Dirasat: Shari'a and Law Sciences, Volume 50, No. 3, 2023

Deanship of Scientific Research

Cyber-Attacks on Smart City: Infrastructure, Legal Challenges and Confrontation Strategy

Emad El Din Mohamed Kamel Abdul Hamid *

Department of Law, Imam Malik College of Sharia & Law, Government of Dubai, United Arab Emirates.

Received: 22/10/2022
Revised: 23/11/2022
Accepted: 16/2/2023
Published: 1/9/2023

* *Corresponding author:*
emadeldin@imc.gov.ae

Citation: Abdul Hamid, E. E. D. M. K. (2023). Cyber-Attacks on Smart City: Infrastructure, Legal Challenges and Confrontation Strategy. Dirasat: Shari'a and Law Sciences, 50(3), 54–70.
https://doi.org/10.35516/law.v50i3.2864

Abstract

Objectives: The study seeks to elucidate the concept of smart cities, outlining their distinctive pillars and characteristics compared to traditional cities. It delves into the legal aspects of cyber-attacks, particularly focusing on the increase of cyber-terrorism and cyber-warfare incidents. The analysis defines the legal nature of these attacks and proposes strategies for combating them, accompanied by pertinent recommendations.

Methods: The study used inductive and comparative analytical approaches to evaluate smart cities and police, emphasizing protective measures against cyber-terrorism and cyber-warfare. It assessed the effectiveness of cybersecurity systems and explored causes for rising cyber-attacks despite existing security measures. The analysis also involved reviewing legislation governing the UAE's Smart Police and comparing experiences with other countries to gauge success in reducing such crimes.

Results: The study showed that the conflict between technologies and the weakness of the cyber security system is the main factor in the increase in cybercrimes against smart cities' infrastructure. The study also revealed that cyber-terrorism and cyber-wars are among the greatest threats to the national security of smart cities, and it is extremely difficult to determine the legal nature of each. Therefore, achieving physical security is the first line of defense to promote and protect the cyber national security facilities of the smart city infrastructure.

Conclusions: The study recommends warning against not importing ready-made protection systems for cyber security because of their risk to countries' national security . The study also highlights the need to promote and spread a culture of cyber security among citizens of smart cities.

Keywords: Cyberspace, smart cities, cyber-attacks, cyber security, legal challenges.

الهجمات السيبرانية على البنى التحتية للمدن الذكية: التحديات القانونية واستراتيجية المواجهة

عماد الدين محمد كامل عبد الحميد*

قسم القانون، كلية الإمام مالك للشريعة والقانون، حكومة دبي، دولة الإمارات العربية المتحدة.

ملخّص

الأهداف: بيان مفهوم المدن الذكية وركائزها وخصائصها التي تميزها عن المدن التقليدية، وطبيعة الهجمات السيبرانية الواقعة عليها، وأسباب تزايدها، خاصة هجمات الإرهاب السيبراني والحروب السيبرانية، مع تحديد الطبيعة القانونية لكل تلك الهجمات، وبيان طرائق مكافحتها، مع وضع التوصيات اللازمة.

المنهجية: المنهج الاستقرائي باستقراء حقيقة المدن الذكية وطبيعة الشرطة الذكية القائمة على حمايتها، ودورها في مكافحة جرائم الإرهاب السيبراني والحروب السيبرانية التي ترتكب ضد تلك المدن، واستقراء حقيقة منظومة الأمن السيبراني المقررة لحمايتها جراء تلك الهجمات. كما تم استخدام المنهج التحليلي المقارن بتحليل ومقارنة طبيعة الهجمات السيبرانية، وأسباب تزايدها رغم وجود منظومات الأمن السيبراني والتطبيقات الذكية وأنظمة الذكاء الاصطناعي لشرطة تلك المدن. كما اعتمدت الدراسة على تحليل نصوص تشريعات تنظيم الشرطة الذكية لدولة الإمارات لاستخلاص الأحكام العامة التي تنظم عملها، مع عقد مقارنة بين تجارب بعض الدول ودولة الإمارات في مجال الشرطة الذكية، للوقوف على مدى النجاح في مكافحة جرائم تلك الهجمات أو الحد من ارتكابها.

النتائج: صراع التقنيات وضعف منظومة الأمن السيبراني يُعد العامل الجوهري والأساسي لتزايد جرائم الهجمات السيبرانية المرتكبة ضد البنى التحتية للمدن الذكية، وأن الإرهاب السيبراني والحروب السيبرانية يُعدان من أكبر التهديدات للأمن القومي للمدن الذكية، وهناك صعوبة بالغة لتحديد الطبيعة القانونية لكل منهما. لذا فإن تحقيق الأمن المادي يُعد خط الدفاع الأول لتعزيز وحماية مرافق الأمن القومي السيبراني للبنى التحتية للمدن الذكية.

الخلاصة: تُوصي الدراسة بعدم استيراد منظومات الحماية الجاهزة الخاصة بالأمن السيبراني لخطورتها على الأمن القومي للدول، كما تُشدد على ضرورة تعزيز ونشر ثقافة الأمن السيبراني لدى مواطني المدن الذكية.

الكلمات الدالة: الفضاء السيبراني، المدن الذكية، الهجمات السيبرانية، الأمن السيبراني، التحديات القانونية.

المقدمة

أدى تدفق سكان مختلف دول العالم إلى المناطق الحضرية، ونمو وتزايد الكثافة السكانية في تلك المناطق إلى أن تُعيد الدول وجهة نظرها في استراتيجيات وسياسات إدارة النمو الحضري، بالاتجاه نحو تأسيس وتطوير بنى تحتية قوية ومستدامة، قادرة على الصمود في مواجهة الاحتياجات الناجمة عن التوسع الحضري والنمو السكاني، خاصة بعد صدور العديد من التقارير التي تؤكد تلك الحقائق، منها تقرير حديث صادر عن منظمة الأمم المتحدة يفيد أن 55%من السكان في العالم يعيشون في مناطق الحضر والمتوقع زيادة تلك النسبة بحلول عام 2050لتصل لـ 60% (Nations,,2018)، الأمر الذي دفع حكومات مختلف دول العالم إلى التحول نحو المدن الذكية تلك القائمة على تكنولوجيا تقنية المعلومات والاتصالات التي كانت بدايتها الاتصالات السلكية واللاسلكية ثم الأقمار الصناعية والألياف البصرية التي انتهت بتقنية شبكات الجيل الخامس (5G) 2020، لتطبيقات الأجهزة اللاسلكية الثابتة والمتنقلة التي استطاعت أن توفر داخل المدن والمناطق بيئات ذكية مترابطة بين الأشخاص والتطبيقات والبيانات والأشياء والآلات وأنظمة النقل، مع سرعة في الأداء وموثوقية عالية.

فأصبحت مرافق ومؤسسات البنى التحتية لأغلب حكومات ومدن دول العالم في كافة مجالات الطاقة: منظومة النقل، المياه، الصحة، قطاع البنوك وأنظمة الدفع، ومختلف المؤسسات المالية والحكومية، يتم إدارتها وتشغيلها والترابط بينها وتقديم خدماتها عبر شبكات الاتصالات وتقنية المعلومات والتطبيقات الذكية وأنظمة الذكاء الاصطناعي، الأمر الذي ترتب عليه أن أصبحت مرافق ومؤسسات البنى التحتية أصبحت قوة جذب كبيرة للاعتداء عليها بمختلف الهجمات السيبرانية، لما تتضمنه مفردات تلك البنى التحتية من معلومات وبيانات وأسرار تتعلق بتلك المرافق والمؤسسات، فضلاً عما ترتبه تلك الهجمات من خسارة اقتصادية تعوق تطور تلك المدن نحو تحقيق الاستدامة.

وأصبحت حماية مرافق ومؤسسات البنى التحتية مصدر قلق دولي بالغ الخطورة لأغلب حكومات ومدن دول العالم ومنظماته الدولية، نظراً لطبيعة تقنيات الهجمات السيبرانية العابرة للحدود حول العالم التي قد تنطلق من الطرف الآخر للكرة الأرضية وتصيب هدفاً واحداً عدة مرات، أو تصيب أهدافاً متعددة في وقت واحد وفي ثوانٍ معدودة، سواء من قبل أفراد أو دول أو جماعات أو منظمات، ودون تحديد مصدر تلك الهجمات أو تعقبها ومن ثم ضبط مرتكبيها وملاحقتهم.

الأمر الذي فرض على الدول ضرورة وجود منظومة قوية ومتطورة للأمن السيبراني لتأمين وحماية مؤسسات ومرافق تلك البنى التحتية، فسارعت مختلف الدول بوضع استراتيجيتها لتحقيق الأمن السيبراني، فاصطدمت بحقيقة علمية أجمع عليها خبراء الأمن السيبراني وهي أنه لا يمكن تحقيق الأمن السيبراني بنسبة مائة في المائة، فعالمنا اليوم يشهد صراعاً للتقنيات، ولم يعد يصلح القول بأن تقنية اليوم تخترق بتقنية الغد، بل كل ثانية هناك تقنية جديدة تخترق وتقوض ما سبقها من تقنيات، وأنه لا يمكن لأي منظومة أمن سيبراني مهما بلغت تقنياتها المتطورة أن تمنع تلك الهجمات السيبرانية، بل مجرد التقليل من المخاطر والتهديدات لتلك الهجمات السيبرانية، وبالقدر الذي يحقق استفادة تلك المدن الذكية من فرص هائلة ومدخرات كبيرة توفرها تطبيقاتها الذكية.

الأمر الذي دفع الباحث في نهاية دراسته المتواضعة إلى وضع استراتيجية حماية قد تُعد خطوة على طريق الحماية المنشودة.

إشكاليات موضوع الدراسة: قانونية وتقنية معقدة ومتشابكة وتتجسد في أن مرافق ومؤسسات البنى التحتية للمدن الذكية لمختلف دول العالم المتقدم، وما تضمنته من أنشطة ومعاملات، وبيانات وأسرار ومعلومات في كافة المجالات قد ارتكزت على ذلك الفضاء السيبراني، فأصبحت قوة جذب للاعتداء عليه بالهجمات السيبرانية، العابر للحدود حول العالم، سواء من قبل الدول أو الأفراد أو التنظيمات أو الجماعات، سواء اتخذت صورة جرائم سيبرانية تقليدية أو إرهاب سيبراني أو حروب سيبرانية بين الدول، الأمر الذي فرض تساؤل رئيسي وجوهري هو كيفية حماية تلك البنى التحتية للمدن الذكية من الهجمات السيبرانية لتلك الجرائم في ظل تطور تقنياتها المستمر؟ هذا التساؤل استوجب عدة تساؤلات فرعية الإجابة عنها تُمثل مفردات البحث ومدى أهميته.

تساؤلات موضوع الدراسة:

1- ما مفهوم المدن الذكية وركائزها وخصائصها التي تتميز به عن مختلف المدن التقليدية؟

2- ما الهجوم السيبراني وأنواعه ووسائله وآثاره على مرافق البنى التحتية للمدن الذكية؟

3- ما أسباب تزايد الهجمات السيبرانية على مرافق البنى التحتية للمدن الذكية؟

4- ما أسباب تزايد الهجمات السيبرانية على مرافق البنى التحتية للمدن الذكية خلال جائحة كوفيد 19؟

5- ما الطبيعة القانونية للهجمات السيبرانية حتى يمكن تصنيف الجرائم الناجمة عنها؟

6-ما نماذج جرائم الهجمات السيبرانية على البنى التحتية للحكومات والمدن الذكية خلال 2022، للوقوف على مدى خطورتها؟

7-ما التحديات القانونية التي تُثيرها جرائم الهجمات السيبرانية على البنى التحتية للمدن الذكية؟

8-ما الإطار التشريعي لمواجهة جرائم الهجمات السيبرانية على البنى التحتية للمدن الذكية؟

9-ما مفهوم الأمن السيبراني ومدى ارتباطه بالأمن القومي للدول؟

10-هل ضعف منظومة الأمن السيبراني للدول يُعد العامل الرئيسي في تزايد تلك الهجمات السيبرانية؟

أهمية موضوع الدراسة: تبدو في بيان ما يلي: ماهية المدن الذكية – ركائزها - خصائصها، مفهوم الهجمات السيبرانية وأنواعها، وأنواعها وأسباب تزايدها على المدن الذكية، الطبيعة القانونية لتلك الهجمات التي تُشكل جرائم الاعتداء على تلك المدن خاصة هجمات الإرهاب السيبراني وهجمات الحروب السيبرانية، مفهوم الأمن القومي وتطوره ومدى ارتباطه بالأمن السيبراني، ماهية الأمن السيبراني، الإرهاب السيبراني الحروب السيبرانية كأكبر التهديدات للأمن القومي للمدن الذكية، ومظاهر جرائم الأمن القومي السيبراني وهجماته على مرافق البنى التحتية للمدن الذكية المقارنة في 2022 وعوامل تزايدها.

الهدف من موضوع الدراسة: تهدف إلي بيان مدى ضرورة الاستفادة من معطيات العلوم الحديثة وتقنيتها وتطورها وتوظيفها في المجال الجنائي، في البحث عن الحقيقة وتسكين نتائجها في مواضعها المناسبة، لتحقيق نسق الحماية المطلوبة لمكافحة جرائم الهجمات السيبرانية المرتكبة على مرافق البنى التحتية للمدن الذكية، وإيجاد الحلول للتحديات القانونية والتقنية التي تمثل إشكاليات موضوع البحث، وذلك من خلال خطة بمحاور للعديد من التوصيات وضعها الباحث لمكافحة جرائم الهجمات السيبرانية على البنى التحتية للمدن الذكية.

الدراسات السابقة: لا توجد دراسات سابقة عن موضوع البحث وكل الدراسات المتواجدة غير متعلقة ومتناثرة، كتناول دراسة الإرهاب السيبراني، الحروب السيبرانية، دون تناول تعلقها أو أثرها على مرافق البنى التحتية للمدن الذكية لتعلقها بالأمن القومي للدول، وذلك على النحو التالي:

أ-د طلال أبو غزالة، المستقبل الرقمي الحتمي-عالم المدن الذكية، طلال أبو غزالة للترجمة والتوزيع والنشر والتوزيع، 2021.

تناولت الدراسة في هذا الكتاب المستقبل الرقمي الحتمي لعالم المدن الذكية، وتعد من أفضل الدراسات التي تناولت هذا الموضوع، وتخصصت في بيان فوائد المدن الذكية، أسس المدينة الذكية، الذكاء الاصطناعي وأنواعه، التطبيقات الذكية، تطوير المدن الذكية، المدن الذكية والأوبئة، ولكنها لم تُشر إلى موضوع الدراسة وهو الهجمات السيبرانية على البنى التحتية للمدن الذكية.

ب- الأمم المتحدة (الإسكوا)، المدن الذكية المستدامة والحلول الرقمية الذكية لتعزيز المرونة الحضرية في المنطقة العربية- دروس من الجائحة، 2021.

تناولت الدراسة المرونة الاقتصادية الحضرية، المدن الذكية المستدامة، المرونة الاقتصادية الحضرية والمدن الذكية المستدامة، المرونة الحضرية في المنطقة العربية، المدن الذكية المستدامة في المنطقة العربية، تنفيذ هدف التنمية المستدامة 11 في المنطقة العربية، القدرة على الصمود في مواجهة الأوبئة ودور الحلول الرقمية الذكية، الحلول الرقمية الذكية لمكافحة كوفيد 19، ولكنها لم تُشر إلى موضوع الدراسة؛ وهو الهجمات السيبرانية على البنى التحتية للمدن الذكية.

ج- شيخه حسني الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، المجلد 17، العدد 1، 2020.

تناولت هذه الدراسة التعاون الدولي في مواجهة الهجوم السيبراني، وتخصصت في بيان التعاون الدولي بين أجهزة الشرطة، تعاون السلطات القضائية للدول، الاتفاقيات الدولية في مجال مكافحة الهجوم السيبراني، تسليم المتهمين للعدالة، لتعاون الدولي في مجال التدريب على الحد من الهجوم السيبراني وأهميته، الصعوبات التي تواجه التعاون الدولي، وكيفية القضاء عليها.

منهج الدراسة: هو المنهج الاستقرائي والمنهج التحليلي المقارن، المنهج الاستقرائي من خلال استقراء حقيقة وجوهر المدن الذكية وركائزها وخصائصها- حقيقة وجوهر جرائم الهجمات السيبرانية على مرافق البنى التحتية للمدن الذكية، ووسائل ارتكابها، وبيان مظاهر ارتكاب تلك الجرائم، للوصول إلى حجم التهديدات والأضرار الواقعة على مرافق الأمن القومي السيبراني للمدن الذكية جراء تلك الجرائم، والمنهج التحليلي المقارن من خلال تحليل ومقارنة طبيعة الهجمات السيبرانية على المدن الذكية، وتحدياتها القانونية، الإطار التشريعي لمواجهة جرائمها، لاستخلاص طبيعتها القانونية، والأحكام العامة لها، وأسباب تزايد ارتكابها، من أجل وضع التوصيات اللازمة لمكافحتها.

خطة الدراسة: تم تقسيمه إلى ثلاث مباحث ولكل مبحث مطلبين، المبحث الأول ماهية المدن الذكية، المطلب الأول منه مفهوم المدن الذكية وركائزها، المطلب الثاني خصائص المدن الذكية، والمبحث الثاني جرائم الهجمات السيبرانية على البنى التحتية للمدن الذكية، المطلب الأول ماهية الهجوم السيبراني، وأسباب تزايده على المدن الذكية، والمطلب الثاني الطبيعة القانونية للهجمات السيبرانية على البنى التحتية للمدن الذكية، المبحث الثالث استراتيجية مواجهة الهجمات السيبرانية على البنى التحتية للمدن الذكية، المطلب الأول الأمن السيبراني لمواجهة الهجمات السيبرانية على البنى التحتية للمدن الذكية، المطلب الثاني خطة الباحث لمواجهة الهجمات السيبرانية على البنى التحتية للمدن الذكية.

المبحث التمهيدي: ماهية المدن الذكية

تمهيد: يتطلب بيان ماهية المدن الذكية أن نقوم بتعريف المدن الذكية، ثم دراسة الركائز التي تقوم عليها المدن الذكية التي لو توافرت تندرج

المدينة تحت مصطلح المدن الذكية، ومن ثم نستطيع أن نستخلص خصائص تلك المدن للوقوف على طبيعتها وذاتيتها التي تميزها عن المدن التقليدية، وذلك على النحو التالي:

المطلب الأول: مفهوم المدن الذكية وركائزها

المطلب الثاني: خصائص المدن الذكية

المطلب الأول: مفهوم المدن الذكية وركائزها

أولا تعريف المدن الذكية:

عرفها بعض الفقه بأنها المدينة " التي تربط بين مختلف البنى التحتية المادية التقليدية، والبنى التحتية الاجتماعية، والبنى التحتية للأعمال، والبنية التحتية لتكنولوجيا المعلومات والاتصالات؛ لتحقيق الاستفادة من الذكاء الجماعي للمدينة"(Eckman, Hamilton, 2010, p2.)،و تستخدم تقنيات الحوسبة الذكية لجعل مرافق ومكونات وخدمات البنية التحتية الحيوية للمدينة أكثر ذكاءً، وترابطًا، وكفاءة" (Washburn, Sindhu 2010, P 5.)،وهي" المدينة التي تملك نظاماً متطوراً يرتكز على بنى تحتية قائمة على تكنولوجيا الاتصالات والمعلومات، لتشغيل وإدارة ومراقبة بنيتها التحتية ومرافقها ومؤسساتها، مثل مرافق الطاقة والمياه وشبكات الطرق، وأنظمة النقل وغيرها " (العقيل، 2014، ص4).

وجاء في تعريف الاتحاد الدولي للاتصالات (ITU) أنها" المدينة المبتكرة القائمة على استخدام تكنولوجيا المعلومات والاتصالات، وذلك من أجل تحسين نوعية وجودة الحياة، ولتحقيق الكفاءة في العمليات والخدمات خاصة الحضرية – ولزيادة القدرة على المنافسة، لتلبية احتياجات الأجيال الحالية، وكذلك القادمة في كافة المجالات سواء كانت اقتصادية أو بيئية أو اجتماعية أو ثقافية (ITU),2021.))، وفي تعريف منظمة التعاون الاقتصادي والتنمية (OECD) هي" مبادرات أو مناهج تستفيد بشكل فعال من الرقمنة لتعزيز رفاهية المواطنين، وتقديم خدمات وبيئات حضرية أكثر كفاءة واستدامة وشمولية كجزء من تعاون عملية أصحاب المصلحة المتعددين"(OECD, 2020, P 8.).

تعريف الباحث المدن الذكية:

يُعرف الباحث المدن الذكية بأنها" المدن القائمة على المزج والتكامل بين تكنولوجيا المعلومات والاتصالات (ICT) وبين إدارة وتشغيل وخدمات مرافق البنى التحتية للمدن، لتوفير خدمات وبيئات حضرية آمنة ومرنة وقابلة للتكيف، وأكثر كفاءة واستدامة وشمولية وصديقة للبيئة بأقل تكاليف، لتحسين جودة الحياة لتلبية احتياجات الأجيال الحالية والقادمة.

ثانياً ركائز المدن الذكية: إن الحديث عن ركائز المدن الذكية في حقيقته يثير بلا شك الحديث عن جوانب تلك المدن وأبعادها ومكوناتها التي لو توافرت في المدينة لارتقت تحت مسمى المدن الذكية، لذا فالواقع العملي لتلك المدن ومن خلفه خبراء تكنولوجياتها يشهد وبحق تبايناً واضحا واختلافا حول عدد تلك الركائز وأولويات ترتيبها لكي تُصنف تلك المدن بأنها ذكية، وذلك يرجع إلى عوامل رئيسية هي التي تُشكل مفردات تلك الركائز وأولوياتها ومسار تطورها والتي تختلف من مدينة إلى أخرى، مثل مستوى التنمية، ومدى توافر الموارد ومدى قدرة رأس المال وكفايته، فضلاً عن درجة الاستعداد للتغيير والإصلاح لدى قيادات تلك المدن وتطلعات سكانها.

إلا أنه يرى الباحث أن هناك قاسماً مشتركاً من تلك الركائز لا يمكن إدراج تلك المدن تحت مُصنف مدن ذكية إلا بتحققها، وهو مزج وتكامل بين تكنولوجيا المعلومات والاتصالات (ICT)وبين إدارة وتشغيل وخدمات مرافق البنى التحتية للمدن، مع وجود مواطن ذكي مدرب ومؤهل لاستخدام تلك الخدمات الذكية والاستفادة منها وتطويرها، وشرطة ذكية لمراقبة السلامة العامة وتحقيق أمن المعلومات والبيانات والمرافق، وذلك لزيادة الكفاءة وخفض التكاليف وتحسين جودة الحياة في تلك المدن.

فهناك من يرى أن المدن الذكية يجب أن تؤسس على ركائز خمس (OusephJuly, 2017)، حلول الطاقة الذكية: حلول السلامة والأمن الذكية: كفاءة البنية التحتية والنقل، الحوكمة الإلكترونية: تكنولوجيا المعلومات والاتصالات.

وهناك بعض من تقارير الخبراء انتهت إلى 10 ركائز للمدن الذكية (CRUICKSHANK, 2018.) **هي:**

الحوكمة، الاقتصاد، البنى التحتية، الموهبة، التمويل: التنقل، البيئة: السلامة العامة: الصحة العامة: أنظمة الدفع الذكية.

قمة المدن الذكية 2020: في قمة المدن الذكية التابعة لرابطة أمم جنوب شرق آسيا ومعرض إكسبو 2020 شارك العديد من العلماء وخبراء التكنولوجيا من مختلف دول العالم وجهات نظرهم حول توليف مجموعة من الركائز تقوم عليها المدن الذكية، وانتهت نتائج بحثهم إلى ضرورة توافر ستة ركائز للمدن الذكية(MOST,2021.) ، مع الأخذ في الاعتبار تباين المدن الذكية بين مختلف دول العالم في مدى اكتمال توافر هذه الركائز لديها، وذلك حسب طبيعة كل مدينة وترتيب الأولويات، ومدى قدرة رأس المال لديها، وهذه الركائز هي:

المواطن الذكي: بالتحسين المستمر لقدراته ومؤهلاته العلمية من أجل الاستجابة لطلب العمل في سوق عمل متكيف ومرن سريع التغير في مجتمع مرتبط بالمدن الذكية.

حركة المرور الذكية النقل الذكي: زيادة تطبيق التكنولوجيا لحل مشاكل منظومة النقل العام، بتشغيل وإدارة المواقف الذكية، ومشاركة خط سير السيارات، ومواعيد تحركاتها وتواجدها، وبتوفير وبإدارة شبكات نقل متعددة الوسائط لتحسين الاتصال وجودة مرافق النقل العام، بتمكين المواطنين من استخدام مرافق تنقل أسرع وأرخص وصديقة للبيئة، مما يقلل من الازدحام المروري، ويزيد من قدرة العبور في المدينة، ويقلل من الانبعاثات السامة التي سيكون لها تأثير كبير على البيئة.

البيئة الذكية: تُعني ضمان الأمن البيئي للبنية التحتية الاجتماعية ومواطنها من خلال تحسين جودة البيئة، وحماية الموارد الطبيعية باستمرار، وقيم المناظر الطبيعية، والحفاظ على النظم البيئية المتدهورة واستعادتها، والبيئة الذكية تتكيف مع تغير المناخ، وتنفذ حلولاً لتقليل انبعاثات غازات الاحتباس الحراري، وزيادة الاستثمار في البحث والتطوير التكنولوجي المتعلق بكفاءة الطاقة والسلامة، لضمان أمن الطاقة والوقود، وتطوير مصادر الطاقة المتجددة وتقليل الأثر البيئي لانبعاثات الطاقة، لتحقيق إدارة فعالة وشاملة للموارد البيئية، والاستخدام السليم للموارد الطبيعية.

الاقتصاد الذكي هو الاقتصاد الذي يقوم على الابتكار وتكنولوجيا المعلومات الحديثة التي تشمل المنافسة العالمية، وروح المبادرة، والإنتاجية العالية، والمرونة مع سوق العمل.

الحوكمة الذكية: من منظور الإدارة الذكية والخدمات العامة، تأخذ سلطة المدينة أولويات مهمة لمشاركة المواطنين في صنع القرار وشفافية الإجراءات من أجل جودة الخدمات العامة وتوافرها، فالحوكمة الذكية هي عملية إيجاد توازن متزايد بين المتطلبات البيئية والضغوط الاجتماعية لتحسين نوعية الحياة.

الحياة الذكية: قائمة على شبكات تقنية المعلومات والاتصالات وأنظمة الذكاء الاصطناعي تتضمن إنشاء نظام فعال للأماكن العامة عالية الجودة في المناطق الحضرية، مساحة حضرية جذابة لكل فرد، آمنة وصديقة للأشخاص المعرضين للخطر في المناطق الحضرية بهواء ومياه أنظف، ومزيد من مناطق الأشجار الخضراء والحدائق ذات المباني عالية الجودة القريبة من المواطنين وتسهيل الاستخدام الموفر للطاقة.

رأي الباحث في ركائز المدن الذكية: يرى الباحث أن هناك خمس ركائز رئيسية للمدن الذكية، الركيزة الأولى **بنى تحتية مستدامة وذكية**، الركيزة الثانية **منظومة تكنولوجيا المعلومات والاتصالات** (التطبيقات ذكية -إنترنت الأشياء – الذكاء الاصطناعي – أجهزة الاستشعار الذكية وغيرها)، الركيزة الثالثة **الحوكمة الذكية**، الرابعة **مجتمع ذكي لتحقيق الاندماج المجتمعي في المنظومة الذكية** بخلق مواطن مؤهل ومبدع ومتعلم، قادر على الاستفادة من الخدمات الذكية القائمة على تكنولوجيا المعلومات والاتصالات، الركيزة الخامسة **الأمن السيبراني الذكي**، فلا يمكن الحديث عن وجود مدن ذكية دون تحقق منظومة متطورة ومرنة ومتصلة للأمن السيبراني، لحماية مفردات البنى التحتية ولحماية مجتمعها الذكي، لأن المدن الذكية غير الآمنة ليست ذكية على الإطلاق ولا يمكن التنبؤ باستدامتها الذكية، فهذه الركائز الخمس من وجهة نظر الباحث تجُبّ كل الركائز السابق ذكرها وتستغرق كل مفرداتها.

المطلب الثاني: خصائص المدن الذكية

يرى البعض (Nations, 2016, P 9-10,) أن نتائج تحليل التعاريف المختلفة للمدن الذكية تؤكد على جوانب مختلفة من المدن الذكية، ومن ثم يُستخلص منها خصائصها وهي التنقل الذكي والاقتصاد الذكي والحياة الذكية والحوكمة الذكية والأشخاص الأذكياء والبيئة الذكية.

كما اجتهد بعض الفقه في بيان خصائص المدن الذكية من خلال بيان الفوائد المرتبطة بتطوير المدن الذكية (Campisi, Severino,2021, P 2-4**): التي تتجسد في(1) أن** المدن الذكية تتمتع بفاعلية أكبر في صنع القرار(Silva, Khan.,2020, P, 975-987.) ، (2) وتتميز بالتوسع في الخدمات الرقمية،(3) وأنها مجتمعات أكثر أمانًا؛ لأنها يمكن أن تستفيد من التقدم التكنولوجي في الحد من النشاط الإجرامي، فقد ساعد استخدام أجهزة الاستشعار وكاميرات 24 ساعة على الحد من الأنشطة الإجرامية ومن ثم الشعور بالأمان بين المواطنين، فضلاً عما توفره المباني الذكية من أجهزة مراقبة كاملة للصحة والسلامة للمستخدمين أو السكان، فقد تضمنت أنظمة الإنذار الأوتوماتيكية المزودة بكاميرات وأقفال ذكية حماية فعالة لأمن وسلامة المنزل، (4) تقليل البصمة البيئية حيث تساعد المدن الذكية بدرجة كبير في الحد من الآثار الضارة على البيئة مع تزايد غازات الاحتباس الحراري، فتُعد المباني الموفرة للطاقة وأجهزة استشعار جودة الهواء ومصادر الطاقة المتجددة للمدن أدوات جديدة لتقليل بصمتها البيئية، (5) تحسين منظومة النقل حيث تتمتع أنظمة النقل الذكي بإمكانيات كبيرة لتحسين الكفاءة في جميع أنحاء المدينة، بدأً من إدارة أفضل لحركة المرور إلى قدرة ركاب النقل العام على تتبع مواقع الحافلات أو القطارات، فتعمل تقنيات مثل إشارات المرور الذكية على تحسين تدفق حركة المرور وتخفيف الازدحام خلال ساعات الذروة، كما يمكن أن تُساعد استخدام التطبيقات وأجهزة الاستشعار (خاصة خلال المراحل الحرجة مثل الأوبئة) في إدارة قطاع النقل والخدمات المقدمة للمستخدمين، (6) يمكن لتقنية المدن الذكية أن تخلق بيئة ذكية إذا تم نشر خدمات عالية السرعة ومنخفضة التكلفة مثل نقاط اتصال Wi-Fi العامة الموضوعة بشكل استراتيجي في المدينة، (7) فرص جديدة للتنمية الاقتصادية من خلال توفير منصة بيانات مفتوحة مع إمكانية الوصول إلى معلومات المدينة، ومن ثم يمكن للشركات اتخاذ قرارات مستنيرة من خلال تحليل البيانات من تقنيات المدن الذكية

المتكاملة، (8) كفاءة الخدمات العامة حيث تُمكن المستشعرات الذكية الآن للمدن من تحديد التسربات في الأنابيب بسرعة وإصلاح الأجزاء التالفة في وقت قصير، مما يقلل من كمية المياه المفقودة، كما تتيح شبكات الكهرباء الذكية أيضًا الاتصال ثنائي الاتجاه بين موردي الكهرباء والمستهلكين للمساعدة في تحديد أوقات ذروة الاستخدام وانقطاع التيار بشكل أفضل، (9) تحسين البنية التحتية حيث يمكن للتكنولوجيا الذكية أن تزود المدن بتحليل تنبؤي لتحديد المناطق التي تحتاج إلى إصلاح قبل حدوث أعطال للبنية التحتية (الطرق والجسور والمباني)، ومن ثم يحقق فرصة هائلة للمدن لتوفير المال وتجنب فشل البنية التحتية الذي يمكن منعه وإدارة الأموال بشكل أفضل، (10) زيادة مشاركة القوى العاملة فتعتبر القوة العاملة عالية الكفاءة معيارًا أساسيًا لتحقيق مدينة ذكية تتسم بالكفاءة، لذا تساعد تطبيقات التقنيات الذكية في تخفيف عبء المهام اليدوية التي يواجهها العديد من موظفي المدينة يوميًا.

المبحث الأول: جرائم الهجمات السيبرانية على البنى التحتية للمدن الذكية

تمهيد: لبيان جرائم الهجمات السيبرانية على البنى التحتية للمدن الذكية، لابد من بيان ماهية الهجوم السيبراني وأسباب تزايده على المدن الذكية، وتحديد الطبيعة القانونية لتلك الهجمات السيبرانية حتى يمكن تصنيف الجرائم الناجمة عنها وبيان مدى خطورتها، على النجو الاتي:

المطلب الأول: ماهية الهجوم السيبراني وأسباب تزايده على المدن الذكية

الجدير بالذكر أنه لا بد من الإشارة إلى حقيقة مهمة، وهي أن الهجوم السيبراني قد يُشكل النموذج القانوني لأركان جرائم تقنية المعلومات التقليدية، وقد يُشكل في أغلب الأحوال جرائم الإرهاب السيبراني أو الحروب السيبرانية، إلا أن الهجوم السيبراني يُعد القاسم المشترك الذي يجمع بين كل هذه الجرائم التي يمكن أن ترتكب على مرافق البني التحتية للمدن الذكية.

أولا ماهية الهجوم السيبراني: الهجوم السيبراني هو" أي محاولة للوصول غير المصرح به إلى جهاز كمبيوتر أو نظام حوسبة أو شبكة كمبيوتر بقصد إحداث ضرر، وتهدف تلك الهجمات السيبرانية إلى تعطيل أو تدمير أو التحكم في أنظمة الكمبيوتر أو تغيير أو حظر أو حذف أو التلاعب أو سرقة البيانات الموجودة داخل هذه الأنظمة (Pratt, 2021, .)، أو هو محاولة متعمدة لاستغلال الأنظمة أو الأجهزة أو الشبكات المعرضة للخطر للتلاعب أو السرقة أو الحصول على وصول غير مصرح به، قد يختلف الدافع وراء الهجمات الإلكترونية، لكن أهم الأسباب التي تبرز هي المكاسب المالية والمعلومات"Wallen,2020, ().

ثانياً وسائل الهجمات السيبرانية على المدن الذكية: تتعدد وتتنوع مظاهر الهجمات السيبرانية على المدن الذكية وذلك حسب نوع الهدف المطلوب تحقيقه وحسب حجم وطبيعة الهدف المطلوب إصابته ومدى قوة الأمن السيبراني المتوافرة، فدائما ما يستهدف المهاجمون السيبرانيون أو المتسللون نقاط ضعف أو نقاط دون حماية لشن هجماتهم، وسوف نتناول أشهر تلك الأساليب وأخطرها وذلك على النحو التالي (Wallen,2020,):

أ- **هجمات الهندسة الاجتماعية:Social Engineering Attacks** في مجال أمن المعلومات، تعتبر الهندسة الاجتماعية مصطلحًا شاملاً لمجموعة واسعة من الأنشطة الضارة، حيث يستخدمها المهاجمون لإقناع الأفراد أو خداعهم للقيام بإجراءات معينة أو للوصول إلى معلومات قيمة، يقومون بتنفيذ هذه الأنواع من الهجمات لاختطاف الحسابات، وانتحال الشخصيات، وإجراء مدفوعات احتيالية وغير ذلك، وتتعدد وسائل تلك الهجمات على النحو التالي:

-**التصيد الاحتيالي**: **Phishing** هو أحد أكثر هجمات الهندسة الاجتماعية استغلالًا، حيث يرسل المهاجمون رسائل بريد إلكتروني ضارة تحتوي على روابط قابلة للنقر.

-**التصيد بالرمح**:Spear Phishing مثل التصيد الاحتيالي، يعد التصيد بالرمح نوعًا من هجمات البريد الإلكتروني الموجهة والمخصصة.

-**التصيد الصوتي: (Vishing)**يُعرف أيضًا voice phishing، وهو يتضمن قيام المحتالين بإجراء مكالمات هاتفية أو ترك رسائل صوتية لخداع الأفراد لإفشاء معلومات حساسة.

-**الاصطياد: Baiting** كما يوحي الاسم يُطعم المهاجم الفرد ليقوم بعمل مرغوب فيه مقابل شيء ما.

-**هجوم "شيء مقابل شيء ما" :Quid Pro Quo** حيث يقدم المتسللون مساعدة أو خدمة مجانية مقابل الحصول على معلومات أو أموال مهمة.

-**إنشاء نص مسبق: Pretexting** ينتحل المهاجم صفة زميل في العمل لبناء الثقة مع المستخدم النهائي، يدعي المحتال أنه شخص ذو أهمية عالية، ويرسل بريدًا إلكترونيًا يطلب من المستخدم النهائي الكشف عن معلومات العمل المهمة.

-**التراجع**: **Tailgating** يلاحق الجاني سرًا شخصًا مخولًا بغرض دخول منطقة مؤمنة دون علم ذلك الشخص.

ب- **هجمات البرمجيات الخبيثة Malware Attacks:** هجمات البرامج الضارة هي أكثر أنواع الهجمات الإلكترونية شيوعًا حيث ينشئ المُهاجم

برامج ضارة بهدف إلحاق الضرر بالأجهزة أو البيانات أو الشبكة الحساسة للضحية دون علمه، ويتم تنفيذها على جميع أنواع الأجهزة وأنظمة التشغيل من أجل الوصول إلى المعلومات، وسرقة البيانات، وبيانات الاعتماد وما إلى ذلك، ويصعب اكتشاف هذه الأنواع من الهجمات على النحو التالي:

-**برامج الفدية (Ransomware)** يطور المجرم السيبراني برامج ضارة لمنع الوصول إلى ملفات أو بيانات الضحية ويطلبون فدية لتسليم الملفات المخترقة.

-**هجوم Drive-By** المعروف أيضًا باسم هجوم التنزيل من محرك الأقراص، يستخدم هذا الهجوم تطبيقات أو أنظمة تشغيل أو متصفحات ويب غير آمنة، يقوم المهاجمون بتضمين برنامج نصي ضار على صفحات موقع الويب الذي يقوم تلقائيًا بتشغيل المتصفح لتنزيل البرامج الضارة عندما يزور الضحية موقع الويب المصاب.

-**أحصنة طروادة: (Trojans)** تبدو هذه الأنواع من برامج الكمبيوتر شرعية وتخدع المستخدمين لتنزيل التطبيقات الضارة، يمكن أن تؤدي هذه الهجمات إلى تعطل جهاز الضحية أو الكشف عن البيانات الشخصية.

-**برامج الإعلانات المتسللة: (Adware)**، وهي نوع من البرامج الضارة التي تتواجد سراً على نظام الهدف وتعرض إعلانات غير مرغوب فيها أو غير ذات صلة، يمكن لبرامج الإعلانات الضارة إتلاف جهاز الضحية أو مراقبة النشاط عبر الإنترنت أو إصابة المتصفحات أو تثبيت الفيروسات.

-**برامج التجسس: (Spyware)** هي برامج ضارة تُستخدم لجمع المعلومات، ومراقبة النشاط دون علم المستخدم.

-**رفض الخدمة (DoS) ورفض الخدمة الموزع(DDoS):**

يتم تنفيذ هجوم DoS عن طريق التحميل الزائد على الجهاز أو الشبكة المستهدفة بحركة مرور ضخمة، مما يجعل الخدمة غير متاحة للمستخدم، من ناحية أخرى يحدث هجوم DDoS عندما تغمر عدة أجهزة شبكة مصابة من مصادر مختلفة النطاق الترددي للنظام المستهدف، مما يتسبب في زعزعة استقراره أو تعطله، وهذا النوع من الهجوم فعال لأنه من الصعب تحديد مصدر الهجوم، مثل هجمات SYN حيث يرسل المهاجم بشكل متكرر طلبات SYN لزيادة التحميل وإشباع موارد الخادم الهدف، مما يؤدي إلى بطء الاستجابة أو انعدامها، وكذلك هجمات Smurf Attacks يحاول فيه المتسلل إرباك خادم الضحية بحزم بروتوكول رسائل التحكم في الإنترنت(ICMP) ، مما يجعل الشبكة المستهدفة غير قابلة للتشغيل، أيضا هجمات Ping of Death حيث يرسل المهاجمون أصواتًا ضارة تحتوي على حزم بيانات تزيد عن الحد الأقصى (65536 بايت)، مما يتسبب في توقف النظام أو تعطله.

ج- **هجمات تطبيقات الويب: Web Application Attacks** وفيه المهاجمون يستغلون نقاط الضعف في التطبيق للوصول غير المشروع إلى قواعد البيانات التي تحتوي على المعلومات الحساسة، سواء كانت بيانات الشخصية أو مالية، ومن أكثر تلك الهجمات شيوعًا:

- **البرمجة النصية عبر المو اقع (XSS) Cross-Site Scripting**تتضمن مهاجمًا يقوم بتضمين JavaScript ضار لاستهداف قاعدة بيانات موقع الويب.

-**حقن SQL Injection (SQLi):** تحدث هجمات حقن لغة الاستعلام الهيكلية (SQL) عندما يحاول الجناة الوصول إلى قاعدة البيانات عن طريق تحميل نصوص SQL غير موثوق بها، يسمح هجوم SQLi الناجح للمهاجم بعرض أو تغيير أو حذف السجلات المخزنة في قاعدة بياناتSQL .

كما أن هناك هجمات أخرى على النحو التالي(Fruhlinger, 2020**)** -**رجل في المنتصف Man in the middle** هجوم رجل في الوسط (MITM)هي طريقة يتمكن من خلالها المهاجمون من التدخل بشكل سري بين المستخدم وخدمة الويب التي يحاولون الوصول إليها، فقد يقوم المهاجم بإعداد شبكة Wi-Fi مع شاشة تسجيل دخول مصممة لتقليد شبكة فندق؛ بمجرد أن يقوم المستخدم بتسجيل الدخول يمكن للمهاجم الحصول على أي معلومات يرسلها المستخدم، بما في ذلك كلمات المرور المصرفية، و**هجوم: Crypto jacking**، و**ثغرات يوم الصفر Zero-day exploits**: وغيرها.

ثالثاً نماذج لجر ائم الهجمات السيبر انية على البنى التحتية للحكومات والمدن الذكية خلال 2022:

سوف نتناول بعض من تلك الجرائم بالقدر الي يتناسب مع أساسيا البحث وجوهره التي تُبرز ضرورة وضع استراتيجية للحد من تلك الجرائم ومكافحتها، وذلك على النحو التالي (,2022,(CSIS)):

- **سبتمبر 2022:** هجوم سيبراني على شبكات حكومة الجبل الأسود، مما جعل المواقع الحكومية الرئيسية في الجبل الأسود ومنصات المعلومات الحكومية غير قابلة للوصول، كما اتهمت الصين وكالة الأمن القومي الأمريكية (NSA) بالعديد من الهجمات الإلكترونية ضد جامعة نورث وسترن بوليتكنيكال الصينية.، حيث زعمت السلطات أن وكالة الأمن القومي قامت بسرقة بيانات المستخدم، واختراق شبكات الاتصالات الرقمية، كما تم استهداف مجموعة قرصنة روسية لموقع الويب الخاص بوكالة المخابرات البريطانية MI5 بهجوم DDoS أدى إلى تعطيل الموقع مؤقتًا.
- **أغسطس 2022:** هجوم على وكالة الطاقة الإيطالية، Gesture dei Servizi Energetici (GSE)، مما أدى إلى اختراق الخوادم، ومنع

الوصول إلى الأنظمة، ووقف الوصول إلى موقع GSE على الويب لمدة أسبوع، كما استهدف قراصنة البرلمان الفنلندي بهجوم DDoS جعل الموقع البرلماني غير ممكن الوصول إليه. أعلنت مجموعة روسية مسؤوليتها عن الهجوم على تلغرام، كما تم استهداف قراصنة الموقع الإلكتروني لوكالة الطاقة الحكومية الأوكرانية المسؤولة عن الإشراف على محطات الطاقة النووية في أوكرانيا. وذكرت الوكالة أن قراصنة روس هم من نفذوا الهجوم، كما تم استهداف أكبر موزع للغاز الطبيعي في اليونان DESFA بهجوم سيبراني تسبب في انقطاع النظام، وعرض البيانات.

- **يوليو 2022:** استهداف قراصنة مزود الطاقة الليتواني المملوك للدولة في هجوم DDoS، وقد أعلنت شركة كيلنيت، التي يربطها مسؤولون ليتوانيون بعلاقتها بروسيا، مسؤوليتها عن الهجوم، أيضا هجوم على حسابات وسائل التواصل الاجتماعي المملوكة للجيش الملكي البريطاني، أسفر عن الاستيلاء على حسابات الجيش البريطاني على تويتر ويوتيوب.
- **يونيو 2022** هجوم استهدف السكك الحديدية والمطارات وشركات الإعلام والوزارات الحكومية في ليتوانيا بهجمات DDoS. وقد أعلنت مجموعة قرصنة مدعومة من روسيا مسؤوليتها عن الهجوم، كما استهدفت حملة تصيد احتيالي المؤسسات الأمريكية في قطاعات الجيش والبرمجيات وسلسلة التوريد والرعاية الصحية والأدوية لخرق حسابات Microsoft Office 365 وOutlook.
- **مايو 2022:** استهدف هجوم DDoS هيئة ميناء لندن، مما أجبر موقعها على الإنترنت على التوقف عن العمل.
- **أبريل 2022:** استهدف قراصنة حسابات Telegram لمسؤولين حكوميين أوكرانيين بهجوم تصيد في محاولة للوصول إلى الحسابات.
- **مارس 2022:** استخدم قراصنة هجوم DDoS لإغلاق الهيئة الوطنية للاتصالات في جزر مارشال، وتسبب الهجوم في تعطيل خدمات الإنترنت في الجزر لأكثر من أسبوع، كما أدى هجوم على خدمة النطاق العريض عبر الأقمار الصناعية التي تديرها شركة Viasat الأمريكية إلى تعطيل خدمات الإنترنت في جميع أنحاء أوروبا، بما في ذلك الاتصالات العسكرية الأوكرانية في بداية الغزو الروسي، حيث اخترق المهاجمون أجهزة مودم الأقمار الصناعية التابعة لآلاف الأوروبيين لتعطيل خدمة الشركة.
- **فبراير 2022:** هجوم سيبراني أدى إلى تعطل المواقع الإلكترونية لمجلس الوزراء الأوكراني، ووزارات الخارجية، والبنية التحتية والتعليم في الأيام التي سبقت غزو القوات الروسية لأوكرانيا، كما تم استخدام البرمجيات الخبيثة لاختراق شبكات مؤسسة مالية أوكرانية، كما تسبب هجوم DDoS في تعطيل مواقع الويب التابعة لوزارة الدفاع الأوكرانية، واثنين من أكبر البنوك في البلاد.
- **يناير 2022:** اخترقت مجموعة قرصنة صينية العديد من شركات الأدوية والتكنولوجيا الألمانية، وكما صرحت الحكومة الألمانية كان اختراق شبكات مزودي الخدمات والشركات بهدف سرقة الملكية الفكرية، كما استهدفت سلسلة من هجمات DDoS دورة Minecraft عالية المخاطر، وانتهى بها الأمر بالتأثير على Andorra Telecom، المزود الوحيد لخدمة الإنترنت في البلاد. تسبب الهجوم في تعطيل خدمات الجيل الرابع والإنترنت للعملاء.

رابعاً عوامل تزايد جرائم الهجمات السيبرانية على البنى التحتية للمدن الذكية:

لعل العامل الجوهري وراء تزايد تلك الهجمات السيبرانية هو تزايد وتيرة إدراج أغلب دول العالم مرافق ومؤسسات البنى التحية لحكوماتها ومدنها الذكية عبر الفضاء السيبراني، وبما تتضمنه تلك المرافق والمؤسسات من بيانات ومعلومات وأنشطة وأسرار، أو كانت تتعلق بقطاع الأفراد والشركات، سواء من خلال ما تقدمه تلك المرافق والمؤسسات من خدمات ومعاملات لهؤلاء، أو كانت ناتجة عن أنشطة ومعاملات الأفراد فيما بينهم.

- صعوبة تحديد مصدر الهجوم السيبراني وتعقبه سواء اتخذ شكل إرهاب سيبراني أو حرب سيبرانية، ومن ثم صعوبة معرفة هوية مرتكب الهجوم لضبطه وتعقُّبه وملاحقته، أو تقرير مسؤوليته خاصة إذا كان مرتكب الهجوم دولة كما في الحروب السيبرانية.
- إن الهجوم السيبراني عابراً للحدود، ومن ثم آلية للتدمير عن بُعد، ويُجنب المعتدي سواء كان دولة أو منظمة إرهابية أي خسائر في الأموال أو المعدات العسكرية أو الأرواح كما يحدث في الحروب التقليدية، أو الإرهاب التقليدي، فبمجرد اكتشاف الثغرة الأمنية على الطرف الأخر من الكرة الأرضية، يبدأ وينتهي في ثوان معدودة محققاً هدفه المطلوب، وقد يُصيب أهدافا متعددة أو هدف واحد عدة مرات وفي ثوان معدودة، ومن ثم يوفر للمعتدي الوقت والمال والجهد.
- إن الأثار المدمرة للهجمات السيبرانية على دولة معينة تفوق قدراتها بمراحل الآثار المدمرة للهجوم العسكري في الحروب التقليدية، كما تفوق قدراتها الآثار المدمرة للإرهاب التقليدي.
- صعوبة اكتشاف ارتكاب الهجوم السيبراني، أو تحديد حجم الأضرار التي ترتبت عليه، خاصة إذا كان هدف ذلك الهجوم هو الحصول على معلومات أو أسرار حساسة من القطاعات الحيوية أو الاستراتيجية أو العسكرية، فقد يتم الهجوم وينتهي دون حتى اكتشافه أو اكتشاف حجم ونوعية المعلومات التي تم الاستيلاء عليها، وقد ينتهي الأمر بمجرد تحليلات وتخمينات حول الجهة المعتدية، دون وجود أي دليل مادي أو حتى تقني على تحديد هوية المعتدي.
- إن أساليب الهجوم السيبراني وتقنياته يمكن استخدامه في إصابة أهداف متعددة في وقت واحد وفي ثوان معدودة، كما يمكن أن يُصيب

الهجوم السيبراني هدف واحد مرات متكررة وفي ثوان معدودة أيضا حتى يُحقق الهدف المطلوب من الاعتداء، ومن ثم يستطيع مرتكب الهجوم تحقيق أهدافه بسهولة ودون وجود ردود أفعال قوية تجاهه أو مشاكل عند التنفيذ، وذلك كله عكس هجمات الإرهاب أو الحروب التقليدية.

- وقد يكون هدف ووسيلة الهجوم السيبراني في الحروب السيبرانية من قبل الدولة المعتدية هو ذات هدف ووسيلة المنظمات الإرهابية في الإرهاب السيبراني، وهو التهديد والترويع وإشاعة الذعر لدى الدولة المعتدى عليها وأجهزتها ومؤسساتها وأفرادها لإرغامها للقيام بعمل ما أو الامتناع عن عمل معين، وذلك بإصابة مرفق حيوي أو استراتيجي تُحقق من خلاله تلك الأهداف، كما قد يكون هدف الحروب السيبرانية هو زعزعة الأمن والاستقرار داخل الدولة المعتدي عليها أو إشاعة الفوضى لقلب أو تغيير نظام الحكم فيها لصالح طرف معارض فيها تسانده الدولة المعتدية.
- أن تكنولوجيا الهجوم السيبراني وتقنياته أصبحت متاحة على نطاق واسع ورخيصة نسبيًا.

خامساً عوامل زيادة الهجمات السيبرانية خلال 2020-2021:

- **ضعف ثقافة الأمن السيبراني:** لدى المستخدمين وما قد ينجم عنها من ثغرات يستغلها المجرم السيبراني.
- **ضعف البنى التحتية للأمن السيبراني** لدى كثير من الدول، الأمر الذي ترتب عليه وجود نقاط ضعف وأصول رقمية دون حماية متطورة تواجهه التقنيات التي يستخدمها المهاجمون في الاختراق والتسلل، الأمر الذي دفع الكثير من الدول إلى تعزيز البني التحتية للأمن السيبراني لديها وإدراجه كأحد أولويات الأمن القومي، ومن ثم قد تضاعف حجم الإنفاق العالمي على البنى التحتية للأمن السيبراني.
- **جائحة كورونا المسمى بـ كوفيد 19**: فقد ساعد النطاق غير المسبوق للعمل عن بُعد في جميع أنحاء العالم الناجم عن جائحة COVID-19 المجرم السيبراني على تكثيف شن هجماته، مستغلاً الخوف وعدم اليقين المرتبطين بتلك الجائحة، فضلاً عن نقاط الضعف الجديدة الناتجة عن التحول إلى الوضع الافتراضي، فقد حطم عام 2020 جميع الأرقام القياسية فيما يتعلق بالبيانات المفقودة في الانتهاكات والأعداد الهائلة للهجمات الإلكترونية على الشركات والحكومات والأفراد.

فقد تعرضت مؤسسات الرعاية الصحية لمزيد من الهجمات السيبرانية في ظل COVID-19،(Hardiman,2020) فقد أفاد مركز شكاوى جرائم الإنترنت (IC3) التابع لمكتب التحقيقات الفيدرالي الأمريكي (FBI) أنه تلقى 1200 شكوى تتعلق بالتهديدات الإلكترونية لفيروس كورونا حتى شهر مارس 2020، وهو ما يتجاوز بكثير عدد الشكاوى التي تلقاها بشأن جميع أنواع الاحتيال عبر الإنترنت في عام 2019، كما كان لتلك الهجمات امتداد عالمي، ففي مارس 2020 حذر المركز الكندي للأمن السيبراني من قراصنة ضارين يستهدفون قطاع الرعاية الصحية لديهم خاصة المتعلقة بالملكية الفكرية والبحث والتطوير المتعلقين بـ COVID-19، في الوقت نفسه واجهت جمهورية التشيك سلسلة من حوادث الأمن السيبراني بما في ذلك هجوم على أحد أكبر مرافق اختبار COVID-19، مما أدى إلى إنهاء العمليات ونقل المرضى إلى مستشفيات أخرى، كما دفع الخطر على الصحة العامة والسلامة الناتج عن مثل تلك الهجمات السيبرانية وزارة الخارجية الأمريكية إلى إدانة هذه الحرب السيبرانية في دعوة لاتخاذ إجراءات عالمية.

ولقد بلغت الهجمات السيبرانية ذروتها في هجوم سلسلة التوريد Solar winds التي تعرضت له الولايات المتحدة الأمريكية في 13 ديسمبر 2020، والذي يُعد أسوأ هجوم سيبراني حكومي على الإطلاق، فقد تم استهداف الوكالات الفيدرالية الرئيسية، من وزارة الأمن الداخلي إلى الوكالة التي تشرف على ترسانة الأسلحة النووية الأمريكية، وشركات التكنولوجيا، والأمن القومي بما في ذلك Microsoft (Constantin, 2020,)، فكان بمثابة تذكير لصانعي القرار في جميع أنحاء العالم بالأهمية المتزايدة للأمن السيبراني، وكما جاء في التقرير الخاص بالمخاطر العالمية 2021 والصادر عن منتدى الاقتصادي العالمي، أن المخاطر السيبرانية تستمر في الترتيب بين المخاطر العالمية، فقدت أدت جائحة COVID-19 إلى زيادة تلك المخاطر، والكشف عن نقاط الضعف وعدم الاستعداد السيبراني، وتفاقم التفاوتات التكنولوجية داخل المجتمعات وفيما بينها(Pipikaite,2021,) .

المطلب الثاني: الطبيعة القانونية للهجمات السيبرانية على البنى التحتية للمدن الذكية

أولاً الطبيعة القانونية للهجمات السيبرانية:

تجسدت الطبيعة القانونية للهجمات السيبرانية **في ثلاث أنماط من الجرائم تُعد تلك الهجمات القاسم المشترك الذي يجمع بينهما، الجرائم الخاصة بتقنية نظم المعلومات، جرائم الإرهاب السيبراني، الحروب السيبرانية التي ترتكبها بعض الدول، وذلك على النحو التالي:**

أ- **الإرهاب السيبراني:** الإرهاب السيبراني وفقاً دراسة أعدتها كلية الدراسات العليا البحرية التابعة لوكالة استخبارات الدفاع الأمريكية في أكتوبر 1999 هو "التدمير غير القانوني أو تعطيل الممتلكات الرقمية بغرض تخويف / إجبار المجتمعات أو الحكومات لتحقيق أي هدف قد تكون سياسي أو ديني أو أيديولوجي"، ومن ثم عندما يستخدم الإرهابيين التكنولوجيا الخاصة بالمعلومات والاتصالات في أنشطتهم الداعمة لا يعتبر إرهابًا إلكترونيًا وفقاً لهذا التعريف(Nelson, 1999, P 7-9,) ، وتُعرِّف الوكالة الفيدرالية لإدارة الطوارئ (FEMA) الإرهاب السيبراني بالهجمات غير المشروعة أو التهديد بارتكابها على الشبكات والمعلومات أو أجهزة الكمبيوتر، بهدف التخويف أو الإكراه لحكومة معينة أو شعبها من أجل تحقيق أهداف قد تكون سياسية أو اجتماعية (Wilson,2008,p4,)،كما حدد تقرير الدفاع السيبراني والأمن السيبراني الوطني لليابان الصادر في سبتمبر

2020 الإرهاب السيبراني (CYBERDEFENSE, 2020, P5,)بأنه "أي هجمات تستخدم شبكات المعلومات والاتصالات والأنظمة الخاصة بالمعلومات وتؤثر على حياة الناس وأنشطتهم سواء كانت اجتماعية أو اقتصادية".

والجدير بالذكر أنه إذا كان الإرهاب التقليدي والإرهاب السيبر اني كلاهما لهما الطابع التخريبي والتدميري، أيضا الترهيب والتهديد، وكلاهما قد تكون لهما نفس الأهداف، إلا أنهما يختلفان في وسيلة ارتكابهما، فوسيلة الإرهاب التقليدي هي الأسلحة التقليدية بينما وسيلة الإرهاب السيبر اني فهي تقنية المعلومات أو الشبكة المعلوماتية والانترنت وأجهزة الكمبيوتر (محمود، 2020، ص 453).

فالهجوم الإرهابي على مفردات البنى التحتية يترتب عليه أضرار بالغة للأمن القومي، فالأنظمة المصرفية والمالية يتم تحويلها رقميًا ومتصلة بالإنترنت بشكل متزايد، كما أنه من خلال اختراق البنية التحتية للطاقة أو المرافق، يمكن أن يتسبب الإرهابيون في حدوث الفوضى، فضلاً عن أضرار أخرى تمس الأمن القومي للدول، جراء إمكانية نشر أو إفشاء تلك المعلومات، وقد تمنع تلك الهجمات الوصول إلى شبكات الكمبيوتر التابعة لوزارة الدفاع بما في ذلك البريد الإلكتروني والأنظمة الحساسة الأخرى، وقد تمتد إلى صناعات الطاقة وتوليد الكهرباء وتوزيعها، بما في ذلك مصافي النفط وأنابيب النفط والغاز، أو بنى تحتية حيوية مثل خدمات الطوارئ، والمستشفيات، وتوليد الطاقة وتوزيعها، أو النقل، إلا أن منفذ تلك الهجمات غالبا ما تكون دول قوية، وأن دولا كالولايات المتحدة وروسيا والصين هي مراكز قوة بشأن الاستخدام الدفاعي والهجومي لتقنية المعلومات وتقنية الاتصالات ((ICT، على الرغم من أن هناك بعض الدول أكثر من قادرة على ذلك باستخدام الأسلحة السيبرانية(Das.,2020,) .

ب-ماهية الحروب السيبر انية: الحروب السيبرانية تتضمن الإجراءات التي تتخذها دولة أو جهة لمهاجمة ومحاولة إتلاف أجهزة الكمبيوتر أو شبكات تقنية المعلومات لدولة أخرى، من خلال على سبيل المثال فيروسات الكمبيوتر أو هجمات رفض الخدمة(rand,2022,) ، فالحروب المستقبلية ستشهد استخدام كود الكمبيوتر لمهاجمة البنية التحتية للعدو، والقتال إلى جانب القوات باستخدام أسلحة تقليدية مثل البنادق والصواريخ (Ranger,2018,)، فهي استخدام التكنولوجيا لمهاجمة أجهزة الكمبيوتر وشبكات المعلومات لدولة أخرى، وفي بعض الحالات، يمكن أن تسبب ضررًا مشابهًا للحرب الفعلية (McCallion,2021,)

ج- ماهية الحروب الإلكترونية: يتضح لنا أن الحرب السيبرانية تختلف عن **الحرب الإلكترونية** التي كما حددتها وزارة الدفاع الأمريكية بأنها الأنشطة العسكرية التي تستخدم فيها لطاقة كهرومغناطيسية للتحكم في الطيف الكهرومغناطيسي(نطاق الترددات الكهرومغناطيسية) أو مهاجمة العدو(congress,2020.p1,) ، فتدعم الحرب الإلكترونية القيادة والسيطرة من خلال السماح للقادة العسكريين بالوصول إلى نطاق الترددات الكهرومغناطيسية للتواصل مع القوات، مع منع أي خصوم محتمل من الوصول إلى تلك الترددات لتطوير العمليات والتواصل مع القوات.

د- تعريف الباحث للإرهاب السيبر اني والحروب السيبر انية:

الإرهاب السيبر اني: هو هجوم سيبراني الغرض منه تهديد الحكومات أو العدوان عليها، أو الإخلال بالنظام العام أو تعريض سلامة أو مصالح أو أمن المجتمع وأفراده للخطر، لتحقيق أهداف سياسية -عقائدية - أيدولوجية.

الحروب السيبر انية: هي هجوم سيبراني تقوم به دولة أو أحد من يعملون لمصلحتها على مرافق ومؤسسات البني التحتية المدرجة عبر الفضاء السيبراني لدولة أخرى، يترتب عليه وقوع أضرار بالأمن القومي بمفهومه الشامل للدولة المعتدى عليها.

ثانياً التحديات القانونية لجر ائم الهجمات السيبر انية على البنى التحتية للمدن الذكية:

تتجسد جوهر التحديات القانونية لجر ائم الهجمات السيبر انية على البنى التحتية للمدن الذكية فيما يلي:

- **صعوبة إثباتها:** ومن ثم ملاحقة مرتكبيها، فتُرتكب تلك الجرائم ويستطع الجاني محو أدلتها في ثوان معدودة.
- **أن مسرح ارتكاب جر ائم تلك الهجمات قد يتعدى حدود الدول:** فقد تُرتكب عبر الفضاء السيبراني الممتد الذي قد يتعدى حدود الدول، فبمجرد اكتشاف الثغرة الأمنية على الطرف الأخر من الكرة الأرضية يبدأ، وينتهي في ثوان معدودة محققاً هدفه المطلوب، وقد يُصيب أهدافا متعددة أو هدف واحد عدة مرات وفي ثوان معدودة، **الأمر الذي يُثير إشكالات قانونية في معرفة القانون الواجب التطبيق**، فضلاً عن صعوبة ضبط أدلة ذلك المسرح.
- **صعوبة تحديد مصدر الهجوم السيبر اني:** وتعقبه سواء اتخذ شكل إرهاب سيبراني أو حرب سيبرانية، ومن ثم صعوبة معرفة هوية مرتكب الهجوم لضبطه وتعقُبه وملاحقته أو تقرير مسؤوليته، خاصة إذا كان مرتكب الهجوم دولة كما في الحروب السيبرانية، فقد يتم الهجوم وينتهي دون حتى اكتشافه أو اكتشاف حجم ونوعية المعلومات التي تم الاستيلاء عليها، وقد ينتهي الأمر بمجرد تحليلات وتخمينات حول الجهة المعتدية، دون وجود أي دليل مادي أو حتى تقني على تحديد هوية المعتدي.
- **صعوبة تحديد الطبيعة القانونية للهجمات السيبر انية وما إذا كانت إرهاب سيبر اني أو حرب سيبر انية:**

فقد يكون هدف ووسيلة الهجوم السيبراني في الحروب السيبرانية من قبل الدولة المعتدية هو ذات هدف ووسيلة المنظمات الإرهابية في الإرهاب السيبراني، وهو التهديد والترويع وإشاعة الذعر لدى الدولة المعتدى عليها وأجهزتها ومؤسساتها وأفرادها لإرغامها للقيام بعمل ما أو الامتناع عن عمل

معين، وذلك بإصابة مرفق حيوي أو استراتيجي تُحقق من خلاله تلك الأهداف، كما قد يكون هدف الحروب السيبرانية هو زعزعة الأمن والاستقرار داخل الدولة المعتدي عليها أو إشاعة الفوضى لقلب أو تغيير نظام الحكم فيها لصالح طرف معارض فيها تسانده الدولة المعتدية.

- **أشهر الهجمات السيبرانية 2020 تؤكد صعوبة تحديد الطبيعة القانونية للهجمات السيبرانية:**

فقد تعرضت الولايات المتحدة الأمريكية لأسوأ هجوم سيبراني حكومي على الإطلاق، وهو ما يسمى بهجوم Solar Winds (Fruhlinger,2020,)، فقد تم استهداف الوكالات الفيدرالية الرئيسية، من وزارة الأمن الداخلي إلى الوكالة التي تشرف على ترسانة الأسلحة النووية الأمريكية وشركات التكنولوجيا والأمن القومي بما في ذلك Microsoft، وبدأ الاختراق عندما تم التسلل إلى تحديثات برمجية ضارة لبرنامج مشهور يسمى Orion، من إنتاج شركة Solar Winds، فقد تم الكشف عن أن شركة (Austin) أوستن وهي شركة برمجيات إدارة تكنولوجيا المعلومات، التي توفر مراقبة الشبكة والخدمات الفنية الأخرى لمئات الآلاف من المنظمات حول العالم ومقرها سولارويندز (Solar Winds)، قد تعرضت لهجوم من سلسلة التوريد أدى إلى اختراق التحديثات لمنصة برمجيات أوريون ((Orion software platform التابعة لها، أدخل المهاجمون البرامج الضارة الخاصة بهم المعروفة الآن باسم Sunburst أو Solorigate في التحديثات، والتي تم توزيعها على العديد من عملاء Solar Winds الضحية الأولى المؤكدة كانت شركة الأمن السيبراني FireEye، أظهرت التحقيقات أن المتسللين الذين يُعتقد أنهم تحت رعاية حكومة احدى الدول، ولم يتم التوصل إلى دليل قاطع على إدانة تلك الدولة (Ranger,2021,).

ولقد كان هناك جدل قانوني في الأوساط الأمريكية حول تحديد طبيعة الهجوم هل هو إرهاب سيبراني- تجسس -أم حرب (Wolfe,2020,)؟، فقد وصفه السناتور الأمريكي Dick Durbin ديك دوربين بأنه "إعلان حرب فعليًا"، لكن وصفه خبراء الأمن السيبراني والقانونيين إنه اختراق فلن يعتبر عملاً حربياً بموجب القانون الدولي لتطلب ذلك مستوى معينًا من القوة أو التدمير، لذا يدخل التاريخ باعتباره عملاً من أعمال التجسس، ويرى Duncan Hollis دنكان هوليس، أستاذ القانون في جامعة تمبل والمتخصص في الأمن السيبراني أن "الحرب تعني العنف والموت والدمار"، ويرى Hollis هوليس وخبراء آخرون إن الهجوم نفذ على ما يبدو لسرقة معلومات أمريكية حساسة، ويجب أن يُنظر إليه على أنه تجسس، كما يرى

Benjamin Friedman بنجامين فريدمان، مدير السياسات في مركز أبحاث "أولويات الدفاع": إن مجرد سرقة المعلومات، بقدر ما لا نحبها، ليس عملاً من أعمال الحرب بل يُعد تجسس.

ثالثاً الإطار التشريعي لمواجهة جرائم الهجمات السيبرانية على البنى التحتية للمدن الذكية:

أ- الإطار التشريعي:

أصدرت دولة الإمارات العديد من التشريعات الجزائية الخاصة المساندة التي تؤصل وتُدعم حماية المدن الذكية من جرائم الهجمات السيبرانية التي تُرتكب ضد مرافق ومؤسسات البني التحتية لتلك المدن، أو تُرتكب عبر الفضاء السيبراني وهو ما يعرف بالجرائم الإلكترونية، فأصدرت قانون مكافحة الشائعات والجرائم الإلكترونية رقم34 لسنة 2021، الذي ألغى القانون السابق المرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات وتعديلاته، ومن ثم عرّف الهجمات الإلكترونية بموجب المادة الأولى منه بأنها "لهجمات الإلكترونية: كل استهداف متعمد ومخطط للأنظمة المعلوماتية أو البنية التحتية أو الشبكات الإلكترونية أو وسائل تقنية المعلومات يقلل من قدرات ووظائف أي منها، سواء كان ذلك لغرض شخصي أو لأغراض الاعتراض أو التسلل أو الاختراق أو التسريب أو بغرض تعريض البيانات أو المعلومات للخطر أو تعطيل العمليات وما في حكمه"، كما عرفت تلك المادة الدليلُ الرقميُ: بأنه" دليل مستمد من المعلومات الإلكترونية المخزنة أو المنقولة أو المستخرجة أو المأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها، والتي لها قوة أو قيمة ثبوتية، ويمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة، كما أعطى المشرع وبموجب المادة 65 من ذلك القانون حجية الأدلة الجنائية المادية في الإثبات الجنائي لكل الأدلة المستخرجة أو المستمدة من الأجهزة أو الوسائط أو المعدات أو الدعامات الإلكترونية أو برامج الحاسب أو النظام المعلوماتي أو من أي وسيلة تقنية المعلومات ".

كما أصدر المشرع الإماراتي قانون استخدام تقنية الاتصال عن بُعد في الإجراءات الجزائية رقم (5) لسنة 2017، وعرف بموجب المادة الأولى منه الإجراءات عن بُعد: بأنها" تلك الإجراءات الجزائية التي تتم عبر استخدام تقنية الاتصال عن بعد، لاستقصاء الجرائم وجمع أدلتها، أو التحقيق أو المحاكمة، كما كفل المشرع حجية لتفريغ تلك الإجراءات بموجب المادة العاشرة بأن " لتلك الجهات المختصة السلطة في تفريغ الإجراءات الجزائية المتخذة عن بعد في المحاضر أو المستندات الورقية أو الإلكترونية المعتمدة منها، ودون الحاجة لتوقيع من أصحابها.

كما أعطت المادة 13 من قانون الجرائم الإلكترونية الأردني لسنة 2015 السلطة لمأموري الضبط القضائي في دخول أنظمة شبكات الاتصالات ونظم المعلومات والتفتيش وجع أدلة الجرائم الإلكترونية بعد الحصول على إذن من السلطات المختصة بأن قررت" مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكى عليه الشخصية، يجوز لموظفي الضابطة العدلية، بعد الحصول على ادن من المدعي العام المختص أو من المحكمة المختصة، الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما

يجوز لهم تفتيش الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم، وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضرا بذلك ويقدمه إلى المدعي العام المختص.

وجرمت المادة الثالثة من ذلك القانون الدخول للشبكة المعلوماتية دون تصريح أو بما يخالف أو يجاوز التصريح، وكذلك كل من دخل قصداً إلى موقع إلكتروني لتغييره، أو إلغائه، أو إتلافه، أو تعديل محتوياته، أو أشغاله، أو انتحال صفته، أو انتحال شخصنة مالكه.

كما أعطى المشرع الأردني بموجب قانون البيانات رقم 30 سنة 1952 والمعدل في 2022حجية الأدلة الجنائية المادية في الإثبات الجنائي لكل الأدلة المستخرجة أو المستمدة من الأجهزة أو الوسائط أو المعدات أو الدعامات الإلكترونية أو برامج الحاسب أو النظام المعلوماتي أو من أي وسيلة تقنية المعلومات، بنفس مضمون ما أورده المشرع الإماراتي.

ب- أحكام القضاء:

وقد تواترت أحكام القضاء على الحكم بحرية القاضي الجنائي في تقييم الدليل الجنائي والاقتناع به، أيا كان نوع ذلك الدليل طالما توافرت مشروعية الحصول عليه واستوفى شروط قبوله وكان له أصل ثابت في أوراق القضية وتم طرحه على الخصوم، فكما قررت محكمة النقض المصري " أن الأصل في المحاكمات الجزائية هو اقتناع القاضي بناء على الأدلة المطروحة عليه فله أن يكون عقيدته من أي دليل أو قرينة يرتاح إليها إلا إذا قيده القانون بدليل معين"(نقض مصري، 1985، ص 436).

كما قضت محكمة التمييز الأردنية بالحكم الصادر بتاريخ 10 / 7 / 2014 بأنه" يُستفاد من (المادة 147) من قانون أصول المحاكمات الجزائية أنها أمدت محكمة الموضوع في المسائل الجزائية بالحرية الكاملة في الاقتناع بالأدلة المقدمة إليها دون رقابة عليها من محكمة التمييز في هذه المسألة الموضوعية ما دام أن النتيجة التي توصلت إليها لها ما يؤيدها في بيانات الدعوى وتتفق مع العقل والمنطق"(تمييز أردني، 2014).

وفي حكم حديث في عام 2021 قضت محكمة التمييز الأردنية بصفتها الجزائية بأنه" لمحكمة الاستئناف بوصفها محكمة موضوع بمقتضى المادة (147/2) من قانون أصول المحاكمات الجزائية سلطة واسعة في وزن البيانات وتقديرها والأخذ بما تقنع به من بيانات الإثبات والنفي متى توافرت لديها القناعة بها، أو طرحه إذا ساورها الشك بصحته دون معقب عليها في هذه المسألة الموضوعية، شريطة سلامة النتائج التي توصلت إليها سائغة ومقبولة ومبنية على أدلة مقدمة في الدعوى ولها أصل ثابت فيها، وأنها وبموجب تلك الصلاحية قنعت من البيانات المقدمة في الواقعة (الجريمة) التي توصلت إليها، وأنها لتكوين قناعتها ناقشت أدلة الدعوى مناقشة وافية وسليمة واستخلصت منها النتائج استخلاصاً سائغاً ومقبولاً تؤدي إليه هذه الأدلة، وبالتالي لا رقابة لمحكمتنا عليها في هذه المسألة الموضوعية، طالما أن البيانات التي أشارت إليها في متن قرارها تؤدي إلى النتيجة التي توصلت إليها"(تمييز أردني، 2021).

المبحث الثاني: استراتيجية مواجهة الهجمات السيبرانية على البنى التحتية للمدن الذكية

تمهيد وتقسيم: تجسدت استراتيجيات الدول لمواجهة الهجمات السيبرانية على البنى التحتية للمدن الذكية في وضع واستحدث وتطوير منظومات للأمن السيبراني تكون قادرة إن لم يكن على مكافحتها فعلى الأقل الحد من أثارها، تلك المنظومات القائمة على تقنيات مواجهة لتقنيات تلك الهجمات، الأمر الذي دفع الباحث إلى وضع استراتيجية مكافحة لتلك الهجمات على النحو التالي:

المطلب الأول: الأمن السيبراني لمواجهة الهجمات السيبرانية على البنى التحتية للمدن الذكية

أولاً تطور مفهوم الأمن القومي للدول: أصبحت مرافق ومؤسسات البنى التحتية لحكومات ومدن العالم الذكية قائمة على شبكات تقنيةُ المعلومات والاتصالات، وما تتضمنه تلك المرافق والمؤسسات من أسرار تشكل مفردات للأمن القومي وتُمثل في ذات الوقت جوانبه الرئيسية، مثل جانب الأمن الاقتصادي، والصناعي، والسياسي، والبيئي، والمائي، والغذائي، والصحي، والاجتماعي، والفكري، والشخصي أو الجسدي.

ثانياً ارتباط الأمن القومي بالأمن السيبراني: وقد ترتب على إدراج معلومات وبيانات وأنشطة وأسرار مؤسسات ومرافق البني التحتية لمختلف دول العالم عبر الفضاء السيبراني أن ارتبطت حماية منظومة الأمن القومي للدول بمدى تأمين وحماية وتحقيق الأمن السيبراني لمرافق ومؤسسات البني التحتية لمختلف دول العالم التي تُشكل مفردات الأمن القومي لها، لذا أصبح الأمن السيبراني متصدراً على لائحة أولويات سياسات واستراتيجيات تلك الدول، باعتبار حمايته جزء من حماية الأمن القومي.

فدولة مثل أمريكا قد وضعت قضايا الأمن القومي على رأس أولوياتها، ويختص مكتب التحقيقات الفيدرالي (FBI)بصفته الوكالة الفيدرالية الرائدة في التحقيق في الجرائم السيبرانية لأنها تهدد السلامة العامة والأمن الاقتصادي، كما تُعد خصوصية البيانات (Data Privacy) مصدر قلق كبير للأمن القومي لكل من الشركات والحكومة الفيدرالية، فيمكن أن يؤدي خرقه إلى إحداث فوضى في المخابرات والجيش والبيانات الأمريكية (Oberheiden,2021,).

ثالثاً ماهية الأمن السيبراني:

عرّفه الاتحاد الدولي للاتصالات (International Telecommunication Union) (ITU) بأنه" هو مجموع من السياسات والأدوات والمفاهيم الأمنية المستخدمة لحماية بنى البيئة السيبرانية من أصول ومستخدمين" (ITU-T,2022,)، كما ورد تعريفاً للأمن السيبراني بموجب المادة 1 من القانون الإماراتي الاتحادي رقم 3 لعام 2012 الخاص بهيئة الأمن الإلكتروني بأنه" استخدام الوسائل لإلكترونية لتأمين ولحماية شبكات تقنية الاتصالات والمعلومات وشبكتها المعلوماتية، والعمليات الخاصة بالمعلومات" (جريدة الإمارات الرسمية، 2012).

رابعاً ضعف منظومة الأمن السيبراني يهدد الأمن القومي للدول: تتعرض البنى التحتية المدرجة عبر الفضاء السيبراني لمختلف الدول للعديد من الهجمات السيبرانية، سواء اتخذت تلك الهجمات أشكال الحروب السيبرانية أو الإرهاب السيبراني، أو الجرائم الأخرى المرتبطة بالإنترنت، ويتوقف نجاح تلك الهجمات السيبرانية في تحقيق أهدافها على منظومة الأمن السيبراني ومدى قوتها وتطورها لمواجهه تلك الهجمات، فوجود منظومة ضعيفة للأمن السيبراني أو خلل في أحد مفرداتها قد يعرض الأمن القومي للخطر من قبل أشخاص قد يدفعهم مجرد حب الفضول للعبث بأحد مرافق الأمن القومي، فقد دفع حب الفضول المراهق البولندي آدم دابروفسكي (Adam Dabrowski) البالغ من العمر 14 عامًا في أوائل عام 2008 إلى اقتحام محطة الترام في مدينة لودز Lodz ليلاً، باستخدام جهاز تحكم عن بُعد قديم للتلفزيون بعد تحويله، مستغلاً خلل في نظام الإشارات القائم على الأشعة تحت الحمراء والتقاط إشارة تبديل المسار عند نقطة تقاطع واحدة وتشغيلها مرة أخرى عند نقطة تقاطع أخرى للحصول على نفس النتيجة (Bull,2017,)، وفي تصريح لميروسلاف ميكور (Miroslav Micor) المتحدث باسم شرطة لودز أفاد أن ذلك الهجوم قد أحدث فوضى وخروج بعض عربات القطار عن مسارها وحدوث إصابات لدى بعض الركاب(Leyden,2008,) .

المطلب الثاني: خطة الباحث لمواجهة الهجمات السيبرانية على البنى التحتية للمدن الذكية

المحور الأول: تحقيق الأمن المادي يُعد خط الدفاع الأول لتعزيز وحماية مرافق الأمن القومي السيبراني للبني التحتية للمدن الذكية:

يرى الباحث أن تأمين منظومات الأمن السيبراني بتقنيات الحماية المتطورة يُشكل أولوية أساسية وجوهرية، إلا أنها لم تعد كافية لتحقيق نسق الحماية الكاملة المطلوبة لأننا في عصر صراع تطور التقنيات التي كل يوم هناك جديد، حتى استقرت حقيقة علمية مفادها أنه **لا يمكن تحقيق الأمن السيبراني للمرافق والمؤسسات لأي دولة في العالم بنسبة 100%**، لذا فكل ما يمكن أن تفعله الدول أو المؤسسات هو التقليل لمخاطر التهديدات والهجمات السيبرانية إلى الحد الذي يسمح معه الاستفادة من فرص التكنولوجيا الرقمية، فخط الدفاع الأول من وجهة نظر الباحث لحماية منظومة الأمن القومي السيبراني لمرافق البني التحتية للمدن الذكية هو **تحقيق الأمن المادي** لتلك المنظومة، الذي يتجسد في اتخاذ سلسلة من الإجراءات والتدابير لحماية الأجهزة وشبكات المعلومات الخاصة بتلك المنظومة، بدايتها حصر وتحديد النقاط والموارد المعرّضة لخطر الوصول غير المشروع إليها أو العبث بها أو سرقتها، ومن ثم اتخاذ تدابير حمايتها بتعزيز الأبواب المغلقة لضمان عدم الوصول إليها، ثم حصر وتحديد أصول المعلومات عالية القيمة، لتأمينها وحمايتها، من خلال استخدام تقنيات الذكاء الاصطناعي وأجهزة الاستشعار عن بُعد والكاميرات المتطورة عالية الجودة والدقة.

المحور الثاني: تحديث وتطوير منظومة الأمن السيبراني لمرافق البنى التحتية للمدن الذكية وتنمية وتدريب قدرات القائمين عليها

فيجب على المدن تطوير استراتيجية تفصيلية للأمن السيبراني تتسق مع استراتيجيتها الشاملة للمدينة الذكية، والنظر في إجراء تقييم شامل لتأثير بياناتهم وإجراءاتهم وأصولهم الإلكترونية لتحديد وتقييم وتقليل المخاطر المرتبطة بالعمليات والسياسات والحلول الفنية، وذلك كله من خلال بناء شراكات استراتيجية لتنمية القدرات السيبرانية، لأن فجوة المهارات السيبرانية لن تختفي في أي وقت قريب، فيجب على المدن أن تكون مبدعة واستباقية في سد هذه الفجوة في مجتمعاتها، فيمكن للتعاون الاستراتيجي والعقود مع مقدمي الخدمات أن تساعد المدن على استكمال مهاراتها الحالية. (Vasiliki, Demertzis,2023,P27-28)

المحور الثالث: مراجعة دورية لمنظومة الأمن السيبراني لمرافق البنى التحتية للمدن الذكية لتطور وتعقد الأصول المشفَرة المرتبط بمنظومات الأمن السيبراني في تطبيقاتها وبنيتها التحتية العابرة للحدود بين الدول، مع ضرورة المراجعة المستمرة للتشريعات الصادرة المرتبطة بها، للتحقق من مدى ملائمة تلك التشريعات لهذا النوع من الأصول، وما إذا كانت هناك حاجة لتعديلها.

فقد أظهر تحليل أبحاث الأمن وإدارة المخاطر للشبكات الديناميكية للمدينة الذكية أن الأمر يتطلب فرض أساليب جديدة لتقييم المخاطر، حيث أن الأساليب التقليدية غير قادرة على العمل مع تفاصيل أصول الشبكة المتغيرة بسرعة (Vasiliy,Maxim,2021,P17-18,).

المحور الرابع: تعزيز وتطوير كفاءة وقدرة الأجهزة الخاصة بالعدالة الجنائية في التحقيقات السيبرانية: ودعمها بكافة أشكال الدعم التقني السيبراني، وذلك بأنظمة الذكاء الاصطناعي المتطورة وأجهزة الاستشعار عن بُعد وخوارزميات وبرمجيات تحليل البيانات المتطورة وغيرها، فضلاً عن دعم وتطوير كفاء وقدرة العاملين، من أجل الاستجابة والتفاعل مع تلك الأنظمة الذكية وتطويرها لخدمة العدالة الجنائية.

المحور الخامس: دعم وتطوير التعاون الدولي مع الدول المتقدمة في مجال الأمن السيبراني: للوقوف على أحدث تقنيات أساليب الهجمات

السيبرانية وكيفية مواجهتها، وأنظمة الحماية المقررة، وإنشاء قواعد بيانات مشتركة لتبادل المعلومات والخبرات وأساليب التهديدات وكيفية التنبؤ بها، لخلق مراكز جديدة ومتطورة للابتكار السيبراني، وذلك كله لرفع القدرة على حماية الأمن السيبراني لمرافق البنى التحتية للمدن الذكية.

المحور السادس يحذر الباحث ويشدد على عدم استيراد منظومات الحماية الجاهزة الخاصة بالأمن السيبراني:

لأن تلك المنظومة المستوردة تتضمن في أغلبها مخاطر وتهديدات للأمن القومي للدول بمفهومه الشامل، فتلك المنظومة المستوردة قد تتضمن تقنيات مشفَرة مجهولة للتجسس على المنظومة الوطنية وفقه أسرارها، أو لإتلاف البيانات والمعلومات والأسرار أو العبث بها، أو سرقتها أو تغيير آلية تداول أصولها خاصة في المؤسسات المصرفية أو المالية الوطنية المستضيفة لتلك المنظومة، لافتعال هبوط أسهمها أو حتى مجرد سرقة هامش بسيط لا يُلحظ عند تداول أصولها المالية، ولمنع هذه المخاطر والتهديدات يلزم منع تشغيل منظومات الحماية المستوردة في القطاعات والمؤسسات الاستراتيجية أو الحيوية، بل تجربتها أولاً بصحبة كفاءات وطنية مدربة في قطاعات غير حيوية أو قطاعات محاكاة تدريبية، لفك شفراتها وفقه تكوينها وأسرار، ثم بعد ذلك الاعتماد عليها.

المحور السابع: تعزيز ونشر ثقافة الأمن السيبراني لدى مواطني المدن الذكية:

إذا كان مواطن المدن الذكية هو المستفيد الأول من خدمات تلك المدن وبيئتها الذكية، فإنه يُعتبر في ذات الوقت خط الدفاع الأول لحماية الأمن القومي السيبراني لمرافق تلك المدن، فهو أول من يتلقى تدفق خدمات وتداول الأصول المالية لتلك المرافق من خلال استخدامه للتطبيقات الذكية، لذا فسلامة تداول تلك الأصول المالية تتوقف على مدى ثقافة ووعي ذلك المواطن بقضايا الأمن السيبراني لتأمين تلك الأصول ولتفعيل جودة هذه الخدمات، لذا يلزم رفع كفاءة وقدرات ومؤهلات المواطن فيما يتعلق بقضايا الأمن السيبراني في جميع مراحل حياته التعليمية ومهنته.

وفي النهاية فقد أكدت نتائج أحدث الدراسات أنه من الضروري التغلب على التحديات الرئيسية للأمن السيبراني والتي تتجسد في ظهور سلسلة من تهديدات الأمن السيبراني، مثل فقدان الخصوصية والسرية، التهديدات المادية وضعف الأنظمة والتطبيقات، وهجمات حقن البرامج الضارة، ورفض الخدمة (DoS)،" التهديدات الداخلية الخبيثة، وتسرب البيانات(João, Pedro,2022,P 10-11.)، لذا جاءت خطة الباحث لمواجهة تلك التحديات.

خاتمة الدراسة

الحقيقة أن موضوع الدراسة وهو الهجمات السيبرانية على البنى التحتية للمدن الذكية من الموضوعات المتجددة التي تُثير دائما العديد من التحديات القانونية والفنية التي تتطلب استراتيجية للمواجهة، نظراً لطبيعة تلك الهجمات السيبرانية التي قد تتمثل في صعوبة تحديد مصدر الهجوم السيبراني وتعقبه ومعرفة هوية مرتكبه لضبطه وملاحقته وتقرير مسؤوليته، خاصة إذا كان عابراً للحدود، والذي قد يُرتكب بمجرد اكتشاف الثغرة الأمنية على الطرف الآخر من الكرة الأرضية، فقد يبدأ وينتهي في ثوان معدودة محققاً هدفه المطلوب، وقد يُصيب أهدافا متعددة أو هدف واحد عدة مرات وفي ثوان معدودة، بل قد يبدأ وينتهي الهجوم محققاً هدفه المطلوب دون حتى اكتشافه أو معرفة طبيعة وأنواع المعلومات التي تم الاستيلاء عليها، فضلاً عن صعوبة تحديد الطبيعة القانونية للهجمات السيبرانية، وما إذا كانت إرهاب سيبراني أو حرب سيبرانية، وذلك التداخل الي يُثير دائماً جدلاً قانونياً، خاصة أن محل ارتكاب ذلك الهجوم هو مرافق ومؤسسات البنى التحتية للحكومات والمدن الذكية لمختلف دول العالم، وما تتضمنه من معلومات وبيانات وأسرار تتعلق بمفردات الأمن القومي للدول، الأمر الذي يُثير دائما ضرورة توافر منظومة قوية ومتطورة للأمن السيبراني قادرة على صد تلك الهجمات أو الحد من ارتكابها، في ظل تطور تقنيات تلك الهجمات السيبرانية المستمر، لذا كان هناك ارتباط قوي بين الأمن القومي والأمن السيبراني، لأن ضعف منظومة الأمن السيبراني يهدد الأمن القومي للدول، وما قد يتطلبه كل ذلك من إطار تشريعي متطور وقوي ينظم مفردات جرائم تلك الهجمات ويُجرم سلوك ارتكابها المتطور، لذا انتهت الدراسة إلى العديد من النتائج والتوصيات بالإضافة إلى خطة توصياته في متن البحث، قدمت من خلالهم حل لتلك التحديات القانونية والفنية لموضوعها التي شكلت مفرداتها على النحو التالي:

أولا النتائج:

1- أصبح الفضاء السيبراني وما يتضمنه من مرافق ومؤسسات البنى التحتية لحكومات الدول ومدنها الذكية قوة جذب للاعتداء عليه بمختلف الهجمات السيبرانية، لما تتضمنه تلك المرافق والمؤسسات من بيانات ومعلومات وأسرار تُشكل مفردات الأمن القومي لمختلف الدول.

2- جسد صراع التقنيات وضعف منظومة الأمن السيبراني لمختلف الدول العامل الجوهري في تزايد تلك الهجمات السيبرانية على المدن الذكية، مع سرعة تطور تقنياتها المستمر.

3- مع تزايد الهجمات السيبرانية على البنى التحتية للمدن الذكية، أصبح الأمن السيبراني جزء من الأمن القومي لتلك الدول.

4- الهجوم السيبراني هو وسيلة ارتكاب جرائم الأمن القومي السيبراني على البنى التحتية للمدن الذكية، سواء شكل هذا الهجوم النموذج

القانوني لأركان جرائم تقنية المعلومات التقليدية، أو جرائم الإرهاب السيبراني، أو حروب سيبرانية ترتكبها دول.

5- الهجمات السيبرانية تتزايد خطورتها وتثير إشكاليات قانونية وفنية، سبق بيانها، قد يتعذر التغلب عليها من قبل حكومات الدول ومدنها الذكية.

6- يُعرف الباحث المدن الذكية بأنها "تلك المدن القائمة على المزج والتكامل بين تكنولوجيا المعلومات والاتصالات (ICT) وبين إدارة وتشغيل وخدمات مرافق البنى التحتية للمدن، لتوفير خدمات وبيئات حضرية آمنة ومرنة وقابلة للتكيف، وأكثر كفاءة واستدامة وشمولية وصديقة للبيئة بأقل تكاليف، لتحسين جودة الحياة لتلبية احتياجات الأجيال الحالية والقادمة.

7- تُعد دولة الإمارات العربية المتحدة من الدول الرائدة في تحقيق التنمية المستدامة، وفي مجال المدن الذكية.

8- الإرهاب السيبراني والحروب السيبرانية يُعدان من أكبر التهديدات للأمن القومي للمدن الذكية.

9- هناك صعوبة بالغة لتحديد الطبيعة القانونية لما يُعد إرهاب السيبراني أو حروب السيبرانية.

10-عرف الباحث الإرهاب السيبراني والحروب السيبرانية كما بينت الدراسة.

ثانيا التوصيات: بالإضافة للتوصيات التي وردت في الخطة المقدمة من الباحث يوصي أيضاً بـ:

1-ضرورة الاستثمار الوطني في صناعة وإنتاج التطبيقات الذكية وتقنياتها وأنظمة الذكاء الاصطناعي.

2-ضرورة وضع الأمن السيبراني في أولويات التدريس في المدارس والجامعات، على أن يقرر كمساق تدريسي، له خطته وأهدافه ومخرجاته، لنشر ثقافة الأمن السيبراني في تلك القطاعات، وتدعيم أخلاقيات التعامل مع الانترنت، على أن يسبق ذلك عقد ورش عمل ودورات تدريبية في تلك القطاعات.

3-إنشاء كلية خاصة للأمن السيبراني بالجامعات، لتكون نواة لبنية تحتية متطورة من الكفاءات الوطنية القادرة على حماية المنشآت الحيوية والاستراتيجية للدولة من أي تهديد أو هجوم سيبراني، على أن تقسم شعب الكلية إلى شعبة الأمن السيبراني لقطاع الصحة، القطاع المالي، القطاعي الصناعي وهكذا حسب القطاعات التي لها أولوية في الحماية.

4-إنشاء شعبة في إدارة الإعلام الأمني بوزارة الداخلية تكون خاصة بالأمن السيبراني، تختص بنشر ثقافة الأمن السيبراني، وتدعيم أخلاقيات التعامل مع الانترنت، موجهه إلى جميع أفراد المجتمع، بالتنسيق مع أجهزة إعلام الدولة كالإذاعة والتليفزيون والصحافة.

5-إنشاء إدارات خاصة بالأمن السيبراني في جميع المؤسسات والهيئات والوزارات التابع للدولة، خاصة القطاعات الحيوية والاستراتيجية، كقطاع الصحة والقطاع المالي والصناعي وغيرها، لنشر ثقافة الأمن السيبراني وتدعيم أخلاقيات التعامل مع الإنترنت.

المصادر والمراجع

عبد الله، ع. (2014). المدن والمباني. *مجلة العلوم والتقنية، الرياض، مدينة الملك عبد العزيز للعلوم والتقنية*، 28(111)، 4.

الكاكا، م. (2020). اختصاصات مجلس الأمن في التصدي للإرهاب الدولي الإلكتروني. دراسات: علوم الشريعة والقانون الجامعة الأردنية، 47 (1)، 450–461.

الاتحاد الدولي للاتصالات. (2021). *هيئة الأمم المتحدة*. https://www.itu.int/ar/mediacentre/backgrounders/Pages/smart-sustainable-cities.aspx

النيابة العامة في رأس الخيمة. (2012). *دولة الإمارات العربية المتحدة*.

https://rakpp.rak.ae/ar/Pages/%D9%85%D8%B1%D8%B3%D9%88%D9%85-%D8%A8%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D8%AA%D8%AD%D8%A7%D8%AF%D9%8A-3-%D9%84%D8%B3%D9%86%D8%A9-2012-.aspx

محكمة التمييز الأردنية، الحكم رقم 651 لسنة 2013، الصادر بتاريخ 10 / 7 / 2014.

محكمة التمييز الأردنية، الحكم رقم 966 لسنة 2021، الصادر بتاريخ 25-7-2021.

References

Anto, O. (2017). *The 5 Pillars of a Smart City*. https://www.quest-global.com/blogs/the-5-pillars-of-a-smart-city/.

ALICE, C. (2018). *10 pillars of a smart city*. https://placetech.net/strategy/10-pillars-of-a-smart-city/.

Anjali, D. (2020). U.S. Government Warns Companies of Legal Risk for Paying Ransom to Cybercriminals. *The National Law Review*, 6(280). https://www.natlawreview.com/article/us-government-warns-companies-legal-risk-paying-ransom-to-cybercriminals.

Algirde, P. (2021). *These are the top cybersecurity challenges of 2021*. World Economic Forum. https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/.

Harrison, C., Eckman, B., Hamilton, R., Hartswick, P., Kalagnanam, J., Paraszczak, J., & Williams, P. (2010). Foundations for smarter cities. *IBM Journal of research and development*, *54*(4), 1-16. https://ieeexplore.ieee.org/document/5512826.

Silva, B. N., Khan, M., & Han, K. (2020). Integration of Big Data analytics embedded smart city architecture with RESTful web of things for efficient service provision and energy management. *Future generation computer systems*, *107*, 975-987. https://www.sciencedirect.com/science/article/abs/pii/S0167739X17305174.

Center for Strategic &International Studies (CSIS). (2022). Significant Cyber Incidents. Retrieved from https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

Wilson, C. (2008). *Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress* (Vol. 29). Washington, DC: Congressional Research Service. https://sgp.fas.org/crs/terror/RL32114.pdf.

Soesanto, S. (2020). *Japan's national cybersecurity and defense posture: Policy and organizations*. ETH Zurich. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-08-Japans-national-cybersecurity-defense-posture.pdf.

Congressional Research Service. (2020). *Defense Primer: Electronic Warfare*. Retrieved from https://sgp.fas.org/crs/natsec/IF11118.pdf.

David, E. (2021). *Russian Hackers Broke into Federal Agencies*. Retrieved from https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html.

Dave, W. (2020). *Types of Cyber Attacks: A Closer Look at Common Threats*.

Demertzi, V., Demertzis, S., & Demertzis, K. (2023). An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities. *Applied Sciences*, *13*(2), 790.

Doug, W., & Usman, S. (2010). *Helping CIOs Understand "Smart City" Initiatives*.

ITU. (2019). *BDT Cyber Security Programme, Global Cybersecurity Index (GCI), Guidelines for Member States*. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCI_V4_Guidelines_for_Member%20States.pdf.

John, B. (2017). *You Hacked: Cyber-Security and the Railways*. London Reconnections. https://www.londonreconnections.com/2017/hacked-cyber-security-railways/

John, L. (2008). *Polish teen derails tram after hacking tram network*. Retrieved from https://www.theregister.com/2008/01/11/tram_hack/.

Jane, M. (2021). *What is cyber warfare?* Retrieved from https://www.itpro.co.uk/security/28170/what-is-cyber-warfare.

Josh, F. (2020). *What is a cyber-attack?* Retrieved from https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html.

Jan, W. (2020). Suspected Russian Hack of U.S. Government: Espionage or Act of War? *Insurance journal*. https://www.insurancejournal.com/news/national/2020/12/21/594810.htm.

Kalinin, M., Krundyshev, V., & Zegzhda, P. (2021). Cybersecurity risk assessment in smart city infrastructures. *Machines*, *9*(4), 78. https://www.mdpi.com/2075-1702/9/4/78.

Lucian, C. (2020). Solar Winds attack explained: And why it was so hard to detect. Retrieved from https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html.

Nelson, B., Choi, R., Iacobucci, M., Mitchell, M., & Gagnon, G. (1999). Cyberterror: Prospects and implications. *Center for the Study of Terrorism and Irregular Warfare Monterey, CA*. https://calhoun.nps.edu/bitstream/handle/10945/27344/Cyberterror%20Prospects%20and%20Implications.pdf?sequence=1&isAllowed=y.

Ministry of Science and Technology (MOST). (2021). *The main pillars of smart cities and consultation to choose the right pillars to develop and build smart cities*. Retrieved from https://www.most.gov.vn/en/news/813/the-main-pillars-of-smart-cities-and-consultation-to-choose-the-right-pillars-to-develop-and-build-smart-city.aspx.

Mary, P. (2021). *Cyber-attack*. Retrieved from https://www.techtarget.com/searchsecurity/definition/cyber-attack#:~:text=A%20cyber%20attack%20is%20any,data%20held%20within%20these%20systems.

Megan, H. (2020). Corona Viruses and Computer Viruses: It's Time for a Cyber Health Check-Up. The National Law Review, 6(217). https://www.natlawreview.com/article/corona-viruses-and-computer-viruses-it-s-time-cyber-health-check.

Nick, O. (2021). Defending Against National Security Threats. The National Law Review, 6(254). https://www.natlawreview.com/article/defending-against-national-security-threats.

OECD.)2020). *Smart Cities and Inclusive Growth*. Retrieved from https://www.oecd.org/cfe/cities/OECD_Policy_Paper_Smart_Cities_and_Inclusive_Growth.pdf.

Rand. (2022). *Cyber Warfare*. Retrieved from https://www.rand.org/topics/cyber-warfare.html.

Reis, J., Marques, P. A., & Marques, P. C. (2022). Where are smart cities heading? A meta-review and guidelines for future research. *Applied Sciences*, *12*(16), 8328. https://www.mdpi.com/2076-3417/12/16/8328. Steve, R (2018). *What is cyberwar? Everything you need to know about the frightening future of digital conflict*. Retrieved from https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/.

Campisi, T., Severino, A., Al-Rashid, M. A., & Pau, G. (2021). The development of the smart cities in the connected and autonomous vehicles (CAVs) era: From mobility patterns to scaling in cities. *Infrastructures*, *6*(7), 100. https://www.mdpi.com/2412-3811/6/7/100.

Draft, A. U. (2016). Issues paper on smart cities and infrastructure. https://unctad.org/system/files/official-document/CSTD_2015_Issuespaper_Theme1_SmartCitiesandInfra_en.pdf.

United, N. (2018). *The World's Cities in Data Booklet*. Retrieved from https://www.un.org/development/desa/pd/sites/www.un.org.development.desa.pd/files/files/documents/2020/Jan/un_2018_worldcities_databooklet.pdf