

مقترح الدراسة

أهمية حماية المعلومات في ظل تصاعد هجمات القرصنة الإلكترونية:
دراسة ميدانية في المملكة العربية السعودية

The importance of protecting information in light of the
escalation of piracy attacks: A field study in the Kingdom of
Saudi Arabia

إعداد الدراسة:

سلمى محمد الخياط ٥١٩٢٠٠٠٢١٢٠٠ - قائد الفريق

٢٠٢٢٠٠٥٦٧٧	سعد محمد الشهراني	٢٠٢٢٠٠٦١٢٢	فارس راشد الزهراني
٢٠٢٢٠٠٥٥٧٩	محمد عبد الرحمن العضياني	٢٠٢٢٠٠٦١٤٧	حسن عمر الزبيدي
٢٠٢١٢٠٠٥١٣٧	خالد محمد حكيم	٢٠٢٢٠٠٦١٨٧	ماجد عوض السرحاني
٢٠٢٢٠٠٦٢٣٠	عبد الله محمد الفضلي	٢٠٢٢٠٠٥٧٢٠	جمانه هاني المتروك

منصور عبد الله الزامل ٦٠٨٢٠٠٠٢٢٢٠

إشراف:

د. وليد سليمان

الفصل الدراسي الثالث

المقدمة

إن قضية أمن وحماية المعلومات تعتبر من قضايا العصر الهامة نظراً لدورها الفاعل في تحقيق التنمية الاقتصادية والاجتماعية والإدارية و الثقافية، حيث تعتمد عليها اغلب الاقتصادات سواء في الدول المتقدمة منها او الدول النامية بهدف تحسين الأداء، وخفض التكاليف، وتقديم افضل الخدمات. وقد أصبحت المعلومات ثروة وطنية يجب الحفاظ عليها. ومع ازدياد أهمية هذه المعلومات ازدادت المخاطر التي تتهدها، وتنوعت دوافع المجرمين تجاهها، وما يترتب عليها من تعرضها للخطر الجسيم. فالعديد من المعلومات والأنظمة والبنى التحتية المتصلة بالشبكات عرضة للخطر بين الحين والآخر، حيث تواجه بشتى انواع الخروقات ، كما تتعرض لأنشطة إجرامية (هاكرز) تعطل خدماتها وتدمر ممتلكاتها ، وتختلف هجمات الهاكرز من جهة لأخرى ، ومن مكان لآخر ومن زمن الى زمن مستخدمة أدوات وآليات اختراق متجددة ومتطورة طول الوقت. لذلك تضاعفت الجهود لمكافحة هذه الجرائم سواء التي تستهدف الحاسب الآلي وما يرتبط به من برامج، أو شبكة الإنترنت والأنظمة العاملة عليها، أو البريد الإلكتروني. وشملت اهم المخاطر او الجرائم التي تهدد امن المعلومات التلصص، وسرقة المعلومات، أو اعتراضها، وتشويهها، أو حتى تحويل مسارها. كما اصبح بالإمكان قرصنة هذه المعلومات واعتراضها، وكشف سريتها، مما يؤدي إلى خلق تحدٍ جديد أمام مختصي أمن المعلومات.

ولقد شكلت التعاملات بالوسائل الإلكترونية قوة التطور في التبادل المعلوماتي بين الأفراد، والشركات، والجهات الحكومية. لذلك أصبحت حماية هذه الوسائل او المعلومات ضرورة من ضرورات التطور التقني في العصر الحديث. لذا سنحاول من خلال أطروحة (أهمية حماية المعلومات في ظل تصاعد هجمات القرصنة الإلكترونية) دراسة المخاطر على المعلومات والعمل لتحقيق أمنها خاصة في ظل تصاعد القرصنة الإلكترونية حاضراً ومستقبلاً، وازدياد وتيرة الهجمات السيبرانية في الآونة الأخيرة وما تتسبب به من تأثيرات مدمره، أمنياً واقتصادياً ، واستخدامها كذلك كأدوات إدارة حروب وصراعات المستقبل، بالنظر لما تتسم به من انخفاض في التكلفة، وصعوبة الجهات التي تقف ورائها. ولعل ما يفاقم من مخاطر هذه الهجمات هي العقوبات التي تحول دون تطبيق مبادئ القانون الدولي عليها، ما يجعل من الصعوبة معاقبة الجهات التي تقف ورائها.

مشكلة الدراسة

برزت في الآونة الأخيرة ظاهرة القرصنة الإلكترونية والتي تهدف بالأساس إلى الاستيلاء على المعلومات الهامة سواء بين الشركات المتنافسة أو بين دول ضد بعضها البعض، وتلك ظاهرة خطيرة يجب الحذر منها وخاصة في المؤسسات الحيوية في الدولة التي تحتوي على معلومات خطيرة تمس أمن الدولة واستقرارها، ولذلك تكمن معضلة هذا البحث في (التعرف على أهمية حماية المعلومات في ظل تصاعد هجمات القرصنة الإلكترونية والتأثيرات المتعددة على المعلومات وخاصة في المؤسسات الحيوية والعلاقات بين الدول وسبل مكافحتها وما هو مستقبلها في ظل التقدم التقني).

أهمية الدراسة

تكمن الأهمية العلمية لهذه الدراسة في انها إضافة معرفية من خلال تتبع الدراسات السابقة والمفاهيم والنظريات التي تناولت ظاهرة القرصنة الإلكترونية وأهمية حماية المعلومات ودوره في حماية المصلحة العامة ومصالح المستخدمين والمحافظة على سرية الاتصالات وأمن المعلومات، وفقاً لأعلى معايير الجودة والأمان. لذا يعتبر هذا البحث أداة قيمة للمؤسسات العامة والخاصة التي ترغب في تعزيز أمنها الإلكتروني وحماية المعلومات والحد من مخاطر القرصنة الإلكترونية التي قد تتعرض لها هذه القطاعات. كما تكمن أهمية هذا البحث في المساهمة في إيجاد طرق لمواجهة القرصنة الإلكترونية بطريقة أكثر فعالية، وفي التوعية المجتمعية حول مخاطر استمرار القرصنة الإلكترونية في المستقبل بتهديد الإبداع والابتكار والسيطرة على معلومات وبيانات غاية في السرية قد تستخدم استخداماً سيئاً لتدمير دولة ما أو مجتمع معين.

كما تكمن الأهمية العملية في انها تسلط الضوء على أحد المواضيع الرئيسية المتمثل في حماية المعلومات للحد من القرصنة الإلكترونية في القطاعات الحكومية والخاصة للمملكة العربية السعودية. كما تسلط الضوء على جوانبه الإيجابية والمشكلات والتحديات التي تعترضه. وتعتبر هذه الدراسة ذات فوائد هائلة لهذه القطاعات المختلفة في المملكة العربية السعودية كونها توضح الدور الاستراتيجي لتطبيق استراتيجية أمن المعلومات في الحد من هجمات القرصنة الإلكترونية.

أهداف الدراسة

- نظراً لأهمية حماية المعلومات في ظل تنامي القرصنة والهجمات الإلكترونية، تهدف هذه الدراسة الى تحديد أهمية حماية المعلومات في ظل تصاعد هجمات القرصنة الإلكترونية من خلال اجراء دراسة ميدانية في المملكة العربية السعودية، وما ينبثق عن هذا الهدف من اهداف فرعية تتمثل فيما يلي:
- أ. دراسة أمن المعلومات في ظل تطور التقنية الرقمية ، والتعرف على القرصنة الإلكترونية وتأثيراتها.
 - ب. تحديد التأثيرات الاقتصادية والعسكرية والسياسية التي قد تنشئ عن القرصنة الالكترونية وسبل حماية البيانات والمعلومات المتعلقة بهذه القطاعات.
 - ج. تحديد التشريعات والتنظيمات والضوابط التي سنتها المملكة العربية السعودية للحد من اضرار القرصنة الالكترونية وتأثيراتها المدمرة ائقتصادياً وسياسياً وعسكرياً.

أسئلة الدراسة

- لقد تم إعداد هذه الدراسة للإجابة على السؤال الرئيسي: "ما أهمية حماية المعلومات في ظل تصاعد هجمات القرصنة الإلكترونية"، كما تفرعت عن هذا السؤال عدد من التساؤلات الفرعية أهمها:
- أ- ما أهداف القرصنة الإلكترونية ، وما هي التأثيرات المتعددة للقرصنة الإلكترونية على المعلومات؟
 - ب- كيف يمكن حماية المعلومات في ظل تصاعد القرصنة الإلكترونية ؟ وماهي التشريعات والتنظيمات والضوابط التي يمكن اعتمادها للحد من اثارها المدمرة في ظل رؤية المملكة ٢٠٣٠م.
 - ت- ما هو مستقبل القرصنة الإلكترونية في ظل التقدم التقني ؟

الدراسات السابقة والإطار النظري

سيقوم الباحثون بجمع المراجع المختلفة ودراستها بتمعن واختيار المراجع الجديرة بالرجوع إليها والاعتماد على معلوماتها كمراجع أصلية لهذا البحث. كما سيقوم بكتابة الفصول، وتقسيم المشروع إلى عدة فصول أهمها المقدمة والاطار النظري والدراسات السابقة وتحليل البيانات ومناقشة النتائج والخاتمة والتوصيات حسبما حدده دليل مقرر مشروع التخرج، وقد قام الباحثون بتقسيم الفصل الثاني الى عدة محاور ، يشمل الجزء الأول من

الفصل الثاني- الاطار النظري ، و يتضمن الجزء الثاني من الفصل الثاني – الدراسات السابقة . وقد تم ادراج كافة الدراسات السابقة المقترح اعتمادها في هذه لدراسة في قسم الملاحق.

المنطلقات النظرية للدراسة

تكمن أهمية هذه الدراسة في انها ستجرى ضمن سياقات تاريخية وثقافية واقتصادية متنوعة وتستند لمنطلقات نظرية ومنهجية تعكس تلك السياقات . كما ان معرفة طبيعة الإشكاليات التي سيحاول الباحثون الإجابة عنها والفرضيات التي سيتم طرحها، تاتي من خلال الارتكاز على جملة من النظريات و الاستناد إلى إجراءات منهجية ملائمة. سيتم معالجة المنطلقات النظرية التي يستند اليها هذا البحث في تحليل لظاهرة وكيفية حماية البيانات او المعلومات للحيلولة دون حدوث أي هجمات قرصنة الكترونية وكذلك المقاربات والأسس والأدوات المنهجية المتبعة في هذه الدراسة.

المنهجية وطرق البحث

ستعتمد الدراسة على المنهج الاستقرائي في إعداد الجزء النظري، حيث سيتم استقراء المواضيع والدراسات المتعلقة بموضوع البحث وذلك لتكوين الإطار النظري. اما في الجانب العملي فستعتمد الدراسة على المنهج الوصفي التحليلي في الحصول على كافة المعلومات والبيانات اللازمة لتحقيق اهداف الدراسة واغراضها. ويتمثل المنهج الوصفي التحليلي فيما يلي:

(١) المنهج الوصفي كونه منهجًا يناسب أهداف الدراسة الحالية. ويتمثل المنهج الوصفي طريقة لوصف الموضوع المراد دراسته من خلال منهجية علمية صحيحة، وتصوير النتائج التي يتم التوصل إليها على أشكال رقمية معبرة يمكن تفسيرها (المحمودي، ٢٠١٩). ويتضمن وصف متغيرات الدراسة المستقلة والمتمثلة في أهمية حماية المعلومات ، والمتغير التابع المتمثل في تصاعد هجمات القرصنة الإلكترونية.

(٢) المنهج التحليلي ويهدف الى تحليل وتقييم أهمية حماية المعلومات في ظل تصاعد هجمات القرصنة الإلكترونية. كما سيعتمد الباحثون إلى جمع البيانات بعدة طرق، أهمها:

- البيانات الثانوية، من خلال المراجعة والمسح للدراسات السابقة، والكتب والمقالات والتقارير والرسائل الجامعية، وشبكة الإنترنت ، وذلك لوضع الأسس العلمية والإطار النظري لهذه الدراسة.
- البيانات الأولية من خلال المصادر الميدانية، حيث سيتم تطوير استبانة تشمل كافة محاور الدراسة.

أدوات الدراسة

سيتم استخدام الاسنينة كأداة للدراسة لجمع اراء ووجهات نظر افراد العينة وسيتم توزيعها عن طريق البريد الالكتروني. ستشمل عينة الدراسة (١٠٠) مفردة من العاملين المختصين في الامن السيبراني في المملكة العربية السعودية. وسيتم استخدام برنامج (SPSS) لتحليل كافة البيانات الإحصائية التي تم جمعها من افراد العينة.

مجالات الدراسة

تتمثل مجالات الدراسة بما يلي:

- المجال الموضوعي: أهمية حماية المعلومات في ظل تصاعد هجمات القرصنة الإلكترونية.
- المجال المكاني: سيطبق هذا البحث على عدد من القطاعات الحكومية والخاصة في المملكة العربية السعودية.
- المجال الزمني: سيتم إعداد هذا البحث في العام ١٤٤٤ هـ / ٢٠٢٣ م
- المجال البشري: يضم مجتمع الدراسة عدد من المختصين في مجال حماية المعلومات والعاملين في مجال الامن السيبراني وعدد من الجهات ذات العلاقة بهذا الموضوع.

التبويب المقترح وفق الخطة الزمنية

يضم التبويب المقترح لاعداد هذه الدراسة عدد من الأبواب وفصول والمباحث التي سيتم مناقشتها بالتفصيل وتتمثل اهم هذه الأبواب والفصول ما يلي :

أ. الباب الاول (نبذة عن القرصنة الإلكترونية وعلاقتها بالمعلومات). في هذا الفصل سيتم التطرق إلى مفهوم القرصنة الإلكترونية، والتطرق إلى أهداف وطرق القرصنة الإلكترونية، وبيان علاقة القرصنة الإلكترونية بالمعلومات.

ب. الباب الثاني (تأثيرات القرصنة على المعلومات). من خلال هذا الفصل سوف نتعرف على تأثير القرصنة الإلكترونية على معلومات المؤسسات الحيوية للدولة، على الاقتصاد العالمي، وعلى العلاقات بين الدول.

ج. الباب الثالث (سبل حماية المعلومات من القرصنة الإلكترونية). سوف يتم في هذا الفصل عن تحديث

القوانين المتعلقة بالقرصنة الإلكترونية، اختيار برامج فعالة لمكافحة التجسس، ويقدم الباحثون مقترحات لحماية المعلومات من القرصنة الإلكترونية.

د. الباب الرابع (نظرة مستقبلية للقرصنة الإلكترونية في ظل التقدم التقني). في هذا الفصل سيتم استشراف

المستقبل من خلال تحديات المجتمع المعلوماتي مستقبلاً، مستقبل العالم الأمني في ظل تصاعد عمليات القرصنة الإلكترونية، ومستقبل العالم الاقتصادي في استمرار عملية القرصنة الإلكترونية.

إضافة الى (الدراسات السابقة) حيث سيتم انتقاء واختيار عدد من الدراسات العربية والأجنبية التي ناقشت الموضوع من جوانبه المختلفة.

قائمة المراجع والمصادر المبدئية

المراجع العربية

- ❖ البابلي، عمار ياسر محمد زهير. (٢٠٢١). التحديات الأمنية المعاصرة للهجمات السيبرانية. الفكر الشرطي، مج ٣٠، ع ١١٨، ١٩ - ٨٣.
- ❖ التيماني، مداخل زيد عبدالرحيم. (٢٠٢١). واقع الوعي المعلوماتي بالأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بالأمن السيبراني. مجلة الخدمة الاجتماعية، ع ٦٧، ج ١، ٢٣ - ١.
- ❖ الجمل، حازم حسن أحمد. (٢٠٢٠). الحماية الجنائية للأمن السيبراني في ضوء رؤية المملكة ٢٠٣٠. مجلة البحوث الأمنية، مج ٣٠، ع ٧٧، ٢٤٣ - ٣٢٨.
- ❖ جوهرى، عزة فاروق عبدالمعبود، و حسن، طه محمد طه. (٢٠١٩). أمن المعلومات الرقمية وسبل حمايته في ظل التشريعات الراهنة. مجلة المركز العربي للبحوث والدراسات في علوم المكتبات، مج ٦، ع ١٢٤، ٨٥ - ١٣٢.
- ❖ حمد، معاذ أحمد عبدالرازق، و أحمد، نصر الدين حسن. (٢٠١٦). أمن المعلومات ودوره في الحد من القرصنة الإلكترونية المركز القومي للمعلومات: دراسة حالة (رسالة ماجستير غير منشورة). جامعة أم درمان، أم درمان.
- ❖ دلالي، الجيلالي، و بلبشير، يعقوب. (٢٠٢١). رهانات الأمن السيبراني الوطني في ظل التحول الرقمي: قراءة في التأصيل المعرفي واستراتيجية المواجهة التشريعية. مجلة كلية القانون الكويتية، مج ١٠، ع ٣٧، ٥٢٥ - ٥٧٦.
- ❖ شلوش، نورة. (٢٠١٨). القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول. مجلة مركز بابل للدراسات الإنسانية، مج ٨، ع ٢٤، ١٨٥ - ٢٠٦.
- ❖ الشوابكة، عدنان عواد. (٢٠١٩). دور إجراءات الأمن المعلوماتي في الحد من مخاطر أمن المعلومات في جامعة الطائف. دراسات وأبحاث. مج ١١، ع ٤، أكتوبر ٢٠١٩. ص ١٦٤-١٨٧.

- ❖ الشيتي، إيناس ابراهيم (٢٠١٩) تقييم سياسات أمن وخصوصية المعلومات في المؤسسات التعليمية بالمملكة العربي السعودية دراسة تطبيقية علي جامعة القصيم ، ماجستير غير منشورة، جامعة القصيم.
- ❖ الطاهري، عبدالفتاح. (٢٠١٩). الأمن المعلوماتي وعلاقته بالأمن القومي. مجلة الباحث للدراسات القانونية والقضائية، ع ١٠، ٢١ - ٦٥.
- ❖ العتيبي، عبد الرحمن بن بجاد (٢٠١٧) دور الأمن السيبراني في تعزيز الأمن الإنساني أطروحة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية.
- ❖ القحطاني، عادل بن محمد ; مسعد، محمد رئيس مشرف. ; حربة، محمد خالد مناقش. ; المبرز، عبد الله بن إبراهيم مناقش. (٢٠١٤) . تصور استراتيجي لتطوير أمن المعلومات تعزيزا للأمن الوطني في المملكة العربية السعودية بالتطبيق على شركة سابك. أطروحة (ماجستير)-جامعة نايف العربية للعلوم الأمنية.
- ❖ محمود عزت، (٢٠١٨)، الفضاء السيبراني وتحديات الأمن المعلوماتي العربي، المجلة العربية العدد ٤٩٨.
- ❖ محمود، لمى عبد الباقي، و كيطان، إسماء نادر. (٢٠٢١). المسؤولية الدولية عن الأضرار التي تحدثها الهجمات الإلكترونية. مجلة العلوم القانونية، مج ٣٦، عدد خاص ، ٣٣٦ - ٣٦٢.

المراجع الأجنبية:

- Al-Harbi, I. (2017). The Information Security in Kingdom of Saudi Arabia : Ulum Islamiyah. 22. 89-102.
- Kitsios, F.; Chatzidimitriou, E.; Kamariotou, M. (2022). Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. Sustainability, 14, 1269.
- Mokhor, V., Honchar S. and Onyskova, A. (2020). Cybersecurity Risk Assessment of Information Systems of Critical Infrastructure Objects, *IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, pp. 19-22.

Sureshkumar, V and Baranidharan, B (2021). A study of the cloud security attacks and threats. *Journal of Physics: Conference Series*. 1-12.

Vakulyk, O., Petrenko, P., Kuzmenko, I., Pochtovyi, M., & Orlovskyi, R. (2020). Cybersecurity as a Component of The National Security of The State. *Journal of Security & Sustainability Issues*, 9(3).

Wibowo, E. & Ramli, K. (2022). Impact of Implementation of Information Security Risk Management and Security Controls on Cyber Security Maturity (A Case Study at Data Management Applications of XYZ Institute). *Jurnal Sistem Informasi*. 18. 1-17.

الملاحق

الدراسة	الأهداف	المتغير المستقل	المتغير التابع	منهجية الدراسة	اهم النتائج والتوصيات
دراسة (كلاع، ٢٠٢٢) الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني	تهدف هذه الدراسة إلى تقديم دراسة تحليلية تحاول الإلمام بمدى أهمية موضوع الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول، وذلك من خلال التطرق إلى مختلف المفاهيم ذات الصلة كمفهوم الفضاء السيبراني، الجوسسة الإلكترونية، الأمن السيبراني،	الأمن السيبراني	تحديات الجوسسة والاختراقات الإلكترونية	تم الاعتماد في هذا البحث على المنهج التاريخي وكذا الإحصائي	لقد خلق الفضاء السيبراني تهديدات جعلت من باب الالاحاح أن تعتد الدول استراتيجيات مصممة لتحقيق الأمن السيبراني الوطني خاصة في ظل التحديات الراهنة. وستكون الغلبة في الفضاء السيبراني لمن يملك التقنيات المتقدمة ويتحكم بها بشكل منفرد، ما يجعل من يحقق ذلك يمتلك السيطرة في هذا المجال. واوصت الدراسة بضرورة تعزيز الدول لامنها السيبراني لمواجهة تحديات الجوسسة والاختراقات الالكترونية.
دراسة (إبراهيم، ٢٠٢٢) الفضاء الإلكتروني وأثره على الأمن القومي للدول: الحروب الإلكترونية نموذجاً	تهدف هذه الدراسة الى التعرف على ماهية الفضاء الإلكتروني ومكوناته الأساسية. والتعرف على أهم الخصائص التي تتميز بها الحروب الإلكترونية. ومعرفة الدور الذي تلعبه الحروب الإلكترونية على الأمن القومي. وكذلك معرفة أفضل السبل والإمكانات المتاحة لمواجهة هذ النوع من الحروب	الفضاء الإلكتروني	وأثره على الأمن القومي	اعتمدت الدراسة على التكامل المنهجي، وشملت هذه المناهج (المنهج الوصفي والتحليلي ودراسة الحالة والمنهج القانوني)	أن الفضاء الإلكتروني قد فرض نفسه كبُعد إستراتيجي جديد في الصراعات العالمية، على الرغم بما يتمتع به من خصائص عديدة. وزيادة التطور التكنولوجي الهائل تم توظيفه من الدول والفواعل غير الدولية في أعمال مهددة للأمن القومي لدول أخرى، حروب الفضاء الإلكتروني ليست كلها على نفس المستوى. وقد اوصت الدراسة بضرورة فهم وإدراك طبيعة الفضاء الإلكتروني واعتباره عنصر رئيسي في الأمن القومي، ضرورة تحديث الجيوش وتدريبها على هذه الحروب والاعتماد على تكنولوجيا المعلومات.

دراسة (شادي، ٢٠٢١)	تحديد تأثير أبعاد حوكمة تكنولوجيا المعلومات بأبعادها الرئيسية ممثلةً بكل من (التخطيط والتنظيم، الاكتساب والتنفيذ، الدعم والتوصيل، المتابعة والتقييم) في تعزيز أمن المعلومات في المصارف المدرجة في سوق دمشق لأوراق المالية.	دور حوكمة تكنولوجيا المعلومات	تعزيز أمن المعلومات	المنهج الوصفي التحليلي مع الاستعانة بأداة الاستبانة لجمع المعلومات	هناك خطة للحماية تتطلب المزيد من إجراءات إغلاق منافذ الاختراق والتدقيق في الإجراءات الداخلية والاحتفاظ بنسخة احتياطية من المعلومات. هناك تحديد دقيق للعناصر المتعلقة بتركيب وتشغيل النظام مثل: التدريب وحجم أداء البرمجيات التطبيقية وخطط التنفيذ وتحويل النظام والبيانات وفحص خطط واستراتيجيات التغيير. هناك نظام فاعل وكفؤ لمعالجة المشكلات التي تعترض سير العمل في الشركة ولكنه بحاجة لإعادة النظر في إجراءات معالجة المشكلات والوقاية منها. وأوصت الدراسة بضرورة تبني المصارف الخاصة السورية لمفاهيم حوكمة تكنولوجيا المعلومات باعتبارها إطار عام يمكن من خلاله حماية أمن المعلومات. وضرورة وضع الإطار التشريعي الخاص بأمن تكنولوجيا المعلومات من الجهات المختصة.
دراسة (دلالي و بلبشير، ٢٠٢١)	تحفيز إرادة الرسميين نحو تأسيس منظومة شاملة للسيبرانية في الجزائر، من خلال حزمة من الآليات التشريعية والمؤسسية لضمان مواكبة ثورة المعلومات، والإحاطة بكل مستجدات عالم السيبرانية	هانات الأمن السيبراني الوطني	التحول الرقمي	المنهج الوصفي التحليلي والمقارن	أن الأمن السيبراني أصبح يشكل جزءاً أساسياً من أي سياسة أمنية وطنية، وأن سوء الاستغلال المتنامي للشبكات الإلكترونية لأهداف إجرامية يؤثر سلباً على سلامة البنى التحتية للمعلومات الوطنية الحساسة لاسيما على المعلومات الشخصية والبنى التحتية الأمنية الاستراتيجية، كما انتهت إلى وجود قصور قانوني وتشريعي في معالجة تطورات الجرائم السيبرانية في بعدها الأمني والاستراتيجي. وأوصت الدراسة المشرع الجزائري بضرورة وضع منظومة وطنية شاملة لأمن الفضاء السيبراني وحمايته، وتعزيز البيئة القانونية بالأدوات اللازمة بالوقاية من الجريمة السيبرانية

					استباقيا، ثم بعد ذلك اعتماد آليات الردع. واوصت الدراسة ضرورة وضع استراتيجية لنشر الوعي وبنائه لدى مختلف شرائح المجتمع، سواء من كان منهم من المستخدمين العاديين أو المهنيين أو المسؤولين عن سياسات الأمن والسلامة، مما يقتضي تأمين انسجام الأنظمة القانونية المكافحة للجرائم السيبرانية.
دراسة (البابلي، ٢٠٢١)	تهدف الدراسة الى التعرف الى التحديات الأمنية المعاصرة للهجمات السيبرانية	التحديات الأمنية المعاصرة	الهجمات السيبرانية	المنهج الاستقرائي والوصفي	أن الحرب السيبرانية "حرب المعلومات" هي عمليات في الفضاء الإلكتروني تستخدم وسائل وأساليب قتال ترقى إلى مستوى النزاع المسلح بسبب ضعف الشبكات الإلكترونية والتكلفة الإنسانية المحتملة من جراء الهجمات السيبرانية، وتزداد التهديدات الناتجة من الفضاء الإلكتروني، وتستمر ظهور التحديات في ظل التغييرات الجذرية التي طرأت على حياتنا، والتحول إلى العمل من المنازل بسبب جائحة كورونا. واوصت الدراسة بضرورة إتخاذ كافة الإجراءات التأمينية السيبرانية لحماية وتأمين البنية التحتية الإلكترونية والتنبؤ بالجرائم والهجمات السيبرانية.
دراسة محمود و كيطان، (٢٠٢١)	يسلط البحث الضوء على موضوع جديد من مواضيع القانون الدولي وأهمها؛ والذي لا تزال تدور حوله علامات استفهام واختلاف في أغلب جوانبه، وخاصة فيما يتعلق بالمسؤولية الدولية عن الأضرار التي	المسؤولية الدولية	الأضرار التي تحدثها الهجمات الإلكترونية	المنهج الوصفي	الانكشاف الأمني لأسرار الدول بسبب التجسس والقرصنة وازدادت الهجمات على البنى التحتية للدول وأن سكوت الدول في بعض الأحيان وصعوبة معرفة المهاجم أو نسبة الفعل لدولة أو جهة معينة أدى إلى تفاقم المشكلة التي قد تتحول من مجرد هجوم إلى حرب على أرض الواقع، لذلك يجب تخطي مشكلة إخفاء هوية المهاجم وتفعيل نظام المسؤولية الدولية في هذا الفضاء لأنها الأساس للنظام القانوني الدولي كما يمكن من خلال

تحديثها الهجمات الإلكترونية في الفضاء الافتراضي				تفعيلها مواجهة الأخطار والحفاظ على الأمن السيبراني الذي أصبح مسألة مهمة في وقتنا الحاضر.
دراسة التيماني، (٢٠٢١). واقع الوعي المعلوماتي بالأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بأمن المعلومات	استهدف هذا البحث معرفة واقع الأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بأمن المعلومات	واقع الوعي المعلوماتي	بالأمن السيبراني	المنهج الوصفي
الجملي، (٢٠٢٠). الحماية الجنائية للأمن السيبراني في ضوء رؤية المملكة ٢٠٣٠	تهدف الدراسة الى معالجة حالات تدخل القانون الجنائي في مجال حماية الأمن السيبراني، وضوابطه، وصوره، وأهميته، وفاعليته، بالمعنى الواسع، وتشتمل على مجموع الأطر، والمفردات، والعناصر، والقيم، والأصول، والموجودات، والمقومات التنظيمية، والتقنية، والإدارية، والفنية، وهياكلها	الحماية الجنائية	للأمن السيبراني	المنهج الوصفي
إمكانية الاستفادة من منهج هذه الدول في الشأن السعودي، ويهدف تعزيز البيئة والاقتصاد. والاستثمار الرقمي في المملكة، بما يتوافق وطموحات المملكة حسب رؤية ٢٠٣٠ في جمال التحول الرقمي وتقنية المعلومات. اجراء المزيد من الدراسات المتعلقة بالأمن السيبراني واليات تعزيزه وتطوير تشريعاته في ضوء رؤية المملكة ٢٠٣٠.				

دراسة (جوهري وحسن، ٢٠١٩)	تهدف الدراسة الحالية إلى التعرف على المخاطر التي يتعرض لها أمن المعلومات الرقمية بأشكالها المختلفة والتدابير المضادة للحد من هذه المخاطر مثل التدابير التنظيمية والمادية والتقنية بالإضافة إلى التدابير التشريعية على المستويين الوطني والدولي وأهم المعايير الدولية التي تضعها منظمة الأيزو لضبط ممارسات أمن المعلومات.	أمن المعلومات الرقمية	والتدابير المضادة للحد من المخاطر مثل التدابير التنظيمية والمادية والتقنية والتشريعية	المنهج الوصفي التحليلي وذلك من خلال الاستعانة بالمصادر العلمية ذات العلاقة بأمن معلومات	أن أمن المعلومات يتعرض للعديد من المخاطر والتهديدات التي تتم في بيئة الإنترنت مع صعوبة مواكبة التدابير الأمنية المضادة لسرعة تطور الأساليب الحديثة المستخدمة في عمليات الاعتداءات على أمن المعلومات، ضعف التشريعات الموجودة على أرض الواقع سواء على المستوى الوطني أو الدولي مع وجود بطء ملحوظ في مدى كفاية التشريعات الموجودة للحد من عمليات التعدي على أمن المعلومات. واهتدت الدراسة بضرورة تدريب العاملين داخل نظام أمن المعلومات والقيام بالعديد من الدورات وضرورة القيام بدورات لتوعية المستخدمين أنفسهم على حماية بياناتهم الشخصية على الإنترنت و العمل على ملاحقة التطورات التي تظهر في أساليب وتقنيات الجرائم الإلكترونية عن طريق عمل برمجيات مضادة للحد من هذه الجرائم. وضرورة تطوير التشريعات الخاصة بأمن المعلومات بشكل مستمر على المستويين الوطني والدولي
دراسة الشوابكة، ٢٠١٩)	هدفت الدراسة الى التعرف على دور اجراءات الامن المعلوماتي في الحد من مخاطر امن المعلومات في جامعة الطائف	دور اجراءات الامن المعلوماتي	الحد من مخاطر امن المعلومات	المنهج الوصفي التحليلي مع الاستعانة بالمسح المكتبي	أن الاجراءات الامنية في الحد من مخاطر امن المعلومات في الجامعة عالية. والاجراءات الامنية لمنع الاختراق عن طريق الشبكة الحاسوبية Network Hacking جاءت مرتفعة بينما الاجراءات الامنية لمنع الاختراق عن طريق الهندسة الاجتماعية والاجراءات الامنية لمنع الاختراق عن طريق البرمجيات الضارة Malware منخفضة وتساهم اجراءات الامن المعلوماتي في الحد من المخاطر الداخلية والخارجية والطبيعية التي يتعرض لها

					النظام. واوصت لدراسة بضرورة القيام بوضع تصنيفات للمعلومات بالطريقة التي تناسب اعمالها وسرية معلوماتها مع عزل البيانات والمعلومات التي يشكل عرضها للعامة ضرر للنظام. وتقييم المخاطر التي يتعرض اليها النظام بشكل دوري للوقوف على ما يمكن عمله وايجاد السبل الكفيلة باستعادة العمل،
دراسة (الطاهري، ٢٠١٩) الأمن المعلوماتي وعلاقته بالأمن القومي	التعرف على علاقة الأمن المعلوماتي والأمن القومي	الأمن المعلوماتي	الأمن القومي	المنهج الوصفي	-يلعب الأمن الإلكتروني المعلوماتي دورا مهما في حماية الأمن القومي للدول، فهو قد يهدد أمن الدولة لية إذا ما تعرض للانكشاف أو الاختراق، الأمر الذي قد يكلف الدولة الكثير من الخسائر الأمنية والاجتماعية والسياسية والاقتصادية وغيرها. كما ان مستقبل الحروب الإلكترونية مرهون بمدى التطورات التقنية والمعلوماتية التي تواكب عصرنا الحالي والعصور التي ستليه، فعالم الاتصالات وتكنولوجيا المعلومات مستمر في إنتاج وطرح كل ما هو جديد، لتجندة البشرية جمعاء في صراعاتها الرقمية والتقنية المستقبلية. واوصت الدراسة بضرورة العمل على رفع مكانة وثقافة امن المعلومات الالكترونية، من خلال التحرر من التبعية التقنية، وتوظيف جميع الطاقات التكنولوجية، وذلك من خلال الاستفادة من التجارب المعلوماتية العالمية. وتأمين هذه المعلومات بشدة لتلك الدول المتعمدة على شبكات المعلومات وأدوات الاتصال الحديثة، لأن تداولها وإدارتها إلكترونية وعبر شبكات المعلومات والاتصالات التي ترابطت

دراسة (شلوش، ٢٠١٨).	التعرف على الاستراتيجيات والآليات التي يمكن تفعيلها من قبل الأنظمة الدولية لتجسيد الأمن السيبراني ومعرفة مدى علاقة القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول	القرصنة الإلكترونية	التهديد المتصاعد لأمن الدول	المنهج الوصفي من خلال استعراض اهم المفاهيم والنظريات المتعلقة بالموضوع	محلية وإقليمية وعالمية جعلها معرضة لخطر الاختراقات الأمر الذي يخلف العديد من الآثار على أمنها القومي.
دراسة (الحربي، ٢٠١٧)	تهدف هذه الدراسة الى التحقق من أمن المعلومات وعلاقته بالأمن القومي ، وشرح للعناصر الأساسية لأمن المعلومات وتهديداته ، وتحليل طرق الحماية من جرائم أمن المعلومات	امن المعلومات	علاقته بالأمن القومي	استخدم المنهج الوصفي والتحليلي في جمع المعلومات	أن أمن المعلومات ركيزة أساسية من ركائز الأمن الوطني، لا يتم الأمن الوطني إلا به . وان امن المعلومات يتطلب توفر عناصره الثلاثة وهي: سرية المعلومات وسلامتها وتوافره. لا حصر للجرائم المعلوماتية فيشمل كل اعتداء يتم متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية،وقد أحسن المنظم السعودي حين عرف الجريمة المعلوماتية في الفقرة الثامنة من المادة الأولى من

Kingdom of Saudi Arabia	وحماية أمن المعلومات في المملكة العربية السعودية.				نظام مكافحة جرائم المعلوماتية بأنها "أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام. حادثة الأنظمة والتقنين لحماية أمن المعلومات، رغم سرعة تطور الجريمة المعلوماتية. ولا يمكن تطبيق الحكومة الإلكترونية وغيرها من الأنظمة الإلكترونية الحديثة دون وجود الأمن المعلومات. وقد اوصت الدراسة بضرورة تطوير الاتفاقيات الأمنية على المستويات المختلفة لمنع الاعتداء او لضبط المجرمين او لتبادل وتسلم المجرمين او المعلومات او تبادل الخبرات. استخدام تقنية تشفير المواقع .
دراسة (حمد واحمد، ٢٠١٦)	هدفت الدراسة إلى التعرف على مهددات المعلومات والتصدي لها بالمقترحات والأنظمة الكفيلة بالحد من تلك الظواهر السالبة، وهدفت الدراسة أيضا إلى التعرف على وسائل حماية المعلومات والبيانات	أمن المعلومات	الحد من القرصنة الإلكترونية	المنهج الوصفي التحليلي في الدراسة، مع إيراد الملاحظات والمقترحات حول ما تم عرضه من موضوعات، كما تم تصميم برنامج (Spam Detection) عن طريق برنامج فيجوال بيسك كمقترح لحماية المعلومات	إن أنسب الطرق التي يمكن اتباعها للحد من مخاطر القرصنة الإلكترونية هي استخدام أنظمة الحماية، إن استخدام المعايير العالمية في أمن المعلومات يعتبر مؤشرا جيدا لمواكبة التقدم التكنولوجي، خطورة الآثار الكارثية التي يمكن أن تحدثها عمليات القرصنة الإلكترونية المتصلة بعمليات الحرب الإلكترونية. وقد اوصت الدراسة بإنشاء وحدة تعنى بأمن المعلومات في كافة مرافق الدولة بإشراف المركز القومي للمعلومات، تأمين فرص التدريب الداخلي والخارجي اللازمة للمستخدمين على أحدث الأنظمة والتقنيات المستخدمة في مجالات أمن المعلومات، الاهتمام بالجانب التوعوي لكافة شرائح المجتمع من خلال النشاطات الإعلامية التي تعنى بأمن المعلومات.

دراسة (القحطاني، واخرون، ٢٠١٤)	تصور استراتيجي لتطوير أمن المعلومات	تعزيزا للأمن الوطني في المملكة العربية السعودية	المنهج الوصفي التحليلي مع الاستعانة بأداة الاستبانة لجمع المعلومات	أن هناك أخطار يمكن أن تتعرض لها أنظمة المعلومات في شركة سابق مثل: اختراق لتعديل البيانات و تغييرها أو إتلافها وتنزيل برامج غير مصرح بها. ويترتب على اختراق أنظمة المعلومات تأثير سلبى على الأداء الاقتصادي من خلال سرقة الأسرار أو المعلومات التجارية أو التسويقية أو التعرف على حسابات الشركة . ويتم تطبيق اجراءات عقابية على الموظف الذي ينتهك اجراءات وسياسات أمن المعلومات بشركة سابق. واوصت بأهمية التوافق بين استراتيجية الشركة واستراتيجية تقنية المعلومات لضمان نجاح تنفيذ أنشطتها بكفاءة عالية. وضرورة دعم الإدارة لأنشطة الرقابة الداخلية على أمن المعلومات من خلال توفير الكوادر المؤهلة في قسم التحقيق الداخلي بالإضافة لتوفير التدريب اللازم لهم للتعرف على التحديات الجديدة التي تواجه أمن المعلومات وأساليب مكافحتها.
-----------------------------------	---	---	---	---

Study	Objectives	Dependent Variable	Independent Variable	Methodology	Results & Recommendations
Sureshkumar & Baranidharan, (2012) A study of the cloud security attacks and threats	This paper provides a survey into some of the prevalent challenges, risks, and ways to resolve these challenges in cloud platforms. We also discussed major cloud storage service for data storage and protection model	Cloud security	Attacks and Threats	Quantitative Method – Survey	The key contributing factors to cloud services are protection issues surrounding data and application maintenance. Owing to data sensitivity, regulatory enforcement or audit issues, many companies do not choose to preserve their data in a shared space.
Wibowo & Ramli, (2022) Impact of Implementation of Information	This study aims to risk identification, risk analysis, risk evaluation, risk treatment, risk acceptance, risk	Implementation of Information Security Risk Management	Cyber Security Maturity	Quantitative Method – Questionnaires	Information security is an important concern for governments and industry due to the increase in cyber-attacks during Covid-19.

Security Risk Management and Security Controls on Cyber Security Maturity (A Case Study at Data Management Applications of XYZ Institute)	control, and analysis of cyber security maturity gaps in the domain of governance, identification, protection, detection, and response.				
Kitsios, et al., (2022). Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT	The purpose of this paper was to develop a risk assessment framework that a company followed in the information technology sector to conduct the risk assessment process to comply with International	Developing a Risk Analysis Strategy Framework	Information Security Management	Case Study	The findings analyze the conditions that force organizations to invest in protecting information and the benefits they can derive from this process. Considering the lessons learned from its application by more software development companies will provide valuable

Consulting Industry	Organization for Standardization (ISO) 27001				guidelines for practitioners in the information technology sector
Vakulyk, et al, (2020) Cybersecurity as a Component of The National Security of The State	The aim is to the study of cybersecurity as a component of the national security of the state	Cybersecurity	National Security of The State	legal method organizational method and technological method	Each country's cybersecurity mechanism provides for the development and adoption of a cybersecurity strategy, the national cybersecurity system, the strengthening of the security. It is recommended that the entities should establish cooperation with the non-state sector and establish effective institutional and legal instruments for such cooperation

Mokhor, et al, (2020) Cybersecurity Risk Assessment of Information Systems of Critical Infrastructure Objects	The study aims to identify the cybersecurity risk assessment of information systems of critical infrastructure objects	cybersecurity risk assessment	infrastructure objects	Model Methodology	The results obtained can be used to assess the cybersecurity risk of information systems of critical infrastructure objects in the construction and implementation of information security management systems, integrated information protection systems in automated systems in the development of a threat model, security policy, and protection plan.
---	--	-------------------------------	------------------------	-------------------	---