مجلة دراسات إنسانية واجتماعية / جامعة وهران02/ المجلد 15 ع 01.
ISNN : 2253-0592 EISSN : 2588-199X / Prefix: 10.46315

مستقبل الأمن السيبراني في عصر الميتافيرس وتأثيره في الأمن المجتمعي

The Future of Cybersecurity in the Metaverse Era and Its Impact on Community Security

أحمد سالم النعماني Ahmed Salem Alnamani
Alnamani.a.s@hotmail.com
عبد العزيز يوسف جاهوني * Abdulaziz Yousef Jahouni
Azza.jah@hotmail.com
دراسات أمنية – وزارة الداخلية – دولة قطر.

DOI:10.46315/1714-015-001-035
الإرسال: 2025/06/22 **القبول**: 2025/09/18 **النشر**: 2026/01/16

**

ملخص:

يُعَدُّ مستقبل الأمن السيبراني في عصر الميتافيرس عاملاً رئيسياً في حماية الأمن السيبراني، حيث تتطلب البيئات الافتراضية أنظمة متطورة لضمان الخصوصية، وحماية البيانات والتصدي للهجمات السيبرانية، ومع تزايد الاعتماد على الميتافيرس يزداد خطر الجرائم الرقمية، مما يجعل تعزيز الأمن السيبراني ضرورة أساسية للحفاظ على استقرار المجتمعات وتعزيز الأمن المجتمعي.

هدفت الدراسة إلى التعرف على مفهوم الأمن السيبراني في عصر الميتافيرس، وبيان مستقبل الأمن السيبراني في عصر الميتافيرس وتأثيراته على الأمن المجتمعي. وأظهرت النتائج على أنه يسهم استخدام الميتافيرس بشكل سلبي في ظل الاعتماد المتزايد عليه في المستقبل في ظهور أنواع جديدة من الجرائم التي تعكس تحديات غير مسبوقة للأمن المجتمعي، ويسهم الأمن السيبراني ايجابياً في تعزيز الثقة المجتمعية من خلال تطبيق سياسات صارمة لحماية البيانات والخصوصية، إذ يمكن للمستخدمين والمؤسسات التعامل بأمان في الميتافيرس دون قلق ومخاوف من الاحتيال والاختراقات. كما أوصت الدراسة بضرورة حث الدول على نشر ثقافة الأمن الرقمي من خلال برامج توعية وتدريب تستهدف الأفراد والمؤسسات لتعريفهم بالمخاطر السيبرانية في العالم الافتراضي وطرق الوقاية منها.

كلمات مفتاحية: أمن سيبراني، ميتافيرس، جرائم رقمية، أمن مجتمعي، خصوصية بيانات، ثقافة أمن رقمي.

Abstract:

The future of cybersecurity in the metaverse era is a key factor in protecting cybersecurity. Virtual environments require advanced systems to ensure privacy, protect data, and combat cyberattacks. With increasing reliance on the metaverse, the risk of digital crimes increases, making enhancing cybersecurity a fundamental necessity to maintain societal stability and enhance community security.

This research aimed to understand the concept of cybersecurity in the metaverse era and to outline the future of cybersecurity in the metaverse era and its impact on community security. The results showed that the use of the metaverse, given its increasing reliance in the future, contributes negatively to the emergence of new types of crimes that pose unprecedented challenges to community security. Cybersecurity contributes positively to enhancing community

* الباحث المُراسل: Azza.jah@hotmail.com

trust through the implementation of strict data protection and privacy policies, allowing users and organizations to operate safely in the metaverse without fear of fraud and hacking. The research also recommended the need to encourage countries to promote a culture of digital security through awareness and training programs targeting individuals and organizations to educate them about cyber risks in the virtual world and ways to prevent them.

Key words: Cybersecurity, Metaverse, Digital crimes, Community security, Data privacy, Digital security culture.

**

1- مقدمة (Introduction):

يُعَدُّ الأمن السيبراني من أهم وسائل في العصر الحالي، حيث يقوم على ممارسات الدفاعات الإلكترونية وبناء هياكل دفاعية تقوم على صد الهجمات الإلكترونية سواء كانت على أجهزة الحاسوب أو المواقع الإلكترونية أو الهواتف الذكية أو الخوادم، لذلك فإنَّ الأمن السيبراني أصبح هاماً بشكل متزايد في عصر التكنولوجيا الحديثة، ويشمل كذلك تطوير وتنفيذ إجراءات الأمان والسياسات والتقنيات التي تساعد في حماية الأنظمة والشبكات والأجهزة الإلكترونية من التهديدات السيبرانية والاختراقات الإلكترونية والتهديدات الأمنية الأخرى.

إنَّ عجلة التطورات في مجال تقنية المعلومات والإنترنت والثورة المعلوماتية المستمرة أصبحت تهدد الخصوصيات الفردية والمجتمعية، خاصةً أنه في المستقبل القريب سوف يدخل العالم في عصر الميتافيرس، أي عالم رقمي يمكن الدخول إليه واستكشافه بسهولة مثل العالم الحقيقي، وتجربة أي شيء يمكن تخيله، وبالتالي التدخل في خصوصيات الآخرين وتهديد الأمن السيبراني.

لقد ازدادت التهديدات والجرائم السيبرانية في الآونة الأخيرة، التي ترتكب من محترفي القرصنة الإلكترونية إلى جماعات فائقة التنظيم وعصابات إجرامية متقدمة، ودول تهدف إلى تحقيق أهداف سياسية للأضرار بدول أُخرى، وأصبحت الهجمات أكثر تحديداً للأهداف وأكثر تطوراً، وفي عصر الميتافيرس عصر المستقبل سوف تزداد الهجمات والتهديدات الأمنية، وتهديد الأمن السيبراني الذي ينعكس على الأمن المجتمعي.

والأمن المجتمعي لا يتوقف على نوع محدد من الأمن، وذلك لأن كل عناصر الأمن تتكامل مع بعضها البعض، وبالتالي فإنَّ فقدان الأمن السيبراني في عصر الميتافيرس سوف يؤدي إلى تهديد الأمن المجتمعي وزعزعة الأمن والاستقرار المجتمعي ومن ثم نشر الفوضى في المجتمع، إضافة إلى تأثير الأمن الغذائي والأمن الصحي والأمن البيئي والأمن السياسي، مما يؤدي إلى انعدام الأمن المجتمعي.

تتناول هذه الدراسة موضوعاً هاماً استشرافياً يتعلق بمستقبل الأمن السيبراني في عصر الميتافيرس وتأثيره في الأمن المجتمعي بالبحث والتحليل والاستنتاج للوقوف على أهم التحديات المرتبطة بعصر الميتافيرس، ووضع الحلول العلمية والعملية لمواجهتها.

مشكلة الدراسة:

يشكل الأمن السيبراني أهم مجالات الأمن في الوقت الحاضر، الذي يتضمن حماية الأنظمة التقنية الحديثة التي تستخدمها الدول لحماية الشبكات وأجهزة الحاسب الآلي وكل ما هو موجود على الشبكة

الدولية للمعلومات، وهو أمر ضروري وحيوي في ظل انتشار الهجمات السيبرانية، ومع التطور السريع في مجال تكنولوجيا المعلومات والاتصالات، ظهرت تقنيات جديدة، منها تقنية الميتافيرس، والتي أثار ظهورها مخاوف خاصة فيما يتعلق بالأمن السيبراني، وأمن الأفراد على الشبكة الدولية للمعلومات، بما ينعكس على تهديد الأمن المجتمعي، ومن هنا تكمن مشكلة البحث في الإجابة على السؤال الرئيس التالي: ما هو مستقبل الأمن السيبراني في عصر الميتافيرس وتأثيره على الأمن المجتمعي؟

أهمية الدراسة:

تتمثل أهمية البحث بما يلي:

1. الأهمية العلمية: تكمن الأهمية العلمية للبحث فيما أحدثته تقنيات الميتافيرس في واقع العالم الافتراضي إلى مستويات غير مسبوقة، والدخول إلى عوالم جديده، تخدم جميع المجالات بشكل واسع بحيث لا يمكن التنبؤ بحدود يمكن أن تقف عندها تلك التقنيات، التي تنعكس سلباً على الأمن السيبراني باعتباره الأساس في حماية البيانات والمعلومات الرقمية والشخصية للأفراد والمجتمع، والتي يمكن أن تنعكس على الأمن المجتمعي، وبالتالي تدعو الحاجة إلى وجود منظور شامل وواسع لمعالجة التهديدات السيبرانية الناجمة عن عصر الميتافيرس ضمن نطاق الأمن السيبراني من خلال تغطية الفجوة البحثية في البحوث السابقة، إضافةً إلى جاهزية الدولة لمثل هذه التهديدات والجرائم السيبرانية، كما يعتبر هذ البحث مساهمة متواضعة يمكن الاستفادة من استنتاجاته وتوصياته في تطوير وتحديث السياسات والآليات الكفيلة بمكافحة التهديدات السيبرانية التي تهدد الأمن المجتمعي.
2. الأهمية العملية: تحظى الأهمية العملية في هذا البحث في بيان مخاطر وتحديات الأمن السيبراني في عصر الميتافيرس وانعكاساتها على الأمن المجتمعي، مما يتطلب دعم الجهود الدولية والوطنية في تحقيق الأمن السيبراني ومواجهة الجرائم والتهديدات السيبرانية، وقدرة مساهمة السياسات والاستراتيجيات الوطنية والدولية في مواجهة التحديات المتوقعة في عصر الميتافيرس والحد من تداعياتها على الأمن المجتمعي.

تساؤلات الدراسة:

تسعى هذه الدراسة الإجابة على التساؤلات التالية:

1. ما مفهوم الأمن السيبراني في عصر الميتافيرس وما أهميته وأهدافه وعناصر إدارته؟
2. ما التحديات المعاصرة للأمن المجتمعي؟
3. ما مستقبل الأمن السيبراني في عصر الميتافيرس وتأثيراته على الأمن المجتمعي؟

أهداف الدراسة:

يهدف هذا البحث إلى ما يلي:

1. التعرف على مفهوم الأمن السيبراني في عصر الميتافيرس وأهميته وأهدافه وعناصر إدارته.

2. التعرف على التحديات المعاصرة للأمن المجتمعي.
3. بيان مستقبل الأمن السيبراني في عصر الميتافيرس وتأثيراته على الأمن المجتمعي.
4. التوصل إلى الاستنتاجات المناسبة التي تسهم في وضع التوصيات لحماية خصوصية الأفراد وتحقيق الأمن المجتمعي.

الدراسات السابقة:

1.دراسة (البعاج، 2023). بعنوان "الوعي الاجتماعي بالأمن السيبراني لدى الطلبة – دراسة ميدانية على طلبة الجامعات كلية الإمام الكاظم انموذجاً"، هدفت الدراسة إلى معرفة الوعي بمفهوم الأمن السيبراني وتطبيقاته، وسبل تعزيز الوعي بمفاهيم الأمن السيبراني، لدى طلبة كلية الإمام الكاظم، وقد اعتمدت الدراسة على المنهج الوصفي المسحي من خلال استخدام أداة الاستبيان على عينة (50) مبحوثاً، وقد توصلت الدراسة إلى العديد من النتائج، أهمها: أنَّ أفراد مجتمع الدراسة يملكون درجة متوسطة من الوعي بمفاهيم الأمن السيبراني، وهو ما يشير إلى محدودية الوعي بالنسبة للطلبة، كذلك وجد أن افراد مجتمع الدراسة يملكون درجة (متوسطة) من الوعي بتطبيقات الأمن السيبراني، وهذا يوضح حقيقة عدم كفاية الوعي بتطبيقات الأمن السيبراني، وأن أفراد مجتمع الدراسة وافقوا على جميع سبل تعزيز الوعي بالأمن السيبراني. أغفلت هذه الدراسة الجوانب الأخرى للتوعية الاجتماعية والضوابط الدينية والمجتمعية، كما أنَّها أخذت رأي عينة واحدة من طلبة كلية الإمام الكاظم والتي لا تعمم نتائجها على باقي المجتمعات.

2.دراسة (سليمان وآخرون، 2023). بعنوان " الميتافيرس: الفرص والتحديات الأمنية"، هدفت هذه الدراسة إلى معرفة مهددات الميتافيرس للأمن الوطني، وقد حددها في تسع فئات تندرج تحتها هذه المهددات الأمنية: البنية التحتية المعرضة للخطر، التلاعب بالهوية، محاذير انتهاكات الخصوصية، الاختراق، الإرهاب الإلكتروني، الجرائم السيبرانية، انتشار المعلومات المضللة والزائفة، المخاطر التي تهدد السيادة والثقافة، التعبئة الاجتماعية والسياسية. خاصة في ظل الانجذاب العالمي الكبير للفرص التي تُقَدِّمُها تقنية الميتافيرس، وقد اعتمدت الدارسة على المنهج الوصفي التحليلي، وتوصلت الدراسة إلى العديد من النتائج، أهمها: اتجاه غالبية دول العالم نحو استكشاف الطرق الممكنة للاستفادة من إمكاناتها، ومع التوقعات الواعدة وإمكانات التجارب الرقمية التحويلية، وبينت أنَّ جميع الدول تسعى نحو الاستفادة من المزايا المحتملة للميتافيرس، وعلى الرغم من أن عالم الميتافيرس مليءٌ بالفرص والمزايا التجارية، إلا أنها بينت تأثيراً محتملاً هائلاً على قطاع الأمن الوطني. أغفلت هذه الدراسة الجوانب العلمية الأخرى لمواجهة التحديات الناجمة عن الميتافيرس وعلاقتها بالأمن السيبراني، وحددت فرص معينة للتصدي لمواجهة التحديات الأمنية فقط دون التحديات والتهديدات الأخرى المرتبطة بالأمن الوطني الأخرى.

3.دراسة (المرداس، 2023). بعنوان " الأمن السيبراني في المملكة العربية السعودية بين الواقع والمأمول - دراسة نظرية تحليلية"، هدفت الدراسة إلى إلقاء الضوء على الوضع الواقعي الحالي

والوضع المأمول مستقبلاً للأمن السيبراني، كما تهدف إلى تناول الأمن السيبراني والمتمثل في الحفاظ على سرية وأمن المعلومات والذي قد يعرض العديد من القطاعات للأزمات، وقد اعتمدت الدراسة على المنهج الوصفي القائم على مراجعة عدد من الأدبيات السابقة، توصلت الدراسة إلى العديد من النتائج، أهمها: إنَّ التحدي الحالي للدول هو مواجهة الجريمة الإلكترونية العابرة للقارات لتفادي أي آثار قد تسببها، وبالتالي تحقيق الأمن السيبراني، من خلال مختلف الاتفاقيات الدولية أو الإقليمية في هذا المجال، كما تسعى جهود الدول إلى توحيد الرؤى لمواجهة الإرهاب السيبراني، وخلق آليات تساعد في التحقيق والمتابعة القانونية للمجرمين الالكترونيين. ركزت هذه الدراسة على الأمن السيبراني المتعلق في حماية البيانات، ولم تتطرق لتأثيرات المتيافيرس في المستقبل، كما أنَّ هذه الدراسة أغفلت الجوانب المرتبطة بالأمن المجتمعي، وهذا ما سوف تركز عليه الدراسة الحالية من خلال تناول جوانب متعددة للأمن السيبراني ومستقبله في عصر الميتافيرس وتأثيره في الأمن المجتمعي.

4.الدراسة الحالية: ما يميز الدراسة الحالية عن الدراسات السابقة في أنّها تتناول مستقبل الأمن السيبراني في عصر الميتافيرس وتأثيره على الأمن المجتمعي، حيث أنَّ الدراسات السابقة لم تتناول الأمن السيبراني وتأثيره في الأمن المجتمعي ولم تتطرق إلى عصر الميتافيرس، كما يسعى البحث الحالي للإسهام في سد بعض الثغرات في الدراسات السابقة في ظل عدم وجود دراسات سابقة تناولت هذا الموضوع بجميع أبعاده.

منهجية الدراسة:

تم اتباع المنهج الوصفي التحليلي لتفسير كل الجوانب العلمية المتعلقة بالأمن السيبراني في عصر الميتافيرس، إضافةً إلى المنهج الاستشرافي، وذلك لاستشراف المخاطر المستقبلية وحلولها في بيئة الميتافيرس.

المبحث الأول: ماهية الأمن السيبر اني والميتافيرس

يُعَدُّ مصطلح السيبرانية والميتافيرس من المصطلحات الحديثة، حيث ارتبط هذا المصطلح بالجرائم والتهديدات السيبرانية التي ظهرت نتيجة لظهور أنظمة المعلومات ذاتها.

مفهوم الأمن السيبر اني

يستخدم مصطلح السيبرانية لوصف مفاهيم وأنواع مختلفة من الجرائم التي تتم من خلال الإنترنت وأجهزة الحاسوب، فهنالك من عرّفه بأنَّه مجموعة من الأساليب الدفاعية التي تستخدم للكشف عن المتسللين المحتملين وإحباط عملياتهم (أبو حسين، 2021: 13).

عرّف أيضاً بأنه مجموعة المعارف والتكنولوجيا والمؤسسات والأنشطة التي تحمي وتحافظ الوجود البيولوجي للحياة البشرية، والسلام الجماعي والازدهار لتعزيز حرية الأنسان، ويتضمن الحد من مخاطر الهجمات الضارة على البرامج وأجهزة الحاسوب والشبكات (الدوسري، 2019: 18).

كما عرف بأنَّه مجموعة التقنيات والعمليات والممارسات وتدابير الاستجابة والتخفيف المصممة لحماية الشبكات والحواسيب والبرامج والبيانات من الهجوم أو وقوع الضرر أو الوصول غير المصرح به (بانقا، 2019: 16).

ينظم ويجمع الأمن السيبراني الموارد والعمليات والهياكل المستخدمة لحماية الفضاء السيبراني والأنظمة التي تدعم الفضاء الإلكتروني، فهو النشاط الذي يعمل على تأمين الحماية اللازمة للموارد البشرية والمالية المتعلقة بتقنيات المعلومات والاتصالات، حيث يضمن آليات للحدّ من الخسائر والأضرار التي تترتب عن المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج، وبحيث لا تتحول الأضرار إلى خسائر دائمة (الحيدري، 2019: 26).

يرتبط مصطلح الأمن السيبراني بالعديد من المصطلحات ذات العلاقة بالسيبرانية، ومن هذه المصطلحات ما يلي

1. الفضاء السيبراني: يتضمن التواصل من خلال الربط بين التقنيات الرقمية المختلفة، حيث تشمل مجموعة من العناصر المادية وغير المادية، وتتكون من البرمجيات وشبكات التواصل، والتطبيقات الاجتماعية والمستخدمين سواء مشغلين أو مستخدمين (السمحان، 2020: 11).

2. الردع السيبراني: توفير الحماية ومنع الأعمال التي تهدف إلى الأضرار في أصول الدولة في الفضاء السيبراني، إضافةً إلى تلك التي تدعم العمليات الفضائية (زروقة، 2018: 36).

3. الهجمات السيبرانية: يقصد بها أي فعل يعرض وظائف وقدرات شبكة الحاسوب لهدف سياسي أو أمني، من خلال استغلال ثغرات أمنية معينة تُمكّن المستهدف من التخريب، وتعريض النظام إلى الخطر (بن علية، 2022: 301).

4. الجريمة السيبرانية: نشاط غير مشروع محله معطيات الحاسوب أو كل فعل أو امتناع عن فعل مخالف للقانون صادر عن إرادة آثمة يعاقب عليه القانون (بن علية، 2022، 302).

يمكن الإشارة إلى أنَّ الأمن السيبراني مجموعة من الأدوات والسياسات والمبادئ التوجيهية والتقنيات التي يمكن أن تستخدم لحماية البيئة السيبرانية وأصول المنظمة للحدّ من المخاطر والتهديدات السيبرانية.

مفهوم الميتافيرس وتطوره

يشير مصطلح الميتافيرس إلى شبكة من العوالم الافتراضية ثلاثية الأبعاد المترابطة التي تركز على التفاعل الاجتماعي، إذ يُمكن للأفراد دخول هذه العوالم باستخدام أجهزة الواقع الافتراضي أو الواقع المعزز والتفاعل مع الآخرين ومع البيئة المحيطة بهم بطرق غير ممكنة في العالم الحقيقي، ويُعتبر الميتافيرس امتداداً لعالم الإنترنت، حيث لا يقتصر على النصوص والصور، بل يشمل تجارب غامرة

وتفاعلية تُمكّن المستخدمين من الشعور كما لو كانوا يعيشون في هذا العالم الافتراضي (عقوني، 2023: 13).

بدأت فكرة الميتافيرس تتشكل في الثمانينيات مع تطور التكنولوجيا الرقمية وألعاب الفيديو، وخاصةً عوالم الألعاب متعددة اللاعبين عبر الإنترنت، وظهر مصطلح الميتافيرس لأول مرة في رواية سنو كراش للكاتب نيل ستيفنسون عام 1992، حيث تخيل عالماً افتراضياً ضخماً يتفاعل فيه الأفراد عبر فلترات رقمية، وفي التسعينيات وأوائل الألفية الجديدة، طورت شركات تقنية منصات افتراضية مثل سيكند لايف، التي أطلقتها شركة ليندن لاب في 2003، مما أتاح للمستخدمين بناء عوالمهم الخاصة والتفاعل في بيئات افتراضية حية، ومع تقدم التكنولوجيا في مجالات الواقع الافتراضي والواقع المعزز أصبحت فكرة الميتافيرس أكثر واقعية، وفي القرن الواحد والعشرين ساهمت شركات كبرى مثل فيسبوك، ومايكروسوفت في تطوير الميتافيرس عبر استثمارات ضخمة في هذه التقنيات (الصاوي، 2022: 139).

يتكون الميتافيرس من مجموعة من العناصر الأساسية التي تعمل معاً لتوفير تجربة ومغامرة شاملة للمستخدمين، وتشمل هذه المكونات ما يلي:

1. البيئات الافتراضية: أي المساحات الرقمية التي يمكن أن تكون أي شيء من مناظر طبيعية واقعية إلى عوالم خيالية بالكامل، وتسمح هذه البيئات للمستخدمين بالتجول والتفاعل، والاستكشاف كما لو كانوا في العالم الحقيقي (القاضي، 2023: 520).

2. الأفاتار: يمكن تخصيص الأفاتار للتمثيل الرقمي للمستخدم في الميتافيرس، مما يسمح للمستخدمين بتغيير مظهرهم وجنسهم وحتى صفاتهم الشخصية (القاضي، 2023: 521).

3. التفاعل الاجتماعي: الأدوات الاجتماعية مثل الرسائل الفورية، الصوت والفيديو المباشر، والأحداث الافتراضية تجعل من الممكن للمستخدمين التواصل والتفاعل بطرق غير ممكنة في العالم الحقيقي (عبد العال، 2022: 441).

4. الاقتصاد الرقمي: يشمل تداول السلع والخدمات باستخدام العملات الافتراضية، ويمكن للمستخدمين شراء وبيع الأصول الرقمية مثل الملابس الافتراضية، العقارات الرقمية، وحتى الأعمال الفنية الرقمية باستخدام العملات المشفرة أو النقود التقليدية (عقوني، 2023: 17).

5. الأمن والخصوصية: التقنيات المتقدمة مثل التشفير وإدارة الهوية الرقمية تساعد في حماية البيانات الشخصية ومنع الاختراقات والاحتيال (بريك، 2022: 59).

تتمثل التقنيات الداعمة للميتافيرس بالواقع الافتراضي (VR) يتيح للمستخدمين الانغماس في بيئات افتراضية بالكامل، إضافة إلى الواقع المعزز (AR) يدمج العناصر الرقمية مع العالم الحقيقي، والذكاء الاصطناعي، حيث تستخدم لتحسين التفاعل داخل أنظمة الواقع الافتراضي، والبلوك تشين الذي يوفر الأمان والشفافية في العمليات الاقتصادية (القاضي، 2023: 522).

طبيعة ارتباط الميتافيرس في الأمن السيبراني

يختبر العالم تزايدًا متواصلًا في التهديدات السيبرانية بكافة أنواعها من جرائم سيبرانية وإرهاب وتجسس سيبراني وحروب سيبرانية، وتعرض المخاطر والتهديدات الأمنية أمن البيانات والمعلومات للخطر وتهديد الأمن السيبراني، وفي ظل التدافع بين تنامي مهددات الأمن السيبراني وجهود تحقيقه، هناك دائماً ركيزة أساسية تتمثل في أنّ عالم الأمن السيبراني يواجه محاولات الاختراق والتهديد التي تتطلب الاستعداد للتصدي لها في عصر المتيافيرس (عقوني، 2023: 18).

يرتبط مصطلح الميتافيرس بالأمن السيبراني بشكل وثيق، وذلك في ظل التقنيات والأنشطة الرقمية التي يتضمنها، إذ أنَّ الميتافيرس هو بيئة رقمية حديثة تتيح تفاعل المستخدمين في فضاءات افتراضية ثلاثية الأبعاد، حيث يجتمع الناس للتواصل، والتعلم، والعمل، والتجارة باستخدام تقنيات مثل الواقع الافتراضي والواقع المعزز والذكاء الاصطناعي (بريك، 2022: 51).

إن طبيعة العلاقة بين الميتافيرس والأمن السيبراني متداخلة ومتشابكة، حيث تتداخل احتياجات ومتطلبات الأمن السيبراني مع تلك التقنية الحديثة في مدى قدرة الأمن السيبراني في حماية الأنظمة والشبكات والأجهزة من الهجمات الرقمية مع التطورات في عصر الميتافيرس ثلاثي الأبعاد (سليمان وآخرون، 2023: 23).

الأمن السيبراني وحماية الهوية الرقمية في عصر الميتافيرس

إنَّ التطورات المصاحبة للميتافيرس تتضمن في أن يمتلك كل شخص هوية رقمية تمثله في العالم الافتراضي، ويمكن لهذه الهوية أن تحتوي على معلومات شخصية وخاصة، إضافة إلى بيانات ومعلومات ذات أهمية لصاحبها، ويمثل تحدي الأمن السيبراني في عصر المتيافيرس في خطر اختراق وسرقة الهوية وانتحال الشخصية، مما أصبحت الحاجة الملحة إلى تطوير الأمن السيبراني لضمان أمان الهوية الرقمية (الصاوي، 2022: 139).

وفي عصر الميتافيرس هنالك كميات كبيرة من البيانات والمعلومات الشخصية للمستخدمين، بما في ذلك بيانات تحركاتهم وتفاعلاتهم داخل العالم الافتراضي، إذ أنَّ هنالك حاجة لحماية هذه البيانات من الوصول غير المصرح به أو الاستغلال، خاصة مع تزايد القلق حول الخصوصية، ويتطلب ذلك سياسات صارمة حول خصوصية البيانات، إلى جانب تقنيات تشفير لحماية المعلومات الحساسة (القاضي، 2023: 521).

يمكن للقراصنة استهداف الرموز غير القابلة للاستبدال المُستخدمة لتحديد الهوية الرقمية في الميتافيرس، للقيام بعمليات التصيد الاحتيالي ونشر برامج الفدية والاحتيال وغيرها من الهجمات، كما أنَّ استخدام هذا العالم الموازي الافتراضي لغسل الأموال باستخدام العقارات الافتراضية والرموز غير القابلة للاسترداد، ومن المرجح تزايد مخاطر الاعتداءات الشخصية في عالم الميتافيرس، خاصة على الأفراد تحت السن القانوني وتهديد الأمن السيبراني علاوةً على ذلك، فإنَّ تمثيل الأفراد بواسطة صورة رمزية مستعارة في البيئات الافتراضية لميتافيرس يمهد الطريق لعصر جديد من التجسس، نظراً لأن وجود

بيئة رقمية تشمل جميع جوانب الحياة تقريباً، من حيث العلاقات والعمل والهوية، سوف يجعلها عرضة للانتهاكات أو التلاعب بها من قِبل بعض الأفراد أو الجماعات والدول (عبد العال، 2022: 441).

تحدث تهديدات الميتافيرس عندما يقوم المهاجمون بمسح نقاط الضعف في الأجهزة ومحاولة الاتصال بالمنافذ غير القياسية، إذ تُعدُّ الخصوصية والأمان من الاهتمامات الكبيرة التي يجب أخذها في الاعتبار فيما يتعلق بالميتافيرس في ظل نقل كل بيانات إنترنت الأشياء وهذا يزيد من خطورة فقدان الخصوصية، وتهديد الأمن السيبراني، ويمكن اختراق البرنامج وإساءة استخدام المعلومات الشخصية (سليمان وآخرون، 2023: 52).

الأمن السيبراني ومخاطر الهجمات السيبرانية في عصر الميتافيرس

تُعدُّ التهديدات السيبرانية من أخطر وأعقد التهديدات التي تستهدف الدول والأفراد على حدٍّ سواء، نظراً لطبيعتها المتطورة وتكلفتها الضئيلة، الأمر الذي يكشف أهمية دور الأمن السيبراني المعني بحماية الأنظمة المعلوماتية والشبكات والبرامج من الهجمات الرقمية الخبيثة، التي تستهدف عادة الوصول للمعلومات السرية وسرقتها أو إتلافها خاصة في عصر الميتافيرس، أو ابتزاز المستخدمين وانتهاك خصوصياتهم وأمن معلوماتهم الشخصية، وغيرها من السلوكيات التي تضر المستهدفين (بانقا، 2019: 22).

تجدر الإشارة إلى وجود علاقة طردية بين أهمية الأمن السيبراني واستخدام التكنولوجيا في عصر الميتافيرس، حيث تزداد هذه الأهمية كلما ارتفع حجم الاعتماد على التقنيات الحديثة ثلاثية الأبعاد (بريك، 2022: 58).

تُعَدُّ أنظمة الميتافيرس هدفاً للهجمات الإلكترونية وبرامج الفدية، مثل هجمات الاحتيال والبرمجيات الخبيثة وهجمات الحرمان من الخدمة، إذ أنَّ الهجمات على الميتافيرس قد تؤدي إلى تعطيل الأنشطة العلمية والعملية والتجارب الرقمية، وقد تعرض المستخدمين والمستثمرين لخسائر كبيرة (زروقة، 2018: 30).

يستخدم الميتافيرس الهندسة الاجتماعية للتلاعب النفسي لخداع المستخدمين لارتكاب أخطاء أمنية أو الكشف عن معلومات حساسة، إذ يمكن الاستفادة من التزييف العميق لارتكاب جريمة، وسيكون بوسع المجرمين التسلل إلى الميتافيرس لانتحال شخصية الشركات أو مقدمي الخدمات أو المسؤولين في ظل الثغرات والفجوات المتوقعة في حماية البيانات وتهديد الأمن السيبراني وعدم القدرة على مواجهة التهديدات السيبرانية (القاضي، 2023: 211).

يمكن تنفيذ جميع أنواع الأنشطة الإجرامية دون ترك أي أثر، وبالتالي يمكن أن يكون الميتافيرس وسيلة للمجرمين وتجار المخدرات والاتجار بالبشر، وغيرها لتنفيذ جرائمهم دون أن يتم اكتشافهم، بناءً عليه من المتوقع أن يكون عصر الميتافيرس تهديدًا للأمن السيبراني في ظل العالم الافتراضي لمستقبل الميتافيرس، ومن أبرز عمليات الاختراق السيبراني استهداف شركة أمريكية مختصة في إدارة الشبكات "SolarWinds"، وقد وقعت عملية الاختراق في عام 2020م عندما تمكن قراصنة من التسلل إلى تحديث

لبرنامج "Orion"، وهو أحد المنتجات الأساسية للشركة، هذا التحديث الذي تم تحميله من قبل العملاء، حيث يسمح للمهاجمين بالوصول إلى أنظمة العملاء وسرقة بياناتهم (الصاوي، 2022: 142).

التحليل:

ظهر مصطلح الأمن السيبراني نتيجة التطورات الحديثة في الوسائل والتطبيقات الحديثة، وما ارتبط في هذا التطور من جرائم وتهديدات سيبرانية، مما أدى إلى اهتمام الدول في وضع آليات لحماية البيئة السيبرانية، وما يلاحقها من تهديدات تضمن حماية البيانات والمعلومات وأصول المنظمة للحدّ من المخاطر والتهديدات المستقبلية.

وأدى التطور في الوسائل الحديثة إلى ظهور الميتافيرس ثلاثي الأبعاد الذي فتح آفاقاً جديدة في المستقبل للتفاعل مع الآخرين، الأمر الذي تطلب من الجهات المختصة في الدول تعزيز قدرات الأمن السيبراني ومواجهة التهديدات المستقبلية، وذلك من خلال توفير بيئة رقمية آمنة لحماية البيانات والمعلومات.

تمثل مكونات الميتافيرس وحدة مترابطة ومتكاملة فيما بينها، لتقديم خدمات وواقع شبه حقيقي معزز في العالم الافتراضي، في ظل ما تحمله في طياتها من بيئة افتراضية غنية في المعلومات والبيانات تستطيع تلبية احتياجات المستخدمين والتفاعل مع بعضهم البعض، مما قد تسهم في تطوير عصر الميتافيرس.

يستخدم الأمن السيبراني لمنع سوء استغلال المعلومات الإلكترونية، وحمايتها واتخاذ التدابير اللازمة لحماية المجتمع من المخاطر والتهديدات السيبرانية وحماية الأنظمة الإلكترونية والشبكات والأجهزة من التهديدات والهجمات السيبرانية، وبالتالي بات توفير الأمن السيبراني ضروري لحماية المعلومات والبيانات الشخصية والرقمية للأفراد.

تمكن إدارة الأمن السيبراني قدرة الدول والمؤسسات العامة والخاصة في مواجهة الجرائم والتهديدات السيبرانية، وما يواكب الفضاء السيبراني من تطور في الأساليب والأدوات المستخدمة التي أصبحت تشكل تحدياً للأفراد والدول، في ظل التطور المستمر للوسائل والتقنيات الحديثة الذي يشهده العالم خاصة في ظل ظهور عصر الميتافيرس.

إنَّ العلاقة بين الميتافيرس والأمن السيبراني علاقة طردية، وبالتالي فإنَّ بيئة الميتافيرس تتطلب حماية آمنة متكاملة لحماية المستخدمين والأصول الرقمية من التهديدات السيبرانية المختلفة، وهذا يعني أنَّ الأمن السيبراني جزء لا يتجزأ من بيئة الميتافيرس لتحقيق بيئة آمنة في العالم الافتراضي.

إن تحقيق الأمن السيبراني في عصر الميتافيرس وما قد يصاحبه من تهديدات بات ضرورياً لحماية الهويات الرقمية والبيانات، مما يتطلب لتحقيق الأمن السيبراني في عصر الميتافيرس تشفير المعلومات، واتخاذ الإجراءات والتدابير اللازمة لمواجهة أية تهديدات مستقبلية.

المبحث الثاني: التحديات المعاصرة للأمن المجتمعي

تطور مصطلح الأمن بوتيرة متسارعة، وقفز من مفهومه التقليدي إلى المفهوم المجتمعي، الذي يرتكز على أساس المشاركة المجتمعية، مما دعا لإيجاد متطلبات واحتياجات جديدة لمواجهة التطورات الناجمة عن الاستخدامات الحديثة ومنها الميتافيرس.

مفهوم الأمن المجتمعي:

الأمن بسكون الميم لغةً ضد الخوف، وهو من باب أمن وفهم، والأمن بكسر الميم أي المستجير ليأمن على نفسه، ومنه الآمن أي غير الخائف، واصطلاحاً لم يختلف المعنى عن المعنى اللغوي، عدم توقع مكروه في الزمان الآتي، ويقصد بالخوف الذعر ولا يكون إلا في المستقبل، كما أنه الاستقرار وعدم الخوف (العباسي، 2016: 41).

يعرف الأمن المجتمعي كلفظ مركب إضافي وهو تعبير حديث يقصد به أنْ يعيش الفرد ويحيا حياة اجتماعية آمنة مطمئنة مستقرة على نفسه ورزقه ومكانه الذي يعيش فيه هو ومَنْ يعوله من أفراد أسرته (علي وخليفة، 2024: 75).

يشير مفهوم الأمن إلى توفير الحماية والاطمئنان والأمان النفسي والبدني لأفراد المجتمع من أية مخاطر، ويتضمن سد الحاجات الإنسانية التي يحتاجها الفرد ليعيش حياة مطمئنة مستقرة، إذ إنَّ تحقيق الحماية والطمأنينة والأمن والاستقرار، والاكتفاء المادي لأفراد المجتمع من الاحتياجات الغذائية والصحية والروحية والترفيهية يعكس قدرة المجتمع على مواجهة التحديات المعاصرة وتحقيق أكبر قدر ممكن من الاعتماد على الذات لضمان تحقيق الاستقرار والتنمية المستدامة ومواجهة التحديات المعاصرة (الصبحيين والرصاعي، 2018: 206).

كما يشير الأمن المجتمعي إلى حالة من الإحساس أو الشعور أو الاحتياج لمجموعة من الضمانات تحقق الأمن للإنسان في يومه ومستقبله، وهذه الضمانات تتمثل في توفير التعليم الأساسي الملائم، والرعاية الصحية المناسبة، والخدمات الثقافية والاجتماعية، وتوفير المسكن الملائم، وخدمات الأمن والعدل، وتوفير الغذاء المناسب (حسين وجميل، 2016: 135).

ويرتكز الأمن المجتمعي في تكوين وخلق التماسك المجتمعي، وذلك من خلال تعزيز روح الانتماء والولاء للوطن أو المجتمع، فالأمن في المجتمع يرتبط بما يوفره لمواطنيه من أسباب الشعور بالطمأنينة والرفاهية وما يمنحه لأفراده من حرية التعبير عن الرأي بما يجعل الفرد فاعلاً في تحقيق أهداف المجتمع ومسهمًا في تطوره ورقيه (نورهان وآخرون، 2021: 152).

أهمية الأمن المجتمعي:

يعتبر الأمن المجتمعي أمراً هاماً لبناء مجتمع مستدام وعادل ومزدهر، حيث يساهم في تعزيز رفاهية الأفراد وتحقيق التنمية الشاملة والاستقرار الاجتماعي والاقتصادي ويركز على حماية الأفراد والمجتمعات من التهديدات التي تمس حياتهم وهويتهم (علي وخليف، 2024: 77).

تبرز أهمية الأمن المجتمعي في تحقيق السلم المجتمعي في المجتمع من خلال التصدي للجرائم، ومظاهر العنف، فهو صمام لتوفير بيئة آمنة ومستقرة تعزز الإنتاجية والتماسك الاجتماعي، فهو ركيزة أساسية لرقية وتطور المجتمع ومواكبة احتياجات العصر الذي نعيشه، فمسؤولية الأمن المجتمعي ليس على عاتق الدولة وحدها، بل على كافة شرائح المجتمع من الأفراد والمؤسسات والحكومات، وجميع القوى التي تشكل البناء العام للمجتمع (حواوسه، 2018: 139).

ترتبط أهمية الأمن المجتمعي في إقامة السلم المجتمعي بين جميع فئات المجتمع بغية تحصينه من الجرائم التي تهدده، والمرتبطة بالمستجدات والتطورات الحديثة التي تتخذ التقنيات العالية والتكنولوجيا وسيلة سريعة تسهل ممارسة الأنشطة الإجرامية، وأنه في رحاب الأمن المجتمعي يمكن تحقيق التنمية والتقدم، وتكاتف الجهود في خدمة المجتمع والوطن (البعاج، 2023: 454).

إنَّ تحقيق مجتمع آمن ومستقر يرتكز على أساس التضامن والتكافل والاستقرار الاجتماعي في المجتمعات، ويسهم في بناء مجتمع واعي قادر على مواجهة التحديات المعاصرة، ويدرك أهمية الأفكار التي من الممكن أن تنهض بالدولة ومؤسساتها (العباسي، 2016: 41).

يعزز الأمن المجتمعي من تمسك الفرد بهويته الثقافية ويحميها من التشتت في ظل الانفتاح العالمي على أفكار متباينة، حيث يشعر الفرد بأهمية تمسكه بهويته وأنها الحصن المنيع الذي يحميه من الأفكار الشاذة والهدامة، ويحقق استقرار المجتمع من خلال تعزيز الأمن المجتمعي، ويكون أقل عرضة للصراعات الداخلية والانقسامات، حيث يتم تقبل الاختلافات بطريقة مبنية على التفاهم، وينشأ بين أفراد المجتمع حالة من التماسك والتعاون (حسين وجميل، 2016: 136).

علاقة الأمن المجتمعي في الأمن السيبراني:

تُشَكل التهديدات والجرائم السيبرانية على اختلاف مستوياتها وأهدافها وأشكالها تحدياً وتهديداً للأمن بشكل عام ومنها الأمن المجتمعي، لا سيما وأنها تأخذ هذه التهديدات أشكالاً مختلفة ومتنوعة، مثل اختراق النظم المعلوماتية والإنترنت، والنزاعات الجيوسياسية، والتجسس، والتخريب، وغسل الأموال، الأمر الذي يتطلب اعداد السياسات والاستراتيجيات الوطنية الخاصة بالأمن السيبراني وتطويرها بالشكل الذي يضمن تعزيز قدرة الدول على مواجهة الآثار السلبية لتلك التهديدات على أمن المجتمع واستقراره (الدوسري، 2019: 36).

لا شك في أن الأمن السيبراني يمثل الدرع الرقمي الذي يحمي العالم المتصل بالإنترنت، وفي عصر تكنولوجيا المعلومات حيث تتداخل معظم مجالات الحياة مع الشبكة العنكبوتية، ويصبح الأمن السيبراني أمراً حيوياً للحفاظ على خصوصيات الأفراد وبياناتهم مع الاختراق والتعدي عليها، مما يشكل خطراً على الأمن المجتمعي (بانقا، 2019: 32).

تتجسد التهديدات السيبرانية في تأثير المخاطر الاجتماعية والتهديدات السيبرانية في تشكيل بنية المجتمع ومنها زيادة الجرائم المستحدثة، تهديد البنية التحتية، تهديد القيم والأخلاق، واستهداف الأمن الوطني، تصدير أزمة ثقة في الحكومة والأجهزة المختصة (بن برغوث، 2023: 451).

يؤدي الامن السيبراني إلى تحقيق التوازن بين التقدم التكنولوجي والحفاظ على الأمن المجتمعي، الذي يُعدُّ تحدياً مستمراً يتطلب تطوير وتبني استراتيجيات فعّالة للدفاع عن العالم والفضاء الرقمي، حيث يلعب الأمن السيبراني في هذا العالم الرقمي المعقد دوراً حيوياً في حماية المعلومات الشخصية، وضمان استمرارية العمليات الأساسية للدول والمجتمع على حد سواء، فهوم صمام الأمان للمجتمع (السمحان، 2023: 13).

إنَّ العلاقة بين الأمن المجتمعي والأمن السيبراني تتعلق بالحماية من تدني المستويين القيمي والأخلاقي، فالمحتويات غير المشروعة وغير المرغوب بها ذات تأثير سلبي على أخلاقيات المجتمع وعلى ارتفاع نسبة الممارسات الإجرامية، والترويج للإتجار بالممنوعات، والدعارة، والإرهاب، والتجنيد لقضايا تمس الأمن والسلام، وعليه لا بد من بناء مجتمع مسؤول ومدرك لمخاطر الفضاء السيبيرانى، قادر على التعامل مع قواعد السلامة ومدرك للعواقب القانونية التي ممكن أن ترتب على التعرض لسلامة الأفراد والمؤسسات ورؤوس الأموال (فوزي، 2019 :112).

يرتبط الأمن المجتمعي والأمن السيبراني في تحقيق الأمن الشامل؛ حيث إن الأمن السيبراني يشكل أحد الأعمدة الأساسية لتعزيز استقرار والأمن المجتمعي، وفي ظل تزايد الاعتماد على التكنولوجيا في مختلف مجالات الحياة اليومية، أصبح للأمن السيبراني دوراً هاماً في حماية البيانات والمعلومات والبنية التحتية الرقمية التي يعتمد عليها الأفراد والمجتمعات (المرداس، 2023: 212).

لتحقيق الأمن في المجتمع من خلال الأمن السيبراني يجب الحد من الهجمات الإلكترونية التي قد تؤدي إلى تعطل الخدمات الأساسية، وتعزيز الثقة الرقمية في ظل وجود بيئة آمنة على الإنترنت تشجع أفراد المجتمع على استخدام التكنولوجيا بشكل إيجابي، فضلاً أنَّ الأمن السيبراني يحقق الأمن المجتمعي من خلال التصدي للمنصات التي تنشر الأخبار الكاذبة التي قد تؤثر سلباً على السلم المجتمعي (أبو حسين، 2021: 33).

تحديات الأمن المجتمعي المرتبطة بالذكاء الاصطناعي:

يُعدُّ الذكاء الاصطناعي تقنية رئيسية في العصر الحالي ويفرض العديد من التحديات على الأمن المجتمعي، وتشمل أهم هذه التحديات فقدان فرص العمل أو قلتها، إذ يمكن أن يؤدي التطور التكنولوجي والتقني في مجال الذكاء الاصطناعي إلى التشغيل الآلي وفقدان وظائف بشرية في بعض الصناعات، مما يؤثر على دخل بعض أفراد المجتمع وينعكس سلباً على الأمن المجتمعي (أبو منصور، 2021: 7).

يمكن أن يتسبب انتشار التقنيات المبنيّة على الذكاء الاصطناعي وخاصة التطبيقات القائمة على جمع البيانات الشخصية، في إثارة المخاوف بشأن حماية الخصوصية، وبالتالي يعرض الأفراد إلى الابتزاز والاحتيال والتنمر الإلكتروني وغيرها من الجرائم المرتبطة بالتكنولوجيا المتطورة وسوء استغلال المعطيات الشخصية.

ويتفاعل الأفراد مع التكنولوجيا بشكل كبير، إذ يقضون ساعات طويلة في استخدام التطبيقات الاجتماعية وينعزلون عن محيطهم المجتمعي، بما ينعكس سلباً على الأمن المجتمعي، وبالتالي فإنَّ

التحديات التي يفرضها الميتافيرس على الأمن المجتمعي تشمل مختلف مكوناتها وعلى جميع الأبعاد (أبو منصور، 2021: 7).

تحديات الأمن المجتمعي المرتبطة بالجرائم السيبرانية:

تشكّل الجرائم السيبرانية تحدياً كبيراً في العصر الرقمي وتؤثر بشكل مباشر على الأمن المجتمعي، إذ يتم استخدام التكنولوجيا المتطورة في ارتكاب هذا النوع من الجرائم، وعليه، انتقل السلوك الجرمي من واقع مادي ملموس إلى عالم رقمي افتراضي، مما أسهم في زيادة انتشار الجرائم السيبرانية بشكل كبير التي تنعكس سلبًا على الأمن المجتمعي (الدوسري، 2019: 44).

إن تهديد الأمن المجتمعي يرتبط بشكل مباشر بالتحديات المعاصرة، التي تهدد عمليات الاحتيال والاختراقات الإلكترونية ومدخرات المجتمع والبيانات الشخصية لأفرادها وخاصة مع اتساع خارطة استعمال التطبيقات الإلكترونية في الحياة اليومية بما يؤدي إلى توتر مالي في البيئة المجتمعية (بانقا، 2019: 54).

شكلت كذلك التحديات المعاصرة تهديداً للأمن المجتمعي، وذلك في ظل استغلال التكنولوجيا الحديثة والفضاء الإلكتروني الواسع في انتشار العديد من الجرائم التي تهدد الأمن المجتمعي، مثل جرائم التحرش والابتزاز الإلكتروني، إضافةً إلى التأثيرات الاجتماعية المتمثلة في قطع العلاقات الاجتماعية والعزلة الاجتماعية، وتهديد القيم والعادات السائدة في المجتمع، وتنعكس هذه الحالات على أمن المجتمع ونوعية العلاقات، فتتضاعف التوترات والنزاعات المجتمعية، ويساهم عدم أخذ احتياطات الأمان في إجراء المعاملات الرقمية المجرمين على ارتكاب جرائم الاعتداء على الخصوصية الشخصية للمتعامل وتعريض الأمن المجتمعي للخطر، فيواجه المجتمع تحديات تهدد أمنه المجتمعي (بن برغوث، 2023: 456).

تحديات الأمن المجتمعي المرتبطة بوسائل التواصل الاجتماعي:

تمثل وسائل التواصل الاجتماعي أخطر التحديات المعاصرة على الأمن المجتمعي، إذ يستخدم البريد الإلكتروني الذي يعتبر من أهم الوسائل المستخدمة في "الإرهاب الإلكتروني"، وذلك من خلال استخدام البريد الإلكتروني في التواصل بين الإرهابيين وتبادل المعلومات بينهم، بل أنَّ كثيراً من العمليات الإرهابية التي حدثت كان البريد الإلكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية، إذ يتم نشر أفكارهم والترويج لها من خلال المراسلات الإلكترونية (أبو العينين، 2019: 239).

يعمل الإرهابيون على إنشاء وتصميم مواقع لهم على وسائل التواصل الاجتماعي لنشر أفكارهم والدعوة إلى مبادئهم، بل التعليم والتدريب على الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية، فقد أنشئت مواقع لتعليم صناعة المتفجرات، وكيفية اختراق وتدمير المواقع، وكيفية الدخول إلى المواقع المحجوبة، ووجدوا قدرتهم على تنفيذ عملياتهم الإرهابية من خلال وسائل التواصل الاجتماعي التي جلبتها التكنولوجية المتطورة، فأصبح تلك الوسائل تحدياً للأمن بشكل عام والأمن المجتمعي بشكل خاص (السالم، 2022: 619).

وباتت تلك الوسائل من أبرز أشكال الإرهاب الإلكتروني التي يستخدمها الإرهابيون لنشر أفكارهم الهدامة وتحقيق أهدافهم السيئة والسلبية التي تهدد الأمن المجتمعي، إذ تتم عملياتهم من خلال الاتصال الخفي، وجمع المعلومات الإرهابية، والتخطيط والتنسيق للقيام بأعمالهم غير المشروعة، إضافةً إلى الحصول على التمويل لتجنيد وتعبئة الإرهابيين، وتدريبهم من خلال إنشاء المواقع السرية، وإصدار بياناتهم الجرمية وفق أحدث الوسائل والطرق، حيث باتت هذه الوسائل بدلاً من أن تكون نعمة واستخدامها بشكل إيجابي للتواصل، أصبحت نقمة تهدد الكيانات البشرية والمجتمعية (المدني، 2020: 198).

ويستخدم الإرهابيون وسائل التواصل الاجتماعي بطريقة مباشرة في توظيف الجماعات المتطرفة للإنترنت لإحداث الأثر المطلوب مباشرة في الأنظمة المحوسبة المرتبطة بالإنترنت لتحقيق أهدافها، ومن أبرزها التهديد السيبراني وهو التوعُّد بترويع الناس، وبإلحاق الضرر بالأفراد وأسرهم، باستخدام البريد الإلكتروني، ووسائل التواصل الاجتماعي، ومن أنواعه سرقةُ البيانات والملفَّات، وابتزاز الجهات المستهدَفة، واستخدام البيانات للقتل، أو التهديد باختراق واجهات المواقع الإلكترونية ووضع أعلام التنظيمات الإرهابية عليها (المقدادي، 2017: 64).

تحديات الأمن المجتمعي المرتبطة بالعولمة:

تعبر العولمة عن ظاهرة تتداخل بأمور السياسة والاقتصاد والثقافة والاجتماع والسلوك، وتحدث فيها تحولات على مختلف الصور التي تؤثر في حياة الناس، وعلى الرغم من الآثار الإيجابية التي أتاحتها العولمة، فقد فرضت العديد من التحديات على الأمن المجتمعي، حيث أدت الصراعات العديدة والحروب الداخلية في دول العالم إلى نزوح الأسر وتفككها، كما أدت العولمة إلى زيادة عدم المساواة في الحياة وارتفاع تكاليف المعيشة وتضاعف أسعار العقارات، بما يمثّل تحدياً للأمن المجتمعي (عبد المطلب، 2020: 23).

يواجه الأمن المجتمعي تحديات نتيجة ما يطلق عليه بالعولمة الثقافية، التي تعرف بأنها اتجاه شامل يجعل الثقافات العالمية المختلفة تتفتح وتتأثر ببعضها، بما ينعكس على الأمن المجتمعي، حيث أسهمت في إشاعة مفاهيم ومصطلحات غريبة عن المجتمع، والاعتراف بالعلاقات المخالفة للعادات والتقاليد والدين، وتغييب نظام القيم الاجتماعية لصالح قيم جديدة مثل القيم المادية والإباحية، والحرية المُطلقة (المقدادي، 2016: 91).

التحليل:

يشكل الأمن المجتمعي عنصرًا رئيسًا لتحقيق الأمن والاستقرار في المجتمع، حيث يهدف إلى مواجهة كافة أشكال التهديدات والتحديات التي تواجه المجتمع.

تلعب مرتكزات الأمن المجتمعي التي ترتبط بالفرد دوراً في تعزيز الأمن والاستقرار، إذ أنَّ هذه المرتكزات تهدف إلى حماية الأفراد وتمكينهم من المساهمة الإيجابية في بناء مجتمع آمن ومستقر، وهذا يتطلب تحقيق تعاوناً بين أفراد المجتمع والمؤسسات المدنية والدولة لضمان بيئة تعزز قيم الأمن المجتمعي.

تعتبر الجماعة الإنسانية وحدة اجتماعية أساسية في تشكيل المجتمع، حيث تعمل من خلال تكويناتها وعلاقتها الاجتماعية في توفير بيئة مستقرة آمنة تعزز من تماسك المجتمع، وهذا يعتمد بالأساس على وعي المجتمع لتحقيق الأمن المجتمعي فيه ومواجهة التحديات المستقبلية.

إنَّ الأمن السيبراني ليس مجرد تقنية بل هو جزء من حماية الأمن المجتمعي، وذلك عندما تكون الأنظمة الرقمية محمية، ينعكس ذلك على أمن المجتمعات واستقرارها، وحماية الأفراد من التهديدات، وبالتالي فإنَّ الأمن السيبراني هو الحصن المنيع في تحقيق الأمن المجتمعي، وهذا يؤكد على العلاقة الإيجابية بين الأمن المجتمعي والأمن السيبراني.

يعتبر الذكاء الاصطناعي من التحديات المعاصرة الذي أصبح يهدد انتهاك الخصوصية واستغلال الأفراد مادياً، ويحمل مخاطر كبيرة تتطلب التعامل معها بحذر، الأمر الذي يتطلب التعامل مع هذا التطور تحقيق التوازن في استخدام هذه التكنولوجيا الحديثة.

أصبحت الجرائم السيبرانية من أبرز التحديات التي تهدد الأمن المجتمعي في العصر الرقمي، وذلك من خلال استخدام أنشطة غير مشروعة تنفذ باستخدام التكنولوجيا المعاصرة، مما جعل تأثيرها يشكل خطورة على الأمن المجتمعي.

إنَّ وسائل التواصل الاجتماعي رغم الإيجابيات التي وفرتها، فإنها تعتبر أداة تحمل في طياتها العديد من التهديدات على الأمن المجتمعي بسبب سوء استخدامها واستغلالها من قبل الجماعات الإرهابية لنشر الأفكار الهدامة وتهديد الأمن والاستقرار في المجتمع.

تعتبر العولمة من التحديات المعاصر التي تهدد الأمن المجتمعي في ظل التأثيرات السلبية على العادات والتقاليد والقيم المجتمعية، وتفكك الهوية الثقافية والوطنية، وتعلم ثقافات تختلف عن العادات والتقاليد السائدة في المجتمع، مما أصبحت تشكل تهديداً للأمن المجتمعي.

المبحث الثالث: التأثيرات الحالية والمستقبلية للميتافيرس على الأمن المجتمعي

يحاول كل الفاعلين سواء الدول أو المؤسسات أو الأفراد الوصول إلى أفضل الطرق لتحقيق الأهداف والغايات المرجوة في مجال الأمن السيبراني، وفي ظل تنامي مهددات الأمن السيبراني في عصر الميتافيرس وانعكاساتها على الأمن المجتمعي يتطلب الاستعداد لأهم التحولات والتهديدات.

التأثيرات الإيجابية للميتافيرس

ينطوي عالم الميتافيرس على العديد من الإيجابيات، حيث يُركز على إنشاء اقتصاد افتراضي، يُعَدُّ بمثابة منصة مثالية لتبادلات الأصول الرقمية ذات القيمة الاقتصادية الحقيقية، ويتمتع الميتافيرس بإدخال أنشطة ووظائف تجارية جديدة في المساحات الافتراضية المشتركة بالإضافة إلى العالم الحقيقي، كما أنه جعل الحواجز الجغرافية من الأمور التي لا يجب وضعها في الاعتبار، إذ بمجرد الدخول إلى هذا العالم الأكثر تطوراً لم يعد الموقع الفعلي مهماً، لأن هذه التقنية ببساطة تعمل كمساحة محايدة (طاهر، 2024: 706-707).

توفر العوالم الافتراضية بيئة للتعلم النشط، إذ يمكن للأفراد التفاعل مع ثقافات مختلفة بشكل مباشر، بما يعزز التفاهم والتقارب الثقافي بين المجتمعات، كما يساهم في تعزيز الأعمال وتطوير البيئة الرقمية الابتكارية والابداعية، ومن التأثيرات الإيجابية تعزيز التجارة الالكترونية والتعاون بين الأفراد والمؤسسات، وتبرز أهميته في تعزيز الصحة العقلية والنفسية، وذلك في ظل ابتعاد الأفراد عن الضغوط اليومية، والتمتع بالواقع الافتراضي لتقنية الميتافيرس (Kye et al, 2021: 47).

التأثيرات السلبية للميتافيرس:

يشكل الأمن المجتمعي إحساس الأفراد والجماعات التي يتشكل منها المجتمع بالطمأنينة، والشعور بالأمن والاستقرار، وهوما يحفزهم على العمل والإنتاج، لذلك فإنَّ الهدف الأساسي في الأمن المجتمعي وقاية المجتمع من عوامل الانحراف التي تهدد كيانه (سيد، 2024: 14).

ومن أبرز التأثيرات السلبية للميتافيرس، يمكن إجمالها على النحو التالي:

1. المضايقات والتنمر: احتلت ظاهرة التنمر عبر الوسائل الحديثة في هذا العصر مشكلة، وذلك نظراً للمضايقات العديدة التي يعرض لها الشباب والمراهقين عبر الوسائل الحديثة والتطبيقات الاجتماعية المختلفة (العلوي والتوزاني، 2022: 134).
2. مشاكل الصحة العقلية: يعد إدمان الإنترنت أو الألعاب مشكلة كبيرة بالفعل للأطفال والكبار في وقتنا الحالي، وقد يكون الانخراط في قضاء كل الوقت بالميتافيرس مشكلة أكبر في المستقبل (المدني، 2020: 205).
3. سرقة الهوية: يشعر العديد من الخبراء بالقلق بشأن احتمالية أن تصبح حوادث سرقة الهوية أسهل في عصر الميتافيرس، إذا لم يتم تنفيذ تدابير أمنية صارمة، ففي العالم الافتراضي، سوف يتم استخدم الصور الرمزية AVATARS إذا حدث ذلك، فقد يتظاهر المخترق بأنه أنت، ويمكن أن يتسبب ذلك في إحداث فوضى في العالم الافتراضي وكذلك أيضاً الواقعي (سيد، 2024: 17).
4. مشاكل الخصوصية: هناك العديد من المخاوف المشروعة بشأن الخصوصية في عصر الميتافيرس، فالتكنولوجيا التي تتعقب بالفعل سلوك عبر الإنترنت ستكون موجودة أيضاً في الميتافيرس، ومن المرجح أن يصبح التعقب أكثر توغلاً، بسبب الأجهزة التي يتم استخدامها في العوالم الافتراضية (بريك، 2022: 64).
5. صعوبة تتبع استخدام الأطفال للميتافيرس: سيكون فهم ما يفعله الأطفال عبر هذه العوالم أكثر صعوبة، لأن الآباء لا يمكنهم رؤية العالم الذي ينظر إليه أطفالهم عبر نظارات الواقع الافتراضي الخاصة بهم (بن برغوث، 2023: 453).
6. اتساع الفجوة الرقمية: يتطلب الوصول إلى عوالم الميتافيرس المختلفة أجهزة عالية التقنية ومكلفة للغاية، ولا يمتلك كل شخص في العالم الإمكانيات المادية التي تؤهله لشراء

الأجهزة المستخدمة في تقنية الميتافيرس وهو ما يجعل المساواة في الوصول إلى الميتافيرس شبه منعدمة (العلوي، والتوزاني، 2022: 141).

7. جمع بيانات غير مصرح بها: يعتبر من أبرز سلبيات الميتافيرس، هو احتمالية قيام الشركات بجمع بيانات غير مصرح بها عن المستخدمين، فالواقع الافتراضي لديه القدرة من خلال الأجهزة الخاصة به على جمع ونقل البيانات إلى مستوى بعيد (المرداس، 2023: 217).

8. الهجمات عبر برامج الفدية: برامج الفدية هي برامج ضارة، تقوم بتشفير البيانات وتمنع أي شخص من الوصول إليها، وبما أنَّ ملف التعريف الخاص على منصات الميتافيرس سوف يحتوي على معلومات أكثر حساسية من تلك الموجودة على حسابات مواقع التواصل الاجتماعي، فإنَّ مخاطر هذه البرامج سوف تتعاظم في المستقبل (سيد، 2024: 21).

و اقع جر ائم الميتافيرس وتأثير اته المستقبلية:

يمتلك الميتافيرس القدرة على تغيير الطريقة التي نتفاعل بها ونشارك مع بعضنا البعض والتكنولوجيا، ومع ذلك، هناك كذلك عيوب ومخاطر محتملة تماماً كما هو الحال مع أي تقنية جديدة، حيث تُعدُّ المشكلات المحتملة المتعلقة بالخصوصية والأمان جزءاً من الجانب السلبي للميتافيرس (بريك، 2022: 65).

علاوة على ذلك قد يكشف الأشخاص عن بيانات ومعلومات شخصية أكثر حساسية في تقنية الميتافيرس، مما يزيد من أخطار القرصنة وخرق البيانات، وبالتالي فإنَّ تقنية الميتافيرس مفتوحة لمخاطر أمنية مختلفة بما في ذلك جرائم الميتافيرس، مثل: القرصنة وسرقة الملكية والضرر المالي والإضرار بسمعة واستقرار المجتمعات الافتراضية، حيث قد يستخدم المجرمون الميتافيرس لارتكاب جرائم إضافية أو نشر البرامج الضارة أو سرقة البيانات الشخصية. (الصاوي، 2022: 144).

وقد تجد الحكومات والمؤسسات صعوبة في مواكبة التكنولوجيا وتفتقر إلى الموارد أو الأدوات اللازمة لمواجهة الميتافيرس، كما قد يؤدي هذا الغياب للرقابة إلى مشاكل مثل النشاط غير القانوني والمحتوى الخطير (القاضي، 2023: 532).

ومن أمثلة الجرائم التي حدثت في الميتافيرس قضية سرقة عناصر رقمية في لعبة runescape في هولند، حيث كان يمتلك الضحية وهو مراهق يمتلك أرقامًا خاصة داخل اللعبة تعرف باسم Amulet of fury، ومن ثم قام مراهقان بمهاجمته في الواقع الحقيقي في منزله وهدداه بالعنف وأجبراه بالقوة على تسجيل الدخول إلى حسابه في اللعبة ونقل الأرقام الخاصة بالضحية إلى حساب أحد الجناة (Lodder, 2013: 2).

مواجهة التهديدات الناجمة عن الميتافيرس

يشكل الميتافيرس نوعًا من الحياة الاجتماعية الافتراضية، وهي أشبه بحياة ثانية موازية للحياة البشرية، وينتج عن ذلك مميزات وسلبيات في الحياة الاجتماعية.

أولاً: تأمين الشبكات على نحو يمنع من اختراقها: تُعَدُّ محاولة الشركات والمؤسسات والحكومات تأمين شبكاتها المعلوماتية ضد الاختراق بمثابة وسيلة تحدّ إن لم تمنع مطلقاً من عملية الاختراق لهذه الشبكات، ومن ثم فهي تؤدي بطريقة غير مباشرة إلى منع اختراق هذه الشبكات والحد من تأثيراتها خاصة في عصر الميتافيرس، ومن طرق تحصين الشبكات الداخلية كذلك من الاختراق عملية التشفير، والتشفير يعني تحويل البيانات المكتوبة إلى أرقام أو رموز لا يمكن حلها إلا بالنسبة لمن يمتلك شفرة حل هذه الرموز والأرقام، وهناك برامج تشفير متقدمة لحماية البيانات المخزنة على شبكات الحاسب الآلي للعبور تحتاج إلى التوقيع السيبراني وهناك شهادات التصديق على هذا التوقيع السيبراني وجميعها برامج معلوماتية تساعد في الحماية من التهديدات الناجمة عن الميتافيرس (الحيدري، 2019: 211).

تتمثل وسائل تأمين البيانات من المخاطر الناجمة عن الميتافيرس بما يلي:

1. الجدار الناري أو حوائط المنع: يعرف الجدار الناري بأنه مجموعة أنظمة معلوماتية وبرامج توفر سياسات أمنية حتى يتم إجبار جميع عمليات الخروج من الشبكة والدخول إليها بأن تمر من خلال هذا الجدار الناري والذي يمنع أي مخترق أو متطفل من الوصول إلى الشبكة، فهي برامج تقوم بصد محاولات الاختراق أو الهجوم الوافد من شبكة الميتافيرس لتهديد الشبكة الداخلية أو النظام المعلوماتي (عقوني، 2023: 89).
2. مكافحة الفيروس المعلوماتي: يعرف الفيروس المعلوماتي بأنه برنامج للحاسب الآلي مثل أي برنامج آخر لكنه يهدف إلى إحداث أكبر ضرر بنظام الحاسب الآلي وله القدرة على ربط نفسه بالبرامج الأخرى، وتتم مواجهته ببرامج حماية، وهو ما يتطلب تأهيل وتدريب المعنيين على مكافحة المخاطر السيبرانية فلابد من وضع سياسة رشيدة تستند على تدريب المختصين على مواجهة هذه المخاطر (سليمان وآخرون، 2023: 76).

متطلبات مواجهة التهديدات الناجمة عن الميتافيرس:

إنَّ تطور أساليب المواجهة التقنية لن يغني بأي حال من الأحوال عن ضرورة التكاتف الدولي، ووضع برامج للتوعية، أو وضع تشريعات جديدة من أجل الحد من المخاطر المتصاعدة للأمن السيبراني، وقد حدد المنتدى الاقتصادي العالمي الأولويات التالية لمواجهة التهديدات السيبرانية المتزايدة، وهي بناء المرونة السيبرانية، وتعزيز التعاون العالمي، وفهم التكنولوجيا والشبكات المستقبلية (بريك، 2022: 75).

1. بناء المرونة السيبرانية: هي قدرة النظام على التعافي من الصدمة بطريقة مثلى، إما بالعودة إلى حالته الأصلية أو إلى حالة معدلة جديدة، ويمكن تعزيز المرونة السيبرانية عن طريق تطوير وتأطير الحلول المستقبلية الكفيلة بالتصدي للتهديدات الناجمة عن الميتافيرس، وتعزيز الممارسات الفعالة عبر النظم الرقمية الحديثة (الصاوي، 2022: 150).

2. تعزيز التعاون الدولي: زيادة التعاون العالمي بين أصحاب المصلحة من القطاعين العام والخاص، من خلال تعزيز الاستجابة الجماعية للجرائم الإلكترونية، والتصدي المشترك للتحديات الأمنية الرئيسية (القاضي، 2023: 533).

3. فهم شبكات وتكنولوجيا المستقبل: تحديد فرص وتحديات الأمن السيبراني المستقبلية ذات الصلة بتقنيات الثورة الصناعية الرابعة وخاصة الميتافيرس، وتصميم الحلول التي تساعد على بناء الثقة لمواجهة التحديات الناجمة عن هذه التطورات، وما يمكن أن تسببه في اختراق الأنظمة وخصوصية الأفراد (عبد العال، 2022: 466).

4. التوعية بالأمن السيبراني: مع انتشار التهديدات والمخاطر السيبرانية على نطاق واسع، لابد من أن تستثمر الدول في عمل برامج التدريب وتثقيف المواطنين، والعاملين في المؤسسات، حول حماية البيانات الحساسة، ومن الأهمية توجيه النصيحة لمستخدمي عالم الميتافيرس بأن يبقوا على الحذر والوعي لما يقومون به في هذا العالم والتعامل مع منصات تعمل بجدية على حماية مستخدميها (العلوي والتوزاني، 2022: 155).

5. إدارة المخاطر السيبرانية: أي تحديد التهديدات والمخاطر التي تتعرض لها الدولة، والمؤسسات في القطاعين العام والخاص، وذلك في ظل الاحتفاظ بقائمة جرد بجميع أصول نظم التحكم الصناعي، بما في ذلك الأجهزة والبرامج وتقنيات البنية التحتية الداعمة، ومن ثم الانتقال إلى وضع سياسات وإجراءات وتدريبات ومواد تعليمية للأمن السيبراني تنطبق على نظم التحكم الصناعي، وتطوير وممارسة إجراءات الاستجابة للحوادث التي تدمج تكنولوجيا المعلومات وعمليات تكنولوجيا التشغيل (الهزاني، 2023: 101).

6. وضع القواعد والتشريعات الجديدة: إن زيادة الهجمات والتهديدات في الفضاء السيبراني وظهور الميتافيرس يتطلب الاستمرار في وضع لوائح وتشريعات وسياسات جديدة لتحقيق متطلبات الأمن السيبراني، حتى يتم مواكبة تلك التطورات المتسارعة في مجال مهددات ومخاطر الأمن السيبراني وحمايتها من الاختراقات (سليمان وآخرون، 2023: 136).

7. التعاون الدولي: قد يتطلب الردع السيبراني الفعال مخططاً واسع النطاق من القدرات السيبرانية الدفاعية والهجومية، مدعومة بإطار قانوني دولي قوي، وإن تصميم القدرات السيبرانية الدفاعية وتصميم أفضل الأدوات القانونية غير متنازع عليها نسبياً، وإن تعقيد الأمن السيبراني الحديث يتطلب سرعة التعاون بين مختلف الجهات المعنية، في سبيل مكافحة التهديدات الإلكترونية الناجمة عن الميتافيرس التي تتعرض لها الدول والأفراد، وإن العمل الجماعي الدولي هو السبيل الوحيد للوصول إلى النتائج المنشودة لموجهة مخاطر وتهديدات الأمن السيبراني في عصر الميتافيرس (سيد، 2024: 39-40).

يمكن الإشارة إلى أنَّ الميتافيرس يعتبر مستقبل التكنولوجيا الرقمية، ولكن في الوقت ذاته يأتي بتحديات سيبرانية تستدعي صياغة استراتيجيات مبتكرة لضمان أمن المستخدمين

واستقرار المجتمع من خلال تعزيز التعاون الدولي وتطوير الحلول التقنية المناسبة وتوظيف أنظمة الذكاء الاصطناعي في مواجهة التهديدات الناجمة عن الميتافيرس.

التحليل:

يعتبر الميتافيرس بيئة افتراضية تجمع بين الواقع الافتراضي والواقع المعزز، حيث يحدث تجولاً كبيراً في طريقة تفاعل الأفراد والمؤسسات، وعلى الرغم من الفرص التي يقدمها، إلا أنه يحمل العديد من المخاطر التي قد تهدد الأمن المجتمعي في ظل تداخل العالم الافتراضي مع الحياة الواقعية.

يشكل واقع جرائم الميتافيرس في ظل الاعتماد المتزايد في المستقبل على هذا العالم الافتراضي ظهور أنواع جديدة من الجرائم الرقمية التي تعكس تحديات غير مسبوقة في الأمن المجتمعي، حيث تخلف آثارًا نفسية واجتماعية في ظل عدم شعور الأفراد في الآمان.

يمثل الميتافيرس مستقبل البشرية في المستقبل، ولكن يأتي بتحديات أمنية تهدد الأمن السيبراني، حيث تفرض هذه البيئة الافتراضية أهمية وضع الضوابط السيبرانية التي تضمن حماية البيانات والهوية الرقمية من خلال الجمع بين التقنيات المتقدمة لمواجهة المخاطر المحتملة في المستقبل.

أصبح الأمن السيبراني في العصر الرقمي أحد الركائز الأساسية لتحقيق الأمن المجتمعي، الذي يهدف إلى حماية المجتمع من التهديدات الناجمة عن التطورات الحديثة في العالم وتؤثر في الاستقرار الاجتماعي والاقتصادي.

يشكل تأمين الشبكات في عصر الميتافيرس عاملاً رئيسًا لضمان أمان المستخدمين واستدامة هذه البيئة الافتراضية في المستقبل من خلال وضع سياسات أمنية صارمة وتعزيز التعاون بين الجهات المختلفة لمنع الاختراقات وتوفير تجربة آمنة للمستخدمين من تهكير واختراق الخصوصيات.

إنَّ الميتافيرس بيئة مبتكرة مليئة بالفرص، ولكن يولد تحديات مختلفة للبشرية، حيث أنَّ مواجهة التهديدات ووضع استراتيجيات شاملة لمواجهتها، لمواجهة المخاطر وتحقيق تجربة آمنة تتمثل في التعاون وإدارة المخاطر السيبرانية التي تحد من هذه المخاطر.

استخدام التكنولوجيا المتطورة لمواجهة الميتافيرس وتحليل الأنشطة المشبوهة والكشف عن السلوكيات الضارة وتأمين البيانات والمعلومات الرقمية من خلال تقنيات تشفير متقدمة، وتطبيق تقنيات للتحقق المتعدد لتأمين الهوية الرقمية للأفراد.

***- خاتمة**

مع التطور السريع لتقنيات الميتافيرس، يواجه الأمن السيبراني تحديات جديدة تتطلب حلولاً متقدمة لحماية البيانات والخصوصية والهويات الرقمية، إذ يتيح الميتافيرس بيئات افتراضية مترابطة، مما يزيد من مخاطر الجرائم السيبرانية مثل الاحتيال، وسرقة الهوية والاختراقات الأمنية، والتلاعب بالمعلومات، وعلى المستوى المجتمعي، فإنَّ تأمين هذه البيئات الرقمية أصبح ضرورة للحفاظ على الثقة والأمان الرقمي، حيث قد تؤدي الثغرات الأمنية إلى زعزعة الاستقرار المجتمعي، لهذا يتطلب المستقبل تطوير سياسات تنظيمية قوية، وتعزيز الوعي السيبراني بين المستخدمين.

إنَّ تأثير الأمن السيبراني على الأمن المجتمعي سيكون كبيراً، حيث يمكن أن تؤدي الثغرات الأمنية إلى تهديد الاستقرار الاجتماعي والاقتصادي، بينما تسهم الحلول الفعالة في بناء بيئة رقمية آمنة تعزز الثقة في التقنيات المستقبلية، لذلك، فإنَّ الاستثمار في تقنيات الحماية، والتشريعات الرقمية، والتوعية

السيبرانية سيحدد مدى قدرة المجتمعات على الاستفادة من الميتافيرس بأمان واستقرار، هذا يعني أنَّ نجاح الميتافيرس كمساحة رقمية آمنة يعتمد على مدى تكيف الأمن السيبراني مع هذا الواقع الجديد، مما سيؤثر بشكل مباشر على الأمن المجتمعي ويحدد مستقبل التفاعل البشري في العوالم الافتراضية.

1. يؤدي التوسع في انتشار واستخدام الميتافيرس بشكل سلبي إلى ارتفاع معدلات الجرائم والهجمات السيبرانية، حيث أنَّ الاختراقات الأمنية المتكررة وانتهاك الخصوصية ينعكس على ثقة الأفراد والمؤسسات في استخدام بيئة الميتافيرس، مما قد يعيق تطوره واعتماده على نطاق واسع.
2. تسهم التهديدات السيبرانية بشكل سلبي في زيادة المخاطر المجتمعية، إذ يمكن استغلال الهجمات السيبرانية والمعلومات الزائفة في المتيافيرس لنشر الفوضى والفتن وزعزعة الاستقرار المجتمعي، مما يؤثر على فعالية الأمن السيبراني في مواجهة التهديدات المستقبلية.
3. تسهم التحولات التكنولوجية الحديثة بشكل طردي في فرض تحديات جديدة في الأمن المجتمعي، إذ انَّ التوسع في استخدامات الذكاء الاصطناعي والميتافيرس وانترنت الأشياء، مما يزيد من المخاطر المتعلقة بالخصوصية والجرائم السيبرانية، الأمر الذي يتطلب استجابة أمنية متطورة للحفاظ على استقرار المجتمعات.
4. تسهم التحديات المعاصرة وما صحابها من ظهور جرائم مستحدثة التي تُعَدُّ من أبرز التحديات التي تهدد الأمن المجتمعي في العصر الرقمي في ظل استخدام أنشطة غير مشروعة تنفذ باستخدام التكنولوجيا المعاصرة، مما أصبحت تشكل طردياً في تهديد الأمن المجتمعي.
5. هنالك علاقة طردية بين التحديات المعاصرة ومستوى تعقيد تحقيق الأمن المجتمعي، حيث يؤدي زيادة التحديات إلى ارتفاع مستوى المخاطر التي تواجه المجتمعات وهذا يعني أنَّ الأمن السيبراني جزء لا يتجزأ من بيئة الميتافيرس لتحقيق بيئة مجتمعية آمنة لضمان الاستقرار وحماية المجتمعات من المخاطر المستقبلية.

بناءً على ما توصلت إليه الدراسة من نتائج، يوصي الباحث بما يلي:

1. تعزيز الدول تقنيات الحماية السيبرانية، وذلك من خلال دعم الدراسات المتخصصة في الذكاء الاصطناعي لتطوير حلول أمنية متقدمة تحمي المستخدمين في بيئة الميتافيرس.
2. تطوير المجتمع الدولي تشريعات وأطر قانونية، وذلك من خلال وضع قوانين تنظيمية واضحة تحكم الهوية الرقمية وحماية البيانات وحقوق المستخدمين في الميتافيرس، مع ضمان الالتزام بالمعايير الدولية للأمن السيبراني.
3. حث الدول على نشر ثقافة الأمن الرقمي من خلال برامج توعية وتدريب تستهدف الأفراد والمؤسسات لتعريفهم بالمخاطر السيبرانية في العالم الافتراضية وطرق الوقاية منها.
4. إنشاء الدول وحدات متخصصة لمراقبة ومنع الاحتيال والاختراقات والهجمات السيبرانية في الميتافيرس، بالتعاون بين الحكومات والقطاع الخاص.
5. تعزيز المجمع الدولي التعاون في مجال الأمن السيبراني، ودعم الشراكات بين الدول والمؤسسات التقنية لمشاركة أفضل الممارسات والتقنيات الحديثة لمواجهة التهديدات السيبرانية في الميتافيرس.

**

قائمة المصادروالمراجع

الكتب

- الحيدري، زينب (2019). الأمن السيبراني – المخاطر – التحديات – المواجهة، ط1، الدوحة: دار الشرق للطباعة والنشر والتوزيع.
- الدوسري، خليفة (2019). الجريمة السيبرانية - المحددات النظرية والسياسات الجنائية وآليات المكافحة والوقاية، دار الوتد: الدوحة.
- سليمان، محمد، وغزال صلاح وفنسنت كارشيدي والعدوي عادل (2023). الميتافيرس - الفرص والتحديات الأمنية، الرياض: دار جامعة نايف العربية للعلوم الأمنية.
- عقوني، محمد (2023). ميتافيرس، ط1، القاهرة، در الكتاب الجديد.
- المقدادي، خالد غسان (2017). ثورة الشبكات الاجتماعية – ماهية مواقع التواصل الاجتماعي وأبعادها، ط1، عمان: دار النفائس للنشر والتوزيع.

المجلات والدوريات العلمية

- أبو العينين، يسر عطية محمد (2019). أثر استخدام شبكات التواصل الاجتماعي في التطرف الفكري، مجلة تطوير الأداء الجامعي، (5)، 234-243.
- أبو منصور، حسين (2021). الذكاء الاصطناعي وأبعاده الأمنية، أوراق السياسات الأمنية، 2 (1)، 1-18.
- بانقا، علم الدين (2019). مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية – دراسة حالة دول مجلس التعاون الخليجي، سلسلة دراسات تنموية، المعهد العربي للتخطيط، العدد (63)، دولة الكويت، 11-64.
- برجل، الصالح (2023). مقومات الأمن المجتمعي، المجلة الجزائرية للأمن والتنمية، العدد (2)، 63-75.
- بريك، أيمن محمد (2022). تطبيقات الميتافيرس وعلاقتها بمستقبل صناعة الصحافة الرقمية – دراسة استشرافية، المجلة المصرية لبحوث الإعلام، العدد (78)، 45-76.
- البعاج، هديل تومان (2023). الوعي الاجتماعي بالأمن السيبراني لدى الطلبة – دراسة ميدانية على طلبة الجامعات كلية الأمام الكاظم أنموذجاً، مجلة العلوم الإنسانية، العدد (12)، 451-471.
- بن برغوث، ليلى (2023). الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي والذكاء الاصطناعي، المجلة الدولية للاتصال الاجتماعي، العدد (1)، 443-459.
- بن عليه، جدو (2022). تحديات الأمن السيبراني لمواجهة الجريمة الالكترونية، المجلة الجزائرية للأمن الإنساني، العدد (7)، 299-319.
- حسين، رامي، وجميل أشرف (2016). دور الأسرة في مواجهة المخاطر والتحديات التي تواجه الأمن المجتمعي في ماليزيا، مجلة جامعة النجاح للأبحاث والعلوم الإنسانية، (7)، 135-137.
- زروقة، إسماعيل (2018). الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، جامعة محمد بو ضياف المسيلة، المجلد (10) العدد (1)، الجزائر، 23-51.
- السالم، فاطمة (2022). دور مواقع التواصل الاجتماعي في الترويج للتطرف الفكري، المجلة المصرية لبحوث الإعلام، (79)، 611-647.
- السمحان، مني عبد الله (2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، العدد (111)، 1-27.
- سيد، جمال عبده (2024). السؤال القانوني لمستقبل الأمن الشرطي في مواجهة جرائم الميتافيرس الإلكترونية، مجلة معهد دبي القضائي، العدد (17)، 1-58.
- الصاوي، محمد كرم كمال الدين (2022). العالم الما ورائي (الميتافيرس) بين الواقع والمأمول وفاعليتها في مجال الجرافيك، مجلة القانون والعلوم التطبيقية، العدد (4)، 135-151.

- الصبحيين، عيد حسن، والرصاعي، محمد سلامة (2018). دور المدرسة ومناهج التعليم في تحقيق الأمن المجتمعي من وجهة نظر القادة التربويين في الأردن، مجلة العلوم الإنسانية والاجتماعية، (4)، 201-128.
- طاهر، هاله محمد (2024). الجرائم السيبرانية في الميتافيرس "نحو استراتيجيات قانونية فعالة، المجلة القانونية، العدد (2)، 691-720.
- العباسي، غسق غازي (2016). الأمن الاجتماعي وعلاقته بالمسؤولية الاجتماعية، مجلة الأستاذ، العدد (216)، 32-67.
- عبد العال، إسراء صابر (2022). توظيف تقنية الميتافيرس داخل الأخبار بالمؤسسات الصحفية العربية – دراسة تطبيقية، المجلة المصرية لبحوث الرأي العام، العدد (2)، 431-468.
- عبد المطلب، حسين محمد (2020). العولمة مفهومها ومجالاتها وأخطارها وموقف الإسلام منها، المجلة العلمية، العدد (4)، 13-62.
- العلوي، سكينة والتوزاني محمد (2022). مستقبل الذكاء الاصطناعي – الميتافيرس نموذجاً، مجلة القانون والأعمال الدولية، العدد (24)، 130-157.
- علي، أحمد وخليفة عمر (2024). الأمن البيئي والاجتماعي ودورهما في تحقيق التنمية المستدامة، مجلة أبحاث كلية الآداب، جامعة سرت، العدد (16)، 72-87.
- فوزي، إسلام (2019). الأمن السيبراني – الأبعاد الاجتماعية والقانونية تحليل سيكولوجي، المجلة الاجتماعية القومية، العدد (2)، 99-139.
- القاضي، لمياء محمود (2023). تقنية الميتافيرس ومستقبل تعليم الاقتصاد المنزلي في ظل التعلم الرقمي، المجلة العلمية لعلوم التربية، العدد (17)، 511، 549.
- المدني، محي الدين أحمد (2020). دور وسائل التواصل الاجتماعي في تفشي ظاهرة الإرهاب والتطرف في ضوء استراتيجية مقترحة للمواجهة، المجلة الدولية أبحاث في العلوم التربوية والإنسانية والآداب واللغات، (2)، 178-212.
- المرداس، ندى خالد (2023). الأمن السيبراني في المملكة العربية السعودية بين الواقع والمأمول - دراسة نظرية تحليلية، المجلة الدولية لنشر الأبحاث والدراسات، العدد (49)، 204-225.
- نورهان، محمد، وحسنين، إلهام، وشيحه، هناء، وعلوان، رشا، والشامي، منال (2021). الأمن المجتمعي وعلاقته بواقع التمكين الاجتماعي والاقتصادي للمرأة السعودية في ضوء التنمية المستدامة – - دراسة وصفية، مجلة الفنون والعلوم التطبيقية، (1)، 145-166.
- الهزاني، نورة بنت ناصر (2023). ضوابط ومتطلبات الأمن السيبراني لحماية البيانات، مجلة مكتبة الملك فهد الوطنية، العدد (28)، 61-121.

الرسائل العلمية

- أبو حسين، حنين جميل (2021) الإطار القانوني لخدمات الأمن السيبراني، (رسالة ماجستير)، جامعة الشرق الأوسط، عمان، الأردن.

المراجع الأجنبية

- Kye, B., Han, N., Kim, E., Park, Y., & Jo, S. (2021). Educational applications of metaverse: possibilities and limitations. Journal of Educational Evaluation for Health Professions, 18, 41-49.
- Lodder, Arno (2013). Dutch Supreme Court 2012: Virtual Theft Ruling a One-Off or First in a Series?, Journal of Virtual Worlds Research, Vol. 6, No. 3, 1-12.