إستراتيجية الأمن الوطني في مكافحة الهجمات السيبرانية في التشريع الأردني

The National Security Strategy in Combating Cyberattacks in Jordanian Legislation

د.علي أحمد الزعبي[١] د.شيماء "محمد سعيد" الحسين[٢] د. برجس خليل أحمد الشوابكة[٣]

الملخص

تُعد الدراسات المتعلقة بالجريمة الالكترونية والأمن السيبراني إحدى أهم المحاور والملفات البحثية التي نالت اهتمام الدارسين في الأوساط الأكاديمية والباحثين القانونيين، كما يولي صناع القرار السياسي والأمني والعسكري اهتماماً بالغاً وواسعاً به، نظراً لخطورته وتأثيره على أمن وسيادة الدول.

وتهدف الدراسة الى استعراض أهم الإجراءات التي اتخذتها الأردن للحد من الهجمات السيبرانية خلال عام ٢٠٢٣ المنصرم وتوفير البيئة الآمنة للعمل عبر الشبكات والمحافظة على سلامة المعلومات. وعليه فقد اتبعت الدراسة منهج التحليل الوصفي للنصوص القانونية ذات العلاقة بموضوع البحث.

وقد خلصت الدراسة إلى أن الأمن السيبراني هو مجموعة الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية والبنى التحتية الحرجة من الهجمات السيبرانية، وجسد المشرع الأردني هذا المفهوم من خلال إصدار قانون الأمن السيبراني رقم (١٦) لسنة ٢٠١٩ وقانون الجرائم الإلكترونية رقم (١٧) لسنة ٢٠٢٣، بالإضافة إلى إنشاء الهيئة الوطنية للأمن السيبراني.

وفي ختام الدراسة أوصينا الحكومة إلى ضرورة تحسين التعاون الدولي مع دول الجوار ودول العالم بما يخص المعلومات الاستخباراتية المتعلقة بالتهديدات الإلكترونية وإعداد التقارير عن جميع الحوادث الإلكترونية.

كلمات مفتاحية: الأردن، الأمن السيبراني، الهجمات الإلكترونية، الإستراتيجية الأمنية.

---

[١] أستاذ القانون الجنائي المشارك – كلية الحقوق – جامعة البلقاء التطبيقية.
[٢] أستاذ القانون المدني المساعد – كلية الحقوق – جامعة عجلون الوطنية
[٣] أستاذ القانون الجنائي المساعد – كلية الحقوق – جامعة إربد الأهلية

Abstract

Studies related to cybercrime and cybersecurity have been one of the pivotal research areas that have garnered attention from academics, legal researchers, and policymakers alike. The seriousness and impact of cyber threats on national security and sovereignty have prompted profound interest from political, security, and military decision-makers.

The study aimed to review the key measures taken by Jordan to mitigate cyber-attacks during the past year, 2023, and ensure a secure working environment across networks while safeguarding information integrity. Consequently, the study employed a descriptive analysis approach to examine legal texts pertinent to the research topic.

The study concluded that cyber security encompasses a set of measures designed to protect information systems, networks, and critical infrastructures from cyber-attacks. The Jordanian legislature has embodied this concept through the enactment of Cybersecurity Law No. 16 of 2019 and Electronic Crimes Law No. 17 of 2023, in addition to establishing the National Cyber Security Agency.

In conclusion, the study recommended that the government enhance international cooperation with neighboring and global countries concerning intelligence on cyber threats and the preparation of reports on all cyber incidents.

Keywords: Jordan, Cybersecurity, Cyberattacks, Security Strategy.

المقدمة

يُعتبر الأمن السيبراني من المواضيع المعاصرة المهمة، وذلك لأن المؤسسات العسكرية والحكومية والمالية والشركات التجارية والمرافق الطبية تقوم بمعالجة وجمع وتخزين كم هائل من المعلومات والبيانات على أجهزة الحاسوب والأجهزة الذكية الأخرى، والتي يمكن أن يكون جزء من هذهِ البيانات معلومات سرية وحساسة سواء أكانت معلومات شخصية أو مالية أو ملكية فكرية أو أنواع أخرى من البيانات التي إذا تم الكشف عنها بطريقة غير مشروعة يترتب عليها نتائج سلبية مدمرة.

وأمام هذا الوضع وجدت دول العالم نفسها مضطرة إلى مواجهة تحديات الأمن السيبراني، لأنه لا توجد قواعد تحكم حروب الأمن السيبراني أمام الهجمات غير المشروعة، والواضح أن بعض الدول وخصوصاً الدول النامية لا تملك خطة وإستراتيجية مدروسة لتوفير الحماية لتعاملاتها ومعلوماتها الإلكترونية التي غالباً ما تتعرض لتطفل بعض القراصنة الذين يسرقون ويخترقون المواقع في سبيل

الحصول على معلومات مهمة وسرية يتم استغلالها لابتزاز أصحابها وتهديدهم مادياً ومعنوياً.

أهمية الدراسة:

تبرز أهمية الدراسة في أنها تلقي الضوء على موضوع قانوني دقيق وحديث، إذ يشكل التحدي الذي يواجه تكنولوجيا المعلومات وعالم الاتصالات.

مشكلة الدراسة:

تكمن مشكلة الدراسة في نشر الوعي بين الناس للحد من الهجمات السيبرانية وأن هذا الدور لا يقتصر على الدولة فحسب، بل يقع على عاتق كل مواطن اتخاذ إجراءات معينة لتقويض تلك الهجمات وهذا لا يتم إلا من خلال توضيح إستراتيجية الدولة.

تساؤلات الدراسة:

لهذه الدراسة تساؤلات، وتتمثل بما يلي:

١- ما المقصود بالأمن السيبراني ودوره في الحياة العملية في الوقت الحاضر؟

٢- مامدى علاقة الجريمة الالكترونية بالأمن السيبراني؟

٣- وهل للأمن السيبراني أبعاد استراتيجية؟

٤- هل يواجه الأردن تحديات أمنية؟

أهداف الدراسة:

تهدف الدراسة إلى توضيح مفهوم الأمن السيبراني وبيان أنواعه وأهميته وفوائده والبحث في التحديات الأمنية مع استعراض أهم الإجراءات التي اتخذتها المملكة الأردنية الهاشمية للحد من الخروقات الأمنية السيبرانية.

منهج الدراسة:

انتهجت هذهِ الدراسة المنهج التحليلي الوصفي من خلال تحليل النصوص القانونية ذات العلاقة بموضوع البحث في سبيل التوصل إلى حلول قانونية لإشكاليات الدراسة.

الدراسات السابقة:

بيّن الشيتي (الشيتي، ٢٠١٩) تقييم سياسات الأمن والخصوصية في المؤسسات التعليمية في السعودية، وخلصت إلى ضرورة وجود برامج لتوعية موظفي الدولة وتشجيع البحث في المجال السيبراني وأهمية صحة وتكامل البيانات في المؤسسات التعليمية، ودراسة (الهيسي وآخر، ٢٠١٨) تركزت هذه الدراسة على محاولة إيجاد اطار لحوكمة الأمن السيبراني في المؤسسات التعليمية في المغرب واستعرضت فوائدها الإدارية والمادية والأكاديمية، وأيضا دراسة العتيبي

(العتيبي، ٢٠١٧) ذهبت هذه الدراسة إلى استعراض دور الأمن السيبراني في تعزيز الأمن الإنساني من خلال إجراء الدراسة على عينة من العاملين في شركة أرامكو السعودية، طبقت استبانة لجمع المعلومات من العينة التي يتم الدراسة عليها.

المبحث الأول: ماهية الأمن السيبراني

Chapter One: The Nature of Cybersecurity

يُعد الأمن السيبراني من أهم التحديات الأمنية في الوقت الحاضر التي لاقت إشكالية في فهمها ومسايرتها خاصة بالنسبة للدول النامية، مما جعلها ميداناً خصب للباحثين في الأوساط المعرفية والأكاديمية، لإيجاد منهج يسهل على صانع القرار الوصول إلى حلول قانونية، وعليه سنقسم هذا المبحث إلى مطلبين.

المطلب الأول: التعريف بالأمن السيبراني

Section One: Definition of Cybersecurity

باعتبار الأمن السيبراني وسيلة للحد من الهجمات على أجهزة الحاسوب والشبكات والبرمجيات، وعلى ضوء ما تقدم سنقسم هذا المطلب إلى ما يلي:

الفرع الأول: مفهوم الأمن السيبراني

First Subsection: The Concept of Cybersecurity

الأمن السيبراني لغةً: الأمن هو نقيض الخوف، أي بمعنى السلامة. والأمن مصدر الفعل أمنَ أمناً وأماناً وأمنةً: أي اطمئنان النفس وسكون القلب، السيبراني (Cyber) لفظة يونانية مشتقة من كلمة (Kybernetes) بمعنى "الشخص الذي يدير دفة السفينة حيث تستخدم مجازاً للمتحكم"[١].

أما اصطلاحاً: فهو منهاج عمل تقوم به بعض الهيئات والدول المختصة بتوفير الحماية للبرامج والأنظمة من الهجمات السيبرانية والتي تهدف إلى الحصول على المعلومات الحساسة لاستغلالها أو إتلافها أو استخدامها لابتزاز الدول والمؤسسات بمقابل مادي[٢].

وتعريفه قانوناً: "هو الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الأمن السيبراني والقدرة على استعادة عملها واستمراريتها سواء أكان الوصول إليها بدون تصريح أو سوء استخدام أو نتيجة الإخفاق في إتباع الإجراءات الأمنية أو التعرض للخداع الذي يؤدي لذلك"[٣].

ويمكن أن نعرف الأمن السيبراني أنه الإجراءات التي تتخذها الدولة لتأمين البيانات والمعلومات الحساسة من خطر الاستيلاء والاختراق للمحافظة على الأمن الوطني وحماية الخصوصية والسرية للبيانات الشخصية للمواطنين.

الفرع الثاني: تمييز مصطلح الأمن السيبراني عما يشتبه به:

Second Subsection: Distinguishing the Term Cybersecurity from Similar Concepts

يكون نهج الأمن السيبراني محدداً مكون من عدة طبقات لتوفير الحماية للشبكات والبيانات وأجهزة الكمبيوتر التي ينوي الشخص حمايتها، لذا توجد العديد من المصطلحات التي تتشابه مع الأمن السيبراني منها:

أولاً: الفضاء السيبراني (Cyber space): عبارة عن محيط تفاعلي رقمي يشمل عناصر منها المادية وغير المادية، مكون من مجموعة من أنظمة الشبكات والأجهزة الرقمية والبرمجيات والمستخدمين ويطلق عليه بـ (الذراع الرابعة للجيوش المعاصرة).

ثانياً: الجريمة الإلكترونية[٤]: هي التعدي الذي يرتكب ضد المجموعات والأفراد بدافع الحرية ونية الإيذاء سواء أكان إيذاء مادي أو معنوي وأداة الجريمة هي شبكات الاتصالات الذكية.

ثالثاً: الجريمة السيبرانية (Cyber-crime): أي عمل غير مشروع يتم بواسطة أجهزة إلكترونية عبر الشبكة العنكبوتية الانترنت، وهي جزء من الجريمة الإلكترونية إلا أنها تختلف عن الأخيرة من حيث النية إذ قد ترتكب الجريمة السيبرانية بدافع الفضول أما الجريمة الإلكترونية بهدف الإيذاء[٥].

رابعاً: عمليات الأمن السيبراني: هي الإجراءات الخاصة بمراقبة واكتشاف الخروقات والتهديدات السيبرانية التي تقع ضمن نطاق القضاء السيبراني ووضع خطط تنفيذها والاستجابة لها.

الفرع الثالث: مفاهيم مرتبطة بالأمن السيبراني

Third Subsection: Concepts Related to Cybersecurity

في إطار رفع مستوى الأمن السيبراني وتعزيزه في مجال الاتصال، ومن أجل خلق الاستقرار والائتمان في التعامل ظهرت أنواع متعددة من الأمن السيبراني، والتي سنوضحها كالآتي:

أولاً: برامج مكافحة الفيروسات (Antivirus): تقوم بكشف وفحص أنظمة الكمبيوتر بحثاً عن التهديدات.

ثانياً: أمن الشبكات (Network Security): يوفر الحماية لمرور البيانات من خلال الشبكة، وذلك عن طريق التحكم بالاتصالات الصادرة والواردة ومنع التهديدات من دخول الشبكة.

ثالثاً: التشفير: هو تشفير البيانات وجعلها غير مفهومة، لمنع سرقتها أثناء النقل.

رابعاً: إدارة الهوية والوصول (IAM): هو مراقبة الوصول إلى الشبكات لمنع الهجمات غير المشروعة على الأنظمة الداخلية.
خامساً: أنظمة منع فقد البيانات (DLP): يوفر الحماية للبيانات وقواعدها أثناء تخزينها أو انتقالها خلال الشبكة.

المطلب الثاني: أهمية الأمن السيبراني

Section Two: The Importance of Cybersecurity

أصبحت المملكة الأردنية الهاشمية تولي اهتماماً واسعاً للأمن السيبراني، وتوظف البعد التكنولوجي والافتراضي والرقمي في تنظيم الشأن العام محلياً وإقليمياً ودولياً، لأنه متعلق بمخاطر خارجية مصدرها الانترنت، خصوصاً عدم استقرار المنطقة ومحاولة الكثير من الأطراف ضرب استقرار المملكة وسلامة أراضيها، وتأسيساً على ما تقدم تظهر أهمية الأمن السيبراني وأبعادهِ وهذا ما سنبينه كما يأتي:

الفرع الأول: فائدة الأمن السيراني

First Subsection: The Benefits of Cybersecurity

في الوقت الحاضر العالم مترابط بواسطة الشبكات، وجميع سكان الكرة الأرضية يستفيد من برامج الدفاع السيبراني، وتتمثل أهمية الأمن السيبراني كما يأتي:

أولاً: توفير البيئة الآمنة للعمل عبر شبكة الانترنت.
ثانياً: المحافظة على سلامة المعلومات وتجانسها، وذلك بمنع العبث بها وتحقيق جاهزية البيانات والمعلومات ووفرتها.
ثالثاً: اكتشاف الثغرات ونقاط الضعف في الأنظمة المعلوماتية ومعالجتها.
رابعاً: تكوين درع واقي للبيانات والمعلومات وحماية الشبكات والأجهزة ككل.
خامساً: توفير السرية من خلال التحكم بالولوج إلى المعلومات والبيانات.
سادساً: حماية المعلومات والبيانات والحفاظ على سلامتها من السرقة والهجمات التخريبية[٦].

الفرع الثاني: الأبعاد الإستراتيجية للأمن السيبراني

Second Subsection: The Strategic Dimensions of Cybersecurity

بما أن الأمن السيبراني يتعامل مع جميع التهديدات بناءً على منطق استباقي علمي قائم على التوقع والاحتمال والتركيز على الأبعاد الإستراتيجية للأمن السيبراني للحفاظ على منظومة الأمن الأردنية وهي على النحو الآتي:

أولاً: البعد العسكري.

بتقوية المنظمة العسكرية الأمنية من خلال ربط جميع الوحدات العسكرية بالعالم الافتراضي مما يسهل تبادل المعلومات والذي ينعكس بصورة إيجابية على حماية القدرات الهجومية والدفاعية وتحقيق الأهداف العسكرية(٧).

ثانياً: البعد الاجتماعي.

يتمثل بتأمين منصات التواصل الاجتماعي ومواقع السوشيال ميديا، وذلك لأنها خلقت فضاء تواصلي غير مسبوق مما يسهل على المخترقين استخدام برامج مضادة وفتح حروب افتراضية بين الفئات البشرية داخل الدول التي تحمل هويات وأيديولوجيات متناقضة، وعليه لا بد من توعية المواطن بالأخطار المترتبة على الاستخدام الخاطئ لمواقع السوشيال ميديا لتحقيق الأمن السيبراني ببعده الاجتماعي(٨).

ثالثاً: البعد السياسي.

تُعد السياسة عصب الحياة للمجتمعات والدول على حدٍ سواء، مما قد يدفع الكثير من الصراعات على أرض الواقع بتحولها إلى صراعات افتراضية خاصة في الفترة الأخيرة إذ وظيفة القوة السيبرانية التغلب على الخصوم السياسيين من خلال ضرب المنظومة التكنولوجية وتنفيذ أجندات خاصة(٩).

رابعاً: البُعد الاقتصادي.

التوجه للاقتصاد الرقمي أصبح رهان المملكة الأردنية الهاشمية والشركات الاقتصادية الكبرى والمؤسسات العسكرية والأمنية والتي تسعى إلى تطوير قدراتها العلمية والسيبرانية لمنع أي محاولة اختراق خاصة في ظل الصراعات الإقليمية للمملكة(١٠).

وعلى ضوء ما تقدم يمكن القول إن الأبعاد الإستراتيجية المذكورة آنفاً لا بد من لزوم التركيز عليها وخاصة البعد العسكري والبعد الاقتصادي مع خلق جيل رقمي يستوعب ويفهم المخاطر الأمنية المترتبة عن الجرائم الالكترونية.

المبحث الثاني: التحديات والاستراتيجيات الأردنية في مجال الأمن السيبراني

Chapter Two: Jordanian Challenges and Strategies in the Field of Cybersecurity

تواجه الأردن شأنها شأن الدول الأخرى في المنطقة والعالم هجمات متنامية، نبهت حكومات الدول مؤخراً إلى الحاجة لاعتماد توجه منسق متكامل لغاية إدارة تلك المخاطر وتحديات الأمن الوطني.

وعليه سنقسم هذا المبحث إلى مطلبين.

المطلب الأول: التحديات الأمنية التي تواجه الأردن.

Section One: Security Challenges Facing Jordan

في هذا الجزء من البحث تبرز أهم التهديدات والثغرات الأمنية التي تعرضت لها أنظمة وشبكات المعلومات الحكومية في الأردن خلال العام ٢٠٢٣ وذلك على النحو الآتي:

الفرع الأول: التهديدات المتنامية.

First Subsection: Growing Threats

سنستعرض أبرز الحوادث الأمنية التي تعرضت لها المؤسسات والأفراد في الأردن وذلك على سبيل المثال وليس الحصر ومنها:

أولاً: الربع الأول من عام ٢٠٢٣.

وفقاً للإحصاءات التي تم إعدادها من قبل جهات الأمن السيبراني الأردني أن ٥% فقط من إجمالي البيانات والمعلومات الافتراضية المخزنة حول العالم آمنة، وهي نسبة قليلة جداً بالمقارنة مع أهمية تلك البيانات والمعلومات في الوقت الحاضر.

لذلك من المتوقع أن يصل الإنفاق على خدمات الأمن السيبراني في العالم إلى ١٧٠.٤ مليار دولار بحلول عام ٢٠٢٤ لمنع الهجمات السيبرانية[١١].

فعلى سبيل المثال أهم الحوادث التي تم رصدها في الربع الأول من عام ٢٠٢٣:

- رصد نشاط بعض أنواع البرمجيات الخبيثة المعروفة مثل Dark Comet ٢%، Raccon stealer ٦%، Lcedl D ٩٢%.
- تغيير محتوى (Defacements) لموقعين حكوميين.
- تسريبات لبيانات متعلقة بحسابات لـ (٢٥٤٥) لموظفي قطاع حكومي[١٢].
- من الثغرات المهمة المستخدمة في الهجمات السيبرانية هي البريد الإلكتروني (Ms Outlook).

وعليه بلغ عدد الحوادث السيبرانية خلال الربع الأول من عام ٢٠٢٣ (٥٦٣) حادثة استهدفت عدد من المؤسسات الحكومية والوزارات، وبلغت عمليات الاستجابة لتلك الحوادث (٢٤) عملية قام فريق التحقيقات بـ (٢٠) عملية تحليل رقمي للأدلة المرتبطة بهذه الحوادث.

ثانياً: الربع الثاني من عام ٢٠٢٣.

من المهم اليوم أن نعلم أن كل كلمات المرور البالغ عددها (٣٠٠) مليار كلمة التي تستخدمها المؤسسات والشركات والأفراد في جميع أنحاء العالم،

تتعرض بشكل مستمر للهجوم بواسطة البرامج المقرصنة الموضوعة في رسائل البريد الالكتروني، وتنوعت أهداف هذه الهجمات بين تحقيق المكاسب المادية أو الحصول على المعلومات.

ومن أبرز الحوادث التي رصدها الأمن السيبراني في هذهِ الفترة على سبيل المثال:

- رصد إعلانات لشراء شرائح اتصال Sim – Cards والتي يتم استخدامها لإرسال البريد غير المرغوب (Spam) أو إجراء مكالمات نصب واحتيال.
- رصد هجمات من نوع (Brute Force) على عدد من المؤسسات باستخدام بروتوكول (RDP) التحكم عن بعد من أنظمة التشغيل Ms Windows.
- رصد عدد من الهجمات على المؤسسات الحكومية لحجب الخدمة الموزعة (DDoS).
- رصد هجمات على شركتين أردنيتين بواسطة برمجيات الفدية.

وعليه بلغ عدد الحوادث السيبرانية في الربع الثاني والتي تعامل معها المركز (٥٢٤) حادثة استهدفت عدد من المؤسسات والوزارات الحكومية، وبلغ عدد عمليات الاستجابة للحوادث (٢٩) قام من خلالها فريق التحقيقات بإجراء (٣٢) عملية تحليل رقمي[١٣].

ثالثاً: الربع الثالث من عام ٢٠٢٣.

بلغ عدد الحوادث السيبرانية في الربع الثالث من عام ٢٠٢٣ والتي تعامل معها المركز الوطني الأردني (٤٥٣) حادثة استهدفت مواقع تابعة للحكومة والمؤسسات العامة والحيوية. وبلغ عدد عمليات الاستجابة (٢٠) عملية قام بها الفريق المختص بالاستجابة وأجرى (٢٢) عملية تحليل رقمي للأدلة المرتبطة بهذه الحوادث، ومن أهم الحوادث السيبرانية التي تم رصدها خلال هذه المدة:

- ٧% حوادث تصيد إلكتروني.
- ٨% برمجية الفدية.
- ٨% محاولات اختراق.
- ٧% عدم الالتزام بالسياسات.
- ٧٠% برمجيات خبيثة أخرى.

- بلغ عدد الثغرات في مؤسسات حكومية ومركز البيانات الحكومي (٨٢,٧٣٣) ثغرة وكان مجموع الثغرات الأمنية على المواقع الإلكترونية (٧٠٨) ثغرة لـ (٨٩) موقع.

رابعاً: الربع الرابع من عام ٢٠٢٣.

شهد الربع الرابع من عام ٢٠٢٣ زيادة ملحوظة بنسبة (٧٥%) مقارنة بالربع الثالث بالهجمات السيبرانية على المؤسسات الوطنية، نتيجة استخدام برمجيات وأنظمة غير محدثة وعدم الالتزام بدقة بالسياسات الأمنية مما سهل تنفيذ عدة عمليات خبيثة بهدف جمع المعلومات.

إذ تعامل المركز خلال هذه الفترة (٩١٥) حادثة استهدفت المؤسسات الحساسة والحيوية للدولة، وبلغت عمليات الاستجابة للحوادث السيبرانية والتي قام بها فريق الاستجابة (٣٠) عملية و(٣١) عملية تحليل رقمي.

ولوحظ انخفاض بنسبة (٥٠%) في أعداد المخاطر في الربع الأخير من عام ٢٠٢٣ بالمقارنة بالربع الثالث منه؛ وذلك مع استمرار رصد نقاط الضعف ورصد المخاطر وقد يعود السبب في هذا الانخفاض إلى الوعي المتزايد لدى المؤسسات الحكومية بتلك المخاطر وتطبيق إجراءات فاعلة تعمل على تقليص أو إزالة المخاطر والتقيد بالسياسات والإرشادات والتنبيهات التي قدمها المركز خلال الأشهر الماضية.

ولا بد من الإشارة أن أبرز نقاط الضعف والمخاطر الأمنية هي استخدام البرمجيات غير محدثة وغير مرخصة واستخدام بروتوكولات غير مشفرة (مفتوحة) ووجود خدمات داخلية مكشوفة على شبكة الإنترنت للمؤسسات.

والعديد من الثغرات التي تُستغل مرتبطة بأنظمة وبرمجيات منتهية الدعم أو غير محدثة، عليه لا بد من إتباع التوصيات الصادرة من الشركة المنتجة وتثبيت حزم التصحيح (Patches) لتقليل محاولات استغلال الثغرات من قبل المهاجمين.

بالإضافة إلى أننا لاحظنا انخفاض عدد الثغرات المرصودة في الربع الرابع بنسبة (٥٧%) تقريباً، ويعود السبب إلى الجهود المبذولة من قبل المركز من توعية وتنبيه المؤسسات وحثها على تحديث الأنظمة التي تحتوي على تلك الثغرات الحرجة[١٤].

الفرع الثاني: جهات التهديد.Second Subsection: Threat Actors

تدل غالبية عمليات تسريب البيانات أنها تتم عن طريق برمجيات خبيثة تهدف بصورة أساسية إلى سرقة معلومات أو برمجيات (Info Stealers)، ومن أبرز تلك التهديدات هي:

أولاً: مجموعات التهديد المتطورة.

وهي نوع من القراصنة تمتلك مهارات متفوقة وموارد غير محددة، إذ تستخدم تقنية متطورة تمكنها من التخفي لأطول وقت ممكن لتحقيق أهداف معينة مثل حذف وتشفير البيانات أو سرقة معلومات حساسة.

ثانياً: برمجيات سرقة المعلومات.

هي نوع خبيث من البرمجيات يتم استخدامها من القراصنة لتحقيق هدف مادي بشكل أساسي، وتشمل على سبيل المثال: اللغة، الموقع، معلومات المستخدم.

ثالثاً: هجوم سلسلة التوريد.

هو من الهجمات الإلكترونية الذي يستخدم للحصول على بيانات أو أنظمة المؤسسة المستهدفة وهذا النوع من الهجمات يستلزم التخطيط لها بعناية.

رابعاً: هجمات الفدية (Ransom ware).

هذا النوع من الهجوم يشمل تشفير البيانات ومنع الوصول إليها إلا بدفع فدية.

خامساً: هجوم رفض الخدمة (DDoS).

عندما يستولي المهاجم على عدد من الأجهزة وإغراقها بعدد كبير من البيانات والطلبات.

سادساً: الهجمات على انترنت الأشياء (IoT).

ويتم ذلك من خلال الهجوم على أجهزة الاستشعار الصناعية وحرمانها من خدمة (DDoS) والحصول عليها بطريقة غير مشروعة على البيانات التي يتم جمعها في الجهاز.

سابعاً: حصان طروادة (Trojans).

نوع من أنواع البرامج الضارة والتي تكون مخفية على سبيل المثال في لعبة أو برنامج.

ثامناً: هجوم رجل في الوسط (MITM).

عندما يتوسط المهاجم بين المرسل ومستلم الرسائل الإلكترونية، ويقوم بالتعديل في مضمون الرسالة وإعادة إرسالها، وعادة ما يستخدم هذا الهجوم في الجيش لإرباك العدو.

تاسعاً: الخداع / التصيد (Phishing).

يتمثل هذا النوع من الهجوم بخداع مستلم الرسالة الإلكترونية بتنزيل برامج ضارة بالنقر عليها أو الكشف عن معلومات سرية[١٥].

المطلب الثاني: الإستراتيجيات الأمنية الأردنية.

Section Two: Security Strategies in Jordan

السياق الإستراتيجي للخطة الأمنية في الأردن تنص على: "أردن واثق وآمن ضمن العالم الرقمي ومقاوم للتهديد السيبراني" والتي وضحت الآلية لتحقيق أهدافها منها؛ الحماية والكشف والتحري والاستجابة والتطور. بالإضافة إلى أن الإستراتيجية حددت أبرز التهديدات التي تواجه الأردن وهي:

- الجريمة والفساد.
- خدمات الاستخبارات الأجنبية.
- القراصنة الناشطون.
- المطلعون الداخليون.
- الإرهاب والاضطرابات الجيوسياسية[١٦].

وعلى ضوء ما تقدم يمكن تحديد أهم الاستراتيجيات التي اتخذتها الجهات الأمنية في الأردن، كما يلي:

الفرع الأول: التشريعات الأردنية فيما يخص الأمن السيبراني.

First Subsection: Jordanian Legislation Related to Cybersecurity

وضع المشرع الأردني قوانين خاصة تعنى بحماية أمن المملكة الأردنية منها:

أولاً: قانون الأمن السيبراني رقم (١٦) لسنة ٢٠١٩ [١٧]

يهدف هذا القانون إلى بناء قدرات الأمن الوطني السيبراني ومواجهة التهديدات التي تتعرض لها البنى التحتية وأنظمة المعلومات، إذ تنص المادة (٣/أ) من هذا القانون على إنشاء مجلس يسمى بـ (المجلس الوطني للأمن السيبراني)[١٨]، وحددت مهامه وصلاحياته وفقاً للمادة (٤) منه؛ كما أقرت الاستراتيجيات والخطط والبرامج اللازمة لقيام المركز بواجباته ومهامه بما فيها برامج التعاون الإقليمي والدولي[١٩].

كذلك بينت المادة (٥/أ) من القانون ذاته بأن المركز مرتبط برئيس الوزراء ويهدف إلى إنشاء منظومة فعالة للأمن السيبراني وتنظيمها وتطويرها[٢٠].

ثانياً: نظام المركز الوطني للأمن السيبراني.

بموجب المادة (٥/أ) من قانون رقم (١٦) لسنة ٢٠١٩ إنشاء مركز وطني للأمن السيبراني، وعلى أثر هذا القانون تم إصدار نظام رقم (١) لسنة ٢٠٢٠ وهو نظام المركز الوطني للأمن السيبراني والذي حدد مهام هذا المركز منها:

- التنسيق بين المركز والجهات المختصة بالتحقيق في الجرائم والحوادث المتعلقة بالأمن السيبراني.
- بناء منصة مركزية لتبادل المعلومات بين مختلف فرق الاستجابة لحوادث الأمن السيبراني المحلية والدولية وإدارة قنوات الاتصال.
- الإشراف على قيام المركز بتقديم خدماته بما فيها فحص قابلية الاختراق وتقييم ومسح المخاطر والدعم الفني والاستشاري.
- ووفقاً للمادة (٤) من نظام المركز الوطني يتم التنسيق مع الأجهزة الأمنية والعسكرية لاتخاذ ما يلزم من إجراءات لمعالجة الأخطار السيبرانية[٢١].

ثالثاً: قانون الجرائم الإلكترونية الأردني لسنة ٢٠٢٣ [٢٢].

بيّن قانون الجرائم الإلكترونية رقم (١٧) لسنة ٢٠٢٣، جزاءات مقررة في حالة الاستعمال غير المشروع بالتكنولوجيا والإعلام والاتصالات وإجراءات مراقبة الاتصالات الإلكترونية وتفتيش وحجز ومصادرة المنظومة المعلوماتية وذلك في (٤١) مادة، وأبرز ما لفت نظري بالإضافة إلى العقوبات الرادعة في الفضاء الافتراضي أن المشرع الأردني أضفى الحماية القانونية للبيانات الشخصية، تأكيداً لأسمى نص في النظام القانوني الأردني ألا وهو الدستور هذا في إطار القواعد العامة إذ تنص المادة (٧) من الدستور الأردني على أن: "الحرية الشخصية مصونة، وكل اعتداء على الحقوق والحريات العامة أو حرمة الحياة الخاصة للأردنيين جريمة يعاقب عليها القانون"[٢٣].

وتأكيداً للمبدأ المتقدم نصت المادة (٤/٣٣) على أنه: "٤- الحفاظ على السرية"[٢٤]. فالمادة المتقدمة تشير إلى أنه لا يمكن المساس بالبيانات الشخصية دون أمر معلل من الجهة المختصة.

الفرع الثاني: الهيئة الوطنية للأمن السيبراني.

Second Subsection: The National Cybersecurity Commission

تُعد الهيئة الوطنية للأمن السيبراني مركزاً للدفاع السيبراني الفعال في التحري والاستجابة للحوادث، ويعتبر حلقة وصل بين قطاعات الدولة المختلفة مع المواطنين لتحقيق الأهداف الإستراتيجية.

ومن أهم مسؤوليات الهيئة هي:

- جمع وتحليل البيانات والمعلومات من مصادرها للإعلام عن تقدير التهديدات السيبرانية والإبلاغ عن سلوكيات الأشخاص المجهولي الهوية واتخاذ ما يلزم من إجراءات.

- توفير القدرات القانونية الضرورية لدعم إدارة جميع المتطلبات القانونية والتنظيمية.
- تحديد المتطلبات المستقبلية عن طريق التخطيط الاستراتيجي، فضلاً عن التحقق من الإمكانيات الحالية لضمان تفعيل مستويات الأمن السيبراني.
- حصر الأصول الوطنية الحساسة والمعرضة للتهديدات السيبرانية مع إدامة تقييم المخاطر التي تتعرض لها.
- تطوير فهم البيئة السيبرانية لمؤسسات القطاعين العام والخاص وذلك لزيادة التوعية بالتهديدات والتدابير الأمنية.
- وضع منهجية منسقة وتنفيذها لإدارة الحوادث السيبرانية وضمان احتوائها من قبل المؤسسات الحكومية.
- توفير وسائل وآليات لنشر وجمع التنبيهات السيبرانية لكل موظفي الدولة، وتتمثل الأولويات الرئيسية للهيئة الوطنية في القيادة والحوكمة من خلال قيادة التعاون على المستوى المحلي ودعم تبادل المعلومات بين جميع القطاعات وإنشاء علاقات دولية وإقليمية ملائمة من أجل التعاون بقضايا الأمن السيبراني من خلال الدخول في اتفاقيات دولية تساعد الأردن على التطور في مجال الأبحاث السيبرانية الهامة وفي الوقت نفسه تمكن الأردن من تقديم المجرمين السيبرانيين للعدالة، فضلاً عن تبادل المعلومات الاستخباراتية السيبرانية بين الأردن ودول العالم[٢٥].

الخاتمة

أصبحت الهجمات الإلكترونية هاجساً أمنياً يهدد دول العالم كافة مما يتطلب تأمين المعلومات والبيانات والمعاملات التي تعد قوام البيئة الرقمية.

وعلى ضوء ما تقدم تم إعداد الإستراتيجية الأمنية الأردنية بناءً على مجموعة شاملة من مؤشرات ومقاييس أداء الجهات الأمنية والتي لها الدور في حماية أنشطة المؤسسات الحكومية وغير الحكومية ورسم مستقبل الأردن وتعزيز أمن المعلومات.

وعليه توصلنا من خلال البحث إلى جملة من النتائج والتوصيات:

أولاً: النتائج.

١- الأمن السيبراني هو "الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الأمن السيبراني والقدرة على استعادة عملها واستمراريتها سواء أكان الوصول إليها بدون تصريح

أو سوء استخدام أو نتيجة الإخفاق في إتباع الإجراءات الأمنية أو التعرض للخداع الذي يؤدي إلى ذلك".

٢- اتضح من خلال البحث أن للأمن السيبراني فائدة كبيرة في توفير البيئة الآمنة للعمل عبر الشبكات والمحافظة على سلامة المعلومات واكتشاف الثغرات ونقاط الضعف في الأنظمة المعلوماتية.

٣- تبين لنا أن المشرع الأردني سعى جاهداً إلى توفير البيئة الآمنة للمعلومات في الفضاء السيبراني من خلال إصدار عدة تشريعات منها: قانون (١٦) لسنة ٢٠١٩ قانون الأمن السيبراني وقانون الجرائم الإلكترونية رقم (١٧) لسنة ٢٠٢٣.

٤- واتضح لنا اتخاذ الحكومة الأردنية إجراءات معينة لصد الهجمات السيبرانية منها إنشاء الهيئة الأردنية للأمن السيبراني، والذي يعد مركزاً للتحري والاستجابة للحوادث وهمزة وصل بين مؤسسات الحكومة والمواطنين لتحقيق أهدافه الإستراتيجية.

ثانياً: التوصيات.

١- أتمنى على الحكومة الأردنية السعي إلى إنشاء صناعة وطنية متعلقة ببرمجة نظم حاسوبية تطبيقية، تضمن حماية البنى المعلوماتية من هجمات القراصنة.

٢- نوصي وزارة التعليم العالي والبحث العلمي، بجميع كلياتها المتخصصة في هندسة الحاسوب وهندسة البرمجيات والمراكز الاستشارية ومراكز البحوث المتخصصة، بتهيئة قاعدة نظرية متينة لتقنيات الأمن المعلوماتي من خلال:

- اعتماد مادة (علوم التشفير Cryptography) ضمن المواد الدراسية لأقسام هندسة الحاسوب وعلوم الحسابات.
- إرسال البعثات العلمية إلى الدول التي أحرزت تقدماً واضحاً في مجال الأمن السيبراني.
- استحداث مادة بإسم (الحروب المعلوماتية) لجميع الاختصاصات العلمية.

٣- نحتاج كدولة إلى تحسين التعاون مع الدول الإقليمية والعالمية بخصوص المعلومات الاستخباراتية المتعلقة بالتهديدات الإلكترونية وإعداد التقارير عن جميع الحوادث الإلكترونية.

قائمة الهوامش

١. انظر: السمحان، منى عبد الله (٢٠٢٠)، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، بحث منشور في مجلة كلية التربية، جامعة المنصورة، العدد ١١١، ص٩.
٢. انظر: لطفي، وفاء (٢٠٢٢)، الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني: التجربة الماليزية نموذجاً، جامعة القاهرة، بحث منشور في مجلة كلية الاقتصاد والعلوم السياسية – المقالة ٥، المجلد ٢٣، العدد ١، ص١٥١-١٥٣.
٣. انظر: المادة (٢) من قانون رقم (١٦) لسنة ٢٠١٩، قانون الأمن السيبراني لسنة ٢٠١٩، منشور في الجريدة الرسمية عدد (٥٥٩٥)، صفحة ٥١٤٣، بتاريخ ٢٠١٩/٩/١٦.
٤. لم يعرف قانون الجرائم الإلكترونية الأردني رقم (١٧) لسنة ٢٠٢٣ الجريمة الإلكترونية وإنما ترك الأمر للفقه والقضاء.
٥. البداينة، ذياب موسى (٢٠١٤)، الجرائم الإلكترونية: المفهوم والأسباب، الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، عمان، الأردن، ص٣.
٦. انظر: السمحان، منى عبد الله، مرجع سابق، ص١٢.
7. Leho Martti, Neittaanmak Pekka. Cyber Security: Analytics, Technology and Automation, Switzerland: Springer International Publishing, 2015, web site: https://www.pdfdrive.com.
٨. تقرير منشور لمركز سينا التركي للدراسات السياسية، الأمن السيبراني: الهجرات السيبرانية، حروب غير مرئية، منشور في ٢٠٢١/٥/١٠، الرابط الإلكتروني: https://www.IFEGypt.ORG/NEWSDETAILS.ASPX?PAGE
٩. انظر: الزهراني، يحي مفرح (٢٠١٧)، الأبعاد الإستراتيجية والقانونية للحرب السيبرانية، بحث منشور في مجلة البحوث والدراسات، جامعة نايف للعلوم الأمنية، السعودية، العدد ٢٣، السنة ١٤، ص٢٢٦.
١٠. انظر: مرعي، إسراء جبريل رشاد (٢٠١٦)، الجرائم الإلكترونية: الأهداف – الأسباب – طرق الجريمة ومعالجتها، المركز الديمقراطي العربي، مقال منشور في موقع المركز، الرابط الإلكتروني: http://democraticac.de/?p=35426
١١. تقرير صادر عن هيئة الإعلام الأردنية، قسم الدراسات والاتصال والعلاقات العامة، الأمن السيبراني (٢٠٢١)، ص١١.
١٢. تقرير الموقف الأمني السيبراني الصادر عن المركز الوطني للأمن السيبراني، الربع الأول لعام ٢٠٢٣ info@ncsc.jo
١٣. تقرير الموقف الأمني السيبراني الصادر عن المركز الوطني للأمن السيبراني، الربع الثاني لعام ٢٠٢٣، info@ncsc.jo
١٤. تقرير الموقف الأمني السيبراني، الربع الرابع لعام ٢٠٢٣، المركز الوطني للأمن السيبراني، عمان، الجندويل، info@ncsc.jo .
١٥. الأمن السيبراني، إعداد هيئة الإعلام الأردني قسم الدراسات والاتصال والعلاقات العامة لعام ٢٠٢١.
١٦. الإستراتيجية الوطنية للأمن السيبراني ٢٠١٨-٢٠٢٣، مديرية السياسات والاستراتيجيات – استراتيجيات الحكومة الإلكترونية، وزارة الاتصالات وتكنولوجيا المعلومات، ص٢٩.
١٧. نشر في الجريدة الرسمية عدد (٥٥٩٥) على الصفحة ٥١٤٣ بتاريخ ٢٠١٩/٩/١٦.
١٨. انظر: المادة (٣/أ) من قانون الأمن السيبراني الأردني لسنة ٢٠١٩.
١٩. انظر: المادة (٤) من القانون ذاته.
٢٠. انظر: المادة (٥/أ) من القانون ذاته.
٢١. انظر: المادة (٤) من نظام المركز الوطني للأمن السيبراني رقم (١) لسنة ٢٠٢٠ المنشور في العدد (٥٦١٤) صفحة (١) بتاريخ ٢٠٢٠/١/٢.
٢٢. منشور في العدد (٥٨٧٤) على الصفحة (٣٥٧٩) بتاريخ ٢٠٢٣/٨/١٣ والساري بتاريخ ٢٠٢٣/٩/١٢.
٢٣. دستور المملكة الأردنية الهاشمية لعام ١٩٥٢ المعمول به.
٢٤. قانون الجرائم الإلكترونية الأردني لعام ٢٠٢٤.
٢٥. الأمن السيبراني، هيئة الإعلام، قسم الدراسات والاتصال والعلاقات العامة، مرجع سابق، ص١٨.