدف إتلافها أو تدميرها أو فقدان السيطرة عليها والتحكم بها أو إلحاق أضرار مادية أم معنوية في البنى التحتية لهذا الفضاء أو التسبب بإصابة أو وفاة أشخاص نتيجة هذه الهجمات سواء كانت موجهة من دولة أو فرد ضدّ دولة أخرى، أو من شخص طبيعي أم معنوي ضدّ شركة أم مؤسسة عامة أو خاصة، محلية أم أجنبية".

تجدر الإشارة أنه من الضروري تكييف الهجمات السيبرانية ضمن أحكام القانون الدولي الإنساني من أجل حماية المدنيين من آثار هذه الهجمات التي يمكن أن تصيبهم شأنها شأن اي سلاح جديد ظهر على الساحة الدولية يتم تنظيمه ضمن الأحكام الواردة في إتفاقيات جنيف الأربعة والبروتوكولين الإضافين، فالهجمات السيبرانية كي تعتبر أنها إستخدام القوة في الفضاء السيبراني لا بدّ من توافر كافة المعايير الموضوعية المحددة من قبل خبراء تالين أي الهجمات التي تصل الى مستوى النزاع المسلح أما الهجمات التي لا تصل الى هذا المستوى لا يمكن تصنيفها على أنها إستخداماً للقوة بالمعنى المتعارف عليه بل يتم تكييفها ضمن قواعد قانونية خاصة ولا يعطى الحق للضحية اللجوء الى الأساليب المكرسة قانونياً (حق الدفاع والتدابير المضادة) بإستثناء الهجمات الجرثومية والبيولوجية والأمراض المفتعلة التي تلحق تؤثرعلى حياة الأشخاص وأضرار جسيمة في الأرواح، كذلك بالنسبة الى الهجمات الإقتصادية التي من شأنها أن تمنع وصول المواد الغذائية لبلد ما، وعلى المتنازعين الإلتزام بالمبادئ التي ترعى سير العمليات العدائية والاّ إعتبر الفعل بمثابة إنتهاك لحقوق الإنسان ولقواعد القانون الدولي الإنساني.

أيضاً يجب أن نشير أن المدني يظل متمتعاً بالحماية المعترف بها دولياً الى حين مشاركته في العمليات العدائية ويفقد الحماية الممنوحة له ويصبح هدفاً للخصم ولا يستطيع إستعادتها ضمن شروط معينة على عكس المقاتل الذي لا يترتب عليه أي مسؤولية، نضيف أن المجتمع الدولي حاول تنظيم مسألة الهجمات السيبرانية من أجل السيطرة عليها والحدّ من آثارها التي تلحق أضرار جسيمة بالأرواح والممتلكات،

فالجهود الدولية والإقليمية كثيرةٌ وجميعها تهدف الى مواجهة التهديدات السيبرانية التي تضع الأمن الدولي على المحك، فالهدف الأسمى هو التوصل الى إتفاقية محددة تنظم مسألة الهجمات السيبرانية، أما القانون اللبناني لم ينظم هذه الهجمات ولم يتضمن قانون العقوبات اية بنود تعاقب المهاجم السيبراني عن أي عمل غير شرعي يقوم به.

يعتبر هذا الدليل كنقطة إنطلاق مهمة في تحليل و توضيح كيفية تطبيق قواعد و مبادئ القانون الدولي الإنساني على العمليات و الهجمات السيبرانية التي تفقر الى اي تنظيم قانوني و لكن من أبرز السلبيات أن قواعده لا تتمتع باي قيمة الزامية بل هي على سبيل التمنيات و التوصيات التي وجهها خبراء هذا الدليل الى المجتمع الدولي في محاولة منهم لتنظيم هذه الهجمات و برأينا أن هذا الدليل يتمتع بكافة المواصفات القانونية التي نحتاجها من أجل الحد من مساوئ الهجمات السيبرانية و غيرها من الجرائم السيبرانية و جبر الطرف المتضرر.

المقترحات :

على الصعيد الدولي :

- ان مسألة مواكبة المشرع الدولي للمستجدات السيبرانية الحديثة أصبحت امراً واقعاً وضرورة أساسية تستدعي تعديل بعض الإتفاقيات والأنظمة الدولية القائمة وخاصةً نظام روما الأساسي، فلا تزال الجرائم التي تدخل ضمن اختصاص المحكمة الجنائية الدولية محددة حصراً بأربعة جرائم وكي تصبح المحكمة قادرة على النظر في دعوى معينة يجب أن تكون صاحبة ولاية في نظرها وكل ما لم يدخل في اختصاصها لا يجوز لها أن تنظر به الاّ في حال تعديل كل من المادتين ١٢١ و ١٢٣ من النظام الأساسي للمحكمة الجنائية الدولية كي تستطيع عندئذ النظر في مسألة الهجمات السيبرانية، مما يحتم ضرورة تعديل هاتين المادتين وأن نوسع أختصاص هذه المحكمة كي تمتد الى الجرائم التي ترتكب على إقليم دولة ليست طرفاً في هذا النظام، و كذلك الأمر بالنسبة الى الجرائم المرتكبة على إقليم دولة طرف أو في هذه الأخيرة .

اذاً تستنتج أنه لا بدّ من ان يتم التوسع في اختصاص المحكمة الجنائية الدولية كي تشمل :

-الجرائم التي ترتكب في اقليم دولة طرف

- الجرائم التي ترتكب من قبل راعايا دولة طرف أو ضدّ رعايا دولة طرف في هذا النظام

- الجرائم التي ترتكب من على اقليم دولة لم يكن طرفاً في هذا النظام و لكن اثارها السلبية ظهرت في اقليم دولة طرف بهذا النظام الأساسي.

- تبني الأحكام والأسس الواردة في دليل تالين عن طريق عقد اتفاقية دولية متعددة الأطراف، يمكن تسميتها: " الإتفاقية الدولية المنظمة للتهديدات السيبرانية "، تساهم هذه الإتفاقية فضلاً عن تنظيم حل مسألة الهجمات السيبرانية دولياً، تحديد المسؤولية الجنائية المترتبة على الفاعلين والمشاركين والمحرضين وكيفية محاكمة هؤلاء والمحاكم المختصة بهذا الشأن، على أن تتمتع هذه الإتفاقية بالصفة الآمرة.

- ان محكمة العدل الدولية هي المرجع الصالح للفصل في مسائل الهجمات السيبرانية دولياً ولكن في حال تأملنا في تكوين هذه المحكمة نجد أنها لا تحتوي على أية غرفة خاصة بالتهديدات والهجمات السيبرانية مما يحتم إنشاء غرفة خاصة تفصل في النزاعات السيبرانية الدولية القائمة بين الدول .

- ان تنوع وإختلاف النظم الإجرائية بين الدول، فضلاً عن اجراءات التحقيق والمحاكمة في مجال الهجمات السيبرانية يؤدي الى صعوبة تحقيق العدالة بسبب الطبيعة الخاصة للهجمات السيبرانية مما نرى انه من الضروري توحيد النظم الإجرائية في مجال الهجمات السيبرانية على الأقل من أجل التخفيف من امكانية وجود تنازع قضائي بين الدول الذي يعيق سير العدالة الجزائية، بالإضافة الى التشديد على دور الإستنابة القضائية في حل العراقيل التي تعترض الدول .

- الغاء شرط التجريم المزدوج الذي يمثل عائقاً اساسياً في مجال تحقيق العدالة وتسليم المجرم للدولة الطالبة التسليم بشأن جرم ارتكبه، هذا الشرط يساهم في إفلات المجرم من العقاب لأن قوانين الدولة المطلوب منها التسليم لا تجرم الفعل الذي إرتكبه الفاعل مما يدفعها الى رفض تسليمه، وخاصةً في مجال الهجمات السيبرانية الغير منظمة في قوانين الكثير من الدول، فضلاً عن تشجيع المجرمين على إرتكاب المزيد من الجرائم المماثلة طالما أن الدولة لا تعاقب عليه .

- تعزيز التعاون بين الدول لناحية تبادل الخبرات والآليات التقنية التي من شأنها أن تساعد الدول النامية في تنمية قدراتها السيبرانية، والقيام بورش عمل سيبرانية مع منظمة الأمم المتحدة لبحوث الجريمة والعدالة والإتحاد الأوروبي والإقليمي والأنتربول والمنظمات والوكالات الدولية، نذكر منها على سبيل المثال لا الحصر : ,Europol , Cepol, CSIRT,Enisa والمعاهد الدولية التي تعنى بمقاييس الأطر (Ebios) و غيرها من الجهات المختصة التي تساهم في تدريب الجهات الأمنية الخاصة في مبادرة منها لتطوير قدراتهم وكفائتهم، مع الأخذ بعين الإعتبار كافة الصعوبات الشخصية والمادية المعترضة.

- إنشاء مركز دولي لدى منظمة الأمم المتحدة يختص بالنظر بكافة التفاصيل المتعلقة بأمن وإستقرار الفضاء السيبراني والكشف عن أي انتهاك لهذا الفضاء والقيام بكافة الإجراءات الضرورية لمحاسبة المعتدين .

على الصعيد المحلي :

- تنظيم إستراتجية الردع الخاصة بمواجهة الجرائم السيبرانية، التي تمر غالباً بسلسلة القتل السيبرانية (تتمثل الهجمات السيبرانية المحلية بثماني مراحل : الإستطلاع، التسلل، الإستغلال، تصعيد الصلاحيات، الحركة الجانبية، التعتيم، رفض الخدمة، الإنسحاب) .

- تشجيع قدرة الدولة على الإستجابة للتهديدات السيبرانية من خلال دعمها للمؤسسات التي تعنى بتصنيع منتجات الأمن السيبراني وتوفير التمويل اللازم لهذه المشاريع، فلبنان يعتمد على استيراد هذه المنتجات دون تصنيعها وتكون غالباً مرتفعة الكلفة ومعظم المنشآت والمؤسسات لا تستطيع الحصول عليها لأسباب مادية.

- تسهيل تبادل المعلومات بين القطاعين العام والخاص من خلال إنشاء قاعدة بيانات مختصة بالجرائم و الحوادث السيبرانية التي ترتكب و توفير إمكانية الإطلاع عليها و تقييمها لمراحل تطور الهجمات السيبرانية و اتخاذ التدابير المناسبة لكل مرحلة من مراحل هذا التطور .

-إنشاء جهاز مختص بالنظر بالجرائم والهجمات السيبرانية يعنى فقط بالشؤون السيبرانية ويتكون من قضاة مخولين وفق مؤهلاتهم التقنية والعليمة النظر في الجرائم والهجمات السيبرانية وإتخاذ كافة الإجراءات المختصة بمرحلتي الملاحقة والتحقيق، على أن يكون أفراده مختصين ومدربين ويتمتعون بالكفاءة اللازمة التي تخولهم القيام بإجراءات الملاحقة والتفتيش عن الأدلة والحفاظ عليها بالطريقة المناسبة، فضلاً عن علمهم المسبق بكيفة التحقيق مع المجرم المعلوماتي.

- تطوير الأطر والأنظمة القانونية التقليدية القائمة من خلال إقتراح مشروع قانون مختص بمسألة التهديدات السيبرانية، معالجاً لكافة جوانب هذه الممارسات وتحديد العقوبات المتناسبة مع الأفعال المرتكبة .

- السعي الى توقيع إتفاقيات ثنائية الأطراف أو متعددة الأطراف مع الدول الأخرى بشأن تنظيم الأحكام السيبرانية المختصة بتسليم المجرمين ومحاكمتهم مما يؤدي الى زيادة التفاهم بين الدول وخلق ثقة متبادلة.

- خلق منصة إفتراضية تعنى بنشر الثقافة السيبرانية وتوعية المواطنين حول المخاطر والتهديدات السيبرانية التي تهدد أمنهم المعلوماتي وخصوصيتهم وكيفية التعامل مع الأمر والتنسيق مع الأجهزة الأمنية الخاصة إذا لزم الأمر .

- توفير التمويل اللازم للبحوث ومعاهد الدكتوراه من أجل تمكينهم القيام بالأبحاث العلمية والفنية والتقنية اللازمة من أجل تطوير برمجيات معينة تساهم في مواجهة الهجمات السيبرانية التي تتعرض لها البلاد والمنشآت بسرعة قياسية .

- تعزيز التعاون الجدي بين القطاعين العام من جهة والقطاع الخاص ودوائر الصناعة من جهة أخرى من أجل تعزيز الشراكات الوطنية في مجال الحد من الهجمات وانتاج وتطوير منتجات سيبرانية منافسة لتلك التي يتم استرادها .

- تعزيز القدرة التعليمية اللبنانية عن طريق إدخال موضوع الأمن السيبراني الى المدارس والجامعات عن طريق تنظيم أنشطة في الفصول الدراسية ودورات تدريبية تساعد التلاميذ على التعامل مع التهديدات السيبرانية واستعاب أشكالها وأنواعها المختلفة للحدّ من الهجمات التي يمكن أن تتعرض لهذه الفئة الضعيفة من المجتمع ,عبر الترويج لثقافة النظافة السيبرانية، أما بالنسبة للجامعات، أصبح من الضروري تحديث الأنظمة الجامعية عن طريق توفير للطلاب إختصاص الأمن السيبراني بالتنسيق مع وزارة التربية والتعليم العالي والوزارات المعنية .

لائحة المراجع باللغة العربية

المؤلفات :

- أيمن (عبد الحفيظ) : **" الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية"**، ٢٠٠٥، دار النهضة العربية، مصر.

- ابو عيطة (سيد) :" **الجزاءات الدولية بين النظرية والتطبيق "**، ٢٠٠١، مؤسسة الثقافة الجامعية، الاسكندرية ، مصر

- الزهراني (شيخة حسين): " **مواجهة القانون الدولي للهجوم الإلكتروني (السيبراني)"** ، ٢٠٢١ ، دار النهضة العربية، الإمارات العربية المتحدة

- الحسيني (عماد عباس) : **" جرائم الحاسوب والإنترنت (الجرائم المعلوماتية)"** , الطبعة الأولى, منشورات زين الحقوقية, بيروت- لبنان

- أحمد (عبدالله هلالي) : **" الجوانب الموضوعية والإجرائية للجرائم المعلوماتية – على ضوء اتفاقية بودابست ٢٠٠١"** ، طبعة ٢٠٠١، دار النهضة العربية، القاهرة، مصر

- الصقيلي (اياد يونس محمد) : **" الخطر الدولي في القانون الدولي العام : دراسة قانونية "**، ٢٠١٤، دار الفكر الجامعي، الاسكندرية، مصر

-الخطابي (عبد العزيز رمضان على) **:" الدفاع الوقائي في القانون الدولي العام "** ،٢٠١١، دار الجامعة الجديدة، الاسكندرية، مصر

- جبار الشلال (علي) :**" المبادئ العامة في قانون العقوبات "**، الطبعة الثانية، مكتب زاكي للطباعة، بغداد

- الخوري (جنان) : **" الجرائم الإقتصادية الدولية والجرائم المنظمة العابرة للحدود (الجرائم المعلوماتية- جرائم الشركات المتعددة الجنسية - الجريمة المنظمة -الفساد -الاتجار بالرقيق الأبيض وبالأسلحة "** ، منشورات صادر الحقوقية، لبنان

- رستم (هشام محمد فريد) : **" قانون العقوبات ومخاطر تقنية المعلومات "**، طبعة ١٩٩٢، مكتبة الالات الحديثة، مصر

- سليمان (عبدالمنعم سليمان) : **" الجوانب الإشكالية في النظام القانوني لتسليم المجرمين "**، ١٩٩٩، دار المطبوعات الجامعية، الإسكندرية، مصر

- سليمان (سليمان عبدالله) : **" المقدمات الأساسية في القانون الدولي الجنائي"**، ١٩٩٢، ديوان المطبوعات الجامعية، الجزائر

- صالح (عبيد حسين) :**" القضاء الجنائي الدولي : تاريخه، تطبيقاته، مشروعاته "** ، ١٩٧٧، دار النهضة العربية، القاهرة، مصر

- عبدالباقي الصغير (جميل) : **" الجوانب الإجرائية للجرائم المتعلقة بالإنترنت "** ، ٢٠٠١، دار النهضة العربية، مصر

- عطية (طارق ابراهيم الدسوقي)**: " الإحتلال وأثره على حقوق الانسان : دراسة تطبيقية على الإحتلال الأميريكي البريطاني للعراق "** ، ٢٠٠٥، دار النهضة العربية، مصر

- عبد الصادق (عادل)**:" اسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني "**، ٢٠١٦، مكتبة الإسكندرية، مصر

- عبدالحليم (رمضان مدحت) : **" جرائم الاعتداء على الأشخاص والإنترنت "**، ٢٠٠١، دار النهضة العربية، مصر

- علام (وائل أحمد) : **" مركز الفرد في النظام القانوني للمسؤولية الدولية "**، طبعة ٢٠٠١، دار النهضة العربية، القاهرة، مصر

- عبد العال (مصطفى السيد مصطفى)، **" دليلك الشامل الى شبكة الإنترنت"**، الطبعة الثالثة، دار الكتب العلمية للنشر والتوزيع، القاهرة، مصر

- فتلاوي (أحمد عبيس نعمة): **"الهجمات السيبرانية : دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر"**، الطبعة الأولى، منشورات زين الحقوقية، بيروت – لبنان .

- فاضل (سليمان أحمد) : **" المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية"** ، ٢٠٠٧، دار النهضة العربية، مصر

- كاسيزي (أنطونيو):**" القانون الدولي الجنائي "**، الطبعة الأولى باللغة العربية، منشورات صادرالحقوقية، لبنان

- مصطفى(محمود محمود) : **"شرح قانون العقوبات – القسم العام "**، الطبعة الثامنة، دار النهضة العربية، مصر

- محمود عبدالله(حسين علي) :**" سرقة المعلومات المخزنة في الحاسب الالي "** ، الطبعة الأولى، دار النهضة العربية، مصر

الإتفاقيات والمواثيق الدولية :

- إتفاقية لاهاي الخاصة بإحترام قوانين وأعراف الحرب البرية لعام ١٩٠٧

- إتفاقية لاهاي بالنسبة الى حقوق وواجبات الدول المحايدة في الحرب البرية لعام ١٩٠٧

- ميثاق الأمم المتحدة لعام ١٩٤٥

- النظام الأساسي لمحكمة العدل الدولية لعام ١٩٤٥

- إتفاقية جنيف الأولى لتحسين حال الجرحى و المرضى بالقوات المسلحة في الميدان لعام ١٩٤٩

- إتفاقية جنيف الثانية لتحسين حال جرحى ومرضى وغرقى القوات المسلحة في البحار لعام ١٩٤٩

- إتفاقية جنيف الثالثة لناحية معاملة أسرى الحرب لعام ١٩٤٩

- إتفاقية جنيف الرابعة بشأن حماية الأشخاص المدنيين في وقت الحرب لعام ١٩٤٩

- إتفاقية لاهاي لحماية الممتلكات الثقافية في حالة النزاع المسلح لعام ١٩٥٤

- العهد الدولي الخاص بالحقوق المدنية والسياسية لعام ١٩٦٦

- البروتوكول الإضافي الأول لإتفاقيات جنيف المتعلق بحماية ضحايا المنازعات الدولية المسلحة لعام ١٩٧٧

- البروتوكول الإضافي الثاني لإتفاقيات جنيف المتعلق بحماية ضحايا المنازعات المسلحة غير الدولية لعام ١٩٧٧

- البروتوكول الثاني لإتفاقية لحظر أو تقييد إستعمال أسلحة تقليدية معينة يمكن إعتبارها مفرطة الضرر أو عشوائية الأثر لعام ١٩٨٠

- نظام روما الأساسي للمحكمة الجنائية الدولية لعام ١٩٩٨

- التعديلات الواردة على نظام روما الأساسي للمحكمة الجنائية الدولية فيما يختص بجريمة العدوان (اتفاقية كامبالا لعام ٢٠١٠

- مشروع المسؤولية الدولية عن الأفعال غير المشروعة دولياً و تعليقاته المنشور في حولية لجنة القانون الدولي لعام ٢٠٠١

- فتوى محكمة العدل الدولية بشأن الأثار القانونية النشئة عن تشييد جدار في الارض الفلسطينية المحتلة لعام ٢٠٠٤

- المعاهدة الأمم المتحدة النموذجية بشأن تسليم المجرمين لعام ١٩٩٠

- الإستراتجية الوطنية اللبنانية للأمن السيبراني لعام ٢٠١٩

الأبحاث والدراسات والمقالات :

- زروقة (إسماعيل) : **" الفضاء السيبراني والتحول في مفهوم القوة والصراع "**، مجلة العلوم القانونية والسياسية، ٢٠١٩ ، ص ١٠١٦-١٠٣١

- رستم (هشام محمد فريد) :**" جرائم الحاسوب كصورة من صور الجرائم الأقتصادية "** ، مجلة الدراسات القانونية- كلية الحقوق- جامعة أسيوط، جمهورية مصر العربية، دون سنة، ص ١٠٥-١٢٢

- حمود (رؤى) : **" أشهر الهجمات الإلكترونية حتى ٢٠٢٢ : حروب من نوع آخر "**، مقال نشر على موقع " مجموعة ريناد المجد لتقنية المعلومات RMG – المملكة العربية السعودية – دون سنة، ص١-٢

- بهاء (قيصر) :**" أشهر الهجمات السيبرانية : آلية عملها وطرق تجنبها "**، الفريق الوطني المصري للإستجابة للأحداث السيبرانية (CERT)، جمهورية مصر العربية، ص ١-٢٣

- عبد الرحمن (دعاء حامد محمد) : **" الموافقة و دورها في تقنين التعامل في البيانات الصحية الحساسة وتأثيرها على الأمن المعلوماتي : قراءة في قانون حماية البيانات الشخصية رقم ١٠١ لسنة ٢٠٢٠ "**، جامعة عين نصر – كلية الحقوق ، جمهورية مصر العربية، ٢٠٢٢، ص١-٤٩

- كريم (خلفان) : **" الأسس القانونية لتراجع نظام الحصانة القضائية الجنائية لكبار المسؤولين في القانون الدولي المعاصر "**، المجلة الجزائرية للعلوم القانونية والإقتصادية والسياسية، جامعة مولود معمري وكلية الحقوق، ٢٠٠٨، ص ٢١٣-٢٢٧

- سفيان (دخلافي) : **" تكييف الهجمات السيبرانية في ضوء أحكام القانون الدولي "**، المجلة الأكاديمية للبحث القانوني " ، ٢٠٢٢، ص ٣٠٣-٣٢٣

- بيضون (فاديا) : " : **نظرية جرائم ذوي الياقات البيضاء عام ١٩٣٩ لأدوين سذرلاند "** ، مجلة محكمة، ٢٠٢١، لبنان ، متوفرة على الرابط التالي : www.mahkama.net

- بشور (فتحية) :

" مفهوم النزاع المسلح بين قواعد القانون الدولي الإنساني و قواعد القانون الدولي الجنائي "، مجلة المعارف العلمية، الجزائر، ٢٠١٢, ص ٢١-٣٧

- " مفهوم القانون الدولي الجنائي "، مجلة المعارف العلمية ٢٠١٢، العدد ١٢

- مسعف (محمد دهام) : **" مشروعية إستخدام الهجمات السيبرانية في النزاعات الدولية والمسؤولية الدولية عنها"** تحت إشراف محمد خليل جعفر، عدد خاص لبحوث التدريسيين مع طلبة الدراسات العليا، الجزء الرابع، المجلد ٤٦، كانون الأول، ٢٠٢١، ص ٦٧٨-٧٠٤

- قلته بخيت (شريف نسيم) :**" دليل تالين : الهجمات الإلكترونية وحظر إستخدام القوة في القانون الدولي"**، المركز العربي لأبحاث الفضاء الإلكتروني "، ٢٠١٧، ص ١

- محمد الحاج (ابراهيم طلال) : **" الهجمات السيبرانية على شبكات الحاسوب في ضوء القانون الدولي الانساني "**، جامعة دمشق – كلية الحقوق (قسم القانون الدولي)، أطروحة دكتوراه، سوريا

- سعود (يحي ياسين) : **" الحرب السيبرانية في ضوء القانون الدولي الانساني "**، المجلة القانونية

المجلد ٤ , العدد ٤ – كلية الحقوق – جامعة القاهرة –مصر

-منية (العمري رقار) : **" الدفاع الشرعي في القانون العام "** –جامعة الأخوة منتوري، كلية الحقوق والعلوم السياسية، رسالة ماجستير، الجزائر، عام ٢٠١١

-سمودي (رزق أحمد):**" حق الدفاع عن النفس نتيجة الهجمات الالكترونية في ضوء قواعد القانون الدولي العام "**، مجلة جامعة الشارقة للعلوم القانونية، المجلد ٥، العدد ٢، ٢٠١٨

- حتحاني (محمد) : **" التدابير المضادة في القانون الدولي "**، رسالة ماجستير، الجزائر ٢٠١٠

- قنديل (عابدين عبد الحميد حسن) : **" التدابير المضادة في النظام القانوني الدولي , دراسة نظرية و تطبيقية "** , رسالة دكتوراه – جامعة القاهرة، كلية الاقتصاد والعلوم السياسية، سنة ٢٠٠٦

- قاسم (طه احمد علي) : **" التدابير المضادة في اطار منظمة التجارة العالمية : دراسة نظرية وتطبيقية "** ، رسالة دكتوراه –جامعة القاهرة –كلية الاقتصاد والعلوم السياسية سنة ٢٠١٠

- ابراهيم (عماد حسن محمد) : **" التدابير المضادة ومدى مشروعيتها في مواجهة الهجمات السيبرانية المعادية في القانون الدولي العام "**، مجلة البحوث القانونية والإقتصادية، المقالة رقم ٣، المجلد ٥٤، العدد ٣، ٢٠٢١

- محمد (حتحاتي) : **" التدابير المضادة في القانون الدولي "**، جامعة الجزائر – كلية الحقوق بن عكنون، رسالة ماجستير، الجزائر

- شميث (مايكل) :**" الحرب بواسطة شبكات الإتصال: الهجوم على شبكات الكمبيوتر والقانون في الحرب"**، المجلة الدولية للصليب الأحمر,٢٠٠٩

- أحمد صالح (لواء محمد منير) : **" الأساليب المستحدثة لمواجهة العمليات الارهابية "**، اكاديمية الشرطة المصرية، مصر، بدون سنة،٧٠ص .

- بكتيه (جان) **:" مبادئ القانون الدولي الانساني: تطوره و مبادئه"**، دراسات في القانون الدولي الانساني، تقديم / مفيد شهاب دار المستقبل العربي، اصدارات اللجنة الدولية للصليب الاحمر، الطبعة الثانية – القاهرة , ٢٠٠٩

- نعوس (مصطفى) : **" حقوق و التزامات الدول في الحرب المعلوماتية "** , مجلة دراسات لعلوم الشريعة و القانون، المجلد٤٠, ملحق ١ , ٢٠١٣, متوفرة على الرابط التالي : www.mohamah.net
- أيات محمد سعود : **" دراسات و أبحاث قانونية "**، العدد ٥٨١٠ في ٩-٣-٢٠١٨، متوفرة على الرابط التالي
https://www.ahewar.org/debat/show.art.asp?aid=591797

- بو مرعي (علاء الدين) : **"مبدأ التمييز والأساليب والوسائل الحربية الحديثة – دراسة على ضوء مبادئ القانون الدولي الانساني"** ، المركز الاستشاري للدراسات والتوثيق، العدد ٣٢،٢٠٢٣

- دياب (نادر اسكندر) : **"تطور مفهوم المشاركة المباشرة في العمليات العدائية في القانون الدولي الانساني "**، مؤسسة عامل وجامعة الحكمة، ٢٠١١

- محمد (اسامة صبري) **:" فقدان المدنيين الحق في الحماية من الهجمات المباشرة"**، جامعة الأنبار للعلوم القانونية والسياسية، ٢٠١٢

- بو معزه (منى) : **" دور القضاء الدولي لجنائي في تطبيق القانون الدولي الانساني "**، جامعة باجي مختلر عنابة، كلية الحقوق، ٢٠٠٩

- فاروق (خلف) : **" الآليات القانونية لمكافحة الجريمة المعلوماتية "**، مجلة الحقوق والحريات، العدد ٢ ، عام٢٠١٥

- خليل (بشار) :**" ما هي الحرب السيبرانية ؟ - مستقبل مخيف للصراع الرقمي "**، الجمعية العلمية السورية للمعلوماتية، عدد ١٥٤، آب ٢٠٢٠

- عودة (جميل): **" المنظمات الحكومية والغير حكومية "**، مقال متوفرعلى الرابط التالي www.siironline.org

- أبو سعده (أحمد أمين) :**" الشبكة الفتراضية الخاصة VPN للربط بين المؤسسات المتخصصة "** ,مجلة العربية للدراسات المعلوماتية – العدد ١، ٢٠١٢

- شامبي (بغدادي) : **" تأمين الخطر السيبراني "** , مجلة هيرودوت للعلوم الانسانية و الاجتماعية , المجلد ٧, العدد ٢٥ , ٢٠٠٥

- مقال بعنوان : **" كيف تستخدم الدول قطع الإنترنت لصالحها ؟"** متوفرعلى الرابط التالي: https://www.noonpost.com/

- الشوابكة (عدي محمد علي) : **" معوقات مكافحة الجرائم الإلكترونية في المجتمع الاردني من نظر ذوي الاختصاص "** , جامعة مؤتة, كلية العلوم الاجتماعية، أطروحة دكتوراه، ٢٠٢٢

- غايب (محروس نصار) : **" الجريمة المعلوماتية "** وجامعة الأنبار، المعهد التقني، ٢٠١٠، متوافر على الرابط التالي : https://www.iasj.net/iasj/download/5cd8d60110b50ba7

- صفير (رلى) : **" الدعوى الجزائية و أبرز مراحلها "**، مجلة الجيش اللبناني، العدد ٢١٣ ،٢٠٠٣

- لخضر (غزالي) : **" التحريات المستحدثة في جرائم التكنولوجيا الحديثة "**، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد الخامس، العدد الأول – ٢٠٢٠

- اليوت (جنيفر) وجنكينسون (نايجل) : **" المخاطر السيبرانية...التهديد الجديد للاستقرار المالي "** مقال منشور على موقع مجلة IMF في ٧-١٢-٢٠٢٠، متوفر على الرابط التالي : https://www.imf.org/ar/Blogs/Articles/2020/12/07/blog-cyber-risk-is-the-new-threat-to-financial-stability

- هاثاواي (ميليسا) : **" إدارة الخطر السيبراني الوطني"** ، مقال منشور على موقع potomacinstitute , متوفر على الرابط التالي : https://potomacinstitute.org/images/CRI/Managing-National-Cyber-Risks_FINAL-Arabic.pdf

- الموقع الرسمي للمركز الدولي لمنع الجريمة : https://cipc-icpc.org

- بودرو بنجامين: **" تهديدات مجهولة المصدر – نحو مسائلة دولية في الفضاء الالكتروني "** ، مؤسسة RAND، سانتا مونيكا، كاليفورنيا، ٢٠١٧، ص ٧، مقال متوفرعلى الرابط التالي : https://www.rand.org/pubs/research_reports/RR2081.html

- زيدان (روان) : " البرمجيات الخبيثة: الدودة، وحصان طروادة، والبوت والفرق بينها" ، مقال منشور على موقع ناسا بالعربي، ٢٠١٧، ص ١، متوفر على الرابط التالي :

https://nasainarabic.net/main/articles/view/malicious-software-worms-trojans-and-bots-oh-my

- مقال بعنوان : **"ما هو فيروس دفع الفِدية Ransomware؟ كيفية إزالته؟ أنواع برمجيات رانسوم وير ٢٠٢٢؟! "** متوافر على الرابط التالي : https://mohamedovic.com/ransomware/

- مقال بعنوان : **" ما هي هجمات DDoS؟ "**، ص١، متوافرعلى الرابط التالي : https://me.kaspersky.com/resource-center/threats/ddos-attacks

- مقال بعنوان : **" ما هو هجوم الوسيط أو الرجل في الوسط Man-In-The-Middle Attack؟ "** متوفر على الرابط التالي :

https://thaqafati.com/%D8%AA%D9%83%D9%86%D9%88%D9%84%D9%88%D8%AC%D9%8A%D8%A7/%D9%87%D8%AC%D9%88%D9%85-%D8%A7%D9%84%D8%B1%D8%AC%D9%84-%D9%81%D9%8A-%D8%A7%D9%84%D9%88%D8%B3%D8%B7/

- أيات محمد سعود **:" دراسات و أبحاث قانونية "** ،العدد ٥٨١٠ في ٩-٣-٢٠١٨، متوفرة على الرابط التالي : https://www.ahewar.org/debat/show.art.asp?aid=591797

لائحة المراجع باللغة الإنكليزية :

Books :

- Marco Roscini, "**World Wide Warfare –Jus ad Bellum and the use of CyberForce"**, Max Planck yearbook of United Nations Law,2010,Vol. 14 .p91

Articles :

- Zimet.E and C.L Barry ,**" Military services Overview , Cyber power and National Security"** .National Defense University Press, Washington,DC,USA,2009.P.1-300

- Michael S.Fuertes , **"cyber warfare ,Unjust Actions in a Just war"** , Florida International University , Full 2013,p.1.

- James E.Cartwright , **" Memorandum for Chiefs of the Military Serve , commanders of the Combattant Commands,Dirs, of the Joint staff Directories on joint Terminology for cyberspace operations**" , Washington, 2018 ,p1-16 available on : https://info.publicintelligence.net/DoD-JointCyberTerms.pdf

- **Shanhai Cooperation Agreement,Annex I** , p, 203-213

- Collin Allan : **" Direct Participation in Hostilities From Cyberspace"** , Virginia Journal of International Law, Vol. 54, No. 1, 2013 p 174-193

- Michael N.Schmmitt **: " wired warfare : computer network attack and Jus in Bello"** , Vol.84,N 846, 2002 p365-399

- David trurns : **"Cyberwarefare and the Notion of Direct Participation in Hostilities**" , Journal of conflict & Security law , Oxford University , Press, 2012,Vol, p 295-296

- USA ,American department of Defense Law of War Manual , office of General Consul department of Defense , June 2015, p1-1176 available on : https://dod.defense.gov/Portals/1/Documents/pubs/Law-of-War-Manual-june-2015.pdf

- Elissa(Okoniewski) : **“ The french Challenge to Free Expression on the Internet “** , American University International Law review,2002,article 6, p311

- Presidential Address to the Nation (11 September 2001) : https://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010911-16.html#:~:text=Terrorist%20attacks%20can%20shake%20the,and%20opportunity%20in%20the%20world

Theses:

- Maiyin Akveld **: “ Crossing Digital borders :Direct participation in cyber hostilities”** , master’s Thesis, Amesterdam University p 7 , 2016

- Emily Crawford: **“Virtual Battlegrounds: Direct Participation in Cyber Warfare”** , Sydney Law School, master’s Thesis, The University of Sydney ,2012

- Willem van poll **“ Direct Participation in Hostilities : A Cyberspace Oddity?**”, Master’s Thesis, Faculty of law , University of Amsterdam, 2013

- NostBakken , Ase Tordahl **: “ Consequences Under International Humanitarian Law of Civilians who take a direct part in hostilities “**, University of Bergen , Faculty of Law – Norwegian , Master’s thesis , 2011

International Case Law :

- Fausto Bukar : " The International Tribunal for the Former Yugoslavia" , The united Nations, Audiovisual library of international law , p2

المحتويات