

جرائم الامن السيبراني في ضوء التشريعات الوطنية والمواثيق الدولية -دراسة تحليلية-

Doi: 10.23918/ilic9.35

م.م. أردلان عبدالرحمن محمد
جامعة گرميان/ كلية القانون

ardalan.abdallah@garmian.edu.krd

م.م. كوچهر محمد احمد
جامعة حلبجة/ كلية القانون والإدارة/ قسم قانون

kocher.ahmad@uoh.edu.iq

م.م. هورامان جلال احمد
جامعة حلبجة/ كلية القانون والإدارة/ قسم قانون
hawraman.jalal@uoh.edu.iq

Cybersecurity Crimes in Light of National Legislation and International Conventions
Asst. Lect. Kocher Mohammed Ahmed Asst. Lect. Ardalan Abdulrahman Muhammad
University of Halabja/ College of Law Garmian University / Faculty of Law
and Administration/ Department of Law
Asst. Lect. Hawraman Jalal Ahmed
University of Halabja/ College of Law and Administration/ Department of Law

المخلص

عموماً ان الامن ذات أهمية كبيرة للمجتمع والدولة، وهو مفهوم ديناميكي يتطور مع تطور الظروف والأدوات المحلية والإقليمية والدولية، فالدولة لا تتوقف عند حد معين من الامن او الوصول الى قدر معين من الاستقرار، وانما تستمر لتحقيق الأفضل خوفاً من التهديدات في المستقبل، لذلك يعد الامن حالة نسبية وغير مطلقة، وان لفظ السيبراني اشتق اصل كلمة من اللغة الانكليزية من الكلمة cyber والتي تعني شبكات الاتصال والانترنت وشبكات المعلومات والانظمة الرقمية المختلفة، وان الأمن السيبراني هو حزمة عمليات وإجراءات تتوخى تأمين وحماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من الهجوم أو التلف أو السرقة والوصول غير المصرح به، وكذلك من التعطيل أو العرقلة في الخدمات التي تقدمها، وفيما يخص تحديات الامن السيبراني يجد بأن هناك عدة من التحديات امام الامن السيبراني ومنها: ضعف البنى التحتية، ضعف التخطيط التنموي، ضعف الأمن الالكتروني، يحمل مفهوم الأمن أبعاداً كثيرة، ومن أبرزها: البعد العسكري، البعد الإقتصادي، البعد الاجتماعي، البعد القانوني، ولاشك فيه ان لجرائم الامن السيبراني اركان الثلاث والمتمثلة بكل من: الركن المادي والركن المعنوي والركن المفترض.

تعتبر اتفاقية بودابست اول وابرز اتفاقية تختص بالجرائم السيبرانية وهي اوروبية المنشأ ولكنها ذات طابع عالمي، وقعت عليها (٢١) دولة، ففي ذات السياق يلاحظ بأن ذكر هذه الاتفاقية على تسمية مجموعة من الأعمال الإرهابية عبر الوسائل السيبرانية غير المشروعة، وبصدد الإطار التشريعي لمواجهة جرائم الأمن السيبراني وسلامتها في العراق واقليم كردستان وعند تتبع موقف المشرع العراقي والكوردستاني، نلاحظ خلو نظام التشريع الجنائي العراقي والكوردستاني من أي قانون جنائي خاص بمكافحة جرائم الأمن السيبراني، الا ان عمل المشرع العراقي والكوردستاني على اتخاذ عدد من الاجراءات بصورة غير مباشر لمواجهة جرائم الأمن السيبراني وجرائم امن الدولة وسلامتها في العراق، وعلى سبيل المثال: قانون العقوبات العراقي النافذ، قانون مكافحة الارهاب في العراق، قانون جهاز مكافحة الارهاب العراقي، قانون منع إساءة استعمال أجهزة الاتصالات في اقليم كردستان -العراقي، قانون مكافحة الإرهاب في اقليم كردستان -العراقي.

الكلمات المفتاحية: الامن السيبراني، الأمن الوطني، جرائم الامن السيبراني، تحديات الامن السيبراني، التشريعات الوطنية، الاتفاقيات الدولية.

Abstract

In general, security is of great importance to society and the state, and it is a dynamic concept that develops with the development of local, regional and international conditions and tools. The state does not stop at a certain level of security or reach a certain level of stability, but rather continues to achieve the best for fear of threats in the future. Therefore, security is a relative and not absolute state. The word cyber is derived from the English word cyber, which means communication networks, the Internet, information networks and various digital systems. Cyber security is a package of operations and procedures that aim to secure and protect networks, computers, programs and data from attack, damage, theft and unauthorized access, as well as from disruption or obstruction of the services they provide. Regarding the challenges of cyber security, it is found that there are several challenges facing cyber security, including: weak infrastructure, weak development planning, weak electronic security. The concept of security has many dimensions, the most prominent of which are: the military dimension, the economic dimension, the social dimension, and the legal dimension. There is no doubt that cyber security crimes have three pillars, represented by each of: the material pillar, the moral pillar and the supposed pillar. The Budapest Convention is the first and most prominent convention on cybercrimes. It is European

in origin but has a global character. It has been signed by (21) countries. In the same context, it is noted that this convention stipulated the designation of a group of terrorist acts through illegal cyber means. Regarding the legislative framework for confronting cybersecurity crimes and their safety in Iraq and the Kurdistan Region, and when following the position of the Iraqi and Kurdish legislators, we notice that the Iraqi and Kurdish criminal legislation system is devoid of any criminal law specific to combating cybersecurity crimes. However, the Iraqi and Kurdish legislators have taken a number of measures indirectly to confront cybersecurity crimes and state security and safety crimes in Iraq. For example: Iraqi Penal Code, Anti-Terrorism Law in Iraq, Iraqi Counter-Terrorism Service Law, Law on Preventing the Misuse of Communications Devices in the Kurdistan Region - Iraq, Anti-Terrorism Law in the Kurdistan Region - Iraq.

Keywords: cybersecurity, national security, cybersecurity crimes, cybersecurity challenges, National legislation, international agreements.

پوخته

بەگشتی ئاسایش بۆ کۆمەڵگا و دەوڵەت گرنگیەکی گەورە هەیە و چەمکی دینامیکیە کە لەگەڵ پەرەسەندنی هەلومەرج و ئامرازەکانی ناوخرۆی و ناوچەیی و نێودەوڵەتی گەشە دەکات، کەواتە ئاسایش دۆخێکی رێژمیە ئەکە رەها، وە وشەیی سایبەر سەرچاوەکە لە زمانێ ئینگلیزییە وەرگیراوە کە بە مانای تورەکانی پەيوەندی و ئینتەرنێت و تورەکانی زانیاری و سیستەمە جۆراوجۆرەکانی دیجیتاڵ دیت، وە هەرچی ئاسایشی سایبەر ئەوە ئەو رێوشوێنە دەگرتەوه کە بۆ پاراستنی تورەکان، کۆمپیوتەرەکان، بەرنامەکان و داتاكان دادەنرێت لەدژی هەر زیان، دزی و دەستگەشتنێکی رێگەپێندراو، هەروەها پاراستنیانە لە پچران و رێگرتنە لە خزمەتگۆزارییەکان کە پێشکەش دەکەن، وە سەبارەت بە ئاستەنگەکانی ئاسایشی ئەلیکترۆن، دەرکەوتووێ کە چەندین ئاستەنگ بۆ ئاسایشی ئەلیکترۆنی بوونی هەیە، لەوانە: ئاستەنگی ژێرخانی نابووری، ئاستەنگی پلانی پەرمێدان، ئاستەنگی ئاسایشی سایبەر، وە چەمکی ئاسایشی سایبەر چەندین رەهەندی هەیە، دیارترینیان: رەهەندی سەربازی، رەهەندی نابووری، رەهەندی کۆمەڵایەتی، رەهەندی یاسایی، وەگومانی تێدا نییە کە تاوانەکانی ئاسایشی ئەلیکترۆنی سێ پایە هەیە: پایە ماددی، پایە مەعنەوی، و پایە تایبەتی.

وە پەیماننامەیی بوداپێست یەکم و دیارترین پەیماننامەیی تاوانی ئەلیکترۆنی یە، وە خاوەنی سەروشتیکی جیهانییە، وە لە لایەن (٢١) وڵاتەوه واژۆکراوە، وە لە هەمان چوارچێوەدا ئامارە بەوه کراوە کە ئەم رێکەوتننامەییە ناوی کۆمەڵێک کردووی تیرۆری ئەلیکترۆنی دیاری کردووە، وەگومانی تێدا نییە کە چوارچێوەیی یاسایی تاوانەکان بۆ رووبەر و بوونەوهی تاوانەکانی ئاسایشی ئەلیکترۆنی و دانیابوون لە سەلامەتی واتە دەستتێوەردانی یاسایی لەرێگەیی بەتاوانکردنی ئەو کارانەیی رێکخراوەکان و خەڵک ئەنجامی دەدەن لەگەڵ دیاریکردنی سزاكان بۆ ئەو کردار و رەفتارانە و رووبەر و بوونەوهیان، وە لەسەر ئاستی ناوخرۆی و تایبەت بە تاوانەکانی ئاسایشی ئەلیکترۆنی پێویستە رووبەر و بوونەوهی یاسایی گونجاویان لەدژ بگێتە بەر، ئەمەش وەک وەلامدانەوهیەکی پێویست بۆ مامەڵەکردن لەگەڵ ئەم تاوانانە، بەجۆریک لەگەڵ پێشکەوتنەکانی بواری تاوانی ئەلیکترۆنی بگونجیت، ئەمەش لەرێگەیی دەرچوواندنی یاسای پێویست بۆ رووبەر و بوونەوهی تاوانەکانی ئاسایشی ئەلیکترۆنی، وە سەبارەت بە چوارچێوەیی یاسایی بۆ رووبەر و بوونەوهی تاوانەکانی ئاسایشی ئەلیکترۆنی لەعێراق و هەریە کوردستان، تێبینی ئەوە دەکەیت کە سیستەمی یاسای تاوانکاری لە عێراق و کوردستان هیچ جۆرە یاسایەکی تاوانکاری بۆ بەرەنگاربوونەوهی تاوانەکانی ئاسایشی ئەلیکترۆنی دەرەچوواندووە، بەلام بەشێوازیکی ناراستەوخۆ چەن یاسایەکی بوونیان هەیە بۆ رووبەر و بوونەوهی تاوانەکانی ئاسایشی ئەلیکترۆنی و تاوانەکانی ئاسایشی نیشتمانی، بە نمونە: یاسای سزادانی عێراقی، یاسای بەرەنگاربوونەوهی تیرۆر لە عێراق، یاسای دەرگای دژە تیرۆری عێراقی، یاسای قەدەغەکردنی خراب بەکارهێنانی ئامێرەکانی پەيوەندی کردن لە هەریە کوردستان -عێراق، یاسای بەرەنگاربوونەوهی تیرۆر لە هەریە کوردستان-عێراق.

کلیە ووشە: ئاسایشی سێبرانی، ئاسایشی نەتەوهیی، تاوانەکانی ئاسایشی سێبرانی، ئاستەنگەکانی ئاسایشی سێبرانی، یاسا نیشتمانیەکان، رێکەوتننامە نێودەوڵەتیەکان.

المقدمة

إن الانفتاح الذي شهده العراق وبضمنه إقليم كوردستان في تكنولوجيا المعلومات والاتصالات في ظل التطور التكنولوجي العالمي تزامن مع عدم وجود بنية تحتية متكاملة ومؤمنة لأنظمة الامن السيبراني سواء أكانت أمنية أم مصرفية أم شخصية، وان هذا الامر أدى إلى أن يكون العراق وبضمنه إقليم كوردستان ساحة مفتوحة لظهور جرائم الامن السيبراني، إذ يلاحظ بأن تزايدت المخاطر على الامن السبراني في العراق وبضمنه إقليم كوردستان بشكل كبير، لذلك يجد بأن تطور مفهوم الامن السيبراني في ظل تطور تكنولوجيا المعلومات حتى يمكن اعتبار تحدي الامن السيبراني أعلى تحديات وعراق الامن الوطني العراقي والكوردستاني، ومن ثم يعتبر جرائم الامن السيبراني الهاجس والشبح المرعب الذي تعيشه كل الدول وتتخوف منه، إذ لا يكاد يمر يوماً تقريباً دون أن تقع نوع من انواع جرائم الامن السيبراني في مكان ما في الدول العالم وان تأثير تلك الجرائم هو تأثير حسي وواقعي على الامن بأكملها إلى حد يمكن القول مع انها تعرض الافراد ومرافق الدولة للخطر المباشر، لذا يمكن القول بأن لجرائم الامن السيبراني آثار عدة على الأمن الوطني على وجه العموم، إذ تؤثر هذه الجرائم على بناء المجتمع، وبالتالي اهتم المجتمع الدولي بوضع آليات مختلفة لمحاربة ومكافحة جرائم الامن السيبراني، إذ بدأ المجتمع الدولي يولي هذه الظاهرة اهتماماً خاصاً من خلال اصدار جملة من المواثيق الدولية ومن أبرزها معاهدة بودابست لمكافحة الجرائم المعلوماتية، ومن ثم اهتم الدول العالم بإصدار العديد من القوانين الجنائية لمعالجة جرائم الامن السيبراني التي باتت من الضروري التفات المشرع إليها كونها تعد طوائف جديدة من السلوكيات التي تؤثر سلباً على الأمن السيبراني وذلك بسبب انتشار ظاهرة العولمة والتقدم التكنولوجي وما رافقهما من ظهور جرائم مستحدثة التي لم تتم معالجتها من قبل.

أهداف البحث

يسعى البحث الى التأكيد على مفهوم جرائم الامن السيبراني وبنیان القانوني لجرائم الامن السيبراني باعتباره احد المواضيع الحديثة التي اخذت اهتماماً واسعاً من لدن الباحثين، والوقوف على طرق مكافحة تلك الجرائم ضمن القوانين الوطنية في العراق وبضمنه إقليم كردستان وكذلك ضمن المواثيق الدولية.

أهمية البحث

يتبلور أهمية هذه الدراسة في مايلي:

١. ان الأمن السيبراني اصبح من اهم قضايا الأمن الوطني لأي دولة بحكم علاقته المباشرة بمؤسساتها وبنيتها التحتية ومواطنها، وان اي تعرض بالهجمات السيبراني لها سوف يؤثر مباشرة بأمنها الوطني بل سوف يؤدي الى خسائر الكبيرة، وفيما يتعلق بالعراق وبضمنه إقليم كردستان زادت أهمية الأمن السيبراني بحكم الاستخدام الواسع للفضاء السيبراني.
٢. أن وسائل شبكات الإنترنت واجهزت الحاسوب جاءت وليدة الواقع العملي والعلمي، لذلك أضحت الحاجة إلى دراسة هذه الجرائم من الناحية القانونية في ضوء القوانين الوطنية في العراق وبضمنه إقليم كردستان وكذلك في ضوء المواثيق الدولية.
٣. ان هناك آليات حماية الأمن في مواجهة جرائم الامن السيبراني، وكلما كان هذه الآليات منسجمة مع نظام التجريم والعقاب كلما كان الامن اكثر استقراراً، وتتجسد بالآليات الدولية والوطنية الفعالة لحماية الأمن في مواجهة جرائم الامن السيبراني، إذ ان أهمية هذه الدراسة تتبلور في استظهار مدى فعالية المواثيق الدولية في حماية الأمن الدولة في مواجهة جرائم الامن السيبراني.

إشكالية البحث

ان اشكالية البحث تتمثل في تساؤل مفاده كيف يؤثر جرائم الامن السيبراني على الأمن الوطني، ويتفرع من هذا التساؤل تساؤلان هما: ماهي الاخطار والتهديدات الناجمة عن جرائم الامن السيبراني وهل يستطيع العراق وبضمنه إقليم كردستان من تحقيق الامن السيبراني كبعد جديد في إستراتيجية الأمن الوطني؟ وكذلك تكمن اشكالية البحث بالجرائم الامن السيبراني فيما مدى كفاية الحماية القانونية الجنائية على صعيدي الدولي والوطني لمواجهة الجرائم الأمن السيبراني؟ وبالتالي يلاحظ بأن يعاني العراق وبضمنه إقليم كردستان من عدم وجود سياسة تشريعية واضحة، خصوصاً في العراق وبضمنه إقليم كردستان أن الاجهزة التي تعنى بالامن السيبراني موزعة بين جهاز الامن الوطني والمخابرات العامة ووزارة الداخلية وجهاز مكافحة الارهاب، ولا توجد هيئة مستقلة للأمن السيبراني.

منهجية البحث

لغرض دراسة موضوع البحث اتبعنا استعمال المنهج التحليلي وذلك من خلال دراسة وتحليل احكام الوارد ذكره في التشريعات المحلية في العراق وبضمنه إقليم كردستان والمواثيق الدولية قدر تعلقها بموضوع البحث مع تحليل الآراء الفقهية المتعلقة بموضوع بحثنا هذا.

هيكلية البحث

بغية الاحاطة بموضوع البحث سنقسمه الى مبحثين كما يأتي:

المبحث الأول: الإطار المفاهيمي لجرائم الامن السيبراني

المبحث الثاني: سبل مكافحة جرائم الأمن السيبراني في التشريعات الوطنية والدولية

المبحث الأول**الإطار المفاهيمي لجرائم الامن السيبراني**

من اجل دراسة مسألة الإطار المفاهيمي لجرائم الامن السيبراني سنقسم هذا المبحث الى مطلبين، كما يأتي:

المطلب الأول**ماهية الامن السيبراني**

لغرض البحث عن مسألة ماهية الامن السيبراني سنقسم هذا المطلب الى فرعين، كما يأتي:

الفرع الاول**تعريف الامن السيبراني وتحدياتها**

ان الامن في اللغة جاءت لدلالة عدة كلمات ومنها الامن او الأمان او الأمانة وهو ضد الخوف^(١)، والامن كلمة لها نفس المعنى للامان او الطمأنينة او الحماية وهي مساوية للتفادي المخاطر، وجاءت كلمة الامن بدلالة الحد من الخوف بمعنى الشعور بحالة الطمأنينة فيقال اطمأن ولم يخف أي الامن^(٢)، واما بالنسبة للفظ (السيبراني) يجد بأن أساس نشأة كلمة السيبراني (Cybernetic) ارتبطت باللغة اليونانية والذي يعني التوجيه والسيطرة و مأخوذة من كلمة (Kybernetes) أي الفرد الذي يدير السفن البحرية، اذ تستعمل للتحكم وبذلك بإمكاننا القول ان السيبرانية هي التحكم عن بعد، فهي عندما تأتي مع كلمة أخرى تعني التحكم بها او ادارتها كما في الأمن السيبراني^(٣).

والمقصود بالأمن السيبراني هو تلك عمليات وإجراءات يؤدي الى ضمان وحماية الشبكات وأجهزة الحاسوب والبرامج والمعلومات من الهجوم أو التلف أو السرقة والوصول غير المسموح به، وكذلك من التعطيل في الخدمات التي تقدمها^(٤)، او أنه حماية الأصول المعلوماتية من خلال معالجة التهديدات التي تتعرض لها المعلومات التي تتم معالجتها وتخزينها ونقلها بواسطة أنظمة المعلومات المتداخلة بين الشبكات^(٥)، أو هو مجموعة من الآليات والإجراءات والوسائل والأطر التي تهدف إلى حماية البرمجيات وأجهزة الكمبيوتر من مختلف الهجمات الإخترقات التهديدات السيبرانية التي قد تهدد الأمن القومي للدول، أو انه يكون الأمن السيبراني وسيلة عسكرية استراتيجية

(١) ابن منظور، لسان العرب، ج ١، مطبعة الادب العربي، بيروت، ١٩٨٥، ص ٢٧.

(٢) محمد بن ابي بكر الرازي، مختار الصحاح، ط ١، بيروت، دار الكتب العربية، ١٩٨١، ص ٢٦.

(٣) اسراء شريف، الأمن السيبراني الصيني، دراسة في الدوافع والتحديات، مجلة قضايا سياسية، العدد ٦٥، ص ٣٥.

(٤) منى الأشقر جبور، الأمن السيبراني، التحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، ٢٠١٢، ص ٣.

(٥) د. أسامة زيد محمد منوخ، تأثير الأمن السيبراني على فاعلية نظام الرقابة الداخلية (نموذج مقترح)، المجلة العراقية للبحوث الانسانية والاجتماعية والعلمية، العدد ١٢، ٢٠٢٤، ص ٤٦٦.

تستخدمها الدول والمواطنون بالشكل الذي لا يمكن اغفاله ان الحرب الافتراضية أصبحت جزء من الاستراتيجيات المعاصرة للدول وفي الصراعات المسلحة فيما بينها^(١).

وفيما يخص بتحديات الامن السيبراني يجد بأن هناك عدد من التحديات امام الامن السيبراني ومنها:

١. ضعف البنى التحتية

يقصد بالبنية التحتية (Infrastructure) البنية المادية والتنظيمية الأساسية التي تشكل مجموعة من المرافق والأنظمة المترابطة التي تساهم في النهوض بالمجتمع والاقتصاد والنمو وتطوير الحياة العامة نحو الأفضل، وذلك من خلال توفير الوسائل اللازمة التي تخدم الأفراد والمجتمعات والأعمال والمؤسسات، وخلق بيئة مناسبة للاستثمار^(٢).

ومن ثم تعد ضعف البنى التحتية كأحد تحديات الامن السيبراني من اهم القضايا التي تواجه العراق وفي ضمنه اقليم كردستان في الوقت الحالي، حيث ان في ظل التطور التكنولوجي السريع وانتشار استخدام الانترنت بشكل كبير، أصبحت الهجمات السيبرانية تشكل تهديداً حقيقياً على مختلف القطاعات سواء كانت حكومية أو خاصة، ولدى تقييم للبنية التحتية الرقمية والأمنية في العراق وفي ضمنه اقليم كردستان -العراق يجد بأن مازالت في طور النمو على الرغم من وجود بعض التحسينات في السنوات الاخيرة، حيث تفتقر الى التجهيزات والتقنيات الحديثة اللازمة لمواجهة الهجمات السيبرانية بشكل فعال، ويعد نقص التكنولوجيا الحديثة اذ ان العراق وفي ضمنه اقليم كردستان يواجه نقصاً كبيراً في مجالات المتعلقة بالامن السيبراني، العديد من المؤسسات تعتمد على تقنيات قديمة وغير محدثة، مما يجعلها عرضة للهجمات السيبرانية، وهناك نقص في مراكز البيانات المجهزة بشكل جيد هذه الظروف تجعل من الصعب تطبيق حلول أمنية متقدمة وحماية البيانات بشكل فعال^(٣).

٢. ضعف التخطيط التنموي

يعد التخطيط من المهام الرئيسية للقيادة الإستراتيجية، وعنصراً مهماً لثبات منظومة الأمن الوطني، إذ إن التخطيط يرتبط بالمستقبل واستخدام علم المستقبل والنظريات والأساليب العلمية الحديثة التي تساعد على ذلك، فهو عملية تقوم بها المؤسسات الإستراتيجية من أجل تحديد الأهداف المستقبلية ومواجهة التحديات، واتخاذ القرارات بشأن تخصيص مواردها لردع هذه التحديات وتحقيق الأهداف المنشودة، ونتيجة للتداعيات والانعكاسات السلبية التي تمس مسار عمل المؤسسات العراقية والكوردستانية الإستراتيجية، ويعاني العراق واقليم كردستان اليوم من حالة ضعف في منظومة التخطيط الاستراتيجي، وهو ما انعكس سلباً على عمل معظم مؤسسات الدولة العراقية والكوردستانية ونتائجها التي باتت تعاني من ضعف في التخطيط الاستراتيجي الذي يمثل أحد السمات الرئيسية للعصر الحديث، وأساس عمل المؤسسات الحكومية لأجل تحقيق الأهداف الوطنية المنشودة، لذلك فإنه يتطلب قدرات خاصة على التوقع والتنبؤ فيما يخص المستقبل، أن العراق واقليم كردستان في هذه المدة الحساسة يحتاج إلى رؤية تخطيطية يقع على عتقها حل المعضلات المالية والأمنية التي باتت تعصف بالمنظومة المؤسساتي للعراق والكوردستان، من خلال وضع برنامج حكومي ثابت الأركان مع أساليب تخطيطية واجب إتباعها لمواجهة التحديات المرحلة القادمة، بمعنى التفكير والتخطيط قبل الأداء بوضع حلول لمشكلات العراقية والكوردستانية لتحسين أداء المنظومة الإستراتيجية الشاملة في ضوء الإمكانيات المتاحة^(٤).

٣. ضعف الأمن الإلكتروني

تتمثل التهديدات السيبرانية بتحديات غير مرئية تؤثر على منظومة الأمن الوطني العراقي والكوردستاني، ومن الملاحظ أن أكثر المؤسسات العراقية والكوردستانية تتعاقد لتجهيز معلوماتها من أقمار صناعية ذات مورد خدمة واقع خارج الحدود العراقية الذي يؤدي إلى مرور تلك المعلومات في خوادم دول الاجنبية، ورجوعها إلى العراق إذ يشكل هذا الإجراء خرقاً لأمن المعلومات العراقي والكوردستاني^(٥).

الفرع الثاني أبعاد الأمن السيبراني

يحمل مفهوم الأمن أبعاداً كثيرة، ومن ابرزها:

أولاً: البعد العسكري

تتمثل الميزة الأساسية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء السيبراني، بما يسمح باتخاذ القرارات والقدرة على تحديد الأهداف وتدميرها، لقد كانت البدايات الأولى للانترنت في بيئة عسكرية وتزايدت بشكل متسارع وذلك لتتنقل في سياق آخر نحو الاوساط العلمية والاكاديمية المختلفة، وكذلك ابحاث تخدم القدرات العسكرية، وتمثل الميزة النسبية للامن السيبراني في بعده العسكري عن طريق قدرة القوة السيبرانية على ربط الوحدات العسكرية ببعضها البعض عبر العالم الافتراضي، وهذا ما يسهل عملية تبادل المعلومات والذي ينعكس ايجاباً على تحقيق الاهداف العسكرية العليا^(٦).

ثانياً - البعد الاقتصادي:

تظهر أهمية الأمن السيبراني بشكل أوسع وأكبر في المجال الإقتصادي لأن الفضاء السيبراني أصبح أساساً للتعاملات التجارية والمالية والإقتصادية وأصبح الحاسوب أداة لتسيير الصناعة والإقتصاد وهذا يستدعي الحرص على تحقيقه، ويرتبط الأمن السيبراني بالإقتصاد ارتباطاً وثيقاً فإعتماد إقتصاد المعرفة يتصل وثيقاً بتكنولوجيا والاتصالات كما بالقيمة التي تمثلها لبيانات المتداولة وتتيح تقنيات

(١) نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني التهديد المتصاعد لأمن الدول، مجلة مركز بابل للدراسات الانسانية، المجلد ٨، العدد ٢ ص ١٥٦.

(٢) د. زهير خضير عباس الزبيدي ود. ظفر عبد مطر التميمي، العراق والأمن السيبراني، الفرص والتحديات، ص ١٠-١١.

Michael krepon, Julia Thompson, deterrence and Sino-American relations, united states, stimson-center, 2013, P.15.

(٣) محمد عبد الفتاح احمد، التحديات الامنية السيبرانية في العراق، تحليل استراتيجي، مجلة الدراسات الامنية، العدد ٥، ٢٠١٩، ص ١٧.

(٤) د. زهير خضير عباس الزبيدي ود. ظفر عبد مطر التميمي، العراق والأمن السيبراني، الفرص والتحديات، ص ١٠-١١.

(٥) د. زهير خضير عباس الزبيدي ود. ظفر عبد مطر التميمي، المصدر السابق، ص ١٣.

(٦) محمود علي عبد الرحمن، أسامة فاروق مخيمر، الفضاء الإلكتروني وأثره على مفاهيم القوة والأمن والصراع في العلاقات الدولية، مجلة كلية السياسة والإقتصاد جامعة محمد البشير الإبراهيمي، برج بوغريز، المجلد السادس عشر العدد الخامس عشر، الجزائر، ٢٠٢٢، ص ٤٣٨.

المعلومات تعزيز التنمية الاقتصادية للعديد من البلدان من فرص الاستخدام التي تقدمها الشركات الدولية الكبرى ولاننسى حلول عصر المال الإلكتروني ضمن بيئة تقنية متحركة كوجود المحفظة الإلكترونية وإصدار بطاقات الدفع الإلكتروني^(١).

ثالثاً: البعد الاجتماعي:

يأخذ الأمن السيبراني شكلاً مهماً ومختلفاً تماماً في المجال الاجتماعي، فقد أصبحت مواقع التواصل الاجتماعي أداة إتصال عالمية بين البشر تمد بالمعلومات والأفكار ولكن من ناحية أخرى قد عرضت أخلاق المجتمع للخطر من ناحية أنه يمس هوية الأشخاص ويهدد السلم الاجتماعي وعليه لابد من العمل أولاً على تكريس مفهوم الأمن السيبراني ثم توعية الأفراد بمخاطر إختراقه، ويرتبط الأمن السيبراني بشبكات التواصل الاجتماعي التي تسمح وتتيح جمع المعلومات المتعلقة بالأفراد بالخصوص بما أصبح يعرف " الهندسة الاجتماعية" من خلال معرفة تطلعاتهم السياسية والاجتماعية واستغلالها لتحقيق تطلعاتهم، وتعد الشبكة الدولية للمعلومات مجاًلاً مفتوحاً لجميع الأشخاص، حيث يمكن لجميع المتعاملين السيبرانيين ان يستفيدوا من البنى التحتية والخدمات المتاحة لهم دون تحمل مخاطر أمنية وهنا يجب معرفة ضرورة الاحساس باخلاقية الأمن السيبراني^(٢).

رابعاً: البعد السياسي

قد يشكل الأمن السيبراني وسيلة حماية للمعلومات والوثائق الأساسية الحساسة لعمل قطاعات الدولة، وعليه لابد من تحقيقه حتى لا تخلق خلافات دبلوماسية بين الدول، وفي حالات أخطر شهدت العلاقات الدولية حروب فعلية شرسية جراء إختراق الأمن السياسي وأبرز مثال الحرب الروسية الأوكرانية ٢٠٢٢ التي بدأت بحرب سيبرانية إنتهت بحرب فعلية مدمرة^(٣).

خامساً: البعد القانوني

يمثل التشريع أداة ضبط المجتمعات وهو يحمل نفس الوظيفة بالنسبة للفضاء السيبراني حيث لابد أن تتركس الدول تشريعات خاصة وأطر قانونية تحدد مجالات للفضاء السيبراني ، كما أصبح الأمن السيبراني حقاً جماعياً من الحقوق الحديثة وتفرعت منه عدة حقوق كحق النفاذ إلى الشبكة العالمية للمعلومات وحق إنشاء المدونات الإلكترونية والحق في حماية البرامج المعلوماتية ويقابلها مجموع التزامات مثل التزام الإبلاغ عن مخالفات وجرائم خاصة بالمحتوى، كل هذا يتطلب وجود قوانين تواكب هذا التطور^(٤).

المطلب الثاني

بنيان القانوني لجرائم الامن السيبراني

بغية دراسة موضوع البنيان القانوني لجرائم الامن السيبراني سنقسم هذا المطلب على فرعين، وكما يأتي:

الفرع الاول

تعريف جرائم السيبراني

يعرف جرائم السيبراني بأنه استخدام الطيف الإلكتروني أو الكهرومغناطيسي لتخزين وتعديل وتبادل البيانات وجها لوجه مع أنظمة تحكم في بنى تحتية مرتبطة به^(٥)، او عبارة عن " كل فعل أو امتناع عن فعل باستعمال نظام معلوماتي معين للإضرار بمصلحة أو حق يحميه القانون من الآلي أو بمساعدته أو أن يكون أداة رئيسية في ارتكابه أو له دوراً هاماً إيجابياً في هذا الارتكاب"^(٦)، أو هو "مجموعة من الأنشطة التي تتم من بواسطة استخدام الكمبيوتر بشكل أساسي أو يتم تسهيلها من خلال استخدام الكمبيوتر، وهي تعتبر إما غير قانونية أو غير مشروعة من قبل أطراف معينة، ويمكن أن يتم إجراء تلك الأنشطة من خلال الشبكات الإلكترونية العالمية"، او عرف بأن "هو أي جريمة يتم تسهيلها أو ارتكابها باستخدام كمبيوتر، شبكة، أو جهاز"^(٧)، او هو " استخدام الحاسوب كأداة لإرتكاب الجريمة بالإضافة الى الحالات دية المتعلقة بالولوج غير المصرح به للحاسوب الآلي أو البيانات الرقمية لتشمل الإعتداءات المالية المادية"^(٨).

ولكن بالنسبة لموقف التشريعات الوطنية بصدد تعرف جرائم السيبراني وعند الرجوع الى قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ والقوانين الجنائية الخاصة، نستنتج بأن لم يذكر المشرع العراقي والكوردستاني تعريف جرائم الامن السيبراني، لعل سبب هذا يرجع في كون أن وضع التعريفات للمفاهيم القانونية العامة هو عمل فقهي وليس من عمل المشرع^(٩).

الفرع الثاني

أركان جرائم الامن السيبراني

لأشك فيه ان لجرائم الامن السيبراني اركان الثلاث والمتمثلة بما يلي:

١. الركن المادي لجريمة

ان الركن المادي للجريمة هو مظهر الخارجي للجريمة أو كيانها المادي او هو الماديات المحسوسة في العالم الخارجي كما حددتها نصوص التجريم فكل جريمة لا بد لها من ماديات تتجسد فيها الإرادة الاجرامية لمرتكبها ويخرج من مجال التجريم أذن الافكار او المعتقدات أو الآراء التي لا يعبر عنها بمظاهر خارجية يجرمها القانون ذلك ان الايمان بفكرة أو التصميم عليها أو حتى مجرد الافصاح عنها للغير من مجال الآراء ويرتبط بها الى مرتبة الاعمال الخارجية التي تستحق التجريم^(١٠).

(١) منى جبور الاشقر، السيبرانية هاجس العصر، جامعة الدول العربي، القاهرة المركز العربي للبحوث القانونية والقضائية، ٢٠١٧، ص٧٦.

(٢) اسماعيل زروق، الفضاء السيبراني والتحول في مفاهيم القوة والصراع الجزائر، مجلة العلوم القانونية والسياسية، العدد ١، المجلد ١، ٢٠١٩، ص٤٦.

(٣) منى جبور الاشقر، السيبرانية هاجس العصر. جامعة الدول العربي ، القاهرة المركز العربي للبحوث القانونية والقضائية، ٢٠١٧، ص١٧١.

(٤) عطية إدريس، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، المجلد ١، العدد ١، ٢٠١٩، ص١٠٧.

(5) Micheal S.Fuertes, "Cyber warfare, Unjust Actins in a just war", Florida International University, Full 2013, p.1.

(٦) د. قطاف سليمان، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، المجلد ٥، العدد ٢، ٢٠٢٢، ص٦٠.

(٧) دنيا محمد قاسم سالم، تأثير جرائم الأمن السيبراني على مخاطر المراجعة وإنعكاسه على آتباع المراجعة، ص٩٨٠.

(٨) محمد أمين الشواكة جرائم الحاسوب الإنترنت، ط٤ ، دار الثقافة للنشر والتوزيع، الأردن، ٢٠١١، ص٨.

(٩) قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩.

(١٠) علي عبد القادر القهوجي، شرح قانون العقوبات، القسم العام، منشورات الحلبي الحقوقية، ٢٠٠٨، ص ٣٠٧.

ومن خلال الرجوع الى قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ نجد بأن تم تعريف الركن المادي للجريمة بأن عبارة عن "سلوك إجرامي بارتكاب فعل جرمه القانون أو الامتناع عن فعل أمر به القانون"^(١)، ففي سياق المتصل يمكن القول بأن الركن المادي للجريمة يتكون من عدة عناصر ومن أبرزها:

أ. السلوك الإجرامي

السلوك هو المظهر الخارجي للركن المادي للجريمة، فمن المعروف أن فكرة الجريمة هي أول ما ينشأ في ذهن الفرد، وهذه الفكرة هي مجرد نشاط نفسي لا يمكن وصفه بالسلوك، ولكن متى ما بدأت هذه الفكرة بالتحقق في العالم الخارجي بنشاط إيجابي أو موقف سلبي، يعتبر سلوكاً^(٢)، وقد يكون السلوك الإجرامي نشاطاً إيجابياً ويتحقق عند قيام الجاني بعمل يحرمه القانون كإطلاق الرصاص أو الضرب أو السرقة وهو شأن غالبية الجرائم وقد يكون موقفاً سلبياً أي تركاً كإمتناع شاهد من أداء الشهادة^(٣).

ب. النتيجة الضارة

عبارة عن التغيير الذي يحدث في العالم الخارجي كأثر للسلوك الإجرامي، فيحقق عدواناً ينال مصلحة أو حقا قدر الشارع جدارته بالحماية الجزائية، مما يعني أن للنتيجة الضارة مدلولين أحدهما مادي، وهو التغيير الناتج عن السلوك الإجرامي في العالم الخارجي، والآخر قانوني وهو العدوان الذي ينال مصلحة أو حقا يحميه القانون^(٤).

٢. الركن لمعنوي للجريمة

إن أساس التجريم في التشريع ليس هو السلوك المعين في النموذج القانوني فقط، وإنما هو أيضاً اتصال هذا الفعل بإرادة إحداثه من قبل إنسان على النحو الذي يحدده القانون وهذه الإرادة هي التي تعطي للسلوك صفته الإنسانية، أي تخرجه من حوادث الطبيعة، وتضمه إلى الظواهر الإنسانية والاجتماعية، فموت الإنسان مثلاً، يحدث في كل لحظة بفعل حوادث الطبيعة، كالمرض والفيضانات والزلازل، وهذا الموت لا يشكل جريمة، لأنه واقعة طبيعية خارجة عن نطاق القانون الجنائي، إن الموت الذي يعده القانون الجنائي جريمة هو الذي يحدث بفعل إنسان تربطه بهذا الفعل علاقة ذهنية ونفسية على النحو الذي يحدده النموذج القانوني لهذه الجريمة^(٥).

والركن المعنوي يرتكز على الإرادة الأثمة، ويفترض توافر الأهلية الجزائية، أي الأهلية للمسؤولية الجزائية، أو كما يسميها البعض المسؤولية العقابية أو المسؤولية الجنائية التي قوامها الإدراك (التمييز)، ولهذا السبب أيضاً يجعل الكثير من الكتاب الأهلية الجزائية من عناصره فيشترطون لتحقيق الركن النفسي (أولاً) تحقق الإرادة أي حرية الاختيار، ويراد بها قدرة الإنسان على توجيه نفسه إلى عمل معين أو الامتناع عنه، وهذه القدرة لا تتوافر لدى شخص إلا إذا انعدمت المؤثرات التي تعمل في إرادته وتفرض عليه اتباع وجهة خاصة، و(ثانياً) تحقق الإدراك أي التمييز، ويراد به استعداد الشخص أو قدرته على فهم ماهية أفعاله وتقدير نتائجها^(٦).

وتتمثل الإرادة الأثمة في الجرائم العمدية بالقصد الجنائي حيث يشترط فيها أن يكون الجاني قد أراد العمل المادي المكون للجريمة السلوك الإجرامي الذي أتاه كما وأراد النتيجة الجرمية التي حصلت منه أو أية نتيجة جرمية أخرى غيرها كجريمة القتل العمد والسرقة والإيذاء العمد وغيرها. وتتمثل في (الجريمة غير العمدية)^(٧).

٣. الركن المفترض للجرائم الامن السيبراني

إن أغلب الجرائم تلتقي بينها بأركانها أساسية عامة ومشتركة وهي الركن المادي والركن المعنوي كما تطرقنا اليهم آنفاً، ولكن هذا الحال لا يستوي في جميعها، فهناك نوع من الجرائم عند قيامها لا تكفي بتلك العناصر الأساسية العامة المشتركة، ذلك إن نموذجها القانوني يتطلب فضلاً عن ذلك توافر الأركان الخاصة بها^(٨)، أي فإن لكل جريمة على وحده أركانها الخاصة التي تميزها عن غيرها من الجرائم الأخرى، وكذلك الحال في الجرائم الامن السيبراني وإن تلك الصفات ترتبط بهذا النوع من الجرائم وجوداً أو عدماً، وإن الجرائم الامن السيبراني ولكي يكتمل نموذجها الإجرامي يقتضي توافر الأركان العامة للجريمة وهما الركن المادي والركن المعنوي، ويلاحظ بأن الجرائم الامن السيبراني هي من الجرائم التي تتطلب الأركان العامة المذكورة أعلاه كأية جريمة أخرى، يتطلب إضافة إلى ذلك توافر الركن المفترض فيها^(٩).

المبحث الثاني

سبل مكافحة جرائم الأمن السيبراني في التشريعات الوطنية والدولية

سنبحث عن مسألة سبل مكافحة جرائم الامن السيبراني في التشريعات الوطنية والدولية كما يأتي:

المطلب الأول

دور الاتفاقيات الدولية في مكافحة جرائم الأمن السيبراني وآثارها الدولية

سنلقى الضوء على دور الاتفاقيات الدولية في مكافحة جرائم الأمن السيبراني وآثارها الدولية تباعاً:

الفرع الاول

دور اتفاقية بودابست لعام ٢٠٠١ في مكافحة جرائم الأمن السيبراني

تعتبر اتفاقية بودابست اول وابرز اتفاقية تختص بالجرائم السيبرانية، وهي اوربية المنشأ ولكنها ذات طابع عالمي، وقعت عليها (٢١) دولة اوربية بالاضافة الى كندا وامريكا وجنوب افريقيا^(١٠).

(١) المادة (٢٨) قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩.

(٢) عيود السراج، شرح قانون العقوبات القسم العام، نظرية الجريمة، ص ١١٨.

(٣) د. علي حسن خلف و سلطان عبدالقادر الشاوي، مبادئ العامة في القانون العقوبات، شركة العاتك لصناعة الكتب، القاهرة، بدون سنة النشر، ص ٦٨.

(٤) د. علي حسن خلف و سلطان عبدالقادر الشاوي، المصدر السابق، ص ٦٩-٧٠.

(٥) عيود السراج، شرح قانون العقوبات القسم العام، نظرية الجريمة، ص ١٢٣.

(٦) د. علي حسن خلف و سلطان عبدالقادر الشاوي، مصدر سابق، ص ٧٦.

(٧) د. علي حسن خلف و سلطان عبدالقادر الشاوي، مصدر سابق، ص ٧٥.

(٨) محمود محمود مصطفى، شرح قانون العقوبات، القسم العام، ط ٩، دار النهضة العربية، القاهرة، ١٩٨٣، ص ٣٨.

(٩) د. عمر السعيد الرضمان، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، ١٩٨٦، ص ١٥٢. و سعد صالح الجبوري، الجرائم الإرهابية في القانون الجنائي، ط ١، شركة المؤسسة الحديثة للكتاب طرابلس، لبنان، ص ١٣٧.

(١٠) عمر عباس خضير عبيد، الارهاب الالكتروني في نطاق القانون الدولي، المركز العربي للدراسات والبحوث العلمية، القاهرة، ٢٠٢١.

ومن الجدير بالإشارة ان هذه الاتفاقية أكد على ضرورة التزام دول الاعضاء بتسليم المجرمين و تبادل المساعدات في تحقيق وجمع الأدلة واتخاذ تدابير تشريعية التي تمكنها من الوفاء بالالتزامات، وهدف من ابرامها وضع سياسة جنائية مشتركة بين دول المجلس بهدف حماية ممتلكاتها من الجريمة السيبرانية من خلال اعتماد تشريعات ملائمة و تقرير التعاون الدولي^(١). ويشتمل الاتفاقية على مقدمة وأربعة فصول، كما تضمنت الاتفاقية عدة طوائف من الجرائم السيبرانية، وهي على النحو الآتي:

المجموعة الأولى: الجرائم التي تستهدف عناصر أمن المعلومات السيبرانية.

المجموعة الثانية: الجرائم المرتبطة بالحاسوب الإلكتروني.

المجموعة الثالثة: الجرائم المرتبطة بالمحتوى الإلكتروني.

المجموعة الرابعة: الجرائم السيبرانية^(٢).

الفرع الثاني

آثار الجرائم الامن السيبراني على الأمن والسلم الدوليين والعلاقات الدولية

تشكلت الجرائم الأمن السيبراني عبر الوسائل الإلكترونية في الآونة الأخيرة أشكالاً ذات آثار ضارة على الأمن والسلم الدوليين والعلاقات الدولية، وأصبحت تهدد الأمن والسلم الدوليين والعلاقات الدولية، ويتصور حدوث هذا إذا قامت شبكات إتهام دولة ما بأنها قامت بإيواء مرتكبي هذه الجرائم^(٣).

ومن الأمثلة العملية التي قامت به داعش من استغلال الوسائل السيبرانية لأعمال إرهابية أدت إلى توتر والسلم الدوليين والعلاقات الدولية، وكذلك العمل الذي قام به موقع "ويكيليكس" والذي يُعرف بصراع السيبراني ذو طبيعة ناعمة أدت إلى الصراع الدولي السيبراني والتأثير في المشاعر والأفكار وشحن حرب نفسية وإعلامية من خلال تسريب المعلومات والأسرار واستخدامها عبر منصات إعلامية بما يؤثر على طبيعة العلاقات الدولية، فإن هذا الصراع من شأنه أن يُهدد السلم العالمي بإعتباره حرباً سيبرانياً بين الدول مما يحدث خلل بنظام الأمن والسلم الدوليين والعلاقات الدولية^(٤).

ومن ثم تركت الهجمات على الأمن السيبراني أثراً كبيراً في بنية مجتمعات دول العالم، واستطاعت هذه العمليات بتقسيم الدول مذهبياً وطائفيّاً وعرقياً وإثنيّاً، وذلك لغرض تحقيق هدف هذه الظاهرة المتمثلة بضرب المؤسسات والأفراد للنيل من الأمن والسلم الدوليين، إذ أخذت الدول على عاتقها القيام بما هو ممكن بغية تحقيق السلام والاستقرار داخل دولها عن طريق الدعوة إلى ضرورة مواجهة ظاهرة الجرائم الامن السيبراني الدولي الذي أخذ يضرب دولاً مختلفة، حيث أصبح الفضاء السيبراني مجالاً جديداً للتفاعلات الدولية سواء أكانت تفاعلات صراعية أم تعاونية، مما أثر على تغير طبيعة القوة و بروز تهديدات الفضاء السيبرانية، وأثر بدوره على استراتيجيات الأمن الوطني للدول، والسعي إلى الإستحواذ على مصادر القوة داخل الفضاء الإلكتروني لمنع تعرض بنيتهما التحتية والحيوية للخطر، ومن ثم دخول المجال الإلكتروني ضمن المحددات الجديدة للقوة وأبعادها الجديدة من حيث طبيعتها وأنماط استخدامها وطبيعة الفاعلين فيها^(٥).

المطلب الثاني

الإطار التشريعي الوطني لمواجهة جرائم لأمن السيبراني وسلامتها

للبحث عن الإطار التشريعي لمواجهة جرائم الأمن السيبراني وسلامتها سنقسم هذا المطلب على فرعين، وكما يأتي:

الفرع الاول

الإطار التشريعي لمواجهة جرائم الأمن السيبراني وسلامتها في العراق

لاشك فيه ان الإطار التشريعي الجنائي لمواجهة جرائم لأمن السيبراني وضمان وسلامتها يعني التدخل التشريعي من خلال تجريم ما تقوم به المنظمات والاشخاص بجميع سلوكيات وتشديد العقوبات على هذه الافعال والسلوكيات، فمواجهة جرائم الأمن السيبراني تشريعياً يكون من الضرورة بمكان مواكبة التطور الحاصل في مجال الجرائم السبرانية من خلال المواجهة التشريعية الكافية والتصدي اللازم للتعامل مع هذه الجرائم من خلال ايجاد قواعد قانونية غير تقليدية الازمة لمعالجة جرائم الأمن السيبراني وكافية للتعامل معها، بصدد الإطار التشريعي لمواجهة جرائم لأمن السيبراني وسلامتها في العراق وعند تتبع موقف المشرع العراقي نلاحظ خلل نظام التشريع الجنائي العراقي من أي قانون جنائي خاص بمكافحة جرائم الأمن السيبراني، الا ان عمل المشرع العراقي على اتخاذ عدد من الاجراءات بصورة غير مباشر لمواجهة جرائم الأمن السيبراني وجرائم امن الدولة وسلامتها في العراق، وعلى سبيل المثال:

١. قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩

يلاحظ بأن يعتبر قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ جرائم الاعتداء على وسائل الاتصالات السلكية واللاسلكية في الجرائم ذات الخطر العام المضادة بالمصلحة العامة، لذلك عاقب بالسجن مدة لا تزيد على سبع سنوات او بالحبس من عطل عمدا وسيلة من وسائل الاتصال السلكي أو اللاسلكية المختصة بالمنفعة عامة أو قطع أو تلغي شيئاً من اسلاكها او اجهزتها از حال عمدا دون اصلاحها وتكون العقوبة بالسجن الما ارتكب الجريمة باستعمال مواد مفرقة او متفجرة، اذا ارتكب في وقت حرب او فتنه از هياج^(٦).

٢. قانون مكافحة الارهاب في العراق رقم (١٣) لسنة ٢٠٠٥

نظراً لتزايد العمليات الارهابية وتجديد حياة المواطنين في العراقي فقد ادى الى ضرورة اصدار قانون خاص ومستقل لمكافحة الارهاب في العراق لذا وافقت الجمعية الوطنية العراقية على قانون رقم (١٣) لسنة ٢٠٠٥ وعرف هذا القانون لإرهاب على انه كل سلوك اجرامي يقوم به فرد او جماعة منظمة تستهدف فردا از مجموعه افراد أو جماعة أو مؤسسات رسمية أو غير رسمية أو وقع الأضرار

(١) د. حمدان رمضان محمد، الارهاب الدولي وتداعياته على الامن والسلم العالمي، دراسة تحليلية، مجلة ابحاث التربية الاساسية، جامعة الموصل، المجلد ١١، العدد ١، دون سنة النشر، ص ١٥٥.

(٢) د. خالد حسن أحمد لطفي جرائم الإنترنت بين القرصنة الإلكترونية والإبزاز الإلكتروني، ط ١، دار الفكر الجامعي، الإسكندرية، ٢٠١٨، ص ٥٤.

(٣) عمران كمال الدين، السياسة الجنائية المنتهجة ضد الجرائم الإلكترونية دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أبو بكر بلقايد، تلمسان، الجزائر، ٢٠١٦، ص ١١٠-١١١.

(٤) خليل يوسف جندى، المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني، دراسة مقارنة، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، المجلد ٧، العدد ٢٦، العراق، ٢٠١٨، ص ٩٣.

(٥) نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية، المكتب العربي للمعارف، القاهرة، ٢٠١٥، ص ١٠٨٠.

(٦) قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩.

بالممتلكات العامة أو الخاصة بغية الاخلال بالوضع الأمني أو الاستقرار والوحدة الوطنية أو ادخال الرعب والخوف والفرع بين الناس والاراة الفوضى تحقيقا لغايات اراهبية^(١).

٣. قانون جهاز مكافحة الارهاب العراقي رقم ٣١ لسنة ٢٠١٦

يعتبر مؤسسة مكافحة الارهاب العراقي احد اهم المؤسسة في مجال مناهضة جرائم الارهابية وجرائم الامن السيبراني، ويعرف بأنه " ذلك الجهاز الذي يتبع تكتيكات وتطبيقات وتقنيات واستراتيجيات تعتمد عليها الحكومة العراقية والقوات المسلحة وادارات والوكالات الامنية المختلفة لمنع ورود، او تنتسب اليها او تعلن عن ورود التهديدات الارهابية التي تقوم بها الجماعات الارهابية فعليا مسؤوليتها عنها، ويشمل ذلك اكتشاف الاعمال الارهابية المحتملة، والرد الحاسم والقوي على مثل هذه الاعمال، حيث تعطي لهذه القوات مهام البحث والتحري عن المنظمات الارهابية وعن قياداتها وعناصرها، والتعرف على المتعاونين معها، وتتبع مراكز الخطط اللازمة لاعتراضها وتدميرها، وعجز قدرات مفكرها ومنظمها، فـجهاز مكافحة الارهاب العراقي هو الصفوة المختارة من شباب القوات المسلحة العراقية ممن تتوفر فيهم الكفاءة البدنية والعقلية والمهارة^(٢).

وبالتالي فان الرئيس الاعلى للجهاز هو المسؤول عن تنفيذ اعماله وتوحيد سياسته، اذ يمارس رئيس الجهاز مهام الرقابة والاشراف على الأنشطة والاداء كما تصدر عنه التعليمات والانظمة الداخلية والقرارات والاوامر كل ماله علاقة بمهام الجهاز وتشكيلاته فضلا عن سائر شؤونه الادارية والفنية والمالية والتنظيمية وفق احكام القانون، ووفق المادة (٥) من قانون جهاز مكافحة الارهاب العراقي رقم ٦١ لعام ٢٠١٦، يتولى رئيس الجهاز بعض من المهام ومن ابرزها: ثاني عشر: التنسيق مع الجهات الاعلامية المختصة في تنظيم رسائل وحملات اعلامية مناسبة ضد الارهاب وبثها. ثالث عشر: طلب تجميد حسابات مصرفية محددة وفق المعلومات التي ترد اليه من الجهات ذات العلاقة على ان يقرن الطلب بموافقة اللجنة الوزارية للامن الوطني وفقا للقانون^(٣).

وتجدر الاشارة الى ان جهاز مكافحة الارهاب العراقي يتالف من تشكيلات عدة، ومن ابرزها: وكالة الجهاز الامنية والاستخبارية، ووكالة الجهاز الفنية والادارية، ومكتب المفتش العام، ومديرية الدائرة القانونية، وقيادة العمليات الخاصة (الاولى، الثانية، الثالثة)، واكاديمية جهاز مكافحة الارهاب، ومكتب رئيس الجهاز، وجناح طيران مكافحة الارهاب، ويشير قانون جهاز مكافحة الارهاب العراقي رقم ٣١ لسنة ٢٠١٦ الى ان اهداف هذا الجهاز والقوات التابعة له تدور حول عدة امور هي: ثانياً: تنفيذ العمليات الامنية و الخطط الاستراتيجية فيما يتعلق بفعاليات مكافحة الارهاب و له في سبيل ذلك وفقا للقانون: ت. مراقبة الاتصالات و مواقع التواصل الاجتماعي و المواقع الالكترونية بناء على امر قضائي^(٤).

الفرع الثاني

الإطار التشريعي لمواجهة جرائم لأمن السيبراني وسلامتها في اقليم كردستان

بصدد موضوع الإطار التشريعي لمواجهة جرائم لأمن السيبراني وسلامتها في اقليم كردستان، نجد بأن اقليم كردستان -العراق كجزء من العراق الذي يتمتع بسلطات دستورية ومنها سلطة اصدار القوانين ومن خلال برلمان اقليم كردستان العراق قام بإصدار عدد من التشريعات لمواجهة جرائم الالكترونية ومن ابرزها:

١. قانون منع إساءة استعمال أجهزة الاتصالات في اقليم كردستان -العراق رقم ٦ لسنة ٢٠٠٨

ان المشرع في اقليم كردستان -العراق قام بإصدار قانون فيما يخص الجرائم الالكترونية تحت عنوان (قانون منع إساءة استعمال أجهزة الاتصالات في اقليم كردستان -العراق رقم ٦ لسنة ٢٠٠٨)، وان هذا القانون قضت على انه يعاقب بالحبس مدة لا تقل عن ستة اشهر ولا تزيد على خمس سنوات وبغرامة لا تقل عن مليون دينار ولا تزيد عن خمس ملايين دينار او يا حدي هاتين العقوبتين كل من أساء استعمال الهاتف الخليوي او اي اجهزة اتصالية سلكية او لاسلكية او انترنت او البريد الالكتروني وذلك عن طريق التهديد او القذف او السب او نشر اخبار مختلفة وكذلك ذكر نفس القانون على انه يعاقب بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد عن سنة وبغرامة لا تقل عن سبعمائة وخمسون الف دينار ولا تزيد على ثلاثة ملايين دينار او بإحدى هاتين العقوبتين كل من تسبب عمدا باستخدام و استغلال الهاتف الخليوي او اي اجهزة اتصالية سلكية او لاسلكية او الانترنت او البريد الالكتروني في الزعاج غيرة في غير الحالات الواردة في المادة الثانية من هذا القانون^(٥).

٢. قانون مكافحة الإرهاب في اقليم كردستان -العراق رقم (٣) لسنة ٢٠٠٦

يعتبر قانون مكافحة الإرهاب في اقليم كردستان -العراق رقم (٣) لسنة ٢٠٠٦ احد اهم القوانين في مجال مكافحة جرائم الارهابية، اذ ذهب المشرع الى تنظيم الفعل الإرهابي وتحديد صور هذا الجرائم وعقوباتهم المقررة، وان هذا القانون يتكون من الثامنة عشرة مادة مع ديباجة، ولم يتطرق الى تنظيم جرائم الامن السيبراني في نطاق تلك المواد، ويحتوي هذا القانون على الاحكام الموضوعية والاجرائية الخاصة بهذه الطائفة من الجرائم.

الخاتمة

أولاً: الإستنتاجات

١. ان الجرائم الامن السيبراني خطر يتعين التصدى له بتوعية وتنشيف الأفراد عن الفضاء السيبراني وبالتدابير الوقائية الكفيلة بتقليل خطر الوقوع في مسار الجريمة الالكترونية الهجمات السيبرانية ساحة جديدة للحروب بعيداً عن المواجهات العسكرية والتقليدية .
٢. عموماً يهدف الامن السيبراني الى تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات وما تحويه من بيانات، وكذلك التصدي لهجمات وحوادث امن السيبرانية التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص، ومن ثم توفير بيئة آمنة موثوقة للتعاملات في مجتمع السيبرانية، وصمود البنى التحتية الحساسة

(١) قانون مكافحة الارهاب في العراق رقم (١٣) لسنة ٢٠٠٥.

(٢) د. علي هادي حميدي الشكراوي، الأحزاب السياسية وحماية القواعد الدستورية، دراسة المقارنة، مجلة بابل للعلوم الإنسانية، كلية التربية جامعة بابل، العدد الحادي عشر، ٢٠٠٧، ص ١٣٧.

(٣) قانون جهاز مكافحة الارهاب العراقي رقم ٦١ لعام ٢٠١٦.

(٤) قانون جهاز مكافحة الارهاب العراقي رقم ٣١ لسنة ٢٠١٦.

(٥) قانون منع إساءة استعمال أجهزة الاتصالات في اقليم كردستان -العراق رقم ٦ لسنة ٢٠٠٨.

للهجمات السيبرانية، وتوفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين، ومقاومة البرمجيات الخبيثة، ما تستهدفه من أحداث أضرار بالغة للمستخدمين، وحد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد.

٣. لا توجد قوانين تهتم بالأمن الوطني السيبراني، وان العراق واقلیم كوردستان تفتقر لوجود مجالس للأمن السيبراني أو أي هيئات مستقلة أخرى ممولة بشكل كاف تتولى هذه المهمة.

٤. عدم وجود هيئة مختصة بحماية الأمن السيبراني في العراق وفي ضمنه اقلیم كوردستان حالياً، الا أن العراق قد حاول أن يساير بعض الدول في موضوع الأمن السيبراني فأنشأ هيئة وحيدة للأمن السيبراني هي فريق الاستجابة السريعة للأحداث السيبرانية، وهي هيئة تابعة لمستشارية الامن الوطني التي هي ذاتها تفتقر لقانون ينظمها لها وانما انبثقت عن اللجنة الوزارية للأمن القومي.

ثانياً: التوصيات والمقترحات

١- ضرورة تشديد اجراءات الرقابة على مستعملي الفضاء الامن السيبراني واتخاذ اجراءات ردعية وفرض قوانين صارمة على مستخدميها في العراق واقلیم كوردستان، وكذلك ضرورة ادراج مجال الفضاء السيبراني ضمن مناهج التعليم في جميع مراحلها للتوعية بخطورة الاستخدام الخاطيء الوسائل الاتصالات وتكنولوجيا المعلومات، ومن ثم ضرورة عقد دورات تدريبية لتوعية الافراد والعاملين بالمؤسسات الحكومية لقواعد استخدام المعلومات والبيانات وتنمية مهاراتهم الاحترافية، وكذلك عقد بروتوكولات تعاون بين المؤسسات الحكومية داخل الدولة وتبادل الخبرات بين الخبراء المدنيين والعسكريين لمتابعة المستجدات على الفضاء السيبراني والاستعدادات الوقائية لمواجهة كل ما هو جديد في هذا المجال.

٢- إصدار اتفاقية مستقلة لمكافحة الجرائم الامن السيبراني الدولي، لمواجهة التهديدات الموجودة على الامن والسليم الدوليين.

٣- نصي المشرعين في العراق واقلیم كوردستان ان يعملوا على اصدار قانوناً جنائياً خاصاً من اجل مكافحة جرائم الامن السيبراني، وذلك لوجود قصور التشريعي في مجال حماية المجتمع عن مخاطر جرائم الأمن السيبراني، إذ لا توجد تشريعاً خاصاً تهتم بالأمن السيبراني، وان العراق واقلیم كوردستان العراق تفتقر لوجود مجالس للأمن السيبراني أو أي هيئة مستقلة أخرى ممولة بشكل كاف تتولى هذه المهمة.

المصادر والمراجع

أولاً: الموسوعات

١. ابن منظور، لسان العرب، ج ١، مطبعة الادب العربي، بيروت، ١٩٨٥.
٢. محمد بن ابي بكر الرازي، مختار الصحاح، ط ١، بيروت، دار الكتب العربية، ١٩٨١.

ثانياً: الكتب القانونية

١. خالد حسن أحمد لطفي، جرائم الإنترنت بين القرصنة الإلكترونية والإبتزاز الإلكتروني، ط ١، دار الفكر الجامعي، الإسكندرية، ٢٠١٨.
٢. زهير خضير عباس الزبيدي ود. ظفر عبد مطر التميمي، العراق والأمن السيبراني، الفرص والتحديات.
٣. سعد صالح الجبوري، الجرائم الإرهابية في القانون الجنائي، ط ١، شركة المؤسسة الحديثة للكتاب طرابلس، لبنان.
٤. علي حسن خلف و سلطان عبدالقادر الشاوي، مبادئ العامة في القانون العقوبات، شركة العاتك لصناعة الكتب، القاهرة، بدون سنة النشر.
٥. علي عبد القادر القهوجي، شرح قانون العقوبات، القسم العام، منشورات الحلبي الحقوقية، ٢٠٠٨.
٦. عمر السعيد الرمضان، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، ١٩٨٦.
٧. عمر عباس خضير عبيد، الارهاب الالكتروني في نطاق القانون الدولي، المركز العربي للدراسات والبحوث العلمية، القاهرة، ٢٠٢١.
٨. محمد أمين الشواكة جرائم الحاسوب الإنترنت، ط ٤، دار الثقافة للنشر والتوزيع، الأردن، ٢٠١١.
٩. محمود محمود مصطفى، شرح قانون العقوبات، القسم العام، ط ٩، دار النهضة العربية، القاهرة، ١٩٨٣.
١٠. منى الأشقر جبور، الأمن السيبراني، التحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، ٢٠١٢.
١١. منى جبور الاشقر، السيبرانية هاجس العصر، جامعة الدول العربي، القاهرة المركز العربي للبحوث القانونية والقضائية، ٢٠١٧.
١٢. نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية، المكتب العربي للمعارف، القاهرة، ٢٠١٥.

ثالثاً: الأطاريح والرسائل الجامعية

١. عمراني كمال الدين، السياسة الجنائية المنتهجة ضد الجرائم الإلكترونية دراسة مقارنة، إطروحة دكتوراه، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أبو بكر بلقايد، تلمسان، الجزائر، ٢٠١٦.

رابعاً: البحوث القانونية

١. أسامة زيد محمد منوخ، تأثير الأمن السيبراني على فاعلية نظام الرقابة الداخلية، نموذج مقترح، المجلة العراقية للبحوث الانسانية والاجتماعية والعلمية، العدد ١٢، ٢٠٢٤.
٢. اسراء شريف، الأمن السيبراني الصيني، دراسة في الدوافع والتحديات، مجلة قضايا سياسية، العدد ٦٥.
٣. اسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع الجزائر، مجلة العلوم القانونية والسياسية، العدد ١، المجلد ١، ٢٠١٩.
٤. حمدان رمضان محمد، الارهاب الدولي وتداعياته على الامن والسلم العالمي، دراسة تحليلية، مجلة ابحاث التربية الاساسية، جامعة الموصل، المجلد ١١، العدد ١، دون سنة النشر.
٥. خليل يوسف جندي، المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني، دراسة مقارنة، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، المجلد ٧، العدد ٢٦، العراق، ٢٠١٨.

جرائم الامن السيبراني في ضوء التشريعات الوطنية والمواثيق الدولية -دراسة تحليلية-

٦. عطية إدريس، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، المجلد ١، العدد ١، ٢٠١٩.
٧. علي هادي حميدي الشكر اوي، الأحزاب السياسية وحماية القواعد الدستورية، دراسة المقارنة، مجلة بابل للعلوم الإنسانية، كلية التربية جامعة بابل، العدد الحادي عشر، ٢٠٠٧.
٨. قطاف سليمان، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، المجلد ٥، العدد ٢، ٢٠٢٢.
٩. محمد عبد الفتاح احمد، التحديات الامنية السيبرانية في العراق، تحليل استراتيجي، مجلة الدراسات الامنية، العدد ٥، ٢٠١٩.
١٠. محمود علي عبد الرحمن، أسامة فاروق مخيمر، الفضاء الإلكتروني وأثره على مفاهيم القوة والأمن والصراع في العلاقات الدولية، مجلة كلية السياسة والإقتصاد جامعة محمد البشير الإبراهيمي، برج بوعريش، المجلد السادس عشر العدد الخامس عشر، الجزائر، ٢٠٢٢.
١١. نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني التهديد المتصاعد لأمن الدول، مجلة مركز بابل للدراسات الانسانية، المجلد ٨، العدد ٢.

خامساً: القوانين

١. قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩.
٢. قانون مكافحة الارهاب في العراق رقم (١٣) لسنة ٢٠٠٥.
٣. قانون منع إساءة استعمال أجهزة الاتصالات في اقليم كردستان -العراق رقم ٦ لسنة ٢٠٠٨.
٤. قانون جهاز مكافحة الارهاب العراقي رقم ٦١ لعام ٢٠١٦.

سادساً: الاتفاقيات والمعاهدات

١. اتفاقية بودابست لعام ٢٠٠١.

سابعاً: المصادر الاجنبية

1. Micheal S.Fuertes, "Cyber warfare, Unjust Acts in a just war", Florida International University, ٢٠١٣.
2. Michael krepon, Julia Thompson, deterrence and Sino-American relations, united states, stimson-center, 2013.