الأمن السيبراني في مواجهة النزاع الدولي وحماية المعلومات

[1] ميلاد صالح مفتاح علي [*]

[1]جامعة عبدالملك السعدي طنجة (المغرب)

Cybersecurity in the face of international conflicts and disputes and information protection

[1] Milad Sahl Muftah Ali[*]

[1] https://orcid.org/0009-0008-3831-7827

[1] Abdelmalek Essaadi University Tangier (Morocco) (Country), milad115909@gmail.com

تاريخ الاستلام: 09 / 02 /2025 تاريخ القبول: 08 / 03 / 2025 تاريخ النشر: 01 / 06 / 2025

الملخص:

هدفت الدراسة التعرف على الأمن السيبرانى فى مواجهة النزاع الدولي وحماية المعلومات حيث أدى نمو قطاع تكنولوجيا المعلومات إلى ظهور أنماط مختلفة تُدار عن بُعد في الفضاء الإلكتروني، مثل الإرهاب الإلكتروني والهجمات السيبرانية والحروب الإلكترونية، مما جعل النزاعات بين الدول أكثر سهولة. وبالتالي، أصبح ذلك يشكل تهديدًا للأمن القومي للدول. انتقل نمط الحرب من الشكل التقليدي المباشر إلى الشكل الحديث غير المباشر، مما دفع الدول إلى دمج الفضاء الإلكتروني ضمن حساباتها الاستراتيجية وأمنها القومي. وقد ظهر بُعد جديد في النزاعات الدولية يُعرف بحروب الفضاء الإلكتروني، حيث يمكن لأحد أطراف النزاع أن يُلحق خسائر كبيرة بالطرف الآخر ويشل بنيته المعلوماتية، مما يؤدي إلى خسائر عسكرية واقتصادية جسيمة. وهكذا، فتح الفضاء الإلكتروني آفاقًا جديدة للنزاع وأضاف مستويات متعددة من التعقيد للعلاقات الدولية. وتسعى العديد من الدول حاليًا إلى تعزيز قدراتها في مجالي الدفاع والهجوم من خلال تبني استراتيجيات وطنية للأمن السيبراني تهدف إلى وضع السياسات وفتح المجال للتطبيقات. ولا يقتصر هذا على تحقيق الأهداف الأمنية والسياسية فحسب، بل يشمل أيضًا الحفاظ على فرص النمو الاقتصادي في ظل ملامح الثورة الصناعية الرابعة، وتأثير ذلك على الثقة بالإجراءات والسياسات المتبعة. وفي هذا السياق، شكلت القفزات التكنولوجية الهائلة في مجال الاتصالات والمعلومات في أواخر القرن العشرين وبداية القرن الحادي والعشرين مسارات جديدة لاندلاع نزاعات النفوذ السيبراني في الفضاء الإلكتروني، حيث اعتُبر الأخير ساحة واسعة للتفاعلات العالمية التي شملت في الأساس شبكات رقمية ذات اتصال كبير بين الحواسيب وأنظمة الاتصالات وتكنولوجيا المعلومات والإنترنت لغرض تدفق المعلومات. وتكتنف ظاهرة النزاع السيبراني حالة من الغموض وعدم اليقين، وهي أقرب إلى ما سمي بالغموض النووي خلال الحرب الباردة.

كلمات مفتاحية: الأمن، السيبرانى.، النزاع المعلومات.، الإلكتروني.

Abstract:

The study aimed to identify cybersecurity in the face of international conflicts and disputes and information protection, as the growth of the information technology sector has led to the emergence of

[*] المؤلف المرسل.

[*] Corresponding author.

different patterns that are managed remotely in cyberspace, such as cyberterrorism, cyberattacks and cyberwars, which has made conflicts between countries easier, and thus has become a threat to the national security of countries, as the pattern of war has shifted from the traditional direct form to the modern indirect form, which has prompted countries to integrate cyberspace into their strategic calculations and national security, and a new dimension has emerged in international conflicts known as cyberspace wars, where one party to the conflict can inflict significant losses on the other party and paralyze its information infrastructure, leading to huge military and economic losses, thus opening cyberspace to new horizons for conflict and adding multiple levels of complexity to international relations, and many countries are currently seeking to enhance their capabilities in the areas of defense and attack by adopting national cybersecurity strategies aimed at setting policies and opening the field for applications.

Keywords: Cybersecurity; Conflict; Dispute; Information; Electronic.

مقدمة:

يشهد العالم اليوم تحولات عميقة نتيجة التوسع السريع في حجم المعلومات، مما أدى إلى بروز العديد من العلاقات والأنشطة المختلفة على الصعيد العالمي. ومن أبرز هذه التحولات التكنولوجيا الحديثة، التي تُعد واحدة من الركائز الرئيسية للمجتمع في شتى المجالات. وبهذا أصبح العصر الحالي يُعرف بعصر الثورة الرقمية والإلكترونية، التي تعمل في الفضاء الإلكتروني، وهو مجال يتجاوز حدود الأرض ويُعتبر أكثر خطورة على سكانها. وقد اخترقت هذه الثورة جميع المجالات الإنسانية بقوة، ليصبح الفضاء الإلكتروني عنصراً أساسياً ومؤثراً في النظام الدولي، نظراً لما يحويه من أدوات تكنولوجية متطورة جعلته وسيلة فعّالة في التأثير على أنماط القوة والأمن والحروب.

وأدى نمو قطاع تكنولوجيا المعلومات إلى ظهور أنماط مختلفة تُدار عن بُعد في الفضاء الإلكتروني، مثل الإرهاب الإلكتروني والهجمات السيبرانية والحروب الإلكترونية، مما جعل النزاعات بين الدول أكثر سهولة. وبالتالي، أصبح ذلك يشكل تهديدًا للأمن القومي للدول. انتقل نمط الحرب من الشكل التقليدي المباشر إلى الشكل الحديث غير المباشر، مما دفع الدول إلى دمج الفضاء الإلكتروني ضمن حساباتها الاستراتيجية وأمنها القومي. وقد ظهر بُعد جديد في النزاعات الدولية يُعرف بحروب الفضاء الإلكتروني، حيث يمكن لأحد أطراف النزاع أن يُلحق خسائر كبيرة بالطرف الآخر ويشل بنيته المعلوماتية، مما يؤدي إلى خسائر عسكرية واقتصادية جسيمة. وهكذا، فتح الفضاء الإلكتروني آفاقًا جديدة للنزاع وأضاف مستويات متعددة من التعقيد للعلاقات الدولية.

ويعتبر الأمن السيبراني حاليًا أحد أهم عناصر الأمن في الدول المتقدمة، خاصة مع الانتقال الكامل نحو العالم الرقمي في جميع جوانب الحياة. تعتمد فكرة الأمن السيبراني على حماية البنية التحتية المعلوماتية للدول، والتي تشمل المنشآت الحيوية ونظم المعلومات الأساسية مثل نظم إدارة الحكومات الإلكترونية التي تُشغّل مؤسسات الدولة الهامة، بالإضافة إلى النظم العسكرية والأمنية والقضائية والاقتصادية والصناعية والتجارية وغيرها. وأي تهديد لهذه الأنظمة يُعتبر تهديدًا للأمن القومي. لذلك، قامت العديد من الدول بإنشاء هيئات متخصصة لحماية الأمن السيبراني، وأصبح معيارًا لقياس مدى تقدم الدول واستعدادها السيبراني لمواجهة التهديدات. ويصدر الاتحاد الدولي للاتصالات سنويًا مؤشرًا يُصنّف الدول بناءً على جاهزيتها السيبرانية.

وشبكة المعلومات الإلكترونية جزءًا لا يتجزأ من حياتنا اليومية. اليوم، تستخدم جميع المؤسسات الحكومية والأهلية، وحتى في الاستخدامات الشخصية، المعلومات الرقمية لمعالجتها وتخزينها ومشاركتها. ومع زيادة حجم هذه المعلومات وانتشارها، أصبحت حماية هذه المعلومات أكثر أهمية ولها تأثير كبير على الأمن القومي واستقرارنا الاقتصادي.

وأصبحت دراسة الأمن السيبراني واحدة من متطلبات التطور التكنولوجي الذي نعيشه في العالم مؤخرًا، ولكن هناك جانب آخر مظلم لهذا التطور الرقمي الذي نشهده، قد يجعل أكبر الدول والشركات والمؤسسات التجارية والاقتصادية مهددة بالاختراق، وربما هذا أحد أسباب أهمية دراسة الأمن السيبراني.

- الإشكالية:

مما سبق يتضح أن الأمن السيبراني يحتل مكانة هامة في حياة البشر وفي مختلف جوانب حياتهم، حيث تنوعت أشكال ووسائل الاختراقات في عصرنا الحالي في ظل ثورة المعلومات الحديثة، مما أدى إلى تأثيرات سلبية على وسائل الحماية الفعلية للبيانات والمعلومات. وقد ظهرت المشكلة هنا نتيجة لعدم الوعي الكافي بأهمية الأمن السيبراني، وتم تحديد الإشكالية البحثية في محاولة الإجابة على السؤال التالي: ما هو دور الأمن السيبرانى في حماية المعلومات في ظل النزاع الدولي؟

- الأهمية:

تبرز أهمية الدراسة في الآتي:

الأهمية العلمية:

هناك فجوة علمية في مجالات الكتابات القانونية التي تنظم الأمن السيبراني في سياق النزاع الدولي وحماية تكنولوجيا المعلومات، وتأثير ذلك على العلاقات الدولية وانتهاك قواعد القانون الدولي والحفاظ على السلم والأمن الدوليين.

الأهمية العملية:

وهي تطبيق القوانين الدولية على الأمن السيبراني، باعتباره انعكاسًا للنظام الدولي، مما يجعل من الضروري تطبيق القانون الدولي على العالم الرقمي وابتكار قوانين جديدة للتعامل مع النزاعات والحروب السيبرانية التي تفتقر إلى نصوص قانونية تحميها بسبب حداثتها.

- الهدف:

تسعى الدراسة الحالية إلى تحقيق مجموعة من الأهداف لعل أهمها التالي:

1- التعرف على تداعيات النزاع السيبرانى الدولي في ظل التطور التكنولوجي للمعلومات.

2- التعرف على المفاهيم المرتبطة بالأمن السيبراني والمفاهيم المرتبطة به.

3- التعرف على المخاطر السيبرانية التي تؤثر على الأمن الدولي.

- المنهجية:

وللإجابة على سؤال الدراسة الذي تبنته الدراسة، تم الاعتماد بشكل أساسي على المنهج الوصفي والتحليلي للأمن السيبراني باعتبارها ظاهرة حديثة تحتاج إلى تحليل، وكذلك رصد تأثير تكنولوجيا المعلومات على النزاعات الدولية.

- الهيكلية:

تم تقسيم الهيكلية إلى الآتي:

المبحث الأول: الإطار المفاهيمي للأمن السيبراني:

المطلب الأول: مفهوم الأمن السيبراني وتطوره التاريخي.

المطلب الثاني: خصائص الأمن السيبراني وأبعاده.

المبحث الثاني: النزاع السيبراني وحماية المعلومات:

المطلب الأول: النزاع السيبراني.

المطلب الثاني: الموقف الدولي من النزاع السيبراني.

المبحث الأول

الإطار المفاهيمي للأمن السيبراني

إن الهدف الأساسي للأمن السيبراني هو تعزيز قدرة الدول على مقاومة التهديدات الكامنة في الفضاء الإلكتروني، وهو ما دفع العديد من دول العالم إلى وضعه على أجندتها، في ظل ظهور الحروب السيبرانية التي تتعرض لها العديد من الدول. إن انتشار القوة السيبرانية بين عدد كبير من الفاعلين على الساحة الدولية ضرب قدرة الدول على السيطرة والهيمنة، بل وأعطى حتى الفاعلين الأصغر مساحة أكبر لممارسة لعب دور مهم عبر الفضاء الإلكتروني، وهو ما يعني تغيير قدرات القوى في النظام الدولي، الأمر الذي غيّر طبيعة بعض التفاعلات بين الوحدات الدولية الفاعلة، مثل النزاع والتعاون والردع والقوة عبر العالم الافتراضي المترابط[1].

لقد جعل انفجار الثورة المعلوماتية من التكنولوجيا أحد أشكال القوة التي اكتسبت أهمية كبيرة ومضاعفة لأنها تمكنت من إزالة المسافات بين الدول وأصبح العالم متناسقا ومتقاربا، وما رافق هذا التطور الهائل من التهديدات من نوع جديد شملت أبعادا وخصائص من نوع آخر، بسبب ظهور التهديدات والجرائم السيبرانية، أصبحت تشكل تحديا كبيرا للأمن الوطني والدولي لدرجة أن العديد من المتخصصين في المجال الأمني والاستراتيجي والسياسي اعتبروا الفضاء الإلكتروني ضمن الجيل الخامس من الحروب بعد الحروب البرية والبحرية والجوية والفضائية، مما استدعى ضرورة وجود ضمانات أمنية ضمن هذه البيئة الرقمية، والتي تبلورت بشكل أساسي في ظهور الأمن السيبراني كبعد جديد ضمن أجندة مجال الدراسات الأمنية[2].

أصبح الأمن السيبراني ضرورة ملحة لجميع الدول دون استثناء، حيث يرتبط بحماية الأنظمة من التهديدات المحتملة التي تأتي من مصادر خارجية عبر الإنترنت. يشكل الأمن السيبراني عنصراً أساسياً في منظومة الأمن الحديثة، التي يجب على الجهات الوطنية تحقيقها في ظل تزايد الجرائم الرقمية والاستغلال المتزايد للشبكات الإلكترونية لأغراض إجرامية. هذا الوضع يؤثر بشكل سلبي على سلامة البنى التحتية للمعلومات الحساسة، خاصة المعلومات الشخصية[3].

وبالنظر إلى أن الأمن السيبراني يُعدّ جزءًا أساسيًا من الأمن الوطني، تسعى العديد من الدول حاليًا إلى تعزيز قدراتها في مجالي الدفاع والهجوم من خلال تبني استراتيجيات وطنية للأمن السيبراني تهدف إلى وضع السياسات وفتح المجال للتطبيقات. ولا يقتصر هذا على تحقيق الأهداف الأمنية والسياسية فحسب، بل يشمل أيضًا الحفاظ على فرص النمو

الاقتصادي في ظل ملامح الثورة الصناعية الرابعة، وطبيعة العلاقة بين الأمن والاقتصاد في العصر الرقمي، وتأثير ذلك على الثقة بالإجراءات والسياسات المتبعة[4].

ومن المبادرات الإيجابية التي تم تنفيذها في مجال الأمن السيبراني تطوير مؤشر عالمي للأمن السيبراني من قبل الاتحاد الدولي للاتصالات التابع للأمم المتحدة (GCI) وهو اختصار لـ Global Cyper Security Index وذلك لمعرفة مدى تطور الدول في مجال الأمن السيبراني[5].

المطلب الأول: مفهوم الأمن السيبراني وتطوره التاريخي:

أولاً: مفهوم الأمن السيبراني:

1- تعريف الأمن السيبراني لغة:

لقد وردت كلمة "الأمن" في القرآن الكريم في مواضع كثيرة، وهو ضد الخوف مثل قوله تعالى: "**الذي أطعمهم من جوع وآمنهم من خوف**"[6]، وأيضاً في قوله تعالى "**ادخلوها بسلام آمنين**"[7].

ورد في المعجم الوسيط بمعنى الأمن، أي الشعور بالأمان والسلامة والثقة، حيث يشعر الإنسان بالاطمئنان دون خوف، وهو يشير إلى أمن البلاد الذي يبعث الاطمئنان في نفوس أهلها[8]، أما مصطلح السيبرانية فقد اشتقت من لفظة سيبر Cyber اليونانية الأصل، وقد اشتقت من كلمة Cybernetics بمعنى (الشخص الذى يدير دفة السفينة)، وقد تستخدم مجازاً لتعبر عن المتحكم[9]، فهناك أيضاً من يرجع أصلها إلى منتصف القرن العشرين لعالم الرياضيات الأمريكي Norbert Wiener، حيث استخدمها للتعبير عن التحكم الآلي[10]، وهذا يعني أن مصطلح "سيبر" يشير إلى الفضاء الإلكتروني أو الفضاء السيبراني، حيث ظهر مع ظهور الإنترنت. وقد اكتسب حديثاً معنى يشمل: مجموعة القوانين السياسية، الأدوات، النصوص، المفاهيم، آليات الأمن، طرق إدارة المخاطر، والممارسات التكنولوجية المتعلقة بتكنولوجيا المعلومات والاتصالات المستخدمة لحماية الدول والمنظمات والأفراد[11].

2- تعريف الأمن السيبراني اصطلاحاً:

هناك تعريفات عديدة لمصطلح الأمن السيبراني، فالبعض يعرفه بأنه: "أمن الشبكات وأنظمة المعلومات والبيانات والمعلومات والأجهزة المتصلة بالإنترنت، وبالتالي فهو المجال الذي يتعلق بالإجراءات والتدابير ومعايير الحماية التي يجب اتخاذها أو الالتزام بها لمواجهة التهديدات والحد من آثارها"[12].

وبحسب دراسة الاتحاد الدولي للاتصالات فإن الأمن السيبراني هو: "مجموعة من المهام مثل جمع أساليب الأمن والأدوات والسياسات والإجراءات والمبادئ التوجيهية والإرشادات وطرق إدارة المخاطر والتدريب وأفضل الممارسات واستراتيجيات الأمن التي يمكن استخدامها لحماية البيئة السيبرانية والمؤسسات والمستخدمين"[13].

يمكن تعريف الأمن السيبراني، استنادًا إلى أهدافه، على أنه النشاط الذي يضمن حماية الموارد البشرية والمالية من الخسائر والأضرار الناتجة عن المخاطر والتهديدات، مع تمكين استعادة الوضع إلى طبيعته في أسرع وقت ممكن لضمان استمرار عجلة الإنتاج وتجنب تحول الأضرار إلى خسائر دائمة[14].

ويُعرف أيضًا باسم: "الوسائل الدفاعية التي تكشف عن محاولات المتسللين وتعرقلها"[15].

ومن الناحية الإجرائية، يمكن القول إن الأمن السيبراني هو "مجموعة من الآليات والإجراءات والوسائل والأطر التي تهدف إلى حماية البرمجيات وأجهزة الكمبيوتر في الفضاء الإلكتروني من مختلف التهديدات والهجمات والاختراقات التي تهدد الأمن القومي للدولة نفسها"[16].

تعرفها موسوعة العلوم الاجتماعية على أنها: "قدرة الدولة على حماية قيمها من التهديدات الخارجية"[17].

ويُعرف أيضًا بأنه: "أمن الشبكات وأنظمة المعلومات والبيانات والمعلومات والأجهزة المتصلة بالإنترنت، وعليه فهو المجال الذي يتعلق بالإجراءات والتدابير ومعايير الحماية التي يجب اتخاذها أو الالتزام بها لمواجهة التهديدات ومنع الانتهاكات أو على الأقل الحد من آثارها"[18].

كما يعرف بأنه: "الأساليب التي تقلل من خطر الهجوم على البرامج أو أجهزة الكمبيوتر أو الشبكات. وتشمل هذه الأساليب الأدوات المستخدمة لمواجهة المتسللين، واكتشاف الفيروسات وإيقافها، وتوفير الاتصالات المشفرة"[19].

وقد عرفه آخرون بأنه: "أمن الشبكات وأنظمة المعلومات والبيانات والمعلومات والأجهزة المتصلة بالإنترنت، وهو المجال الذي يتعلق بإجراءات الحماية والتدابير والمعايير التي يجب اتخاذها أو الالتزام بها لمواجهة التهديدات ومنع الانتهاكات أو الحد من آثارها في أشد الحالات وأسوأها"[20].

وعرفه آخرون بأنه: "ممارسة الدفاع عن أجهزة الكمبيوتر والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الضارة"[21].

وعليه يمكن تعريف الأمن السيبراني بأنه: الجهود المبذولة لضمان حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات. يشمل ذلك تحديد وتقييم المخاطر والتهديدات المحتملة، واتخاذ الإجراءات الوقائية والتصحيحية لتقليل فرص حدوث خسائر أو أضرار. الهدف هو تحقيق توازن بين الأمان والتشغيل الفعال، مع ضمان تقديم استجابة فعالة في حالة وقوع هجمات أو انتهاكات.

ثانياً: التطور التاريخي للأمن السيبراني:

مع تطور العصر التكنولوجي وزيادة الجهود نحو بناء اقتصاد يعتمد على المعرفة، أصبحت المعلومات والاتصالات أداة أساسية في إنتاج المعرفة وحفظها. كما أصبحت تكنولوجيا المعلومات ومعالجتها وتبادلها من العوامل الرئيسية التي تسهم في تحقيق التنمية المستدامة وخلق فرص عمل جديدة. وقد شهد هذا المجال نموًا ملحوظًا في أعداد المستخدمين الشباب، مما ساهم في تعزيز النمو الاقتصادي وانتشار الأجهزة المحمولة. ومع ذلك، أدى هذا الانفتاح الذي يميز الفضاء الإلكتروني إلى تعريض مستخدميه للهجمات وجعلهم ضحايا لأنشطة إجرامية يرتكبها القراصنة والمجرمون الرقميون[22].

1- ظهور الإنترنت:

ظهرت شبكة الإنترنت قبل الأمن السيبراني، حيث عانى العالم في القرن العشرين من أهوال الحربين العالميتين الأولى والثانية بين عامي 1914 و1945. ومع تطور المد الشيوعي والتقدم التكنولوجي بعد الحرب العالمية الثانية، بدأت الولايات المتحدة الأمريكية في تكوين حلفاء جدد، من أجل تعزيز وجودها لمواجهة المد الشيوعي للاتحاد السوفييتي. واكتسبت الولايات المتحدة حلفاء عسكريين، بالإضافة إلى اهتمامها بالعلم والتكنولوجيا، لوقف هذا التهديد[23].

وبعد ذلك بدأت حرب من نوع مختلف، حيث انتقلت ساحة المعركة إلى الفضاء الإلكتروني عندما أطلق الاتحاد السوفييتي القمر الصناعي سبوتنيك في عام 1957، وهو ما دق ناقوس الخطر في الولايات المتحدة بشأن الفجوة في العلوم، وانتقلت نحو الاستثمارات الحكومية في العلوم والتكنولوجيا[24].

تم إنشاء شبكة الإنترنت لأول مرة في ستينيات القرن العشرين نتيجة لمشروع حكومي أمريكي يسمى أربانت ARPANET [25]، وكان الهدف من ذلك تأمين شبكة اتصال خاصة لا يمكن إتلافها أو تدميرها في حال وقوع عمليات تخريب أو اندلاع حرب مفاجئة. وقد أوكلت وزارة الدفاع هذه المهمة إلى وكالة مشاريع الأبحاث المتقدمة، التي تتمتع بقدرة على مقاومة الكوارث والاستمرار في العمل حتى في حالة حدوث هجوم. وكانت هذه الشبكة تربط بين أربع آليات ضخمة لأغراض التجربة.

2- نشأة الأمن السيبراني:

سُجِّل أول ظهور للأمن السيبراني في عام 1970، عندما طُرِح مشروع الأمن السيبراني في منتصف الطريق بعد عدة عقود من اختراع الحواسيب. وكان المشروع ينمو بشكل متناسب مع البيانات الحاسوبية التي كانت تستخدمها منظمات معينة فقط، ولم يكن انتشاره واسع النطاق كما هو عليه الآن، وكان من السهل تحديد أنواع الهجمات ومصدرها في حال حدوثها. ثم تطوَّر هذا المشروع في الثمانينيات نتيجة للانتشار الأوسع للحواسيب والأنظمة الإلكترونية، مما مهد الطريق لهجمات أكثر تطوراً لسرقة واختراق البيانات، وكذلك بسبب اختراع أول نظام فيروسي يتسبب في تدمير البيانات في الخوادم. وفي تسعينيات القرن الماضي، بدأ التطور الهائل في الأجهزة الإلكترونية والأنظمة الافتراضية، وتزامن ذلك مع تطور البرامج الفيروسية والهجمات الإلكترونية. لذلك، تم تطوير بروتوكولات الحماية لمواقع الويب، والتي يمكن من خلالها للمستخدم الوصول إلى البيانات المخزنة بأمان دون التعرض لخطر الفيروسات وسرقة بياناته الخاصة [26].

مع تزايد الهجمات الإلكترونية وتهديدات التجسس في ثمانينيات القرن العشرين، ظهرت مصطلحات جديدة مثل فيروسات الكمبيوتر Trojan Horse، لذا وضعت وزارة الدفاع الأميركية معايير لتقييم نظام حاسوبي موثوق في عام 1985. ولكن في عام 1986، تعرضت بوابة الإنترنت في كاليفورنيا للاختراق، وتم اختراق 400 حاسوب عسكري، بالإضافة إلى الأجهزة المركزية في مقر البنتاغون، بهدف بيع المعلومات. ثم في عام 1987، تم إطلاق أول برنامج تجاري لمكافحة الفيروسات. ثم في عام 1988، ظهرت شركات تطوير برامج مكافحة الفيروسات، بما في ذلك أفاست. واقتصر عمل المكافحة على الاستجابة للهجمات الحالية. ويذكر أن عدم وجود شبكة واسعة ساعد في الحد من نشر التحديثات. وشهد هذا العقد إنشاء أول منتدى إلكتروني مخصص لأمن مكافحة الفيروسات، بالإضافة إلى إنشاء مطبعة مكافحة الفيروسات، لحماية بيانات مستخدمي الفضاء الإلكتروني من أي اختراق إلكتروني إجرامي، مما مهد الطريق لظهور الأمن السيبراني بعد ذلك[27].

المطلب الثاني: خصائص الأمن السيبراني و أبعاده:

يرتبط الأمن المعلوماتي بالجرائم الإلكترونية التي تشكل أساس الأمن المعلوماتي الذي يعمل على مكافحتها، وهي جريمة ذكية تنشأ في البيئة الإلكترونية أو الافتراضية، حيث يقوم بها أفراد أو منظمات على درجة عالية من الذكاء ويمتلكون المعرفة والتكنولوجيا، مما يسبب خسائر فادحة للمجتمع. وتظهر أهميتها في عالمنا المترابط عبر الشبكة العالمية، حيث أصبحت عنصراً مهماً في حياة الإنسان على كافة المستويات السياسية والاقتصادية والاجتماعية، وهي الآن عصب الحياة الحالية التي تعتمد عليها الدول والأفراد في كافة معاملاتهم، بل ينظر إليها باعتبارها رافداً جديداً للأمن القومي وجزءاً من الأمن الجماعي، لأن العلاقة بين الأمن والتكنولوجيا علاقة مترابطة ومتزايدة، مع إمكانية تعرض المصالح الاستراتيجية للمخاطر الإلكترونية، مما يهدد بتحويل دور الأنظمة الإلكترونية إلى وسيط ومصدر لأدوات النزاع الدولي، ودورها في تأجيج الثورات الدولية[28].

أولاً: خصائص الأمن السيبراني:

يتميز الأمن السيبراني بعدة خصائص من أهمها[29]:

1- الأمن السيبراني ليس مجرد إجراء يُنفّذ مرة واحدة، بل هو عملية مستمرة تتضمن آليات دفاع مبتكرة لمواجهة التهديدات التي تستهدف الأنظمة والشبكات وغيرها.

2- يسهم في إنشاء بيئة سيبرانية آمنة وبناء نظام موثوق به.

3- يقوم بإجراء وقائي ورقابي استباقي يهدف إلى البحث عن المخاطر ومعالجتها وسد الثغرات.

4- يعمل على توفير دفاع لاحق يتمثل في استعادة الوضع إلى حالته الأصلية.

5- يقدم خاصية التنبيه بوجود أخطاء أو إساءة استخدام للشبكات التي تعرض البيانات والمعلومات للخطر داخل المؤسسات، بالإضافة إلى تغطية المخاطر الخارجية ومراقبة التهديدات.

ثانياً: أبعاد الأمن السيبراني:

إن الاهتمام بأبعاد الأمن السيبراني يجعلنا نأخذ بعين الاعتبار طبيعة المخاطر والتهديدات التي يتعرض لها، فالأمن السيبراني له أبعاد ترتبط في الغالب بالأمن الوطني وتختلف عن بعضها البعض، وتشمل ما يلي:

1- الأبعاد العسكرية:

تكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها عبر شبكات عسكرية في الفضاء الإلكتروني، وتبادل المعلومات وتدفقها، فضلاً عن السرعة، وإعطاء الأوامر العسكرية، والقدرة على إيصال الأهداف عن بعد وتدميرها. وقد تتحول هذه الميزة إلى نقطة ضعف بدلاً من قوة إذا لم تكن الشبكة الإلكترونية المستخدمة لذلك مؤمنة بشكل جيد من أي اختراق خارجي قد يُعزى إلى شن هجمات مضادة إلكترونية على شبكات القوات المسلحة وأجهزة الاستخبارات، وبالتالي التجسس على الأمن العسكري للدول، وتعطيل قدرة الدولة على نشر قدراتها وقواتها بسرعة، أو قطع أنظمة الاتصال بين الوحدات العسكرية وتعطيل شبكات الكمبيوتر. كما أنه من الممكن شل وتعطيل عمل أنظمة الدفاع الجوي أو التوجيه الإلكتروني، بالإضافة إلى إمكانية فقدان السيطرة على وحدات القيادة[30].

2- الأبعاد السياسية:

إن البعد السياسي للأمن السيبراني هو في الأساس حق الدولة في حماية نظامها السياسي وكيانها ومصالحها الاقتصادية، مما يعني حقها وواجبها في السعي لتحقيق رفاهية شعبها في وقت يؤثر فيه توازن القوى داخل المجتمع نفسه عليه. فالفرد الآن يستطيع أن يصبح لاعباً رئيسياً في اللعبة السياسية، ويمكنه الآن الاطلاع على خلفيات ومبررات القرارات السياسية التي تتخذها حكومته من خلال الكم الهائل من المعلومات التي يمكنه الوصول إليها. وفي المقابل، لا يتردد العاملون في الشأن السياسي في الاستفادة مما تقدمه هذه التقنيات للوصول إلى أكبر شريحة ممكنة من الأفراد والترويج لسياساتهم في العالم، ومدى التأثير الذي يتركه ذلك بغض النظر عن صحة السياسات.

3- الأبعاد القانونية:

إن العلاقة بين القانون والتكنولوجيا علاقة تبادلية، فالتطورات التكنولوجية المختلفة تتطلب تشريعات قانونية تواكبها، وذلك بوضع أطر وتشريعات للأفعال المشروعة وغير المشروعة. ولكن بشكل عام، تفتقر الجرائم الإلكترونية في الوقت الحالي إلى أطر قانونية صارمة للتعامل معها. وقد يعود ذلك إلى عوامل مثل طبيعة الجريمة الإلكترونية نفسها، وصعوبة تحديد مرتكبي هذه الجرائم، ومرونة التعريفات المرتبطة بتكنولوجيا المعلومات. بالإضافة إلى ذلك، فإن الجرائم الإلكترونية لا تقيدها حدود الدول، الأمر الذي يتطلب تفعيل التعاون الدولي المشترك لمكافحتها [31].

4- الأبعاد الاجتماعية:

إن الأبعاد الاجتماعية بمعناها الواسع تشمل البعد الاقتصادي الذي نتحدث عنه أولا، ثم البعد الاجتماعي بمعناه الضيق.

أ- **البعد الاقتصادي:** الأمن السيبراني يرتبط ارتباطاً وثيقاً بالاقتصاد، فالارتباط واضح بين اقتصاد المعرفة وتوسع استخدام تكنولوجيا المعلومات والاتصالات، وكذلك القيمة التي تمثلها البيانات والمعلومات المتداولة والمخزنة والمستخدمة على كافة المستويات. كما تعمل تكنولوجيا المعلومات والاتصالات على تمكين التنمية الاقتصادية للعديد من الدول من خلال الاستفادة من الفرص التي توفرها الشركات العالمية والشركات الكبرى التي تسعى إلى إدارة تكاليف إنتاجها في أفضل الظروف. بالإضافة إلى ذلك، دخل العالم عصر النقود الإلكترونية ضمن بيئة تقنية ديناميكية بعد إطلاق الخدمات الإلكترونية، حيث تتزايد استثمارات البنوك والمؤسسات المالية في مجال النقود الرقمية وتتنافس الشركات على إصدار التطبيقات التي تسمح بآليات الدفع الآمنة. وقد وضعت بعض الدول تشريعات خاصة لحماية أموالها وما قد يسببه ذلك من صعوبات والتشريعات المطلوبة للحد من بعض الجرائم الاقتصادية والمالية الخطيرة العابرة للحدود، مثل غسيل الأموال والتهرب الضريبي. ويضمن الأمن السيبراني توفير الخدمات التي توفرها تكنولوجيا المعلومات والاتصالات، كما يضمن الطلب عليها، وهو ما يترجم عملياً إلى تنمية اقتصادية سليمة [32].

ب- **البعد الاجتماعي:** تساهم شبكات التواصل الاجتماعي بشكل خاص في فتح المجال أمام الأفراد للتعبير عن تطلعاتهم السياسية وطموحاتهم الاجتماعية بأشكال مختلفة، كما تشكل مشاركة كافة شرائح المجتمع ومكوناته وسيلة من وسائل تطوير المجتمع، مما يتيح الفرصة للنظر إلى الأفكار والمعلومات وما تشكله من حاجة للمجتمع في الحفاظ على استقرار الفضاء الإلكتروني والمجتمع الذي يقوم عليه، فضلاً عن أن انفتاح المجتمع على المجتمعات الأخرى يؤسس لتبادل الخبرات والأفكار وتكوين آفاق التعاون والتكامل.

المبحث الثاني

النزاع السيبراني وحماية المعلومات

بما أن الفضاء الإلكتروني أصبح ساحة للتفاعلات الدولية، فقد ظهرت أنماط عديدة لتوظيفه سواء من حيث الاستخدامات العسكرية أو المدنية، الأمر الذي جعل من هذا الفضاء ساحة لنزاعات مختلفة سواء للجهات الفاعلة من الدول أو غير الدول، من أجل الاستحواذ على أكبر قدر من النفوذ والتأثير الإلكتروني. ويمكن تعريف النزاع الإلكتروني بأنه استخدام تكنولوجيا الكمبيوتر في الفضاء الإلكتروني لأغراض التدمير بهدف تغيير أو التأثير أو تعديل التفاعلات الدبلوماسية والعسكرية بين مختلف الجهات الفاعلة. كما يُعرف النزاع الإلكتروني بأنه نموذج للحرب غير المتكافئة التي تسعى من خلالها جميع أطراف النزاع المختلفة إلى تعظيم الاستفادة من الفضاء الإلكتروني وبسط النفوذ والهيمنة وحماية أمنها القومي، بالإضافة إلى تحقيق مكاسب استراتيجية واقتصادية وسياسية ومالية لم يكن من الممكن أن تحققها من خلال الوسائل العسكرية التقليدية، خاصة وأن امتلاك القدرات الإلكترونية لم يعد حكراً على جهة معينة، حيث أصبحت الدول الصغيرة والمتوسطة والجهات الفاعلة من غير الدول قادرة على الاستفادة من القدرات الإلكترونية، بما في ذلك تطوير الأسلحة الرقمية وتهديد الخصوم بها[33].

وساعد الفضاء الإلكتروني أيضًا على نشر القوة بين مختلف الجهات الفاعلة، وأعطى مساحة متزايدة للجهات الفاعلة من غير الدول للتأثير على التفاعلات الإقليمية والدولية، مما أدى إلى زيادة التهديدات والمخاطر التي تواجه الدول من خلال الفضاء الإلكتروني [34].

وفي هذا السياق، شكلت القفزات التكنولوجية الهائلة في مجال الاتصالات والمعلومات في أواخر القرن العشرين وبداية القرن الحادي والعشرين مسارات جديدة لاندلاع نزاعات النفوذ السيبراني في الفضاء الإلكتروني، حيث اعتُبر الأخير ساحة واسعة للتفاعلات العالمية التي شملت في الأساس شبكات رقمية ذات اتصال كبير بين الحواسيب وأنظمة الاتصالات وتكنولوجيا المعلومات والإنترنت لغرض تدفق المعلومات. وتكتنف ظاهرة النزاع السيبراني حالة من الغموض وعدم اليقين، وهي أقرب إلى ما سمي بالغموض النووي خلال الحرب الباردة [35].

وبناء على هذه المعطيات، أصبح النزاع في الفضاء الإلكتروني ظاهرة جديدة تتبلور في التفاعلات العالمية، نتيجة الاعتماد المتزايد عليها، سواء من قبل الأفراد أو الجماعات أو الدول. وتطرح هذه الظاهرة في بعض جوانبها خصوصية من حيث طبيعة معنى النزاعات الإلكترونية وأدواتها والجهات الفاعلة فيها. ومن ناحية أخرى، تصطدم بنظيرتها التقليدية لتصبح إحدى أدواتها في التنافس على النفوذ والهيمنة في العالم. وهنا من المهم الإشارة إلى أن هناك أربعة أسلحة رئيسية في النزاعات الإلكترونية، وهي: التخريب والهجوم على المواقع الإلكترونية، وتعطيل الخدمة، والاختراق الفيروسي، وعمليات التسلل [36].

المطلب الأول: النزاع السيبراني:

يُعَدّ الفضاء السيبراني ساحةً للحروب والنزاعات، حيث يتم استغلال غياب النصوص في القانون الدولي التي تنظم هذا المجال. وازدادت الحاجة إلى وضع قوانين سيبرانية مع تصاعد خطر تعرض البنية التحتية للنظام الدولي للمعلومات لهجمات إلكترونية. بالإضافة إلى استخدامه من قِبَل أطراف فاعلة غير حكومية، مثل الجماعات المسلحة، والمافيات، والتجارة غير المشروعة وغيرها. ولهذا السبب، تواجه الدول مخاطر كبيرة في هذا السياق على جميع هياكلها المؤسسية التي تعتمد على الأنظمة الإلكترونية، مما يهدد أمنها وسيادتها ويؤثر على مصالحها.

إن افتراض أن "الحروب والنزاعات السيبرانية لها قوانين تجرمها وتحمل مرتكبيها المسؤولية الدولية" هو افتراض يحتاج إلى التحقق، حيث تناولت القوانين الدولية الحروب والنزاعات التقليدية بمختلف أنواعها ومواقعها على البر والبحر والجو والفضاء الخارجي، ولكن المجال الخامس (الفضاء السيبراني) لم يكن مشمولاً ضمن تلك القوانين. وقد تعقد الوضع أكثر مع ظهور جماعات تنكر شرعية القانون الدولي في الفضاء السيبراني وعدم قبول تبرير الهجمات السيبرانية قانونياً. سنعرض ذلك على النحو التالي:

أولاً: الوصف الدلالي للنزاع السيبراني:

ولعل الجميع لاحظوا انتشار مصطلحات وقوانين لم تكن موجودة من قبل في القرن الحادي والعشرين، مثل قوانين الجرائم الإلكترونية، وقوانين الخصوصية الرقمية، وقوانين الفضاء الإلكتروني، مصحوبة بمفاهيم جديدة مثل مفهوم الحوكمة السيبرانية، والفضاء الإلكتروني، والعلاقات السيبرانية الدولية، والتجارة والاستثمار عبر الإنترنت [37].

وإذا ما تجذرنا أصل كلمة سايبر (**cyber**) تعود الى اليونان(Kybernetes) وهو ما يعني التحكم عن بعد [38]، ومن ثم بدأ الإشارة إلى قانون الأمن السيبراني أو قانون تكنولوجيا المعلومات باسم قانون الإنترنت، أي أن قانون الأمن السيبراني يمكن تعريفه بأنه نظام قانوني مصمم للتعامل مع الإنترنت والحوسبة والفضاء الإلكتروني والقضايا القانونية ذات الصلة، وبعبارة أخرى فإن الوصف المناسب لقانون الإنترنت هو: إنشاء "قوانين ورقية" لتنظيم "العالم الخالي من الورق".

لا شك أن العالم بعد فيروس كورونا شهد تحولاً نوعياً نحو الفضاء الإلكتروني، مصحوباً بزيادة في حجم النزاعات والحروب الإلكترونية، وبدأ الباحثون والمتخصصون والمهتمون في البحث عن وصف متفق عليه للحروب والنزاعات الإلكترونية بين علماء القانون الدولي، وقد عرفها أحد جوانب الفقه بأنها عملية الاستغلال المتعمد لأنظمة شبكات الإنترنت لإرسال برامج خبيثة[39]، وقد تم وصفه أيضًا بأنه سلوك عدواني إلكتروني يهدف إلى إيذاء الآخرين[40]، هو عبارة عن الإجراءات التي تتخذها الدولة لمهاجمة أنظمة المعلومات الخاصة بالعدو بهدف التأثير عليها والدفاع عن أنظمة المعلومات الخاصة بالدولة المهاجمة[41].

وهنا نرى تشابهاً بين الهجوم الإلكتروني والهجوم العادي في أن مرتكب الهجومين لديه دافع لتنفيذ الهجوم، وقد يكون الضحية شخصاً طبيعياً أو اعتبارياً، إلا أن الفارق بينهما يظهر في أداة الهجوم وموقع الهجوم، ففي الهجوم الإلكتروني تكون الأداة عالية التقنية، والموقع الذي انطلق منه الهجوم لا يتطلب من مرتكبه التحرك جسدياً؛ لأنه يتم عن بعد عبر خطوط وشبكات اتصال بين المهاجم وموقع الهجوم، والهجمات الإلكترونية لا يقوم بها أشخاص عاديون، بل مجموعة من محترفي القرصنة الحاسوبية عبر شبكات إلكترونية يشكلون جيشاً إلكترونياً[42].

ومن الواضح أن أسباب الحروب والنزاعات السيبرانية هي ضعف الأمن السيبراني للدول، وظهور العديد من الجهات الفاعلة غير الحكومية في العالم السيبراني التي لا يمكن السيطرة عليها أو فرض القوانين عليها بسهولة، خاصة وأنها تمتلك قدرات تقنية تفوق قدرات الحكومات. والتهديد العالي مقابل ضعف الأمن يشكل فرصة ذهبية للاختراق السيبراني العدواني[43].

ثانياً: النزاع السيبراني و انعكاساته على الأمن والسلم الدوليين:

لا شك أن انتشار الهجمات الإلكترونية الضارة والمدمرة بعد عام 2011 على المستوى الدولي يعود إلى ضعف أنظمة الأمن السيبراني في دول العالم؛ الأمر الذي جعل تهديد السلم والأمن الدوليين أمراً وارداً دائماً، حيث ظهرت هذه الهجمات في حالات كثيرة، منها ثورات التغيير العربية (الربيع العربي) في إستونيا وإيران، وأصبحت أكثر وضوحاً في الحرب الروسية

الأوكرانية، بالإضافة إلى تسريبات أوراق بنما، وحادثة اختراق وكالة أبحاث الإنترنت الروسية، بالإضافة إلى نشر وسائل الإعلام لتفاصيل عن منزل الرئيس الروسي فلاديمير بوتن. ومع اتساع هذه الهجمات، برز السؤال، لماذا لا توجد منظومة محاسبة ومساءلة دولية للحد من هذه الهجمات الإلكترونية؟

لذلك تكمن أهمية قوانين الفضاء الإلكتروني في أنها تفرض إجراءات الاستخدام وتقيس ردود الفعل العامة في الفضاء الإلكتروني، وتزيد من مستوى الأمن والحماية للمعاملات التي تتم عبر الإنترنت، وتخضع جميع الأنشطة عبر الإنترنت للمراقبة من قبل مسؤولي قانون الفضاء الإلكتروني، وتوفر الحماية لجميع البيانات والممتلكات الخاصة بالأفراد والمنظمات والحكومة، وتساعد في الحد من الأنشطة الإلكترونية غير القانونية من خلال توفير الرقابة والعناية الواجبة من قبل مؤسسات الدولة المختصة، كما أن ردود الفعل المقاسة على أي فضاء إلكتروني لها زاوية قانونية مرتبطة بها تختلف باختلاف توجهها سواء كانت متعلقة بالتجارة أو الخدمات أو الأمن بأنواعه المختلفة، ووجود قوانين الفضاء الإلكتروني يعني وجود اتفاقيات دولية في هذا المجال، مما يسمح بتتبع جميع السجلات الإلكترونية من خلال تحقيق التعاون الدولي لتعقب الجرائم المنظمة، ويساعد في إرساء الحوكمة الإلكترونية، مما يرفع بدوره من جودة حياة المستفيدين من خدمات الحكومة الإلكترونية[44].

ولكن ما لا يمكن إنكاره هو الآثار الناجمة عن النزاعات والحروب الإلكترونية وعواقبها الوخيمة على المدنيين، وهناك حاجة لتطبيق القانون الدولي على العمليات الإلكترونية في النزاعات المسلحة والحروب، وذلك بسبب الضرر الذي تسببه للمؤسسات والأفراد وانتهاك أمن الدول وسيادتها[45].

وهنا نذكر "مبدأ التمييز وحظر الهجمات العشوائية وغير المتناسبة". ويتطلب مبدأ التمييز أن تميز أطراف النزاع دائماً بين المدنيين والمقاتلين، وبين الأهداف المدنية والأهداف العسكرية. وفي سياق تطبيق مبدأ التمييز على الهجمات السيبرانية، أشار دليل تالين، على الرغم من قواعده غير الملزمة، إلى أن الأهداف المدنية لا يجوز أن تكون هدفاً للهجمات السيبرانية. على سبيل المثال، لا يجوز توجيه الهجمات السيبرانية التي من المرجح أن تدمر الأنظمة والبنية الأساسية المدنية ما لم تكن هذه الأنظمة من بين الأهداف العسكرية التي يجوز استهدافها وفقاً للظروف السائدة[46].

وبما أن الفضاء الإلكتروني يتألف من عدد لا يحصى من أنظمة الكمبيوتر المترابطة حول العالم، وكثيراً ما تبدو أنظمة الكمبيوتر العسكرية متصلة بأنظمة تجارية ومدنية وتعتمد عليها كلياً أو جزئياً، فمن المستحيل تقريباً شن هجوم إلكتروني على البنية التحتية العسكرية وحصر التأثيرات على هدف عسكري فقط. على سبيل المثال، فإن استخدام دودة تتكاثر ولا يمكن السيطرة عليها وتسبب أضراراً كبيرة للبنية التحتية المدنية من شأنه أن يشكل انتهاكاً للقانون الإنساني الدولي. إن تطبيق مبدأ التمييز بين المقاتلين والمدنيين على الهجمات الإلكترونية أمر معقد للغاية، على عكس الهجمات التقليدية، حيث يكون المهاجم غالباً على بعد مئات الكيلومترات، وهذا يعني أن التمييز بين هدف الهجوم وربما مسافة أبعد من المقاتلين والمدنيين أمر صعب إن لم يكن مستحيلاً. إن مسألة التمييز بين الأهداف، حيث أن التمييز بين الأهداف المدنية والعسكرية في الهجمات الإلكترونية أمر صعب، خاصة وأن أنظمة الكمبيوتر العسكرية غالباً ما تكون متصلة بأنظمة تجارية ومدنية وتعتمد عليها كلياً أو جزئياً، وقد يكون هناك حتى تداخل بينها. وترتبط الاستخدامات المدنية والعسكرية بشبكة واحدة ووسيلة واحدة، وهي الفضاء الإلكتروني. ومن ثم فإنه من غير الممكن شن هجوم سيبراني على البنية التحتية العسكرية وحصر آثاره على هدف عسكري فقط دون الإضرار بالمدنيين والمرافق المدنية[47].

المطلب الثاني: الموقف الدولي من النزاع السيبراني:

إن البحث في إمكانية تطبيق قواعد القانون الدولي على الحرب السيبرانية يتطلب في المقام الأول التكيف القانوني لهذه المسألة من حيث شرعية الحرب السيبرانية وعدم شرعيتها في ظل استخدام القوة في العلاقات الدولية. إن العلاقة بين حق اللجوء إلى الحرب وقانون الحرب تتسم بتوتر لا مفر منه. إن قواعد القانون الدولي المعاصرة تحظر استخدام القوة، باستثناء حق الدول بشكل فردي أو جماعي في الدفاع عن نفسها، أو بموجب استخدام تدابير إنفاذ القانون التي يتخذها مجلس الأمن. وهذا الأمر يتطلب موقفا من المنظمات الدولية مثل الأمم المتحدة لتطبيق القانون الدولي على مرتكبي السلوك العدواني السيبراني، ونوضح ذلك على النحو التالي:

أولاً: دور الأمم المتحدة في تقنين الفضاء السيبراني

فما إن وصل عدد سكان العالم إلى (7.9) مليار نسمة حسب إحصائيات الأمم المتحدة وأكثر من نصف هذا العدد يستخدمون الإنترنت، ليس هذا فحسب بل يستقبل محرك البحث جوجل وحده (3.5) مليار عملية بحث يومياً في المتوسط، ومن المتوقع أن يصل عدد الأجهزة المتصلة بالإنترنت إلى (50) مليار جهاز خلال بضع سنوات، بالإضافة إلى أن منصة الفيسبوك يستخدمها أكثر من (2.9) مليار مستخدم شهرياً وأكثر من (1.9) مليار شخص يومياً، حتى زادت الهجمات والنزاعات والحروب السيبرانية وغيرها من الأعمال العدوانية من الكراهية والابتزاز والتجارة الإلكترونية غير المشروعة في الفضاء الإلكتروني[48].

وهذا دفع الأمم المتحدة في عام 2015 إلى وضع معايير محددة لمواجهة الهجمات الإلكترونية، وتم الاتفاق عليها في عام 2021 بالإجماع من قبل جميع الدول الأعضاء في الأمم المتحدة، بهدف إرساء إطار ملزم سياسيا لجميع الدول التي تستخدم الفضاء الإلكتروني. ومن بين هذه المعايير أن تتعهد الدول بمنع استخدام شبكات الإنترنت في أعمال تهدد أو تضر بالسلم والأمن الدوليين، وعدم السماح عمدا باستخدام أراضيها لأعمال غير قانونية.

وقد أثبتت التجارب الدولية أن الاتفاق على معايير وقواعد دولية خاصة بالفضاء الإلكتروني لا يكفي في حد ذاته لتحقيق الأمن الإلكتروني، بل لابد من وضع استراتيجية دبلوماسية جماعية لمراقبة تطبيق هذه المعايير وفرض العقوبات عند انتهاكها، وهذا يتطلب تحركا سياسيا دوليا لتفعيل المنظومة القانونية في الفضاء الإلكتروني.

إن أحد نقاط الضعف في المعايير التي وضعتها الأمم المتحدة هو غياب المساءلة عن الهجمات السيبرانية الخبيثة. فمن الناحية النظرية، تقع المسؤولية عن أي إجراء فعلي على عاتق المجتمع الدولي من خلال مجلس الأمن التابع للأمم المتحدة.

ولكن الواقع يشير إلى أن التوصل إلى اتفاق داخل الأمم المتحدة لمواجهة الأنشطة الإلكترونية غير القانونية التي تنافي الشرعية الدولية وتُوصَف بالعدوانية يُعَد أمرًا محدودًا للغاية، وذلك لأن المجتمع الدولي يتحرك فقط عندما تُستخدم القوة، وهو أمر غير متوفر في الهجمات الإلكترونية، حيث لم يحدث أن تسبب هجوم إلكتروني في وفاة أي شخص.

ولهذا السبب، لم تُطرح قضية الأمن السيبراني أمام مجلس الأمن الدولي حتى عام 2020، مما يجعلها قضية غير خطيرة في نظر معظم الدول الأعضاء غير المتورطة بشكل مباشر في النزاع السيبراني. لكن هذا الوضع بدأ يتغير مع تزايد مخاطر الأنشطة السيبرانية غير المشروعة، والاعتماد المتزايد على الشبكات العالمية، وتطور المنافسة بين القوى العظمى. وللتغلب على هذه المشكلة، يرى القائمون على الأمم المتحدة ضرورة اتخاذ بعض التدابير المتوافقة مع القانون الدولي والمعايير المتفق عليها، من أجل خلق المساءلة الدولية لمواجهة الهجمات السيبرانية؛ لأنها قضايا خطيرة[49].

والمشكلة هي أن إسناد قضايا الأمن السيبراني إلى كيان مستقل تابع لطرف ثالث لن يحظى بدعم دولي. وقد أظهرت المناقشات في هذا الصدد أنه من الصعب التحقيق في قوى سيبرانية كبرى مثل الصين أو الولايات المتحدة، لكنها مع ذلك أعربت عن استعدادها للتحقيق في عدد قليل من الدول الضعيفة، مثل كوريا الشمالية، أو المجرمين السيبرانيين، إذا كان من الممكن تحديد أنهم لا يعملون كوكيل لدولة. أحد التحديات التي تواجه المعايير المقدمة في عام 2015 هو أنها تدعو جميع الدول إلى المشاركة في التحقيق اللازم لتوضيح ظروف الهجوم السيبراني، مما يجعل الإسناد مهمة معقدة، لأنه في حالة وقوع حادث سيبراني، ستكون الدول ملزمة بالكشف عن جميع المعلومات ذات الصلة بالحادث، ومن المتوقع أن تعترض الدول على هذا التدخل. ينص الاقتراح الروسي الذي تم تقديمه على أنه ستكون هناك حدود للاعتراضات المحتملة من الدول المعنية في حالة إسناد حادث سيبراني إلى دولة معينة أو اتهامها. بالطبع، سوف تنفي الصين وروسيا (أو على الأرجح أي قوة سيبرانية) الاتهام، لكن الهدف ليس إقناعهما بقبول الاتهام، بل إقناع القادة الوطنيين والجمهور العالمي. أما بالنسبة للشركات الخاصة مثل FireEye أو Cloudstrike، فهي تمتلك حاليًا القدرة على اكتشاف مصدر الهجوم السيبراني المعادي، لكن هذا التقدم في تحديد المصدر غير معترف به في المجتمع الدولي، حيث لا يوجد اتفاق على مستوى الإسناد المطلوب للعمل التعاوني بين الدول[50].

ويدعم هذا الاستنتاج بقوة الرأي الاستشاري لمحكمة العدل الدولية المعنون "مشروعية التهديد باستخدام الأسلحة النووية أو استخدامها"، حيث لاحظت المحكمة أن المبادئ والقواعد الراسخة للقانون الإنساني الدولي المنطبقة في النزاعات المسلحة تنطبق "على جميع أشكال الحرب وجميع أنواع الحرب". وخلصت اللجنة الدولية للصليب الأحمر إلى أن هذا الاستنتاج ينطبق على استخدام العمليات السيبرانية في النزاعات المسلحة[51].

لهذا، يجب على الطرف المسؤول عن أي هجوم اتخاذ التدابير اللازمة، بقدر الإمكان، لتجنب أو تقليل الضرر العرضي الذي قد يصيب البنية التحتية المدنية أو يضر المدنيين. ويتطلب ذلك التحقق من طبيعة الأنظمة المستهدفة والأضرار المحتملة الناتجة عن الهجوم. وهذا يعني أنه إذا تبين بوضوح أن الهجوم سيتسبب في إصابات أو أضرار مدنية عرضية، فيجب إلغاؤه.

وعلاوة على ذلك، يجب على أطراف النزاعات اتخاذ الاحتياطات اللازمة لتجنب آثار الهجمات. لذلك، يُنصح هذه الأطراف بتقييم مدى فصل أنظمة الكمبيوتر العسكرية عن الأنظمة المدنية بشكل كافٍ، لضمان حماية السكان المدنيين من آثار الهجمات العرضية. كما أن الاعتماد على أنظمة الكمبيوتر العسكرية وربطها بأنظمة الكمبيوتر التي يديرها متعاقدون مدنيون تُستخدم أيضًا لأغراض مدنية قد يثير القلق.

من جهة أخرى، يمكن أن تسهم تكنولوجيا المعلومات في تقليل الأضرار العرضية التي قد تصيب المدنيين أو البنية التحتية المدنية. فعلى سبيل المثال، يؤدي تعطيل بعض الخدمات المستخدمة لأغراض عسكرية ومدنية إلى أضرار أقل مقارنة بتدمير البنية التحتية بالكامل. وفي مثل هذه الحالات، يفرض مبدأ الحيطة والحذر على الدول اختيار الوسائل الأقل ضرراً لتحقيق أهدافها العسكرية. وفي الحالات التي لا تشملها القواعد الحالية للقانون الإنساني الدولي، يظل المدنيون والمقاتلون محميين بموجب ما يُعرف بـ"بند مارتنز"، مما يعني أنهم يبقون تحت حماية وسلطة مبادئ القانون الدولي كما أقرتها الأعراف، ومبادئ الإنسانية، وإملاءات الضمير العام[52].

وشهدت هذه المرحلة بداية ظهور شبكة الويب العالمية، والتي يعود تاريخها إلى عام 1991 من خلال جهود العالم البريطاني تيم بيرنرز لي أثناء عمله في المنظمة الأوروبية للأبحاث النووية[53]، كان أول هجوم إلكتروني يمكن أن يهدد السلام والأمن الدوليين في مايو 1998، عندما هاجمت مجموعة من القراصنة الصينيين يطلقون على أنفسهم "مركز الاستجابة

السريعة للقراصنة الصينيين" المكون من 3000 قراصنة مواقع الحكومة الإندونيسية بسبب انتشار المظاهرات في إندونيسيا. ومن هذه الحادثة، أدركت الأمم المتحدة الخطر الحقيقي الذي يمكن أن تشكله إندونيسيا على الصين[54].

وقد ازداد الاهتمام الدولي بهذه القضية بعد العرض الروسي لقضية العلاقة بين تطورات الإنترنت والأمن الدولي أمام الجمعية العامة في عام 1998 بناء على طلب الاتحاد الروسي. وقررت الجمعية العامة إدراج هذه القضية على جدول أعمالها تحت عنوان "التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي" وطلبت من البلدان إبداء آرائها[55].

وقد استجابت الأمم المتحدة لذلك بإنشاء أول فريق خبراء في العام 2004، واستمرت اجتماعاته لأكثر من عامين بين عامي 2004 و2005، إلا أنه لم يتوصل إلى إجماع بشأن المبادئ الواجب اتباعها بسبب صعوبة الرصد والتجريم في هذا المجال وعدم إيلائه اهتماماً دولياً كافياً، حيث لا يرقى إلى مستوى العدوان أو التهديد الحقيقي[56]، لكن عامي 2006 و2007 شهدا زيادة في الهجمات الإلكترونية، وأهمها ما حدث في إستونيا عام 2006، والذي أدى إلى تعطيل أغلب مرافق البلاد. ونتيجة لذلك، أعقبت ذلك حوادث مماثلة في جورجيا عام 2008، ووجهت الاتهامات إلى روسيا، ولكن من دون أدلة[57].

وقد دفع الضرر الذي لحق بإستونيا في عام 2007 إلى مطالبة الأمم المتحدة بإدانة هذه الهجمات وإعطاء أهمية أكبر للقواعد التي تحكم السلوك السيبراني للدول[58]، وفي الواقع، قررت الجمعية العامة إنشاء فريق ثانٍ في عام 2009، يتكون من خمسة عشر عضواً[59]، وعقد الفريقان اجتماعات من عام 2009 إلى عام 2010، ثم أعقب ذلك فريق ثالث بدأ العمل من عام 2012 إلى عام 2013، بشكل مطول ومفصل، دون التوصل إلى مبادئ بشأن السلوك السيبراني[60] وأشار فقط إلى "ضرورة مواصلة الحوار لمناقشة المعايير المتعلقة باستخدام البلدان لتكنولوجيا المعلومات والاتصالات"[61]، وتمكن من التوصل إلى المبادئ الأولية لقواعد السلوك، لكن الفريق الرابع الذي شكلته المنظمة في عام 2014[62]، وتبين أن الدولة التي تقوم بعمل عدائي تتحمل المسؤولية الدولية بعد إثبات قيامها بهذا العمل في الفضاء الإلكتروني، حيث أشار التقرير لأول مرة إلى أن القانون الدولي ينطبق على الفضاء الإلكتروني[63]، تم تشكيل الفريق الخامس في عام 2016 لاستكمال عمل الفريق السابق[64]، ولكنه أعلن عدم قدرته على التوصل إلى إجماع بشأن المبادئ الأساسية للسلوك[65]، تم تشكيل فريق سادس على أساس التوزيع الجغرافي العادل للدول في 2 يناير 2019. وبعد عامين من الاجتماعات وظهور علامات التوافق السياسي بين الدول الأطراف، تمكن الفريق من إصدار[66] وفي 14 يوليو/تموز 2021، تم اعتماد تقرير نهائي بالإجماع بين جميع أعضائها وتضمن لأول مرة معايير السلوك المقبول في الفضاء الإلكتروني. ومع ذلك، شهدت هذه المرحلة إنشاء مجموعة خبراء ثانية، بناءً على اقتراح من الاتحاد الروسي، وأطلق عليها اسم مجموعة العمل المفتوحة العضوية المعنية بالتطورات في مجال المعلومات والاتصالات في سياق جميع أعضاء الجمعية العامة للأمم المتحدة[67].

ومن هنا نستنتج أن المبادئ التقليدية يمكن تطبيقها على الفضاء الإلكتروني، مثل: مبدأ احترام السيادة في الفضاء الإلكتروني، ومبدأ عدم استخدام القوة في العلاقات الدولية السيبرانية، ومبدأ حل النزاعات السيبرانية بالوسائل السلمية، ومبدأ عدم التدخل في الشؤون الداخلية في الفضاء الإلكتروني، ووضع قواعد للفضاء الإلكتروني الدولي، ومبدأ التعاون الدولي في الفضاء الإلكتروني، ومبدأ التحقيق في القضايا السيبرانية، ومبدأ احترام حقوق الإنسان في الفضاء الإلكتروني.

إن مبرر ضرورة التطبيق هو ظهور وانتشار قواعد إقليمية تتنافس مع القانون العام الدولي لتنظيم قواعد الإنترنت إقليمياً. وهناك حالياً ثلاث مجموعات من القواعد التي تنظم موضوع الإنترنت، مثل:

1. قواعد (Tallinn) للقانون الدولي في الفضاء السيبراني 2017 والتي تتكون من (154) قاعدة قانونية[68].
2. قواعد باريس (Paris Call) لعام 2018، تتكن من (9) مبادئ لتنظيم الفضاء السيبراني، انضمت لها (81) دولة[69].

3. واعد شنغهاي لعام 2015 ، والذي اطلقته منظمة شنغهاي لتظيم العمل في الفضاء السيبراني[70].

ثانياً: المسئولية وضوابط المساءلة:

إن الإسناد هو الخطوة الأولى لتحقيق الأمن السيبراني، لكنه غير كافٍ. قد تعرف الأمم المتحدة جيداً من المسؤول، لكنها لا تتخذ أي إجراء فعلي، حيث يتطلب ذلك قراراً من مجلس الأمن وبناءً على طلب الدولة التي تعرضت للهجوم. أما فيما يتعلق بالتدابير الحالية، فلا يمكن تجاهل بعض الجهود الدولية لتحقيق المساءلة وتحديد شروط العمل الجماعي والاتفاق عليها، مثل إطار الاستجابة الدبلوماسية السيبرانية للاتحاد الأوروبي، وقانون الفضاء السيبراني الدولي، والالتزامات ضمن معاهدات الدفاع الجماعي عن النفس، والبيان المشترك الصادر عن وزارة الخارجية الأميركية في سبتمبر/أيلول 2019 بشأن تعزيز السلوك المسؤول للدول في الفضاء السيبراني. وقد وافقت (28) دولة في هذا البيان على التعاون بشكل طوعي لمحاسبة الدول عند التصرف بشكل مخالف، من خلال اتخاذ تدابير وفقاً للقانون الدولي بهدف توسيع الامتثال لمعايير 2015 وزيادة الأمن السيبراني. بالإضافة إلى ذلك، تشمل هذه التدابير العقوبات التي يفرضها الاتحاد الأوروبي أو الاتهامات والعقوبات التي تفرضها الولايات المتحدة الأميركية.

وإذ يؤكد أن القانون الإنساني الدولي، بما في ذلك مبادئ التمييز والتناسب والحذر، ينطبق على العمليات السيبرانية أثناء النزاعات المسلحة بموجب أحكامه، بما في ذلك:

1. يحظر استخدام القدرات السيبرانية العشوائية بطبيعتها والمصنفة كأسلحة.
2. يحظر توجيه الهجمات ضد المدنيين والأهداف المدنية بشكل مباشر، بما في ذلك عند استخدام وسائل أو أساليب الحرب السيبرانية.
3. يحظر ارتكاب أعمال العنف أو التهديد بها بهدف نشر الرعب بين السكان المدنيين، بما في ذلك عند ارتكابها من خلال وسائل أو أساليب الحرب السيبرانية.
4. يحظر ارتكاب هجمات عشوائية، أي الهجمات التي تضرب الأهداف العسكرية والمدنيين أو الأهداف المدنية دون تمييز، بما في ذلك عند استخدام وسائل أو أساليب الحرب السيبرانية.
5. يحظر ارتكاب هجمات غير متناسبة، بما في ذلك عند استخدام وسائل أو أساليب الحرب السيبرانية. الهجمات غير المتناسبة هي تلك التي من المتوقع أن تسبب خسائر عرضية في أرواح المدنيين أو إصابتهم أو إلحاق الضرر بالأهداف المدنية، أو التي قد تكون مفرطة مقارنة بالميزة العسكرية الملموسة والمباشرة المتوقعة.
6. يحظر مهاجمة أو تدمير أو إزالة أو جعل الأشياء الضرورية لبقاء السكان المدنيين غير صالحة للاستخدام، بما في ذلك عند استخدام وسائل أو أساليب الحرب السيبرانية.
7. يجب حماية الوحدات الطبية واحترامها، بما في ذلك عند تنفيذ العمليات السيبرانية أثناء النزاعات المسلحة.

8. ممارسة الحذر الدائم في إدارة العمليات العسكرية، بما في ذلك عند استخدام وسائل أو أساليب الحرب الإلكترونية، من أجل تجنب السكان المدنيين والأهداف المدنية؛ واتخاذ جميع الاحتياطات الممكنة عند تنفيذ الهجمات من أجل تجنب التسبب في ضرر عرضي للمدنيين، بما في ذلك عند استخدام وسائل أو أساليب الحرب الإلكترونية.

ثالثاً: التكيف القانوني للنزاع السيبراني:

وعلى حد تعبير كوردولا دروغيت، المستشارة القانونية في المفوضية الدولية، "لا يوجد فراغ قانوني في الفضاء الإلكتروني"[71]، في مختلف أنحاء العالم، يدرس صناع السياسات والقادة العسكريون الآثار المترتبة على الحرب السيبرانية. وتوضح كوردولا دروغي، المستشارة القانونية في اللجنة الدولية للصليب الأحمر، أن الإطار القانوني القائم قابل للتطبيق ويجب احترامه حتى في الفضاء الإلكتروني، ووصفته بأنه سلوك إلكتروني له تأثير في "العالم الحقيقي". وعلى نحو مماثل، لا يوجد معنى قانوني متفق عليه دوليا لمصطلحات مثل "الهجمات السيبرانية" أو "العمليات السيبرانية" أو "الهجمات على شبكات الكمبيوتر"، والتي تشير إلى الهجمات والنزاعات والحروب عبر الأجهزة الإلكترونية[72].

ومن أخطر استخداماته كان ضد نزاع كوسوفو عام 1999 من قبل حلف شمال الأطلسي. فبعد استهداف طائرات الحلف للسفارة الصينية في بلغراد، قام عدد من القراصنة الصينيين، ردا على ذلك، بمهاجمة المواقع الرسمية للولايات المتحدة الأمريكية، وخاصة موقع البيت الأبيض، مما أدى إلى الحصول على آلاف البيانات الرقمية التي كانت تعتبر سرية للغاية في ذلك الوقت[73].

هناك هجوم إلكتروني على المفاعل النووي الأميركي "ديفيد بيس" لتوليد الكهرباء في أوهايو في 2 يونيو/حزيران 2003، نتيجة اختراق وتعطيل أنظمة شبكات التحكم والتحكم الإلكترونية في المفاعل نفسه[74].

ومن المعروف أن القانون الدولي الإنساني لا ينطبق إلا إذا ارتكبت العمليات السيبرانية في سياق نزاع مسلح، سواء بين الدول، أو بين الدول والجماعات المسلحة المنظمة، أو بين الجماعات المسلحة المنظمة[75]، وعليه، فمن الضروري التمييز بين القضية العامة المتمثلة في الأمن السيبراني والقضية الخاصة بالعمليات السيبرانية في النزاعات المسلحة. ففي حالات النزاع المسلح، ينطبق القانون الإنساني الدولي عندما تلجأ الأطراف إلى أساليب ووسائل حرب تعتمد على العمليات السيبرانية[76].

إن استخدام العمليات السيبرانية أثناء النزاعات المسلحة أمر واقع. ورغم أن عدداً قليلاً من الدول اعترفت علناً بإجراء مثل هذه العمليات، فإن استخدام هذه العمليات من المرجح أن يزداد في المستقبل مع قيام المزيد من الدول بتطوير قدراتها السيبرانية لأغراض عسكرية[77].

إن التكنولوجيات الجديدة من كافة الأنواع تتطور باستمرار، والقانون الدولي الإنساني شامل بما يكفي لاستيعاب هذه التطورات. ومع ذلك، فهو ينظم من خلال قواعده العامة جميع أساليب ووسائل الحرب، بما في ذلك استخدام جميع الأسلحة، خاصة وأن المادة (36) من البروتوكول الإضافي الأول لاتفاقيات جنيف تنص على ما يلي: "يلتزم كل طرف سام متعاقد، عند دراسة أو تطوير أو اقتناء سلاح جديد أو وسيلة حرب أو أسلوب حرب، بالتأكد مما إذا كان مثل هذا الاستخدام محظوراً في كل أو بعض الظروف بموجب هذا البروتوكول أو بموجب أي قاعدة أخرى من قواعد القانون الدولي تكون الدولة الطرف المتعاقدة ملزمة بها". وبخلاف نطاق الالتزام المحدد الذي تفرضه هذه القاعدة على الدول الأطراف، فمن الواضح أن القواعد العامة للقانون الدولي الإنساني تنطبق على التكنولوجيا الجديدة[78].

ولكن هذا لا يعني أنه لا توجد حاجة إلى مزيد من تطوير القانون مع تطور التكنولوجيات، أو مع تزايد فهمنا لتداعياتها الإنسانية. ويتعين على الدول أن تقرر هذا، وإذا لم تقرره بعد، فمن الضروري التأكيد على أنه لا يوجد فراغ قانوني في الفضاء الإلكتروني، بل على العكس من ذلك[79].

ولكن الجهات الفاعلة المجهولة تشكل جانباً واحداً من صعوبة محاسبة المسؤولين في الفضاء الإلكتروني. ففي العمليات الإلكترونية التي تحدث يومياً، يشكل عدم الكشف عن الهوية القاعدة وليس الاستثناء، وفي بعض الحالات من المستحيل تعقب المصدر؛ سواء كان الجاني شخصاً ينطبق عليه القانون الإنساني الدولي، أو مؤسسة حكومية ينطبق عليها القانون العام الدولي[80].

ويجب توضيح أن التأكيد على إمكانية تطبيق القانون الإنساني الدولي على العمليات السيبرانية أثناء النزاعات المسلحة لا يضفي الشرعية على الحرب السيبرانية أو يشجع على عسكرة الفضاء الإلكتروني. والواقع أن القانون الإنساني الدولي يفرض بعض القيود على عسكرة الفضاء. وعلاوة على ذلك، فإن أي لجوء إلى القوة من جانب الدول السيبرانية من خلال حظر تطوير القدرات السيبرانية العسكرية التي تنتهك القانون الإنساني الدولي ذي الطبيعة السيبرانية أو الحركية يظل خاضعاً لميثاق الأمم المتحدة وقواعد القانون الدولي العرفي ذات الصلة، وخاصة حظر اللجوء إلى القوة. ويجب تسوية النزاعات الدولية بالوسائل السلمية، في الفضاء الإلكتروني كما هو الحال في جميع المجالات الأخرى[81].

وصدر تقرير فريق الخبراء في عام 2021، متضمناً مجموعة من المبادئ المتعلقة بتطبيق القانون الدولي العام على العمليات التي تقوم بها الدول في الفضاء السيبراني. وكان لمنظمة الأمم المتحدة دور أساسي في تشكيل هذا الفريق، الذي ساهم في إعداد هذه المبادئ. وهذا يبرز أهمية دور المنظمة في وضع قواعد متكاملة للتعامل مع التهديدات التي يفرضها الفضاء السيبراني على الأمن والسلم الدوليين.

الخاتمـة:

وبالمحصلة، نجد أن القانون الدولي لا ينطبق على معظم هذه الحالات، حيث إن القانون الدولي العام يقتصر تطبيقه على العمليات السيبرانية التي تُنفذ في سياق حرب عدوانية تشنها دولة ضد أخرى أو ضد مجموعة من الدول بهدف إلحاق الضرر بها وتدمير بنيتها التحتية. وبالمثل، فإن القانون الدولي الإنساني لا يسري على أغلب هذه الأعمال السيبرانية غير القانونية، إذ إنه يقتصر على العمليات السيبرانية التي تحدث في سياق نزاع مسلح. ومن المُعترف به أن مسألة مدى تطبيق القانون الدولي الإنساني على العمليات السيبرانية تُعد نقطة خلاف في المناقشات الجارية التي تقودها الأمم المتحدة بشأن هذا الموضوع.

أولاً: النتائج:

وأظهرت الدراسة العديد من النتائج وأهمها:

1. ينطبق القانون الدولي بفروعه على السلوك السيبراني العدواني وفقًا لاختصاصه، شرط وجود أدلة تثبت هوية مرتكب الجريمة، سواء كان شخصًا طبيعيًا (فردًا) أو شخصًا اعتباريًا (جهة أو مؤسسة رسمية)، مما يؤكد عدم وجود فراغ قانوني في الفضاء السيبراني.

2. تعاني أغلب الدول من نقص في التشريعات التي تنظم عمل أفرادها ومؤسساتها وسياساتها في الفضاء السيبراني، وحتى في حال وجود قوانين، فإنها تحتوي على ثغرات قانونية في هذا المجال.

3. إدراج الهجمات السيبرانية ضمن الإطار القانوني الدولي الحالي يُعد أمرًا بالغ الصعوبة بسبب طبيعتها الخاصة، بالإضافة إلى غياب بيان قانوني رسمي ونهائي متفق عليه بشأن التسلح السيبراني والإلكتروني بين الدول.
4. التكييف القانوني لتجريم العمليات السيبرانية العدوانية دوليًا يجعل الدولة مسؤولة عن الهجمات السيبرانية التي تقوم بها والتي تلحق الضرر بدولة أخرى، بناءً على الأعمال السيبرانية التي تنفذها الدولة.
5. يُعتبر الهجوم الإلكتروني استخدامًا غير مشروع للقوة بسبب آثاره المدمرة التي توازي الهجوم المسلح، بل قد تكون أكثر خطورة وتدميرًا، مما يجعله يرتقي إلى مستوى الهجوم التقليدي.
6. الجرائم الإلكترونية، كونها جرائم عالمية عابرة للحدود، لا يمكن التصدي لها إلا من خلال التعاون الدولي على المستوى الإجرائي الجنائي.
7. يمكن تطبيق القوانين الدولية في الفضاء الإلكتروني في حالات الحروب والنزاعات الإلكترونية للحفاظ على السلام والأمن الدوليين، حيث لا يوجد فراغ قانوني في الفضاء الإلكتروني.

ثانياً: التوصيات:

بناءً على ما جاء في الدراسة من محتوى يجب التوصية بالآتي:

1- وضع تشريعات دولية تحت مسمى "القانون السيبراني الدولي" لتطبيقها في حالات النزاعات والحروب بين الدول والأفراد.
2- وضع قوانين وطنية تنظم عمل الأفراد والمؤسسات الحكومية في الفضاء السيبراني.
3- تطوير الإطار التشريعي الجنائي الوطني بما يتماشى مع الجهود الدولية لمكافحة الجرائم السيبرانية.
4- تعزيز التعاون الدولي وتفعيل دور المعاهدات الدولية ومبدأ المساعدة القانونية والقضائية والأمنية المتبادلة في مكافحة الجرائم السيبرانية.
5- إنشاء شراكات بين القطاعين العام والخاص على المستويات الوطنية والإقليمية والدولية لمكافحة الجرائم السيبرانية، وتبادل الخبرات، وتحسين أساليب مواجهتها، كونها جرائم عابرة للحدود الوطنية قبل أن تتطور إلى نزاعات تؤثر على السلم والأمن الدوليين.
6- تعزيز التعاون وتبادل المعلومات مع المنظمات الدولية والإقليمية ذات الصلة بالمبادرات المتعلقة بالأمن السيبراني، مع الأخذ في الاعتبار احتياجات الدول النامية للمساعدة.
7- إنشاء نظام سريع وفعال للتعاون الدولي، مع ضمان حفظ البيانات المخزنة إلكترونيًا والإفصاح الجزئي عن حركة هذه البيانات، وتدريب الكوادر الوطنية على تعزيز الأمن الإلكتروني وحماية البنية التحتية الرقمية.

8- اتخاذ التدابير اللازمة لحماية الدول من الهجمات الإلكترونية من خلال تعزيز قدرات المؤسسات المختلفة على التعامل مع هذه الهجمات والحد من تداعياتها، بالإضافة إلى نشر الوعي الإلكتروني في المجتمع وبناء منظومة متكاملة للأمن الإلكتروني لضمان الحماية والسيادة الرقمية.

قائمة المراجع:

أولاً: المعاجم:

- ابن منظور، محمد بن مكرم (2000): لسان العرب، ط1، ج1، دار صادر، بيروت، لبنان.
- عطية، شعبان عبد العاطى، وآخرون (2004): المعجم الوسيط، ط4، مكتب الشروق الدولية، مجمع اللغة العربية، مصر.

ثانياً: الكتب:

- أبو عامود، محمد سعد (2013): المفهوم العام للأمن المعلوماتى، جامعة حلوان، مصر.
- الأشقر، منى جبور (2017): السيبرانية هاجس العصر، المركز العربى للبحوث القانونية والقضائية، بيروت، لبنان.
- بوخضرة، إيناس (2022): الأحكام العامة لمفهوم الأمن السيبرانى، بحث منشور، كتاب جماعى دولى "التحكيم الدولى وتحديات الأمن السيبرانى"، المملكة المتحدة – بريطانيا، المركز المغاربى شرق أدنى للدراسات الاستراتيجية، ط1.
- التلمسانى، مؤنس عبد اللطيف أحمد (2022): الأمن السيبرانى والتحليل السسيولوجى للمجتمع، دار البازورى العلمية، للنشر والتوزيع.
- الحمامصة، إبراهيم، والعمارات، فارس محمد (2022): الأمن السيبرانى – المفهوم الحديث والمعاصر، ط1، دار الخليج للنشر والتوزيع، عمان، الأردن.
- خليفة، إيهاب (2017): القوة الإلكترونية، العربى للنشر والتوزيع، ط1، القاهرة.
- سمودى، رزق أحمد (2018): حق الدفاع عن النفس نتيجة الهجمات الإلكترونية.
- شفيق، نوران (2014): أثر التهديدات الإلكترونية على العلاقات الدولية، دراسة فى أبعاد الأمن الإلكترونى، المكتب العربى للمعارف، القاهرة.
- عبد الصادق، عادل (2009): الإرهاب الإلكترونى، القوة فى العلاقات الدولية – نمط جديد وتحديات مختلفة، مركز الدراسات والسياسات الاستراتيجية، القاهرة، مصر.
- عبد الصادق، عادل (2016): أسلحة الفضاء الألكتروني في ضوء القانون الدولي الإنساني، مكتبة المستقبلية، مصر.
- عبد الصادق، عادل (2020): الاقتصاد الرقمى – تحديات السيادة السيبرانية، المركز العربى لأبحاث الفضاء الإلكترونى، القاهرة، مصر.
- العلى، على زياد، وحميد، على حسين (2023): تكتيكات الحروب الحديثة "الأمن السيبرانى والحروب المعززة والهجينة"، دار العربى للنشر والتوزيع، القاهرة، مصر.

- اللقانى، عبد الرحمن على (2022): دور الأمن السيبرانى فى تعزيز أمن المعلومات المالية الإلكترونية، دار البازورى العلمية، للنشر والتوزيع.
- هنكرتس، ودوزوالد -بك (2005): القانون الدولي الانساني العرفي، مج1، قواعد اللجنة الدولية، مطبعة جامعة كامبريدج.
- الهيئة الوطنية للأمن السيبرانى: (2018): الضوابط الأساسية للأمن السيبرانى، المملكة العربية السعودية.
- الاتحاد الدولى للاتصالات (2007): دليل الأمن السيبرانى للبلدان النامية، الموجز التنفيذى للمعلومات.

ثالثاً: الرسائل العلمية:

- دير، أمينة (2014): أثر التهديدات البيئية على واقع الأمن الإنسانى فى أفريقيا حالة دول القرن الأفريقى، مذكرة لنيل شهادة الماجستير فى العلوم السياسية والعلاقات الدولية، جامعة محمد خيضر بسكرة.
- الزهرانى، عبد الله يحيى سعيد (2020): استراتيجيات الأمن السيبرانى فى ضوء التقنيات والتحديات الحديثة، دراسة مقارنة، رسالة ماجستير، فى العلوم الاستراتيجية، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية، قسم الدراسات الاستراتيجية، السعودية.
- الشوابكة، محمد أمين أحمد (2002): الجرائم المرتكبة عبر الإنترنت، رسالة لنيل درجة الماجستير فى القانون، معهد البحوث العربية للتربية والثقافة والعلوم، جامعة الدول العربية، القاهرة.

رابعاً: الأبحاث العلمية المنشورة:

- إبراهيم، يسرى خالد (2011): حرب المعلومات ماهيتها وأنواعها ومستوياتها، مجلة الباحث الإعلامى، مج3، ع13، كلية الإعلام، جامعة بغداد.
- الأشقر، منى جبور (2012): الأمن السيبرانى: التحديات ومستلزمات المواجهة، المركز العربى للبحوث القانونية والقضائية، جامعة الدول العربية.
- دروغيه، كوردولا (2023): ما من فراغ قانوني في الفضاء السيبراني، اللجنة الدولية للصليب الأحمر.
- السيد محمد السيد احمد،القانون في الفضاء السيبراني، المنصة القانونية مقال منشور في 7/ 6/ 2022، متاح على الرابط :http://www.sajplus.com
- شميت، مايكل (2012): الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر.
- عبد الصادق، عادل (2017): خطر الحروب السيبرانية عبر الفضاء الإلكترونى، مجلة الأهرام للكمبيوتر والإنترنت، والاتصالات، عدد مارس.
- عبد الصبور عبد الحى، سماح (2017): النزاع السيبرانى – طبيعة المفهوم وملامح الفاعلين، مجلة السياسة الدولية، ملحق اتجاهات نظرية، النزاع السيبرانى، التنازع العالمى على قوة الفضاء الإلكترونى، ع208، مركز الأهرام للدراسات الاستراتيجية.
- عثمان، أحمد زكى (2017): تأثير القدرات السيبرانية فى النزاعات الإقليمية، ملحق مجلس السياسة الدولية، اتجاهات نظرية، النزاع السيبرانى، مركز الأهرام للدراسات الاستراتيجية، ع208، القاهرة.

- عطية، إدريس (2019): مكانة الأمن السيبرانى فى منظومة الأمن الوطنى الجزائرى، دراسة منشورة، جامعة العربى التبسى، الجزائر.
- عفيفى، عبد الغفار (2018): استراتيجية الردع السيبرانى... التجربة الأمريكية، مجلة السياسة الدولية، مركز الأهرام للدراسات الاستراتيجية، ع213، القاهرة.
- الفتلاوى، أحمد عبيس نعمة (2016): الهجمات السيبرانية مفهومها والمسئولية الدولية الناشئة عنها فى ضوء التنظيم الدولى المعاصر، مجلة المحقق المحلى للعلوم القانونية والسياسية، مج8، ع4، كلية القانون، جامعة بابل، العراق.
- فرحان، علاء الدين (2021): من الردع النووى إلى الردع السيبرانى، دراسة لمدى تحقيق مبدأ الردع فى الفضاء السيبرانى، مجلة الفكر، مج16، ع1، جامعة بسكرة، الجزائر.
- كلنتر، زهراء عماد محمد (2020): تكييف الهجمات السيبرانية فى ضوء القانون الدولى، مجلة الكوفة للعلوم القانونية والسياسية، مج1، ع1/44.
- المطيرى، خالد ظاهر عبد الله جابر السهيل (2022): دور التشريعات الجزائية فى حماية الأمن السيبرانى بدول مجلس التعاون الخليجى، مجلة البحوث الفقهية والقانونية، ع38.

خامساً: الوثائق والقرارات والتقارير الدولية:

- محكمة العدل الدولية، مشروعية التهديد بالأسلحة النووية أو استخدامها، فتوى،8 تموز/ يوليو ،1996 الفقرة86.
- ديباجة اتفاقية الهاي الثانية لعام 1899.
- ديباجة اتفاقية لاهاي الرابعة لعام 1907.
- قرار الجمعية العامة للأمم المتحدة في 4 كانون الثاني 1999، وثائق الامم المتحدة، الوثيقة (A/RES/53/70).
- مذكرة الامين العام للأمم المتحدة في 5 اب 2005، وثائق الامم المتحدة، الوثيقة(A/60/202) .
- قرار الجمعية العامة للأمم المتحدة في 6 كانون الثاني2006، وثائق الامم المتحدة، الوثيقة (A/RES/60/45).
- قرار الجمعية العامة للأمم المتحدة في 13 كانون الاول، 2011 وثائق الامم المتحدة، الوثيقة (A/RES/66/24).
- قرار الجمعية العامة للأمم المتحدة في 6 كانون الثاني، 2014 وثائق الامم المتحدة، الوثيقة (A/RES/68/243).
- قرار الجمعية العامة للأمم المتحدة في 30 كانون الثاني2015 ،وثائق الامم المتحدة، الوثيقة (A/RES/70/237).
- تقرير الأمين العام للأمم المتحدة في 14 اب2017 ،وثائق الامم المتحدة، الوثيقة (A/72/327).
- قرار الجمعية العامة للأمم المتحدة في 2 كانون الثاني2019 وثائق الامم المتحدة، الوثيقة (A/RES/73/266).
- تقرير الخبراء المذكور في مذكرة الأمين العام للأمم المتحدة في 14 تموز ، 2021وثائق الامم المتحدة، الوثيقة (A/76/135).
- الملحق (البروتوكول) الأول الإضافي لاتفاقيات جنيف.
- اللجنة الدولية (2015): القانون الدولي الانساني وتحديات النزاعات المسلحة المعاصرة.
- مذكرة الامين العام للأمم المتحدة، في30 تموز ،2010 وثائق الامم المتحدة، الوثيقة (A/65/201).
- مذكرة الامين العام للأمم المتحدة في 22 تموز ،2015 وثائق الامم المتحدة، الوثيقة(A/70/174).
- البروتوكول الإضافي الأول، اتفاقيات جنيف المؤرخ 8 حزيران/ يونيو 1977.

سادساً: المراجع الأجنبية:

- Andreea bendovschi (2015): cyber -attacks - trends, patterns and security counter measures, Procedia economics and finance, Elsevier, Vol .28.
- Andrzej Kozlowski (2014): Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan, European Scientific Journal February, Special edition Vol.3 ISSN.
- Brent Kesler (2011): The vulnerability of Nuclear Facilities to Cyber Attack, Strategic Insight Journal, Vol 10, Issue 01.
- Cairtriona Heinl (2018): Cyber Dynamics and World Order: Enhancing International Cyber Stability, Irish Studies in International Affairs, Vol. 29.
- Danielle Flonk (2021): Emerging illiberal norms: Russia and China as promoters of internet content control, International Affairs Vol 97, No: 2.
- Gerard O'Regan (2016): Introduction to the History of Computing a Computing History Primer, Springer International Publishing, Switzerland.
- Heather Harrison Dinniss (2008): The status and use of computer network attacks in international law, PHD thesis, London school of a economics and Political science.
- Herbert Lin (2012): Cyber conflict and international humanitarian law International review of the red cross, Vol. 94, N886.
- Herbert Lin (2012): Cyber conflict and international humanitarian law, International Review of the red cross, Vol .94, No. 886.
- James Andrew Lewis (2022): Creating Accountability for Global Cyber Norms, Center for Strategic , and International Studies (CSIS), February 23.
- Janet (ABBATE.) (1999): Inventing The Internet, Published by the Mit Press Cambridge, London.
- Jeffrey Carr, Inside Cyber Warfare (2012): O'Reilly Media Inc, United States of America.
- Jeffrey T. G Kelsey (2008): Hacking in to international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare, Michigan law review, Vol. 106, No. 7.
- Junaidu Bello Marshall (2000), Cyber attacks (the legal response, International journal of international law), Vol. 1, No. 2, universal multidisciplinary research institute, India.
- Katie Chadd (2020), "The history of cybersecurity" Avast, Retrieved 20/11/2024. Edited.
- Michael N. Schmit (2013): (Tallinn manual on the international law applicable to cyber warfare), Cambridge university press, first publishes.
- Michael N. Schmitt & Jeffery S. Thumher, Autonomous weapon systems and the law of armed conflict, Harvard notional security journal.

- Paris Call (2018): Trust and Security in Cyberspace of 12 November, https://pariscall.international/en.
- Priyanka R. Dev (2015): (Use of Force and Armed Attack) Thresholds in Cyber Conflict; The Looming Definitional Gaps and the Growing Need for Formal U.N. Response), Texas International Law Journal Vol 50, Issue 2.
- Schmitt, M. N. (1999): (computer network attack and the use force in international law through on normative), the Colombia journal of transitional law, Vol. 27, No. 885.
- Tallinn manual 2.0 on the international law applicable to cyber operations (2017): Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press.
- Thomas W. Smith (2002): The New Law of War: Legitimizing Hi-Tech and Infrastructural, International Studies Quarterly, Vol. 46.
- Yan Xuetong (2020): Bipolar Rivalry in the Early Digital Age, The Chinese Journal of International Politics.
- Zaruka, Ismail. (2018): Cyberspace and the shift in the concepts of power and conflict, Journal of Legal and Political Sciences. Algeria, Vol. 10, No. 1, 1016 - 1031.

الهوامش:

(1) Cairtriona Heinl (2018): Cyber Dynamics and World Order: Enhancing International Cyber Stability, Irish Studies in International Affairs, Vol. 29, pp. 53-72.

(2) التلمسانى، مؤنس عبد اللطيف أحمد (2022): الأمن السيبرانى والتحليل السسيولوجى للمجتمع، دار البازورى العلمية، للنشر والتوزيع، ص 157، الحمامصة، إبراهيم، والعمارات، فارس محمد (2022): الأمن السيبرانى – المفهوم الحديث والمعاصر، ط1، دار الخليج للنشر والتوزيع، عمان، الأردن، ص 9.

(3) الحمامصة، إبراهيم، والعمارات، فارس محمد (2022)، المرجع السابق، ص 11.

(4) عبد الصادق، عادل (2020): الاقتصاد الرقمى – تحديات السيادة السيبرانية، المركز العربى لأبحاث الفضاء الإلكترونى، القاهرة، مصر، ص 16.

(5) المطيرى، خالد ظاهر عبد الله جابر السهيل (2022): دور التشريعات الجزائية فى حماية الأمن السيبرانى بدول مجلس التعاون الخليجى، مجلة البحوث الفقهية والقانونية، ع38، ص 921.

(6) ابن منظور، محمد بن مكرم (2000): لسان العرب، ط1، ج1، دار صادر، بيروت، لبنان، ص 163.

(7) عطية، شعبان عبد العاطى، وآخرون (2004): المعجم الوسيط، ط4، مكتب الشروق الدولية، مجمع اللغة العربية، مصر.

(8) الأشقر، منى جبور (2017): السيبرانية هاجس العصر، المركز العربى للبحوث القانونية والقضائية، بيروت، لبنان.

(9) الاتحاد الدولى للاتصالات (2007): دليل الأمن السيبرانى للبلدان النامية، الموجز التنفيذى للمعلومات.

(10) الأشقر، منى جبور (2012): الأمن السيبرانى: التحديات ومستلزمات المواجهة، المركز العربى للبحوث القانونية والقضائية، جامعة الدول العربية.

(11) الفتلاوى، أحمد عبيس نعمة (2016): الهجمات السيبرانية مفهومها والمسئولية الدولية الناشئة عنها فى ضوء التنظيم الدولى المعاصر، مجلة المحقق المحلى للعلوم القانونية والسياسية، مج8، ع4، كلية القانون، جامعة بابل، العراق.

(12) إبراهيم، يسرى خالد (2011): حرب المعلومات ماهيتها وأنواعها ومستوياتها، مجلة الباحث الإعلامى، مج3، ع13، كلية الإعلام، جامعة بغداد.

(13) عبد الصادق، عادل (2009): الإرهاب الإلكترونى، القوة فى العلاقات الدولية – نمط جديد وتحديات مختلفة، مركز الدراسات والسياسات الاستراتيجية، القاهرة، مصر.

(14) العلى، على زياد، وحميد، على حسين (2023): تكتيكات الحروب الحديثة "الأمن السيبرانى والحروب المعززة والهجينة"، دار العربى للنشر والتوزيع، القاهرة، مصر.

(15) الحمامصة، إبراهيم، والعمارات، فارس محمد (2022)، مرجع سابق.

(16) كلنتر، زهراء عماد محمد (2020): تكييف الهجمات السيبرانية فى ضوء القانون الدولى، مجلة الكوفة للعلوم القانونية والسياسية، مج1، ع1/44.

(17) دير، أمينة (2014): أثر التهديدات البيئية على واقع الأمن الإنسانى فى أفريقيا حالة دول القرن الأفريقى، مذكرة لنيل شهادة الماجستير فى العلوم السياسية والعلاقات الدولية، جامعة محمد خيضر بسكرة، ص 10.

(18) Zaruka, Ismail. (2018): Cyberspace and the shift in the concepts of power and conflict, Journal of Legal and Political Sciences. Algeria, Vol. 10, No. 1, 1016 - 1031.

(19) عطية، إدريس (2019): مكانة الأمن السيبرانى فى منظومة الأمن الوطنى الجزائرى، دراسة منشورة، جامعة العربى التبسى، الجزائر، ص 2.

(20) الزهرانى، عبد الله يحيى سعيد (2020): استراتيجيات الأمن السيبرانى فى ضوء التقنيات والتحديات الحديثة، دراسة مقارنة، رسالة ماجستير، فى العلوم الاستراتيجية، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية، قسم الدراسات الاستراتيجية، السعودية، ص 11.

(21) اللقانى، عبد الرحمن على (2022): دور الأمن السيبرانى فى تعزيز أمن المعلومات المالية الإلكترونية، دار البازورى العلمية، للنشر والتوزيع، ص 166.

(22) الهيئة الوطنية للأمن السيبرانى: (2018): الضوابط الأساسية للأمن السيبرانى، المملكة العربية السعودية، ص6 – 38.

(23) بوخضرة، إيناس (2022): الأحكام العامة لمفهوم الأمن السيبرانى، بحث منشور، كتاب جماعى دولى "التحكيم الدولى وتحديات الأمن السيبرانى"، المملكة المتحدة – بريطانيا، المركز المغاربى شرق أدنى للدراسات الاستراتيجية، ط1، ص 866 – 867.

(24) Janet (ABBATE.) (1999): Inventing The Internet, Published by the Mit Press Cambridge, London, p 8.

(25) الشوابكة، محمد أمين أحمد (2002): الجرائم المرتكبة عبر الإنترنت، رسالة لنيل درجة الماجستير فى القانون، معهد البحوث العربية للتربية والثقافة والعلوم، جامعة الدول العربية، القاهرة، ص 15.

(26) بوخضرة، إيناس (2022)، مرجع سابق، ص 868.

(27) Katie Chadd (2020), "The history of cybersecurity" Avast, Retrieved 20/11/2024. Edited.

(28) فرحان، علاء الدين (2021): من الردع النووى إلى الردع السيبرانى، دراسة لمدى تحقيق مبدأ الردع فى الفضاء السيبرانى، مجلة الفكر، مج16، ع1، جامعة بسكرة، الجزائر، ص 2246.

(29) المطيرى، خالد ظاهر عبد الله جابر السهيل (2022)، مرجع سابق، ص 1006.

(30) شفيق، نوران (2014): أثر التهديدات الإلكترونية على العلاقات الدولية، دراسة فى أبعاد الأمن الإلكترونى، المكتب العربى للمعارف، القاهرة، ص 40.

(31) أبو عامود، محمد سعد (2013): المفهوم العام للأمن المعلوماتى، جامعة حلوان، مصر، ص 7.

(32) عبد الصادق، عادل (2017): خطر الحروب السيبرانية عبر الفضاء الإلكترونى، مجلة الأهرام للكمبيوتر والإنترنت، والاتصالات، عدد مارس، ص 27.

(33) عثمان، أحمد زكى (2017): تأثير القدرات السيبرانية فى النزاعات الإقليمية، ملحق مجلس السياسة الدولية، اتجاهات نظرية، النزاع السيبرانى، مركز الأهرام للدراسات الاستراتيجية، ع208، القاهرة، ص 17.

(34) خليفة، إيهاب (2017): القوة الإلكترونية، العربى للنشر والتوزيع، ط1، القاهرة، ص 62.

(35) عفيفى، عبد الغفار (2018): استراتيجية الردع السيبرانى... التجربة الأمريكية، مجلة السياسة الدولية، مركز الأهرام للدراسات الاستراتيجية، ع213، القاهرة، ص 196.

(36) عبد الصبور عبد الحى، سماح (2017): النزاع السيبرانى – طبيعة المفهوم وملامح الفاعلين، مجلة السياسة الدولية، ملحق اتجاهات نظرية، النزاع السيبرانى، التنازع العالمى على قوة الفضاء الإلكترونى، ع208، مركز الأهرام للدراسات الاستراتيجية، ص 7 - 10.

(37) Andreea bendovschi (2015): cyber -attacks - trends, patterns and security counter measures, Procedia economics and finance, Elsevier, Vol .28, p. 3.

(38) الفتلاوى، أحمد عبيس نعمة، مرجع سابق، 614.

(39) Junaidu Bello Marshall (2000), Cyber attacks (the legal response, International journal of international law), Vol. 1, No. 2, universal multidisciplinary research institute, India, p. 3.

(40) Michael N. Schmit (2013): (Tallinn manual on the international law applicable to cyber warfare), Cambridge university press, first publishes, p. 92.

(41) Schmitt, M. N. (1999): (computer network attack and the use force in international law through on normative), the Colombia journal of transitional law, Vol. 27, No. 885, p. 07.

(42) Heather Harrison Dinniss (2008): The status and use of computer network attacks in international law, PHD thesis, London school of a economics and Political science, p. 33.

(43) Jeffrey T. G Kelsey (2008): Hacking in to international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare, Michigan law review, Vol. 106, No.7 , p. 1437.

(44) Herbert Lin (2012): Cyber conflict and international humanitarian law International review of the red cross, Vol. 94, N886, p. 515.

(45) سمودى، رزق أحمد (2018): حق الدفاع عن النفس نتيجة الهجمات الإلكترونية، ص 338.

(46) شميت، مايكل (2012): الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر، ص915.

(47) عبد الصادق، عادل (2016): أسلحة الفضاء الألكتروني في ضوء القانون الدولي الإنساني، مكتبة المستقبلية، مصر، ص96.

(48) السيد محمد السيد احمد،القانون في الفضاء السيبراني، المنصة القانونية مقال منشور في 7/ 6/ 2022، متاح على الرابط: http://www.sajplus.com

(49) James Andrew Lewis (2022): Creating Accountability for Global Cyber Norms, Center for Strategic and International , Studies (CSIS), February 23, p. 1-5.

(50) James Andrew Lewis, Creating Accountability for Global Cyber Norms,Op.Cit,p5-8.

(51) محكمة العدل الدولية، مشروعية التهديد بالأسلحة النووية أو استخدامها، فتوى،8 تموز/ يوليو ،1996 الفقرة86.

(52) المادة (1، 2) من البروتوكول الإضافي الأول، اتفاقيات جنيف المؤرخ 8 حزيران/ يونيو 1977؛ الفقرة 9 من ديباجة اتفاقية الهاي الثانية لعام 1899؛ والفقرة 8 من ديباجة اتفاقية لاهاي الرابعة لعام 1907.

(53) Gerard O'Regan (2016): Introduction to the History of Computing a Computing History Primer, Springer International Publishing, Switzerland, p. 163.

(54) Jeffrey Carr, Inside Cyber Warfare (2012): O'Reilly Media Inc, United States of America, p. 2.

(55) قرار الجمعية العامة لألمم المتحدة في 4 كانون الثاني 1999، وثائق الامم المتحدة، الوثيقة (A/RES/53/70).

(56) مذكرة الامين العام للامم المتحدة في 5 اب 2005، وثائق الامم المتحدة، الوثيقة(A/60/202) .

(57) Andrzej Kozlowski (2014): Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan, European Scientific Journal February, Special edition Vol.3 ISSN, pp. 238, 239.

(58) الهجمات السيبرانية وحالات التعاون ضدها، الأمم المتحدة، متاح على الرابط:

https://news.un.org/en/story/2007/09/232832-estonia-urges-un-member-states cooperate-against-cyber-crimes

[59] قرار الجمعية العامة للأمم المتحدة في 6 كانون الثاني2006، وثائق الامم المتحدة، الوثيقة (A/RES/60/45).

(60) قرار الجمعية العامة للأمم المتحدة في 13 كانون الاول، 2011 وثائق الامم المتحدة، الوثيقة (A/RES/66/24).

(61) مذكرة الامين العام للأمم المتحدة، في30 تموز ،2010 وثائق الامم المتحدة، الوثيقة (A/65/201).

(62) الفقرة (٤) من قرار الجمعية العامة للأمم المتحدة في 6 كانون الثاني، 2014 وثائق الامم المتحدة، الوثيقة (A/RES/68/243).

[63] مذكرة الامين العام للأمم المتحدة في 22 تموز ،2015 وثائق الامم المتحدة، الوثيقة(A/70/174).

(64) قرار الجمعية العامة للأمم المتحدة في 30 كانون الثاني2015 ،وثائق الامم المتحدة، الوثيقة (A/RES/70/237).

(65) الفقرة (5) من تقرير الأمين العام للأمم المتحدة في 14 اب2017 ،وثائق الامم المتحدة، الوثيقة (A/72/327).

(66) الفقرة (3)من قرار الجمعية العامة للأمم المتحدة في 2 كانون الثاني2019 وثائق الامم المتحدة، الوثيقة (A/RES/73/266).

[67] تقرير الخبراء المذكور في مذكرة الأمين العام للأمم المتحدة في 14 تموز ، 2021وثائق الامم المتحدة، الوثيقة (A/76/135).

(68) Tallinn manual 2.0 on the international law applicable to cyber operations (2017): Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, p.3.

(69) Paris Call (2018): Trust and Security in Cyberspace of 12 November, https://pariscall.international/en/.

(70) Danielle Flonk (2021): Emerging illiberal norms: Russia and China as promoters of internet content control, International Affairs Vol 97, No: 2, p. 1931.

[71] دروغيه، كوردولا (2023): ما من فراغ قانوني في الفضاء السيبراني، اللجنة الدولية للصليب الأحمر، مقابلة تم الاطلاع عليها في 2024/11/26، على الرابط: https://www.icrc.org/ar/doc/resources/documents/interview/

(72) Yan Xuetong (2020): Bipolar Rivalry in the Early Digital Age, The Chinese Journal of International Politics, p.313.

(73) Thomas W. Smith (2002): The New Law of War: Legitimizing Hi-Tech and Infrastructural, International Studies Quarterly, Vol. 46, p. 366.

(74) Brent Kesler (2011): The vulnerability of Nuclear Facilities to Cyber Attack, Strategic Insight Journal, Vol 10, Issue 01. p. 19.

(75) Herbert Lin (2012): Cyber conflict and international humanitarian law, International Review of the red cross, Vol .94, No. 886, p. 515.

(76) Michael N. Schmitt & Jeffery S. Thumher, Autonomous weapon systems and the law of armed conflict, Harvard notional security journal, P. 232.

(77) The Potential Human Cost of Cyber Operations (2019): https://www. icrc. org/en/download/file/96008/the-potential-human-cost-of-cyber-operations.pdf

[78] المادة (36) من الملحق (البروتوكول) الأول الإضافي لاتفاقيات جنيف.

[79] اللجنة الدولية (2015): القانون الدولي الانساني وتحديات النزاعات المسلحة المعاصرة، ص 42.

(80) . Priyanka R. Dev (2015): (Use of Force and Armed Attack) Thresholds in Cyber Conflict; The Looming Definitional Gaps and the Growing Need for Formal U.N. Response), Texas International Law Journal Vol 50, Issue 2, p. 380.

[81] هنكرتس، ودوزوالد -بك (2005): القانون الدولي الانساني العرفي، مج1، قواعد اللجنة الدولية، مطبعة جامعة كامبريدج، ص23-44.