إشكالية الحرب السيبرانية وصور الاختراقات السيبرانية

ايمان هاتف نايف تفاح
الجامعة الإسلامية /لبنان

المستخلص:

إن الاهتمام الفقهي والتشـــريعي بالحرب الســـيبرانية من الموضـــوعات بالغة التعقيد فعلى الرغم من وجود تشـــريعات حمائية رامية إلى الإحاطة بالتطورات الفائقة التي تتصـــل بصـــور الإرهاب والجرائم الســـيبرانية، فالحروب الســـيبرانية باتت تتخذ أســـاليب متطورة في الابتزاز والاختراق للأمن الدول والأفراد، وعليه أصـــبح استخدام الفضاء السيبراني محاط بالمخاطر ويلزم معه تعظيم الدور الرقابي للدول لحماية أمنها وأمن مواطنيها. تقوم المؤسسات والمنظمات العالمية كالأمم المتحدة بإصدار الاتفاقيات التي تضمن من خلالها المواجهة والحد من الآثار المدمرة، وكذلك التشريعات الوطنية للدول وهو ما يلزم معه التكاتف المؤسساتي داخل الدول من أجل تحقيق الحماية اللازمة.

الكلمات المفتاحية: الحرب السيبرانية – الأمن السيبراني- المخاطر السيبرانية.

Abstract

Jurisprudential and legislative interest in cyberwarfare is a highly complex topic. Despite the existence of protective legislation aimed at addressing the dramatic developments related to forms of terrorism and cybercrime, cyberwarfare has become increasingly sophisticated in its use of blackmail and infiltration of the security of states and individuals. Consequently, the use of cyberspace has become fraught with risks, requiring states to enhance their oversight role to protect their security and that of their citizens.

Global institutions and organizations, such as the United Nations, are issuing agreements to ensure confrontation and mitigation of the destructive effects, as are national legislation. This requires institutional cooperation within states to achieve the necessary protection.

Keywords: Cyberwarfare - Cybersecurity - Cyber Risks

المقدمة

تتميز الحرب السيبرانية عن الحرب التقليدية في أن الأخيرة تعتمد على الجيوش النظامية وتتطلب إعلانًا رسميًا للحرب وتحديدًا لميدان المعركة. أما الهجمات السيبرانية، فهي غير محكومة بمحددات جغرافية أو أهداف واضحة، إذ تتم عبر الشبكات الإلكترونية التي تتخطى الحدود الوطنية. تعتمد هذه الهجمات على أدوات إلكترونية متطورة تستهدف البنى التحتية الحيوية أو تُنفذ بواسطة عملاء استخباراتيين.

من جهة أخرى، يمكن التمييز بين الحرب السيبرانية والحرب التقليدية استنادًا إلى نوع الأسلحة المستخدمة، حيث تتميز الحرب السيبرانية باستخدام أسلحة غير تقليدية تؤدي إلى تدمير واسع النطاق. أحد الأمثلة على ذلك هو هجمات "رفض الخدمة" (DoS)، التي تستهدف تعطيل الأنظمة عن طريق إغراق المواقع الإلكترونية بطلبات وهمية تمنع الوصول إليها، مما يعرقل العمليات الحيوية.

تعرف الأسلحة غير التقليدية وفقًا للأمم المتحدة بأنها تشمل الأسلحة النووية والكيميائية والبيولوجية، بالإضافة إلى أي أسلحة مستقبلية قد تظهر وتتمتع بتأثير تدميري مماثل للأسلحة النووية.[١].

يعرض تعريف الموضوع في البحث مسألة جوهرية تتعلق بتصنيف الهجمات السيبرانية كجزء من نزاع مسلح، سواء كان دوليًا أو غير دولي. فالقانون الدولي الإنساني، الذي يهدف إلى تقليل تبعات النزاعات المسلحة لأسباب إنسانية، يختص بمثل هذه الحالات. ومن هنا، يصبح من الضروري تحديد بوضوح الحالات التي تُعتبر نزاعًا مسلحًا، وهو أمر بالغ التعقيد في حال الهجمات السيبرانية، التي تتميز بارتكابها في ظروف غير منظمة بشكل أساسي.[٢].

أولاً: أهمية البحث:

تتصل أهمية البحث بموضوع الحروب السيبرانية والتي تعد من الموضوعات التي تمس أمن المجتمع الدولي واستقرار الدول وهو ما يلقي على عاتق المؤسسات الأمنية والرقابية مسؤولية معقدة تدور بين الكشف عن الجرائم ومرتكبيها وبين حماية خصوصية المواطنين من جراء الهجمات السيبرانية، وهو ما يتم بيانه من خلال البحث.

[١] عمر بن عبد الله بن سعيد البلوشي مشروعية أسلحة الدمار الشامل وفقًا لقواعد القانون الدولي منشورات الحلبي الحقوقية بيروت ٢٠٠٧ ص ١٧.
[٢] عمر مكي القانون الدولي الإنساني والإرهاب اللجنة الدولية للصليب الأحمر ص ٩٣.

ثانيًا: أهداف البحث:

يهدف هذا البحث إلى تشكيل العي والمعرفة حول مفهوم الحرب السيبرانية والمفاهيم ذات الصلة كالأمن السيبراني، بالإضافة إلى الحديث حول المخاطر السيبرانية وصور الهجمات السيبرانية وآثارها المدمرة.

ثالثًا: المنهجية:

اعتمدت المنهج الوصفي من أجل العرض للحروب السيبرانية وماهيتها، وكذلك البيان المخاطر السيبرانية وهو ما اعتمدت فيه على المرجعيات والأبحاث ذات الصلة.

رابعًا: الإشكالية:

حيث إن الحرب السيبرانية تهدد الاستقرار عالميًا وهو ما يسترعي الاهتمام والمواجهة التشريعية والحماية اللازمة لحقوق الافراد من الاختراق وأمن الدول من الحروب السيبرانية التي تهدد الاستقرار والبنى التحتية.

وهي ما تتمثل في الإجابة على التساؤل:

ما هي مخاطر الحروب السيبرانية على أمن الأفراد والدول؟

خامسًا: خطة البحث:

من أجل الإجابة على الإشكالية فإنني قسمت البحث إلى مبحثين الأول خاص بالتعريفات والمفاهيم والثاني خصص للحديث عن مخاطر الحرب السيبرانية والتجسس السيبراني.

- **المبحث الأول:**
- **مفهوم الحرب السيبرانية**

مع تطور الحروب، أصبح من الواضح أن أساليبها أصبحت أكثر تدميرًا وقسوة، مع تقليص الخسائر في المعدات والأرواح. ويرتبط هذا التحول بشكل وثيق بالتقدم التكنولوجي، حيث أصبح استخدام التقنيات المتطورة والحروب السيبرانية هو السمة الرئيسية للصراعات المعاصرة[٣]، تركز القوات العسكرية على تدمير الأنظمة الدفاعية مثل الرادارات وأجهزة الدفاع الجوي قبل بدء الاشتباكات المباشرة. في المقابل، تسعى الدول إلى تعزيز أنظمة دفاعها بهدف الكشف المبكر عن أي هجمات سيبرانية أو محاولات لتجاوز دفاعاتها.[٤]

[٣] القانون الدولي الإنساني وفتوى محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها اللجنة الدولية للصليب الأحمر موقع إلكتروني ٢٠١٨/٨/١٠ -WWW.icrc.org.

[٤] نوال أحمد بسيح القانون الدولي الإنساني وحماية المدنيين والأعيان المدنية في زمن النزاعات المسلحة ط ١ منشورات الحلبي الحقوقية ٢٠١ ص ٨٧.

وقد دفعني ذلك إلى دراسة مفهوم الحرب السيبرانية في هذا البحث من خلال تحليلها من الجوانب اللغوية والاصطلاحية، مع استعراض مختلف الآراء الفقهية والقانونية المتعلقة بها، وذلك على النحو التالي.

- **المطلب الأول: التعريف بالحرب السيبرانية**

يعود مصطلح "السيبرانية" في اللغة إلى الكلمة اليونانية "cybernetes"، التي تعني القيادة والتحكم عن بُعد. [٥] عرف مايكل ن. شمية الهجمات السيبرانية بأنها الإجراءات التي تتخذها دولة لاستهداف نظم المعلومات الخاصة بالعدو بهدف تعطيلها أو إلحاق الضرر بها، بالإضافة إلى حماية نظم المعلومات الخاصة بها. مثال على ذلك الهجوم السيبراني المعروف بـــ "الجندي البرونزي" في إستونيا، الذي استهدف تمثالًا برونزيًا يمثل أحد رموز الاتحاد السوفيتي السابق. أدى هذا الهجوم إلى تعطيل مواقع الحكومة والبنوك في إستونيا، ما تسبب في توقف عمل البنوك وتعطل شبكات الاتصال في المنطقة.

إذا تحولت الهجمات السيبرانية إلى نزاع مسلح، فإنها تُعتبر جزءًا من الحرب السيبرانية، وهي عملية إلكترونية هجومية أو دفاعية قد تؤدي إلى إصابة أو قتل أفراد أو تدمير أعيان. وبذلك، يمكن للهجمات السيبرانية أن تتجاوز نطاق الحرب السيبرانية، وتحدث خارج سياق الحروب التقليدية، بل وقد تكون دافعًا لاندلاع الحرب. [٦]

وبناءً على ذلك، تعد الهجمات السيبرانية جزءًا من الحرب السيبرانية عندما تُستخدم ضمن نزاع مسلح لتحقيق أهداف عسكرية. ويمكن تعريفها بأنها الإجراءات التي يتخذها أطراف النزاع للاستفادة من التقنيات المتطورة والأفراد المتخصصين في الفضاء الرقمي للسيطرة على الأنظمة الإلكترونية للعدو. وتشمل هذه الهجمات تدمير أو تعطيل أو اختراق أنظمة الحاسوب أو الحصول على معلومات سرية عبر التجسس السيبراني أو استغلال الشبكات، شريطة أن تتم في سياق نزاع مسلح يصل إلى مرحلة الحرب. [٧] في عام ٢٠٢٢، نفذ قراصنة روس هجومًا سيبرانيًا على الوكالات الحكومية الأوكرانية لاستهداف معلومات أمنية حيوية تتعلق بالاستجابة للطوارئ. أدى الهجوم إلى تعطيل نظام الاستجابة الفورية للحكومة الأوكرانية لبلاغات المواطنين، مما أحدث

---

[٥] د. أحمد عبيس نعمة التلاوي الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر مجلة المحقق الحلي للعلوم القانونية والسياسية جامعة بابل – كلية القانون العدد الرابع السنة الثامنة ٢٠١٦ ص ٦١٤.

[٦] عمر بن عبد الله بن سعيد البلوشي مشروعية أسلحة الدمار الشامل وفقًا لقواعد القانون الدولي منشورات الحلبي الحقوقية بيروت ٢٠٠٧ ص ١٥

[٧] المادة (٥١) من ميثاق الأمم المتحدة.

حالة من الشلل في العمليات الحيوية، بالإضافة إلى تسريب بيانات سرية تمس الأمن القومي الأوكراني.[٨]

يُعد مبدأ منع استخدام القوة في العلاقات الدولية من القواعد الأساسية في القانون الدولي، حيث يُعتبر التزامًا جوهريًا على الدول بعد أن عانت من آثار الحروب والصراعات التي أسفرت عن خسائر جسيمة في الأرواح والموارد. وقد أقر ميثاق الأمم المتحدة هذا المبدأ في مادته الثانية، الفقرة الرابعة، التي تحظر على الدول الأعضاء تهديد أو استخدام القوة ضد سلامة الأراضي أو الاستقلال السياسي للدول الأخرى، أو بأي وسيلة تتناقض مع أهداف الأمم المتحدة. وقد تم تأكيد هذا المبدأ في العديد من الوثائق الدولية، إذ تتيح بعض استثناءات القانون الدولي استخدام القوة في حالات معينة، مثل تحرير الرهائن أو مكافحة الإرهاب، وفق ضوابط وشروط محددة.

على الرغم من ثبات هذا المبدأ كقاعدة قانونية دولية ملزمة، إلا أن الحروب والنزاعات المسلحة لم تتوقف، ما دفع الدول إلى تعزيز قدراتها العسكرية وتوسيع ترساناتها لحماية أمنها. وقد لعب التطور التكنولوجي دورًا رئيسيًا في ابتكار أسلحة جديدة وطرق مبتكرة لشن الحروب، ما أسفر عن ظهور الفضاء السيبراني كأداة حيوية في العمليات العسكرية. أصبح هذا الفضاء وسيلة أساسية لتنفيذ الهجمات وإدارة النزاعات باستخدام تقنيات حديثة تمامًا مقارنة بأساليب الحرب التقليدية.

الفضاء السيبراني هو بيئة افتراضية تعتمد على أنظمة الحاسوب، الشبكات الإلكترونية، والبيانات الضخمة. وقد عرّف الاتحاد الدولي للاتصالات الفضاء السيبراني كمنظومة مادية وغير مادية تشمل مكونات مثل أجهزة الكمبيوتر، الشبكات، البرمجيات، محتوى الإنترنت، وأنظمة النقل والتحكم الرقمي. من جهة أخرى، نظر بعض الخبراء إلى الفضاء السيبراني من منظور عسكري، معتبرين إياه الذراع الرابعة للجيوش الحديثة. وقد تبنت فرنسا هذا المفهوم في قواتها المسلحة، حيث اعتبرت الفضاء السيبراني من الأفرع الحيوية التي لا تقل أهمية عن الأسلحة والقطاعات العسكرية الأخرى في الجيش، بل أصبح جزءًا أساسيًا من استراتيجياتها الدفاعية. [٩]

---

[٨] رؤى حمود، مقال بعنوان (أشهر الهجمات الإلكترونية حتى ٢٠٢٢: حروب من نوع آخر!)، منشور على موقع rng، ٢٠٢٢،

[٩] د. إبراهيم سيف منشاوي، دمج القدرات السيبرانية في تقرير التوازن العسكري ٢٠٢٠، مركز المستقبل للأبحاث والدراسات المتقدمة، ٢٠٢١،
https://futureuae.com/ar/Mainpage/Item/٦١٥٩/%D٨٪AA%D٨٪AD%D٩٪٨٨٪D٩٪٨٤٪D٨٪A٧٪D٨٪AA-%D٨٪A٧٪D٩٪٨٤٪D٩٪٨٢٪D٩٪٨٨٪D٨٪A٩-%D٨٪AF%D٩٪٨٥٪D٨٪AC-%D٨٪A٧٪D٩٪٨٤٪D٩٪٨٢٪D٨٪AF%D٨٪B١٪D٨٪A٧٪D٨٪AA-%D٨٪A٧٪D٩٪٨٤٪D٨٪B٣٪D٩٪٨A%D٨٪A٨٪D٨٪B١٪D٨٪A٧٪D٩٪٨٦٪D٩٪٨A%D٨%A٩-%D٩٪٨١٪D٩٪٨A-%D٨٪AA%D٩٪٨٢٪D٨٪B١٪D٩٪٨A%D٨٪B١-

عرفت الوكالة الفرنسية لأمن أنظمة المعلومات (ANSSI)، وهي الهيئة الحكومية المكلفة بالدفاع السيبراني في فرنسا، الفضاء السيبراني على أنه "مجال التواصل المتشكل من خلال الربط المتبادل بين أجهزة المعالجة الآلية للبيانات الرقمية». يُعتبر الفضاء السيبراني بيئة تفاعلية حديثة تضم عناصر مادية وغير مادية، تتكون من مجموعة من الأجهزة الرقمية، أنظمة الشبكات، البرمجيات، والمستخدمين سواء كانوا مشغلين أو مستعملين. من جهته، عرف أستاذ العلوم السياسية الأمريكي "جوناي" الفضاء السيبراني على أنه القدرة على استخدام الفضاء الإلكتروني لخلق مزايا استراتيجية والتأثير على الأحداث في البيئات التشغيلية الأخرى.

الفضاء السيبراني هو البيئة الافتراضية التي تتفاعل فيها المعلومات السيبرانية عبر شبكات الكمبيوتر، حيث يُعتبر أيضًا المجال الكهرومغناطيسي الذي يُستخدم لتخزين وتعديل أو تغيير البيانات المتصلة بشبكة البنية التحتية الطبيعية. يشمل ذلك عملية التكامل بين الإنترنت، الأجهزة المحمولة، شبكات الاتصالات، والأقمار الصناعية. ويُعتبر الفضاء السيبراني أوسع من الإنترنت، إذ يحتوي على قدرات توجيهية للطاقة التي تتواجد ضمن نطاق الموجات الكهرومغناطيسية. [١٠].

في الوقت الراهن، يُعتبر الفضاء السيبراني، وفقًا للمفهوم الأمريكي، البُعد الخامس في الحروب بعد البر والبحر والجو والفضاء. كما أعلنت حكومة المملكة المتحدة أن استراتيجيتها في الحرب السيبرانية تجاوزت مجرد تأمين البلاد ضد الهجمات الإلكترونية، لتصبح استراتيجية تسعى إلى تطوير أسلحة إلكترونية استعدادًا لمتطلبات المستقبل. جاء هذا التوجه بعد تعرض المملكة المتحدة لعدة هجمات سيبرانية استهدفت بيانات الجنود في الجيش البريطاني، وكان أبرزها الهجوم الذي طال وزارة الدفاع البريطانية.[١١]

تُعرف المخاطر بأنها التهديدات التي تستهدف أمن الأفراد والبيئة والمجتمعات، والتي قد تكون على وشك الحدوث أو قد حدثت بالفعل، ويمكن السيطرة عليها إذا لم تتفاقم. وتشمل المخاطر أي تهديد يواجه مؤسسات الدولة، سواء كان ناتجًا عن الأيديولوجيات أو عن استخدام عناصر قوة

%D٨٪A٧٪D٩٪٨٤٪D٨٪AA%D٩٪٨٨٪D٨٪A٧٪D٨٪B٢٪D٩٪٨٦-
%D٨٪A٧٪D٩٪٨٤٪D٨٪B٩٪D٨٪B٣٪D٩٪٨٣٪D٨٪B١٪D٩٪٨A-٢٠٢٠

[١٠] انظر: د. عادل عبد الصادق الفضاء الإلكتروني والرأي العام تغير المجتمع والأدوات والتأثير المركز العربي لبحوث الفضاء الإلكتروني: قضايا استراتيجية ٢٠١٣ ص:٢٩.

[١١] مقال بعنوان(تسريب بيانات جنود الجيش البريطاني في اختراق لوزارة الدفاع)، بوابة الجزيرة ، ٧/ ٥/ ٢٠٢٤،
https://www.ajnet.me/tech/٢٠٢٤/٥/٧/%D٨٪AA%D٨٪B٣٪D٨٪B١٪D٩٪٨A%D٨٪A٨-
%D٨٪A٨٪D٩٪٨A%D٨٪A٧٪D٩٪٨٦٪D٨٪A٧٪D٨٪AA-
%D٨٪AC%D٩٪٨٦٪D٩٪٨٨٪D٨٪AF-%D٨٪A٧٪D٩٪٨٤٪D٨٪AC%D٩٪٨A%D٨٪B٤-
%D٨٪A٧٪D٩٪٨٤٪D٨٪A٨٪D٨٪B١٪D٩٪٨A%D٨٪B٧٪D٨٪A٧٪D٩٪٨٦٪D٩٪٨A-
%D٩٪٨١٪D٩٪٨A

دولة ضد دولة أخرى. ويمكن أن يشمل ذلك تهديدًا لإقليم الدولة، استقلالها، أو أمنها، حيث قد تنبع التهديدات من الخارج أو من داخل الدولة نفسها. [١٢].

تتعدد المفاهيم المتعلقة بالمخاطر السيبرانية، ومن أبرزها:

الأمن السيبراني: يشمل مجموعة من العمليات التقنية الحديثة والممارسات التي تهدف إلى حماية الشبكات وأجهزة الكمبيوتر والبيانات من الهجمات، الأضرار، أو الوصول غير المصرح به. وفي سياق التقنيات الحديثة، يتم تعريف الأمن السيبراني إلى جانب الأمن المادي على أنه مجموعة من الأدوات والاستراتيجيات الأمنية، بالإضافة إلى المبادئ التوجيهية وأساليب الإدارة المستخدمة لحماية الفضاء السيبراني والموارد التنظيمية للمستخدمين. من الأمثلة على ذلك برامج مكافحة الفيروسات والشبكات التي توفر حماية للبيانات والمعلومات، والتي تتسم بالتعقيد، وتستمر في التحديث لمكافحة التهديدات والكشف عن البرمجيات الخبيثة. [١٣].

عرف الاتحاد الدولي للاتصالات الأمن السيبراني على أنه "مجموعة من الأدوات، السياسات، المفاهيم الأمنية، الضمانات الأمنية، المبادئ التوجيهية، والتقنيات، بالإضافة إلى أساليب إدارة المخاطر التي تُستخدم لحماية البيئة الإلكترونية وتنظيم أصول المستخدمين. ويشمل ذلك تأمين أجهزة الحوسبة، الموظفين، البنية التحتية، الخدمات، نظم الاتصالات السلكية واللاسلكية، وجميع المعلومات المرسلة أو المخزنة في البيئة الإلكترونية» [١٤].

يمكن تعريف الأمن السيبراني من خلال أهدافه كالنشاط الذي يهدف إلى حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، وضمان الحد من الخسائر والأضرار الناتجة عن المخاطر والتهديدات السيبرانية. كما يسعى إلى تمكين عملية التعافي السريع وإعادة الأمور إلى طبيعتها في أقرب وقت ممكن. ويُعتبر الأمن السيبراني النشاط أو القدرة التي تحمي نظم المعلومات والاتصالات الخاصة بالدولة، حيث تكون المعلومات الواردة فيها محمية من التلف أو الاستخدام غير المصرح به أو التحليل أو الاستغلال.

الأمن السيبراني يشمل مجموعة من الوسائل التقنية، التنظيمية والإدارية التي تُستخدم لمنع الاستخدام غير المصرح به أو سوء الاستغلال، واستعادة المعلومات الإلكترونية ونظم الاتصالات

---

[١٢] تيري ديبي استراتيجية الشئون الخارجية منطق الحكم الأمريكي ترجمة وليد شحادة دار الكتب العربية مؤسسة محمد بن راشد آل مكتوم بيروت ٢٠٠٩ ص: ٢٥٨.

[١٣] قاسم محمد حسين، اساسيات في الأمن السيبراني، كلية الكنوز الجامعة- قسم الأمن السيبراني-، ٢٠٢٣، ص٣.

[١٤] الاتحاد الدولي للاتصالات ITU دراسة عن تأمين شبكة المعلومات والاتصالات قطاع تنمية الاتصال فترة الدراسة (٢٠٠٦- ٢٠١٠) متاع على الموقع الإلكتروني التالي:
https://WWW.Ittu.Int/net/Itunews/issues/٢٠١٠/٩/Pdf/٢٠١٠٠٩-٢٠-ar.pdf

في حال حدوث اختراقات. الهدف من ذلك هو ضمان توافر واستمرارية عمل نظم المعلومات، وتعزيز حماية سرية البيانات الشخصية وخصوصيتها، بالإضافة إلى اتخاذ التدابير اللازمة لحماية الأفراد والمستهلكين من المخاطر في الفضاء السيبراني.

يُعد الأمن السيبراني سلاحًا استراتيجيًا مهمًا لكل من الحكومات والأفراد، خاصةً مع تزايد دور الحرب السيبرانية كجزء أساسي من التكتيكات الحديثة في الحروب والهجمات بين الدول. يشمل الأمن السيبراني حماية المعلومات على أجهزة الحاسوب وشبكات الإنترنت، بما في ذلك جميع العمليات والآليات التي تهدف إلى حماية المعدات والخدمات من أي تدخل غير مرغوب فيه أو تغيير أو تلف قد يحدث. [١٥].

الجريمة السيبرانية هي مجموعة من الأفعال غير القانونية التي تُنفذ عبر الأجهزة الإلكترونية أو شبكة الإنترنت، أو تُبث من خلالها. وتُعد من أنواع الجرائم التي تتطلب معرفة متخصصة بتقنيات الحاسوب ونظم المعلومات سواء في تنفيذها أو التحقيق فيها أو ملاحقة مرتكبيها.

وقد عرفها البعض بأنها "أي فعل أو امتناع عن فعل يتم باستخدام نظام معلوماتي معين للإضرار بمصلحة أو حق محمي قانونيًا عبر جزاء جنائي، سواء كانت هذه المصالح أو الحقوق تتمثل في نماذج معلوماتية جديدة أو كانت تندرج ضمن الحقوق والمصالح المحمية جنائيًا وفقًا للطرق التقليدية. كما يمكن أن يحدث الاعتداء داخل حدود الدولة أو يتجاوزها ليشمل مجموعة من الدول» [١٦]. ومثال ذلك ما وقع في دولة قطر[١٧] مثال على ذلك هو اختراق وكالة الأنباء القطرية، حيث تم بث مقاطع وأخبار مفبركة تتعلق بأمير الدولة. وقد اعتبرت دولة قطر هذا الحادث جريمة سيبرانية تتعلق بالاعتداء على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية. وقد نصت القوانين القطرية على عقوبة في هذه الحالة تتمثل في الحبس لمدة أقصاها ٣ سنوات وغرامة مالية تصل إلى ٥٠٠ ألف ريال[١٨]

---

[١٥] د. لامية طالة الإرهاب السيبراني والأمن القومي: قراءة في تحولات الاستراتيجية الدفاعية حوليات جامعة الجزائر١ المجلد ٣٥ العدد ٤ ٢٠٢١م ص٣٥٦.

[١٦] د. هلالي عبد اللاه أحمد جرائم الحاسب والإنترنت بين التجريم الجنائي وآليات المواجهة دار النهضة العربية ٢٠١٥ ص:١١٧.

[١٧] موقع الجزيرة، مقال- حصار قطر كيف بدأ؟ وإلى أين وصل؟ -، ٢٠١٨م.
https://www.aljazeera.net/encyclopedia/events/٢٠١٨/٥/٢٣/حصار-قطر-كيف-بدأ-وإلى-أين-وصل

[١٨] المادة ٢ من الباب الثاني، قانون ١٤ لسنة ٢٠١٤ الخاص بمكافحة الجرائم الإلكترونية، بوابة الميزان، https://almeezan.qa/LawView.aspx?opt&LawID=٦٣٦٦&language=ar

الهجمات السيبرانية، وفقًا لمبادئ "تالين" حول الحروب السيبرانية، تُعرَف بأنها العمليات الإلكترونية التي تهدف إلى إلحاق الأذى بالأشخاص أو تدمير الأهداف والممتلكات. وتشمل هذه العمليات الهجومية والدفاعية التي قد تؤدي إلى إصابات أو وفيات أو أضرار جسيمة للأعيان [١٩]

- **المطلب الثاني: طبيعة المخاطر السيبرانية وسماتها**

تتيح تكنولوجيا المعلومات والاتصالات إمكانيات استثنائية في تحسين الإنتاجية وتعزيز التواصل العالمي. لكن البنية التحتية لهذه التقنيات تربط مصالح وخدمات متعددة عبر عدة دول، مما يخلق تهديدات سيبرانية ذات طابع عالمي. وبناءً على ذلك، لا يمكن لأي جهة أن تضمن حمايتها الكاملة ما دامت هناك مخاطر تهدد الآخرين. - **المخاطر التقنية:**

تتميز تقنيات المعلومات والاتصالات بخصوصيات تجعلها عرضة لمخاطر محددة ترتبط بطبيعتها وبيئتها التشغيلية في الفضاء السيبراني. ورغم دورها الكبير في توسيع نطاق الاتصال الرقمي، فإن الاعتقاد بأنها يمكن أن تحل محل القانون في تنظيم الفضاء السيبراني وضبط المخالفات الأمنية غير دقيق. لقد أثبتت هذه التقنيات عجزها عن ضمان سلامة الأفراد والمؤسسات والدول التي تعتمد عليها بشكل متزايد.

الدول المتقدمة أبرزت هشاشة الوضع الأمني، مشيرة إلى الثغرات الموجودة في البرمجيات والأجهزة التي يمكن للقراصنة استغلالها. ورغم وجود حلول تقنية، فإنها تظل غير كافية، إذ تقدم ردود فعل محدودة لا تتماشى مع سرعة تغير المخاطر. بالإضافة إلى ذلك، تتضاعف التحديات بسبب تنوع الجهات المعنية بالأمن السيبراني وتعدد المهارات المطلوبة، مما يعقد قدرة الجميع على فهم المخاطر واتخاذ تدابير فعالة. كما أن تقنيات الحماية تحتاج بدورها إلى أنظمة حماية أخرى لضمان فعاليتها.

- يمكننا الاستنتاج أن الاعتماد على الحلول التقنية يعد بمثابة الاقتراب من المجهول، خاصة في ظل صعوبة التحكم في هذه التقنيات وما قد تطرأ عليها من أعطال أو مشاكل غير مرئية، والتي قد لا تظهر إلا بعد أن يتم تطبيقها عمليًا. ولكن، رغم هذه القيود التقنية، لا يعني ذلك التقليل من أهمية تطوير آليات الحماية التقنية، بل يجب تعزيزها بشكل مستمر. يتعين الاستفادة من البرامج والتطبيقات المصممة خصيصًا للحد من الوصول غير المصرح به إلى البنى التحتية والأنظمة المعلوماتية. ومن بين هذه التدابير، تكمن أهمية إدارة الهوية

[١٩] دليل تالين وهو مجموعة من المبادئ أعدها بعض الخبراء في القانون الدولي الإنساني عام ٢٠١٣ أبرزهم الأستاذ مايكل شيمت بالتعاون مع حلف شمال الأطلنطي ويدعم من فريق مؤلف من خبراء الليبرالية واللجنة الدولية للصليب الأحمر والقيادة الليبرالية الأمريكية الذين شاركوا في المداولات كافة.

الإلكترونية، واستخدام برامج مكافحة الفيروسات، وتطبيق بروتوكولات التشفير لضمان أمان المعلومات وحمايتها.

- **ـ المخاطر القانونية:**

تكمن المخاطر القانونية في غياب الإطار التشريعي والتنظيمي المناسب للتعامل مع نتائج الأفعال القانونية وغير القانونية التي تتم في الفضاء السيبراني. إذ يتطلب النشاط الاقتصادي والتجاري تحديدًا دقيقًا للحقوق والواجبات، مما يعزز الثقة في قدرة تقنيات المعلومات والاتصالات على تقديم خدمات موثوقة عبر الإنترنت. في هذا السياق، تتمثل المخاطر القانونية في غياب الاستقرار القانوني، وتضارب الأحكام والتشريعات، فضلاً عن التداخل بين الأنظمة القانونية. كما تتفاقم هذه المخاطر مع تزايد انتشار الجرائم الإلكترونية، التي لا تقتصر فقط على الأفراد، بل تشمل أيضًا تهديدات تمس أمن واستقرار الدول. إن ضعف التعاون الدولي في ملاحقة مرتكبي هذه الجرائم يزيد من تعقيد الأمور ويعزز من انتشار هذه المخاطر.

المخاطر السيبرانية وحق الدفاع الشرعي وفقًا للمادة ٥١ من ميثاق الأمم المتحدة:

نص ميثاق الأمم المتحدة في مادته الثانية، الفقرة (٤)، على حظر استخدام القوة أو التهديد بها في العلاقات الدولية من قبل جميع الأعضاء. ومع ذلك، حدد الميثاق بعض الاستثناءات لهذه القاعدة، أبرزها المادة (٥١)، التي تمنح الدول حق الدفاع عن نفسها في حال تعرضها لهجوم مسلح. وقد تبنت محكمة العدل الدولية تفسيرًا محدودًا لهذه المادة، مؤكدةً على أن حق الدفاع يقتصر فقط على الحالات التي يكون فيها الهجوم المسلح من دولة ضد دولة أخرى. وفي قضية "منصات النفط" عام ٢٠٠٣، قدمت المحكمة أمثلة توضح هذا الهجوم، معتبرةً أن استهداف منشآت أو منصات عسكرية قد يصل إلى مستوى الهجوم المسلح الذي يبرر حق الدفاع[٢٠].

في قضية "نيكاراجوا" عام ١٩٨٦، قررت محكمة العدل الدولية استبعاد ما اعتبرته مجرد حادثة حدودية من نطاق الهجوم المسلح. وأكدت المحكمة أن الأعمال التي تقتصر على نزاع حدودي أو تلك التي لا تمثل تهديدًا مباشرًا للسلامة الإقليمية لدولة ما، لا يمكن تصنيفها على أنها هجوم مسلح يبرر الدفاع وفقًا للمادة (٥١) من ميثاق الأمم المتحدة.[٢١] في رأيها الانفرادي في قضية "الجدار العازل" التي نظرتها المحكمة عام ٢٠٠٤، أوضحت القاضية "Rosalyn" أنها غير مقتنعة بأن التدابير غير القسرية، مثل بناء الجدار، يمكن أن تُعتبر ضمن نطاق الدفاع عن النفس وفقًا للمادة

[٢٠] حكم محكمة العدل الدولية في قضية (Oil Platforms) ٢٠٠٣ الفقرات (٥٧: ٦١).
[٢١] حكم محكمة العدل الدولية في قضية (Nicaragua v, USA) ٢٧ يونيو ١٩٨٦ الفقرة ١٩٥.

(٥١) من ميثاق الأمم المتحدة. وأكدت أنه من أجل تفعيل هذا الحق، يجب أن تواجه الدولة تهديدًا مسلحًا.

وبناءً على ذلك، يضمن القانون الدولي للدول حق الدفاع عن نفسها باستخدام وسائل فردية أو جماعية. وهذا يعني أن لكل دولة الحق في اتخاذ التدابير التي تراها ضرورية لضمان بقائها واستقرارها، بما في ذلك استخدام الوسائل الدفاعية المناسبة ضد المخاطر الداخلية أو الخارجية التي تهدد أمنها ومصالحها العليا.[٢٢] نظرًا للطبيعة العابرة للحدود للهجمات السيبرانية التي يمكن أن تتجاوز حدود السيادة الوطنية، فإن مواجهتها تتطلب تعاونًا دوليًا متكاملًا لضمان السلم والأمن على المستوى العالمي. في هذا السياق، يرى البعض أن الإجراءات التي اتخذتها دولة "إسبانيا" ضد محاولة استقلال إقليم "كتالونيا" تمثل دفاعًا شرعيًا عن أمن الدولة واستقرارها. وقد نالت إسبانيا دعمًا دوليًا في مواجهة هذه المحاولة، حيث أكدت غالبية الدول أن ما يحدث هو شأن داخلي لا ينبغي التدخل فيه. وعُدّ ما تقوم به إسبانيا من خطوات بمثابة تجسيد للسيادة الوطنية واحترامًا لدستورها وتشريعاتها الداخلية، مما ساهم في إضعاف قوة المحاولة الانفصالية من جانب إقليم "كتالونيا".

إن استخدام معيار درجة الخطورة لتصنيف العمليات السيبرانية كهجوم مسلح يطرح إشكالية تتعلق بكيفية تقدير هذه الخطورة وتقييمها. ومع ذلك، يمكن اللجوء إلى تقييم تأثير العملية على الدولة المستهدفة. على سبيل المثال، إذا تسببت عملية سيبرانية في تعطيل أو إعاقة مؤسسات الدولة عن أداء مهامها، ونتج عنها أضرار يصعب تداركها، مثل تخريب الأجهزة الحيوية في المنشآت الطبية مما يؤدي إلى وفيات، فإن مثل هذه العمليات يمكن أن تُعتبر معادلة لاستخدام القوة العسكرية. وبالتالي، يكون للدول الحق في الرد عليها استنادًا إلى المادة (٥١) من ميثاق الأمم المتحدة التي تقر بحق الدفاع عن النفس في مواجهة الهجمات المسلحة.

على المستوى الوطني، اعتمدت بعض الدول معيار درجة الخطورة لتصنيف العمليات السيبرانية وتحديد ما إذا كانت تشكل هجومًا مسلحًا يستدعي الرد وفقًا للمادة (٥١) من ميثاق الأمم المتحدة. ومن بين هذه الدول، الولايات المتحدة الأمريكية التي قدمت تقريرًا إلى الأمم المتحدة في عام ٢٠١١، أكدت فيه أن الأنشطة التخريبية في الفضاء السيبراني قد تشكل في بعض الحالات هجومًا مسلحًا. وفي مثل هذه الظروف، لا ينبغي الاقتصار على الرد الإلكتروني المضاد فقط، بل يتطلب الأمر اتخاذ إجراءات عسكرية تقليدية للرد على الهجوم.

---

[٢٢] د. إسماعيل صبري مقلد أصول العلاقات الدولية في إطار عام دار النهضة العربية الطبعة الأولى ٢٠٠٧ ص: ٦-٢٠.

كان الفقه الدولي واضحًا في تحديد الخط الفاصل بين الهجوم السيبراني والاعتداء العسكري التقليدي. وقد ساهم الفقيه الدولي "جان بيكلت" في هذا المجال بتحديد مجموعة من المعايير التي يجب توافرها لكي يُعتبر الاعتداء هجومًا عسكريًا. هذه المعايير تشمل: النطاق، الذي يشير إلى نطاق التأثير الجغرافي والزمني للهجوم؛ الشدة، التي تقيس مدى قوة الهجوم وأثره على الأهداف المستهدفة؛ والمدة الزمنية، التي تحدد مدى استمرارية الهجوم وأثره على القدرة الدفاعية للدولة المهاجمة.[٢٣]

المبحث الثاني:

وسائل الحروب السيبرانية ونماذج الاختراق

- **المطلب الأول: وسائل الحرب السيبرانية**

تختلف الحرب السيبرانية عن الحرب التقليدية في العديد من الجوانب الجوهرية. في الحرب التقليدية، يتضمن الصراع استخدام الجيوش النظامية مع إعلان صريح لحالة الحرب وميدان قتال محدد، مما يجعل النزاع قابلًا للتحديد من حيث المكان والزمان. في المقابل، تتميز الهجمات السيبرانية بعدم تحديد مجال واضح وهدف غامض، حيث تتحرك عبر شبكات المعلومات والاتصالات التي تتجاوز الحدود الوطنية. كما أن هذه الهجمات تعتمد على "أسلحة إلكترونية" حديثة ومتطورة، صممت خصيصًا لمواكبة التطور السريع في عالم المعلومات. يتم توجيه هذه الهجمات ضد المنشآت الحيوية أو من خلال عملاء تابعين لأجهزة الاستخبارات، ما يجعلها أكثر تعقيدًا وتخفيفًا للحدود التقليدية في الحروب. وبالتالي، يُمكن تمييز الحرب السيبرانية عن الحرب التقليدية من خلال نوع السلاح المستخدم، الذي يعتمد على التكنولوجيا الرقمية بدلاً من الأسلحة المادية المعروفة.[٢٤].

تتمثل أمثلة استخدام العمليات السيبرانية خلال النزاعات في مجموعة من الأنشطة المتنوعة مثل التجسس على المعلومات، تحديد الأهداف، وتنفيذ عمليات معلوماتية تهدف إلى التأثير على معنويات العدو وإرادته تجاه الاستمرار في القتال. كما تشمل هذه العمليات قطع أو تشويش نظم اتصالات العدو لتقليل قدرته على تنسيق قواته، إضافة إلى دعم العمليات الحركية عبر تعطيل محطات الرادار العسكرية لضمان فعالية الضربات الجوية. ومع أن الحرب السيبرانية تركز في

---

[٢٣] موقع الجزيرة، مقال- حصار قطر كيف بدأ؟ وإلى أين وصل؟ -، ٢٠١٨م.
https://www.aljazeera.net/encyclopedia/events/٢٠١٨/٥/٢٣/حصار-قطر-كيف-بدأ-وإلى-أين-وصل

[٢] يحيى ياسين سعود الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني المجلة القانونية المجلد ٤ العد ٤ ٢٠١٨ متاح على الرابط: https://jlaw.journals.ekb.eg/article_٤٥١٩٢.html

جزء كبير منها على استهداف القدرات والأنظمة العسكرية، إلا أنها تتجاوز ذلك لتشمل الهجمات على البنية التحتية الحيوية للمجتمع، مما يعكس التحديات الجديدة التي تطرأ على أمن الدول في عصر التقنيات المتطورة.[٢٥].

تشمل الأسلحة السيبرانية مجموعة واسعة من الأدوات والوسائل التكنولوجية التي تستخدم في الهجمات الإلكترونية، مثل الفيروسات والديدان الحاسوبية التي تهدف إلى تدمير أو تعطيل الأنظمة. كما تشمل عمليات جمع البيانات السيبرانية التي تستهدف المعلومات الحساسة، بالإضافة إلى أجهزة تشويش اتصالات البيانات اللاسلكية التي تعوق نقل المعلومات عبر الشبكات. هناك أيضًا برمجيات حاسوبية مزيفة تروج للتطبيقات المضللة، وأسلحة النبض الكهرومغناطيسي التي تستخدم لتدمير الأنظمة الإلكترونية. بالإضافة إلى ذلك، تشمل الأسلحة السيبرانية أدوات استطلاعات الحاسوب والشبكات والقنابل الزمنية الطروادية المدمجة التي تهدف إلى اختراق الأنظمة الإلكترونية بشكل خفي وتهديد البنية التحتية للمؤسسات. [١]

يرى البعض أن الحرب السيبرانية أو الهجمات السيبرانية يمكن تصنيفها إلى ثلاثة مستويات رئيسية.

المستوى الأول: يتمثل في العمليات المصاحبة للحروب التقليدية، مثل الهجوم على نظام الدفاع الجوي، وهو ما قد يؤدي إلى خسائر استراتيجية كبيرة نتيجة أهمية الدفاع الجوي بالنسبة للدول.

المستوى الثاني: يتضمن الحرب الإلكترونية المحدودة، حيث تستهدف الهجمات السيبرانية البنية التحتية والأهداف المدنية بشكل محدد، مما يسبب أضرارًا واسعة في هذه القطاعات الحيوية.

المستوى الثالث: يتعلق بالحرب الإلكترونية غير المحدودة، حيث يسعى المهاجم إلى تعظيم الأضرار المدمرة للبنية التحتية للدولة. يتضمن ذلك مهاجمة أسواق المال، خدمات الطوارئ، الأنظمة الإلكترونية الخاصة بمولدات الطاقة، وغيرها من الأهداف ذات التأثير التدميري الواسع. الهدف من هذا النوع من الهجمات هو تعظيم الخسائر المادية على نطاق واسع. [٢]

أصبح استخدام العمليات السيبرانية أثناء النزاعات المسلحة أحد السمات المميزة للحروب الحديثة، حيث يُنظر إليه اليوم كأداة فعّالة في ساحة المعركة الرقمية. ويُشير بعض المحللين إلى أن أول تطبيق فعلي للهجمات السيبرانية وقع خلال حرب كوسوفو عام ١٩٩٩، حين استهدفت هجمات إلكترونية نظم الاتصالات الهاتفية في يوغسلافيا السابقة، في محاولة لتعطيل قدرات سلاح الجو التابع لحلف شمال الأطلسي (الناتو). [٣]

---

[٣] لور انجيزلو تيلمان رودنها وسرو كنوند ورمان القانون الدولي الإنساني وحماية المدنيين من أثار العمليات السيبرانية أثناء النزاعات السلحة المجلة الدولية للصليب الأحمر مجلد ٢٠٢٠٩١٣١٠٢ من

اعترفت عدد من الدول بشكل علني بتنفيذها عمليات سيبرانية خلال نزاعات مسلحة معاصرة. فقد أعلنت كل من الولايات المتحدة، والمملكة المتحدة، وأستراليا، عن استخدام تلك العمليات في إطار مواجهتها لتنظيم الدولة الإسلامية، ضمن استراتيجية متعددة الأبعاد. كما وردت تقارير تفيد بقيام إسرائيل بشن هجمات إلكترونية استهدفت البنية التحتية التابعة لحركة حماس. ولم تقتصر آثار هذه العمليات على تلك الدول فحسب، بل امتدت لتشمل دولًا أخرى انخرطت في نزاعات، مثل الهجمات التي استهدفت جورجيا في عام ٢٠٠٨، وأوكرانيا في الفترة ما بين ٢٠١٥ و٢٠١٧، مما يعكس اتساع نطاق الحروب السيبرانية وتأثيرها المتزايد على الساحة الدولية.[٤] في عام ٢٠٠٩، كشفت تقارير استخباراتية أمريكية أن بعض الجماعات المسلحة استغلت فترة احتلال العراق لاختراق أنظمة إلكترونية كانت تستقبل معلومات حساسة من طائرات الاستطلاع بدون طيار، مما مكنها من تتبع التحركات العسكرية الأمريكية والتعامل معها بفعالية. وفي السياق ذاته، بدأت روسيا بشن هجمات إلكترونية على أوكرانيا منذ عام ٢٠١٤، استهدفت من خلالها البنية التحتية والمعلومات الحيوية بهدف التخريب. وكررت هذه المحاولات عام ٢٠٢٢، سعيًا لزرع الفوضى وشل قدرات الدفاع الأوكرانية، من خلال استهداف شبكات الطاقة، ومزودي الخدمات، والمؤسسات المالية، ووسائل الإعلام.[٥]

- **المطلب الثاني: الاختراقات السيبرانية والتجسس السيبراني**

شهدت أساليب القرصنة تطورًا ملحوظًا بفضل التقدم التقني، حيث استغل القراصنة أدوات التكنولوجيا الحديثة لتنفيذ هجماتهم بطرق مبتكرة، أبرزها نشر البرامج المقرصنة عبر مواقع إلكترونية مخصصة، إما مجانًا أو مقابل مبالغ زهيدة. هذا التحول ألحق أضرارًا جسيمة بالشركات العاملة في مجال تطوير البرمجيات، خاصة تلك المختصة بأمن المعلومات وأنظمة التشغيل، مما دفعها إلى تأسيس جهات رقابية لمتابعة هذه الظاهرة وتحليلها، مثل اتحاد برمجيات الأعمال، الذي يضطلع بإجراء دراسات متخصصة ووضع استراتيجيات للحد من تفشي السوق السوداء للبرمجيات.[٢٦].

يشير مصطلح "القرصنة" إلى أي عملية اختراق غير مصرح بها تستهدف أنظمة الحواسيب أو الشبكات أو البيانات، بغرض التلاعب بها أو إلحاق الضرر. وتتجلى هذه الممارسات في صور متعددة من السلوك الإجرامي، أبرزها الجرائم السيبرانية التي تمثل أحد أبرز مظاهرها.

[٢٦] د. أميرة عبد العظيم محمد عبد الجواد المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام المرجع السابق ص: ٤٠٨.

تُعدّ القرصنة من أبرز صور التهديدات السيبرانية، خاصة إذا استهدفت تعطيل أنظمة المعلومات أو الإضرار بالبنية التحتية الحساسة التي تُدار عبر الشبكات، وقد تمتد آثارها لتشمل الإيذاء الجسدي أو القتل بدوافع سياسية أو أيديولوجية أو مالية وغيرها.

- **وتتنوع أنماط الهجمات والاختراقات السيبرانية، ومنها:**

١. التسلل إلى المواقع الإلكترونية وصفحات الإنترنت بقصد تخريبها أو حذفها أو تعديل محتواها أو إتلاف البيانات المخزنة عليها.

٢. اختراق قواعد البيانات بهدف حذف أو تعديل محتوياتها، أو سرقة معلومات حساسة مثل أسماء المستخدمين وكلمات المرور وبيانات الاتصال، واستخدامها بشكل غير قانوني أو بيعها لجهات ذات مصالح اقتصادية أو سياسية أو أمنية.[٢٧].

توجد وسائل تقنية متعددة تسهم في تسهيل عمليات القرصنة، من أبرزها اعتراض حزم البيانات أثناء انتقالها عبر الشبكات، وهجمات العاصفة التي تستهدف إغراق الأنظمة بالطلبات لتعطيلها، إضافة إلى تقنيات كسر كلمات المرور، وتجاوز الذاكرة المؤقتة بهدف الوصول غير المشروع إلى المعلومات والأنظمة.

تنقسم تهديدات الأمن السيبراني إلى ثلاث فئات رئيسية من حيث النية: التجسس الإلكتروني بهدف الربح المالي، أو تعطيل الأنظمة العسكرية والبرمجيات الحساسة، أو مراقبة المسارات السياسية للدول، وتشمل كذلك تجسس الشركات، سرقة الملكية الفكرية، والتجسس الذي ترعاه الدول. وتندرج غالبية الهجمات الإلكترونية ضمن واحدة من هذه الفئات.

أما من حيث الأساليب، فهناك طيف واسع من الأدوات التي تعتمدها الجهات المعادية للوصول إلى أهدافها، إذ يتوفر لديها العديد من التقنيات الهجومية، وتُعد عشرة منها الأكثر شيوعًا على مستوى العالم. ومن أبرز الأمثلة على التهديدات التي تستهدف الدول:

١- **البرمجيات الخبيثة:** تشمل التهديدات السيبرانية استخدام برمجيات خبيثة تُصمَّم لتنفيذ مهام ضارة على الأجهزة أو الشبكات المستهدفة، مثل تدمير البيانات أو السيطرة على الأنظمة. وقد ظهر هذا النوع من الهجمات بشكل واضح في روسيا عام ٢٠١٣، عندما كشفت شركة أمن سيبراني روسية عن انتشار واسع لبرامج خبيثة أصابت ملايين من مستخدمي أجهزة Android، خاصة في روسيا والدول الناطقة بالروسية. كما شهد العالم في عام ٢٠١٠ هجومًا سيبرانيًا استهدف البرنامج النووي الإيراني، حيث تم توجيه ضربة إلكترونية لأجهزة الطرد المركزي

---

[٢٧] للمزيد انظر: د. عادل عبد الصادق أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني وحدة الدراسات المستقبلية المرجع السابق ص: ٤٣.

المســـتخدمة في تخصـــيب اليورانيوم، وهو ما دفع طهران إلى اتهام الولايات المتحدة بالوقوف وراء الهجوم.

وتشـــير هذه الأحداث إلى أن الحروب القادمة قد لا تعتمد على الســـلاح التقليدي، بل على "قوات إلكترونية" ترسل عبر الفضاء الرقمي، قادرة على اختراق الشبكات، وتعطيل البنى التحتية، وشل الأنظمة الحيوية للدول المستهدفة.

٢-**التصـــيد.** يعد التصـــيد الاحتيالي عبر البريد الإلكتروني أحد أســـاليب الهجوم التي تعتمد على خداع الضـــحية للكشـــف عن معلومات حســـاســـة أو تنزيل برمجيات ضـــارة من خلال النقر على روابط مشبوهة في الرسائل. أما التصيد بالرمح، فهو شكل أكثر تطورًا من التصيد التقليدي، حيث يقوم المهاجم بتحديد الضحية بدقة، ويتنكر في شخصية شخص موثوق به من محيط الضحية، مما يزيد من مصداقية الهجوم.

على سبيل المثال، في حادثة وقعت في الهند، شنّت مجموعة تجسس إلكتروني هندية حملة تصيد احتيالي استهدفت الوكالات الحكومية الصينية والشركات المملوكة للدولة. كان الهدف من الهجوم الحصـول على معلومات حسـاسـة تتعلق بالأنشـطة الاقتصـادية والتجارية، بالإضـافة إلى قضـايا الدفاع والعلاقات الخارجية.[٢٨]

٣- **هجوم رفض الخدمة أو هجوم رفض الخدمة الموزع.** هجوم الحرمان من الخدمة الموزع (DDoS) هو هجوم يســـتهدف تعطل الأنظمة عبر اســـتغلال العديد من الأجهزة المخترقة، التي تقوم بإرســـال طلبات مكثفة إلى النظام المســـتهدف، مثل موقع ويب، مما يؤدي إلى تعطيله بســـبب الحمل الزائد. ومن الدول التي تسـجل أعلى معدلات لهذه الهجمات تأتي الصـين في المقدمة بنسـبة ٢٩,٥٦٪، تليها الولايات المتحدة بنسبة ٢١,٥٩٪، ثم المملكة المتحدة بنسبة ٦١,١٧٪.

وفي عام ٢٠١٥، تعرض نظام الطاقة في أوكرانيا لانقطاع كبير في التيار الكهربائي نتيجة هجوم منســق اســتهدف أنظمة SCADA وشــبكات النظام المضــيف، مما أدى إلى تعطيل العمليات. تم اســتخدام برامج ضــارة لاســتغلال الثغرات في الشــبكة، وإنشــاء نظام قيادة وتحكم لتأخير عملية الاستعادة. بالإضـافة إلى ذلك، تم شـن هجوم DDoS على أنظمة المراسـلة، مما منع العملاء من الإبلاغ عن الأضـرار. أثّر ذلك على حوالي ٢٢٥,٠٠٠ شـخص، واسـتمر الانقطاع من ٣ إلى ٦ ساعات حتى استعادة النظام.

[٢٨] . عادل عبد الصادق أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني وحدة الدراسات المستقبلية المرجع السابق ص: ٤٥

في يناير ٢٠١٣، أعلن مجموعة عز الدين القسام الإيرانية عن مسؤوليتها عن سلسلة من هجمات DDoS ضد مواقع البنوك الأمريكية كجزء من عملية "أبابيل" المرحلة الثانية. كما تواصلت هجمات DDoS من قبل دول أخرى مثل الصين، إذ تصاعدت هذه الهجمات في السنوات الأخيرة.

وفي عام ٢٠١٠، كشفت Google عن اكتشاف برامج ضارة تستهدف مستخدمي الكمبيوتر في فيتنام. على الرغم من أن البرامج كانت بسيطة في تصميمها، إلا أنها كانت تستخدم للتجسس على الآلاف من المستخدمين الذين قاموا بتنزيل برامج لوحات المفاتيح الفيتنامية، بالإضافة إلى شن هجمات DDoS ضد المدونات التي تعارض مشاريع تعدين البوكسيت في فيتنام.

أما هجوم "رجل في الوسط" (MitM)، فيتمثل في قيام المهاجم بوضع نفسه بين المرسل والمستقبل، ليتمكن من اعتراض وتغيير الرسائل أثناء انتقالها، فيعتقد كل من المرسل والمتلقي أنهما يتواصلان بشكل مباشر. يمكن استغلال هذه التقنية في الأغراض العسكرية لزعزعة استقرار العدو وإرباكه

٥- **الاحتيال الإلكتروني:** في السنوات الأخيرة، شهدت العديد من الدول خروقات واختلالات كبيرة في مجالات عدة مثل الغش في الامتحانات، التلاعب في نتائج الانتخابات، وتزوير الوثائق الرسمية. وقد أُثيرت العديد من الاعتراضات على نتائج الانتخابات في العديد من الدول، حيث أشارت الحكومات إلى وجود عمليات اختراق إلكتروني واحتيال رقمي أسفرت عن تغيير نتائج الانتخابات وتسريب بيانات الناخبين.

على سبيل المثال، في أبريل ٢٠١٦، تم اختراق قاعدة بيانات لجنة الانتخابات الفلبينية (COMELEC)، حيث تم كشف المعلومات الشخصية لـ ٥٥ مليون ناخب فلبيني، بما في ذلك بصمات الأصابع وأرقام جوازات السفر وتواريخ انتهاء صلاحيتها، وكذلك نوايا الترشح للمنصب. وفي أغسطس من نفس العام، تعرضت وكالتان حكوميتان في هونغ كونغ للاختراق في هجوم يُعتقد أن الصين كانت وراءه، وقد وقع الهجوم قبل أسابيع قليلة من الانتخابات التشريعية في المدينة. [٢٩]

٦- **حصان طروادة.** حصان طروادة هو نوع من البرمجيات الخبيثة التي تُخفي نواياها الحقيقية عبر التسلل إلى النظام المستهدف بشكل غير ملاحظ، حيث يبدو في البداية كبرنامج عادي أو قطعة من البرمجيات المشروعة، ثم يبدأ في تنفيذ الأكواد الضارة بمجرد دخول النظام. تم تسمية

[٢٩] . عادل عبد الصادق أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني وحدة الدراسات المستقبلية المرجع السابق ص: ٤٦

هذا النوع من البرمجيات بهذا الاسم نسبة إلى حصان طروادة في التاريخ اليوناني القديم، الذي كان يحمل جنودًا مختبئين بداخله.

في يوليو ٢٠١٢، تم اكتشاف حصان طروادة الملقب بـــ "المهدي"، الذي تمكن من جمع البيانات من حوالي ٨٠٠ جهة تشمل شركات هندسة البنية التحتية، وكالات حكومية، مؤسسات مالية، وأوساط أكاديمية في مناطق متنوعة من الشرق الأوسط، بما في ذلك إسرائيل وإيران. الفيروس استخدم لغة السلاسل الفارسية في برمجته.

وفي أغسطس ٢٠١١، تم اختراق بريد إلكتروني ووثائق خاصة بـــ ٤٨٠ عضوًا في البرلمان الياباني، بالإضافة إلى المشرعين وموظفيهم، بعد هجوم تصيد احتيالي أدى إلى زرع حصان طروادة في أجهزة الكمبيوتر وخوادم النظام الحكومي. تم الاتصال بخوادم في الصين، حيث كانت التعليمات البرمجية تحتوي على أحرف صينية، مما يشير إلى مصدر الهجوم.[٣٠]

٧- **برامج دفع الفدية.** يُعد هجوم الفدية من أبرز التهديدات السيبرانية الحديثة، حيث يقوم المهاجم بتشفير بيانات النظام المستهدف ويمنع المستخدم من الوصول إليها، ثم يطالب بدفع فدية مقابل استعادة البيانات. تتفاوت خطورة هذه الهجمات، من مجرد إزعاج بسيط إلى حوادث تعطل أنظمة كاملة وتؤثر بشكل كبير على المؤسسات والأفراد.

غالبية نسخ برامج الفدية الحديثة تعتمد على تشفير الملفات، بينما تستخدم بعض الأنواع الأخرى أساليب مختلفة مثل قفل النظام بالكامل. بعد حجب الوصول، يُطلب من الضحية دفع مبلغ فدية، يتراوح غالبًا بين ٢٠٠ و٣٠٠٠ دولار في الولايات المتحدة، لكن في بعض الحالات تُطلب العملات الرقمية أو بطاقات الهدايا كوسيلة للدفع.

تستهدف هذه البرامج الضارة ضحاياها بشكل عشوائي، سواءً على أجهزة الكمبيوتر أو الهواتف الذكية، مما يُعرضهم لخطر فقدان البيانات أو التعرض لخسائر مالية كبيرة، سواء بدفع الفدية أو نتيجة توقف الأعمال، وتكاليف استعادة النظام، والدعم القانوني، وتعديلات البنية التحتية، وأحيانًا نفقات خدمات حماية البيانات مثل مراقبة الائتمان للعملاء والموظفين

٨- **الهجمات على أجهزة إنترنت.** أجهزة إنترنت الأشياء وأجهزة الاستشعار الصناعية تُعد من الأهداف الرئيسية للتهديدات السيبرانية، نظرًا لكونها منتشرة على نطاق واسع وغالبًا ما تعمل بأنظمة تشغيل قديمة تفتقر إلى التحديثات الأمنية. وتشمل هذه التهديدات سيطرة المهاجمين على

[٣٠] . عادل عبد الصادق أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني وحدة الدراسات المستقبلية المرجع السابق ص: ٤٩

الأجهزة لتحويلها إلى أدوات ضمن هجمات DDoS، أو الوصول غير المشروع إلى البيانات التي تجمعها هذه الأجهزة.

وبسبب كثافة انتشارها وتوزيعها الجغرافي، تُعد هذه الأجهزة بيئة مثالية للجهات الخبيثة التي تسعى لاختراق الشبكات أو تنفيذ هجمات رقمية معقدة يصعب تتبعها.

٩- التجسس الإلكتروني: تُعد أنشطة التجسس الإلكتروني من أخطر التهديدات السيبرانية، خاصة حين تستهدف مجالات حساسة مثل الأمن القومي، الاستخبارات، أو البنى التحتية العسكرية. وغالبًا ما تلجأ بعض الدول إلى هذه العمليات لاختراق الشبكات وسرقة البيانات أو تسريبها لأغراض سياسية أو استراتيجية.

فعلى سبيل المثال، في عام ٢٠١٥، شنت حملة إيرانية هجومًا سيبرانيًا استهدف قطاعات الطاقة والهيئات الحكومية والتكنولوجيا في المملكة العربية السعودية. كما كشفت تحليلات أمنية لاحقًا عن حملة تجسس واسعة النطاق طالت أكثر من ٥٠٠ جهة، معظمها في الشرق الأوسط، تركزت على مجالات الدفاع والدبلوماسية والصحافة وحقوق الإنسان.

وفي أبريل ٢٠١٧، تم الكشف عن حملة تجسس إلكتروني مصدرها الصين، استهدفت مؤسسات وشركات متخصصة في البناء، والهندسة، والاتصالات، والفضاء، بالإضافة إلى وكالات حكومية في الولايات المتحدة وأوروبا واليابان. وقد تضمنت الحملة جمع معلومات من منظمات مرتبطة بالأقمار الصناعية والدفاع.

أما في عام ٢٠١٤، فقد برزت حملات تجسس إلكتروني روسية اعتمدت على استغلال ثغرات "يوم الصفر" في أنظمة Windows، مستهدفة أجهزة تعود للناتو، والاتحاد الأوروبي، والحكومة الأوكرانية. وفي نفس العام، نُفذت عمليات اختراق كبيرة طالت قطاعات الطاقة في دول متعددة مثل الولايات المتحدة، إسبانيا، فرنسا، ألمانيا، إيطاليا، تركيا، وبولندا، في واحدة من أكبر الهجمات السيبرانية المنظمة على الإطلاق.[٣١]

١٠- البرامج الضارة على تطبيقات الجوال. الأجهزة المحمولة لا تقل عرضة لهجمات البرمجيات الخبيثة عن أجهزة الحواسيب، إذ يمكن للمهاجمين استغلالها عبر تطبيقات مزيفة، أو مواقع إلكترونية ضارة، أو من خلال رسائل تصيد تصل عبر البريد الإلكتروني أو الرسائل النصية. وبمجرد نجاح الهجوم، يمكن للمخترقين الوصول إلى بيانات حساسة أو السيطرة على الجهاز.

[٣١] . عادل عبد الصادق أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني وحدة الدراسات المستقبلية المرجع السابق ص: ٥٠

في مارس ٢٠١٣، تعرضت مؤسسات مالية ومحطات تلفزيونية في كوريا الجنوبية لهجوم باستخدام برمجيات خبيثة صُممت خصيصًا لتجاوز برامج الحماية المحلية، ويُعتقد أن مصدر الهجوم كان من كوريا الشمالية. كما شهد يونيو ٢٠١١ حادثة اختراق لشبكات صندوق النقد الدولي، نفذته جهة حكومية يُشتبه فيها، من خلال رسائل بريد إلكتروني احتيالية تحمل مرفقات ضارة، مما أدى إلى تسريب كمية كبيرة من البيانات، شملت مستندات ومراسلات إلكترونية حساسة. [٣٢]

- **<u>التجسس السيبراني</u>**

على الرغم من حداثة مصطلح "التجسس السيبراني"، فإن جوهر التجسس كأداة للحصول على معلومات سرية ليس جديدًا، بل هو ممارسة عريقة استخدمتها الدول منذ العصور القديمة. في شكله التقليدي، كان التجسس يتم بإرسال عملاء إلى أراضي الخصم لجمع معلومات حساسة.

ومع التقدم التكنولوجي، تطورت أساليب التجسس، فاستُخدمت وسائل مثل الطائرات والسفن والأقمار الصناعية لتوسيع نطاق المراقبة، ومع توسع الفضاء الرقمي، أصبح الإنترنت بيئة جديدة يُمارَس فيها التجسس عن بُعد.

يعتمد التجسس السيبراني على التسلل إلى أنظمة الحواسيب والشبكات بهدف الوصول إلى معلومات محمية، دون إذن من أصحابها، لتحقيق أهداف سياسية أو عسكرية أو اقتصادية. ويتم ذلك غالبًا باستخدام أدوات مثل البرمجيات الخبيثة، وأحصنة طروادة، وتقنيات الاختراق المتقدمة. ويُنظر إلى هذا النوع من التجسس على أنه شكل حديث من سرقة البيانات، قد تنفذه جهات منظمة أو أفراد عاديون، تختلف دوافعهم بين التخريب، وتحقيق مصالح خاصة، أو مجرد الفضول، وقد ازداد انتشاره بشكل ملحوظ مع تطور تقنيات الهجوم الإلكتروني في العصر الرقمي. [٣٣]. ويرى اتجاه آخر أن التجسس السيبراني يتمثل في توظيف القدرات الرقمية والتقنيات المتقدمة لاعتراض الاتصالات الإلكترونية أو مراقبتها، سواء كانت هذه البيانات متبادلة بشكل مباشر أو محفوظة داخل أنظمة رقمية، بهدف الحصول على معلومات أو تسريبها دون إذن مسبق من أصحابها.

يتضح مما سبق أن التجسس السيبراني قد يُعد أحد مظاهر الإرهاب الإلكتروني، إذا ما تم توظيفه بطريقة عدائية تستهدف إحداث أضرار جسيمة في أنظمة التحكم الحاسوبية والبنى التحتية لشبكات الاتصال. إذ يُمكن استخدامه كأداة استباقية لجمع معلومات حساسة وتحديد مكامن

---

[٣٢] . عادل عبد الصادق أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني وحدة الدراسات المستقبلية المرجع السابق ص: ٥٢

[٣٣] د. عصام فاعور ملكاوي الفضاء الإلكتروني ساحة حرب دولية مُفترضة إربد للبحوث والدراسات – القانون جامعة إربد الأهلية – عمادة البحث العلمي والدراسات العليا مج١٨ ع٢ تموز ٢٠١٥ ص:١٢٠.

الضـــعف داخل الأنظمة الرقمية، تمهيدًا لتطوير برمجيات خبيثة تســتغل تلك الثغرات لاحقًا في تنفيذ هجمات مدمرة تهدف إلى زعزعة الأمن والاستقرار. [٣٤].

يُعد التجسـس السـيبراني وسـيلة خفية لاختراق الأنظمة الرقمية بهدف الحصـول على معلومات ســرية، وغالبًا ما يتم ذلك باســتخدام تقنيات التخفي المتقدمة. وقد يُنفَّذ هذا النوع من التجســس بواسطة عناصر داخلية في المؤسسة المستهدفة، من خلال زرع شفرات تجسسية في أنظمتها المحمية. تعمل هذه الشــفرات على جمع البيانات الضــرورية، مما يتيح للجهات الإرهابية تحليل نقاط الضــعف واســتغلالها في هجمات لاحقة. وحالما تُثبت البرمجيات الخبيثة، قد تبدأ بإرســال معلومات إلى جهة خارجية، تمهيدًا لتفعيل أوامر هجومية. ويمكن لتلك الأوامر أن تُســبب تعطيلًا خطيرًا، مثل إغلاق صــمامات تحكم حيوية في منشــآت البنية التحتية، أو تنفيذ تعليمات خاطئة تؤدي إلى تلف أجهزة حســاســة، مما يجعل هذا النوع من التجســس تهديدًا حقيقيًا للأمن الرقمي والمادي على حد سواء. [٣٥]

تمكنت وكالة الأمن القومي الأمريكية (NSA) من كشـف حالات تجسـس دولية واسـعة النطاق، من بينها شــبكة ضــخمة تُدار بتنســيق بين كندا وبريطانيا وأســتراليا ونيوزيلندا، هدفها مراقبة الاتصــالات الهاتفية وتبادل الرســائل بأنواعها المختلفة، وتُعرف هذه الشــبكة باســم "ECHELON".

وفي مواجهة هذا النوع من التهديدات، بُذلت جهود تقنية ملموســة للحد من مخاطر التجســس الســيبراني، أبرزها تطوير تقنيات التشــفير وإخفاء البيانات، إلى جانب تعزيز بروتوكولات الحماية، وتفعيل أنظمة كشف التسلل ومنع الاختراقات. [٣٦].

---

[٣٤] د. حسين المحمدي بوادي الرهاب الدولي بين التجريم والمكافحة دار الفكر العربي ٢٠٠٦ ص:٥٤.

[٣٥] د. ممدوح عبد الحميد عبد المطلب جرائم استخدام شبكة المعلومات الجريمة عبر الإنترنت بحث مقدم لمؤتمر القانون والكمبيوتر كلية الشريعة والقانون جامعة الإمارات ٢٠٠٠ ص:٢٠.

[٣٦] د. مصطفى جاد مقال بعنوان «مستقبل الإرهاب السيبراني» في ندوة نظمها المركز الدولي للدراسات المستقبلية والاستراتيجية في ١١ أبريل ٢٠١٢ جريدة السياسة الدولية التابعة لمؤسسة الأهرام إعداد/شريهات نشأت المنيري على الموقع السيبراني:
http://www.siyassa.org.eg//newsContent/٦/٥١/٢٤٥٠

الخاتمة

تمثل الجهود الدولية من جانب المؤسسات والمنظمات العالمية في مكافحة الحروب السيبرانية في العديد من المساعي التي تستهدف الحماية للبيانات أي ضمان بقاء البيانات سرية وعدم تمكين الوصول إليها إلا لمن يمتلك الصلاحيات اللازمة، والتأكد من عدم العبث بالمعلومات أو تعديلها من قبل جهات غير مصرح لها، مع التحقق من هوية المستخدمين الذين يتعاملون مع تلك البيانات.

إن من أبرز ما يشمله تصنيف جرائم التجسس السيبراني؛ جرائم التجسس الاقتصادية والتجارية: تهدف هذه الجرائم إلى الحصول على معلومات اقتصادية وتجارية سرية. يتضمن ذلك التجسس الصناعي، الذي يتم عادة من قبل الشركات أو المؤسسات التجارية بهدف سرقة الأسرار الصناعية من الشركات المنافسة. يرتبط هذا النوع من التجسس بشكل خاص بالصناعات التقنية مثل البرمجيات، والتقنية الحيوية، وتقنيات الفضاء، والاتصالات، والطاقة. ويعد هذا التجسس أسلوبًا غير قانوني لتحقيق ميزة اقتصادية تنافسية غير عادلة.

وجرائم التجسس الثقافية والتعليمية: يشمل هذا النوع من الجرائم استهداف المعلومات الثقافية والتعليمية بهدف سرقتها أو التلاعب بها. من الأمثلة على ذلك التجسس على الأبحاث العلمية، المخترعات، الدراسات الأكاديمية، والتعاون الثقافي والتعليمي بين الدول. يهدف هذا التجسس إلى الحصول على معارف أو تقنيات جديدة قد تعزز مكانة الدولة أو المنظمة التي تقوم به.

وعليه يمكن القول بأن تأثيرات الإرهاب والحروب السيبرانية غير محدودة وهو ما تم التوصل إليه في ختام البحث، ويمكن أن ابين ما تم من نتائج وتوصيات:

النتائج:

١- إن الإرهاب السيبراني يشير إلى الهجمات غير المشروعة أو التهديدات ضد أنظمة الكمبيوتر والشبكات الإلكترونية بهدف زرع الرعب والخوف في الحكومات أو المواطنين لتحقيق أهداف سياسية، اجتماعية، أو أيديولوجية. يكون هذا الهجوم مدمرًا وهدفه تدمير أو تعطيل النظام المعلوماتي، مما يؤدي إلى خلق حالة من الفوضى والرعب مشابهة للأعمال الإرهابية المادية

٢- تعتبر الحروب السيبرانية كل نشاط إجرامي يتم من خلال شبكة الإنترنت بهدف بث الأفكار المتطرفة سواء كانت سياسية أو دينية أو عنصرية للسيطرة على وجدان الأفراد وإفساد عقائدهم وإذكاء تمردهم واستغلال معاناتهم في تحقيق مآرب خاصة تتعارض مع مصالح المجتمع»

٣- من أشكال الإرهاب الإلكتروني يأتي التجنيد السيبراني عبر ما يُعرف بـ "التلقين السيبراني"، بالإضافة إلى التهديد والترويع السيبراني. حيث تمكنت الجماعات الإرهابية من الاستفادة من الإنترنت للتواصل فيما بينها عبر مسافات شاسعة، وهو ما كان يستغرق وقتًا طويلاً في السابق. من خلال ذلك، أصبحت الهجمات السيبرانية المدمرة على المواقع الحيوية، مثل أنظمة القيادة والسيطرة، ومحطات الطاقة، وأسواق المال، ومرافق الطيران، أمراً واقعاً. هذا النوع من الهجمات يمكن أن يؤدي إلى تعطيل هذه الأنظمة، مسببا أضراراً قد تفوق ما تسببه القنابل والمتفجرات. بالإضافة إلى ذلك، قد تشمل الهجمات الإلكترونية محاولات الاستيلاء على البيانات أو الأموال، كما يحدث في الهجمات على المصارف المالية التي تهدف إلى تمويل التنظيمات الإرهابية

التوصيات

١- ينبغي على المنظمات العالمية أن تصدر اتفاقيات ملزمة تتضمن جانب إلزامي وتطبق بصورة فورية دن الحاجة إلى تعديل تشريعي أي أن تتساوى مع مرتبة القانون، وأن تتضمن جانب عقابي مقيد للحرية وغرامات للحد من آثار الجرائم السيبرانية، وأن تتغير القيمة المالية للغرامة بحسب عملة الدولة أما العقوبات المقيدة للحرية فلابد أن تكون مشددة لتحقيق الردع المناسب.

٢- أن تتم زيادة التعاون الدولي بين الدول في شان تبادل المعلومات والبيانات وآليات كشف الهجمات السيبرانية من اجل تحقيق التكامل والمواجهة المناسبة للحروب السيبرانية؛ وهو ما يتم من خلال عقد اتفاقيات ثنائية وجماعية لتحقيق هذه الأهداف.

٣- زيادة التوعية والتثقيف للمواطنين من خلال عقد المؤتمرات والبرامج التثقيفية حول خطورة الهجمات السيبرانية وأثرها على أمن الافراد والدول.

المراجع

١. عادل عبد الصادق أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني وحدة الدراسات المستقبلية المرجع السابق ص: ٤٣.

٢. ، قانون ١٤ لسنة ٢٠١٤ الخاص بمكافحة الجرائم الإلكترونية، بوابة الميزان، https://almeezan.qa/LawView.aspx?opt&LawID=٦٣٦٦&language=ar

٣. https://WWW.Ittu.Int/net/Itunews/issues/٢٠١٠/٩/Pdf/٢٠١٠٠٩-٢٠-ar.pdf

٤. الاتحاد الدولي للاتصالات ITU دراسة عن تأمين شبكة المعلومات والاتصالات قطاع تنمية الاتصال فترة الدراسة (٢٠٠٦- ٢٠١٠) متاع على الموقع الإلكتروني التالي:

٥. تيري ديبي استراتيجية الشئون الخارجية منطق الحكم الأمريكي ترجمة وليد شحادة دار الكتب العربية مؤسسة محمد بن راشد آل مكتوم بيروت ٢٠٠٩

٦. حكم محكمة العدل الدولية في قضية (Nicaragua v, USA) ٢٧ يونيو ١٩٨٦ الفقرة ١٩٥.

٧. حكم محكمة العدل الدولية في قضية (Oil Platforms) ٢٠٠٣ الفقرات (٥٧: ٦١).

٨. د. إبراهيم سيف منشاوي، دمج القدرات السيبرانية في تقرير التوازن العسكري ٢٠٢٠، مركز المستقبل للأبحاث والدراسات المتقدمة، ٢٠٢١، https://futureuae.com/ar/Mainpage/Item/٦١٥٩/%D٨٪AA%D٨٪AD%D٩٪٨٨٪D٩٪٨٤٪D٨٪A٧٪D٨٪AA-%D٨٪A٧٪D٩٪٨٤٪D٩٪٨٢٪D٩٪٨٨٪D٨٪A٩-%D٨٪AF%D٩٪٨٥٪D٨٪AC-%D٨٪A٧٪D٩٪٨٤٪D٩٪٨٢٪D٨٪AF%D٨٪B١٪D٨٪A٧٪D٨٪AA-%D٨٪A٧٪D٩٪٨٤٪D٨٪B٣٪D٩٪٨A%D٨٪A٨٪D٨٪B١٪D٨٪A٧٪D٩٪٨٦٪D٩٪٨A%D٨٪A٩-%D٩٪٨١٪D٩٪٨A-%D٨٪AA%D٩٪٨٢٪D٨٪B١٪D٩٪٨A%D٨٪B١-%D٨٪A٧٪D٩٪٨٤٪D٨٪AA%D٩٪٨٨٪D٨٪A٧٪D٨٪B٢٪D٩٪٨٦-%D٨٪A٧٪D٩٪٨٤٪D٨٪B٩٪D٨٪B٣٪D٩٪٨٣٪D٨٪B١٪D٩٪٨A-٢٠٢٠

٩. د. أحمد عبيس نعمة التلاوي الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر مجلة المحقق الحلي للعلوم القانونية والسياسية جامعة بابل – كلية القانون العدد الرابع السنة الثامنة ٢٠١٦

١٠. د. إسماعيل صبري مقلد أصول العلاقات الدولية في إطار عام دار النهضة العربية الطبعة الأولى ٢٠٠٧ ص: ٦-٢٠.

١١. د. أميرة عبد العظيم محمد عبد الجواد المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام المرجع السابق ص: ٤٠٨.

١٢. د. حسين المحمدي بوادي الرهاب الدولي بين التجريم والمكافحة دار الفكر العربي ٢٠٠٦ ص:٥٤.

١٣.د. عصام فأعور ملكاوي الفضاء الإلكتروني ساحة حرب دولية مُفترضة إربد للبحوث والدراسات – القانون جامعة إربد الأهلية – عمادة البحث العلمي والدراسات العليا مج١٨ ع٢ تموز ٢٠١٥ ص:١٢٠.

١٤.د. لامية طالة الإرهاب السيبراني والأمن القومي: قراءة في تحولات الاستراتيجية الدفاعية حوليات جامعة الجزائر١ المجلد ٣٥ العدد ٤ ٢٠٢١م ص٣٥٦.

١٥.د. مصطفى جاد مقال بعنوان «مستقبل الإرهاب السيبراني» في ندوة نظمها المركز الدولي للدراسات المستقبلية والاستراتيجية في ١١ أبريل ٢٠١٢ جريدة السياسة الدولية التابعة لمؤسسة الأهرام إعداد/شريهات نشأت المنيري على الموقع السيبراني: http://www.siyassa.org.eg//newsContent/٦/٥١/٢٤٥٠

١٦.د. ممدوح عبد الحميد عبد المطلب جرائم استخدام شبكة المعلومات الجريمة عبر الإنترنت بحث مقدم لمؤتمر القانون والكمبيوتر كلية الشريعة والقانون جامعة الإمارات ٢٠٠٠ ص:٢٠.

١٧.د. هلالي عبد اللاه أحمد جرائم الحاسب والإنترنت بين التجريم الجنائي وآليات المواجهة دار النهضة العربية ٢٠١٥ ص:١١٧.

١٨.دليل تالين وهو مجموعة من المبادئ أعدها بعض الخبراء في القانون الدولي الإنساني عام ٢٠١٣

١٩.رؤى حمود، مقال بعنوان (أشهر الهجمات الإلكترونية حتى ٢٠٢٢: حروب من نوع آخر!)، منشور على موقع rng، ٢٠٢٢،

٢٠.عادل عبد الصادق الفضاء الإلكتروني والرأي العام تغير المجتمع والأدوات والتأثير المركز العربي لبحوث الفضاء الإلكتروني: قضايا استراتيجية ٢٠١٣

٢١.عمر بن عبد الله بن سعيد البلوشي مشروعية أسلحة الدمار الشامل وفقًا لقواعد القانون الدولي منشورات الحلبي الحقوقية بيروت ٢٠٠٧

٢٢.عمر مكي القانون الدولي الإنساني والإرهاب اللجنة الدولية للصليب الأحمر

٢٣.قاسم محمد حسين، اساسيات في الأمن السيبراني، كلية الكنوز الجامعة- قسم الأمن السيبراني-، ٢٠٢٣، ص ٣

٢٤.القانون الدولي الإنساني وفتوى محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها اللجنة الدولية للصليب الأحمر موقع إلكتروني ٢٠١٨/٨/١٠ -WWW.icrc.org.

٢٥.لور انجيزلو تيلمان رودنها وسرو كنوند ورمان القانون الدولي الإنساني وحماية المدنيين من أثار العمليات السيبرانية أثناء النزاعات السلحة المجلة الدولية للصليب الأحمر مجلد ٢٠٢٠٩١٣١٠٢ من

٢٦.مقال بعنوان(تسريب بيانات جنود الجيش البريطاني في اختراق لوزارة الدفاع)، بوابة الجزيرة ، ٧/ ٥/ ٢٠٢٤،

https://www.ajnet.me/tech/٢٠٢٤/٥/٧/%D٨٪AA%D٨٪B٣٪D٨٪B١٪D٩٪٨A%D٨٪A٨-%D٨٪A٨٪D٩٪٨A%D٨٪A٧٪D٩٪٨٦٪D٨٪A٧٪D٨٪AA-%D٨٪AC%D٩٪٨٦٪D٩٪٨٨٪D٨٪AF-%D٨٪A٧٪D٩٪٨٤٪D٨٪AC%D٩٪٨A%D٨٪B٤-

%D٨٪A٧٪D٩٪٨٤٪D٨٪A٨٪D٨٪B١٪D٩٪٨A%D٨٪B٧٪D٨٪A٧٪D٩٪٨٦٪D٩٪٨A
-%D٩٪٨١٪D٩٪٨A

٢٧.موقع الجزيرة، مقال- حصار قطر كيف بدأ؟ وإلى أين وصل؟ -، ٢٠١٨م.
https://www.aljazeera.net/encyclopedia/events/٢٠١٨/٥/٢٣/حصار-قطر-كيف-بدأ-
وإلى-أين-وصل

٢٨.ميثاق الأمم المتحدة.

٢٩.نوال أحمد بسيج القانون الدولي الإنساني وحماية المدنيين والأعيان المدنية في زمن النزاعات المسلحة ط ١ منشورات الحلبي الحقوقية ٢٠١١

٣٠.يحيى بياسين سعود الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني المجلة القانونية المجلد ٤ العد ٤ ٢٠١٨ متاح على الرابط: https://jlaw.journals.ekb.eg/article_٤٥١٩٢.html