

الأمن الفكري وتحديات الأمن السيبراني: دراسة نظرية

Intellectual Security and Cybersecurity Challenges:
A Theoretical Study

سفيان يوسف

مخبر التغير والعلاقات العامة، جامعة محمد خيضر، بسكرة، (الجزائر)

soufiene.yousfi@univ-biskra.dz

كلثوم مسعودي

جامعة محمد خيضر، بسكرة، (الجزائر)

kaltoum.messaoudi@univ-biskra.dz

تاريخ النشر: 2024/09/30

تاريخ القبول: 2024/09/19

تاريخ الإرسال: 2024/04/26

المؤلف المراسل: سفيان يوسف، soufiene.yousfi@univ-biskra.dz

الملخص:

تهدف الدراسة الحالية إلى استكشاف مساهمة الأمن السيبراني في تعزيز الأمن الفكري وتوفير بيئة آمنة وموثوقة للتكنولوجيا والمعلومات في المؤسسات والمجتمعات. وذلك نتيجة تزايد التهديدات والانتهاكات السيبرانية التي تشكل تحدياً كبيراً للأمن العالمي والوطني. الأمر الذي يتطلب البحث عن آليات فعالة لمكافحة هذه التهديدات وتعزيز الأمن الفكري للمؤسسات والأفراد. ويلعب الأمن السيبراني دوراً حيوياً في تعزيز الأمن الفكري وحماية البيانات والمعلومات الحساسة من الاختراقات والهجمات السيبرانية. فهو يعزز الوعي بأهمية الحماية الإلكترونية والاستخدام الآمن للتكنولوجيا، ويوفر الإطار القانوني والتقني لمكافحة الجرائم السيبرانية وتعزيز الأمن الرقمي. ويمكن القول خلاصة أن تبني استراتيجيات الأمن الفكري المناسبة، يُمكننا من تقليل التهديدات السيبرانية وتحقيق الثقة في العالم الرقمي.

الكلمات المفتاحية:

الأمن؛ الأمن الفكري؛ الأمن السيبراني؛ البيئة الرقمية؛ الفضاء السيبراني

Abstract:

The current study aims to explore the contribution of cybersecurity in enhancing intellectual security and providing a safe and reliable environment for technology and information in institutions and communities. This comes as a result of the increasing cyber threats and violations that pose significant challenges to global and national security. This necessitates the search for effective mechanisms to combat these threats and enhance intellectual security for both institutions and individuals. Cybersecurity plays a vital role in enhancing intellectual security and protecting sensitive data and information from cyber breaches and attacks. It promotes awareness of the importance of electronic protection and safe use of technology, and provides the legal and technical framework for combating cyber-crimes and enhancing digital security. In conclusion, adopting appropriate intellectual security strategies enables us to mitigate cyber threats and build trust in the digital world.

Keywords:

Security; Intellectual Security; Cybersecurity; Digital Environment; Cyberspace.

1. مقدمة

في ظل التطور السريع للتكنولوجيا والابتكارات، أصبحت الحاجة إلى حماية الأفراد والمجتمعات من الأفكار الضالة أمراً حيوياً لكونها تهدد السلامة الفكرية والأخلاقية على المستوى العالمي والوطني. يشير مصطلح الأمن الفكري إلى مجموعة من الحقوق القانونية والتدابير التي تهدف إلى حماية الإبداعات والاختراعات والأعمال الأدبية والفنية في ظل تحول العالم نحو التكنولوجيا الرقمية. ويعتبر الأمن السيبراني جزءاً حيوياً لضمان سلامة الأفراد والمؤسسات.

في عصر التكنولوجيا الرقمية، أصبح الأمن السيبراني ذا أهمية بالغة للأفراد والشركات والحكومات. يعبر مصطلح الأمن السيبراني عن مجموعة من الجهود والتدابير التي تهدف إلى حماية الأنظمة الإلكترونية والشبكات من التهديدات السيبرانية. ويشمل ذلك الحفاظ على سرية البيانات وضمان توافر الخدمات الرقمية ومنع الوصول غير المصرح به وتقوية الأمن السيبراني لحماية المعلومات الحساسة، سواء كانت ذات طابع شخصي أو تجاري أو حكومي.

إنّ الأمن الفكري ضرورة ملحة لحماية أفكار الأفراد والجماعات من الغزو الفكري الذي يهدد استقرار المجتمعات والدول في ظل التطورات الرقمية واتساع الفضاء السيبراني، الذي يمكن أن يساهم في انتشار الجريمة والعنف. ومن خلال تعزيز آليات الأمن الفكري بالنظر إلى المعطيات المتداخلة، سواء كانت دينية، أو اقتصادية، أو سياسية، أو اجتماعية، يمكن تعزيز الأمن والاستقرار لأفراد المجتمع والدول.

1.1. إشكالية الدراسة

في ظلّ التطور السريع للتكنولوجيا وانتشار الرقمنة في كافة جوانب الحياة اليومية، نجد أنفسنا أمام تحديات متزايدة في مجال أمن المعلومات والخصوصية الفكرية، حيث تزايدت التهديدات السيبرانية بشكل كبير، مما جعل الحاجة لدراسة التفاعل بين الأمن السيبراني والأمن الفكري أكثر أهمية من أي وقت مضى. في هذا السياق، سعت الدراسات الحديثة إلى فهم هذا التفاعل وتحديد تأثيره على الأمن العام والخصوصية الفردية. وعليه، تعتبر هذه الإشكالية محورية في مجال أمن المعلومات والتكنولوجيا، حيث تمثل تحدياتها

ونتاؤها العديدة تحدياً جوهرياً يجب مواجهته بأساليب علمية واعية لضمان الحفاظ على أمن المعلومات والخصوصية الفكرية في هذا العصر الرقمي المتطور.

بناء على ما سبق، نطرح التساؤل الرئيس التالي:

ما مدى مساهمة الأمن السيبراني في تعزيز الأمن الفكري؟

ومن خلال التساؤل الرئيسي تتبثق مجموعة من التساؤلات الفرعية التالية:

- كيف يساهم الأمن السيبراني في تعزيز الأمن الفكري؟
- ما هي التحديات التي تواجه الأمن العالمي والوطني نتيجة للتهديدات والانتهاكات السيبرانية؟
- ما هي الآليات الفعالة المطلوبة لمكافحة التهديدات السيبرانية وتعزيز الأمن الفكري للمؤسسات والأفراد؟

1.2. أهداف الدراسة

جاءت هذه الدراسة لتحقيق الأهداف التالية:

- فهم تأثير التهديدات والانتهاكات السيبرانية على الأمن الفكري.
- تحديد العلاقة بين الأمن الفكري والأمن السيبراني ودور كل منهما في تحقيق الأمن الرقمي.
- استكشاف الآليات والإجراءات التي يمكن اتخاذها لمكافحة التهديدات السيبرانية وتعزيز الأمن الفكري.
- تقديم توصيات عملية لتعزيز التعاون بين مجالي الأمن الفكري والأمن السيبراني.

1.3. أهمية الدراسة

تأتي أهمية هذه الدراسة من ضرورة فهم التفاعل بين الأمن الفكري والأمن السيبراني في العصر الرقمي الحديث. فهذه الدراسة تسلط الضوء على تأثير التهديدات السيبرانية على الأمن الفكري للأفراد والمؤسسات، وتبحث في كيفية دور الأمن السيبراني في حماية البيئة الفكرية وتعزيز الثقة في استخدام التكنولوجيا وتبادل المعلومات.

1.4. منهج الدراسة

اعتمدت الدراسة الحالية على منهج تحليلي شامل، حيث يتم جمع وتحليل البيانات من مصادر متعددة، بما في ذلك المقالات العلمية، والتقارير الحكومية، والإحصائيات الرسمية. يتم تحليل هذه البيانات بشكل نقدي لفهم العلاقات بين الأمن الفكري والأمن السيبراني، وتقديم استنتاجات موضوعية وتوصيات مدروسة للتعامل مع التحديات المرتبطة بهما.

2. الأسس الفكرية والنظرية للدراسة

1.2. الأمن الفكري (Intellectual Security)

يُعدّ الأمن الفكري ضرورةً من ضرورات استقرار المجتمع ورغبةً ضروريةً للفرد؛ إذ لا يمكن الاكتفاء بالأمن النفسي أو الأمن المادي، فالأمن الفكري لا يقل أهميةً وربما يكون أكثر أهميةً نظراً لعدم قدرة الإنسان على التعايش مع ذاته ومع الآخرين إذا فقدت الركيزة الفكرية المستقرة التي يسير عليها. لذلك، يعتبر الأمن الفكري حاجزاً لحماية الأفراد والمجتمعات ضد السقوط في الفوضى الفكرية غير المضبوطة بمبادئ العلم والحكمة وغير المستندة إلى عقيدة دينية سليمة. يجب أن يكون الأمن الفكري محورياً للحماية والتأهيل الفكري، حيث يتعين على الأفراد والمجتمعات الحفاظ على استقرار فكري يستند إلى مبادئ العلم والحكمة وقيم الأخلاق.

1.1.2. مفهوم الأمن الفكري (Concept of intellectual security)

تعددت تعريفات الأمن الفكري حسب السياق والتخصص، فهو لا يقتصر على حماية الأفكار والإبداعات الفكرية فحسب، بل يتجاوز ذلك إلى أبعاد أكثر تعقيداً وشمولاً. من الناحية اللغوية، نجد أنّ كلمة "الأمن" جاءت في اللغة العربية مشتقة من الفعل "أَمَنَ"، يَأْمَنُ، أَمَاناً¹، وتعني الحماية وهي ضد الخوف. فالأمان النفسي والجسدي مطلب الانسان للحصول على السكينة. وفي الاصطلاح، يُفهم الأمن على أنّه "إحساس أفراد المجتمع بمشاعر الطمأنينة، وعدم الخوف نحو أنفسهم وأسرهم وأموالهم، ومن هذا المنطلق فإنّ الأمن يبدأ بالفرد حيث الخلية الأولى في المجتمع، وأمن الفرد يرتبط ارتباطاً وثيقاً بحمايته وتجنبه مهاوي الانحراف والجريمة"². ولا يمكن تحقيق هذا إلا من خلال حماية الفكر من الأفكار الضالة والمضللة التي تهدف إلى إثارة الفوضى والتشويش.

أما الفكر، لغةً، فجاء من القول "فكر في الأمر فكرًا أي أعمل العقل فيه ورتب بعض ما يعلم ليصل به إلى معرفة المجهول، والفكر إعمال العقل في المعلوم للوصول إلى معرفة مجهول".³ (مجمع اللغة العربية، 1985). وفي الاصطلاح، هو جملة ما يتعلق بمخزون الذاكرة الإنسانية من الثقافات والقيم الأخلاقية التي يتغذى بها الإنسان من المجتمع الذي ينشأ فيه ويعيش بين أفرادهِ.⁴ لذا، يحقق الأمن الفكري الأمان الأخلاقي.

ومن الناحية المفهومية، يُعرّف الأمن الفكري، حسب (القرارعة، 2005)، بأنه "مجموعة التصورات والقيم التي تضمن صون الفكر وحفظه من الشطط والميل إلى الانحراف، والتي تؤدي إلى ضياع وظيفته الأساسية في إثراء الحياة بالسلوك القويم والآثار النافعة وحفظ الضروريات".⁵ وعلى العكس من ذلك، فإنّ الأمن الفكري يشكل عامل هدم للضروريات الاجتماعية والمصالح العامة". لذا، يجب حماية عقل الإنسان وفكره من الغزو الفكري الضال وتجنب الانحرافات الفكرية التي تهدد أمن المجتمع وتؤدي إلى سلوكيات مقيتة. ويشير (الجحني، 2006) إلى أنّ أعمال الإنسان وسلوكه في الحياة هي صدى لفكره وعقله، وأي اضطراب ملحوظ في الأمن الفكري يؤدي إلى تدهور الأمن العام.⁶

وفقاً لما سبق، يمكن تعريف الأمن الفكري بأنه: سلامة فكر الإنسان وعقله من تلوث الأفكار الدخيلة، والتي تؤدي إلى انحراف سلوك الفرد وخروجه عن منهج الاعتدال والتوازن الفكري، ويؤثر على مواقفه السياسية والاجتماعية والثقافية والدينية والأخلاقية.

2.1.2. أسس الأمن الفكري (Foundations of intellectual security)

للأمن الفكري أسس يقوم عليها، ومن خلال هذه الأسس نستطيع تحقيقه، فلا بد من الاهتمام بها والعمل على تنفيذها بأفضل ما يكون حتى تترسخ قيم المواطنة والانتماء إلى الوطن، فالانتماء هو شعور بالمسؤولية تجاه أمر معين مما يؤسس في النفس الإحساس بالولاء له، وهذا نهج سلفنا الصالح، فقد شهدوا نزول الرسالة، ولا بد من الاقتداء والاهتمام بهم، وتعد هذه الأسس مهمة في بناء الأمن الفكري وتعزيزه لدى أفراد المجتمع.

ولعل من أبرز هذه الأسس ما ذكره (العتيبي، 2010)، حيث أوضح بأنه قائم على ثوابت شرعية. فلا شك أن من يستمد قوته من قوة الشرع يحصل به على سعادة الدارين، ويتحقق منه الأمن والطمأنينة وترسيخ التسامح بين أبناء المجتمع والاهتمام بشباب الأمة ووضعهم على الطريق الصحيح، وعدم التفريط في ذلك أو إهماله أو تركه لمن هو ليس أهلاً للقيام بهذا الأمر،⁷ وذلك لأنّ الحوار هو أهم سبل مناقشة وجهات النظر المختلفة بالدلائل والبراهين، وهو ما يفيد في تحقيق الأمن الفكري بين أطراف المجتمع وتعزيز بنيانه الحصين المبني على الثبات.

وعليه، نرى أنه لتعزيز الأمن الفكري لدى أفراد المجتمع يجب تنمية مهارات التفكير لديهم، بحيث يتمكنوا من تمييز الصح من الخطأ. يجب أن تكون هذه المهارات مبنية على أسس متينة وموثوقة. ويجب تعزيزها باستخدام مختلف الوسائل الممكنة لتحقيق أهداف المجتمع الآمن والمستقر، وإشباع رغباتهم النفسية والاجتماعية.

3.1.2. أهمية الأمن الفكري (Importance of intellectual security)

يستمد الأمن الفكري أهميته من قيمة عقل الإنسان الذي كرمه الله عز وجل، وهو مناط التكليف الإلهي، فهو القائد والموجه للسلوك الإنساني وهو مركز الإيجابية والسلبية، وبه يمكن للإنسان أن يتخذ قراراته في هذه الحياة الدنيا.

تظهر الأهمية البالغة للأمن الفكري من خلال اعتبارات عديدة، منها ما يلي:⁸

- حماية القيم والمعتقدات في المجتمع، بما في ذلك الدين والعقيدة والحريات الأساسية.
- تعزيز الرقابة الذاتية لدى أفراد المجتمع، حيث يوحد الأفكار والقناعات التي تتفق مع العقيدة السليمة وضوابط المجتمع وتقاليد.
- يمهّد الطريق أمام الابتكار والإبداع، ويقلل من معدلات الجرائم.
- يتطلب مكافحة الانحراف الفكري في مراحل متأخرة مزيداً من الجهود، ولذلك فإن تعزيز الأمن الفكري يُعد وقاية ضرورية باستخدام جميع الآليات والجهود المتاحة.
- يؤثر الانحراف الفكري السلبي ليس فقط على الأفراد المنحرفين بل يمتد تأثيره ليشمل المجتمع بأسره والأفراد بشكل خاص.

- توجد مصادر عديدة وسهلة للغزو الفكري، ولذا فمن الضروري حماية العقل البشري وتحصينه وتأمين المعتقدات والقناعات التي تحميه من الانحراف والضلال.
- تكمن الأهمية الأساسية للأمن الفكري في حماية الكيان الفكري والعقدي للمجتمع من الأفكار الدخيلة، حيث يؤدي سلامة الفكر إلى استقراره وحماية أمنه .
- وعليه، نرى أن أهمية الأمن الفكري تتجلى في حماية سلامة الفكر الإنساني وعقله من الوقوع في الانحرافات المضللة و الدخيلة، والتي تعوق تطور المجتمع وتسهم في انتشار اضطرابات سلوكية سلبية تضر بالمصلحة العليا للمجتمع.

4.1.2. آليات تعزيز الأمن الفكري (Enhancing intellectual security)

من أجل تعزيز الأمن الفكري، يجب وجود آليات فعالة وأساليب وقائية تحمي عقل الفرد من الانحراف الفكري وتتوافق مع قيم المجتمع النبيلة. ينبغي العمل على نشر الفكر المعتدل في المجتمع وبين الشباب، حيث يكمن أساس الفكر الصحيح. ويجب أن يكون العمل في هذا السياق مبنياً على المنطق العلمي، وذلك للحفاظ على الهوية الوطنية. يتعين كشف التهديدات التي تشكل خطراً على هذه الهوية والتصدي لها بفعالية من قبل جميع المؤسسات المجتمعية.

وتتمثل الآليات التي تعزز الأمن الفكري في إكساب صفات المواطنة الصالحة وقبول الآخر، وذلك من خلال احترام الآخرين بغض النظر عن اختلاف معتقداتهم وممارساتهم الفكرية، وعدم التمييز في المعاملة بناءً على هذا الأساس. ويجب تعزيز ثقافة الحوار البناء وإتاحة الفرصة للحوار وتقويم الانحراف الفكري بواسطة البراهين والحجج القوية في ظل تشويش الأفكار الضالة والمضللة.

وفقاً لـ (شرقاوي، 2016)، يتطلب الحفاظ على الهوية الوطنية الكشف عن التهديدات التي تشكل خطراً عليها والتصدي لها بفعالية من قبل جميع المؤسسات المجتمعية، مع تحمل المسؤولية، فيجب حث الشباب على ضرورة القيام بهذا الدور سواء تجاه الجماعة التي ينتمون إليها أو المجتمع الذي يعيشون فيه، وتعزيز ثقافة التسامح من خلال تنشئة الشباب وإكسابهم ممارسات قيم المواطنة ونفي الذات، بالإضافة إلى احترام التعامل المتبادل مع الآخرين.⁹

وحسب (الحوشان، 2016)، فإنه يجب فهم النصوص الشرعية على حقيقتها والسعي للحصول على العلم المفيد وممارسة الأعمال الصالحة، بالإضافة إلى التركيز على التنشئة الصحيحة والاهتمام بتربية الشباب على قيم الفكر المعتدل وتوضيح أهم الصفات والسلوكيات والأفكار التي يحملونها لتجنبها. كما يجب تعزيز الوعي الفكري والتثقيف من خلال وسائل الإعلام والتعليم، وتشجيع البحث العلمي والنقاش الهادف في المجتمع. كما يجب تعزيز القدرة على التفكير النقدي وتحليل المعلومات، وتعليم الأدوات والمهارات اللازمة للتمييز بين الحقائق والأخبار المضللة أو المزيفة. ويجب أيضاً أن يكون هناك تعاون بين الحكومة والمجتمع المدني والمؤسسات الأكاديمية والدينية والثقافية لتطوير برامج توعية شاملة وشبكات دعم لمكافحة الانحراف الفكري¹⁰.

وبالإضافة إلى ذلك يجب تعزيز الشمولية والتسامح والعدالة في المجتمع، وتعزيز الحوار بين الثقافات والأديان المختلفة. ويتطلب ذلك جهوداً متواصلة لبناء جسور التواصل والاحترام المتبادل بين المجتمعات المختلفة¹¹.

وعليه، يمكن القول أنه يجب أن يكون هناك تفاعل واسع النطاق بين المؤسسات والأفراد في المجتمع لتعزيز الأمن الفكري، وذلك من خلال تبني مبادئ وقيم تعزز الحوار والتسامح والتعايش السلمي، ومن خلال التركيز على التعليم والتثقيف والتوعية وتشجيع البحث العلمي والتفكير النقدي.

5.1.2. التحديات المعاصرة التي يواجهها الأمن الفكري (Challenges to IS)

في ظل التطورات المتسارعة التي تحدث في شتى المجالات والميادين المختلفة، ظهرت تحديات متعددة تواجه الأمن الفكري. ومن بين هذه التحديات، يبرز تأثير ثورة المعلومات والاتصالات التي ألغت المسافات والحواجز بين الدول والشعوب. أدت هذه الثورة إلى سرعة انتشار الأفكار والسلوكيات بين المجتمعات، ولها تأثيرات عميقة في المجالات السياسية والاقتصادية والاجتماعية والثقافية والأمنية والنفسية¹².

إنّ تهديدات الأمن الفكري تتطور باستمرار في العصر الحديث، وتشمل مجموعة من التحديات التي يجب التصدي لها بشكل فعال. فيما يلي توضيح لكل منها.

أ- التحديات والأخطار التي تواجه العالم

لقد تزايدت التحديات التي تواجه العالم في الوقت الحاضر، وكان سببها الانفتاح الكبير الذي يشهده العالم في كل مناحي الحياة، مما كان له أثر كبير في تعرض الأمن الوطني لتحديات كبيرة، جاءت على شكلين: تحديات داخلية، وتحديات خارجية. بالنسبة للتحديات الداخلية، كثير من الدول بدأت تنزعج من أوضاعها السياسية والاجتماعية، وتأخرها الثقافي، وتخلفها عن ركب الحضارة الإنسانية، بالإضافة إلى سوء أوضاعها الاقتصادية، وخاصة مع توفر وسائل الاتصال والتواصل، ومقارنة نفسها بغيرها من الدول المتقدمة والمرفهة، فلذلك بدأت تلجأ إلى محاولة تغيير الأوضاع (...)، فكثرت الاضطرابات الداخلية، (...) في كثير من الدول¹³.

أمّا بالنسبة للتحديات الخارجية فهي تعرض الدول للاعتداء من قبل دولة أقوى منها؛ طمعاً بثروة تملكها، أو خلاف حدودي، أو رغبة في السيطرة والتوسع. لذلك فإنّ هذه العسكرة الجديدة للعالم، قد أدت إلى تطور مفاهيم جديدة لم تكن لها أهمية (...)، ولعل انعكاس الظروف والأوضاع الجديدة الداخلية أو الخارجية (...) جعلت العالم اليوم يبذل كل ما يستطيع من قواه المادية، والمعنوية؛ للتخلص من هذه الولايات المهلكة¹⁴.

وعليه، يمكن القول أنّ التحديات الداخلية والخارجية التي يواجهها العالم في الوقت الحاضر تشكل تهديداً جدياً للأمن العام، وتعزيز التعاون الدولي وتبادل المعلومات بين الدول يُعد أحد السبل الفعالة لمواجهة هذه التحديات وتحقيق الأمن والسلام الدوليين.

ب- التحديات والأخطار التي تواجه الوطن العربي:

يشهد الوطن العربي الآن واقعاً حضارياً لا يحسد عليه، فهو يفتقر إلى الوحدة السياسية، كما يفتقر إلى الوحدة الاقتصادية، حيث يتعرض إلى اعتداءات آثمة (...) حيث إنّ الواقع السياسي والثقافي في الوطن العربي، أدى إلى زيادة نزعات الغلو، وانتشار الأفكار المنحرفة (...) المثيرة للقلق، و تفشي ممارسات فجة تمثل انتهاكاً صارخاً للحقوق الأساسية للإنسان¹⁵.

وعليه، يمكن القول أنّ التحديات المعاصرة التي يواجهها الأمن الفكري متعددة ومتداخلة الأبعاد السياسية، والاجتماعية، والاقتصادية، والثقافية، والدينية، لاسيما في ظل التطورات المتسارعة للعصر الرقمي، وسهولة تدفق المعلومات عبر الشبكات العنكبوتية، وتأثيراتها السلبية على أفكار الانسان وعقله. لذلك، وجب إيجاد حلول مناسبة لهذه المشكلات.

6.1.2. الأمن السيبراني (Cybersecurity)

نتيجة للتطورات الرقمية المتسارعة، زادت حالات سوء استخدام النظم الإلكترونية لأغراض إجرامية، مما يعرض المصالح العامة والخاصة للضرر. وبناءً على ذلك، أصبح من الضروري تطوير تطبيقات وبرامج خاصة للحماية السيبرانية. تزايدت التهديدات التي تواجه الأنظمة الإلكترونية، مثل القرصنة والتجسس والاختراق، لدرجة أن الفضاء السيبراني أصبح ساحة للحروب. وتزايدت حالات الاختراق الإلكتروني، مما دفع دول العالم إلى عقد مؤتمر دولي يشارك فيه خبراء في حروب الفضاء السيبراني.

في هذا المؤتمر، تمّ التوصية بضرورة إنشاء اتفاقيات دولية للتعاون في تحقيق الأمن السيبراني. بحكم أنّ جميع الدول معرضة للهجمات الإلكترونية، التي تتجم عنها خسائر اقتصادية عالمية، وتهديدات اجتماعية وأمنية كبيرة، قد تهدد السلم والأمن الدوليين.

7.1.2. مفهوم الأمن السيبراني (Concept of cybersecurity)

هناك تعريفات متعددة ومتباينة للأمن السيبراني ؛ إلا أنّ كلاً منها يدور حول معانٍ متقاربة، وتتجاوز المجردة لغويًا إلى أبعاد أكثر تعقيدًا وشمولًا.

من الناحية اللغوية، وجدنا سابقاً أنّ كلمة "الأمن" جاءت في اللغة العربية ضدّ الخوف وتعني طمأنينة النفس وزوال الخوف¹⁶. ويشير أيضاً إلى الحالة التي توفر للفرد الإحساس بعدم الخطر والأمان على نفسه، وممتلكاته، وأمواله¹⁷.

أمّا كلمة "السيبراني"، لغةً، فجاءت من من كلمة "سيبر" وتعني صفة آلي شيء مرتبط بتقافة الحواسيب، أو تقنية المعلومات أو الواقع الافتراضي¹⁸. وفي الاصطلاح، نجد أنّ كلمة السيبراني استعملت لأول مرة من قبل عالم الرياضيات الأمريكي Norbert Winner عام (1948)، وتعني علم القيادة والتحكم في أجهزة الحاسوب ودراسة آليات التواصل، والتي تتضمن تكنولوجيا المعلومات، والواقع الافتراضي¹⁹.

ومن الناحية المفهومية، يُعرّف الأمن السيبراني، حسب (ايمان، 2020) بأنه "عملية الدفاع عن أمن الشبكات والمعلومات والأجهزة والبرامج بطريقة تقنية تكنولوجية من خلال اتخاذ الإجراءات والتدابير والوسائل التكنولوجية الحديثة، بقصد الحماية من أي هجمات إلكترونية لضمان أمن وسلامة وتوافر المعلومات".²⁰

ومنه فالأمن في ظل الفضاء السيبراني كان ولا يزال يأخذ اهتمام دول العالم ، بغض النظر عن مدى تواجدهم في هذا الفضاء، مما يعنى ارتباط أمن المعلومات ارتباطاً وثيقاً بالأمن القومي في معظم دول العالم، ذلك أنّ الاعتداءات المتكررة على البنى التحتية المهمة كالاتصالات، والأنظمة الإلكترونية يمكن أن يؤثر سلباً على سيادة الدول وأمنها الاستراتيجي، والتي تشكل بنيتها التحتية للاتصالات جزءاً مهماً من هذا الفضاء السيبراني. وتعرف (منى، 2020) الأمن السيبراني بأنه "ينطوي على حماية شبكات الكمبيوتر والمعلومات التي تحويها من الاختراق أو التعطيل، وتتمثل هذه الحماية في وقف هجمات الهاكرز الاجرامية".²¹

بمعنى آخر، يشير إلى الجهود والتدابير التي تتخذها المؤسسات والأفراد لحماية أنظمة المعلومات والشبكات الإلكترونية من الاختراقات والهجمات الإلكترونية الضارة. ويعرفه كذلك (Ji tendra; Parashu, 2017) بأنه "الأمن المادي للبرامج والتطبيقات والشبكات وأجهزة الكمبيوتر، والأمن المعنوي المتعلق بالبيانات والمعلومات من أي أضرار متعمدة وسرقتها والتحكم في الوصول الصحيح للأجهزة، والتطبيقات والشبكات لحمايتها من مختلف الأضرار".²²

أي أنّ الأمن السيبراني يشمل جوانب مادية ومعنوية، حيث يهدف إلى حماية الأنظمة والشبكات والبيانات من الاختراقات والتهديدات السيبرانية المختلفة، بما في ذلك البرامج الضارة والهجمات الإلكترونية والاختراقات الهجينة. ومن أهم أسس الأمن السيبراني تأمين البيانات وحمايتها من الوصول غير المرخص إليها، بالإضافة إلى تطوير وتنفيذ سياسات وإجراءات تأمينية فعالة للتصدي للتهديدات السيبرانية بشكل شامل ومنهجي.

وعليه، يمكن تعريف الأمن السيبراني بأنه: تأمين فضاء الإنترنت وأجهزة الحاسوب من تهديدات القرصنة، والاختراقات الذي قد يحدث عبر الشبكات، والأنظمة الإلكترونية للحد من الاستخدام غير المصرح به، باستخدام تدابير ووسائل تقنية لضمان استمرارية مجتمع المعلومات، والتصدي للتعطيلات التي تصيب شبكات الكمبيوتر، مع كشف الفيروسات الضارة المعرقة لخدمات الأنظمة الإلكترونية، وقرصنة الحسابات الشخصية، وتخريب قاعدة المعطيات لبرامج الحاسوب.

8.1.2. أهمية الأمن السيبراني (Importance of cybersecurity)

يُعتبر الأمن السيبراني أمراً ذو أهمية بالغة لجميع فئات المجتمع، بدءاً من الأفراد والأسر حتى المنظمات والحكومات والمؤسسات. إذ يُعزّز الأمن السيبراني حماية الأسر، ولاسيما الأطفال، من عمليات الاحتيال عبر الإنترنت ويحمي المعلومات الشخصية. ويُعد تعلم مهارات الحماية وتوفير بيئة آمنة عند استخدام أنظمة الحواسيب ضرورياً.

لهذا السبب، يُولي الأمن السيبراني أهمية بالغة، حيث تقوم الحكومات والمؤسسات العسكرية والشركات والهيئات المالية والطبية بجمع ومعالجة وتخزين كميات كبيرة من البيانات الحساسة على أجهزة الكمبيوتر والأجهزة الأخرى. وتشمل هذه البيانات الملكية الفكرية والمعلومات الأمنية والمالية والبيانات الشخصية.

وتُظهر الدلائل أن الأمن السيبراني أصبح أمراً حيوياً في عصرنا الحالي، حيث يركز المجرمون الإلكترونيون جهودهم على استهداف البنية التحتية للمؤسسات والحكومات. ويستفيد هؤلاء المجرمين من الثغرات في أنظمة الحماية التقليدية، بشرط أن يمتلكوا مهارات تقنية متقدمة. كما يزداد تعقيد الوضع بسبب صعوبة تحديد المسؤولية عن الهجمات السيبرانية، وصعوبة التنبؤ بالتهديدات المستقبلية واتخاذ الإجراءات الوقائية في الوقت المناسب، وهذا يشير إلى أهمية تعزيز القدرات السيبرانية وتطوير استراتيجيات متقدمة لمواجهة التهديدات الإلكترونية المتزايدة.

وحسب (Tadas, 2017) فإن الهجمات السيبرانية تتطور وفقاً لخمس مراحل، بدءاً من اكتشاف ثغرة أمنية في النظام والسيطرة عليها، وإدخال برامج ضارة في النظام وإصابة مكوناته الأخرى، وصولاً إلى هجوم على النظام بأكمله أو جزء منه.²³ وتتسبب الثغرات في الأمن السيبراني في مشكلات معقدة لأي مالك أو مشغل للنظام. ولمنع الحوادث السيبرانية، يُعد تحسين الأمن السيبراني باستمرار ومواكبة تطورات العصر الرقمي هو الحل الأمثل.

وعليه، فإن الأمن السيبراني يعتبر أمراً ذا أهمية بالغة في العصر الحالي، حيث يتركز المجرمون الإلكترونيون على استهداف البنية التحتية الحيوية للمؤسسات والحكومات، مما يتطلب تطوير استراتيجيات متقدمة لمواجهة التهديدات المستمرة، وتشير الدلائل إلى تطور الهجمات السيبرانية عبر مراحل مختلفة، مما يسلط الضوء على ضرورة تعزيز القدرات السيبرانية وتحسين التدابير الأمنية للحد من الثغرات والتهديدات.

9.1.2. الأبعاد الاجتماعية للأمن السيبراني (Social dimensions)

لقد أصبح العالم يعاني من مشكلات اجتماعية أفرزتها استخدامات تطبيقات العصر الرقمي، ومن ضمنها الجرائم السيبرانية، والاختراقات الإلكترونية لأنظمة الحاسوب، وفي ضوء هذه البيئة الرقمية المتغيرة، ثمة حاجة ملحة لاتخاذ تدابير عاجلة على الصعيدين المحلي والدولي لحماية البيانات السرية والخصوصية الشخصية ومجابهة شتى الأخطار المحدقة بأمن المجتمع وأفراده، وتأمين النظم الإلكترونية من الهاكرز (المخترقين)، والتي قد تهدد أمن المجتمع.

وتظهر الأبعاد الاجتماعية للأمن السيبراني حسب (عالم، 2018) باستهداف الأمن الوطني عبر التهديدات الأمنية المتزايدة بطرق متسارعة لم يشهدها العالم من قبل حتى شملت السياحة والتجارة والاقتصاد، وطالت أمن الدول والمجتمعات.

وفي هذا الخصوص، أشار تقرير صادر عن وكالة الأمن القومي الأمريكي إلى أن هناك 232 جهاز حاسب آلي تعرض لاختراقات وهجمات سيبرانية في كل دقيقة على امتداد العالم مما أضاف صعوبة عالية في المقدرة على اللحاق بمجرمي الفضاء الرقمي.²⁴

أما (جبور، 2012) فيشير إلى تهديد القيم والأخلاق من خلال تدني المستويين القيمي والأخلاقي، فالمحتويات غير المشروعة ذات تأثير سلبي على أخلاقيات المجتمع وعلى ارتفاع نسبة الممارسات الإجرامية كالإباحية، والترويج للإتجار بالممنوعات، والدعارة، والإرهاب، والتجنيد لقضايا خارج النظام²⁵.

و في سياق آخر يرى (حمدون، 2011) أنّ المخاطر طويلة الأجل للمجتمع تمثل عنصرا جوهريا يجب دراسته، فقد تستمر الهجمات لبضع ثوانٍ، ولكنها تحدث آثارا واسعة، وقد تتطلب الخسارة المجتمعية للثقة في هذه الثواني سنوات لإعادة بنائها، وتقويض الثقة بين المواطنين والشركات، وبين الدول نفسها يمكن أن يولد نتائج مدمرة على المجتمعات، والاستقرار العالمي، قد تمس المقدرات والأنظمة العسكرية وتستهدف البنية التحتية الحيوية للمجتمع بما في ذلك الشبكات الذكية، وشبكات المراقبة، وحيازة البيانات التي تسمح لها بالعمل والدفاع عن نفسها قد تنخفض عنه عواقب تُهدد حياة المجتمع²⁶.

وعليه، يمكن القول أنّ الأبعاد الاجتماعية للأمن السيبراني تُظهر مخاطر رهيبية تهدد أنساق المجتمع وقد تؤثر سلبا على البناء الاجتماعي لما لهذه الأفعال الإجرامية من آثار سيئة على الأمن الوطني والضبط الاجتماعي والاستقرار المجتمعي، لذا وجب استخدام تدابير وقائية للحد من مختلف أضرارها، خصوصا مع استحداث جرائم سيبرانية جديدة نظرا للاستخدام المتزايد في الحياة اليومية على الأنظمة المعلوماتية والأجهزة المتصلة بالشبكات الدولية، وازدياد عدد المتصلين بالفضاء الرقمي سهل الحصول على طرق القرصنة والتجسس المهددة لأمن الدول.

10.1.2. التداعيات المستقبلية للأمن السيبراني (Future Implications)

يتّضح أنّ التداعيات المستقبلية تدور حول مخاوف تفاقم معضلة الدفاع ضد الثغرات الأمنية وعدم فعالية الاستراتيجيات المعتمدة للحد من التهديدات والهجمات السيبرانية التي تستهدف المرافق التي تعتمد على الإنترنت في تعاملاتها، مثل مراكز البحث ونوادي الشباب والمصارف المالية والمؤسسات العمومية والشركات المتعددة الجنسيات وغيرها من المجالات الحساسة التي تشكل جزءا أساسيا في الصراعات الأمنية على المستوى المحلي والدولي.

ويرجع ظهور هذه المخاطر، وفقاً للمختصين، إلى عدم وجود رؤية صحيحة لدى الشركات العاملة في هذا المجال حول الأساليب المستخدمة في شبكتها، مما يتيح للقراصنة الوصول إليها والخروج منها بسهولة.

وتظهر التداعيات المستقبلية للأمن السيبراني، وفقاً لدراسة أجرتها مؤسسة الرند للدراسات في عام 2016، أنّ الاستخدام المفرط للوسائط الرقمية يجعل الفضاء السيبراني هدفاً للاستهداف، ويسهم في زيادة عمليات الاختراق من قبل القراصنة المتقنين. يستغل القراصنة الثغرات والأخطاء في البنية التحتية الرقمية، سواء كانت هذه الأخطاء قد نشأت بشكل متعمد أو غير متعمد نتيجة للأخطاء البشرية.²⁷

وعلى الرغم من دور البشر في تطوير التكنولوجيا والاستفادة منها، فإن التهديدات السيبرانية المعقدة أدت في النهاية إلى توتر العلاقة بين الأفراد والمؤسسات. هذا التوتر يرجع جزئياً إلى ضعف المعلومات الرسمية ونقص التعاون الدولي في تبادل المعلومات والخبرات في مجال الأمن السيبراني.

وعليه، يمكن القول أنّ التداعيات الاستشرافية للأمن السيبراني تشير أنّ الاستراتيجيات المطروحة غير كافية، لأنّ التهديدات مستمرة بسبب التطورات الرقمية المتسارعة في ظل مؤشرات حروب سيبرانية إلكترونية عالمية بين الدول تؤثر سلباً على أمن المجتمعات، لاسيما مع اتخاذ العديد من الحكومات إجراءات مستحدثة لحماية فضاءها الإلكتروني، ونشر الوعي بين مستخدمي تكنولوجيا الاتصال حول تأثير الجرائم الإلكترونية على أنماط الحياة الشخصية لأفراد المجتمع. وهو ما يتطلب تبنى استراتيجيات شمولية تركز على تعزيز التعاون الدولي وتبادل المعلومات والخبرات في مجال الأمن السيبراني، بالإضافة إلى تعزيز الوعي بين المستخدمين حول أفضل الممارسات والتدابير الوقائية في استخدام التكنولوجيا الرقمية.

11.1.2. علاقة الأمن الفكري بتهديدات الأمن السيبراني (Intellectual security Vs Cybersecurity)

في ظل ثورة المعلومات المتسارعة واستخدام تكنولوجيا الوسائط الرقمية بشكل واسع في جميع جوانب الحياة، أصبح من الضروري ضمان الأمن السيبراني للحماية من الهجمات السيبرانية. الهجمات السيبرانية غالبًا ما تكون غير مرئية وتؤثر سلبًا على الأمن الفكري، مما يؤدي إلى اضطراب وعدم استقرار المجتمع وتعطيل نموه. يعتمد استقرار المجتمع على الأمن الفكري الذي يوفر الطمأنينة النفسية للأفراد ويحمي المعتقدات والجوانب الثقافية والسياسية والاجتماعية والاقتصادية للدولة.

من خلال الدراسات التحليلية، يمكننا رصد بعض التأثيرات الناتجة عن التهديدات السيبرانية في مجالات مختلفة نوجزها فيما يلي:

– **التأثير الاجتماعي:** تشير دراسة (حسنين، 2006) إلى أنّ التهديدات السيبرانية يمكن أن تؤدي إلى انتشار الأفكار المتطرفة في المجتمع، حيث يتم ترويح خطابات عاطفية مركزة وعنيفة عبر الشبكة العنكبوتية. يتم استغلال المظالم التي قد تواجهها فئة معينة من الشعب، مما يؤدي إلى زيادة ثقافة الشك في كل المؤسسات (...). لذلك، يجب مناقشة القضايا الاجتماعية المختلفة وتعزيز ثقافة المشاركة المسؤولة لأفراد المجتمع في خدمة مصلحتهم ومستقبلهم²⁸.

ولتقليل التأثير الاجتماعي السلبي للتهديدات السيبرانية، يجب مناقشة القضايا الاجتماعية المختلفة بشكل مفتوح وشامل، وتعزيز ثقافة المشاركة المسؤولة لأفراد المجتمع في خدمة مصلحتهم ومستقبلهم. وتعتبر هذه الخطوات ضرورية لتعزيز الوعي بأهمية التحلي بالوسطية والتعايش السلمي.

– **التأثير العسكري:** تشير دراسة (خالد، 2018) إلى أنّ التهديدات السيبرانية يمكن أن تؤثر على البعد العسكري من خلال استهداف الأنظمة الأمنية في الدولة وتعطيل مراكز القيادة ووسائل الاتصال. وبالتالي، فإن استقرار الدولة وأمنها يتوقف على الحفاظ على قوة عسكرية قادرة على منع التسلل الإلكتروني وحماية الأنظمة العسكرية²⁹.

ويتطلب هذا تطوير استراتيجيات دفاعية متقدمة واعتماد تقنيات الأمان السيبراني في جميع جوانب التدريب والتجهيز العسكري. كما يتعين على الدول الاستثمار في تحديث وتطوير البنية التحتية السيبرانية العسكرية وتعزيز التعاون الدولي لمكافحة التهديدات السيبرانية المحتملة.

– **التأثير الاقتصادي:** تشير دراسة (علي، 2019) إلى أن التهديدات السيبرانية يمكن أن تسبب خسائر اقتصادية جسيمة. تتسبب الجرائم الإلكترونية المتزايدة في خسائر مادية كبيرة للأفراد والمنظمات، وهذا يؤثر سلباً على الاقتصاد بشكل عام. يُلاحظ أيضاً أن هجمات القرصنة السيبرانية يمكن أن تستهدف البنية التحتية الحيوية للدولة مثل الشبكات الكهربائية والماء والنقل، مما يؤدي إلى تعطيل الخدمات الأساسية وتكبد خسائر اقتصادية هائلة.

كما تشير دراسة منظمة الشركات المستقلة (ISACA, 2020) إلى أن التهديدات السيبرانية يمكن أن تشكل تهديداً كبيراً على القطاع المالي وتؤثر على الاستقرار الاقتصادي. وتوضح الدراسة أن الهجمات السيبرانية على البنوك والمؤسسات المالية يمكن أن تؤدي إلى تعطيل الخدمات المالية وتسبب فقدان الثقة لدى العملاء، وهو ما ينعكس سلباً على حجم التعاملات المالية وتؤثر سلباً على النمو الاقتصادي.

ولمكافحة هذه التهديدات السيبرانية، تعتمد الدول على تطوير استراتيجيات وسياسات أمنية سيبرانية قوية. وتشمل هذه الاستراتيجيات التحسين المستمر للبنية التحتية السيبرانية، وتعزيز الوعي السيبراني للمواطنين والمؤسسات، وتطوير القدرات التقنية للتعرف والاستجابة للهجمات السيبرانية، وتعزيز التعاون الدولي في مجال مكافحة الجرائم السيبرانية. بالإضافة إلى ذلك، يجب أن يشارك القطاع الخاص في جهود مكافحة التهديدات السيبرانية عبر تبني ممارسات أمنية قوية، وتوفير التدريب والتوعية للموظفين، وتعزيز البحث والتطوير في مجال أمن المعلومات.

وعليه، يمكن القول أن الأمان السيبراني يُعد تحدياً مستمراً ومتطوراً، ويتطلب جهوداً مشتركة من الأفراد والمؤسسات والحكومات للتصدي للتهديدات السيبرانية والحفاظ على أمان واستقرار المجتمعات.

3. خاتمة:

إنّ التطورات السريعة في مجال التكنولوجيا الرقمية ووسائل الاتصال قد أدت إلى ظهور جرائم سيبرانية جديدة وتهديدات أمنية. لذلك، ينبغي اتخاذ خطوات علمية وأكاديمية للتصدي لهذه التحديات. من بين الخطوات المقترحة تعزيز التوعية والتثقيف لدى الأفراد بشأن الأمن الفكري والسيبراني، وتنمية الكوادر المتخصصة في هذا المجال، وتحسين التشريعات والقوانين ذات الصلة. كما ينبغي تعزيز دور المؤسسات الاجتماعية مثل المدارس والجامعات في تعزيز الأمن الفكري وتوجيه الشباب نحو المفاهيم المعتدلة. ويجب أيضاً تعزيز التعاون الدولي وتبادل المعلومات والخبرات في مجال مكافحة الجريمة السيبرانية. أخيراً، يمكن القول أنّ الأمن الفكري والسيبراني يتطلبان تبني استراتيجيات تمكن من تقليل التهديدات السيبرانية وتحقيق الاستقرار والثقة في العالم الرقمي. من خلال اعتماد نهج شامل وعلمي يشمل التعليم والتدريب والتشريعات وتكوين الكوادر وتعزيز الوعي العام. حيث يجب أن تكون هناك جهود مشتركة من الأفراد والمؤسسات والدول لمكافحة الجريمة السيبرانية وتحقيق الأمن السيبراني في عصر الرقمية الحديث.

4. الهوامش

- ¹ إسماعيل بن حماد الجوهري، **الصاحح**، تحقق: أحمد عبد الغفور. ط 2، الجزء 15، دار العلم، للملايين. بيروت، لبنان، 1997، ص 89.
- ² السدحان، عبدالله، **الأنشطة المدرسية ودورها في وقاية الشباب من الانحراف**، بحث مقدم لندوة المجتمع والأمن، كلية الملك فهد الأمنية، الرياض، السعودية، 2001، ص 3.
- ³ مجمع اللغة العربية، **المعجم الوسيط**. ط 2، الجزء الثاني، دار عمران، مصر. 1985، ص 724.
- ⁴ التركي، عبد الله بن عبد المحسن، **الأمن الفكري وعناية المملكة العربية السعودية**. جامعة نايف العربية. الرياض، 1996، ص 66.
- ⁵ القرارعة، جميل بن عبيد، **الأمن الفكري في الإسلام**، قسم الدراسات الإسلامية والعربية، جامعة الملك فهد للبترول والمعادن، الدمام، السعودية، 2005، ص 14.
- ⁶ الجحني، علي فايز، **مراكز البحوث الأمنية ودورها في التصدي لمهددات الأمن**، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2006، ص 185.

- ⁷ العتيبي، سهل بن رفاع، دور خطب الجمعة والعلماء في تعزيز الأمن الفكري، المؤتمر الوطني الأول للأمن الفكري: المفاهيم والتحديات، جامعة الملك سعود، السعودية، 2009، ص 37.
- ⁸ البراشي، بكيل بن محمد، دور الأمن الفكري في الوقاية من الإرهاب، رسالة ماجستير غير منشورة، كلية الدراسات العليا، قسم العلوم الشرطية، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 1432هـ، ص 68.
- ⁹ شرقاوي، عماد ثروت، رؤية مستقبلية لتطوير آليات طريقة العمل مع الجامعات لتحقيق الأمن الفكري لدى الشباب، المجلس الأعلى للجامعات، القاهرة، مصر، 2016، ص 112.
- ¹⁰ الحوشان، بركة، وظيفة الأسرة والمدرسة في تحصين أبنائها ضد التطرف والإرهاب وتعزيز المواطنة، مطابع الحمضي، الرياض، السعودية، 2016، ص 41.
- ¹¹ شرقاوي، عماد ثروت، مرجع سابق، ص 112.
- ¹² الخزاعلة، ياسر، أضواء على الرؤية الأمنية في الفكر الهاشمي من المنقذ الأعظم إلى الملك المعزز: دراسة تحليلية تاريخية، دار الخليج، عمان الأردن، 2009، ص 87.
- ¹³ طشطوش، هائل، الأمن الوطني وعناصر قوة الدولة في ظل النظام العالمي الجديد، المكتبة الوطنية للنشر والتوزيع، عمان، الأردن، 2009، ص 91.
- ¹⁴ طشطوش، هائل، المرجع نفسه، ص 91.
- ¹⁵ الخزاعلة، ياسر، مرجع سابق ص 88.
- ¹⁶ الأصفهاني، الحسين بن علي، المفردات في غريب القرآن، دار المعرفة، بيروت، لبنان، 2005، ص 34.
- ¹⁷ البراشي، بكيل بن محمد، مرجع سابق، ص 83.
- ¹⁸ إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، دراسة منشورة، جامعة العربي التبسي، الجزائر، 2019، ص 56.
- ¹⁹ إدريس عطية، المرجع نفسه، ص 57.
- ²⁰ إيمان محمد الشورة، الأمن السيبراني في البنوك الإسلامية الأردنية، مذكرة بكالوريوس، كلية الشريعة، الجامعة الأردنية الأردن، 2020، ص 33.
- ²¹ منى عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية، مجلة كلية التربية، جامعة المنصورة، المجلد 111، العدد 1، المملكة العربية السعودية، 2020، ص 2-29.

²² Jitendra Jain and Parashu Ram Pal, **A Recent Study over Cyber Security and its Elements**, International Journal of Advanced Research in Computer Science (India: Rajasthan, Janardan Rai Nagar Rajasthan Vidyapeeth, Vol. 8, No. 3, 2017.

²³ Tad as Limba and others, **Cyber security management model for critical infrastructure**, The International Journal Entrepreneurship & Sustainability Issues (European Union: Entrepreneurship & Sustainability Center, Vol.4, No.4, June2017.

²⁴ محمد أسعد عالم، الهدم والتخريب تقنيات، المجلة العربية: الأمن السيبراني وحروب الأرقام الصماء، الرياض، السعودية، 2018، ص76.

²⁵ منى الأشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة، جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني بيروت، لبنان، 2012، ص99.

²⁶ حمدون تورية، البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات، فريق الرصد الدائم لأمن المعلومات، الاتحاد العالمي للعلماء، ارتشيه، صقلية، 2011، ص47.

²⁷ سكوت وارين هارولد، مارتن سي. ليبكي، و يفالوس ستوث، التوصل إلى إتفاق مع الصين بشأن الفضاء الإلكتروني، مؤسسة RAND - البحث والتطوير الداخلي، 2016، متاح على الموقع:

https://www.rand.org/content/dam/rand/pubs/research_reports/.arabic.pdf

²⁸ حسنين بوادي، إرهاب الأنترنت: الخطر القادم، ط1، دار الفكر الجامعي، الاسكندرية، مصر، 2006.

²⁹ خالد حسن أحمد لطفي، الارهاب الإلكتروني آفة العصر الحديث والاليات القانونية للمواجهة، ط 1، دار الفكر الجامعي، الاسكندرية، مصر، 2018.

4. قائمة المراجع:

قائمة المراجع باللغة العربية:

الكتب:

- (1) إدريس عطية: مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، (2019)، الجزائر، جامعة العربي التبسي.
- (2) إسماعيل بن حماد الجوهري: الصحاح، تحقق: أحمد عبد الغفور، (1997)، ط 2، الجزء 15. بيروت، لبنان، دار العلم، للملايين.
- (3) الأصفهاني، الحسين بن علي: المفردات في غريب القرآن، (2005)، بيروت، لبنان، دار المعرفة.
- (4) التركي، عبد الله بن عبد المحسن: الأمن الفكري وعناية المملكة العربية السعودية، (1996)، الرياض، السعودية، جامعة نايف العربية.

- (5) الجحني، علي فايز: مراكز البحوث الأمنية ودورها في التصدي لمهددات الأمن، (2006)، الرياض، السعودية، جامعة نايف العربية للعلوم الأمنية.
- (6) حسنين بوادي: إرهاب الأنترنت: الخطر القادم، (2006)، ط1. الاسكندرية، مصر، دار الفكر الجامعي.
- (7) حمدون تورية: البحث عن السلام السيبراني، (2011)، الاتحاد الدولي للاتصالات، فريق الرصد الدائم لأمن المعلومات، ارتشيه، صقلية، الاتحاد العالمي للعلماء.
- (8) الحوشان، بركة: وظيفة الأسرة والمدرسة في تحصين أبنائها ضد التطرف والإرهاب وتعزيز المواطنة، (2016)، الرياض، السعودية، مطابع الحميضي.
- (9) خالد حسن أحمد لطفي: الإرهاب الإلكتروني آفة العصر الحديث والليات القانونية للمواجهة، (2018)، ط1. الاسكندرية ، مصر، دار الفكر الجامعي.
- (10) الخزاولة، ياسر: أضواء على الرؤية الأمنية في الفكر الهاشمي من المنفذ الأعظم إلى الملك المعزز: دراسة تحليلية تاريخية، (2009)، عمان، الأردن، دار الخليج.
- (11) شرقاوي، عماد ثروت: رؤية مستقبلية لتطوير آليات طريقة العمل مع الجامعات لتحقيق الأمن الفكري لدى الشباب، (2016)، القاهرة، مصر، المجلس الأعلى للجامعات.
- (12) طشطوش، هائل: الأمن الوطني وعناصر قوة الدولة في ظل النظام العالمي الجديد، (2009)، عمان، الاردن، المكتبة الوطنية للنشر والتوزيع.
- (13) القرارة، جميل بن عبيد: الأمن الفكري في الإسلام، في كتاب الأمن رسالة الإسلام، (2005)، الدمام، السعودية، جامعة الملك فهد للبترول والمعادن.
- (14) مجمع اللغة العربية: المعجم الوسيط، (1985)، ط 2، الجزء الثاني. القاهرة، مصر، دار عمران.

الرسائل الجامعية:

- (1) إيمان محمد الشورة، (2020)، الأمن السيبراني في البنوك الإسلامية الأردنية، مذكرة بكالوريوس ، كلية الشريعة، الجامعة الأردنية الأردن.
- (2) البراشي، بكيل بن محمد، (1432هـ)، دور الأمن الفكري في الوقاية من الإرهاب، رسالة ماجستير غير منشورة، كلية الدراسات العليا، قسم العلوم الشرطية، جامعة نايف العربية للعلوم الامنية، الرياض، السعودية.

المقالات والندوات:

- (1) السدحان، عبدالله، (2001). « الأنشطة المدرسية ودورها في وقاية الشباب من الانحراف ». بحث مقدم لندوة المجتمع والأمن، كلية الملك فهد الأمنية، الرياض، السعودية.
 - (2) العتيبي، سهل بن رفاع، (2009). « دور خطب الجمعة والعلماء في تعزيز الأمن الفكري ». المؤتمر الوطني الأول للأمن الفكري: المفاهيم والتحديات، جامعة الملك سعود، 22-25 جمادى الأولى 1430هـ، الرياض، السعودية.
 - (3) محمد أسعد عالم، (2018). « الهدم والتخريب تقنياً ». المجلة العربية: الأمن السيبراني وحروب الأرقام الصماء، الرياض، السعودية، العدد 498.
 - (4) منى الأشقر جبور، (2012). « الأمن السيبراني "التحديات ومستلزمات المواجهة" ». جامعة الدول العربية، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، المركز العربي للبحوث القانونية والقضائية، 27-28 أغسطس (آب) بيروت، لبنان.
 - (5) منى عبد الله السمحان، (2020). « متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية ». مجلة كلية التربية، جامعة المنصورة، المملكة العربية السعودية، المجلد 111، العدد 1، ص 2-29.
- مواقع الشبكة الإلكترونية:**

- (1) سكوت وارين هارولد، مارتين سي. ليبكي: و يفالوس ستوث، التوصل إلى اتفاق مع الصين بشأن الفضاء الإلكتروني، مؤسسة RAND - البحث والتطوير الداخلي، 2016، متاح على الموقع: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1335/RA_ND2.arabic.pdf

قائمة المراجع باللغة الأجنبية:

- 1) Jitendra Jain and Parashu Ram Pal, (2017). A Recent Study over Cyber Security & its Elements, International Journal of Advanced Research in Computer Science (India: Rajasthan, Janardan Rai Nagar Rajasthan Vidyapeeth, Vol.8, N^o.3.
- 2) Tad as Limba and others, (2017). Cyber security management model for critical infrastructure, The International Journal Entrepreneurship & Sustainability Issues (European Union: Entrepreneurship and Sustainability Center, Vol.4, N^o.4.