أوجه التعاون الدولي في تعزيز الأمن السيبراني بدولة الكويت

فهيد سعد العجمي

قسم المقررات الشرطية، كلية الشرطة، أكاديمية سعد العبد الله للعلوم الأمنية، الكويت.

البريد الإلكتروني: feheid١١١@gmail.com

ملخص البحث

هدفت الدراسة إلى توضيح أبعاد الأمن السيبراني، وأوجه تنظيم الامن السيبراني في القانون الكويتي، مع بيان أوجه التعاون الدولي في مجال الأمن السيبراني بين أجهزة الشرطة، وكذلك توضيح مظاهر التعاون القضائي على المستوى الدولي في مجال مكافحة الجرائم السيبرانية، واتبع الباحث المنهج التحليلي والاستقصائي وذلك من خلال تحليل الموضوع من أمهات الكتب والمراجع ذات العلاقة والأبحاث والدراسات التي تناولت الموضوع. وتوصلت نتائج الدراسة إلى أن الأمن السيبراني أصبح ضرورة مطلقة، فهو خط الدفاع الأول القادر على صد الهجمات السيبرانية المحتملة، وهو الآلية التي يتم من خلالها حماية أمن المعلومات والاتصالات والمرافق والمنشآت الحيوية المهمة أي حماية الأمن القومي الكلي حيث تحولت بيئة التهديد للبنية التحتية الحيوية من شكلها التقليدي القديم إلى شكلها التكنولوجي الحديث، وهذا التحول لا بد أن يصاحبه تحول في التشريعات والقوانين الخاصة بحماية الأمن السيبراني، كما أوضحت النتائج حرص الكويت على وضع أسس متينة للبنية التحتية الخاصة بالمعلومات والأمن المعلوماتي والسيبراني، إيماناً بأهمية التحول نحو مجتمع معرفي متمرس على تكنولوجيا المعلومات، وأوصت الدراسة بوجوب المشاركة بنشاط في المبادرات الدولية للأمن السيبراني، وتبادل المعلومات الاستخباراتية مع الشركاء الدوليين، والمساهمة في تطوير المعايير والمعايير الدولية للأمن السيبراني، مع محاولة الفصل بين الجرائم السيبرانية والهجمات السيبرانية، إذ إن ما ينطبق على الجريمة السيبرانية تعالجه القوانين الوطنية عادة، في حين أن ما ينطبق على الهجوم السيبراني

يندرج ضمن القوانين الدولية، والقانون الدولي الإنساني على وجه الخصوص.، بالإضافة إلى تدريب الكوادر البشرية الخليجية على أحدث مستجدات الأمن السيبراني وأمن المعلومات، وما يرتبط بها من متغيرات وذلك نظراً للحاجة إلى كفاءات وطنية خليجية قادرة على التصدي للتهديدات السيبرانية الحالية والمستقبلية، وذلك بما يتفق مع توصيات اللجنة الوزارية للأمن السيبراني بدول مجلس التعاون.

كلمات مفتاحية: امن، جرائم ، سيبراني، انترنت الأشياء، تعاون دولي ، أمن قومي.

Aspects of International Cooperation in Strengthening Cybersecurity in Kuwait

==========

Fahid Saad Al-Ajmi

Police Courses Department, Police College, Saad Al-Abdullah Academy for Security Sciences, Kuwait.

Email: feheid١١١@gmail.com

Abstract:

The study aimed to clarify the dimensions of cybersecurity, the aspects of cybersecurity regulation in Kuwaiti law, the aspects of international cooperation in the field of cybersecurity between police agencies, as well as clarifying the aspects of judicial cooperation at the international level in combating cybercrime, and the researcher followed the analytical and investigative approach by analyzing the topic from relevant books and references, research and studies that dealt with the topic. The results of the study concluded that cybersecurity has become an absolute necessity, as it is the first line of defense capable of repelling potential cyber-attacks, and it is the mechanism through which the security of information, communications, facilities and important vital facilities is protected, i.e. the protection of total national security as the threat environment for vital infrastructure has shifted from its old traditional form to its modern technological form, and this transformation must be accompanied by a shift in legislation and laws to protect cybersecurity, and the results showed that Kuwait urged to lay solid foundations for information infrastructure and information and cybersecurity, believing that , The study recommended that GCC countries should actively participate in international cybersecurity initiatives, exchange intelligence information with international partners, contribute to the development of international

cybersecurity standards and norms, and try to separate cybercrime from cyberattacks, as what applies to cybercrime is usually addressed by national laws, while what applies to a cyberattack falls under international laws, and international humanitarian law in particular, in addition to training Gulf human resources on the latest developments in cybersecurity and information security, and the associated variables, according to the study.

Keywords: Security, Crimes , Cyber , Internet of Things , International Cooperation , National Security.

المقدمة

إن التطور الحاصل على مستوى تكنولوجيات الإعلام والاتصال، حتم على العالم مواكبة هذا التطور، حيث تعد رقمنة البيانات والمعلومات من بين أهم مراحل التقدم بالنسبة للدول، وذلك تسهيلاً للوصول إلى المعلومة والمرونة في التعامل مع البيانات، وأيضا الاقتصاد في الجهد والوقت والتكاليف المادية.(جربوعة، بوطمين، ٢٠٢٣، ص ٤٥٣)

والحقيقة التي لا يمكن إنكارها أننا أصبحنا اليوم نعيش عصر تكنولوجيا المعلومات والاتصالات التي باتت هي الأساس الذي يعتمد عليه في شتى المجالات، ولدى جميع المؤسسات، سواء أكانت مؤسسات عامة تملكها حكومات الدول أم مؤسسات خاصة يمتلكها الأفراد، فتقنية المعلومات وشبكات الاتصالات هي الأداة الأساسية المستخدمة في إدارة شؤون الدول وتقديم الخدمات وتسهيلها عن طريقها (الصغير، ٢٠١١، ص٧٢).

إلا أن الانفتاح الذي يميّز شبكة الإنترنت، والفضاء السيبراني عموماً، جعلها عرضة للتعديات والأنشطة الإجرامية، فصار مستخدمو الفضاء السيبراني عرضة للانتهاكات من قبل مخترقي الشبكات. (عزت، ٢٠١٨، ص٤٥٦)

والجرائم السيبرانية أصبحت تشكل تحدياً كبيراً للأمن القومي وكذلك الدولي، لدرجة أن العديد من الباحثين اعتبر الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء هو ما استدعى ضرورة وجود ضمانات كافية لمواجهته.

حيث يعتبر الأمن القومي لأية دولة بمثابة ركيزة أساسية في استقرارها وحماية استقلاليتها وأمنها؛ إذ إنه يرتبط بأمن الأرواح والممتلكات في المقام الأول، وتعزيز هذا الأمن يتطلب عدم وجود تهديدات يمكن أن تضعف من أركان استقرار الدولة. (لامية، ٢٠٢١، ص ٦٦)

إلا أنه، وفي ظل هيمنة تكنولوجيا المعلومات على جميع مفاصل الحياة

المختلفة خلال السنوات القليلة الماضية توسع مفهوم الأمن القومي بشكل أكبر، وأصبح يشمل الأمن السيبراني للدول إضافة إلى المكونات السابق ذكرها، وهكذا، فإن الأمن السيبراني أصبح ركيزة أساسية من ركائز الأمن القومي: إذ أدرك المختصون أن المخاطر المترتبة على اختراق الأمن السيبراني لا تقل أهمية بأي حال من الأحوال عن مخاطر اختراق الأمن السياسي أو الاقتصادي أو العسكري للدولة. ومن ثم بدأ الأمن السيبراني يشكل لدى العديد من الدول أولوية قصوى في مقابل الأشكال التقليدية للأمن؛ إذ إنه يمكنه أن يفتح ثغرات أمام الأعداء لتقويض استقرار الدولة وأمنها القومي وهو ما زاد من أهمية المرونة السيبرانية التي تمكن الدول من مواجهة هذه التهديدات (كلاع، ٢٠٢٢، ص ١٥)

فيتمثل الهدف الأساسي للأمن السيبراني في تعزيز قدرة الدول على مقاومة التهديدات الكامنة في الفضاء السيبراني، الأمر الذي دفع كثير من دول العالم لوضعه على أجندة عملها، في ظل ظهور الحروب الإلكترونية التي تتعرض لها الكثير من الدول، فانتشار القوة السيبرانية بين عدد كبير من الفاعلين على الساحة الدولية ضرب في قدرة الدول على السيطرة والهيمنة، بل ومنحت فاعلين أصغر قدرة مساحة أكبر لممارسة للعب دور مهم عبر الفضاء السيبراني؛ مما يعني تغير في مقدرات القوى بالنظام الدولي. الأمر الذي غير ماهية بعض التفاعلات بين الوحدات الدولية الفاعلة، كالصراع، والتعاون، والردع والقوة عبر العالم الافتراضي المتشابك. (جمال الدين، ٢٠٢٣، ص ١٩٥)

وتواجه الكويت، مثل العديد من الدول، مجموعة متنوعة من التهديدات السيبرانية تتراوح بين اختراقات البيانات وسرقة الهوية وهجمات الفدية والتجسس المدعوم من قبل الدولة. تتجاوز العواقب المترتبة عن هذه التهديدات مجرد الخسائر المالية، لتشمل مخاطر الأمن القومي وعدم الاستقرار الاقتصادي والضرر الذي يلحق بالثقة العامة.

في حين أصدر الاتحاد الدولي للاتصالات التابع لمنظمة الأمم المتحدة

المتخصصة بتكنولوجيا المعلومات والاتصالات، مؤشر الأمن السيبراني العالمي للعام ٢٠٢٤، والمتضمن ترتيب ١٩٤ دولة عالمياً في المؤشر لخمس فئات، وجاءت الكويت متأخرة في الفئة الثالثة.

ولقد أعلنت الهيئة العامة للاتصالات وتقنية المعلومات الكويتية حصول دولة الكويت على المركز الأول عالمياً في مؤشر تطوير وتنمية قطاع الاتصالات وتقنية المعلومات(IDI) الصادر من الاتحاد الدولي للاتصالات، للمرة الثانية على التوالي. (كونا، ٢٠٢٤)

ويرى الباحث أن دولة الكويت تولي الأمن السيبراني اهتمامًا بالغًا؛ باعتباره اليوم قوة دفاعية مهمة، خاصة أن الجرائم الإلكترونية لا تقتصر على الأفراد والمؤسسات، بل تتعدى ذلك لتهدد الأمن القومي وسلامة مرافق واقتصاد الدولة.

وإذا نظرنا للأمن السيبراني وتأثيره على هيكل النسق الدولي نجد أننا أمام عدة إشكاليات في هذا الشأن كسرية مقدرات القوى السيبرانية أي عدم إفصاح بعض الدول عن واقع ما تمتلكه من قدرات سيبرانية حقيقية، والطبيعة ودورها في التأثير على سلوك الفاعلين الدوليين كبيئة محفزة لزيادة الهجمات السيبرانية التي ترتكبها الوحدات الدولية الفاعلة، وتهديد القوى العسكرية بفعل القدرات السيبرانية، الأمر الذي يؤثر على بنية وقيادة النظام الدولي ككل. (جمال الدين، ٢٠٢٣، ص ١٩٦)

لذا فإن التعاون على الساحة الدولية أمر أيضاً حيوي في مكافحة الجريمة السيبرانية. حيث يجب على الكويت المشاركة بنشاط في المبادرات الدولية للأمن السيبراني، وتبادل المعلومات الاستخباراتية مع الشركاء الدوليين، والمساهمة في تطوير المعايير والمعايير الدولية للأمن السيبراني. (القلاف، ٢٠٢٤)

مشكلة الدراسة:

أدى التطور السريع مجال تقنية المعلومات والاتصالات وشبكة الإنترنت في العالم كله إلى ظهور أنماط جديدة من الجرائم جاءت عن طريق الاستغلال السيئ للتكنولوجيا، مما ترتب معه خلق ظاهرة إجرامية جديدة، وهي الجرائم المتعلقة بالحاسب الآلي والإنترنت، والتي تتم عن طريق هجمات واختراقات وتسلل داخل النظم المعلوماتية بغرض أما تدمير تلك النظم أو الحصول على معلومات سرية سواء عسكرية أو اقتصادية الأمر الذي ينبه بوجود مخاطر على الصعيد الدولي والوطني إذا لم يتم تدارك هذه الظاهرة التي سوف ينشأ عنها، إذا ما تركت، خسائر هائلة على المستوى العسكري والاقتصادي والاجتماعي لجميع دول العالم. مما يستوجب معه والحال كذلك إيجاد سبل للتصدي لهذه الظاهرة. (لخضر، ٢٠٢٣، ص ٢٥٦)

وتتحدد أهمية الأمن السيبراني في القيام بتأمين المعلومات الحساسة البالغة الأهمية الدول الأفراد على حد سواء المعرضة للخطر والاختراق والاستيلاء كي تحافظ على الأمن الوطني وحفظ وحماية السرية والخصوصية للبيانات الشخصية للمواطنين. وتكمن الأخيرة كقضية ناشئة في حفل العلاقات الدولية من خلال حداثة هذا المجال السياق العام لظهور الأمن السيبراني هذا المجال، فهناك تاريخ طويل من التخمينات حول دور التكنولوجيا الرقمية في الدراسات الأمنية يستفيد الجميع أيضا من عمل الباحثين في مجال الأمن السيبراني.(الأمم المتحدة، ٢٠١٩، ص١٢٣)

وهذا ما جعل للأمن السيبراني أهمية كبيرة للمجتمع الكويتي، حيث أن الأمن السيبراني مهم على مستوى الفرد في حماية البيانات الشخصية والصور والملفات والفيديوهات والحسابات الشخصية وكلمات المرور والحسابات البنكية وغيرها من الأمور التي ترتبط بحياة المواطن الكويتي، وعلى مستوى المجتمع الكويتي، من حيث حماية المجتمع من الهندسة الاجتماعية واستهداف السلوك الاجتماعي والبيانات المجمعة والخصوصيات للمجتمع، وعلى مستوى

الشركات والمؤسسات، في حماية الأصول الإلكترونية والبيانات والمعلومات وبيانات الموظفين والعملاء والمواقع الإلكترونية، وعلى مستوى الدولة، في حماية أمنها الإلكتروني وحماية الأنظمة المالية والاقتصادية وغيرها من الهجمات الإلكترونية والابتزاز والقرصنة والتعطيل.

ومما سبق يمكن صياغة إشكالية الدراسة في التساؤل الآتي:

ما هي أوجه التعاون الدولي في تعزيز الأمن السيبراني بدولة الكويت؟

أهمية الدراسة:

(أ) أهمية علمية

١. في عصر يسود فيه الاتصال الرقمي كل جانب من جوانب الحياة الحديثة، لا يمكن التقليل من أهمية الأمن السيبراني، خاصة في بلد مثل الكويت. مع استمرار تقدم التكنولوجيا، تزداد التهديدات التي تواجهها الحكومات والأفراد من جراء المجرمين السيبرانيين، ما يجعل التدابير الفعالة للأمن السيبراني أمراً حيوياً للغاية.

٢. تستمد الدراسة أهميتها من الآثار والتداعيات الحالية والمستقبلية التي قد تنتج عن التهديدات السيبرانية التي من الممكن أن تقوض الأمن السيبراني للكويت، وامتداد هذه التأثيرات على كل من الأمن السياسي والاقتصادي والعسكري.

(ب) أهمية عملية:

١. يظهر الدور القانوني للأمن السيبراني في ضمانه لاستمرارية توافر المعلومات في النظام المعلوماتي وأخذ جميع الاحتياطات لحماية المستهلكين من الأخطار المحتملة التي تعزز حماية وسرية البيانات الشخصية لهم التصدي لأي محاولة ولوج غير مسموح به لأهداف غير سليمة إلى الأنظمة التشغيلية والسعي لتعزيز حماية مكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات وما تحتويه من بيانات.

٢. إن مكافحة الهجوم السيبراني وجرائم الإنترنت أصبح من أهمية بمكان أن نبحث في السبل التي يجب اتباعها للتصدي لتلك الجرائم العابرة للحدود والتي تستلزم تحديد ماهيتها وخصائصها وطبيعتها وخصائص مرتكبيها وكيفية مساءلتهم جنائياً ومدنياً. كذلك لا بد من أن نبحث في أساليب وإجراءات التعاون دولي الذي يتفق مع طبيعة الجرائم المتعلقة بالشبكة المعلوماتية والتي تتميز بطابع خاص يقتضي أن تكون هناك ردود فعل سريعة. ترتيبا على ما سبق فإن الحد من الهجوم السيبراني ومكافحة الجريمة السيبرانية على المستوى الدولي لابد له من تواجد روح التعاون بين الأنظمة القانونية الداخلية للدول.

تساؤلات الدراسة:

١- ما هو أبعاد الأمن السيبراني؟

٢- ما هي أوجه تنظيم الامن السيبراني في القانون الكويتي؟

٣- ما هي أوجه التعاون الدولي في مجال الأمن السيبراني بين أجهزة الشرطة؟

٤- ما هي مظاهر التعاون القضائي على المستوى الدولي في مجال مكافحة الجرائم السيبرانية؟

أهداف الدراسة:

١- توضيح أبعاد الأمن السيبراني.

٢- عرض أوجه تنظيم الامن السيبراني في القانون الكويتي.

٣- بيان أوجه التعاون الدولي في مجال الأمن السيبراني بين أجهزة الشرطة.

٤- توضيح مظاهر التعاون القضائي على المستوى الدولي في مجال مكافحة الجرائم السيبرانية.

منهج الدراسة:

إن إشكالية البحث لها دور رئيسي في اختيار المنهج الذي يجب اتباعه في

تناول ... موضوع البحث وعلى ذلك اتبع الباحث المنهج التحليلي والاستقصائي وذلك من خلال تحليل الموضوع من أمهات الكتب والمراجع ذات العلاقة والأبحاث والدراسات التي تناولت الموضوع .

مفاهيم ومصطلحات الدراسة

(أ) مفهوم السيبرانية والأمن السيبراني:

مصطلح السيبرانية والآن هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي. وتشير المقاربة الإيتيمولوجية لكلمة "**cyber** " إلى أنها لفظة يونانية الأصل مشتقة من كلمة "**kybernetes**" بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للمتحكم "**governor**". (الفتلاوي، ٢٠١٧، ص ٥٥)

واصطلاحاً: هناك العديد من التعاريف التي قدمت لمفهوم الأمن السيبراني، حيث يُعرف بأنه مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة.

فلقد عرف الأمن السيبراني بأنه ": مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات الإدارة المخاطر، وتدريبات وممارسات فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين". (القاضي، ٢٠١١، ص٤٢)

كما يمكن تعريف الأمن السيبراني هو عملية حماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية، التي تهدف إلى الوصول إلى المعلومات الحساسة أو تغييرها أو تدميرها؛ بغرض الاستيلاء على المال من المستخدمين أو مقاطعة عمليات الأعمال العادية. (الدهيسات، ٢٠٢٣، ص ٤٩)

ومن هنا يمكن القول إن الأمن السيبراني هو مجموعة الآليات والإجراءات والوسائل والأطر التي تهدف إلى حماية البرمجيات وأجهزة الكمبيوتر (الفضاء السيبراني بصفة عامة)، من مختلف الهجمات والاختراقات التهديدات السيبرانية

التي قد يهدد الأمن القومي للدول. (الأمم المتحدة ، ٢٠١٩، ص١٢٢)

وبما أن الأمن السيبراني عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير.(الحيمودي، ٢٠٢٣، ص٥)

فالأمن السيبراني يعبر عن مجموعة من الآليات والإجراءات والوسائل والاطر التي تهدف إلى حماية البرمجيات وأجهزة الكمبيوتر من الهجمات والاختراقات والتهديدات. (الضفيري، ٢٠٢٤، ص ٣)

(ب) مفهوم التعاون الدولي:

نتيجة للقناعة الدولية بضرورة التعاون الأمني لمحاربة الجريمة العابرة للحدود، جاءت فكرة إنشاء منظمات دولية وإقليمية كجبهة مشتركة تعنى بتأمين وتنمية هذا التعاون الأمني.

والتعاون الدولي لمكافحة الجريمة بصفة عامة يتمثل في تبادل المساعدة وتكاثف الجهود المشتركة بين طرفين دوليين أو أكثر في مجال العدالة الجنائية، وذلك لتخطي مسائل الحدود والسيادة، وتكون هذه الجهود عالمية أو إقليمية، وتتنوع وتتخذ عدة صور قضائية أم شرطية. (غازي، ٢٠١٤، ص٣٥١)

ويتحدد التعاون الدولي في مجال المواد الجنائية في تنفيذ ما يستلزمه التحقيق الابتدائي من سماع أقوال المتهمين وشهادة الشهود والخبراء والتفتيش وضبط الأشياء وتسليم المستندات وكل ما يتعلق بالدعوى الجنائية والانتقال للمعاينة للتحقق من الوقائع وإعلان الأوراق والمستندات. (العبيدي، ٢٠١٢، ص٤٦)

خطة الدراسة:

المبحث الأول: ماهية الامن السيبراني ووضعه في النظام الكويتي

المطلب الأول: ماهية الأمن السيبراني

المطلب الثاني: تنظيم الامن السيبراني في القانون الكويتي

المبحث الثاني: أوجه التعاون الدولي في مجال الأمن السيبراني

المطلب الأول: التعاون الدولي بين أجهزة الشرطة

المطلب الثاني: مظاهر التعاون الشرطي والقضائي على المستوى الدولي في مجال مكافحة الجرائم السيبرانية.

المبحث الأول

ماهية الامن السيبراني ووضعه في النظام الكويتي

يعد التطور الهائل الذي شهده عالم الاتصالات في مطلع الألفية الثالثة تعاظمت الأنشطة التي يتم أداءها عبر الفضاء السيبراني، وتعاظمت أهميته بالتالي، وازدادت المخاطر التي يتعرض لها هذا الفضاء، وإزاء الاتجاه العالمي نحو تنظيم هذا الفضاء والممارسات التي تجري من خلاله وكذلك إيجاد السبل القانونية والتقنية لتأمينه، وتأمين الخدمات التي تقدم عبره، كان لابد من أبعاد الأمن السيبراني وأنماط الجرائم السيبرانية وذلك في المطلب الأول، بالإضافة إلى تنظيم الامن السيبراني في القانون الكويتي في المطلب الثاني.

المطلب الأول

ماهية الأمن السيبراني

بعد توضيح مفهوم الأمن السيبراني، سوف أوضح أبعاد الامن السيبراني وأهم أنماط الجرائم السيبرانية في الفرعين الآتيين:

الفرع الأول

أبعاد الأمن السيبراني

تعدد أبعاد الأمن السيبراني فتشمل جميع الجوانب الاقتصادية الاجتماعية، والسياسية، والإنسانية، فهو له القدرة على حماية أمن ومصلحة الدولة وشعبها في مختلف مجالات حياته اليومية وذلك لكونه مرتبط ارتباطا وثيقا بسلامته وأمن البيانات والمعلومات والتي تعد ثروة هذا العصر حيث هي مصدر الإنتاج الإبداع الابتكار، والقدرة على الاتصال والتواصل بين البشر.

أولاً: الأبعاد العسكرية:

تنشأ أهمية الأمن السيبراني في هذا البعد من خطورة الهجمات السيبراني والاختراقات التي تؤدى إلى نشأة الحروب والصراعات المسلحة واختراقات أنظمة المنشأت النووية، وما قد يحدث عنها من تهديد لأمن الدول والحكومات

ويؤدى إلى كوارث. (المناعسة، الزعبي، ٢٠١٠، ص٦٥)

ثانياً: الأبعاد السياسية:

تقوم الأبعاد السياسية للأمن السيبراني على أساس حماية نظام الدولة السياسية وكيانها، حيث يمكن أن تستخدم التقنيات في بث معلومات وبيانات قد يحدث من خلالها زعزعة لاستقرار أمن الدول والحكومات حيث تصل بسرعة فائقة إلى أكبر شرائح من المواطنين بغض النظر عن صحة البيانات والمعلومات التي يتم نشرها. الأشقر، ٢٠١٦،ص ٦٤)

ثالثاً: الأبعاد الاقتصادية:

يرتبط الأمن السيبراني ارتباطاً وثيقاً بالحفاظ على المصالح الاقتصادية لكل الدول، فالترابط وثيق بين الاقتصاد والمعرفة فأغلب الدول تعتمد في تعزيز اقتصادها وازدهاره على إنتاج وتداول المعرفة والمعلومات على كل المستويات مما يبرز الدور الخطير للأمن السيبراني في حماية الاقتصاد المعرفي من السرقة والملكية الفكرية. (الجامعة اللبنانية، ٢٠١٧)

رابعاً: الأبعاد القانونية :

ترتبط الأنشطة المختلفة التي يقوم بها الأفراد والمؤسسات بالقوانين ومع ظهور المجتمع المعلوماتي ظهرت القوانين الجديدة التي تعد البيئة التنظيمية التشريعية المنظمة لحماية هذا المجتمع وحفظ الحقوق فيه بكافة ما يتضمن من أبعاد ويقوم الأمن السيبراني في هذا البعد على حماية المجتمع المعلوماتي ويساعده في تطبيق وتنفيذ هذه القوانين والتشريعات. (الضفيري، ٢٠٢٤، ص١٢٥)

خامساً: الأبعاد الاجتماعية:

تسمح طبيعة الإنترنت المفتوحة عبر شبكات التواصل الاجتماعي لكل مواطن بأن يعبر عن أفكاره والاطلاع على مختلف المعلومات والانفتاح عبر الثقافات المختلفة، وهنا يكمن دور وأهمية الأمن السيبراني في حماية وصيانة

القيم الجوهرية في المجتمع كالانتماء المعتقدات الدينية، والعادات والتقاليد ...الخ. وفي هذا السياق تعمل المنظمات والهيئات على نشر ثقافة الأمن السيبراني وتطالب بضرورة تعاون كل أفراد المجتمع في تحقيقه للحد من مخاطر الهجمات والجرائم السيبرانية التي مما لا شك فيه تتطول المجتمع ككل وتهدد أمنه واستقراره بالعمل على هدم القيم وضياع الهوية الثقافية. (الأشقر، ٢٠١٦، ص ٦٥)

الفرع الثاني

أنماط (سيناريوهات) جرائم الإرهاب السيبراني

قام خبراء الجرائم السيبرانية والأمن المعلوماتي بتحديد مجموعة سيناريوهات محتملة، ومجموعة سيناريوهات لما وقع بالفعل من جرائم سيبرانية، ويمكن تقسيم هذه السيناريوهات إلى الآتي:

أولاً: تدمير المواقع والبيانات السيبرانية والنظم المعلوماتية:

أ-يتم عملية الاختراق السيبراني بتسريب رموز معينة تتعلق ببرامج وتطبيقات شبكة إنترنت، وهذه العملية من الممكن تنفيذها من أي موقع في العالم، من غير أن يحتاج المنفذ أن يتواجد بنفس الدولة التي سيقع عليها هذا الهجوم، وفي هذه الحالة يشن الإرهابي هجوماً مدمراً لغلق المواقع الحساسة والحيوية على شبكات المعلومات، وإصابتها بالشلل التام، خاصة إذا نجح هذا الإرهابي في الوصول إلى أنظمة القيادة والسيطرة والاتصالات، بالإضافة إلى محطات الطاقة الكهربية والمياه، ومواقع بورصات الأوراق المالية، وعندئذ تصاب هذه المواقع الحساسة بالشلل التام، وهي مواقع استراتيجية وحيوية وفي تعطلها تهديد للأمن الوطني. (يوسف، ٢٠١١، ص ١٤٨)

ب-يقوم الإرهاب السيبراني بإرسال عدد وغير من الرسائل الإلكترونية للهدف المحدد بهدف إضعاف القدرة على تخزين البريد فيؤدي ذلك إلى إنهاك

الموقع أو انفجاره، فتفرق البيانات المخزونة في الموقع. فيسهل التجوال ببساطة في الموقع والحصول على ما يريد الإرهابي، بالإضافة إلى توظيف الفيروسات الفتاكة التي هي عبارة عن برامج حاسوبية لها القدرة على أن تتزايد بقدرات رهيبة، ويمكنها الانتشار على أجهزة حاسوبية في فترة وجيزة بمجرد اتصال الجهاز المصاب بأي جهاز آخر. (يوسف، ٢٠١١، ص ١٤٨)

ثانياً: استهداف النظم العسكرية:

يهدف هذا النوع من الهجمات المواقع العسكرية الخاصة بالقوات المسلحة لإحدى الدول، ويعد هذا السيناريو من أخطر السيناريوهات المحتملة التي قد تعصف بمجتمعنا المعاصر، وتبدأ المرحلة الأولى من هذا السيناريو باختراق المنظومات الخاصة بالأسلحة الاستراتيجية، ونظم الدفاع الجوي والصواريخ النووية. (داود، ٢٠١٧، ص٤٧)

ثالثاً: استهداف محطات توليد الطاقة والماء:

أصبح الاعتماد على شبكات المعلومات وخصوصا في الدول المتقدمة من الوسائل المهمة لإدارة نظم إنتاج الكهرباء، ويمكن للهجمات على مثل هذا النوع من شبكات المعلومات أن تؤدي إلى نتائج مرعبة، وخصوصاً في ظل اعتماد الإنسان المعاصر على الطاقة الكهربائية التي لا يمكن الاستغناء عنها تحت أي ظرف من الظروف، ولذلك تدرك عناصر الإرهاب السيبراني حيوية وأهمية هذه المواقع فتعمل على استهدافها. (داود، ٢٠١٧، ص٤٧)

رابعاً: استهداف البنية التحتية الاقتصادية:

إن الشبكات المعلوماتية أصبحت هدفاً جذاباً للإرهاب السيبراني، وهي كذلك لأنها تتأثر بشكل ملموس مهما كانت درجة إصابتها طفيفة، لأن تعطلها أو تقليل كفاءتها يصنع رأياً عاماً سلبياً، وهذا هو ما تتمنى حدوثه تلك التنظيمات الإرهابية من إضعاف الثقة في الدولة المستهدفة.

خامساً: استهداف نظم المواصلات:

ويتضمن هذا السيناريو اختراق نظم التحكم بخطوط الملاحة الجوية والبرية والبحرية، وإحداث خلل في برامج هبوط الطائرات وإقلاعها مما قد ينجم عنه حصول تصادم فيما بينها، أو تعطيل نظم الهبوط فلا تستطيع الطائرات الوصول إلى مدرج مطار من المطارات، كما يحتمل تمكن قراصنة المعلومات من السيطرة على نظم التحكم بتسيير القطارات وتغيير مواعيد الانطلاق فتسود الفوضى أو تتصادم القطارات فيما بينها، ومثل ذلك السفن والناقلات والغواصات البحرية. (حسين،٢٠٢٤،ص٤٩)

سادساً: استهداف نظم الاتصالات:

ويشمل هذا السيناريو استهداف شبكات المعلومات والشبكات الهاتفية للدولة، وتعطيل محطات توزيع الكهرباء والهاتف، وكذا الهجوم على أبراج بث الإرسال لخطوط الهواتف الجوالة وتوقف الاتصال والتواصل بين أفراد المجتمع والمؤسسات الحيوية، وهو ما ينشر الهلع والرعب، وحدوث نوع من الفوضى.

سابعاً: التهديد والترويع السيبراني

تقوم المنظمات الإرهابية بنشر التهديدات عبر الإنترنت وتتعدد هذه النماذج من التهديدات والهدف من ذلك نشر الخوف والرعب بين الأفراد والجماعات والدول والشعوب. (حسين،٢٠٢٤، ص٥٠)

ثامناً: التجسس السيبراني:

يقوم الإرهابيون بالتجسس على الأفراد أو الدول أو المنظمات أو لهيئات أو المؤسسات الدولية أو الوطنية، ويتميز التجسس السيبراني بالطريقة الحديثة التي تتمثل في توظيف الموارد المعلوماتية والأنظمة. الإلكترونية التي أنت بها تكنولوجيا عصر التقنية المثير وتستهدف عمليات التجسس السيبراني ثلاثة أهداف رئيسية وهي التجسس العسكري والتجسس السياسي والاقتصادي. (عباس، ٢٠٢٣، ص٩٩)

ومحاولة الدخول للشبكات والمعلومات والمواقع السيبرانية ممن يعبثون بهدف الاختراق المعلوماتي (**hackers**) لا يعد إرهاباً، فمخاطر هؤلاء تقتصر غالباً على العبث أو إتلاف المحتويات والتي يمكن استعادة نسخة أخرى مخزنة في موقع أمن، ويكمن الخطر الحقيقي في عمليات التجسس الإرهابي، وأجهزة الاستخبارات للحصول على أسرار الدولة وإفشائها لدول أخرى معادية. (كلاع، ٢٠٢٢، ص٥١)

تاسعاً: سرقة الهوية السيبرانية والبيانات الذاتية:

تعد سرقة الهوية السيبرانية من أخطر الجرائم التي تهدد مستخدمي الإنترنت، فقد تتعرض البيانات الذاتية للفرد المستخدم إلى السرقة بهدف تقمص شخصيته، والحصول على ما يملك من نقود وممتلكات أخرى، أو للزج باسمه في عمليات مشبوهة وغالباً ما يستعين سارق هذه الهوية بمعلومات متوفرة على الإنترنت وبخاصة على شبكات التواصل الاجتماعي، أو قواعد البيانات والمعلومات الوطنية، وشبكات الخدمات الحكومية، وما يتعلق بخدمة الضمان الاجتماعي للفقراء، ومواقع شبكات الرعاية الصحية، ومواقع التجارة الإلكترونية، والأسواق الافتراضية، وشبكات الصراف الآلي، وأسواق الأوراق المالية، وكل هذا يشكل خطراً كبيراً على مصالح المستخدمين، بالإضافة إلى مستقبل الخدمات السيبرانية، وقد تؤثر الهجمات الموسعة على القطاع المالي بوجه عام. (دوار، ٢٠١٧، ص ٢٥)

المطلب الثاني

تنظيم الامن السيبراني في القانون الكويتي

في ضوء التسارع نحو التحول التكنولوجي الذي تشهده دولة الكويت بدأ المشرع الكويتي بالعمل على تطوير قوانين قائمة تلبي احتياجات العصر التقني الحديث، وسن قوانين جديدة تتلاءم والمتغيرات الحاصلة في المستويين المحلي والدولي يتناول هذا المطلب كلاً من البنية التحتية للأمن السيبراني في الكويت. بالإضافة إلى التشريعات الجزائية الخاصة بحماية الأمن السيبراني في الكويت، وذلك على النحو الآتي:

الفرع الأول

البنية التحتية للأمن السيبراني في الكويت

بدأت الكويت أولى خطواتها تجاه تطوير مجتمع المعرفة وتوظيف التكنولوجيا الحديثة في جميع قطاعات الدولة عام ٢٠٠٩، ووضعت خطة التنمية القطاعية في مجال تكنولوجيا المعلومات كإستراتيجية الكترونية وطنية ضمن الخطة التنموية الخمسية للدولة (٢٠٠٩-٢٠١٤)، وأخذت بنظر الاعتبار إعلان مبادئ جنيف وخطة عمل جنيف والتي شملت المرحلة الأولى من القمة العالمية المجتمع المعلومات التي عقدت في جنيف خلال الفترة ١٠-١٢ كانون الأول (ديسمبر) ٢٠٠٣. وتضمنت وثيقتي إعلان المبادئ وخطة العمل على الصعيد العالمي، وبذلك أطلقت مرحلة التعاون الدولي لردم الفجوة الرقمية بين البلدان المتقدمة والبلدان النامية والتزام تونس، حيث عقدت مرحلة تونس من القمة العالمية المجتمع المعلومات من ١٦-١٨ (نوفمبر) ٢٠٠٥.

وينطبق النظام الداخلي والترتيبات الأخرى التي اتفق عليها في الاجتماع الأول للجنة التحضيرية المرحلة جنيف على مرحلة تونس من القمة والعملية التحضيرية التي سبقتها، والوثيقة الوطنية لبناء مجتمع المعلومات بدولة الكويت، والتي أقرت عام ٢٠٠٥ وصدرت عن الجهاز الفني المركزي لمشروع تطبيق

استخدام التكنولوجيا في الأعمال الحكومية في الكويت. والإستراتيجية العربية للاتصالات والمعلومات، التي وضعت أسسها عام ٢٠٠٩ بالتعاون بين جامعة الدول العربية واللجنة الاقتصادية والاجتماعية الغربي آسيا الإسكواء التابعة للأمم المتحدة، وحدثت هذه الإستراتيجية في ٢٩ (سبتمبر) ٢٠٢٢ من خلال عرضها على الاجتماع الحادي والثلاثين لفريق عمل الإستراتيجية العربية لتكنولوجيا المعلومات والاتصالات في بيروت. (الوثيقة الوطنية لبناء مجتمع المعلومات بدولة الكويت)

ومن هذه الانطلاقة حرصت الكويت على وضع أسس متينة للبنية التحتية الخاصة بالمعلومات والأمن المعلوماتي والسيبراني، إيماناً بأهمية التحول نحو مجتمع معرفي متمرس على تكنولوجيا المعلومات. وكان من أهم مبادئ الوثيقة الوطنية لبناء مجتمع المعلومات إعداد آلية تشريعية وقانونية المواجهة التطور الحديث في مجال استخدام تكنولوجيا المعلومات وتطوير السياسات والتشريعات الخاصة بأمن المعلومات (عبدالرحمن، ٢٠٢٣، ص ٢٥٧)

وفي التوجه نحو تأسيس للبنية التحتية للأمن السيبراني في الكويت تضمنت الخطة مشروع الإطار العام لأمن المعلومات الوطني"، بهدف وضع وتنفيذ إدارة خطة متكاملة لإنشاء بنية تحتية لأمن المعلومات الإلكتروني والأمن السيبراني، وهي خطة إستراتيجية للأمن السيبراني تغطي في مرحلتها الأولى القطاع الحكومي، ويتناول الإطار العام لأمن المعلومات الوطني كلاً من التصديق الإلكتروني على مستوى الدولة، وإجراءات إدارة الكوارث وضمان استمرارية الأعمال، بالإضافة إلى التشريعات والقوانين الخاصة بالأمن المعلوماتي الوطني، وقانون المعاملات الإلكتروني (عبدالرحمن، ٢٠٢٣، ص ٢٥٧).

وطورت الكويت بنيتها التحتية الخاصة بالأمن السيبراني استناداً إلى ما شهده العالم في العقدين الأخيرين من تسارع وتيرة الهجمات السيبرانية التي تضرب دول منطقة الخليج إذ شهدت هذه الدول العديد من التهديدات المرتبطة

بالهجمات السيبرانية التي طالت بعض المرافق الحساسة والمنشآت النفطية في بعض دول مجلس التعاون، وهذا بدوره تطلب تطويراً في التشريعات الجزائية الخاصة بحماية الأمن السيبراني في دول المجلس، وبما ينسجم مع المعايير والاتفاقيات والمعاهدات الدولية الخاصة بهذا الشأن (عبدالرحمن، ٢٠٢٣، ص ٢٥٧).

وكانت أحدث الخطوات التي اتخذت في مجال تطوير حماية البنى التحتية من الهجمات السيبرانية وتعزيز مستويات الأمن السيبراني في الدولة في سنة ٢٠٢١ إذ أعلن مؤخراً في دولة الكويت عن إنشاء وزارة الشؤون الاتصالات وتكنولوجيا المعلومات، التي عهد إليها تطوير البنية التحتية الإلكترونية. وتعزيز الأمن السيبراني، والارتقاء بمستوى الخدمات الحكومية الإلكترونية، وتنمية قطاع الاتصالات. (مرسوم أميري رقم ٢٠٢١/١٨)

كم تم انشاء المركز الوطني للأمن السيبراني، وهو جهاز حكومي كويتي يُعنى بالأمن السيبراني في دولة الكويت ووضع الإستراتيجية الوطنية لهذا القطاع لتأمين وحماية الشبكات المعلوماتية، وشبكة الاتصالات، ونظم المعلومات، وعمليات جمع وتبادل المعلومات باستخدام أي وسيلة إلكترونية. أسس في ٥ فبراير ٢٠٢٢ بمرسوم أميري أصدره نائب الأمير وولي العهد الشيخ مشعل الأحمد الجابر الصباح. (مرسوم أميري رقم ٢٠٢٢/١٥)

في حين أصدر الاتحاد الدولي للاتصالات التابع لمنظمة الأمم المتحدة المتخصصة بتكنولوجيا المعلومات والاتصالات، مؤشر الأمن السيبراني العالمي للعام ٢٠٢٤، والمتضمن ترتيب ١٩٤ دولة عالمياً في المؤشر لخمس فئات، وجاءت الكويت متأخرة في الفئة الثالثة.

في الختام، ليس الأمن السيبراني مجرد مسألة تكنولوجية؛ بل هو جانب أساسي من جوانب الأمن القومي والاستقرار الاقتصادي والخصوصية الفردية. في الكويت، كما في أي بلد آخر، يتطلب التصدي للتهديدات السيبرانية جهداً

مشتركاً من الأفراد والحكومات. من خلال تنفيذ تدابير الأمن السيبراني القوية وتعزيز التعاون وإيلاء الأولوية للتثقيف والتوعية.

الفرع الثاني

التشريعات الجزائية الخاصة بحماية الأمن السيبراني في الكويت

على المستوى الوطني، ونتيجة لتعدد المخاطر المرتبطة بالأمن السيبراني، ومواكبة للتوجهات العالمية والإقليمية الحديثة والخاصة بوضع سياسات جنائية لمواجهة الجرائم السيبرانية والهجمات المرتبطة بالفضاء السيبراني، قام المشرع الكويتي بخطوات حثيثة في مجال تطوير البيئة القانونية الخاصة بهذا الشأن فأصدر القانون رقم ٢٠ لسنة ٢٠١٤ بشأن المعاملات الإلكترونية، وبعدها أصدر القانون رقم ٣٧ لسنة ٢٠١٤ المتعلق بإنشاء هيئة تنظيم الاتصالات وتقنية المعلومات، تلاه لاحقاً القانون رقم ٩٨ لسنة ٢٠١٥ المتعلق بتعديل أحكام القانون رقم ٣٧ لسنة ٢٠١٤، وذلك في محاولة لاستكمال تطوير البيئة القانونية الخاصة بالتعامل مع الأمن السيبراني وجوانبه المختلفة وآثاره.

واستكمالاً لجهود تحديث القوانين والتشريعات الخاصة بالأمن السيبراني أطلقت الإستراتيجية الوطنية للأمن السيبراني في دولة الكويت ٢٠١٧-٢٠٢٠. (الهيئة العامة للاتصالات وتقنية المعلومات، ٢٠١٧)

وبهذا دخلت الكويت عالم الأمن السيبراني متأخرة مقارنة بدول مجلس التعاون الخليجي إذ أعلنت الحكومة الكويتية عن إستراتيجيتها الخاصة بالأمن السيبراني التي تعتبر فنية أكثر منها قانونية، وتقوم على ثلاثة أمور هي الرؤية والمهمة والأهداف، أما من حيث الأهداف الخاصة بهذه الإستراتيجية فقد تمثلت في كل من تعزيز ثقافة الأمن السيبراني التي تدعم الاستخدام الأمن والصحيح للفضاء الإلكتروني، وحماية ومراقبة الأصول والبنى التحتية الحيوية والمعلومات الوطنية والشبكة المعلوماتية بالكويت، بالإضافة إلى إتاحة سبل التعاون والتنسيق وتبادل المعلومات فيما بين مختلف الجهات المحلية والدولية في مجال الأمن السيبراني. (الجفناوي، ٢٠٢٣، ص ١٢٥)

واستمراراً في النهج الهادف إلى استحداث قوانين جديدة خاصة بالأمن

السيبراني أدخلت الجريمة السيبرانية إلى التشريع الكويتي بموجب القانون (رقم ٦٣ لسنة ٢٠١٥) المتعلق بمكافحة جرائم تقنية المعلومات، ويعتبر هذا القانون من أوائل القوانين الخليجية الخاصة بتجريم الأنشطة الإجرامية التي ترتكب في بيئة الفضاء السيبراني حيث يجرم كل من الدخول غير المشروع إلى نظام الحاسب أو نظامه أو إلى نظام المعالجة الإلكترونية للبيانات أو إلى نظام كومبيوتر مؤتمت أو إلى شبكة معلوماتية، والدخول غير المشروع إلى موقع أو نظام معلوماتي وجريمة تزوير مستند أو سجل أو توقيع إلكتروني، وجريمة التهديد والابتزاز والاستيلاء على الأموال والجرائم الماسة بالآداب العامة والجرائم الواقعة على الأطفال، وجرائم الاتجار بالبشر وجرائم المخدرات المرتكبة بوساطة تقنية المعلومات وغيرها. (المادة ٣ وما بعدها من القانون رقم ٦٣ لسنة ٢٠١٥)

ولعل أبرز ما يميز التشريعات الكويتية المنظمة للأمن السيبراني المرونة، وقد امتازت بها عن سواها من دول مجلس التعاون الخليجي. وقد حرصت على وجود دور فاعل الممثلين عن القطاع الخاص، وذلك من خلال تفعيل دور مشاركة القطاع الخاص في صياغة الإستراتيجيات الإلكترونية، ووجود مجموعة من ممثلي القطاع الخاص في المجلس الأعلى للتخطيط والتنمية، وهو الجهة المسؤولة عن الخطة التنموية الخمسية للدولة التي تتضمن الخطة القطاعية لتكنولوجيا المعلومات وأمنها، وما تضمنته إستراتيجية الأمن السيبراني التي خصصت مساحة كبيرة المشاركة القطاع الخاص. كما سعت الكويت جاهدة إلى تلبية المتطلبات الدولية الخاصة بإصدار قوانين ولوائح تتعلق بمكافحة الجرائم والهجمات السيبرانية، وحرصت على تفعيل بعض المبادرات الوطنية والإقليمية الخاصة بتأهيل وتدريب الكوادر الوطنية العاملة في مجال الأمن السيبراني. (محكمة الجنايات الكويتية بتاريخ ٢٠٢٠/١٠/٢٦)

إلا أنه على الرغم من التكلفة المرتفعة التي خصصت للإستراتيجية الوطنية للأمن السيبراني التي تشرف عليها الهيئة العامة للاتصالات وتقنية المعلومات في

الكويت التي بلغت ما يقارب ٣٨٢ مليون دولار أمريكي، فإن الكويت ما زالت تحتل المركز الخامس على المستوى الخليجي، والمركز ٦٥ على المستوى الدولي في تصنيف مؤشرات الأمن السيبراني.

إضافة إلى الإبطاء في إعداد مشروع قانون موحد للأمن السيبراني في دول مجلس التعاون الخليجي، فإن الأمر سيان على المستوى الدولي عموماً: فلا يوجد حتى اليوم صك دولي خاص بالأمن السيبراني ومخاطره، وفي ظل غياب مثل هذا الصك فإن دول مجلس التعاون الخليجي تستمر في تجريم أفعال الأمن السيبراني، مثل الجرائم السيبرانية والهجمات السيبرانية، وفقاً لما هو وارد في المعاهدات والاتفاقيات الدولية والإقليمية التي وضعت من أجل مكافحة الجرائم السيبرانية والهجوم السيبراني وما يرتبط بهما من أفعال إرهابية ترتكب في بيئة الفضاء السيبراني، ولا شك أن غياب صك دولي منظم للأمن السيبراني يعوق الجهود الخليجية الخاصة بالأمن السيبراني، ويعرقل عملية التعاون بشأن القضايا الخاصة بالإرهاب السيبراني. (العميري، ٢٠٢٤، ص١٩)

وقضت محكمة الجنايات الكويتية بتاريخ ٢٠٢٠/١٠/٢٦ بمعاقبة أحد المخترقين بالحبس لمدة سبع سنوات مع الشغل والنفاذ لاختراقه حساب وكالة الأنباء الكويتية (كونا) وإذاعته خبر غير صحيح عن القوات الأمريكية في الكويت.

المبحث الثاني

أوجه التعاون الدولي في مجال الأمن السيبراني

التعاون على الساحة الدولية أمر، أيضاً، حيوي في مكافحة الجريمة السيبرانية لذا يجب على الكويت المشاركة بنشاط في المبادرات الدولية للأمن السيبراني، وتبادل المعلومات الاستخباراتية مع الشركاء الدوليين، والمساهمة في تطوير المعايير والمعايير الدولية للأمن السيبراني.

المطلب الأول

التعاون الدولي بين أجهزة الشرطة

أدى التطور الكبير في وسائل المواصلات بصفة عامة والشبكة المعلوماتية بصفة خاصة إلى انتقال المجرمين من بلد إلى آخر، وقد أدرك المجتمع الدولي أنه بات من المستحيل على أي دولة أن تقوم بالقضاء على الجرائم العابرة للحدود، ذلك أن الإجراءات العامة لأجهزة الشرطة في كل دولة لا تجعل لجهازها الأمني تعقب المجرمين ومتابعتهم إذا ما عبروا حدود الدولة. وعليه فإن الحاجة إلى تعاون أجهزة الشرطة فيما بين الدول وتنسيق العمل فيما بينهم لمطاردة المجرمين. (الزهراني، ٢٠٢١، ص ٧٤٦)

وتتمثل هذه الصور والوسائل فيما يلي:

أولاً: ربط شبكات الاتصال والمعلومات:

يجري الاتصال بين أجهزة العدالة الجنائية الوطنية بصفة عامة وأجهزة الشرطة بصفة خاصة وبين تلك الأجهزة في الدول الأخرى عن طريق السلك الدبلوماسي، وحيث إن الاتصالات الشرطية تحتاج إلى اتصالات خاصة تحقق لها السرعة المطلوبة؛ لذا حاولت المنظمة الدولية للشرطة الجنائية «الإنتربول» وكذلك العديد من الدول تطوير نظم الاتصال وتبادل المعلومات فيما بينها، حتى يتم الوصول وتعقب المجرمين بمجرد خروجهم من الدولة التي تم ارتكاب الجريمة فيها فتقوم أجهزة شرطة الدولة المجني عليها بالاتصال السريع بالأجهزة

الأمنية في الدولة المتفق معها أمنيا للقيام بملاحقة المجرمين في حدود دولتهم التي هرب إليها. (شحاتة، ٢٠١١، ص١١٠)

ثانياً: المنظمة الدولية للشرطة الجنائية (إنتربول):

يعد الإنتربول 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 وتطوير كل النظم القادرة على المساهمة بفاعلية في الوقاية والعقاب على جرائم القانون العام. (سعود، ٢٠١٧، ص ١٣٩)

هذا ويعهد بتلك المهمة إلى المكاتب المركزية والوطنية في كل دولة عضو والى جهاز دائم يتم تعيينه بواسطة السلطات الحكومية الوطنية، وبمساعدة فرق الإنتربول للتحرك إزاء الأحداث التي يمكنها تيسير مجموعة من خدمات التحقيق والتحليل في موقع الحدث بالتنسيق مع الأمانة العامة. ويقوم الإنتربول بتعميم التحذيرات والتنبيهات المتضمنة المعلومات الاستخبارية والإحاطات والمشورة التحليلية والفنية عن الأخطار الإجرامية المحتملة، ويستخدم الإنتربول أدواته الخاصة كمنظومة النشرات الدولية بمختلف أنواعها و التقصي في قواعد البيانات وتقديم الخبرات والدورات التدريبية في مجال مكافحة جرائم الإنترنت، وذلك بالاستعانة بمجموعة من الخبراء الدوليين والمختبرات الدولية على الصعيد العالمي، وتيسير تبادل وتحليل وتخزين البيانات الجنائية حيث تقوم المنظمة بتزويد شرطة الدول الأطراف بكتيبات إرشادية حول جرائم الإنترنت وكيفية التدريب على مكافحتها والتحقيق فيها، ويعد الإجرام المالي المرتبط بالتكنولوجيا المتقدمة من الجرائم التي تركز عليها منظمة الإنتربول. (الزهراني، ٢٠٢١، ص ٧٥٠)

ثالثاً: 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 والإمكانيات وهو ما لا يمكن تحقيقه إلا بتركيز الجهود الدولية في مسار واحد، فعلى سبيل المثال: مشاركة قوات الإنقاذ والدفاع المدني للدول المنكوبة اثر الزلازل والأعاصير والفيضانات أو المشاركة بخبراء أو تقديم معدات متطورة. كذلك المشاركة بقوات خاصة أو خبراء أو تجهيزات في تحرير رهائن محتجزين، أو مباني هامة محتلة أو طائرات أو سفن مختطفة.(يوسف، ٢٠١١، ص ١٤٨)

رابعاً القيام ببعض عمليات شرطية دولية مشتركة:

من أمثلة 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. (الشمري، ٢٠١٦، ص٩٨)

المطلب الثاني

مظاهر التعاون الشرطي والقضائي على المستوى الدولي في مجال مكافحة الجرائم السيبرانية

يوازن التعاون الدولي بين استقلال الدولة في ممارسة اختصاصها الجنائي على حدود إقليمها، وبين ضرورة ممارسة حقها في حفظ الأمن وعقاب الخاطئ، فبدون هذا التعاون فلا يمكن للدولة من الناحية العملية إقرار حقها في حفظ الأمن وعقاب الجاني.

الفرع الأول

مظاهر التعاون الدولي الشرطي في مجال مكافحة الجرائم السيبرانية

أولاً: شرطة الويب الدولية:

أنشئت هذه المنظمة في الولايات المتحدة الأمريكية عام ١٩٨٦ لتلقي شكاوى مستخدمي الشبكة وملاحقة الجناة والقراصنة إلكترونيا والبحث عن الأدلة ضدهم وتقديمهم للمحاكمة. ويضم فريق العمل بهذه المنظمة متخصصين من هيئات إنفاذ القانون والمؤسسات الحكومية وضباط الشرطة ومتطوعين فنيين من ٦١ دولة حول العالم. ونظرا لاتساع نشاط هذه المنظمة وما تقوم به من إجراءات بالتعاون مع وكالات إنفاذ القانون في الدول الأعضاء فإن ذلك يسهل الأمر لفريق العمل بتتبع الأنشطة الإجرامية التي ترتكب من خلال شبكة الإنترنت على مستوى العالم. وفي إطار مسألة الضوابط القانونية التي تحكم حركة مرور المعلومات عبر شبكة الإنترنت، فهناك من يرى أنه من الضروري وضع ضوابط وقواعد بحيث لا تؤدي إلى المساس بالحريات العامة في تبادل المعلومات وحقوق الإنسان من ناحية، والا تستخدم الشبكة لأغراض إجرامية أو نشر مواد إباحية تسيء إلى المجتمع من ناحية أخرى. (http://www.web-police.org)

ويرى الباحث أن الإشكالية ليست في حجب الصور والمواقع الإباحية، بل من الأكثر من ذلك المواقع التي تبث أفكار تفسد المجتمع والتي تدعو إلى

التظاهرات أو الانقلابات تحت ما يسمى بالحريات العامة وحقوق الإنسان، فحق المجتمع في الاستقرار والتقدم والرقي أهم بكثير من النظر إلى حق الفرد أو المصلحة الخاصة.

إلا أن الصعوبة التي تواجه أجهزة شرطة الإنترنت عندما تنفذ الجريمة من خلال مقاهي الإنترنت، ففيها يقوم العملاء بتنفيذ ما يريدون من جرائم دون إمكانية تحديدهم حيث لا تتطلب هذه المقاهي من عملائها أثبات شخصيتهم. ومثال على ذلك إن المباحث الفدرالية بالولايات المتحدة بعد أن تتبعت أحد القراصنة، والذي اخترق شبكة معلومات أحد المصارف إلا أنها لم تستطع تحديده ومحاكمته؛ لأنه تبين انه نفذ عمليته من خلال عدة مقاهي للإنترنت. (الزهراني ، ٢٠٢١، ص ٧٤٨)

ولحل تلك الإشكالية يرى الباحث أنه يجب على الدول إلزام أصحاب مقاهي الإنترنت بإثبات شخصيات رواد المقهى قبل الدخول بالإضافة إلى وجود كاميرات مراقبة تبين بوضوح تفاصيل وجه جميع رواد المقهى ولا يعتمد على إثبات الشخصية فقط لأنه من الممكن أن تكون البيانات الواردة في تحقيق الشخصية مزورة فتقوم الكاميرات بتحديد شخص المستخدم.

ثانياً: مركز بلاغات احتيالات الإنترنت:

تم إنشاء هذا المركز في الولايات المتحدة الأمريكية بتاريخ ٢٠٠٠/٥/١٨ ليتعاون مع مكتب التحقيقات الفيدرالي **FBI** و المركز القومي لجرائم ذوي الياقات البيضاء(**National white collier crime center**)، وذلك بهدف تلقى البلاغات وتتبع الجرائم والاحتيالات التي ترتكب من خلال شبكة الإنترنت بالتنسيق مع أجهزة المكافحة والضبط المعنية داخل الولايات المتحدة الأمريكية وخارجها من خلال موقع المركز على الشبكة الدولية.

ومن أجل إحكام الرقابة على شبكة الإنترنت طبقت دولة الإمارات العربية المتحدة ما يعرف بنظام الرقيب **proxy** الذي يقوم بمراجعة نوعية الخدمات

المقدمة عبر شبكة الإنترنت. فعندما يطلب المشترك موقعا على الشبكة الأم، تصل الإشارة إلى الرقيب الذي يقوم بدوره بعرض الموضوع على قائمة كبيرة جدا من المواقع الممنوعة فإذا تبين له أن الموقع المطلوب يدخل ضمن هذه القائمة المحظورة فلا يستطيع المشترك الحصول على هذا الموقع وتظهر له على الشاشة رسالة بعنوان "تم منع هذا الموقع بواسطة رقيب إنترنت الإمارات". (الصغير، ٢٠١١، ص٦٠)

الفرع الثاني

مظاهر التعاون الدولي القضائي في مجال مكافحة الجرائم السيبرانية

لابد من التعاون القضائي الدولي لسببين:

السبب الأول: إن الدولة تتقيد بحدودها الإقليمية، فقانون العقوبات يمكن أن يتعدى نطاق تطبيقه إلى ما يجاوز حدود إقليم الدولة، إلا أنه لا يمكن مباشرة الإجراءات خارج الإقليم الوطني لأن ممارستها تمس سيادة الدول الأجنبية الأخرى. (المري، ٢٠٢٣، ص٢٥٦)

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 فإنه يجب عدم الاصطدام بمشكلة الحدود الإقليمية بين الدول، ووجب الالتجاء إلى التعاون القضائي لتذليل هذه الصعوبة، ويتمثل هذا التعاون في مجموعة من الوسائل التي بواسطتها تقدم إحدى الدول المعاونة سلطاتها العامة أو مؤسساتها القضائية إلى سلطة التحقيق أو الحكم أو التنفيذ في دولة أخرى.

أولاً: المساعدة القضائية:

وحيث إن جرائم الإنترنت ذات طابع عالمي وبالتالي يمكن أن تتعدى آثارها عدة دول فإن ملاحقة مرتكبي هذه الجرائم وتقديمهم للمحاكمة وتوقيع العقاب عليهم يستلزم القيام بأعمال إجرائية خارج حدود الدولة، مثل المعاينة، أو ضبط القراص الصلبة التي توجد عليها معلومات غير مشروعة أو تفتيش الوحدات الطرفية في حالة الاتصال عن بعد أو القبض على المتهمين أو سماع الشهود أو اللجوء إلى الإنابة القضائية أو تقديم المعلومات التي يمكن أن تسهم في تحقيق الجرائم. فكل ذلك لن يتحقق إلا بمساعدة الدول الأخرى. (الغافري، ٢٠٠٩، ص ١٩٩)

وتتخذ المساعدة القضائية عدة صور

١ـ تبادل المعلومات:

يتمثل ذلك في تقديم المعلومات والوثائق التي تطلبها سلطة قضائية أجنبية بصدد جريمة من الجرائم عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم، كما أن هناك مظهر آخر من مظاهر تبادل المعلومات وهو ما يتعلق بالسوابق القضائية للجناة من خلالها تتعرف الجهة القضائية بدقة على الماضي الجنائي للفرد المحال إليها، فهي التي تساعد في تطبيق الأحكام الخاصة بالعود ووقف تنفيذ العقوبة وعدم الأهلية.(الزهراني، ٢٠٢١، ص ٧٥١)

٢ـنقل الإجراءات:

يقصد بنقل الإجراءات قيام الدولة بناء على اتفاق باتخاذ إجراءات جنائية بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة وذلك إذا توافرت الشروط التالية:

١-أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب منها.

٢-يجوز لأي طرف متعاقد أن يطلب من أي طرف آخر أن يتخذ الإجراءات الجزائية في أي حالة من الحالات الآتية:

*إذا كان الشخص المتهم خاضعًا أو سيخضع لحكم يقيد الحرية في الدولة الطالبة.

*إذا كانت الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة.

*أن يكون الإجراء المطلوب اتخاذه يؤدي إلى الوصول إلى الحقيقة، كأن تكون أدلة الجريمة الموجودة بالدولة المطلوب إليها.

*إذا كان تنفيذ الحكم في الدولة المطلوب إليها يحقق إعادة التأهيل الاجتماعي للشخص المحكوم عليه.

*إذا كان حضور الشخص المتهم في الجلسة لا يمكن ضمانه في الدولة الطالبة بينما يتحقق ضمان حضوره في الدولة المطلوب إليها.

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

*إذا كان طلب نقل الإجراءات ليس له ما يبرره بأن تكون الأسباب التي ذكرتها الدولة الطالبة لا تدعو لاتخاذ مثل هذ الإجراءات.

*إذا ثبت أن الباعث من وراء طلب نقل الإجراءات اعتبارات عنصرية أو دينية أو سياسية.

*إذا كانت الدولة المطلوب إليها قد طبقت قانونها على الجريمة قبل استلامها من الدولة الطالبة وكان الإجراء الذي سبق اتخاذه مطابقا للقانون.

*إذا كانت الإجراءات التي تطلبها الدولة الطالبة مخالفة لواجبات ملتزمة بها الدولة المطلوب إليها.

*إذا كانت الإجراءات المطلوبة مخالفة للمبادئ الأساسية للنظام القانوني في الدولة المطلوب إليها.

إلا أن هناك رأي يرى وبحق، أن تطبيق هذه الآليات التقليدية من الاتفاقيات يثير بعض المشاكل، مثل وجود عقبات خاصة بالجرائم التي ترتكب عبر شبكة الإنترنت وأن كانت تلك العقبات موجودة على المستوى المحلى أو الوطني إلا أنها تثار أيضا على المستوى الدولي، ومن بين هذه العقبات، تتبع الاتصالات الإلكترونية عن طريق سلطات التحقيق وإقامة الدليل على الجرائم التي ترتكب في مجال الإنترنت وذلك بالنظر إلى الاختلافات التي توجد بين التشريعات المختلفة فيما يتعلق بشروط قبول الأدلة وتنفيذ بعض الإجراءات مثل التفتيش عبر الحدود ووقف بث الرسائل ذات المحتوى غير المشروع. (الصغير، ٢٠١١، ص٩٢)

ثانياً: الإنابة القضائية الدولية :

تعد الإنابة القضائية احدى صور المساعدة القضائية للتعاون العقابي الدولي، فهي تجعل دولة ما تتمكن من الاستفادة من السلطات العامة لدولة أخرى إذا ما حالت الحدود الإقليمية دون نفاذ قانونها تجاه المجرم. (الغافري، ٢٠٠٩، ص ٢٥٩)

ويقصد بالإنابة القضائية الدولية، طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجزائية تتقدم به دولة الدولة الطالبة إلى الدولة المطلوب إليها لضرورة ذلك للفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها. (الزهراني، ٢٠٢١، ص ٧٦٦)

وعلى ذلك فالإنابة القضائية هي إجراء لتسهيل الإجراءات الجزائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة، والتغلب على عقبة السيادة الإقليمية التي تمنع الدول الأجنبية من ممارسة بعض الأعمال

القضائية داخل إقليم الدول الأخرى. ومن أمثلة ذلك سماع الشهود وإجراءات السير في الدعوى الجزائية. (السند، ٢٠١١، ص١٠٨)

وتتم الإنابة القضائية بين الدول عن طريق الاتفاقيات والتي تتضمن شروط وأساليب تنفيذ الإنابة القضائية، وغالبا ما تتضمن شرط باستبعاد تنفيذ الأحكام في المجال السياسي والضريبي والعسكري، أو اذا قدرت الدولة المطلوب منها أن التنفيذ المطلوب من شأنه المساس بسيادة الدولة أو النظام العام أو المصالح الأساسية الأمر الذي يترك للدولة سلطة تقديرية لتنفيذ أو عدم تنفيذ ما يطلب منها وذلك خشية قيام مسؤوليتها دوليا عن إهمالها. وفي ظل عدم وجود اتفاقية فإن الإنابة القضائية لا يمكن تنفيذها إلا إذا وافقت الدولة المطلوب إليها على ذلك وفقا للإجراءات والشروط المنصوص عليها في القانون الداخلي لها. (الصغير، ٢٠١١، ص ٨٥)

كذلك برز التعاون الدولي في مجال مكافحة الجرائم السيبرانية عن طريق عقد دورات التدريب الدولية للأجهزة الوطنية للدول المنوط بها التصدي لتلك الجرائم على المستوى الوطني، والوصول إلى نتيجة مهمة وهي أن الدول المتقدمة لن تستطيع بمفردها مواجهة تلك الجرائم دون تعاون مشترك مع الدول النامية والعمل على تدريب الجهات الأمنية داخل الدول النامية لمواجهة تلك الجرائم.

وعلى الرغم من وجود هذا التعاون الدولي الملموس إلا أن هناك صعوبات ومعوقات أمام هذا التعاون تحد من فاعلية إنفاذ التعاون تمثلت في: (الزهراني، ٢٠٢١، ص٧٧٥)

١-تنوع واختلاف النظم القانونية والإجرائية من دولة إلى أخرى من حيث طرق التحري والتحقيق ومدى قانونية ومشروعية الإجراءات الجنائية من دولة إلى أخرى، فما يعتبر إجراء مشروع في دولة قد يعتبر غير مشروع في دولة أخرى.

٢-كذلك مشكلة الاختصاص القضائي قد يحد من هذا التعاون حيث إن اختلاف التشريعات والنظم القانونية ينتج عنه تنازع في الاختصاص القضائي بين الدول مما يعوق التعاون الدولي.

٣-وجود شرط التجريم المزدوج الواجب توافره لا نفاذ تسليم المتهمين بعد عائقاً يحول دون إنفاذه لأنه قد يجرم فعل في دولة دون الأخرى مما يترتب معه عدم إمكانية تسليم المجرم.

٤-كذلك اذا كان هناك مساعدات قضائية دولية إلا أن آلية تنفيذها يتم عن طريق دبلوماسي يتميز بالبطء والتعقيد الذي يتعارض مع طبيعة الجريمة السيبرانية والإنترنت الذي يتميز بالسرعة.

□

الخاتمة

لا تزال الكويت في حاجة ماسة إلى مزيد من الاستثمار في الأمن السيبراني، وذلك في ثلاثة اتجاهات مالية وتقنية وقانونية، وتدعو التطورات التكنولوجية الحديثة إلى مزيد من الاستثمارات المالية في القطاعين العام والخاص من أجل تطوير البنية التحتية وحمايتها، بالإضافة إلى الحاجة إلى مزيد من الكوادر الوطنية المؤهلة في العمل السيبراني: إذ إن حساسية هذا القطاع وخطورته تتطلب وجود كوادر وطنية خليجية مؤهلة ومدربة قادرة على التعامل مع مخاطر الهجمات السيبرانية وآثارها، بالإضافة إلى ضرورة تطوير البيئة التشريعية الخاصة بالأمن السيبراني، من خلال فرض مزيد من المرونة على التعامل والتكامل بين القطاعين العام والخاص في هذا الشأن؛ إذ إن الأمن السيبراني الكامل لا يمكن أن يتم تحقيقه في ظل جهود حكومية رسمية فحسب وإنما هو نتاج تضافر جهود كل من القطاعين العام والخاص؛ حيث إن البيئة السيبرانية تمتد لتربط بين المؤسسات العامة والخاصة، كما تمتد لتربط بين المؤسسات المدنية والمؤسسات العسكرية على حد سواء.

والتطوير التقني والقانوني لبيئة الأمن السيبراني لا يتم بمعزل عن تطوير المناهج والعملية التعليمية الخاصة بهذا الشأن؛ ففي حين بدأت العديد من الدول إدراج الفضاء السيبراني في مناهجها الجامعية منذ عقد أو أكثر، فلا تزال الجامعات الحكومية والخاصة تعاني من تأخر ملموس في هذا الميدان، حتى في التخصصات الأكاديمية التي ترتبط بالحاسوب وأنظمته.

وفي ضوء ذلك يمكن حصر مجموعة من النتائج والتوصيات الآتية:

(أ) نتائج الدراسة:

١-تكنولوجيا المعلومات والاتصالات أصبحت بنية تحتية عالمية لكل من الحكومات والشركات، ولا تقل أهمية في أي حال من الأحوال عن البنيات التحتية التقليدية.

٢-الأمن السيبراني أصبح ضرورة مطلقة، فهو خط الدفاع الأول القادر على صد الهجمات السيبرانية المحتملة، وهو الآلية التي يتم من خلالها حماية أمن المعلومات والاتصالات والمرافق والمنشآت الحيوية المهمة أي حماية الأمن القومي الكلي حيث تحولت بيئة التهديد للبنية التحتية الحيوية من شكلها التقليدي القديم إلى شكلها التكنولوجي الحديث، وهذا التحول لا بد أن يصاحبه تحول في التشريعات والقوانين الخاصة بحماية الأمن السيبراني.

٣-في الكويت، كما في أي بلد آخر، يتطلب التصدي للتهديدات السيبرانية جهداً مشتركاً من الأفراد والحكومات. من خلال تنفيذ تدابير الأمن السيبراني القوية وتعزيز التعاون وإيلاء الأولوية للتثقيف والتوعية.

٤-وجود تعاون بين أجهزة الشرطة في مختلف الدول وأبرز هذا التعاون إنشاء المنظمة الدولية للشرطة الجنائية (الإنتربول) وذلك لمكافحة الجرائم العابرة للحدود ومن بينها الجرائم السيبرانية.

٥-الأمن السيبراني مجرد مسألة تكنولوجية؛ بل هو جانب أساسي من جوانب الأمن القومي والاستقرار الاقتصادي والخصوصية الفردية.

٦-الجرائم السيبرانية أصبحت تشكل تحدياً كبيراً للأمن القومي وكذلك الدولي، لدرجة أن العديد من الباحثين اعتبر الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء هو ما استدعى ضرورة وجود ضمانات كافية لمواجهته

٧-حرصت الكويت على وضع أسس متينة للبنية التحتية الخاصة بالمعلومات والأمن المعلوماتي والسيبراني، إيماناً بأهمية التحول نحو مجتمع معرفي متمرس على تكنولوجيا المعلومات. وكان من أهم مبادئ الوثيقة الوطنية لبناء مجتمع المعلومات إعداد آلية تشريعية وقانونية المواجهة التطور الحديث في مجال استخدام تكنولوجيا المعلومات وتطوير السياسات والتشريعات الخاصة بأمن المعلومات

٨-تعدد أبعاد الأمن السيبراني فتشمل جميع الجوانب الاقتصادية الاجتماعية، والسياسية، والإنسانية، فهو له القدرة على حماية أمن ومصلحة الدولة وشعبها في مختلف مجالات حياته اليومية وذلك لكونه مرتبط ارتباطا وثيقا بسلامته وأمن البيانات والمعلومات

٩-في ضوء التسارع نحو التحول التكنولوجي الذي تشهده دولة الكويت بدأ المشرع الكويتي بالعمل على تطوير قوانين قائمة تلبي احتياجات العصر التقني الحديث، وسن قوانين جديدة تتلاءم والمتغيرات الحاصلة في المستويين المحلي والدولي .

١٠-يوازن التعاون القضائي الدولي بين استقلال الدولة في ممارسة اختصاصها الجنائي على حدود إقليمها، وبين ضرورة ممارسة حقها في العقاب، فبدون هذا التعاون فلا يمكن للدولة من الناحية العملية إقرار حقها في العقاب.

١١-يبرز دور المجتمع الدولي في مواجهة تلك الجرائم من خلال التعاون الدولي القضائي من خلال تبادل المعلومات والوثائق التي تطلبها السلطات القضائية الأجنبية بصدد جريمة من الجرائم وكذا نقل الإجراءات وذلك من خلال قيام الدولة بناء على اتفاق باتخاذ إجراءات جنائية بصدد جريمة ارتكبت في إقليم دولة أخرى، وتفعيل الإنابة القضائية التي تجعل دولة ما تتمكن من الاستفادة من السلطات العامة في دولة أخرى إذا ما حالت الحدود الإقليمية دون نفاذ قانونها تجاه المجرم.

ثانياً: توصيات الدراسة:

١) يجب على الكويت المشاركة بنشاط في المبادرات الدولية للأمن السيبراني، وتبادل المعلومات الاستخباراتية مع الشركاء الدوليين، والمساهمة في تطوير المعايير والمعايير الدولية للأمن السيبراني.

٢) تنفيذ عمليات شرطية مشتركة بين الدول لتعقب الجناة الذي يبدأ في دولة وينتهي على إقليم دولة أخرى، وإنشاء شرطة الويب الدولية ومركز بلاغات الاحتيالات الإنترنت بهدف تلقي البلاغات وتتبع الجرائم والاحتيالات التي ترتكب من خلال شبكة الإنترنت.

٣) محاولة الفصل بين الجرائم السيبرانية والهجمات السيبرانية، إذ إن ما ينطبق على الجريمة السيبرانية تعالجه القوانين الوطنية عادة، في حين أن ما ينطبق على الهجوم السيبراني يندرج ضمن القوانين الدولية، والقانون الدولي الإنساني على وجه الخصوص.

٤) تدريب الكوادر البشرية الخليجية على أحدث مستجدات الأمن السيبراني وأمن المعلومات، وما يرتبط بها من متغيرات وذلك نظراً للحاجة إلى كفاءات وطنية خليجية قادرة على التصدي للتهديدات السيبرانية الحالية والمستقبلية، وذلك بما يتفق مع توصيات اللجنة الوزارية للأمن السيبراني بدول مجلس التعاون.

٥) على الرغم مما أحرزته دول الخليج من تقدم على مؤشرات الأمن السيبراني، فإن سن قانون موحد للأمن السيبراني لا يزال يشكل أهمية مطلقة في ظل التكتلات الدولية التي يشهدها العالم في بيئة الفضاء الإلكتروني إذ إن أمن المعلومات والاتصالات لا يعمل بمعزل عن باقي الدول، وإنما هو شبكات دولية ممتدة بين مختلف الدول والقارات ومن ثم فإن الفاعلية الحقيقية المرجوة من قوانين الأمن السيبراني تصبح أكثر جدوى إذا ما تمت على نطاقات إقليمية، وليس وطنية فقط.

٦) العمل على إبرام اتفاقيات دولية يتم فيها توحيد وجهات النظر بين الدول في مسألة تنازع الاختصاص القضائي فيما يتعلق بجرائم الإنترنت وتحديث القوانين الجنائية الموضوعية والإجرائية بما يتناسب مع خصوصيات الجرائم السيبرانية.

قائمة المراجع

(أ) كتب ومصادر علمية:

الإستراتيجية الوطنية للأمن السيبراني في دولة الكويت ٢٠١٧-٢٠٢٠ أعدتها الهيئة العامة للاتصالات وتقنية المعلومات بدولة الكويت سنة ٢٠١٧.

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

الجامعة اللبنانية (٢٠١٧)، مؤتمر الأمن السيبراني والدفاع السيبراني تحديات وآفاق – AEF٦.

الدهيسات، معاذ (٢٠٢٣)، الأمن السيبراني، وزارة الثقافة، الأردن.

شحاتة، علاء الدين (٢٠١١)، التعاون الدولي في مجال مكافحة الجريمة، دار الكتب، القاهرة.

الصغير، جميل عبد الباقي (٢٠١١)، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة.

الغافري، حسين بن سعيد (٢٠٠٩)، الجهود الدولية في مواجهة جرائم الإنترنت، دار النهضة العربية، القاهرة.

القاضي، رامي متولي (٢٠١١)، مكافحة الجرائم المعلوماتية، ط١، دار النهضة العربية، القاهرة.

مكتب الأمم المتحدة المعني بالمخدرات والجريمة (٢٠١٩)، الجريمة السيبرانية والإيقاع الإجرامي التقليدي بالضحايا، دراسة شاملة عن الجريمة السيبرانية، مسودة شباط / فبراير.

المناعسة، أسامة، الزعبي، جلال (٢٠١٠)، جرائم تقنية نظم المعلومات الإلكترونية، دار الثقافة للنشر، عمان.

يوسف، حسن يوسف (٢٠١١) الجرائم الدولية للإنترنت المركز القومي للإصدارات القانونية، القاهرة.

(ب) أبحاث علمية منشورة:

جربوعة، عادل، بوطمين، عبد الجبار (٢٠٢٣)، الفضاء الرقمي والامن السيبراني، مجلة العلوم الإنسانية، مج٣٤، ع٣، جامعة منتوري قسنطينة، الجزائر.

الجنفاوي، خالد (٢٠٢٣)، التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت، حوليات آداب عين شمس، مج٥١، جامعة عين شمس، سبتمبر.

حسين، أحمد سالم (٢٠٢٤)، الأمن السيبراني القوة الرابعة لتعزيز الأمن والدفاع: البنية التحتية

- الفوائد والمخاطر، مجلة الدراسات المستدامة، مج٦، ع١، الجمعية العلمية للدراسات التربوية المستدامة، العراق.

الحيمودي، بدر (٢٠٢٣)، الامن السيبراني وحماية الأنظمة المعلوماتية، مجلة شمال أفريقيا للنشر العلمي، مج١، ع٢، المغرب

الزهراني، شيخة (٢٠٢١)، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، مج١٧، ع١، وحدة النشر العلمي، جامعة الشارقة للعلوم القانونية، الإمارات العربية المتحدة.

سعود، صالح (٢٠١٧)، الانتربول ودوره في التعاون الأمني الدولي، مجلة المنارة للدراسات القانونية والإدارية، ع٢١، المغرب.

الضفيري، ناجي (٢٠٢٤)، الوعي بالأمن السيبراني لدى معلمي المرحلة المتوسطة بدولة الكويت وعلاقته بمستوى توظيفهم للتكنولوجيا في التدريس، مجلة الدراسات والبحوث التربوية، مج٤، ع١١، مركز العطاء للاستشارات التربوية، الكويت.

عباس، محمد خزعل (٢٠٢٣)، أمن الفضاء السيبراني " قراءة في المفهوم القانوني"، مجلة العلوم القانونية، مج٣٧، كلية القانون، جامعة بغداد، العراق.

العبيدي، أسامة بن غانم (٢٠١٢)، أهمية التعاون الدولي في مكافحة جرائم الانترنت، مجلة الدبلوماسي، ع٦٣، معهد الأمير سعود الفيصل للدراسات الدبلوماسية، الرياض.

عزت، محمود (٢٠١٨)، الفضاء السيبراني وتحديات الأمن المعلوماتي العربي ، المجلة العربية ، العدد ٤٩٨ أبريل.

العميري، مطلق (٢٠٢٤)، استراتيجيات الإعلام الالكتروني في الكويت تجاه الامن السيبراني، المجلة العربية للعلوم الإنسانية، مج٤٢، ع١٦٥، مجلس النشر العلمي، الكويت.

غازي، فاروق السيد (٢٠١٤)، التعاون الدولي في مجال الوظيفة القمعية للمحكمة الجنائية الدولية، مجلة التواصل، ع٣٨، جامعة عنابة، المغرب.

الفتلاوي، أحمد عبيس (٢٠١٧)، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، الجزائر.

كلاع، شريفة (٢٠٢٢)، الأمن السيبراني وتحديات الجوسسة والاختراقات الالكترونية عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، ع١٥، كلية الحقوق، جامعة السادات.

لامية، طالة (٢٠٢١)، الإرهاب السيبراني والأمن القومي: قراءة في تحولات الاستراتيجية الدفاعية، حوليات جامعة الجزائر، مج٣٥، ع٤، جامعة الجزائر، ديسمبر.

لخضر، حرزالله (٢٠٢٣)، جرائم الإنترنت وتحديات الأمن السيبراني: دراسة في متغيرات الجريمة ومقارباتها العلاجية، مجلة المفكر، مج١٨، ع١، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر.

المري، راشد (٢٠٢٣)، الأمن السيبراني وحماية الأنظمة الالكترونية "دراسة تحليلية تأصيلية"، مجلة الدراسات القانونية والاقتصادية، مج٩، ع١، كلية الحقوق، جامعة السادات.

(ج) رسائل وأطروحات علمية:

داود، عيسى سليم (٢٠١٧)، جرائم القرصنة الإلكترونية رسالة ماجستير غير منشورة، كلية الحقوق، جامعة الإسكندرية.

دوار، نسيمة (٢٠١٧)، الأمن المعلوماتي وسبل مواجهة مخاطرة في التعامل الإلكتروني، أطروحة دكتوراه غير منشورة، جامعة أبو بكر بالقايد، يلميسان.

السند، متعب (٢٠١١)، التعاون الدولي في تنفيذ الأحكام الجنائية واثره في تحقيق العدالة، رسالة ماجستير غير منشورة، كلية الدراسات العلياء جامعة نايف العربية للعلوم الأمنية الرياض ٢٠١١.

(د) قوانين وأحكام قضائية:

أنشئت الوزارة بموجب المرسوم الأميري رقم ٢٠٢١/١٨ الصادر في ٢٠٢١/٣/٢ الخاص بتشكيل الوزارة منشور في الجريدة الرسمية الكويت اليوم العدد ١٥٢٥ السنة السابعة والستون، بتاريخ ٢٠٢١/٣/٧.

القانون رقم ٦٣ لسنة ٢٠١٥ المتعلق بمكافحة جرائم تقنية المعلومات.

مرسوم أميري بإنشاء المركز الوطني للأمن السيبراني" .جريدة الرأي الكويتية. ٥ (فبراير) ٢٠٢٢. مؤرشف من الأصل في ٤ يونيو ٢٠٢٣ .

المرسوم الأميري رقم ٢٠٢١/١٨ الصادر في ٢٠٢١/٣/٢ الخاص بتشكيل الوزارة منشور في الجريدة الرسمية الكويت اليوم العدد ١٥٢٥ السنة السابعة والستون، بتاريخ ٢٠٢١/٣/٧.

(هـ) مواقع الكترونية:

القلاف، على وليد (٢٠٢٤) أهمية الامن السيبراني لحماية الكويت، جريدة القبس

-أهمية-الأمن-السيبراني-لحماية-الكويت/٥٩٣٠٦٣٨/**www.alqabas.com/article**

معلومات عن الإنتربول لمحة عامة الموقع الرسمي لمنظمة الشرطة الجنائية الدولية، على الموقع الإلكتروني

https://www.interpol.int/ar/