المجلة الإلكترونية الشاملة متعددة التخصصات
العدد التاسع والخمسون شهر (٥) ٢٠٢٣

بحث

# الجرائم الإلكترونية ودور الحكومات الفعال في إدارة الأمن السيبراني في ضوء التحديات المستحدثة

**إعداد الباحث**

**أحمد مصبح الخياط**

**الهيئة العامة للتعليم التطبيقي والتدريب – الكويت**

**Am.alazmi@paaet.edu.kw**

**ملخص البحث**

الأمن السيبراني هو ممارسة حماية أنظمة الحاسوب والشبكات والمعلومات الرقمية من الوصول غير المصرح به أو السرقة أو التلف أو أي أنشطة ضارة أخرى. ومع الاعتماد المتزايد على التكنولوجيا والإنترنت، أصبح الأمن السيبراني جانبًا أساسيًا من جوانب الحياة الحديثة. يمكن أن تأتي تهديدات الأمن السيبراني بأشكال عديدة، بما في ذلك البرامج الضارة وهجمات التصيد وبرامج الفدية والقرصنة

وتواجه الحكومات في جميع أنحاء العالم تحدي الجرائم الإلكترونية، والتي تشير إلى الأنشطة الإجرامية التي تُرتكب باستخدام أجهزة الحاسوب أو الإنترنت. يمكن لمجرمي الإنترنت استهداف الأفراد والشركات وحتى الدول بأكملها بهدف سرقة المعلومات الحساسة أو تعطيل الخدمات الأساسية أو التسبب في الفوضى

ولمواجهة الجرائم الإلكترونية، طورت الحكومات استراتيجيات مختلفة، بما في ذلك إنشاء وكالات الأمن السيبراني، وسن القوانين واللوائح التي تجرم الجرائم الإلكترونية، ونشر التقنيات المتقدمة لاكتشاف ومنع

الهجمات الإلكترونية. كما تعمل الحكومات بشكل وثيق مع الشركات الخاصة والمنظمات الدولية لتبادل المعلومات وتنسيق الجهود لمكافحة الجريمة السيبرانية

ومع ذلك، يعد الأمن السيبراني مجالًا يتطور باستمرار، ويبحث مجرمو الإنترنت دائمًا عن طرق جديدة لاستغلال نقاط الضعف في أنظمة وشبكات الحاسوب. نتيجة لذلك، يجب على الحكومات أن تظل يقظة وأن تكيف استراتيجياتها للبقاء في طليعة التهديدات السيبرانية

سوف أتناول في هذا البحث تعريف الأمن السيبراني وأهميته وأبعاده والاستراتيجيات التي يعتمد عليها. وأيضا الجرائم الإلكترونية وخطورتها وأنواعها. كما يتعرض البحث أيضا إلى التحديات التي تواجه تطبيق الأمن السبراني من قبل المؤسسات والحكومات من أجل ضمان أمن البيانات وقواعد المعلومات على حد سواء. سوف أتطرق بالإضافة إلى ذلك لأنواع الأمن السبراني ومدى اختلافه عن مفهوم أمن المعلومات من جهة ومن جهة أخرى سوف يقي البحث الضوء على الإجراءات الواجب اتخاذها من قبل الحكومات للحد من هذه الجرائم التكنولوجية من خلال طرح بعض التوصيات في ختام البحث لتأخذ بعين الاعتبار من قبل الجهات المختصة لخلق وعي متزايد لدى الأفراد بمخاطر الجرائم الإلكترونية والذي يسهم بدوره للحد من هذه المخاطر وإدارتها بشكل فعال.

**الكلمات المفتاحية**: الجريمة الإلكترونية - الأمن السبراني -أمن المعلومات -الاختراق التشريع -الأمن التشغيلي -قواعد البيانات -الأنماط -الاستراتيجيات.

## The abstract

Cybersecurity is the practice of protecting computer systems, networks, and digital information from unauthorized access, theft, damage, or other malicious activities. With the increasing reliance on technology and the internet, cybersecurity has become an essential aspect of modern life. Cybersecurity

threats can come in many forms, including malware, phishing attacks, ransomware, and hacking.

Governments around the world face the challenge of cybercrime, which refers to criminal activities that are committed using computers or the internet. Cybercriminals can target individuals, businesses, and even entire nations with the aim of stealing sensitive information, disrupting essential services, or causing chaos.

To tackle cybercrime, governments have developed various strategies, including the creation of dedicated cybersecurity agencies, the enactment of laws and regulations that criminalize cybercrime, and the deployment of advanced technologies to detect and prevent cyber-attacks. Governments also work closely with private companies and international organizations to share information and coordinate efforts to combat cybercrime.

However, cybersecurity is a constantly evolving field, and cybercriminals are always looking for new ways to exploit vulnerabilities in computer systems and networks. As a result, governments must remain vigilant and adapt their strategies to stay ahead of cyber threats.

**Keywords**: Cybersecurity - computer systems- strategies – threats- governments

**مقدمة البحث**

في عصرنا الحديث، تزداد الجرائم الإلكترونية بشكل متزايد، مما يشكل تحديًا كبيرًا للحكومات في إدارة الأمن السيبراني. تتضمن هذه الجرائم الهجمات الإلكترونية، والاحتيال الإلكتروني، والتجسس الإلكتروني، والابتزاز الإلكتروني، والتحريض على الكراهية والإرهاب الإلكتروني، والحقوق الملكية الفكرية الإلكترونية

وتتخذ الحكومات الفعالة إجراءات كبيرة للحد من هذه الجرائم، وتعزيز الأمن السيبراني، من خلال التعاون مع القطاع الخاص والدولي، والتحديث المستمر للتشريعات المتعلقة بالأمن السيبراني، وتطوير الخطط الوطنية للأمن السيبراني. وتحاول الحكومات أيضًا مواجهة التحديات المستحدثة، مثل الجرائم الإلكترونية الجديدة والمتطورة، وتهديدات الأمن السيبراني المتزايدة التي تنشأ عن الابتكارات التكنولوجية، مثل الذكاء الاصطناعي والحوسبة السحابية والإنترنت الجديدة

ولتحقيق هذه الأهداف، ينبغي على الحكومات تطوير استراتيجيات وخطط عمل مستمرة لتحسين الأمن السيبراني، بما في ذلك تعزيز قدرات الشرطة والجهات القضائية على التحقيق في الجرائم الإلكترونية، وتوفير التدريب والتعليم للمواطنين والشركات، وتطوير تقنيات جديدة للكشف عن الهجمات الإلكترونية ومنعها

علاوة على ذلك، يجب على الحكومات الفعالة أن تتعامل مع الجرائم الإلكترونية على المستوى الدولي، من خلال التعاون الدولي والتبادل الإلكتروني للمعلومات والخبرات، يمكن للحكومات الفعالة تعزيز قدراتها على مكافحة الجرائم الإلكترونية والتحديات المستحدثة المتعلقة بالأمن السيبراني. ويتطلب ذلك تعزيز التعاون الدولي وتبادل المعلومات بين الحكومات، بالإضافة إلى تطوير تقنيات وأدوات فعالة للتحقق من الهوية الإلكترونية ومكافحة الجرائم الإلكترونية

بالإضافة إلى ذلك، ينبغي للحكومات الفعالة أن تدعم تطوير مهارات الأمن السيبراني في المجتمعات المحلية، وتوفير الموارد اللازمة للشركات والمؤسسات لتحسين قدراتهم في الأمن السيبراني، وتعزيز الوعي العام بأهمية الأمن السيبراني والتحديات المستحدثة المتعلقة به

**مشكلة البحث**

يقوم هذا البحث بتناول مشكلة ازدياد معدل الجرائم الإلكترونية بشتى أنواعها وما له من تأثير سلبي على الأفراد والمؤسسات والدول بشكل عام. كما يتعرض البحث لخصائص هذه الجرائم والدوافع التي تكمن وراء ارتكابها. يتناول البحث ـأيضا عدم الوعي السائد في الوقت الراهن بكيفية التعامل مع مثل هذه الجرائم. ويتعرض البحث للمشاكل التي تواجه الحكومات في تطبيق الأمن السيبراني والتحديات التي تعترضها وكيفية إدارة الأمن السبراني بشكل جيد وفعال للقضاء على الجرائم التكنولوجي أو الحد من خطورتها وتأثيرها المدمر.

**أهداف البحث**

* الوقوف على دور الحكومات في تطبيق الأمن السبراني وكيفية تضافر جميع الجهود لتحقيق ذلك.

* التعريف بخطورة الموقف الحالي واستحداث وثائق وسائل تقنية جديدة تتعلق بالجرائم التكنولوجية والتي ساهمت في صعوبة التنبؤ بها والقضاء عليه.

**عناصر البحث**

- ماهية الجرائم الإلكترونية وكيفية نشأتها

- أنواع الجرائم الإلكترونية خصائصها ودوافعها

- مفهوم الأمن السيبراني أهميته وأبعاده

- التحديات المستحدثة التي تواجه الأمن السيبراني

-دور الحكومات في إدارة الأمن السيبراني

-التوصيات

**ما هي الجرائم الإلكترونية وكيفية نشأتها؟**

مما لا شك فيه أن أنظمة المعلومات وما يتعلق بها تتواصل عن بعد من خلال شبكة مترابطة وهذا أدى إلى إمكانية اختراق المعلومات عن طريق التوصل إلى هذا الربط بين الشبكات. وقد كان أول ظهور للجرائم الإلكترونية في بداية الستينات من القرن الماضي مع بداية استخدام الكومبيوتر وكانت في الماضي تم مناقشتها على أنها مجرد فساد أخلاقي في مجال المعلوماتية ولم ترتق لكونها جرائم يحاسب عليها القانون. حيث لم يتبين وقتها مدى خطورتها وتأثيرها على المؤسسات والدول حتى في عملية وضع القرارات الهامة. وقد تم حصرها في الستينات من القرن الماضي على هذا التصنيف.

مع بداية الثمانينات ازدادت الجرائم الإلكترونية بداية من اقتحام معلومات سرية مخزنة إلى سرقة مثل هذه المعلومات والقيام بعمليات ابتزاز للمالك وإن لم يستجب يتم تدمير الملفات والبرامج عن طريق فيروسات عبر شبكة الحاسوب. بدأ الشباب في هذه الفترة الانقياد وراء هذه الظاهرة ومحاولة اختراق البيانات أو سرقتها وهو ما أطلق عليه لفظ المخترق باللغة الإنجليزية الهاكر ولكن سرعان ما يتزايد الخطر وأصبح يهدد أمن الأفراد والمجتمعات. وماذا ظهور مواقع التسويق الشبكي في فترة التسعينات أصبح من السهل اقتحام النظام الشبكي لتكون هذه المواقع التسويقية معرضة بشكل كبير لمثل عمليات الاختراق عن طريق تعطيل النظام أو إرسال فيروسات قد تؤدي إلى خسارة مثل هذه المواقع خسارة هائلة.

بعد عام 2000 تطور الأمر بشكل هائل حيث لم يعد مقتصرا فقط على السرقة أو الاختراق، بل يمتد إلى الإرهاب الدولي والذي استهدفت أمن الدول وتهديد كياناتها. وقد بات هذا الخطر المحدق يهدد كل مؤسسات الدولة خاصة المؤسسات العسكرية والأمنية والاقتصادية. (حشيفه, عبد الهادي 2020). "تعد الجريمة

الالكترونية من أخطر أنواع الجرائم لان أساليبها وتطورها مرتبطان ارتباطا وثيقا بتطور تكنولوجيا المعلومات والاتصالات، وهو ما يشكل خطرا كبيرا على الأفراد والمؤسسات، بل ووصل الأمر إلى أمن الدول واستقرارها وهذا ما يستدعي وجود كيان دولي متمثل في هيئات أمنية وقضائية تسعى لاتخاذ جميع التدابير الضرورية والإجراءات لمكافحة هذا النوع من الجرائم من خلال تشريع القوانين التي تجرم هذه الأفعال".

**تعريف الجرائم الإليكترونية**

تعرف الجرائم الإلكترونية بأنها تلك الجرائم التي يستخدم فيها أجهزة الحاسوب والتي يقوم بها أشخاص مخترقون بهدف الاحتيال، الابتزاز، السرقة، أو للإضرار بشكل، أو بآخر بشخص، أو جهة، أو مؤسسة، أو دولة.

وقد عرفها البعض بأنها أي فعل متعمد يهدف إلى اللحاق خسارة بشخص ما أو تربح كسب لشخص غير مستحق بطرق ملتوية مستخدما شبكات الإنترنت. وقد تم تعريفها قانونيا بأنها الاعتداء المتعمد أو غير المتعمد على مصلحة شخص أو مؤسسة يرى المشرع أنه يجب حمايتها وتجريم الاعتداء عليها لتحقيق مصلحة المجتمع ككل. ومن هنا ظهرت لنا خصائص لهذه الجرائم والتي جرمها القانون فيما بعد وعقب عليها بشكل رسمي.

أولا: لا بد من وجود جهاز حاسوب للقيام بمثل هذه الجرائم.

ثانيا: لا تمنع من ارتكاب مثل هذه الجرائم أي حدود جغرافية أو دولية.

ثالثا: يقوم الفعل باستخدام شبكات الإنترنت وشبكة المعلومات في ارتكاب جريمته.

رابعا: لا بد أن يتوافر لدى مرتكب هذه الجرائم الذكاء والمهارة ليستطيع اختراق البرامج واستخدام الفيروسات بشكل غير مألوف.

**أنواع الجرائم الإلكترونية**

انتشرت الجرائم الإلكترونية وتنوعت في الآونة الأخيرة وكان من بينها أنواع أكثر انتشارا في شتى أنحاء العالم ومنها:

**1-الابتزاز الإلكتروني للحصول على المال**

يتم عن طريق استهداف الأموال أو الممتلكات من خلال الاستيلاء على البيانات الخاصة بشخص أو بمؤسسة بهدف ابتزازه للحصول على الأموال. ويطلب المبتز أن يقوم المجني عليه بدفع فيديا عن طريق العملات الإلكترونية المستحدثة (البيتكوين). (جدي, مروة 2019). من أهم أسباب ارتكاب الجرائم الالكترونية هي الابتزاز، ويعد الفيس بوك هو أكثر المواقع التي تحدث فيه الجريمة الالكترونية بشكل عالي جدا، وذلك راجع للاستخدام الواسع له على المستوى العالمي."

**2-سرقة الهوية**

وهو ما يعرف بسم سرقة الحسابات الخاصة بالشخص وانتحال شخصية أخرى بغرض سرقة حسابات بنكية أو الاحتيال على أشخاص بعينهم وذلك عن طريق اختراق بريدهم الإلكتروني لتهديدهم لاحقا.

**3-الإرهاب الأمني**

وفي هذه الجرائم تكون الدولة وأمنها هي المستهدف الأول حيث يقوم أشخاص أو مؤسسات باختراق الأجهزة الأمنية والدخول على أجهزتها وشبكاتها بهدف تهديد أمن الدولة أو ارتكاب جرائم تجسس دولي أو مسح بيانات أو تشفيرها بهدف أغراض إرهابية أخرى.

**4-القيام بأعمال غير مشروعة**

حيث يقوم الجانب استخدام المعلومات المخترقة من خلال جهاز الحاسب الآلي أو الهاتف النقال الخاص بالشخص للحصول على معلومات. يقوم بدوره بإرسالها لأشخاص آخرين بغرض التحريض على القيام بأعمال غير مشروعة أو بغرض تشويه سمعة المجني عليه وإلحاق الأذى النفسي له.

**5-انتهاك حقوق الملكية**

يتضمن ذلك حقوق الملكية الفكرية حيث يتم من خلالها استنساخ نسخة غير أصلية من برامج الوسائط المتعددة ولا شريها على شبكات الإنترنت. مما يتسبب بخسارة لا تقدر للمؤسسات التي قامت بصنع البرامج الأصلية.

**الدوافع وراء ارتكاب الجريمة الإلكترونية**

الجرائم الإلكترونية كونها جريمة لا بد لها من دوافع لارتكابها هي التي تدفع الجاني للتفكير وارتكاب جريمته بحرفية وإتقان ومن هذه الدوافع ما يلي:

* جني الأموال: حيث أوضحت الدراسات أن أكثر من 60 في المئة بالنسبة الجرائم الإلكترونية المرتكبه تكون بغرض الحصول على المال وتحقيق الثراء السهل السريع بشكل غير مشروع. ومن هنا كانت البنوك والقطاع المالي بشكل أكبر هي الفئة المستهدفة من مثل هذه الجرائم من حيث اللجوء لتزوير بطاقات الدفع الإلكتروني أو التحايل على تزوير مستندات والتلاعب فيها من أجل تحقيق ربح مادي.

* الانتقام المبرر: تصدر هذه الجرائم عادة من أشخاص لديهم دافع الانتقام من أفراد آخرين كانو قد ألحقوا بهم الضرر في السابق. أو في بعض الأحيان من مؤسسات تم فصلهم منها بشكل تعسفي وبالتالي يلجأوا إلى الاستيلاء على بيانات المؤسسة السرية والتي يكون على علم مسبق بها للعمل فيها في الماضي والتسبب

خسائر مادية للشركة. أيضا يكون دافعهم هو إلحاق الأذى النفسي لأشخاص بهدف رغبة الانتقام سواء بالقيام بذلك بشخص أو الاستعانة بشخص محترف في ارتكاب مثل هذه الجرائم لتحقيق هدف الانتقام.

* الشعور بالنقص والرغبة بإثبات التفوق: ينمو لدى البعض الشعور بالنقص من نجاح أشخاص آخرين مما يدفعهم إلى الإقدام عن ارتكاب جرائمهم الإلكترونية لتعويض هذا الشعور بالفشل والدونية. في شعر الجاني بأنه قد حقق ذاته وأثبت قدرته على اكتشاف عالم المعلومات واختراق أي نظام شبكي ليشعر بالفخر والتفوق المعنوي الذي يمكنه أن يحققه عن طريق ارتكاب مثل هذه الجرائم الإلكترونية.

**مفهوم الأمن السيبراني أهميته وأبعاده**

شهدت العديد من البلدان في الآونة الأخيرة انتشار كبير للجرائم الإلكترونية بكافة أنواعها، مما استدعى أن تقوم التدابير القانونية بإيجاد حل سريع وعاجل يتضمن ما يطلق عليه الأمن السيبراني لمواجهة هذه الجرائم. ليس فقط للحد منها، بل القضاء عليها. بالإضافة إلى زيادة الوعي لدى مستخدمي شبكات الإنترنت حول أخطار هذه الجرائم وتأثيرها السلبي على حياتهم. وقد تم تعريف الأمن السبراني بأنه مجموعة القوانين والسياسات التي تسعى إلى حماية المواقع الإلكترونية والأنظمة والبرامج أه من الهجمات الرقمية الشرسة التي تهدف باختراق نظم المعلومات والبيانات الخاصة أو الحكومية بغرض إتلافها أو ابتزاز مستخدميها. والأمن السبراني مصطلح مكون من مقطعي المقطع الأول وهو الآن بما يعني الدفاع والكلمة الثانية السبراني وهي كلمة لاتينية تعني إلكتروني.

وقد يختلط على البعض مفهوم الأمن السيبراني وأمن المعلومات وبالتالي يجب أن نعرف الفرق بين المصطلحين. فالأمن السيبراني كما تم تعريفه يعد فرع من أفرع أمن المعلومات حيث إن أمن المعلومات مصطلح عام يتضمن الوسيلة التي تحمي بها الأفراد والشركات قواعد بياناتهم عن طريق تخزينها في ملفات أو محركات الأقراص أو على أجهزة الحاسوب نفسها، وبالتالي تتضمن وسائل الحماية لأمن المعلومات حماية المعلومات الرقمية والمادية من الاختراق أو الاستيلاء أو التدمير. ومن هنا يعد مصطلح أمن

المعلومات أكثر شمولا من الأمن السيبراني والذي يهدف للحفاظ على أمن البيانات الرقمية فقط على العكس من أمن المعلومات الذي يندرج تحت حمايته البيانات الرقمية منها والمادية على نحو سواء، وبالتالي لا يمكن استخدام الأمن السبراني وأمن المعلومات كمصطلحين بنفس المعنى.

مما لا شك فيه أن الأمن السيبراني أصبح هو خط الدفاع الأول الذي يهدف إلى حماية الأنظمة الإلكترونية بشكل عام ضد هجمات القرصنة بشتى أنواعها. وبالتالي لابد أن نتطرق إلى أنواع الأمن السيبراني وأهميته وأبعاده للوقوف على مدى تأثيره في مكافحة الجرائم الإلكترونية.

**أنواع الأمن السيبراني**

كنا قد أوضحنا من قبل أن الجرائم الإلكترونية تعتمد اعتمادا كليا على موصولية الشبكات وسهولة الوصول إلى قواعد البيانات المختلفة أو اختراق السري والأمني منها، فكان لا بد من وجود أنواع متعددة من الأمن السبراني يهدف كل واحد منها إلى حماية خاصة حيث يوجد أنواع متعددة من الأمن السيبراني ومنها:

-أمن الشبكات: والتي تهدف إلى حماية الشبكات بشكل عام من خطر أي هجمة إلكترونية يمكن القيام بها من أي جهة غير معلومة.

-أمن التطبيقات: وهو الأمن المتعلق بكل تطبيقات الإنترنت والتي يستخدمها الملايين وكيفية حفظ هذه التطبيقات من أي عملية إتلاف أو استيلاء أو حتى توقف ولو بشكل مؤقت.

-الأمن السحابي: هو مجموعة من البروتوكولات التي تهدف إلى حماية الحوسبة السحابية والتي تعني وبشكل كبير بأمن المعلومات لدى الشركات والمؤسسات الكبرى.

-الأمن التشغيلي: وفي بعض الأحيان يطلق عليه أيضا الأمن الإجرائي حيث تقوم المؤسسة بتبني عقلية وتفكير المخترق حتى تتمكن من إيجاد مواطن الضعف في جهازها الأمني ومحاولة سد الثغرات لتفادي أي هجمة إلكترونية محتملة.

**أهمية الأمن السيبراني**

أصبح للأمن السبراني أهمية كبيرة في مناحي مختلفة على مستوى الأفراد والمؤسسات والشركات وأيضا على مستوى المجتمعات وسوف نقوم بسرد هذه الأهمية على كل مستوى على حدة.

أولا مستوى الأفراد: حيث يكون الغرض الرئيسي والجوهري للأمن السبراني فيما يتعلق بالأفراد هو حماية بياناتهم الشخصية وحساباتهم بما فيها من متعلقات (فيديوهات، صور، حسابات بنكية، ملفات وغيرها) من أي عملية اختراق أو استيلاء أو إبتزاز أو إتلاف.

ثانيا مستوى المؤسسات والشركات: حيث تقوم كل شركة ببناء إطار أمني لها شبكيا حيث تعمل جاهدة على حماية قواعد بياناتها وحساباتها والمعلومات الخاصة بالموظفين والعملاء لديها من أي هجمات إلكترونية محتملة.

ثالثا مستوى المجتمعات: تكون أهمية الأمن السبراني فيما يتعلق بالمجتمعات بحمايتها من الهجمات المنظمة على الشباب والتي تستهدف استقطاب البعض منهم للتنظيمات الإرهابية بهدف زعزعة أمن الدولة أو بهدف التجسس والتلاعب بالمعلومات الأمنية والمعني بها هدم الدولة بشكل عام.

**أبعاد الأمن السيبراني**

إن أبعاد الأمن السيبراني مصطلح شامل يندرج تحته أربعة أبعاد مهمة وهي البعد الاجتماعي، الاقتصادي، القانوني والسياسي.

**البعد الاجتماعي:**

يجب على أفراد أي مجتمع يقوم باستخدام تكنولوجي المعلومات أن يكون ملم بقدر كبير بنوعية الهجمات الإلكترونية وكيفية التعامل معها والتصدي لها. وهو ما يتوجب على المنصات الإعلامية من ضرورة القاء الضوء والقيام بحملات توعية لجميع مستخدمي الشبكات لخلق نوع من الوعي الإلكتروني على طول

المعرفة المسبقة لمخاطر الجرائم الإلكترونية وأنواع الاختراقات المحتملة، وبالتالي يتمكن مستخدمو الإنترنت من اتخاذ الإجراءات الاحترازية للحد من أخطار تلك الهجمات الممنهجة. (الشهري, علي زايد محمد الجبيري وآخرون 2019). من الضروري تطوير التقنيات الحالية لرفع كفاءة رصد وملاحقة الجريمة الإلكترونية، والبحث عن شركاء دوليين ومحليين متخصصين في مواجهة الجرائم الإلكترونية مع تنمية الكوادر البشرية العاملة في مجالات مكافحة الجرائم الإلكترونية والأمن السيبراني من خلال التوسع في عمليات البحث العلمي وإلحاق العاملين بدورات متخصصة في هذا المجال لرفع كفاءتهم

**البعد الاقتصادي:**

تؤدي الهجمات الإلكترونية وبخاصة على الشركات والمؤسسات إلى حدوث خسائر مالية فادحة هذا المنطلق كان تجاه الشركات لبناء نظام أمني متكامل لحماية مقدراتها مهما كلف الأمر. حيث إن احتياجات المؤسسة ومدى قيمة وأهمية قواعد البيانات بها هي العامل الأول الذي يحدد قدر التكاليف التي يتم إطلاقها لحماية تلك الموجودات لتجنب الخسائر المستقبلية.

**البعد القانوني:**

يجب أن يكون هناك تشريع قانوني يحرم الهجمات الإلكترونية وتكون الدولة هي المسؤول الأول عن سن مثل هذه التشريعات وتطبيقها على المخترقين لكي يتحملوا المسؤولية الأمنية في حال انتهاكهم لهذه القوانين المنصوص عليها بمواد تشريعية معلنة من قبل القضاء والهيئات القانونية. وبالتالي يساعد سن مثل هذه القوانين على بناء قاعدة أمنية تحمي بسياج أمني قانوني يشجع المستثمرين على الإقدام على الاستثمار في وجود حماية قانونية لاستثماراتهم من أي اختراقات في ظل بناء جسر من الثقة بين الحكومات والمستثمرين على أسس قانونية.

**البعد السياسي:**

يجب ألا تقتصر عمليات حماية البيانات عن طريق الأمن السبراني على المؤسسات والشركات أو الأفراد فقط، بل يجب على الدولة أن تلعب دورا فعالا من خلال وضع الإطار القانوني لتحقيق هذا الأمن مما يتضمنه من تطبيق إجراءات قانونية مشددة على مرتكبي الجرائم المعلوماتية. وبالتالي يجب على الدولة القيام بعمل توازن بين القوانين التي تسنها السلطة التشريعية وبين الجهات التي يجب ينبغي عليها تطبيق مثل هذه التشريعات والتي تكون مخولة من قبل الحكومة بصياغة التعليمات والأنظمة المتعلقة بالأمن السبراني. نجد أيضا أن الوعي الثقافي بأهمية الأمن السيبراني هو جزء لا يتجزأ من دور الحكومة السياسي تجاه الشعب بما فيه من أفراد ومؤسسات بتشجيع الثقافة الأمنية والقدرة على الإبلاغ عن أي جرائم إلكترونية من قبل أي منظمات أو أفراد.

**التحديات التي تواجه الأمن السيبراني**

يواجه الأمن السبراني العديد من التحديات نظرا لتعامله مع مخترقين محترفين شديد الذكاء وبرامج وفيروسات شديدة التعقيد وقد برزت أهم هذه التحديات في الآتي:

*** قلة الكوادر المؤهلة**

تعاني إدارات الأمن السيبراني يا للأسف لنقص في الكوادر المؤهلة التي باستطاعتها التصدي لهذا التحدي الكبير لأن أغلب المدربين غير قادرين بشكل كبير على تحديد التهديدات التي تواجه المؤسسات والشركات أو التنبؤ بها وبالتالي يقع على عبء الشركات أن تقوم بإحضار فرق خارجية ممثلة في كوادر مؤهلة ولديها من الخبرة والاحترافية ما يمكنها من إنشاء نظام أمني قوي لا يمكن اختراقه لكي تتمكن من المحافظة على سرية البيانات وحماية قاعدة المعلومات لديها.

*** عدم الإلمام الكافي بجوانب البنية التحتية**

من الضروري أن يكون هناك رؤية واضحة وإلمام شامل بجوانب البنية التحتية حتى يتمكن الأمن السبراني من اكتشاف التحديات التي تكمن في الحوادث المعقدة والتي من الممكن ألا يتم اكتشافها إلا بعد حدوث الكارثة. فمن المنطقي أن تكون جوانب البنية التحتية واضحة المعالم أمام مدافع الأمن السبراني حتى لا تتفاقم الأمور إذا تم الرد دون فهم ووعي كامل وشامل للوضع القائم.

*** عدم وجود تنسيق بين فرق العمل**

لابد من وجود خطة طوارئ مسبقة وتنسيق شامل بين فرق العمل حيث تقوم فرق الأمن السيبراني بعمل خطة شاملة تتكاتف فيها الجهود والرؤى حتى لا يتم إعاقة بعض الفرق لعمل فرق أخرى. حيث إن لكل فرقة نهج وأسلوب متبع في حالة تعامل مع جريمة إلكترونية وربما يتعارض مع فكر وطريقة فرقة أخرى وبالتالي يحدث التضارب ويزداد الأمر تعقيدا ويزيد من كمية الضرر بدل من إيجاد الحلول.

*** تعقيد السلوكيات والتهديدات الإلكترونية**

مع تزايد معدل الجرائم الإلكترونية يقوم المخترقين بابتكار وسائل وأساليب معقدة في الهجوم الإلكتروني منها الاستعانة ببرامج أو شبكات حديثة شديدة التعقيد والتي يجب أن تكون أنظمة الأمن على دراية شاملة بها كيف تتمكن من التعامل معها وإيجاد حلول أمنية سريعة يستطيع بها التعرف على مرتكبي الجرائم الإلكترونية.

**دور الحكومات في إدارة الأمن السيبراني**

مما لا شك فيه أنه يقع على عاتق الحكومات العبء الأكبر في إدارة وتنفيذ الأمن السبراني. حيث إن العديد من الأنظمة والبنية التحتية ذات الاتصال بالشبكات تتعرض لشتى أنواع الاختراقات والتي من الممكن أن تعطل خدماتها، بل قد تصل إلى تدميرها بشكل كلي. وفي ظل عالم يسوده انعدام الأمن السبراني يجب أن

تتكاتف الحكومات والمؤسسات وتتشارك المسؤولية من أجل وضع نهج منضبط واتخاذ كافة الإجراءات الاحترازية من أجل التصدي الهجمات الخارجية والتي تستهدف الإضرار بالبنية التحتية لهدم الدولة.
وبالتالي يتوجب على الحكومات ألا تألو جهدا ولا تدخر وسعا فيما يتعلق بإدارة الأمن السبراني وأن تتحرك في عدة محاور منها:

**-فهم الخطر السيبراني**

لابد من الدولة أن تدرك إدراكا تاما حجم الخطر السبراني الذي يحيط بالدولة متمثلة في كيانها الاقتصادي والسياسي والأمني. وأيضا يجب عليها مراعاة الخطر الذي يواجه الشركات والأفراد. حيث تتعامل الحكومات مع قطاعات حساسة فيجب تقييم الموقف بشكل حازم ودقيق. فمن المنطقي أن نعلم أنه لا توجد دولة تستطيع وبشكل جذري وضع برنامج أمني سيبراني متكامل لا يمكن اختراقه، ولكن يجب أن يكون هناك جاهزية واستعداد لفهم ماهية الخطر وتقييم الأمور المعرضة لها.

**- تقييم الخطر**

يندرج المحور الثاني بعد أن نفهم الخطر والتهديد الإلكتروني بكافة أنماط وجوانبه تأتي مرحلة التقييم. حيث تقوم الحكومات بإجراء تقييم مستمر للخطر على مختلف القطاعات وأهمها الأمني والاقتصادي والتي تعتمد على الاستخدام الشبكي. أيضا يجب أن تتبنى العديد من الإجراءات لإدارة المخاطر المحددة وعمل تخطيط استراتيجي على المدى البعيد حتى يكون إدارة الأمن الوطني على سلم الأولويات لدى الحكومة.

**- خفض حجم المخاطر**

حيث تقوم الحكومة في هذا المحور بوضع خطة لخفض حجم المخاطر بعد تقييم الخطر لتقف على أوجه القصور في خطة الأمن السبراني لديها لتفاديها. وأيضا يجب العمل الدؤوب مع كل الأطراف المعنية والمعرضة للخطر السبراني لكي يتمكنوا من تعيين الكوادر البشرية المدربة ووضع الخطة المالية اللازمة للاستراتيجيات المستخدمة في إدارة الأمن السيبراني.

**- زيادة الوعي بالأمن السيبراني**

وهو ما تقوم به الحكومات من إنشاء الحملات التوعوية بأهمية الأمن السيبراني والقيام ببناء ثقافة عامة لجميع مستخدمي الشبكات من المواطنين والشركات والمؤسسات لكي يكون جزء من الحل وليس جزء من المشكلة. وبالتالي يجب أن تتضافر الجهود مع زيادة الوعي بين الحكومة والأفراد لمواجهة الخطر السيبراني المستقبلي. كما يجب أن يكون للمدارس دورا بارزا في هذا الأمر. (الصانع, نورة عمر وآخرون 2020). يجب على وزارات التربية نشر ثقافة الوعي بالأمن السيبراني بين معلمي جميع المرحل الدراسية العامة لتوعية الطلبة بمخاطر الإنترنت بمختلف أنواعها وإقامة دورات تدريبية للمعلمين في مجال تعزيز القيم وغرسها في نفوس الطلاب

**- التعاون الدولي المشترك**

إن الخطر السيبراني لا يهدد دولة بعينها، بل هو خطر قادم على دول العالم أجمع. ومما لا شك في أنه يجب على حكومات الدول المختلفة إيجاد حل دولي مشترك يتم من خلاله وضع معايير عالمية للأمن السيبراني. أيضا يجب القيام بعقد اتفاقيات مشتركة لتحسين أمن ومرونة الشبكات وتفادي أي قصور في الجيل الثاني من البنية التحتية وزيادة الجاهزية للأزمات السبرانية المحتملة.

**- تشريع أطر قانونية**

إن من أهم أدوار الحكومة في إي إدارة الأمن السيبراني هو إعداد القطر التنظيمية والقانونية المتعلقة بالجريمة السيبرانية وإيجاد تشريع قانوني لها يجرم ويحاسب المتسبب بها . وأيضا يجب تخصيص موارد مالية لتمويل استراتيجيات الأمن السيبراني من قبل الدولة لكي تتمكن من تأمين البني التحتية وخدمات الأمن السبراني لتحقيق مستقبل رقمي آمن للأجيال القادمة.

**التوصيات**

1-يجب أن تكون هناك توعية من قبل الأفراد والمؤسسات بخطورة الجرائم الإلكترونية عمليات الاختراق وتدريب العاملين على كيفية تجنبها أو على الأقل قد عامل معها بشكل آمن لتحقيق أقل الخسائر الممكنة.

2-استخدام أحدث برامج الحماية والإصدارات الحديثة ضد الفيروسات والاختراق أصبح أمر في غاية الأهمية وضرورة ملحة للحد من عملية الاختراق أو إيقافها.

3-يجب على مستخدمي الشبكات تغيير كلمة المرور الخاصة بهم بين الحين والآخر واختيار كلمة مرور صعبة تتضمن العديد من الأرقام والرموز والحروف حتى يصعب التنبؤ بها أو الوصول إليها من قبل مرتكبي الجرائم الإلكترونية.

4-عدم تحميل أي ملفات أو برامج مجهولة الهوية أو فتح أي بريد إلكتروني غير موثوق فيه حيث يستخدمها بعض المخترقون للوصول السهل إلى قاعدة البيانات والمعلومات فيجب على المستخدم التأكد من خلو الملفات أو البرامج من الفيروسات قبل فتحها.

5-سن قوانين رادعة لمرتكبي الجرائم الإلكترونية وتغليظ العقوبة من قبل الدولة ووجود تعاون دولي مشترك لكي تتمكن الدول من محاصرة مرتكبي الجرائم وإيجاد تشريع دولي موحد للقضاء على انتشار هذه الجرائم المستحدثة والتي يصعب اكتشافها لأنها تقع في إطار غير ملموس مما يزيد الأمر تعقيدا للسلطات الأمنية.

6-يجب على مستخدمي الإنترنت عدم تخزين البيانات الهامة في أماكن غير آمنة، بل يجب أن يحتفظوا بها في أماكن غير مصرح لغير المستخدمين للوصول إليها لكي تبقى في مأمن من أي هجمات إلكترونية.

7-عدم استخدام الشبكات العامة لأنه عندما تتصل بشبكة عامة فأنت تكون مشارك لكل شخص على هذه الشبكة وبالتالي أي معلومات مرسلها تكون معروضة على كل متصل ولهذا يجب تجنب استخدام مثل هذه الشبكات العامة تماما.

8-أه يمكن إنشاء جهات اتصال مركزية بسيطة للأمن السيبراني أو تعيين أوصياء مرشدين لتكنولوجيا المعلومات في المؤسسات لتقديم الدعم والمشورة وتدريب الموظفين على الممارسات الأمنية بالشركات.

9-عمل نسخ احتياطية من البيانات الهامة حتى تكون في مأمن في حال فقدانها أو التعرض للاختراق الأمني من أي جهة والاحتفاظ بها في أماكن لا يمكن الوصول إليها.

10-إنشاء بروتوكولات واضحة مع العملاء للتواصل وتبادل المعلومات والإصرار على اتصال مباشر مع أفراد محددين أو وجود كلمات مشفرة للتواصل خاصة في مجال المدفوعات والاتصالات المتعلقة بالشؤون المادية.

**المراجع العربية**

- الشهري, علي زايد محمد الجبيري& الشهراني, معلوي بن عبد الله. مشرف (2019). رؤية استراتيجية للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية. أطروحة دكتوراه جامعة نايف العربية للعلوم الأمنية

-- الشيتي، إيناس ابراهيم (٢٠١٩). تقييم سياسات أمن وخصوصية المعلومات في المؤسسات التعليمية بالمملكة العربي السعودية دراسة تطبيقية على جامعة القصيم، رسالة ماجستير غير منشورة، جامعة القصيم

الصانع, نورة عمر وآخرون. (2020). وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم. مجلة كلية التربية (أسيوط), 36(6), 41-90

الماحي , أسامه صلاح محمود. (2023). الجرائم المعلوماتية المهددة للأمن القومي المصري. مجلة البحوث القانونية والاقتصادية-المنوفية

جدي, مروة (2019). واقع الجريمة الالكترونية في مواقع التواصل الاجتماعي من وجهة نظر الطلبة الجامعيين- أطروحة دكتوراه- جامعة محمد بوضياف كلية العلوم الانسانية والاجتماعية- الجزائر

حشيفة, عبد الهادي. (2020). التعاون الدولي في مجال مكافحة الجرائم الإلكترونية. كلية الحقوق والعلوم السياسية جامعة زيان عاشور الجلفة – الجزائر

محمد, مديحة فخري محمود. (2020). دراسة مستقبلية لدور الجامعات المصرية في مواجهة الجرائم الإلكترونية لدي الطلاب. المجلة الدولية للعلوم التربوية والنفسية, 58(1), 28-71

**المراجع الاجنبية**

- Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & security, 105, 102248.

- Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-

attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186.

- Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. Journal of King Saud University-Computer and Information Sciences, 34(8), 5766-5781.

- Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011, October). The role of cyber-security in information technology education. In Proceedings of the 2011 conference on Information technology education (pp. 113-122).

- Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. International Journal of Advanced Research in Computer and Communication Engineering, 7(11), 125-128.

- Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015, November). An investigation on cyber security threats and security models. In 2015 IEEE 2nd international conference on cyber security and cloud computing (pp. 307-311). IEEE.