

التخطيط الاستراتيجي الأمني ودوره في مواجهة الجرائم السيبرانية**Strategic security planning and its role in combating cybercrime**

الدكتور محمد خميس العثماني

مدير عام أكاديمية الشارقة للعلوم الشرطية -

الإمارات العربية المتحدة

تاريخ النشر: 2025/06/30

تاريخ المراجعة: 2025/04/08

تاريخ الإستلام: 2025/04/04

الملخص:

هدفت الدراسة إلى معرفة دور التخطيط الاستراتيجي الأمني في مواجهة الجرائم السيبرانية، واستخدمت المنهج الوصفي التحليلي، وقد توصلت الدراسة إلى عدد من النتائج من أهمها: للتخطيط الاستراتيجي الأمني أهمية كبرى في مواجهة الجرائم السيبرانية فهو يعتمد على منهجية علمية واضحة تهدف للحد من انتشار هذه الجرائم وحماية فئات المجتمع من مخاطرها، يعتمد التخطيط الاستراتيجي الأمني على عمليات الرصد التي تهدف إلى المراقبة الفورية والدائمة للثغرات والتهديدات المحتملة وتأثيرها على مستخدمي التقنيات الحديثة، إن أكثر الجرائم السيبرانية ضد الأشخاص هي المضايقات عبر البريد الإلكتروني، المطاردة عبر الإنترنت، التشهير، انتحال البريد الإلكتروني، أما الجرائم ضد الممتلكات فتتمثل في جرائم الملكية الفكرية، التخريب السيبراني، إرسال الفيروسات، فيما جاءت أبرز الجرائم ضد المجتمع فتشمل: المواد الإباحية المتعلقة بالأطفال، الاتجار والمقاومة عبر الإنترنت، ويتميز المجرمون السيبرانيون بأنهم محترفون ويمتلكون المهارة الفنية في استخدام التكنولوجيا الحديثة.

الكلمات المفتاحية: التخطيط، التخطيط الاستراتيجي، التخطيط الاستراتيجي الأمني، الجريمة، الجرائم السيبرانية

Abstract;

The study aimed at exploring the role of strategic and security planning and its role in confronting Cyber-crimes. The study followed the descriptive analytic approach. The study reached some results, the most important of which are: there is a great importance for the Strategic and security planning in confronting Cyber-crimes as it depends on a clear scientific methodology that aims at the limitation of these crimes and the protection of the society sectors from their dangers. The greatest cyber-crimes against persons are represented in the harassment through e-mails, chasing through internet, defamation, hacking and impersonation of e-mail. As for the crimes against properties, they are represented through intellectual property crimes, cyber vandalism, computer hacking. The most prominent crimes against the society include: pornographic material related to children, internet gambling. Cybercriminals are professionals and technically adept at using modern technology.

Keywords: planning, strategic planning, strategic security planning, crime, cybercrime



مقدمة

يشهد العالم تطورات عديدة في كافة المجالات بفعل التطور التقني والتكنولوجي الذي يسير في خطوات متسارعة؛ خاصة بعد اجتياح جائحة كوفيد 19 للعالم والتأثيرات التي نتجت عن تلك الجائحة وأدت إلى تغيير جذري في خطط الدول والمؤسسات لمواجهتها والتغلب على التحديات الناجمة عنها، كما أن تقدم المؤسسات التي تسعى للمنافسة عالمياً لا يتوقف على الإمكانيات المادية أو التكنولوجية فحسب؛ بل يجب أن يكون لديها الكادر البشري المؤهل والقادر على إحداث النقلة النوعية والوصول بالمؤسسة إلى أعلى المستويات.

ويمثل التخطيط الإستراتيجي مرحلة من مراحل تطور الفكر التخطيطي، وهو التخطيط الذي يقوم على أساس حساب الظروف البيئية المتغيرة وحاجات سوق العمل مع الأخذ في الاعتبار نوعية المجتمع والحياة فيه في المستقبل، وتتضمن خطواته: تحليل عناصر البيئة المحيطة الداخلية والخارجية، وتحليل وتحديد المصادر اللازمة (معونات - تسهيلات... الخ)، وتحليل الفرص التنافسية، وتحليل مصادر القوة والضعف للمؤسسة، وصياغة الأهداف (حالياً ومستقبلياً) (غنايم، 2008، ص 101)

وتكمن أهمية التخطيط الاستراتيجي الأمني في تركيزه على الربط الفعال بين المؤسسة وبيئتها المحيطة بشكل يضمن نجاحها في تحقيق رسالتها، ويرجع ذلك: لوجود اتفاق عام بين القادة والخبراء على أن التخطيط الإستراتيجي مكون حاسم للإدارة والحكم الجيد، ويساعد التخطيط الإستراتيجي المؤسسات على فهم احتياجات تحقيق الأهداف المتنوعة، وخطط التنفيذ، وغالباً ما يكون التخطيط بعيد المدى - تخطيط لمدة سنة أو سنتين - صعب التنفيذ وأقل في العائد، ويعتبر التخطيط الإستراتيجي تخطيطاً هاماً جداً في البيئة المتغيرة. (McKay, 2001, p.1).

مشكلة الدراسة

في ضوء التحديات السيبرانية التي تواجهها المؤسسات الأمنية بشكل عام وأجهزة العدالة الجنائية بشكل خاص أثناء عملها، وما تحمله تلك التحديات من مخاطر في بعض الأحيان على حياة العاملين، وسلامتهم الشخصية، وأمنهم الصحي والنفسي، كان لا بُد لهذه المؤسسات أن تهتم بالتخطيط الاستراتيجي الأمني لمواجهة تلك التحديات والمخاطر الناجمة عن الهجمات السيبرانية سواء على الأفراد أو المؤسسات،



ويلعب التخطيط الاستراتيجي دوراً مهماً لضمان تحقيق سلامة البيئة الأمنية واستمراريتها، وإحداث نقلة نوعية في جودة وتطوير أداء العاملين في مواجهة تلك التحديات، ورفع معدل الجاهزية لدى العاملين في المؤسسات الشرطية، والاستعداد المبكر لمواجهة كافة التحديات الأمنية وعلى وجه الخصوص تحديات ومخاطر الأمن السيبراني.

وبناءً عليه فإن مشكلة الدراسة تتمثل في الإجابة على التساؤل التالي: ما أثر التخطيط الاستراتيجي في مواجهة الجرائم السيبرانية؟

تساؤلات الدراسة

- 1- ما هي أهداف وأهمية التخطيط الاستراتيجي الأمني في مواجهة الجرائم؟
- 2- ما هي أهم الجرائم السيبرانية وخصائصها؟
- 3- ما هي أبرز أساليب مواجهة الجرائم السيبرانية التي تهدد المجتمعات؟

أهمية الدراسة

تتجلى أهمية الدراسة في الجوانب التالية

الأهمية النظرية:

- 1- إثراء الأدب النظري حول موضوع التخطيط الاستراتيجي الأمني ودوره في مواجهة الجرائم السيبرانية.
- 2- محاولة وضع تصور أولي حول موضوع الجرائم السيبرانية ومخاطرها المستقبلية على الأمن.
- 3- فتح المجال للمزيد من الدراسات اللاحقة حول موضوع الجرائم السيبرانية وأساليب التخطيط الاستراتيجي الأمني في مواجهة تلك الجرائم في موضوعات بحثية وبيئات مشابهة.

الأهمية التطبيقية

- 1- توعية الشباب بمخاطر الأمن السيبراني وتأثيرها على المجتمع ومدى مساهمتها على أفراد ومؤسساته للوقوع ضحايا للجرائم دون علمهم.
- 2- لفت أنظار أصحاب القرار إلى أهمية الاستعداد والتخطيط الاستراتيجي الأمني المسبق لمواجهة مخاطر الجرائم السيبرانية على المجتمع.
- 3- المساهمة في وضع تصور مقترح لأفضل الأساليب التي تساعد في مواجهة الجرائم السيبرانية.

أهداف الدراسة

- 1- إدراك أهداف وأهمية التخطيط الاستراتيجي الأمني في مواجهة الجرائم.
- 2- التعرف على أهم الجرائم السيبرانية ومعرفة أبرز خصائصها.
- 3- استنتاج أبرز أساليب مواجهة الجرائم السيبرانية التي تهدد المجتمعات.

منهج الدراسة

اعتمدت الدراسة على المنهج الوصفي التحليلي؛ لتحقيق أهداف الدراسة، والإجابة على تساؤلاتها، فالمنهج الوصفي يهدف إلى وصف الخصائص، والمتغيرات المتصلة بمشكلة الدراسة، والتي تتمثل في التخطيط الاستراتيجي الأمني؛ بوصفه متغيراً مستقلاً، والجرائم السيبرانية بوصفها متغيراً تابعاً، كما تستخدم الدراسة المنهج التحليلي لمعرفة العلاقة بين (التخطيط الاستراتيجي الأمني) ومدى قدرته في الحد من الجرائم السيبرانية.

الدراسات السابقة ذات الصلة بموضوع البحث

- دراسة الشهري (2019) بعنوان الإطار القانوني للحد من الجرائم الالكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية، وهدفت إلى الوقوف على الإطار القانوني للحد من الجرائم الالكترونية والتعرف على طبيعتها وأسبابها والاستبصار للمهددات والمخاطر التي تعترض الأمن السيبراني في المملكة العربية السعودية للوصول إلى الإطار القانوني الذي يحد من الجرائم الالكترونية وتعزيز الأمن السيبراني، واستخدمت الدراسة المنهج الوصفي، وكانت أداة الدراسة هي الاستبانة لجمع البيانات، وكان من أهم النتائج التي توصلت لها؛ إن الجرائم الالكترونية لا تعترف بأي حدود زمانية أو مكانية، وهذه الخاصية تمثل أهم السمات المميزة لطبيعة الجرائم الالكترونية، كما بينت أن التقنيات الحديثة وفرت فرصاً غير مسبوقة لانتشار الجرائم الالكترونية، وأن انتهاك السياسات الأمنية الخاصة بالأمن السيبراني تمثل أهم التهديدات التي تواجه الفضاء السيبراني في المملكة العربية السعودية .

- دراسة نير كشيترى ولياني لينسا الكانتارا(2015) Nir Kshetri and Lailani Laynesa Alcantara ، بعنوان التهديدات السيبرانية وتحديات الأمن السيبراني- منظور متعدد الثقافات، حيث هدفت إلى التعرف على العلاقة بين العوامل الثقافية وبين أشكال الجرائم الالكترونية، واستخدمت المنهج الوصفي التحليلي، وتوصلت إلى بعض النتائج من أهمها: ترتبط العوامل الثقافية ارتباطاً وثيقاً بالجرائم الإلكترونية والهجمات



الإلكترونية والأمن السيبراني، وأن بعض الجرائم الإلكترونية قد تكون مقبولة في ثقافة بعض المجتمعات وتلعب أدواراً أكثر أهمية من العوامل البيئية الأخرى .

دأسة طالب (2012) والتي هدفت إلى التعرف على مدى إمام القيادات في الأجهزة الأمنية بمفهوم وأهداف التخطيط الاستراتيجي، وكذلك التعرف على مدى إسهام التخطيط الاستراتيجي في تطوير أداء العاملين في الأجهزة الأمنية، والتعرف على مقومات التخطيط الاستراتيجي في الأجهزة الأمنية، ومعرفة التحديات التي تحد من دور التخطيط الاستراتيجي في تطوير أداء العاملين، وتم تطبيق الدراسة على عينة عشوائية طبقية قوامها (291) من الضباط العاملين بمديرية الأمن العام في الأردن، وتم استخدام المنهج الوصفي التحليلي ومنهج المسح الاجتماعي باستخدام الاستبانة، وتوصلت إلى مجموعة من النتائج من أهمها: إمام القيادات بمفهوم وأهداف التخطيط الاستراتيجي وأهميته في تطوير أداء العاملين بدرجة كبيرة، أن برامج التخطيط الاستراتيجي تسهم بدرجة كبيرة في تطوير أداء العاملين، وأن ضعف الإمكانيات المالية المتاحة يشكل أهم العوائق لتنفيذ الخطط الاستراتيجية في الأجهزة الأمنية .

أما دراسة (Masilamony,2010) فقد هدفت إلى معرفة مدى مساهمة التخطيط الاستراتيجي في فعالية المؤسسات غير الربحية، وما هي العمليات المستخدمة في التخطيط الاستراتيجي، وقد تكون مجتمع الدراسة من منظمين غير ربحيين، باستخدام منهج دراسة الحالة، بهدف مقارنة العمليات المستخدمة في كلا المنظمين، وتوصلت الدراسة إلى مجموعة من النتائج منها: أن المنظمين كانتا فعاليتين لأنهما اعتمدتا على استخدام المنهج التعاوني في التخطيط، وأن كلا المنظمين لديها لجنة للتخطيط وتسهيل عملية التنفيذ، إلا أن إحدى المنظمين كان شكل التنفيذ فيها غير واضح، ولا يوجد لديها جدول زمني للتنفيذ، وهناك ضعف في توفير الموارد البشرية، أما العوامل التي ساعدت على نجاح تنفيذ الخطط هو ما يلي: الدعم النشط والكامل لعملية التنفيذ، إضافة إلى نوعية التقارير النهائية، وكذلك وجود القيادة الفعالة.

التعقيب على الدراسات السابقة: تناولت الدراسات السابقة الموضوع من عدة جوانب فقد هدفت تلك الدراسات إلى الوقوف على الإطار القانوني للحد من الجرائم الإلكترونية والتعرف على طبيعتها وأسبابها والاستبصار للمهددات والمخاطر التي تعترض الأمن السيبراني ، كذلك التعرف على العلاقة بين العوامل الثقافية وبين أشكال الجرائم الإلكترونية، إضافة إلى مدى إمام القيادات في الأجهزة الأمنية بمفهوم وأهداف

التخطيط الاستراتيجي، وكذلك التعرف على مدى إسهام التخطيط الاستراتيجي في تطوير أداء العاملين في الأجهزة الأمنية، والتعرف على مقومات التخطيط الاستراتيجي في الأجهزة الأمنية معرفة مدى مساهمة التخطيط الاستراتيجي في فعالية المؤسسات غير الربحية، وما هي العمليات المستخدمة في التخطيط الاستراتيجي.

وبناء على ذلك فإن ما يميز الدراسة الحالية عن الدراسات السابقة هو محاولة دراسة أحد الجوانب الخاصة بالتخطيط الاستراتيجي الأمني التي لم تتطرق له الدراسات السابقة بالبحث فجاءت هذه الدراسة للتعرف على دور التخطيط الاستراتيجي الأمني في مواجهة مخاطر الأمن السيبراني، ومدى فعالية هذا التخطيط في عملية التصدي لهذه المخاطر والوقاية منها، والاستعداد لها.

1. التخطيط الاستراتيجي الأمني

يعتبر التخطيط الاستراتيجي هو الأداة الأساسية في تنمية وتطوير المؤسسات بشكل عام، ولهذا تلجأ تلك المؤسسات له للبحث عن الحلول والارشادات التي يمكن أن تساهم في حل مشكلات المؤسسات على اختلاف أنواعها

وأضحى التخطيط الاستراتيجي هو الوسيلة الفعالة للاستقامة والمحافظة على الحركة في الاتجاه الصحيح؛ إذ إنه عملية مستمرة تستطيع المؤسسات بشكل عام والمؤسسات الشرطية بشكل خاص من خلاله أن تحافظ على اتجاه تطورها في المستقبل، وذلك بإجراء التغييرات التي تتلاءم مع التحولات السريعة في البيئتين الداخلية والخارجية له

ويمثل التخطيط الاستراتيجي مرحلة من مراحل الفكر التخطيطي، وهو التخطيط الذي يقوم على حساب الظروف البيئية وحاجات سوق العمل، مع الأخذ في الاعتبار نوعية المجتمع والحياة المستقبلية فيه، وتتضمن عناصر البيئة المحيطة الداخلية والخارجية، وتحليل وتحديد المصادر اللازمة مثل المعونات والتسهيلات وغيرها، وتحليل

1.1 مفهوم التخطيط الاستراتيجي الأمني:

التخطيط الاستراتيجي حسب رؤية ديانا سكيلدر (Schilder, 1997) هو تحديد الوضع الحالي للمؤسسة، ومعرفة المصادر التي تمتلكها المؤسسة، ومن ثم إلى أين تريد أن تكون في المستقبل،

ولهذا فإن التخطيط الاستراتيجي هو الصورة الواضحة التي يريد النظام أن يصل إليه، وهذه الصورة تتسم بالتغير المُنظم وعدم الثبات.

ويمكن تعريف التخطيط الاستراتيجي على أنه العملية التي تستطيع المؤسسة من خلالها معرفة الوضع الحالي وتصور مستقبله المحتمل، ومن ثم يتم تطوير الاستراتيجيات والسياسات والإجراءات الهادفة إلى اختيار وتنفيذ أفضل تلك الاستراتيجيات، فالتخطيط الاستراتيجي يركز على التعامل مع المستقبل، وفهم البيئة المحيطة بالمؤسسة، وتحديد جوانب القوة والضعف فيها، والقدرة على استخدام المعلومات المتاحة لاتخاذ القرارات المناسبة التي من شأنها تحقيق رفاهية المؤسسة⁽¹⁾

(العجمي، 2020، ص 393)

وبناء عليه يمكن للتخطيط الاستراتيجي الأمني أن يحقق التحسين المستمر في المؤسسة من خلال العناصر التالية (Zechlin, 2010)

- 1- يمكن للتخطيط المساعدة على تحديد الأهداف والوصول إليها وتوضيحها بشكل مناسب للعاملين، مما يساعد في تسهيل مهمة تنفيذها.
- 2- تحديد الإمكانيات المادية والبشرية اللازمة للوصول إلى تحقيق الأهداف.
- 3- تقليل التعارض والتضارب بين المهام المختلفة داخل المؤسسة.
- 4- يعتبر وسيلة فعالة لتحقيق الرقابة الداخلية والخارجية.
- 5- يساهم في تنمية وتطوير مهارات العاملين.

ولكي يكون التخطيط الاستراتيجي الأمني فعالاً لا بُد له من تحقيق ما يلي: (الكبيسي، 2010، ص 17)

- المشاركة وتكوين فرق العمل
 - تعبئة الطاقات الفكرية وتشجيع الابداع من أجل استشراف المستقبل.
 - توظيف أحدث وأدق المعلومات.
 - رسم المسارات الآمنة التي تحقق تطلعات ورغبات العاملين.
- أما بترسون Petron, 2009 فقد أشار إلى أن عمليات التخطيط الاستراتيجي هي (Paterson, 2009)
- عملية تعلم تعمل على توفير الفرص للمشاركين لفهم ما يسعون إليه بصورة أوضح وأشمل.



- عملية اكتشاف، فمن خلالها يمكن التعرف على الفرص والحلول الغير معروفة.
 - عملية انفتاح على التصورات والمفاهيم المختلفة التي تعتبر الأساس لإيجاد الحلول للمشكلات المختلفة.
 - عملية تركيز على فصل القضايا الاستراتيجية عن القضايا الأخرى.
 - عملية تتضمن صناعة القرار من خلال اختيار البدائل الأصلح من بين البدائل المتاحة، ودعم الأولويات والمصادر المتاحة، وتقويم القرارات والخطط وتقييم المخاطر.
 - التخطيط عملية تنظيم للجهود، بحيث يتم تقييم المصادر والإمكانات المؤسسية المتاحة لتنفيذ القرارات.
 - عملية تتسم بالمرونة ورسم العلاقات الواضحة بين مخرجات مرحلة واحدة والتي تمثل مدخلات رئيسية لمرحلة تالية أو مراحل لاحقة.
 - وضع الأهداف وترتيبها بصورة منطقية وحسب الأولوية، ومعرفة مدى تطابق تلك الأهداف مع بعضها البعض، مع مراعاة الحاجة الى التتابع المنطقي بمرور الوقت.
- ويمكن القول بأن التخطيط الاستراتيجي الأمني في مجال مكافحة الجرائم السيبراني بأنه: عملية تفكير مسبق لما يمكن أن يكون عليه الوضع الأمني لاحقاً، من خلال التنبؤ بما يمكن أن يحدث في المستقبل فيما يتعلق بمخاطر الجرائم السيبرانية، بطريقة منظمة تقوم على وضع الأهداف وترتيبها، وتحديد الإمكانات الحالية سواء المادية أو البشرية وتعبئة الطاقات وتشجيع الابداع والابتكار واستشراف المستقبل، إضافة إلى ان التخطيط الاستراتيجي الأمني يتميز بالمرونة، والانفتاح وصناعة القرارات المتعلقة بالمستقبل.

2.1 أهداف التخطيط الاستراتيجي:

- تتلخص أهداف التخطيط الاستراتيجي الأمني من خلال الاعتبارات التالية : (علي ، 2010، ص 48)
- 1- تحديد التوجه الاستراتيجي للمؤسسة من خلال صياغة رسالة ورؤية المؤسسة وتحديد أهدافها، وتحديد مسار العمل فيها، وتوفير متطلبات تحسين الأداء وتحقيق التقدم والتطور، وربط الأهداف الاستراتيجية بطموحات الإدارة العليا ومصلحة الشركاء الفاعلين فيها.



2- تطوير وتحسين أداء المؤسسة: ويأتي ذلك من خلال السعي نحو تحقيق أهداف المؤسسة ورسالتها، ثم تقييم الأداء وتحديد عناصر القوة والضعف، وتدعيم الأداء المرتفع للأفراد والجماعات، وتوفير متطلبات التحسين للأداء المنخفض، إضافة إلى دعم وتطوير العلاقات الخارجية للمؤسسة مع أصحاب العلاقة والعمل على تطوير الشراكات مع جميع المؤسسات التي قد تساهم في تطوير أداء المؤسسة.

3- تطوير النظام الإداري في المؤسسة: من خلال تشجيع الأفكار الابتكارية، وتوفير المناخ التنظيمي المناسب لتوليد هذه الأفكار، وتحقيق المرونة في الإجراءات وحرية التصرف بما يكفل تحقيق الإنجازات والأهداف المخطط لها، وكذلك تسهيل عملية الاتصال الإداري بين أعضاء و فرق العمل، بالإضافة إلى توفير الإطار العام للمتابعة والرقابة والتقييم لتحديد جوانب القوة والضعف داخل المؤسسة والمحافظة على موارد المؤسسة وإمكاناتها.

4- مواجهة التغير في بيئة العمل: فالتخطيط الاستراتيجي هو عملية تهدف إلى التوصيف الدقيق لبيئة العمل في المؤسسة ووضع الاستراتيجيات المناسبة للتعامل الفعال معها، وتطوير إمكانيات المؤسسة، والتغلب على التحديات ووضع أفضل السبل لمواجهةها، وتدعيم قدرة المؤسسة على تحديد نقاط القوة والضعف وكيفية التعامل معها، وتوفير المرونة الكافية للتكيف مع التغيرات التي قد تطرأ على بيئة العمل سواء كانت هذه التغيرات متوقعة أم غير متوقعة.

3.1 أهمية التخطيط الاستراتيجي الأمني في المؤسسات الشرطية والأمنية:

للتخطيط الاستراتيجي أهمية بالغة في المؤسسات الشرطية والأمنية ويمكن إجمال تلك الأهمية في النقاط التالية: (McKay, 2001, p.1).

- الربط الفعال بين المؤسسة الشرطية والبيئة المحيطة بها بشكل يضمن النجاح في تحقيق رسالتها.
- يساعد التخطيط الاستراتيجي الأمني على فهم احتياجات البيئة المحيطة بالمؤسسة وكيفية تحقيق تلك الأهداف.
- يساهم التخطيط الاستراتيجي في وضع تصور لمستقبل المؤسسة من خلال الكشف عن الواقع الفعلي لإمكانات المؤسسة ومواردها المتاحة، واستثمار تلك الموارد بشكل أفضل.

- التركيز على القضايا الأساسية التي تُشكل جوهر العمل الشرطي واتخاذ القرارات التي تتناسب مع طبيعة العمل الشرطي، وتحديد برامج العمل والمسؤوليات المحددة لكل الأطراف في بيئة العمل داخل المؤسسة.
- يركز التخطيط الاستراتيجي الأمني على أهمية خلق الشراكات والتعاون بين المؤسسات الشرطية والمجتمع المحلي؛ لتحقيق الأهداف وتحديد الأولويات في العمل والتنفيذ.
- تحديد التحديات التي تواجه العمل الشرطي، ووضع الخطط الاستراتيجية المناسبة لحلها والتغلب عليها، وإيجاد الطرق والآليات الابتكارية التي تساعد في تحسين مستوى الأداء في العمل.

نستنتج مما سبق بأن التخطيط الاستراتيجي الأمني في المؤسسات الشرطية له أهمية كبرى فهو يسعى لتطوير عمل المؤسسات من خلال تطوير النظام الإداري، فالنظام الإداري يحدد التوجه الاستراتيجي ويسعى للارتقاء بالمؤسسة من خلال وضع تصور مستقبلي للعمل، وتنمية وتطوير أداء العاملين، ومراعاة التغير المستقبلي الذي قد يحدث، ووضع الخطط المناسبة لمواجهة تلك التغيرات، إضافة إلى خلق بيئة تشاركية فعالة مع البيئة المجتمعية فهي داعم حقيقي لعمل أي مؤسسة وتطورها.

وبناء على التغيرات المتسارعة في التطور التقني والتكنولوجي، وما يصاحب ذلك من تطور في أنماط الجرائم المُرتكبة عبر الفضاء السيبراني، وتطور في أساليب ارتكابها؛ لا بُد من التفكير المستمر في مراجعة الخطط الاستراتيجية الخاصة بالمؤسسات الأمنية ذات العلاقة بمكافحة الجرائم السيبرانية وتقييمها باستمرار ومواكبة التطور في أساليب تنفيذها، لكي تكون قادرة على مواجهة الجرائم السيبرانية، والحد من مخاطرها سواء على الفرد أو المجتمع.

4.1 التخطيط الاستراتيجي لتقييم حالة التهديدات السيبرانية:

من أجل تحديد مستوى الخطر، من الضروري عند التخطيط لتقييم حالة التهديدات السيبرانية اتباع الخطوات الأربع الرئيسية التي تشكل منهجية لتقييم التهديدات السيبرانية للأمن، وهي (Grzybowski, 2012):

أولاً: مرحلة الرصد: عملية المراقبة الفورية والدائمة للثغرات والتهديدات المحتملة وتأثيرها على الأمة الذكية، وهي التحقيق الدائم ومراقبة المخاطر السيبرانية من قبل جميع المؤسسات والشركات ومجموعات المصالح في الدولة، وجمع أجهزة الاستشعار من المنتشرة محلياً معلومات التهديد السيبراني.

ثانياً: مرحلة النمذجة: وهي تتبع نموذجاً لقياس التهديدات السيبرانية من خلال المؤسسات والإدارات المختلفة في المدينة، بعد مرحلة المراقبة والنمذجة، والتي تم الكشف عن بعضها، حتى من خلال تطوير نماذج التهديدات الخاصة بهم بما يتناسب مع وضعهم.

ثالثاً: مرحلة التحليل: تتبع عملية المراقبة والنمذجة هي عملية التحليل، والتي تساعد على تحديد الثغرات وتحديد التهديدات وشدها من خلال مراجعة مؤشرات حالة الأمن السيبراني داخل المنظمة وتحليل مدى تأثير المخاطر على السلامة العامة.

رابعاً: مرحلة مشاركة المعلومات: تتم مشاركة هذه البيانات والمعلومات مع فريق إدارة المخاطر أو التهديد السيبراني، سواء كانت الوزارات ذات الصلة أو فرق وكالة الأمن السيبراني الوطنية.

وبناءً على هذه المعلومات المشتركة، يمكن للمؤسسات استخدام المعادلة السابقة لتحديد الثغرات والتهديدات، وحجم تأثيرها على المجتمع، واحتمال حدوثها والتأثير على الأمن القومي، مما يساعد في النهاية على تحديد الأصول الموجودة تهديد حقيقي، مما يؤثر على الأمن القومي، وما هو مستوى الحماية المطلوب ومدى الضرر إذا لم يكن موجهاً ضد مثل هذا التهديد.

2. الجرائم السيبرانية

الجريمة السيبرانية هي جريمة تختلف مسمياتها عبر التطور الزمني الذي رافقه تطور تكنولوجي وتطور معه تطور هذا المفهوم، بدءاً من مصطلح إساءة استخدام الكمبيوتر، إلى مصطلحات الاحتيال الحاسوبي، وجرائم المعلومات، واتفاقية جرائم الكمبيوتر، والجرائم المتعلقة بالكمبيوتر، وجرائم التكنولوجيا الفائقة، وجرائم القرصنة، وصولاً إلى أحدث مصطلح وهو الجرائم السيبرانية، ولهذا فإننا نجد في كل مرة مع ظهور مصطلح جديد لجرائم الإنترنت يظهر لنا تعريفاً جديداً.

وهذا التنوع في المفاهيم ووجهات النظر يعود إلى حداثة الجرائم السيبرانية، والاختلافات الثقافية والقانونية بين البلدان، بالإضافة إلى المخاوف من أنها تحصر المصطلح في نطاق ضيق أو محدود



2.1 مفهوم الجرائم السيبرانية

تعرف الجريمة السيبرانية على أنها: الجريمة التي يتم تنفيذها بواسطة جهاز كمبيوتر أو تقنية حديثة على وسيلة كمبيوتر أخرى، أو الوسائل التكنولوجية الحديثة، فمن الضروري توفير الشبكة بينهما. (مهمل، 2018، ص1)

يعرفها آخرون على أنها نشاط إجرامي تُستخدم فيه تكنولوجيا الكمبيوتر، بشكل مباشر أو غير مباشر، كوسيلة أو هدف لارتكاب عمل إجرامي محدد سلفاً. (القرعان، 2017، ص 11)

وبناءً على ما سبق أصبح تعريف الجريمة السيبرانية غير مرتبط بأجهزة الكمبيوتر فقط؛ بل أصبح يشمل جميع الأجهزة الإلكترونية التي تتصل بالشبكات الخاصة والعامة، ولا تحدث الجريمة السيبرانية إلا من خلال مهاجمة البيانات عبر الفضاء السيبراني، أما بالنسبة للهواتف الخلوية التي تحدث فيها الجريمة حيث يكون موقع الجريمة أو الضحية عبارة كيان مادي. (محمود، 2015، ص52)

2.2 خصائص وسمات الجرائم السيبرانية

للجريمة السيبرانية عدد من السمات والخصائص منها:

- 1- جرائم تُرتكب من خلال الأجهزة الإلكترونية وأجهزة الهواتف المحمولة: تتم في بيئة رقمية معلوماتية قوامها النظم المعلوماتية، وأجهزة ومعدات وأدوات وتجهيزات الحاسب الآلي، أي أنها تتم في وبواسطة جناحي الحاسب الآلي، (مكوناته المادية ومكوناته البرمجية)، فهذه الأدوات تمكن المجرمين من الدخول للإنترنت لارتكاب الجرائم.
- 2- جرائم ذات طابع خفي: إن القدرة التقنية التي يتمتع بها المجرم تكون في الغالب أكبر من قدرة الضحية، وقد يكون السبب في ذلك أن الضحايا غالباً ما يخشون الإبلاغ عن الجرائم التي يتعرضون لها، فقد يؤثر ذلك على سمعتهم الشخصية أو على السمعة المهنية والمصداقية أما العملاء، لهذا تصبح من الجرائم الخفية التي لا ترد إلى علم السلطات ومن الصعب اكتشافها. (القرعان، 2017، ص 31)
- 3- السرعة في تنفيذها: أصبحت الجرائم السيبرانية جرائم ذات سرعة فائقة عند ارتكابها، فهي لا تأخذ وقتاً طويلاً وتحضيراً مسبقاً بشكل كبير قبل التنفيذ. (التميمي، 2016، ص 16)

4- **جرائم تُرتكب عن بُعد:** فقد مكنت التكنولوجيا الحديثة للمجرمين فرصة ارتكاب الجرائم عن بُعد، فالجاني قد يكون في بلد مُعين والضحية في بلد آخر، دون أن يعرفان بعضهما البعض. (التميمي، 2016، ص 17)

5- **جرائم عابرة للحدود:** فهي جرائم غير مدركة للحدود الجغرافية للبلدان، وهي عابرة للحدود الوطنية والقارية، ولا يحدها مكان محدد، وليست مقتصرة على دولة معينة، بل يُعتبر العالم كله مسرحاً لمثل هذه الجرائم، حيث يستطيع الفرد ارتكاب الجرائم السيبرانية من أي مكان في العالم ويستهدف أماكن أخرى بعيدة عن مكان تواجده. (الغافري، 2011)

6- **جرائم صعبة الإثبات:** تكمن صعوبة الإثبات في الجرائم السيبرانية في أن العثور عليها بطريقة التعقب العرضي، وحصرها في مكان معين، حيث أن هذا النوع من الجرائم لا يترك آثاراً واضحة ولا تُرى بالعين المجردة، فهي تحتاج إلى خبراء وفنيون على مستوى عالٍ جداً لإثباتها، ويرجع صعوبة عملية الإثبات إلى عدة عوامل منها: (القرعان، 2017، ص 42)

أ- صعوبة ترك الأثر بعد ارتكاب الجريمة.

ب- صعوبة المحافظة الفنية على الآثار.

ت- عملية الإثبات تحتاج إلى خبراء وفنيون متخصصون ولا يمكن لعملية الإثبات أن تتم عن طريق المحققون العاديين.

ث- تتميز الجرائم السيبرانية على عملية الخداع والتدليس.

ج- مرتكبو الجرائم السيبرانية يمتازون بالذكاء العالي والقدرة على التخفي.

7- **جرائم ناعمة:** تختلف الجرائم السيبرانية عن الجرائم التقليدية، فهي جرائم لا تتصف بطابع العنف ولا تتطلب القوة العضلية أو البدنية في ارتكابها، لهذا نجد أن المجرم السيبراني يتميز بمهارة وذكاء كبير، ومعرفة بالأساليب التقنية التي يتطلبها لخرق الحواجز الأمنية التقنية، كما أن بعض المجرمين لديهم دوافع أيولوجية أو دوافع شخصية كالانتقام من المؤسسات أو من دولة معينة، أو من الشركة التي كان يعمل بها، أو لغايات التجسس وانتهاك سرية المعلومات. (التميمي، 2016، ص 18)

8- **جرائم فنية:** يتسم المجرمون الذين يرتكبون مثل هذه الجرائم خصائص تميزهم عن المجرمين الذين يرتكبون الجرائم التقليدية لأنها في الغالب جرائم تقنية، وعادة ما يكون مرتكبوها خبراء في مجال



تكنولوجيا المعلومات، ذوي طبيعة خاصة وإمكانات خاصة علمية معلوماتية. ويستخدم في ارتكاب جرائمهم الموارد المعرفية والأساليب الاحترافية.

9- الهدوء في أسلوب ارتكابها: يتميز هذا النوع من الجرائم بأن ارتكابها يتم بطريقة هادئة، ولا تتطلب العنف مثل الجرائم التقليدية، فقط تحتاج إلى القدرة على التعامل مع التكنولوجيا. (الردفاني، 2014، ص 157)

يتضح مما سبق بأن الجرائم السيبرانية تختلف عن الجرائم التقليدية سواء في شكلها، وتأثيرها، وأساليب ارتكابها، وحتى في نوعية الضحايا، إضافة إلى فئات المجرمين الذين يرتكبون هذا النوع من الجرائم فهم مجرمون محترفون وعلى درجة عالية من المهارة الفنية في استخدام التكنولوجيا الحديثة، ولديهم القدرة على التخفي، إضافة إلى إمكانية تكرار المحاولة في مثل هذا النوع من الجرائم

2.3 فئات الجرائم السيبرانية

يمكن تقسيم الجرائم الإلكترونية إلى الفئات الرئيسية التالية:

الجرائم السيبرانية ضد الأشخاص: تشمل الأعمال الرقمية غير القانونية ضد الأشخاص انتشار المواد الإباحية للأطفال، واستخدام أجهزة الكمبيوتر لمضايقة الآخرين، والخداع الأمني الكاذب، والمواد الإباحية على الإنترنت، والاتجار في المواد الإباحية، والتحريض على الكراهية، وغيرها، وهي الجرائم الأكثر خطورة حيث أصبحت انتهاكات القانون السيبراني معروفة الآن لدرجة أنه من الصعب تفسير الضرر المحتمل للإنسانية من مثل هذه الجرائم، المضايقات الجنائية الرقمية على وجه الخصوص هي نوع من الجرائم السيبرانية ويمكن أن تحدث أنواع مختلفة من المضايقات على الإنترنت أو باستخدامه. ويمكن أن تكون الأنواع المختلفة من الاستفزازات جنسية أو عرقية أو دينية أو غير ذلك. (Neilson, 2011)

تعد انتهاكات الأمن السيبراني من الجرائم الإلكترونية الخطيرة، ويمكن وصف الجرائم المؤكدة التي تؤثر على هوية الأشخاص على النحو التالي:

- المضايقات عبر البريد الإلكتروني: هذا النوع من المضايقات يتم عن طريق إرسال الرسائل وتسليم المستندات والمغلفات، أي عن طريق الرسائل، عبر المواقع المختلفة مثل Facebook و Twitter و Orkut وما إلى ذلك، وهو توسع تدريجي خطوة بخطوة.

- المطاردة عبر الإنترنت: من خلال استخدام تكنولوجيا أجهزة الكمبيوتر (مثل الإنترنت أو الهاتف أو البريد الإلكتروني أو الرسائل الفورية أو موقع الويب أو كاميرا الويب أو الوظائف (N. Leontiadis, 2006)
- التشهير: يشمل أي شخص من خلال اختراق سجلات بريده وإرسال بعض الرسائل بلغة بذيئة لإخفاء حساب بريد الشخص.
- القرصنة: هذا يعني التحكم والوصول غير المصرح به إلى إطار الكمبيوتر الشخصي ودليل القرصنة التي تدمر المعلومات وبرامج الكمبيوتر تمامًا، وغالبًا ما يخترق المبرمجون الاتصال والأنظمة متعددة الاستخدامات.
- .(Phil Williams, 2006).
- التفسير: عرض لاقتحام إطار عمل جهاز الكمبيوتر الخاص بك والتلاعب بالمعلومات والبيانات السرية القيمة دون مشاهدتك وموافقتك.
- انتحال البريد الإلكتروني: يمكن للمرء القول إن رسائل البريد الإلكتروني التصيدية هي واحدة من هذه الرسائل، مما يسيء إلى مصداقيتها، ويشير إلى أنه بدأ بشكل مختلف عما بدأ بالفعل.
- انتحال الرسائل القصيرة: الانتحال هو أسلوب لمنع البريد العشوائي يعني الرسائل غير المرغوب فيها غير المرغوب فيها، ويأخذ الطرف المذنب شخصية شخص آخر كرقم هاتف محمول ويرسل رسالة نصية عبر الشبكة من رقم الهاتف الخليوي للشخص الذي تم استغلاله.
- البطاقات: تعني بطاقات الصراف الآلي المزيفة، أي الرسوم وبطاقات الائتمان التي يستخدمها المحتالون للحصول على ميزة مالية عن طريق سحب النقود من الرصيد المالي للشخص المتضرر، في هذا النوع من الجرائم الإلكترونية، غالبًا ما تُستخدم بطاقات الصراف الآلي بدون إذن (Steel, 2006).
- الغش والاحتيال: وهذا يعني أن الشخص الذي يثبت ارتكابه جريمة رقمية (أي يحصل على كلمات سرية ويخزن المعلومات) ذو طبيعة مستهجنة، مما يؤدي إلى التحريف والخداع.
- استغلال الأطفال في المواد الإباحية: في هذه الجريمة الرقمية، ينتج الجاني أو يثبت أو يحصل على مواد تسيء للأطفال القصر. (Mishra, 2001)



- التهديد: الإيحاء بأن الفرد أصبح منهكاً بسبب الخوف على حياة أحد أفراد الأسرة من خلال استخدام نظام الكمبيوتر مثل البريد الإلكتروني أو الوظائف أو الهاتف.

2. الجرائم السيبرانية ضد الممتلكات.

النوع الثاني من الجرائم السيبرانية هو الجرائم ضد أشكال مختلفة من الممتلكات. وتشمل هذه الجرائم تخريب أجهزة الكمبيوتر (إزالة ممتلكات الآخرين) ونشر العدوى أو العناصر الخبيثة، ويمكن تحديد الانتهاكات التي تؤثر على الممتلكات الشخصية على النحو التالي: (Neilson, 2012, p997)

- جريمة الملكية الفكرية: تتكون الملكية الفكرية من مجموعة من الحقوق، أي تظاهرة غير قانونية يُحرم فيها المالك حقوقه كلياً أو جزئياً تعتبر جريمة، يمكن القول إن أكثر أشكال التعدي على الملكية الفكرية شيوعاً هي سرقة البرمجة وانتهاك حقوق النشر والعلامات التجارية وانتهاك الترخيص وانتهاكات علامة المسؤول، سرقة الكود لجهاز الكمبيوتر، إلخ.
- القرفصاء السيبراني: Cyber Squat ينطوي على شخصين يكفلان نفس اسم المجال من خلال الادعاء أنهما قاما أولاً بتسجيل الاسم قبل الآخر من خلال حقوق الاستخدام أو استخدام شيئاً مشابهاً بالفعل، مثال على ذلك اسمان متشابهان، www.yahoo.com و www.yahhoo.com
- التخريب السيبراني: التخريب المتعمد هو الإضرار المتعمد بممتلكات شخص آخر على هذا المنوال، يعني التخريب الرقمي إتلاف أو تلف المعلومات أو البيانات المخزنة في جهاز الكمبيوتر عند إيقاف إدارة النظام أو تعطيلها، وقد يشمل أي شكل من أشكال الضرر المادي لأي جهاز كمبيوتر شخصي ضمن مجاله.
- قد تتخذ هذه العروض التوضيحية شكل سرقة الكمبيوتر، أو جزء من جهاز كمبيوتر، أو عمل جانبي، أو أداة مرتبطة بجهاز كمبيوتر.
- اختراق نظام الكمبيوتر: يهاجم المتسللون بما في ذلك Twitter الشهير مرحلة المدونة من خلال الوصول أو التحكم غير المصرح به على جهاز الكمبيوتر.
- إرسال الفيروسات: الفيروسات عبارة عن عناصر تم إنشاؤها بواسطة المطورين الذين يربطون أنفسهم بجهاز كمبيوتر أو مستند، ثم يتدفقون إلى مستندات مختلفة وأجهزة كمبيوتر مختلفة على النظام،

وتؤثر بشكل أساسي على المعلومات الموجودة على جهاز الكمبيوتر عن طريق تعديل المعلومات أو حذفها (Higginsm, 2008, p921)

- التعدي السيبراني: ويكون بنية الوصول إلى جهاز كمبيوتر أو نظام خاص بشخص ما دون الموافقة من المالك، للعبث بالمعلومات أو تغييرها أو إساءة استخدامها أو المساومة عليها من خلال استخدام اتصال إنترنت لاسلكي.
- سرقة وقت الإنترنت: يتم اختراق الإنترنت من قبل شخص غير مصرح له، ويستخدم وقت الإنترنت الذي دفعه شخص آخر، يستخدم الأفراد الذين يتعلمون معرف ISP وكلمة المرور الخاصين بآخر من خلال القرصنة أو الوسائل غير القانونية للوصول إلى الإنترنت دون الحصول على المعلومات الشخص الآخر.

3. الجرائم السيبرانية ضد الحكومة: النوع الثالث من الجرائم السيبرانية الموجه ضد الحكومة، والإرهاب الرقمي هو نوع محدد من الجرائم في هذه الفئة.

يظهر تطور الإنترنت أن الناس والتجمعات يستخدمون وسيط الفضاء السيبراني لإضعاف الحكومات العالمية وتدمير السكان الوطنيين، وتتجلى هذه الجريمة في شكل إرهاب عندما يقتحم شخص ما وكالة حكومية أو موقع إلكتروني خاص بالجيش. (Hinduja, 2012, p405)

لقد صاغت الاتفاقية الأوروبية اتفاقية الجرائم الإلكترونية، إلا أنها لم تعطي معنى دقيقاً للجريمة الرقمية، حيث أن لكل دولة طريقته الخاصة في وصف الجريمة الرقمية، والتي لا يمكن تجاهلها بسبب ظروفها الاجتماعية والاجتماعية.

من الواضح أن الأمم المتحدة تحاول تطوير أداة عالمية لزيادة اليقظة وتمكين الجهود القوية وبذلها لبناء أمن الجريمة الرقمية، وبالمثل، تم وضع اتفاقية مجلس أوروبا بشأن الجرائم الإلكترونية، حيث تحتاج البلدان إلى رفع مستوى قوانينها الوطنية إلى مستوى عالمي ثم الموافقة على أن تحذو حذوها.

4. الجرائم السيبرانية المضادة للمجتمع: من المؤكد أن المظاهر غير القانونية التي تهدف إلى

الإضرار بالإنترنت ستؤثر على أعداد كبيرة من الناس، وتشمل هذه الجرائم: (Holt, 2014, p1-25)

- المواد الإباحية المتعلقة بالأطفال: يتم استخدام نظام كمبيوتر لإنشاء أو توزيع أو الوصول إلى المواد التي تعتدي جنسياً على الأطفال دون السن القانونية .

- الاتجار عبر الإنترنت: بما في ذلك الاتجار بالمخدرات والأشخاص والأسلحة وما إلى ذلك، مما يؤثر على عدد كبير من الناس، علاوة على ذلك فإن الاتجار بالجرائم السيبرانية هو أخطر الجرائم.
- المقامرة عبر الإنترنت: يعد الابتزاز والاحتيال عبر الإنترنت من أكثر المؤسسات ربحية على الإنترنت اليوم.
- الجريمة المالية: هذا النوع من الجرائم شائع بسبب النمو الهائل في عملاء إدارة النظام والمنظمات الهاتفية، وسيحاول المجرمون الهجوم عن طريق إرسال رسائل كاذبة على الشبكة. على سبيل المثال: استخدام بطاقة ائتمان عن طريق اختراق كلمة المرور بشكل غير قانوني.
- التزوير: نظرًا لأن المعاملات عبر الإنترنت أصبحت ضرورة دائمة لنمط الحياة اليوم، بهدف خيانة أعداد كبيرة من الأشخاص عن طريق إرسال رسائل مرهقة.

ويمكن القول بأن الجرائم السيبرانية لا تختلف عن الجرائم التقليدية من حيث أنواعها وأهدافها، فهي جرائم تستخدم الأشخاص، والأموال والممتلكات سواء ممتلكات خاصة أو حكومية، لذلك وجب على أجهزة الدول الاستعداد التام وبناء أنظمة حماية فعالة للمؤسسات والشركات، إضافة إلى توعية الأفراد بالوقاية من مخاطر الجرائم والتهديدات السيبرانية التي تستهدفهم

2.3 أساليب منع الجرائم السيبرانية

يؤكد الخبراء في مجال الأمن السيبراني على ضرورة القيام بعدد من الخطوات الضرورية لتجنب الوقوع ضحية للجرائم السيبرانية، حيث يدعو Sailesh Kumar Zarkar ، المتخصص وخبير أمان النظام لخلية الجريمة الإلكترونية في شرطة مومباي ، إلى شعار P5 للأمن عبر الإنترنت: الوقاية والاحتياطات والحفظ والحماية والمثابرة، حيث تمكنهم من مواجهة الصعوبات التي تواجههم في هذا المجال، ومن هذه الخطوات ما يلي: (Gordon, 2013, p 636)

تحديد المخاطر من خلال التدريب سيساعد المنظمات والشركات التي يمكنهم الاعتماد عليها لمواجهة هذه الصعوبات.

تجنب الكشف عن أي بيانات شخصية للغرباء أو الأفراد الذين ليس لديهم مفهوم غامض عبر البريد الإلكتروني أو الكلام أو أي موقع ويب تفاعلي شخصي.

تجنب إرسال أي صور إلى الغرباء عبر الإنترنت لأن دورة إساءة استخدام الصور أو تغييرها سوف تتسع تدريجياً.

تصميم تحديث نظام مكافحة الفيروسات لمنع هجمات الفيروسات التي يجب على جميع مستخدمي الإنترنت استخدامها، والحفاظ على مستوى الصوت منخفضاً لتجنب سوء حفظ المعلومات التي تظهر في حالة التلوث بالفيروسات.

يجب على الأفراد عدم إرسال رقم البطاقة إلى أي موقع ويب غير آمن لمنع الاحتيال. يعتمد على من يحتاج إلى إيلاء اهتمام وثيق لوجهة الطفل لمنع أي ضرر أو مضايقة للطفل. يجب على مالكي الموقع مراقبة حركة المرور والتحقق من أي تناقضات على الموقع. مع نمو العديد من عملاء الويب، تقع على عاتق مالكي مواقع الويب مسؤولية تبني استراتيجيات لتجنب الجريمة الرقمية. حماية خوادم الويب التي تشغل جهات مفتوحة مادياً من الأنظمة الداخلية للشركة من الأفضل للشركات استخدام برامج الأمان للتحكم في البيانات على الوجهات. يجب أن تمرر أقسام تكنولوجيا المعلومات قواعد وتحذيرات معينة لتأمين إطار عمل جهاز الكمبيوتر، ويجب عليها بالإضافة إلى ذلك فرض بعض القوانين الأكثر صرامة لكسر التدريبات على الجرائم السيبرانية (G. Mark, 2012, p1).

التعاون الدولي في مجال مكافحة الجرائم السيبرانية لأنها أصبحت هي الخطر الحقيقي لجميع الدول، لذا لا بُد من القيام بخطوات موحدة من أجل مواجهتها والوقاية منها.

الخاتمة

تم استعراض موضوع الورقة البحثية في محورين أساسيين؛ المحور الأول تناول موضوع التخطيط الاستراتيجي الأمني من حيث مفهومه وأهميته وأهدافه، وكذلك التخطيط الاستراتيجي الأمني لتقييم حالة التهديدات السيبرانية، وفي المحور الثاني تم تناول موضوع الجرائم السيبرانية من حيث المفهوم، الخصائص والسمات لها، فئات الجرائم السيبرانية، أساليب منع الجرائم السيبرانية، وقد تم توضيح أهداف وأهمية التخطيط الاستراتيجي الأمني باعتباره منهج عمل وطريقة لمواجهة الجرائم السيبرانية والحد منها، وبهذا فإن التخطيط الاستراتيجي الأمني هو من الركائز الهامة في العمل الأمني الخاص بمواجهة الجرائم خاصة الجرائم السيبرانية، إذ أن مواجهة هذا النوع من الجرائم لا بُد وأن يتم التخطيط له بأساليب مختلفة عن مواجهة الجرائم



التقليدية؛ نظراً للخصائص والسمات التي يتمتع بها المجرم السيبراني وطبيعة الجرائم التي تستهدف الأشخاص والممتلكات ومؤسسات الدولة والمجتمع، كما تأتي أهمية التخطيط الاستراتيجي الأمني من أنه أسلوب علمي منظم لمواجهة الجرائم السيبرانية، أما فيما يتعلق بالجرائم السيبرانية فقد تم تناول هذا المحور من حيث التعرف على مفهوم الجرائم السيبرانية وخصائصها وسماتها، كما تم تناول فئات تلك الجرائم، وأهم الأساليب الخاصة بمواجهتها، وفي الختام تم التوصل لعدد من النتائج كما يلي:

النتائج

- 1- للتخطيط الاستراتيجي الأمني أهمية كبرى في مواجهة الجرائم السيبرانية فهو يعتمد على منهجية علمية واضحة تهدف للحد من انتشار هذه الجرائم وحماية فئات المجتمع من مخاطرها.
- 2- الجرائم السيبرانية تستهدف كافة المجتمعات والأفراد والمؤسسات، شأنها شأن الجرائم التقليدية لكنها تختلف من حيث أسلوب ارتكاب تلك الجرائم، والوسائل المستخدمة فيها، وبيئة المكان والزمان في ارتكابها.
- 3- يعتمد التخطيط الاستراتيجي الأمني على عمليات الرصد التي تهدف إلى المراقبة الفورية والدائمة للثغرات والتهديدات المحتملة وتأثيرها على مستخدمي التقنيات الحديثة، ثم تحليل تلك التهديدات وبيان مخاطرها والفئات المستهدفة منها، ثم مشاركة المعلومات مع بقية الفرق والمؤسسات ذات العلاقة بمواجهة تلك الجرائم ومرتكبيها.
- 4- إن أكثر الجرائم السيبرانية ضد الأشخاص تتمثل في المضايقات عبر البريد الإلكتروني، المطاردة عبر الإنترنت، التشهير، القرصنة، انتحال البريد الإلكتروني، أما الجرائم ضد الممتلكات فتتمثل في جرائم الملكية الفكرية، التخريب السيبراني، اختراق نظام الكمبيوتر، إرسال الفيروسات، فيما جاءت أبرز الجرائم ضد المجتمع فتشمل؛ المواد الإباحية المتعلقة بالأطفال، الاتجار والمقامرة عبر الإنترنت، الجرائم المالية، التزوير.
- 5- يتميز المجرمون الذين يرتكبون هذا النوع من الجرائم بأنهم محترفون وعلى درجة عالية من المهارة الفنية في استخدام التكنولوجيا الحديثة، ولديهم القدرة على التخفي، إضافة إلى إمكانية تكرار المحاولة في مثل هذا النوع من الجرائم.

التوصيات

بناء على النتائج التي توصلت لها الدراسة فإنها توصي بما يلي :

- 1- ضرورة الاهتمام بالتخطيط الاستراتيجي الأمني والاعتماد عليه في مجال مكافحة الجرائم السيبرانية؛ خاصة وأن الأجهزة الأمنية لديها المقدرة على التخطيط وفقاً لمراحل زمنية بعيدة بناءً على ما يتوفر لديها من معلومات أمنية حول هذه الجرائم.
- 2- العمل على تدريب الكوادر البشرية العاملة في مجال مكافحة الجرائم السيبرانية على الأساليب الحديثة في مواجهة تلك الجرائم وأن يكون التدريب وفقاً لخطة استراتيجية تمر من خلالها عملية التدريب بمراحل متطورة.
- 3- عقد دورات متخصصة في مجال التخطيط الاستراتيجي الأمني لمواجهة الجرائم السيبرانية والاعتماد على نماذج الاستشراف المستقبلي والسيناريوهات الخاصة بذلك.
- 4- إجراء مراجعة دورية للخطة الأمنية في مجال مكافحة الجرائم السيبرانية، وتقييم تلك الخطط وتحديد نقاط القوة والضعف فيها وفقاً لمستجدات كل مرحلة من مراحل التخطيط.
- 5- زيادة مستوى التوعية الأمنية في مجال الأمن السيبراني للوقاية من مخاطر الجرائم السيبرانية التي تقع ضد الأشخاص والمؤسسات والمجتمع.

المراجع

المراجع العربية

- مهمل، أسامة (2018) الإجرام السيبراني ، رسالة ماجستير ، كلية الحقوق والعلوم السياسية ، جامعة محمد بوضياف.
- التميمي تميم عبد الله سيف ، الجرائم المعلوماتية في الاعتداء على الأشخاص ، مكتبة القانون والاقتصاد، الرياض، الطبعة الأولى، 2016، ص 16
- الغافري، حسين بن سعيد (2011). الجوانب القانونية للمعلوماتية بين النظرية والتطبيق، مسقط: بحث مقدم لكلية الحقوق جامعة السلطان قابوس في الفترة من 1413/3/2011.

- طالب، محمد فهد (2012)، دور التخطيط الاستراتيجي في تطوير أداء العاملين في الأجهزة الأمنية بالمملكة العربية السعودية، رسالة ماجستير غير منشورة، قسم العلوم الاستراتيجية .كلية العلوم الاستراتيجية، جامعة نايف العربية للعلوم الأمنية، بالرياض.
- العجمي محمد حسنين (2020). الإدارة والتخطيط التربوي – النظرية والتطبيق، دار المسيرة للنشر والتوزيع، الأردن، عمان، الطبعة 4، .
- الشهري، علي زايد محمد، (2019) الإطار القانوني للحد من الجرائم الالكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية، رسالة دكتوراه، جامعة نايف العربية للعلوم الأمنية.
- علي، أسامة محمد سيد، (2010). التخطيط الاستراتيجي وجودة التعليم واعتماده، مصر، القاهرة، دار العلم والإيمان، الطبعة 2.
- الكبيسي، عامر خضير (2010). التخطيط الاستراتيجي، عناصر هو نماذجه، الحلقة العلمية الخاصة بمنسوبي قوات الأمن الخاصة، كلية التدريب، جامعة نايف العربية للعلوم الأمنية، الرياض.
- الردفاني، محمد قاسم أسعد (2014) تحقيقات الشرطة في مواجهة الجرائم السيبرانية، الرياض، المجلة العربية للدراسات الأمنية والتدريب، المجلد 31، العدد 61
- القرعان، محمود أحمد (2017). الجرائم الإلكترونية ، دار وائل للنشر والتوزيع ، عمان .
- محمود، عمر محمود (2015) الجرائم المعلوماتية والإلكترونية ، الأردن، عمان، خوارزم العلمية للنشر.
- غنايم، مهني محمد إبراهيم (2008) "مدخل متكامل لتخطيط التعليم العالم العربي في إطار التخطيط الإستراتيجي"، المؤتمر الثاني لتخطيط وتطوير التعليم والبحث العلمي في الدول العربية، المجلد 1، جامعة الملك فهد للبترول والتعدين، الظهران، المملكة العربية السعودية.

المراجع الأجنبية

- Gordon, S., and Ford, R. (June 2013), Cyber terrorism? Computers & Security, vol. 21, issue 7, pp. 636-647.
- G. Mark Hardy, Beyond Continuous Monitoring: Threat Modeling for Real-time Response, SANS Institute InfoSec Reading Room, October 2012, p1, Accessed Feb 21, 2018, on <https://bit.ly/2UKIABs>

- Grzybowski, K. M.(Mar 2012), An examination of cybercrime and cybercrime research: self-control and routine activity theory, Book Reference.
- Higgins, G. E., & Makin, D. A. (2008), Self -control, deviant peers, and software piracy, *Journal of Technology Education*, vol. 20, issue 1, pp. 921-931.
- Hinduja, S., & Ingram, J. R. (2012), Social learning theory and music piracy: The differential role of online and offline peer influence, *Criminal Justice Studies*, vol. 22, issue 4, pp. 405-420, ISSN: 1521- 0456.
- Holt, T. J., and Bossler, A. M. (Apr 30- May 1, 2014), Examining the applicability of lifestyle routine activities theory for cybercrime victimization. *Deviant Behavior*, vol. 30, issue 1, pp. 1-25, (IJCC) ISSN: 0974 – 2891.
- Kshetri, Nir, and Alcantara, Lailani Laynesa (2015). “Cyber-threats and cybersecurity challenges: A cross-cultural perspective *to Cross-Cultural Management*, London and New York: Routledge.
- Masilamony, D.(2010). Strategic planning: Contextual factors that facilitated and/or challenged the implementation of strategic planning in two nonprofit organizations Available from ERIC. (881466063; ED520934).Retrieved <http://search.proquest.com/docview/881466063?accountid=44936>
- McKay, Emily Gantz; Strategic Planning: A Ten-Step Guide, National Council of La Raza, La Raza, July 2001, P. 1
- McKay, Emily Gantz; ***Strategic Planning: A Ten-Step Guide***, National Council of La Raza, La Raza, July 2001, P. 1.
- Mishra, R.C. (2001), Crime Trends and Criminal Justice, Authors Press: Delhi, Book Reference.
- Neilson Ratings (2011), Top ten global web parent companies, home and work.
- Neilson Ratings (2012), Top ten global web parent companies, home and work, vol. 3, Issue 5, pp. 997-1002.
- Leontiadis, N. T. Moore, and N. Christin (Aug 2011), Measuring and analyzing search-redirection attacks in the illicit online prescription drug trade, In *Proceedings of USENIX Security*, San Francisco, CA.
- Paterson, Andrew; (2009). ***A review of Strategic Planning practice that may be applied by the South African National Planning Commission***, Development Bank of Southern African, Midrand, P. 6.

Phil Williams (Dec 5, 2006), Crime and Cybercrime: Synergies, Trends, and Responses. Available: [http:// www.pitt.edu/~rcss/toc.html](http://www.pitt.edu/~rcss/toc.html)

Schilder, Diane; Strategic Planning Process: Steps in Developing Strategic Plans, Harvard Family Research Project, Harvard University, 2008, P.2.

Steel.C. (2006), Windows Forensics: The Field Guide for Corporate Computer Investigations, Wiley

Zechlin, L. (2010). Strategic Planning in Higher Education, *International Encyclopedia of Education (Third Edition)*, P. 260.