مواجهة القانون الدولى للهجوم الإلكترونى (السيبرانى)

الباحث ميلاد صالح مفتاح على
جامعة عبد الملك السعدى – طنجة – المغرب
مستشار قانونى بوزارة المواصلات والنقل – ليبيا

ملخص:

تتجاوز الهجمات السيبرانية الأبعاد العسكرية وتمتد إلى استهداف البنية التحتية الحيوية مثل الكهرباء والمياه وأنظمة الاتصالات بالإضافة إلى قطاعات تشمل المالية والاقتصاد. تتميز أعمال الحرب السيبرانية هذه بتركيزها العرضي على الهياكل المجتمعية والسياسية بقصد زعزعة استقرار المجتمعات من الداخل.

تمثل هذه الجرائم السيبرانية اتجاهًا أوسع حيث يستهدف المهاجمون، فرديًا وجماعيًا، البنى التحتية الأساسية كوسيلة لإرهاب المواطنين، أو ابتزاز الشركات أو السلطات للحصول على المال. وفي هذا السياق، لاحظت شركة الأمن السيبراني تريند مايكرو أن الكيانات ذات النوايا الخبيثة اختارت حاليًا المطالبة بفديات أعلى من الأهداف التي من المحتمل أن تكون قادرة على دفعها، مثل مقدمي الرعاية الصحية والحكومات المحلية.

تختلف الحرب السيبرانية اختلافًا كبيرًا عن الحرب التقليدية التي تتضمن عادةً جيوشًا تقليدية تشارك في معارك معلنة في ساحات معارك محددة. الصراعات السيبرانية غامضة وذات أهداف غير محددة تتحرك عبر شبكة المعلومات الإلكترونية.

في عصرنا الحالي، أصبحت الهجمات السيبرانية معقدة وخطيرة، حيث تحدث أنواع متعددة بمعدل متزايد. وعندما تصل هذه الأهداف إلى تفكيك البنية التحتية لدول بأكملها، فإنها تصبح ذات أهمية قصوى في أولويات الدفاع الوطني المشابهة للقدرات العسكرية بما في ذلك القوى النووية؛ يمكن للقدرات السيبرانية أن تخترق المحطات النووية أو تعطل القواعد العسكرية التي تتحكم فيها أو تعطلها بشكل فعال.

هناك إجماع بين المتخصصين في القانون الدولي الإنساني على أن الهجمات الإلكترونية خارج نطاق النزاع المسلح النشط لا ينبغي بالضرورة أن ينظمها القانون الدولي الإنساني.

كلمات مفتاحية: القانون الدولى، الإنسانى، مواجهة، الهجوم، الإلكترونى، السيبرانى.

Abstract:

Cyber attacks transcend military dimensions and extend to targeting critical infrastructure such as electricity, water, and telecommunications systems as well as sectors including finance and economics. These acts of cyber warfare are distinguished by their occasional focus on societal and political structures with an intent to destabilize societies from within.

These cyber crimes represent a broader trend where attackers, both individually and collectively, target essential infrastructures as a means to terrorize citizens, extorting companies or authorities for money. In this context, the cybersecurity firm Trend Micro has noted that entities with malevolent intentions have currently opted for demanding higher ransoms from targets likely able to pay them, such as healthcare providers and local governments.

Cyber warfare differs significantly from traditional warfare which typically involves conventional armies engaging in declared combats over identifiable battlegrounds. Cyber conflicts are nebulous with unspecified objectives moving across the electronic information network.

In today's era, cyber attacks are complex, dangerous with multiple types occurring at an increasing rate. When these reach goals of dismantling entire countries' infrastructures it becomes paramount in national defense priorities akin to military capabilities including nuclear powers; cyber capabilities can penetrate nuclear plants or disrupt military bases effectively controlling or disabling them.

There is consensus amongst international humanitarian law specialists that electronic attacks outside active kinetic armed conflict should not necessarily be regulated by international humanitarian law.

Keywords: International Law, Humanity, Confrontation, Attack, Electronic, Cyber.

مقدمة:

شهد العالم اهتماماً كبيراً بالحرب الإلكترونية في السنوات الأخيرة. ويعود هذا الاهتمام إلى التقدم التكنولوجي السريع في مجال الاتصالات وتبادل المعلومات، والذي أدى إلى زيادة الاعتماد على البنية التحتية الرقمية والإنترنت في مختلف جوانب الحياة.

وتمتد الهجمات السيبرانية إلى ما هو أبعد من الجوانب العسكرية، حيث يمكن أن تشمل استهداف البنية التحتية الحيوية مثل الكهرباء والمياه والاتصالات، فضلا عن الهجمات التي تستهدف القطاعين الاقتصادي والمالي. وما يميز هذا النوع من الحروب هو أنه أحيانًا ما يكون موجهًا نحو جوانب مجتمعية وسياسية، بهدف زعزعة استقرار المجتمع من الداخل.

ومع التقدم التقني المعاصر الكبير في مجال المعلومات والاتصالات عبر شبكة الإنترنت، أصبح من السهل جداً على المجرمين والإرهابيين توظيف هذه التقنيات المتقدمة في تطوير وتنفيذ وترويج مخططاتهم الإجرامية والإرهابية. حتى أصبحت هذه الأساليب الحديثة تشكل تحدياً خطيراً وخطيراً يهدد المجتمع الدولي برمته.

وقد انتشرت الهجمات الإلكترونية أو السيبرانية الضارة في العالم مؤخرًا. مما يهدد السلم والأمن الدوليين، حيث ظهرت تلك الهجمات على البنية التحتية في الحرب الروسية الأوكرانية، بالإضافة إلى تسريبات أوراق بنما، وحادثة اختراق وكالة أبحاث الإنترنت الروسية، بالإضافة إلى نشر وسائل الإعلام تفاصيل عن الرئيس الروسي منزل فلاديمير بوتين الجديد الذي تبلغ تكلفته ملايين الدولارات.

وتشكل هذه الجرائم السيبرانية جزءًا من اتجاه أوسع، حيث بدأ المهاجمون، فرديًا وجماعيًا، في استهداف البنية التحتية الرئيسية كوسيلة لترويع المواطنين وابتزاز الشركات أو السلطات مقابل المال. وفي هذا الصدد، أوضحت شركة تريند مايكرو للأمن السيبراني أن "الجهات ذات النوايا الخبيثة اختارت حاليًا المطالبة بفدية أكبر من الأهداف التي من المحتمل أن يدفعوها، مثل شركات الرعاية الصحية والحكومات المحلية".

أهمية البحث:

لقد أصبحت مكافحة الهجمات الإلكترونية (السيبرانية) والجرائم الإلكترونية في غاية الأهمية بالنسبة لنا لدراسة الأساليب التي يجب اتباعها لمواجهة هذه الجرائم العابرة للحدود، والتي تتطلب تحديد طبيعتها وخصائصها وطبيعة مرتكبيها. ويجب علينا أيضًا دراسة المخاطر السيبرانية وتأثيرها على التهديد الذي يهدد السلام والأمن الدوليين، فضلاً عن الجهود الرامية إلى مكافحة الهجمات الإلكترونية (السيبرانية) الدولية.

وبناء على ما سبق فإن الحد من الهجمات الإلكترونية (السيبرانية) ومكافحة الجرائم السيبرانية على المستوى الدولي يجب أن يتحلى بروح التعاون بين الأنظمة القانونية الداخلية للدول.

أهداف البحث:

يهدف البحث الحالي إلى تسليط الضوء على عدة أهداف كان أبرزها:

- التعرف على الهجوم الإلكتروني (السيبراني).
- التعرف على أبرز الإجراءات التي اتخذها القانون الدولي في مكافحة جريمة الهجوم الإلكتروني (السبراني).
- شرح إمكانية التوافق مع القواعد والمبادئ القانونية الدولية فيما يتعلق بالهجمات الإلكترونية (السيبرانية).

إشكالية البحث:

تتلخص الإشكالية القانونية التي يطرحها موضوع البحث في محاولة الإجابة على عدة تساؤلات، من بينها ما يتعلق بتعريف مفهوم الهجوم الإلكتروني (السبراني)، ومدى تطبيق القواعد والمبادئ الرئيسية للقانون الدولي الإنساني بشأنه. مع مشكلة أن وسائل وأساليب الحرب تتطور مع مرور الوقت والاستخدام الأمثل للتكنولوجيا في تحديد الأهداف وإمكانية مطابقتها لقواعد القانون الدولي الإنساني.

تنبع مشكلة البحث من العلاقة الوثيقة بين استجابة القانون الدولي للهجمات السيبرانية، لذا ستكون المشكلة الأساسية في السؤال التالي: إلى أى مدى استطاع القانون الدولى مواجهة ومكافحة الهجوم الإلكترونى (السيبرانى)؟

ويتفرع من السؤال الرئيسى بعض الأسئلة الفرعية، وذلك على النحو التالى:

1- ماهية الهجوم الإلكترونى (السيبرانى) وصوره؟

2- ما هى مخاطر الهجوم الإلكترونى (السيبرانى) على الأمن القومى الدولى؟

3- ما هى أبرز الجهود الدولية فى مكافحة الهجوم الإلكترونى (السيبرانى)؟

منهج البحث:

المنهج العلمي المتبع في البحث هو الوصفي، حيث تم عرض النصوص القانونية ونصوص المعاهدات الدولية المتعلقة بالهجمات الإلكترونية (السيبرانية).

الخطة البحثية:

المبحث الأول: ماهية الهجوم الإلكتروني (السيبراني):

المطلب الأول: مفهوم الهجوم الإلكتروني (السيبراني).

المطلب الثاني: الهجوم الإلكتروني (السيبراني) ما دون استخدام القوة.

المبحث الثاني: الجهود الدولية للتنظيم القانوني للهجوم الإلكتروني (السيبراني):

المطلب الأول: الجهود الدولية المباشرة للتنظيم القانوني للهجوم الإلكتروني (السيبراني).

المطلب الثاني: الجهود الدولية غير المباشرة للتنظيم القانوني للهجوم الإلكتروني (السيبراني).

الخاتمة والنتائج والتوصيات.

المبحث الأول

ماهية الهجوم الإلكتروني (السيبراني)

شهد الفضاء السيبراني في السنوات الأخيرة ارتفاعاً حاداً في عدد الهجمات السيبرانية، وذلك بسبب تعدد التهديدات السيبرانية، ومنها: الحروب، والإرهاب، والتجسس الرقمي، وغيرها. ولذلك يصعب تحديد الحجم الحقيقي لهذه الهجمات، خاصة أن العديد منها لم يتم الإبلاغ عنها، ورغم اختلاف غرض وهدف كل منها، إلا أن القاسم المشترك بينها هو استغلال الثغرات ونقاط الضعف في الفضاء الإلكتروني. الميدان بهدف اختراق أجهزة الكمبيوتر وشبكات الكمبيوتر، حتى ارتفعت الأصوات المطالبة بتكييف الردع بما يناسب ذلك المجال[1].

إن السيطرة على المعلومات حول مسارات الدولة الحديثة أصبحت قادرة على شل وهزيمة الدول الكبرى دون إطلاق رصاصة واحدة عليها. وتتعدد أغراض القرصنة الإلكترونية، كما أن هناك هجمات تهدف إلى تدمير اقتصاد دولة ما، أو سرقة البنوك والحسابات المصرفية، الأمر الذي دفع العديد من دول العالم إلى مواكبة التطورات العالمية في هذا المجال، استعداداً لمواجهة هذه التهديدات الخطيرة. الهجمات[2].

وتختلف الحرب السيبرانية عن الحرب التقليدية، حيث تنطوي الأخيرة على استخدام جيوش نظامية مع إعلان مسبق للحرب وساحة معركة محددة، في حين أن الأولى غامضة ولها أهداف غير محددة أثناء تحركها عبر شبكة المعلومات الإلكترونية[3].

المطلب الأول

مفهوم الهجوم الإلكتروني (السيبراني)

لقد شكلت الثورة الرقمية والمعلوماتية نقلة تكنولوجية كبيرة، حيث جعلت الفضاء السيبراني عنصرا حاسما في النظام الدولي الحديث نظرا لقدراته التكنولوجية المتقدمة. لقد أدخل هذا التطور أبعادًا جديدة وأضاف طبقات متعددة من التعقيد إلى العمليات العسكرية، مما أثر بشكل متزايد على الحسابات الإستراتيجية للدول. إن الدولة التي تفتقر إلى تقنيات الأمن السيبراني القوية تصبح عرضة للخطر. إن الفضاء الإلكتروني الخاص بها، الذي يشمل الأصول والموارد والمعلومات والخدمات والبنية التحتية الحيوية – بما في ذلك القطاعات الأمنية والعسكرية والمصرفية والتجارية والتعليمية والرعاية الصحية والاقتصادية – معرض بشدة لخطر مواجهة الهجمات السيبرانية المنهكة التي يمكن أن تسبب أضرارًا واسعة النطاق[4].

واستجابة للثورة الرقمية المعاصرة، التي تنشأ من مشهد سيبراني يعتمد على البنية التحتية العالمية لتكنولوجيا المعلومات والاتصالات، شهد العالم شكلاً غير تقليدي من سباق التسلح. يتضمن هذا النوع الجديد إنشاء وتطوير برامج تكنولوجية مصممة للاستخدام في الفضاء الإلكتروني للأغراض العسكرية. تسهل هذه البرامج الهجمات عالية السرعة ضد الخصوم من مسافات طويلة دون تعريض النفس للخطر، وتسمى هذه الظاهرة بالحرب السيبرانية [5].

وتشترك غالبية التعريفات المتعلقة بالهجمات السيبرانية في فهم مشترك يدور حول استهداف مواقع الويب أو أنظمة الكمبيوتر من خلال وسائل الاتصال الإلكترونية المختلفة، وتهدد هذه الإجراءات سرية المعلومات المخزنة أو سلامتها أو توفرها، وعادةً ما يتم تنفيذها بواسطة مصدر غير معروف يصل إلى الأصول المستهدفة أو يعدلها أو يدمرها عن طريق اختراق الأنظمة الحساسة[6]، على الرغم من الغموض المعترف به الذي يحيط بالمصطلح بسبب عدم وجود توافق في الآراء حول تعريفه المحدد، فقد اعتمد خبراء القانون الدولي العام مصطلحات مختلفة بناءً على أسس مفاهيمية مختلفة. يستخدم بعض المتخصصين مصطلح "الفضاء الإلكتروني" استنادًا إلى البيئة التي تحدث فيها الهجمات الإلكترونية، بينما يفضل البعض الآخر "الحرب الإلكترونية"، المرتكزة على الأيديولوجيات الأمنية أو العسكرية ضد الخصوم المتصورين. ومع ذلك، يختار العديد من الباحثين "الهجمات السيبرانية" كمصطلح بديل لأن فكرة الحرب غير مفضلة حاليًا ضمن الأطر القانونية الدولية. ومن ثم فإن مصطلح "الهجمات السيبرانية" يحمل أهمية وأهمية أكبر بما يتماشى مع المتطلبات المعاصرة للقانون الدولي[7].

بالإضافة إلى ذلك، فإن الهجمات السيبرانية أوسع نطاقاً من الحرب السيبرانية، وقد تحدث خارج نطاق النزاعات المسلحة، لذا قد تكون سبباً لبدء صراع السلع، أو قد تحدث ضمن نطاق النزاعات المسلحة، لذا فهي تشكل جزءا من الحرب السيبرانية. وعليه، فسوف نتناول تعريف الهجمات السيبرانية من خلال شرح معناها أولاً لغوياً واصطلاحياً، وثانياً. في شرح خصائصه.

أولاً: الهجوم السيبراني لغة:

المصطلح "سيبرانية" أو "سايبر" أو "سيبراني" يُعد ترجمة حرفية لكلمة الإنجليزية "Cyber"، وهذه الأخيرة مشتقة من "Cybernetics"[8].

تم استخدام هذا المصطلح لأول مرة أكاديميا من قبل عالم الرياضيات الأمريكي نوربرت وينر في عام 1948. في عمله الأساسي، "علم التحكم الآلي: أو التحكم والتواصل في الحيوان والآلة"، استخدم وينر هذا المصطلح لوصف آليات التنظيم الذاتي[9].

وفيما يخص استقصاء مصدر كلمة "سايبر" Cyber ويبدو أنه لا يوجد مصطلح في قواميس اللغة العربية المعتمدة يمكن مقارنته مباشرة بـ«السايبر» Cyber إذ جاء المعنى فى الآتى:

1- يُعرف مصطلح "علم التحكم الآلي" في الطبعة المعاصرة من قاموس المورد بأنه علم التحكم أو دراسة أنظمة التنظيم التلقائي، ويوصف باستخدام صفات مثل "محوسب" أو "حديث للغاية"[10].

2- وفي قاموس المعاني، يُعرَّف بالمصطلح "تخيلي" [11].

ثانياً: الهجوم السيبراني اصطلاحاً:

إن مفهوم الهجوم السيبراني حديث نسبيًا، مما دفع العديد من الخبراء وعلماء القانون إلى محاولة تعريفه بدقة. وسوف نستكشف هذه التعريفات وفقًا لوجهات النظر التي يتبناها مؤيدوها.

وصف فويرتس الهجمات السيبرانية بأنها "عمليات تعتمد على الوصول غير المصرح به إلى مواقع الويب بهدف تعطيلها أو تدميرها أو استخراج البيانات التي يمكن الوصول إليها منها. وهي تنطوي على سلسلة من الأنشطة السيبرانية التي تقوم بها دولة ضد أخرى." وفي الوقت نفسه، عرّفها شميت بأنها "مجموعة من الإجراءات التي تتخذها دولة ما لمهاجمة أنظمة معلومات الخصم للتأثير عليها وإلحاق الضرر بها بينما تدافع في الوقت نفسه عن أنظمة المعلومات الخاصة بالدولة المهاجمة"[12].

ويعرف أيضاً بأنه: "المشاركة المتعمدة في الأنشطة التي تهدف إلى تغيير أو إفساد أو خداع أو إضعاف أو تدمير أنظمة الكمبيوتر أو الشبكات الخاصة بالخصم، بما في ذلك المعلومات والبرامج الموجودة داخل هذه الأنظمة أو المنقولة من خلالها تعكس محاولة محسوبة لتقويض البنى التحتية التكنولوجية"[13].

وإذا كانت الهجمات السيبرانية تستخدم نفسها لاختراق الأنظمة الإلكترونية المصممة لحماية أو تنظيم عمل المرافق الحيوية للسيطرة عليها وتدميرها، فإن الهجمات السيبرانية تعتبر وسيلة للقتال، أي سلاح يستخدم لمهاجمة العدو[14].

من أهم المشاكل التي تواجه المجتمع الدولي في طريقة التعامل مع الهجمات السيبرانية ما يتعلق بالجدل الدائر حول إمكانية اعتبار الأنشطة السيبرانية سلاحا وإمكانية خضوعها لقيود الاتفاقيات المعنية بالحد من السلع، كما رأى بعض الخبراء أنه من غير الصحيح وصف الهجمات السيبرانية بأنها "سلاح" لأنها تفتقر إلى الطاقة الحركية. ولذلك، فهي لا تخضع للأنظمة الدولية المتعلقة باستخدام الأسلحة[15]، وهذا مخالف للواقع، إذ لا يشترط أن تحتوي الأسلحة على طاقة حركية، وخير مثال على ذلك الأسلحة الكيميائية أو البيولوجية. وحقيقة السلاح هو كل ما يمكن أن يحدث ضرراً جسدياً أو مادياً، ويستخدم لغرض الدفاع أو الهجوم أو التهديد[16].

والهجمات السيبرانية في هذا العصر معقدة وخطيرة ولها أنواع متعددة وهي في تزايد مستمر. وعندما تصل أهدافهم إلى محاولة تدمير البنية التحتية لدول بأكملها، أصبح تطويرها في مقدمة أهداف الدول. وتعتبر قدرة ثانية لا تقل أهمية عن القدرات العسكرية وحتى النووية، حيث أن القدرة السيبرانية يمكنها اختراق المنشآت النووية والقاذفات والقواعد العسكرية أو تعطيلها أو السيطرة عليها[17].

وفي هذا السياق، يمكن التأكيد على أن الهجمات السيبرانية، كما نفهمها، تشمل مجموعة من العمليات السيبرانية التي تجريها كيانات حكومية أو مجموعات حكومية وغير حكومية. قد تكون هذه العمليات هجومية أو دفاعية بطبيعتها، وهي مصممة في المقام الأول لإلحاق الضرر أو التسبب في الوفاة أو إتلاف الممتلكات أو تعطيل أهداف محددة من خلال الوصول غير المصرح به إلى جهاز كمبيوتر أو نظام معلومات أو موقع إنترنت. ويتم ذلك دون حق أو سلطة قانونية، ويشمل حذف البيانات وتغييرها وتشفيرها؛ وإعاقة الوصول إلى الخدمة؛ تعطيل الخدمات عمدا باستخدام أي وسيلة؛ تقليل سيطرة المالك على موقعه الإلكتروني؛ أو استخدام البرامج الضارة بأشكال مختلفة لاختراق أنظمة الكمبيوتر أو الشبكات. وإن مفهوم الهجوم السيبراني واسع ويمكن أن يحدث في أي وقت؛ لديها القدرة على إثارة أو الإشارة إلى بداية الأعمال العدائية. إذا حدث مثل هذا الهجوم في خضم نزاع مسلح مستمر، فسيتم تصنيفه على أنه حرب إلكترونية، لأنه يشكل جزءًا من جهد حربي قائم.

المطلب الثاني

الهجوم الإلكتروني (السيبراني) ما دون استخدام القوة

معظم الهجمات الإلكترونية التي حدثت على الأرض تم تنفيذها دون استخدام القوة المسلحة. وتتخذ الهجمات الإلكترونية الأكثر شيوعًا شكل اختراق أجهزة الكمبيوتر وشبكات الويب عن طريق نشر الفيروسات بهدف تعطيلها، أو عن طريق تطعيمها بمعلومات كاذبة بهدف تضليل المستخدمين. هذا النوع من الهجمات هو عبارة عن عملية من عمليات التخريب السيبراني، وهناك شكل آخر شائع وهو استطلاع شبكات الكمبيوتر، حيث يتم اختراق شبكات الخصم من أجل الحصول على البيانات والمعلومات دون تدميرها. وتعتبر مثل هذه الأعمال من أعمال التجسس، خاصة عندما تستهدف معلومات تمس أمن الدولة، مثل الأسرار العسكرية أو الاستخباراتية. وفي كلتا الحالتين، يتم انتهاك الأمن السيبراني دون عنف أو استخدام القوة العسكرية[18].

يمكن النظر إلى العديد من عمليات التطفل الإلكتروني والتدخل في أنظمة الكمبيوتر لجمع المعلومات على أنها أعمال تجسس بين الدول، ويعتبر التجسس جريمة موجودة منذ القدم، ويعتبر التجسس ضد الدولة جريمة بموجب القانون الداخلي للعديد من الدول. . ويتناول القانون الدولي الإنساني أيضًا كيفية التعامل مع الجواسيس أثناء... النزاعات المسلحة، وعلى الرغم من هذا التنظيم القانوني، إلا أن المشكلة تكمن في أن القانون الدولي لا يتناول التجسس الذي يحدث في وقت السلم. إن صمت القانون الدولي تجاه هذا النوع من التجسس يجعل من أعماله مشروعة قانونيا، على الرغم من اعتبارها مستهجنة أخلاقيا وسياسيا، على الأقل من قبل الدولة الضحية[19].

وتتطلب دراسة التجسس الإلكتروني مواجهة مشكلتين: الأولى هي فشل القانون الدولي في معالجة التجسس بشكل صريح، والثانية هي عدم وجود تدوين مناسب في القانون الدولي لممارسات الفضاء الإلكتروني. المشكلة الأولى دفعت جانباً من الفقه القانوني من خلال الاعتراف بأن التجسس ليس محظوراً في القانون الدولي، وهو الأمر الذي عززته الممارسة. تنص على. عقود طويلة من ممارسة بعض الدول التجسس على الدول المعادية والصديقة، لم يقابلها مطلب جدي باعتبار التجسس انتهاكا لمبدأ السيادة. ومن الممارسات التي تؤكد أن التجسس ليس محرماً، قيام بعض الدول بتبادل الجواسيس المعتقلين[20].

يشوب العلاقات بين الدول الكثير من المنافسة والعداء في بعض الأحيان، ولتعزيز معرفة الدول بمنافسيها ونقاط القوة والضعف لديهم، يأتي دور التجسس، والذي يتمثل في جمع المعلومات الاستخبارية. التجسس بمعناه التقليدي هو الممارسة التي تقوم بموجبها دولة ما بإرسال عميل إلى أراض أخرى من أجل الحصول على معلومات سرية، ويشار إليها باسم استخدام الأفراد للحصول على معلومات بذكاء بشري Human Intelligence[21]، والتجسس هو جمع معلومات غير مصرح بها وغير متاحة للعامة. ويجب التمييز بين جمع المعلومات الاستخبارية من مصادر متاحة للجمهور، وهو ما لا يواجه أي مشكلة قانونية، وجمعها من مصادر خاصة غير مصرح بها، وهو ما يرقى إلى مستوى التجسس.

وأصبحت أساليب التجسس أكثر ابتكارا وتنوعا مع التطور التكنولوجي، حيث يتم استغلال السفن والطائرات والأقمار الصناعية لمراقبة المعارضين. وامتدت هذه الأساليب لتشمل الإنترنت، وبسبب الكم الهائل من المعلومات المخزنة إلكترونيا، بالإضافة إلى إمكانية جمعها دون معرفة هوية مرتكب الجريمة، أصبح التجسس الإلكتروني وسيلة جذابة لمرتكب الجريمة[22]، يمكن تعريف التجسس الإلكتروني بأنه العمليات التي تتم عبر شبكة الإنترنت، بغرض جمع معلومات استخباراتية من أجهزة الكمبيوتر أو أنظمة المعلومات أو الاتصالات أو الشبكات، دون علم الضحية أو موافقتها[23]. وتتسم قواعد القانون الدولي بطابع متقدم، فهي قادرة على مواكبة تطورات الأمور على الساحة الدولية[24].

وحق الدولة في التصرف بشكل منفرد في ممتلكاتها، التي تشمل البيانات والمعلومات الرقمية والبنية التحتية للإنترنت، يتطلب تدخل الدول الأخرى، حيث يمنح القانون الدولي الحماية السياسية للبيانات الوطنية، ويطبق احترام سيادة الدول وسلامتها السياسية بالتوازي. لمبدأ عدم التدخل، الذي يحمي حق الدولة السيادي في تقرير شؤونها الداخلية والخارجية دون تدخل خارجي، ويمكن اعتبار مبدأ عدم التدخل مكملاً لمبدأ السيادة. وحماية السيادة تتطلب منع التدخل الخارجي. التدخلات المعنية هي تدخلات من أشخاص القانون الدولي العام، بما في ذلك الدول والمنظمات، ولا تعني تدخل أفراد أو مجموعات، إلا إذا كانت مدعومة من دول أخرى، وقد أكد ميثاق الأمم المتحدة في نصه على هذا المعنى: " ليس في هذا الميثاق ما يجيز للأمم المتحدة التدخل في الشؤون الأساسية للسلطة الداخلية لدولة ما، وليس فيه ما يقتضي من الأعضاء أن يعرضوا مثل هذه الأمور لتحل بأحكام هذا الميثاق"[25].

وإن العديد من عمليات التجسس التي تتم عن طريق التسلل الفعلي تشبه عمليات التنصت الإلكتروني. ومن الناحية النظرية، قد يرى البعض أن الدخول سراً إلى أحد المكاتب لسرقة وثائق سرية لا يختلف عن التسلل الإلكتروني لجهاز الكمبيوتر وسرقة ملف إلكتروني. إن الاعتراف بهذا التشابه ينطوي على الكثير من التبسيط الذي يتجاهل التفاصيل. مهمة تتعلق بالتطفلات الإلكترونية. يوضح فريق من الباحثين في مجال الأمن السيبراني، أن الخيارات المتاحة أمام الجاسوس الذي يتسلل شخصياً إلى أحد المكاتب مستهدفاً ملفاً ما، تظل تقتصر على إما سرقته، أو تدميره بالكامل، أو تغيير محتواه. ومع ذلك، فإن الخيارات المتاحة أمام من يقوم بعملية التسلل الإلكتروني هي أكثر وتتنوع بشكل كبير، بدءًا من مجرد تغيير رقم واحد له تأثير محدود، إلى عمليات اقتحام أوسع لشبكات الإنترنت لأغراض استخباراتية، وحتى إلى تعطيل أكثر تدميراً. مثل شل المعاملات المالية وقطع الاتصالات بشكل كامل لفترات طويلة[26].

والاختلاف في غرض التجسس يغير بشكل جذري تكييف إجراءات التسلل الإلكتروني. ولتوضيح ذلك طرحنا فرضية، وهي أن تقوم دولة ما بزرع برنامج أو جهاز تنصت إلكتروني في منطقة حساسة بدولة أخرى، ويقوم البرنامج بتسجيل المحادثات بغرض جمع المعلومات. وهنا يبدو الغرض واضحا وهو التجسس، لذا فإن أهداف الدولة التجسسية قد لا تتوقف عند هذا الحد، بل تهدف إلى استغلال هذه المعلومات لشن هجمات تخريبية إلكترونية عن طريق إرسال فيروس إلى حواسيب الدولة المستهدفة. ولو تم اكتشاف برنامج التنصت قبل تفعيل الفيروس، فسنكون أمام مشروع تخريبي وليس تجسسياً فقط. يوضح هذا المثال مدى التداخل بين التجسس الإلكتروني والهجمات الإلكترونية الأخرى مثل التخريب. ويعتمد نجاح مثل هذه الهجمات الإلكترونية على نجاح التجسس الإلكتروني[27].

ومع توسع استخدام الفضاء الإلكتروني وإمكانية استغلال ثغرة إلغاء التجريم الصريح للتجسس الإلكتروني، فإن قواعد المعلومات، بما فيها السياسية والاقتصادية والأمنية، قد تتعرض لخطر التخريب أو العبث. في الوقت الحالي تعتمد الدول بقطاعاتها العامة والخاصة بشكل كبير على شبكة الإنترنت وأنظمة المعلومات، لذا فإن أي عمليات تخريب إلكترونية سيكون لها تأثير سلبي على أمن الدولة الداخلي والخارجي، ونقصد بالتخريب الإلكتروني العمليات التي ترتكب لصالح الدولة. بغرض التأثير سلباً على نظم المعلومات وشبكات الاتصال الإلكترونية. ومن أمثلة التخريب الإلكتروني قطع الإنترنت، وحجب الخدمة، والتلاعب بالبيانات والمعلومات، وكذلك استخدام الإنترنت للتأثير على البنية التحتية[28].

وآثار الهجمات السيبرانية ليس لها حدود، حيث يمكن أن تسبب انفجارات في مخازن الوقود والمحطات النووية وجميع المراكز الحيوية، أو تعطيل وسائل النقل البرية أو البحرية أو الجوية، أو تغيير مسار الرحلات الجوية، بالإضافة إلى تعطيلها أنظمة الطاقة وقطع الكهرباء عن مدن بأكملها، وتعطيل أنظمة التحكم والتشويش على الصواريخ والطائرات وتغيير مسارها. أو تعطيل أنظمة الدفاع أو حواسيب أمن المعلومات، وتمتد إمكانياتها إلى تعطيل أجهزة الاتصالات بمختلف أنواعها، ناهيك عن اختراق البنوك وسرقة الحسابات والتلاعب بالتحويلات[29].

ونخلص إلى أنه لكي يتم اعتبار أي هجوم هجومًا إلكترونيًا، يجب أن يتم تنفيذه من قبل جهات حكومية أو غير حكومية، وأن يتضمن سلوكًا نشطًا، ويهدف إلى تعطيل وظائف شبكة الكمبيوتر، وأن يكون له غرض سياسي أو أمني وطني.

وتعتبر بعض الهجمات الإلكترونية أيضًا جرائم إلكترونية، ولكن ليست كل الجرائم الإلكترونية عبارة عن هجمات إلكترونية. ومن ناحية أخرى، فإن الحرب السيبرانية تلبي دائمًا شروط الهجوم السيبراني، ولكن ليست كل الهجمات السيبرانية هي حرب سيبرانية، فقط الهجمات السيبرانية التي لها آثار تعادل آثار "الهجوم المسلح". أما الحروب التقليدية، أو تلك التي تحدث في سياق الصراع المسلح، فهي التي ترقى إلى مستوى الحرب السيبرانية.

المبحث الثاني

التعاون الدولي في مواجهة الهجوم الإلكتروني (السيبراني)

وعلى الرغم من تزايد وتيرة الهجمات السيبرانية والمخاطر المصاحبة لها، هناك غياب ملحوظ لإطار قانوني دولي شامل لتنظيم هذه الأنشطة. ومع ذلك، فإن هذا لا يعني النقص المطلق في الجهود الدولية لمعالجة قضايا الأمن السيبراني. لقد كانت هناك مبادرات مهمة من قبل المنظمات الدولية والإقليمية مثل الأمم المتحدة وحلف شمال الأطلسي ومجلس أوروبا تهدف إلى التخفيف من هذه التهديدات. بالإضافة إلى ذلك، اتخذت كيانات عالمية مختلفة تدابير تساهم بشكل غير مباشر في إدارة منهجيات الهجمات السيبرانية التي يمكن تكييفها لمكافحة الأنشطة السيبرانية الضارة. على سبيل المثال، قد تخدم اللوائح التي وضعها الاتحاد الدولي للاتصالات منذ عام 1947 إلى جانب القوانين التي تحكم الجو والبحر والفضاء أدوارًا ذات صلة في معالجة الجوانب المتعلقة بالأمن السيبراني[30].

واستنادًا إلى مبادئ القانون الدولي الإنساني، فإن شرط مارتنز la clause de Martens وهي وسيلة فعالة لمواجهة التطورات التقنية في وسائل وأساليب القتال كما وردت لأول مرة في اتفاقية لاهاي الثانية لعام 1899 والذي ينص على: "في الحالات التي لا تنطبق فيها المعاهدات أو القانون العرفي، يتمتع المدنيون والعسكريون بالحماية بموجب مبادئ القانون الدولي المستمدة من الأعراف الراسخة، ومن المبادئ الإنسانية، ومن ما يمليه الضمير العام". وانطلاقاً من هذا المعنى، يمكن حظر الأسلحة التي يكرهها الضمير العام[31].

المطلب الأول

التعاون الدولي في مواجهة الهجوم الإلكتروني (السيبراني)

إن مسألة مواجهة الهجمات الإلكترونية (السيبرانية) عند تناولها بشكل عام، قد تثير وتتفرع عن عدة مواضيع بحكم ارتباطها بها. ومواجهتها هي الجانب الفني على أساس أن الهجوم السيبراني كجريمة هي إحدى الجرائم التي لا يمكن أن يرتكبها إلا شخص متخصص تقنيا في تفاصيل وخفايا تكنولوجيا المعلومات. وشبكات المعلومات، بالإضافة إلى الجانب القانوني في مواجهة الآثار وانتهاكات الحقوق الناجمة عن هذه الجرائم، وكذلك على المستوى القانوني نجد أن الرد القانوني قد يكون على المستوى الوطني أو المحلي للدول، ويكون ويمكن أن تكون على المستوى الدولي على أساس أن هذه الجريمة هي جريمة عابرة للحدود ولها طبيعة عابرة للحدود الوطنية والدولية[32].

من الممكن أن يشارك أكثر من شخص في أكثر من دولة في ارتكاب جريمة واحدة يصبح ضحيتها عدة أفراد مقيمين في دول متعددة. ومما يزيد الأمر صعوبة هو اختلاف البيئات والعادات والتقاليد والثقافات والأديان بين الدول المتصلة بالإنترنت، مما يؤدي إلى اختلاف التشريعات المتعلقة بالقضايا الأساسية بين الدول. الشرق والغرب والعالم الإسلامي. قد يتم بث معلومات أو صور على الإنترنت، وقد تكون هذه المعلومات قانونية في البلد الأصلي، ولكنها قد تكون غير قانونية في بلد آخر. كما أن اختلاف التشريعات في تحديد اختصاصها الجنائي بسبب تعدد الأسس التي يقوم عليها هذا الاختصاص قد يؤدي إلى... تضارب الاختصاص بين الدول فيما يتعلق بالجرائم الإلكترونية العابرة للحدود. قد يحدث أن ترتكب جريمة على أراضي دولة معينة ويكون

مرتكب الجريمة شخصًا أجنبيًا. ومن ثم فإن هذه الجريمة تخضع للولاية الجنائية للدولة الأولى على أساس مبدأ الإقليمية، كما تخضع أيضا للولاية القضائية للدولة الثانية على أساس مبدأ الاختصاص الشخصي في جانبه الإيجابي(33).

وتنشأ فكرة تنازع الاختصاص القضائي أيضا في حال قيام الاختصاص على مبدأ الإقليمية، كأن يقوم مرتكب الجريمة ببث معلومات غير قانونية أو صور إباحية من أراضي دولة معينة وتم مشاهدتها في دولة أخرى. ووفقاً لمبدأ الإقليمية، يتم تحديد الولاية القضائية الجنائية والقضائية لكل دولة من البلدان المتضررة من الجريمة. وسواء وقع فعل الإذاعة أو الذي وقع نتيجة الفعل، فهنا نجد أن الأمر سيترتب عليه مخالفة مبدأ عدم جواز محاكمة الشخص على الفعل الواحد أكثر من مرة، وهو واحد للمبادئ الأساسية التي يقوم عليها القانون الجنائي(34).

أولاً: التعاون الدولي بين الأجهزة الشرطية:

أدى التطور الكبير في وسائل النقل بشكل عام وشبكة المعلومات بشكل خاص إلى انتقال المجرمين من دولة إلى أخرى. لقد أدرك المجتمع الدولي أنه أصبح من المستحيل على أي دولة القضاء على الجرائم العابرة للحدود، لأن الإجراءات العامة لأجهزة الشرطة في كل دولة لا تجعل أجهزتها الأمنية تتعقب المجرمين وتتابعهم إذا تجاوزوا حدود الدولة. وعليه لا بد من تعاون الأجهزة الشرطية بين الدول وتنسيق العمل فيما بينها لملاحقة المجرمين. ومن أبرز مظاهر التعاون إنشاء المنظمة الدولية للشرطة الجنائية "الإنتربول" وظهور العديد من أشكال وأشكال ووسائل التعاون بين الأجهزة الشرطية. وهذه الصور والطرق هي كما يلي(35):

- **ربط شبكات الاتصالات والمعلومات:**

يتم الاتصال بين وكالات العدالة الجنائية الوطنية بشكل عام وأجهزة الشرطة بشكل خاص، وبين تلك الأجهزة في البلدان الأخرى من خلال السلك الدبلوماسي. وبما أن الاتصالات الشرطية تحتاج إلى اتصالات خاصة لتحقيق السرعة المطلوبة، فقد حاولت منظمة الشرطة الجنائية الدولية (الإنتربول) وكذلك العديد من الدول تطوير أنظمة الاتصال وتبادل المعلومات فيما بينها، بحيث يمكن الوصول إلى المجرمين وملاحقتهم في أسرع وقت. حيث يغادرون البلد الذي ارتكبت فيه الجريمة، لتسارع أجهزة شرطة البلد الضحية إلى الاتصال بأجهزة الأمن في البلد الذي اتفقوا معه على الأمن للقيام بملاحقة المجرمين داخل حدود بلدهم الذي فرارهم(36).

- **المنظمة الدولية للشرطة الجنائية (الإنتربول):**

يعد الإنتربول أهم آلية للتعاون الشرطي الدولي لمكافحة الجرائم العالمية العابرة للحدود الوطنية بشكل عام والجرائم الإلكترونية بشكل خاص. مهمة الإنتربول الأساسية هي تفعيل التعاون بين الأجهزة الشرطية في الدول الأعضاء في المنظمة من خلال توحيد إجراءات تسليم المجرمين، ومن خلال تنسيق العمل الشرطي وجمع البيانات وتبادل المعلومات لتسهيل أجهزة التحقيق لضبطهم... ملاحقة المجرمين الهاربين وتسليمهم إلى الجهات الأمنية. الدولة التي تطلب تسليمهم، وإنشاء وتطوير كافة الأنظمة القادرة على المساهمة بفعالية في منع جرائم القانون العام والمعاقبة عليها(37).

تُسند هذه المهمة إلى المكاتب المركزية والوطنية في كل دولة عضو وإلى هيئة دائمة تعينها السلطات الحكومية الوطنية، وتساعدها فرق الإنتربول للعمل في الأحداث التي يمكن أن تسهل مجموعة من خدمات التحقيق والتحليل في موقع الموقع. الحفل بالتنسيق مع الأمانة العامة. يقوم الإنتربول بتعميم التحذيرات والتنبيهات المضمنة. المعلومات الاستخباراتية والإحاطات والمشورة التحليلية والفنية بشأن المخاطر الإجرامية المحتملة. ويستخدم الإنتربول أدواته الخاصة، مثل نظام النشرات الدولية بمختلف أنواعها، والتحقيق في قواعد البيانات، وتقديم الخبرات والدورات التدريبية في مجال مكافحة الجرائم الإلكترونية، بمساعدة نخبة من الخبراء الدوليين والمختبرات الدولية على المستوى العالمي، وتسهيل تبادل البيانات الجنائية وتحليلها وتخزينها: وتقوم المنظمة بتزويد شرطة الدول الأطراف بأدلة إرشادية حول الجرائم الإلكترونية وكيفية التدريب على مكافحتها والتحقيق فيها. وتعد الجرائم المالية المرتبطة بالتكنولوجيا المتقدمة إحدى الجرائم التي يركز عليها الإنتربول(38).

- **تبادل المعاونة لمواجهة الكوارث والأزمات:**

في حالة الأزمات وفي المواقف الحرجة، يعتبر عنصر الوقت أحد الأمور الحاسمة في مواجهة تلك الأزمة أو الكارثة، الأمر الذي يتطلب تكثيف وزيادة الجهود والخبرات والإمكانات، وهو ما لا يتأتى إلا بتركيز الجهود الدولية في اتجاه واحد. طريق. على سبيل المثال: مشاركة قوات الإنقاذ والدفاع المدني للدول المنكوبة بالزلازل والأعاصير والفيضانات، أو المشاركة مع خبراء أو توفير معدات متطورة، وكذلك المشاركة بقوات خاصة أو خبراء أو معدات في تحرير الرهائن المحتجزين أو احتلال المباني المهمة، أو طائرات أو سفن مختطفة(39).

- **مظاهر القيام ببعض عمليات شرطية دولية مشتركة:**

1- شرطة الويب الدولية(40):

تأسست هذه المنظمة في الولايات المتحدة الأمريكية عام 1986 لتلقي الشكاوى من مستخدمي الشبكة وملاحقة الجناة والمتسللين إلكترونياً والبحث عن الأدلة ضدهم وتقديمهم للمحاكمة. ويضم فريق العمل في هذه المنظمة متخصصين من جهات إنفاذ القانون والمؤسسات الحكومية وضباط الشرطة والمتطوعين الفنيين من 61 دولة حول العالم، ونظراً لاتساع نطاق نشاط هذه المنظمة. إن التنظيم والإجراءات التي تتخذها بالتعاون مع أجهزة إنفاذ القانون في الدول الأعضاء تسهل على فريق العمل تتبع الأنشطة الإجرامية المرتكبة عبر شبكة الإنترنت في جميع أنحاء العالم. وفي إطار مسألة الضوابط القانونية التي تحكم حركة المعلومات عبر الإنترنت، هناك من يرى أنه من الضروري وضع ضوابط وقواعد لا تؤدي إلى المساس بالحريات العامة في تبادل المعلومات وحقوق الإنسان على حد سواء. من ناحية، وعدم استخدام الشبكة لأغراض إجرامية أو نشر مواد إباحية تضر المجتمع من ناحية أخرى[41].

2- مركز بلاغات احتيالات الإنترنت[42]:

تأسس هذا المركز في الولايات المتحدة الأمريكية عام 2000 للتعاون مع مكتب التحقيقات الفيدرالي FBI والمركز القومى لجرائم ذوى الياقات البيضاء National white collier crime center وذلك بهدف تلقي البلاغات وتتبع الجرائم وعمليات الاحتيال المرتكبة عبر الإنترنت بالتنسيق مع الجهات الرقابية والرقابية المعنية داخل وخارج الولايات المتحدة الأمريكية من خلال الموقع الإلكتروني للمركز على الشبكة الدولية.

ومن أجل تشديد الرقابة على شبكة الإنترنت، طبقت دولة الإمارات العربية المتحدة ما يعرف بنظام الرقيب Proxy والذي يستعرض جودة الخدمات المقدمة عبر الإنترنت. عندما يطلب أحد المشتركين موقعا على الشبكة الرئيسية، تصل الإشارة إلى الرقيب، الذي بدوره يعرض الموضوع على قائمة كبيرة جدا من المواقع المحظورة. فإذا تبين له أن الموقع المطلوب يقع ضمن هذه القائمة المحظورة، فلا يمكن للمشترك الحصول عليه. ويظهر هذا الموقع ورسالة على الشاشة بعنوان: "تم منع هذا الموقع بواسطة رقيب إنترنت الإمارات"[43].

ثانياً: تعاون السلطات القضائية للدول:

ويوازن التعاون القضائي الدولي بين استقلال الدولة في ممارسة اختصاصها الجنائي داخل حدود إقليمها، وضرورة ممارسة حقها في العقاب. ولا يمكن لهذا التعاون، من الناحية العملية، أن ينشئ حقه في العقاب. ومع ذلك، فإن التعاون الدولي ضروري لسببين:

السبب الأول: تلتزم الدولة بحدودها الإقليمية. ويجوز أن يمتد قانون العقوبات في نطاق تطبيقه إلى ما يتجاوز حدود إقليم الدولة. إلا أنه لا يمكن البدء بإجراءات خارج التراب الوطني لأن ممارستها تنتهك سيادة الدول الأجنبية الأخرى.

السبب الثاني: ولا يجوز تطبيق قانون العقوبات دون قانون الإجراءات الجزائية. تعتبر الإجراءات الجزائية الوسيلة اللازمة لتطبيق قانون العقوبات ونقله من حالة السكون إلى الحركة. ولذلك، إذا كان تطبيق قانون العقوبات يقتضي توجيه بعض الإجراءات الجزائية خارج حدود إقليم الدولة، فلا يجب أن تصطدم مشكلة الحدود الإقليمية بين الدول. ولا بد من اللجوء إلى التعاون القضائي للتغلب على هذه الصعوبة، ويتمثل هذا التعاون في مجموعة من الوسائل التي من خلالها تقوم إحدى الدول المساعدة بإخضاع سلطاتها العامة أو مؤسساتها القضائية لسلطة التحقيق أو الحكم أو التنفيذ في دولة أخرى[44].

تتخذ المساعدة القانونية عدة أشكال:

1- تبادل المعلومات:

يتمثل ذلك في تقديم المعلومات والمستندات التي تطلبها جهة قضائية أجنبية بشأن جريمة ما بشأن الاتهامات الموجهة ضد رعاياها في الخارج والإجراءات المتخذة ضدهم. كما أن هناك جانب آخر لتبادل المعلومات، وهو ما يتعلق بالسوابق القضائية للجناة، والتي من خلالها تتعرف السلطة القضائية بدقة على الماضي الإجرامي للفرد المحال إليها، كما تساعد في تنفيذ الأحكام المتعلقة بالعودة، ووقف الجريمة. تنفيذ الحكم، وفقدان الأهلية[45].

2- نقل الإجراءات:

نقل الإجراءات يعني أن تقوم الدولة، بناء على اتفاق، باتخاذ الإجراءات الجنائية فيما يتعلق بجريمة ارتكبت في إقليم دولة أخرى ولصالح هذه الدولة، إذا توافرت الشروط التالية:

- أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب منها.
- يجوز لأي طرف متعاقد أن يطلب من أي طرف آخر اتخاذ الإجراءات الجنائية في أي من الحالات التالية:

- إذا كان المتهم محكوماً عليه أو سوف يحكم عليه بعقوبة مقيدة للحرية في الدولة الطالبة.
- إذا كانت الإجراءات المطلوب اتخاذها منصوص عليها في قانون الدولة المطلوب إليها بالنسبة لنفس الجريمة.
- أن تؤدي الإجراءات المطلوب اتخاذها إلى الوصول إلى الحقيقة، مثل وجود أدلة على الجريمة في الدولة المطلوب منها.
- إذا كان تنفيذ العقوبة في الدولة المطلوب إليها يحقق التأهيل الاجتماعي للمحكوم عليه.

- إذا كان حضور المتهم في الجلسة غير مضمون في الدولة الطالبة بينما حضوره مضمون في الدولة الطالبة بينما حضوره مضمون في الدولة المطلوبة.

- ويجوز للدولة المطلوب إليها أن ترفض نقل الإجراءات في الحالات الآتية:

- إذا كان طلب نقل الإجراءات غير مبرر بأن الأسباب التي ذكرتها الدولة الطالبة لا تستدعي اتخاذ مثل هذه الإجراءات.
- إذا ثبت أن الدافع وراء طلب نقل الإجراءات هو لاعتبارات عنصرية أو دينية أو سياسية.
- إذا كانت الدولة المطلوب إليها قد طبقت قانونها على الجريمة قبل استلامها من الدولة الطالبة وكان الإجراء الذي تم اتخاذه سابقاً وفقاً للقانون.
- إذا كانت الإجراءات التي تطلبها الدولة الطالبة تخالف الواجبات التي تقوم بها الدولة الطالبة.
- إذا كانت الإجراءات المطلوبة تخالف المبادئ الأساسية للنظام القانوني في الدولة المطلوبة.

إلا أن هناك رأياً يُعتقد بحق أن تطبيق هذه الآليات التقليدية للاتفاقيات يثير بعض الإشكاليات، مثل وجود معوقات خاصة بالجرائم المرتكبة عبر الإنترنت. ورغم أن هذه العقبات موجودة على المستوى المحلي أو الوطني، فإنها تنشأ أيضًا على المستوى الدولي[46].

3- الإنابة القضائية الدولية:

تعد الإنابة القضائية أحد أشكال المساعدة القضائية للتعاون الجزائي الدولي، حيث تمكن دولة ما من الاستفادة من السلطات العامة لدولة أخرى إذا كانت الحدود الإقليمية تمنع إنفاذ قانونها ضد المجرم[47].

والمقصود بالتفويض القضائي الدولي هو طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجزائية المقدمة من الدولة الطالبة إلى الدولة المطلوب إليها لضرورة ذلك للبت في أمر معروض على السلطة القضائية في الدولة الطالبة وما يستحيل عليه أن يفعله بنفسه[48]، وعليه فإن الإنابة القضائية هي إجراء لتسهيل الإجراءات الجنائية بين الدول لضمان إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة، وللتغلب على عقبة السيادة الإقليمية التي تمنع الدول الأجنبية من ممارسة بعض الأعمال القضائية داخل الإقليم من بلدان أخرى. ومن الأمثلة على ذلك سماع الشهود وإجراءات إقامة الدعاوى الجنائية.[49].

وتتم الإنابة القضائية بين الدول من خلال اتفاقيات تتضمن شروط وطرق تنفيذ الإنابة القضائية، وغالباً ما تتضمن شرط استبعاد تنفيذ الأحكام في المجالات السياسية والضريبية والعسكرية، أو إذا قدرت الدولة المطلوب إليها أن التنفيذ المطلوب من شأنه الإخلال سيادة الدولة أو النظام العام أو المصالح الأساسية. مما يترك للدولة سلطة تقديرية في تنفيذ أو عدم تنفيذ ما يطلب منها خوفاً من تحميلها المسؤولية الدولية عن إهمالها. وفي حالة عدم الاتفاق، لا يجوز تنفيذ الإنابة القضائية إلا بموافقة الدولة المطلوب إليها ذلك وفقاً للإجراءات والشروط المنصوص عليها في قانونها الداخلي[50].

المطلب الثاني

إمكانية تطبيق القانون الدولي الإنساني على الهجوم الإلكتروني (السيبراني)

على الرغم من أن الهجمات السيبرانية لم تكن موجودة عندما تم إبرام اتفاقيات جنيف الأربع لعام 1949 والبروتوكولين الإضافيين لعام 1977، إلا أن هناك اتفاق دولي واسع النطاق على أن القدرة على استخدام الهجمات السيبرانية بموجب القانون الإنساني الدولي لا ينبغي تقييمها في ضوء مثالية افتراضية. بل يجب مقارنتهم بالبشر. وبناء على ذلك، يمكننا القول إن قواعد القانون الدولي الإنساني التي تنطبق على الأهداف العسكرية المشروعة، معظمها أصبحت قواعد عرفية ومعترف بها من قبل الدول، وبالتالي يمكن تطبيقها على الهجمات السيبرانية[51].

يوفر القانون الإنساني الدولي حماية خاصة لبعض البنى التحتية، مثل الخدمات الطبية والأشياء التي لا غنى عنها لبقاء السكان المدنيين على قيد الحياة، بغض النظر عن نوع العملية التي تسبب الضرر. ومع ذلك، فإن معظم القواعد تنشأ من مبادئ التمييز والتناسب والحيطة التي توفر الحماية العامة للمدنيين والأعيان. تنطبق المدنية فقط على العمليات العسكرية التي تشمل "هجمات" وكما هو محدد في القانون الإنساني الدولي، يتم تعريف الهجمات على أنها: "أعمال العنف ضد الخصم، سواء تم تنفيذها في الهجوم أو الدفاع وبغض النظر عن المنطقة التي يتم فيها تنفيذ هذه الأعمال"[52].

من وجهة نظر اللجنة الدولية للصليب الأحمر، فإن العمليات السيبرانية التي تنفذها الفيروسات والديدان وغيرها من الوسائل التي تسبب ضررًا جسديًا للأشخاص أو أضرارًا مادية للممتلكات بخلاف برامج الكمبيوتر أو البيانات التي تعرضت للهجوم نتيجة للهجوم المباشر أو المتوقع تعتبر الآثار غير المباشرة (أو المرتدة) للهجوم "أعمال عنف" هجوم بالمعنى المقصود في القانون الإنساني الدولي، على سبيل المثال وفاة مرضى في وحدات العناية المركزة نتيجة لعملية سيبرانية ضد شبكة الكهرباء، مما أدى إلى قطع إمدادات الكهرباء عن المستشفى. ومن ثم فمن المتفق عليه على نطاق واسع أن العمليات السيبرانية التي من المتوقع أن تسبب الوفاة أو الإصابة أو الأضرار المادية التي تشكل هجمات بموجب القانون الدولي الإنساني[53].

ومع ذلك، تتعلق بعض البيانات المدنية بأعيان محددة تتمتع بحماية خاصة بموجب القانون الإنساني الدولي[54] وهي الأعيان والمواد التي لا غنى عنها لبقاء السكان المدنيين على قيد الحياة، والأعيان الطبية، والأعمال الهندسية والمنشآت التي تحتوي على مواد وقوى وطاقات خطرة، والبيئة الطبيعية، والأعيان الثقافية وأماكن العبادة[55]، يفترض الالتزام باحترام وحماية هذه الأشياء الخاصة أنه يشمل حماية بيانات هذه الأشياء الخاصة أيضًا[56].

ويقتضي القانون الدولي الإنساني وصف المدني بالمشاركة المباشرة، وذلك باستيفاء ثلاثة شروط: الوصول إلى مدى الضرر، والارتباط بالعمل الحربي، والعلاقة السببية بينهما. في إطار العمل التحضيري للهجمات السيبرانية، غالبًا ما يتم تصميم الأسلحة السيبرانية وبرمجتها خصيصًا لتنفيذها على أهداف محددة ومحددة مسبقًا. مما يجعل من كل هذه التصرفات مشاركة مباشرة في هجمات إلكترونية تؤدي بشكل واضح إلى فقدان الحماية من الهجمات المباشرة وآثار القتال، بالإضافة إلى العقوبة التي قد يتعرض لها المدني المشارك. المشاركة المباشرة في الأعمال العدائية السيبرانية من خلال تصميم وبرمجة الفيروسات والأسلحة السيبرانية وفقاً للقانون الوطني[57].

وبالإضافة إلى ذلك، فإن القانون الدولي لا يمنع أي شخص من حمل السلاح في نزاع مسلح والتحول إلى مقاتل محروم من الامتيازات، لكنه يتطلب ببساطة من كل من يفعل ذلك الالتزام بقواعده التي تحكم سير الأعمال العدائية[58].

علاوة على ذلك، فإن طبيعة التكنولوجيا السيبرانية المختارة تحدد أيضًا ما إذا كان من الممكن الوفاء بالالتزام. يمكن تعطيل الهجمات إذا تم تصنيف الهدف بشكل خاطئ، ولكن فقط إذا كان المهاجم قادرًا على التحكم في السلاح أو الوسائل المستخدمة. ومع ذلك، على سبيل المثال: إذا كان من الصعب إيقاف استخدام برنامج الدولة، الذي يكرر نفسه دون مزيد من السيطرة على الشخص الذي أطلقه للهدف، بسبب طبيعته الفنية، ولا يمكن الالتزام بالالتزام، مما يؤدي إلى المخالفة. للقانون الدولي الإنساني[59]، ومع ذلك، إذا تم تطويرها لتتفوق على البشر، فقد تكون قادرة على الامتثال بشكل أفضل لقواعد القانون الإنساني الدولي[60].

ليس من الضروري شن الهجمات السيبرانية أثناء النزاع المسلح، بل نتيجة للتطور التكنولوجي والاعتماد الشامل على أجهزة الكمبيوتر وشبكات الاتصالات، يمكننا أن نجد مجال تطبيق واسع لها في جميع الأوقات. وقد تستخدم هذه الهجمات في أوقات السلم، مثلاً نتيجة التوتر السياسي أو الهجمات الاقتصادية بين بلدين، أو لتبني سياسة معينة لا تفضلها دولة أخرى، أو لأسباب عديدة أخرى. قد تستهدف الهجمات السيبرانية البنية التحتية للمعلومات والإنترنت، أو يتم توجيهها ضد البنية التحتية الحيوية التي تعتمد على شبكات الكمبيوتر والإنترنت لتشغيلها ووظيفتها. وقد تستهدف القطاع الخاص، بما في ذلك الشركات والبنوك، وهناك إجماع بين المتخصصين في القانون الإنساني الدولي على أن الهجمات الإلكترونية التي تحدث خارج نطاق النزاع المسلح الحركي القائم لا يشترط أن ينظمها القانون الإنساني الدولي. ويتابع لوان جيزيل المستشار القانوني للجنة الدولية للصليب الأحمر: "هذا لا يعني أن القانون الدولي الإنساني ينطبق" وفيما يتعلق بجميع العمليات الإلكترونية، أو ما يسمى في اللغة المشتركة "الهجمات السيبرانية"، فإن القانون الدولي الإنساني لا ينظم العمليات الإلكترونية التي تحدث خارج سياق النزاع المسلح"[61].

الخاتمة

أصبحت دراسة الهجمات السيبرانية ضرورة ملحة في العالم المعاصر الذي يشهد فرض الاستخدامات السلبية للتكنولوجيا. ويتجلى تأثير هذه التطورات بشكل متزايد من خلال التقدم التكنولوجي والتحديات التي تولدها. وهناك ارتباط بين هذه التطورات وقدرة المجتمعات والمنظمات الدولية على التكيف، خاصة فيما يتعلق بالقانون الإنساني.

ومن ثم، لا تظهر الهجمات السيبرانية أي علامات على التراجع، ومن الضروري أن تعمل جميع البلدان على معالجة المخاطر المحتملة المرتبطة بها. ويجب على كل دولة أن تلتزم بمكافحة أي شكل من أشكال الهجمات السيبرانية. كما لا بد من التوعية حول تداعيات هذه الهجمات وضمان الحماية اللازمة على النحو المنصوص عليه في القانون الدولي الإنساني. وقد أسفرت دراستنا الحالية عن العديد من النتائج الهامة والتوصيات الرئيسية، وسوف نوضحها على النحو التالي:

أولاً: النتائج:

- يعد مفهوم الهجمات السيبرانية قضية حديثة نسبيًا ولم تحظ بإجماع دولي بعد. ويمكن الإشارة إليها في المادة 26 من البروتوكول الإضافي الأول لعام 1977، وكذلك من خلال مختلف أحكام وآراء محكمة العدل الدولية، بما في ذلك تلك المتعلقة بشرعية التهديد بالأسلحة النووية أو استخدامها.
- يتسم الهجوم السيبراني بكفاءته في التنفيذ نظرًا لانخفاض تكاليفه مقارنةً بالعمليات العسكرية التقليدية، والتي قد تشمل حشد الجنود وآلاف من المعدات والأسلحة.
- سهولة استخدام الهجوم السيبراني من قبل شخص واحد أو مجموعة صغيرة لديهم الخبرة والمهارة في مجال التكنولوجيا السيبرانية ونقاط الضعف البرمجية لاستخدامها ضد دولة أو دول أخرى.
- وجود قوانين تنظم الأنشطة السيبرانية، مثل الاتفاقيات الدولية والوطنية، رغم أنها تسبق ظهور الهجوم الإلكتروني (السيبراني)، إلا أنها تنظم الوسائل والأدوات التي يمكن استخدامها في تنفيذها، والتي يمكن الرجوع إليها، مع العلم أنهم لم يرتقوا إلى مستوى التنظيم الشامل لهذا الهجوم.

ثانياً: التوصيات:

- السعي الحثيث لاعتماد الاتفاقيات الدولية لتنظيم الهجمات السيبرانية.
- التأكد من الوعي الشامل بالتقنيات والمهارات المطلوبة للتعامل مع الهجمات السيبرانية من خلال تدريب وتثقيف مهندسي تكنولوجيا المعلومات الناشطين في هذا المجال.
- تطوير أساليب الأمن السيبراني لتأمين وحماية البنية التحتية الوطنية من التهديدات السيبرانية.
- تعزيز تبادل المعلومات بين الدول والمنظمات الدولية والإقليمية لمكافحة سوء استخدام تكنولوجيا المعلومات.

الهوامش:

(1) البغى، رغدة (2017): الردع السيبرانى – المفهوم والإشكاليات والمتطلبات، المركز الديمقراطى العربى، ع1، مجلة العلوم السياسية والقانونية، القاهرة، ص 3.

(2) البابلى، عمار ياسر زهير (2018): الآليات الحديثة لحماية وتأمين نظم المعلومات وآثارها على المنظومة الأمنية، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، ص 44.

(3) Philip Levitz, The law of cyber attack, 2012, vol.37, issue 4,p 890.

(4) الموصلى، أنور أمير (2021): الهجمات السيبرانية فى ضوء القانون الدولى الإنسانى، رسالة ماجستير، فى القانون الدولى الإنسانى، الجامعة الافتراضية السورية، سوريا، ص 7.

(5) المرجع السابق، ص 7.

(6) Pande, Nihar Ranjan: Cyber Attacks and Counter Measures: User Perspective, (Post Graduate Diploma in Cyber Security), Uttarakhand Open University, Haldwani 2016, P1.

(7) بن صابر، بلقاسم (2017): الهجمات السيبرانية ومواجهتها في ضوء القانون الدولى المعاصر، مجلة حقوق الإنسان والحريات العامة، ع4، جامعة عبد الحميد بن باديس، الجزائر، ص 188.

(8) Microsoft Computer Dictionary, Fifth Edition, Microsoft Press, Washington, 2002, p138.

(9) Cybernetics or Control and Communication in The Animal and The Machine. See: Wiener, Norbert: Cybernetics or Control and Communication in The Animal and The Machine, M.I.T, Press, Second Edition, Cambridge, Massachusetts, 1948.

([10]) البعلبكي، رمزي منير (2009): المورد الحديث، دار العلم للملايين، بيروت، ص 307.

([11]) موقع قاموس المعاني: معنى كلمة سايبر، على الرابط: https://www.almaany.com/ar/dict/ar-en/cyber/

([12]) الفتلاوي، أحمد عبيس نعمة (2018): الهجمات السيبرانية (دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر)، ط1، منشورات زين الحقوقية، بيروت (لبنان)، ص 16.

([13]) لين، هربرت (2012): النزاع السيبراني والقانون الدولي الإنساني، مختارات من المجلة الدولية للصليب الأحمر، مج94 (886)، ص 518.

([14]) الفتلاوي، أحمد عبيس نعمة، مرجع سابق، ص 21.

([15]) كلنتر، زهراء عماد محمد (2016): المسئولية الدولية الناشئة عن الهجمات السيبرانية، كلية القانون، جامعة الكوفة، العراق، ص 31.

([16]) شهاب، محمود إبراهيم عبد الرحمن (2007): الأسلحة غير التقليدية في الفقه الإسلامي، الجامعة الإسلامية، كلية الشريعة والقانون، غزة، فلسطين، ص 2.

([17]) الموصلي، أنور أمير، مرجع سابق، ص 16.

([18]) عبد الصادق، عادل (2020): الاقتصاد الرقمي وتحديات السيادة السيبرانية، المركز العربي لأبحاث الفضاء الإلكتروني، القاهرة، ص 36.

(19) Geoffrey B. Demarest, "Espionage in International Law", Denver Journal of International Law and Policy 24 (1996): 326.

(20) Gary Brown and Keira Poellet, "The Customary International Law of Cyberspace", Strategic Studies Quarterly Vol. 6, No. 3, (2012), 133.

(21) Russell Buchan, "The International Legal Regulation of State-Sponsored Cyber Espionage" in Anna-Maria Osula and Henry Rõigas (eds.), International Cyber Norms: Legal, Policy and Industry Perspectives Tallinn: NATO CCD COE, 2016, 65-66.

([22]) آل مواش، ضرغام جابر عطوش (2017): جريمة التجسس المعلوماتي، المركز العربي للنشر، القاهرة، ص 82.

(23) Presidential Policy Directive/PPD-20, U.S. Cyber Operations Policy (October 2012), http://www.fas.org/irp/offdocs/ppd/ppd-20.pdf

([24]) عبيد، عيسى (2017): محكمة العدل الدولية ودورها في تطوير قواعد القانون الدولي الجنائي، دار أمجد، عمان، ص 105.

([25]) الفقرة الثانية من المادة (7) من ميثاق الأمم المتحدة، 26 يونيو 1945.

(26) Brown, Gary and Poellet, Keira, "The Customary International Law of Cyberspace", Strategic Studies Quarterly, vol. 6, No. 3, Cyber Special Edition (2012), pp. 135 - 136.

(27) Idem, pp. 135.

([28]) خليفة، إيهاب (2016): القوة الإلكترونية – كيف يمكن أن تدير الدولة شؤونها في عصر الإنترنت؟، العربي للنشر والتوزيع، القاهرة، ص 88.

([29]) علاو، غيث (2020): الهجمات السيبرانية.. أكبر حروب نووية بوسائل إلكترونية، مقال منشور على الموقع الإلكتروني: https://aljadah.media/archives/77072

([30]) الموصلي، أنور أمير، مرجع سابق، ص 21.

([31]) دوسولد، لويز، ونويتن، بك وآنا (2000): الأسلحة الحديثة والقانون الدولي الإنساني، ندوة علمية حول القانون الدولي الإنساني: الواقع والطموح، اللجنة الدولية للصليب الأحمر، جامعة دمشق كلية الحقوق، ص 158.

([32]) الزهراني، شيخة حسين (2020): التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، مج 17، ع1، ص 743.

(33) الصغير، جميل عبد الباقي (2001): الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، ص 72، فضل، سليمان أحمد (2007): المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، مصر، ص 411.

(34) الأجولي، سالم محمد سليمان (1997): أحكام المسئولية الجنائية عن الجرائم الدولية في التشريعات الوطنية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ص 419.

(35) الزهراني، شيخة حسين، مرجع سابق، ص 744.

(36) الأجولي، سالم محمد سليمان، مرجع سابق، ص 421، شحاتة، علاء الدين (2000): التعاون الدولي في مجال مكافحة الجريمة، د.ن، القاهرة، ص 110، فضل، سليمان أحمد، مرجع سابق، ص 414، داود، عيسى سليم (2017): جرائم القرصنة الإلكترونية، رسالة ماجستير، جامعة الإسكندرية، ص 134.

(37) العازمي، فهد عبد الله العبيد (2016): الإجراءات الجنائية للمعلوماتية، دار الجامعة الجديدة، مصر، ص 651.

(38) العازمي، فهد عبد الله العبيد، مرجع سابق، ص 653، داود، عيسى سليم، مرجع سابق، ص 134، وانظر أيضاً: معلومات عن الإنتربول، لمحة عامة، الموقع الرسمي لمنظمة الشرطة الجنائية الدولية، على الموقع الإلكتروني: https://www.interpol.int/ar/interne.

(39) يوسف، حسن يوسف (2011): الجرائم الدولية للإنترنت، المركز القومي للاتصالات القانونية، القاهرة، ط1، ص 148، الشمري، غانم مرضي (2016): الجرائم المعلوماتية، دار الثقافة، الأردن، ص 98.

(40) انظر موقع المنظمة http://www.web-police.org

(41) فضل، سليمان أحمد، مرجع سابق، ص 417.

(42) http://www.ifccbi.gov/index.asp.

(43) الصغير، جميل عبد الباقي، مرجع سابق، ص 78.

(44) عبيد، حسنين صالح (1977): القضاء الجنائي الدولي (تاريخه – تطبيقاته – مشروعاته)، دار النهضة العربية، القاهرة، ص 99 – 100.

(45) الدسوقي، طارق إبراهيم، مرجع سابق، ص 569، داود، عيسى سليم، مرجع سابق، ص 136، فضل، سليمان أحمد، مرجع سابق، ص 422.

(46) الصغير، جميل عبد الباقي، مرجع سابق، ص 80.

(47) صدقي، عبد الرحيم (1983): التعاون الدولي في الفكر المعاصر، مجلة القانون والاقتصاد، جامعة القاهرة، ص 249.

(48) مهدي، عبد الرؤوف، مرجع سابق، ص 102، الدسوقي، طارق إبراهيم، مرجع سابق، ص 572.

(49) السند، متعب بن عبد الله (2011): التعاون الدولي في تنفيذ الأحكام الجنائية وأثره في تحقيق العدالة، رسالة ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، ص 108 – 109.

(50) الصغير، جميل عبد الباقي، مرجع سابق، ص 85.

(51) الموصلي، أنور أمير، مرجع سابق، ص 33.

(52) البروتكول الإضافي الأول لعام 1977، المادة 49.

(53) اللجنة الدولية للصليب الأحمر (2019): القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، ورقة موقف اللجنة الدولية للصليب الأحمر، ص 7.

(54) حمدان، إيمان (2020): التكنولوجيا الجديدة والقانون الدلي الإنساني (الحرب السيبرانية)، دراسات معمقة في القانون الدولي الإنساني، رسالة ماجستير في القانون الدولي الإنساني، الجامعة الافتراضية السورية، سوريا، ص 9.

(55) كلزي، ياسر (2020): النظرية العامة في القانون الدولي الإنساني، رسالة ماجستير في القانون الدولي الإنساني، الجامعة الافتراضية السورية، سوريا، ص 102.

(56) حمدان، إيمان، مرجع سابق، ص 9.

(57) الموسوي، علي محمد كاظم (2019): المشاركة المباشرة للهبة الجماعية في الهجمات السيبرانية، مجلة كلية الحقوق، جامعة النهرين، بغداد، ص 15.

(58) ميلزر، نيلس (2016): مقدمة شاملة القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، ص 165 – 166.

([59]) Lülf, Charlotte: Modern Technologies and Targeting Under International Humanitarian Law, Working Paper, Vol.3, No3, IFHV, Ruhr University Bochum, Germany,2013, p. 44.

([60]) سعود، يحي ياسين (2018): الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، جامعة يحي فارس، الجزائر، ص99.

([61]) كلنتر، زهراء عماد محمد ، مرجع سابق، ص 42 – 44.