مهددات الامن السيبراني واثرها على سيادة الدول (نماذج مختارة)

سجى ياسين خضير
كلية العلوم السياسية / جامعة بغداد
Sajaalyassen32@gmail.com

أ.د.هشام عز الدين مجيد
كلية العلوم السياسية / جامعة بغداد
Hesham14@copolicy.uobaghdad.edu.iq

الكلمات المفتاحية: الامن السيبراني ، مهددات الامن السيبراني ، مبدأ السيادة .

كيفية اقتباس البحث

خضير، سجى ياس، هشام عز الدين مجيد ، مهددات الامن السيبراني واثرها على سيادة الدول (نماذج مختارة) ،مجلة مركز بابل للدراسات الانسانية، آب ٢٠٢٦، المجلد:١٦ ،العدد:٨ .

مفهرسة في Indexed
IASJ

مسجلة في Registered
ROAD

Cybersecurity threats and their impact on state sovereignty (selected examples)

Saja Yassin Khodair
College of Political Science / University of Baghdad

Husham Ezzulddin Majeed
College of Political Science / University of Baghdad

Keywords : Cybersecurity, Cybersecurity threats, Sovereignty principle.

How To Cite This Article
Khodair, Saja Yassin , Husham Ezzulddin Majeed, Cybersecurity threats and their impact on state sovereignty (selected examples),Journal Of Babylon Center For Humanities Studies, August 2026,Volume:16, Issue 8.

Abstract

Cyberspace has become the fifth battleground between international powers, after land, sea, air, and outer space. This advanced technological field is a new arena for global conflicts, as cyberattacks targeting information infrastructure have become one of the most dangerous tools used in modern warfare. Such attacks can lead to the complete economic collapse of a country or cause catastrophic damage extending to all sectors, whether military or civilian. This danger is compounded by the increasing global reliance on technology and digital systems in all aspects of daily and strategic life. The individual nature of cyberspace as a virtual dimension is not subject to the direct autonomy of states makes it an ideal environment for hostile acts. While states can impose control over their land, airspace, or territorial waters, they cannot as easily assert their autonomy over cyberspace. This shared space depends on the technology used by individuals, institutions, companies, and governments, making it vulnerable to exploitation by cyber attackers. The study posits that cybersecurity challenges stemming from escalating

cyber threats pose a growing risk to national sovereignty. It also suggests that achieving cybersecurity depends on international and global efforts to combat these threats, the modernization of national and international legislation, and the development of robust cyber infrastructure and advanced technological capabilities capable of addressing these challenges.

الملخص

لقد تحول الفضاء السيبراني إلى ساحة المعركة الخامسة بين القوى الدولية وذلك بعد البر والبحر والجو والفضاء الخارجي، ويعد هذا المجال التكنولوجي المتطور ساحة جديدة للصراعات العالمية، اذ أصبحت الهجمات السيبرانية التي تستهدف البنية التحتية المعلوماتية إحدى أخطر الأدوات المستخدمة في الحروب الحديثة فمثل هذه الهجمات قد تؤدي إلى انهيار اقتصادي كامل لدولة من الدول أو التسبب في أضرار كارثية تمتد إلى كافة القطاعات سواء كانت عسكرية أو مدنية، ان هذا الخطر يتضاعف مع ازدياد الاعتماد العالمي على التكنولوجيا والأنظمة الرقمية في كافة جوانب الحياة اليومية والإستراتيجية، إن الطبيعة الفردية للفضاء السيبراني بوصفه بعدا" افتراضيا" لا يخضع للسيادة المباشرة للدول تجعله بيئة مثالية للاعمال العدائية، فبينما يمكن للدول فرض سيطرتها على أراضيها أو أجوائها أو مياهها الإقليمية فإنها لا تستطيع بنفس السهولة فرض سيادتها على الفضاء السيبراني، هذا الفضاء المشترك بين الجميع يعتمد على التكنولوجيا التي يستخدمها الأفراد والمؤسسات والشركات والحكومات، مما يجعله عرضة للاستغلال من قبل المهاجمين السيبرانيين . تفترض الدراسة أن التحديات الأمنية في الفضاء السيبراني الناتجة عن التهديدات السيبرانية المتزايدة تمثل خطرا" متناميا على سيادة الدولة ، كما ترجح ان تحقيق الامن السيبراني يعتمد على جهود دولية واممية لمكافحة التهديدات، وتحديث التشريعات الوطنية والدولية، بالإضافة إلى بناء بنية تحتية سيبرانية قوية وقدرات تقنية متقدمة قادرة على مواجهة هذه التحديات

المقدمة

يعد التطور التكنلوجي وخاصة في مجال الفضاء السيبراني من اهم ثورات القرن الحادي و العشرين ، ومع هذا التطور اصبح الانترنيت والحاسوب والهواتف الذكية جزء لا يتجزأ من حياتنا ، مع ذلك اصبحت كل وسائل الحياة الخاصة و العامة و المرتبطة بالانترنيت معرضة للهجمات السيبرانية لاغراض الحاق الضرر او كسب المال بطرق سهلة ، وقد استخدم الحاسوب الالي كأداة لارتكاب الجرائم الغير مشروعة ، وقد اتت الهجمات السيبرانية بتحديات جديدة غير موجودة في القانون الدولي الانساني .

كما قد اسهم هذا التطور في خرق سيادة الدولة واصبحت بيانات ومعلومات الدولة قابلة للاختراق ، لان قدرة كل دولة لم تعد مؤكدة في الحفاظ على اتصالاتها وقياداتها وسيطرتها وقدرتها الحاسوبية ضد التهديدات الجديدة من الهجمات السيبرانية التي تواجهة العالم باكملة .

١-**مشكلة الدراسة** : وجود جرائم الكترونية داخلية وهجمات سيبرانية خارجية تؤثر على سيادة الدول ، يجب على الدول ايجاد السبل و الاجراءات التي يجب ان تتخذ من اجل حماية السيادة من التهديدات السيبرانية المتزايدة التي تستهدف البنية الرقمية للدول و المؤسسات .

٢-**فرضية الدراسة** : تفترض الدراسة أن التحديات الأمنية في الفضاء السيبراني الناتجة عن التهديدات السيبرانية المتزايدة تمثل خطرا" متناميا على سيادة الدولة ، كما ترجح ان تحقيق الامن السيبراني يعتمد على جهود دولية واممية لمكافحة التهديدات، وتحديث التشريعات الوطنية والدولية، بالإضافة إلى بناء بنية تحتية سيبرانية قوية وقدرات تقنية متقدمة قادرة على مواجهة هذه التحديات .

٣-**اهداف الدراسة** : معرفة اثر التهديدات السيبرانية على الحدود السياسية للدولة من خلال التاثير على البنية الرقمية الحيوية ، وبالتالي التاثير على السيادة الوطنية للدولة .

٤-**منهجية البحث** : استخدم الباحث منهج التحليل الوصفي وذلك من خلال اعطاء تحليل وصفي عن الموضوع واهميته وتاثيره على السيادة .

مهددات الامن السيبراني واثرها على سيادة الدول (نماذج مختارة)

نتناول في هذه الدراسة التهديدات الماسة بأمن الدولة السيبراني والتي يمكن حصرها بالرغم من تعدد انواعها واختلاف اثارها في نوعين اساسيين وبالشكل التالي :

المطلب الاول : مهددات الامن السيبراني الداخلية

يشهد المجتمع اليوم تطوراً متسارعاً لتكنولوجيا المعلومات والاتصالات، كما يشهد تزايداً وتنوعاً في التطبيقات والخدمات الإلكترونية التي تعتمد أساساً على الفضاء السيبراني، إلا أن الانفتاح الذي يميز الإنترنت و الفضاء السيبراني عموما جعله عرضت للتعديات والانتهاكات والأنشطة الإجرامية والتعدي على حقوق الناس، وجعل من مستخدمي الفضاء السيبراني عرضة للانتهاكات من قبل المجرمين و مخترقي الشبكات، مما يؤثر سلبا على جميع المستخدمين من أفراد و شركات مؤسسات حكومية ومنظمات . [١]

وعليه سوف نتناول في هذا المطلب بالدراسة مفهوم الجريمة السيبرانية وخصائصها التي تفرق بها عن غيرها من الجرائم الاخرى ، ثم نعرض لأبرز صور هذه الجريمة ، وعلى النحو الاتي :

اولا" : مفهوم الجريمة السيبرانية وخصائصها

تعد الجرائم السيبرانية من الجرائم المستحدثة و التي تتطور بشكل مستمر بتطور تكنولوجيا المعلومات و الاتصالات و عليه سنعالج هنا مفهوم الجريمة السيبرانية فيما يلي : [٢]

تعددت التعاريف للجريمة السيبرانية وجاءت حسب اتجاهات ووجهات نظر مختلفة و ذلك راجع لحداثة المفهوم عالميا، فمن التعريفات ما يركز على استخدام الحاسب كوسيلة و أداة للجريمة و منها ما يركز على موضوع الجريمة أي أنها تقع على مكونات الحاسب كالبيانات و البرامج، و منها ما يشترط أن يكون للمجرم معرفة فنية تمكنه من فعل الجريمة، ومنها ما جمع في التعريف بين الوسيلة و الموضوع . [٣]

حيث عرفها الفقيه الألماني "تاديمان: " هي كل أشكال السلوك غير المشروع أو الضار بالمجتمع و الذي يرتكب باستخدام الحاسب الآلي[٤]" ، كما يعرفها الخبير القانوني "جون فورستر" بأنها: "كل فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية .[٥]

ثانيا" : خصائص الجرائم السيبرانية

تتميز الجريمة السيبرانية بمجموعة من الخصائص التي تميزها عن الجرائم المنظمة الاخرى وندرج هذه الخصائص بالشكل التالي : [٦]

١-**ان الجريمة السيبرانية ترتكب عبر شبكة الإنترنت** : فهذه الشبكة هي حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم كالبنوك والشركات الصناعية وغيرها من الأهداف التي غالبا ما تكون الضحية لتلك الجرائم وهو ما دعا معظم تلك الأهداف إلى اللجوء إلى نظم الأمن والحماية الإلكترونية في محاولة منها لحماية نفسها أو على الأقل لتحد من خسائرها عند وقوعها ضحية لتلك الجرائم . [٧]

٢-**الجريمة السيبرانية عابرة للحدود الوطنية:** أن هذا النوع من الجرائم لا يعتد بالحدود الجغرافية للدول ولا بين القارات، فمع انتشار شبكة الاتصالات بين دول العالم وأقاليمه، امكن ربط أعداد لا حصر لها من أجهزة الكمبيوتر عبر مختلف دول العالم بهذه الشبكة، حيث يمكن أن يكون الجاني في بلد والمجنى عليه في بلد آخر .

٣-**صعوبة اكتشاف وأثبات الجرائم السيبرانية** :ان الجريمة السيبرانية لا تترك اثارا ملموسة ولا تترك شهود يمكن الاستدلال بأقوالهم او ادلة مادية يمكن فحصها كونها تحدث في بيئة افتراضية يتم فيها نقل المعلومات وتناولها بواسطة نبضات الكترونية غير مرئية او بإدخال رموز وأرقام وتوظيف تقنيات معقدة يصعب اكتشافها ثباتها من قبل

خبير او محقق تقليدي كونها تتطلب المام خاص بتقنيات الحاسوب ونظم المعلومات المتطورة، .[٨]

٤-**جريمة مكلفة للضحايا** : يحمل إنتشار الجريمة السيبرانية في طياته تكاليف و خسائر مالية كبير ة سواء أكان ذلك بصفة مباشرة أو غير مباشرة، وتتجسد التكاليف المباشرة وغير المباشرة في الأموال المسحوبة من حسابات الضحية، أو الوقت والجهد المستغرق لإصالح نظم الحاسوب. [٩]

٥-**أسلوب ارتكاب الجريمة السيبرانية:** تبرز ذاتية الجرائم السيبرانية بصورة أكثر وضوحا في أسلوب وطريقة ارتكابها [١٠] ، فإذا كانت الجرائم التقليدية تتطلب نوعا من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة القتل أو الاختطاف، أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو الحال في جريمة السرقة والتجسس أو اختراق خصوصيات الغير أو التغرير بالقاصرين .. الخ. [١١]

ثالثا": صور الجرائم السيبرانية

ان صور الجرائم السيبرانية والتي تكون الحواسيب او الاجهزة الذكية هدفا لها او وسيلة في ارتكابها تمثل اهم السلوكيات التي تتهدد الأمن السيبراني والتي يلجأ المشرع الى حظرها لما لها من مساس كبير بمصالح الدولة والافراد على حد سواء، فأنى كانت تلك الصور و كيف ما تم ارتكابها فإنها تنعكس بشكل سلبي على الانشطة السيبرانية في الدولة . [١٢]

وتشمل الجريمة السيبرانية عدد واسعة من الجرائم المرتكبة بدافع مالي والجرائم المتصلة بالمحتوي الحاسوبي[١٣] ، فضلا عن الأعمال التي تمس بسرية النظم الحاسوبية وسالمتها وقابلية النفاذ إليها، و فيما يلي مجموعة من الجرائم السيبرانية و التي تم إعدادها من قبل الأمم المتحدة اللجنة الإقتصادية و الإجتماعية لغربي آسيا "الإسكوا : [١٤] " unescwa

١-**جرائم التعدي على البيانات المعلوماتية وتشمل كل من:** جرم التعرض (تعديل أو إلغاء أو محو أو إفساد أو تدمير للبيانات المعلوماتية (، جرم اعتراض بيانات معلوماتية.

٢-**جرائم التعدي على الأموال والمعاملات و تشمل كل من:** جرم الاحتيال أو الغش بوسيلة معلوماتية ، جرم التزوير المعلوماتي – جرم الاختلاس أو سرقة أموال بوسيلة معلوماتية – جرم الاطلاع على معلومات سرية أو حساسة أو إفشائها . [١٥]

٣-**جرائم الاستغلال الجنسي للقاصرين و تشمل كل من:** جرم إنتاج مواد إباحية لقاصرين بقصد بثها بواسطة نظام معلوماتي – جرم توزيع أو بث أو نقل مواد إباحية لقاصرين بواسطة نظام

معلوماتي – جرم حيازة مواد إباحية لقاصرين على وسيطة إلكترونية أو نظام معلوماتي معلوماتية – جرم التحرش الجنسي بالقاصرين بوسيلة معلوماتية .[١٦]

٤-**جرائم التعدي على الملكية الفكرية للأعمال الرقمية و تشمل كل من :** جرم وضع اسم مختلس على عمل – جرم تقليد عمل رقمي أو قرصنة البرمجيات.

٥-**جرائم البطاقات المصرفية والنقود الإلكترونية و تشمل كل من:** جرم تقليد بطاقة مصرفية– جرم استعمال بطاقة مصرفية مقلدة – جرم تزوير النقود الإلكترونية.

٦- **الجرائم التي تمس المعلومات الشخصية و تشمل كل من:** جرم معالجة معلومات ذات طابع شخصي دون حيازة تصريح أو ترخيص –جرم معالجة معلومات ذات طابع شخصي دون احترام القواعد القانونية. – جرم إفشاء معلومات ذات طابع شخصي .

٧-**جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية و تشمل كل من:** تشمل الجرائم المرتكبة عبر الوسائل الإلكترونية عددًا من الأفعال التي تمس حقوق الإنسان والأمن المجتمعي، ومن أبرزها: نشر أو تداول المواد ذات الطابع العنصري باستخدام وسائل تقنية المعلومات، أو تهديد الأشخاص والاعتداء عليهم بسبب انتمائهم العرقي أو الديني أو المذهبي أو بسبب لونهم من خلال الوسائط الإلكترونية. كما تمتد هذه الجرائم إلى نشر أو توزيع محتوى إلكتروني يتضمن إنكار جرائم الإبادة الجماعية أو تحريفها أو تبريرها، فضلًا عن إنكار الجرائم المرتكبة ضد الإنسانية أو التقليل من خطورتها. ويُعد كذلك من الجرائم السيبرانية كل فعل يتمثل في المساعدة أو التحريض، عبر الوسائل الإلكترونية، على ارتكاب جرائم ضد الإنسانية أو التشجيع عليها بأي صورة كانت. . [١٧]

٨-**جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية و تشمل كل من:** جرم تملك وادارة مشروع مقامرة على الأنترنت – جرم تسهيل وتشجيع مشروع مقامرة على الأنترنت – جرم ترويج المواد المخدرة على الأنترنت .

٩-**جرائم المعلوماتية ضد الدولة والسلامة العامة و تشمل كل من:** جرم تعطيل الأعمال الحكومية بوسيلة معلوماتية – جرم الإخفاق في الإبلاغ أو الإبلاغ الخاطئ عن جرائم المعلوماتية – جرم الحصول بوسيلة معلوماتية على معلومات سرية تخص الدولة – جرم العبث بالأدلة القضائية المعلوماتية[١٨] .)

رابعا" : الاليات التشريعية لمكافحة الجرائم السيبرانية

ان مسألة تحقيق الامن السيبراني لازالت تثير اشكالات قانونية ، خاصة مع تزايد التهديدات الامنية الالكترونية التي اضحت تشكل تهديد خطير سواء على الدول او الافراد [١٩] ، لذلك كان

لابد من صياغة نصوص قانونية جديدة لتحكم مفاهيم جديدة غير ملموسة مثل البيانات والانظمة المعلوماتية [٢٠] ، اذ يصعب تحديد صاحب او حائز المعلومة، ولاسيما على صعيد التجريم والاختصاص القضائي واجراءات التحقيق والادلة المعلوماتية ، لذلك لا بد من وجود بنية تشريعية تعني بوجود هيكل تشريعي يحدد ويعرف الجرائم الالكترونية ويضع العقوبات اللازمة على مرتكبيها بهدف الحفاظ على نظم الدولة الالكترونية وتحقيق الامن السيبراني للأفراد ، كما تحرص الاليات التشريعية على استخدام الفضاء السيبراني لتحقيق اهداف الدولة الاستراتيجية[٢١] . وعليه سوف نتناول مجموعة من النماذج التطبيقية لدول اجنبية وعربية وبالشكل الاتي : [٢٢]

١-الولايات المتحدة الامريكية

هنالك جملة من التشريعات المعنية بالتعاطي مع التهديدات السيبرانية في الولايات المتحدة، والتي تسعى من بين ما تسعى اليه الى مكافحة الجرائم السيبرانية، ونعرض لأبرز تلك التشريعات في الاتي:

١-ان أول قانون إلكتروني في الولايات المتحدة الامريكية ، ويطلق عليه قانون الاحتيال وإساءة استخدام الكمبيوتر، والذي أصدر في عام ١٩٨٦، هدف هذا القانون الى حظر الوصول غير المصرح به إلى أجهزة الكمبيوتر والاستخدام غير القانوني للمعلومات الرقمية . [٢٣]

٢-قانون حماية الاتصالات الإلكترونية لعام ١٩٨٦ (Electronic The Act) (ECPA Protection Communications ،(و يحمي هذا القانون بصبغته المعدلة الاتصالات السلكية والإلكترونية أثناء إجراء تلك الاتصالات وأثناء نقلها وعند تخزينها على أجهزة الحاسوب، وينطبق القانون حيث جرم على البريد الإلكتروني والمحادثات الهاتفية والبيانات المخزنة إلكترونيا . [٢٤]

٢- الدول الاوربية

جعلت فرنسا الامن السيبراني من اولوياتها ، ففي عام ١٩٧٨ صدر قانون حماية البيانات النافذة الذي ينظم حرية ابداع الاشخاص ، واليوم تخضع الممارسات الرقمية في فرنسا لنظام قانوني ينص على عقوبات تصل الى السجن لدة خمس سنوات وغرامه تصل الى ٧٥٠٠٠ يورو على هجمات الكمبيوتر ، كما ينص القانون على زيادة العقوبات على الهجمات الالكترونية التي تستهدف الدولة بشكل مباشر ، وفي عام ٢٠٠٩، تم انشاء وكالة امن نظم معلومات وطنية (نافذه جديدة) للدفاع عن انظمة المعلومات و المستخدمين الرقمين وحمايتهم من الهجمات الالكترونية ، وكذلك فأن عودة التهديد الارهابي في عام ٢٠١٥ دفعت نحو تكثيف الجهود في هذا المجال وقد حددت الاستراتيجية الوطنية للامن الرقمي خمسة اهداف : [٢٥]

١-ضمان السيادة الوطنية

٢-الرد على الاعمال الخبيثة السيبراني

٣-اعلام الجمهور العام

٤-جعل الامن الرقمي ميزه تنافسية للشركات

٥-تقوية صوت فرنسا

اما سويسرا فقد اعتمدت القانون الفدرالي بشأن حماية البيانات في ١٩ يونيو ١٩٩٢ وحماية البيانات يضمنها اولا وقبل كل شيء الدستور الاتحادي المنقح الذي دخل حيز السريان عام ٢٠٢٢ [٢٦] ، اما المانيا فقد كان اول قانون قد اصدر بشأن حماية المعلومات عام ١٩٧٧ وتم تحديثه فيما بعد على وفق الحاجة و التطور التكنلوجي ، وفي بلجيكا كان اول قانون عام ١٩٩٢ ، اما كندا كان اول قانون للحماية الشخصية وحماية الوثائق الالكترونية عام ١٩٨٢. [٢٧]

٣-اليابان :

فيما يتعلق بالجرائم السيبرانية فان القوانين الاساسية المتعلقة بمكافحتها تتمثل في قانون العقوبات الياباني رقم (٤٥) لسنة ١٩٩٧ المعدل ، وقانون حظر الوصول غير المصرح به إلى الحاسوب رقم (١٢٨) لسنة ١٩٩٩ المعدل. [٢٨]

٤-جمهورية مصر العربية

اهتم المشرع المصري مبكرًا بوضع إطار قانوني ينظم الجرائم المرتبطة باستخدام تكنولوجيا المعلومات ويحمي الحقوق المرتبطة بها، وذلك من خلال تضمين عدد من التشريعات أحكامًا تتعلق بالخصوصية والحقوق الرقمية. فقد تضمن قانون الأحوال المدنية رقم (١٤٣) لسنة ١٩٩٤ نصوصًا تهدف إلى حماية البيانات الشخصية وصون الحق في الخصوصية، كما تناول قانون حماية حقوق الملكية الفكرية لسنة ٢٠٠٢ الجوانب القانونية المتعلقة بحماية المصنفات الفكرية في البيئة الرقمية. وفي عام ٢٠٠٨، استحدث المشرع المصري أحكامًا قانونية لمكافحة جرائم الاستغلال الجنسي للأطفال عبر شبكة الإنترنت، في إطار تعزيز الحماية الجنائية للفئات الأكثر عرضة للانتهاك.

وعلى الصعيد الدستوري، أولى دستور جمهورية مصر العربية لعام ٢٠١٤ اهتمامًا خاصًا بأمن الفضاء المعلوماتي، إذ نص في المادة (٣١) على أن: «أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون». ويعكس هذا النص إدراك المشرع الدستوري للأهمية المتزايدة للأمن السيبراني، واعتباره أحد المرتكزات الأساسية لحماية المصالح الاقتصادية والأمنية للدولة في ظل

التطور المتسارع لتقنيات المعلومات والاتصالات. [٢٩] . واختُتم الإطار التشريعي المصري في هذا المجال بإصدار قانون مكافحة جرائم تقنية المعلومات عام ٢٠١٨، الذي مثّل نقلة نوعية في تنظيم الجرائم المرتبطة بالفضاء الإلكتروني، إذ وضع قواعد قانونية لمواجهة الاعتداءات التي تستهدف أنظمة المعلومات والشبكات الإلكترونية، وحدد المسؤوليات والعقوبات المترتبة على مرتكبيها، بما يسهم في تعزيز الأمن السيبراني وحماية البنية التحتية الرقمية للدولة.

وعلى الصعيد التنفيذي، أولت وزارة الاتصالات وتكنولوجيا المعلومات اهتمامًا متزايدًا بقضايا الأمن السيبراني، حيث أدرجت ضمن استراتيجيتها للفترة (٢٠١٢–٢٠١٧) محورًا خاصًا بأمن المعاملات الإلكترونية والشبكات المعلوماتية. وركزت هذه الاستراتيجية على تطوير منظومات أمن الشبكات، ورفع مستوى الحماية للقطاع المصرفي وأنظمة الدفع الإلكتروني، إلى جانب تعزيز إجراءات حماية الخصوصية، وتأمين خدمات الإنترنت، بما يضمن توفير بيئة رقمية أكثر أمنًا وموثوقية لمختلف المستخدمين .

٥- الجمهورية التونسية

في تونس كان اول قانون للجرائم المعلوماتية عام ١٩٩٩، والقانون المتعلق بدعم الجهود الدولية في مكافحة الارهاب ومنع غسل الاموال عام ٢٠٠٢ ، كما اصدرت تونس مجموعة من التشريعات المتعلقة مباشر او غير مباشر بالأمن السيبراني وهو القانون رقم (٥) لسنة ٢٠٠٤ [٣٠] ، المتعلق بتنظيم مجالات السلامة المعلوماتية وضبط القواعد العامة لحماية النظم المعلوماتية والشبكات ، وكذلك القانون التوجيهي حول الاقتصاد الرقمي عام ٢٠٠٧ . [٣١]

٦-**جمهورية الجزائر** صدر في الجزائر بعض التشريعات الدستورية القانونية المتعلقة بمكافحة الجرائم الالكترونية ومن بين هذه القوانين رقم (٤٠-١ (5عالج قانون العقوبات الجزائري الجرائم الالكترونية من خلال المواد (٣٩٤ مكرر) الى غاية (٣٩٤ مكرر٧) [٣٢] ، وتصل هذه العقوبات الى حد الغرامة المالية والحبس، وكذلك القانون رقم (٤٠- ٩٠) المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصالات ومكافحتها ، وكذلك المرسوم الرئاسي (261 -15) المتعلق بتشكيل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها. [٣٣]

٧-المملكة المغربية

لم يصدر عن المشرع المغربي قانون خاص ينظم احكام الجرائم السيبرانية بشكل مستقل ، وانما اتجه المشرع المغربي الى تعديل مجموعة القانون الجنائي بإضافة الفصل العاشر اليها والذي نظم بعض صور الجرائم السيبرانية وذلك في العام

٢٠٠٣ [٣٤] ، وعند اصداره لقانون الأمن السيبراني في العام ٢٠٢٠ نص على بعض العقوبات التي تتعلق بمخالفة احكامه مما يجعلها ناظمة لبعض صور الجرائم السيبرانية [٣٥] .

٨-الامارات العربية المتحدة

اصدرت الامارات قانون جرائم تقنية المعلومات في عام ٢٠٠٦ ، كما اوصى مجلس التعاون الخليجي في مؤتمر انعقد في يونيو ٢٠٠٧ بوضع اتفاقية حول الجرائم السيبرانية تجمع بين اعضائه ، وفيما بعد صدر القانون الاتحادي رقم (5) لسنة ٢٠١٢ المعدل بالقانون الاتحادي رقم (١٢) لسنة ٢٠٠٦ تقنية المعلومات الحديثة وهذا القانون هو القانون الاول في العالم العربي الذي يعني بالجرائم المعلوماتية ، ولقد نص هذا القانون على تجريم الافعال التالية : [٣٦]

١.اختراق المواقع و الانظمة الالكترونية .

٢.تزوير مستندات معترف بها في نظام معلوماتي .

٣.التعطيل او العبث .

٤.التنصت و التهديد

٥.السرقة و الاحتيال

٦.المساس بالآداب العامة والتحريض عليها والمساس الاديان وانتهاك حرمة الحياة الخاصة والاتجار بالبشر او المخدرات وغسل الاموال والافعال الإرهابية و الحصول على معلومات . [٣٧] حكومية او التحريض على ارتكاب أي جريمة من هذا القانون ، او التحريض على ارتكاب أي جريمة من هذا القانون ، واخيرا" قانون مكافحة الشائعات و الجرائم الالكترونية في عام ٢٠٢٢ . [٣٨]

٩-المملكة العربية السعودية

اصدرت المملكة العربية السعودية بتاريخ ٢٠٠٨/١/٢٤ ،نظامها الخاص بمكافحة الجرائم الالكترونية ، وقد نص هذا القانون بتجريم الافعال التي اصبحت مجرمة في نظره ، وان كان صدور هذا القانون قد جاء متأخر نوعا" ما مقارنة بالأمارات،الا انه يعتبر ضمن القوانين العربية الفعالة في مكافحة الفضاء السيبراني.[٣٩]

المطلب الثاني : مهددات الامن السيبراني الخارجية

تتجلى مهددات أمن الدولة السيبراني على المستوى الخارجي بتلك الهجمات التي يتعرض لها فضاؤها السيبراني من قبل جهات خارجية كأن تكون دولاً أو منظمات أو وكلاء لأي منهما وبما ينعكس سلباً على أمنها السيبراني، وتالياً الخدمات والانشطة التي تقدم في داخل الدولة . [٤٠]

واستناداً على ذلك فان الهجمات السيبرانية تعد من أكبر المهددات التي تستهدف الأمن السيبراني، مما يستوجب التصدي لها بشتى الطرق الممكنة، ونتناول في هذا المطلب بيان مفهوم الهجمات السيبرانية، وخصائصها ، كما ونعرض لأبرز أنواعها والجهود الدولية والأممية في تحقيق الآمن السيبراني، وعلى النحو الآتي:

اولا" : مفهوم الهجمات السيبرانية وخصائصها

١-مفهوم الهجمات السيبرانية

بالرغم مما يدور في هذا المجال إلا أنه لا يوجد تعريف ثابت وشامل لتلك الحوادث، وأن الغموض في تحديد تعريف شامل ومحدد جعل من الصعب على المحللين في مختلف الدول وضع توصيات منسقة أو اتفاق دولي على مبادئ موحدة لمنع أو التقليل من حدوث هذه الكوارث. [٤١]

واختلفت التعريفات التي تناولت مصطلح الهجمات السيبرانية على ضوء الاجتهادات الفقهية، والممارسات العملية الدولية، فيعتبر جانب من الفقه إن تُعد الهجمات السيبرانية امتدادًا معاصرًا للحروب التقليدية، إذ انتقل الصراع من ساحات القتال المادية إلى الفضاء الإلكتروني، ولم يعد يقتصر على القوات العسكرية النظامية، بل أصبح يشمل أيضًا خبراء التقنية والمهندسين والمبرمجين إلى جانب العناصر العسكرية. وتمثل هذه الهجمات في جوهرها حربًا معرفية تعتمد على توظيف القدرات الفكرية والتقنية، وتركز على استهداف البنية المعلوماتية والعلمية والرقمية للخصم، بهدف إضعاف قدراته التشغيلية، وتعطيل أنظمته الحيوية، والإخلال بكفاءة مؤسساته الاستراتيجية. [٤٢]وتتخذ الهجمات السيبرانية صورًا متعددة تبعًا لطبيعة أهدافها والجهات المستهدفة، إذ قد تستهدف تعطيل منظومات الاتصال والسيطرة بين القيادات العسكرية ووحداتها الميدانية، أو إرباك شبكات النقل وسلاسل الإمداد اللوجستي، كما يمكن أن تطال الأنظمة الاقتصادية وقواعد البيانات المالية، فضلًا عن التلاعب بالمحتوى الرقمي وإتلاف البيانات أو تعديلها بما يؤثر في كفاءة البنية المعلوماتية للدولة ومؤسساتها الحيوية.

وفي إطار تحديد مفهومها القانوني، عرّفت مجموعة الخبراء التابعة لحلف شمال الأطلسي (الناتو) في دليل تالين الخاص بتطبيق قواعد القانون الدولي على النزاعات السيبرانية، الهجمات السيبرانية بأنها: «كل عملية سيبرانية، سواء كانت ذات طبيعة هجومية أم دفاعية، يُتوقع أن يترتب عليها وقوع إصابات أو وفيات بين الأشخاص، أو إحداث أضرار أو تدمير للممتلكات والأعيان المادية». ويُبرز هذا التعريف أن معيار الهجوم السيبراني لا يقتصر على الوسيلة

المستخدمة، وإنما يرتبط بالآثار والنتائج المترتبة على العملية الإلكترونية، ولا سيما عندما تبلغ مستوى يماثل آثار الهجمات العسكرية التقليدية.. [٤٣]

كما عرف القانون الدولي الهجوم السيبراني بأنه: "عملية الكترونية سواء أكانت هجومية أم دفاعي، يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بالمنشآت أو تدميرها" .[٤٤]

اما التعريف الرسمي الأول من نوعه فهو ما ورد في معجم الاستخدامات العسكرية الذي نشرته هيئة الأركان المشتركة عام ٢٠١١ بعد تأسيس (القيادة السيبرانية الأمريكية) ، إذ عرف الهجوم السيبراني أنه " نشاط عدائي باستخدام الكمبيوتر أو الشبكات أو الأنظمة ذات الصلة، يهدف إلى تعطيل أو تدمير أنظمة الخصم السيبرانيه الحرجة أو ممتلكاته أو وظائفه، إن النتائج المرجوة من الهجوم السيبراني لا تقتصر بالضرورة على أنظمة كمبيوترية مستهدفة أو البيانات نفسها، وأن تفعيل أو تأثير الهجوم السيبراني قد يفصل زمنياً أو مكانياً عن النشاط السيبراني " . [٤٥]

وعلى ذلك فيكون من المناسب تعريف الهجمات السيبرانية لأغراض هذه الدراسة بأنها (مجموعة الاجراءات السيبرانية الهجومية او الدفاعية التي تقوم بها دولة او منظمات دولية او الافراد مستهدفين الاضرار بالأنشطة ذات البعد السيبراني لدولة أخرى سواء كان هذا الاستهداف موجه الى البنى التحتية السيبرانية او نظم معلومات او الى تلك البنى التي يتم إدارتها عبر الفضاء السيبراني، وبما ينعكس سلباً على أمن وسيادة الدولة السيبراني) . [٤٦]

ثانيا" : خصائص الهجمات السيبرانية

تتسم الهجمات السيبرانية التي توجه من خلال الفضاء السيبراني بخصائص تميزها عن غيرها من الهجمات العادية ومن أبرزها ما يلي: [٤٧]

١-الهجمات السيبرانية هي هجمات تقنية متطورة، عكست قمة التطور الذي وصلت إليه ثورة المعلومات .

٢-التكلفة المتدنية نسبياً للهجمات السيبرانية، فلا تحتاج الدول إلى تخصيص ميزانيات ضخمة لإنتاج أسلحتها السيبرانية على خلاف الأسلحة المستخدمة في النزاعات العنيفة التقليدية ذات الكلفة العالية جداً كحاملات الطائرات والمقاتلات المتطورة .

٣-لا تعرف الهجمات السيبرانية بالحدود الجغرافية فهي متنوعة ومتطورة بوسائلها المرتبطة بأكثر المجالات التقنية تطوراً وتغيراً في الحياة المعاصرة للدول، وهي علاوة على ذلك، غير محدودة الأهداف والنتائج، إذ قد تتعدى مخاطرها ميادين القتال التقليدية لتصل بثمارها إلى أكثر المواقع السيادية والحساسة تحصيناً وبعداً عن دائرة القتال .

٤-صعوبة تحديد موقع وشخصية القائم بالهجمات السيبرانية ذات التأثير العالي، لكونها لا تترك أثر أو دليل على حصولها، إذ إن معظم الهجمات السيبرانية يتم اكتشافها بالصدفة، وبعد فترة طويل وبمساعدة المهارات الفنية عالية المستوى لاكتشاف مصدر الهجوم .

ثالثا" : انواع الهجمات السيبرانية

تعد الهجمات السيبرانية هجمات معقدة وخطيرة ولها أنواع متعددة ويمكن تناولها على نحو التالي :

١- هجوم الحرمان من الخدمة

هدف هذا البرنامج حرمان المستخدمين من خدمة معينة والتأثير عليها، ويطلق على أخطر أنواعه اسم Distributed Denial of service (DDOS) حيث أن المهاجم يستغل في هذا الهجوم مجموعة من أجهزة الكمبيوتر لأشخاص لا يعرفهم ولكنه قام باستغلال ثغرات موجودة في أجهزتهم في أكثر من مكان ويقوم بمهاجمة (سيرفر) معين أو شبكة باستخدام هذه الأجهزة دون علم أصحابها. [٤٨]

٢-الفايروسات (البرامج الخبيثة)

الفايروس (virus) هو برنامج مثل أي برنامج تطبيقي آخر، لكنه مصمم من قبل أحد المخربين لإحداث أكبر قدر ممكن من الضرر للنظام بعد ربطه بالبرامج الأخرى ولديه القدرة على تكرار نفسه حتى يبدو وكأنه يتوالد ذاتياً، وهذا يمنحه القدرة على استهداف البرامج الأخرى في الحاسب ومواقع أخرى في الذاكرة بهدف تدميرها. [٤٩]

٣-برامج القنابل المعلوماتية

تُعرف القنبلة المعلوماتية أو ما يُطلق عليها الشفرة الموقوتة (Logic Bomb) بأنها أحد أنواع البرمجيات الخبيثة التي تُصمم لتنفيذ أوامر ضارة عند تحقق شرط أو حدث محدد مسبقًا. وتتميز هذه البرمجيات بصغر حجمها وإمكانية زرعها داخل البرامج أو الأنظمة الحاسوبية بطرق غير مشروعة، بحيث يصعب اكتشافها أثناء التشغيل الاعتيادي.

ولا تكون القنبلة المعلوماتية عادةً برنامجًا مستقلًا، بل تتكون من مجموعة من الشفرات البرمجية التي تُدمج داخل ملفات أو تطبيقات أخرى، وقد تُوزَّع على أجزاء متفرقة داخل النظام لإخفاء طبيعتها الحقيقية وتجنب اكتشافها من قبل برامج الحماية. وعند حلول الوقت المحدد أو تحقق الشرط الذي بُرمجت عليه، تتجمع هذه الشفرات وتُفعِّل تعليماتها تلقائيًا، لتنفذ الوظيفة التخريبية التي أُعدت من أجلها، سواء تمثلت في تعطيل النظام، أو إتلاف البيانات، أو إحداث أضرار في مكونات البيئة الرقمية المستهدفة.. [٥٠]

٤-برامج الدودة

تعرف برامج الدودة بالبرامج التي تستفيد من الثغرات الموجودة في نظام تشغيل الكمبيوتر للانتقال من كمبيوتر إلى آخر، مما يؤدي إلى احتلال الشبكة بالكامل والتسبب في النهاية بآثار مدمرة، وبفضل الوصلات التي تربط الشبكات بعضها ببعض، يمكنهم الانتقال من شبكة إلى أخرى والتكاثر مثل البكتيريا في عملية النقل. (٥١)

المطلب الثالث : الجهود الدولية لمواجهة الهجمات السيبرانية

يعد التعاون بين الدول هو الاداة الرئيسية لمواجهة مخاطر الهجمات السيبرانية المتزايدة ، وخصوصا" انها مخاطر عابرة للحدود الوطنية ، الامر الذي يستدعي تنسيق الحد الادنى من تدابير الامن ، وتبادل المعلومات والممارسات الجيدة وتدوين قواعد السلوك وذلك من خلال الاتي :

اولا" : التعاون في مجال الاتفاقات الدولية هناك العديد من الاتفاقيات التي عقدت للحد من الجرائم السيبرانية وبناء امن سيبراني فعال ، ومن هذه الاتفاقيات اتفاقية كومنولث الدولة المستقلة ٢٠٠١ ، واتفاقية بودابست لعام ٢٠٠١ ، و مبادرة منظمة شنغهاي للتعاون عام ٢٠٠٩ ، والاتفاقية العربية لعام ٢٠١٠ ، وسيتم التركيز هنا على اتفاقية بودابست لعام ٢٠٠١ ، و مبادرة منظمة شنغهاي للتعاون عام ٢٠٠٩ ، والاتفاقية العربية لعام ٢٠١٠، لكونها الاكثر تفصيلا" و الاقرب للموضوع . (٥٢)

١-الاتفاقية الاوربية للجرائم الالكترونية (بودابست)

تعد هذه الاتفاقية اول اتفاقية دولية تسعى الى معالجة جرائم الانترنيت وجرائم الكمبيوتر ، من خلال مواءمة القوانين الوطنية وتحسين تقنيات التحقيق وزيادة التعاون بين الدول ، وقد صاغها المجلس الأوربي في ستراسبورغ بفرنسا بمشاركة فعالة من دول المراقبة في مجلس أوربا (كندا واليابان والفلبين وجنوب افريقيا و الولايات المتحدة الامريكية) ، وقد دخلت هذه الاتفاقية حيز التنفيذ في ١ تموز ٢٠٠٤ .(٥٣)

وتعبر هذه الاتفاقية عن سياسة جنائية مشتركة تهدف الى حماية المجتمع من الجريمة السيبرانية المتمثلة بالمحافظة على الخصوصية والسلامة للانظمة وبيانات الكمبيوترية . (٥٤)

٢-مبادرات منظمة شنغهاي للتعاون

يعد اعلان (يكاترينبورغ) بتاريخ ١٦ يونيو عام ٢٠٠٩، ابرز الجهود التي حققتها هذه المنظمة في سبيل التعاون في مجال الامن السيبراني ،اذ جاء فيه (تؤكد الدول الاعضاء في منظمة

شنغهاي للتعاون على اهمية مسألة ضمان امن المعلومات الدولي بوصفة احد العناصر الرئيسية لنظام الامن الدولي المشترك) .[٥٥]

٣-الاتفاقية العربية لمكافحة تقنية المعلومات :

جاءت هذه الاتفاقية كنتيجة لارتفاع معدلات الجرائم الالكترونية في الشرق الاوسط ، بسبب مكاسبها الكبيرة وانخفاض المخاطر وسهولة الوصول لها ،واستجابة لهذا الواقع ،برزت الحاجة الماسة الى عقد اتفاقية في هذا المجال ، وتم توقيع الاتفاقية من قبل مجلس وزراء الداخلية العرب في ٢١ كانون الاول ٢٠١٠، اذ وقعت احدى وعشرون دولة عربية من ضمنها العراق الذي صدق على الاتفاقية في ايلول ٢٠١٣،ودخلت الاتفاقية حيز النفاذ في٧تموز ٢٠١٤ .[٥٦]

ثانيا" : التعاون الدولي بين أجهزة الشرطة

أدى التطور المتسارع في تكنولوجيا المعلومات والاتصالات، وما صاحبه من اتساع نطاق الجرائم والهجمات السيبرانية العابرة للحدود، إلى إدراك المجتمع الدولي أن مواجهتها لا يمكن أن تتم من خلال الجهود الوطنية المنفردة، وإنما تتطلب تعاونًا دوليًا وثيقًا بين الأجهزة الأمنية وجهات إنفاذ القانون. فطبيعة هذه الجرائم، التي تتجاوز الحدود الجغرافية للدول، فرضت ضرورة تنسيق الجهود وتبادل المعلومات والخبرات لملاحقة مرتكبيها وتقديمهم إلى العدالة.

ومن أبرز صور هذا التعاون الدولي إنشاء المنظمة الدولية للشرطة الجنائية (الإنتربول)، التي أسهمت في تعزيز التنسيق بين أجهزة الشرطة في مختلف الدول، وتيسير تبادل المعلومات الاستخباراتية والبيانات الجنائية المتعلقة بالمجرمين العابرين للحدود. كما تطورت آليات التعاون الأمني لتشمل العديد من الوسائل والإجراءات الرامية إلى مكافحة الجرائم السيبرانية، والتي يمكن إجمال أهمها فيما يأتي: [٥٧]

١.**ربط شبكات الاتصال والمعلومات:** يتم ذلك عن طريق ربط الاتصال بين أجهزة العدالة الجنائية الوطنية بصفة عامة وأجهزة الشرطة بصفة خاصة وبين تلك الأجهزة في الدول الأخرى عن طريق السلك الدبلوماسي واتصالات خاصة. [٥٨]

٢.**المنظمة الدولية للشرطة الجنائية (إنتربول(** : تعد منظمة الإنتربول من أهم آليات التعاون الشرطي الدولي لمكافحة الجرائم العالمية العابرة للحدود الوطنية بصفة عامة والجريمة المعلوماتية بصفة خاصة، فمهمة الإنتربول الأساسية تفعيل التعاون بين أجهزة الشرطة التابعة للدول الأعضاء في المنظمة بتوحيد إجراءات التسليم، ومن خلال تنسيق العمل الشرطي وتجميع البيانات وتبادل المعلومات لتيسير خدمات التحقيق لضبط وملاحقة المجرمين

الهاربين وتسلمهم إلى الدولة التي تطلب تسلمهم، وإنشاء و تطوير كل النظم القادرة على المساهمة بفاعلية في الوقاية والعقاب على جرائم القانون العام .)[٥٩]

٣. تبادل المعاونة لمواجهة الكوارث والأزمات : في حالة وجود أزمة وفي المواقف الحرجة، فإن عنصر الوقت يعد من الأمور الحاسمة في مواجهة تلك الأزمة أو الكارثة، الأمر الذي يحتاج معه إلى تكثيف وزيادة الجهود والخبرات والمكانيات وهو ما لا يمكن تحقيقه الا بتركيز الجهود الدولية في مسار واحد) .[٦٠]

٤.القيام ببعض عمليات شرطية دولية مشتركة: من أمثلة على ذلك، التسليم المراقب في مجال مكافحة المخدرات، فهو يعني السماح لشحنة غير مشروعة بالمرور تحت المراقبة عبر إقليم ما، وكذلك المطاردات الساخنة والتي يقصد بها تعقب الجناة الذي يبدأ في احدى الدول ويواصل في أراضي دولة أخرى.)[٦١]

ثالثا" : مظاهر التعاون الشرطي على المستوى الدولي في مجال مكافحة الهجوم السيبراني ويشمل :[٦٢]

١. شرطة الويب الدولية:

تُعد شرطة الويب الدولية إحدى المبادرات الرائدة في مجال مكافحة الجرائم الإلكترونية، إذ أُنشئت في الولايات المتحدة الأمريكية عام ١٩٨٦ بهدف توفير آلية متخصصة لتلقي شكاوى مستخدمي شبكة الإنترنت، ومتابعة الجرائم التي تُرتكب عبر الفضاء الإلكتروني. كما تتولى تعقب القراصنة الإلكترونيين، وجمع الأدلة الرقمية اللازمة لإثبات الجرائم، والعمل على إحالة مرتكبيها إلى الجهات القضائية المختصة لاتخاذ الإجراءات القانونية بحقهم.

٢. مركز بلاغات احتيال الإنترنت:

أُسس هذا المركز في الولايات المتحدة الأمريكية بتاريخ ١٨ أيار/مايو ٢٠٠٠، ليكون جهة وطنية متخصصة في استقبال البلاغات المتعلقة بجرائم الاحتيال الإلكتروني التي تُرتكب عبر شبكة الإنترنت. ويعمل المركز بالتنسيق مع مكتب التحقيقات الفيدرالي (FBI) والمركز الوطني لجرائم ذوي الياقات البيضاء (National White Collar Crime Center)، بهدف رصد أنماط الاحتيال الإلكتروني، وتحليلها، وتتبع مرتكبيها، وتبادل المعلومات مع أجهزة إنفاذ القانون داخل الولايات المتحدة وخارجها. كما يوفر منصة إلكترونية لاستقبال الشكاوى والبلاغات، بما يسهم في تعزيز التعاون الأمني الدولي ومكافحة الجرائم السيبرانية العابرة للحدود.

رابعا" : تعاون السلطات القضائية للدول

تعالج قواعد الولاية القضائية بموجب القانون الدولي العرفي قضية أي دولة (مقابل دول اخرى) لها الحق في تنظيم أي حدث عابر للحدود الوطنية ، أي وضع وتطبيق وانفاذ قوانينها [٦٣] ، ويوازن التعاون القضائي الدولي بين استقلال الدولة في ممارسة اختصاصها الجنائي على حدود إقليمها، وبين ضرورة ممارسة حقها في العقاب، فبدون هذا التعاون لا يمكن للدولة من الناحية العملية إقرار حقها في العقاب وعلى ذلك فلا بد من التعاون الدولي لسببين: [٦٤]

السبب الأول: إن الدولة تتقيد بحدودها الإقليمية، فقانون العقوبات يمكن ان يتعدى نطاق تطبيقه إلى ما يجاوز حدود إقليم الدولة، إلا أنه لا يمكن مباشرة الإجراءات خارج الإقليم الوطني لان ممارستها تمس سيادة الدول الأجنبية الأخرى .

السبب الثاني: لا يمكن تطبيق قانون العقوبات بدون قانون الإجراءات الجزائية، فالإجراءات الجزائية هي الوسيلة اللازمة لتطبيق قانون العقوبات ونقله من حالة السكون إلى الحركة، وعلى ذلك فإنه إذا تطلب تطبيق قانون العقوبات مباشرة بعض الإجراءات الجزائية خارج حدود إقليم الدولة فانه يجب عدم الاصطدام بمشكلة الحدود الإقليمية بين الدول [٦٥])

المطلب الثالث :اثر الامن السيبراني على مبدأ السيادة

ارتبط قيام الدولة منذ القدم بمفاهيم عديدة، أهمها مفهوم السيادة الذي يعد مبدأ من مبادئ القانون الدولي والمحدد لعمل الدول والتزاماتها، وما يرتبط به من أمن واستقرار، غير أن التغير الذي طرأ على الساحة الدولية منذ بداية القرن الحادي والعشرين، مع بروز الثورة المعلوماتية وما أحدثته من تطورات كبيرة على مستوى النظم السياسية يعبر عن حركة متسارعة عملت على ترويض السيادة الوطنية وفقا لما يتطلبه العصر الرقمي الجديد، فبعد أن كان المنظور التقليدي يتضمن حق الدولة في فرض سيادتها على حدود إقليمها في الداخل والخارج، فإن هذه الحقوق أخذت في الانحسار في ظل العالم الرقمي، لتتصاعد بذلك المشكلات المرتبطة بإشكالية تراجع مفهوم السيادة الوطنية، وبروز ما يوحي بزوال الحدود الجغرافية التقليدية لصالح حدود جديدة فرضها عصر التطور التكنلوجي الحديث . [٦٦]

وعليه سوف نتناول في هذا المطلب صور التعدي على سيادة للدول من خلال عرض الانتهاكات التي تتعرض لها الدول في قدرتها على إدارة وحماية بياناتها الرقمية ومعلوماتها وبنيتها التحتية والامنية ، وندرج ادناه أبرزها هذه الانتهاكات: [٦٧]

أولا" : الهجوم الإلكتروني

يعني استخدام الطاقة الكهرومغناطيسية أو الأسلحة المضادة للإشعاع لمهاجمة الأفراد والمرافق بهدف إضعاف القدرة القتالية للعدو وتقليل استخدامه الفعال للطيف المغناطيسي تشمل هذه الهجمات التشويش والتضليل الكهرومغناطيسي، وعادة ما تؤدي الخسائر الناتجة عن الهجوم الإلكتروني إلى خسائر مادية كبيرة.

ثانيا: التجسس الإلكتروني انتهاك للسيادة السيبرانية

يعد التجسس الإلكتروني أحد أهم المراحل التمهيدية للعمليات الحربية السيبرانية، وتعرف على أنه وسيلة الاعتراض غير مصرح به لأنظمة الاتصالات والشبكات والبيانات بهدف الحصول على معلومات والتلاعب بها.

ثالثا" : الاختراق الإلكتروني

يتضمن اختراق الأنظمة للحصول على معلومات استخباراتية عن دولة أو منظمة، فهو نظام أو برنامج مصمم الاستغلال بيانات الخصم والحاق الضرر بها، بالإضافة إلى تحميل نظامه الحاسوبي، بهدف التفوق عليه في المجالات الأمنية السكرية والسياسية تتم هذه العملية على مستويات متعددة، سواء كانت قرية مؤسسية أو على مستوى الدول .

رابعا" : القرصنة الإلكترونية

هي عملية الدخول غير المصرح بها إلى أجهزة الغير وشبكاتهم الإلكترونية تهدف إلى المساس بالسرية وخصوصية الأفراد، أو التأثير على سلامة المحتوى من خلال تغييره أو إتلافه ولا تقتصر القرصنة على المعلومات الشخصية للمواطنين فحسب، بل تتجاوز ذلك من خلال الكشف عن أسرار أمن الدول واختراق مواقع المؤسسات الحكومية والبريد الإلكتروني لبعض قادة الدول حول العالم. [٦٨]

رابعا" : استهداف البنى التحتية للدولة

تتعرض البنية التحتية للدول سواء المدنية أو العسكرية لهجمات إلكترونية خطيرة تهدف إلى تعطيل أنظمتها وتشغيلها مما يؤدي إلى شلل كامل في الأنشطة الحيوية وتدفق المعلومات ، اذ تؤدي هذه الهجمات إلى إرباك العمليات اليومية وتعطيل مرافق الحياة الأساسية، اذ تشمل استهداف محطات الطاقة وشبكات الوقود بالإضافة إلى الخدمات المالية والمصرفية وكذلك نظم الاتصالات ووسائل النقل، وفي ظل هذا التحدي باتت الدول تواجه مخاطر غير مسبوقة نتيجة تصاعد وتيرة الهجمات السيبرانية التي تستهدف أمنها واستقرارها ففي عام ٢٠٠٧ قامت روسيا بشن حرب سيبرانية شاملة على استونيا ما سبب بتعطيل الخدمة وشلل كامل للبنية التحتية ،

وفي حادثة أخرى بعد فيروس ستاكسنت (Stunnel) الذي ضرب منشأة الإيرانية لتخصيب اليورانيوم عام ٢٠١٠ أحد أخطر الأمثلة على الهجمات السيبرانية المتطورة، كما لم تكن الولايات المتحدة بمنأى عن هذه الهجمات اذ شهدت شبكات الكهرباء فيها هجمات مماثلة عام ٢٠٠٩ تسببت في انقطاعات واسعة النطاق، أن الهجمات السيبرانية لم تقتصر على القطاعات العسكرية أو المالية فقط بل طالت أيضا قطاع الطاقة بشكل ملحوظ ، ففي عام ٢٠٠٨ تعرض خط أنابيب النفط التركي الهجوم سيبراني غامض أدى إلى اشتعال النيران فيه دون إطلاق أي إنذارات أو مستشعرات، فيما اعتبرت التقارير الأمريكية ان روسيا كانت وراء الهجوم يسبب اعتراضها على إنشاء خط الأنابيب باكو – تبليسي – جيهان[٦٩]، أما في كوريا الجنوبية، فقد تعرضت شركة الطاقة المائية والنووية لهجوم إلكتروني كبير في ديسمبر ٢٠١٤ ، ما أثار قلقا عالميا بشأن هشاشة البنية التحتية أمام التهديدات السيبرانية، وشهدت السعودية عام ٢٠١٧ هجوما سيبرانيا خطيرا باستخدام فيروس "الصخرة الدوارة" الذي استهدف قطاعات الطيران والبتروكيماويات، مما تسبب في خسائر كبيرة للشركات العاملة في هذه القطاعات، وفي عام ٢٠١٩ تم استهدف شبكات المعلومات والبنية التحتية في السعودية، الإمارات، قطر، الكويت والبحرين واستمرت هذه الهجمات لفترات طويلة بهدف تعميق تأثيرها وضمان تحقيق أهداف استراتيجية. [٧٠]

خامسا" : اختراق الأنظمة العسكرية وتدميرها

تعد الهجمات المسيرانية التي تستهدف الأنظمة العسكرية من أخطر التهديدات في العصر الحديث، فهي قد تتجاوز مجرد التخريب أو التعطيل لتصل إلى مرحلة السيطرة الكاملة على نظم القيادة والتحكم ، اذ تستهدف الهجمات اختراق نظم القيادة والسيطرة عن بعد مما يمكنهم من الاستيلاء على منظومات عسكرية حساسة مثل الطائرات بدون طيار والغواصات النووية وحتى الأقمار الصناعية العسكرية، إذا نجحت هذه الهجمات فإن العواقب قد تكون وخيمة، اذ يمكن إعادة توجيه الأسلحة نحو أهداف غير مقصودة، سواء كانت داخلية أو ضد دول صديقة وحليفة، على سبيل المثال، يمكن اختراق طائرة بدون طيار وإعادة توجيهها لتنفيذ هجوم داخل أراضي الدولة المالكة لها أو استغلالها لتهديد أمن دولة أخرى، وبالمثل إذا تعرضت غواصة نووية للاختراق فإن القراصنة قد يتمكنون من تعطيلها أو استخدامها بطريقة تهدد الأمن البحري. [٧١]

الخاتمة

ان الهجمات تبرز لنا الحاجة الملحة لتعزيز الدفاعات الإلكترونية ووضع أنظمة حماية قوية قادرة على التصدي للتهديدات المستمرة فالتهاون في مجال الامن السيبراني قد يؤدي إلى عواقب كارثية تهدد الأمن الوطني للدول واستنادا" الى ذلك فان هناك حاجة ملحة وضرورية الى وضع

استراتيجية وطنية تواكب التطورات الحاصلة في العالم وتسير جنبا إلى جنب في كنف المعلومات الإلكترونية والبحث في سبل حمايتها من التدخلات الأجنبية والعمل على استخدامها بشكل صحيح لخدمة المجتمع ، ولهذا تحاول العديد من الدول وضع حد للتحكم الأجنبي في وسائل الاتصال الحديثة كالأنترنت والاعتماد على الجهد الذاتي لتطوير البرمجيات والآلات الهادفة إلى تنمية المجتمع ، ومن اهم الإجراءات التي اتخذتها بعض الدول في حماية امن فضائها السيبراني هو بناء فضاء سيبراني خاص بها كما فعلت الصين وروسيا وإيران ودول أخرى.

الاستنتاجات

١.تآكل الحدود التقليدية للسيادة: الفضاء السيبراني العابر للحدود يجعل من الصعب على الدولة فرض سيطرتها الكاملة، مما يستدعي تعاوناً دولياً لا يتعارض مع المصالح الوطنية.

٢.ازدواجية العلاقة بين الأمن السيبراني والسيادة: فبينما يُعد الأمن السيبراني أداة لحماية السيادة، فإن غيابه أو ضعفه يتحول إلى أداة لانتهاكها (مثل التجسس وسرقة البيانات الحكومية.

٣.التبعية التقنية تهديد سيادي غير مباشر: اعتماد الدول النامية بشكل خاص على بنى تحتية وبرمجيات أجنبية يخلق "سيادة منقوصة" حتى دون وقوع هجوم فعلي.

٤.الحاجة إلى تشريعات وطنية ودولية متطورة: القوانين الحالية غير كافية لمواكبة سرعة التهديدات، مما يستدعي:

- بناء استراتيجيات وطنية للأمن السيبراني
- تطوير قدرات وطنية في الدفاع السيبراني
- تعزيز التعاون الدولي مع الحفاظ على الاستقلالية الرقمية

٤- الأمن السيبراني كركن جديد من أركان الأمن القومي: لا يمكن فصله عن الأمن العسكري والاقتصادي والسياسي، بل أصبح بُعداً محورياً يحدد قوة الدولة ومدى تمتعها بسيادة فعلية في القرن الحادي والعشرين.

الهوامش

[1] احمد عبيس نعمة الفتلاوي ، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر ، مكتبة زين الحقوقية والادبية ، بيروت ، ٢٠١٨ ، ص٢٧.

[2] مثنى فائق مرعي ، هدى عبد السلام خطاب ، المتغير السيبراني واثره على العلاقات الدولية ، الدار البابلية للدراسات والبحوث العلمية ، مصر ، ٢٠٢٥ ، ص ٢٠ .

[٣] عادل عبد العزيز صالح الرشيد، قرائن الجريمة الإلكترونية وأثرها في الإثبات، دار كنوز إشبيليا للنشر و التوزيع، الرياض، المملكة العربية السعودية ،٢٠١٧ ، ص ٢٤.

[٤] محمد محمود العمري، مدخل إلى الأمن السيبراني، دار زهران للنشر و التوزيع، ٢٠٢٠ ، ص ٤٢ .

[٥] محمود مدين، فن التحقيق والثبات في الجرائم الإلكترونية، المصرية للنشر والتوزيع، ٢٠٢٠ ، ص ٢٩ .

[٦] رحموني محمد ، خصائص الجريمة الالكترونية ومجالات استخدامها ، مجلة الحقيقة ، العدد ٤١ ، ٢٠١٨ ، ص ٤٤١– ٤٤٣ .

[٧] باسم علي خريسان ، الفضاء السيبراني مدخل ابستيمولوجي ، بغداد، دار القناديل للنشر و التوزيع ،٢٠٢١ ، ص١٥ .

[٨] امال بن صويلح، التعاون الاقليمي الاوربي في مواجهة الجريمة الالكترونية (اتفاقية بودابست نموذجا)، بحث منشور ضمن كتاب الجرائم الالكترونية في الفقه الاسلامي والقانون الوضعي، جمع وتنسيق د. عباس حفصي، صادر عن المركز الديمقراطي العربي، برلين، ٢٠٢٢ ، ص ٤٢.

[٩]مكتب الأمم المتحدة المعني بالمخدرات و الجريمة، دراسة شاملة عن الجريمة السيبرانية، الأمم المتحدة، نيويورك، ٢٠١٣ ، ص ٤١.

[١٠]مصطفى محمود منجود ، الأبعاد السياسية لمفهوم الامن في الاسلام ، المعهد العالمي للفكر الاسلامي ، القاهرة ، ١٩٩٦، ص٣٠.

[١١]نهلا عبد القادر المومني، الجرائم المعلوماتية ، دار الثقافة للنشر و التوزيع، عمان، ٢٠١٠ ، ص ٥٧ –٥٨ .

[١٢] جمعة علي بن جمعة ، الامن العربي في عالم متغير ، مكتب مدبولي ، القاهرة ، ص ٣٢ .

[١٣] محمد جاسم على الله ، التنافس المعلوماتي بين الولايات المتحدة الامريكية و الصين : دراسة في الامن السيبراني ، عمان ، دار امجد للنشر و التوزيع ، ٢٠٢٢ ، ص٢٦ .

[١٤]الأمم المتحدة اللجنة الاقتصادية و الاجتماعية لغربي آسيا، إرشادات الإسكوا للتشريعات السيبرانية، بيروت، ٢٠١٢ ، ص١٣٣.

[١٥] Kurtulus, Ersun N , “The Notion of a ‘Pre-Emptive War’: the Six Day War Revisited”, Middle East Journal,(2007), Vol. 61, No. 2, pp. 220-238.

[١٦]الأمم المتحدة اللجنة الاقتصادية و الاجتماعية لغربي آسيا، المصدر السابق، ص ١٣٥.

[١٧] Yuval Shany & Tal Mimran, Israel International Regulation of Cyber Operations, The Hebrew University of Jerusalem Faculty of Law Mt. Scopus, Jerusalem, Hebrew University of Jerusalem Legal Studies Research Paper Series No. 22-2,2021 ,p17-23 .

[١٨]الأمم المتحدة اللجنة الاقتصادية و الاجتماعية لغربي آسيا، المصدر السابق، ص ١٣٦.

[١٩] Cristopher D. DeLuca, “The Need for International Laws of War to Include Cyber Attacks InvolvingState and Non-State Actors”, 3 Pace International Law Review OnlineCompanion, 2013, p. 279.

[٢٠] محمد عادل محمد عسكر، وضع العمليات السيب ارنية في القانون الدولي مع التطبيق علي ممارسة التجسس وقت السلم: دارسة علي ضوء دليل "تالين" بشأن القانون الدولي المطبق علي العمليات السيبرانية ٢٠١٧ – ٢٠١٣ ، ص ٢٦٣.

[٢١] وسن احسان عبد المنعم ، احمد قيس احمد ، تكنولوجيا المعلومات و الامن السيبراني : زمنية التطور وافتراضية الواقع وتخطي الحدود ، دار ومطبعة الرفاة للطباعة و النشر ، ٢٠٢٢ ، ص ٥١ .

[٢٢] قاسم محمد عبد ، الحروب السيبرانية ومستقبل الأمن الدولي ، اطروحة دكتوراه ، جامعة النهرين ، قسم السياسة الدولية ، ٢٠٢٢ ، ص ١٨٣ .

[٢٣] اسماعيل محمود الرزاز ، مصدر سبق ذكره ، ص ١١٢.

[٢٤] Edward R. McNicholas and Kevin J. Angle, USA, Published in (Cybersecurity 2021: A practical cross-border insight into cybersecurity law), Fourth Edition, editors by Nigel Parker & Overy LLP, Global Legal Group Limited, London, 2020, p 220.

[٢٥] اسماعيل محمود الرزاز ، مصدر سبق ذكره ، ص ١٠٩ .

[٢٦] شموئيل إيفن ودافيد سيمان طوف،" حرب في الفضاء السبراني: مفاهيم، واتجاهات، ودلالات لإسرائيل"، معهد دراسات الأمن القومي، مذكرة رقم ١٠٩، تل أبيب، ٢٠١١.

[٢٧] الاتحاد الدولي للاتصالات ، دليل الامن السيبراني ، سويسرا ، ٢٠٠٦ ، ص ٨٢ .

[٢٨] Mori Hamada, Matsumoto and Hiromi Hayashi, japan, Published in (Cybersecurity 2020: A practical cross-border insight into cybersecurity law), Third Edition, editors by Nigel Parker and Alexandra Rendell Allen & Overy LLP, Global Legal Group Limited, London, 2019, p 122.

[٢٩] اسماعيل محمود الرزاز ، مصدر سبق ذكره ، ص١٠١ .

[٣٠] عامر عبد الفتاح الجومرد ، السيادة ، مجلة الرافدين للحقوق ، جامعة الموصل ، العدد الاول ، ٢٠١٩ ، ص ١٦٣.

[٣١] اسماعيل محمود الرزاز ، المصدر السابق ، ص ١٠. 6

[٣٢] (Michael N. Schmitt, S.Watts, The Decline of International Humanitarian Law Opinion Juries and the law of Cyber Warfare, 50(2) Texas International Law Journals, United State, 2015.

[٣٣] وليد لعايب ، تقييم تجربة نظام الدفع الالكتروني الجزائري في ظل ثورة التكنولوجيا المصرفية:دراسة مقارنة ، مجلة الابحاث و الدراسات التنمية ، جامعة محمد البشير الإبراهيمي برج عر يريج ، الجزائر ، ٢٠٠٨، ص ١٤٤ .

[٣٤] المصدر نفسه ، ص ١٤٥.

[٣٥] منشور في الجريدة الرسمية بالعدد ٦٩٠٤ بتأريخ ٩ ذو الحجة ١٤٤١(٣٠ يوليو ٢٠٢٠) ، ص ٤١٦٠ .

[٣٦] عبد الوهاب ملياني ، امن المعلومات في بيئة الاعمال الالكترونية ، اطروحة دكتوراه ، كلية الحقوق و العلوم السياسية ،جامعة تلمسان ،6 ٢٠١ – ٢٠١٧ ، ص ١٥٩ .

[٣٧] المصدر نفسه ، ص١٥٩.

[٣٨] منزر رابح ، درويش سعيد ، الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول ، كلية الحقوق جامعة الجزائر ، مجلة صوت القانون ، المجلد الثامن ، العدد ١ ، ٢٠٢١ ، ص ٥٤٧ .

[٣٩] المصدر نفسه ، ص ٥٤٧ .

[٤٠] Al-Saidi, Saad Obaid Alwan, and Tamara Kadim Manati. “Transformations of the World Order after the Corona Pandemic COVID-19: The Role of Culture, Science, and the Environment.” Journal of International Crisis and Risk Communication Research 7, no. S10 (2024). https://jicrcr.com/index.php/jicrcr/article/view/1154/924.

[٤١] Oona A. Hathaway, Rebecca Crootof, Philip Leviz, Halay Nix,Aileen Nowlan, William Perdue & Julia Spiegel, "The law of Cyber – Attack ", California law review, 2012, p.824

[٤٢] Schmitt, M.N, "Computer network attack and the use of force in international law": thoughts on a normative framework. In the Use of Force in International Law, 2017, Vol.27, No. 379-431, p.7.

[٤٣] سعيد درويش، الحروب السيبرانية وأثرها على حقوق الأنسان ، دارسة على ضوء أحكام دليل " تالين"، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد ٥٤ ، العدد الخامس، ٢٠١٧ ، ص ١٨١ .

[٤٤] Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to cyber operations, Cambridge University Press, USA, 2017, p 415.

[٤٥] James E. Cartwright, Memorandum for Chiefs of the Military Serve. Commanders of the Combatant Commands, Dirs the Joint Staff Directories on Joint Terminology for Cyberspace Operations 5 (No. 2011).

[٤٦] Ali, Inass Abdulsada, and Faieq Hassen Jasem. “Sub-National Governments’ Interactions in International Affairs: An Arab Perspective on Paradiplomacy.” International Area Studies Review 27, no. 4 (December 2024). https://iasr.or.kr/_common/do.php?a=full&b=12&bidx=3911&aidx=43280

[٤٧] محمد منذر جلال وسرى غضبان غيدان، تكنلوجيا الحروب السيبرانية، دار ومكتبة عدنان للطباعة والنشر والتوزيع، بغداد، ٢٠٢١ ، ص ١٤٣ .

[٤٨] Kenneth Boyte, The Evolution of Cyber Warfare in Information Operations Targeting Estonia, the U.S., and Ukraine, Published in (Developments in Information Security and Cybernetic Wars), IGI Global, USA, 2019, p 143.

[٤٩] عمار باسم الحسيني، جرائم الحاسوب والأنترنت(الجرائم المعلوماتية) ، منشورات زين الحقوقية، بيروت (لبنان) ،٢٠١٧ ، ص١٤٠_١٤١.

[٥٠] Anitta Patience Namanya, Andrea Cullen, Irfan U. Awan and Jules Pagna Disso, The World of Malware: An Overview, IEEE 6th International Conference on Future Internet of Things and Cloud, Spain, 2018, p 420.

[٥١] عمار باسم الحسيني ، المصدر السابق ، ص ١٤٥-١٤٦ .

[٥٢] أحمد زكريا الباسوسي، الجهود الدولية لمكافحة الهجمات السيبرانية على قطاع الطاقة : حالات مختارة، مجلة كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، المجلد (٢٤) ، العدد (٤) أكتوبر ٢٠٢٣، ص١٦٧.

[٥٣] محمد جاسم على الله ، مصدر سبق ذكره ، ص٧٣ .

[٥٤] اسماعيل محمود الرزاز ، مصدر سبق ذكره ، ص٩٣ .

[٥٥] المصدر نفسه ، ص٩٤ .

[٥٦] محمد جاسم على الله ، مصدر سبق ذكره ، ص ٧٥ .

[٥٧] أحمد زكريا الباسوسي، مصدر سبق ذكره ، ص ١٦٨ .

[٥٨] سالم محمد سليمان الاوجلي، أحكام المسئولية الجنائية عن الجرائم الدولية في التشريعات الوطنية، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، ١٩٩٧ ، ص ٤٢١ .

[٥٩] فهد عبد اهلل العبيد العازمي ، الإجراءات الجنائية المعلوماتية ، دار الجامعة الجديدة ، ط ٢٠١٦ ، مصر، ص ٦٥١ .

[٦٠] يوسف حسن يوسف ، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية ، القاهرة ، ط١ ، ٢٠١١ ، ص ١٤٨

[٦١] غانم مرضي الشمري، الجرائم المعلوماتية، دار الثقافة، الاردن ، ٢٠١٦ ، ص ٩٨ .

[٦٢] سليمان احمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، ط ٢٠٠٧ ،مصر، ص٤١٧ . ينظر: Shyae, Wafaa Satar, and Hayer Abed Kathem. “The Impact of the Security and Military Institution on Achieving Iraqi National Security after 2014.” Journal of Positive School Psychology 6, no. 5 (2022). https://journalppw.com/index.php/jpsp/article/view/٦٦٦٢.

[٦٣] باسم علي خريسان ، مصدر سبق ذكرة ، ص١٧٢ .

[٦٤] حسنين صالح عبيد، القضاء الجنائي الدولي، تاريخه – تطبيقاته– مشروعاته، دار النهضة العربية، ط١ ، القاهرة ، ١٩٧٧ ، ص٩٩–١٠٠ .

[٦٥] سليمان احمد فضل، مصدر سبق ذكره ، ص ٤٢٢ . وينظر كذلك : سالم محمد سليمان الاوجلي ، مصدر سبق ذكره ، ص ٤٢٧ .

[٦٦]سالم محمد سليمان الاوجلي ، المصدر السابق ، ص ٤٢٨.

[٦٧] أنديرا عراجي، القوة في الفضاء السيبراني، فصل عصري من التحدي والاستجابة، دار ميرزا، بيروت، ٢٠١٩ ، ص ٨٣–٨٦ .

[٦٨] أنديرا عراجي، المصدر السابق ، ص ٨٣–٨٦. ينظر: Hameed, Muntasser Majeed. "Political Structure and the Administration of Political System in Iraq." Instituto de Estudios Políticos y Derecho Público "Dr. Humberto J. La Roche," Facultad de Ciencias Jurídicas y Políticas, Universidad del Zulia 37, no. ٦٥ (٢٠٢٠).

[٦٩] كريم رقولي والعصر نويوة، الأمن السيبراني المتوسطي بين الواقع والرهانات الأمنية مجلة طينة للدراسات العلمية الأكاديمية المجلد ٢، العدد ٢ ٢٠١٩، ص٧٤. ينظر : Azzaz, Abbas Hashim. "Concept of Conflict and Identifying a Form CR: SIPPABIO Conceptual and Theoretical Framework." Res Militaris. https://resmilitaris.net/menu-script/index.php/resmilitaris/article/view/2624/2195.

[٧٠] إيهاب خليفة، تنامي التهديدات السيبرانية للمؤسسات العسكرية، مجلة اتجاهات االحداث، العدد (٢٢) ،٢٠١٧ ، ص٥٧ .

[٧١] ينظر: شريفة كلاع ، الأمن السيبراني والتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية ، جامعة الجلفة ، المجلد ١ ، العدد ١، ٢٠٢٢ ، ص ٢٩٥.

المصادر

اولا" : المصادر العربية

١.الاتحاد الدولي للاتصالات ، دليل الامن السيبراني ، سويسرا ، ٢٠٠٦ ، ص ٨٢ .

٢.أحمد زكريا الباسوسي، الجهود الدولية لمكافحة الهجمات السيبرانية على قطاع الطاقة : حالات مختارة، مجلة كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، المجلد (٢٤) ، العدد (٤) أكتوبر ٢٠٢٣.

٣.احمد عبيس نعمة الفتلاوي ، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر ، مكتبة زين الحقوقية والادبية ، بيروت ، ٢٠١٨.

٤.امال بن صويلح، التعاون الاقليمي الاوربي في مواجهة الجريمة الالكترونية (اتفاقية بودابست نموذجا)، بحث منشور ضمن كتاب الجرائم الالكترونية في الفقه الاسلامي والقانون الوضعي، جمع وتنسيق عباس حفصي، صادر عن المركز الديمقراطي العربي، برلين، ٢٠٢٢ .
٥.الأمم المتحدة اللجنة الاقتصادية و الاجتماعية لغربي آسيا، إرشادات الإسكوا للتشريعات السيبرانية، بيروت، ٢٠١٢
٦.أنديرا عراجي، القوة في الفضاء السيبراني، فصل عصري من التحدي والاستجابة، دار ميرزا، بيروت، ٢٠١٩.
٧.إيهاب خليفة، تنامي التهديدات السيبرانية للمؤسسات العسكرية، مجلة اتجاهات االحداث، العدد (٢٢) ،٢٠١٧ .
٨.باسم علي خريسان ، الفضاء السيبراني مدخل ابستيمولوجي ، بغداد، دار القناديل للنشر و التوزيع ،٢٠٢١.
٩.جمعة علي بن جمعة ، الامن العربي في عالم متغير ، مكتب مدبولي ، القاهرة .
١٠.حسنين صالح عبيد، القضاء الجنائي الدولي، تاريخه – تطبيقاته– مشروعاته، دار النهضة العربية، ط١ ، القاهرة ، ١٩٧٧.
١١.رحموني محمد ، خصائص الجريمة الالكترونية ومجالات استخدامها ، مجلة الحقيقة ، العدد ٤١ ، ٢٠١٨ .
١٢.سالم محمد سليمان الاوجلي، أحكام المسئولية الجنائية عن الجرائم الدولية في التشريعات الوطنية، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، ١٩٩٧ ، ص ٤٢١ .
١٣.سعيد درويش، الحروب السيبرانية وأثرها على حقوق الأنسان ، دارسة على ضوء أحكام دليل " تالين"، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد ٥٤ ، العدد الخامس، ٢٠١٧ ، ص ١٨١ .
١٤.سليمان احمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، ط، مصر ، ٢٠٠٧.
١٥.شريفة كلاع ، الأمن السيبراني والتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية ، جامعة الجلفة ، المجلد ١ ، العدد ١، ٢٠٢٢.
١٦.شموئيل إيفن ودافيد سيمان طوف،" حرب في الفضاء السبراني: مفاهيم، واتجاهات، ودلالات لإسرائيل"، معهد دراسات الأمن القومي، مذكرة رقم ١٠٩، تل أبيب، ٢٠١١.
١٧.عادل عبد العزيز صالح الرشيد، قرائن الجريمة الإلكترونية وأثرها في الإثبات، دار كنوز إشبيليا للنشر و التوزيع، الرياض، المملكة العربية السعودية، ٢٠١٧ .
١٨.عامر عبد الفتاح الجومرد ، السيادة ، مجلة الرافدين للحقوق ، جامعة الموصل ، العدد الاول ، ٢٠١٩.
١٩.عبد الوهاب ملياني ، امن المعلومات في بيئة الاعمال الالكترونية ، اطروحة دكتوراه ، كلية الحقوق و العلوم السياسية ،جامعة تلمسان ،. 2017 – 201 6
٢٠.عمار باسم الحسيني، جرائم الحاسوب والأنترنت(الجرائم المعلوماتية) ، منشورات زين الحقوقية، بيروت (لبنان) ،٢٠١٧.
٢١.غانم مرضي الشمري، الجرائم المعلوماتية، دار الثقافة، الاردن ، ٢٠١٦.

٢٢.فهد عبد اهلل العبيد العازمي ، الإجراءات الجنائية المعلوماتية ، دار الجامعة الجديدة ، ط ٢٠١٦ ، مصر.
٢٣.قاسم محمد عبد ، الحروب السيبرانية ومستقبل الأمن الدولي ، اطروحة دكتوراه ، جامعة النهرين ، قسم السياسة الدولية ، ٢٠٢٢ ، ص ١٨٣ .
٢٤.كريم رقولي والعصر نويوة، الأمن السيبراني المتوسطي بين الواقع والرهانات الأمنية مجلة طينة للدراسات العلمية الأكاديمية المجلد ٢، العدد ٢ ٧٤ ٢٠١٩، ص٧٤.
٢٥.مثنى فائق مرعي ، هدى عبد السلام خطاب ، المتغير السيبراني واثره على العلاقات الدولية ، الدار البابلية للدراسات والبحوث العلمية ، مصر ، ٢٠٢٥ .
٢٦.محمد جاسم على الله ، التنافس المعلوماتي بين الولايات المتحدة الامريكية و الصين : دراسة في الامن السيبراني ، عمان ، دار امجد للنشر و التوزيع ، ٢٠٢٢.
٢٧.محمد عادل محمد عسكر، وضع العمليات السيب ارنية في القانون الدولي مع التطبيق علي ممارسة التجسس وقت السلم: دارسة علي ضوء دليل "تالين" بشأن القانون الدولي المطبق علي العمليات السيبرانية ٢٠١٧ – ٢٠١٣.
٢٨.محمد محمود العمري، مدخل إلى الأمن السيبراني، دار زهران للنشر و التوزيع، ٢٠٢٠ .
٢٩.محمد منذر جلال وسرى غضبان غيدان، تكنلوجيا الحروب السيبرانية، دار ومكتبة عدنان للطباعة والنشر والتوزيع، بغداد، ٢٠٢١ ، ص ١٤٣ .
٣٠.محمود مدين، فن التحقيق والثبات في الجرائم الإلكترونية، المصرية للنشر والتوزيع، ٢٠٢٠ .
٣١.مصطفى محمود منجود ، الأبعاد السياسية لمفهوم الامن في الاسلام ، المعهد العالمي للفكر الاسلامي ، القاهرة ، ١٩٩٦.
٣٢.مكتب الأمم المتحدة المعني بالمخدرات و الجريمة، دراسة شاملة عن الجريمة السيبرانية، الأمم المتحدة، نيويورك، ٢٠١٣.
٣٣.منزر رابح ، درويش سعيد ، الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول ، كلية الحقوق جامعة الجزائر ، مجلة صوت القانون ، المجلد الثامن ، العدد ١ ، ٢٠٢١.
٣٤. منشور في الجريدة الرسمية بالعدد ٦٩٠٤ بتأريخ ٩ ذو الحجة ١٤٤١(٣٠ يوليو ٢٠٢٠) .
٣٥.نهلا عبد القادر المومني، الجرائم المعلوماتية ، دار الثقافة للنشر و التوزيع، عمان، ٢٠١٠ .
٣٦.وسن احسان عبد المنعم ، احمد قيس احمد ، تكنولوجيا المعلومات و الامن السيبراني : زمنية التطور وافتراضية الواقع وتخطي الحدود ، دار ومطبعة الرفاة للطباعة و النشر ، ٢٠٢٢.
٣٧.وليد لعايب ، تقييم تجربة نظام الدفع الالكتروني الجزائري في ظل ثورة التكنولوجيا المصرفية:دراسة مقارنة ، مجلة الابحاث و الدراسات التنمية ، جامعة محمد البشير الإبراهيمي برج عر يريج ، الجزائر ، ٢٠٠٨.
٣٨.يوسف حسن يوسف ، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية ، القاهرة ، ط١ ، ٢٠١١ .

المصادر الاجنبية

1.Edward R. McNicholas and Kevin J. Angle, USA, Published in (Cybersecurity 2021: A practical cross-border insight into cybersecurity law), Fourth Edition, editors by Nigel Parker & Overy LLP, Global Legal Group Limited, London, 2020.
2.Mori Hamada, Matsumoto and Hiromi Hayashi, japan, Published in (Cybersecurity 2020: A practical cross-border insight into cybersecurity law), Third Edition, editors by Nigel Parker and Alexandra Rendell Allen & Overy LLP, Global Legal Group Limited, London, 2019.
3.Oona A. Hathaway, Rebecca Crootof, Philip Leviz, Halay Nix,Aileen Nowlan, William Perdue & Julia Spiegel, "The law of Cyber – Attack ", California law review, 2012.
4.Schmitt, M.N, "Computer network attack and the use of force in international law": thoughts on a normative framework. In the Use of Force in International Law, 2017, Vol.27, No. 379.
5.Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to cyber operations, Cambridge University Press, USA, 2017, p 415.
6.James E. Cartwright, Memorandum for Chiefs of the Military Serve. Commanders of the Combatant Commands, Dirs the Joint Staff Directories on Joint Terminology for Cyberspace Operations 5 (No. 2011).
7.Kenneth Boyte, The Evolution of Cyber Warfare in Information Operations Targeting Estonia, the U.S., and Ukraine, Published in (Developments in Information Security and Cybernetic Wars), IGI Global, USA, 2019.
8.Anitta Patience Namanya, Andrea Cullen, Irfan U. Awan and Jules Pagna Disso, The World of Malware: An Overview, IEEE 6th International Conference on Future Internet of Things and Cloud, Spain, 2018.
9.Al-Saidi, Saad Obaid Alwan, and Tamara Kadim Manati. “Transformations of the World Order after the Corona Pandemic COVID-19: The Role of Culture, Science, and the Environment.” *Journal of International Crisis and Risk Communication Research* 7, no. S10 (2024). https://jicrcr.com/index.php/jicrcr/article/view/1154/924.

10.Ali, Inass Abdulsada, and Faieq Hassen Jasem. “Sub-National Governments’ Interactions in International Affairs: An Arab Perspective on Paradiplomacy.” *International Area Studies Review* 27, no. 4 (December 2024). https://iasr.or.kr/_common/do.php?a=full&b=12&bidx=3911&aidx=43280

11.Hameed, Muntasser Majeed. “Political Structure and the Administration of Political System in Iraq.” *Instituto de Estudios Políticos y Derecho Público “Dr. Humberto J. La Roche,” Facultad de Ciencias Jurídicas y Políticas, Universidad del Zulia* 37, no. 65 (2020).

12.Azzaz, Abbas Hashim. “Concept of Conflict and Identifying a Form CR: SIPPABIO Conceptual and Theoretical Framework.” *Res Militaris*. https://resmilitaris.net/menu-script/index.php/resmilitaris/article/view/2624/2195.

13.Shyae, Wafaa Satar, and Hayer Abed Kathem. “The Impact of the Security and Military Institution on Achieving Iraqi National Security after 2014.” *Journal of Positive School Psychology* 6, no. 5 (2022). https://journalppw.com/index.php/jpsp/article/view/6662.

14.Yuval Shany & Tal Mimran, Israel International Regulation of Cyber Operations, The Hebrew University of Jerusalem Faculty of Law Mt. Scopus, Jerusalem, Hebrew University of Jerusalem Legal Studies Research Paper Series No. 22-2,2021.

15.Cristopher D. DeLuca, "The Need for International Laws of War to Include Cyber Attacks InvolvingState and Non-State Actors", 3 Pace International Law Review OnlineCompanion, 2013.

16.Michael N. Schmitt, S.Watts, The Decline of International Humanitarian Law Opinion Juries and the law of Cyber Warfare, 50(2) Texas International Law Journals, United State, 2015.

Sources

First :Arabic sources

1.Cybersecurity Guide , Switzerland, 2006, p. 82.
2.Ahmed Zakaria Al-Basousi , International Efforts to Combat Cyber Attacks on the Energy Sector: Selected Cases, Journal of the Faculty of Economics and Political Science, Cairo University, Volume (24 ،(Issue (4), October 2023.
3.Ahmed Abis Naama Al-Fatlawi , Cyber Attacks: An Analytical Legal Study on the Challenges of Regulating Them Contemporaryly ،Zain Legal and Literary Library, Beirut, 2018.
4.Amal Ben Souilah , European Regional Cooperation in Combating Crime Electronic Crimes (The Budapest Agreement as a Model), a research paper published within the book Electronic Crimes in Islamic Jurisprudence and Positive Law, compiled and coordinated by Abbas Hafsi, issued by the Arab Democratic Center , Berlin , 2022.
5.United Nations Economic and Social Commission for Western Asia, ESCWA Guidelines for Cyber Legislation , Beirut, 2012
6.Indira Araji, Power in Cyberspace , A Modern Chapter of Challenge and Response, Dar Mirza, Beirut, 2019.
7.Ehab Khalifa, The Growing Cyber Threats to Military Institutions, Trends in Events Magazine , Issue (22), 2017.
8.Basem Ali Khraisan , Cyberspace : An Epistemological Introduction , Baghdad, Al-Qanadil Publishing and Distribution House, 2021.
9.Jumaa Ali Bin Jumaa, Arab Security in a Changing World, Madbouli Office, Cairo.
10.Hassanein Saleh Obeid, International Criminal Justice, Its History - Applications - Projects ،Dar Al Nahda Al Arabiya, 1st Edition, Cairo, 1977.
11.Rahmouni Mohamed, Characteristics of Cybercrime and its Areas of Use, Al-Haqiqa Magazine, Issue 41, 2018.
12.Salem Mohamed Suleiman Al-Awjali , Provisions of Criminal Responsibility for International Crimes in National Legislations, PhD Thesis, Faculty of Law, Ain Shams University, 1997, p. 421.
13.Saeed Darwish, Cyber Wars and their Impact on Human Rights, A Study in Light of the Provisions of the "Tallinn" Guide, Algerian Journal of Legal, Economic and Political Sciences, Volume 54, Issue 5, 2017, p. 181.
14.Sulaiman Ahmed Fadl, Legislative and Security Confrontation of Crimes Arising from the Use of the International Information Network, Dar Al Nahda Al Arabiya, Egypt.٢٠٠٧ ،
15.Sharifa Kelaa, Cybersecurity and the challenges of espionage and electronic intrusions into countries via cyberspace , Journal of Law and Humanities, University of Djelfa, Volume 1, Issue 1, 2022.
16.Samuel Even and **David** Siman Tov ، " War in Cyberspace : Concepts, Trends, and Implications for Israel " Institute for National Security Studies, Memorandum No. 109, Tel Aviv, 2011.
17.Adel Abdul Aziz Saleh Al-Rashid, Evidence of Cybercrime and its Impact on Proof, Dar Kunooz Ishbiliya for Publishing and Distribution, Riyadh, Kingdom of Saudi Arabia, 2017.
18.Amer Abdel Fattah Al-Jumard , Sovereignty, Al-Rafidain Journal of Law, University of Mosul, Issue 1, 2019.

19.Abdelwahab Miliani, Information Security in the Electronic Business Environment, PhD Thesis, Faculty of Law and Political Science, University of Tlemcen ،2016-2017 .
20.Ammar Basem Al-Husseini, Computer and Internet Crimes (Cybercrimes), Zain Legal Publications, Beirut (Lebanon), 2017.
21.Ghanem Mardi Al-Shammari, Cybercrimes, Dar Al-Thaqafa, Jordan, 2016.
22.Fahd Abdullah Al-Obaid Al-Azmi, Cybercrime Procedures, Dar Al-Jami'a Al-Jadeeda ،٢٠١٦ ،Egypt.
23.Qasim Muhammad Abd, Cyber Wars and the Future of International Security, PhD Thesis ،Al-Nahrain University, Department of International Politics, 2022, p. 183.
24.Karim Ragouli and Al-Asr Nouioua , Mediterranean Cybersecurity between Reality and Security Stakes, Tina Journal for Academic Scientific Studies, Volume 2, Issue ،٢٠١٩ ،٧٤ p. 74.

25.Muthanna Faiq Mar'i, Huda Abdel Salam Khattab, The Cyber Variable and its Impact on International Relations, The Babylonian House for Scientific Studies and Research, Egypt, 2025.
26.Mohammed Jassim Ali Allah, Information Competition between the United States of America and China: A Study in Cybersecurity , Amman, Amjad Publishing and Distribution House, 2022.
27.Mohammed Adel Mohammed Askar, The Status of Cyber Operations in International Law with Application to Peacetime Espionage Practices: A Study in Light of the Tallinn Manual on International Law Applicable to Cyber Operations 2013-2017.
28.Mohammed Mahmoud Al-Omari, Introduction to Cybersecurity , Zahran Publishing and Distribution House, 2020.
29.Mohammed Munther Jalal and Sari Ghadban Ghaidan , Cyber Warfare Technology , Adnan House and Library for Printing, Publishing and Distribution, Baghdad, 2021, p. 143.
30.Mahmoud Madin, The Art of Investigation and Proof in Cybercrimes, Egyptian Publishing and Distribution, 2020.
31.Mustafa Mahmoud Manjoud, The Political Dimensions of the Concept of Security in Islam ،International Institute of Islamic Thought, Cairo, 1996.
32.United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime , United Nations, New York, 2013.
33.Munzer Rabah, Darwish Said, The Legal Nature of Cyber Attacks that Occur Between States, Faculty of Law, University of Algiers, Voice of Law Journal, Volume 8 ،Issue 1, 2021.
34. Published in the Official Gazette, Issue No. 6904, dated 9 Dhu al-Hijjah 1441 (July 30, 2020.(
35.Nahla Abdul Qader Al-Momani, Cybercrimes , Dar Al-Thaqafa for Publishing and Distribution , Amman, 2010.
36.Wasan Ihsan Abdul-Munim, Ahmed Qais Ahmed, Information Technology and Cybersecurity : The Timeline of Development, Virtual Reality and Crossing Boundaries, Al-Rafaa Printing and Publishing House, 2022.
37.Walid Laaïb, Evaluating the Algerian Electronic Payment System Experience in Light of the Banking Technology Revolution: A Comparative Study, Journal of Research and Development Studies ،Mohamed El Bachir El Ibrahimi University ، Bordj Bou Arreridj , Algeria, 2008.
38.Youssef Hassan Youssef, International Internet Crimes, National Center for Legal Publications, Cairo, 1st Edition.٢٠١١ ،

Foreign sources

1.Edward R. McNicholas and Kevin J. Angle, USA, Published in (Cybersecurity 2021: A practical cross-border insight into cybersecurity law), Fourth Edition, editors by Nigel Parker & Overy LLP, Global Legal Group Limited, London, 2020.
2.Mori Hamada, Matsumoto and Hiromi Hayashi, japan, Published in (Cybersecurity 2020: A practical cross-border insight into cybersecurity law), Third Edition, editors by Nigel Parker and Alexandra Rendell Allen & Overy LLP, Global Legal Group Limited, London, 2019.
3.Oona A. Hathaway, Rebecca Crootof, Philip Leviz, Halay Nix,Aileen Nowlan, William Perdue & Julia Spiegel, "The law of Cyber – Attack ", California law review, 2012.
4.Schmitt, M.N, "Computer network attack and the use of force in international law": thoughts on a normative framework. In the Use of Force in International Law, 2017, Vol.27, No. 379.
5.Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to cyber operations, Cambridge University Press, USA, 2017, p 415.
6.James E. Cartwright, Memorandum for Chiefs of the Military Serve. Commanders of the Combatant Commands, Dirs the Joint Staff Directories on Joint Terminology for Cyberspace Operations 5 (No. 2011).
7.Kenneth Boyte, The Evolution of Cyber Warfare in Information Operations Targeting Estonia, the U.S., and Ukraine, Published in (Developments in Information Security and Cybernetic Wars), IGI Global, USA, 2019.
8.Anitta Patience Namanya, Andrea Cullen, Irfan U. Awan and Jules Pagna Disso, The World of Malware: An Overview, IEEE 6th International Conference on Future Internet of Things and Cloud, Spain, 2018.
9.Al-Saidi, Saad Obaid Alwan, and Tamara Kadim Manati. “Transformations of the World Order after the Corona Pandemic COVID-19: The Role of Culture, Science, and the Environment.” *Journal of International Crisis and Risk Communication Research* 7, no. S10 (2024). https://jicrcr.com/index.php/jicrcr/article/view/1154/924.
10.Ali, Inass Abdulsada, and Faieq Hassen Jasem. “Sub-National Governments’ Interactions in International Affairs: An Arab Perspective on Paradiplomacy.” *International Area Studies Review* 27, no. 4 (December 2024). https://iasr.or.kr/_common/do.php?a=full&b=12&bidx=3911&aidx=43280
11.Hameed, Muntasser Majeed. “Political Structure and the Administration of Political System in Iraq.” *Instituto de Estudios Políticos y Derecho Público “Dr. Humberto J. La Roche,” Facultad de Ciencias Jurídicas y Políticas, Universidad del Zulia* 37, no. 65 (2020).
12.Azzaz, Abbas Hashim. “Concept of Conflict and Identifying a Form CR: SIPPABIO Conceptual and Theoretical Framework.” *Res Militaris*. https://resmilitaris.net/menu-script/index.php/resmilitaris/article/view/2624/2195.
13.Shyae, Wafaa Satar, and Hayer Abed Kathem. “The Impact of the Security and Military Institution on Achieving Iraqi National Security after 2014.” *Journal of Positive School Psychology* 6, no. 5 (2022). https://journalppw.com/index.php/jpsp/article/view/6662.
14.Yuval Shany & Tal Mimran, Israel International Regulation of Cyber Operations, The Hebrew University of Jerusalem Faculty of Law Mt. Scopus, Jerusalem, Hebrew University of Jerusalem Legal Studies Research Paper Series No. 22-2,2021.
15.Cristopher D. DeLuca, “The Need for International Laws of War to Include Cyber Attacks InvolvingState and Non-State Actors”, 3 Pace International Law Review OnlineCompanion, 2013.

16.Michael N. Schmitt, S.Watts, The Decline of International Humanitarian Law Opinion Juries and the law of Cyber Warfare, 50(2) Texas International Law Journals, United State, 2015.