Winter 1-1-2021

Cybercrimes against National Security of Smart City Infrastructures - Legal and Technical Challenges and Confrontation Strategy

Dr. Emadeldin Mohamed Kammel Abdulhamed
Imam Malik College for Sharia and Law, emadeldin@imc.gov.ae

Al-miʿyār

Volume 10 Article 7

1-1-2021

Attacking National Cyber Security of Smart City Infrastructure legal and technical challenges and coping strategies

Emad El-Din Mohamed Kamel Abdel Hamid
Imam Malik College for Sharia and Law, almiyar@imc.gov.ae

جرائم الاعتداء على الأمن القومي السيبراني للبنى التحتية للمدن الذكية
التحديات القانونية والتقنية واستراتيجية المواجهة

الدكتور عماد الدين محمد كامل عبد الحميد

أستاذ القانون الجنائي المساعد

كلية الإمام مالك للشريعة والقانون – دبي

270

Attacking National Cyber Security of Smart City Infrastructure

legal and technical challenges and coping strategies

Dr. Emad El-Din Mohamed Kamel Abdel Hamid

Assistant Professor of Criminal Law

Imam Malik College for Sharia and Law – Dubai

الملخص:

لسرعة وزيادة تدفق سكان العالم إلى المناطق الحضرية ونمو وتزايد الكثافة السكانية في تلك المناطق، اتجهت مختلف دول العالم نحو تأسيس وتطوير بنى تحتية قوية ومستدامة، قادرة على الصمود في مواجهة الاحتياجات الناجمة عن التوسع الحضري والنمو السكاني، ومن ثم التحول نحو المدن الذكية لمواجهة تلك التحديات، مستفيدة من التطور العلمي والتكنولوجي الحديث المتمثل في تكنولوجيا تقنية المعلومات والاتصالات، لما تقدمه تلك التقنيات من سهولة وسرعة في تخزين وحفظ المعلومات ومعالجتها واسترجاعها وتعديلها، فارتكزت مرافق ومؤسسات البنى التحتية لمختلف دول العالم المتقدم خاصة المدن الذكية فيها على الفضاء السيبراني، في كافة المؤسسات الحيوية والاستراتيجية، فأصبح الفضاء السيبراني وما يتضمنه من أسرار ومعلومات وبيانات لتلك المرافق والمؤسسات قوة جذب للاعتداء عليه بمختلف الجرائم سواء جرائم المعلومات التقليدية أو جرائم الأمن القومي السيبراني التي قد تتمثل في جرائم الإرهاب السيبراني أو الحروب السيبرانية والتي استخدمت وسيلة ارتكابها الهجمات السيبرانية العابرة للحدود حول العالم، والتي تبدأ بمجرد اكتشاف الثغرة الأمنية على الطرف الأخر من الكرة الأرضية ومن ثم تنتهي تلك الهجمات في ثوان معدودة مُحققة هدفها المطلوب، وقد تُصيب أهداف متعددة أو هدف واحد عدة مرات وفي ثوان معدودة، مع صعوبة تحديد مصدرها أو حتى اكتشافها أو تعقبها أو ملاحقة مرتكبيها، فضلاً عن الأثار المدمرة لتلك الهجمات على مراكز البنى التحتية للمدن الذكية والتي تفوق قدراتها بمراحل الأثار المدمرة للهجمات التقليدية الإرهابية أو العسكرية في الحروب التقليدية.

لذا فقد فرض هذا الواقع على حكومات دول العالم وأجهزة عدالتها الجنائية العديد من التحديات والإشكالات القانونية والتقنية ووضعها في اختبار حقيقي أمام مجتمعاتها في مدى قدرتها على تلبية تأمين وحماية البنية التحتية لمؤسسات وهيئات ومرافق دولها القائمة على ذلك الفضاء السيبراني جراء تلك الجرائم، ويُشكل مفردات هذا البحث إبراز هذه التحديات وتلك الإشكالات وسبل مواجهتها.

الكلمات المفتاحية: الفضاء السيبراني - الأمن القومي السيبراني - الهجوم السيبراني - المدن الذكية - الإرهاب السيبراني - الحروب السيبرانية - الأمن السيبراني.

Abstract

The facilities and infrastructure institutions of smart cities in various countries of the world have been based on cyberspace. The cyberspace and the data it contains for these facilities and institutions have become attractive for various attacks, whether information crimes or cyber national security crimes.

Cyber national security crimes may be committed in the form of cyber terrorism crimes or cyber wars, and the means of committing them are cross-border cyber-attacks, which start and end these attacks in few seconds, achieving their desired goal. It is difficult to determine their source or track their perpetrators, in addition to the devastating effects of these attacks on the infrastructure centers of smart cities, which exceed the effects of traditional terrorist or military attacks in conventional wars.

Therefore, this reality imposed on the governments of the countries and their criminal justice agencies many challenges and legal and technical problems. This research aims to highlight these challenges and presents ways to overcome them.

Key words: cyber space - cyber national security - cyber-attack - smart cities - cyber terrorism - cyber wars - cyber security.

مقدمة عامة

مع زيادة تدفق سكان العالم إلى المناطق الحضرية ونمو وتزايد الكثافة السكانية في تلك المناطق كان لابد من إعادة النظر 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 2050 لتصل لـ 68%[587]، الأمر الذي دفع حكومات مختلف دول العالم إلى التحول نحو المدن الذكية لمواجهة تلك التحديات ولتلبية احتياجات الأجيال الحالية والقادمة مع تحسن نوعية الحياة، مستفيدة من التطور العلمي والتكنولوجي الحديث المتمثل في تكنولوجيا تقنية المعلومات والاتصالات، فاستطاعت الاتصالات الحديثة والتي كانت بدايتها الاتصالات السلكية واللاسلكية ثم الأقمار الصناعية والألياف البصرية والتي انتهت بتكنولوجيا الجيل الخامس (5G) 2020، أن تحول وباقتدار العالم كله الى قرية إعلامية صغيرة، واستطاعت تقنية شبكات الجيل الخامس لتطبيقات الأجهزة اللاسلكية الثابتة والمتنقلة أن توفر داخل المدن والمناطق بيئات ذكية مترابطة بين الأشخاص والتطبيقات والبيانات والأشياء والآلات وأنظمة النقل، مع سرعة في الأداء وموثوقية عالية.

واستطاعت شبكات تقنية المعلومات والاتصالات سواء كانت شبكات محلية أو إقليمية أو عالمية أن تربط بين أجزاء العالم في تناسق وتشابك عجيب، تلاشت عبرها الحواجز الجغرافية بين الدول والمسافات، وتدفقت عبر أرجائها المعلومات، على اختلاف أنواعها واتجاهاتها، وعبر كل طرف من أطراف تلك الشبكات الضخمة والمتداخلة ينم التعامل معها، فعند كل طرف منها قد يتم إدخال المعلومات أو معالجتها

587 United Nations Department of Economic and Social Affairs, date to visit,1-8-2021, Available at: https://www.un.org/development/desa/ar/news/population/2018-world-urbanization-prospects.html.

أو تخزينها أو استرجاعها أو تعديلها... لذا فقد تواترت أغلب دول العالم على إدراج وتخزين معلوماتها وأسرارها عبر تلك الشبكات، في كافة المجالات العسكرية أو الصناعية أو السياسية أو الاقتصادية خاصة فيما يتعلق بقطاع البنوك، لما تقدمه تلك التقنيات من سهولة وسرعة في تخزين وحفظ المعلومات ومعالجتها واسترجاعها وتعديلها، كما لم تقتصر تلك شبكات على احتواء أسرار الدول ومعلوماتها، بل تضمنت وشكلت مفرداتها معلومات أفراد تلك الدول وتعاملاتهم في كافة نواحي الحياة، خاصة النواحي الاقتصادية فشهدت تلك الشبكات مختلف لأنواع المعاملات الاقتصادية والتجارية، وتبادل حقيقي للسلع والخدمات، وتدفق سريع وفي ثواني لرؤوس الأموال عبر تلك الشبكات، فتشكلت شريحة اقتصادية وتجارية أطرافها **أفراداً** وشركات، محددة وواضحة المعالم تشكل أحد جوانب ومفردات الاقتصاد القومي لأغلب دول العالم.

فأغلب البنى التحتية لحكومات دول العالم تُنشأ وتدار عبر تلك الشبكات، تُصاغ من مفرداتها السياسات، وتُقر بشأنها الميزانيات، ويُصدر لها جلّ القرارات، وتشُب بين أرجائها الحروب والهجمات، لما تتضمنه عبر أرجائها من أسرار ومعلومات وبيانات تشكل مفردات الأمن القومي للدول، ومن ثم فمجرد الوصول غير المشروع إليها أو الاعتداء عليها يُعد جريمة من جرائم الأمن القومي السيبراني.

ومع تسارع مختلف دول العالم نحو شبكات تقنية المعلومات والاتصالات تولدت كمية هائلة من البيانات والمعلومات لدى أغلب الحكومات الذكية لمختلف تلك الدول، والتي تُعرف عمومًا باسم "Big Data" أي "البيانات الكبيرة"، مما دفع تلك الحكومات إلى أن تقوم بترحيل تخزين تلك البيانات والمعلومات ومعالجتها إلى السحابة، بهدف جني المزايا الهائلة لتقنية الحوسبة السحابية.

لذا فإن التحدي الأكبر الذي يواجه دول العالم هو ذلك الفضاء السيبراني ذاته الذي صنعه الإنسان لنفسه، الذي يُطالع دول العالم كل يوم بل كل ثانية بتكنولوجيات وتقنيات جديدة، لا يمكن التغاضي عنها أو الهروب منها، حتى أصبح العالم اليوم أسيراً بدوله وأفراده وجماعاته ومؤسساته لذلك الفضاء السيبراني ولا يملك منه فكاكاً، رهينة تحت تصرفه يحترم قواعده ويُصغي لآلياته ويناقش فرضياته، وعلى الرغم من السباق

المحموم لمختلف دول العالم بإحاطة ذلك الفضاء السيبراني وما يتضمنه من أسرار ومعلومات لتلك الدول، بسياج منيع من الحماية سواء من خلال برامج حماية أو بتشفير تلك المعلومات والأسرار، أو إحاطتهما بسياج من الحماية المادية والمراقبة التكنولوجية والتقنية، لمنع الوصول إليها أو فك شفراتها، إلا أنه قد تم اختراق البني التحتية لحكومات دول العالم المدرجة عبر تلك الشبكات، وتعرضت أسرارها لأشد الهجمات، التي تنتهك أمنها القومي للأسرار والمعلومات.

لذا فقد فرض هذا الواقع على أجهزة العدالة الجنائية لمختلف دول العالم العديد من التحديات، ووضعها في اختبار حقيقي أمام مجتمعاتها في مدى قدرتها على تلبية تأمين وحماية البنية التحتية لمؤسسات وهيئات ومرافق دولها القائمة على ذلك الفضاء السيبراني، تجاه التهديدات والهجمات المتعلقة بأمن المعلومات والأسرار، وتجاه التحديات التي تواجهها جراء مختلف الجرائم سواء كانت جرائم تقليدية أو جرائم تقنية معلومات.

وتُعد دولة الإمارات العربية المتحدة من الدول الرائدة وبحق التي استطاعت أجهزة عدالتها الجنائية أن تنجح في هذا الاختبار الحقيقي، في تأمين وحماية حكومتها الذكية ومؤسساتها ومرافقها وقطاعاتها الحيوية، ضد أي تهديدات أو هجمات، ومكافحة كل صنوف الجرائم التي قد ترتكب ضدها، عبر آليات تقنية وتكنولوجية متطورة، وسلسة من التشريعات المُحكمة المتجددة، وأجهزة عدالة جنائية تعمل من خلال تقنيات وتطبيقات ذكية متطورة، وكوادر مدربة على أحدث التقنيات والأجهزة، وخبراء يطبقون أحدث النظم العقابية وبدائل تنفيذها الحديثة.

مشكلة موضوع البحث: يُثير العديد من الإشكاليات القانونية والتقنية المعقدة والمتشابكة والتي تتجسد في أن البنى التحتية للمدن الذكية لمختلف دول العالم المتقدم قد ارتكزت على الفضاء السيبراني القائم على تكنولوجيا تقنية المعلومات وتقنية الاتصالات، وما تضمنته تلك البنى التحتية من مرافق ومؤسسات، وأنشطة ومعاملات، وبيانات وأسرار ومعلومات في كافة المجالات، (الصناعية والعسكرية، الاقتصادية والمالية، السياسية والإدارية، التشغيلية والخدمية، الطاقة والمياه- الصحة ومنظومة النقل - قطاع البنوك والمؤسسات المالية والحكومية)، لذا فقد أصبح الفضاء السيبراني بمكوناته السابقة 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، تُجسد مفردات جرائم الأمن القومي السيبراني، **الأمر الذي فرض تساؤلا جوهريا** هو كيفية حماية تلك البنى التحتية للمدن الذكية من الهجمات السيبرانية لتلك الجرائم في ظل تطور تقنياتها المستمر؟ هذا التساؤل يُجسد إشكاليات قانونية وتحديات تستوجب عقد مقارنة بين تجارب أهم مدن العالم الذكية ومنظومة أمنها السيبراني وتطبيقاتها الذكية في إثبات ومكافحة تلك الجرائم، كما استوجب هذا التساؤل عدة تساؤلات فرعية الإجابة عليها تُمثل مفردات البحث ومدى أهميته.

تساؤلات موضوع البحث:

1- ما هي أسباب تزايد الهجمات السيبرانية على مرافق البنى التحتية للمدن الذكية بمختلف دول العالم؟

2- ماهو الهجوم السيبراني وأنواعه ووسائله وأثاره على مرافق البنى التحتية للمدن الذكية؟

3- ما هو النموذج القانوني لتجريم الهجوم السيبراني؟

4-ما هي المدن الذكية وركائزها وخصائصها التي تتميز به عن مختلف المدن التقليدية؟

5- ما هو مفهوم الشرطة الذكية وأجهزتها وتطبيقاتها الذكية عبر مختلف دول العالم المتقدم، وما هو دورها في مكافحة الجرائم أو الحد من ارتكابها في المدن الذكية المقارنة بين مختلف دول العالم؟

5- ما هو مفهوم الأمن القومي للدول ومدى ارتباطه بالأمن السيبراني، ومدى حقيقة الأمن القومي السيبراني؟

6- ما هي جرائم الأمن القومي السيبراني وأنواعها ووسائل ارتكابها على مرافق البنى التحتية للمدن الذكية المقارنة وطرق مكافحتها؟

7- ماهي مخاطر التخزين السحابي على الأمن القومي السيبراني؟

أهمية موضوع البحث: تبدو أهمية موضوع البحث في بيان ما يلي:ماهية المدن الذكية – ركائزها - خصائصها، أهم التجارب العالمية المقارنة في مجال المدن الذكية وفقاً لمؤشر المدن الذكية (2020)، تجارب دولة الإمارات العربية المتحدة في مجال المدن الذكية، بيان دور الشرطة الذكية لضبط الجرائم والحد من ارتكابها في المدن الذكية المقارنة خاصة في أهم المدن الذكية في العالم في الولايات المتحدة الأمريكية – سنغافورة والتي جاءت في المركز الأول في مؤشر ترتيب المدن الذكية حول العالم (2020)، دور الشرطة الذكية في مكافحة الجرائم والحد من ارتكابها في دولة الإمارات، مفهوم الأمن القومي وتطوره ومدى ارتباطه بالأمن السيبراني، ماهية الأمن السيبراني ومؤشره العالمي وركائزه، الصادر عن الاتحاد الدولي للاتصالات (بمنظمة الأمم المتحدة)، الإرهاب السيبراني الحروب السيبرانية كأكبر التهديدات للأمن القومي للمدن الذكية، ومظاهر جرائم الأمن القومي السيبراني (2021-2020) (التصيد الاحتيالي- هجمات الهندسة الاجتماعية- هجمات البرمجيات الخبيثة- رفض الخدمة (DoS) ورفض الخدمة الموزع (DDoS) وغيرها)، هجمات جرام الأمن القومي السيبراني على مرافق البنى التحتية للمدن الذكية المقارنة في (2020-2021) وعوامل تزايدها.

الهدف من موضوع البحث: تهدف دراسة موضوع البحث 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 الأمن القومي السيبراني المرتكبة على مرافق البنى التحتية للمدن الذكية، وإيجاد الحلول للتحديات القانونية والتقنية التي تمثل إشكاليات موضوع البحث، وذلك من خلال استراتيجية وضعها الباحث لمكافحة جرائم الأمن القومي السيبراني على البنى التحتية للمدن الذكية.

الدراسات السابقة: لا توجد دراسات سابقة عن موضوع البحث وكل الدراسات الموجودة غير متعلقة ومتناثرة، كتناول دراسة الإرهاب السيبراني، الحروب السيبرانية، دون تناول تعلقها أو أثرها على الأمن القومي للدول.

منهج البحث: هو المنهج الاستقرائي والمنهج التحليلي المقارن، المنهج الاستقرائي من خلال استقراء حقيقة وجوهر المدن الذكية وركائزها وخصائصها، ودور الشرطة الذكية لضبط الجرائم والحد من ارتكابها في المدن الذكية خاصة في أهم المدن الذكية في العالم، أيضاً حقيقة وجوهر جرائم الأمن القومي السيبراني المرتكبة على مرافق البنى التحتية للمدن الذكية، ووسائل ارتكابها باستخدام الهجوم السيبراني سواء اتخذ هذا الهجوم نموذج لجرائم الإرهاب السيبراني، أو حروب سيبرانية، وبيان مظاهر ارتكاب تلك الجرائم، للوصول إلى حجم التهديدات والأضرار الواقعة على مرافق الأمن القومي السيبراني للمدن الذكية جراء تلك الجرائم، على الرغم من جهود الشرطة الذكية في مكافحتها، والمنهج التحليلي المقارن، من خلال مقارنة وتحليل لهجمات جرائم الأمن القومي السيبراني الواقعة على مراكز البنى التحتية للمدن الذكية لمختلف دول العالم خلال (2020-2021) وعوامل تزايد تلك الهجمات، وتحليل التحديات القانونية والتقنية التي تُثيرها تلك الجرائم بين مختلف أهم المدن الذكية المقارنة في مختلف دول العالم، والتي تُجسدها صراع التقنيات وضعف منظومة الأمن السيبراني، وذلك كله لوضع استراتيجية للمواجهة.

خطة البحث: تم تقسيمه إلى ثلاثة مباحث وكل مبحث لمطلبين، المبحث التمهيدي ماهية المدن الذكية، المطلب الأول: مفهوم المدن الذكية وركائزها، المطلب الثاني: خصائص المدن الذكية، المبحث الأول: مكافحة الجرائم والحد من ارتكابها في المدن الذكية، المطلب الأول: تجارب دول العالم في مجال المدن الذكية، المطلب الثاني: الشرطة الذكية لضبط الجرائم والحد من ارتكابها في المدن الذكية، المبحث الثاني: مظاهر جرائم الاعتداء على الأمن القومي السيبراني للبنى التحتية للمدن الذكية، المطلب الأول: ماهية الأمن القومي السيبراني، المطلب الثاني: هجمات جرائم الأمن القومي السيبراني على البنى التحتية للمدن الذكية.

المبحث التمهيدي: ماهية المدن الذكية

تمهيد: يتطلب بيان ماهية المدن الذكية أن نقوم بتعريف المدن الذكية سواء لدى المنظمات الدولية، أو لدى الشركات العالمية في مجال تكنولوجيا المدن الذكية، ولدى الفقه ثم دراسة الركائز التي تقوم عليها المدن الذكية والتي 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، لذا سوف نخصص المطلب الأول لدراسة مفهوم المدن الذكية وركائزها، والمطلب الثاني لدراسة خصائصها، وذلك على النحو التالي:

المطلب الأول: مفهوم المدن الذكية وركائزها

مفهوم المدن الذكية (smart cities) في أغلب دول العالم يُستخدم تحت مسميات مختلفة وفي سياق ومعاني متباينة، نظراً للتطور التاريخي لمسار المدن الذكية بين دول العالم، الأمر الذي ترتب عليه عدم وجود اتفاق حول الجوانب والأبعاد والركائز المطلوب توافرها حتى تندرج المدن تحت مسمى المدن الذكية، ومن ثم تعددت وتنوعت وتنافرت في بعض الأحيان التعريفات الصادرة بشأن مصطلح "المدن الذكية"[(588)]، إلا أننا سوف نورد بعض التعريفات التي تُبرز جوهر وطبيعة مصطلح المدن الذكية بالقدر الذي يتناسب مع أساسيا البحث وجوهره والهدف منه.

أولا تعريف المدن الذكية:

أ-تعريف المدن الذكية لدى المنظمات الدولية: جاء 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

588- د أحمد محمود يسري، م طاهر عبد السلام حامد وآخرون " صياغة المفهوم العمراني للمدن الذكية"، كلية التخطيط العمراني والإقليمي جامعة القاهرة، مجلة البحوث الحضرية، المجلد 21، يونيو 2016، **ص51-54.**

date to visit,1-8-2021, Available at:
https://jur.journals.ekb.eg/article_89834_5e0f0b53fab1aaf73322fd261ffba2

ثقافية[589]، 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"[590].

ووفقاً لتعريف منظمة الأمم المتحدة فهي" مدينة تعمل بأسلوب ابتكاري طموح يعتمد على خليط ذكي من الدعم والمشاركة الفاعلة من المواطنين المستقلين الواعيين القادرين على اتخاذ القرار، لتغطية مجلات الاقتصاد – البيئة – والسكان – والحوكمة - وقابلية التحرك "[591]، وفي دراسة (2014) للبرلمان الأوربي حددت تعريف عملي للمدن الذكية " فهي المدينة التي تستخدم تكنولوجيا المعلومات والاتصالات، لمعالجة كافة القضايا العامة، من خلال أسس الشراكة القائمة على أصحاب المصلحة المتعددين"[592].

ب- تعريف الشركات العالمية في مجال تكنولوجيا المدن الذكية: أفادت شركة Digital 14 أن هناك عدة طرق لتعريف المدينة الذكية ، ولكن كل التعريفات تحمل مضمون واحدًا في جوهرها وهو استخدام التكنولوجيا لحل التحديات طويلة الأجل الناتجة عن زيادة التوسع الحضري، من أجل تعزيز قابلية المدينة للعيش والعمل

589- الاتحاد الدولي للاتصالات (ITU) وهو احدى الوكالات المتخصصة التابعة لهيئة الأمم المتحدة.
date to visit,2-8-2021, Available at:
https://www.itu.int/ar/mediacentre/backgrounders/Pages/smart-sustainable-cities.aspx

590 OECD,' Smart Cities and Inclusive Growth", 2020, P 8. date to visit,2-8-2021, Available at:
https://www.oecd.org/cfe/cities/OECD_Policy_Paper_Smart_Cities_and_Inclusive_Growth.pdf

591- منظمة الأمم المتحدة- القمة الحكومية- سلسلة بحوث القمة الحكومية" المدن الذكية المنظور الإقليمي"، فبراير 2015، ص 14.
date to visit,2-8-2021, Available at:
https://www.worldgovernmentsummit.org/api/publications/document/3f505fc4-e97c-6578-b2f8-ff0000a7ddb6

592 European Parliament,' Mapping Smart Cities in the EU", Director General for Internal Policies, Policy Department A: Economic and Scientific Policy, Study, January 2014, P 17. date to visit,2-8-2021, Available at:
https://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET(2014)507480_EN.pdf

والاستدامة، فالمدن الذكية متصلة ، وسريعة الاستجابة ، وذكية[593]، وقدمت شركة IBM تعريفاً للمدينة الذكية بأنها "مدينة تقوم بالاستخدام الأمثل لجميع المعلومات المترابطة والمتاحة، من أجل فهم تلك المعلومات والتحكم فيها ، وحسن إدارة واستخدام الموارد المحدودة "، ووفقًا لتعريف شركة Cisco سيسكو فإن المدن الذكية هي تلك التي تتبنى "حلولًا قابلة للتطوير تستفيد من تكنولوجيا المعلومات والاتصالات لزيادة الكفاءة وخفض التكاليف وتحسين جودة الحياة"، كما قامت مؤسسات بعض الدول بمبادرات لتعريف المدن الذكية مثل إسبانيا والمملكة المتحدة، ففي إسبانيا تبنت الحكومة الإسبانية المفهوم الذي حددته الجمعية الإسبانية للتوحيد القياسي "فمفهوم المدينة الذكية هو نهج شامل للمدن التي تستخدم تكنولوجيا المعلومات والاتصالات، لتحسين نوعية حياة السكان، وتضمن التحسين المستمر للنواحي الاقتصادية والاجتماعية المستدامة، والتنمية البيئية، وتوفير البيانات والحلول المفتوحة والخدمات الموجهة نحو المواطنين لتحقيق التفاعل الشامل بينهما وبين المدن"، أما في المملكة المتحدة فقد أفادت وزارة الأعمال والطاقة في المملكة المتحدة "بأن مفهوم (المدينة الذكية) ليس ثابتًا فلا يوجد تعريف مطلق للمدينة الذكية، ولا نقطة نهاية، بل هو عملية، أو سلسلة من الخطوات، من خلالها تصبح المدن "ملائمة للعيش" وتتسم بالمرونة، وبالتالي تكون قادرة على الاستجابة بشكل أسرع للتحديات الجديدة "[594].

ج-تعريف المدن الذكية لدى الفقه: هي 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"

593 Digital 14," Cyber Resilience Report, Smart Cities, The Power, The Risks, The Response", May 2020, P 4.- date to visit,2-8-2021, Available at: https://www.digital14.com/docs/default-source/reports/cyber-resilience-report.pdf

594 OECD,' Smart Cities and Inclusive Growth", 2020, P 10,11. date to visit,2-8-2021, Available at: https://www.oecd.org/cfe/cities/OECD_Policy_Paper_Smart_Cities_and_Inclusive_Growth.pdf

[595]،وهي التي تستخدم تقنيات الحوسبة الذكية لجعل مرافق ومكونات وخدمات البنية التحتية الحيوية للمدينة أكثر ذكاءً، وترابطًا، وكفاءة"[596] 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 "[597]، وقد قام بعض الفقه في جامعة القاهرة بعمل دراسة بحثية ضمت مائة وستة عشر تعريفاً لمصطلح المدن الذكية من مصادر مختلفة سواء أبحاث أكاديمية، أو مبادرات دولية حكومية عالمية كالاتحاد الأوربي والأمم المتحدة، أو مبادرات شركات تكنولوجيا المعلومات والاتصالات، وانتهت الدراسة إلى وضع تعريف مطوّل وشامل لمصطلح المدن الذكية يحقق مواصفاتها ويلبي جميع معايير دراسته، بأنها المدينة الذكية المستدامة التي تدعم البنى التحتية أو الأساسية لتكنولوجيا المعلومات والاتصالات، وذلك من أجل تحسين جودة حياة المواطن، وضمان نمو اقتصادي يلمسه المواطنين (يتمثل في ارتفاع مستويات المعيشة - توفير فرص عمل- رعاية صحية – حرية – تعليم – سلامة بدنية)، تلبية الاحتياجات اليومية وعدم التضحية باحتياجات الأجيال القادمة، تطوير خدمات المدينة (والتي تتمثل خدمات النقل – خدمات مرافق المياه والطاقة –قطاعات الصناعات التحويلية – الاتصالات)، تدعيم كافة وظائف الوقاية وتحقيق آليات فعالة ومتوازنة وتنظيمية وحكومية، خاصة آليات التعامل مع الكوارث سواء كانت كوارث طبيعية أو صناعية، مثل معالجة آثار تغير المناخ [598].

595 Harrison, C., Eckman, et all," Foundations for Smarter Cities", IBM Journal of Paraszczak, J., & Williams, P. (2010). Research and Development, 54(4). date to visit,2-8-2021, Available at: https://ieeexplore.ieee.org/document/5512826

596 Washburn and Usman Sindhu, " Helping CIOs Understand "Smart City" Initiatives", February 11, 2010, P 5. date to visit,2-8-2021, Available at: https://s3-us-west-2.amazonaws.com/itworldcanada/archive/Themes/Hubs/Brainstorm/forrester_help_cios_smart_city.pdf

597- م عبد الله محمد العقيل،" المدن والمباني"- مجلة العلوم والتقنية- الرياض- مدينة الملك عبد العزيز للعلوم والتقنية، سنة (28)، عدد (111)، رجب 1435 – مايو 2014، ص 4.

598- د أحمد محمود يسري، م طاهر عبد السلام حامد وآخرون " صياغة المفهوم العمراني للمدن الذكية"، المرجع السابق ص 61،62.

تعريف الباحث المدن الذكية: 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.

ثانياً ركائز المدن الذكية: إن الحديث عن ركائز المدن الذكية في حقيقته يثير بلا شك الحديث عن جوانب تلك المدن وأبعادها ومكوناتها والتي لو توافرت في المدينة لارتقت تحت مسمى المدن الذكية، لذا فالواقع العملي لتلك المدن ومن خلفه خبراء تكنولوجياتها يشهد وبحق تبايناً واضح واختلاف 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 [599]،حلول الطاقة الذكية (Smart energy solutions) : ، حلول السلامة والأمن الذكية Smart) (safety and security solutions: ، كفاءة البنية التحتية والنقل Efficient) (infrastructure and transportation،الحوكمة الإلكترونية-E)

599 Anto OusephJuly," The 5 Pillars of a Smart City", July 12, 2017. date to visit,2-8-2021, Available at: https://www.quest-global.com/5-pillars-smart-city/

(governance:،تكنولوجيا المعلومات والاتصالات Information and communication technology).

وهناك بعض من تقارير الخبراء انتهت إلى (10) ركائز للمدن الذكية[600] هي:

الحوكمة (Governance)، الاقتصاد(Economy)، البنى التحتية (Efficient infrastructure and transportation)، الموهبة (Talent)، التمويل (Funding): التنقل (Mobility)، البيئة (Environment): السلامة العامة (Public safety): الصحة العامة (Public health): أنظمة الدفع الذكية (Payment systems).

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[601]، 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، حركة المرور الذكية / النقل الذكي، البيئة الذكية، الاقتصاد الذكي، الحوكمة الذكية، الحياة الذكية، وذلك على النحو التالي:

المواطن الذكي (Smart citizens): هو التحسين المستمر لقدرات ومؤهلات المواطن في جميع مراحل حياته ومهنته مع نظام تعليمي متنامٍ، لتحقيق جودة الموارد البشرية، من أجل الاستجابة لطلب العمل في سوق عمل متكيف ومرن سريع التغير في مجتمع مرتبط بالمدن الذكية.

600 ALICE CRUICKSHANK."10 pillars of a smart city", 12 Dec 2018, date to visit,2-8-2021, Available at: https://placetech.net/strategy/10-pillars-of-a-smart-city/

601 Ministry of Science and Technology (MOST), Vietnam," The main pillars of smart cities and consultation to choose the right pillars to develop and build smart city", Monday, 22/02/2021. date to visit,2-8-2021, Available at: 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

حركة المرور الذكية / النقل الذكي (Smart traffic, Smart transportation): 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 (Smart environment): ترتبط المدينة الذكية ارتباطًا وثيقًا بمفهوم المدينة البيئية، وهو المفهوم الرئيسي للمدينة الخضراء، والبيئة الذكية تُعني ضمان الأمن البيئي للبنية التحتية الاجتماعية ومواطنيها 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 ، وتطوير المهارات لمنع وتخفيف الآثار البيئية السلبية على الأنشطة الاقتصادية، لتحقيق هدف الحفاظ على التوازن البيئي.

الاقتصاد الذكي (Smart Economy): هو الاقتصاد الذي يقوم على الابتكار، وروح المبادرة، والإنتاجية العالية، والمرونة مع سوق العمل، والانفتاح على التعاون الدولي والإقليمي، والقدرة على التغيير، فالاقتصاد الذكي اقتصاد جديد قائم على المعرفة، تكون فيه القوة الدافعة للتنمية هي الابتكار وتكنولوجيا المعلومات الحديثة التي تشمل المنافسة العالمية، وتكنولوجيا الابتكار، والتحسين التنظيمي المستمر.

الحوكمة الذكية (Smart Governance): 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 والحلول المتاحة على مستوى المناطق المحلية.

الحياة الذكية (Smart life): تتضمن إنشاء نظام فعال للأماكن العامة عالية الجودة في المناطق الحضرية، مساحة حضرية جذابة لكل فرد، فأحد أهداف الحياة الذكية يتمثل في خلق مساحة 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 -انترنت 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

ثالثاً خصائص المدن الذكية:

يرى البعض[602] 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.

602 United Nations Commission on Science and Technology for Development, "Issues Paper On Smart Cities and Infrastructure", Prepared

كما اجتهد بعض الفقه في بيان خصائص المدن الذكية من خلال بيان الفوائد المرتبطة بتطوير المدن الذكية[603]، وذلك على النحو التالي:

1-المدن الذكية تتمتع بفاعلية أكبر في صنع القرار استنادًا إلى البيانات الضخمة: فقد أتاحت التطورات في البيانات الضخمة والأجهزة المتصلة للمدن الوصول إلى كمية هائلة من المعلومات لم تكن متوفرة سابقًا، وتحليلها - واستنباط رؤى هادفة وقابلة للتنفيذ بسهولة ، لا سيما في الظروف شديدة الخطورة، والجدير بالذكر أن البيانات الضخمة وإنترنت الأشياء (IoT) توفر إمكانيات لا حصر لها لتمكين اتخاذ قرارات أقوى، مما يحسن حياة السكان من خلال خفض التكاليف وتحسين الخدمات[604].

2 -التوسع في الخدمات الرقمية: التوسع في الخدمات الرقمية في المجتمعات يجعل المدن الذكية أكثر جاذبية للمقيمين ويعزز تجربة المدينة المتصلة، جنبًا إلى جنب مع نهج التخطيط من القاعدة إلى القمة، فتساعد هذه التقنيات الذكية على زيادة المشاركة المدنية والثقة في مسؤولي البلدية.

3- مجتمعات أكثر أمانًا (Safer Communities) المدينة الذكية أكثر أمانًا لأنها يمكن أن تستفيد من التقدم التكنولوجي، وتساعد متابعة الشراكات بين القطاعين العام والخاص في الحد من النشاط الإجرامي، فقد ساعد استخدام أجهزة الاستشعار

---

by the UNCTAD secretariat,11-13 January 2016, P 9-10, date to visit,6-8-2021, Available at:
https://unctad.org/system/files/official-document/CSTD_2015_Issuespaper_Theme1_SmartCitiesandInfra_en.pdf

603 Tiziana Campisi, Alessandro Severino, et all, "The Development of the Smart Cities in the Connected and Autonomous Vehicles (CAVs) Era: From Mobility Patterns to Scaling in Cities", Infrastructures Journal,8 July 2021, MDPI, Basel, Switzerland. P 2-4, date to visit,6-8-2021, Available at:
https://www.mdpi.com/2412-3811/6/7/100
file:///C:/Users/DrEmad1PC/Downloads/infrastructures-06-00100-v3.pdf

604 Silva, B.N.; Khan, M.; Han, K. 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, Volume 107, June 2020, Pages 975-987. date to visit,6-8-2021, Available at:
https://www.sciencedirect.com/science/article/abs/pii/S0167739X17305174

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، **يُضاف إلى ذلك أن ما تضمنه** أنظمة التحكم عن بعد من منح المستخدمين مزيدًا من التحكم في ظروف معيشتهم.

4 -تقليل البصمة البيئية (Reduced Environmental Footprint) 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، على سبيل المثال يمكن أن يوفر نشر مستشعرات جودة الهواء حول المدينة بيانات لتتبع لحظات الذروة من انخفاض جودة الهواء، وتحديد أسباب التلوث وتوفير البيانات التحليلية التي يحتاجها المسؤولون لتطوير خطط العمل والتخفيف ، لا سيما في المجال الطبي.

5 -تحسين النقل (Improving Transport) 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، فتمكّن التقنيات الذكية المدن من تقديم خدمة أفضل لمواطنيها على الرغم من النمو السكاني السريع في كثير من الأحيان، فتعمل تقنيات مثل إشارات المرور الذكية على تحسين تدفق حركة المرور وتخفيف الازدحام خلال ساعات الذروة، كما تسمح تقنيات النقل الذكية الأخرى مثل الإدارة الذكية لمواقف السيارات للمدن بالاستفادة من تدفقات الإيرادات الإضافية، كما يمكن أن تُساعد استخدام التطبيقات وأجهزة الاستشعار (خاصة خلال المراحل الحرجة مثل الأوبئة) في إدارة قطاع النقل والخدمات المقدمة للمستخدمين.

6 -حقوق ملكية رقمية أكبر (Greater Digital Equity) يمكن لتقنية المدن الذكية أن تخلق بيئة أكثر إنصافًا للمواطنين إذا تم نشر خدمات عالية السرعة ومنخفضة التكلفة مثل نقاط اتصال Wi-Fi العامة الموضوعة بشكل استراتيجي في المدينة.

7 -فرص جديدة للتنمية الاقتصادية New Opportunities for Economic Development

من خلال توفير منصة بيانات مفتوحة مع إمكانية الوصول إلى معلومات المدينة، يمكن للشركات اتخاذ قرارات مستنيرة من خلال تحليل البيانات من تقنيات المدن الذكية المتكاملة.

8 -كفاءة الخدمات العامة (Efficient Public Services) 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 (Improving Infrastructure) 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 (Increased Workforce Engagement)تعتبر القوة العاملة عالية الكفاءة معيارًا أساسيًا لتحقيق مدينة ذكية تتسم بالكفاءة، تساعد تطبيقات التقنيات الذكية في تخفيف عبء المهام اليدوية التي يواجهها العديد من موظفي المدينة يوميًا.

11 -تكامل النقل (Transport Integration) يتم تنفيذ الاختيار النموذجي للنقل من خلال نشر المنصات الرقمية مثل التنقل كخدمة والنقل عند الطلب، التي تسمح للمستخدم بتصور الطرق الممكنة والمختلفة لوسائل النقل مع الأخذ في الاعتبار الحلول المستدامة والفعالة من حيث التكلفة، فتسمح هذه المنصات للعديد من الشركاء بتبادل ومشاركة البيانات لاتخاذ قرارات بشأن خدمات التنقل.

المبحث الأول: مكافحة الجرائم والحد من ارتكابها في المدن الذكية

تمهيد: لدراسة مكافحة الجرائم والحد من ارتكابها في المدن الذكية يتطلب أن نستعرض أولاً تجارب دول العالم في مجال المدن الذكية، خاصة أهم التجارب العالمية في مجال

المدن الذكية وفقاً لمؤشر المدن الذكية (2020)، وهي الدول الرائدة في هذا المجال وفقاً لهذا المؤشر مثل سنغافورة -هلسنكي – زيورخ- أو سلو - كوبنهاجن - أمستردام – نيويورك – هونج كونج ثم تجارب دولة الإمارات العربية المتحدة في مجال المدن الذكية، وذلك للتعرف على طبيعة تلك المدن والجرائم المرتبطة بها، و بيان دور الشرطة الذكية لضبط تلك الجرائم والحد من ارتكابها في تلك المدن ، خاصة في الولايات المتحدة الأمريكية وسنغافورة ودولة الإمارات، وذلك كله من خلال مطلبين على النحو التالي:

المطلب الأول: تجارب دول العالم في مجال المدن الذكية

أولاً أهم التجارب العالمية في مجال المدن الذكية وفقاً لمؤشر المدن الذكية (2020)[605]:

أصدر معهد التنمية الإدارية IMD، بالتعاون مع جامعة سنغافورة للتكنولوجيا والتصميم Singapore University for Technology and Design (SUTD) تقريراً في سبتمبر (2020) يتضمن مؤشراً لترتيب المدن الذكية لعام (2020)، مع التركيز على الدور الذي لعبته التكنولوجيا في مدن العالم الذكية في عصر كوفيد (COVID-19)، والأخذ في الاعتبار هذا العامل في ترتيب قائمة المدن الذكية، فقد شهدت بعض المدن انخفاضًا في ترتيبها في القائمة العالمية للمدن الذكية مثل نيودلهي ومومباي وحيدر أباد ، بينما شهدت بعض المدن الذكية مثل مدينة أبوظبي صعوداً في ترتيب قائمة المدن الذكية، فقد كان ترتيبها في مؤشر (2019) رقم (56) وصعدت في مؤشر (2020) إلى رقم (42) في القائمة، فشهدت صعود (14) درجة في ترتيب قائمة المدن الذكية، وكذلك مدينة دبي الذكية شهدت هي الأخرى صعوداً في الترتيب، فقد كان ترتيبها رقم (45) في مؤشر (2019) وصعدت في ترتيب قائمة مؤشر المدن الذكية (2020) إلى (43) بصعود (2) درجة، وكذلك مدينة نيويورك

605 Institute for Management Development IMD, Smart City Index 2020, A tool for action, an instrument for better lives for all citizens, September 2020, P7-10. date to visit,10-8-2021, Available at: https://www.imd.org/smart-city-observatory/home/ file:///C:/Users/DrEmad1PC/Downloads/smart_city_index2021.pdf

فقد كان ترتيبها في القائمة في مؤشر (2019) (38) وصعدت في مؤشر (2020) إلى المركز العاشر، بينما تصدرت Singapore سنغافورة القائمة.

فقد جاءتSingapore سنغافورة في المركز الأول، ثم مدينة Helsinki هلسنكي في المركز الثاني، ومدينة Zurich زيورخ في المركز الثالث، ومدينة Auckland أوكلاند في المركز الرابع، ومدينة Oslo أوسلو في المركز الخامس، ومدينة Copenhagen كوبنهاجن في المركز السادس، ومدينة Geneva جينيف في المركز السابع، ومدينة Taipei تايبيه في المركز الثامن، ومدينة Amsterdam أمستردام في المركز التاسع، ومدينة New York نيويورك في المركز العاشر، وسوف نقدم موجز بسيط عن طبيعة بعض تلك المدن بالقدر الذي يتناسب مع أساسيا هذا البحث وجوهره والهدف منه وذلك على النحو التالي:

1-سنغافورة Singapore: تعد دولة سنغافورة المدينة الواقعة في جنوب شرق آسيا ثاني أكثر دول العالم كثافة سكانية، حيث يبلغ عدد سكانها حوالي (8000) شخص لكل كيلومتر مربع، ولمواجهة تزايد النمو السكاني لجأت الحكومة إلى التطورات الرقمية لزيادة الإنتاجية في اقتصاد متقدم بالفعل، من خلال رؤية Smart Nation الأمة الذكية في عام (2014) التي تهدف إلى جمع المعلومات رقميًا من جميع أنحاء المدينة باستخدام أجهزة استشعار مرتبطة بصناديق التجميع، ويتم إرسال البيانات التي تم جمعها حول حجم حركة المرور أو نشاط المشاة إلى الوكالات المناسبة لتحليلها واتخاذ إجراءات في تقديم الخدمات، فلدى المدينة ما يقرب من (95) في المائة من المنازل الذكية المتصلة، إضافة إلى المصادر المفتوحة للمعلومات التي توفر للمواطنين والقطاع الخاص الاستفادة الكاملة من البيانات لأسباب شخصية أو تجارية، فقد تم دمج التقنيات الذكية في الإسكان من خلال إطار يراعي التخطيط والبيئة والمباني والمعيشة، فعلى سبيل المثال يقوم المهندسون بتحليل تدفق الرياح، وتغلغل الطاقة الشمسية، والمناطق المظللة لتحسين تصميم وإنشاء مبانٍ جديدة، وبحلول عام (2022)، تخطط

الحكومة لتنفيذ إنارة ذكية وموفرة للطاقة لجميع الطرق العامة، وتركيب الألواح الشمسية على أسطح منازل (6000) مبنى[606].

كما أعلنت سنغافورة في عام (2021) عن خططها لمدينة ذكية بيئية جديدة خالية تمامًا من المركبات، تقع هذه المدينة المخطط لها في تينجا في المنطقة الغربية من سنغافورة، وستكون موطنًا لخمس مناطق سكنية تضم (42000) منزل، بالإضافة إلى مناطق آمنة للمشاة وراكبي الدراجات. [607].

2- هلسنكي Helsinki: حددت هلسنكي (عاصمة فنلندا) لنفسها هدفًا يتمثل في أن تصبح محايدة للكربون بحلول عام (2035) وثبت فعلاً أنها في طريقها للوصول إلى ذلك الهدف، ففي عام (2017) تمكنت المدينة من خفض الانبعاثات بنسبة (27٪)، كما أن هناك هدف آخر تعمل هلسنكي على تحقيقه وهو تقليل انبعاثات حركة المرور بنسبة (69٪) في غضون ثلاثة عقود بحلول عام (2035)، مع اتخاذ تدابير مثل تحويل أسطول حافلات المدينة بالكامل إلى الكهرباء وتوسيع شبكات المترو وشبكات شحن السيارات الكهربائية، نظرًا لأن التدفئة تمثل أكثر من نصف انبعاثات هلسنكي، كما تركز المدينة على تنفيذ تدابير كفاءة الطاقة أثناء عمليات التجديد، والتي يمكن أن تقلل الانبعاثات من المباني بنسبة (80٪)، فضلاً عن دمج المزيد من استخدام الطاقة المتجددة في مباني المدينة[608].

3- زيورخ Zurich: بدأت زيورخ بمشروع إنارة الشوارع فقدمت المدينة سلسلة من مصابيح الشوارع التي تكيفت مع مستويات حركة المرور باستخدام أجهزة الاستشعار، مما أدى إلى زيادة سطوعها أو تعتيمها وفقًا لتلك المستويات، كما مكّن المشروع من

606 John Kosowatz, "Top 10 Growing Smart Cities", The American Society of Mechanical Engineers(ASME), Feb 3, 2020. date to visit,10-8-2021, Available at:
https://www.asme.org/topics-resources/content/top-10-growing-smart-cities
607OLIVIA LA," Top 7 Smart Cities in the World", JUL 2021. date to visit,10-8-2021, Available at:
https://earth.org/top-7-smart-cities-in-the-world/
608 OLIVIA LA," Top 7 Smart Cities in the World", Op.cit. date to visit,10-8-2021, Available at:
https://earth.org/top-7-smart-cities-in-the-world/

توفير الطاقة بنسبة تصل إلى (70٪) منذ ذلك الحين، وشملت أضواء الشوارع الذكية الخاصة بها جميع أنحاء المدينة، كما أنشأت زيورخ مجموعة كبيرة من التقنيات الحسية التي يُمكنها جمع البيانات البيئية، وقياس تدفق حركة المرور، مع توافر WIFI ، ومن ثم أثبت نظام إدارة المباني الذكي الذي يربط بين تدفئة المدينة والكهرباء والتبريد، فعاليته[609].

4- أوسلو Oslo: تتبنى أوسلو استخدامًا واسعًا لأجهزة الاستشعار للتحكم في الإضاءة والتدفئة والتبريد، فتهدف المدينة إلى خفض الانبعاثات بنسبة (36) بالمائة بحلول عام (2020) وما يصل إلى (95) بالمائة بحلول عام (2030)، عن طريق خلق فرص في تطوير السيارات الكهربائية والشبكة الذكية وتكنولوجيا شحن المركبات الكهربائية، فهناك أكثر من (2000) محطة شحن للسيارات الكهربائية، مع إعفاء أصحابها دفع ضريبة المبيعات ومنحهم مواقف مجانية للسيارات وشحن ونقل على العبّارات، كما أعلنت النرويج عن خطط لبناء مدينة ذكية مستدامة على مساحة (260) فدانًا بالقرب من مطار أوسلو لتطوير مجتمعات تعتمد على التكنولوجيا، مصممة ليتم تشغيلها بالطاقة المتجددة فقط وإعادة بيع الفائض إلى الشبكة، فتعمل الأنظمة المستندة إلى أجهزة الاستشعار على تشغيل الإضاءة التلقائية للشوارع والمباني جنبًا إلى جنب مع إدارة النفايات والأمن[610].

5- مدينة كوبنهاجن Copenhagen: بدأت العاصمة الدنماركية نحو التنمية الذكية المتكاملة مع سياساتها البيئية الصارمة، فقد حصلت حاضنة Copenhagen Solutions Labعلى جائزة في عام (2017) لنظام يراقب حركة المرور وجودة الهواء وإدارة النفايات واستخدام الطاقة، ويربط أنظمة وقوف السيارات وإشارات المرور والمباني والقياس الذكي وأنظمة الشحن للمركبات الكهربائية لتوجيه حركة المرور في الوقت الفعلي وتحسين استخدام الطاقة وفقًا لأسعار الوقود وحركة المرور

609 OLIVIA LA,", Op.cit. date to visit,10-8-2021, Available at: https://earth.org/top-7-smart-cities-in-the-world/.

610 John Kosowatz, "Top 10 Growing Smart Cities", Op.cit. date to visit,10-8-2021, Available at: https://www.asme.org/topics-resources/content/top-10-growing-smart-cities,

والطقس، ويعمل نصف سكان المدينة على ركوب الدراجات، و يستخدم راكبوا الدراجات تطبيقًا تم تطويره من أجل توجههم عبر شوارع المدينة ويخبرهم بمدى السرعة التي يحتاجون إليها للدواسة للحصول على الضوء الأخضر التالي، كما يقيس المسافة المقطوعة بالدورة والسعرات الحرارية المحروقة[611].

6- أمستردام Amsterdam تبنت المدينة الهولندية التكنولوجيا الذكية، وأنشأت قاعدة بيانات مفتوحة تضم (12000) مجموعة بيانات تم الحصول عليها من كل منطقة حضرية، من خلال IoT Living Lab ، وهي منطقة تبلغ مساحتها (3700) متر مربع مزودة بإشارات تدعمIoT ، يمكن للمستخدمين الوصول إلى البيانات باستخدام أجهزة Bluetooth تستخدم المنارات LoRaWan ، وهو بروتوكول من آلة إلى آلة، لإرسال حزم البيانات إلى مسافات تصل إلى ثلاثة كيلومترات، ويستخدم العديد من السكان الدراجات لكن منصات مشاركة السيارات تجمع بين السائقين والركاب، وتنقل المركبات المستقلة السائقين عبر خمسة تقاطعات بين محطة مترو أنفاق ومجمع مكاتب، وتتميز أمستردام أيضًا بإضاءة ذكية مع مصابيح LED عاكسة للضوء، ومع ذلك يمكن للمشاة وراكبي الدراجات استخدام تطبيق لزيادة الإضاءة عند المرور وتخفت الأضواء بعد مرورهم[612].

7-نيويورك New York: وضعت حكومة المئات من أجهزة الاستشعار الذكية وشبكات واسعة منخفضة الطاقة في العديد من المناطق، لجمع البيانات التي ساعدت في إدارة جمع القمامة ومراقبة حاويات النفايات المزودة بأجهزة استشعار، والتي تُرسل الإشارات وتنقل المعلومات إلى أطقم التخلص في جميع أنحاء المدينة عندما تكون تلك الحاويات ممتلئة، كما تحل أكشاك الشحن عبر الإنترنت محل أكشاك الهواتف العامة لتمكين الاتصال بالإنترنت، واستخدمت إدارة الشرطة البرامج المستندة إلى الويب من Hunch Lab والتي تستخدم بيانات الجريمة التاريخية ونمذجة التضاريس وغيرها

611 John Kosowatz, '', Op.cit. date to visit,10-8-2021, Available at: https://www.asme.org/topics-resources/content/top-10-growing-smart-cities.

612 John Kosowatz, '"', Op.cit. date to visit,10-8-2021, Available at: https://www.asme.org/topics-resources/content/top-10-growing-smart-cities

من المعلومات للتنبؤ بالجريمة والاستجابة لها مما أدى إلى انخفاضًا ملحوظًا في جرائم العنف[613].

8-**هونج كونج** Hong Kong: في عام (2017) تم إطلاق أكثر من (70) مبادرة منها "الحكومة الذكية" و"الاقتصاد الذكي"، ومع بداية عام (2019) أعلن سكرتير هونغ كونغ للابتكار والتكنولوجيا عن دفع حكومي كبير لتسريع خدمات المدن الذكية، من خلال سلسلة من المبادرات أهمها شاشة لوحة أجهزة القياس للمدينة المتوافقة مع الجوّال، حيث يتم استخدام البيانات المستقاة من الإدارات الحكومية المختلفة لعرض الصور في الوقت الفعلي والخرائط والأيقونات والرسوم البيانية للمعلومات مثل متوسط سرعة حركة المرور في مختلف المناطق والأنفاق، بالإضافة إلى درجة الحرارة أو هطول الأمطار أو توفر مواقف للسيارات، مع تعزيز الأمن الرقمي بمقاييس بيو مترية مثل التعرف على الوجه أو الصوت[614].

ثانياً تجارب دولة الإمارات العربية المتحدة في مجال المدن الذكية: تُعد دولة الإمارات العربية المتحدة من الدول الرائدة في تحقيق التنمية المستدامة، لسعيها الدؤوب إلى تحقيق التوازن بين التنمية الاقتصادية والاجتماعية، واعتمادها المتزايد على الطاقة النظيفة وتدعيم التنمية الخضراء، فضلاً عن تعزيز توفير جودة الكهرباء والمواصلات والاتصالات حتى ارتقت مكانتها بين دول العالم في الخدمات الذكية[615]، بعد تحقق

613 John Kosowatz, "", Op.cit. date to visit,10-8-2021, Available at: https://www.asme.org/topics-resources/content/top-10-growing-smart-cities.

614 John Kosowatz, Op.cit. date to visit,10-8-2021, Available at: https://www.asme.org/topics-resources/content/top-10-growing-smart-cities.

615- وقد شهدت بكل تلك المنجزات تقارير عالمية دولية، فقد حصلت دولة الإمارات على المرتبة (7) عالمياً، كما ورد في تقرير هيئة الأمم المتحدة حول استطلاع الحكومة الإلكترونية تاريخ القياس 2020، وفقاً للمؤشر العالمي للبنية التحتية للاتصالات، وحصلت دولة الإمارات على المرتبة (8) عالمياً كما ورد في تقرير هيئة الأمم المتحدة حول استطلاع الحكومة الإلكترونية تاريخ القياس 2021، وفقاً لمؤشر الخدمات الإلكترونية(الذكية) تحت مسمى بيئة مستدامة وبنى تحتية متكاملة، كما حصلت على المرتبة (11) عالمياً كما أورده البنك الدولي تاريخ القياس 2021، وفقاً لمؤشر الأداء اللوجستي تحت مسمى بيئة مستدامة وبنية تحتية متكاملة، كما حصلت على المرتبة (12) عالمياً كما أورده المنتدى الاقتصادي العالمي – في تقريره التنافسية العالمية تاريخ القياس 2020، كما حصلت على المرتبة (8) عالمياً كما أورده المنتدى الاقتصادي العالمي – تقرير التنافسية العالمية تاريخ القياس 2020، وفقاً لمؤشر جودة النقل الجوي تحت مسمى بيئة

وتوافر بنية تحتية ذكية متطورة للمطارات والموانئ والطرق وغيرها من مرافق البني التحتية، ولضمان استمرارية التنمية المستدامة سعت دولة الإمارات إلى تطوير العديد من المدن الذكية المستدامة خاصة مدينة أبوظبي ومدينة دبي ومشروعات مدن أخرى في طريقها لتحقيق نموذج المدن الذكية، مثل مشروع زايد للمدن الذكية والتي أطلقته دائرة التخطيط العمراني والبلديات بأبوظبي (2018)، والذي يقع ضمن الخطة الخمسية للمدن الذكية والذكاء الاصطناعي (2018-2022)، ويهدف إلى إدارة عناصر البنية التحتية بتقنية انترنت الأشياء، لتحقيق بنية تحتية عالمية المواصفات، وكذلك واحة دبي للسليكون (DSCO) ومدينة دبي الجنوب ومدينة زهرة الصحراء بدبي، وغيرها من المبادرات والمشاريع.

مدينة أبو ظبي الذكية: تُعد مدينة أبو ظبي من المدن المستدامة الذكية وقد شهدت صعوداً في ترتيب قائمة المدن الذكية وفقاً لمؤشر المدن الذكية (2020) تحت رقم (42) في القائمة، ، حيث كان ترتيبها في المؤشر السابق لـ (2019) تحت رقم (56)، ومن ثم فشهدت صعود (14) درجة كما بينا، وذلك للجهود المستمرة نحو تطوير استدامتها الذكية والتي جاءت من خلال سلسلة من المبادرات الذكية والمشروعات، أهمها مبادرة" سياسة المرة الواحدة" للخدمات الحكومية في أبوظبي، بقيام المتعاملين بتقديم بياناتهم مرة واحدة فقط للجهات الحكومية، عبر منصة (TAMM) "تم"[(616)] التي تديرها هيئة أبوظبي الرقمية، بحيث يتم تخزين بياناتهم ومشاركتها بين الجهات الحكومية عبر المنصة الرقمية الحكومية المتكاملة والمختصة بتوفير وتبادل البيانات الرقمية بين الجهات الحكومية، لتمكين المتعاملين مواطنين ومقيمين من الوصول إلى

مستدامة وبنية تحتية متكاملة، وهو مؤشر مركب يقيس مرتبة الدولة في جودة النقل الجوي ومدى توافقها مع المعايير الدولية.

-حكومة دولة الإمارات – بيئة مستدامة وبنية تحتية متكاملة- رؤية 2021- تاريخ الزيارة 15-8-21 https://www.vision2021.ae/%D8%A7%D9%84%D8%A3%D8%AC%D9%86%D8%AF%D8%A9-%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A%D8%A9-2021/list/environment-circle.

616 https://www.tamm.abudhabi/ar-AE/about-tamm.تاريخ الزيارة 15-8-21

https://www.tamm.abudhabi/ar-AE/تاريخ الزيارة 15-8-21

مجموعة شاملة من الخدمات الحكومية الإلكترونية وإنجازها عبر نقطة اتصال واحدة في أي وقت وفي أي مكان في إمارة أبوظبي، دون الحاجة إلى التردد على مختلف الجهات الحكومية، ومن ثم تقديم خدمات أسهل وأسرع مع تقليص الوثائق المطلوبة من المتعاملين مع ضمان الشفافية والخصوصية، كما أنه من بين المبادرات التي أطلقتها حكومة أبوظبي أيضاً "مبادرة سداد" وهي أحدث منصة موحدة للدفع الرقمي في سهولة ويسر وأمان لجميع الخدمات الحكومية في إمارة أبوظبي للمتعاملين التي تمكنهم من إتمام عمليات الدفع، والمصالحة، والتسويات، والتقارير، والتدقيق، فضلاً عن تمكينهم من القيام بعملية دفع واحدة لخدمات متعددة، وكذلك للجهات الحكومية ذاتها بمنحها منصة رقمية موحدة للدفع، ومبادرة نظام "عنواني" وهو نظام يعتمد على أحدث التقنيات الذكية المتطورة مثل خدمة رموز استجابة سريع (QR) على لافتات الطرق والمباني والتطبيقات الذكية للهاتف المتحرك، والتي توفر معلومات بالغة الدقة عن المواقع المطلوب تحديدها، فضلاً عن أن رمز الاستجابة السريع (QR) الذي يوفر للجمهور أيضاً واجهة لتطبيقات ذكية ومزودة بالمعلومات الأساسية حول الأسماء الخاصة بالشوارع ومعلومات أخرى، كما أطلق مركز أبوظبي للأنظمة الإلكترونية والمعلومات منصة ذكية متطورة متكاملة متصلة مع (95) جهة حكومية بالإمارة تتمثل في تطبيق" حارس المدينة"، الذي يتيح إمكانية الإبلاغ عن الجرائم والقضايا التي تهمّ إمارة أبوظبي، عبر التقاط صور أو مقاطع فيديو أو تسجيلات أو مقاطع صوتية، مع قدرة برنامج التطبيق على تحديد موقع البلاغ بدقة باستخدام خرائط تفاعلية مدمجة، وإنشاء بلاغاً تلقائياً لدى مركز اتصال حكومة أبوظبي، الذي يقوم بدوره في تحويله إلى الجهات المعنية، فضلاً عن توفير WIFI مجاني في جميع سيارات الأجرة العاملة في الإمارة[617]، وتطبيقات ذكية أخرى مثل التطبيق الذكي (ADDC APP) الذي طورته شركة أبوظبي للتوزيع لتسهيل حصول العملاء على الخدمات التي تقدمها الشركة وسداد الرسوم المستحقة، وبطاقات مواقف (MAWAQIF) القابلة لإعادة

617- مبادرات أبو ظبي الذكية. تاريخ الزيارة 15-8-21
https://u.ae/ar-AE/about-the-uae/digital-uae/smart-abu-dhabi

التعبئة، خدمة للجمهور للتسهيل عليهم عند سداد رسوم المواقف العامة في إمارة أبوظبي[618].

مدينة مصدر (أبو ظبي) [619]: بعد تحقيق وتوافر بنى تحتية مستدامة في كافة إمارات الدولة بدأ مسار جعل مدينة مصدر مدينة ذكية في عام (2006) وفق خطة رئيسية تستند على ركائز ومكونات، تتضمن الاستغلال الأمثل للطاقة الشمسية لطبيعة تلك المدينة الجغرافية والمناخية، خاصة توافر أشعة الشمس لفترات طويلة، واستغلال حركة الهواء المنعش لتوفير برودة طبيعية أثناء ارتفاع درجة الحرارة في الصيف، وتصميم تلك المدينة وفقاً لأصول العمارة العربية التقليدية الممتزجة بالتكنولوجيا العصرية، وفق منظومة إنشائية من مباني محدودة الارتفاع والحجم، ومُثبت عليها الألواح الشمسية لتوليد الطاقة الكهربائية النظيفة من الطاقة الشمسية، مع توزيع المناطق السكنية بما يقلل من استخدام المواصلات، حتى تحقق لتلك المدينة تكامل جودة أوجه الحياة، ضمن منظومة بيئية ذكية استطاعت بها أن تستوعب التوسع الحضري المتزايد والسريع، وخفض استهلاك المياه والطاقة، والحد من التلوث وكذلك النفايات ومن ثم تحقيق البصمة الخضراء، فهي من المدن الرائدة لامتلاكها احدى أضخم التجهيزات الكهروضوئية في الشرق الأوسط، الأمر الذي جعلها ترتقي وتستضيف المقر الرئيسي للوكالة الدولية للطاقة المتجددة (إيرينا)- The International Renewable Energy Agency (IRENA) [620].

مدينة دبي الذكية: تُعد مدينة دبي من المدن المستدامة الذكية وقد شهدت صعوداً في ترتيب قائمة المدن الذكية وفقاً لمؤشر المدن الذكية (2020) تحت رقم (45) في

618- القنوات الذكية لتسديد رسوم الخدمات حكومية الإمارات. تاريخ الزيارة 15-8-21
https://u.ae/ar-ae/more/service-channels-and-modes-of-payment/payment-channels

619- حكومة الإمارات - البوابة الرسمية. تاريخ الزيارة 15-8-21
https://u.ae/ar-AE/about-the-uae/digital-uae/smart-sustainable-cities#efforts-in-abu-dhabi

620- الوكالةُ الدولية للطاقة المتجددة (IRENA) - منظمة حكومية دولية- تساعد وتدعم البلدان في التبني والانتقال لاستخدام كل أشكال الطاقة المتجددة، سواء طاقة حيوية – حرارية أرضية- طاقة كهرومائية – طاقة شمسية – طاقة رياح، لتحقيق تنمية مستدامة وطاقة أمنة ونمو اقتصادي منخفض الكربون. تاريخ الزيارة 15-8-21
https://www.irena.org/aboutirena

القائمة، حيث كان ترتيبها في المؤشر السابق لـ (2019) تحت رقم (43)، ومن ثم فشهدت صعود درجتين كما بينا، وقد بدأ مسار جعل المدينة مدينة ذكية في عام (2013) عندما أعلن **صاحب السمو محمد بن** راشد آل مكتوم عن مبادرة تحويلها إلى ذكية، وذلك من خلال إدارة كل المرافق والخدمات بالمدينة عبر الأنظمة الذكية والمتطورة والمترابطة، وقد وضعت حكومة دبي استراتيجية لتحويل ألف خدمة حكومية إلى خدمات إلكترونية بحول عام (2017) لمؤسسات ومرافق البنى التحتية خاصة النقل والكهرباء والاتصالات وتخطيط المدن والخدمات المالية، بهدف جعل كافة المؤسسات والجهات الحكومية لتصبح جهة أو مؤسسة واحدة تقدم خدمات شاملة بأسلوب سهل وفعال للمتعاملين، عبر مسارات ثلاث تحققها هي حياة ذكية تتناول (مختلف القطاعات مثل قطاع النقل، الصحة، خدمات الطاقة، التعليم، المرافق العامة، الاتصالات)، ومسار اقتصاد ذكي يتناول (تطوير شركات ذكية، سوق أسهم ذكي، خدمة موانئ، وظائف ذكية)، ومسار السياحة الذكية المتمثل في تأشيرات الدخول والطيران، خدمات الفنادق الذكية، البوابات الذكية[621].

استراتيجية دبي الذكية (2021)[622]: ركائز خطة دبي (2021): تقوم على أربعة ركائز الركيزة الأولى هي السلاسة وتعني تقديم خدمات متكاملة للارتقاء بحياة الأفراد، والركيزة الثانية هي الكفاءة وتعني الاستخدام الأمثل لموارد الإمارة، الركيزة الثالثة الأمان وتعني التوقع والتنبؤ بالمخاطر وحماية الأفراد والمعلومات، الركيزة الرابعة التخصيص وتعني إثراء الجميع وذلك بتجارب وخبرات الحياة والأعمال.

أبعاد مدينة دبي الذكية: ستة أبعاد للمدينة تتمثل في الحياة الذكية - الاقتصاد الذكي - الحوكمة الذكية - التنقل الذكي - البيئة الذكية - الأشخاص الأذكياء.

621- حكومة الإمارات- البوابة الرسمية. تاريخ الزيارة 15-8-21
https://u.ae/ar-AE/about-the-uae/digital-uae/smart-sustainable-cities#efforts-in-abu-dhabi

622 Smart Dubai 2021, Preparing Dubai to embrace the future, now, WELCOME TO THE HAPPY CITY, date to visit,15-8-2021available at: https://2021.smartdubai.ae/

- استراتيجية دبي الذكية 2021 - حكومة الإمارات- البوابة الرسمية. تاريخ الزيارة 15-8-21
https://u.ae/ar-ae/about-the-uae/strategies-initiatives-and-awards/local-governments-strategies-and-plans/smart-dubai-2021-strategy

الأهداف الاستراتيجية لخطة دبي الذكية (2021): وضعت خطة دبي الذكية (2021) ستة أهداف استراتيجية لرسم خرائط أبعاد المدينة الستة، وتتمثل هذه الأهداف الاستراتيجية فيما يلي:

1- مدينة ذكية قابلة للحياة ومرنة: عن طريق تحقيق التمكين الكامل لتكنولوجيا المعلومات والاتصالات للبنية التحتية الحيوية والموارد وذلك لتعزيز (الكفاءة - التوافر - المرونة - قدرة الإمارة على الصمود)، ولتعزيز الالتزام والتعاون بين أصحاب المصلحة المتعددين في إمارة دبي، وذلك كله من خلال التخطيط التعاوني المتصل وبناء الوعي وتنمية قدرات وجاهزية الفرد والمجتمع، من أجل تقديم تجربة حضرية (متكاملة – ذكية – مستدامة)، لتحسين ترابط المدن لتبسيط أوجه الحياة.

2-اقتصاد تنافسي عالمي مُدَعم بالتكنولوجيا الحديثة المتطورة: اقتصاد تنافسي عالمي عن طريق الاستفادة من أحدث النظم والوسائل القائمة على تكنولوجيا الاتصالات والمعلومات من أجل تحويل الكيانات الاقتصادية الحيوية والاستراتيجية رقميا، وإرساء قواعد وآليات جديدة لتحقيق التنمية الاقتصادية، وخلق بيئة ريادية تدعمها الاستثمارات قائمة على الابتكار والتعاون والمشاركة والبحث والتطوير لرفع الإنتاجية، والنهوض بالتقنيات الناشئة، خاصة في براءات الاختراع، وذلك كله من خلال قوى عاملة ماهرة وذكية ومبتكرة، لتعزيز ريادة دبي لتكون أذكى مدينة في العالم.

3-مجتمع مترابط مع خدمات اجتماعية يسهل الوصول إليها: بالتأثير على حياة الأفراد في الإمارة المقيمين أو الزائرين من خلال رقمنة وتبسيط الوصول إلى الخدمات واستخدامها في الحياة اليومية لجعل الحياة أسهل، تحسين نوعية الحياة لدى الأفراد من خلال الاستفادة من التكنولوجيات الناشئة المتطورة، العمل على تنمية وتطوير المدينة من خلال المشاركة الفاعلة مع أصحاب المصلحة المتعددين.

4-نقل سلس من خلال منظومة نقل ذكي ذاتي التحكم: قائم على حلول تنقل ذكية ومبتكرة رائدة لتجربة نقل سلسة وآمنة في الإمارة، لرفع الكفاءة وزيادة الإنتاجية والقضاء على الازدحام المروري، لمساعدة السكان والزوار على الوصول إلى وجهاتهم بشكل أكثر أمانًا وسرعة وسعادة.

5 .بيئة نظيفة مستدامة بتكنولوجيا المعلومات والاتصالات المتطورة: لضمان استمرارية استدامة المدينة وجودة مواردها من ماء وهواء وطاقة وأرض، ومن ثم تقليل بصمة الكربون من أجل بيئة نظيفة وآمنة صحياً.

6- حكومة ذكية رقمية عالية الجودة والكفاءة: حكومة بدون زيارات تلغي الحاجة إلى الانتقال إليها من خلال توفير (100٪)خدمات عامة مؤهلة بواسطة القنوات الرقمية وتحقيق التبني الرقمي الكامل، حكومة غير ورقية، غير نقدية، مدفوعة بأحدث التقنيات.

ولقد قامت حكومة دبي بسلسة من المبادرات الذكية[623] لدعم واستدامة وتطوير التحول الذكي لمدينة دبي بلغت أكثر من (100) مبادرة ذكية، بعض هذه المبادرات كانت قبل إطلاق المشروع الأول لتحويل مدينة دبي إلى مدينة ذكية وذلك لدعم استدامة المدينة ولدعم تحولها إلى مدينة ذكية، منها مبادرة (تحديد الهوية بموجات الراديو)- (RFID) نظام سالك للتعرفة المرورية، ومبادرة " بطاقة نول الذكية" التي تُمكن حاملها من سداد تعريفة التنقل لوسائل نقل هيئة طرق ومواصلات دبي، الحافلات العامة- مترو دبي- الباص المائي – ترام دبي-خدمات المواقف مدفوعة الأجر، ومبادرة المحفظة الإلكترونية لهيئة الطرق والمواصلات التي أطلقتها الهيئة عام (2013)، والتي تضمن خاصية حفظ الأموال على حساب إلكتروني، مسبق الدفع بدلاً من استخدام وسائل الدفع النقدي وبطاقات الائتمان، لتأدية خدمات الهيئة، ومبادرة " تطبيق نظام رمز الاستجابة السريعة (OR code) والتي أطلقتها بلدية دبي في عام (2011) لربط أنظمة بلدية دبي بنظام واحد، من خلال توفير رقم ورمز لكافة أنواع المباني، ومن خلال هذا التطبيق يستطيع المستخدم أو المتعامل الدخول السريع لخدمات بلدية دبي والتعرف على كافة البيانات والمعلومات التي يرغب الحصول عليها سواء رقم الأرض، أو بيانات المالك، الاستخدام التخطيطي، رخصة البناء، التخطيط الصادر على الأرض، مخالفات الصحة والسلامة الواردة على المؤسسات الغذائية والصحية...إلخ

وهناك العديد من المبادرات التي أطلقتها حكومة دبي بعد إطلاق مشروع تحويل دبي إلى مدينة ذكية بهدف دعم استمرارية وتطوير المدينة لكي ترتقي إلى الريادة العالمية

623- مبادرات مدينة دبي الذكية - حكومة الإمارات- البوابة الرسمية. تاريخ الزيارة 15-8-21
https://u.ae/ar-ae/about-the-uae/digital-uae/smart-dubai

في مجال المدن الذكية أهمها مبادرة " نظام مكاني الذكي" أطلقته حكومة دبي في عام (2015) (نظام العنونة الذكي في مدينة دبي) من أجل تحديد المواقع بدقة، بالضغط على أي مبني مدرج على الخريطة الإلكترونية التفاعلية الخاصة بالتطبيق، التي تُظهر تظليل للحدود الخاصة بالمبنى مع تحديد مداخله الرئيسية بالمؤشرات التي تبين رقم مكاني لكل مؤشر، وكذلك مبادرة الدراجة الكهربائية الذكية الصديقة للبيئة لمساعدة دوريات الشرطة، والتي أطلقتها شرطة دبي عام (2014)، والعديد من المبادرات الذكية التي أطلقتها حكومة دبي والتي تتعلق بالتطبيقات الذكية التي تتيح وصول المتعاملين لخدمات المدينة وإنجاز المعاملات الحكومية وسداد الفواتير، ومبادرة تطبيق (Dubai Now)، الذي يوفر باقات خدمية للمتعاملين في العديد من المجالات مثل خدمات التعليم، الصحة، تأشيرات الإقامة، الأمن، قيادة المركبات، المواصلات العامة، العدل، فواتير مرافق الكهرباء والمياه والمواصلات، خدمات الأعمال، خدمة إسلام، ومبادرة "خدمة التأجير الذكي للمركبات"، لفتر قصيره لا تتجاوز (6) ساعات عبر تطبيق (Udrive) من خلال التسجيل في نظام التطبيق للحصول على الخدمة، الذي يتطلب إدراج كافة بيانات بطاقات الهوية ورخص القيادة والبطاقات الائتمانية وصورة شخصية.

ومن المبادرات الحديثة مبادرة "ختم (100) بالمائة لا ورقية" وأُطلقت هذه المبادرة تنفيذاً لاستراتيجية حكومة دبي للمعاملات الرقمية اللاورقية، بتحويل حكومة دبي إلى حكومة لا ورقية بحلول شهر ديسمبر (2021)، والتي تهدف إلى القضاء على المعاملات الورقية وتحويلها إلى معاملات رقمية، سواء المعاملات الداخلية التي تُجريها الحكومة مع مؤسساتها وجهاتها المختلفة، أو تلك المعاملات التي تُجريها الحكومة مع المتعاملين، ومن أجل المساهمة في توفير مليار ورقة سواء تستخدمها حكومة دبي في العام الواحد، وكذلك مبادرة "مركز خدمات 1" التي تم إطلاقها عام (2017) وتهدف إلى أن تحقق دولة الإمارات المركز الأول على مستوى العالم في مجال الخدمات الحكومية بحلول عام (2020)، وتعتمد مركز خدمات 1 على أحدث التقنيات في مجال الذكاء الصناعي، ومن خلال زيارة واحدة يستطيع المتعامل انجاز خدمات حكومية متكاملة عبر باقات خدمية تشترك فيها تلك الجهات الحكومية، كباقة

الزواج وباقة المولود الجديد وباقة التوظيف وخدمات أخرى تقدمها الموارد البشرية والتوطين متعلقة بالتوظيف.

المطلب الثاني: الشرطة الذكية لضبط الجرائم والحد من ارتكابها في المدن الذكية

سوف نتناول دراسة الشرطة الذكية لضبط الجرائم والحد من ارتكابها في بعض المدن الذكية لدول العالم ومن بينها دولة الإمارات العربية المتحدة، وذلك بالتركيز على دور الشرطة التنبئية للحد من ارتكاب الجرائم باعتبارها تقوم بدور جوهري ليس فقط في منع ارتكاب الجرائم بل في مكافحتها في تلك المدن، وذلك بالقدر الذي يتناسب مع طبيعة هذا البحث على النحو التالي:

أولاً وظائف جهاز الشرطة: وظائف الشرطة التقليدية ترتكز على محورين، المحور الأول وهو ما يسمي **بالشرطة التفاعلية** القائمة على استقصاء الجرائم وجمع الأدلة وتحقيقها، وهو ما يسمي بالإعداد للرد على ارتكاب الجرائم بضبطها وضبط مرتكبيها وأدلتها أو إنقاذ ضحاياها، والمحور الثاني وهو ما يسمى **بالشرطة التنبئية** القائمة على قيام إدارة الشرطة بجمع البيانات والمعلومات عن الجرائم المرتكبة وطرق ارتكابها ومرتكبيها وضحاياها من واقع السجلات والإحصائيات المدرجة، وهو ما يُعرف بالسجل التاريخي للجريمة، ثم القيام بتحليل تلك البيانات والإحصائيات للتنبؤ بما سوف يرتكب من جرائم، وقد تُسفر نتائج القيام بعملية التحليل عن التنبؤ عن تحديد الأماكن والأوقات التي تنطوي على مخاطر عالية لارتكب الجريمة، أو بتحديد الأفراد أو الجماعات الذين من المحتمل ارتكابهم جريمة، أو أن يكونوا ضحايا لجريمة ما، من خلال تحليل عوامل الخطر مثل أوامر القبض أو أنماط الإيذاء المرتكب.

ثانياً تعريف الشرطة التنبئية: وقد تعدد أراء الفقه في تعريف الشرطة التنبئية ومن ثم تعذر وجود إجماع للفقه حول تعريف موحد لها، وإن كان هناك التقاء بينهم حول مضمون وظيفتها، فقد عرفها Pearsall [624] بأنها" أخذ البيانات من مصادر متباينة

624 Pearsall, Beth," Predictive policing: The Future of Law Enforcement? ",. National Institute of Justice Journal, No 266: 16–19, 2010, P 16, U.S. Department of Justice, date to visit,20-8-2021, Available at: https://nij.ojp.gov/topics/articles/predictive-policing-future-law-enforcement

وتحليلها، ثم استخدام النتيجة للتنبؤ بالجرائم المستقبلية، ومنعها والاستجابة لها بشكل أكثر فعالية"، وعرفها Tim Lau بأنها" استخدام الخوارزميات لتحليل كميات هائلة من المعلومات، من أجل التنبؤ بالجرائم المحتملة في المستقبل والمساعدة في منعها[625]، كما عرفها Perry بأنها" تطبيق الأساليب التحليلية لا سيما التقنيات القابلة للقياس الكمي، لتحديد الأهداف المحتملة لتدخل الشرطة ومنع الجريمة أو حل الجرائم الماضية من خلال وضع تنبؤات إحصائية"[626]، وحاول البعض تقديم تعريف مبسط للشرطة التنبئية[627] بأنها" نموذج للشرطة يستخدم الجريمة التاريخية والبيانات الاجتماعية والديموغرافية من مصادر مختلفة، لتوقع جرائم المستقبل باستخدام تطبيقات الكمبيوتر المتطورة"، وعرفتها مؤسسة RAND بأنها" تطبيق تقنيات تحليلية لتحديد الأهداف الواعدة لتدخل الشرطة، بهدف الحد من مخاطر الجريمة أو حل الجرائم الماضية[628].

ومع تطور جرائم تكنولوجيا المعلومات والاتصالات المرتكبة ضد البنى التحية الذكية لأغلب دول العالم خاصة المدن الذكية في تلك الدول، تطور المشهد الشرطي وتغيرت

https://www.ojp.gov/pdffiles1/nij/230409.pdf

625 Tim Lau, "Predictive Policing Explained "April 1, 2020. date to visit,20-8-2021, Available at:
https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained

626 Perry, Walter L., et all," Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations", Washington, DC: RAND Corporation, 2013. date to visit,20-8-2021, Available at:
https://www.jstor.org/stable/10.7249/j.ctt4cgdcz
https://www.jstor.org/stable/10.7249/j.ctt4cgdcz.9?refreqid=excelsior%3Ad57b649ee2501bc13e91caf9564def32&seq=2#metadata_info_tab_contents

627 Ishmael Mugari, Emeka E. Obioha, "Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing", 20 June 2021, P3-4. date to visit,20-8-2021, Available at:
https://www.mdpi.com/2076-0760/10/6/234
file:///C:/Users/DrEmad1PC/Downloads/socsci-10-00234-v2.pdf

628 RAND Corporation," Predictive Policing, Forecasting Crime for Law Enforcement", RB-9735-NIJ (2013), P 1. date to visit,20-8-2021, Available at:
https://www.rand.org/content/dam/rand/pubs/research_briefs/RB9700/RB9735/RAND_RB9735.pdf

معه استراتيجية عمل إدارة الشرطة، من أسلوب عملها التقليدي التفاعلي إلى التركيز على العمل الشرطي الاستباقي القائم على منع الجريمة بدلاً من الرد عليها، من خلال استخدام وتوظيف تكنولوجيا المعلومات والاتصالات والبيانات والتقنيات التحليلية، من أجل تحديد الأماكن والأوقات المحتملة للجرائم المستقبلية، أو الأفراد المعرضين لخطر ارتكاب جريمة، أو أن يصبحوا ضحايا لها.

فالشرطة الذكية هي تلك القائمة على التطبيقات الذكية (انترنت الأشياء – الذكاء الاصطناعي – أجهزة الاستشعار الذكية- كاميرات الدوائر التلفزيونية المغلقة CCTV (cameras)-التقنيات اللاسلكية الخلوية والمنخفضة الطاقة واسعة النطاق (LPWAN)- خوارزميات وبرمجيات تحليل البيانات)، استطاعت توظيف تلك المقومات لخدمة العدالة الجنائية ، سواء بضبط الجرائم وملاحقة مرتكبيها، أومن الحد من ارتكابها في تلك المدن وجعلها أكثر أمناً، لأن المدن الذكية غير الآمنة ليست ذكية على الإطلاق ولا يمكن التنبؤ باستدامتها الذكية كما قررنا من قبل، ولقد أشارت إلى تلك الحقائق دراسة حديثة بأن التقنيات الذكية يمكن أن تساعد المدن على تقليل الجريمة بنسبة (30) إلى (40) في المائة، وتمكين أوقات استجابة أسرع بنسبة (20) إلى (35) في المائة لخدمات الطوارئ[629].

ثالثا تعريف الشرطة الذكية: اختلف الفقه في تعريف الشرطة الذكية[630] اختلاف يعكس وجهات النظر حول مفهوم الشرطة الذكية والهدف منها، ما بين اتجاه مضيق يُعرف الشرطة الذكية بالتركيز على استخدامها لتكنولوجيا المعلومات والاتصالات

629 Peter Sloly, "Emerging tech that can make smart cities safer High-tech still needs to be high-touch", Security & Justice series Deloitte's, 2021. date to visit,20-8-2021, Available at: https://www2.deloitte.com/ca/en/pages/public-sector/articles/emerging-tech-smart-cities-safer.html.

630 Ramolobi L.G. Matlala," Defining e-policing and smart policing for law enforcement agencies in Gauteng Province", The International Journal of Social Sciences and Humanities Invention, Volume 3 issue 12-2016-page no. 3058-3070ISSN: 2349-2031. date to visit,20-8-2021, Available at: https://valleyinternational.net/index.php/theijsshi/article/view/634 https://valleyinternational.net/index.php/theijsshi/article/view/634/619

ومفرداتها وتطبيقاتها الذكية، من أجل منع الجريمة ومكافحتها بطريقة فعالة لخلق شعور بالأمن والأمان داخل مجتمعات المدن الذكية، وما بين اتجاه موسع لمفهوم الشرطة الذكية يرى أنها مزيجًا من التنفيذ الذكي للابتكارات في تكنولوجيا ضبط الأمن مع تنفيذ استراتيجيات الشرطة الحالية الأخرى مثل الشرطة القائمة على الاستخبارات، والشرطة المجتمعية والشرطة الساخنة، والموجهة نحو المشكلات، فيجب أن يكون الهدف النهائي لتطبيق نموذج الشرطة الذكية هو منع الجريمة ومكافحتها، والاستفادة من الموارد من مختلف الجهات الفاعلة من خلال تكوين شراكات استراتيجية وتعزيز تعبئة المجتمع والمشاركة الفعالة في مبادرات منع الجريمة.

تعريف الباحث للشرطة الذكية: يرى الباحث أن الشرطة الذكية هي تلك القائمة على منظومات تكنولوجيا المعلومات والاتصالات ومفرداتها وتطبيقاتها الذكية، لمكافحة ارتكاب الجرائم والحد من ارتكابها، ولتنمية وتطور استدامة المدن الذكية.

والجدير بالذكر أن منظومات الشرطة الذكية الخاصة بتكنولوجيا المعلومات والاتصالات ومفرداتها قادرة على تحقيق أهدافها التفاعلية والتنبئية، لخلق شعور بالأمن والأمان وتحقيق السلامة العامة داخل مجتمعات المدن الذكية.

رابعاً الشرطة الذكية لمكافحة الجرائم والحد من ارتكابها في الولايات المتحدة الأمريكية[631]:

أ-الشرطة التنبئية في الولايات المتحدة الأمريكية:

الجدير بالذكر أنه إذا كانت مشاريع الشرطة التنبئية في الولايات المتحدة الأمريكية يتم تنفيذها من قبل إدارات الشرطة البلدية، إلا أنها تُنفذ من خلال شراكات رئيسية بينها وبين القطاع الخاص والوكالات الفيدرالية، وتُعد إدارة شرطة لوس أنجلوس (LAPD)من أوائل الإدارات التي بدأت العمل مع الوكالات الفيدرالية في عام (2008) لاستكشاف مناهج الشرطة التنبئية، فقد نفذت دائرة شرطة لوس أنجلوس

631 Tim Lau, "Predictive Policing Explained " Op.cit. date to visit,20-8-2021, Available at:
https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained

مجموعة متنوعة من برامج الشرطة التنبئية، مثل برنامج LASER الذي يحدد المناطق التي يُعتقد أن من المحتمل أن يحدث فيها عنف باستخدام الأسلحة النارية، وبرنامج PredPol الذي يحسب "النقاط الساخنة" ذات الاحتمالية العالية للجرائم المتعلقة بالممتلكات، وعلى الرغم من أنه تم إغلاق LASER في عام (2019) وإيقاف بعض أقسام الشرطة برامج PredPol الخاصة بهم، وذلك لظهور بعض المشاكل في تطبيق تلك البرامج، إلا أن لتلك البرامج أثبتت فاعلية الشرطة التنبئية في الحد من ارتكاب الجرائم.

كما بدأت إدارة شرطة نيويورك (NYPD) والتي تُعد أكبر قوة شرطة في الولايات المتحدة في اختبار برامج الشرطة التنبئية في وقت مبكر من عام (2012)، من خلال شراكات تنفيذية مع القطاع الخاص المتمثل في شركات Azavea و KeyStats و PredPol إلى أن طورت شرطة نيويورك خوارزميات الشرطة التنبئية الخاصة بها وبدأت في استخدامها في عام (2013)، وكانت تُغذي تلك الخوارزميات بالمعلومات والبيانات الخاصة بالشكاوي المتعلقة بسبع فئات جرائم كبرى، وحوادث إطلاق النار، ومكالمات (911) لإطلاق النار ، ونجحت تلك الخوارزميات التنبئية في الحد والمنع للعديد من الجرائم مثل عمليات إطلاق النار والسطو والاعتداءات الجنائية والسرقات الكبرى وسرقات المركبات، فضلاً عن استخدام تلك الخوارزميات في تعيين الضباط لمراقبة مناطق معينة.

وأدارت إدارة شرطة شيكاغو أحد أكبر برامج الشرطة التنبئية في الولايات المتحدة، فقد تم تجريب البرنامج لأول مرة في عام (2012)، والذي أطلق عليه (heat list) "قائمة الحرارة" أو قائمة الموضوعات الاستراتيجية (strategic subjects list,)، والذي بموجبه تم إنشاء قائمة بالأشخاص الذين لديهم خطورة إجرامية لارتكاب أعمال عنف باستخدام السلاح، وتحديد الأشخاص المعرضون لأن يكونوا ضحايا لتلك الجرائم، وعلى الرغم من أن ذلك البرنامج أثبت نجاحه، إلا أنه قد أثير حوله بعض الإشكاليات خاصة المتعلقة بالحقوق المدنية، واعتماده بشكل مفرط على سجلات الاعتقال لتحديد المخاطر حتى في حالة عدم وجود مزيد من أوامر الاعتقال أو اعتقالات لم تؤد إلى إدانات، فضلاً عن استهدافه مجتمعات ملونة، الأمر الذي ترتب عليه تأجيل البرنامج.

ومن مشاريع الشرطة التنبئية التي تم تبنيها من قبل إدارات إنفاذ القانون في الولايات المتحدة برنامج (RTM) لتحليل الجريمة، وذلك بالنظر إلى جغرافية مكان ارتكاب الجريمة لبيان عوامل الخطر البيئية المرتبطة بالجريمة ولتحديد المجالات التي يرتبط فيها تأثيرها المكاني على السلوك الإجرامي[632]، وكذلك برنامج (HunchLab) ويطلق عليه اسم "نظام إدارة الدوريات" لدعم الضباط في الدوريات، وقد تم تصميمه في الأجهزة المحمولة للسماح لضباط دوريات الشرطة بالاطلاع في الوقت الفعلي على المناطق التي من المحتمل أن تحدث فيها الأنشطة الإجرامية، ولقد أظهر البرنامج تأثيرًا إيجابيًا في الحد من الجريمة في شيكاغو وفيلادلفيا[633].

ب-الشرطة الذكية في الولايات المتحدة الأمريكية[634]:

تتضمن الشرطة الذكية في الولايات المتحدة الأمريكية العديد من التقنيات أثبتت فاعليتها في مكافحة الجرائم من خلال ضبطها وملاحقة مرتكبيها، من هذه التقنيات:

-برنامج التعرف على الوجه (Facial Recognition Software): فقد أثبت استخدام ذلك البرنامج نجاحه وفعاليته في العثور على المشتبه به في الكثير من الجرائم، فقد تمكن ضباط شرطة نيويورك من العثور على المشتبه به بالاغتصاب واعتقاله في غضون 24 ساعة من الهجوم باستخدام ذلك البرنامج، وتتوقع وزارة الأمن الداخلي الأمريكية أنه سيتم استخدامه على (97٪) من المسافرين بحلول عام (2023).

632 Caplan, Joel, et all, " Crime in Context: Utilising Risk, Terrain Modelling and Conjunctive Analysis of Case Configuations to Explore the Dynamics of Criminogenic Behaviour Settings", Journal of Contemporary Criminal Justice Volume 33, pp.133–151,2017. date to visit,20-8-2021, Available at: https://journals.sagepub.com/doi/10.1177/1043986216688814

633 Ferguson, Andrew," Predictive Policing Theory", American University, Washington College of Law Research 24: 2020–10, P 6-7, date to visit,20-8-2021, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3516382 file:///C:/Users/DrEmad1PC/Downloads/SSRN-id3516382%20(1).pdf

634 Erik Fritsvold,"12 Innovative Police Technologies", University of San Diego 2021. date to visit,20-8-2021, Available at: https://onlinedegrees.sandiego.edu/10-innovative-police-technologies/

- أجهزة القياسات الحيوية: (Biometrics): التي تستخدم في الكشف عن غموض بعض الجرائم والتعرف على مرتكبيها من خلال استخدام بصمة الصوت، وقزحية العين وبصمات الكف، وعروق الرسغ، وتحليل المشي وحتى ضربات القلب، فقد قام (FBI) مكتب التحقيقات الفيدرالي بتطوير قاعدة بيانات تسمى (the Next Generation Identification system) (NGI) نظام تحديد هوية الجيل التالي، من أجل دعم مؤسسات العدالة الجنائية بتزويدها بأكبر وأكفأ مستودع إلكتروني في العالم لمعلومات التاريخ الحيوي والجنائي.

-تقنية الصوت (Voice Technology): وتُعد واحدة من أحدث الابتكارات التي يتم دمجها في سيارات الشرطة وهي تقنية الأوامر الصوتية الجديدة التي تُمكن الضباط من التحكم في العديد من الوظائف في سياراتهم أثناء القيادة وأداء واجبات الدوريات الأخرى.

-الروبوتات (Robots) تستخدم الشرطة الذكية في الولايات المتحدة الأمريكية الروبوتات الذكية خاصة الجيل التالي من الكاميرات الروبوتية، لتقديم مراقبة مرئية وصوتية لمسرح جريمة قد يُشكل خطورة بالغة في طبيعته أو في الوصول إليه، تتعرض فيها سلامة الضباط البشريين للخطر، فلتلك الروبوتات القدرة الواسعة في جمع المعلومات والاتصالات وتلقي وإرسال تقارير الشرطة، فضلاً عن قيامها بدوريات في البنوك والمطارات والمدارس ومناطق أخرى.

-جرس الباب بالفيديو Video Doorbells: تم تثبيت أجراس أبواب الفيديو من قبل الآلاف من مالكي المنازل كوسيلة لتعزيز أمن المنزل ومنحهم راحة البال، كما تساعد أنظمة المراقبة هذه في إنفاذ القانون عندما يتعلق الأمر بالتحقيقات الجنائية، في عام (2020) وحده قدمت وكالات إنفاذ القانون في جميع أنحاء الولايات المتحدة أكثر من (20000) طلب في العام الماضي للحصول على لقطات تم التقاطها بواسطة أجراس باب الفيديو من Ring وكاميرات أمنية منزلية أخرى، كما أبرمت أمازون - التي تمتلك - Ring أكثر من (2000) اتفاقية تعاونية مع وكالات إنفاذ القانون، والتي تسمح لهم تلقائيًا بمطالبة مالكي الكاميرات بالتصوير الأمني الخاص بهم إذا كانوا يعيشون بالقرب من مسرح الجريمة .

-تقنية (ShotSpotter): والتي تستخدم لتحديد موقع إطلاق النار بدقة، وتقوم المدن بتطبيق تقنية ShotSpotter التي تستخدم أجهزة استشعار لاكتشاف إطلاق النار بتحليل البيانات ونقلها على الفور إلى الشرطة، مما يمكنهم من الوصول إلى مكان الحادث بسرعة أكبر من أي وقت مضى، وقد صرحت الشركة المصنعة لتلك التقنية ومقرها كاليفورنيا أنه يمكن أن تكلف الخدمة (40.000) دولار إلى (60.000) دولار لكل ميل مربع سنويًا للمدن لتغطية المناطق عالية الجريمة، وأنها تستطيع "اكتشاف أكثر من (90٪) من حوادث إطلاق النار مع تحديد موقع دقيق في أقل من (60) ثانية لتحسين أوقات الاستجابة بشكل كبير"، وفي عام (2017) وبالتحديد في فريسنو كاليفورنيا استخدمتها الشرطة للقبض على مرتكب جرائم قتل من خلال تتبع تحركات القاتل والقبض عليه في (4) دقائق و(13) ثانية.

-التصوير الحراري Thermal Imaging: أصبح التصوير الحراري أداة تقنية مهمة للشرطة مفيدة بشكل خاص في الظروف المظلمة، فتستخدم كاميرات الصور الحرارية التي يتوفر بعضها كوحدات صغيرة محمولة باليد، التصوير بالأشعة تحت الحمراء للكشف عن الحرارة المنبعثة من أشياء مثل البشر والحيوانات، ولتقديم "صورة حرارية" أو "خريطة حرارية" للبيئة المعنية، كما يمكن استخدام تلك التقنية لتتبع حركة المشتبه بهم في مبنى مظلم، وحالات الإنقاذ للحياة في ظروف صعبة يصعب فيها الرؤية.

-الذكاء الاصطناعي Artificial Intelligence يستخدم الذكاء الصناعي كأداة فعالة في مكافحة الجرائم من خلال إنترنت الأشياء (IoT) حيث يتم إنشاء وجمع وتحليل كميات هائلة من البيانات لاستخلاص رؤى قابلة للتنفيذ، هذه العملية تستغرق وقتًا طويلاً بشكل لا يصدق وتكلفة عالية عندما يقوم بها البشر، كما يتم استخدام الذكاء الاصطناعي لدعم العديد من تقنيات الشرطة الأخرى مثل ShotSpotter ، والتعرف على الوجه والقياسات الحيوية، كما يتم استخدامه أيضًا لرسم خرائط الجريمة من خلال تحليل البيانات التي يمكن استخدامها لتحديد المناطق عالية الجريمة بشكل أكثر فاعلية ، بحيث يمكن للشرطة مراقبتها عن كثب ونشر موارد إضافية، فضلاً عن استخدامه في التنبؤ بالجريمة باستخدام ما يسمى بخوارزميات "deep learning"التعلم

العميق" ، حيث يمكن للمبرمجين تدريب أجهزة الكمبيوتر على تحليل البيانات من مجموعة واسعة من المصادر والفئات للتنبؤ فعليًا بالوقت والمكان المحتمل لحدوث الجرائم، وهذا يسمح لقيادات الشرطة بتخصيص الموارد بشكل صحيح ويزيد من احتمالية تواجد الضباط في المكان المناسب في الوقت المناسب.

-تقنية Automatic License Plate Recognition **(ALPR)**

تستخدم الشرطة هذه التقنية التي تمكّن محصلي الرسوم من المسح الضوئي لأرقام التسجيل والحروف الموجودة على لوحة الترخيص الخاصة وجمعها لتحصيل الرسوم المقررة، فضلاً عن استخدامها في مكافحة الجرائم والحد من ارتكابها فيمكن لكاميرات ALPRتحديد طراز السيارات ولونها وتمييز الأحرف الفردية على لوحات الترخيص حتى في الإضاءة المنخفضة والطقس السيئ، فتمكّن تلك التقنية الشرطة من القدرة على تتبع تحركات السيارة بمرور الوقت، والكشف عن تفاصيل مكان وجودها، ومن ثم قد تساعد في القبض على المجرمين.

-كاميرات محسّنة يمكن ارتداؤها على الجسم Enhanced Body-Worn Cameras

هذه الكاميرات المحسّنة ذات الدقة العالية يستخدمها ضباط الشرطة في الشارع أو أثناء تأدية مهامهم الصعبة، للحصول على مجالات رؤية واسعة وصوت أكثر وضوحًا ومقاومة عالية للظروف البيئية مثل البرودة الشديدة، وموثقة بفيديوهات تُسجل السيناريوهات وكل التحركات في الشارع، ومتصلة بالأنظمة الذكية داخل سيارة الشرطة ومنظومة القيادة، تزودهم أول بأول بتقارير وتنبيهات عند حدوث أي طوارئ في المكان أو لدى ضابط الشرطة الذي يرتديها، كما قد تكون مزودة بقدرات التعرف على الوجه.

-طائرات بدون طيار Drones تُعرف أيضًا باسم المركبات الجوية غير المأهولة (UAVs)، ويتم استخدامها بشكل متزايد من قبل الشرطة للحصول على نقاط مراقبة جوية للعمل في مسرح الجريمة، وجهود البحث والإنقاذ، وإعادة بناء الحوادث، ومراقبة الحشود والمزيد، كما يمكن تزويد تلك الطائرات بعض التقنيات الذكية الخاصة

بالتصوير الحراري أو برنامج رسم الخرائط ثلاثي الأبعاد لتقديم دقة مُحسَّنة عبر نظام تحديد المواقع العالمي (GPS) للمناطق التي يتم مسحها، أو تزويدها بكاميرات تكبير، مما يجعلها ذات قيمة لا تصدق لتقديم معلومات قابلة للتنفيذ في الوقت الفعلي في المواقف عالية الخطورة و "المسلحة والخطيرة".

خامسا الشرطة الذكية لمكافحة الجرائم والحد من ارتكابها في سنغافورة:

تعد سنغافورة وهي دولة يبلغ عدد سكانها حوالي 5.7 مليون نسمة واحدة من أكثر الدول أمانًا في العالم، وفقًا لاستطلاع أجرته مؤسسة غالوب Gallup poll عام (2019)، وجاءت في المركز الأول في مؤشر ترتيب المدن الذكية حول العالم (2020) كما ذكرنا، لكونها من الدول الرائدة في نجاح منظومة الشرطة الذكية والتنبئية، فقد امتزجت Singapore Police Force (SPF) قوة شرطة سنغافورة وغيرها من وكالات الفريق المحلي بأحدث التقنيات والتطبيقات الذكية[635] للحفاظ على سلامة الجمهور ومن ثم الحد من ارتكاب الجرائم، فلديها مثلاً اسطول من روبوتات الدوريات المستقلة والطائرات بدون طيار وسيارات الشرطة الذكية، فقد أطلقت SPF سيارة شرطة ذكية Smart Police Cars جديدة في أواخر العام الماضي، تُعرف باسم سيارة الاستجابة السريعةFast Response Car ، لتعزيز استجابة ضباط الخطوط الأمامية، فهذه السيارات مزودة بنظام التعرف الآلي على لوحة الأرقام، مما يساعد الضباط على اكتشاف "المركبات ذات الأهمية" أثناء التنقل، كما أنها مزودة بنظام تسجيل فيديو يلتقط لقطات عالية الجودة بزاوية (360) درجة ويبثها مباشرة إلى مركز قيادة عمليات الشرطة، ومن المقرر طرح هذه السيارات الجديدة تدريجياً واستبدال الأسطول الحالي بحلول عام (2024).

كما تم نشر الطائرات بدون طيار والروبوتات للقيام بدوريات في مرافق عزل (Covid-19)، وساعدت الروبوتات المستقلة متعددة الأغراض All Terrain

635 Shirley Tay, "How Singapore is reimagining policing with smart cars and drones"19 APR 2021. date to visit,20-8-2021, Available at: https://govinsider.asia/cyber-futures/how-singapore-is-reimagining-policing-with-smart-cars-and-drones-singapore-police-force/

Autonomous Robots، على ضمان مسافة آمنة وتقليل تعرض عمال الخطوط الأمامية للفيروس، وبث الفيديو في الوقت الفعلي إلى مركز قيادة عمليات الشرطة للمساعدة في اتخاذ القرار، وقد صرح وزير الداخلية السنغافوري K Shanmugam ك.شانموغام بأن سنغافورة تهدف إلى امتلاك أكثر من (200) ألف كاميرا شرطة بحلول عام (2030) على الأقل، أي أكثر من ضعف العدد الحالي من الكاميرات المنتشرة في جميع أنحاء الدولة، وأن لديها قوانين صارمة وأدوات المراقبة الخاصة بها تشمل أكثر من (90) ألف كاميرا شرطة مثبتة بالفعل في جميع أنحاء المدينة[636].

وساعدت شبكة كاميرات الشرطة المنتشرة في سنغافورة في مكافحة الجريمة، فقد قامت شرطة سنغافورة بتركيب أكثر من (80000) كاميرا في جميع أنحاء البلاد، لتشمل (10000) كاميرا في مجلس الإسكان والتنمية (HDB) ومواقف السيارات متعددة الطوابق (MSCPs) كجزء من برنامج يعرف باسم PolCam. PolCam وهي مبادرة عامة متعددة السنوات لتعزيز سلامة وأمن الأحياء والأماكن العامة باستخدام شبكة كبيرة من كاميرات الشرطة، ونظراً لارتفاع جرائم الاحتيال عبر الانترنت بنسبة (27%) في (2020) بالمقارنة بعام (2018) وتضاعف نسبة الخسائر الناجمة عن تلك الجرائم، (خاصة جرائم الوصول غير المصرح به لمعاملات حسابات الأفراد عبر الإنترنت ، وعمليات الشراء غير المصرح بها باستخدام بطاقات الائتمان / الخصم ، ورسائل التصيد الاحتيالي التي حصلت على معلومات شخصية حساسة، وعمليات الاحتيال في التجارة الإلكترونية والائتمان مقابل الجنس وعمليات الاحتيال على القروض، و كانت أهم خمس منصات رقمية مستخدمة في عمليات الاحتيال في التجارة الإلكترونية هي Carousell (1239) حالة، ومنصة Facebook, (602) حالة، ومنصة Shopee (279) حالة، ومنصة Lazada, (197) حالة، ومنصة Instagram (103) حالة، لذا فقد أثارت تلك الجرائم قلق SPF فأطلقت برنامج ScarAlert.sg ليقدم دعم حقيقي وفعال للحد من

636 Reuters Staff, "Singapore to double police cameras to more than 200,000 over next decade", AUGUST 4, 2021. date to visit,23-8-2021, Available at: https://www.reuters.com/article/us-singapore-security-cameras-idAFKBN2F50IW.

تلك ارتكاب الجرائم ومكافحتها، لما يتضمنه من معلومات عن أحدث عمليات الاحتيال في سنغافورة، ويسمح للجمهور بمشاركة خبراتهم ، ويمكن للضحايا أيضًا الإبلاغ عن عمليات الاحتيال إلى خط المساعدة الخاص بمكافحة الاحتيال [637].

سادساً الشرطة الذكية لمكافحة الجرائم والحد من ارتكابها في دولة الإمارات العربية المتحدة:

تستخدم وزارة الداخلية بدولة الإمارات أحدث وسائل تكنولوجيا المعلومات والاتصالات لمكافحة الجرائم والحد من ارتكابها، ومن ثم تأمين وحماية بنيتها التحتية الذكية المتطورة في مختلف القطاعات والمرافق، ولتحقيق الأمن والسلامة لكل متواجد على أرض الدولة مواطن أو مقيم.

فاستطاعت منظومة الشرطة الذكية من خلال القيام بوظائفها سواء التفاعلية أو التنبئية أن تكون قادرة على مكافحة الجريمة والحد من ارتكابها، وذلك من خلال منظومتها الذكية القائمة على أنظمة الذكاء الاصطناعي، كاميرات الدوائر التلفزيونية المغلقة، التقنيات اللاسلكية الخلوية والمنخفضة الطاقة واسعة النطاق،أجهزة الاستشعار الذكية، خوارزميات وبرمجيات تحليل البيانات، الروبوتات الذكية، الطائرات بدون طيار، وغيرها من الأجهزة والتقنيات الحديثة المتطورة، وسوف نتناول بعض منها بالقدر الذي يتناسب مع جوهر البحث والهدف منه.

فقد أطلقت حكومة دبي وحكومة أبوظبي وحكومة الشارقة وغيرها من حكومات إمارات الدولة العديد من البرامج والأنظمة والتطبيقات الذكية التي كان لها دور فعال في مكافحة الجرائم والحد من ارتكابها[638]، فقد أطلق مركز المتابعة والتحكم التابع لحكومة أبو ظبي نظام عين الصقر للمراقبة والتحكم في مدينة أبو ظبي، وهو نظام مركزي متكامل للمراقبة والتحكم، يربط بين جميع أجهزة المراقبة الحديثة المرئية

637 Singapore 2020 Crime & Safety Report, U.S .Overseas Security Advisory Council, 4-6-2020. date to visit,23-8-2021, Available at: https://www.osac.gov/Country/Singapore/Content/Detail/Report/7f0cc2bc-ba9b-4485-b58b-1861aa0f8fc3.

638- أنظمة الأمن والسلامة - حكومة الإمارات- البوابة الرسمية، تاريخ الزيارة 23-8-2021 https://u.ae/ar-AE/information-and-services/justice-safety-and-the-law/maintaining-safety-and-security/security-systems-.

المنتشرة بالمدينة، ومنها آلاف الكاميرات المثبتة بالشوارع والمنشآت والمرافق الحيوية، يستقبل منها البث الحي لحظة بلحظة ويقوم بتحليل البيانات والمعلومات والصور الواردة من البث، وإرسال تنبيهات محددة في الحالات التي تستدعي تدخل الجهات المعنية، أو إنذارات ذكية تستدعي سرعة التعامل والوصول إلى الحدث، وذلك كله عبر واجهته الإلكترونية، كما يدعم نظام عين صقر عملية رصد المخالفات المرورية، والتفاعل الحي مع حوادث السير للتعامل معها، فضلاً عن ضبط الطرق ورصد مظهر المدينة وتسجيل أي متغيرات أو ظواهر، سواء تعلقت بسلوكيات مؤثرة أو بتجمعات بشرية في غير الأماكن المخصصة لها وغيرها من المتغيرات والظواهر التي يمكن أن تحدث، كما استخدمت شرطة أبوظبي أجهزة القياس الحيوية مثل نظام بصمة العين IRIS للتعرف على هوية الأشخاص بالتقاط صورة لقزحية العين وتخزينها ومعالجتها وإعطاء البيانات المطلوبة في ثوان معدودة، ومن ثم ساعدت تلك التقنية في الكشف عن غموض الكثير من الجرائم وضبط المطلوبين أو المشتبه فيهم، وكذلك الدوريات ذاتية القيادة التي أطلقتها حكومة دبي، وهي مركبات شرطية ذاتية القيادة تعمل من خلال برمجيات خاصة ومزودة بكاميرات ورادارات استشعار، تُمكنها من إرسال كافة البيانات والمعلومات والصور والفيديوهات والتقارير المتعلقة بمنطقة تجوالها إلى غرف عمليات القيادة الشرطية ، فضلاً عن خاصية المحادثات الصوتية مع غرف مراكز القيادة، وخاصية إطلاق الطائرات بدون طيار إلى الأماكن التي يتعذر الوصول إليها، ومن ثم تستطيع تلك الدوريات التعرف على جميع الأشخاص في منطقة التجوال، ومتابعة الأشخاص المشتبه فيهم وكشف الأجسام المشبوهة، كما أطلقت شرطة دبي الدراجة الذكية هوفر سيرف التي تعمل بالكهرباء وتتسع لرجل شرطي واحد، ويمكن التحكم فيها عن بعد، ويمكن لهذه الدراجة الذكية الطيران على ارتفاع خمسة أمتار ولمسافة (6) كيلوا مترات ولمدة (25) دقيقة وبسرعة (70) كم/ س وأن تحمل (300) كم، ويتم استخدامها في حلات الازدحام المروري وحالات الطوارئ.

كما أطلقت شرطة أبو ظبي خدمة أمان الذكية وهو قناة أمنية عالية السرية تعمل على مدار (24) ساعة، يتم تعامل الجمهور معها عبر بريدها الإلكتروني أو رقمها المجاني الذي يستقبل المكالمات أو الرسائل النصية، لتمكين الجمهور من المشاركة المجتمعية

في مكافحة الجرائم والحد من ارتكابها، من خلال الإبلاغ عن أي جرائم أو حوادث مشبوهة أو ضارة، بتوصيل المعلومات الأمنية والمرورية والمجتمعية لشرطة أبو ظبي، أيضا خدمة الأمين التي أطلقتها شرطة دبي والتي تُعد هي الأخرى قناة للمشاركة المجتمعية لمكافحة الجرائم والحد من ارتكابها، من خلال بلاغات الجمهور عبر وسائل التواصل الاجتماعي ورقم هاتف مجاني، وخدمة نجيد لاستقبال البلاغات سراً التي أطلقتها القيادة العامة لشرطة الشارقة كقناة للمشاركة المجتمعية عبر أرقام مجانية خاصة لمكافحة الجرائم والحد من ارتكابها، والإبلاغ عن أي معلومات تساهم في حفظ الأمن واستقرار الوطن، ومن المشاركات المجتمعية التي أطلقتها القيادة العامة لشرطة الشارقة أيضا خدمة أمني من أمن جاري التي تهدف إلى مشاركة الجمهور(الجيران) الجهات الأمنية في حماية الأحياء السكنية بمدينة الشارقة أثناء سفر أصحابها أو غيابهم، عن طريق الإبلاغ عن أي جرائم أو تصرفات مشبوهة أو تعدي جنائي على مسكن الجار أثناء غيابه [639].

كما أطلقت شرطة دبي منصة eCrime للإبلاغ عن الجرائم السيبرانية، وأطلقت النيابة العامة الاتحادية التطبيق الذكي مجتمعي آمن لتمكين الجمهور من المشاركة المجتمعية في مكافحة الجرائم والحد من ارتكابها، عبر الصور والفيديوهات والتسجيلات الصوتية التي تتضمن الإبلاغ عن الجرائم، مع ضمان السرية التامة لهوية من قام بالإبلاغ[640]، وأطلقت القيادة العامة لشرطة دبي الشرطي الآلي الذكي ويُعد الأول في العالم من نوعه في العالم يستطيع كشف مشاعر الإنسان، وكذلك كشف حركة الأجسام، أيضاً التعرف على الإيماءات والإشارات عن بُعد، وقراءة وجه الإنسان لرصد تعبير الحزن والسعادة والابتسام، فضلاً عن خاصية التفاعل والدردشة والرد على كل الاستفسارات وتقديم التحية العسكرية، أيضا الروبوت الآلي للإنقاذ البحري التي أطلقته بلدية دبي لتحقيق السلامة العامة لشواطئ دبي، والذي يمكنه العمل في

639- تعزيز الأمن والسلامة - حكومة الإمارات- البوابة الرسمية، تاريخ الزيارة 23-8-2021
https://u.ae/ar-AE/information-and-services/justice-safety-and-the-law/maintaining-safety-and-security

640- السلامة السيبرانية والأمن الرقمي - حكومة الإمارات- البوابة الرسمية، تاريخ الزيارة 23-8-2021
https://u.ae/ar-AE/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security

أسوء الظروف المناخية التي يصعب على المنقذ البشري السباحة فيها، خاصة مع وجود الأمواج العالية أو تيارات بحرية الساحبة، ويستطيع إنقاذ أربعة إلى خمس أشخاص في آن واحد[641]، كما أطلق مركز أبوظبي للأنظمة تطبيق الذكي يسمى حارس المدينة، والذي يُعد منصة مجانية ذكية متكاملة لتحقيق المشاركة المجتمعية في مكافحة الجرائم والحد من ارتكابها، فضلاً عن الإبلاغ عن كافة القضايا التي تهم الإمارة واتصاله مع (95) جهة حكومية بأبوظبي، حيث يتضمن خاصية استقبال بلاغات الجمهور المرسلة بالتقاط الصور والفيديوهات والتسجيلات الصوتية، مع تحديد موقع البلاغ باستخدام خريطة تفاعلية مدمجة على وجه الدقة، وتسجيل بلاغ الجمهور تلقائياً في مركز الاتصال الخاص بحكومة أبو ظبي الذي يحوله إلى الجهات المختصة والمعنية[642].

إحصائيات الشرطة الذكية في ضبط الجرائم: والجدير بالذكر أن منظومة الشرطة الذكية لدولة الإمارات العربية المتحدة من خلال القيام بوظائفها التفاعلية والتنبئية قد استطاعت وبحق مكافحة الجرائم والحد من ارتكابها، ولقد ترجمت الإحصائيات الرسمية الصادرة عن الدولة تلك الحقائق، ففي عام (2018) سجلت إمارة دبي نسبة (99.5%) في كشف الجرائم من إجمالي البلاغات لديها وهي نسبة غير مسبوقة، كما ساعد استخدام التقنيات الذكية في منع ارتكاب الجرائم خاصة تقنية منظومة عيون التي تتيح مراقبة المساكن والشوارع على مدار الساعة والتي حققت صفر جريمة في تلك المناطق، كما أن منظومة كاميرات المراقبة الخاصة بالجهات الحكومية في الإمارة تدار عبر الذكاء الاصطناعي، وتركز على قطاعات رئيسية الجنائي و المروري والسياحي، مع توافر خاصية ربط تلك المنظومة بغرفة عمليات متطورة بإدارة الحد من الجريمة، وكذلك تقنية وجوه التي استطاعت رصد (87) مطلوباً و(507) مشتبه فيهم خلال ثلاث شهور، الأمر الذي ترتب علية انخفاض في مؤشر ارتكاب الجريمة،

641- الروبوت وتطبيقات الذكاء الاصطناعي - حكومة الإمارات -البوابة الرسمية، تاريخ الزيارة 23-8-2021
https://u.ae/ar-AE/about-the-uae/digital-uae/robotics-and-ai-applications

642- مبادرات أبو ظبي الذكية - حكومة الإمارات -البوابة الرسمية، تاريخ الزيارة 23-8-2021
https://u.ae/ar-ae/about-the-uae/digital-uae/smart-abu-dhabi

فانخفضت سرقة المساكن (3%)، والسرقة من المرافق العامة انخفضت (7%)، والحريق العمد (22%)، فضلاً عن انخفاض مؤشر القضايا المجهولة[643]، كما أظهرت الإحصائيات خلال خمس سنوات حتى 2018 انخفاض مؤشر الجرائم المقلقة بنسبة (38%)[644] وفي يناير (2021) بلغت نسبة كشف الجرائم في إمارة دبي (99.7%)[645]

المبحث الثاني: مظاهر جرائم الاعتداء على الأمن القومي السيبراني للبنى التحتية للمدن الذكية

تمهيد: لبيان مظاهر جرائم الاعتداء على الأمن القومي السيبراني للبنى التحتية للمدن الذكية، يتطلب الأمر أولاً بيان ماهية الأمن القومي السيبراني من خلال معرفة ماهية الأمن القومي وتطوره وماهية الأمن السيبراني ومؤشره العالمي، ومدى ارتباط الأمن القومي بالأمن السيبراني، وكيف أن ضعف منظومة الأمن السيبراني يُهدد منظومة الأمن القومي للدول، وأن الإرهاب السيبراني والحروب السيبرانية من أكبر التهديدات للأمن القومي للمدن الذكية، ثم بيان هجمات جرائم الأمن القومي السيبراني على البنى التحتية للمدن الذكية، والتي يُمكن أن تتخذ نموذج لجرائم الإرهاب السيبراني أو حروب سيبرانية؟، وجرائم الأمن القومي السيبراني التي تم ارتكابها على مرافق البنى التحتية للمدن الذكية (2020-2021) وأسباب تزايدها، ثم بيان الاستراتيجية التي وضعها الباحث لمكافحة جرائم الاعتداء على الأمن القومي السيبراني للبنى التحتية للمدن الذكية، وذلك كله من خلال مطلبين على النحو التالي:

643- جلاف جمال ، - الإدارة العامة للتحريات والمباحث الجنائية شرطة دبي – جريدة الإمارات اليوم، 6 مارس 2019، تاريخ الزيارة 23-8-2021
https://www.emaratalyoum.com/local-section/accidents/2019-03-06-1.1189029

644- اللواء المنصوري خليّل، شؤن البحث الجنائي لشرطة دبي – جريدة البيان، 5 مارس 2018، تاريخ الزيارة 23-8-2021
https://www.albayan.ae/across-the-uae/news-and-reports/2018-03-05-1.3202473

645 الفريق المري عبد خليفة، القائد العام لشرطة دبي – جريدة الخليج، 3 يناير 2021، تاريخ الزيارة 23-8-2021
https://www.alkhaleej.ae/2021-01-03/997.

المطلب الأول: ماهية الأمن القومي السيبراني

أولاً تطور مفهوم الأمن القومي للدول: أصبحت مرافق البنى التحتية لحكومات ومدن العالم قائمة على شبكات تقنيةُ المعلومات و الاتصالات، سواء كانت مرافق ومؤسسات صناعية أو عسكرية أو مؤسسات مالية خاصة قطاع البنوك أو مرافق النقل - المياه – الصحة -الطاقة، لذا فقد أصبحت مرافق الأمن القومي ومؤسساته مدرجة عبر ذلك الفضاء السيبراني، 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 أسرار ومعلومات وبيانات 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.

فلم تعد قضايا الأمن القومي للدول تقتصر على حماية حدودها الخارجية من التهديدات والإرهاب، بل تتضمن أيضًا قضايا جديدة مثل الجرائم السيبرانية والهجمات السيبرانية والجرائم الأخرى المرتبطة بالإنترنت، فمع تزايد وتيرة الجرائم السيبرانية تظل ضوابط الأمن السيبراني من أولويات 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، فعلى سبيل المثال يمكن أن تحدث انتهاكات خصوصية البيانات عندما يتم تسريب بيانات حساسة إلى

مصادر خارجية، أو حيث يسيء الموظفون الداخليون استخدام بيانات اعتمادهم ويستفيدون من وصولهم إلى هذه المعلومات، ولمواجهة مثل هذه التهديدات، يجب على الشركات التصرف بشكل استباقي من خلال استخدام تدابير شاملة لتأمين بياناتها وحماية عملياتها[646].

ثالثاً ماهية الأمن السيبراني:

عرَفه الاتحاد الدولي للاتصالات(International Telecommunication Union) (ITU) بأنه "هو مجموع من السياسات والأدوات والمفاهيم الأمنية المستخدمة لحماية بنى البيئة السيبرانية من أصول ومستخدمين" [647]، 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"[648].

رابعاً مؤشر الأمن السيبراني العالمي (Global Cybersecurity Index) (GCI) [649]: مؤشر يصدره الاتحاد الدولي للاتصالات (International

646 Dr. Nick Oberheiden. "Defending Against National Security Threats," The National Law Review, Volume XI, Number 254, September 11, 2021. date to visit,23-8-2021, Available at: https://www.natlawreview.com/article/defending-against-national-security-threats

647https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

648- الجريدة الرسمية الإماراتية، 13-8-2012.

649- ITU/BDT Cyber Security Programme, Global Cybersecurity Index (GCI), Guidelines for Member States, Version 0.9.04 September 2019. date to visit,23-8-2021, Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCI_V4_Guidelines_for_Member%20States.pdf

https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx#:~:text=As%20cybersecurity%20has%20a%20broad,(v)%20Cooperation%20%E2%80%93%20and%20then

(Telecommunication Union (ITU) وهو فرع من أجهزة الأمم المتحدة الخاص بتكنولوجيا الاتصالات والمعلومات (ICT)، وهو مؤشر ومرجع موثوق به لقياس مدى التزام الدول بالأمن السيبراني على المستوى العالمي، ويعتمد المؤشر على خمس من الركائز الأساسية، وتتمثل في (1) ركيزة تدابير قانونية، (2) تدابير التقنية، (3) التدابير التنظيمية، (4) بناء القدرات ، و(5) التعاون - ثم يتم تجميعها في النتيجة الإجمالية.

خامساً 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[650]، وفي تصريح لميروسلاف ميكور Miroslav

- يدعو قرار مؤتمر المندوبين المفوضين للاتحاد الدولي للاتصالات 130 (المُراجع في دبي 2018) الدول الأعضاء إلى "دعم مبادرات الاتحاد بشأن الأمن السيبراني، بما في ذلك مؤشر الأمن السيبراني العالمي (GCI)، من أجل تعزيز الاستراتيجيات الحكومية وتبادل البيانات والمعلومات وتعزيز ثقافة عالمية للأمن السيبراني ودمجها في صميم تقنيات المعلومات والاتصالات، ويهدف GCI إلى تقليل الفجوة المرئية في مستوى مشاركة الأمن السيبراني بين مختلف المناطق حول العالم، فضلاً عن استخدامه كمرجع من قبل الدول الأعضاء في الاتحاد والبلدان الأخرى لتحسين التزامها بالأمن السيبراني.

650- John Bull, 'You Hacked: Cyber-Security and the Railways', London Reconnections, May 12, 2017. date to visit,23-8-2021, Available at: https://www.londonreconnections.com/2017/hacked-cyber-security-railways/

(Micor) المتحدث باسم شرطة لودز أفاد أن ذلك الهجوم قد أحدث فوضى وخروج بعض عربات القطار عن مسارها وحدوث إصابات لدى بعض الركاب[651].

سادساً مخاطر التخزين السحابي للبيانات على الأمن القومي السيبراني:

1-مفهوم التخزين السحابي: التخزين السحابي هو وسيلة للشركات والمستهلكين لحفظ البيانات وتخزينها عبر الإنترنت، مع الاحتفاظ بملفاتهم مخزنة مع مزود الخدمات السحابية للوصول إليها عند الطلب على أي من أجهزتهم، مع إمكانية النسخ الاحتياطي لتلك البيانات واستردادها ومشاركتها بسهولة في أي وقت مع أي طرف مسموح له[652]، ويُعرّف التخزين السحابي بأنه نموذج إيداع البيانات حيث يتم تخزين المعلومات الرقمية مثل المستندات والصور ومقاطع الفيديو وغيرها من أشكال الوسائط على خوادم افتراضية أو سحابية يستضيفها طرف ثالث، مع سماح الوصول إليها عند الحاجة[653]، فالحوسبة السحابية هي تقديم خدمات الحوسبة حسب الطلب - من التطبيقات إلى التخزين وقوة المعالجة - عادةً عبر الإنترنت وعلى أساس الدفع أولاً بأول، فبدلاً من امتلاك البنية التحتية للحوسبة الخاصة بها أو مراكز البيانات، يمكن للشركات تأجير الوصول إلى أي شيء من التطبيقات إلى التخزين من مزود خدمة السحابة، وتتمثل إحدى فوائد استخدام خدمات الحوسبة السحابية في أنه يمكن للشركات تجنب التكلفة الأولية والتعقيد لامتلاك البنية التحتية لتكنولوجيا المعلومات الخاصة بها وصيانتها، وبدلاً من ذلك تدفع ببساطة مقابل ما تستخدمه عند استخدامها، وفي المقابل

651- John Leyden, 'Polish teen derails tram after hacking tram network', The Register, 11 Jan 2008. date to visit,23-8-2021, Available at:
https://www.theregister.com/2008/01/11/tram_hack/

652- JAKE FRANKENFIELD,"Cloud Storage "March 04, 2022. date to visit,12-3-2022, Available at:
https://www.investopedia.com/terms/c/cloud-storage.asp

653- Neha Pradhan Kulkarni, Chiradeep BasuMallick, "What Is Cloud Storage? Definition, Types, Benefits, and Best Practices" July 8, 2021. date to visit,12-3-2022, Available at:
https://www.toolbox.com/tech/cloud/articles/what-is-cloud-storage/

يمكن لمقدمي خدمات الحوسبة السحابية الاستفادة من وفورات الحجم الكبيرة من خلال تقديم نفس الخدمات لمجموعة واسعة من العملاء[654].

والجدير بالذكر أن الطرف الثالث الذي يقوم بتزويد الخدمات السحابية هي شركات عالمية كبرى تقوم باستضافة تلك البيانات، وتمتلك بنى تحتية متطورة لتكنولوجيا المعلومات والاتصالات، في مبنى مجهز بخوادم ضخمة مع انترنت فائق السرعة ومزودات للطاقة وكافة متطلبات الطوارئ للحفاظ على تلك الأجهزة والمعدات، ومثال لتلك الشركات:

Google Cloud Platform ،Amazon Web Services (AWS) (GCP)، Infrastructure-as-a-Service (IaaS)، وعلى الرغم من أن تلك الشركات قد توفر حماية خاصة لتلك البيانات المستضافة إلا أنها قد تتعرض لمزيد من التهديدات، مثل الإهمال البشري الذي يمكن أن يؤدي إلى فتح الطريق للوصول غير المصرح به إلى الخادم الخاص بصاحب البيانات، فضلاً عن فقدان البيانات وانتشارها عند ترحيل كميات كبيرة من البيانات إلى السحابة ومن ستكون هناك دائمًا فرصة لفقدان البيانات، أيضاً هجمات DoS وضخ أكواد لاقتحام الخادم السحابي والوصول إلى البيانات الشخصية للمؤسسة، وهجمات البرمجيات الخبيثة [655].

2- مخاطر التخزين السحابي لبيانات الحكومات الذكية:

استعانت أغلب الحكومات الذكية لمختلف دول العالم بالتخزين السحابي للبيانات والمعلومات الخاصة بمرافقها ومؤسساتها، الأمر الذي يُعرض أمنها القومي السيبراني

654- Steve Ranger, "What is cloud computing? Everything you need to know about the cloud explained", February 25, 2022. date to visit,12-3-2022, Available at:
https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud/

655- Zainap Al Mehdar, "Cybersecurity and Cloud Computing: Risks and Benefits", January 18, 2022. date to visit,12-3-2022, Available at:
https://rewind.com/blog/cybersecurity-and-cloud-computing-risks-and-benefits/

للعديد من المخاطر والتهديدات نورد بعض منها بالقدر الذي يتناسب مع طبيعة البحث في النقاط التالية[656]:

مخاطر تعدد المستأجرين للحوسبة السحابية:

تعتمد الحوسبة السحابية على تأجير البنية التحتية لمستخدمين آخرين بحيث يكون هناك العديد من العملاء الذين يتشاركون نفس البنية التحتية، فإذا حدثت مشكلات فنية من خلال الهجمات السيبرانية مثل Virtual Machine Monitor أو برنامج Hypervisor، المسؤول عن فصل الأجهزة الافتراضية، فقد يتم كشف بيانات العملاء لبعضها البعض.

صعوبة تحديد المسئول عن الخروقات الأمنية: لإخفاء هوية موظفي تكنولوجيا المعلومات المسؤولين عن بيانات العملاء في مراكز البيانات، ولتطبيق سياسة "الاعتماد المتبادل في الأمن" الأمر الذي يتسبب في فقدان تتبع الكيان أو الشخص المسؤول.

المشاكل القانونية: تنشأ التهديدات القانونية المتعلقة بالحوسبة السحابية من حقيقة أن مزود خدمة الحوسبة السحابية يخضع لسلطات قضائية وقانونية مختلفة في دول مختلفة في نفس الوقت؛ مثل دولة المستخدم ودولة مقدم الخدمة والدول التي تمر البيانات من خلالها، وتزداد الأمور تعقيدًا في حالات التناقض بين القوانين واللوائح في مختلف الدول فيما يتعلق بالحقوق، وحماية البيانات، وتشفير البيانات، وتدمير البيانات، والكشف عن البيانات لسلطات الدولة، وما إلى ذلك، ومن ثم تقف الدول عاجزة عن استكمال تحقيقاتها في قضايا مختلفة بسبب العوائق التشريعية المختلفة وسيادة الدول الأخرى.

656- Hedaia-t-Allah Nabil Abd Al Ghaffar, "Government Cloud Computing and National Security", Review of Economics and Political Science, ISSN: 2631-3561, 23 March 2020. date to visit,12-3-2022, Available at: https://www.emerald.com/insight/content/doi/10.1108/REPS-09-2019-0125/full/html

والجدير بالذكر أنه يتبين لنا أن منظومة التخزين السحابي لا تختلف في جوهرها عن منظومة تخزين بيانات الأمن السيبراني الوطني لأي دولة، ومن ثم تخضع لنفس تهديدات جرائم الأمن القومي السيبراني، وإن كان الاختلاف قد يرجع إلى حجم مساحة التخزين الخارق المدرج في التخزين السحابي، مع الأخذ في الاعتبار أن التخزين السحابي يتم من خلال استضافة شركات عالمية أجنبية لتلك البيانات خارج موقع الدولة الوطني وبما يحمله من مخاطر وتهديدات وخروقات وضغوط على تلك الشركات المستضيفة للبيانات من قبل أجهزة الأمن الوطني لتلك الشركات، وما قد يصاحبها من حصول تلك الأجهزة الأمنية على أذونات من محاكمها تُقدم إلى تلك الشركات للسماح لها بالاطلاع على تلك البيانات، أو قيام تلك الأجهزة الأمنية بمعاونة تلك الشركات المستضيفة للبيانات باستخدام برامج خاصة وبرمجيات خبيثة لاختراق تلك البيانات أو العبث بها أو تدميرها أو محوها، وما قد يُصاحبه من أضرار على الأمن القومي السيبراني للدولة صاحبة تلك البيانات.

سابعاً الإرهاب السيبراني والحروب السيبرانية أكبر التهديدات للأمن القومي للمدن الذكية:

أصبح الفضاء السيبراني وبما يتضمنه من مؤسسات ومرافق البني التحتية للدول قوة جذب كبيرة للاعتداء عليه من قبل الأفراد بارتكاب الجرائم الخاصة بتقنية نظم المعلومات، أو من قبل التنظيمات الإرهابية وهو ما يُعرف بالإرهاب السيبراني، أو من قبل الدول وأجهزتها الاستخباراتية والعسكرية وهو ما يُعرف بالحروب السيبرانية، لكونه هدفاً سهلاً وأمناً وغير مكلفاً وناجحاً في تحقيق أهداف المعتدي وفي ثوان معدودة.

ماهية 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[657]، وتُعرّف 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 [658]،كما حدد تقرير الدفاع السيبراني والأمن السيبراني الوطني لليابان الصادر في سبتمبر 2020 الإرهاب السيبراني[659] بأنه "أي هجمات تستخدم شبكات المعلومات والاتصالات والأنظمة الخاصة بالمعلومات وتؤثر على حياة الناس وأنشطتهم سواء كانت اجتماعية أو اقتصادية".

فالهجوم الإرهابي على مفردات البنى التحتية يترتب عليه أضرار بالغة للأمن القومي، فالأنظمة المصرفية والمالية يتم تحويلها رقميًا ومتصلة بالإنترنت بشكل متزايد، ومن ثم تعرضها إلى الهجمات الإرهابية كما قرر خبراء الأمن السيبراني قد يؤدي إلى عدم استقرار اقتصادي واسع النطاق، مما قد يتسبب في ركود أو كساد، كما أنه من خلال اختراق البنية التحتية للطاقة أو المرافق، يمكن أن يتسبب الإرهابيون في حدوث

657- Major Bill Nelson, USAF, Major Rodney Choi, USMC, Major Michael Iacobucci, USAF, Major Mark Mitchell, USA, Captain Greg Gagnon, USAF,"Cyberterror Prospects and Implications", White Paper, Center for the Study of Terrorism and Irregular Warfare Monterey, CA, October 1999, P 7-9, Prepared for: Office for Counterterrorism Analysis (TWC-1). date to visit,23-8-2021, Available at
file:///C:/Users/alfat/Downloads/442884.pdf
https://calhoun.nps.edu/bitstream/handle/10945/27344/Cyberterror%20Prospects%20and%20Implications.pdf?sequence=1&isAllowed=y

658- Clay Wilson, Cong. Research Serv., RL32114, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress 4 (2003) (Quoting Ron Dick, then Director of the NIPC), Updated January 29, 2008, P4. date to visit,23-8-2021, Available at
https://sgp.fas.org/crs/terror/RL32114.pdf

659- CYBERDEFENSE REPORT, Japan's National Cybersecurity and Defense Posture, Policy and Organizations, Zürich, September 2020,P5, Cyber Defense Project (CDP) Center for Security Studies (CSS)، ETH Zürich date to visit,23-8-2021, Available at
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

الفوضى، فضلاً عن أضرار أخرى تمس الأمن القومي للدول، جراء إمكانية نشر أو إفشاء تلك المعلومات، كما تتعدد وتتنوع مظاهر وأهداف العمليات الإرهابية على البنى التحتية لمختلف دول العالم، فقد يكون محل ارتكاب الهجوم الإرهابي السيبراني هي الصناعة المالية مثل البنوك وتداول الأوراق المالية، 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 الدول الأخرى أكثر من قادرة على ذلك باستخدام الأسلحة السيبرانية[660].

ماهية الحروب السيبرانية: الحروب السيبرانية تتضمن الإجراءات التي تتخذها دولة قومية أو جهة لمهاجمة ومحاولة إتلاف أجهزة الكمبيوتر أو شبكات تقنية المعلومات لدولة أخرى، من خلال على سبيل المثال فيروسات الكمبيوتر أو هجمات رفض الخدمة[661]، فالحروب المستقبلية ستشهد استخدام كود الكمبيوتر لمهاجمة البنية التحتية للعدو، والقتال إلى جانب القوات باستخدام أسلحة تقليدية مثل البنادق والصواريخ [662]،

660- Anjali C. Das,"U.S. Government Warns Companies of Legal Risk for Paying Ransom to Cybercriminals", The National Law Review, Volume XI, Number 280, Tuesday, October 6, 2020. date to visit,23-8-2021, Available at https://www.natlawreview.com/article/us-government-warns-companies-legal-risk-paying-ransom-to-cybercriminals

661- rand, "Cyber Warfare', date to visit,23-8-2021, Available at https://www.rand.org/topics/cyber-warfare.html

662- Steve Ranger," What is cyberwar? Everything you need to know about the frightening future of digital conflict", December 4, 2018. date to visit,23-8-2021, Available at https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/

فهي استخدام التكنولوجيا لمهاجمة أجهزة الكمبيوتر وشبكات المعلومات لدولة أخرى، وفي بعض الحالات، يمكن أن تسبب ضررًا مشابهًا للحرب الفعلية [663].

ماهية الحروب الإلكترونية: يتضح لنا أن الحرب السيبرانية تختلف عن **الحرب الإلكترونية** والتي كما حددتها وزارة الدفاع الأمريكية بأنها الأنشطة العسكرية التي تستخدم فيها لطاقة كهرومغناطيسية للتحكم في الطيف الكهرومغناطيسي(نطاق الترددات الكهرومغناطيسية) أو مهاجمة العدو[664]، 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.

تعريف الباحث للإرهاب السيبراني والحروب السيبرانية:

الإرهاب السيبراني: 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 السيبرانية: 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.

المطلب الثاني: هجمات جرائم الأمن القومي السيبراني على البنى التحتية للمدن الذكية

الجدير بالذكر أنه لا بد من الإشارة إلى حقيقة هامة وهي أن جرائم الأمن القومي السيبراني على البنى التحتية للمدن الذكية قد يتم ارتكابها بنشاط إجرامي يُشكل أركان

663- Jane McCallion, "What is cyber warfare?", 2 Mar 2021. date to visit,23-8-2021, Available at https://www.itpro.co.uk/security/28170/what-is-cyber-warfare

664- congressional Research Service, "Defense Primer: Electronic Warfare", Updated October 29, 2020,P1. date to visit,23-8-2021, Available at https://sgp.fas.org/crs/natsec/IF11118.pdf

جرائم تقنية المعلومات التقليدية، وقد يُشكل في أغلب الأحوال الإرهاب السيبراني والحروب السيبرانية النموذج القانوني لأركان ارتكاب تلك الجرائم، إلا أن الهجوم السيبراني يُعد القاسم المشترك الذي يجمع بين نماذج ارتكابها سواء اتخذت تلك النماذج جرائم تقنية المعلومات التقليدية أو الإرهاب السيبراني أو الحروب السيبرانية، فالهجوم السيبراني هو وسيلة ارتكاب جرائم الأمن القومي السيبراني على البنى 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"[665]، 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"[666].

ثانياً مظاهر جرائم الأمن القومي السيبراني: تتعدد وتتنوع مظاهر جرائم الأمن القومي السيبراني والتي تُجسدها أساليب الهجمات السيبرانية 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[667]:

665- Mary K. Pratt," cyber-attack. January 2021. date to visit,23-8-2021, Available at https://www.techtarget.com/searchsecurity/definition/cyber-attack#:~:text=A%20cyber%20attack%20is%20any,data%20held%20within%20these%20systems.

666- Dave Wallen," Types of Cyber Attacks: A Closer Look at Common Threats", October 6, 2020. date to visit,23-8-2021, Available at https://securityboulevard.com/2020/10/types-of-cyber-attacks-a-closer-look-at-common-threats/

667- Dave Wallen," Types of Cyber Attacks: A Closer Look at Common Threats", Op.cit. date to visit,23-8-2021, Available at

أ- هجمات الهندسة الاجتماعية:Social Engineering Attacksفي مجال أمن المعلومات، تعتبر الهندسة الاجتماعية مصطلحًا شاملاً لمجموعة واسعة من الأنشطة الضارة، حيث يستخدم المهاجمون السيبرانيون الهندسة الاجتماعية 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 الهامة.

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

https://securityboulevard.com/2020/10/types-of-cyber-attacks-a-closer-look-at-common-threats/

ب- هجمات البرمجيات الخبيثة Malware Attacks: هجمات البرامج الضارة هي أكثر أنواع الهجمات الإلكترونية شيوعًا حيث ينشئ المجرمون الإلكترونيون 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) يُشار إليها أيضًا باسم برامج الإعلانات، 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 هجماتSmurf 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 المواقع Cross-Site Scripting (XSS) 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 SQLغير 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[668]:-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

668- Josh Fruhlinger, "What is a cyber-attack? Recent examples show disturbing trends"FEB 27, 2020. date to visit,23-8-2021, Available at https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html

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 جرائم الأمن القومي السيبراني التي تم ارتكابها على مرافق البنى التحتية 2020-2021:

سوف نتناول بعض من تلك الجرائم بالقدر الي يتناسب مع أساسيا البحث وجوهره والتي تُبرز ضرورة وضع استراتيجية للحد من تلك الجرائم ومكافحتها وذلك على النحو التالي[669]:

*أغسطس (2021) أدى هجوم إلكتروني على حكومة بيلاروسيا إلى اختراق عشرات من قواعد بيانات الشرطة ووزارة الداخلية، وكان هذا الاختراق جزء من محاولة للإطاحة بنظام الرئيس ألكسندر لوكاشينكو.

*أغسطس (2021) هجوم إلكتروني على موقع جدولة لقاح (Covid-19) في منطقة لاتسيو الإيطالية أجبر الهجوم الموقع على الإغلاق مؤقتًا، وتعذر تحديد مواعيد التطعيم الجديدة لعدة أيام بعد الهجوم.

* يوليو (2021) ذكرت إستونيا أن أحد المتسللين المقيمين في تالين قام بتنزيل (286438) صورة هوية من قاعدة بيانات حكومية، مما كشف عن ثغرة أمنية في منصة تديرها هيئة نظم المعلومات (RIA).

669- Center for Strategic &International Studies, (CSIS), Significant Cyber Incidents date to visit,23-8-2021, Available at https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents https://csis-website-prod.s3.amazonaws.com/s3fs-public/220302_Significant_Cyber_Incidents.pdf?zfBZmYrk6vwP41YiNzone.S75Nqm.8C7

* يوليو (2021) شركة Transnet Port Terminals (TPT)، شركة تشغيل الموانئ التي تديرها الدولة في جنوب إفريقيا وتحتكر سكة حديد الشحن، تعطلت خدمات السكك الحديدية بعد اختراق من قبل جهات غير معروفة.

* يوليو (2021). زعمت وزارة الدفاع الروسية أنها تعرضت لهجوم DDoS تسبب في إغلاق موقعها على الإنترنت، مشيرة إلى أن الهجوم جاء من خارج الاتحاد الروسي.

* يونيو (2021) قادت مجموعة قرصنة ناطقة بالصينية جهود تجسس مستمرة ضد الحكومة الأفغانية من خلال رسائل البريد الإلكتروني الاحتيالية، انتحل قراصنة صفة مكتب رئيس أفغانستان واستهدفوا مجلس الأمن القومي الأفغاني.

* يونيو (2021) تم تسريب جدول بيانات يحتوي على تفاصيل شخصية سرية عن (1182) جنديًا من القوات الخاصة البريطانية على WhatsApp.

* مايو (2021) في (6) مايو كان خط أنابيب كولونيال، أكبر خط أنابيب وقود في الولايات المتحدة، هدفًا لهجوم برمجيات الفدية، أغلقت شركة الطاقة خط الأنابيب ودفعت لاحقًا فدية قدرها (5) ملايين دولار. يُنسب الهجوم إلى Dark Side، وهي مجموعة قرصنة ناطقة بالروسية.

* مايو (2021) في (4) و(5) مايو تعرضت شركة تكنولوجيا الطاقة النرويجية Volue لهجوم من برمجيات الفدية، وقد أدى الهجوم إلى إغلاق مرافق معالجة المياه والمياه في (200) بلدية، مما أثر على ما يقرب من (85٪) من السكان النرويجيين.

* أبريل (2021) تم اختراق هيئة النقل الحضرية (MTA) في مدينة نيويورك من قبل جهات مدعومة من الصين، لكنها لم تتمكن من الوصول إلى بيانات المستخدم، أو أنظمة المعلومات.

* مارس (2021) أعلنت أجهزة الأمن البولندية أن قراصنة روس مشتبه بهم استولوا لفترة وجيزة على المواقع الإلكترونية للوكالة الوطنية للطاقة الذرية ووزارة الصحة في بولندا لنشر تنبيهات كاذبة عن وجود تهديد إشعاعي غير موجود.

* مارس (2021) استهدف قراصنة صينيون مشتبه بهم مشغلي شبكات الكهرباء في الهند في محاولة واضحة لتمهيد الطريق لهجمات مستقبلية محتملة.

* فبراير (2021) أعلنت وكالة الأمن السيبراني الوطنية الفرنسية أن حملة مدتها أربع سنوات ضد مزودي تكنولوجيا المعلومات الفرنسيين كانت من عمل مجموعة قرصنة روسية.

* فبراير (2021) حاول قراصنة مجهولون رفع مستويات هيدروكسيد الصوديوم في إمدادات المياه في (أولدسمار) بولاية فلوريدا بمعامل (100) عن طريق استغلال نظام الوصول عن بعد.

* يناير (2021) اخترق قراصنة مجهولون أحد مراكز البيانات التابعة للبنك المركزي النيوزيلندي.

* ديسمبر (2020) أعلنت CISA ومكتب التحقيق الفيدرالي (FBI) أن قراصنة ترعاها دولة استهدفت مراكز أمريكية ترتكز على الأمن القومي والشؤون الدولية.

* نوفمبر (2020) استهدف القراصنة الصينيون المنظمات اليابانية في قطاعات صناعية متعددة تقع في مناطق متعددة حول العالم، بما في ذلك أمريكا الشمالية وأوروبا وآسيا والشرق الأوسط.

* أكتوبر (2020) أعلن مكتب التحقيقات الفيدرالي و CISAأن مجموعة قرصنة روسية اخترقت شبكات الحكومة الأمريكية والمحلية، وكذلك شبكات الطيران، وبيانات مسروقة.

* أكتوبر (2020) كشفت وزارة الأمن الداخلي الأمريكية أن المتسللين استهدفوا مكتب الإحصاء الأمريكي في محاولة محتملة لجمع بيانات مجمعة أو تغيير معلومات التسجيل أو اختراق البنية التحتية للتعداد أو شن هجمات DoS

* في سبتمبر (2020). تعرضت بعض شركات الرعاية الصحية الأمريكية مثل شركة (يونيفرسال هيلث سيستمز) لهجوم فدية تسبب في وتحويل سيارات الإسعاف، وإعادة جدولة العمليات الجراحية، وتعطل شبكات المستشفيات المتضررة واضطرارها إلى العودة النسخ الاحتياطية اليدوية.

رابعاً عوامل تزايد هجمات جرائم الأمن القومي السيبراني على البنى التحتية للمدن الذكية:

- إدراج مختلف دول العالم مرافق ومؤسسات البنى التحتية عبر الفضاء السيبراني.
- 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 إذا كان مرتكب الهجوم دولة خاصة في الحروب السيبرانية.
- أن الهجوم السيبراني سواء اتخذ شكل إرهاب سيبراني، أو حرب سيبرانية 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 أهداف متعددة، أو هدف واحد عدة مرات وفي ثوان معدودة، ومن ثم يوفر للمعتدي الوقت والمال والجهد.
- أن الأثار المدمرة للهجوم السيبراني سواء اتخذ شكل إرهاب سيبراني، أو حرب سيبرانية على أحد مراكز البني التحتية لدولة معينة تفوق قدراتها بمراحل الآثار المدمرة للهجوم العسكري في الحروب التقليدية، كما تفوق قدراتها الأثار المدمرة للإرهاب التقليدي.
- صعوبة اكتشاف ارتكاب الهجوم السيبراني سواء اتخذ شكل إرهاب سيبراني، أو حرب سيبرانية، 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 والعسكرية، 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.
- أن أساليب الهجوم السيبراني وتقنياته سواء اتخذ شكل إرهاب سيبراني، أو حرب سيبرانية 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، عكس العمليات العسكرية في الحروب التقليدية، وعكس أسلحة الإرهاب التقليدية التي لا يمكن استخدامها إلا مرة واحدة، كالهجوم المسلح للمنظمات الإرهابية بالأسلحة والقنابل على هدف معين.

- أن وقت الهجوم السيبراني سواء اتخذ شكل إرهاب سيبراني، أو حرب سيبرانية لاستغلال ثغرة أمنية بعد اكتشافها قصير نسبيًا، ومن ثم يستطيع مرتكب الهجوم تحقيق أهدافه بسهولة ودون وجود ردود أفعال قوية تجاهه أو مشاكل عند التنفيذ، في حين عند تنفيذ الحرب أو الإرهاب خارج الفضاء السيبراني قد يحتاج إلى الأمر إلى وقتاً طويلاً لمواجهة مشاكل عند التنفيذ، سواء تصادفت تلك المشاكل قبل أو أثناء أو بعد التنفيذ عند المطاردة أو الملاحقة أو رد العدوان.
- 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، خاصة في مجال الإرهاب السيبراني مقارنة بأساليب الإرهاب التقليدية الأخرى.

خامساً عوامل زيادة الهجمات السيبرانية خلال العامين السابقين: فقد تزايدت وتيرة الهجمات السيبرانية سواء على منشآت ومراكز البني التحتية للدول أو على المواقع أو الشبكات التابعة للأفراد أو شركات القطاع الخاص خلال العامين السابقين، وذلك يرجع للعديد من الأسباب، لعل أهم هذه الأسباب هو **ضعف ثقافة الأمن السيبراني** لدى المستخدمين وما قد ينجم عنها من ثغرات يستغلها المجرم السيبراني، **وثان** هذه الأسباب **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، **وثالث** هذه الأسباب **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، وفيما يلي[670] وقائع وهجمات وإحصائيات توثق تلك الأسباب السابق ذكرها، فوفقًا لتقرير سوق الأمن السيبراني لعام (2019) الصادر عن Cybersecurity Ventures من المتوقع أن يتجاوز الإنفاق العالمي على الأمن السيبراني تريليون دولار أمريكي في الفترة من (2017) إلى (2021)، ووفقًا لتقرير التحقيقات في خرق البيانات لعام (2019) (94٪) من البرامج الضارة تم تسليمها من خلال البريد الإلكتروني، (34٪) من خروقات البيانات التي حدثت كانت بسبب المطلعين، (22٪) من خروقات البيانات تضمنت الهجمات الاجتماعية، (17٪) من خروقات البيانات تضمنت برمجيات خبيثة، (8٪) من خروقات البيانات كانت بسبب سوء الاستخدام من قبل المستخدمين المصرح لهم، كما تضمنت تقاريرCSO Online أكثر من (80٪) من الخروقات الأمنية كانت نتيجة لهجمات التصيد، (60٪) من الخروقات الأمنية حدثت بسبب نقاط ضعف غير مصححة، زادت الهجمات على أجهزة إنترنت الأشياء بمقدار ثلاثة أضعاف في أوائل عام (2019)، وصرحت شركة Broadcom على أن ملفات Office تشكل (48٪) من مرفقات البريد الإلكتروني الضارة، فدائما يبحث المهاجمون عن الأفراد والمؤسسات المعرضين للخطر، والذي لديهم نقاط ضعف لشن هجماتهم، وفقًا للبحث الذي أجرته جامعة مريلاند يحدث هجوم إلكتروني كل (39) ثانية في المتوسط، وهو

670- Dave Wallen," Types of Cyber Attacks: A Closer Look at Common Threats", Op.cit. date to visit,23-8-2021, Available at https://securityboulevard.com/2020/10/types-of-cyber-attacks-a-closer-look-at-common-threats/

ما يُترجم إلى (2244) هجومًا مذهلاً يوميًا؟، وأنه يتم فقدان أو سرقة ما يقرب من (7) ملايين سجل بيانات كل يوم واختراق (56) سجل بيانات كل ثانية استنادًا إلى التقرير، واختراق ما يقرب من (2.55) مليار سجل بيانات سنويًا، كما يشير تقرير NETSCOUT Threat Intelligence إلى أنه تم تنفيذ أكثر من (23000) هجوم DDoS يوميًا في النصف الثاني من عام (2019)، كما توقعت شركة Cybersecurity Ventures [671] للأمن السيبراني أن تقع الشركات في عام (2021) ضحية لهجوم برمجيات الفدية كل (11) ثانية، بانخفاض عن كل (14) ثانية في عام (2019).

كما تعرضت مؤسسات الرعاية الصحية لمزيد من الهجمات السيبرانية في ظل COVID-19،[672] 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

671- Linn F. Freedman," Ransomware Attacks Predicted to Occur Every 11 Seconds in 2021 with a Cost of $20 Billion", The National Law Review, Volume XI, Number 82. March 23, 2021. date to visit,23-8-2021, Available at https://www.natlawreview.com/article/ransomware-attacks-predicted-to-occur-every-11-seconds-2021-cost-20-billion
file:///C:/Users/DrEmad1PC/Downloads/The%20National%20Law%20Review%20-%20Ransomware%20Attacks%20Predicted%20to%20Occur%20Every%20

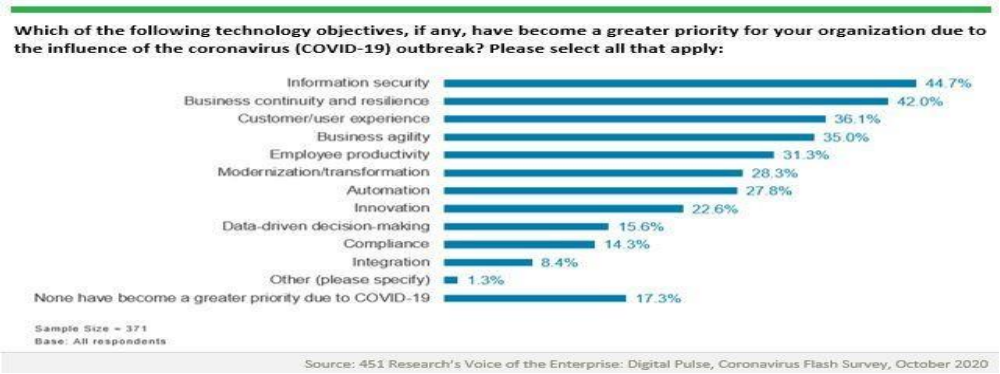
672- Megan Hardiman," Corona Viruses and Computer Viruses: It's Time for a Cyber Health Check-Up", The National Law Review, Volume XI, Number 217. Tuesday, August 4, 2020, date to visit,23-8-2021, Available at https://www.natlawreview.com/article/corona-viruses-and-computer-viruses-it-s-time-cyber-health-check
file:///C:/Users/DrEmad1PC/Downloads/The%20National%20Law%20Review%20-

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، كما حذر تقرير استشاري مشترك صادر عن CISA و(NCSC) وهو مركز المملكة المتحدة الوطني للأمن السيبراني في من تلك الهجمات السيبرانية وأثرها على الرعاية الصحية والطب، و استجابةً للتهديد المستمر بهجمات برامج الفدية التي تستهدف قطاع الرعاية الصحية، حذر فريق Microsoft Threat Protection Intelligence Team المستشفيات من أن أجهزتهم الشبكية وشبكات VPN الخاصة بهم كانت أهدافًا محددة مع انتقال المؤسسة إلى قوة عاملة بعيدة، وكان التحذير متسقًا مع تنبيه مشترك صادر عن (كالة الأمن السيبراني وأمن البنية التحتية) (CISA) ومكتب التحقيق الفيدرالي (FBI) في (22) مايو (2020)، حيث أفادت الوكالات أن شبكات VPN غير المصححة تصدرت قائمة نقاط الضعف التي يتم استغلالها بشكل روتيني من الجهات الفاعلة السيبرانية الأجنبية في عام (2020).

فقد كانت انتهاكات الأمن السيبراني بعيدة المدى لعام (2020)، والتي بلغت 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 [673]، 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

673- Lucian Constantin" Solar Winds attack explained: And why it was so hard to detect", DEC 15, 2020. date to visit,25-8-2021, Available at https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html

إلى زيادة تلك المخاطر، والكشف عن نقاط الضعف وعدم الاستعداد السيبراني، وتفاقم التفاوتات التكنولوجية داخل المجتمعات وفيما بينها[674].



سادساً استراتيجية الباحث لمكافحة جرائم الاعتداء على الأمن القومي السيبراني للبني التحتية للمدن الذكية: ترتكز استراتيجية الباحث على عدة محاور على النحو التالي:

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

674- Algirde Pipikaite, et, al " These are the top cybersecurity challenges of 2021", World Economic Forum, 21 Jan 2021. date to visit,25-8-2021, Available at https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/

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:

إن تحديث وتطوير منظومة الأمن السيبراني لمرافق البنى التحتية للمدن الذكية وتدريب وتنمية قدرات الكفاءات الوطنية القائمين عليها تُشكل الأولية الثانية لتحقيق الأمن السيبراني لمكافحة جرائم الاعتداء على الأمن القومي للبني التحتية للمدن الذكية.

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.

المحور الرابع: تعزيز وتطوير كفاءة وقدرة الأجهزة الخاصة بالعدالة الجنائية في التحقيقات السيبرانية: ودعمها بكافة أشكال الدعم التقني السيبراني لضبط جرائم الاعتداء على الأمن القومي السيبراني والحد من ارتكابها وضبط وملاحقة مرتكبيها، 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: الاستثمار الوطني في صناعة وإنتاج التطبيقات الذكية وتقنياتها وأنظمة الذكاء الاصطناعي: يحذر الباحث من شراء التطبيقات الذكية وأنظمة الذكاء الاصطناعي الخاصة بتحقيق الأمن السيبراني خاصة في مجال الطائرات المسيرة، نظراً لما قد تتضمنه من تقنيات تجسس متطورة ومجهولة داخل تلك التطبيقات والأنظمة، تستطيع التقاط البيانات والترددات وتحليلها، ورسم الخرائط ثلاثية الأبعاد للمواقع الاستراتيجية، وإرسال كل التقارير إلى الطراف الأخر، لذا فيوصي الباحث بصناعة وإنتاج الطائرة المسيرة وتقنياتها محلياً مع توفير الاعتمادات المالية والكوادر المدربة للنهوض بتلك الصناعات، ومن ثم يحذر الباحث من عدم شراء أو استيراد تلك المنظومة، وخير دليل على ذلك مراجعة الولايات المتحدة الأمريكية منظومة استيراد أو شراء تلك المنظومات من دولة الصين لاكتشافها تحقق المخاطر السابقة.

المحور الثامن: 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 فالتحسين المستمر لقدرات ومؤهلات المواطن فيما يتعلق بقضايا الأمن السيبراني في جميع مراحل حياته التعليمية ومهنته، ومن ثم تعزيز ونشر ثقافة الأمن السيبراني لديه يُعد خط الدفاع الأول لحماية الأمن القومي السيبراني لمرافق المدن الذكية، ويخلق مجتمع ذكي لتحقيق الاندماج المجتمعي في المنظومة الذكية لتلك المدن.

خاتمة البحث

نحمد الله سبحانه وتعالى على نعمه الظاهرة والباطنة، ونسأله أن يشملنا بشكره وحسن عبادته، وفي نهاية هذا البحث نستطيع أن نستخلص النتائج ونقدم التوصيات التالية:

أولا النتائج:

1- ارتكزت مرافق ومؤسسات البنى التحتية لمختلف دول العالم المتقدم خاصة المدن الذكية فيها على الفضاء السيبراني، في كافة المؤسسات الحيوية والاستراتيجية، فأصبح الأمن السيبراني جزء من الأمن القومي لتلك الدول.

2-أصبح الفضاء السيبراني وما يتضمنه من تلك المرافق والمؤسسات قوة جذب للاعتداء عليه بمختلف الهجمات السيبرانية.

3-خطورة جرائم الأمن القومي السيبراني المرتكبة على مرافق البنى التحتية للمدن الذكية لمختلف دول العالم لارتباط تلك الجرائم بكيان تلك الدول ووجودها، ولانتهاكها المتجدد والمتطور والمستمر لأمنها القومي السيبراني.

4-أن 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-صعوبة تحديد مصدر تلك الهجمات الإرهابية السيبرانية وتعقبها، ومن ثم يأمن الجناة مشاكل التنفيذ ومخاطر التعرف عليهم وضبطهم وملاحقاتهم.

6-الهجمات السيبرانية عابر للحدود حول العالم ومن ثم يستطيع مرتكبيها خاصة في حالات الإرهاب السيبراني أو الحروب السيبرانية استهداف وتدمير أهداف معينة لمراكز البنى التحتية للمدن الذكية عبر الفضاء السيبراني، فبمجرد اكتشاف الثغرة الأمنية على الطرف الأخر من الكرة الأرضية تبدأ وتنتهي تلك الهجمات في ثوان معدودة مُحققة هدفها المطلوب، وقد تُصيب أهداف متعددة أو هدف واحد عدة مرات وفي ثوان معدودة، عكس هجمات الإرهاب أو الحروب التقليدية، ودون الحاجة إلى السفر وتكاليفه وإعداداته، ومن ثم تُوفر لمرتكبيها الوقت والمال والجهد.

7-أن الأثار المدمرة للهجوم السيبراني على مراكز البنى التحتية للمدن الذكية سواء اتخذ صورة إرهاب سيبراني أو حرب سيبرانية تفوق قدراتها بمراحل الأثار المدمرة للهجمات التقليدية الإرهابية أو العسكرية في الحروب التقليدية، ويجنب المُعتدي أي خسائر في الأموال أو المعدات أو الأرواح.

8- صعوبة اكتشاف ارتكاب الهجوم السيبراني، أو تحديد حجم الأضرار التي ترتبت عليه، خاصة إذا كان هدف ذلك الهجوم هو مجرد الحصول على معلومات أو أسرار حساسة من القطاعات الحيوية أو الاستراتيجية للمدن الذكية، 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.

9-أن الهجمات السيبرانية تتم عبر تقنيات عالية ومتطورة، لأننا في عصر صراع التقنيات، فكل يوم هناك تقنيات جديدة بل كل ثانية هناك تقنيات جديدة، تخترق بل وتقوض كل التقنيات السابقة ، ومن ثم فهناك العديد من التحديات القانونية والتقنية التي يصعب التغلب عليها لمكافحة تلك الجرائم، تتعلق بصعوبة ضبط تلك الجرائم وملاحقة مرتكبيها، وإيجاد تشريع قانوني قوي ومتطور ومُحكم البناء، وأجهزة عدالة جنائية

تعمل من خلال تقنيات وتطبيقات ذكية متطورة، وكوادر مدربة على أحدث التقنيات والأجهزة، ومنظومة للأمن السيبراني قوية ومتطورة، لحماية أسرار الأمن القومي السيبراني للبنى التحتية للمدن الذكية من مجرد الوصول غير المشروع إليها، وقادرة على صد الهجمات.

10-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.

11-يرى الباحث أن هناك قاسم مشترك بين ركائز المدن الذكية 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.

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

13-يُعرف الباحث الشرطة الذكية بأنها هي الشرطة القائمة على منظومات تكنولوجيا المعلومات والاتصالات ومفرداتها وتطبيقاتها الذكية، لمكافحة ارتكاب الجرائم والحد من ارتكابها، ولتنمية وتطور استدامة المدن الذكية.

14-لعبت الشرطة الذكية دوراً كبيراً في ضبط الجرائم والحد من ارتكابها في مختلف المدن الذكية لدول العالم وفي دولة الإمارات.

15-أن ضعف منظومة الأمن السيبراني يهدد الأمن القومي للدول لتعرض البنى التحتية المدرجة عبر الفضاء السيبراني لتلك الدول للعديد من الهجمات السيبرانية، سواء اتخذت أشكال الحروب السيبرانية أو الإرهاب السيبراني، أو الجرائم المرتبطة بالإنترنت.

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

17- يُعرف الباحث **الإرهاب السيبراني** بأنه 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.

18-يُعرف الباحث الحروب السيبرانية: بأنها 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.

19-تعددت وتزايدت وتنوعت مظاهر جرائم الأمن القومي السيبراني على البنى التحتية للمدن الذكية والتي تُجسدها أساليب الهجمات السيبرانية وذلك حسب نوع الهدف المطلوب تحقيقه وحسب حجم وطبيعة الهدف المطلوب إصابته ومدى قوة الأمن السيبراني المتوافرة.

20-كانت انتهاكات جرائم الأمن القومي السيبراني بعيدة المدى لعام 2020، والتي بلغت 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.

21-أن جرائم الأمن القومي السيبراني والتي اتخذت وسيلتها الهجمات السيبرانية المرتكبة ضد مرافق البني التحتية خاصة المدن الذكية يصُعب تحديد مصدرها أو حتى اكتشافها أو إثباتها ومن ثم صعوبة ضبط مرتكبيها وملاحقاتهم، فهي عابرة للحدود ومن ثم آلية للتدمير عن بُعد وفي ثوان معدودة، والأثار المدمرة لتلك الجرائم تفوق قدراتها الأثار المدمرة لجرائم الأمن القومي التقليدية.

22- أن التخزين السحابي لبيانات الحكومات الذكية يمثل خطورة بالغة على الأمن القومي السيبراني.

ثانيا التوصيات: بالإضافة للتوصيات التي وردت في الاستراتيجية المقدمة يوصي الباحث:

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 الانترنت.

6- عدم التخزين السحابي لبيانات الحكومات الذكية لخطورتها على الأمن القومي السيبراني.

قائمة المراجع

أولاً المراجع العربية:

1- د أحمد محمود يسري، م طاهر عبد السلام حامد وآخرون " صياغة المفهوم العمراني للمدن الذكية"، كلية التخطيط العمراني والإقليمي جامعة القاهرة، مجلة البحوث الحضرية، المجلد 21، يونيو 2016.

2- جمال جلاف، - الإدارة العامة للتحريات والمباحث الجنائية شرطة دبي – جريدة الإمارات اليوم، 6 مارس 2019.

3- اللواء خليّل إبراهيم المنصوري، شؤن البحث الجنائي لشرطة دبي – جريدة البيان، 5 مارس 2018.

4- م عبد الله محمد العقيل،" المدن والمباني"- مجلة العلوم والتقنية- الرياض- مدينة الملك عبد العزيز للعلوم والتقنية، سنة (28)، عدد (111)، رجب 1435 – مايو 2014.

5- الفريق عبد خليفة المري، القائد العام لشرطة دبي – جريدة الخليج، 3 يناير 2021.

المواقع الإلكترونية:

1-الاتحاد الدولي للاتصالات (ITU) وهو احدى الوكالات المتخصصة التابعة لهيئة الأمم المتحدة.
https://www.itu.int/ar/mediacentre/backgrounders/Pages/smart-sustainable-cities.aspx
https://www.itu.int/ar/about/Pages/default.aspx

2-منظمة الأمم المتحدة- القمة الحكومية- سلسلة بحوث القمة الحكومية" المدن الذكية المنظور الإقليمي"، فبراير 2015.
https://www.worldgovernmentsummit.org/api/publications/document/3f505fc4-e97c-6578-b2f8-ff0000a7ddb6

3- بوابة حكومة دولة الإمارات.
https://u.ae/ar-AE/about-the-uae/digital-uae/smart-sustainable-cities#efforts-in-abu-dhabi
-https://u.ae/ar-AE/about-the-uae/digital-uae/smart-abu-dhabi
-https://u.ae/ar-ae/about-the-uae/strategies-initiatives-and-awards/local-governments-strategies-and-plans/smart-dubai-2021-strategy
-https://u.ae/ar-AE/information-and-services/justice-safety-and-the-law/maintaining-safety-and-security/security-systems-

https://u.ae/ar-AE/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security
https://u.ae/ar-AE/about-the-uae/digital-uae/robotics-and-ai-applications

ثانيا المراجع باللغة الأجنبية:

1- Anto OusephJuly," The 5 Pillars of a Smart City", July 12, 2017.
2- ALICE CRUICKSHANK."10 pillars of a smart city", 12 Dec 2018
3- Anjali C. Das,"U.S. Government Warns Companies of Legal Risk for Paying Ransom to Cybercriminals", The National Law Review, Volume XI, Number 280, Tuesday, October 6, 2020.
4- Algirde Pipikaite, et, al " These are the top cybersecurity challenges of 2021", World Economic Forum, 21 Jan 2021.
5- Caplan, Joel, et all, " Crime in Context: Utilising Risk, Terrain Modelling and Conjunctive Analysis of Case Configuations to Explore the Dynamics of Criminogenic Behaviour Settings", Journal of Contemporary Criminal Justice Volume 33, pp.133–151,2017.
6- Clay Wilson, Cong. Research Serv., RL32114, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress 4 (2003) (Quoting Ron Dick, then Director of the NIPC), Updated January 29, 2008.
7- CYBERDEFENSE REPORT, Japan's National Cybersecurity and Defense Posture, Policy and Organizations, Zürich, September 2020, Cyber Defense Project (CDP) Center for Security Studies (CSS) ،ETH Zürich.
8- congressional Research Service, "Defense Primer: Electronic Warfare", Updated October 29, 2020.
9-Center for Strategic &International Studies, (CSIS), Significant Cyber Incidents.
10-Donato Toppeta, " The Smart City vision: How Innovation and ICT can build smart, “liveable”, sustainable cities", October 2010.
11-Dave Wallen," Types of Cyber Attacks: A Closer Look at Common Threats", October 6, 2020.
12-Digital 14," Cyber Resilience Report, Smart Cities, The Power, The Risks, The Response", May 2020.

13-Erik Fritsvold,"12 Innovative Police Technologies", University of San Diego 2021.
14-European Parliament,' Mapping Smart Cities in the EU", Director General for Internal Policies, Policy Department A: Economic and Scientific Policy, Study, January 2014.
15-Ferguson, Andrew," Predictive Policing Theory", American University, Washington College of Law Research 24: 2020–10.
16-Harrison, C., Eckman, et all ," Foundations for Smarter Cities",. IBM Journal of Paraszczak, J., & Williams, P. (2010). Research and Development, 54(4).
17-Hedaia-t-Allah Nabil Abd Al Ghaffar, "Government Cloud Computing and National Security", Review of Economics and Political Science, ISSN: 2631-3561, 23 March 2020.
18-Ishmael Mugari, Emeka E. Obioha, "Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing", 20 June 2021.
19-Institute for Management Development IMD, Smart City Index 2020, A tool for action, an instrument for better lives for all citizens, September 2020.
20-ITU/BDT Cyber Security Programme, Global Cybersecurity Index (GCI), Guidelines for Member States, Version 0.9.04 September 2019.
21-JAKE FRANKENFIELD,"Cloud Storage "March 04, 2022.
22-John Kosowatz, "Top 10 Growing Smart Cities", The American Society of Mechanical Engineers(ASME), Feb 3, 2020.
23-John Bull, 'You Hacked: Cyber-Security and the Railways', London Reconnections, May 12, 2017.
24-John Leyden, 'Polish teen derails tram after hacking tram network', The Register, 11 Jan 2008.
25-Jane McCallion, "What is cyber warfare?", 2 Mar 2021.
26-Josh Fruhlinger, "What is a cyber-attack? Recent examples show disturbing trends"FEB 27, 2020.
27-Linn F. Freedman," Ransomware Attacks Predicted to Occur Every 11 Seconds in 2021 with a Cost of $20 Billion", The National Law Review, Volume XI, Number 82. March 23, 2021.

28-Lucian Constantin" Solar Winds attack explained: And why it was so hard to detect", DEC 15, 2020.
29-Mary K. Pratt," cyber-attack. January 2021.
30-Megan Hardiman," Corona Viruses and Computer Viruses: It's Time for a Cyber Health Check-Up", The National Law Review, Volume XI, Number 217. Tuesday, August 4, 2020.
31-Ministry of Science and Technology (MOST), Vietnam," The main pillars of smart cities and consultation to choose the right pillars to develop and build smart city", Monday, 22/02/2021.
32-Major Bill Nelson, USAF, Major Rodney Choi, USMC, Major Michael Iacobucci, USAF, Major Mark Mitchell, USA, Captain Greg Gagnon, USAF,"Cyberterror Prospects and Implications", White Paper, Center for the Study of Terrorism and Irregular Warfare Monterey, CA, October 1999, Prepared for: Office for Counterterrorism Analysis (TWC-1).
33-Neha Pradhan Kulkarni, Chiradeep BasuMallick, "What Is Cloud Storage? Definition, Types, Benefits, and Best Practices" July 8, 2021.
34-Nick Oberheiden. "Defending Against National Security Threats," The National Law Review, Volume XI, Number 254, September 11, 2021.
35-OECD,' Smart Cities and Inclusive Growth", 2020.
36-Pearsall, Beth," Predictive policing: The Future of Law Enforcement? ",. National Institute of Justice Journal, No 266: 16–19,2010, U.S. Department of Justice.
37-Perry, Walter L., et all," Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations", Washington, DC: RAND Corporation, 2013.
38-Peter Sloly, "Emerging tech that can make smart cities safer High-tech still needs to be high-touch", Security & Justice series Deloitte's ,2021.
39-RAND Corporation," Predictive Policing, Forecasting Crime for Law Enforcement", RB-9735-NIJ (2013).
40-Ramolobi L.G. Matlala," Defining e-policing and smart policing for law enforcement agencies in Gauteng Province", The International Journal of Social Sciences and Humanities Invention, Volume 3 issue 12 2016.

41-Reuters Staff, "Singapore to double police cameras to more than 200,000 over next decade", AUGUST 4, 2021.
42-Silva, B.N.; Khan, M.; Han, K. Integration of Big Data analytics embedded smart city architecture with RESTful web of things for efficient service provision and energy management. Future. Gener. Comput. Syst. 2020, 107, 975–987. [CrossRef].
43-Shirley Tay, "How Singapore is reimagining policing with smart cars and drones"19 APR 2021.
44-Smart Dubai 2021, Preparing Dubai to embrace the future, now, WELCOME TO THE HAPPY CITY.
45-Singapore 2020 Crime & Safety Report, U.S. Overseas Security Advisory Council, 4-6-2020.
46-Steve Ranger," What is cyberwar? Everything you need to know about the frightening future of digital conflict", December 4, 2018.
47-Steve Ranger, "What is cloud computing? Everything you need to know about the cloud explained", February 25, 2022.
48-Tiziana Campisi, Alessandro Severino, et all, "The Development of the Smart Cities in the Connected and Autonomous Vehicles (CAVs) Era: From Mobility Patterns to Scaling in Cities", Infrastructures Journal,8 July 2021, MDPI, Basel, Switzerland.
49-Tim Lau, "Predictive Policing Explained "April 1, 2020.
50-United Nations Commission on Science and Technology for Development, "Issues Paper On Smart Cities and Infrastructure", Prepared by the UNCTAD secretariat,11-13 January 2016.
51-Washburn and Usman Sindhu, " Helping CIOs Understand "Smart City" Initiatives", February 11, 2010.
52-Zainap Al Mehdar, "Cybersecurity and Cloud Computing: Risks and Benefits", January 18, 2022.

Arabic references:

1- Dr. Ahmed Mahmoud Yousry, Taher Abdel-Salam Hamed and others, "Formulation of the Urban Concept of Smart Cities", Faculty of Urban and Regional Planning, Cairo University, Urban Research Journal, Volume 21, June 2016.
2- Jamal Jallaf - General Department of Criminal Investigations, Dubai Police – Emaratalyoum newspaper, March 6, 2019.
3- Major General Khalil Ibrahim Al Mansouri, Criminal Investigation Affairs of Dubai Police - Al Bayan Newspaper, March 5, 2018.
4- Abdullah Muhammad Al-Aqeel, "Cities and Buildings" - Science and Technology Journal - Riyadh - King Abdulaziz City for Science and Technology, year (28), issue (111), Rajab 1435 - May 2014.
5- Lieutenant General Abdul Khalifa Al Marri, Commander-in-Chief of Dubai Police - Al Khaleej Newspaper, January 3, 2021

Websites:

1- **The International Telecommunication Union (ITU)**, which is one of the specialized agencies of the United Nations.

https://www.itu.int/ar/mediacentre/backgrounders/Pages/smart-sustainable-cities.aspx

https://www.itu.int/en/about/Pages/default.aspx

2- **The United Nations - Government Summit - Government Summit Research Series** "Smart Cities Regional Perspective", February 2015. https://www.worldgovernmentsummit.org/api/publications/document/3f505fc4-e97c-6578-b2f8-ff0000a7ddb6

3- **UAE Government Portal.**

https://u.ae/ar-AE/about-the-uae/digital-uae/smart-sustainable-cities#efforts-in-abu-dhabi

-https://u.ae/ar-AE/about-the-uae/digital-uae/smart-abu-dhabi

-https://u.ae/ar-ae/about-the-uae/strategies-initiatives-and-awards/local-governments-strategies-and-plans/smart-dubai-2021-strategy

-https://u.ae/ar-AE/information-and-services/justice-safety-and-the-law/maintaining-safety-and-security/security-systems-

https://u.ae/ar-AE/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security

https://u.ae/ar-AE/about-the-uae/digital-uae/robotics-and-ai-applications