https://www.doi.org/10.34120/0382-049-190-008

الإطار القانوني للأمن السيبراني لدول مجلس التعاون الخليجي

فهد أحمد عبدالرحمن[1]

ملخص

الأهداف: هدفت الدراسة إلى استعراض واقع القوانين الدولية والخليجية المنظمة للأمن السيبراني، ووضع تصور مقترح لقانون موحد ومنظم له في دول مجلس التعاون؛ للتصدي للتهديدات الحالية والمستقبلية، والمواءمة بين المركزية والمرونة في التشريعات الخاصة بالأمن السيبراني في دول المجلس، عبر المفاضلة بين إيجابيات كل منهما وسلبياته، وتقديم توصيات مستقبلية لصناع القرار والقانونيين المختصين لحماية الأمن السيبراني لدول المجلس. **المنهج:** اتبعت الدراسة المنهج التاريخي الخاص بالقوانين المنظمة للأمن السيبراني في دول المجلس، سواء على المستوى الوطني لكل دولة، أو على المستوى الإقليمي للدول مجتمعة، والقوانين العربية والدولية الخاصة بالأمن السيبراني ومدى انسجام القوانين الخليجية معها. والمنهج التحليلي لكيفية المواءمة بين المركزية والمرونة الخاصة بالأمن السيبراني في دول المجلس دون المساس بالسيادة الوطنية وقوانينها، ووضع تصور مقترح لأهم البنود الواجب تضمينها في القانون الخليجي الموحد للأمن السيبراني. **النتائج:** أظهرت النتائج عدم وجود تعريف دولي موحد لمفهوم الأمن السيبراني، وعدم وجود تعريفات محددة لكل من الجريمة السيبرانية والهجوم السيبراني والفرق بينهما. كذلك انطباق قواعد القانون الدولي الإنساني على الهجمات السيبرانية في حال تحقق شرط التزامن بين الهجوم السيبراني والهجوم التقليدي، وغياب قانون موحد للأمن السيبراني في دول مجلس التعاون، وغياب إستراتيجية إقليمية كلية جامعة لهذه الدول. **الخاتمة:** غياب قانون خليجي موحد للأمن السيبراني في دول مجلس التعاون يضعف من قدراتها على مواجهة الهجمات السيبرانية، وغياب تعريفات محددة للجريمة السيبرانية والهجوم السيبراني والفروقات بينهما يعطل الآلية القانونية الملائمة للتعامل معهما.

الكلمات المفتاحية: الأمن السيبراني، الأمن القومي، القانون الخليجي الموحد للأمن السيبراني، السيادة الوطنية

(1) باحث قانوني مستقل، الكويت، الإيميل: L-F8D@hotmail.com
- تُسلم البحث في: 2022/10/4، عُدّل في: 2022/12/5، أجيز للنشر في: 2022/12/28.

للاستشهاد بهذه المقالة انظر ص.298

The legal framework of cyber security for the Gulf Cooperation Council Countries

Fahed A. Abdulrahman[(1)]

Abstract

Objectives: The study aimed to review reality of international and Gulf laws regulating of cyber security, and develop a proposed vision for unified and regulating law in the GCC to address current and future threats, and to harmonize between centralization and flexibility in cyber security legislation, through weighing the pluses to the minuses, and presenting recommendations for decision makers and legal professionals to protect cyber security. **Method:** The study followed historical approach of the regulating of cyber security in the GCC, whether at the national level for each country, or at the regional level combined, and the Arab and international laws related to cyber security and the extent to which Gulf laws are compatible with them. And analytical approach to harmonize between centralization and flexibility related to cyber security in the GCC without prejudice to national sovereignty and its laws. **Results:** The results showed no unified international definition of the concept of cyber security, and the absence of specific definitions for both cyber crime and cyber attack and the difference between them. The rules of international humanitarian law also apply to cyber attacks if the condition of simultaneity between the cyber attack and the conventional attack is met. The absence of unified cyber security law in the GCC countries, and the regional strategy for these countries. **Conclusion:** The absence of unified Gulf cyber security law in the GCC weakens the capabilities to confront cyber attacks, and the absence of specific definitions of cyber crime and cyber attack, and the differences between the two defunction the adequate legal mechanism to deal with both.

Keywords: cyber security, national security, the unified Gulf cyber security law, national sovereignty

(1) Independent law researcher, Kuwait, E-mail: L-F8D@hotmail.com

- Submitted: 4/10/2022, Revised: 5/12/2022, Accepted: 28/12/2022.

To cite p.298

المقدمة

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. والأمن القومي هو قدرة الأمة على السيطرة الكاملة على جميع المواقف الداخلية والخارجية التي من الممكن أن تعرض أمن الأرواح والممتلكات للخطر؛ ومن ثم فإن تأمين سلامة الدولة ضد أية أخطار داخلية أو خارجية يحمي الدولة من الوقوع تحت سيطرة قوة أجنبية نتيجة لذلك (Asogwa, 2020).

والأمن القومي وفقاً لما أورده Nmah (2019) هو "تجميع للمصالح الأمنية للأفراد والكيانات السياسية والجمعيات الإنسانية والفئات الاجتماعية التي تشكل الأمة، ويشمل كلاً من العوامل البيئية والسياسية والموارد الاقتصادية والاجتماعية للدولة، وهو مجمل الجهود المبذولة لحماية السيادة والقيم العزيزة للأمة، وضمان سلامتها من الكوارث الطبيعية والصناعية".

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 (حمزة، 2017).

وتأكيداً لأهمية الأمن السيبراني وانعكاساته على الأمن القومي للدول، أكد تقرير صادر عن المعهد الملكي للشؤون الدولية (Chatham House) في لندن

(2020) بعنوان "هل تتسم سيبرانية دول الخليج بالمرونة؟"، أن دول مجلس التعاون الخليجي لا تزال تواجه مجموعة واسعة من التهديدات، قد تكون أكثر خطورة وضرراً عليها وتنعكس على الاستقرار السياسي والاقتصادي والاجتماعي لها. وقد تمثلت هذه التهديدات في مهاجمة إيران البنية التحتية السعودية للطاقة في مطلع عام 2010 و2011، وكما حصل في الهجوم على شركة أرامكو السعودية في الفترة نفسها، إضافة إلى الهجوم الذي تعرضت له شركة راس غاز القطرية عام 2012، وتكرر لاحقاً في عامي 2016 و2017، وعلى الرغم من أن الأضرار التي نتجت عن هذه الهجمات السيبرانية على بعض شركات الطاقة في دول الخليج قد تم احتواء أضرارها سريعاً ولم ينتج عنها خسائر جسيمة، فإنها كانت مؤشراً واضحاً على حجم الضرر الذي يمكن أن تحدثه الهجمات السيبرانية في زعزعة استقرار دول المجلس، على مختلف الصُّعُد السياسية والاقتصادية والأمنية (as cited in Shires & Hakmeh 2020).

وعلى الرغم مما يشكله الأمن السيبراني من مرونة وإيجابية في دول مجلس التعاون الخليجي مقارنة بباقي دول الإقليم، فإن المركزية التي تتسم بها هياكل دول المجلس تجعلها أكثر عرضة للتهديدات السيبرانية، بعيداً عن حجم الميزانيات الكبيرة التي تخصصها هذه الدول لمنظومة الأمن السيبراني، وهذه التهديدات عرضة للزيادة بشكل أكبر في ظل عمليات دمج التكنولوجيا في الاقتصاد والمجتمع، التي اتبعتها دول الخليج بشكل متسارع في الآونة الأخيرة، دون تأمين هذه التكنولوجيا بشكل كافٍ ومتناسب مع حجم التوسع في استخدامات التكنولوجيا في مختلف نواحي الحياة؛ ما يسهل عملية الوصول والاختراق من قبل أطراف معادية (وزارة الاتصالات وتكنولوجيا المعلومات، 2014).

ومن أجل معالجة هذه الفجوة القائمة بين انتشار التكنولوجيا المتسارع في دول مجلس التعاون من جهة، وعدم وجود قوانين تنظم عملية الأمن السيبراني بالشكل الكافي في هذه الدول من جهة أخرى، اقترح Shires & Hakmeh (2020) ضرورة إعادة

التوازن بين الانتشار التكنولوجي المتسارع وغياب القوانين المنظمة للأمن السيبراني من خلال التخلص من المركزية في دول المجلس، وتفويض صلاحيات جهات في القطاع الخاص للسيطرة على بعض جوانب الشبكة المعلوماتية؛ وهذا من شأنه ضمان عدم توقف الشبكة بشكل كامل عن تأدية مهام أعمالها في حال تعرضها لهجمات سيبرانية، إلا أن هذا المقترح -من جهة أخرى- من شأنه أن يجعل حكومات دول مجلس التعاون تحت رحمة شركات من القطاع الخاص تديرها غالباً جهات أجنبية خارجية؛ مثل الولايات المتحدة الأمريكية أو بريطانيا، أو حتى الصين والهند.

بناءً عليه، وفي ظل حق الدول في حماية نفسها وأمنها من خطر الهجمات السيبرانية وتداعياتها المختلفة على الدولة، وفي ظل نشاط شبكات اتصال داخلي وخارجي إلكترونية لا تحترم القوانين والمعاهدات والمواثيق الدولية، ولا يمكن السيطرة عليها بشكل كامل، ازدادت الحاجة إلى سن تشريعات وقوانين منظمة للأمن السيبراني في دول مجلس التعاون تكون امتداداً للقوانين الدولية التي تنظم هذا الأمر وتعتبره جزءاً من الأمن الإقليمي والدولي، في حال تعرُّض دولة ما لتهديدات سيبرانية (الحازمي، 2021).

بناءً على ما سبق؛ جاءت هذه الدراسة محاولة مناقشة الإطار القانوني للأمن السيبراني لدول مجلس التعاون الخليجي، وذلك في ضوء القوانين الدولية الخاصة بالأمن السيبراني، مع ملاحظة أن هذه القوانين الفاعلة حالياً هي قوانين تنظيمية للأمن السيبراني وليست قوانين تجريمية؛ أي أن الحاجة إلى سن قانون خاص بدول مجلس التعاون الخليجي يكون ذا طابع تنظيمي، كما هو ذو طابع تجريمي، قد أصبح ضرورة ملحّة في ظل تزايد مخاطر الأمن السيبراني وانعكاساتها على الأمن القومي لمنظومة دول المجلس، وهو ما يوضح حقيقة التهديدات التي قد تتعرض لها دول مجلس التعاون الخليجي في السنوات والعقود القادمة في ظل غياب قانون موحد قادر على ضبط الأمن السيبراني من الناحيتين التنظيمية والتجريمية.

مشكلة الدراسة

يشير الطرح الذي قدمه Shires & Hakmeh (2020) حول المرونة السيبرانية المحتملة لدول مجلس التعاون الخليجي في مواجهة الهجمات القائمة ضد البنية التحتية والمجتمع والدولة، أنه على الرغم من أن هذه الدول خطت خطوات كبيرة في الأمن والدفاع السيبراني في السنوات الأخيرة، فإن الطبيعة المركزية لشبكتها جعلتها عرضة للأعمال العدائية السيبرانية التي تقوم بها دول، مثل إيران.

وتمثل المرونة السيبرانية ركيزة أساسية في عملية سن قانون ينظم الأمن السيبراني في دول المجلس، وقد أكد Shires & Hakmeh (2020) أن عملية تنظيم مركزية الأمن السيبراني ومرونته عملية شائكة ودقيقة، وأشار التقرير إلى أن الإبقاء على مركزية عمليات صنع القرار في موقع أو هيئة واحدة هو أمر ضرورة في أثناء عملية سن القوانين الخاصة بالأمن السيبراني؛ حيث تمتاز الأنظمة المركزية بقدرة أكبر على مواجهة التهديدات التي تطول المعلومات الإستراتيجية للدولة؛ مثل حملات شن الشائعات والتضليل.

إلا أنه -من جهة أخرى- يرى التقرير أن المرونة واللامركزية في القوانين الخاصة بالأمن السيبراني تمنح مزيداً من الكفاءة والفاعلية لمواجهة التدخلات المتكررة والمتباينة في الشبكات الإلكترونية، التي تستهدف عادة كلاً من البنية التحتية والحكومة والمجتمع، وتمتاز الأنظمة المرنة الموزعة بعدم وجود نقطة ضعف مركزية يمكن استهدافها من قبل الأعداء، وذلك على العكس من الأنظمة المركزية التي يمكن أن تتلقى ضربة سيبرانية تؤدي إلى حالة من الشلل التام في عمل أجهزة الحكومة. ويظل الأمر أكثر تعقيداً في حال تفويض جهات من القطاع الخاص لتولي بعض مهام الشبكة الإلكترونية؛ نظراً لما يشكله ذلك من تعدٍّ على السيادة الوطنية للدولة وقوانينها الداخلية.

بناءً عليه؛ تتمثل مشكلة الدراسة في مناقشة الإطار القانوني للأمن السيبراني لدول مجلس التعاون الخليجي، ومحاولة وضع تصور مقترح لقانون موحد ومنظَّم للأمن السيبراني في دول المجلس في محاولة للتصدي للتهديدات السيبرانية الحالية والمستقبلية على الأمن القومي الخليجي. وتسعى الدراسة إلى الإجابة عن الأسئلة الآتية:

1- ما واقع القوانين الدولية المنظِّمة للأمن السيبراني؟
2- ما واقع القوانين الخليجية المنظِّمة للأمن السيبراني في بعض دول مجلس التعاون وأبرز إيجابياتها وسلبياتها؟
3- ما واقع القوانين الكويتية المنظمة لأمن المعلومات والأمن السيبراني؟
4- ما إمكانية وضع تصور مقترح لقانون موحد للأمن السيبراني في دول مجلس التعاون؟

أهمية الدراسة

تستمد الدراسة أهميتها من الأهمية المطلقة التي يتسم بها الأمن القومي لدول منطقة الخليج العربي من جهة، ونظراً لبحثها في الآثار والتداعيات الحالية والمستقبلية التي قد تنتج عن التهديدات السيبرانية التي من الممكن أن تقوض الأمن السيبراني لدول المجلس، وامتداد هذه التأثيرات على كل من الأمن السياسي والاقتصادي والعسكري لهذه الدول.

كما تتضح أهمية الدراسة من كونها تلقي الضوء على القوانين المنظمة للأمن السيبراني في دول مجلس التعاون الخليجي، في ضوء القوانين الدولية الخاصة بهذا الشأن، ومحاولة وضع تصور مقترح ينظم مدى مركزية الأمن السيبراني ومرونته في دول المجلس دون المساس بالقوانين الوطنية لهذه الدول وسيادتها واستقرارها، وذلك سعياً لبناء إطار قانوني يتسم بالمرونة والحداثة، ويواكب التطورات التكنولوجية المتسارعة التي يشهدها العالم فيما يتعلق بالأمن السيبراني على المستويات الدولية والإقليمية والوطنية.

أهداف الدراسة

تسعى الدراسة إلى تحقيق هدفها الرئيس، المتمثل في مناقشة الإطار القانوني للأمن السيبراني لدول مجلس التعاون الخليجي، بالإضافة إلى تحقيق الأهداف الفرعية الآتية:

1- استعراض واقع القوانين الدولية والخليجية المنظمة للأمن السيبراني في مختلف الدول.

2- وضع تصور مقترح لقانون موحد ومنظّم للأمن السيبراني في دول مجلس التعاون، قادر على التصدي للتهديدات السيبرانية الحالية والمستقبلية على الأمن القومي الخليجي.

3- محاولة المواءمة بين المركزية والمرونة في التشريعات الخاصة بالأمن السيبراني في دول مجلس التعاون الخليجي، وذلك من خلال المفاضلة بين إيجابيات كل منهما وسلبياته.

4- تقديم بعض التوصيات المستقبلية لصناع القرار والقانونيين المختصين ذوي العلاقة بحماية الأمن السيبراني لدول مجلس التعاون الخليجي.

المنهج

اتبعت الدراسة المنهج التاريخي التحليلي، ويتضمن المنهج التاريخي سرداً توضيحياً لما سُنَّ من قوانين منظمة للأمن السيبراني في دول مجلس التعاون الخليجي، سواء على المستوى الوطني لكل دولة، أو على المستوى الإقليمي الخليجي لدول المجلس مجتمعة، بالإضافة إلى ما سُنَ من قوانين دولية خاصة بالأمن السيبراني ومدى انسجام القوانين الخليجية معها.

بالإضافة إلى ذلك اتبعت الدراسة المنهج التحليلي الذي يتضمن توضيحاً لكيفية المواءمة بين المركزية والمرونة الخاصة بالأمن السيبراني في دول المجلس دون المساس بالسيادة الوطنية وقوانينها في هذه الدول، وكذلك وضع تصور مقترح لأهم

البنود الواجب تضمينها في القانون الخليجي الموحد للأمن السيبراني، التي تمكّن من مواجهة أية تهديدات حالية أو مستقبلية محتملة من الهجمات السيبرانية.

الدراسات السابقة

أجرى حميد (2021) دراسة هدفت إلى تحليل التهديدات المحتملة للأمن السيبراني في ضوء التطورات التكنولوجية الحديثة، وتعرّف أهم تحديات الأمن السيبراني التي لها دور في حركة التفاعلات والتحولات المتسارعة كحقل جديد في العلاقات الدولية، وذلك في ضوء قواعد القانون الدولي. وتبنت الدراسة المنهج الوصفي التحليلي، وكذلك المنهج القانوني كلما دعت الحاجة في الدراسة. وأظهرت الدراسة أن تأثير الحروب الإلكترونية يتجاوز الحدود الوطنية؛ ما يصعب من عملية السيطرة القانونية على أفعال هذه الحروب ونتائجها، وأن من يسيطر على الفضاء السيبراني في ظل غياب أو ضعف القوانين الدولية الرادعة يمكنه، من ثم، السيطرة على هرم النظام الدولي ككل.

في حين أجرى فياض (2020) دراسة هدفت إلى بيان موقف القانون الدولي الإنساني من الهجمات السيبرانية. اتبعت الدراسة المنهج التحليلي؛ بهدف استعراض موقف القانون الدولي الإنساني من الهجمات السيبرانية، والمنهج المقارن بهدف مقارنة بعض التشريعات الوطنية والدولية الخاصة ببعض الدول حول الأمن السيبراني والهجمات السيبرانية. وأظهرت الدراسة أن غياب اتفاقية دولية خاصة بتقييد الأمن السيبراني وتقنينه وتوقيع جميع الدول الأعضاء في الأمم المتحدة عليها، ما زال يشكل عائقاً كبيراً أمام محاسبة ومعاقبة الأطراف التي ترتكب الهجمات السيبرانية بموجب القوانين والاتفاقيات والمعاهدات الدولية الخاصة بذلك، كما أن غياب تعريف موحد ومحدد للأمن السيبراني جعل من الإمكانية اتباع بعض الثغرات القانونية في حال ارتكاب جريمة سيبرانية من قبل أفراد أو مجموعات، أو حتى دول.

كذلك قام سليمان (2020) بدراسة هدفت إلى تحديد القوة الناشئة عن الهجوم السيبراني وحق الدولة المعتدى عليها في الرد، كما هدفت إلى بيان مدى إمكانية

تطبيق المادة (51) من ميثاق الأمم المتحدة على الهجوم السيبراني. واتبعت الدراسة المنهج التحليلي الوصفي لأحكام ميثاق الأمم المتحدة والاتفاقيات الدولية ذات العلاقة؛ من أجل الوصول إلى حلول مناسبة للإشكالات المطروحة. وأظهرت الدراسة أن الفقرة الرابعة من المادة الثانية من ميثاق الأمم المتحدة جاءت مرنة بالشكل الكافي لاستيعاب الهجوم السيبراني كصورة من صور القوة؛ نتيجة الآثار المتشابهة بالنسبة للقوة العسكرية التقليدية، وأظهرت الدراسة أيضاً أن الدولة المعتدى عليها يكون لها الحق في استخدام القوة في الدفاع عن النفس وفقاً للمادة (51) من ميثاق الأمم المتحدة، كما أظهرت الدراسة أن تأثير الهجمات السيبرانية تكون بمثابة الهجوم التقليدي (المسلح)؛ لأنهما يحملان الهدف نفسه.

وأجرت الرفادي (2018) دراسة هدفت إلى بيان أثر الحروب السيبرانية في التنظيم الدولي. اتبعت الدراسة المنهج التحليلي القائم على تحليل القوانين المتعلقة بتنظيم العمل السيبراني ووضع قواعد الاتفاقيات والمعاهدات الدولية الخاصة بالأمن السيبراني. وأظهرت الدراسة أن القانون الدولي يعتبر الحروب السيبرانية مخالفة لقواعد القانون الدولي، وطالما أدت إلى الإضرار بالأفراد والمنشآت العسكرية والمدنية، سواء جزئياً أو كلياً؛ الأمر الذي يستوجب معه تطبيق القوانين التي تحكم العلاقات بين الدول المتنازعة زمن الحروب؛ مثل اتفاقيات جنيف، والقانون الدولي الإنساني، والمبادئ الواردة في ميثاق الأمم المتحدة، الخاصة بحفظ السلم والأمن الدوليين.

أما دراسة سمودي (2018)؛ فهدفت إلى بيان حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون. اتبعت الدراسة المنهج الوصفي التحليلي المقارن لما عليه الحال بشأن الهجمات الإلكترونية. وأظهرت الدراسة أن الاستناد إلى القواعد العامة في القانون الدولي العام، وتحديداً المادة 51 من ميثاق الأمم المتحدة الخاصة بالدفاع عن النفس وانطباقها على حالة الهجمات الإلكترونية، له ما يدعمه في فقه القانون الدولي؛ اعتماداً على فقه محكمة العدل الدولية التي كانت مهيأة في العديد من القضايا التي عرضت أمامها، إلى ضم فئات أخرى غير الهجوم الحركي لكي يعطي الحق للدولة التي تتعرض إلى هجوم الارتكاز إلى المادة 51 والدفاع

عن نفسها، ولكن ضمن شروط، أبرزها الحجم والتأثير؛ أي أن المحكمة ركزت على نتائج الهجوم أكثر من تركيزها على الوسائل المستخدمة في تنفيذ الهجوم.

المبحث الأول

مفهوم الأمن السيبراني في ضوء القانون

يتناول هذا المبحث مفهوم الأمن السيبراني في ضوء القانون، وذلك في مطلبين، حيث يتناول المطلب الأول استعراضاً لمفهومي الهجوم السيبراني والجريمة السيبرانية، والفرق بين المفهومين؛ ومن ثم موقف القانون منهما، في حين يتناول المطلب الثاني الأمن السيبراني في ضوء القانون الدولي.

المطلب الأول: مفهوم الهجوم السيبراني والجريمة السيبرانية

يتضمن مفهوم الأمن السيبراني كلاً من الهجوم السيبراني والجريمة السيبرانية، والفرق بين المفهومين كبير وينطوي عليه تحديد القوانين المنظمة لكل مفهوم. يتناول هذا المطلب توضيحاً لكل من مفهوم الهجوم السيبراني ومفهوم الجريمة السيبرانية والفرق بينهما، حتى يتسنى التمييز بين القوانين المنظمة لكل مفهوم.

أولاً: الهجوم السيبراني

الهجوم السيبراني هو فعل يقوض قدرات شبكات الحاسوب ووظائفها؛ من أجل هدف قومي أو سياسي، من خلال استغلال نقاط الضعف لتمكين المهاجم من خرق الأنظمة والعبث بها (Traynor, 2007). ويمتلك الهجوم السيبراني قدرة على تهديد البنية التحتية للدول وإغلاق أجهزة الطرد المركزي النووية التي ترتبط أساساً بشبكات الحاسوب، كذلك أنظمة الدفاع الجوية وشبكات الكهرباء والطاقة؛ وهو ما يجعل من الهجوم السيبراني تهديداً حقيقياً للأمن الوطني للدول، وعليه يجب اعتبار الهجمات السيبرانية بمثابة أعمال حرب؛ نظراً لتشابه أفعالها مع الهجمات المسلحة التي ينظمها قانون الحرب (سليمان، 2020).

وفي الاتجاه ذاته، اتفق القانون الحالي على أن يقتصر مصطلح الهجوم على الأذى الجسدي الذي قد يلحق بالأشخاص أو المنشآت أو الممتلكات المادية؛ إذ إن العملية السيبرانية تعتبر بمثابة هجوم يتطلب عملية إصلاح للضرر الذي وقع نتيجة له (Schmidt, 2015).

بناءً عليه؛ يجب تحديد الهدف من استخدام الهجوم السيبراني حتى يتسنى التمييز إذا كان هذا الهجوم وسيلة قتال أم أسلوب قتال، ومثال ذلك ما قام به العدو "الإسرائيلي" سنة 2007 من هجوم بسلاح الجو على موقع سوري ادعى العدو أنه مفاعل نووي، وفي الوقت نفسه شن العدو هجمات سيبرانية على عدد من أجهزة الدفاع والاتصالات في وزارة الدفاع السورية، بالإضافة إلى عدد من المطارات العسكرية والمدنية داخل الأراضي السورية؛ ما أدى إلى تعطلها بالكامل، وفي هذه الحالة يمكن اعتبار هذا الهجوم السيبراني بمثابة أسلوب قتال وليس وسيلة؛ لأنه يندرج ضمن الخطط العسكرية التي عززت العملية العسكرية التقليدية التي شنها سلاح جو العدو، وساهمت الهجمات السيبرانية في تحقيق أهداف العملية العسكرية التقليدية (Rid & Mcburney, 2012).

من جهة أخرى، يمكن للهجمات السيبرانية أن تكون وسيلة قتال عبر توظيفها للتسلل إلى أنظمة حاسوبية تعمل على حماية منشآت حيوية؛ مثل المحطات النووية المعدة لأغراض سلمية، أو المطارات، أو السدود، أو منظمة النقل والاتصالات، وغيرها؛ وذلك بهدف السيطرة عليها والتحكم بها من خلال هذا الهجوم السيبراني؛ الذي يمكن توظيفه لبرمجة هذه المنشآت لتعطيل أعمالها بنفسها أو تدمير نفسها من خلال تزويدها ببيانات خاطئة، ومثال ذلك الهجوم السيبراني الذي شنته الولايات المتحدة الأمريكية سنة 2011 على محطة "نطانز" الإيرانية الخاصة بتوليد الطاقة النووية؛ حيث استخدمت الولايات المتحدة في هذا الهجوم السيبراني برنامج «Stuxnet»، الذي استطاع تعطيل عمل جميع العمليات الحساسة داخل المنشأة وتسبب في إلحاق أضرار جزئية في عملية تخصيب اليورانيوم (Gervais, 2011).

بناءً على ما سبق؛ فإن التمييز بين كون الهجمات السيبرانية وسيلة أم أسلوب قتال، إنما يعتمد على الهدف من استخدام هذه الهجمات والنتائج المتوقعة منها، وفي حال تسببها بجراح أو قتل أو تعطيل كلي أو جزئي أو تدمير فإنها تعتبر وسيلة قتال، أما إذا تم استخدامها كجزء من مخطط عسكري؛ فإنها تعتبر أسلوب قتال.

ثانياً: الجريمة السيبرانية

من الأهمية وضع تعريف للجريمة السيبرانية وتحديد خصائصها وأركانها لتحديد آلية التعامل معها، وهو أمر شائك ومتداخل؛ إذ إنه يصعب حتى الآن وضع تعريف عام وشامل للجريمة السيبرانية، ويرجع ذلك إلى سرعة تطور تكنولوجيا المعلومات من جهة، وتباين الدور الذي تلعبه هذه التكنولوجيا في الجريمة من جهة أخرى. فالتباين واضح من اللحظة الأولى للتعاريف، فالبعض يسميها جريمة إلكترونية، والآخر يسميها جريمة سيبرانية، وإن كان استخدام كلمة سيبرانية بدأ في الانتشار بشكل أوسع، وقد أكدت قمة برلين العالمية حول الجريمة السيبرانية أنه من المتعذر عالمياً الاتفاق على تعريف موحد للجريمة السيبرانية حتى الآن (هروال، 2013).

وتعتبر الجريمة السيبرانية مخالفة ترتكب ضد الأشخاص أو الجماعات بدافع إجرامي؛ مثل حالة الدخول غير المصرح به وإتلاف البيانات داخل النظم، أو الاعتراض غير القانوني للبيانات عن طريق نقلها من حاسوب إلى آخر، كما في حال إدخال بيانات خاطئة أو محاولة العبث بالبيانات المخزنة، ومن هذا الأساس قدم الفقيه الألماني (Ulrich Sieber) تعريفاً للجريمة السيبرانية على اعتبار أنها "الاعتداءات القانونية التي يمكن أن ترتكب بوساطة المعلوماتية بغرض تحقيق الربح" (كما ورد في سعيد، 1993).

وفي سياق التعريفات المختلفة التي تناولت الجريمة السيبرانية، أشارت اتفاقية التعاون لضمان أمن المعلومات الدولي بين الدول الأعضاء في منظمة شنغهاي للتعاون إلى تعريف الجريمة السيبرانية بأنها "استخدام مصادر

المعلومات والتأثير عليها في فضاء المعلومات؛ من أجل أغراض غير قانونية" (Shanghai Cooperation Organization [SCO] 2013, p.9).

في حين قدمت وكالة تطبيق القانون الأوروبية "اليوروبول" تعريفاً للجريمة السيبرانية بأنها "جريمة تكنولوجيا عالية وتحصل باستخدام المعلومات وتكنولوجيا الاتصالات لارتكاب عمل إجرامي أو تعزيزه ضد شخص ما، الملكية الخاصة، أو منظمة أو نظام شبكة الحاسب الآلي" (حسن، 2021، ص.53).

أما منظمة الشرطة الجنائية الدولية "الإنتربول"، فقدمت تعريفاً للجريمة السيبرانية بأنها "الجرائم المرتكبة ضد أجهزة الكمبيوتر وأنظمة المعلومات؛ حيث يكون الهدف منها هو الوصول غير المصرح به إلى جهاز، أو رفض الوصول إلى مستخدم شرعي" (Interpol, 2017, p.2).

أما تعريف شرطة المفوضية الأوروبية للجريمة السيبرانية؛ فهو أنها "أفعال جرمية تتم عبر الشبكة العنكبوتية باستخدام وسائل الاتصال الإلكترونية والشبكات ونظم المعلومات، وهي جريمة تعاقب عليها القوانين الأوروبية، وتقتضي التعاون بين كافة دول الاتحاد الأوروبي لمواجهتها" (European Commission, 2022, p.2).

ومن التعريفات السابقة يتضح الفرق بين الجريمة السيبرانية والهجوم السيبراني؛ إذ إن الهدف من الجريمة السيبرانية يختلف في دوافعه بشكل كلي عن الهدف من الهجوم السيبراني؛ فالأخير يقوم به جماعات أو دول من أجل دوافع تتعلق بالأمن القومي، في حين أن الجريمة السيبرانية لا ترتبط بالسياسات الخاصة بالدول، ومن المستبعد فيها تورط دول، وإنما يكون المتورطون عادة في مثل هذه الجرائم أفراد أو ما يسمى قراصنة الإنترنت؛ حيث يقومون بتنفيذ جرائمهم السيبرانية من أجل تحقيق أرباح مادية، وهذا ما يحدد الإطار الذي يندرج ضمنه مفهوم الجريمة السيبرانية.

وبناءً عليه؛ يمكن تلخيص الجريمة السيبرانية بأنها ما هي إلا أفعال مخالفة للقانون وتستهدف نظم المعلومات، أو أجهزة الحاسوب، أو شبكات الإنترنت، وهي تتضمن الجريمة التقليدية ولكن يستخدم فيها الفضاء السيبراني وأجهزته

والتطبيقات الملحقة بها، ويتضح من التعريفات السابقة أنها تمحورت حول أن الجريمة السيبرانية تتضمن:

- الاعتداء المباشر على نظم شبكة المعلومات لإصابتها وتعطيلها وتخريب وظائفها.
- استغلال الشبكة لعمليات النصب والاحتيال وسرقة البيانات والاعتداء على الملكيات الفكرية وانتحال الشخصية والتشهير.
- استغلال الفضاء السيبراني الرقمي لنشر محتوى مخالف للقانون والأعراف كالصور الإباحية والإشاعات والأخبار المغلوطة، والأفكار العنصرية والإرهابية وما يشابهها.

ومن أبرز الخصائص المتعلقة بالجريمة السيبرانية، التي تميزها عن الجريمة التقليدية، أنها عابرة للدول، وصعبة الإثبات، ومغرية للمرتكبين، وسهلة الارتكاب (جاب الله، 2021). ومن خلال هذه الخصائص تتحدد الأهداف التي تسعى الجريمة السيبرانية إلى تحقيقها، وهذه الأهداف هي ما يميز الجريمة السيبرانية عن الهجوم السيبراني بشكل دقيق؛ إذ إن الجريمة السيبرانية ترمي إلى تحقيق الأهداف الآتية: (لطفي، 2022)

- الوصول إلى المعلومات بشكل غير قانوني؛ كسرقة المعلومات أو مسحها أو تغييرها عبر الإنترنت.
- الوصول إلى الأجهزة الخادمة الموفرة للمعلومات أو الخدمة وتعطيلها أو تخريبها.
- الوصول إلى الأشخاص أو الجهات المستخدمة للتكنولوجيا؛ بغرض التهديد والابتزاز.
- الاستفادة من تقنية المعلومات من أجل الكسب المادي أو المعنوي أو السياسي.
- استخدام التكنولوجيا في دعم الإرهاب والأفكار المتطرفة.

بناءً عليه؛ فإن الاختصاص القانوني للهجوم السيبراني والجريمة السيبرانية يختلف اختلافاً كبيراً من خلال اختلاف التعريفات الخاصة بكل مفهوم؛ فالهجوم السيبراني يندرج ضمن اختصاص القانون الدولي العام على اعتبار أنه يمثل خرقاً لسيادة الدول، في حين تندرج الجريمة السيبرانية ضمن اختصاص القانون الوطني وفقاً لمبدأ إقليمية القوانين. أي أن الهجوم السيبراني يهدف إلى إضعاف قدرات الدولة أو تعطليها أو تدميرها من خلال استهداف شبكة الإنترنت لأغراض ذات طابع سياسي تمسّ الأمن القومي، في حين أن الجريمة السيبرانية تقوم أساساً على أغراض السرقة وتحقيق الربح المادي من خلال قرصنة البيانات لأغراض السرقة، وفي كلتا الحالتين تكون الدولة مسؤولة مسؤولية دولية عن أعمال مواطنيها التي تسبب ضرراً بمصالح الدول الأخرى.

المطلب الثاني: الأمن السيبراني في ضوء القانون الدولي

عند توقيع المجتمع الدولي على القوانين والاتفاقيات والمعاهدات الدولية التي تعالج مسألة الاعتداءات؛ مثل معاهدة حلف شمال الأطلسي[1]، وميثاق الأمم المتحدة[2]، لم يتم الأخذ بالحسبان مفهوم الهجوم أو الاعتداء غير الحركي بنظر الاعتبار، حيث عالجت المادة الخامسة من اتفاقية حلف شمال الأطلسي مسألة حق الدفاع عن النفس في إطار الاعتداء الحركي، كما هو الحال في المادة (51) من ميثاق الأمم المتحدة، فصياغة القوانين الدولية والمعاهدات والاتفاقيات قد سبق ظهور المفاهيم الإلكترونية بعقود طويلة.

أولاً: الأمن السيبراني في القانون الدولي للمنازعات المسلحة

تميل الدول التي تمتلك تفوقاً تكنولوجياً بارزاً في ميدان التقنيات الإلكترونية الحديثة إلى الابتعاد ما أمكن عن التوقيع على أية اتفاقيات دولية من شأنها الحد

(1) وقِّعَتْ في واشنطن 4 أبريل 1949، وصدَّق عليها مجلس الشيوخ في 21 يوليو 1949، صادق عليها رئيس الولايات المتحدة في 25 يوليو 1949 وأودعت في واشنطن 25 يوليو 1949، دخلت حيز التنفيذ في 24 آب 1949.

(2) جرت مناقشة ميثاق الأمم المتحدة وإعداده وصياغته خلال مؤتمر سان فرانسيسكو الذي بدأ في 25 أبريل 1945، الذي شارك فيه معظم دول العالم ذات السيادة، وبعد موافقة ثلثي كل قسم، اعتمد المندوبون النص النهائي بالإجماع وفتِح للتوقيع في 26 يونيو 1945، وقع عليه في سان فرانسيسكو، الولايات المتحدة، 50 من أصل 51 دولة عضواً، ودخل الميثاق حيز التنفيذ في 24 أكتوبر 1945.

من تفوقها الإلكتروني، ومن هناك اتجه الفقه إلى اعتبار الأمن السيبراني وما يرتبط به من هجمات سيبرانية مندرجاً ضمن القانون الدولي الإنساني في محاولة لسد الفراغ القانوني الذي ينظم الحروب السيبرانية؛ ففي حال وقوع حرب إلكترونية بين دولتين يصبح القانون الدولي الإنساني هو المنظِّم لهذا الشأن وتنطبق قواعده على هذا النزاع؛ أي أن القانون الدولي الإنساني لا ينطبق إلا في حال نُفِّذت الهجمات السيبرانية في سياق نزاع مسلح وكانت مرتبطة به (بن تغري، 2020).

وأشار الاجتهاد إلى انطباق قواعد القانون الدولي الإنساني على الهجمات السيبرانية في حال تحقق شرط التزامن بين الهجوم السيبراني والهجوم التقليدي، وذلك من منطلق أن أياً من الاتفاقيات والمعاهدات الدولية لم تعالج هذا الأمر؛ فميثاق الأمم المتحدة، واتفاقية جنيف 1949، واتفاقية لاهاي 1899 و1907، ومعاهدة حلف شمال الأطلسي، لم يتناول أيٌّ منها النزاع السيبراني، وإنما أشارت بعض مواد هذه الاتفاقيات إلى حق الدفاع عن النفس في سياق النزاع التقليدي، كما جاء في المادة (5) من معاهدة حلف شمال الأطلسي، التي أشارت إلى أنه "يتفق الأطراف، على أن أي هجوم، أو عدوان مسلح، ضد طرف منهم، أو عدة أطراف، في أوروبا أو أمريكا الشمالية، يعتبر عدواناً عليهم جميعاً" (معاهدة حلف شمال الأطلسي، 1949، المادة 5).

أي أن هذه المعاهدات والاتفاقيات لم تصغ بالمرونة الكافية التي يمكن أن تمتلك القدرة على التنبؤ بالتطورات المستقبلية التي حدثت بعد عقود طويلة من صياغة هذه الاتفاقيات، كما لم تُضف أية تعديلات على بعض نصوص موادها بالشكل الذي يتوافق مع التطور التكنولوجي الحديث، وإنما حُدّدت أطرها ضمن النزاعات المسلحة التقليدية واستخدمت مصطلحات من قبيل القوة العسكرية، والقوات الجوية والبحرية والبرية، والهجوم المسلح، وهي في مجملها مصطلحات لا تتوافق بأي حال من الأحوال مع مفاهيم الأمن السيبراني الحديثة، وهو ما يضعها خارج نطاق القانون الدولي.

من هذا المنطلق دعت الحاجة إلى مواءمة الهجمات السيبرانية مع القانون الدولي الإنساني؛ إذ إن أعمال الحروب السيبرانية ستسفر عن خرق أحكام عديدة

في القوانين الحالية المسلحة، أو إنها ستكون خارج نطاق هذه القوانين؛ لهذا نادى القانون الدولي الإنساني بضرورة توفير قدر كافٍ من الحماية للبنية التحتية الحيوية التي تشمل كلاً من المستشفيات، ومراكز دور العجزة، والمراكز الطبية المختلفة، وسلاسل الإمداد، والأنظمة المالية، ووسائل النقل، والمراكز الدينية ودور العبادة، ومرافق الأخبار، والمؤسسات التعليمية، والمسعفين، وأجهزة إنفاذ القانون، وغيرها من المنشآت التي ضمن القانون الدولي الإنساني حمايتها والحفاظ عليها وعلى العاملين فيها (محمود، 2013). وهنا يتضح التزامن بين انطباق قواعد القانون الدولي الإنساني في حالات الحرب التقليدية أو السيبرانية على حد سواء؛ إذ إن الهجمات السيبرانية التي تطول هذه البنى التحتية إنما تندرج تلقائياً في حال تعرضها لهجوم ضمن قواعد القانون الدولي الإنساني، وهو ما يلزم الطرف المسؤول عن الهجوم السيبراني اتخاذ جميع التدابير اللازمة لتجنب الإضرار بالبنى التحتية والمدنيين؛ إذ يمكن أن يتمخض الهجوم السيبراني عن عواقب تُهدد الحياة في حالة إفساد البنية التحتية للمعلومات ذات الأهمية الحرجة، كما يمكن أن تؤدي أيضاً إلى عمليات معلوماتية تؤثر على حقوق الإنسان الدولية وتدفع على العنف وتُسبب ضرراً اقتصادياً خطيراً (توريه، 2011).

وفي حال اتخاذ دولة احتياطات وقائية من خلال فصل نظم الحواسيب العسكرية عن المدنية؛ وذلك بهدف حماية المدنيين من آثار الهجمات السيبرانية، فإن بعض الأنظمة تظل مشتركة بين القطاعين العسكري والمدني في الدول؛ ومن ثم، فإن الأذى أو الضرر غير الضروري والناجم عن تدمير أو تعطيل البنية التحتية الحيوية والذي سوف يتسبب بمصاعب ومعاناة جسيمة، تعمل قوانين النزاع المسلح على منعه، كما أن الضرر الناتج من الهجوم السيبراني أحياناً لا يتناسب مع المزايا العسكرية المستخلصة من الهجوم؛ ومن ثم، فإن مبدأ التناسب في هذه الحالة ينطبق على هذا الهجوم السيبراني (اعمر، 2019).

وبالإضافة إلى مبدأ التناسب، فإن مبدأ التمييز في القانون الدولي الإنساني ينطبق أيضاً في حال الهجمات السيبرانية؛ حيث يلزم هذا المبدأ الدول التمييز في

جميع الأحوال بين المدنيين والعسكريين وبين الأعيان المدنية والأهداف العسكرية، وهو مبدأ أساسي من مبادئ القانون الدولي الإنساني، وقد نصت القاعدة (1) في القانون الدولي الإنساني على أنه "يميّز أطراف النزاع في جميع الأوقات بين المدنيين والمقاتلين، وتوجّه الهجمات إلى المقاتلين فحسب، ولا يجوز أن توجّه إلى المدنيين" (Henckaerts & Doswald-Beck, 2005).

ثانياً: دليل تالين بشأن الهجمات السيبرانية

يعتبر دليل تالين[3] المتعلق بالقانون الدولي في حرب الفضاء الإلكتروني، الذي أصدره حلف شمال الأطلسي، بمثابة إجراء قانوني يسعى إلى تفسير قواعد القانون الدولي الخاصة بالحق في الحرب وقانون الحرب، في محاولة لتفسير جميع القضايا الشائكة فيما يتعلق بالهجمات السيبرانية وموقف القانون الدولي منها؛ حيث يؤكد الدليل الثنائية التقليدية لكل من النزاعات المسلحة الدولية وغير الدولية، ويعتبر أن الهجمات الإلكترونية السيبرانية وآثارها المدمرة بمثابة نزاعات مسلحة؛ على اعتبار أن الهجوم السيبراني هو عملية إلكترونية هجومية أو دفاعية، من المتوقع لها أن تسبب إصابات أو قتل لأفراد أو إلحاق أضرار بأعيان أو تدميرها (دروغيه، 2011).

اعتمد الإصدار الأول من دليل تالين (Tallinn Manual 1.0) -وفقاً للمادة (11) منه- معيار النطاق والأثر لتحديد المدى الذي يمكن للهجوم الإلكتروني الوصول إليه في حال استخدام القوة أو الهجوم المسلح، واعتبر الهجوم الإلكتروني مسلحاً إذا أحدث ضرراً مادياً جسيماً، واستند الخبراء في هذ المعيار إلى رأي محكمة العدل الدولية في قضية «نيكاراجوا»، حين قامت الولايات المتحدة الأمريكية بتدريب قوات الكونترا وتسليحها؛ لمحاربة الحكومة الشرعية في نيكاراجوا، واعتبرت المحكمة أن

(3) دليل تالين تمت كتابته من قبل مجموعة من الخبراء برئاسة مايكل سميث بتكليف من منظمة حلف شمال الأطلسي، الذي يقترح تطبيق القانون الدولي على النزاعات الإلكترونية. ظهر هذا المشروع في عام 2013، وتم تعديل الدليل ونشره في فبراير 2017 تحت مسمى Tallinn Manuel on the International Law Applicable to Cyber Warfare «Tallinn 2.0»، وتتناول الدراسة الجديدة الخيارات التي يقدمها القانون الدولي للدول ضحايا الهجمات الإلكترونية. ويعد هذا الدليل وثيقة غير ملزمة أعدتها مجموعة من الخبراء الدوليين، كما أن هذه الوثيقة لا تعكس الموقف الرسمي لحلف شمال الأطلسي أو موقف كل دولة من الدول الأعضاء في الحلف.

هذا العمل استخدام غير مشروع للقوة، وعلى هذا الأساس قاس الخبراء الهجمات السيبرانية؛ حيث اعتبر الإصدار الثاني من دليل تالين (Tallinn Manual 2.0) أن قيام دولة ما بتزويد قوات أو أفراد بأجهزة وتدريبهم على شن هجمات سيبرانية ضد دولة أخرى يعتبر استخداماً غير مشروع للقوة (Schmitt, 2017).

يشير الدليل إلى أن القانون الدولي الإنساني ينطبق على الحرب الإلكترونية، ويحدد الدور الذي ستلعبه قواعد القانون الدولي الإنساني في هذا المجال؛ فهو يقر بأن العمليات الإلكترونية قد تشكل نزاعات مسلحة تبعاً للظروف، لا سيما الآثار المدمرة لتلك العمليات. كما يعطي دليل تالين الحق للدولة التي تتعرض لهجوم إلكتروني شن حرب هجومية إلكترونية مضادة على الدولة الأخرى، كما ذكر دليل تالين أنه يمكن استخدام القوة العسكرية الحقيقية في حالة شُنَّ هجوم إلكتروني على دولة وأدى هذا الهجوم لخسائر بالأرواح البشرية (الفصل 11).

ويقدم الدليل تقسيماً تقليدياً للنزاعات المسلحة الدولية وغير الدولية، ويعتبر أن العمليات السيبرانية بحد ذاتها قد تشكل نزاعات مسلحة تبعاً لظروف قيام هذه العمليات، وفي حال مقارنة أثر الهجوم السيبراني بالاستخدام الفعلي للقوة وكان مساوياً له أو قريباً منه يعتبر الهجوم السيبراني بمثابة استخدام للقوة (المادة 69)، وفي هذه الحالة تخضع هذه الهجمات لقانون النزاعات المسلحة والاتفاقيات المنظمة لها والآثار المدمرة المترتبة عليها (المادة 80 من دليل تالين). واعتمد الدليل على هذه القاعدة من خلال التعريف الذي قدمه للهجوم السيبراني بأنه "عملية إلكترونية سواء هجومية أو دفاعية، يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بأعيان أو تدميرها" (المادة 92)، كما يعتبر الدليل أن توقف أحد الأعيان عن العمل قد يشكل ضرراً مادياً.

وبرر خبراء اللجنة الدولية وجهة نظرهم في هذا التفسير على اعتبار أن تعطيل أحد الأعيان لا يرتبط بكيفية تعطله سواء بوسائل حركية أو من خلال عملية إلكترونية، أي أن التعطل يشكل ضرراً مادياً؛ ومن ثم، فإن أي عملية إلكترونية

تستهدف تعطيل شبكة مدنية عن العمل، خلاف ما ذكر، لن يشملها الحظر الذي يفرضه القانون الدولي في هذه الحالة (اعمر، 2019).

عموماً، فإن الهجمات السيبرانية التي ترتقي لمستوى النزاع المسلح تخضع لقانون النزاعات المسلحة، إلا أن هناك أهدافاً تستخدم أجهزة خوادم (Servers) مشتركة بين الأغراض المدنية والعسكرية، وقد أشارت المادة (101) من دليل تالين إلى أن الأعيان التي تستخدم لأغراض مدنية وعسكرية مشتركة، مثل أجهزة الحاسوب وشبكاتها والبنية التحتية الإلكترونية تعتبر أهدافاً عسكرية. إلا أن هذا الأمر يثير لبساً وفقاً لما ورد في نص المادة السابقة الذكر؛ إذ إن ما نسبته 90% تقريباً من الاتصالات الحكومية الأمريكية تستخدم الشبكات المدنية، بما فيها الإنترنت والاتصالات والهواتف الخلوية والمستشفيات التي تعتمد على هذه الشبكات، فهل يجعل هذا الأمر من هذه الأعيان أهدافاً عسكرية بموجب ما ورد في دليل تالين؟

أما من حيث مبدأ التمييز؛ فقد حدد دليل تالين الأهداف التي يمكن مهاجمتها خلال النزاعات، واعتبر الدليل أن المدنيين، أفراداً وجماعات، يجب ألا يكونوا هدفاً لأية عمليات سيبرانية، وفي حال الشك في الفرد أهو مدني أم عسكري فإنه يعتبر مدنياً، وقد حددت المادة (96) الأهداف التي من الممكن مهاجمتها في حال النزاع على النحو الآتي:

- أفراد القوات المسلحة.
- أعضاء الجماعات المسلحة المنظمة.
- المدنيون الذين يشاركون مباشرة في الأعمال الحربية.
- المشاركون في الانتفاضة الشعبية، في النزاع المسلح الدولي.

واعتبرت المادة السابقة الذكر أن المدنيين يتمتعون بالحماية خلال الفترة التي لا يشاركون فيها بالعمليات العدائية، ونصت المادة (98) على حظر توجيه هجمات تبث الذعر بين المدنيين. ونصت المادة (99) على أنه لا يجوز استهداف الأعيان المدنية

بالهجمات الإلكترونية التي تشمل أجهزة الكمبيوتر وشبكات الكمبيوتر والبنية التحتية الحاسوبية.

يتضح مما سبق أن ما ورد في هذا الدليل يعدّ تطبيقاً نظرياً لمبدأ التمييز؛ فالقوانين الدولية للنزاع المسلح تسمح باستخدام القوات غير النظامية؛ إذ إن الحكومات تستطيع التعاقد مع شركات لها القدرة الاختراقية واستخدام شبكاتها كمقاتلين شرعيين في النزاعات "السيبرانية"، وهو ما سبق أن حدث فعلياً، ومن الجائز تخويل القوات غير النظامية المشاركة في الأعمال العدائية، ولكن هذه الشبكات الاختراقية ليست مميزة كما أن أسلحتها غير ظاهرة للعيان ولا تحمل شعاراً أو علامة مميزة.

المبحث الثاني

بعض القوانين الخليجية المنظمة للأمن السيبراني

يتناول هذا المبحث القوانين المنظمة للأمن السيبراني في بعض دول مجلس التعاون الخليجي، وذلك في أربعة مطالب، يتناول المطلب الأول اللجنة الوزارية للأمن السيبراني بدول مجلس التعاون، في حين يتناول المطلب الثاني واقع القوانين المنظمة للأمن السيبراني في كل من المملكة العربية السعودية والإمارات العربية المتحدة، ويتناول المطلب الثالث القانون الكويتي المنظم للأمن السيبراني، أما المطلب الرابع؛ فقد خُصّص لأبرز الإيجابيات والسلبيات في القوانين الخليجية المنظمة للأمن السيبراني.

المطلب الأول: اللجنة الوزارية للأمن السيبراني بدول مجلس التعاون

شُكّلت اللجنة الوزارية للأمن السيبراني بدول المجلس، وانطلق الاجتماع الأول لهذه اللجنة بتاريخ 23 تشرين الأول (أكتوبر) من عام 2022، وأعلن عن تأسيس اللجنة الدائمة للأمن السيبراني، التي تضطلع بمهام وضع الأطر والسياسات والإجراءات المشتركة للتصدي للتهديدات السيبرانية، ومواءمة الجهود بين دول المجلس في مختلف القطاعات، ورفع مستوى التعاون الدولي مع الدول والمنظمات

ذات العلاقة، وتعزيز صناعة الأمن السيبراني وتنميتها، وتبادل المعرفة والخبرات والدراسات والتجارب في الأمن السيبراني وتنميتها لتهيئة فضاء سيبراني آمن لحماية دول المجلس من التهديدات السيبرانية. كما تضمن الاجتماع إطلاقاً للتمرين الخليجي الأول للأمن السيبراني؛ وذلك بهدف رفع مستوى الجاهزية السيبرانية والاستعداد لمواجهة التهديدات والمخاطر السيبرانية، بالإضافة إلى إيجاد حلول مبتكرة لمواجهة التحديات والتهديدات السيبرانية، كما أعلن عن تدشين منصة تحليل البرمجيات الخبيثة الخاصة بالأمن السيبراني كمشروع خليجي مشترك يستهدف ضمان أمن المعلومات وحمايتها (وكالة الأنباء الكويتية [كونا]، 2022).

وقدمت اللجنة الدائمة للأمن السيبراني بعض المقترحات التي تهدف إلى تعزيز العمل الخليجي المشترك في الأمن السيبراني، منها إنشاء مركز للأمن السيبراني لدول المجلس لتقديم رؤية واضحة للتهديدات السيبرانية وتعزيز سبل مواجهتها، ودعم فرص تبنّي منهجية متعددة المستويات للاستجابة للتحديات السيبرانية، وتعزيز الاستفادة من تطور بيئة الأعمال الرقمية المبتكرة، كالأتمتة باستخدام الروبوتات وتقنية «بلوك تشين» والذكاء الاصطناعي، وتعزيز مرونة المدن الذكية وجاهزيتها، ومواكبة التطورات التكنولوجية، بما يضمن حماية أنظمة المدن، وتعزيز قدرات الأمن السيبراني في دول المجلس، يضاف إلى ذلك نشرُ الوعي السيبراني خليجياً؛ بما يعزز طرق المواجهة الشاملة للهجمات السيبرانية، وحوكمة وترسيخ ثقافة دمج الحلول الأمنية والخصوصية؛ بما يعزز ثقة السكان بالخدمات الحكومية، فضلاً عن دعم الكثير من الأنشطة الاقتصادية والحيوية، في ظل تصاعد ونمو الهجمات السيبرانية التي تتعرض لها دول المجلس، بالتزامن مع تزايد اتصال الأنظمة والأجهزة بشبكة الإنترنت على نحو غير مسبوق (وكالة أنباء الإمارات [وام]، 2022).

المطلب الثاني: القوانين السعودية والإماراتية المنظمة للأمن السيبراني

وفقاً للتقرير الخاص بموجز المخاطر (Risk Briefing)، الصادر سنة 2019 عن وحدة الإيكونوميست للمعلومات والخاص بقياس المخاطر التشغيلية في 180 دولة حول العالم، صنف التقرير المملكة العربية السعودية في مرتبة متأخرة مسجلة نتائج ضعيفة في مقياس الأمن السيبراني؛ إذ إن السعودية لا تعترف بتبادل المعلومات والأمن السيبراني كمسألة ذات أولوية (Finckenstein, 2019). وكانت الإمارات العربية المتحدة قد أصدرت عدداً من القوانين التي تستهدف مكافحة الجرائم الإلكترونية والسيبرانية وحماية المجتمع منها.

أولاً: تجربة المملكة العربية السعودية

تعتبر السعودية من الدول التي تعرضت للعديد من الهجمات السيبرانية على بنيتها التحتية؛ مثل الهجمات التي استهدفت شركة أرامكو السعودية سنة 2012، وعطلت نشاط الشركة لمدة شهر، كما أعيد الهجوم مرتين متتاليتين في عامي 2016 و2017، وأورد تقرير المجلس الاستشاري للأمن الخارجي في الولايات المتحدة الأمريكية Overseas Security Advisory Council الصادر في 2016، أن الهجوم على شركة أرامكو السعودية قد كلفها تغيير 50000 قرص صلب لأجهزتها الحاسوبية، ولم تستطع استخدام الإنترنت لمدة خمسة أشهر تقريباً، وهذا يعتبر زمناً قياسياً في الإصلاح، خاصة إذا ما أخذنا في الاعتبار إمكانات أرامكو المالية والتقنية (أبو زيد، 2019).

سنّت السعودية عام 2007 قانوناً للجرائم الإلكترونية، يهدف إلى مكافحة الجرائم الإلكترونية عن طريق تحديد الجرائم وتحديد العقوبات لحماية أمن المعلومات، وحماية الحقوق المتعلقة بالاستخدام المشروع لأجهزة الكمبيوتر وشبكات المعلومات، وحماية المصلحة العامة (Saeed & Salem, 2015).

وحرصت المملكة على تطوير الضوابط الأساسية للأمن السيبراني من خلال الهيئة الوطنية للأمن السيبراني، وذلك عبر دراسة متطلبات التشريعات والتنظيمات

والقرارات ذات العلاقة، والاطلاع على أفضل الممارسات والتجارب في مجال الأمن السيبراني والاستفادة منها، وتحليل ما رصد من حوادث وهجمات سيبرانية على مستوى الجهات الحكومية وغيرها؛ إذ إن هذه الضوابط تطبق على الجهات الحكومية، وتشمل الوزارات والهيئات والمؤسسات، والجهات والشركات التابعة لها، وجهات القطاع الخاص التي تمتلك بنى تحتية وطنية حساسة، أو تقوم بتشغيلها أو استضافتها، وذلك بهدف تعزيز منظومة الأمن السيبراني قانونياً وتقنياً (الهيئة الوطنية للأمن السيبراني، 2018).

من جهة أخرى، أطلقت الهيئة الوطنية السعودية للأمن السيبراني عدة مبادرات لمواجهة النقص في الكوادر الوطنية في هذا المجال؛ مثل مبادرة الابتعاث في الأمن السيبراني بالشراكة مع وزارة التعليم؛ وذلك لتلبية حاجة بناء القدرات الوطنية في مجال الأمن السيبراني وسدّ الاحتياج الذي يتطلبه سوق العمل الحكومي والخاص؛ بهدف حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، لحماية الفضاء السيبراني للمملكة وتعزيز القدرات السيبرانية لمواجهة الهجمات الخارجية (مركز سمت للدراسات، 2019).

كما صدر نظام مكافحة جرائم المعلوماتية السعودي عام 2007، وتضمن القانون الجرائم المعلوماتية كما ورد في نصوص المواد (3، 4، 5، 6) منه التي حددت أنواع الجرائم التي يعاقب عليها القانون، أما المادة (7) من القانون السالف الذكر؛ فقد توسعت بمفهوم الجريمة الإلكترونية لتشمل كلاً من.

> إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية ، أو أحد أجهزة الحاسب الآلي أو نشره؛ لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها أو ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية، بالإضافة إلى الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمسّ الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني (نظام مكافحة جرائم المعلوماتية السعودي، 2007، المادة 7).

وفي عام 2014، صدر قانون الجرائم السيبرانية بقرار من مجلس الوزراء السعودي، وهو نظام لمكافحة الجرائم الإلكترونية والمعلوماتية، تلك الجرائم التي تتم من خلال أجهزة الحاسوب بهدف الابتزاز، أو الاحتيال، أو القرصنة، وتستخدم للإضرار بالدول، والمؤسسات وكذلك الأفراد، وذلك عن طريق الوصول إلى معلومات أمنية، أو أسرار تجارية أو شخصية (نظام مكافحة جرائم المعلوماتية السعودي، 2014).

ثانياً: تجربة الإمارات العربية المتحدة

أصدرت الإمارات عام 2012 قانون مكافحة الجرائم السيبرانية، وتعديلاته في عام 2016، وتم تدعيم القانون بمجموعة من السياسات التنظيمية والمعايير التقنية لتمكين مستخدمي الفضاء الإلكتروني ومقدمي الخدمات من الحصول على الظروف الأمنية اللازمة لحماية النظم الحساسة والبنية التحتية والبيانات، فضلاً عن حماية المستخدمين، كما أطلقت مرحلة مهمة من التخطيط للمستقبل، بعدما أعلن عن إستراتيجية الإمارات للثورة الصناعية الرابعة، التي تشمل التزام الدولة بزيادة الجهود لتصبح أول مختبر مفتوح في العالم لاختبار تكنولوجيا الثورة الصناعية الرابعة وتطبيقها، والعمل على تحقيق أمن المستقبل كجزء من الإعداد للاستدامة وعصر ما بعد النفط. كما قامت قبل ذلك بإنشاء الفريق الوطني للاستجابة لطوارئ الحاسب الآلي عام 2008؛ ليكون بمثابة مركز وطني لتطوير برامج التوعية الأمنية للجمهور، وتطوير برامج التدريب وبناء القدرات للمختصين بأمن المعلومات، بالإضافة إلى تجهيز الفريق ليكون بمثابة خط المواجهة للدفاع، والكشف، وتقديم المشورة، والتصدي للتهديدات الأمنية السيبرانية في الدولة. كما أعلنت الهيئة الوطنية للأمن الإلكتروني في دولة الإمارات عن مرونة عالية تمتلكها الدولة فيما يتعلق بقدرة الكيانات والقطاعات والأفراد على العمل في مواجهة السيناريوهات المحتملة التي تعطل وظائف الحياة اليومية داخل المجتمع (قانون مكافحة الجرائم السيبرانية الإماراتي وتعديلاته، 2012).

وأصدرت الإمارات سنة 2022 قانون مكافحة الشائعات والجرائم الإلكترونية رقم (34)، ليحل محل القانون الاتحادي السابق رقم (5) لسنة 2012؛ إذ يعمل هذا القانون على توفير إطار عمل قانوني شامل لتعزيز حماية المجتمع من الجرائم

الإلكترونية المرتكبة من خلال شبكات وتقنيات الإنترنت. وحماية المواقع الإلكترونية وقواعد البيانات الحكومية في دولة الإمارات، ومكافحة انتشار الشائعات والأخبار المزيفة، والاحتيال الإلكتروني، والحفاظ على الخصوصية والحقوق الشخصية، كما يوضح الجرائم والعقوبات ضد أي شخص قد ينشئ أو يستخدم موقعاً إلكترونياً أو أي وسيلة تقنية معلومات لاختراق نظم المعلومات والبيانات الحكومية أو لمهاجمتها أو العبث بها، أو نشر معلومات كاذبة، أو معلومات تضر بمصالح الدولة وأمنها (قانون مكافحة الشائعات والجرائم الإلكترونية رقم 34، 2022).

المطلب الثالث: القانون الكويتي المنظم للأمن السيبراني

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:

أولاً: البنية التحتية للأمن السيبراني في الكويت

بدأت الكويت أولى خطواتها تجاه تطوير مجتمع المعرفة وتوظيف التكنولوجيا الحديثة في جميع قطاعات الدولة عام 2009، ووضعت خطة التنمية القطاعية في مجال تكنولوجيا المعلومات كإستراتيجية إلكترونية وطنية ضمن الخطة التنموية الخمسية للدولة (2009-2014)، وأخذت بنظر الاعتبار إعلان مبادئ جنيف وخطة عمل جنيف[4]، والتزام تونس وبرنامج عمل تونس[5]، والوثيقة الوطنية لبناء مجتمع

(4) المرحلة الأولى من القمة العالمية لمجتمع المعلومات، التي عقدت في جنيف خلال الفترة 10-12 كانون الأول (ديسمبر) 2003، وتضمنت وثيقتي إعلان المبادئ وخطة العمل على الصعيد العالمي، وبذلك أطلقت مرحلة التعاون الدولي لردم الفجوة الرقمية بين البلدان المتقدمة والبلدان النامية (الوثيقة WSIS-03/GENEVA/DOC/4).

(5) عقدت مرحلة تونس من القمة العالمية لمجتمع المعلومات من 16-18 تشرين الثاني(نوفمبر) 2005، وينطبق النظام الداخلي والترتيبات الأخرى التي اتفق عليها في الاجتماع الأول للجنة التحضيرية لمرحلة جنيف على مرحلة تونس من القمة والعملية التحضيرية التي سبقتها.

المعلومات بدولة الكويت[6]، والإستراتيجية العربية للاتصالات والمعلومات[7]، 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 لمواجهة التطور الحديث في مجال استخدام تكنولوجيا المعلومات، وتطوير السياسات والتشريعات الخاصة بأمن المعلومات (الإسكوا، 2009).

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 (الإسكوا، 2009).

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

(6) الوثيقة الوطنية لبناء مجتمع المعلومات بدولة الكويت، أقرت عام 2005، وصدرت عن الجهاز الفني المركزي لمشروع تطبيق استخدام التكنولوجيا في الأعمال الحكومية في الكويت.

(7) الإستراتيجية العربية للاتصالات والمعلومات التي وضعت أسسها عام 2009 بالتعاون بين جامعة الدول العربية واللجنة الاقتصادية والاجتماعية لغربي آسيا «الإسكوا» التابعة للأمم المتحدة، وحدّثت هذه الإستراتيجية في 29 أيلول (سبتمبر) 2022 من خلال عرضها على الاجتماع الحادي والثلاثين لفريق عمل الإستراتيجية العربية لتكنولوجيا المعلومات والاتصالات في بيروت.

الأمن السيبراني في دول المجلس، وبما ينسجم مع المعايير والاتفاقيات والمعاهدات الدولية الخاصة بهذا الشأن (المطيري، 2022).

ثانياً: 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 20 لسنة 2014 بشأن المعاملات الإلكترونية، وبعدها أصدر القانون رقم 37 لسنة 2014 المتعلق بإنشاء هيئة تنظيم الاتصالات وتقنية المعلومات، تلاه لاحقاً القانون رقم 98 لسنة 2015 المتعلق بتعديل أحكام القانون رقم 37 لسنة 2014، 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 2017-2020[8]، 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 الآمن 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.

(8) الإستراتيجية الوطنية للأمن السيبراني في دولة الكويت 2017-2020، أعدتها الهيئة العامة للاتصالات وتقنية المعلومات بدولة الكويت سنة 2017.

واستمراراً في النهج الهادف إلى استحداث قوانين جديدة خاصة بالأمن السيبراني، أدخلت الجريمة السيبرانية إلى التشريع الكويتي بموجب القانون رقم 63 لسنة 2015، المتعلق بمكافحة جرائم تقنية المعلومات، ويعتبر هذا القانون من أوائل القوانين الخليجية الخاصة بتجريم الأنشطة الإجرامية التي ترتكب في بيئة الفضاء السيبراني؛ حيث يجرَّم كلٌّ 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[9].

وكانت أحدث الخطوات التي اتخذت في مجال تطوير حماية البنى التحتية من الهجمات السيبرانية وتعزيز مستويات الأمن السيبراني في الدولة في سنة 2021؛ إذ أعلن مؤخراً في دولة الكويت عن إنشاء وزارة لشؤون الاتصالات وتكنولوجيا المعلومات[10]، التي عهد إليها تطوير البنية التحتية الإلكترونية، وتعزيز الأمن السيبراني، والارتقاء بمستوى الخدمات الحكومية الإلكترونية، وتنمية قطاع الاتصالات.

المطلب الرابع: أبرز الإيجابيات والسلبيات في القوانين الخليجية المنظمة للأمن السيبراني

قامت دول مجلس التعاون بخطوات جادة نحو تطوير أنظمتها القانونية الخاصة بالأمن السيبراني، وسعت إلى مواكبة المعايير الدولية الخاصة بهذا الشأن؛ نظراً لأهمية حماية الأمن السيبراني، خاصة في ظل تعرض بعض دول

(9) المادة (3) وما بعدها من القانون رقم 63 لسنة 2015 المتعلق بمكافحة جرائم تقنية المعلومات.

(10) أنشئت الوزارة بموجب المرسوم الأميري رقم 2021/18 الصادر في 2021/3/2، الخاص بتشكيل الوزارة. منشور في الجريدة الرسمية، الكويت اليوم، العدد 1525، السنة السابعة والستون، بتاريخ 2021/3/7.

المجلس لهجمات سيبرانية عديدة، إلا أن حداثة التجربة في هذه الدول أدت إلى وجود أوجه من القصور في بعض التشريعات؛ ما جعل تشريعات دول المجلس ذات إيجابيات وسلبيات في آن معاً، وعلى النحو الآتي:

أولاً: المملكة العربية السعودية

من أبرز الإيجابيات التي تضمنتها التشريعات السعودية المنظمة للأمن السيبراني النضج في توافقها مع المعايير الدولية الصادرة عن الاتحاد الدولي للاتصالات؛ وهو ما جعل السعودية تحتل المرتبة الأولى بين الدول العربية من حيث بناء القدرات. كما امتازت بكونها جاءت منظمة للقطاعين العام والخاص على حد سواء، وتحديداً لشركات القطاع الخاص العاملة في مجالات حساسة ترتبط بأمن المعلومات. بالإضافة إلى إصدار نظام مكافحة جرائم المعلوماتية السعودي لعام 2014، الخاص بمكافحة الجرائم الإلكترونية والمعلوماتية.

إلا أنه على الرغم من الخطوات المتسارعة التي اتخذتها السعودية في تطوير تشريعاتها الخاصة بالأمن السيبراني، فإن الجهود الحقيقية لا تزال بعيدة عن تنظيم قانون وطني خاص بالأمن السيبراني يحمي من الهجمات الإلكترونية ويفصلها ويجرمها تبعاً لأنواعها وبالشكل الذي ينسجم مع التشريعات والمعاهدات والاتفاقيات الدولية الخاصة بهذا الشأن؛ فالتشريعات الصادرة حتى الآن لا تزال تتمحور - في أغلبها - حول الجرائم السيبرانية أكثر مما تتناول الهجمات السيبرانية، إذ إن هناك اختلافاً جوهرياً بين المفهومين كما سبقت الإشارة إلى ذلك.

ثانياً: الإمارات العربية المتحدة

اتخذت الإمارات خطوات ملموسة فيما يتعلق بتنظيم التشريعات الخاصة بالأمن السيبراني؛ إذ بادرت إلى إنشاء الفريق الوطني للاستجابة لطوارئ الحاسب الآلي عام 2008، كما جاء قانون مكافحة الشائعات والجرائم الإلكترونية لسنة 2022 استجابة للمتغيرات التي شهدها العالم في مجال الأمن السيبراني وما صاحبه من تطور في التقنيات والأدوات والأساليب المستخدمة في الفضاء السيبراني. إلا أنه

من جهة أخرى حذا المشرع الإماراتي حذو المشرع السعودي فيما يتعلق بالأمن السيبراني؛ إذ اكتفى بإنشاء قوانين منظمة للجرائم السيبرانية، وكذا مكافحة الشائعات والجرائم الإلكترونية، إلا أن الهجمات السيبرانية لم تكن محل بحثٍ كافٍ من قبل القوانين الإماراتية، ولا تزال القوانين الوطنية غير فاعلة بالشكل الكافي للتعامل مع الهجمات السيبرانية في إطار القوانين الدولية والمعاهدات والاتفاقيات المنظمة لمسؤولية الأفراد والجماعات والدول تجاه الهجمات السيبرانية، وهو ما يعتبر قصوراً في هذا الشأن.

ثالثاً: دولة الكويت

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 لممثلين 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 لمشاركة القطاع الخاص. كما سعت الكويت جاهدة إلى تلبية المتطلبات الدولية الخاصة بإصدار قوانين ولوائح تتعلق بمكافحة الجرائم والهجمات السيبرانية[11]، وحرصت على تفعيل بعض المبادرات الوطنية والإقليمية الخاصة بتأهيل وتدريب الكوادر الوطنية العاملة في مجال الأمن السيبراني.

إلا أنه على الرغم من التكلفة المرتفعة التي خُصصت للإستراتيجية الوطنية للأمن السيبراني التي تشرف عليها الهيئة العامة للاتصالات وتقنية المعلومات في الكويت، التي بلغت ما يقارب 382 مليون دولار أمريكي، فإن الكويت ما زالت تحتل

(11) قضت محكمة الجنايات الكويتية بتاريخ 2020/10/26 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.

المركز الخامس على المستوى الخليجي، والمركز 65 على المستوى الدولي في تصنيف مؤشرات الأمن السيبراني (International Telecommunication Union, 2020).

رابعاً: دول مجلس التعاون عامة

على الرغم من جهود المجتمع الدولي الحثيثة التي بذلها لعقد اتفاقيات ومعاهدات دولية وثنائية ومتعددة الأطراف خاصة بالأمن السيبراني، وما شهدته القوانين الدولية من تعديلات تواكب التطور التكنولوجي، فإن دول مجلس التعاون لم تعمل حتى اليوم على إنشاء نظام موحد للأمن السيبراني لتدعيم التعاون الإقليمي في التصدي لمحاولات زعزعة الأمن السيبراني، وذلك على غرار الاتحاد الأوروبي الذي قام سنة 2016 بوضع نظام خاص بتوجيه الاتحاد الأوروبي حول أمن الشبكات والمعلومات، الذي يعتبر أول تشريع منظم للأمن السيبراني على المستوى الدولي؛ إذ يشمل هذا النظام مجموعة ضوابط أمنية ترتبط بحماية الأمن السيبراني، ولعل أبرز ما يميز هذا النظام الأوروبي قيامه على مبدأ المرونة التي تربط بين جهود القطاعين العام والخاص، وقد طلبت مفوضية الاتحاد الأوروبي من الشركات في الدول الأعضاء، التي تنشط في مجال البنية التحتية، ومن مشغلي الخدمات الأساسية، ومقدمي خدمات الإنترنت والبيانات، الحرص على ضمان أعلى مستويات الأمن المعلوماتي بالتنسيق مع الجهات الحكومية في القطاع العام وبالشكل الذي يتناسب مع حجم المخاطر المرتبطة بالأمن السيبراني، والحرص على مراعاة أمن النظم والمرافق الحيوية ومنشآت البنية التحتية، والتنسيق مع المؤسسات الرسمية الحكومية في حال وقوع هجمات سيبرانية من أجل التعامل مع آثار هذه الهجمات وضمان استمرارية الأعمال في المنشآت الحيوية ومرافق البنية التحتية المختلفة، بالإضافة إلى تشكيل فرق عمل مشتركة بين القطاعين العام والخاص تختص بعمليات الرصد والتدقيق والاختبار لكل ما يرتبط بأمن المعلومات والمخاطر السيبرانية المختلفة، وبما يتوافق مع القواعد الدولية الخاصة بهذا الشأن (الجمل، 2020).

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.

الخاتمة

لا تزال دول مجلس التعاون الخليجي 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 في دول المجلس، 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 في دول المجلس 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، لا تزال الجامعات الحكومية والخاصة في دول المجلس تعاني من تأخر ملموس في هذا الميدان، حتى في التخصصات الأكاديمية التي ترتبط بالحاسوب وأنظمته.

تكنولوجيا المعلومات والاتصالات أصبحت بنية تحتية عالمية لكل من الحكومات والشركات، ولا تقل أهمية في أي حال من الأحوال عن البنيات التحتية التقليدية؛ ومن ثم، فإن الأمن السيبراني أصبح ضرورة مطلقة لدول المجلس، 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.

إن وجود أطر قانونية وتشريعية وتنظيمية خاصة بحماية أمن المعلومات والاتصالات والفضاء السيبراني في دول المجلس قد أصبح مطلباً ملحاً؛ لضمان حماية المرافق الحساسة والبنية التحتية فيها، بالإضافة إلى أن هذه التشريعات والقوانين بدورها تسهل عمل المؤسسات المختصة وتمكنها من إدارة عملياتها بشكل أكثر فاعلية وقوة، كما تمكن من تسهيل عملية التعاون وتبادل المعلومات بين السلطات الوطنية ومؤسسات القطاع الخاص، سواء على المستوى الوطني داخل الدولة، أو على المستوى الإقليمي بين دول المجلس. وعلى 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.

التوصيات

بناءً على ما عرض في الدراسة، ومن واقع ما تناولته من قوانين وتشريعات خاصة بالأمن السيبراني عالمياً وإقليمياً وخليجياً، يمكن صياغة التوصيات الآتية:

1 - وجوب تضمين التشريعات الخاصة بالأمن السيبراني في دول مجلس التعاون لتعريفات واضحة ومحددة لمفهوم الأمن السيبراني، مع أهمية الإشارة إلى الفروقات بين مفهوم الجريمة السيبرانية والهجوم السيبراني.

2 - وضع إستراتيجية خليجية موحدة للأمن السيبراني، تهدف إلى تنظيم التعاون والتكامل بين دول المجلس لمواجهة مخاطر الهجمات السيبرانية وآثارها الجسيمة على البنية التحتية.

3 - 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.

4 - العمل على سن قانون موحد للأمن السيبراني لدول المجلس، يكون مستمداً من القوانين الوطنية الحالية ومكملاً لها، ومستنداً إلى الاتفاقيات والمعاهدات والقوانين الدولية الخاصة بالأمن السيبراني.

5 - محاولة الفصل بين الجرائم السيبرانية والهجمات السيبرانية في القانون الخليجي الموحد للأمن السيبراني؛ 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.

6 - إضفاء المرونة اللازمة على القانون الخليجي الموحد للأمن السيبراني، وذلك من خلال المرونة في إدراج القطاع الخاص في دول المجلس شريكاً حقيقياً في بناء منظومة الدفاع السيبراني، وإعطاء القطاع الخاص المساحة الكافية من الحرية للعمل والتنسيق مع الجهات الحكومية.

7 - إنشاء مركز خليجي موحد خاص بعمليات الأمن السيبراني، وتحت إشراف السلطات القضائية والتنفيذية المختصة في دول المجلس، تكون مهمته سرعة تبادل المعلومات والبيانات بين الدول الأعضاء، وبالشكل الذي يمكن من سرعة التصدي للهجمات السيبرانية والحد من تداعياتها على البنية التحتية.

المراجع

أبو زيد، عبدالرحمن. (2019). *الأمن السيبراني في الوطن العربي: دراسة حالة المملكة العربية السعودية*. المركز العربي للبحوث والدراسات. http://acrseg.org/41356

الإسكوا. (2009). *الملامح الوطنية لمجتمع المعلومات في دولة الكويت*. اللجنة الاقتصادية والاجتماعية لغربي آسيا «الإسكوا»، النسخة العربية، الأمم المتحدة، نيويورك.

https://www.unescwa.org/sites/default/files/inline-files/Kuwait-09-A.pdf

اعمر، عمر. (2019). الحرب الإلكترونية في القانون الدولي الإنساني. *دراسات، 46*(3)، 134-155.

https://journals.ju.edu.jo/DirasatLaw/article/viewFile/101907/10621?target=_blank

بن تغري، موسى. (2020). الحرب السيبرانية والقانون الدولي الإنساني. *مجلة الاجتهاد القضائي، 12*(22)، 199-218.

توريه، حمدون. (2011). *البحث عن السلام السيبراني*. الاتحاد الدولي للاتصالات.

https://www.asjp.cerist.dz/en/downArticle/124/12/2/112730

جاب الله، وليد. (2021). الأمن السيبراني بين الاحتكار والاستثمار. *مجلة الديمقراطية، 21*(82)، 49-53.

الجمل، حازم. (2020). الحماية الجنائية للأمن السيبراني في ضوء رؤية المملكة 2030. *مجلة البحوث الأمنية، 30*(77)، 243-328. https://search.mandumah.com/Record/1093749

الحازمي، مبارك. (2021). الإعلام العربي والأمن القومي: الرؤى والتحديات، نحو أجندة إعلامية مستقبلية، *المجلة المصرية لبحوث الاتصال الجماهيري، 2*(1)، 9-46.

https://mebp.journals.ekb.eg/article_159616_aa3522c6192cd2be4e1181a647f1786f.pdf

حبريري، نجلاء. (2019، أبريل 6). *السعودية تتحول من مستهلك للمعرفة إلى مصدّر للكفاءات. الشرق الأوسط*. https://bit.ly/2G4kyUa

حسن، كاميران. (2021). *الجهود الدولية في مواجهة الجرائم السيبرانية*. منشورات الحلبي الحديثة.

حمزة، مجيد. (2017). الإعلام الرقمي الإلكتروني للإرهاب وسبل المواجهة إعلامياً. *المجلة السياسة والدولية، 35*(36)، 59-94. https://www.iasj.net/iasj/article/135865

حميد، عبدالوهاب. (2021). الأمن السيبراني: القيود والتحديات في ضوء قواعد القانون الدولي. *مجلة العقد الاجتماعي، 1*، 309-336.

https://www.researchgate.net/publication/354780005_alamn_alsybrany-_alqywd_walthdyat_fy_dw_qwad_alqanwn_aldwly

دروغيه، كوردولا. (2011). *ما من فراغ قانوني في الفضاء السيبراني*. منشورات اللجنة الدولية للصليب الأحمر.

https://www.icrc.org/ar/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm

دليل تالين. (2019). *دليل تالين بشأن القانون الدولي المطبق على الحروب السيبرانية*. (علي الموسوي، ترجمة). اللجنة الدولية للخبراء. مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي «الناتو». شركة المؤسسة الحديثة للكتاب. bit.ly/3MIK8zq

الرفادي، بسمة. (2018). الحروب السيبرانية وأثرها في التنظيم الدولي. *مجلة العلوم والدراسات الإنسانية، 49*، 1-14.

سعيد، كامل. (1993). *جرائم الكمبيوتر والجرائم الأخرى في مجال التكنولوجيا*. بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، جمهورية مصر العربية.

سليمان، فاضل. (2020). حق الدفاع الشرعي على الهجمات السيبرانية. *مجلة جامعة تكريت للحقوق، 4*(4)، 245-260.

سمودي، رزق. (2018). حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون. *مجلة جامعة الشارقة للعلوم القانونية، 15*(2)، 336-362. https://doi.org/10,36394/jls.v15.i2,12

فياض، حسن. (2020). الهجمات السيبرانية من منظور القانون الدولي الإنساني. *مجلة الدفاع الوطني اللبناني*، *114*(10)، 34-5. bit.ly/439Dlpi

لطفي، وفاء. (2022). الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني: التجربة الماليزية نموذجاً. *مجلة كلية الاقتصاد والعلوم السياسية*، *23*(1)، 178-152.
https://jpsa.journals.ekb.eg/article_211371_54250591ebca0fba4f921772704411df.pdf

محمود، خالد. (2013). *الهجمات عبر الإنترنت ساحة الصراع الإلكتروني الجديد*. المركز العربي للأبحاث ودراسة السياسية.
https://siyasatarabiya.dohainstitute.org/ar/issue005/Pages/Siyassat05-2013_Mahmoud.pdf

مركز سمت للدراسات. (2019). *السعودية واقتصاديات المستقبل: خطوة جادة لتحقيق الريادة*، مركز سمت للدراسات. bit.ly/3C4JWpf

المطيري، خالد. (2022). دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي. *مجلة البحوث الفقهية والقانونية*، *38*(7)، 1066-969.
https://journals.ekb.eg/article_250062_798efc55350b93931f7d66f72addfe72.pdf

هروال، نبيلة. (2013). *جرائم الإنترنت: دراسة مقارنة*. منشورات كلية الحقوق والعلوم السياسية، جامعة تلمسان.

الهيئة الوطنية للأمن السيبراني. (2018). *الضوابط الأساسية للأمن السيبراني*. الهيئة الوطنية للأمن السيبراني. bit.ly/3ILtnm3

وزارة الاتصالات وتكنولوجيا المعلومات. (2014). الاستراتيجية الوطنية للأمن السيبراني. وزارة الاتصالات وتكنولوجيا المعلومات القطرية.
https://www.mot.gov.qa/sites/default/files/lstrtyjy_lwtny_llmn_lsybrny.pdf

وكالة الأنباء الإماراتية [وام]. (2022، أكتوبر 24). *الإمارات تشارك في اجتماع اللجنة الوزارية للأمن السيبراني في دول التعاون.. وإطلاق التمرين الخليجي الأول للأمن السيبراني*.
http://wam.ae/ar/details/1395303094178

وكالة الأنباء الكويتية [كونا]. (2022، أكتوبر 23). *اللجنة الوزارية للأمن السيبراني بدول مجلس التعاون تعقد اجتماعها الأول*.
https://www.kuna.net.kw/ArticleDetails.aspx?id=3062862&language=ar

Asogwa, C. (2020). Internet-Based communications: A threat or strength to national security? *SAGE Open, 4*(6), 1-9. https://journals.sagepub.com/doi/epub/10.1177/2158244020914580

European Commission. (2022). *Convention on cybercrime*. European Treaty Series No.185, Council of Europe.

Finckenstein, V. (2019). *Cyber security in the Middle East and North Africa*. Economist intelligence cyber security report, Konrad Adenauer Foundation. bit.ly/3OTeOjU

Gervais, M. (2011). Cyber attacks and the law of warfare. *Berkeley Journal of International Law, 30*(2), 525-579. bit.ly/43u0FxO

Henckaerts, J., & Doswald-Beck, L. (2005). *Customary international humanitarian law*. Chapter 1 - Distinction between civilians and combatants (Rules 1–6). Cambridge University Press. https://www.icrc.org/en/doc/assets/files/other/customary-international-humanitarian-law-i-icrc-eng.pdf

International Telecommunication Union. (2020). *Global cyber security index*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Interpol. (2017). *Global cybercrime strategy*. Interpol General Secretariat. https://www.cybercrimelaw.net/documents/The_Role_of_INTERPOL.pdf

Nmah, O. (2019). *The effects of social media on national security* [Unpublished master's thesis]. Command and General Staff College. https://apps.dtic.mil/sti/pdfs/AD1105214.pdf

Rid, T., & Mcburney, P. (2012). Cyber–Weapons. *The RUSI Journal*, *157*, 6-13. https://www.tandfonline.com/doi/epdf/10.1080/03071847.2012.664354?needAccess=true&role=button

Saeed, M., & Salem, M. (2015). *Cyber security and data privacy law in Saudi Arabia*. Financier Worldwide. https://www.financierworldwide.com/cyber-security-and-data-privacy-law-in-saudi-arabia#.YylejXZBzIU, viewed in 16/9/2022.

Schmidt, M. (2015). The law of cyber targeting. *Naval War College Review, 68*(2), 11-30.https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1199&context=nwc-review

Schmitt, M. (Ed.) (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations* (2nd ed.). Cambridge University Press. https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf

Shanghai Cooperation Organization "SCO". (2013). *Agreement on cooperation in ensuring international information security between the member states of the Shanghai Cooperation Organization*. Shanghai Cooperation Organization. https://cis-legislation.com/document.fwx?rgn=28340

Shires, J., & Hakmeh, J. (2020). *Is the GCC Cyber Resilient?*. International Security Program, Chatham House. https://www.chathamhouse.org/2020/03/gcc-cyber-resilient

Traynor, I. (2007 May 17). *Russia accused of unleashing cyber war to disable Estonia*. Guardian London . bit.ly/3OOatyz

د. فهد أحمد عبدالرحمن، حاصل على دكتوراه في القانون الدولي من الجامعة الأردنية، كلية الحقوق، في المملكة الأردنية الهاشمية سنة 2017. باحث مستقل، الاهتمامات البحثية: جميع جوانب القانون المتعلقة بالقانون الدولي وتطوراته بالإضافة إلى الجرائم الجنائية والجرائم الإلكترونية.
الإيميل: L-F8D@hotmail.com

للاستشهاد:

عبدالرحمن، فهد أحمد. (2023). الإطار القانوني للأمن السيبراني لدول مجلس التعاون الخليجي. *مجلة دراسات الخليج والجزيرة العربية*، *49*(190)، 257-298.
https://www.doi.org/10.34120/0382-049-190-008

To cite:

Abdulrahman, F. A. (2023). The legal framework of cyber security for the Gulf Cooperation Council Countries. *Journal of the Gulf and Arabian Peninsula Studies, 49*(190), 257- 298.
https://www.doi.org/10.34120/0382-049-190-008