جامعة نايف العربية
للعلوم الأمنية
NAIF ARAB UNIVERSITY
FOR SECURITY SCIENCES
تأسست ١٩٧٨ Est. 1978

سلسلة دراسات أمنية

الميتافيرس
الفرص والتحديات الأمنية

دار جامعة نايف للنشر - 2023

جامعة نايف العربية
للعلوم الأمنية
NAIF ARAB UNIVERSITY
FOR SECURITY SCIENCES
تأسست ١٩٧٨ Est. 1978

سلسلة دراسات أمنية

الميتافيرس
الفرص والتحديات الأمنية

محمد سليمان
صلاح غزال
فنسنت كارشيدي
عادل العدوي

2023

Security Studies Series

Metaverse

Security Challenges and Opportunities

Mohammed Soliman

Salah Ghazzal

Vincent Carchidi

Adel El-Adawy

2023

الميتافيرس: الفرص والتحديات الأمنية

محمد سليمان[1]، صلاح غزال[2]، فنسنت كارشيدي[1]، عادل العدوي[3]

[1] معهد الشرق الأوسط، واشنطن، الولايات المتحدة الأمريكية.
[2] جمعية البلوك تشين، واشنطن، الولايات المتحدة الأمريكية.
[3] مركز البحوث الأمنية، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية.

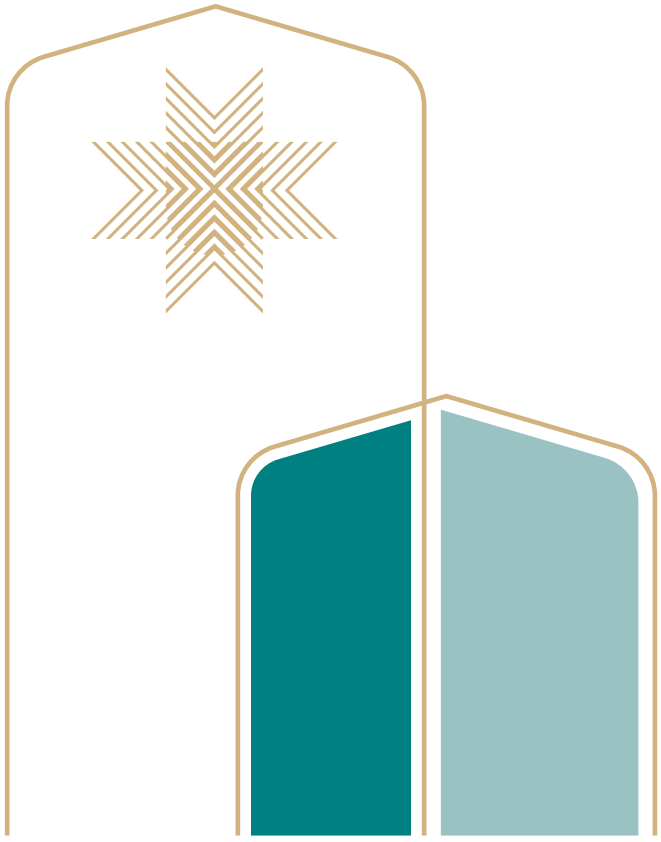
Metaverse: Security Challenges and Opportunities

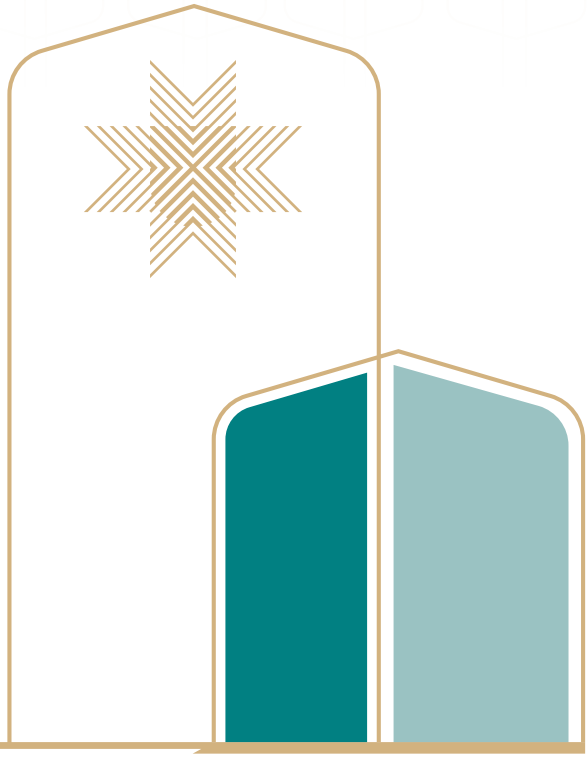
Mohammed Soliman[1], Salah Ghazzal[2], Vincent Carchidi[1], Adel El-Adawy[3]

[1]Middle East Institute, Washington, D.C, USA.
[2]Blockchain Association, Washington, D.C, USA.
[3]Security Research Center, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia.

ردمك (ورقـــي) ISBN (PBK) 978-603-8361-52-8
ردمك (إلكتروني) ISBN (EBK) 978-603-8361-50-4
رقم إيداع (طباعي) pDEPOSIT 1445/4798
رقم إيداع (إلكتروني) eDEPOSIT 1445/4793
DOI:10.26735/978-603-8361-50-4

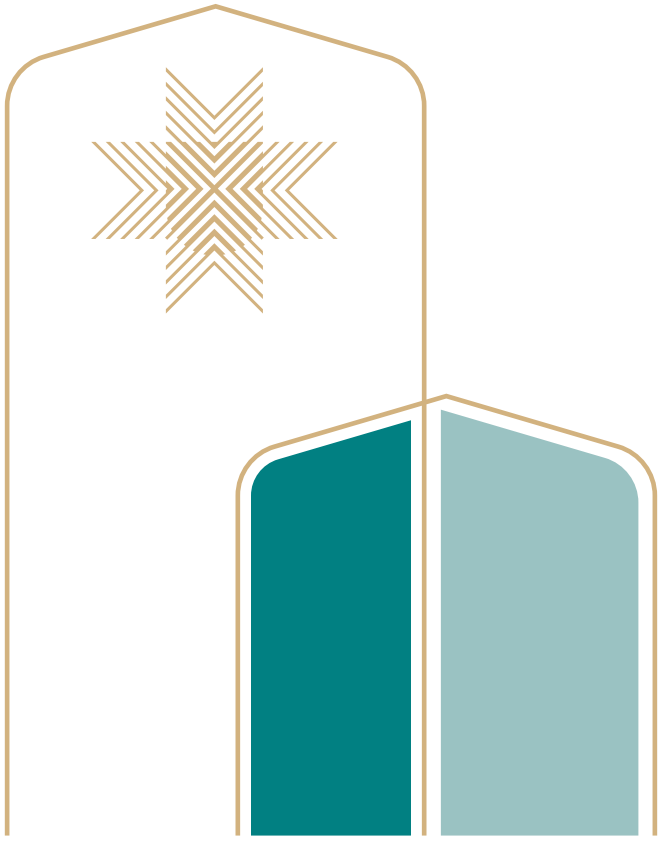
سلسلة دراسات أمنية
ردمد (ورقـــي) ISSN(Print) 8762-1658
ردمد (إلكتروني) ISSN(Online) 8770-1658

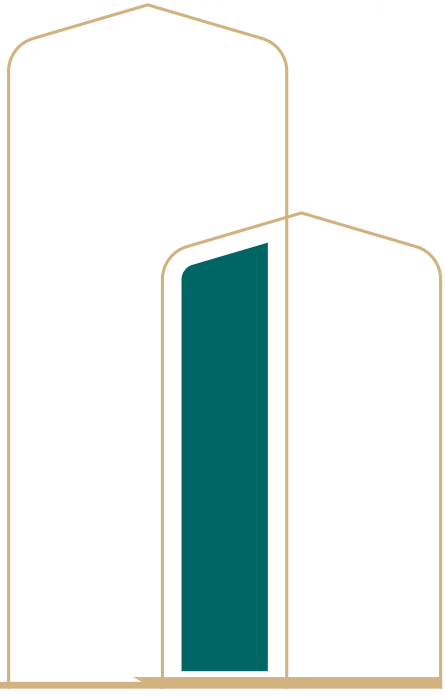




المحتويات

قائمة الأشكال





الملخص التنفيذي

يعتبر الميتافيرس (Metaverse) عَالَماً افتراضيًّا تفاعليًّا، وقد اكْتَسَبَ شعبيةً سريعةً خلال السنوات القليلة الماضية؛ حيث يسمح للمستخدمين بالتفاعل مع المُجَسَّمات الرقمية لأنفسهم (Digital Representations) وللعالم المحيط بهم لحظيًّا، ومن خلال الجمع بين عناصر الواقع الافتراضي والواقع المُعَزَّز والإنترنت، فإن تقنية الميتافيرس تتجاوز الواقع الافتراضي التقليدي من خلال تكامل عناصر التقنيات الحديثة والأجهزة المنزلية ودمجها، وهو ما يَخْلُقُ تجربةً مختلطةً رقميةً وماديةً سَلِسَةً، كما يمكن للمستخدمين الانخراط في مجموعات عديدة من الأنشطة الترفيهية إلى التعليم والتجارة وكذلك الحوكمة.

ولقد أصبحَ وجودُ تقنيةِ الميتافيرس أمرًا متاحًا بفضل مجموعةٍ من التقنيات الأساسية، مثل: شبكة إنترنت الجيل الخامس والجيل السادس المتطورتين، وإنترنت الأشياء (Internet of Things,)، وحوسبة الحافة (Edge Computing)، وربما الأهم من ذلك تقنية سلسلة الكتل (Blockchain Technology) لدورها المُمَيَّز في الأمن. ويمكن للمستخدمين، بغض النظر عن مكان إقامتهم، الوصول إلى هذا النظام الافتراضي باستخدام التقنيات الملحقة، بما في ذلك الواقع المختلط والواقع الافتراضي والواقع المُعَزَّز، كما أنها مزودة بأجهزة استشعار جمع البيانات، وهو ما يوفر تجربةً تفاعليةً جزئيةً أو كليةً داخل الميتافيرس، وبمجرد الدخول، يتعامل المستخدمون بعضهم مع بعضٍ باستخدام الأصول الرقمية المعروفة باسم العملات المشفرة (Cryptocurrencies)، التي تُجَسِّدُ بنيةً جديدةً للتفاعلات الرقمية المعروفة باسم شبكة ويب 3.0 (على عكس شبكة الويب 2.0 الحالية).

وإنَّ تَقَدُّمَ الذكاءِ الاصطناعيِّ وانتشارَهُ، وهو مجال مزدهر فعليًّا في المجتمع العربي، يوفر أدوات جديدة للتفاعل الافتراضي، ومع اهتمام العالم العربي الواضح بالتحول الرقمي وتسخير مزايا التقنيات المتقدمة، فإن التحول أصبح جاهزًا للمشاركة الإقليمية المستندة إلى أسس آمنة، ويتناسب هذا النظام الافتراضي مع الأجندة الإقليمية للعالم العربي، ويُعَدُّ جاهزًا لتسخيره من قِبَلِ الممارسين العرب.

ومع هذا الطموح، تظهرُ مهدداتٌ جسيمةٌ، ولا سيما فيما يتعلق بالأمن الوطني. فإن الانتهاكات المحتملة لهذا النظام متنوعةٌ وحقيقيةٌ، ويجب على الدول العربية التصدي لها أثناء سعيها للاستفادة من هذا النظام؛ حيث تمثل التقنيات التأسيسية والتكميلية المتطورة، التي تؤيد استخدامها والاعتماد عليها، مجموعةً من التحديات الأمنية الجديدة، وهناك في المجمل تسع فئات تندرج تحتها هذه المهددات الأمنية:

(1) البنية التحتية المعرضة للخطر. (2) التلاعب بالهوية. (3) محاذير انتهاكات الخصوصية. (4) الاختراق. (5) الإرهاب الإلكتروني. (6) الجرائم السيبرانية. (7) انتشار المعلومات المضللة والزائفة. (8) المخاطر التي تهدد السيادة والثقافة (9) التعبئة الاجتماعية والسياسية.

ويتنبأ مسؤولو وخبراء الأمن العرب بمخاطر وتحديات محددة في كل فئة من هذه الفئات التسع، فبالنسبة للبنية التحتية المعرضة للخطر، **فمن المرجح أن تزداد احتمالية اختراق الشبكات من قِبَل الجهات الفاعلة الخبيثة،** وقد يتيح الوصول المحلي وغير المُصَرَّح به إلى التقنيات الملحقة، مثل: معدات الواقع الافتراضي من خلال إنترنت الأشياء، سبلًا جديدةً لنشر البرامج الضارة، ويمكن أن يؤدي استخدام أدوات الذكاء الاصطناعي إلى ترسيخ التحيزات الاجتماعية أو الثقافية القائمة في الميتافيرس مع تعزيز القدرة على التواصل بشأن الأنشطة غير المشروعة بين المستخدمين.

وفيما يخص التلاعب بالهوية، فنظرًا لأن الهويات الرقمية أصبحت أكثر أهمية من أي وقتٍ مضى، فإن إمكانية التلاعب بها أو سرقتها، بما في ذلك **الأصول والمعلومات الشخصية للضحية، يمكن إساءة استخدامها بسهولة،** وهو ما يؤدي إلى انتشار عدم الثقة على نطاق واسع، ولا شك أن الجهات الفاعلة الخبيثة سوف تكتشف وسائل الهندسة الاجتماعية الجديدة بلا أدنى شك داخل الميتافيرس، التي تُشَكِّلُ خطرًا كبيرًا على الأمن الوطني، حيث إن هذا النظام الافتراضي سيضفي في الوقت نفسه شرعيةً على التفاعل البشري في عالم افتراضي، في حين أنه يوفر أيضًا نقاط ضعفٍ جديدةٍ.

وتشكل محاذير **انتهاكات الخصوصية العديد من التحديات الفورية في الميتافيرس، ومن ضمنها حماية بيانات المستهلك،** ومعالجة البيانات المؤسسية والاحتفاظ بها، والواقع المُسَلَّم به أن تخزين بيانات الميتافيرس لامركزي (على عكس الأساليب المركزية التقليدية)، ولا يمكن تجاهل احتمال قيام جهة فاعلة خبيثة بدمج نفسها في جزء من الشبكة، وربما اكتساب ثقة الآخرين عند قيامها بهذه العملية.

فضلًا عن تلك المحاذير، فإن تهديد الاختراق، مجال الخطر الرابع، سوف يستمر في الميتافيرس كما حدث في البيئات الرقمية التقليدية، ويمكن للمخترقين استغلال نقاط الضعف في البنية التحتية للميتافيرس، أو شن هجمات تَصَيُّدٍ احتياليةٍ لاختراق المعلومات الشخصية للمستخدمين. كما تنتقل عمليات الاستيلاء على الحسابات، والبرمجيات الخبيثة، وبرمجيات الابتزاز، وسرقة الملكية الفكرية، وتعدين العملات المشفرة غير الشرعي من البيئات الرقمية الحالية إلى العالم الافتراضي للميتافيرس.

ويُشَكِّلُ الإرهابُ الإلكترونيُّ تهديدًا بليغًا، قد يكون على هيئة التجسس السيبراني وخلخلة تماسك أو أُسُس الميتافيرس وتلفيق التهمة للآخرين بارتكاب جرائم عن طريق إخفاء الهوية؛ لذا يتعين على مسؤولي وخبراء الأمن العرب التعامل بجدية مع مثل هذه التهديدات. ومن الممكن تعزيز الجهود، التي تبذلها الجماعات الإرهابية لنشر حملاتها الدعائية وأفكارها المتطرفة، من خلال العمل ضمن مساحة افتراضية شرعية غير مؤهلة للتعرض والتعامل مع هذا المستوى من التنسيق والتنظيم للجهات الفاعلة الخبيثة. وسوف تقوم الجهات

الفاعلة الخبيثة غير الحكومية المنخرطة في أنشطة إجرامية، مثل: الاحتيال، وبيع المخدرات في العالم المادي أيضًا، بمحاولات تمويل الجماعات الإرهابية، والقيام بالتهديدات بغض النظر عن المكان الذي قد تقيم فيه هذه الجهات الفاعلة الخبيثة في العالم المادي.

وقد تصبح الميتافيرس مع نضجها بمرور الوقت بيئةً خصبةً ومناخًا مناسبًا للمزيد من الأخطار والجرائم السيبرانية، التي تشمل عمليات الاحتيال، حيث تُستَخْدَم رموزُ الاستجابة السريعة المزيفة للمعاملات وسرقة الأصول الرقمية ومخططات غسل الأموال، التي تستغل الأنماط الجديدة لخدمات الدفع الرقمية التي تقدمها تقنية الميتافيرس، ويؤدي غياب الأطر القانونية المعلومة والتدابير الأمنية المستخدمة في الميتافيرس إلى احتمالية تعرض الأصول للسرقة وغسلها بسهولة أكبر.

وكما هو مألوف في الجرائم السيبرانية، فإن نشر الجهات الفاعلة الخبيثة للمعلومات المضللة والزائفة من خلفيات متنوعة، تُشَكِّلُ معًا مجال الخطر السابع، حيث يؤدي استخدام تقنية التزييف العميق وأنظمة الذكاء الاصطناعي المولدة لانتحال شخصية من شخصيات العالم الحقيقي إلى جانب الطبيعة التفاعلية للواقع الافتراضي، إلى إتاحة فرصٍ فريدةٍ على مستوى الشركات أو الدول لعمليات التأثير والحملات الدعائية وكذلك التجسس. وسوف تُشَكِّلُ الجهودُ المبذولةُ للرقابة أو حظر المعلوماتِ في الميتافيرس تحديًا كبيرًا.

ويُكَمِّلُ مجالا الخطر الأخيران بعضهما بعضًا، ففي المقام الأول، وفيما يتعلق بالمخاطر التي تُهَدِّدُ السيادةَ والثقافةَ، حيث تشكل تقنية الميتافيرس خطرًا فريدًا يتمثل في الانتشار السهل والسريع لأنماط جديدة من التفاعل الاجتماعي والثقافي التي تتيحها الميتافيرس، في حين يتم تأمينه للاستخدام المستمر من قِبَل الدول العربية على المدى المتوسط والطويل، للمستخدمين بالانفصال عن واقع الحدود المادية التي يقيمون ضمنها. ومع التنبؤ بظهور الوسائط الرقمية، مثل: منصات وسائل التواصل الاجتماعي، يمكن لتقنية الميتافيرس أن تُقَلِّلَ من الحاجة الافتراضية للأفراد لبلدانهم ومجتمعاتهم بطريقة تُقَلِّلُ من ارتباطهم بكليهما.

وتُعَدُّ إمكانيةُ التعبئة الاجتماعية والسياسية داخل الميتافيرس قوية، ومع تنبؤ الوسائط الرقمية مرة أخرى بتأثيرات الميتافيرس، فإن هذا العالم الافتراضي سيسمح للأفراد الذين لديهم مظالم سياسية بالالتقاء والتنظيم دون الاهتمام بالتباعد المادي، وهذا ما يعد أمرًا بالغ الخطورة.

وعلى الرغم من أن هذه القائمة من الاستخدامات السلبية للميتافيرس قد تبدو شاقة، فإنها تدعم وَفْرَةَ الفرصِ التي توفرها للعالم العربي، حيث تنشأ عن طريق هذه الفرص مسؤوليات جديدة للأمن والتنظيم المشترك، ومن الممكن أن تكون هذه الفرص متاحة في قطاعات الدفاع والأمن والتجارة في الدول العربية مع إتاحة فرص للتعاون الإقليمي، الذي يُحَقِّقُ المنفعةَ المتبادلةَ. وتتطلب التبعية المادية للسمات الافتراضية للميتافيرس

بالفعل رأس المال البشري، ومن الممكن معالجة «هجرة ذوي الكفاءات» من العرب بشكل مثمر من خلال اجتذاب الصناعة إلى المنطقة من أجل انتشارها.

ويعتمد النهج المشترك لاستخدام تقنية الميتافيرس على الأسس التجارية للتقنيات الرقمية التي نشأت من الخليج العربي إلى شمال إفريقيا والشرق الأدنى، ومن هذه الأسس تأتي الفرص، ومنها الفرص على مستوى المستهلك بما في ذلك التسوق الافتراضي والألعاب والجوالات والانغماس الثقافي، التي تُعَدُّ أرضًا خصبةً لوجهات النظر المشتركة بين المستخدمين عبر الحدود المادية. وتبرز جودة التعليم وإمكانية الوصول إليه والأساليب المحسنة للعمليات الطبية والطرق الجديدة للوصول إلى الأفراد المحتاجين إلى العلاج الطبيعي وإعادة التأهيل، كفرصٍ جديدةٍ خاصةٍ بالميتافيرس.

وتقدم تقنية الميتافيرس أيضًا فرصًا على مستوى المؤسسات، التي تظهر بشكل واضح في ظهور مساحة العمل الافتراضية، وتلوح في الأفق تجربةُ عملٍ عن بُعْدٍ أكثر مشاركة وتفاعلًا، تُيَسِّرُها تقنية الميتافيرس. حتى الفرص على مستوى الدولة، والفوائد التي تشترك بين الدول في جميع أنحاء المنطقة العربية، تُقَدِّم نفسها بطرقٍ ذات اهتمام مباشر للمسؤولين والخبراء الأمنيين. وتتخذ هذه الفرص أشكالَ تعميقِ وتوسيعِ جهودِ التحول الرقمي الحالية، وتعزيز التدريب الأمني المشترك وتقنياته في عمليات المحاكاة التفاعلية، وتحسين التخطيط الإستراتيجي.

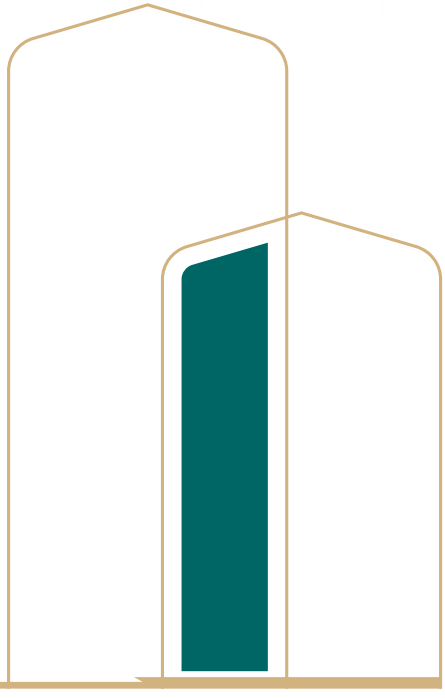
وتصطحب كل فرصة من هذه الفرص مخاطر أمنية ذات صلة، يجب إدارتها بشكل استباقي وتعاوني عبر الدول والقطاعات لضمان أن تُؤْتِيَ ثمارَها، ويعتمد الجذب المستمر لرأس المال البشري إلى المنطقة على تنفيذ هذه الجهود على أسس قوية لازدهار الميتافيرس، فمن الضروري ألا يواكب المسؤولون الأمنيون وتيرة القطاع التجاري في الابتكار ونشر ميزات الميتافيرس داخل المنطقة العربية. وبالتالي، فإن حوكمة الميتافيرس لا بد أن تكون محايدة بخصوصيات أي بلد أو منطقة. وفي الواقع، ونظرًا لأن تقنية الميتافيرس لامركزية بشكل جذري، فلن يتمكن هذا العالم الافتراضي من البقاء والازدهار إلا من خلال نهج مشترك بين الدول، وبالتعاون مع خبراء الأمن والجهات الفاعلة في القطاع الخاص.

كما يمكن أن يشكل مجلس وزراء الداخلية العرب فِرَقَ عملٍ متخصصةٍ في الميتافيرس بهدف العمل على تحقيق هذه الغاية مع ضم خبراء في هذا المجال، ولكن لتوظيف هذه الجهود بشكل مناسب، يجب التوضيح بشكل مفصل للدول العربية الوعي والفهم الأساسي للتحديات الأمنية والسياسية التي يفرضها استخدام الميتافيرس.

ويمكن أن تعقد جامعة نايف العربية مؤتمرًا إقليميًّا بشأن الميتافيرس يهدف إلى وضع جدول أعمال لوزراء الداخلية العرب، وتكمن القيمة الأساسية لهذا المؤتمر في دوره كمنصة انطلاق لصانعي السياسات العرب ومسؤولي الأمن وخبراء الأمن السيبراني وهيئات إنفاذ القانون وممثلي القطاع الخاص؛ لتحقيق التوافق حول مواجهة تلك التحديات الأمنية التي تفرضها الميتافيرس.

ويتمثل الهدف الأساسي لكلٍّ من فرق العمل المعنية بالأمن والسياسة في الميتافيرس في مكافحة الأنشطة الإجرامية الإقليمية، وتعزيز التعاون مع الوكالات السيبرانية العربية لصالح إعطاء الأولوية لأمن الميتافيرس وإعداد بروتوكولات أمنية موحدة. وبالنظر إلى الدور الحيوي الذي تؤديه الأصول الرقمية داخل الميتافيرس، فمن الضروري أيضًا للعالم العربي إنشاء منظمة الأصول الافتراضية العربية؛ لتكون بمثابة هيئة تنظيمية إقليمية حكيمة تعمل في إطار اختصاص جامعة الدول العربية، وينبغي لوزراء الداخلية العرب أيضًا أن يقودوا حملات توعية ومحو الأمية الرقمية والافتراضية لمعالجة الطبيعة الديناميكية للعالم الافتراضي، والمخاطر المتزايدة المرتبطة بالميتافيرس.

وتفرضُ الميتافيرس تحدياتٍ، وتطرحُ فرصًا للمنطقة العربية، وتستطيع الدول العربية تسخير إمكاناتها لتعزيز الأمن الوطني ودفع التنمية الاجتماعية والاقتصادية وتعدد الثقافات، وذلك من خلال فهم تداعيات تطبيق الميتافيرس على الأمن الوطني وتنفيذ الإستراتيجيات المناسبة، ويؤدي التعاون مع الشركاء الدوليين والاستثمار في البحث والتطوير وإعداد أطر تنظيمية قوية أدوارًا حيوية في التغلب على تعقيدات الميتافيرس وضمان تعظيم فوائده. وتستطيع الدول العربية، من خلال اتخاذها تدابير استباقية، أن تضع نفسها في مصافِّ قادة مجال تقنية الميتافيرس، مع حماية مصالح مواطنيها في هذا القطاع الرقمي الجديد.



المقدمة

مُنْذُ بدايةِ ثورةِ عالمِ الميتافيرس في عام 2021، تُقَدِّرُ شركة «ماكينزي الاستشارية» أن العالم استثمر بالفعل أكثر من 177 مليار دولار أمريكي في إعداد العالم الافتراضي واعتماده، وهذا المبلغ مستمر في التزايد؛ ونظرًا لأن المزيد من الشركات تدرك أن تقنية الميتافيرس تُمَثِّلُ فرصةً مربحةً، تتنبأ شركة «أكسنتشر لتكنولوجيا المعلومات» بأن الميتافيرس يمكن أن تصبح فرصةً تجاريةً بقيمة تريليون دولار أمريكي بحلول نهاية عام 2025 (Savitz, 2023). ولقد جذبت الآفاقُ التجاريةُ الواسعةُ لتقنية الميتافيرس الشركاتِ إلى العالم الافتراضي؛ حيث تتوقع نموًّا وتأثيرًا اقتصاديًّا هائلًا، وتنجذب الشركات إلى الفرص التي تُقَدِّمُها تقنية الميتافيرس، وتستكشف بشغف طرقًا للاستفادة من إمكاناتها، ومع التوقعات الواعدة وإمكانات التجارب الرقمية التحويلية، تضع الشركات من مختلف المجالات نفسها في طليعة هذا المشهد الجديد، وتسعى للاستفادة من المزايا المحتملة للميتافيرس، وعلى الرغم من أن عالم الميتافيرس مليءٌ بالفرص والمزايا التجارية، فإن له أيضًا تأثيرًا محتملًا هائلًا على قطاع الأمن الوطني.

وبالنظر إلى تلك الآثار، تتخذ الحكومات وهيئات إنفاذ القانون التدابير اللازمة لضمان السلامة والحماية وسلامة المستخدمين والكيانات العاملة في الميتافيرس، الأمر الذي يستلزم تنفيذ كلٍّ من تدابير المراقبة العلنية، ونشر الجهات الفاعلة السرية، التي تعمل بشكل مجهول عبر الإنترنت لحماية البيئة الافتراضية. ولدى القيادة العربية، الممثلة في جامعة الدول العربية وهيئات الإدارة الإقليمية المعنية، فرصةٌ كبيرةٌ لكي تؤدي دورًا محوريًّا في تشكيل الجهد العالمي لتنظيم أنشطة الميتافيرس مع وضع الأساس اللازم للاستفادة من فوائدها. ويمكنهم أخذ زمام المبادرة في وضع إرشادات وأطر عملٍ تُعَزِّزُ الممارساتِ التجاريةَ الآمنةَ، وتضمن المعاملات المالية الآمنة داخل الميتافيرس. وفي الوقت ذاته، يمكنهم مراقبة أنشطة تقنية الميتافيرس لتحديد عدة تهديدات والتعامل معها، ومن هذه التهديدات على سبيل المثال لا الحصر التجسس والإساءة والمضايقة عبر الإنترنت والإرهاب، وبيع وتوزيع المخدرات، وبيع السلاح وغير ذلك من المخاطر الأمنية، وبأخذ خطواتٍ استباقيةٍ، يمكن للقادة العرب المساهمة في المحافظة على التكامل والأمان والاستخدام المعقول لتقنية الميتافيرس بشكل عالمي.

وفي الوقت الحالي، تُعَدُّ الشركاتُ ذات الأصل الأمريكي في مقدمة الشركات التي تعمل على تطوير تقنية الميتافيرس والتوسع فيها، وقد أدت الشركات المذكورة دورًا محوريًّا في تشكيل بيئة الميتافيرس من خلال الابتكارات والخبرات التقنية والاستثمارات الكبيرة التي ضختها في هذا المجال، وقد كانت الريادة لهذه الشركات في إدخال منصات الواقع الافتراضي والواقع المُعَزّز وتجارب الألعاب الجذابة ومنصات شبكات التواصل الاجتماعي، التي جعلت الناس يعيشون في العالم الرقمي، وكأنهم يعيشون في العالم المادي، بعد أن طمست الحدود بين كلا

العالمين، وعلى الرغم من ذلك، ظهرت الصين في الساحة كمنافس، وضخت استثماراتها الفعالة في منظومة تقنية الميتافيرس كبديل للولايات المتحدة، وقد أدركت الصين مكانة تقنية الميتافيرس ووجهت موارد ضخمة لتطويرها، مدفوعة في ذلك بقطاع تقني قوي لديها، وبقاعدتها الكبيرة من المستخدمين. وفي الوقت الذي تعد فيه الولايات المتحدة رائدةً في مجال تقنية الميتافيرس، دخلت الصين باستثماراتها، التي وضعتها في مكانة مرموقة كمنافس قوي لها في هذا المجال الرقمي المتطور بسرعة مذهلة.

وعلاوة على ذلك، تبذل العديد من المؤسسات والجهات من مختلف القطاعات جهودًا كبيرة لإيجاد مكان لها في تقنية الميتافيرس، ومن بين هذه المؤسسات شركات التكنولوجيا العملاقة التي أدركت إمكانات تقنية الميتافيرس، وخصصت موارد كبيرة لمشاريع ذات صلة بهذه التقنية. ومن هذه الشركات شركة «ميتا» التي كانت معروفة سابقًا باسم شركة فيسبوك، والتي غَيَّرت اسمها وتسويقها التجاري من شركة تعمل في مجال شبكات التواصل الاجتماعي؛ لتصبح الآن شركة مختصة بتقنية الميتافيرس، وضخت استثمارات ضخمة بقيمة (13.7) مليار دولار في عام 2022؛ لإنشاء منصتها الخاصة بها القائمة على تقنية الميتافيرس.

إن استحواذ شركة مايكروسوفت على شركة أكتيفجن بليزارد، بقيمة مذهلة تبلغ 68.7 مليار دولار أمريكي، لا يزال قائمًا وينتظر الموافقة التنظيمية، وبذلك تحتل شركة مايكروسوفت المرتبة الثالثة كأكبر شركة ألعاب على مستوى العالم، وليس ذلك فحسب، وإنما سيضعها أيضًا في صفوف الجهات الرئيسة الفاعلة في تطوير تقنية الميتافيرس، كما ستعتبر إضافة قوية إلى مساعي شركة مايكروسوفت لتطوير منصة الواقع المختلط الخاصة بشركة مايكروسوفت، وتعد شركة «مايكروسوفت ميش» تجسيدًا لمحاولة الشركة الجديدة الطموحة لتوحيد التعاون بين تقنية التصوير المجسم والتقنيات الافتراضية عبر سماعات الواقع الافتراضي وأجهزة الواقع المعزز أو أجهزة الحاسب الآلي المحمولة والهواتف الذكية (Microsoft, n.d). كما بذلت شركة جوجل هي الأخرى محاولاتها للدخول في مجال تقنية الميتافيرس، مستفيدة في ذلك من خبرتها في مجالي الواقع الافتراضي والواقع المعزز، وذلك من خلال عدة مشاريع، مثل: جوجل إيرث للتجول الافتراضي (Google Earth VR)، وجوجل للواقع المُعَزّز (Google ARCore).

وتؤدي شركات الألعاب المعروفة بخبراتها العميقة والممتدة دورًا محوريًّا في تشكيل عالم تقنية الميتافيرس، فمن جانبها قامت شركة إبيك جيمز، مبتكرة اللعبة المشهورة فورتنايت، بتوسيع تجاربها الشبيهة بتقنية الميتافيرس من خلال التعاون مع فنانين موسيقيين (Peters, 2022). أما منصة روبلوكس، وهي منصة ألعاب أنشأها المستخدمون، فقد أثبتت نفسها باعتبارها منصة شبيهة بتقنية الميتافيرس، تسمح لمستخدميها بإنشاء

تجاربهم الافتراضية الخاصة بها ومشاركتها مع غيرهم. وبدأت شركات الإعلام والترفيه التقليدية في التعرف على إمكانات تقنية الميتافيرس، وذلك إلى جانب قطاعات التقنية والألعاب الخاصة بهذه الشركات (Brown, 2022). أما إذا أتينا لشركات الترفيه، مثل: شركة ديزني، وشركة وارنر برذرز، وشركة نتفليكس، فسنجد أنها تسعى للعثور على المشاريع والشراكات المتعلقة بتقنية الميتافيرس، وذلك بغرض توسيع شهرة علاماتها التجارية، وإشراك جمهورها في تجارب رقمية متطورة.

وعلاوة على ذلك، تم إثراء منظومة تقنية الميتافيرس بالمساهمات التي قدمتها العديد من المشاريع الجديدة والشركات الصغيرة. وتشارك هذه المشاريع الابتكارية بشكل فعال في بناء تقنية الميتافيرس وتوسعتها، حيث تركز على مجالات منصات الواقع الافتراضي والتجارب الاجتماعية وأدوات إنشاء المحتوى وتكامل تقنية سلسلة الكتل وغيرها. وتسهم تلك الجهود في تنويع وتحريك تقنية الميتافيرس، والتشجيع على الابتكار، وفتح إمكانات لآفاق جديدة للمستخدمين. وبشكل كلي ومتكامل، تعمل المؤسسات والكيانات المذكورة، التي تشمل الشركات والكيانات التي تعمل في مجالات التقنية والألعاب والترفيه والمشاريع الجديدة، على تأسيس عالم تقنية الميتافيرس، الذي يعد مجالًا هائلًا فيما يتعلق بالتقنيات التحويلية المترابطة، حيث يدلي كل منها بِدَلْوِهِ ويُقَدِّمُ خبراته وإسهاماته الفريدة الخاصة به لتشكيل مستقبل هذه التقنية.

العالم العربي وتقنية الميتافيرس

يتقارب العالم العربي وعالم الميتافيرس بعضه من بعض، كلما ازداد تنامي التحولات الرقمية الإقليمية من جهة، وتنامي تقنيات الميتافيرس من جهة أخرى.

وفكرة الميتافيرس في حَدِّ ذاتِها لا تُعَدُّ فكرةً جديدةً أو غريبةً على دول منطقة الشرق الأوسط وشمال إفريقيا، حيث توجد دول عربية قد أخذت بزمام المبادرة في التقنيات القريبة من تقنية الميتافيرس، وهو ما يجعل اعتماد الفكرة أكثر احتمالًا وأكثر تأثيرًا من اعتمادها في مناطق أخرى من العالم. وفي أوائل عام 2023، وَقَّعَت كُلٌّ من منصة «ساندبوكس» القائمة على تقنية الميتافيرس وهيئة الحكومة الرقمية في المملكة العربية السعودية مذكرةَ تفاهمٍ لبدء «اكتشاف الحلول المبتكرة وتقديم المشورة والدعم» بالتعاون بينهما فيما يتعلق بتطوير تقنية الميتافيرس (Fortis, 2023). ويعد ذلك تماشيًا مع طموحات المملكة لإنشاء منصة الميتافيرس الإدراكية القائمة على التوأمة الرقمية لمشروع مدينتها الذكية نيوم (Flanagan, 2022). ومن الممكن تحقيق

هذه الإمكانات في المنطقة الأوسع في حال توسيع نطاقها بالشكل المناسب، وتتمتع الدول العربية بوضع جيد يسمح لها بتطبيق تقنية الميتافيرس والتقنيات القريبة منها في أطرها التنظيمية، واستخدام هذه التقنية المبتكرة في تحقيق أهداف سياسية أكثر شمولية. وتُشَكِّلُ سلطة تنظيم الأصول الافتراضية بالإمارات العربية المتحدة أحد أوسع الأطر القانونية على مستوى العالم، التي تدعو لجلب سيل من المطورين والمشغلين لتقنية الميتافيرس الجدد إلى العالم العربي.

وعلى الرغم من هذا الزخم الكبير، يتعين العلم بأن سمات تقنيات الميتافيرس تتطلب تقييمًا للإمكانات حتى يتم اعتمادها، وفي العالم العربي، تمتلك العديد من الدول أساسات قوية لبنية تحتية تقنية قوية، وهو ما سيسمح بسهولة التحول نحو استخدام تقنية الميتافيرس بشكل ناجح ومثمر، وفي بداية عام 2022، امتلكت المملكة العربية السعودية والبحرين والإمارات العربية المتحدة والكويت وعمان وقطر شبكات من الجيل الخامس بغرض استخدامها في تلك الدول، كما تعمل كُلٌّ من مصر والأردن ولبنان وتركيا على إنشاء أساسات أفضل لشبكات الجيل الخامس، ومن المقرر أن يتم توفير شبكات مناسبة وأكثر موثوقية لسكان تلك الدول في أواخر عام 2023.

وقد شهدت المملكة العربية السعودية إنشاء أول أكاديمية على مستوى العالم العربي متخصصة في تقنية الميتافيرس، وتأتي في ذلك بعد فرنسا التي تعد أول دولة في العالم في هذا الشأن، وتعمل المملكة العربية السعودية على ربط تقنية الميتافيرس، التي ظهرت على الساحة، بمشروع نيوم، ودفعت ما قيمته 500 مليار دولار أمريكي؛ وذلك بغرض توحيد 14 قطاعًا على هذه التقنية، ولكي تظهر بذلك باعتبارها إحدى أكثر التقنيات المتقدمة على مستوى العالم. وتتولى المملكة زمام القيادة على الصعيد الإقليمي فيما يتعلق بالتنمية والتطوير، وذلك من خلال إدخال تقنية الميتافيرس في مبادراتها السياحية الناشئة وتوفير هذه التقنية لسكانها، وذلك لتطوير المجالات الطبية والتعليمية ومجال الرفاهية الصحية والمجالات المالية والتقنية المستقبلية. وعلى منوال المملكة العربية السعودية، تتولى الإمارات العربية المتحدة زمام القيادة في تطبيق السياسات واللوائح التنظيمية لتقنيات الجيل الثالث للإنترنت، وهو ما يجعلها أول كيان تطويري على مستوى العالم العربي، وليس ذلك فحسب، ولكن أيضًا يجعلها في قمة الكيانات العالمية التي تتبنى تقنيات الميتافيرس والجيل الثالث للإنترنت والذكاء الاصطناعي والتقنيات الجديدة على مستوى العالم.

وتتخذ الاستثمارات العربية حتى الآن فيما يتعلق بتقنية الميتافيرس أشكالًا تختلف اختلافًا كبيرًا، حيث تعطي بعض الدول الأولوية لإنشاء تقنيات معينة أو اعتمادها، والتي يمكن بناء تقنية الميتافيرس عليها أو

اعتبارها تقنيات مساعدة يمكن الوصول من خلالها لتقنية الميتافيرس. ومن ذلك، على سبيل المثال، أنفقت المملكة العربية السعودية بالفعل مليار دولار أمريكي وحدها على استثمار واحد في تقنية الميتافيرس: وهو إنشاء XRVS، كمنصة للميتافيرس الإدراكية القائمة على التوأمة الرقمية لمشروع نيوم (Haddad, 2022). ويتوقع لهذه الاستثمارات أن تُحَقِّقَ عوائدَ هائلةً عند توزيعها بمرور الوقت على مستوى الدول العربية، وبوجه عام، يمكن أن تجني منطقة الشرق الأوسط وشمال إفريقيا عوائدَ هائلةً من وراء اقتناص الفرص الاقتصادية التي توفرها تقنية الميتافيرس. وقد قَدَّرَت مجموعةُ التحليلِ إسهامَ تلك التقنية في الناتج المحلي الإجمالي على الصعيد الإقليمي بما قيمته 360 مليار دولار أمريكي سنويًّا (Analysis Group, 2020). وعلى مستوى كل دولة على حدة، يُتَوَقَّع أن تجني المملكة عائدًا بقيمة 38 مليار دولار أمريكي من الاستثمارات في تقنية الميتافيرس فقط، في حين يُتَوَقَّع أن تجني الإمارات العربية المتحدة منها عائدًا بقيمة 17 مليار دولار أمريكي؛ كما يُتَوَقَّع طبقًا للأرقام والتوقعات الأولية بالنسبة لكل من مصر والمغرب أن يكون العائد 22 مليار دولار أمريكي و5 مليارات دولار أمريكي على التوالي (Deloitte, 2023a). ويستفيد الاستثمار في الميتافيرس من النمو الملحوظ الذي يشهده العالم العربي في الآونة الأخيرة عامًا بعد عام في حجم معاملات العملات المشفرة، والذي زاد زيادة كبيرة بنسبة 48% من عام 2021 إلى عام 2022 (Chainalysis, 2022). وقد شَهِدَ سوقُ الأصولِ الرقميةِ وتقنية سلسلة الكتل (Blockchain) بمنطقة الشرق الأوسط وشمال إفريقيا، والتي تشتمل على تقنية الميتافيرس ومعاملاتها المباشرة بين الأطراف، معاملات بقيمة 566 مليار دولار أمريكي من المعاملات التي تم إجراؤها في العام الماضي. وتعد العملة المشفرة إحدى السمات الأساسية لتجربة تقنية الميتافيرس، وتعد الزيادة في حجم المعاملات بها مؤشرًا كبيرًا على أن السكان العرب يمتلكون الوضع المجتمعي الملائم والمعرفة الرقمية المناسبة لتوجيه تبني تقنية الميتافيرس على الصعيد الإقليمي.

ونظرًا لأنه يُتوقع أن ينفجر حجم سوق تقنية الميتافيرس على الصعيد العالمي بحلول عام 2030، فإن الاعتماد على هذه الاحتمالية سيصب في مصلحة العديد من القطاعات على صعيد العالم العربي (Precedence Research, n.d). ومما لا يدع مجالًا للشك أن الزيادات الكبيرة المذكورة ستؤدي بدورها إلى تشجيع الدول العربية واحدة تلو الأخرى، وسوف يؤدي الاستمرار في التدريب والتعاون واقتناص الفُرَصِ التقنيةِ إلى إفادة المنطقة كما سيؤدي إلى زيادة الفرص الاقتصادية والسياحية والتعليمية الناتجة عن استخدام تقنية الميتافيرس.

قاعدة المستخدمين الكبيرة لتقنية الميتافيرس

لا تزال الإمكانات الحقيقية لتقنية الميتافيرس لم تتحقق بشكلٍ كاملٍ بعد، حيث يُتوقع أن ترتفع تلك الإمكانات؛ لتسهم بمبلغ كبير يُقَدَّر بما يصل إلى 3 تريليونات دولار أمريكي في الناتج المحلي الإجمالي العالمي بحلول عام 2031 (Analysis Group, 2020). وهذه الأرقام تم إعدادها بناءً على الفرص الاقتصادية الكبيرة المتوقع أن يتم جنيها من وراء تقنية الميتافيرس، ولقد جذبت مشاركة المستخدمين في هذا العالم الافتراضي جمهورًا كبيرًا على مستوى العالم بالفعل، بما يتجاوز 400 مليون مستخدم شهريًّا كمتوسط فريد. وتجدر الإشارة في هذا الإطار إلى أن 51% من المستخدمين المذكورين تبلغ أعمارهم 13 عامًا أو أقل، وهو الأمر الذي يؤكد بدوره أن تقنية الميتافيرس تحظى بشعبية كبيرة بين جيل الشباب (Bybit, 2023). كما أن نسبة هائلة تبلغ 83.5% من مستخدمي تقنية الميتافيرس تقل أعمارهم عن 18 عامًا (Bybit, 2023). وتدل هيمنة الفئة السكانية الأصغر عمرًا على أنه كلما زاد تبني تقنية الميتافيرس شيئًا فشيئًا، زادت هذه التقنية زخمًا وجاذبية بشكل كبير، وهو الأمر الذي سيؤدي في نهاية المطاف إلى توسيع قاعدة مستخدميها، ورفع سقف خوض التجارب الافتراضية إلى مستوى غير مسبوق.

وعلاوة على ذلك، وطبقًا لتقرير صادر عن شركة ديلويت بتكليف من شركة ميتا، يُتوقع أنه في إطار زمني أطول يصل مداه لعام 2035، يمكن أن يؤدي اعتماد تقنية الميتافيرس إلى مساهمات سنوية بالأرقام التالية في الناتج المحلي الإجمالي العربي نتيجة لتطبيق المبادرات الحالية لاعتماد تقنية الميتافيرس: في مصر بقيمة 22-11.6 مليار دولار أمريكي؛ وفي الأردن بقيمة 1.7-0.9 مليار دولار؛ وفي المغرب بقيمة 5-2.6 مليارات دولار أمريكي؛ وفي الإمارات العربية المتحدة بقيمة 16.6-8.8 مليار دولار أمريكي؛ وفي المملكة العربية السعودية بقيمة 38.1-20.2 مليار دولار أمريكي، هذا بالإضافة إلى مساهمات أخرى في دول أخرى (Deloitte, 2023b). وينصب التركيز في هذا الشأن بشكل كبير على التوسع في قطاع الألعاب وقطاع البيع بالتجزئة، وكذلك في قطاع العقارات وقطاع السياحة (Bybit, 2023).

وقد لقيت إحدى الدراسات، التي أجريت على رجال الأعمال بتكليف من الشركة المختصة بالتقنية «سيينا» التي يقع مقرها في الإمارات العربية المتحدة في عام 2022، اهتمامًا بشكل متفاوت على الصعيد الإقليمي بتقنية الميتافيرس، فإن هذا الاهتمام يُعَدُّ مهمًّا للغاية لتحقيق أغراض تجارية. وعلى سبيل المثال، أَحَسَّ 94% من المشاركين في الاجتماعات الرسمية في الشرق الأوسط «بالارتياح» عند عقد تلك الاجتماعات في بيئة من الواقع الافتراضي (Ciena, 2022). ومما يثير الانتباه في هذا الشأن تباين مواقف المشاركين حول مدى ملاءمة استخدام

تقنية الميتافيرس للعمل مقارنة باستخدامها في الأنشطة الترفيهية، مثل: التسوق؛ حيث فَضَّل 57% و47% من المشاركين من المملكة العربية السعودية والإمارات العربية المتحدة استخدام تقنية الميتافيرس في الأنشطة الترفيهية، في حين فضل 51% من المشاركين المصريين استخدام تلك التقنية في العمل (Arab News, 2023). ويتوقع بشكل كبير أنه كلما ارتفع حجم التأييد لدمج الواقع الافتراضي في الأنشطة التجارية أو الترفيهية، ازداد نضج التقنيات الأساسية لتقنية الميتافيرس، وانتشرت التقنيات الملحقة بها على نطاق أوسع.

مخاطر تقنية الميتافيرس مقارنة بالفرص المتحققة منها

تُقَدِّمُ تقنية الميتافيرس للعالم العربي عددًا من الفرص، وكذلك عددًا من المخاطر فيما يتعلق بالأمن الوطني، فمن ناحية، يمكن أن تؤدي إلى تقديم طرقٍ جديدةٍ للتواصل والتعاون وتبادل المعلومات على صعيد الأفراد والمؤسسات، كما أنها يمكنها أن تعمل على تسهيل التعاون بين الدول وجمع المعلومات الاستخبارية ودعم جهود الأمن السيبراني. فإنه، على الجانب الآخر، تنشأ مخاطرُ كبيرةٌ من جراء استخدام تقنية الميتافيرس، ومنها مخاطر التهديدات السيبرانية، والتجسس، والانتهاكات المتعلقة بالبيانات، واحتمالية تنفيذ أنشطة إجرامية في المجالات الافتراضية.

وفيما يتعلق بأهمية الحذر من كيفية استغلال الجهات الإجرامية لنقاط الضعف الموجودة في تقنية الميتافيرس، يمكن القول إن المخاطر التي يتعرض لها الأمن الوطني بسبب الطبيعة الناشئة لهذه المنصات- لا تقل أهمية عن أهمية المزايا الناشئة عن التطبيقات المباشرة لهذه التقنية في مجالات الدفاع والمجالات الأمنية؛ حيث يمكن أن تصبح البيئات الافتراضية داخل تقنية الميتافيرس أرضًا خصبة لمجرمي الإنترنت والإرهابيين، ومن الجهات الفاعلة التي ترعاها الدولة. كما يمكن للمجرمين المذكورين استغلال نقطة عدم تحديد هويتهم وأنهم في أمان؛ لأنهم في مساحات افتراضية، فيعملون على تنفيذ أنشطة غير مشروعة كأنشطة غسل الأموال، أو سرقة الملكية الفكرية للآخرين، أو التنسيق لتنفيذ هجمات سيبرانية. وعلاوة على ذلك، يمكن أن تصبح تقنية الميتافيرس منصة يمكن من خلالها نشر المعلومات والدعاية المضللة والأيديولوجيات المتطرفة، على نحوٍ يُشَكِّلُ تهديدًا كبيرًا للاستقرار المجتمعي وللأمن الوطني.

وعلى الرغم من كل التهديدات المحتملة للأمن الوطني من جراء استخدام تقنية الميتافيرس، فإن تقنية الميتافيرس نفسها تُشَكِّلُ فرصةً كبيرةً لتعزيز الأمن الوطني؛ حيث يمكن من خلالها إنشاء عمليات تدريب افتراضية محاكية للتدريبات الفعلية بغرض تدريب الأفراد العسكريين، وضباط إنفاذ القانون، والعاملين

بالمخابرات، وهو ما يوفر التدريب بشكل واقعي دون التعرض لمخاطر جسدية. كما يمكن لهيئات المخابرات أن تستخدم تقنية الميتافيرس في أنشطة المراقبة، ودعم جهود مكافحة الإرهاب، والتعاون الدولي، بما يتيح تبادل وتحليل المعلومات في الوقت المناسب بين الدول. كما تسمح هذه التقنية للجيوش بتقليل تكاليف التدريب العسكري؛ نظرًا لأن تكلفة صيانة منصة الواقع الافتراضي والمعزز ومعداتها اللازمة لها أقل من تكاليف تمويل التدريب العسكري الحقيقي. ومما يبين هذه النقطة تنفيذ شركة إمبروبابل التي تعمل في مجال التقنية، التي يقع مقرها بالمملكة المتحدة، لساحة معركة افتراضية تسمح لعدد 10,000 جندي بإجراء تدريبات افتراضية في وقت واحد استعدادًا لنشرهم في العالم الحقيقي (Linganna, 2022).

واستخدمت البحرية الأمريكية أدوات تقنية الميتافيرس في تدريب طياريها على العمليات البحرية، وتسمح تقنية الميتافيرس بتوصيل الأفراد المنتشرين بعضهم ببعض بشكل افتراضي في أي مكان في العالم، وهي ميزة استغلتها القوات الجوية الأمريكية عندما استخدمت بيئةً افتراضيةً لتوصيل أفراد عسكريين ذوي مستوى رفيع بعضهم ببعض من أكثر من 250 دولة مشاركة (Linganna, 2022). كما تكتسب التطورات العسكرية المتبادلة باستخدام تقنية الميتافيرس قوةً إضافيةً؛ فلقد استثمرت الصين بشكل مكثف في التحضير للمعارك العسكرية داخل العالم الافتراضي، وأطلقت على ذلك اسم "عالم المعركة" (PRNewswire, 2021). وبعيدًا عن التطبيقات العسكرية، توجد مجموعة متنوعة من الفرص، التي يمكن جنيُها من وراء استخدام تقنية الميتافيرس؛ حيث يمكنها تسريع التحول الرقمي في العالم العربي من خلال استغلال تلك الفرص، ولكن مع وجود مجموعة من الآثار الأمنية ذات الصلة. ويمكن أن تشكل منصات الميتافيرس نظامًا افتراضيًّا يتواصل فيه المستخدمون مع الآخرين ويشتركون في تجارب افتراضية كما هو الحال في منصة هورايزن وورلدز الخاصة بشركة ميتا (الشركة الأم لشركة فيسبوك)، أو كما هو الحال في منصة ديسينترالاند، وتقديم تكرارات جديدة للمساحات الافتراضية لشبكات التواصل الاجتماعي، وسبل للتجارة الإلكترونية، وإمكانية امتلاك أصول افتراضية، وغير ذلك من المنافع.

تنظيم تقنية الميتافيرس

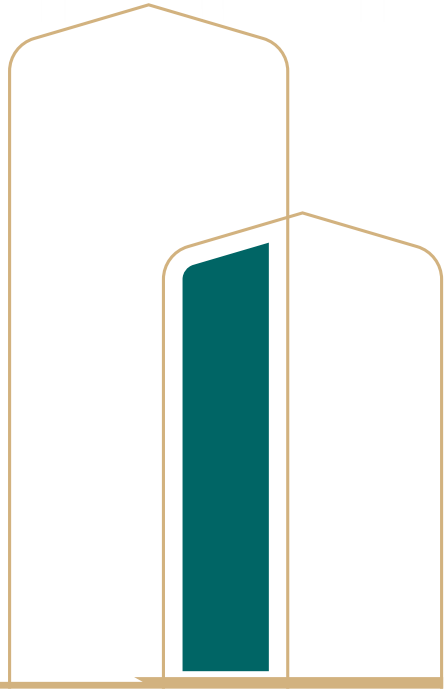
وعلى الرغم من الإثارة الكبيرة لتقنية الميتافيرس على الصعيد الإقليمي، فإن تنظيم هذه التقنية ينطوي على تحديات لا يمكن إغفالها، ويشكل الاعتماد على هذه التقنية على الصعيد الإقليمي أحد هذه التحديات لما لها من مخاطر أمنية خاصة ومعقدة، ويرجع ذلك لطبيعتها غير المحددة بحدود معينة ولأسسها التقنية المعقدة. وسوف نحدد تلك المخاطر بشكل رسمي ضمن تسع فئات واسعة، تشمل بحد ذاتها الانتهاكات المحددة

لتقنية الميتافيرس التي يمكن أن ينفذها مستخدمو تلك التقنية داخل العالم العربي أو خارجه، وتشكل تلك الانتهاكات المحتملة تهديدًا للأمن الوطني، وللاستقرار والتماسك الاجتماعي، ولحريات الأفراد.

وعلى خبراء الأمن ومسؤوليه أخذ هذه الأمور بعين الاعتبار، وأن يدركوا أنها تتطلب الموازنة بدقة بين ضرورات الأمن الوطني وحماية حقوق الأفراد وحرياتهم. وينبغي أن يتمتع المستخدمون بالخصوصية وحرية التعبير والحماية من المراقبة بدون سبب، كما تعد الموازنة السليمة بين التدابير الأمنية وحماية المستهلك أمرًا في منتهى الأهمية للحفاظ على ثقة الناس بها وقبولهم لها. وتتوافر في تقنية الميتافيرس إمكانات هائلة يمكن من خلالها إعادة تشكيل مجالات الترفيه والتعليم والتجارة، وعلى الرغم من ذلك، لا ينبغي أن تطغى تداعيات هذه التقنية على ثمار اعتمادها؛ لذا ينبغي معالجة التهديدات التي يشكلها مجرمو الإنترنت والإرهابيون والجهات الفاعلة التي ترعاها الدولة مع الاستفادة في الوقت نفسه من فرص استخدام هذه التقنية في المجالات الاستخباراتية والتعاون والتدريب. ويعد التنظيم الفعال أمرًا أساسيًّا لضمان المحافظة على الأمن الوطني مع عدم الإخلال بالحقوق والحريات الخاصة بالأفراد مع استمرار تطور التقنية.

هيكل بناء التقرير

يوفر هذا التقرير فهمًا شاملًا لتقنية الميتافيرس ومخاطرها وإمكاناتها ومسار السياسة لأي أطر تنظيمية متعلقة بتقنية الميتافيرس، ويبين هذا التقرير الميزات الأساسية لتقنية الميتافيرس، مع تقديم تفاصيل التقنيات الأساسية، التي تعمل على تشغيل تقنيات الجيل الخامس والجيل السادس، وتقنية سلسلة الكتل، وإنترنت الأشياء، وحوسبة الحافة - والتقنيات الإضافية التي تتيح الوصول إلى تقنية الميتافيرس - الافتراضية والمختلطة والمبتكرة ومعدات الواقع المعزز، والذكاء الاصطناعي، والجيل الثالث من الإنترنت، والأصول الرقمية. كما يوضح التقرير بعد ذلك الآثار الأمنية المترتبة على تقنية الميتافيرس وتطبيقاتها، ويناقش نقاط الضعف في البنية التحتية الأساسية لها، والهوية الرقمية، وخصوصية المستخدمين، والقرصنة، والإرهاب الرقمي، والجرائم السيبرانية، والمعلومات الزائفة والمعلومات المضللة، والتعبئة الاجتماعية والسياسية، والمخاطر التي تهدد السيادة والثقافة. وبعد ذلك ترد الفرص الناشئة عن معالجة هذه المخاطر الأمنية في المنطقة العربية، بما يشمل الفرص التي يمكن أن تتحقق على مستوى المستخدم والمؤسسات والدولة وعلى الصعيد الإقليمي، وفي النهاية، يتم إدراج التوصيات العملية التي يمكن تنفيذها للمحافظة على أمن المسؤولين وصانعي السياسات لوضع أساس إقليمي شامل لتقنية الميتافيرس، الذي سيتم اعتماده على مستوى العالم العربي.



خصائص الميتافيرس

يتعاملُ الخبراءُ ومسؤولو الأمن في الدول العربية مع الميتافيرس بشكل مثمر من خلال تقسيم خصائصه إلى فئتين: التقنيات الأساسية التي تُمَكِّن من وجودها، والتقنيات الملحقة التي تمكن المستخدمين من المشاركة فيها، وتتكون الفئتان من قسمين رئيسين، يكون لكل منهما العلاجات التفصيلية الخاصة به.

وسنتحدث في البداية عن البنية التحتية الأساسية، وهي مفهوم متعمق عن مختلف التقنيات التي تدعم تشغيل الميتافيرس، وذلك في النقاش التالي: يتسلط الضوء على البنية التحتية لشبكات الجيل الخامس والجيل السادس باعتبارها التقنيات التي تدعم تشغيل اتصال الإنترنت بتقنية الميتافيرس، ويتضمن إنترنت الأشياء مجموعةً متنوعةً من الأجهزة المتصلة بالإنترنت بوصفها شبكة حوسبة بيانات، كما يُعتبر المثال الأقرب للوجود المادي للميتافيرس، وتتم مناقشة حوسبة الحافة باعتبارها التقنية المسؤولة عن معالجة البيانات، بما يسمح بالنقل السريع للبيانات بين الأجهزة التي تدخل إلى عالم الميتافيرس، وفي النهاية، فإن تقنية سلسلة الكتل هي التقنية الأكثر شيوعًا المستخدمة في تخزين البيانات في الميتافيرس، وتمكين الهوية الرقمية لمستخدميها، وتسهيل آليات التبادل والتفاعل شبه الخالية من العيوب بين النظراء.

وتُجرى بعد ذلك مناقشة حول التقنيات التي يستعملها المستخدمون داخل الميتافيرس وما يتعلق بها؛ حيث تتيح معدات الواقع المختلط للمستخدمين تعزيز واقعهم وتصورهم للتجارب الافتراضية، في حين تمثل الأصول الرقمية الأصول المشفرة المؤمنة التي تسجل الملكية بشكل آمن وعام في العالم الافتراضي. وبخصوص تقنية الويب الثالث (Web3)، فإنها تُمثل نظام المعلومات الرئيس المستخدم للوصول إلى العوالم الافتراضية، وهو الأكثر توافقًا مع الميتافيرس بسبب تكامله مع تقنية سلسلة الكتل، علاوة على ذلك، تتسع أدوات الذكاء الاصطناعي، مثل: النماذج اللغوية الكبيرة التي تدعمها المحولات التوليدية المدربة مسبقًا؛ لتشمل قدرات المطورين ومقدمي الخدمات الافتراضية والمستخدمين على إنشاء وتصميم وتنفيذ الميتافيرس.

1. تشغيل الميتافيرس: البنية التحتية الأساسية (Powering the Metaverse: Underlying Infrastructure)

تشتهر تقنية الميتافيرس بشكل أساسي بسبب استخدامها الجذاب لمختلف فئات المستخدمين ومنشئي المحتوى ومقدمي الخدمات المؤسسية، وعلى الرغم من ذلك، فإن الجوانب الأكثر إثارة للإعجاب في العالم الافتراضي تتمثل في البنية التحتية الأساسية، وتُعتبر تقنيات الأجهزة المتطورة في غاية الأهمية في تمكين خاصية الميتافيرس كنظام قوي وديناميكي، حيث تمثل العمود الفقري للميتافيرس؛ إذ تدمج العناصر الافتراضية والواقعية لخلق تجارب موسعة بطريقة سلسة.

البنية التحتية لشبكات الجيل الخامس والسادس (5G/ & 6G Network Infrastructure)

تُعتبر التطورات الأخيرة في شبكة البنية التحتية أحد الدوافع الرئيسة وراء ظهور الميتافيرس، فقد أسهمت شبكة الجيل الخامس وتعميمها في تحقيق وصول عالمي وتغطية متسقة، بما في ذلك التجوال والسرعة. وبفضل جميع السمات المميزة لهذه الخصائص، فإن شبكات الجيل الخامس هي تقنية «حجر الأساس» التي تدعم شبكات اليوم، وتمتد أهميتها؛ لتشمل الميتافيرس، حيث يعتمد نظامها على التدفق السريع للبيانات، الذي أصبح ممكنًا بشكل متزايد من خلال تقنيات الشبكة المحسنة والبنية التحتية للشبكة.

وعلاوة على ذلك، تُسهل شبكاتُ الجيل الخامس استخدامَ الحوسبةِ المتطورة لقدرتها على تقليل وقت استجابة الشبكة، وهو ما يخلق لدى مستخدمي الميتافيرس على الفور حالة من الإحساس بالعالم الحقيقي، حيث إن هذا النوع من الشبكات يُمثل عاملًا ضروريًّا تظهر أهميته في الألعاب الافتراضية والقدرة على التفاعل مع المعارض الفنية الرقمية والقيام بعمليات التسوق الافتراضية وأكثر من ذلك. وبالإضافة إلى التفاعل الذي تُحدثه شبكات الجيل الخامس، فإن تلك التقنية تُقَلِّلُ أيضًا من مشكلات (مثل: دوار الحركة)، التي قد تنشأ للمستخدمين الذين يعانون من مشكلة تأخر الإدخال بين الشاشة والجهاز. ويتوقع المطلعون على الأعمال أن يكون لدى منطقة الشرق الأوسط ما يقرب من 80 مليون مستخدم للميتافيرس بحلول عام 2025، وهو ما يُعَزِّز شبكات الجيل الخامس والانتقال إلى تقنيات أكثر تطورًا في جميع أنحاء المنطقة. ومع ذلك، فإن واجهات برمجة التطبيقات لها أيضًا مشاكلها الأمنية، فعلى مستوى التطبيق، ستمكّن شبكات الجيل الخامس «التطبيقات من تكييف معدل البت ودقته بسرعة مع البيئة المتغيرة». وبالاطلاع على الممارسين التقدميين الذين يقودون مجال تقنية الشبكة، فمن المتوقع أن أولئك الأشخاص العاملين على تقنية الميتافيرس يفكرون أيضًا في الإصدار التالي لتقنية الشبكة - شبكات الجيل السادس - وآثارها على طرح نظام ميتافيرس وتوسعته.

لقد وضع العالم العربي بالفعل أساسات متينة لتقنية الجيل الخامس، وقد برزت دول في منطقة الخليج، مثل: المملكة العربية السعودية والإمارات العربية المتحدة وقطر، كمتبنين مبكرين لتقنية الجيل الخامس، مع إعطاء الأولوية لتنفيذها قبل الأحداث العالمية المرموقة، مثل: قمة مجموعة العشرين وإكسبو 2020 وكأس العالم في عام 2022، وبالإضافة إلى ذلك، تتابع دول الخليج بنشاط مبادرة «شبكة الوصول إلى الراديو المفتوح» Open RAN التي تُعزِّز مكانتها باعتبارها رائدة في تسيير حدود تقنية شبكات الجيل الخامس (Soliman, 2022). وتعتمد مبادرة «شبكة الوصول إلى الراديو المفتوح» على واجهات ومعايير مفتوحة، وهو ما يسمح لمشغلي الشبكات بتجنب قفل البائع والتحرر من الاعتماد على بائع واحد، ويمنحهم المرونة لاختيار المكونات الأكثر ملاءمة التي تلبي متطلباتهم المحددة من خلال تبني تقنية شبكات الجيل الخامس، وشهدت العديد من الدول العربية

تحولًا رقميًّا كبيرًا، بالإضافة إلى الاستفادة من إنترنت الأشياء الصادر، وهو شبكة مترابطة من الأجهزة الذكية الشخصية والصناعية التي تعتمد بشكل كبير على تدفق البيانات الأسرع، الذي أصبح ممكنًا بواسطة شبكات الجيل الخامس. ونتيجة لذلك، استفادت الاقتصادات في جميع أنحاء العالم العربي من قوة الجيل الخامس لإطلاق الإمكانات الكاملة لإنترنت الأشياء، وهو ما يتيح تعزيز الاتصال والكفاءة في مختلف القطاعات.

واعتمدت دول الخليج، بما في ذلك المملكة العربية السعودية والبحرين والإمارات العربية المتحدة وقطر، التحول الرقمي بسرعة، مع التركيز بشكل خاص على الخدمات الحكومية والوصول إلى الإنترنت واستخدام الهواتف الذكية (Grace, 2023). ويعد نشر البنية التحتية لشبكات الجيل الخامس، على وجه الخصوص، رمزًا للجهود التي تبذلها هذه الدول، والتي تضعها في وضع يسمح لها بالانتقال السلس إلى عالم الميتافيرس، فعلى سبيل المثال، أعطت المملكة العربية السعودية الأولوية لأن تصبح مركزًا رقميًّا من خلال التنفيذ السريع لتبنيها لتقنية الجيل الخامس وتوسيع نطاقها استعدادًا للأحداث العالمية، مثل: رئاسة المملكة العربية السعودية لمجموعة العشرين في عام 2020، وفي سيناريو آخر، أطلقت زين - إحدى شركات الاتصال - أكبر شبكة من شبكات الجيل الخامس في المنطقة بالتعاون مع هواوي، والتي تغطي 20 مدينة تضم 2000 برج، ومن جانبها تعمل دولة الإمارات العربية المتحدة بنشاط على إنشاء شبكة الجيل الخامس الخاصة بها؛ لتعزيز مكانة مدينة دبي العالمية، ولا سيما مواءمة نشر البنية التحتية للجيل الخامس مع فعاليات، مثل: معرض دبي إكسبو 2020. كما دخل المشغلون الرئيسون مثل شركة الإمارات للاتصالات المتكاملة ش.م.ع (المعروفة تجاريًّا باسم «دو») وشركة اتصالات في شراكة مع هواوي لنشر شبكات الجيل الخامس، في حين حققت الأخيرة أول مكالمة مستقلة من خلال شبكات الجيل الخامس في منطقة الشرق الأوسط وشمال إفريقيا. وأخيرًا، استضافت قطر أول بطولة من بطولات كأس العالم التي تستخدم الجيل الخامس على الإطلاق من خلال التعاون مع هواوي وإريكسون ونوكيا لنشر شبكات الجيل الخامس في الدوحة ومواقع أخرى، وضمت 1200 موقع قوي التأثير لشبكات الجيل الخامس في الدوحة وحدها. وتركز جهود تلك الدول على تقنية الجيل الخامس، ولكنها ترمز إلى إجراءات أوسع وحاسمة؛ لترسيخ نفسها باعتبارها مراكز رقمية لديها القدرة على تبني النطاق الهائل للميتافيرس وحمايته.

وعلى الرغم من أن شبكات الجيل السادس لا تزال قيد التطوير في أولى مراحلها، فإنه يتضح أنها ستكون أسرع بنحو 100 مرة من شبكات الجيل الخامس، ويتم العمل على حوسبة الحافة واعتبارها ميزة قياسية لشبكات الجيل السادس، بدلاً من كونها ميزة إضافية، كما هو الحال في شبكات الجيل الخامس، وسوف تُدرس تقنية الجيل السادس مع التدريب عليها وعلى الذكاء الاصطناعي والتعلم الآلي. ومع ذلك، لا يمكن أن يكون لزيادة السرعات وسعة البيانات تأثير في الموثوقية والسلامة.

وبالنظر إلى سرعة تقنية شبكات الجيل السادس وتطورها، تجدر الإشارة إلى أن التوسع الحالي لنظام الميتافيرس قد يُسرع من تطوير شبكات الجيل السادس ونشرها عاجلًا وليس آجلًا، بحيث إنه من المتوقع استخدام شبكات الجيل السادس بحلول عام 2030، فإن عناصر الاختبارات والأمان والتجارب لا تزال بالفعل قيد العمل. ويتوافق هذا التوقيت مع ظهور خبير الميتافيرس، توني باريزي، في الواقع الممتد، حيث يتوقع توني تحقيقًا كاملًا للميتافيرس، الذي يعرف بأنه عالم افتراضي متصل بالكامل بالأجهزة التي تتيح تجارب ذات فعالية للميتافيرس، وتمزج بسلاسة بين العالمين الرقمي والمادي، بحلول عام 2029.

ونظرًا لأن تقنية شبكات الجيل السادس تُعتبر أساسية لتشغيل الميتافيرس، فإن تطوير شبكات الجيل السادس ونشرها داخل الدول العربية الفردية يزيد من الحاجة إلى نهج مشترك لتنظيم الميتافيرس وتأمينها في المنطقة الأوسع. ولا يمكن إتقان السياسات واللوائح قبل النشر الفعلي للتكنولوجيا، ولكن الفكرة هي أن يقوم هؤلاء الممثلون بتصور الميتافيرس كنظام افتراضي ناضج مع وضع الأساس بشكل استباقي في الوقت الحالي، وكما أن تلك الجهود المبذولة لا تحدث هباءً، فإنه من المتوقع الاعتماد الكامل على تقنية وشبكات الجيل السادس في معظم أنحاء العالم العربي بحلول عام 2030. ومن المتوقع أن تتكيف كل من المملكة العربية السعودية والإمارات العربية المتحدة، باعتبارهما من رواد تقنية الجيل الخامس، وتقدما المساعدات للدول الأخرى في المنطقة فيما يخص تنفيذ الجيل السادس، ولسنا بحاجة لتأخير اعتماد الميتافيرس أكثر من ذلك في ظل انتشار البنية التحتية لشبكات الجيل الخامس على نطاقٍ واسعٍ. ففي ظل تطور تقنية الجيل السادس وطرحها، يمكن لكل دولة اعتماد هذه التقنية الأساسية وسياسات الاستخدام الأفضل الخاصة بها للتأثير في دورها في الأمن المشترك للميتافيرس، وتأثيرها المترتب على تنفيذ إنترنت الأشياء، وحوسبة الحافة، وتقنية سلسلة الكتل.

إنترنت الأشياء (The Internet of Things)

إن إنترنت الأشياء هو شبكة من أجهزة الحوسبة المُضَمَّنَة في الأشياء اليومية المتصلة عبر الإنترنت، والتي تمكنها من إرسال البيانات واستقبالها (Baig, 2016)، ويُعَزِّزُ إنترنت الأشياء من تحليلات البيانات من خلال البنية التحتية فائقة الاتصال للميتافيرس، والأجهزة التي يمكنها قراءة المدخلات من البشر والاتصال بالشبكات الأولية، ويُعتبر إنترنت الأشياء في الأساس مرجعًا للأجهزة المتصلة بالشبكة، مثل: أجهزة الحاسب الآلي والأجهزة اللوحية والهواتف الذكية وغيرها من الأجهزة المتصلة بالإنترنت.

وعلى غرار تقنيات شبكات الجيل الخامس والجيل السادس، يحظى العالم العربي بأساس قوي موجود لأجهزة إنترنت الأشياء أيضًا، وتكشف أبحاث السوق أن أجهزة الاستشعار هي أبرز أجهزة إنترنت الأشياء في جميع أنحاء شبه الجزيرة العربية، مع وجود الروبوتات والكاميرات اللازمة لأنظمة التحكم الإشرافي وتحصيل البيانات (سكادا) بعد أجهزة الاستشعار. ومن المتوقع أن يستمر إنترنت الأشياء في النمو في الشرق الأوسط فقط مع مواصلة تنفيذ الذكاء الاصطناعي والتعلم الآلي، وتأتي المملكة العربية السعودية باعتبارها دولة رائدة مع أكبر عدد من أجهزة إنترنت الأشياء المسجلة في القطاع الصناعي، كما تستخدم إنترنت الأشياء في أطر عملها السحابية ؛ لأنها تسعى جاهدة لتحسين الأمن السحابي. وتعد دولة الإمارات العربية المتحدة رائدة إقليمية أخرى في اعتماد إنترنت الأشياء، حيث ترتبط ٪40 من أجهزتها الخاصة بإنترنت الأشياء مباشرة بالمنتجات الاستهلاكية.

إن المشروع الكبير المتعلق بإنترنت الأشياء القائم في دولة الإمارات العربية المتحدة هو مشروع تابع لهيئة الطرق والمواصلات جرت الموافقة عليه حديثًا (اعتبارًا من عام 2021) وذلك بالاشتراك مع شركة اتصالات، حيث يهدف إلى تحسين التنقل والسلامة والاتصالات في جميع أنحاء دولة الإمارات العربية المتحدة. وفي عام 2024، ستستضيف هيئة الطرق والمواصلات أيضًا المؤتمر العالمي لأنظمة النقل الذكية لمواصلة البحث عن أفضل طريقة لتطبيق إنترنت الأشياء في الحياة اليومية (Ertico and ITS World Congress, 2023).

وتُعتبر المدن الذكية في منطقة الشرق الأوسط وشمال إفريقيا من المناطق الأخرى التي يتوقع نمو معدل استخدام إنترنت الأشياء بشكل كبير فيها، وتعمل المملكة العربية السعودية على تنفيذ مشروع «ذا لاين»، وهو مشروع مدينة ذكية يتم تطويره في نيوم، وسيتم ربط المدينة الفعلية باستخدام إنترنت الأشياء والذكاء الاصطناعي على أمل الحصول على رؤى مهمة حول أنماط المعيشة وخدمات المدينة والاتجاهات التي يقدمها إنترنت الأشياء. وتهدف مصر إلى إطلاق مبادرة لتطوير مركز عمليات المدينة، الذي يهدف إلى استخدام برنامج إنترنت الأشياء للمساعدة في تحسين خدمات إدارة المدينة.

وتتطلب المعدات اللمسية المحيطة بالميتافيرس (مثل: الأجهزة القابلة للارتداء، وسماعات الرأس للواقع الافتراضي، والشبكات العصبية، والقفازات، والبدلات، وغيرها من أغطية الرأس، أو أي تقنية توفر آليةً للتفاعل مع الميتافيرس أو الانغماس فيه)، مراعاة أمان تنسيق المعدات (الأجهزة) والمستخدم، بالإضافة إلى البيانات التي تجمعها وتنقلها وتُخَزِّنها. وتهدف جميع المعدات اللمسية إلى العمل مع أجهزة الاستشعار، وكلما زاد استخدام أجهزة الاستشعار في التقنيات اللمسية الناشئة، زاد ظهور نقاط نقل البيانات وتخزينها وفقًا لذلك. ومع التطور الحادث في تقنية الميتافيرس، سيتطور أيضًا وجود إنترنت الأشياء، حيث إن أجهزة إنترنت الأشياء ستعمل باعتبارها بوابات لعالم آخر، ألا وهو العالم الافتراضي.

حوسبة الحافة (Edge Computing)

حوسبة الحافة هي تقنية أساسية لتمكين المعالجة التي تتسم بالكفاءة والفعالية للبيانات في العصر الرقمي، وقد أصبحت حوسبة الحافة أداة لا غنى عنها مع انتشار شبكات الجيل الخامس وإنترنت الأشياء لمعالجة الكميات الهائلة من البيانات الناتجة عن هذه التقنيات (Krishnasamy et al., 2020).

واعتمدت حكومات الشرق الأوسط أيضًا ونفذت حوسبة الحافة مع ظهور البنية التحتية السحابية في المنطقة كجزء من تركيزها واستعدادها لتقنيات الجيل التالي، ويوضح النهج الشامل للحكومات العربية في تنفيذ الحوسبة السحابية وحوسبة الحافة وأجهزة إنترنت الأشياء وجهة نظر مستقبلية للتقنية من شأنها أن تُغَيِّرَ المنطقةَ بأكملها وتؤثر فيها بشكل إيجابي، وتقضي حوسبة الحافة على الحاجة إلى نقل البيانات إلى موقع مركزي للمعالجة من خلال معالجة هذه البيانات على الجهاز الذي تنشأ فيه أو بالقرب منه، وهذا يؤدي إلى أوقات استجابة أسرع، وانخفاض زمن الوصول، وتحسين جودة البيانات، وهو أمر مهم بشكل خاص في التطبيقات الحساسة للوقت.

ولا تقتصر مزايا حوسبة الحافة على تطبيقات إنترنت الأشياء وشبكات الجيل الخامس، ومع استمرار تطور التقنية، فقد أصبح من الواضح بشكل متزايد أن حوسبة الحافة تُمثل مكونًا حيويًّا للتقنيات الناشئة، مثل: الميتافيرس. ويتطلب الميتافيرس، وهو عالم افتراضي يتميز بتجربته الغامرة والمتسمة بالتفاعلية بشكل تام، كميةً هائلةً من البيانات؛ ليعمل بشكل صحيح، ومع قيام ملايين المستخدمين بتوليد البيانات في وقت واحد، فإن نقل كل هذه البيانات إلى موقع مركزي للمعالجة ليس عمليًّا، وقد توفر حوسبة الحافة حلًّا من خلال السماح بمعالجة البيانات بالقرب من نقطة المنشأ، ومع استمرار تطور الميتافيرس، ستؤدي حوسبة الحافة دورًا أكثر حيوية في ضمان قدرة هذه التقنيات على العمل بفعالية وكفاءة.

تقنية سلسلة الكتل (Blockchain Technology)

يعتبر دمج تقنية سلسلة الكتل في البنية التحتية لميتافيرس وتطبيقاتها ونظامها مفرقًا رئيسًا يميزها عن سابقاتها المفاهيمية، ومن الضروري فهم سلسلة الكتل وتطبيقاتها وعلاقتها بالميتافيرس لمواجهة قيود الأمن الوطني للميتافيرس، حيث تُعتبر سلسلة الكتل كدفتر رقمي أو قاعدة بيانات تخزن المعلومات على شبكة لامركزية. وقد تم الاحتفاظ بها من خلال شبكة عمل المشتركين الذين نشروا المسؤوليات الحوسبية بدون

مدير مركزي، وتسجل سلسلة الكتل المعاملات التي تم الاحتفاظ بها فيها، وتدمجها مع معاملات أخرى داخل الكتلة. وقد تم التحقق من صحة الكتل من خلال المشتركين في الشبكة المحددة الذين يطلق عليهم عمال التعدين، وجعل هذه الكتل ثابتة لا تتغير باستخدام التشفير، ويتقاضى عمال التعدين مكافأة في شكل رموز غير قابلة للاستبدال، يُطلق عليها العملات المشفرة، وذلك نظير إجراء المعاملات والتحقق منها، وهي عملية تتطلب بذل الكثير من الجهود، وتُعتبر العملات المشفرة هي الأصول الرقمية التي يرسلها المستخدمون ويتلقونها، وتمثل متوسط صرف خاص بالمعاملات المسجلة في دفتر الأستاذ الرقمي، ويحفز نظام المكافآت الذي ينتج عملات مشفرة من المشاركة في شبكة العمل والالتزام الكلي ببروتوكول سلسلة الكتل، وتمتد تلك اللامركزية إلى الميتافيرس، وهو ما ينشر الديمقراطية على أرض العالم الافتراضي، وتعد طبيعة الاسم المستعار لسلسلة الكتل وثباتها والسرعة التي تعالج بها المعاملة المذهلة من المزايا التي توضح قيمة تقنية سلسلة الكتل، وتوضح أيضًا قيمة تطبيقها على الميتافيرس (for overviews and explanations, see IBM, 2023).

ويمنح استخدام تقنية سلسلة الكتل المستخدمين الصلاحيةَ؛ كي يكونوا أمناء على بياناتهم وأصولهم الرقمية من خلال تمكين شبكة عمل المشتركين من جميع أنحاء العالم للإقرار بدفتر الأستاذ الذي تم توزيعه وإدارته، وتجعل طبيعة تقنية سلسلة الكتل اللامركزية بين النظراء من الصعب أن تتحكم جهة واحدة بالكامل في الشبكة أو دفتر الأستاذ، كما أنها تضمن إمكانية عمل الشبكة بدون نقطة عطل مفردة منذ نشر المسؤوليات الحوسبية. وتكون الشبكة مدعومة من مخرجات الحوسبة الإجمالية لكل المشاركين، وهو ما يسمح باستمرار عمل الشبكة في حالة تسوية واحد أو عدد من المشاركين.

ويظهر العالم العربي كمحور جذاب لتطوير تقنية سلسلة الكتل وتبنيها، وقد أَدْمَجَت أجزاءٌ مختلفةٌ من المنطقة سلسلةَ كتلٍ في عدد من العمليات الخاصة والعامة، حيث قامت دول الخليج، مثل: الإمارات العربية المتحدة والمملكة العربية السعودية، بتطوير لوائح سلسلة الكتل المثمرة بنجاح، التي دعت إلى موجات من المشتركين الجدد في عملياتهم الاقتصادية، بينما تعمل مصر والإمارات العربية المتحدة حاليًّا على تأسيس ممر للتحويل يسمح بتحويل الأموال باستخدام أصول رقمية قائمة على سلسلة الكتل من الوافدين من الإمارات العربية المتحدة للمجتمعات المتلقية في مصر (Palmer, 2023)، وقد أمدت مبادرات التعدين رواد الأعمال اللبنانيين بشكلٍ من توليد الإيرادات وسط مواجهات اقتصادية وطنية (Shafer, 2022)، وليست المنطقة غريبة على هذه التقنية، فقد أسهمت تلك المعرفة بالتقنية في إلهام التوافق الذي يوجد بين الشعوب العربية والتقنية التي تمثل جزءًا كبيرًا من البنية التحتية الأساسية لتقنية الميتافيرس، وقد استُخْدِمَت تقنيات سلسلة الكتل

لتقوية العوامل الأكثر حيوية بالمنطقة، وقد اشتركت شركة الشوامخ للخدمات النفطية بسلطنة عمان مع شركة فرونتك لتطوير نظام إدارة الطاقة المستدامة المبني على تقنية سلسلة الكتل (Daoud, 2022)، وتتبع شركة الطاقة البارزة وحدات إنتاج الطاقة المستدامة الخاصة بسلسلة الكتل وتديرها، وهو ما يمثل عرضًا تشجيعيًّا على الابتكار في أي قطاع يكون مصدرًا لاقتصاد المنطقة.

وعلى الرغم من أن أمن سلسلة الكتل وإمكانية التوسع التي تجعلها تقنية أساسية مثالية للميتافيرس، فإن هناك حاجة للائحة شاملة تتطلع للمستقبل وتسعى لمعالجة عدد من المحاذير الأمنية ذات الصلة بسلسلة الكتل، وتتبنى منصات ميتافيرس المشهورة في الوقت الحالي شكلًا لامركزيًّا، وتعمل من خلال شبكة موزعة بين النظراء عن طريق دمج تقنية سلسلة الكتل في نظامها، ويمكن استخدام سلسلة الكتل في نظام ميتافيرس لتحقيق الأهداف الآتية:

- إنشاء هوية آمنة ورقمية واضحة لكل مستخدم في الميتافيرس.
- حفظ ملكية الأصول الرقمية وتتبعها، ومنها الأراضي الفعلية والشخصيات الافتراضية والمواد.
- تسهيل المدفوعات والمعاملات بين المستخدمين في الميتافيرس.
- إدارة الميتافيرس وضمان أنها مقبولة وعادلة لكافة المستخدمين.

ويعمل دمج سلسلة الكتل في الميتافيرس على تزويد العالم الافتراضي بالأختام الزمنية وسجلات النشاط التي تستخدم الأختام الزمنية لسلسلة الإمداد الثابتة، وأي خاصية يَثْبُت أنها نافعة للالتزام التنظيمي وعند إجراء التحقيقات الجنائية والاحتيال. وتسهل سلسلة الكتل بشكل راسخ الوضوح وتكون أصلًا للأمن وحفظ السجلات في نظام الميتافيرس.

2. الدخول إلى الميتافيرس: المعدات الإضافية

يتوقف الدخول إلى هذا المجال الرقمي على معدات إضافية محورية في عالم الميتافيرس، وهو عالمٌ افتراضي منفصل عن المادية، وبالرغم من طبيعة المعدات المادية، فإن هذه الأجزاء من المعدات تعتبر بوابات لتقنية الميتافيرس، وعلاوة على ذلك، يُمَكِّنُ دمجُ سلسلةِ الكتل القائمة على البرمجيات والأنظمة والبرامج المُسْتَخْدِمَ من الدخول إلى تقنية الميتافيرس، حيث تقود سعة العالم الافتراضي إلى التصميم الابتكاري وتقوية المستخدمين إلى المشاركة بفاعلية ودمج أنفسهم في هذا المشهد الرقمي. ويتمثل الدور الرئيس للتقنيات المادية والحلول

القائمة على سلسلة الكتل في تمكين الدخول إلى تقنية الميتافيرس والتوسع في فرص التصميم، وتقوية وكالة المستخدم في الحقل الافتراضي.

الواقع المختلط (Mixed Reality)

تُقَدِّمُ تقنيةُ الميتافيرس حقلًا اجتماعيًّا جديدًا، بالإضافة إلى الحقول والحقائق التفاعلية المكملة لوظائفها، وبظهور تقنيات جديدة، تصبح سرعات الشبكة وقدرات نقل البيانات ضرورية بشكل متزايد، وتشمل بيئاتُ الواقعِ المختلطِ الواقعَ الافتراضي والواقعَ المُعَزَّز، ويحاكي الواقعُ الافتراضيُّ الواقعَ الخياليَّ للمستخدمين الذين يستخدمون نظامًا مبرمجًا، في حين يمد الواقعُ المعززُ المستخدمين بواقعٍ معززٍ حول مواضعهم الحالية، وقد تختلف بيئات الواقع في مستوى تركيزها من واقع افتراضي غير غامر بالكامل وشبه غامر، ويتطلبُ الواقعُ الافتراضيُّ، الذي هو سائد تقريبًا في مجتمع الألعاب، أجهزةَ استشعارٍ لجمع البيانات من أعضاء جسم الإنسان، بالإضافة إلى الأجهزة التي تكمل التجربة الغامرة، كما يتطلب الواقعُ المعززُ بعض المدخلات، مثل: الإفصاح عن المواقع، والقياس عن بُعْدٍ، وبيانات التعريف، وتُسَهِّلُ فئةٌ أخرى، وهي الواقع الممتد، من استخدام المحتوى المتاح على نطاقٍ أوسعٍ، ويُعتبر من الضروري مراعاة خصوصية البيانات وسلامة المستخدم عند جمع البيانات المطلوبة والاستفادة منها في الواقع الافتراضي والواقع المعزز والواقع المختلط والواقع الممتد، كما أن حماية كافة الأجهزة وأجهزة الاستشعار والشبكات المستخدمة لجمع البيانات تدخل تحت هذا الاعتبار، ومن الضروري ضمان سلامة البيانات واستخدامها في الغرض المُعَدِّ لها لنجاح هذه التقنيات ونموها.

وشهد العالمُ العربيُّ تطورَ الواقعِ المختلطِ والدمج قبل اهتمامه بتقنية الميتافيرس، وقد جعلت القدرةُ على تجربة الواقع المعزز والافتراضي ووضع ظروف بيئية مختلفة هذه التقنيات واحدةً من أولى الأدوات المستخدمة لقيادة التحول الرقمي بمنطقة الشرق الأوسط وشمال إفريقيا، ومن الأمثلة على ذلك إطلاق منصة الواقع المختلط الشامل لمايكروسوفت وسماعة الرأس وهولولنز2 في الإمارات العربية المتحدة (Microsoft, 2022). وتهدف هولولنز2، مع حلول أعمال مايكروسوفت، إلى تسريع التحول الرقمي والمساهمة في النمو الاقتصادي المستدام، وقد قدرت دراسة فوريستر للتأثير الاقتصادي الإجمالي بأن هولولنز2 تقدم بمفردها عائدًا قدره 177% على الاستثمار على مدار ثلاث سنوات، بالإضافة إلى التحسينات في صحة وسلامة الموظف واستمرار العمل وتجربة العميل ونتائجه (Microsoft, 2022)، وقد ظهر الانتشار المتزايد في تقنية الواقع الافتراضي في عدد من المجالات العربية المتطورة، وهي بالتحديد معدات الطيران والدفاع والعمارة وقطاع التخطيط. وقد سمحت

قدرات الرؤية ثلاثية الأبعاد للقطاع العام والخاص بمنطقة الشرق الأوسط وشمال إفريقيا بدمج نماذج رقمية وخطوط تجميع افتراضية مع رؤى تصميمية، وغير ذلك الكثير في عملياتها، ولم تظهر حالات التبني على مستوى المستهلك فحسب، وطموحات شركة إكس راي غلاس للاستيلاء على الأسهم الكبيرة في سوق المستهلك السعودي مع نظارات الواقع المعزز الخاصة بهم (Cabral, 2023a)، وإنما تظهر أيضًا على المستويات المؤسسية. ومن الجدير بالذكر أن أكاديمية المركز التفاعلي الرقمي بالمغرب، وهي مبادرة تدريبية نشأت من التعاون بين جامعة محمد السادس متعددة التخصصات التقنية، والوكالة الأمريكية للتنمية الدولية، والوكالة المغربية للتطوير الرقمي والواقع المدمج، وهي شركة رائدة عالمية في الواقع المعزز والافتراضي القائم على نقل المعرفة والمهارات الخاصة بالصناعة والتعليم وتقنيات الواقع المعزز والواقع الافتراضي المستفاد منها للترويج للحلول الابتكارية لنظم التقدم في الصناعة المغربية (Chesler, 2020).

الأصول الرقمية (Digital Assets)

الأصول الرقمية هي الرموز القائمة على سلسلة الكتل، وتمثل أي تخزينٍ للقيمة أو الأسهم أو استخدام بند مادي أو رقمي أو افتراضي، وتلقي طبيعة الاستعارة الاسمية لسلسلة الكتل الضوء على نقل القيمة بالعملات المشفرة وفئة الأصول الرقمية، مثل: آلية اختيار المعاملات للجهات أو المستخدمين الذين يرغبون في التعامل بدون وسطاء وبعامل الخصوصية، وفي تقنية الميتافيرس، يمكن استخدام العملات المشفرة كمتوسط للصرف الخاص بالمعاملات بين المستخدمين وبين البائع والمستخدم، ومن منظور أمني، يجب إدراك أن العملات الرقمية تمكن أيضًا المثلين المعاقبين من الهروب من العقوبات وإجراء معاملاتهم على الرغم من حالتهم الجنائية، ولطالما دعا منفذو النظام والخبراء النظاميون والمشاركون في الأمن السيبراني إلى إنشاء جهة عالمية لرصد الأصول الرقمية وتنظيمها، وفي تقنية الميتافيرس، فإن أحد أنواع الأصول الرقمية الأكثر صلة هو الرمز غير القابل للاستبدال، وهي إقرارات رقمية بملكية أصول رقمية فريدة وغير قابلة للصرف بطريقة مشفرة، حيث تسمح تلك الرموز بشكل أصلي لمالك واحد فقط في الوقت، ويمكن استخدامها لترميز المقتنيات والعالم الافتراضي والواقعي والعقاري وغير ذلك. وقد انبثق اقتصاد بالرموز العامة غير القابلة للاستبدال التي زعزعت أسواق القطع الفنية وغَيَّرت اتفاقيات ملكية الأصول التقليدية.

وتعرف الرموز بطبيعتها غير القابلة للاستبدال، وهذه الرموز قد عينت خصائص معينة من مجموعة المتلكات التي تفرق بين كل قيمة للرمز، وأُصدرت تلك الرموز وسكها المطورون، وأتيحت للعملاء لشراء

العملات المشفرة المستخدمة، ويكون توريدها محدودًا بهدف حماية قيمتها التي تزيد من قيمة الملكية بجانب تميز الرمز، كما أن العملاء قادرون على شراء الرموز غير القابلة للاستبدال في الأسواق الفرعية. وتعمل سلسلة الكتل على تأمين بيانات الملكية، وتدعم أدلة الإثبات، وتسمح بنقل الملكية بين طرفين، وتسجل التغييرات في الملكية في دفتر الأستاذ الرقمي، وفي تقنية الميتافيرس، تستخدم الرموز غير القابلة للاستبدال لتمثيل الأصول الافتراضية الفريدة بشكل تشفيري في ألعاب الفيديو في العالم الافتراضي كفن رقمي أو افتراضي، أو كإقرارات بملكية الأرض الافتراضية، وتستخدم الرموز غير القابلة للاستبدال في شعار المستخدم المعروفة كشكل من الهوية الرقمية، وتمثل دخول العضو إلى ميزات العالم الافتراضي والواقعي.

وقد شهدت منطقة الشرق الأوسط وشمال إفريقيا ارتفاعًا كبيرًا في معدل اعتماد الأصول الرقمية، حتى وصلت إلى مستويات غير مسبوقة على الصعيد الدولي، وقد سَنَّت بعضُ الدولِ العربيةِ أطرَ عملٍ تنظيمية وشاملة لوضع أنفسها كمحور لأصل رقمي عالمي، مثل: هيئة الخدمات المالية، وهيئة مراقبة الخدمات المالية في المناطق الحرة المالية بدبي ومركز دبي المالي العالمي وأبو ظبي وسوق أبو ظبي العالمي على التوالي (Sheffield et al., 2022). وقد سمح دمج البيئات الرقابية للمنطقة الحرة المالية مع لوائح الأصول الرقمية المسموح بها لجهات الاختصاص العربية بجذب المشغلين الدوليين الباحثين عن لوائح قائمة على الاعتماد في المنطقة، ويظهر ذلك أيضًا في البحرين بعد إصدار اللوائح النهائية في فبراير 2023 استجابةً للطلب المتزايد على الأصول الرقمية (Rain, n.d). وقد سجلت رين؛ وهي شركة الأصول الرقمية الأولى في البحرين، أكثر من 180,000 مستخدم، واستضافت ما يزيد على 1.9 مليار دولار أمريكي في المعاملات (Daoud, 2022)، وقد سخرت الشعوب العربية الأخرى العملات الافتراضية كأداة لمواجهة التحديات الاجتماعية والاقتصادية (مثل: الاحتفاظ بالمدخرات)، وتتسق الرغبة في اعتماد تلك التقنيات ودمجها في جميع جوانب الحياة على صعيد العالم العربي بأكمله، وتُعتبر تلك الرغبة الدافعَ الرئيسَ للقيادة العربية بين المشتركين العالميين في نظام الأصول الرقمية التي ليس لها حدود.

وتظهر رؤية قيادة العالم العربي في هذا المجال في تأسيس أسواق الأصول الرقمية المحددة بالمنطقة، حيث أُنشئت السوق الأولى UPYO عام 2022 (Zawya, 2022). وبعد تأسيس UPYO بفترة بسيطة، ظهرت في المملكة العربية السعودية سوق «نقطة» وهي سوق مختصة بالرموز غير القابلة للاستبدال (Non-Fun-gible Token) (NFT، 2023) كما تشاركت مؤسسة آرتس داو، التي تمثل المجتمع الأكبر في مجال الرموز غير القابلة للاستبدال في الشرق الأوسط، مع شركة ليدجر الأمنية أكبر المنتجين في مجال التخزين الرقمي للعملات المشفرة، لتوفير حلول التأمين لأعضائها (Kumar, 2023). ويوضح هذا التعاون اعتقادَ عددٍ من أكبر مقدمي خدمة الأصول الرقمية على مستوى العالم بأن منطقة الشرق الأوسط وشمال إفريقيا تُعتبر

واحدةً من أبرز أسواق الأصول الرقمية التي ظهرت على الساحة، وعلى الرغم من تلك البيئة الواعدة، فإنه يجب إدراك حقيقة إمكانية استخدام الأصول الرقمية في تمويل العمليات الخبيثة؛ إذ يمكن للأرباح الناتجة عن المبيعات أن تدعم تجارة المخدرات ومبيعات البرامج الضارة والأنشطة الإرهابية في تقنية الميتافيرس والعالم المادي أيضًا. ويمكن للمجرمين أو الإرهابيين نقل الأموال غير القانونية مباشرة، وتخطي الأنظمة المالية التقليدية من خلال شراء الأموال أو نقلها أو تداولها أو تحويلها إلى عملات مشفرة أو رموز غير قابلة للاستبدال، معتمدين في ذلك على أدوات الخصوصية المعتمدة على سلسلة الكتل.

وتظهر العديد من المخاطر الأخرى أيضًا في سياق تهديدات الأمن السيبراني عن طريق عمليات الاحتيال والقرصنة، وتهدد تلك المخاطر مطوري الأصول الرقمية وحامليها وأسواقها، وكما هو الحال مع التقنيات المعتمدة على سلسلة الكتل، فإن الطبيعة غير المحددة والتطبيقات اللامركزية للأصول الرقمية تخلق مشكلات تنظيمية وقضائية، ويمكن الاستفادة من الأصول الرقمية للتهرب من الضرائب والتشريعات المالية أو نقل القيمة من إطار مطبقي القانون والهيئات الحكومية.

الويب 3 (Web 3)

ستعتمد قابلية التوسع في الميتافيرس، بالإضافة إلى تنسيقها المتطور بشكل كبير، على تصميم الموقع الذي سيدخله المستخدمون للوصول إلى العالم الافتراضي، ويمكن القول بأن الميتافيرس تتماشى أكثر مع النموذج اللامركزي لتصميم شبكة الويب (الويب 3): تكرار ديمقراطي ومركزي للشبكة العنكبوتية العالمية التي تدمج المزايا الأساسية لتقنية سلسلة الكتل، وتعد إشارات (الويب 3) تطورًا للإنترنت تجاه المستأجرين الشائعين للهوية الرقمية وخصوصية البيانات والملكية، ويُسهم الإنترنت اللامركزي، على النحو الوارد في شبكة (الويب 3)، في تمكين المستخدمين وتحول ملكية البيانات بعيدًا عن الخوادم المركزية التي يتم الحفاظ عليها من قبل شركات عمالقة التكنولوجيا تجاه المستخدمين أنفسهم، ويتم الاستبعاد الأساسي لشبكة (الويب 3) لهذه الممارسة عن طريق استخدام تقنية سلسلة الكتل لتخزين البيانات، في حين نعرض نفس المزايا التفاعلية لعالم افتراضي تفاعلي يعرف التوافق الواقع بين شبكة (الويب 3) والميتافيرس.

ولتوضيح الفكرة ببساطة، فإنه يُنْظَرُ إلى البيئة اللامركزية والعملة المشفرة على أنهما «البنزين»، مع اعتبار المستخدم أنه «المركبة»، ويُنْظَرُ إلى شبكة (الويب 3) على أنها «الطرق»، وعلى أن التطبيقات اللامركزية أو التجارب الافتراضية هي «الوجهة»، وتُسْتَخْدَمُ الميتافيرس في توضيح تلك البيئة بطريقة تفاعلية افتراضية.

إن بنية الويب الناشئة لديها مزاياها وعيوبها، حيث تتيح مجموعة متنوعة من الاحتمالات تجاه المستخدم، في حين تمثل أساسًا جوهريًّا لخلق مجموعة جديدة من المخاطر السيبرانية، وقد قوبلت تلك البنية التحتية بمعارضة جماعية من كبرى شركات التكنولوجيا؛ نظرًا لأنها تتولى أدوارهم وتحل محلهم كأمناءٍ على البيانات، وعلى الرغم من زيادة الأداء الوظيفي الذي تقدمه شبكة (الويب 3) لمستخدميها، فإن هناك العديد من المحاذير التي تجعل من اعتمادها على نطاق واسع مصدر قلق للمنظمين، وتُوَسِّعُ شبكةُ (الويب 3) مبدأَ الهويةِ الرقميةِ عن طريق اعتماد طبيعة الأسماء المستعارة لسلسلة الكتل، وعلى الرغم من وجود قيمة في تلك الميزة، فإن الخصوصية ومحاذير التهديدات تنشأ من خلالها، فبدون الرقابة من قِبَلِ السلطة المركزية، يكون الامتثال التنظيمي صعبًا أيضًا. وتنشأ مخاطر أمنية جديدة خاصة فيما يتعلق بمعلومات تحديد الشخصية المخزنة في دفتر (الويب 3) من زيادة الأدوار التي تؤديها مزايا تقنية سلسلة الكتل، حيث تكون عرضة للاحتيال والقرصنة والبرامج الضارة.

ومن خلال الوصول إلى ميتافيرس الويب 3، تطورت الطرق التي يحدد بها المستخدمون أنفسهم عبر الإنترنت من قابلية التشغيل المتبادل، وطبيعة الأسماء المستعارة لتقنية سلسلة الكتل، ويوضح هذا التطور تغيرًا كبيرًا بعيدًا عن قياسات التعريف التي تتم ممارستها في الويب 2.0، فعند الوصول إلى الويب 2.0، يحدد المستهلكون أنفسهم باسم المستخدم وعناوين البريد الإلكترونية التي تحمل البيانات التعريفية، ويمكن تمييز هوية عالم حقيقي فردي عن طريق تلك المعرفات، حيث إنهم مرتبطون بعنوان بروتوكول الإنترنت الخاص بالأجهزة المستخدمة، وتعد الهوية الرقمية للويب 2.0 مرادفة تقريبًا على نحوٍ دائمٍ لهوية العالم الحقيقي، ومع ذلك فإن المستخدمين قادرون على تنفيذِ عددٍ من الإجراءات لحجب هويتهم بدرجة معينة، والوصول لتطبيقات الويب 2.0 وصفحات الإنترنت؛ حيث ترتبط الخدمة بالخدمات المالية والبنكية التي تتطلب من المستخدمين ربط حساباتهم بهوياتهم في العالم الحقيقي باستخدام معلومات التعريف الشخصية (أرقام جواز السفر أو رقم الهاتف أو رقم الضمان الاجتماعي أو عنوان محل الإقامة).

ومن المتوقع ظهور الميتافيرس والويب 3 بناءً على اعتماد الهويات الرقمية، التي تكون حرة من الناحية النظرية، لمعلومات التعريف الشخصية، وللوصول إلى التطبيقات والمنصات في ميتافيرس الويب 3، فإنه يجب على المستخدمين استخدام محافظ العملات المشفرة لربط هوياتهم الرقمية بالمفتاح العام أو عنوان المحفظة لجعل هوياتهم الرقمية مستعارة، وفي هذا السياق، يمتلك المستخدم هويته الرقمية، عوضًا عن استخدام الهوية الرقمية المقدمة له بواسطة خدمات الإنترنت التي يستخدمها، وبربط الهوية الرقمية للمستخدم بعنوان محفظته، فإن الويب 3 يتيح قابلية التشغيل المتبادل للهوية الرقمية. ويحدد دخول المستخدمين للميتافيرس

باستمرار في التطبيقات الأخرى لشبكة الويب 3 بواسطة نفس عنوان المحفظة جاعلًا هوياتهم الرقمية متنقلة بين التطبيقات، ويسمح ذلك بنقل السلع الرقمية أو التمثيل الرقمي لملكية الأصول عبر جميع منصات الويب 3، ويمكن للمستخدم استخدام عددٍ من عناوين المحافظ للوصول إلى الويب 3، ولكن تكون المعاملات مرتبطة مع محافظهم وتكون متاحة للجميع على سلسلة الكتل، وسترتبط مع هوياتهم الرقمية العديدة. وقد أصبحت تلك التقنية سائدة للتحول الرقمي في العالم العربي، حيث قوبل مبدأ الويب 3 بالاعتماد على الصعيد الوطني على نطاق المنطقة (Sadeghian, 2022). وتستند جميع سلاسل الكتل والأصول الرقمية واعتماد الميتافيرس في جميع أنحاء العالم العربي إلى مبدأ شبكة إنترنت الويب 3، وقد استضافت مؤسسة «آرتس داو» أول شبكة ويب 3 من نوعها في المنطقة في مركز دبي المالي العالمي بدبي، حيث ضمت ملاك الأعمال والمستثمرين والمطورين والمستخدمين لتقنية الويب 3.

وتصبح الأنشطة الخبيثة وغير المشروعة الموزعة على شبكة النظراء بشكل طبيعي أكثر صعوبة في تَتَبُّعِهَا وسمة للفرد أو المجموعة، وفي عصر ظهور الأسماء المستعارة للهويات الرقمية، تكون الميتافيرس معرضةً لخطر أن تصبح أساسًا جوهريًّا للتهديد من الجهات التخريبية الذين يسعون للعمل بسرية، وتصبح الهوية الرقمية المخادعة أيضًا تهديدًا، مثل: الذكاء الاصطناعي وتعلم الآلة، حيث يمكن السماح بإنشاء روبوتات ميتافيرس مخادعة، ويمكن للمعالجة الطبيعية للغة تزويد المستخدمين المخادعين الآليين بالقدرة على تقديم أنفسهم كبشر.

لقد ازدادت شعبية اعتماد الهوية الرقمية المستوحاة من سلسلة الكتل على الرغم من المخاطر المحيطة بها، وذلك بين المجتمعات التي عَبَّرَت عن إحباطها من الرقابة الحكومية وتَعَقُّب البيانات من قِبَل مديري الإنترنت؛ ونظرًا لأن مستخدمي الإنترنت أصبحوا على معرفة أكثر بالقراءة والكتابة رقميًّا، فإن المستأجرين أصحاب زيادة الخصوصية على شبكة الإنترنت وحفظ البيانات يمثلون المحركات الرئيسة لاعتماد المستخدم للميتافيرس، وتؤخذ تلك الآراء بجدية من قِبَل مقدمي الخدمة الرقمية اليوم في الإنترنت الحديث، ويعد الاعتماد المؤسسي للميتافيرس إلى حدٍّ ما ردَّ فعلٍ لمثل تلك الآراء لمزودي الخدمة والمنظمين؛ وذلك من أجل المضي قُدُمًا في التطور الوشيك للممارسات عبر الإنترنت والهويات الرقمية.

الذكاء الاصطناعي والأنظمة المولدة (Artificial Intelligence and Generative Systems)

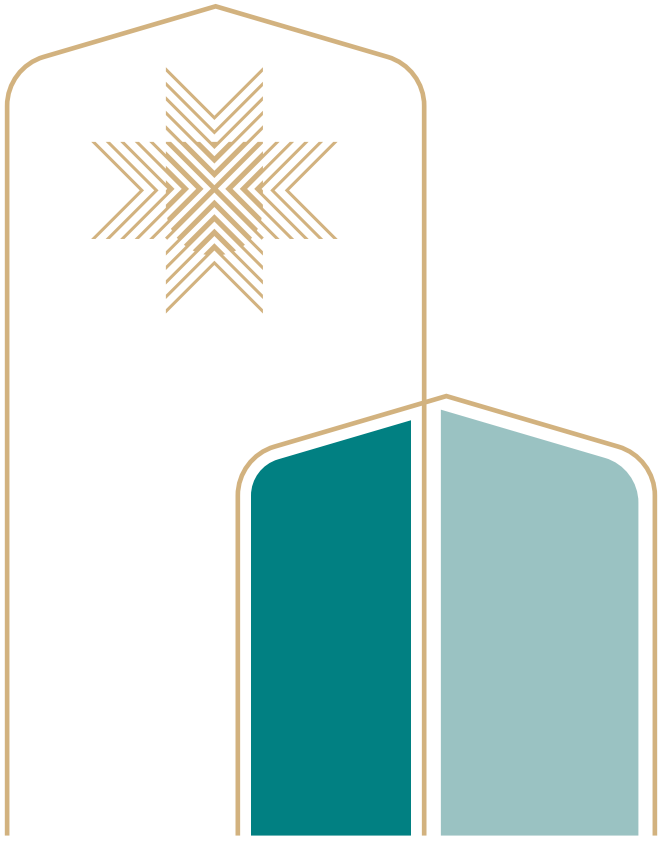
يسمحُ الذكاءُ الاصطناعيُّ لأجهزة الحاسب الآلي بإجراءِ الحساباتِ واتخاذِ القراراتِ في الميتافيرس، ويوفر بذلك تجربةً واقعيةً وسلسةً ومريحةً في العالم الرقمي لجميع المستخدمين. ويدعم الذكاء الاصطناعي المنتجات

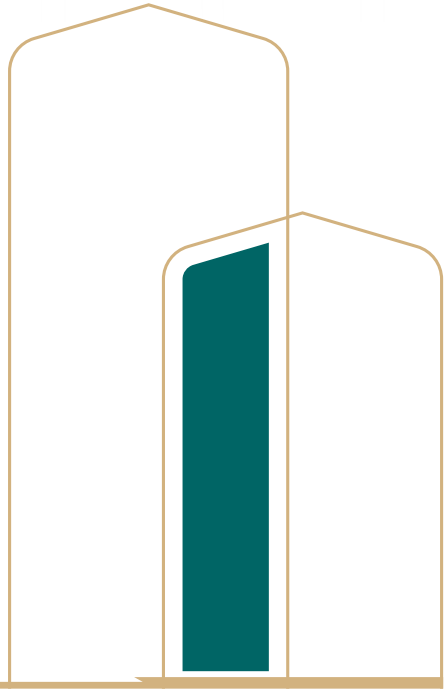
والأعمال/ التجارة في الميتافيرس، وتتضمن الأمثلة توليد الشخصيات الافتراضية وتعبيرات وجهها والسلوكيات والروبوتات التي يمكنها المساعدة في الإجابة عن الأسئلة الشائعة أو إعطاء توجيهات لتجربة أخرى، كما يسمح بتجربة متعددة اللغات وتسهيل التجارة والألعاب وغيرها من التفاعلات بين المستخدمين في الميتافيرس.

وقد نشأ المحول التوليدي المدرب مسبقًا في عام 2018، كنموذج مبدئي من نظام جوجل (Vas-wani et al., 2017) (GPT-1) الصادر عن شركة OpenAI، (Radford et al., 2018)، وتُعتبر المحولات التوليدية المدربة مسبقًا تقنية تعلم آلي تُسْتَخْدَم لبناء نماذج الذكاء الاصطناعي، وهي تقنيات مدربة للتفاعل مع مدخلات المستخدم باستخدام مرجعية أساسية من المعرفة، التي تزداد تعلمًا بواسطة تفاعل المستخدم، ويمكنها أيضًا التطور عندما تُخَصَّص لاحتياجات المنظمات أو الكيانات المؤسسية أو التطبيقات، ويعد ذلك «ضبطًا دقيقًا» (Shanahan, 2023). ويمكن أن تُسَمَّى نماذجُ المحولات التوليدية المدربة مسبقًا بنماذج اللغة الكبيرة، حيث إن المحول التوليدي المدرب مسبقًا هو طريقة لبناء نموذج أو إنشاء نماذج لغة كبيرة، ويعد استخدامها لبناء نماذج اللغة الكبيرة لاستخدام المستهلك توجهًا جديدًا مثل النموذج الثالث للمحول التوليدي المدرب مسبقًا الصادر عن شركة OpenAI المستخدم كقاعدة تقنية للمنتجات، مثل: روبوت الدردشة التفاعلي (شات جي بي تي). وقد صُنِّفَ منذ ذلك الحين (شات جي بي تي) كجزءٍ من حزمة أوسع نطاقًا للذكاء الاصطناعي المعروف بـ(الذكاء الاصطناعي المولد)، والأنظمة التي تولد محتوى جديدًا على سبيل المثال خطابًا جديدًا لم يبرمج سابقًا إليهم (Friedland, 2023).

ويتضح الحماس المدعوم مُسْبَقًا بتطبيقات نماذج اللغة الكبيرة في العالم العربي عقب الشهرة التجارية لشات جي بي تي، وأطلقت الإمارات العربية المتحدة على سبيل المثال روبوت دردشة يسمى «اسألنا» مدعومًا بنفس تقنية الذكاء الاصطناعي المولد (Saleh, 2023). وتبع ذلك ظهور نموذج اللغة الكبيرة فالكون بمعهد الابتكار التكنولوجي بأبو ظبي (Technology Innovation Institute, 2023)، الذي أُصْدِرَ إلى جانب مقارنات ملائمة لأداء أنظمة مستوى التقدم الجاري، مثل: النموذج الثالث للمحول التوليدي المدرب مسبقًا الصادر عن شركة أوبن أيه آي، وما يثير الانتباه أن معهد الابتكار التكنولوجي أتاح الوصول البحثي والتجاري لنموذج فالكون على الصعيد العالمي (Engdahl, 2023)، داعيًا بذلك لاختبارات دراسة الحالة الجديدة بقدراتها كبديل للوصول إلى موارد الحوسبة. ويطور المعهد أيضًا نموذجًا لمعالجة اللغة الطبيعية العربية يسمى «نور» (Tech-nology Innovation Institute, 2023b)، وهو ما يعكس الرغبة في بناء نماذج تختص بـ(اللغة العربية الفصحى الحديثة) التي تجذب انتباهًا أقلَّ نسبيًّا من قِبَل الشركات التقنية الغربية.

وتعاونت الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) بالمملكة مع شركة التكنولوجيا العالمية (نفيديا) لإنشاء مركز التميز للذكاء الاصطناعي التوليدي، بالإضافة إلى إطلاق النسخة التجريبية من تطبيق برنامج علام للدردشة الآلية باللغة العربية، وتهدف هذه الجهود الرائدة إلى رفع مكانة المملكة في مجال الذكاء الاصطناعي (Saudi Gazette, 2023). وتتوافق مبادرات سدايا مع رؤيتها لتحويل المملكة إلى قوة عالمية في مجال الذكاء الاصطناعي، وفي القمة العالمية للذكاء الاصطناعي للمملكة العربية السعودية لعام 2022، قَدَّمَت مُزن، وهي شركة متخصصة في تقنية الذكاء الاصطناعي للمؤسسات، مشروعها الثوري لبناء أكبر نموذج لغوي في مجال فهم وتحليل اللغة العربية بالذكاء الاصطناعي في العالم، كما قدموا تطبيقات برمجية متقدمة، وقدموا التقنية المتطورة لمحرك فهم اللغة العربية الذي يحمل اسم «أُسس» (Saudi Gazette, 2022).





الاستخدامات السلبية لتقنية الميتافيرس

تعكسُ هذه الميزاتُ المتقدمةُ لتقنية الميتافيرس طبيعتها الاستثنائية وإمكاناتها، وعلى الرغم من تشجيعها، فإن تقنية الميتافيرس وافرة بالاستغلال وسوء الاستخدام من بعض المهاجمين، كما هو الحال مع جميع التقنيات الجديدة، ويتطلب تحديد المخاطر التي يواجهها اعتماد تقنية الميتافيرس الاعتراف بأن نشر هذا النظام الافتراضي على نطاق واسع يتضمن استخدام تقنيات متنوعة لتحقيق هدف موحد يعود بالفائدة التجارية. ومع ذلك، تتطور هذه التقنيات بحقوقها الخاصة، وهو ما يجعل الآثار والاستخدامات السلبية لتقنية الميتافيرس مجموعة من التهديدات والتحديات متعددة الجوانب والتطور.

لذلك، يجب على الدول العربية بذل جهود لتشكيل تقنية الميتافيرس كنظام افتراضي متماسك ولا حدود له، ولا يكون ذلك من خلال تطبيق الدروس التنظيمية من الإنترنت التقليدي (ويب 2.0) والأنظمة والأطر التنظيمية الحالية فقط، بل أيضًا من خلال فهم أن بعض التهديدات التي تواجهها تقنية الميتافيرس جديدة حتى إن كانت تندرج تحت فئات معروفة. ولا تتيح معالجةُ هذه التحديات بشكل منفصل للدول العربية فرصةً لا تُضاهى لتنفيذ اعتماد تقنية الميتافيرس وتنظيمها فقط، إنما تتيح أيضًا ربط تقنياته المكونة والناشئة كجزء من حركة أوسع نحو تأمين اهتمام إقليمي متزايد في التحول الرقمي.

والمبدأ التوجيهي للدول العربية هو أن تقنية الميتافيرس هي تحدٍّ أمني مشترك وعابر للحدود يجب التصدي له بشكل مشترك ومفيد للجميع.

ويمكن أن نحدد تسعة مجالات رئيسة للمخاطر التي تواجه الدول العربية، وهي:

- البنية التحتية المخترقة.
- التلاعب بالهوية.
- محاذير الخصوصية.
- الاختراقات.
- الإرهاب الإلكتروني.
- الجرائم السيبرانية.
- نشر المعلومات المضللة والزائفة.
- مخاطر على السيادة والثقافة.
- التعبئة الاجتماعية والسياسية.

وتتضمن التسعة مجالات هذه انتهاكاتٍ محددةً لتقنية الميتافيرس، بما في ذلك الهجمات على البنية التحتية الحيوية، وتنسيق الهجمات السيبرانية، وسرقة الملكية الفكرية، وغسل الأموال، ونشر الدعاية، وجهود الجماعات المتطرفة في التجنيد، والتحديات التي تواجه الاستقرار الاجتماعي، وغيرها.

وتجتمع هذه المجالات معًا، وغالبًا ما تتخطى حدود الأمن الوطني والاحتيال والسرقة والتزوير والتجسس والجريمة والعنف والتحرش وخطابات الكراهية والترهيب، ومن الصفات القياسية لتقنية الميتافيرس، على الرغم من ذلك، هي اختلاط هذه الانتهاكات المحددة، والتداخل بين مجالات التحديات هذه بسبب أسسها التقنية المتنوعة للغاية وطبيعتها غير المحدودة. وعلى الرغم من أن طبيعة التهديدات الأمنية تبدو مألوفة للوهلة الأولى، فإن إساءة استخدام تقنية الميتافيرس المحتملة والناشئة بأشكال جديدة - يمكن للدول العربية أن تمنعها وتخفف منها وتقضي عليها.

وتتلاقى هذه الاستخدامات السلبية لتقنية الميتافيرس في ضرورة وجود تنظيم عالمي لتشكيل هذا النظام الافتراضي، وَيَرِدُ وصفُ ما يجب أن يكون عليه هذا الوجود في الأقسام التالية، ونوضح في هذا الجزء كيف يمكن للاستخدامات السلبية المحتملة والناشئة لتقنية الميتافيرس أن تُعَطِّلَ تطورَها ضمن النظم الاجتماعية والثقافية والاقتصادية.

ويتعلقُ استمرارُ تقنيةِ الميتافيرس بمرونة التقنيات الأساسية لها، مثل: الويب 3، والذكاء الاصطناعي وتعلم الآلة وإنترنت الأشياء، وغيرها. وتتطلب مجموعةُ التحديات الكبيرة، التي تواجه هذه التقنيات الناشئة، المزيدَ من السرعة والنطاق الترددي والمزيد من البيانات. وعلى غرار بناء أمان تقنية الميتافيرس أثناء إنشائها وتبني نهج استباقي بدلًا من نهج رد الفعل، ويجب أيضًا ضبط قواعد ولوائح الذكاء الاصطناعي وتنفيذها عاجلًا غير آجل مع تشكيل هذا المجال، ولا تزال مشكلات ويب 2.0 المتعلقة بالتوسع والتلاعب بالبيانات وقضايا الخصوصية قائمة إلى الآن، وتوفر درسًا قيمًا في حين يتشكل ويب 3.0. وكلتا التقنيتين لها عواقب وخيمة إذا تُرِكَت بدون تنظيم، وسيحتاج الذكاء الاصطناعي إلى ويب 3.0، والعكس صحيح، فهما يكملان بعضهما بعضًا.

ومن خلال توضيح هذه الإساءات المحتملة ومواجهتها بوضوحٍ، يميزُ العالمُ العربيُّ نفسه من مجرد اعتماد تجاري للتقنيات الأساسية التي تدعم تقنية الميتافيرس - وتقنية الميتافيرس نفسها - إلى بناءِ إطارٍ صالحٍ لاستخداماته بفعالية. وينشغل العالم التقني بأخبار الابتكارات في مجالات، مثل: الذكاء الاصطناعي وتعلم الآلة وإنترنت الأشياء والواقع المختلط والواقع المعزز والواقع الافتراضي، وغيرها، وبدأت بالفعل تظهر قيم وطنية وجيوسياسية مستقلة لاعتماد هذه التقنيات الأساسية بوضوحٍ للعديد من الدول العربية مع تطور هذه

الابتكارات، ولكن تطوير تقنية الميتافيرس على وجه التحديد يحتاج إلى جهد طويل الأمد بسبب تعقيد التقنيات الأساسية لها، وهذا ما أكده خبير الذكاء الاصطناعي الرئيس في ميتا «Yann LeCun» (Strickland, 2022). ونظرًا لأن التقنيات التي تدعم تقنية الميتافيرس وتجعلها قادرة على العمل والوصول إليها - جزء من جهد بحث أساسي وتطبيقي طويل الأجل، فمن المرجح أن تظهر تهديدات أمنية جديدة، وبالتالي من الجيد بالنسبة للدول العربية، كما أوضحنا، اعتماد نهج استباقي يضم هذه التهديدات المحتملة في أساس تنظيمي مشترك.

وتخدمُ المنظومةُ التنظيميةُ المطورةُ لتقنية الميتافيرس بين الدول العربية هدفًا ليس معنيًّا فقط بتعزيز الاعتماد السلس لهذا النظام الافتراضي، وإنما بفرض مشاركة متكاملة مع التقنيات التي ستتطلب أُسُسًا في الخبرة الأمنية في السنوات المقبلة على المستويين الوطني والدولي، ويتسبب الاعتراف بتنوع التحديات والتهديدات التي يشكلها العالم الافتراضي مع مرور الوقت في وضع الدول العربية في موقف متوسط وطويل الأجل محسوبٍ للغاية فيما يتعلق بنشر تقنية الميتافيرس واعتمادها.

1. البنية التحتية المخترقة (Compromised Infrastructure)

تلك الخصائص نفسها التي تشغل تقنية الميتافيرس وتوفر لتقنية الميتافيرس إمكاناتها المحتملة يمكن أن تتعرض للاختراق، إما عبر نقاط ضعف في النظام أو كأدوات للأذى. وعند فهم المجالات التي يمكن فيها استخدام تقنية الميتافيرس سلبيًّا، يجب أن يؤخذ في الاعتبار فساد الخصائص الحرجة والبنية التحتية لتقنية الميتافيرس، ونبين أدناه كل منطقة من مناطق البنية التحتية التي تعتبر عرضةً للاختراق.

الشبكات (Networks)

يعتبر قطاع الاتصالات أحد القطاعات الستة عشر للبنية التحتية الحرجة؛ ولذلك فمن الضروري حماية بنية الشبكة التي تحقق التواصل بين المستخدمين والأجهزة بغض النظر عن الثمن، وينطبق هذا على الشبكات التي تدعم تقنية الميتافيرس مباشرة، وكذلك أي شبكات محيطة قد تلامس بيانات تقنية الميتافيرس والبيانات الوصفية والقياس عن بعد، أو تسمح بالوصول إلى الأجهزة، وقد قامت الجهات الضارة، سواء أكانت تدعمها دولٌ مختلفة أو تعمل بمفردها، بتصميم حملات بدقة لمهاجمة الشبكات واستخلاص المعلومات منها، والاستفادة من البيانات التي تتدفق فيها...إلخ، ونفذت هذه الجهات هجوم

حجب الخدمة الموسع والبرامج الخبيثة لمنع الوصول إلى الشبكة وحجب خدمات المنصة، وفي الوقت نفسه سرقة البيانات في الإصدار الحالي للإنترنت. ومع تطور الشبكات واستمرار دعم تقنية الميتافيرس بسرعة وبيانات كبيرة، تصبح حماية الشبكة أمرًا ضروريًّا بنفس القدر.

إنترنت الأشياء (Internet of Things)

يضم إنترنت الأشياء مجموعةً أوسع من المشكلات الأمنية، التي يمكن أن تؤثر في أي نوع من التقنية، وتواجه شبكات ومعدات تقنية الميتافيرس مشكلات أمنية كبيرة، ويجب معالجتها أثناء تصميم هندسة الشبكة. ويشمل استهداف إنترنت الأشياء إمكانية تعرضها للهجمات السيبرانية التقليدية، مثل: هجوم حجب الخدمة الموسع والبرامج الضارة والخبيثة، كما يتيح إنترنت الأشياء حركةً جانبيةً أكثر داخل الشبكة التقليدية، بحيث تكون نقطة دخول واحدة كافية للمهاجم للتنقل بسرعة في جميع أنحاء الشبكة، وهو ما يزيد من خطر تلف البيانات وفقدانها وسرقتها، ولن تسمح الشبكات الأساسية لتقنية الميتافيرس بالحركة الجانبية التقليدية التي يعتاد عليها محترفو الأمن السيبراني والشبكات، وبالإضافة إلى سرقة بيانات الاعتماد والكم الهائل من المعلومات الشخصية المتاحة في تقنية الميتافيرس، فإن حدوث الحركة الجانبية وسوء استخدام الشبكة المتعلق بأجهزة إنترنت الأشياء أمر محتمل، وفي أسوأ السيناريوهات، يمكن للمهاجم الضار استخدام نظارة الواقع الافتراضي لشخص ما في تقنية الميتافيرس للدخول إلى الشبكة والتحرك جانبيًّا لنشر البرامج الضارة أو الخبيثة، وإسقاط جزء كبير من تقنية الميتافيرس، وجعل المشتريات والأصول الرقمية وغيرها غير متاحة تمامًا لرواد تقنية الميتافيرس، وعلى الرغم من أن المخاطر والأضرار الأمنية تتطلب مناقشة أعمق، فإنه ليس من المبكر البدء في مواجهة المخاطر التي يمكن أن تنشأ مع التقنية الجديدة، ويعني تشكيل حواجز وقائية للتقنية الجديدة تمكين تجربة مستخدم أكثر أمانًا عاجلًا وليس آجلًا، وتكون استباقية بدلًا من رد الفعل.

الواقع المختلط (Mixed Reality)

بالإضافة إلى المجال الجديد الذي تقدمه تقنية الميتافيرس، فإن العوالم والواقعيات التفاعلية الإضافية تعد جزءًا أساسيًّا من تقنية الميتافيرس، ويجب حماية جميع البيانات المذكورة سابقًا، كما يجب حماية جميع الأنظمة والمستشعرات والشبكات المستخدمة لجمع البيانات للواقع الافتراضي والواقع المعزز والواقع المختلط

والواقع الممتد، ويمكن أن تتعرض الأجهزة التي توفر تجارب في الواقع المختلط للاختراق، وتقدم مستشعرات الواقع المعزز/ الواقع الافتراضي تحديات جديدة أمام المستخدمين. ويتيح البث المباشر، سواء لمشاهدة وسائل الإعلام، أو ممارسة الأعمال التجارية، أو الألعاب، أو الاستخدامات الأخرى، مشاهدة البيانات آنيًّا بدلًا من الانتظار وجمعها للتحليل الشامل. وبما أن البشر يتجهون حاليًّا إلى تقنية الميتافيرس، التي تتطلب اتصالًا أقوى وأجهزة وتقنية لمتابعة العالم الرقمي والتفاعل معه، فإن هذا الأمر يترتب عليه مزيدٌ من مخاطر فقدان الخصوصية والأذى للأشخاص عندما «يتصلون» بتقنية الميتافيرس وينتقلون بأنفسهم هناك. وستكون حماية الخصوصية والبيانات الشخصية أكثر أهمية من أي وقت مضى مع تطور هذا النظام.

الذكاء الاصطناعي (Artificial Intelligence)

زادت شعبيةُ نماذجِ اللغاتِ الكبيرةِ وروبوتات الدردشة واستخدامها في نهاية عام 2022، وتأثرت كل قطاعات الحياة؛ الطبية والمالية والتقنية والحكومية وغيرها، ومنحت أدوات الذكاء الاصطناعي هذه حياة جديدة للتفاعلات السهلة والفعالة بين الأشخاص والحكومات وعمليات الأعمال التجارية، والآن يمكن معالجة المهام المملة والمكررة بشكل أكثر فاعلية من خلال الأتمتة، وعلى الرغم من ذلك، تتطلب تطبيقات الذكاء الاصطناعي العملية، التي تضم التعرف على الوجوه والأصوات وروبوتات الدردشة، تدريبًا، على أن يُنفذ هذا التدريب بشرٌ متأثرون بتحيزاتهم وانحرافاتهم. وتخضع التحيزات المدرجة في أي نموذج عن طريق التدريب - سواء أكانت عبر الكلام أم النص أم الفيديو - لتقليل تمثيل بعض الثقافات والجنسيات وتضمين العنصرية والتعصب، حتى لو كان ذلك غير مقصود.

وتتأثر كل صناعة بالأدوات التي تعمل بالذكاء الاصطناعي، وعلى الرغم من أن نماذج اللغات الكبيرة هي وسيلة ملائمة لتحليل كميات ضخمة من البيانات في البيئات التجارية واستخدامها، فإن البيانات، التي يتم تدريبها عليها من مصادر متنوعة، مثل: الطب والتمويل والشبكة المظلمة (الويب المظلم) (Deep dark web) - تؤثر مباشرة على تكاملها في البيئات التجارية، وفي ظل تطور هذه التقنية، تبدأ التحذيرات بالظهور، وتتحول نماذج اللغات الكبيرة في بعض الأحيان إلى ببغاوات عشوائية (Bender et al., 2021) أو أنظمة تقلد أنماط البيانات التي تم تدريبها عليها، بما في ذلك الأنماط التي تعكس ببساطة تحيزات الإنسان في العالم الحقيقي، ومع ذلك، فإن العلماء والباحثين الرائدين بالفعل يحذرون من أن تطبيقات الذكاء الاصطناعي المدعومة

بنماذج اللغات الكبيرة، مثل: روبوتات الدردشة (Kosinksi, 2023) التي تستخدم عناصر لم يتم برمجتها بشكل مقصود فيها، وتقوم بتقليد بعض الصفات البشرية أو الصور النمطية التي تكون شخصية بشكل مماثل للإنسان أو مستوحاة منه (Lu et al., 2023).

وينبغي الاعتراف بأنه مع ظهور أدوات الذكاء الاصطناعي وتعلم الآلة، فقد انخفضت العوائق التي تحول دون دخول الجرائم السيبرانية، وقد أتاحت تلك الأدوات الفرصة للمجرمين السيبرانيين غير المحترفين ذوي الخبرة القليلة أو المعدومة لتصميم برامج ضارة تستهدف البيانات، وعلى وجه الدقة، يمكن أن يؤيد الذكاء الاصطناعي في تقنية الميتافيرس إنشاء هرم رقمي أو طبقة اجتماعية من المجتمع (Microsoft Research, 2023)، فضلًا عن تجاهل عوامل اجتماعية ثقافية مهمة. وأدت الجائحة والانتخابات الأخيرة في جميع أنحاء العالم وحركات مدنية أخرى إلى تقسيم المجتمعات وحدوث صراعات مدنية بالفعل، وقد يؤدي توسيع هذا الصراع وتعزيزه في تقنية الميتافيرس باستخدام التقنية، التي تعتمد على التحيزات البشرية وبالتالي تخضع لها، إلى المزيد من التفرقة بين المستخدمين والمشاركين في تقنية الميتافيرس بدلًا من توحيدهم (Microsoft Research, 2023). وتشير الأبحاث المبكرة الأخرى إلى أنه يمكن لنماذج اللغة الكبيرة إعادة صياغة النص بطريقة تخفيف الاحتقان في التفاعلات الرقمية بين المستخدمين البشريين الذين يناقشون موضوعات ساخنة (Argyle et al., 2023) ومن المفترض أنه إذا دعمت النماذج هذه القدرات، فمن الممكن استخدامها. أيضًا لأغراض سلبية في بيئات افتراضية ديناميكية مستقلة عن الدولة أو المنطقة التي يقيم فيها المستخدمون البشريون.

ويمكن أيضًا تعزيز التواصل حول الأنشطة غير المشروعة - مثلما هو الحال في تواصل أعضاء منظمة إجرامية - بواسطة الذكاء الاصطناعي، عندما يتم ربطه بتقنية إخفاء المعلومات، وهي تهديد معروف تُخفى فيه الرسائل داخل صورة أو وسائط أخرى، وتعمل تلك التقنية عند تنفيذها بشكل صحيح على إخفاء وجود رسالة سرية أو أي رسالة (Ornes, 2023)، وقد استخدمت تقنية إخفاء المعلومات في الويب 2.0 في هجمات البرامج الخبيثة والبرامج الضارة سريعة الانتشار. ويمكن للذكاء الاصطناعي تمكين استخدام تقنية إخفاء المعلومات للأنشطة الضارة، ويتيح المحتوى الذي تنشئه الآلة، والخوارزميات التي تشكل الذكاء الاصطناعي، فرصًا أكبر لإخفاء الرسائل وتشفير المعلومات السرية تمامًا (Ornes, 2023). وهذا التهديد الأمني الخاص يتداخل مع الذكاء الاصطناعي بما في ذلك الجرائم السيبرانية، ولكن يتم تعزيزه حديثًا بشكل رئيس باستخدام أدوات الذكاء الاصطناعي المتاحة.

2. التلاعب بالهوية (Identity Manipulation)

تطرح تقنية الميتافيرس تحدياتٍ جديدةً فيما يتعلق باستخدام الهويات الرقمية وسوء استخدامها؛ ونظرًا لأنه عالم افتراضي انغماسي، فإن مفهوم الهوية الرقمية يتجاوز مجرد اسم مستخدم أو ملف تعريف، فقد تشمل الهوية الرقمية شخصيات رمزية قابلة للتخصيص بالكامل وتاريخ شخصي وإنجازات وأصول افتراضية مملوكة، ويثير هذا المستوى الفريد من التخصيص العديد من المحاذير؛ إذ يمكن سرقة هويتك الرقمية أو استنساخها أو إساءة استخدامها، وهو ما يؤدي إلى شكل من أشكال سرقة الهوية، التي تكون النظم النظامية الحالية غير مجهزة بشكل جيد للتعامل معها. ويمكن للمحتالين استغلال هذه الهويات الرقمية وإنشاء نسخ مزيفة مطابقة تقريبًا للشخصيات الافتراضية المعروفة لخداع الآخرين، على غرار عمليات التصيد الاحتيالي في الويب 2.0 الحالي. ويمكن أن تؤدي القدرة على التنكر كأشخاص آخرين إلى أشكال جديدة من التنمر الإلكتروني والتحرش أو المعاملات الاحتيالية، وعلاوة على ذلك، يمكن أن يؤدي سوء استخدام الهويات الرقمية هذا إلى خسارة سمعة الفرد داخل تقنية الميتافيرس، وربما في العالم الحقيقي، ويقدم عمق المعلومات الشخصية داخل الهوية الرقمية أيضًا محاذير الخصوصية، ويمكن للشركات جمع بيانات المستخدمين وتحقيق الربح منها بطرقٍ تعتدي على الخصوصية، وهو ما يؤدي إلى انتهاكات غير متوقعة للأمان الشخصي.

وتَمَثَّلَ اتجاهٌ حديثٌ بين المهاجمين السيبرانيين في نشر تقنية التزييف العميق في المساحات الإلكترونية، ويمثل استخدام تقنية التزييف العميق بشكل ضار مصدر قلق آخر في تقنية الميتافيرس؛ حيث تطور مفهوم الهوية، ونتيجة لتقنية التزييف العميق التي يقدمها الذكاء الاصطناعي، يمكن إنتاج محتوى فيديو أو صوت مركب بشكل شبه واقعي يصور شخصًا يفعل أو يقول شيئًا لم يفعله بالفعل في الواقع، ففي تقنية الميتافيرس، يمكن توسيع استخدام تقنية التزييف العميق (Tariq et al., 2023)، لإعادة إنشاء هويات رقمية كاملة، وهو ما يمكنهم من التنكر في هيئة شخصيات معروفة أو مؤثرة، ويمكن للمجرمين استخدام هذه التكتيكات الخادعة لأغراض خبيثة مختلفة، بدءًا من نشر المعلومات الخاطئة والدعاية إلى الاحتيال على المستخدمين غير الحذرين، ويمكن أن يؤدي هذا النوع من سوء استخدام الهوية في تقنية الميتافيرس إلى انتشار الشك وعدم الثقة على نطاق واسع، وهو ما يجعل من التفاعلات الاجتماعية والتجارة أمرًا مُعَقَّدًا.

الهندسة الاجتماعية (Social Engineering)

تُمَثِّلُ الهندسةُ الاجتماعيةُ التهديداتِ المستمرةَ للأنشطة عبر الإنترنت، بغض النظر عن إصدار التقنية المستخدمة والتحديثات والتصحيحات وتقليل المخاطر. ويمكن القول ببساطة بأن الأشخاص ليسوا دائمًا من

يخبرون أنهم متصلون عبر الإنترنت، ففي تقنية الميتافيرس، التي تركز على التفاعلات الشخصية الغنية، هناك أيضًا احتمالية قوية لحملات التجسس والهندسة الاجتماعية، وهي تكتيكات معروفة تستخدمها مجموعات تابعة للدولة وتكون أقل تقنية. فالمهاجمون الأقل تقنية لا يزالون يجيدون سرقة الملكية الفكرية والمعلومات الشخصية والوثائق الحكومية و/أو المؤسسية الحساسة.

وتؤدي التفاعلات الاجتماعية التي تحدث في تقنية الميتافيرس إلى تكوين اعتلال مشترك سيئ مع الهندسة الاجتماعية للحصول على معلومات لا ينبغي أن تكون متاحة للعامة، وهذا ما يُشَكِّلُ تهديدًا خطيرًا من الناحية الأمنية على المستوى الوطني. وقد يكون هذا أحد أخطر التهديدات للأمن الوطني والمؤسسات والأنشطة عبر الإنترنت بشكل عام، وغالبًا ما يقوم المهاجمون المهددون بالظهور بصورة خاطئة غير صورتهم الحقيقية عمدًا، أو ببساطة يكذبون حول هويتهم للحصول على معلومات من جميع الأنواع، وفي البيئة الافتراضية المتنكر فيها المجهولة، غالبًا ما يكونون أكثر جرأة وشجاعة، وعليه، يتوقع أن يتصاعد هذا السلوك في تقنية الميتافيرس مع تزايد استخدام الذكاء الاصطناعي في إنشاء صور مزيفة وبيانات حيوية وشخصيات افتراضية وأكثر من ذلك، ويمكن للذكاء الاصطناعي إنشاء شخصية ومنظمة ورواية من أي نوع بسرعة، وتوجد احتمالية سوء الاستخدام لهذا المجال بشكل قوي، ومع أنه يعد بالفعل من الصعب التمييز بين المحتوى الذي أنشأه الذكاء الاصطناعي وبين المحتوى الذي أنشأه الإنسان، فإن الجهات الضارة يمكن أن تستخدم هذا الجانب الغامض (Edwards, 2023) لتحقيق غاياتها لإجراء بحوثهم، وتطوير خططهم والاستفادة من مستخدمي تقنية الميتافيرس.

وهناك منصات، مثل: لينكد إن، التي من المفترض أن يكون وجودها مهنيًّا فقط، أصبحت أرضًا خصبةً للمهاجمين الضارين لتنفيذ التجسس المؤسسي وحملات الهندسة الاجتماعية (Syme, 2023). وهذا الخطر ينتقل بشكل كبير إلى تقنية الميتافيرس، حيث يمكن للمهاجمين الضارين استخدام الذكاء الاصطناعي الإنتاجي لإنشاء الشخصيات الافتراضية وإخفاء هوياتهم الحقيقية، ولا ينطبق التنكر فقط على رؤساء الدول الشهيرين، مثل: الملوك أو الرؤساء، بل يمكن تقليد أي إنسان على الإنترنت باستخدام بصمات حقيقية من نشاطهم والنتيجة هي شكل ظاهري مشروع للتعرف، فحتى على المنصات المُراقبة بشكل أكثر صرامة، مثل تلك التي تُجْرِي معاملات مالية، يتم ملاحظة استخدام المهاجمين الضارين للوثائق المزورة والمواد الناتجة من أدوات الذكاء، ويشمل ذلك كل شيء بدءًا من شراء بطاقات هوية مزيفة، وفواتير خدمات عامة مزيفة من منتديات إجرامية مختلفة، إلى تضليل موقعهم أو مكان إقامتهم، ويمكن تزوير تلك المعلومات المسروقة وتغييرها بسهولة؛ بالإضافة إلى إنشاء مقاطع فيديو مزيفة وشخصيات افتراضية ونشاط آخر، ويتلاشى الخط بين هوية إنسان حقيقية وهوية مزيفة ويصعب التمييز بينهما أكثر.

3. محاذير الخصوصية (Privacy Concerns)

لا يمكن مناقشة التقنية بشكل كافٍ دون التطرق إلى محاذير الخصوصية، وحيث يتطلب إنشاءُ حسابٍ جديدٍ أو التسجيل في خدمة أو القيام بأنشطة عبر الإنترنت وجودَ مصادقةٍ، مثل: عنوان البريد الإلكتروني وكلمة المرور واسم المستخدم وتاريخ الميلاد ورقم الهاتف وغير ذلك، ففي التقنيات الأساسية، توجد خدمات ضرورية، ولكن غير معلن عنها في مستويات أعمق من الحزمة التكنولوجية، وتسهم أيضًا في حدوث مشكلات الخصوصية، مثل: تتبع ملفات تعريف الارتباط (الكوكيز) أو شهادات X509، وبحد أدنى، تُسَبِّبُ هذه المعلومات أذًى طفيفًا إذا تم الوصول إليها/ كَشْفُها بشكل غير قانوني أو تم التعامل معها بشكل منفصل، ومع ذلك، فإن البيانات التي يُكشف عنها بشكل جماعي تُشَكِّلُ تهديدًا أكبر وأكثر خطورة. وفي تقنية الميتافيرس، خاصة عندما يتم بناؤها بطريقة فردية أكثر، تتطلب تجربة المستخدم حسابات فردية متعددة لمجالات مختلفة، كما يمكن أن تتطلب تحديد هوية المستخدم من خلال محفظة العملة المشفرة، ويمكن أن تشمل هذه المحافظ الأصول الرقمية وتكون مُؤَمَّنَة بشكل تشفيري لحماية الأصول من السرقة والضياع. ومع اكتساب الجهات الخبيثة مزيدًا من المعرفة حول تقنية الميتافيرس ومحاولتهم مهاجمتها وقاعدة مستخدميها، يجب أن تظل حماية خصوصية مستخدمي تقنية الميتافيرس في المقام الأول، خاصةً مع التشغيل المتبادل القائم على فكرة التوافق والتكامل، حيث إن أي نوع من أنواع التعرض للخصوصية في العالم الرقمي سيؤثر في العالم الحقيقي والعكس بالعكس.

وعلى الرغم من أن تقنية الميتافيرس هي ساحة جديدة، فإن سرية البيانات وسلامتها وتوافرها (ثالوث سي آي إيه) ضرورة غير قابلة للتغيير ومطلقة لجميع الاتصالات الرقمية، ويجب على الدول العربية أن تتابع مدخلات المستخدمين وتبادلهم المعلومات في تقنية الميتافيرس وفقًا لقواعد الخصوصية والحماية، وتكون البيانات هي النطاق الجديد - ودورها المركزي يستدعي حمايتها بأي ثمن، ولقد استخدمت بعض الجهات الإنترنت لفترة طويلة لسرقة المعلومات الشخصية الخاصة بحكومات بعض الدول وبعض المواطنين، كما سرقوا خطط الأسلحة والوثائق الخاصة بالسفن والطائرات وكتيبات التدريب العسكرية والمواد الفكرية والمعدات المتعلقة بالأمن الوطني والكيانات التي تحميه، وطبيعة الإنترنت المظلمة تسمح أيضًا بالإنكار المعقول وتصعيد التوترات بين الحكومات، فضلًا عن الأشخاص، ومن المتوقع أن يزداد توافر البيانات في تقنية الميتافيرس فقط، وهو ما يعني أنه يجب وضع عمليات لحماية البيانات الحساسة والمؤسسات من البداية.

خصوصية بيانات المستهلك (Consumer Data Privacy)

ستستمر الحاجة إلى حماية المستهلك في تقنية الميتافيرس، ويعتبر تنفيذ تدابير لحماية البيانات الفردية وإنشاء المرونة الرقمية والحفاظ على خصوصية البيانات أمرًا بالغ الأهمية، ويتطلب تنفيذ تدابير في جميع نقاط البيانات أثناء الراحة وأثناء الانتقال، ويجب أن يكون التشفير الشامل هو القاعدة العامة لتقنية الميتافيرس، وذلك بدون استثناء، ومن المتوقع أن تكون الإعلانات في الميتافيرس مربحة بقدر ربحها في الويب 2.0. وستستهدف الإعلاناتُ المستخدمين، سواء أكانوا بشرًا أم شخصيات افتراضية، ويجب حماية البيانات الشخصية للمستهلكين، التي تجمعها وتستخدمها خدمات الإعلان في تقنية الميتافيرس، من الجهات الخبيثة التي تحاول سرقة المعلومات الشخصية وبيعها بغرض الربح، تمامًا كما تفعل الجهات الخبيثة الآن في خدمات الويب 2.0 (Vardanyan et al., 2023). وعند التفاعل والتسوق والمشاركة في النظام الافتراضي، سيتم إنشاء بيانات المستهلك بمعدل أعلى بكثير مما يتم إنشاؤه في الويب 2.0 الحالي، ومع تزايد توافر البيانات ينتج المزيد من المخاطر لانتهاك استخدام خصوصية المستهلكين أو إساءة استخدامها.

وعلى مالكي منصات تقنية الميتافيرس ومشغليها بناء منصاتهم بفكرة حماية خصوصية المستهلكين بأي ثمن، ويجب أن يستفيدوا من الدروس المستفادة من الويب 2.0 وتنفيذ سياسات وعمليات أفضل، ويُتناول العديد من هذه التدابير بشكل طبيعي من خلال ميزات الثقة والمراجعة التقنية، التي تعتمد على سلسلة الكتل، والتي تدعم منصات تقنية الميتافيرس اللامركزية، وعلى الرغم من هذه الضمانات، فإن هناك نقاط ضعفٍ وثغرات في عدة نقاط نقل البيانات. ويجب تصميم نقل البيانات وتخزينها لحماية المستخدمين والشخصيات الافتراضية الخاصة بهم والاتصال بينهم، ويتم معالجة اعتبارات الخصوصية بواسطة تقديم واستخدام تقنية سلسلة الكتل، ولكن لا يوجد دواء شافٍ لجميع مشاكل الخصوصية، حيث يتطلب ذلك اليقظة والتحديثات المستمرة.

وفي سلسلة الكتل، تكون بيانات المستخدم خاصة للغاية؛ حيث تكون المعلومات المعرفة الوحيدة هي عناوين المستخدمين المتعاملين، كما تكون عمليات الوصول إلى البيانات خاصة، حيث يمكن أن يفعل ذلك فقط المستخدمون المتعاملون الذين يمتلكون مفاتيح التشفير الخاصة، وتكون سلسلة الكتل مؤمنة بشبكة موزعة من النظراء الذين يدعمون سلسلة الكتل، ويتحقق مشاركو شبكة النظراء من صحة المعاملات، ويمكن للأعضاء الانضمام إلى الشبكة أو مغادرتها دون التأثير على التوافق. ويُشغل المشاركون في الشبكة المتصلة هذه أو العُقد برامج لفرض بروتوكولات سلسلة الكتل والتفاعل بعضهم مع بعض دون الحاجة إلى مدير شبكة

موثوق أو وسطاء للسماح بنقل المعلومات في جميع أنحاء الشبكة، ويمكن للجهات المهددة محاولة التغلب على سلامة سلسلة الكتل من خلال تشغيل عقد ضارة أو تنفيذ هجوم حجب الخدمة الموزع ضد الشبكة لتعطيل حالة سلسلة الكتل. وتمتد هذه التهديدات إلى منصات تقنية الميتافيرس التي تعتمد على تقنيات سلسلة الكتل، وتُصمم سلسلة الكتل بشكل طبيعي للدفاع عن نفسها ضد هذه التهديدات من خلال توزيع مسؤوليات الشبكة لدفتر الأستاذ على عدة عُقد وضمان استمرارية الشبكة في حالة اختراق عقدة واحدة أو عدة عُقد في مواجهة تهديد سيبراني. وتجعل الحماية، التي توفرها تقنية سلسلة الكتل واستخدامها المثبت لتأمين التقنية، مرشحًا مثاليًّا للاستخدام في تقنية الميتافيرس.

خصوصية البيانات المؤسسية (Institutional Data Privacy)

يجب أن تكون سياساتُ كلِّ شركةٍ وبائع تجزئة وتاجر وفنان ومؤسسة محددةً بشكل واضح، عندما يتعلق الأمر بعمليات تقنية الميتافيرس، ويؤدي تفوق التقنية على التنظيم في معظم الأحيان إلى مشكلات؛ لذا يجب على جميع المنظمات والمؤسسات أن تبدأ بسياسات الخصوصية للأجهزة ومعالجة البيانات والاحتفاظ بها؛ ويشبه هذا حاليًّا سياسات استخدام الأجهزة الشخصية في العمل، ولكن يجب تحديدها على نطاق أوسع. وتشمل الأجهزة المدرجة أي جهاز يوفر اتصالًا بتقنية الميتافيرس: أجهزة الحاسب الآلي الشخصية، وأجهزة الحاسب المحمولة، والأجهزة اللوحية، والهواتف المحمولة، بالإضافة إلى تلك الأجهزة التي تسمح بالتفاعل في تقنية الميتافيرس، مثل: نظارات الواقع الافتراضي/ الواقع المعزز.

والتحديد هو أمر ضروري، ويجب على الشركات ومقدمي خدمات الأصول الافتراضية البدء في تحديد ما يلي على الفور:

- كيف ستتعامل الشركات مع مناطقها وشبكاتها للاتصال والتفاعل؟
- كيف سيحمون معلوماتهم الخاصة، بالإضافة إلى معلومات عملائهم ومستخدميهم؟
- كيف سيسمحون لمستخدمي الميتافيرس بالتفاعل والمشاركة؟
- كيف ستفرض الشركات سياساتها؟ وما أفضل طريقة لتحقيق ذلك؟

يوجد تركيز منفصل مطلوب للتوافق التنظيمي: الاعتماد على تجميع أكثر لوائح الخصوصية صرامة، ويجب على واضعي السياسات أن يسعوا لمواءمة السياسات مع معايير الخصوصية المحددة بواسطة القانون

العام لحماية البيانات في الاتحاد الأوروبي، حيث إنها واحدة من أكثر السياسات شمولية على مستوى العالم، مع الاعتراف بالتحول من حوكمة تعتمد على بلدٍ معينٍ إلى طريقة أكثر شمولية ومناسبة افتراضيًّا لمتابعة العالم الرقمي. ويمكن لدول منطقة الشرق الأوسط وشمال إفريقيا أن تعملَ على تحديد سياسات غير تابعة إقليميًّا لتقنية الميتافيرس، ثم العمل على تطبيقها على الشركات المهتمة وعلى المستوى الدولي أيضًا، ولقد لُوحظ ذلك بالفعل في سلطة تنظيم الأصول الافتراضية بالإمارات العربية المتحدة، وينبغي لواضعي السياسات وخبراء الأمن أثناء المنتدى المشترك الأخذ بعين الاعتبار إنشاء هيئات تنظيمية محلية؛ وذلك لضمان تحقيق التشغيل المشترك التنظيمي على المستويين الإقليمي والدولي.

تخزين البيانات (Data Storage)

نشأت قضايا الأمن الخاصة بتخزين البيانات منذ مطلع إجراء تخزين البيانات رقميًّا، ويعتبر تشفير البيانات - سواء أكانت البيانات الموجودة في قاعدة البيانات أم أثناء النقل - من أفضل الممارسات الدائمة في هذا المجال، حيث تتسم كلتا الطريقتين الرئيستين لتخزين البيانات بالمركزية واللامركزية في تقنية الميتافيرس، وتتمتع كلتا الطريقتين بمزايا ومخاطر.

ويُشير التخزين المركزي إلى تخزين البيانات ومشاركتها بين خوادم الحوسبة المادية من خلال الشبكة، ويعد توفير كافة الأجهزة والمعدات المطلوبة لتسهيل عملية التخزين المركزية في مكان واحد، وهي الطريقة الأمثل للتخزين، ومع ذلك، فإنه باستطاعة الجهات السيبرانية الفاعلة، التي تسعى لاختراق الشبكات أن تُحَقِّقَ ذلك من خلال الموارد الوفيرة وطرق التدريب، بمعنى أنه في حال رغبتهم في اختراق طرق الحماية في المكان، ما عليهم سوى الوصول لمستودع تخزين البيانات المتاح لديهم بسهولة، وفيما يلي الطريقة الأكثر شيوعًا لدى الجهات الفاعلة الخبيثة: يمكنهم الحصول على طريقة للوصول إلى الشبكة من خلال استخدام طرقٍ غير قابلة للكشف، ويستمرون في البقاء على نفس الوضع في الشبكة لفترة زمنية معينة، وفي الوقت الذي تدرك تلك الجهات أنها تمكنت من زيادة عملية سرقة البيانات والاختراقات، يقومون بتوزيع البرامج الضارة أو الفيروسات مانعين بذلك المنظمة الأصلية من الوصول للبيانات، كما يقومون بنشر تلك البيانات، وبذلك يمكنهم بيعها على المنصات لمن يدفع أكثر، وتعتبر هذه النتيجة هي أثر كبير للتخزين المركزي (Sanger and Barnes, 2023).

ويمكن رصد أي واقعةٍ تتعلق بإعادة استخدام البيانات المسروقة على الدوام، وتعد الوثائق المعتمدة ومعلومات تحديد الهوية الشخصية من المجالات التي تبدو غير خطرة، مثل: تجارة التجزئة ووسائل التواصل

الاجتماعي وغيرها، والتي ينتج عنها إتاحة الوصول للمجالات التي لها العواقب الأكبر والأشد، مثل: المنظمات الحكومية، والبنية التحتية المهمة، ومنصات الموارد الرئيسة، وسجلات الدخول. وقد يبدو الأمر في منتهى الخطورة، وذلك عندما يؤدي البريد الإلكتروني وكلمة المرور المستخدمان لخدمة غير ضارة إلى تسهيل الوصول للجهات التي لها علاقة بالأمن الوطني، وتعي الجهات التهديدية حقيقة هذا الأمر؛ ولذا تظل البيانات سلعًا ذات قيمة.

ولا تكون المعلومات المخزنة جميعها في نفس المكان في حال التخزين اللامركزي، وإنما توزع بين عدة مستخدمين لشبكة النظراء مع تولي المستخدمين مسؤولية حمايتها، ويعتمد التخزين اللامركزي على تقنية سلسلة الكتل، بينما لا يقضي هذا على المحاذير الأمنية بشأن هذا النوع من التخزين. وعلى الرغم من أن نتائج البيانات المتفاوتة تبدو أقل خطورة بسبب الوصول المحدود إلى كميات جزئية من البيانات فقط في حالة وقوع حادث أو اختراق للشبكة، فإن هناك عواقب أخرى، فعلى الرغم من كونها نماذج غير موثوق بها، فإن دعم الثقة في الشبكة للمستخدمين لأسماء مستعارة ممن يقومون بتشغيل الشبكة يواجه تحديات في العديد من قواعد المستخدمين، وينبغي للمستخدمين أن يكونوا حذرين تجاه الأشخاص القائمين على تشغيل نظام تخزين والمقدمين للخدمات ويواصلون الحذر تجاههم، فبإمكان الجهات الخبيثة إنشاء عقد خبيثة وإجراء التخفي كجزء فعلي من الشبكة، واكتساب ثقة المستخدمين مع عقد النية على الإضرار بالشبكة وسرقة البيانات، ويعد هذا الأمر سهلًا عند تطبيقه في تقنية الميتافيرس مع الأخذ بالاعتبار حداثة المساحة ونقص النماذج الراسخة التي توضح أيًّا من المشاركين يمكن الوثوق به لتوفير الخدمة وتخزين البيانات. فإن الجهات الفاعلة عبر الإنترنت لا توضح حقيقتها دومًا، كما يحدث تمامًا في الشبكة 2.0، وتتطلب الثقة في أي من الخدمات التي تحتاج إلى تخزين بيانات حساسة، للمزيد من البحث والحذر، كما يجب تنفيذ النزاهة لأشخاص متعددين ضمن خدمات التخزين اللامركزية، حتى لا تتمكن أيُّ جهة من الإشراف على أي عملية من شأنها المساس بنزاهة البيانات.

4. الاختراقات (Hacking)

رافقتْ أعمالُ القراصنةِ تلك التقنية في مهدها، محاولين بلا انقطاعٍ اختراقَ المصادقةِ واستغلالها ومراقبة الجهات بهدف الاستفادة من الشبكات وسرقة البيانات وترك بصمتهم الخاصة في العالم الرقمي، وتهدف هذه العمليات، التي يقومون بها، إلى الربح المالي، أو سرقة المواد الرقمية ونشرها في بلادهم، أو نشر رسائل

سياسية من خلال أعمال القرصنة تلك. وتشكل تقنية الميتافيرس باعتبارها المحطة التالية للتكرار الافتراضي للعالم الواقعي مطمعًا للقراصنة المسيرين بدوافع مختلفة. وتكون منصات الميتافيرس ومستخدموها عرضةً للقرصنة، وهو ما يدعو مسؤولي الأمن إلى أخذ ذلك بعين الاعتبار.

الاستيلاء على الحسابات (Account Takeovers)

تعتبر الشخصيات الافتراضية إحدى الطرق الأساسية للتفاعل والمشاركة في تقنية الميتافيرس، وقد تتعرض الشخصيات الافتراضية للخطر، مثلها مثل أي حساب يديره الأشخاص، ومن الصعب إدراك حسابات الشخصيات الافتراضية، وقد لا يكون هناك أي أخطاء إملائية في النص أو الصوت المستخدم من حساب الشخصيات الافتراضية، حيث تم القضاء على حاجز اللغة من خلال استخدام الذكاء الاصطناعي، أو عن طريق استخدام تقنية أخرى للترجمة، كما يستطيع التعرف على الحسابات المخترقة والمزورة والمسروقة وتحديدها مثل المنصات الأخرى، وقد يحتوي الحساب المسروق في تطبيق الميتافيرس على البيانات والبيانات الوصفية من حسابات الشخصيات الافتراضية وحسابات التسوق والبريد الإلكتروني والوثائق المعتمدة الأخرى، كما أن هناك بعض المعايير التي يمكن الاستعانة بها من الأمن السيبراني التقليدي، ومع ذلك ستقدم تقنية الميتافيرس تحديات خاصة بها بشأن سرقة الوثائق المعتمدة والحسابات المسروقة والجهات المزيفة وانتحال الشخصية وما إلى ذلك. ويقصد بالرؤية العامة للتشغيل المشترك واسع النطاق بين منصات الميتافيرس أن يعرض أحد الحسابات المخترقة من ألعاب تقنية الميتافيرس الحسابات والشخصيات الافتراضية ومعلومات شخصية مستخدمة في حسابات ميتافيرس أخرى للخطر.

البرامج الخبيثة وبرامج الفدية (Malware and Ransomware)

باستطاعة الجهة الخبيثة وبضغطة زر بسيطة الوصول إلى الشبكة وتحديد نطاق المعلومات المتاحة وقيمتها، ومن ثم سرقة البيانات وتشفيرها ومنع الوصول إليها، وتوجد هجمات البرامج الخبيثة على مستوى منطقة الشرق الأوسط وشمال إفريقيا (Harika and Campbell, 2022)، وتستهدف الإمارات المتحدة والمملكة العربية السعودية والكويت وعمان والبحرين من بين الآخرين، كما أوضح محللو التهديدات السيبرانية بأن منطقة الشرق الأوسط وشمال إفريقيا تتذيل المناطق المستهدفة على مستوى العالم للبرامج الخبيثة، فإنها ما

زالت تتعرض لحوادث من هذا النوع وتحتاج إلى الحماية منها. وعلى الرغم من انتشار هجمات البرامج الخبيثة على مستوى العالم في العقد الماضي، فإن العديد من الجهات ما زالت بحاجة إلى ملفات نسخ احتياطية.

وللمنظمات التي تتعامل بتقنية الميتافيرس إعداد نفسها لمثل تلك الحوادث السيبرانية غير النهائية من خلال الحصول على نظام حديث للنسخ الاحتياطية تتمكن من خلاله من استعادة البيانات واستكمال العمليات، وتكون حوادث البرامج الضارة والخبيثة متوقعة في تقنية الميتافيرس، ويمكن أن تتسبب في تعطيلها، مثل: إيقاف الأنظمة الصحية الأساسية غير المتصلة بالإنترنت، والتهديدات بكشف المعلومات الشخصية، وابتزاز كل من الشركات والضحايا لجمع الأموال بغرض استعادة المعلومات المشفرة، شأنها كشأن المعوقات التي تحدث في العالم المادي. وقد تؤدي البرامج الخبيثة إلى توقف الوصول إلى الرموز غير القابلة للاستبدال ومنعه، أو إلى أي أصول رقمية ذات قيمة، وينبغي إمعان النظر في حقيقة أن الجهات الخبيثة قادرة على نشر برامج ضارة في منتديات المحادثات أو منصات وسائل التواصل الاجتماعي، وقد تستمر مجموعات البرامج الخبيثة في توجهاتها الخاصة بالابتزاز المزدوج والثلاثي والرباعي؛ لترغم المبدعين أو منتجي المحتوى أو مستخدمي تقنية الميتافيرس بالدفع من أجل استعادة إمكانية الوصول إلى أعمالهم وأصولهم وغيرها، وقد تؤدي البيانات الناتجة عن تجربة التسوق إلى الوصول للمقامرة أو التسلية أو التلاعب بالحسابات، وهو ما يعني تعرض البائعين ومقدمي خدمات الشبكة للابتزاز والتورط في الاتجاه المتنامي الدائم للابتزاز عن طريق البرامج الخبيثة.

وكما هو الحال في تقنية الميتافيرس، فإن هجمات البرامج الخبيثة ليست لها حدود، حيث شهدت منطقة الشرق الأوسط وشمال إفريقيا نصيبًا من تلك الأحداث، وتشمل مجموعات برامج الفدية التي تستهدف الإمارات العربية المتحدة Egregor, LockBit 2.0, Conti, Snatch, DarkSide, REvi, BlackByte, Xing, AvosLocker, Avaddon, Rook, and Pysa، ودائمًا ما اسْتُهْدِفَت المملكةُ العربية السعودية بهذه البرامج الخبيثة، كما شهدت الكويت وعمان والبحرين هجمات تلك البرامج دون معرفة المُستهدف. كما أوضح محللو التهديدات السيبرانية أن منطقة الشرق الأوسط وشمال إفريقيا تتذيل المناطق المستهدفة على مستوى العالم في هجمات البرامج الخبيثة، فإنها ما زالت تتعرض لحوادث من هذا النوع وتحتاج إلى الحماية منها. وتهدف هجمات البرامج الخبيثة التقليدية إلى اختراق نظام ما، حيث تسرق الجهات البيانات الحساسة، ومن ثم تشفرها وتطلب أموالًا من الضحية لاستعادة إمكانية الوصول، ويكون الابتزاز المزدوج عبارة عن قيام الجهات الخبيثة بأداء هجمات تقليدية وتشفير للبيانات، ومع ذلك، في حال استعادة المنظمة بياناتها من خلال النسخ الاحتياطية دون دفع المبلغ المطلوب، تهدد حينها الجهات الخبيثة ببيع تلك البيانات على المنتديات الإجرامية،

أو بيعها من خلال عمليات تقديم العطاءات أو منع الوصول للبيانات المسروقة في حالة عدم الدفع (Amos, n.d)، وبذلك تظل سمعة المنظمة في خطر عند اكتشاف حادث أمني. وفي حال كان باستطاعة المنظمة إنقاذ عملية الوصول للبيانات بطريقتها الخاصة، تطالب حينها الجهات الخبيثة بالدفع مقابل التزام الصمت فيما يتعلق بتلك الأحداث، ويكون الابتزاز الثلاثي عبارة عن نفس العملية المذكورة سابقًا (الطبقة الثالثة من الابتزاز) مضافًا إليها التهديدات (بما في ذلك هجوم حجب الخدمة الموسع لتهديدات البرامج الخبيثة، ويضمن هجوم حجب الخدمة الموسع مستوى إضافيًّا من الفوضى وحجم الخدمات وسرقة البيانات الحساسة وتشفيرها. ويتضمن الابتزاز الرباعي جميع ما سبق ذكره، بالإضافة إلى تهديد الجهات الخبيثة بالتواصل المباشر مع شركاء المنظمة أو عملائها، كما يُهَدِّد السمعة ويُعَرِّض الجهةَ، التي تم اختراقها، للمساءلة.

انتهاك الملكية الفكرية (Intellectual Property Theft)

تعتبر الملكية الفكرية سمةً من السمات لدى كل من تقنية الميتافيرس والواقع المادي، كما تتوافر إمكانية تطوير المحتوى الأصلي في تقنية الميتافيرس من قِبَل المستخدمين، وذلك من خلال ازدهار مجال كتابة النصوص الترويجية في مجالات، مثل: الرموز غير القابلة للاستبدال (Intellectual Property, 2022). وعلى ذكر المخاطر المتعلقة بالقرصنة، فإن الميتافيرس قد تتسبب في إتاحة فرص سرقة الملكية الفكرية؛ نظرًا لطبيعة نطاق العالم الافتراضي، وتعتبر سرقة الملكية الفكرية ثغرة أمنية ذات تداعيات واسعة النطاق؛ ففي غياب تدابير وقائية وأمنية، يمكن أن تفقد الدول العربية الميزة التي كانت تتمتع بها من إنشاء محتوى جديد حتى مع وجودها ضمن حدودهم (الطبيعية).

إن الدعوات إلى تنظيم حقوق ملكية فكرية في الدول العربية ليست وليدة اللحظة (Alobaid, 2021)، ومع ذلك ينبغي تكثيفها مع تبني تقنية الميتافيرس في المنطقة، ولا ينبغي للحملات الداعية لاعتماد بعض مراحل التشغيل المشترك بين الدول أثناء تخطيها لتلك التحديات التي تواجه النظام الافتراضي أن تذهبَ سُدًى، وتحكم أنظمة الملكية الفكرية الحالية ملكية العناصر غير المادية للملكية الخاصة؛ ونظرًا لأن الأنظمة الحالية للملكية الفكرية مصممة بصدد تنظيم جوانب الموجودات «غير الملموسة»، فهي تمنح إطار عمل قائم يفصل من خلاله في مسألة الملكية في الميتافيرس (Ramos, 2022). وعلى نفس المنوال الذي تستوحي به قواعد الخصوصية للبيانات المؤسسية للدول العربية لتقنية الميتافيرس من النظام الأوروبي العام لحماية البيانات، يمكن الاستفادة من إطار العمل القائم للتحكيم من الهيئات الدولية، مثل: منظمة التجارة العالمية من أجل

تبنيهم تقنية الميتافيرس.

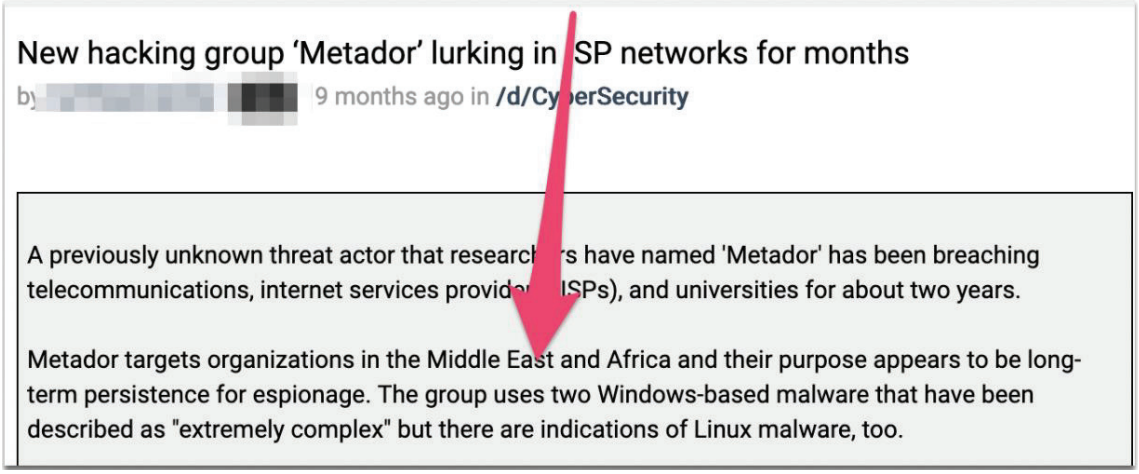
التعدين غير الشرعي للعملات المشفرة (Illicit Crypto-Mining)

يعتبر تعدين العملات المشفرة (عملية التحقق من المعاملات وإضافتها إلى دفتر سلسلة الكتل) هو جزء تكميلي للعديد من العملات المشفرة، ومع ذلك يمكن تعدين العملات المشفرة بطريقة غير مشروعة، وغالبًا ما يتم من خلال استخدام غير مصرح به لموارد حاسوبية لمستخدم آخر (Russo et al., 2022). ويعزو كون تقنية الميتافيرس تكرارًا جديدًا لأنشطة تعدين البيتكوين غير الشرعي، للمستوى العالي من مشاركة المستخدمين بالإضافة إلى التكنولوجيا القوية. وقد يتخذ تعدين العملات المشفرة غير الشرعي صورًا متعددة في الميتافيرس، فعلى سبيل المثال، يمكن تضمين البرامج الضارة ضمن موضوعات أو بيئات في الميتافيرس، وذلك دون علم المستخدمين. وقد يؤدي التعامل مع تلك العناصر المصابة إلى تثبيت برامج تعدين العملات المشفرة على جهاز المستخدم، محولًا بذلك القدرة الحاسوبية لتخضع لهجوم تعدين العملات الرقمية (Joint Counterter-rorism Assessment Team, 2021).

ونظرًا للطبيعة التفاعلية والغامرة للميتافيرس، يقضي المستخدم فترة طويلة من الوقت على تلك التقنية، فيمكن لمستخدمي تعدين العملات المشفرة غير الشرعي أن يحصلوا على مصدر مستمر ومستقر للقدرة الحاسوبية، وقد يتعارض نموذج الاستخدام الموسع مع استخدام تصفح الويب التقليدي أو التطبيقات، التي تميل لأن تكون أكثر تشتتًا. ومما يزيد المشكلة تعقيدًا وجود اللامركزية والطبيعة العالمية للميتافيرس، والتي تجعل الأمر يشكل تحديًا لتطبيق اللوائح أو القيام بإجراءات قانونية ضد من يقومون بتعدين العملات المشفرة غير الشرعي، وقد يؤدي التنظيم غير المتسق بين الولايات القضائية وميزات إخفاء الهوية إلى توفير ملاذات آمنة للمشاركين في هذه الأنشطة.

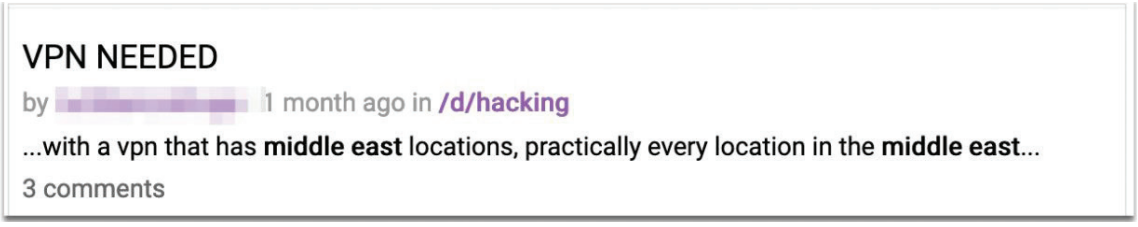
وللتصدي لتلك المشكلة، فيتعين اتخاذ تدابير أمنية قوية وأدوات مراقبة في الميتافيرس للكشف عن الأنشطة الخبيثة ومنعها. ويلزم تثقيف المستخدمين وتوعيتهم بالمخاطر وتزويدهم بالإستراتيجيات اللازمة لحماية أجهزتهم وأصولهم الرقمية. وفي نهاية المطاف، على المطورين والبائعين والمنظمين والمستخدمين التعاون فيما بينهم لضمان إبقاء مساحة الميتافيرس آمنة ومنصفة وبعيدة عن الاستخدام السيئ للموارد واستغلالها.

تُصَوِّرُ الأشكال من 1 إلى 4 أمثلة للنشاط الإجرامي الذي يواجهه هذا المجال في المنطقة.



الشكل 1 - يوضح حملة تستهدف مزودي خدمات الإنترنت والاتصالات السلكية واللاسلكية. منصة دريد المتاحة على (Dark Web, 2023).

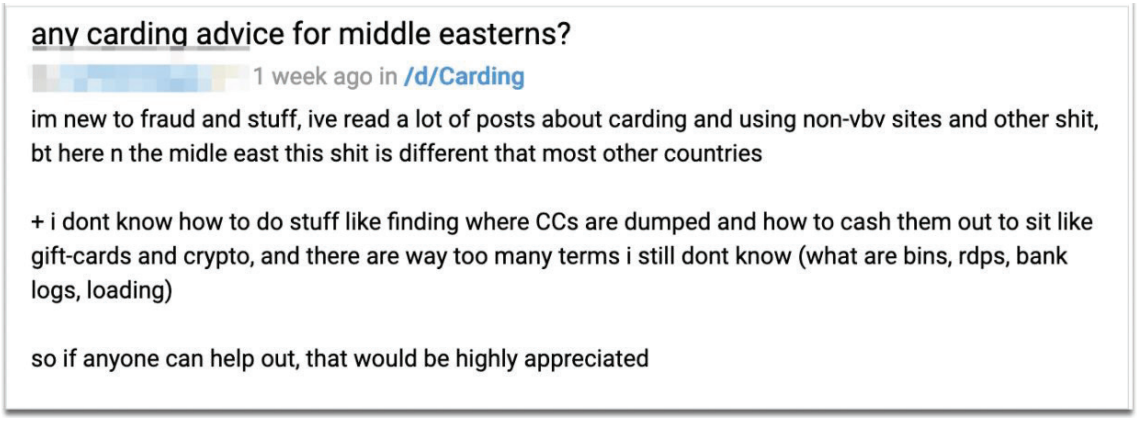
يوضح الشكل (1) إحدى الجهات الفاعلة في منتدى دريد (Dread) المظلم، المشابه لموقع ريديت (Reddit)، تفاصيل بشأن حملة تستهدف على وجه التحديد مزودي خدمات الإنترنت والاتصالات السلكية واللاسلكية في جميع أنحاء الشرق الأوسط. وعلى الرغم من ندرة حدوث ذلك، تتمتع الجهات الفاعلة، التي يمكنها الوصول إلى البنية التحتية الأساسية الحساسة والموارد الرئيسة أو الأساسات التقنية المحورية، بمعدلات نجاح أعلى في تنفيذ أنشطتها الخبيثة.



الشكل 2 - يوضح حاجة الجهات الفاعلة في منتدى دريد المظلم إلى شبكة افتراضية لاستخدامها (Dark Web, 2023)

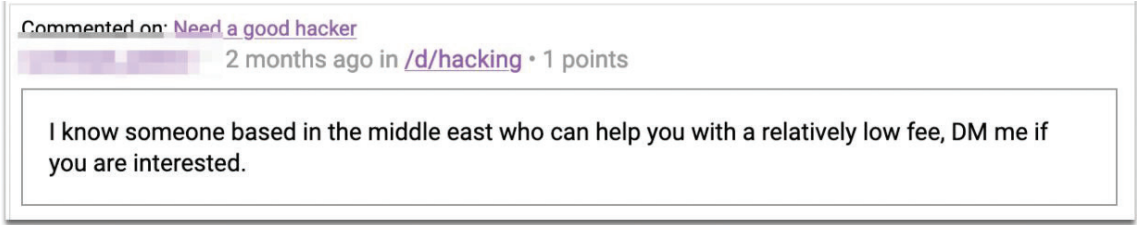
تحتاج إحدى الجهات الفاعلة في منتدى دريد (Dread) المظلم، المشابه لموقع ريديت (Reddit)، إلى شبكة افتراضية خاصة بغرض استخدامها في منطقة دول الشرق الأوسط، وحينئذٍ يمكن للجهات الفاعلة الاندماج في حركة المرور العادية على الإنترنت، وتجنب حصر أدوات مكافحة الفيروسات والأمن السيبراني لها؛ حيث

يسمح استخدام شبكة افتراضية خاصة خارج منطقة الشرق الأوسط أو عدم استخدامها بإمكانية الكشف المبكر وعرقلة الجهات الفاعلة الخبيثة ومكافحة أنشطتها، وتعد هذه المسألة الأمنية شديدة الأهمية.



الشكل 3 - يوضح حاجة الجهات الفاعلة في منتدى دريد المظلم (Dread) إلى المشورة الخاصة بكيفية إجراء الحملات التنشيطية (Dark Web, 2023)

تطلب إحدى الجهات الفاعلة في منتدى دريد (Dread) المظلم، المشابه لموقع ريديت (Reddit)، المشورة والأساليب الخاصة بكيفية إجراء الحملات التنشيطية. وتختلف الأساليب والتقنيات والإجراءات التي يستخدمها قراصنة الإنترنت من منطقة إلى أخرى، وهذا دليل على أهمية التعاون بشأن استخدام المنصات الإلكترونية في الأنشطة الإجرامية، حيث ينمو ذلك النوع من الأنشطة والصلات القائمة بين الشبكات الإجرامية في الميتافيرس فقط.



الشكل 4 - يوضح بحث إحدى الجهات الفاعلة في منتدى دريد المظلم (Dread) عن مخترق (Dark Web, 2023)

حيث تبحث إحدى الجهات الفاعلة في منتدى دريد (Dread) المظلم، المشابه لموقع ريديت (Reddit)، عن مخترق، وتُظهر استجابة شخص ما في الشرق الأوسط تمتعه بمهارات لغوية أجنبية ومعرفته بسياسات الأمن في منطقة الشرق الأوسط

5. الإرهاب الإلكتروني (Digital Terrorism)

يُصاحِبُ ظهورَ الميتافيرس أبعادٌ جديدةٌ في الإرهاب والحرب الإلكترونية. فيمكن أن تصبح الدول والشركات المستثمرة في هذه البيئات الافتراضية والعاملة فيها أهدافًا جذابةً للتهديدات الصادرة عن الجهات الفاعلة الحكومية والمناهضة للحكومة. ويعد استخدام الجهات الفاعلة للميتافيرس بغرض التجسس واحدة من التهديدات المهمة. ونظرًا لعمق وتنوع الأنشطة التي يمكن تنفيذها عبر الميتافيرس من خلال الاجتماعات التجارية والسياحة الافتراضية، فيمكن أن يكون مقدار البيانات الحساسة المتاحة هائلًا، وقد تكون تلك البيانات هدفًا لجواسيس الإنترنت، الذين يسعون إلى الحصول على المعلومات أو إلحاق الضرر.

ويثير التخريب مصدر قلق آخر، حيث يمكن أن تسعى الجهات الفاعلة إلى تعطيل عمل الميتافيرس نفسه، وهو ما سيؤثر في الاقتصادات الافتراضية والبنية الاجتماعية والعمليات التي تعتمد عليه. وقد يشمل ذلك أيًّا من الهجمات المستهدفة على بيئات الميتافيرس المحددة والاضطرابات واسعة النطاق في البنية التحتية الأساسية للميتافيرس، ويمكن أن يكون لهذه الأنواع من الهجمات تأثير فعلي على العالم، ولا سيما إذا اعتمدت المنظمات اعتمادًا كبيرًا على الميتافيرس في عملياتها. كما قد يكون الميتافيرس بمثابة منصةٍ للحرب النفسية وحملات التأثير. وقد تتمكن الجهات الفاعلة من خلق روايات مقنعة أو التلاعب بحشود افتراضية أو حتى انتحال صفة شخصيات مؤثرة مستغلةً طبيعة الميتافيرس الغامرة، وبوسعهم استخدام هذه الأساليب لتوجيه الرأي العام أو إثارة الاضطرابات أو خلق الانقسامات داخل الميتافيرس أو خارجه.

وعلاوة على ذلك، قد تُصَعِّبُ إمكانيةُ عدم كشف الهوية في الميتافيرس من إسناد مثل هذه الهجمات، حيث بإمكان الجهات الفاعلة إخفاء هويتها بسهولة أو حتى الصاق التهمة بآخرين، وهو ما يخلق غموضًا وعدم يقين. وستتطلب معالجة هذه التهديدات نهجًا شاملًا من التدابير الأمنية القوية وتعاونًا دوليًّا وإطارًا قانونيًّا وتنظيميًّا جديدًا إذا اقتضت الضرورة ذلك. وينبغي على المطورين والمستخدمين والمسؤولين والسياسيين التعاون معًا لضمان أمان مساحة الميتافيرس ومقاومة التهديدات التي تفرضها الحرب الإلكترونية.

التجنيد والدعاية (Recruiting and Propaganda)

استغلت الجماعات الإرهابية خصائصَ التقنيةِ التي تسمح باستعمال الأسماء المستعارة منذ نشأتها، إنشاء شخصيةً وهميةً لخدمة كافة أغراضها بما فيها الخبيثة. كما توجد بالفعل منتديات متطرفة على كل من الشبكة السطحية والمظلمة وبعض المنصات، مثل: Gab و4chan المحرضة صراحةً على العنف والدعاية،

وامتلاك مجموعات تتجاهل حقوق الإنسان الأساسية، التي تمتلك حسابات على تويتر ووسائل التواصل الاجتماعي الأخرى النشطة. ولا مفر من وجود ذات الوضع في الميتافيرس، فستنطلق جهود للتجنيد والدعاية حتى إن طُبقت شروط الخدمة. وقد يظهر ذلك كله في صورة مناطق افتراضية حصرية لمجموعات دينية معينة تبحث عن نشر رسالة ونظرة عالمية معينة.

ولا بد من معرفة أن الميتافيرس يُمثل النسخة المقبلة من المساحة العامة. ويوفر الميتافيرس مساحةً مناسبةً لممارسة الأنشطة الديمقراطية، حيث تواجه بعض الشعوب صعوبات في ممارسة الأنشطة المدنية، ولكن ستحظى المجموعات الإرهابية التي تسعى إلى إثارة الفوضى في الأماكن العامة الافتراضية بفرصٍ لاستهدافِ هذه الأنشطة في الميتافيرس كقواعد للتجنيد ومناطق لنشر الدعاية بأسلوب تكتيكي.

وبالإضافة إلى ذلك، يُمكن لمؤلفي مختلف الأوراق البحثية والكتب والمدونات ومقاطع الفيديو وغيرها استضافةُ مساحتِهم الخاصةِ في الميتافيرس، واستخدام التجربة الغامرة العميقة بشكلٍ مماثلٍ للتأثير في مختلف مشاعر وحواس جمهورهم بهدف زيادة جهود التجنيد. ويمكن أن تظهر الدعاية في شكل مقتنيات حصرية أو أصول رقمية أخرى بصحبة مسابقات أو جهود أخرى معتمدةً على الألعاب تؤدي إلى انتشار الدعاية. كما قد تظهر كتيبات إرشادية لتعليم صناعة القنابل والأسلحة والحصول على الوثائق السرية بشكلٍ غير قانوني وتعليمات لإجراء عمليات قرصنة خبيثة في الميتافيرس وبيعها أو جمعها في الميتافيرس. وسيتم مراقبة منصات الميتافيرس وتعديل شروط الخدمة الخاصة بها لمكافحة التجنيد والدعاية. وقد يشمل ذلك مراقبة الكلمات الرئيسة أو إرسال ضباط إنفاذ القانون إما بشكل سري أو صريح إلى رعاة الإرهاب والإرهابيين المشتبه بهم وإلى مناطقهم.

وينظر المدافعون عن التقنية إلى الميتافيرس كمكان يسع فيه للناس تعلم استخدام نماذج ثلاثية الأبعاد وعمليات المحاكاة بسهولة أكبر واكتساب «الممارسة العملية» وصياغة المهارات باستخدام المستشعرات والقفازات في تجربة غامرة، ولكن للأسف، فإن ذلك يُطبق أيضًا على تعلم المهارات الخبيثة، حيث يمكن أن تقع طرق بناء الأسلحة في أيدي أشخاص يرغبون في تعزيز أيديولوجيات متطرفة بدءًا من صناعة الأسلحة إلى كتابة أدلة حول كيفية تنفيذ هجوم جسدي ومحاكاة هذا الهجوم من خلال الميتافيرس.

ومن المؤسف أن يؤدي استخدام التقنية للتجنيد ونشر أيديولوجيات إلى الإضرار بحقوق الإنسان. ويوفر الميتافيرس المترابط منصةً للمراقبة تسمح لدعاة الإرهاب بإجراء جهود التجربة والخطأ لإنشاء منصات من شأنها السماح بنشر أيديولوجيتهم والوصول إلى الشباب المعرض للخطر، وتعزيز رسالتهم داخل المجتمعات الشعبية، وتطويع خطابهم؛ لتبقى خارج نطاق المشرفين ومطبقي القانون. إنها معركة مستمرة لمحاربة

التهديدات الخبيثة وزيادة الوعي بها في الميتافيرس؛ رغبةً في منع جميع المتطرفين من استخدام ميزات النظام الافتراضي لتمويل أهدافها.

تمويل الإرهاب (Terrorism Funding)

يلزم دومًا التحقيق في التفاعلات المجهولة في العالم الرقمي وتقييمها عن كثب، ولا يُستثنى من ذلك تلك التفاعلات المطالبة بالمال مقابل التفاعل. وقد تُجمع الأموال لأي غرض سواء أكان لغرض خيري أم إنساني، ولكنها في النهاية تدعم الإرهاب أو سلسلة التوريد الخبيثة. ويعد تعقب الأموال جهدًا معروفًا في الدوائر الأمنية، وسيتعين مواصلة تَتَبُّعِهِ ومراقَبَتِهِ في الميتافيرس. وقد تُستخدم أدوات تحليل الذكاء الاصطناعي وسلسلة الكتل لِتَتَبُّعِ وتقييمِ أنواعٍ معينةٍ من المعاملات، والمساعدة في تحديد ما إذا كانت وجهة الأموال راعيةً للإرهاب أم لا. وعند شراء أصول رقمية لمنصة ميتافيرس مشكوك بها، أو عند تكرار طلب منصة معروفة في الميتافيرس بتأييد الإرهاب أو الدعوة إلى التطرف بالتبرع بالأموال، فيلزم اعتبارها علامةً حمراء، وسيكون على الجهات الرقابية المالية وجهات إنفاذ القانون التعاون مع مشغلي منصات الميتافيرس والبائعين للتدخل.

وستختلف تدخلات جهات إنفاذ القانون أو الجهات الرقابية في الميتافيرس عن الممارسات المتبعة في التمويل التقليدي. ولا تقبل معاملات التشفير في الميتافيرس التجميد بسبب إضفاء الطابع الديمقراطي أو المركزي لتقنية سلسلة الكتل. وبدلًا من ذلك، يحدد المحققون العناوين التابعة لجهات التهديد أو الكيانات الخاضعة للعقوبات باستخدام برنامج ذكاء تقنية سلسلة الكتل. ثم تُنشر هذه التسميات على مستكشفات سلسلة الكتل؛ وهي برامج تُصَوِّرُ التعاملات والعناوين التي تمت بها المعاملات وغيرها من شبكات قياسات سلسلة الكتل. وتقوم منصات العالم الافتراضي وتطبيقات المحفظة الشهيرة، وهي التطبيقات التي يستطيع المستخدم من خلالها طلب المعاملات، بدمج معلومات التسمية من مستكشفات سلسلة الكتل وتحذير المستخدمين من هوية أي عنوان ضار يحاول المستخدم التفاعل معه. وسيتعين على المستخدمين توخي الحذر عند التفاعل مع هذه الكيانات، حتى لو عن طريق الخطأ، فقد يؤدي ذلك إلى عواقب وخيمة في العالم الافتراضي والحقيقي.

التهديدات المناهضة للحكومة (Non-State Threat Actors)

يجب أن تتوقعَ السلطاتُ وجودَ جهودٍ إجراميةٍ مزدهرةٍ في العالم الافتراضي، مثل: شبكات الإنترنت المظلمة والعميقة (DDW)، فبالتأكيد، ستُنشئ الجهات الفاعلة، سواء أكانوا مدعومين من الدولة أو غير ذلك من

الكيانات، عقارات افتراضية في العالم الافتراضي لبيع البرامج الضارة، مثل: برامج الفدية وخدمة برامج الفدية (RaaS) والفيروسات وغيرها من البرامج الضارة، ويُطلق حاليًّا على هذا المكان الناشئ اسم الدارك فيرس (Darkverse). وتنتشر البرامج الضارة داخل الأنظمة وأجهزة الحاسوب كانتشار الفيروسات في العالم المادي. وسيكون الميتافيرس بيئةً خصبةً لنشر البرامج الضارة وغيرها من الكيانات. كما أنه من المرجح أن يتبع نفس اتجاه وسائل التواصل الاجتماعي، ويسهم في المنصات المستخدمة في عمليات التضليل ونشر المعلومات المضللة.

وبالنظر في المعلومات المادية التي تحاول الجهات الفاعلة الخبيثة جمعها عن الأهداف: فهنالك قيمة في كل شيء ابتداءً من أرقام الرحلات الجوية وغرف الفنادق، إلى الدول التي تُسجل فيها السفن ونظام تحديد المواقع العالمي للسيارات الذي يكشف عن الموقع الدقيق... إلخ. وتكون الجهات الفاعلة من الدول الوطنية وقراصنة الإنترنت على علم بتوافر الكثير من البيانات الشخصية الحساسة الجديدة المصاحبة لإنشاء الميتافيرس، وتشمل هذه البيانات المعلومات البيومترية والمواقع وأنواعًا جديدةً من معلومات المستشعرات والشبكات. وتستهدف الجهات الفاعلة البنية التحتية الجديدة لتوجيه عملياتها وأولوياتها واستخدامها لتعزيز أهداف الدول التابعة لها. ولهذا السبب، تُشَكِّلُ البياناتُ المستخدمةُ في الوصول إلى الميتافيرس والتفاعل معها مشكلةً كبيرةً للأمن الوطني ويجب معالجتها بسرعة. ومن المرجح أن تزدهر الجهات الفاعلة غير الحكومية في الميتافيرس تمامًا كما تفعل في العالم المادي وفي العالم الرقمي في عالمنا المعاصر. كما سيعزز الميتافيرس أو الدارك فيرس (Dark-verse) الناشئُ المجتمعاتِ الإلكترونيةَ الخاصةَ بالجهات الفاعلة الخبيثة التي تُجري جميع أنواع الأنشطة غير القانونية، مثل: الاحتيال والابتزاز وبيع المخدرات وبرامج التجسس وطلب الفدية. وكل هذه مشكلات قائمة تتعامل معها جهات إنفاذ القانون اليوم، وتكمن المشكلة في كيفية إنشاء هيئة استجابة عالمية بإمكانها مراقبة الجهات الفاعلة الخبيثة ومحاولة اعتراض نشاطها وتفريق أماكن تجمعها ومنع ازدهارها.

6. الجريمة السيبرانية (Cyber Crime)

الاحتيال (Scams)

من المُرَجَّح أن يكون الميتافيرس أرضًا خصبةً للمحتالين عند توسعه ونضجه. ويمكن أن تصبح العملات الافتراضية الجديدة والممتلكات الرقمية وغيرها من الأصول الافتراضية أهدافًا للاحتيال. كما تضر عملية الاحتيال نظام سلسلة الكتل بأكمله. ويعد رمز الاستجابة السريع (QR) ظاهرةً حديثةً ومثالًا ممتازًا على التهديد الهجين المادي والرقمي. وقد ظهر رمز الاستجابة السريع المزور على رسائل البريد الفعلي والتصيد الاحتيالي عبر البريد

الإلكتروني. كما ظهر رمز الاستجابة السريع على عدادات مواقف السيارات في المدن والمطاعم. ويسمح مسح رمز الاستجابة السريع المزور للمخترقين بإصابة أي جهاز شخصي بالفيروس، ومن ثم إعادة توجيه إرسال الأموال أو المعلومات الشخصية مباشرة إلى أيدي المحتالين بدلًا من الوجهة المقصودة لرمز الاستجابة السريع. وبناءً على ذلك، سيكون وضع رمز الاستجابة السريع في الميتافيرس هدفًا للمحتالين أيضًا؛ لذا يلزم تصميم عملية تحقق. كما قد أنشأت منصات التطبيقات الرئيسة تطبيقاتٍ تُركِّز على ضمان أمان رمز الاستجابة السريع، ويجب تطبيق هذه التقنية كذلك في العالم الافتراضي. وتتضمن الأنماط الأخرى لعمليات الاحتيال بيع الممتلكات أو السلع الافتراضية غير الموجودة أو التي لا تخص البائع أساسًا. وقد يكون من الصعب تنظيم هذا النمط من الاحتيال ومنعه بسبب الطبيعة الفريدة لملكية الأصول الرقمية في الميتافيرس. كما قد تظهر عمليات احتيال استثمارية يقوم الأفراد فيها بترويج فرصٍ استثماريةٍ مزيفةٍ داخل الميتافيرس. فعلى سبيل المثال، قد يَعِدُ هؤلاء الأفراد بتحقيق عوائد مالية عالية على الاستثمارات في العقارات الافتراضية أو الأعمال التجارية الافتراضية أو الأصول الرقمية الأخرى. كما يمكن أن تتخذ مخططات «بونزي» أو المخططات الهرمية أشكالًا جديدة في الميتافيرس، مستفيدةً من الميزات والفرص الفريدة لهذا العالم الافتراضي لإغراء المشاركين والاحتيال عليهم.

وتعد عملياتُ احتيالِ «سحب البساط» أكثر أنماط تلك العمليات شيوعًا ممثلةً بذلك تهديدًا كبيرًا على الميتافيرس. وتتضمن عملية احتيال سحب البساط (التي نشأت في مجال التمويل اللامركزي) عادةً تخلي المطورين أو المروجين عن المشروع والاختفاء بأموال المستخدمين. ويعني ذلك في سياق الميتافيرس قيام مجموعة من مُنْشِئِي الأصول الرقمية أو الأراضي الافتراضية أو حدث جديد بإغراء المستخدمين للاستثمار في أموالهم أو أصولهم الافتراضية، ومن ثم الاختفاء فجأة وترك المستثمرين مع أصول لا قيمة لها. وقد تُزَعْزِعُ مثلُ هذه العمليات ثقةَ المستخدمين وتُعَرْقِلُ تطورَ الاقتصادِ في الميتافيرس، وتثني الوافدين الجدد عن المشاركة في الاقتصاد الافتراضي الجديد. وبالتالي، فستكون الآليات القوية للتحقق من شرعية المشاريع والاستثمارات ضروريةً لحماية المستخدمين والحفاظ على سلامة اقتصاد الميتافيرس.

غسل الأموال (Money Laundering)

أدى الارتفاع الدولي لخدمات الدفع الرقمية على مدار العقدين الماضيين أو نحو ذلك إلى زيادة مخاطر الجرائم المالية للبنوك والشركات الأخرى، مع كون ممارسات غسل الأموال جزءًا متوقعًا من تدابير الحماية وإجراءاتها لهذه المؤسسات (مثل: ميكلسن Mikkelsen وغيرها). وقد جَنَّدَت بعضُ المؤسساتِ استخدامَ

تقنيات التعلم الآلي لمكافحة غسل الأموال (مثل: كومار Kumar وغيرها). ويمكن لدول مجلس التعاون الخليجي أن تَتَوَقَّعَ التهديدَ الكامنَ خلف غسل الأموال للميتافيرس، حيث يوفر نظام الميتافيرس مساحةً جذابةً بشكلٍ خاصٍّ لجهود نقل الأموال غير المشروعة من موقع فعلي إلى آخر داخل هذا العالم.

ويُعَزِّزُ تهديدُ غسلِ الأموال ضرورةَ إنشاءِ جهةٍ رقابيةٍ مشتركةٍ بين دول مجلس التعاون الخليجي بشكل ملحوظ؛ فغالبًا ما يكون غسل الأموال وسيلة مجدية للحفاظ على الأنشطة الإجرامية التي تؤثر في المنطقة، ومن بينها الإرهاب. وعليه، فإننا نؤكد ضرورة وجود إجراءات مشتركة لتنظيم نقل الأصول الافتراضية، ونسلط الضوء على هذا الخطر كمثال رئيس على كيفية استخدام الميتافيرس في مثل هذه الجرائم كغسل الأموال والإرهاب بطرق جديدة.

7. التضليل ونشر المعلومات المغلوطة (Misinformation and Disinformation)

الميتافيرس عرضةٌ لخطر انتشار المعلومات المغلوطة كما في شبكة الإنترنت في وقتنا الحاضر، ويُقصد بالمعلومات المغلوطة إنشاء ومشاركة المعلومات الكاذبة عمدًا بقصد الخداع أو التضليل. وقد تكون حملات المعلومات المضللة أكثر فاعلية بسبب الطبيعة الغامرة للبيئة الافتراضية. كما يمكن تقديم الروايات الكاذبة بطرقٍ أكثر جاذبية وإقناعًا باستخدام مجموعة متنوعة من أشكال وسائل الإعلام والعناصر التفاعلية. وعلاوة على ذلك، قد تؤدي ميزات الميتافيرس الاجتماعية والتفاعلية إلى توسيع مدى انتشار المعلومات المضللة. فعلى سبيل المثال، يُمكن للجهات الفاعلة التلاعب برأي الشعوب عن طريق خلق حشودٍ من الشخصيات الافتراضية لمحاكاة الدعم الشعبي للروايات الكاذبة. كما يمكن للجهات الفاعلة الخبيثة استغلال تقنية التزييف العميق في الميتافيرس لخلق سناريوهات كاذبة، وفي ذات الوقت واقعية للغاية، أو انتحال شخصية من العالم الحقيقي، مُعَقِّدًا بذلك مشكلة المعلومات المضللة. ويمكن بسهولة إقران هذه التقنية مع نماذج اللغة الكبيرة (هي نماذج حاسوبية تستخدم تقنيات الذكاء الاصطناعي والتعلم العميق لفهم وإنتاج اللغة الطبيعية) وأنظمة الذكاء الاصطناعي المولدة الأخرى المتاحة لتعزيز واقعية السيناريوهات والروايات الكاذبة.

ويوفر الميتافيرس كذلك فرصًا فريدةً للعمليات المعلوماتية وحملات التأثير. ولا تستطيع بعض الجهات الفاعلة، مثل: الجماعات الإرهابية وغيرها من الجماعات المتطرفة، نشرَ الدعاية والمشاركة في جهود التجنيد في الميتافيرس فحسب؛ بل بإمكانها الاستفادة كذلك منه لاستخدام المعلومات المغلوطة دون النية الحصرية للتجنيد. كما يمكن لتلك الجهات الخبيثة استغلال قوة الميتافيرس لنشر المعلومات المغلوطة وغرس بذور

الشقاق والتلاعب برأي الجمهور أو حتى التجسس على مستوى الشركات أو الدولة. وتُشَكِّلُ الشخصياتُ الافتراضيةُ الخادعةُ والزائفةُ حجرَ الأساسِ لمثل تلك العمليات. ونظرًا لأن الميتافيرس يسمح للمستخدمين بإنشاء شخصيات افتراضية قابلة للتعديل بالكامل، فسيصبح من السهل على الجهات الفاعلة الخبيثة تمثيل هويتها أو نواياها بشكل خاطئ. كما يمكنها إنشاء مختلف الشخصيات لمحاكاة الأفراد أو المنظمات أو حتى الحشود في العالم الحقيقي، مُضاعفةً بذلك تأثير حملات التأثير.

ويمكن للجهات الفاعلة من الدول الوطنية وقراصنة الإنترنت البدء بجهود في مجال الحرب الإعلامية في الميتافيرس، مستخدمين المجتمعات الافتراضية لحشد الدعم لمختلف القضايا والدعوة إلى القرصنة. كما قد تستهدف مجموعةٌ معاديةٌ شركةً أو منظمةً أخرى في محاولةٍ لجمع المعلومات أو بيانات اعتمادٍ من أعدائهم المفترضين لإساءة استخدامها. وقد يُعَزِّز الصراعُ الرقميُّ، بمساعدة الشخصيات الافتراضية والطرق الأخرى التي تسهل استخدام الاسم المستعار في الميتافيرس، من الصراعات المادية. ويُعرب الميتافيرس عن استعداده لذلك طارحًا عدة أسئلة: ماذا سيحدث إذا تفاعلت أي مجموعة معادية مع أخرى واستهدفتها في الميتافيرس؟ ما التدابير العقابية المناسبة لمنع مثل هذا النشاط العدائي من النمو؟ كيف يمكن تنفيذ هذه التدابير مع حماية سلامة الميتافيرس المستقرة التي تجعل هذا العالم الافتراضي جذابًا للغاية؟ وقد تظهر مشكلة هجينة أخرى للعيان في الميتافيرس: وهي هجوم الرجل الوسيط (MITM). ويمكن إساءة استخدام المعلومات الرقمية في الميتافيرس، مثل: الأوراق المالية أو المعلومات الشخصية، في العالم المادي للوصول إلى الأنظمة أو الشبكات وتوجيهها بشكل ضارٍّ.

وعلاوة على ذلك، تعد حرية التعبير والرقابة من القضايا المهمة منذ بزوغ فجر الويب 1.0. وكُلفت الجهات الرقابية والتشغيلية والبائعون بالتصدي لتحدي تمكين وتعزيز حرية التعبير عبر الإنترنت دون الترويج للتمييز، أو العنف، أو الجدل، أو أي سلوك آخر ضار. ولا تزال تحاول البشرية تحقيق التوازن بين حماية حرية التعبير ومحاربة المشكلات المتأصلة، ولم يبلغ ذلك ذروة المثالية بعد في الويب 2.0، فالفيسبوك له سياسة مختلفة عن تويتر بشأن حرية التعبير وما يشكله خطاب الكراهية والتحريض على العنف والتحرش. ومن المتوقع استمرار هذا الانقسام وازدياده صعوبةً لا سيما في الساحة اللامركزية للميتافيرس، حيث يكون لدى تاجر واحد أو منصةٍ تعريف مختلف تمامًا ودرجات مختلفة من التسامح مع التحرش.

وقد تستخدم الجهات الفاعلة الخبيثة تقنية واحدة في التهديد، وهي التسويق الماكر أو الدعاية الشعبية الزائفة، ويُقصد بها خلق انطباع زائف من الدعم الشعبي أو معارضة قضية أو فكرة ما. وانتشرت هذه التقنية

كالنار في الهشيم على منصات التواصل الاجتماعي والمساحات الرقمية على حساب المرونة المعلوماتية. ويمكن تطبيق تلك التقنية في الميتافيرس عن طريق خلق العديد من المستخدمين الزائفين المستقلين ظاهريًّا والمُسيطر عليهم عن طريق كيان واحد داخل شبكة منسقة. وقد تنظم الشخصياتُ الافتراضيةُ الخادعةُ اعتصاماتٍ افتراضيةً، وتشارك في المناقشات وتنشر روايات كاذبة تم إعدادها للتلاعب بالإدراك والتأثير بشكلٍ أوسع على مجتمع الميتافيرس، كما يمكن استخدامها لمضايقة المستخدمين عن طريق إرسال رسائل غير مرغوب بها إلى مساحات الميتافيرس ورفع تجارب ومجتمعات افتراضية على الميتافيرس تحمل خطابات ضارة.

وهناك سبيل آخر لنشر المعلومات المضللة، وهو استخدام تقنية التزييف العميق لإنشاء وسائط اصطناعية في الميتافيرس. فعلى سبيل المثال، قد تُنْشِئُ جهاتُ التهديدِ مقاطع فيديو أو تسجيلات صوتية واقعية تصور أفعالًا وأقوالًا غير حقيقة لشخصيات عامة. ونظرًا لطبيعة الميتافيرس الغامرة، فقد يؤثر ذلك المحتوى بشدة لصعوبة دحضه على منصات الإنترنت التقليدية. وبالإضافة إلى ذلك، قد تُسْتَخْدَم الشخصيات الزائفة لكسب الثقة ثم يتم استغلالها لأغراض شريرة. فعلى سبيل المثال، بوسع جهات التهديد التظاهر بكونها أصدقاء أو زملاء أو كيانات موثوقة لاستخراج معلومات حساسة أو للتلاعب بالمستخدمين لتنفيذ إجراءات معينة. ويحتمل حمل مثل هذه الأساليب الهندسية الاجتماعية لفعالية أكثر في الميتافيرس بسبب المستوى العالي من التفاعل الشخصي والمشاركة. وتُبرز هذه التهديدات المحتملة ضرورة إنشاء تدابير أمنية متقدمة وأنظمة تَحَقُّق قوية ومراقبة فعالة للمحتوى في الميتافيرس. وعلى مطوري المنصات والمستخدمين والهيئات التنظيمية بذل جهود جماعية مضنية لتخفيف هذه المخاطر ولضمان استمرار أمان وجدارة العالم الافتراضي بالثقة في التفاعل والاستكشاف.

الرقابة (Censorship)

تطرح الرقابةُ في الميتافيرس أمام صُنَّاع السياسات مجموعةً فريدةً ومعقدةً من التحديات، حيث يمتد الميتافيرس، المُصور غالبًا بكونه مجموعة لا نهائية من المساحات الرقمية المترابطة، إلى ما وراء حدود مساحات الإنترنت التقليدية، مُعَقِّدًا على نحو متزايد مهمة الإشراف على المحتوى والرقابة. ففي المقام الأول، تشكل الطبيعة اللامركزية للميتافيرس تحديًا كبيرًا للرقابة. وإذا تطورت الميتافيرس كما هو مُتصور، فلن يكون هناك كيان أو سلطة واحدة تتحكم في نظامها بالكامل. وقد يُصَعِّبُ التوزيعُ اللامركزيُّ من فرض سياسات محتوى متسقة عبر المساحات الافتراضية المختلفة، حيث تدير جهات مختلفة كلًّا منها بقواعد ومعايير متفرقة كذلك.

وقد يجعلُ حجم المحتوى وتنوعه في الميتافيرس الرقابةَ أمرًا صعبًا للغاية. وقد يتسنى التفاعل وإنشاء المعلومات وتبادلها بطرق مختلفة عن تلك الطرق الخاصة بالمساحات الإلكترونية التقليدية. فقد يشمل المحتوى في الميتافيرس النصَّ والصوتَ والفيديو والعناصر الافتراضية حتى البيئات الافتراضية الكاملة. ونظرًا لهذا التنوع والحجم، فقد يصبح رصد ومراقبة جميع المحتويات أمرًا شاقًّا للغاية.

وعلاوة على ذلك، تُعَقِّدُ ميزةُ عدم الكشف عن الهوية المتاحة للمستخدمين في الميتافيرس الرقابةَ أكثر فأكثر. ويتسنى للمستخدمين تغيير الشخصيات الافتراضية أو هوياتهم باستخدام عناوين بديلة، وهو ما قد يمنحهم إمكانية الإفلات من المساءلة عن أفعالهم. وقد تُصَعِّبُ تلك المرونة من تَتَبُّعِ أو تحذير أو حظر المستخدمين الذين ينتهكون قواعد المحتوى. ونجحت أدوات تحليل سلسلة الكتل جنبًا إلى جنب مع الجهود الحقيقية التي تبذلها شركات ذكاء الويب أو مسؤولو إنفاذ القانون، في تجميع عناوين متعددة إلى هوية واحدة، ولكن قدرة هذه الجهود على التوسع تصبح موضعًا للتساؤل مع نمو الميتافيرس كنظام افتراضي وبلا حدود.

كما تُشَكِّلُ مسألةُ السلطة القضائية معضلةً أخرى لتنظيم الميتافيرس. ونظرًا للطبيعة العالمية للميتافيرس، يعد تطبيق الأنظمة القضائية ذات المصالح القانونية المتنافسة والتنسيق بشأن معايير إدارة المحتوى أمرًا صعبًا. وتختلف معايير وقوانين حرية التعبير وخطاب الكراهية وغيرها من القضايا المتعلقة بالمحتوى من دولة إلى أخرى؛ لذلك فمن المستحيل فرض مجموعة قياسية من القواعد تُرْضِي جميع السلطات القضائية. كما أن بوسع التقنيات المتقدمة، مثل: تقنية التزييف العميق، جعلَ اكتشاف المحتوى الضار أكثر صعوبةً وتحديًا. ويُحتمل أن تزداد صعوبة التمييز بين المحتوى الحقيقي والمحتوى المزيف مع تطور تقنية التزييف العميق، وهو ما يعقد مهمة حذف المحتوى المضلل أو الضار. وعلى الرغم من وجود كل تلك التحديات، فمن الضروري ضمان أمان وشمولية بيئة الميتافيرس. ومن المرجح أن تتطلب هذه المهمة أدوات مراقبة متقدمة تعتمد على الذكاء الاصطناعي وهياكل حوكمة قوية وتعاونًا قويًّا بين منصات الميتافيرس والمستخدمين والجهات الرقابية. وفي نهاية المطاف، قد يتمثل مفتاح الرقابة الفعالة على الميتافيرس في إيجاد التوازن الصحيح بين حرية المستخدم وسلامته وحماية المستخدمين من المحتوى الضار والسماح لهم في الوقت نفسه بالإبداع والتعبير الحر.

8. مخاطر على السيادة والثقافة (Risks to Sovereignty and Culture)

يمكن أن يؤدي الميتافيرس، بوصفه ساحةً افتراضيةً خاليةً من الحدود يمكن الوصول إليها من أي مكان، إلى تقويض سيادة الدول وثقافتها. وبالنظر إلى تركيز سلطة بعض شركات وسائل التواصل الاجتماعي، على

النظام الرقمي الناشئ (Bremmer, 2023) الذي تهيمن الشركات الخاصة عليه بشكلٍ متزايدٍ على حساب الدول، فمن المحتمل أن يأخذ الميتافيرس هذه الخطوة إلى الأمام، وبإمكانه فك مركزية المساحة الافتراضية الغامرة مع الحفاظ على أهمية العالم الرقمي الاجتماعية والاقتصادية والسياسية في الوقت نفسه. ويتيسر للفكرة أو الاعتقاد، الذي يبدأ افتراضيًّا، الانتشارُ بسهولة في العالم المادي، حيث يكتسب زخمًا بين المؤمنين به الذين يعملون على تحقيقه في العالم المادي. كما توفر غرف الدردشة والمنتديات ووسائل التواصل الاجتماعي موطنًا لجمع وشرح الأفكار الاجتماعية والثقافية الجديدة، فلا تكمن الفكرة في وجوب تطرف أو هامشية هذه الأفكار بطبيعتها. وبالأحرى، يمثل الانتشار السهل والسريع لوسائل التواصل الاجتماعي والثقافي تهديدًا خطرًا على سيادة الدول العربية؛ فعلى الرغم من ضمان هذه الدول لأعمال التأسيس والأمن في الميتافيرس، يبدأ المستخدمون المشاركون في هذا العالم الافتراضي غير المحدود في الانفصال عن هذا الواقع.

وقد تَنَبَّأَت وسائطُ الإعلام الرقمية بتلك التهديدات، وخاصة منصات التواصل الاجتماعي، وتنبأ بها كذلك الانخفاضُ المتزامنُ في الأنماط الاجتماعية، التي تُؤْخَذ من المسلمات في العديد من المجتمعات الغربية، وهو ما يؤدي إلى انقطاع مجتمعي. وقد يُعزز الميتافيرس هذا الاتجاه ويُوسِّعه من خلال إبعاد الأفراد عن بلدانهم ومجتمعاتهم. ونظرًا للاندماج بين المعدات المنزلية التي تعمل بتقنية الحوسبة السحابية مع إمكانية الوصول إلى مجموعة من العملات المشفرة مع نقل البيانات الشخصية عالميًّا من خلال التقنية اللامركزية المتأصلة، قد يرى الأفراد أن دولهم وثقافاتهم غير ضرورية أو هامشية، على الرغم من تحصين الدول لهؤلاء الأفراد من أجل ضمان وصولهم المستقر إلى العالم الافتراضي.

ولا يُهَمِّشُ ذلك إمكانية انتشار جماعات متطرفة في الميتافيرس وتهديد سيادة الدول العربية وثقافاتها الأساسية ومجتمعاتها المتلاحمة. وسيكون الميتافيرس بيئةً خصبةً للتعاون وتوليد الأفكار للأشخاص المنبوذين من أقرانهم أو مجتمعاتهم أو بلدانهم. وأدى الإنترنت إلى ظهور العديد من الفئات الجديدة في المجتمع، وهذه الفئات تزدهر الآن وتُحَفِّزُ كُلًّا منها الأخرى، مثل: جماعات العزوبية غير الطوعية (الإنسيلز)، وأصحاب نظرية المؤامرة، والمتداولين في الأسواق المالية الذين منحوا أنفسهم ألقابًا معينة. ومن الممكن لمثل هذه المجموعات أن تكتسب تأييدًا كبيرًا لأفكارها عبر الإنترنت، وأن تستخدم جماهير مشتركة مع مجموعات مشتركة لتشكيل تهديد حقيقي لشعب آخر، أو للقضاء على ثقافة معينة، أو لتنفيذ أمور قد تكون أسوأ من ذلك. وهذا المنظور يمتد ليشمل الجماعات الهامشية، كالجماعات الدينية المتطرفة داخل منطقة الشرق الأوسط وخارجها، وتلك الجماعات ترمي إلى إضفاء الطابع المؤسسي على الآراء التي لا تتمتع بتأييد شعبي، والتي تسعى لتقويض

النظام المؤسسي. ولما كان من الصعب لمجموعة متطرفة أن تنشئ حزبًا سياسيًّا في العالم الحقيقي، فكان العالم الافتراضي ملاذًا لها لامتلاك عقارات افتراضية، من بين أدوات افتراضية أخرى، وهو الأمر الذي يُشَكِّلُ بديلًا خطيرًا من شأنه أن يُقَوِّضَ أو يُضْعِفَ مؤسسات العالم الحقيقي تدريجيًّا.

من أجل ذلك كان من المطلوب في تقنية الميتافيرس إيجاد حلٍّ لمنع وجود تلك الفئات؛ لأن وجودها يشكل خطرًا حقيقيًّا على الدول العربية، التي تسعى إلى المحافظة على النظم الاجتماعية الأساسية لها، بل تسعى أيضًا لتعزيزها داخل حدودها المادية وخارجها؛ ليمتد تعزيزها إلى جميع أرجاء المنطقة؛ لذا كان لزامًا أن يتم تبني تقنية الميتافيرس، ولكن فقط بشكل ناجح (بأن تكون تقنية الميتافيرس ذات طبيعة مضطربة وغير مستقرة لا يمكن لمستخدميها من خلالها تكوين علاقات مستقرة، ولا تكون المجتمعات الافتراضية فعالة بالشكل الخطير الذي يمكنها من احتضان التهديدات المذكورة).

ويتطلب التخفيفُ من حدة هذه التهديدات لتبني تقنية الميتافيرس، أن يُحَقِّقَ المسؤولون الأمنيون، كما ناقشنا فيما سبق، توازنًا مناسبًا بين حقوق الأفراد وبين ضمانات الحماية من تلك التهديدات، كحد أدنى. وبناءً على ذلك، سيتم منع أسوأ التجاوزات المحتملة للفئات الافتراضية الخطيرة المذكورة من الوصول إلى أغراضها أو جني ثمارها. وفي سياق متصل، يتعين في الجهد الإقليمي المبذول من الدول العربية لاعتماد الميتافيرس تحديد النطاق الصحيح للجهاز الأمني المحدد له بوضوح من البداية، مع الاعتراف في الوقت ذاته بأن بعض المسؤوليات ستقع على عاتق الجهاز السياسي وليس جهاز الأمن الوطني.

وفي النهاية، لا بد أن يتم العمل في إطار إدراك أحد الثوابت المهمة، وهي عدم وضع العالم الافتراضي في صراع مع العالم الحقيقي، وأنه يمكن الاستفادة منه في إقامة تعايش طبيعي بين المجالات الافتراضية والمجالات الحقيقية، وهذا أمر ممكن وموجود بالفعل، ومن الممكن ربطه بإنشاء تقنية الميتافيرس، ومن الأمثلة على ذلك، تشترك المدن المتنامية بمنطقة الشرق الأوسط وشمال إفريقيا في الكثير من القواسم المشتركة مع مراكز التقنية الدولية، في سنغافورة وهونج كونج مثلًا: في وجود شركات التقنية الناشئة، وفي جهود الطاقة الخضراء، وفي وجود عدد متزايد من السياح. وتتميز العلاقات العالمية في مجال التقنية وغيرها من المجالات، التي تعمل بناءً على تلك المجالات على تحفيز الازدهار الاقتصادي، بأنها تسمح بإقامة علاقات قوية بين الدول التي لا تشترك معها في حدود مادية، ومثل هذه الروابط العابرة للدول تتحقق في تقنية الميتافيرس، وذلك دون إغفال الروابط الأساسية التي تقوم على أساسها تلك الروابط الافتراضية.

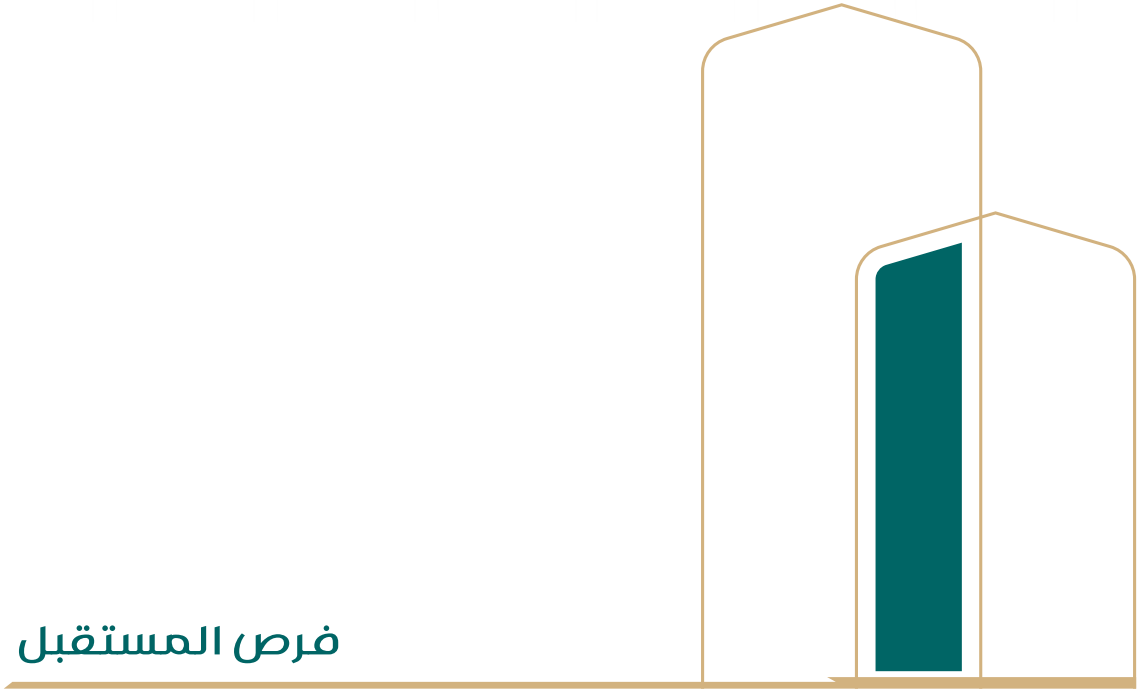
9. التعبئة الاجتماعية والسياسية (Social and Political Mobilization)

تَسْمَحُ تقنيةُ الميتافيرس بحكم طبيعتها العالمية واللامركزية، للأفراد الذين لديهم خلفيات متنوعة بتكوين علاقات عميقة وقوية بشكلٍ لا يمكن تحقيقه بشكلٍ متبادلٍ في الواقع المادي. ويؤدي هذا على الأرجح إلى حقيقة أن عالم اليوم أصبح في ظل العولمة مليئًا بالمجتمعات المشتتة، التي يمكن أن تُشَكِّلَ مزيجًا مع بعضها، وأن تنفجر بسيلٍ من الشكاوى السياسية والتفاعلات الاجتماعية التي أصبحت سهلة وعابرة للحدود المادية. ويُشَكِّلُ تهديد الحشود الاجتماعية والسياسية الناشئة في هذا العالم الافتراضي خطرًا كبيرًا وخصوصًا لبعض الدول العربية.

ومما يميزُ تقنيةَ الميتافيرس أنها لا تعترف بالتفاوت الموجود في العالم الحقيقي؛ لذا تعتبره بعض الفئات المذكورة أنه يحارب النخبوية المتسلطة على أجزاء كثيرة من العالم في هذه الأيام. وإلى جانب هذا المنظور، تأتي الحركات الشعبوية بتحديات إقليمية أو عالمية يرعاها ويحميها عالم افتراضي.

وتؤدي تقنية الميتافيرس إلى تزايد وتوسيع تأثير منصات وسائل التواصل الاجتماعي في هذا الصدد، وفيما يتعلق بإمكانية إحداث ترابط حول القواسم المشتركة عبر الحدود المادية بطريقة صحية، ولكن في الوقت نفسه، سيؤدي هذا الترابط إلى إمكانية تواصل الشكاوى السياسية على نحوٍ يجعل أصحابها مؤسسات أو حركات مناهضة للدولة.

وهذه التهديداتُ لا يمكن التعامل معها من خلال قمع تلك الأنشطة بطريقةٍ لا تحترم حقوق الأفراد داخل عالم الميتافيرس، حتى لا يؤدي عن غير قصد إلى تضخيم المخاطر على سيادة الدول العربية (ومع ذلك، فمن غير المرجح أن يحقق هذا التعامل النتيجة المرجوة منه). وبدلاً من ذلك، يجب على السلطات الأمنية والسياسيين أن يفهموا أن الحشود الاجتماعية والسياسية، التي تحدث داخل الميتافيرس، ستعتمد دائمًا على البنية التحتية المادية التي تسيطر عليها الدول في النهاية. وفي حين أنه سيتعين صياغة سياسات محددة بمرور الوقت ومن المحتمل تحديثها بالخبرة، فإن هذا الفهم الأساسي يجب أن يُعَلِّم الجهات الفاعلة الإقليمية أنه مهما بدت الحركة نشطة أو مؤثرة في العالم الافتراضي، فإن نطاقها مرتبط بالمؤسسات القائمة في العالم المادي.



فرص المستقبل

انطلقت تقنيةُ الميتافيرس في السنوات الحالية، وانتشرت بشكلٍ واسعٍ في الوعي الشعبي وأذهلت العالم بأسره بإمكاناتها الابتكارية الكبيرة. وتحولت تقنية الميتافيرس من موضوع جماهيري على مستوى القاعدة الشعبية إلى تقنية تتسابق الشركات متعددة الجنسيات والحكومات لتطويعها، مدفوعة في ذلك بارتباطها الملفت للانتباه بتقنيات سلسلة الكتل ذات الشعبية المتزايدة والتطبيقات المتطورة لمعدات الواقع المعزّز. وعلى الرغم من قيام البعض بالتشكيك في التطبيقات العملية للميتافيرس في العالم الحقيقي، فإن العالم الافتراضي ظل يثبت باستمرار قيمته الكبيرة في هذا الشأن.

ويدرك العالم العربي بوضوح إمكانات تقنية الميتافيرس، ويتبنى فرص تقنية الميتافيرس بشغف كبير بغرض مواصلة الدفع في اتجاه تطبيق التحولات الرقمية على مستوى المنطقة. ويمكن أن يتأثر المجتمع العربي كله بشكل إيجابي من خلال الوصول إلى تقنية الميتافيرس، وفي الوقت نفسه، يتمتع العالم العربي بالقدرة على قيادة التقنيات الحديثة الناشئة لمواجهة تحديات الأمن الوطني والآثار التي تترتب على استخدامه.

ومن الأمثلة على ذلك، ففي عام 2022، أصدرت دولة الإمارات العربية المتحدة إستراتيجية دبي للميتافيرس، التي تهدف إلى جعل دبي واحدةً من أفضل 10 اقتصادات في الميتافيرس، ومركزًا عالميًّا لمجتمع الميتافيرس. ويعتمد المشروع على نجاح دبي في جذب أكثر من 1000 شركة في مجالات تقنية سلسلة الكتل وتقنية الميتافيرس؛ وذلك بهدف خلق أكثر من 40 ألف فرصة عمل افتراضية بحلول عام 2030. وتركز الإستراتيجية على الابتكار والاستثمار في تعليم الميتافيرس وتطوير تقنية الجيل الثالث من الإنترنت في قطاعات السياحة والتعليم والرعاية الصحية وقطاعات أخرى. كما تركز على أمان المستخدم والمعايير العالمية والاستفادة من البيانات الفورية والذكاء الاصطناعي وحوسبة الحافة. وهذه الإستراتيجية تجعل من دبي رائدةً لتقنية الميتافيرس.

ويظل تطويرُ تقنية الميتافيرس مَحَطَّ اهتمامِ منطقة الشرق الأوسط، ويتجلى ذلك في الأنشطة التي قامت بها المملكة العربية السعودية في هذا المجال في الآونة الأخيرة. وتعد شركة ميتا، هي الجهة الأساسية الفاعلة في سوق مُطَوِّرِي تقنية الميتافيرس بما أحدثته من نقلة إستراتيجية كبيرة في تطوير العالم الافتراضي (Meta, 2022)، وقد أسست أول أكاديمية متخصصة في تقنية الميتافيرس في الرياض، بالمملكة العربية السعودية، وتهدف هذه الأكاديمية إلى إدارة تطوير تقنية الميتافيرس في منطقة الشرق الأوسط وشمال إفريقيا. وتقوم هذه الأكاديمية بتدريب 1000 متدربٍ تدريبًا مُرَكَّزًا مدته 18 شهرًا، كما تزودهم بالمهارات المطلوبة لتشكيل منظومة تقنية الميتافيرس (Cabral, 2023b). وفي المؤتمر التقني الدولي السنوي «ليب» 2022، أُبْرِمَت شراكةٌ بين كل من منصة ساندبوكس القائمة على تقنية الميتافيرس وهيئة الحكومة الرقمية في المملكة العربية السعودية فيما

يتعلق بتطوير تقنية الميتافيرس. وقد أكد سيباستين بورجوت، المؤسس المشارك ورئيس العملياتِ في منصّة ساندبوكس، الطبيعةَ التعاونيةَ للاتفاق الخاص بالشراكة التي تم عقدها مع الحكومة الرقمية، وكشف عن أنها تهدف إلى اكتشاف طرق جديدة وتقديم المشورة والدعم بشكل مشترك بين الطرفين بما يرمي إلى دفع عجلة الابتكارات في تقنية الميتافيرس. وتركز هذه الشراكة الإستراتيجية على التزام المنطقة الراسخ بتسخير كل الخبرات المتاحة والتشجيع على الابتكار بغرض دفع عجلة التنمية في مجال تقنية الميتافيرس في المملكة العربية السعودية (Fortis, 2023).

وعلاوة على ذلك، كشف مؤتمر «ليب» بالمملكة العربية السعودية عن الخطط الطموحة الرامية لإنشاء منصة الميتافيرس الإدراكية القائمة على التوأمة الرقمية لمشروع مدينة نيوم، بهدف تزويد الزوار بتجربة فريدة عند وجودهم بشكلٍ ماديٍّ بمدينة نيوم، وفي الوقت نفسه عند وجودهم بشكلٍ افتراضي من خلال الشخصيات الافتراضية وتقنية التصوير المجسم. وتبين هذه الشراكات التزام المملكة العربية السعودية بتوسيع نطاق حدود تقنية الميتافيرس.

احتياج العالم العربي لتقنية الميتافيرس

تُعَدُّ الفرصُ المُقَدَّمَةُ للحكومات والشركات العربية غيرَ محدودةٍ، لكن لا بُد من التسليم بأنها تتضمن مجموعةً من مخاطر أمنية خاصة بها في سياق محدد. ويتعين تأهيل المسؤولين الأمنيين السعوديين على نحوٍ يمكنهم من مواجهة هذه التداعيات عند جني الفرص ذات الصلة.

وتركز تقنية الميتافيرس على إدخال الطبيعة الديمقراطية على القدرات الرقمية؛ حيث ستسمح تقنية الميتافيرس وتقنية سلسلة الكتل والجيل الثالث للإنترنت والآلات الافتراضية، التي تعمل بتقنية سلسلة الكتل، للمبتكرين العرب بالإبداع والعمل بشكل رقمي دون وجود وسطاء في بيئة غير موثوقة، حيث يحل الكود الشفاف محل التبعيات على السلطات المركزية. ويعد الحافز من وراء تبني تقنية الميتافيرس وتنظيمها هدفًا شاملًا لكن تقنية الميتافيرس تُقَدِّمُ منفعةً للمنطقة. وتفرض المنفعة نفسها بعدة طرق مختلفة وفي ظروف مختلفة على الرغم من أنها في بعض الأحيان تصبح خطيرةً.

ولهذا السبب، يُعَدُّ التنظيمُ ضروريًّا لضمان كون المنظومة الافتراضية آمنة، وأنها تسير بطريقة عادلة. فهؤلاء الذين يقدمون الخدمات في تقنية الميتافيرس باستخدام تقنية سلسلة الكتل أو باستخدام آلة افتراضية

سيحتاجون إلى وجود مَقَرٍّ لهم في مكان ما. وقد ظهرت دول العالم العربي من الخليج العربي إلى شمال إفريقيا وبلاد الشام كمنطقة قادرة على استيعاب الابتكار وقيادة عجلة التقدم أثناء شروعها في تبني جهود التحول الرقمي. وإن الاستثمار في بيئة آمنة قادرة على استضافة التبني الناجح لتقنية الميتافيرس يُعَدُّ خطوةً للأمام، باعتبار ذلك جزءًا من غزو دول العالم العربي لمجال التقدم التقني، وخاصة حينما يكون ذلك في الوقت الذي تتصارع فيه القوى الكبرى والمتوسطة الأخرى على مسألة تنظيم هذه البيئة.

ويعد أقوى مورد إقليمي موجود هو رأس المال البشري، ولكن المعروف تاريخيًّا، أن المواهب العربية تهاجر بحثًا عن فرصٍ أخرى بعيدًا عن المنطقة (Al-Mulla, 2023). ويمكن معالجة هذه الظاهرة المعروفة بهجرة العقول العربية عن طريق الاستفادة من القوى العاملة الماهرة والمراكز المؤسسية القوية تاريخيًّا. إن أي حجم للمشروع أو الاستثمار العام سوف يُؤْتِي ثمارَه على المدى الطويل، خاصة إذا علم الممارسون العرب أصحاب المستويات العالية أن التنفيذ يمكن أن يُشَكِّلَ منفعةً للأجيال المتعاقبة. وإدراكًا لهذا الأمر، فإن التبني المؤسسي والشعبي لتقنية الميتافيرس وتنظيم الدولة لها- تعد خطوات ذات فائدة كبيرة؛ لأنها تجعل من العالم العربي مركزًا عالميًّا لهذا المجال. وتعد المنطقة رائدة عالميًّا في عدة مجالات، وعلى وجه التحديد في تصدير الطاقة وتصدير رأس المال البشري. ومن خلال ترسيخ العالم العربي لمكانه في تأسيس هذا المجال الرقمي، يستطيع العالم العربي أن يستحوذ على قطاع عالمي كبير طوال عدة أجيال قادمة. وإن تكلفة الفرص البديلة تعد واضحةً؛ فما يمكن تحقيقه يجب تحقيقه.

الفرص على مستوى المستهلك

نذكر من الدروس التجارية المستفادة من جائحة كوفيد19-، التي سَبَّبَت شللًا في العالم بأسره، أنه عندما يصبح العالم المادي عاجزًا عن الإنتاج، يمكن استخدام العالم الافتراضي للاستمرار في الإنتاج، وهو الأمر الذي يُقَلِّلُ المشكلات أو الفجوات التنموية التي تتطلب الابتكار باستمرار. وتتيح تقنية الميتافيرس المزيد من الاستقرار الاقتصادي، ولكن شريطة أن تقوم على أساس محميٍّ بالقدر الكافي؛ لجعلها تؤتي ثمارها المرجوة منها.

ويمكن لتقنية الميتافيرس رفع مستوى القطاعات لمستوى لم يكن مُتَصَوَّرًا لها من قبل. ومن الأمثلة على ذلك، يمكن إعطاء بُعْدٍ جديدٍ لمجال التجارة الإلكترونية من خلال المتاجر الافتراضية التي تسمح للمستهلكين بالتفاعل مع المنتجات بشكلٍ مقاربٍ لطريقة التسوق المادي. وبشكلٍ مماثلٍ، يمكن للمستهلكين معاينة العقارات

باستخدام جولات افتراضية غامرة، وهو ما يؤدي إلى إنعاش أسواق العقارات بمزيدٍ من الاستثمارات الأجنبية. كما أننا على أعتاب ثورة هائلة في عالم الألعاب؛ حيث يمكن لبيئات الواقع الافتراضي الغامرة أن تُقَدِّمَ تجاربَ حيةً للألعاب. كما يمكن للمستخدمين أن يحضروا الحفلات الموسيقية والأحداث الرياضية والعروض المسرحية بشكلٍ افتراضي، متجاوزين بذلك الحدود والحواجز الجغرافية، ويحصل الناس على حقوقهم بشكل ديمقراطي في الوصول إلى الفعاليات الثقافية والترفيهية. ويُمكن أن يوفر الميتافيرس بيئات غامرة وتفاعلية في القطاعات التعليمية، التي يمكن أن تجعلَ التعلمَ أكثر جاذبية، وتجعله متاحًا بشكل أوسع، ويبدأ ذلك من الرحلات الميدانية الافتراضية، ويصل إلى تعاون الطلاب مع زملائهم في جميع أنحاء العالم بشكلٍ فوريٍّ.

ومن أفضل الطُّرق للحد من التوترات والانقسامات المجتمعية والجيوسياسية، ربطُ الناسِ بعضهم ببعض، وتوسيع آفاقهم من خلال الثقافة والتعليم؛ لذا تعد تقنية الميتافيرس بُعدًا جديدًا لتعزيز الاستقرار من خلال مد الجسور الثقافية بين الناس. وتشكل التجارب الافتراضية المشتركة، التي تتجاوز الحدود، نقطةَ انطلاقٍ لتعزيز وجود علاقات متماسكة بشكل أفضل، ولتبادل وجهات النظر، وللحد من الصراعات الأهلية، وهذا يسمح بوجود مستوى عالٍ من التفاعل يؤدي إلى تحسين العلاقات بين المواطنين على المستوى الأدنى، وبين الدول على المستوى الأعلى.

وعلى الرغم من ذلك، لا بد من العلم في الوقت ذاته أنَّ كلَّ فرصةٍ تنشأ من خلال تَبَنِّي تقنية الميتافيرس - تتضمنُ ثغراتٍ أمنيةً بالنسبة للمستهلك. وعند إشراك المواطنين في أي مجال من خلال تقنيات الميتافيرس، فلا بُدَّ من تعليمهم كيفية المحافظة على إجراءات السلامة اللازمة لممارسة أي نشاط باستخدام تقنية الميتافيرس. ولا بد من تعليم المستخدمين أهمية المحافظة على المفاتيح الخاصة وكلمات المرور المستخدمة حتى يتم استخدام تقنية الميتافيرس والوصول إليها بطريقة آمنة. ويمكن أن تستهدف أيُّ جهة خبيثة أيَّ مستخدم يمارس أنشطته باستخدام هذه التقنية دون اتباعه إجراءات السلامة، ومن ثَمّ يتم اختراق هويته الرقمية. ومن الممكن أن يؤدي هذا النشاط إلى زيادة خطر سرقة الهوية وتزييفها.

الفرص على المستوى المؤسسي

تُقَدِّمُ تقنيةُ الميتافيرس للمؤسسات عالماً جديدًا من العمليات وتقديم الخدمات والإمكانات التي يمكن من خلالها زيادة الإيرادات. وكمسار مشابه على مستوى المستهلك، تكون الفرص على المستوى المؤسسي مصحوبة

بمجموعة من المخاطر الأمنية الخاصة بها؛ لذا يتعين على المسؤولين الأمنيين أخذ هذه المخاطر في الاعتبار.

وتبحث الشركاتُ في عالم ما بعد فيروس كورونا عن طُرُق يمكن الاستفادة منها للعمل عن بعد، وفي هذا الصدد، تسمح تقنية الميتافيرس بتوفير أماكن احتياطية للعمل، وهي: أماكن العمل الافتراضية. كما يمكن أن تكون تقنية الميتافيرس أكثر جاذبية وأكثر تفاعلية للعمل عن بعد، وهو الأمر الذي يساعد بدوره على المحافظة على العمل التعاوني والابتكاري في فرق متنوعة. كما يمكن للمؤسسات أن تولد إيرادات جديدة من خلال توفير السلع والخدمات من خلال تقنية الميتافيرس. وتوجد الكثير من الإمكانات المهدرة وغير المستغلة بشكل كبير، بدءًا من العقارات الافتراضية ووصولًا إلى الملابس والإكسسوارات الرقمية. كما توفر تقنية الميتافيرس منصة جديدة لمشاركة العملاء، وهو ما يسمح للشركات بإنشاء تجارب غامرة تُعزِّز ولاءَهم للعلامة التجارية للشركة. كما يمكن أن تستخدم الشركات تقنية الميتافيرس في التوظيف والتدريب، حيث يمكن استخدام الوسائل الافتراضية في إطلاق معارض للوظائف وإجراء مقابلات شاملة وبرامج تدريب تفاعلية، وهو ما يُحَسِّن من عمل إدارة الموارد البشرية وعملياتها بشكل كبير.

ولكن تتضمن الاستفادة من تلك الإمكانات بعض نقاط الضعف السلبية، التي تنتاب المؤسسة التي تستخدم تقنية الميتافيرس. فمن الممكن أن يؤدي العرض الافتراضي لأماكن العمل إلى تنفيذ هجمات من جهات خبيثة مُكلفة بالوصول إلى مناطق افتراضية معينة للوصول من خلالها إلى معلومات حساسة، ويُمكن سرقة عنوان بروتوكول الإنترنت، ومن الأمثلة على ذلك على سبيل المثال لا الحصر، يمكن أن تكون إحدى الشركات عرضةً للتسلل وسرقة خطط التصميم أو الأكواد الخاصة بها إذا استخدمت إحدى الشركات المصنعة للتقنية عالماً افتراضيًّا بغرض محاكاة تطبيقات التقنية الإستراتيجية الخاصة بها.

وعلى المؤسسات الصحية أن تضع لنفسها نهجًا مناسبًا يسمح لها بتبني تقنية الميتافيرس والاستفادة منها. فبعض المؤسسات الكبرى التي تُقدِّم الخدمات الطبية كجون هوبكنز ومايو كلينيك، تستخدم الذكاء الاصطناعي للمساعدة في الإجراءات الطبية، ومنها الإعداد لإجراء العمليات الجراحية وتطبيقها في جراحات العمود الفقري ووضع القسطرة. فهذه التقنية توفر التصور الكامل في تشريح المريض، وليس فقط التصوير ثنائي الأبعاد، وهو ما يؤدي إلى تحسين نتائج معدلات الخطأ، وتحسين مستوى سرعة تقديم الخدمة، بالإضافة إلى تحسين النتائج بالنسبة للمرضى. وبالإضافة إلى ما ذكر، تتجه العديد من المستشفيات إلى التحول الرقمي فيما يتعلق بممارسات حفظ بيانات المرضى عن طريق استخدام أنظمة السجلات الطبية الإلكترونية. كما أنه من الممكن دمج السجلات الطبية الإلكترونية القائمة على تقنية سلسلة الكتل، وهي تقنية لا مركزية

أصبحت ذات شعبية في هذا المجال (Han et al., 2022)، مع تطبيق المحاكاة الافتراضية التي تعمل بنظام تقنية الميتافيرس، وذلك لرفع مستوى تقديم الرعاية الصحية.

ولكن توجد مخاطر تتعلق بالخصوصية عند استخدام السجلات الطبية الإلكترونية لتشغيل المحاكاة الافتراضية العكسية فيما يتعلق بأنشطة رعاية المرضى. وكما ذكرنا سابقًا، سيشكل اعتماد المؤسسة على تقنية الميتافيرس لتخزين البيانات الخاصة واستخدامها مصدر قلق مباشر، حيث ستظهر أنشطة رعاية المرضى بأنها تشتمل على نقاط ضعف لدى المستهلك. ومع ذلك، فكما يسمح التأمين المناسب للبيانات لمقدمي الخدمات الطبية وأنظمة الصحة العامة الأكثر تقدمًا بالحفاظ على معلوماتهم الشخصية، سواء باستخدام التدابير الوقائية والقيود الداخلية أو ضد التهديدات الخارجية، سيسمح أيضًا تطبيق أمن البيانات والمحافظة على الخصوصية ذات الصلة على المستوى المؤسسي لاستخدام تقنية الميتافيرس بالوصول إلى نفس النتيجة.

الفرص على مستوى الدولة

تقع الدول العربية في منطقة تواجه تقلبات لعقود من الزمن، واستطاعت مجابهة التطورات الجيوسياسية والأمنية والاقتصادية التي ظهرت في العالم العربي وخارجه. وتتنافس منطقة الشرق الأوسط وشمال إفريقيا، التي يبلغ عدد سكانها 500 مليون نسمة تقريبًا، في حجمها مع قارة كاملة في حجم أمريكا اللاتينية كما تضم أكبر عدد من الناطقين باللغة العربية في العالم. ومن المتوقع بحلول عام 2030 أن يبلغ عدد السكان 581 مليون نسمة (Mendonca et al., 2019)، وهو ما يوفر قوى عاملة كبيرة بالمنطقة، فإن هذا السيناريو يعد سلاحًا ذا حدين؛ فعند توفير التعليم والتوظيف لهذه القوى العاملة، ستتوافر ميزة تنافسية، أما في حال غياب الفرص الكافية، فإن الأمر سيتحول إلى مخاطر على الأمن وعلى الاستقرار. وقد بلغ مجموع الناتج المحلي الإجمالي للمنطقة 3.46 تريليون دولار أمريكي في عام 2021، ومن المتوقع أن يُحقِّقَ ذلك الناتج الإجمالي نموًّا فعليًّا كبيرًا بنسبة 5% في عام 2022. وهذا المعدل يتجاوز معدلات النمو في الاقتصادات المتقدمة والناشئة، المتوقع لها أن تنمو بنسبة 2.4% و3.7% على التوالي. وبناءً عليه، تستمر منطقة الشرق الأوسط وشمال إفريقيا كسوق واعدة بدرجة كبيرة ذات نمو كبير محتمل في الصناعات المتنوعة. فعلى سبيل المثال، وضعت الإمارات العربية المتحدة خططًا وإستراتيجيات طويلة الأجل للاستجابة الرقمية السريعة والفعالة لفيروس كورونا19-، مثل: الإستراتيجية الوطنية للابتكار، وإستراتيجية الذكاء الاصطناعي 2031، وإستراتيجية سلسلة الكتل 2021.

وقد أنشأت إستراتيجية دبي للمعاملات اللاورقية هويةً وطنيةً رقميةً لـ 200.000 مستخدم، التي تمنح الوصول إلى العديد من خدمات الحكومة العامة والخاصة. ولم تضع الإمارات العربية المتحدة نفسها كمحور بارز للتقنية في المنطقة، ولكن حصلت على إقرار بأنها قائد عالمي في الابتكار الرقمي. وقد أصبحت البحرين حكومةً متقدمةً رقميًّا بدعمٍ فعالٍ من شركات التقنية المحلية والدولية. وتهدف رؤية المملكة 2030 إلى تغيير اقتصادها من خلال استخدام التقنية الرقمية. ومنحت المملكة الأولوية لقطاعات، مثل: الصحة والكهرباء والثقافة والسياحة للحلول الرقمية. ولقد دعم استخدام شبكات المجموعة من الجيل الخامس اعتمادات التقنية في السعودية، وهو ما يجذب المستثمرين المهتمين بالصناعات التي تعتمد على قدرات تقنيات الجيل الخامس. واستحدثت الحكومة أدوات ذكية وفعالة، مثل: تطبيق وزارة الصحة (موعد)، والمركز الوطني للتعليم الإلكتروني لتقديم التوجيه والمصادر التعليمية.

وشهدت منطقة شمال إفريقيا تحولاتٍ رقميةً مدعمةً من حكومات إقليمية ودول أيضًا، مثل: المغرب ومصر اللذين تطورا بسرعة. والمغرب هو الدولة الأكثر ارتباطًا في إفريقيا، ولقد أحرز تقدمًا ملموسًا في مجال الأمن السيبراني، وهو ما جعله يصل إلى المركز الخمسين في تصنيف الاتحاد الدولي للاتصالات بسبب اهتمام الحكومة المتزايد بالفضاء. ويهدف المغرب إلى أن يصبح رائدَ الأمنِ السيبراني في إفريقيا ومركزًا إقليميًّا للمبادرات العالمية ضد الجرائم السيبرانية. وتشمل إستراتيجية التحول الرقمي في مصر بالتوازي مع رؤية مصر 2030، رؤيةً وتخطيطًا لوضع الأسس لتحول مصر إلى الاقتصاد الرقمي، الذي يعتمد على مكانة الدولة كمحور أساسي لحركة الإنترنت العالمية بنسبة مرور 30% من خلال إقليمها.

واستجابة لهذه الحالات، أعلنت الحكومات العربية بنجاحٍ عن التحولات الرقمية التي تم تطبيقها على اقتصاداتهم، والتي لعبت دورًا حيويًّا في إدارة الأزمة. ويمكن لتقنية الميتافيرس البناء على هذه الدفعة وإتاحة فرص متعددة للجهات الفاعلة على مستوى الدولة للوفاء بأهداف السياسة. ويمكن للحكومات استخدام تقنية الميتافيرس لتحسين توصيل الخدمة العامة، وهو ما يجعلها أكثر توافرًا وفاعلية. ويمكن للمواطنين التفاعل مع الوكالات الحكومية في أي بيئة افتراضية، أو في دفع الضرائب، أو في تقديم طلب للحصول على تصاريح، أو في الوصول إلى الخدمات العامة. وتوفر تقنية الميتافيرس منصةً جذابةً للتعليم العام وحملات التوعية.

ويمكن أن تشمل حملاتُ الصحةِ العامةِ التجاربَ الافتراضية التي تُعَلِّمَ الأمورَ الصحيةَ وهو ما يجعل التعليمَ أكثر تأثيرًا. ويمكن الاستفادة من تقنيات الواقع الممتد لتقديم خدمات الرعاية الصحية الافتراضية

للمرضى، مثل: استشارات الطب الإلكتروني والعيادات الافتراضية ومراقبة صحة المريض عن بُعْدٍ، وتقليل الحواجز المادية للرعاية الصحية في النهاية. ويمكن أن توفر استشاراتُ الطبِّ الإلكترونيِّ بشكلٍ رئيس من خلال الواقع الافتراضي وصولَ المرضى إلى الأطقم الطبية المتخصصة في دول مختلفة، وتُمَكِّنَ المرضى الذين يعيشون في مناطق نائية/ ريفية من الحصول على الرعاية الصحية بدون السفر لمسافات بعيدة، والحد من آثار النقص في الأطقم الطبية. ويعيد تنشيط هذه المؤسسات ورعاية الدولة لهم الثقة في الخدمات الحكومية والمدنية، التي شَهِدَت انقراضًا في جميع أنحاء العالم أثناء جائحة فيروس كورونا 19-. كما يمكن لتقنية الميتافيرس تحسين الصحة وجمع بيانات الإحصاء البيولوجي والإدارة والتحليل.

كما يسمح النظامُ الافتراضيُّ بِسُبُلٍ جديدةٍ لجذب التدفقات الأجنبية والاستثمار المباشر المحتمل. ويمكن أن تكون تقنية الميتافيرس منصةً لعرض فرص الدولة الاستثمارية للعالم. ويمكن للحكومات استضافة رحلات افتراضية لمناطق التطوير أو المناطق الصناعية أو الوجهات السياحية لجذب المستثمرين الأجانب. ويمكن للتجارب الافتراضية التي أنشأها المطورون العرب في تقنية الميتافيرس التي لا حدود لها، الدعوة إلى السياحة الافتراضية للبائعين الإقليميين، مثل: السعي لإقامة فاعليات رياضية عالمية بعد فرص زيادة الدخل الكبيرة.

السياحة والتعليم مرتبطان إلى حَدٍّ كبيرٍ، ويستفيدان من وجود تقنية الميتافيرس. وكجزء من مبادرة التنوع الاقتصادي، تسعى السعودية لتنشيط السياحة في البلد، وأن يكون لها هدف استقبال 100 مليون زائر بحلول 2030؛ ويمكن أن تمكّن السياحة الافتراضية في تقنية الميتافيرس السعودية من الوفاء بهذا الهدف والتشجيع على النمو الاقتصادي في صناعة السفر والسياحة (في مجلس التعاون الخليجي، ومن المتوقع أن تنمو هذه الصناعات إلى 3.2 مليار دولار أمريكي بحلول 2030). وتمكّن نظارات الواقع الافتراضي وتقنيات الميتافيرس الأخرى المستخدمين من تلقي معلومات استشعارية تشمل الروائح والأصوات والرؤى والمشاعر، وأن يكون لهذه التقنيات المتطورة إمكانية نقل تجارب سفر غامرة. ويمكن للسياحة الافتراضية في تقنية الميتافيرس تقليل ضرورة السفر المادي، وخلق الرغبة في السفر المادي بين المستخدمين، وتوفير تسويق جديد وفرص اشتراك في صناعة السياحة والسفر. وفي حالة عدم قدرة المستخدمين على السفر ماديًّا، (بسبب العجز أو قيود أخرى) يمكن للمستخدمين الاستمرار في رحلات افتراضية غامرة بالكامل لدول مختلفة. كما يجوز للمستخدمين الذين يمكنهم السفر، ولكن يريدون ضمان أن تكون تجاربهم في السفر مفيدة، زيارة الوجهات والمطارات والفنادق والمواقع عند التخطيط للرحلات للحصول على أي فكرة دقيقة قد تشبه خبراتهم المادية.

ومن ناحية الدفاع والأمن، يمكن لتقنية الميتافيرس تحسين التدريب العسكري من خلال توفير بيئات افتراضية تشبه حالات القتال الواقعية، كما يمكن استخدامها للتخطيط الإستراتيجي وللألعاب الحربية.

ويمكن للجيوش العربية تحسين الاستعداد والقدرات التشغيلية من خلال تمثيل ساحة القتال الافتراضية واستخدام أجهزة الواقع المعزز لتعويد أفراد الجيش على بيئات النزاع المستقبلي. وينشئ المستخدمون في تقنية الميتافيرس وفرةً في البيانات التي قد تكون متاحة للحكومات لاستخدام وتحليل البيانات السلوكية للتهديدات الأمنية الوطنية المحتملة، شاملة التفضيلات والارتباطات مع مستخدمين آخرين، والمشتريات، والعادات، والمشاعر. ويمكن لهذه البيانات أن تُقَدِّمَ مؤشرات أفضل للأنشطة الخبيثة، وتزيد من قوة الأمن الرقمي والافتراضي، وتمكّن من إجراءات أكثر في الوقت المناسب، مثل: تدخل إنفاذ القانون لمنع الحوادث الأمنية بما في ذلك تلك الأحداث المرتبطة بالإرهاب.

وبالإضافة إلى الدفاع، ومن خلال تكرار الاتصالات والتفاعل الشخصي، يمكن للشخصيات الافتراضية تمكين الدبلوماسيين في تقنية الميتافيرس من الالتقاء والتعاون في بيئات افتراضية في حالات لم يتمكنوا منها مسبقًا بسبب القيود على السفر والتكلفة المالية والسلامة المادية والتأثير البيئي.

وقد وضعت العديدُ من الدول وجودًا افتراضيًّا أو سفارةً أو مركزًا ثقافيًّا في "الربع الدبلوماسي من الجزيرة الدبلوماسية" في تقنية الميتافيرس التي تُسَمَّى الحياة الثانية. وتكون الحياة الثانية منصةً على الإنترنت متعددة الوسائط، التي تسمح للمستخدمين بإنشاء شخصيات افتراضية لأنفسهم والتفاعل مع مستخدمين آخرين، بالإضافة إلى المحتوى الذي أنشأه المستخدم داخل العالم الافتراضي متعدد الأداء على الإنترنت؛ بعد إطلاقه في 2003، وتكون إحدى المنصات الأولى للعمل في تقنية الميتافيرس وأحد المواقع المبدئية للسفارات الافتراضية. وهذا مثال رائع لاستخدام تقنية الميتافيرس للارتباط بالدول الوطنية ومحو الحواجز اللغوية وإنشاء علاقات عالمية على الإنترنت بشكل صحي. وقد طبق السفير الإسرائيلي ديفيد سرانجا، رئيس قسم الدبلوماسية الرقمية في وزارة الخارجية الإسرائيلية، الذكاء الاصطناعي على الشخصية الافتراضية الخاصة به في تقنية الميتافيرس؛ لتوصيل أي رسائل دبلوماسية بثماني لغات مختلفة بما في ذلك العربية والصينية والروسية. وقد أسست الولايات المتحدة وإسرائيل السفارات الافتراضية المنشأة على الإنترنت للتشجيع على الحوار والانتشار الثقافي بينهما وبين الدول التي ليس لها علاقات ثنائية قوية معهما.

وفي حالة مماثلة، أطلقت الولايات المتحدة سفارةً افتراضيةً في طهران تهدف إلى الترويج للحوار بين الشعب الأمريكي والإيراني؛ ويعمل الفضاء السيبراني الافتراضي كأرض محايدة للاجتماع؛ حيث تُمَكِّنُ الإيرانيين والأمريكيين من بناء جسر على المياه الدولية المتعكرة (National Iranian American Council, 2011). وأطلقت إسرائيل سفارةً افتراضيةً عبر صفحة تويتر للتشجيع على الحوار الإستراتيجي بينها وبين شعوب دول

الخليج الست، التي ليست لديها علاقات رسمية معها. وكمثال على اللامركزية للدولة، في مطلع 2023، عقد المنتدى الاقتصادي العالمي اجتماعه السنوي في قرية التعاون العالمية، وهي منصة واقع مختلط تم تطويرها من خلال أكسنتشر ومايكروسوفت، وفي 2020، عقدت المجموعة 20 قمتها الافتراضية الأولى استجابة لفيروس كوفيد19-؛ وتمت استضافتها على منصة افتراضية اشترك فيها القادة من خلال استخدام الشخصيات الافتراضية (World Economic Forum, 2023). هذه أمثلة قليلة فقط على الميتافيرس التي تُسَهِّل العلاقات الزمنية المستمرة ببطء منذ عقود، والتي توفر مساحة آمنة ومحايدة للتفاعل.

وينبغي إدراك أن تَبَنِّي تقنية الميتافيرس على المستوى الدولي ودمجها يهدف إلى منع المخاطر الأمنية المتأصلة في تقنيات الميتافيرس. وتستفيد مبادرات الدول تقريبًا من العلاقات التاريخية مع رقابة الجهاز الأمني. كما يمكنهم تشجيع العلاقات بشكل أفضل مع شركات تحليل سلسلة الكتل وتقنية الميتافيرس التي تمت الإشارة إليها من خلال معايير إنفاذ القانون؛ ولذلك تكون القيادة في تبني تقنية الميتافيرس من خلال منهج تنازلي طريقًا صحيحًا للتبني الشامل. وبغض النظر عن هذا الواقع، يمكن أن يساعد النهج التصاعدي على الإيحاء بالتبني وإعداد جهات رقابية ومسؤولين أمنين في الدول المُعَدَّة بشكلٍ قليلٍ لدمج تقنيات الميتافيرس بسبب التفاوت في تقنيات البنية التحتية وخبرة الميتافيرس. وعلى أية حال، تكون أيُّ علاقةٍ قويةٍ بين القمة والقاع للمتبنين لتقنية الميتافيرس أساسيةً للدمج الأكثر فاعلية وأمانًا لهذه التقنية الوليدة.

الفرص الإقليمية

تقنيةُ الميتافيرس ليست مقيدةً بالحدود الجيوسياسية، وقد أصبح النظام الافتراضي منصة مناسبة لتحسين إمكانية التعاون عبر الحدود. ويمكن للدول العربية الدخول في المشاريع عبر الحدود في إطار تقنية الميتافيرس سواء أكان ذلك في الأبحاث، أم التعليم، أم التبادل الثقافي، ويمكن أن تساعد هذه المبادرات على بناء علاقات إقليمية أقوى (Bjola, 2022; Diplo, 2023).

كما يمكن أن تكون تقنية الميتافيرس منصةً للتفاعلات والمناقشات الدبلوماسية الإقليمية، بالإضافة إلى أنها قد تكون أداةً للعمليات الأمنية التعاونية والحث على الاستقرار والتعاون الإقليمي. وفي العالم العربي، تمت معالجة الانقسامات الناشئة عن صراعات الأجيال بالتدريج من خلال دبلوماسية رائعة. ويمكن إضافة هذا الهدف من خلال إعادة افتراضية للدبلوماسية الرقمية. ويمكن أن تعمل تقنية الميتافيرس كمنصة للتجارة

الإقليمية وهو ما يسمح للمستهلكين والأعمال بالتعامل عبر الحدود بسهولة تامة. وأصبح بالإمكان تحقيق فرصة وجود أكبر سوق عربية للميتافيرس، وهو ما يُعَزِّز التكامل الاقتصادي والتنمية والنمو في المنطقة. وتستطيع تقنية الميتافيرس توفير البنية التحتية الرقمية المشتركة والخدمات على مستوى الشركاء الإقليميين، وذلك فيما بين مراكز تبادل البيانات الإقليمية والخدمات الرقمية العامة المشتركة. وقد يدفع الانتشار السريع لتبني وتنظيم تلك التقنية الناشئة والمبتكرة إلى التحول المجتمعي وإعادة تعريف الأنشطة الاقتصادية وتعزيز التكامل الإقليمي. ونظرًا لأننا نخطو في هذه المرحلة الجديدة، فمن اللازم استيعاب إمكانات هذه التقنية عند مواجهة التحديات المرتبطة بها، وذلك لضمان استخدام تقنية الميتافيرس شاملة وسهلة الوصول وآمنة.

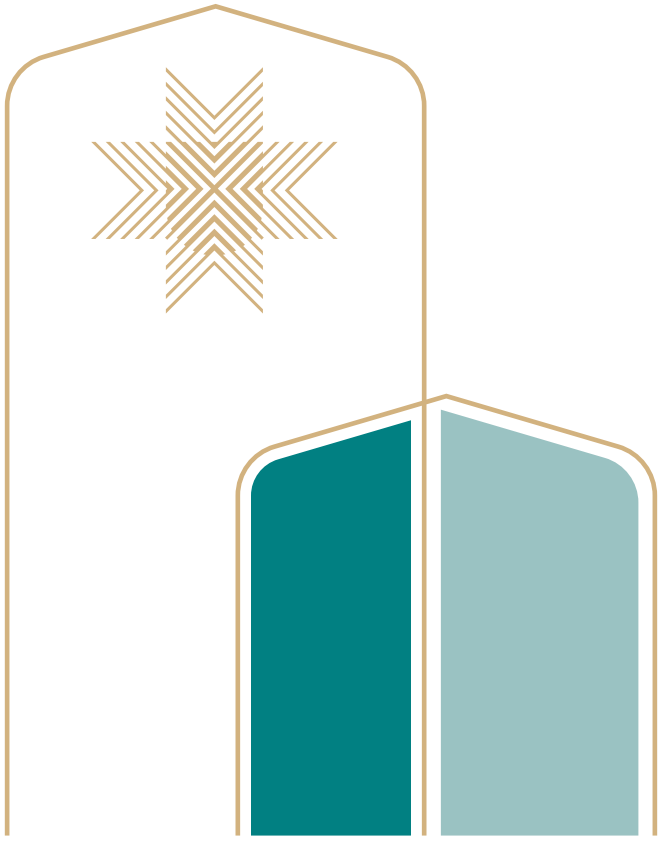
وتفسح طبيعة الميتافيرس المجالَ للحصول على فرص تدريبٍ واقعيَّة، وهو أمر مفيد لقطاعات الأمن الوطني وجهات إنفاذ القانون (Luckenbaugh, 2022). وتحتاج الجهات الإدارية الخاصة بالميتافيرس إلى أن تكون مدربةً أولًا على تلك التقنية، ومنها: أساليب الحماية السرية والعلنية، والإدارة المتسقة التي تتماشى مع الفهم الأساسي العام للمستخدم للتصور المتوقع والمقبول لتقنية الميتافيرس، والتدريب على مواقف معينة، التي تتضمن التجسس وتقليل ومنع حوادث المضايقات عبر الإنترنت، وتحديد العلامات الخاصة بالسلوك الخطر والجهات الإجرامية الفاعلة.

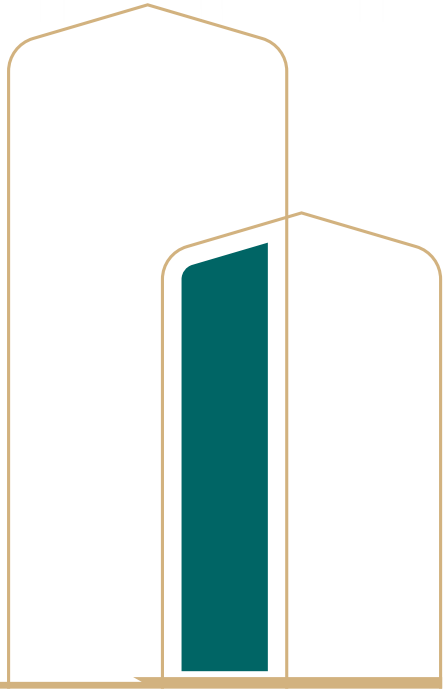
وقد يسهم إنفاذ القانون بالدول العربية في إنشاء دوراتٍ تدريبيةٍ، كما يضمن لأي مستخدم يعمل في العالمين الرقمي والمادي الحصول على تدريب مناسب لعدد هائل من السيناريوهات التي تحتاج إلى الحل من خلال إنفاذ القانون. وبإمكان هذه الدورات تحسين مهارات الاستجابة لدى المستخدمين من خلال التفاعل مع الشخصيات الافتراضية (أفاتار) التي تعالج الموقف وتختار الاستجابات الافتراضية؛ وذلك لحفظ نظام تقنية الميتافيرس، والتي يمكن مناقشتها واستخدامها فيما بعد في الخبرات التدريبية الشاملة والاستجابات المناسبة للحوادث.

ومن المنظور الافتراضي، أصبح بإمكان الحكومات العربية والعسكريين، جمع الأدلة الرقمية واستخدامها لضمان إجراء التحقيقات الشاملة. وتمنح البيانات الوصفية الإضافية، مثل: عناوين بروتوكول الإنترنت، وألقاب الجهات الفعالة والطوابع الزمنية، التي من الممكن مراجعتها للعمل بها، أدلةً لا خلاف عليها عند محاولة التعامل مع الحوادث التي تقع في عالم الميتافيرس. ولا يدعم الجانب الجنائي الرقمي القوي لأية تحقيقات إلا تحقيقات العالم الواقعي والأدلة المادية لضمان تحديد من ينبغي محاكمتهم على ارتكاب الأفعال الإجرامية وحماية الجهات البريئة.

وكما توجد أجهزةُ الاستخبارات والجهات الحكومية في شبكة ويب 2.0 من خلال فرق العمل والعمليات المشتركة، فلا بُد من عمل نفس الشيء في تقنية الميتافيرس. ويتعين على خبراء الأمن التعامل مع الميتافيرس غير المحدود عن طريق استخدام الجهات الفعالة السرية والعلنية والحفاظ على العلاقات مع القطاع الخاص. وعلى خبراء الأمن الإلمام بدوافع الجهات السيبرانية المختلفة، حيث تختلف تلك الدوافع بين أعمال القرصنة بالنسبة لمن يرغبون في إرسال رسائل معينة والجهات الإجرامية المأجورة (Weimann, 2004). وتتطلب مواكبة توجهات الأمن السيبراني والجهات الفعالة للتكتيكات والتقنيات والإجراءات تبادلَ الاجتماعاتِ والمعلوماتِ المنتظمةِ على كافة المستويات. ولا ينبغي للحكومة ومسؤولي إنفاذ القانون الاختباء وراء التصنيف أو تحذيرات المعلومات الحساسة، بل ينبغي عليهم الحفاظ على دورهم الفعال في مراقبة التوجهات والأفعال ضمن تقنية الميتافيرس وجمع المعلومات والبيانات الوصفية، ومن ثَمَّ توثيقها ومشاركتها مع الجهات الفعالة للتكتيكات والتقنيات والإجراءات لكافة المجالات.

ويوفر تأمين الميتافيرس وحمايته فرصةً رائعةً للشراكة بين القطاع العام والخاص. ويتطلب الاندماجُ بين الخبراء في هذا المجال والمتخصصين في حماية المجتمع التعاونَ المستمرَّ وتغييرَ طريقة التفكير في مفاهيم العزلة والعمل المنفرد. ولا تؤثر تقنية الميتافيرس على بلد واحد أو شعب واحد أو ثقافة واحدة، فهي منتدى مفتوح للجهات الفعالة على مختلف خلفياتهم وذلك لتحقيق التعاون والتواصل. وكما يتفاعل مستخدمو ومشتركو الميتافيرس بعضهم مع بعض غير عابئين لخلفياتهم وجنسياتهم وثقافتهم، فيجب مشاركة السياسات المحايدة والمراقبة واللوائح وتبادل المعلومات بشكلٍ منتظمٍ.





التوصيات

تُعَدُّ تقنيةُ الميتافيرس ظاهرةً تستطيع أن تتجاوز الحدود والبلاد ومناطق جغرافية محددة؛ ولذلك ينبغي للسياسات الحاكمة لاستخدامها أن تكون محايدةً لتلك العوامل. ومن الضروري أن تجتمع الكيانات الدولية دوريًّا لإنشاء وتقييم وتحديث السياسات ذات العلاقة بتقنية الميتافيرس، ويشمل ذلك تحديد سبب تخزين البيانات ومشاركتها وكذلك الطرق المستخدمة. وينبغي تَجَنُّبُ اللوائحِ المحددةِ، التي تُطَبَّق على قاراتٍ وبلادٍ بعينها؛ حيث يتطلب الميتافيرس إعدادَ نهجٍ عالميٍّ شاملٍ لتلك الحوكمة. ويعمل نهج الحوكمة العالمي المشترك على معالجة العزلة المتأصلة ضمن الميتافيرس؛ ليقلل بذلك الانقسامات المدنية والاجتماعية المحتملة. وبالنظر إلى تطلعات العالم العربي إلى مكانةٍ تجعله وجهةً لجذب تقنية الميتافيرس الناشئة ومبادرات العملة الرقمية، فإنه ينبغي أن تسعى أي أطر سياسية تتعلق بالميتافيرس أو نظام العملات الرقمية إلى الاحتفاظ بتلك المكانة القيادية من خلال تعزيز التعاون العالمي القائم. وينبغي ترتيب الأولويات الخاصة بالتكامل مع المنظمات الدولية وجهات إنفاذ القانون والجهات الرقابية. ويتطلب حفاظ العالم العربي على مكانته ضمن أصول النظام العالمي الرقمي، الحفاظُ على بيئة متسامحة بغض النظر عن وجود لوائح صارمة للأصول الرقمية؛ وذلك لجذب مبادرات أصولٍ افتراضيةٍ للمنطقة.

ولذلك، فإنه من الضروري الأخذ بعين الاعتبار الآليات المدمجة، مثل: التكامل أو تخصيصات لقوائم حظر الطيران. وعلاوة على ذلك، فإن تمكين المنظمات الدولية، مثل: الإنتربول والأمم المتحدة والهيئات الشرطية الدولية، من إجراء الفحوصات الأمنية ودمج معلوماتهم، قد يسهم في استقرار الوضع الأمني العام. ويعمل هذا النهج الشامل على تسهيل التواصل العالمي، وربما يُعَزِّزُ قواعدَ البياناتِ المصممة لتنظيم الأفعال الإجرامية أو تحديد الأفعال غير الملائمة.

ولتحقيق تلك النتائج، فينبغي تحقيق التعاون بين وزراء الحكومات العربية والجهات الرقابية وجهات إنفاذ القوانين والجهات الأمنية ومطوري تقنية الميتافيرس والممارسين كأمور ضرورية. ولا تستطيع الحكومات بمفردها التعامل مع الحماية والأمن والتعليم المستمر ومتابعة الطلبات لنظام الميتافيرس الناشئ. ولضمان إشراك الخبراء في هذا الأمر، فإننا نقترحُ تشكيلَ فريقين متخصصين من فِرَقِ عملٍ متخصصةٍ في تقنية الميتافيرس من خلال مجلس وزراء الداخلية العرب.

وبالتالي فإننا نقترح تشكيل فريقي عمل خاصين بالميتافيرس عبر مجلس وزراء الداخلية العرب أحدهما تقني مسئول عن تطبيقات الميتافيرس والآخر أمني، ويتم التنسيق المشترك بينهما لمواجهة التحديات الاجتماعية والاقتصادية والتكنولوجية. وترتبط طبيعة التنسيق هذه، ارتباطًا مباشرًا بالمخاطر والفرص التي تطرق إليها هذا

التقرير، خاصة فيما يتعلق بالإرهاب الرقمي وأهمية التأهيل الاجتماعي والسياسي لمواجهة الطبيعة المتطورة للميتافيرس. كما يتطلب الجهد المشترك إطلاق منصات ملائمة تصاغ من خلالها أطر سياسات شاملة تسمح بمسارات آمنة وفعالة في التعامل مع تقنيات الميتافيرس.

وينبغي إعداد نهج السياسة بناءً على ثلاث فئات رئيسة:

1. الترويج للسوق: إنشاء سوق افتراضي منظم وقابل للتشغيل المشترك، والذي يتماشى مع الطموح الاقتصادي للتحول الرقمي الإقليمي وإبقاء العالم العربي كوجهة آمنة للميتافيرس والمبادرات ذات العلاقة.
2. حماية المستهلك: تنفيذ التدابير اللازمة لحماية البيانات المؤسسية والفردية، وتوفير المرونة الرقمية، وحماية استثمارات المستهلك، والحفاظ على خصوصية البيانات في الميتافيرس، وكذلك تطبيق متطلبات رأس المال والسيولة وإدارة المخاطر لمشغلي الأصول الرقمية.
3. المرونة القضائية: تنظيم عالم افتراضي من خلال إطار إقليمي ونهائي وقابل للتشغيل المشترك على المستوى الدولي؛ لتسهيل الاتصال ضمن هياكل الامتثال المشتركة، بالإضافة لحماية الولاية القضائية الرقمية للدولة في الوقت ذاته.

وتعتبر تقنية الميتافيرس أكبر من أن تكون بهذا الغموض، وتحتاج إلى سياسة واسعة النطاق؛ لكي تكون فعالة. ومع ذلك فإن المخاطر الأمنية المحددة فيما سبق، لا بد لها أن تندرج تحت الثلاث فئات المذكورة. وسيكون هناك دومًا احتياجًا للتحديد بسبب التغير الدائم للتقنية والمخاطر الأمنية للميتافيرس، التي تحتاج إلى إعادة التقييم من خلال طرح الأسئلة الآتية:

- ما السياسات واللوائح المحددة اللازمة لإدارة الميتافيرس؟
- ما المخاطر المحتملة ونقاط الضعف لتقنية الميتافيرس وكيفية معالجتها؟
- كيف ستتمكن الشركات من التعامل مع المجالات التابعة لها والشبكات والأجهزة للاتصال والتفاعل؟ كيف ستتمكن من حماية معلوماتها الخاصة، مثل: حمايتها للمعلومات الخاصة بعملائها و مستخدميها؟
- كيف ستسمح الشركات لمستخدمي الميتافيرس بالتفاعل والاشتراك؟

- كيف ستتمكن الشركات من إنفاذ سياساتها، وما أفضل الطرق لإنفاذ سلوك للمستخدم؟

- وهذا يشمل التحكم في الأجهزة والبرمجيات، وكذلك مراقبة المستخدمين والعمل على عمليات الأتمتة؛ وذلك للحفاظ على الموارد البشرية في وقت وقوع الأزمات.

مقترح لعقد مؤتمر لتقنية الميتافيرس

يمكن لجامعة نايف العربية للعلوم الأمنية عقد مؤتمر إقليمي حول تقنية الميتافيرس، والذي يُحَدِّدُ أجندةً للعمل عليها بواسطة وزراء الداخلية العرب، وكذلك معالجة جوانبها الأمنية وتعزيز التعاون الإقليمي. وسينتج عن هذا المؤتمر جمع صناع السياسات العرب ومسؤولي الأمن وخبراء الأمن السيبراني وجهات إنفاذ القانون وممثلي القطاع الخاص للتعمق في الإحاطة بالتحديات الأمنية الناتجة عن الميتافيرس. وستتمكن جامعة نايف العربية للعلوم الأمنية من خلال تنظيم هذا المؤتمر من أن تقود التوعية وتُعَزِّزَ التعاون وتُشَكِّلَ المشهد الأمني للميتافيرس في المنطقة العربية. وسيتم التعامل مع نتائج وتوصيات المؤتمر كأساس للسياسات والمبادرات الإقليمية لضمان توفير بيئة ميتافيرس آمنة ومحمية. ومن ضمن الموضوعات الأساسية للاستخدام السيئ للميتافيرس هو التداخل والترابط بين العديد من مجالات التحدي الثمانية. وينبغي أن يكون مؤتمر جامعة نايف العربية للعلوم الأمنية بمثابة منصة إطلاق واسعة للتعاون بين المسؤولين العرب والخبراء المتخصصين مع الاعتراف بالتميز الذي تقدمه مجموعة المخاطر والتهديدات للنظام الافتراضي والفرص التي توفرها.

وتشمل الموضوعات الرئيسة المعدة للمناقشة:

- فهم تقنية الميتافيرس: اكتساب أفكار حول هيكل الميتافيرس ونموه والمخاطر الأمنية المرتبطة به.
- حالة التهديد: تحليل التهديدات السيبرانية الناشئة ضمن الميتافيرس بما في ذلك خرق البيانات وسرقة الهوية وإمكانية الاستغلال من خلال المنظمات الإجرامية.
- السياسة واللوائح: استكشاف ضرورة إعداد أطر تنظيمية قوية وسياسات فعالة لحماية الميتافيرس. ومناقشة قواعد الحكومات والأطراف المعنية في القطاع في صياغة تلك التدابير.
- التعاون العربي: التأكيد على أهمية التعاون بين الدول العربية ومعالجة المسائل الأمنية المرتبطة بالميتافيرس المجمعة. وتسليط الضوء على دراسات الحالة الناجحة للتعاون الإقليمي.

- بناء القدرات: التركيز على مبادرات بناء القدرات وبرامج التدريب لتعزيز قدرات إنفاذ القوانين وخبراء الأمن السيبراني في مكافحة تهديدات الميتافيرس.
- الشراكات في القطاع العام والخاص: تعزيز التعاون بين الوكالات الحكومية والقطاع الخاص لتطوير الحلول الأمنية المبتكرة ومشاركة المعلومات.

فريق عمل أمن الميتافيرس

قد يُشَكِّلُ وزراءُ الداخلية العرب فريقَ عملٍ للميتافيرس، وذلك للمعالجة الفعالة للتحديات الناشئة عن النظام الناشئ للميتافيرس والأنظمة اللامركزية. وتم تحديد التعاون الإقليمي من أجل مكافحة الأنشطة الإرهابية ومنع الاستغلال ضمن تقنية الميتافيرس، وتشمل الإرهاب والتطرف والاتجار بالمخدرات وغسل الأموال وسرقة الملكية الفكرية واستغلال الأطفال. وينبغي تكليف فريق عمل أمن الميتافيرس بتنسيق التحقيقات بين الدول المشاركة، مع التركيز المحدد على تعطيل وتفكيك المنظمات الإجرامية في الميتافيرس. ويهدف فريق العمل للتصدي بفاعلية لسوء الاستخدام الناشئ عن التقنية من خلال الشبكات الإجرامية والجهات الفاعلة غير الحكومية من خلال تعزيز التعاون المدعم وتخصيص موارد إضافية من كافة البلاد العربية. ويتزامن إنشاء فريق عمل أمن الميتافيرس مع رؤية ورسالة جامعة الدول العربية، التي تدعو إلى تعزيز وحدة الصف والتعاون بين الدول العربية. ويمنح فريق العمل الأولوية لأمن وحماية مستخدمي الميتافيرس واليقضة ضد التهديدات الناشئة من خلال المشاركة الفعالة مع الميتافيرس. ويمكن أن يسهم فريق العمل بصورة واضحة في تحقيق الأمن والاستقرار العام في المنطقة من خلال الاستفادة بالخبرات المشتركة وتطبيق التدابير السليمة. ويبرز هذا الفريق التكيف مع التقدم التقني وحماية الأفراد من المخاطر المحتملة المرتبطة بالأنشطة الإجرامية في الميتافيرس.

فريق عمل سياسة الميتافيرس

نظرًا للطبيعة التحويلية للميتافيرس الناشئة وعدم وجود إطار سياسة ثابت، فمن الضروري لوزراء الداخلية العرب إنشاء فريق عمل مَعْنِيٍّ بسياسات الميتافيرس. وينبغي على فريق العمل التعاون مع الوكالات العربية السيبرانية لإعداد أطر سياسة مشتركة، والتي تعيد ترتيب أولويات الأوجه الأمنية للميتافيرس مع اعتبار كافة العناصر الأمنية ذات الصلة. إن الغرض الأساسي لفريق عمل سياسة الميتافيرس هو معالجة التحديات الفريدة

الناشئة عن الميتافيرس، وكذلك ضمان صياغة سياسات شاملة من شأنها حماية مصالح المنطقة العربية. ويستطيع فريق العمل وضع الإستراتيجيات الفعالة لتعزيز التدابير الأمنية في الميتافيرس من خلال الاستفادة من الخبرات والمعرفة الخاصة بالوكالات السيبرانية.

وينبغي أن تتضمن أطر السياسة، التي أعدها فريق عمل سياسة الميتافيرس، أَوْجُهًا متعددةً على سبيل المثال لا الحصر: خصوصية البيانات، وحماية الهوية، وحقوق الملكية الفكرية، والسلامة عبر الإنترنت، ومكافحة الجرائم السيبرانية. وينبغي التركيز بوجه خاص على ضمان أمن وحماية الأفراد والشركات والبنية التحتية الرئيسة التي تعمل ضمن الميتافيرس. ويستطيع فريق العمل الاستفادة من خبراته في الأمن السيبراني والتهديدات الرقمية للتعرف على المخاطر المحتملة وإدماج إستراتيجيات تقليل فعالة وأطر للسياسة من خلال إشراك وكالات سيبرانية عربية بطريقة فعالة في عملية إعداد السياسات. وسيخلق هذا النهج التعاوني أطرًا سياسيةً قويةً تُعَزِّزُ بيئة الميتافيرس وتجعلها آمنةً وموثوقةً. وينبغي اشتراك فريق العمل في الحوار القائم مع نظرائهم الدوليين، ومشاركة أفضل الممارسات وحشد الجهود لمعالجة التحديات الأمنية العالمية ذات العلاقة بالميتافيرس. وسيسهم هذا التعاون في إنشاء معايير وتوجيهات إرشادية متناغمة من شأنها تعزيز الاستخدام الآمن والمسؤول للميتافيرس على المستوى العالمي.

ومن المزايا الإضافية الحساسة من حيث الوقت للتعاون السيبراني العربي مع فريق عمل سياسة الميتافيرس تلبية احتياجات البنية التحتية للشبكات الخاصة بالميتافيرس. إن الاستفادة من الخبرة السيبرانية داخل الدول العربية تجلب المعرفة الحالية بالأمن السيبراني إلى الميتافيرس، ولكن هذا المجال سوف يجلب تهديدات وتحديات غير متوقعة بسبب اعتماده على مجموعة من التقنيات والأنظمة المتقدمة، مثل: إنترنت الأشياء والحوسبة السحابية. وهذا سيتطلب بلا شك وضع معايير أمنية جديدة، تتداخل مع معايير الشبكة التقليدية، ولكنها تتباعد بأساليب غير متوقعة. وهذه المنفعة حساسة للوقت؛ لأنه مع تأسيس الميتافيرس ووضع أطر السياسات المصاحبة لها، فإن تلك الدول والمنظمات التي تتصرف بسرعة قد تحدد نمط ومضمون العمل اللاحق.

وقد يتضمن جدول أعمال السياسات الافتتاحي لفريق عمل سياسة الميتافيرس، الذي يعكس هذا التركيز، ما يأتي:

- سياسة الاستخدام المقبول: تطبق الجهات الرقابية سياسات الاستخدام المقبول بطريقة مباشرة، وتعمل على الابتعاد عن الميل إلى طمس مثل هذه القواعد في اتفاقيات لغة المستخدم النهائية المطولة، أو الخطوط الصغيرة أو غيرها من الأماكن الغامضة التي يواجهها المستخدمون في الويب 2.0. وبالنسبة

لجميع جوانب الميتافيرس، يجب أن تظهر الشعارات في البداية عند تسجيل الدخول، تمامًا مثل أي متطلبات موقع، تشترط عمر 18 عامًا أو أكبر، مع عرض القواعد الأساسية للسلوك المناسب بشكل واضح وفوري. وقد تفكر الشركات أيضًا في نقل سياسات «السماح أو الرفض» إلى الميتافيرس من الإنترنت التقليدي لحماية الوصول إلى البيانات الحساسة من أجل الحفاظ على الخصوصية والأمن الوطني والسلامة العامة.

- سياسات الخصوصية والحماية الخاصة بالبيانات الأولية: إن النمو الهائل للبيانات وجمع البيانات وتخزينها، الذي يصاحبه تطوير تقنية الميتافيرس ونشرها، يزيد من المخاطر بالنسبة لسياسة حماية البيانات الأولية الفورية التي وضعتها الجهات الرقابية. ويجب أن تركز السياسة بشكلٍ دقيقٍ على حماية البيانات، وتجميع إرشادات الخبراء بشأن إعداد تدابير حماية البيانات قبل ترميزها. واستلهامًا من البنية التحتية المبرمجة، تعد حماية مستودعات الرموز المصدرية أمرًا بالغ الأهمية لخصوصية البيانات، وهو ما يضمن وجود وسائل مشتركة داخل الإدارات والشركات لإنشاء أساس لتخزين آمن للبيانات وأسس منطقية قوية لتطهيرها. ولا يتم تشجيع الشركات، خاصة داخل الميتافيرس، على استخدام أدوات حماية البيانات المخصصة والمصممة ذاتيًّا، بل يجب بدلًا من ذلك اعتماد خدمات سلسلة الكتل المبسطة (على سبيل المثال: سلسلة الكتل المدارة من أمازون) التي تشرف عليها جهات رقابة الأصول الافتراضية المحلية لتخزين البيانات. ويجب صياغة معايير حماية المستهلك بما يتماشى مع المعايير الإقليمية للسماح بقابلية التشغيل البيني للمنصة عبر الحدود والتوافق مع الولايات القضائية.

- التشفير الشامل بدون استثناء: يعد التشفير الشامل، أي أمان البيانات في كل مرحلة من مراحل النقل، ضرورةً ملحةً في الميتافيرس. وينبغي مراعاة إحدى خوارزميات التشفير «المتماثلة» الأكثر أمانًا، وهي معيار التشفير المتقدم، والتي تفتخر بحكومة الولايات المتحدة كعميل، مثالًا رئيسًا لأنواع الأساليب المستخدمة لتشفير البيانات في الميتافيرس.

- المرونة الرقمية: دمج تحسين تقنية التزييف العميق المستخدمة لاستهداف الشخصيات العامة والمواطنين العاديين على حدٍّ سواء مع الطبيعة التفاعلية للميتافيرس بطرقٍ يحتمل أن تكون خطيرة. ومن ثم، فإن الكشف عن التزييف العميق يشمل تثقيف الجمهور حول السمات المميزة لإنشائها والغرض منها. وقد أنشأ معهد ماساتشوستس للتقنية أدوات عبر الإنترنت لتدريب الجمهور على التزييف العميق، ويوفر المعهد أيضًا اختبارات بشأن التمييز بين الفيديو أو الصوت الأصلي مقابل

المزيف. وتوفر الميتافيرس أيضًا تدريبًا أو عروضًا توضيحية لاكتشاف التزييف العميق والتأكيد على سماته المتسقة والمحددة والمشتركة. ويمكن للجهات الإدارية التي تهدف إلى حماية الميتافيرس توفير مواد التدريب والتعريف، والعمل والتعاون مع الجامعات ورواد صناعة التقنية والجهات الإدارية العالمية لتوفير معلومات حديثة والتدريب التعريفي.

منظمة الأصول الافتراضية العربية

مع ظهور جميع الأصول الافتراضية الناشئة في الميتافيرس، يحتاج العالم العربي إلى إنشاء جهةٍ رقابيةٍ إقليميةٍ للأصول الافتراضية، التي من شأنها أن تكون أحد الأنماط المناسبة للرقابة الإقليمية تحت مظلة جامعة الدول العربية. وعلى الحكومات العربية إنشاء منتدى محلي تديره جهة رقابية معتمدة من الحكومة؛ لتوفير اتصالٍ أفضل بين مقدمي خدمات الأصول الافتراضية والجهات الرقابية، والسماح بالرقابة الحكومية الفعالة في العالم الافتراضي. وبرزت سُلطة دبي لتنظيم الأصول الافتراضيّة، وهي أول جهة تنظيمية مستقلة في العالم للأصول الافتراضية، كسلطة توجيهية تتسم بالشفافية والثقة في صناعة الأصول الافتراضية سريعة النمو في دولة الإمارات العربية المتحدة وخارجها، وتمتد مهمتها على مستوى العالم، بهدف إعداد إطار قابل للتطبيق لتنظيم هذا المجال. وتم إطلاق سلطة دبي لتنظيم الأصول الافتراضية في مارس 2022، وتعمل كهيئة تنظيمية مسؤولة عن الإشراف على الأصول الافتراضية والأنشطة ذات الصلة في مناطق مختلفة في جميع أنحاء دبي، باستثناء مركز دبي المالي العالمي. وتحمي سلطة دبي لتنظيم الأصول الافتراضية المستثمرين، وتضع معايير دولية لإدارة الأصول الافتراضية، وتدعم رؤية الاقتصاد بلا حدود، وذلك من خلال إعداد إطار قانوني متقدم.

وقدمت سلطة دبي لتنظيم الأصول الافتراضية مؤخرًا لوائح الأصول الافتراضية والأنشطة ذات الصلة لعام 2023. وتضع هذه اللوائح إطارًا شاملًا للأصول الافتراضية التي تتمحور حول الاستدامة الاقتصادية والأمن المالي عبر الحدود. ويكفل إطار الأصول الافتراضية اليقين التنظيمي، وهو ما يوفر الوضوح فيما يتعلق بمسؤوليات المشغلين في السوق، مع التركيز على مكافحة مخاطر غسل الأموال وتمويل الإرهاب المرتبطة بالتقنيات المتقدمة. ويجب على الكيانات المرخصة داخل دولة الإمارات العربية المتحدة الالتزام بالمعايير الموحدة لتأمين المخاطر ومكافحة غسل الأموال. وتتعاون سلطة تنظيم الأصول الافتراضية أيضًا بشكل نشطٍ مع الكيانات العالمية المعنية لإعداد لوائح فعالة ومصممة خِصِّيصَى، وتعزيز حماية العملاء والحد من الممارسات غير القانونية في مجال الأصول الافتراضية. وستكون هذه الجهة التنظيمية أيضًا مسؤولة عن إصدار تراخيص

التشغيل للشركات ومقدمي خدمات الأصول في كل مناطق النشاط. ويجب أن تحدد الأطر التنظيمية للأصول الافتراضية مبادئ توجيهية واضحة من شأنها أن تخفف من احتمالات التهديدات المرتبطة بالأصول الافتراضية، وتجذب المبادرات الناشئة إلى المجال الافتراضي، وتُعَزِّزُ المسؤوليات المشتركة.

ويجب أن تسعى منظمة الأصول الافتراضية العربية، التي تم إنشاؤها في صورة أطر عمل، مثل: سلطة تنظيم الأصول الافتراضية، والتي تم إنشاؤها خِصِّيصَى للميتافيرس، إلى حماية المعاملات داخل هذا العالم الافتراضي مع احترام خصوصية المستخدم والعميل أيضًا. ويمكن للمنظمة توفير تدابير حماية عديدة لهذه الغايات، وتشمل ما يأتي:

- لائحة الهوية الرقمية: أن تكون معلومات التعريف الشخصية في الهوية الرقمية ليست جديدة. وتتطلب العديد من تطبيقات وخدمات العملات المشفرة رفع رخصة قيادة أو الاتصال بحساب مصرفي لمنع الاحتيال المالي والجريمة. ويمكن أن تطلب الميتافيرس المزيد من معلومات التعريف الشخصية وإثبات الهوية لتقليل الاحتيال. وإن إرفاق الهوية المادية للمستخدمين (رخصة القيادة، رقم الضمان الاجتماعي، جواز السفر، شبكية العين أو بصمة الإصبع) من شأنه أن يساعد على التحقق من الهوية عبر الإنترنت. وعلاوة على ذلك، فإن طلب هذه الوثائق الحساسة والسرية يتطلب أيضًا سياسات حماية بيانات عالية الدقة وأكثر فاعلية.

- مراقبة المعاملات النقدية وعمليات الإفصاح الضرورية: يمكن لكل حكومة في منطقة الشرق الأوسط وشمال إفريقيا أن تحدد مبالغ خاصة توضح للمسؤولين الحكوميين أن المعاملات الخاصة بالعملات المشفرة كبيرة جدًّا، بحيث لا يمكن قبولها عبر الإنترنت، وربما تكون مؤشرًا على نشاطٍ ضار. وفي المقابل، يمكن أن تُوَفِّر المعاملات، التي تتجاوز هذا المبلغ، مسارًا لعمليات الإفصاح للسلطات التنظيمية عندما تكون هذه المعاملات ضرورية لدعم وظائف الخدمة أو المنظومة. ويمكن لكل دولة في منطقة الشرق الأوسط وشمال إفريقيا أن تضع حدودًا خاصة لها، ويمكن للجهة الإدارية الإقليمية، التي تتألف من خبراء تقنيين وممثلي الصناعة والمسؤولين الحكوميين وموظفي إنفاذ القانون والجهات الرقابية المالية من العالم العربي، أن تعمل على تحديد بداية تشير إلى نشاط إقليمي ضار محتمل، مثل: العلاقات مع الإرهاب أو مؤشرات على تهريب الأسلحة. ويجب أن يكون حجم الجهة الإقليمية أعلى مما تحدده كل دولة على حدة كمستوى راحة لها.

- قيود البيانات الجغرافية الانتقائية: إذا علم القادة العرب الإقليميون أن بعض المدن أو المناطق الجغرافية معروفةً بأنها ترتكب أنشطةً إرهابيةً، فيمكن للقادة العرب العمل مع شركات الاتصالات المحلية ووكالات إنفاذ القانون لمنع عناوين بروتوكول الإنترنت أو التبادلات الكاملة المعروفة بأن تعمل داخل تلك المناطق الجغرافية نفسها. ويمكن أن يكون هذا الإجراءُ فَعَّالًا بشكل خاص عندما تقوم الجهات الفاعلة الخبيثة بتحويل عملاتها المشفرة إلى أموال نقدية. وإذا لم تتمكن هذه الجهات من إجراء المعاملات عبر الإنترنت، وتم منع منصات التداول التي يعملون معها من إنشاء اتصال بالميتافيرس، فقد يؤدي ذلك إلى تقليل كمية الأموال التي يتلقاها الإرهابيون بشكل كبير، فضلًا عن منعهم من استخدامها في شكل نقدي.
- مسار معالجة المعلومات: يمكن تحقيق التوازن بين الوفاء بالالتزامات القانونية، والحفاظ على خصوصية مستخدمي تقنية الميتافيرس من خلال تضييق نطاق المعلومات المطلوبة للمستخدمين أو لمعاملات أو مناطق محددة. ويجمع المسؤولون الحكوميون وجهات إنفاذ القانون البيانات الوصفية المرتبطة بمستخدمي الإنترنت ويقومون بالتحقق منها، مثل: البصمات والأسماء المستعارة وعناوين البريد الإلكتروني ومواقع الويب وأرقام المحفظة وأرقام معاملات سلسلة الكتل وأرقام الهواتف والبيانات الوصفية. وينبغي توفير كل هذه المعلومات بحيث يتم التحقيق فقط في النشاط الإجرامي المشتبه فيه، وحماية خصوصية المواطنين غير المشاركين في أنشطة غير مشروعة.

وعندما يتعلق الأمرُ بالعملات المشفرة، تتداخل قوانينُ «اعْرَفْ عَمِيلَكَ» أيضًا مع لوائح الخصوصية، وإن كان ذلك بمستويات متفاوتة من الصرامة. وتختص قوانين «اعرف عميلك» بتحديد هويات العملاء والتحقق منها، وهو ما يساعد على مكافحة السرقة والاحتيال والفساد. وتفتقر بعض المنصات إلى كل متطلبات «اعرف عميلك»، وهو ما يعني أن مقدمي خدمة التبادل ليس لديهم معرفة بهويات عملائهم. وتعتبر مثل هذه المنصات محفوفة بالمخاطر؛ مع قدرتها على توفير خصوصية محسنة، بما يجعلها جذابةً لأنواع معينة من مستخدمي العملات المشفرة.

ومن الضروري أن تمتنع الميتافيرس عن السماح بتبادل العملات المشفرة على المنصات التي تفتقر إلى أي شكل من أشكال قواعد «اعرف عميلك». ويقدم تنفيذ بروتوكولات «اعرف عميلك» الأساسية أو الشاملة درجات متفاوتة من الأمان والخصوصية. وقد تفرض منصة «اعرف عميلك» الأساسية حدودًا على أحجام التداول الأسبوعية أو الشهرية، وقد تطلب ربط حساب مصرفي أو بطاقة ائتمان للتحقق من صحة معلومات المستخدم.

ومن ناحية أخرى، تتطلب العملية القائمة على منصة «اعرف عميلك» على نحو شامل قيام الشركات بالتحقق من هويات المستخدمين من خلال المستندات القانونية، مثل: فواتير المرافق أو الهوية الصادرة عن الحكومة، حيث يتضح أن معظم المنصات التي تعمل على تسهيل أحجام التداول الكبيرة تفرض إجراءات شاملة على عملية «اعرف عميلك».

وعليه، يجب أن تسعى الجهة الإدارية المسؤولة عن الميتافيرس على نطاق عالمي إلى حماية المعاملات داخل هذا المجال الافتراضي مع احترام خصوصية المستخدم والعميل، ويجب التعاون بين مشغلي تحليلات سلسلة الكتل لتوفير خدمات تتبع الرموز المميزة وتحديد المحفظة بدلاً من تقييد اعتماد النظام، مع مراعاة أن التدابير الخاصة بعملية «اعرف عميلك» قد تكون غير قابلة للتطبيق على بعض جوانب تقنية الميتافيرس والمعاملات المتصلة بها.

المبادرات الرقمية والافتراضية لمحو الأمية

يجب أن يقود وزراء الداخلية العرب حملات محو الأمية الرقمية والافتراضية، التي تشمل الجهود التعليمية الرامية إلى مواجهة التهديدات السيبرانية في العالم الافتراضي، على أن يتم إجراء هذه الحملات بالتعاون مع الوكالات السيبرانية لتوجيه رسالة موحدة وشاملة عن الأمن السيبراني إلى السكان العرب. ونظرًا لضعف الوطن العربي الواضح في مواجهة الهجمات السيبرانية، فمن الضروري تطبيق هذه الحملات على المستويين المؤسسي والفردي، بحيث تتولى الحملات على المستوى الفردي أهمية تثقيف المستخدمين حول المخاطر والأخطار المرتبطة بالميتافيرس وخصوصية البيانات والسلامة الشخصية. بالإضافة إلى ذلك، يجب على المستخدمين تحمل مسؤولية تنفيذ تدابير الأمان الخاصة بهم في حال الانتقال إلى أنظمة البيانات التي يتحكم بها المستخدم.

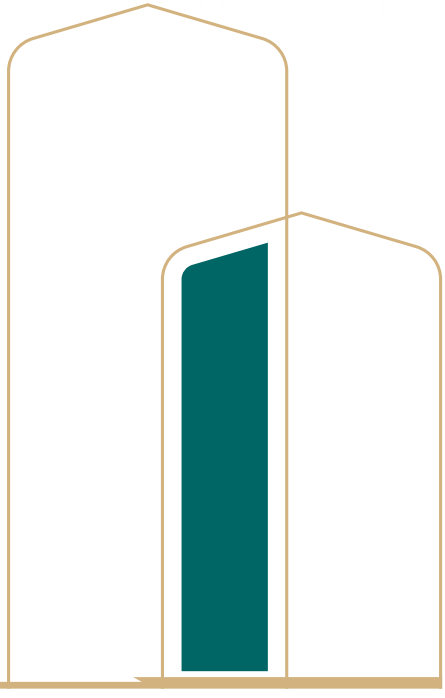
وتركز حملات محو الأمية بالعالم الافتراضي على تثقيف المستخدمين بشأن ما يأتي:

- تهديدات المعلومات المضللة المتمثلة في (التزييف العميق والهوية الرقمية المضللة والتحريف والشركات الصورية).
- الجريمة الافتراضية المتمثلة في (عمليات الاحتيال والبرامج الضارة وتهديدات برامج الفدية).
- التدابير الأمنية الوقائية المتمثلة في (حماية المفاتيح الخاصة، وتبادل المعلومات، وتخزين العبارات الأولية، والمصادقة متعددة العوامل).

- تقنيات التصيد الاحتيالي الشائعة (التصيد بالرمح)، التي تستهدف المستخدمين عبر البريد الإلكتروني والرسائل النصية القصيرة.

ويُمثل المنهج المُقدَّم من أكاديمية الميتافيرس بالرياض نقطةَ انطلاقٍ لتحديد برنامج ناجح لتعليم محو الأمية بالعالم الافتراضي. وبدأت بالفعل الدورات التدريبية والمعسكرات بالظهور للتسجيل العام: تقدم أكاديمية طويق دورات لفترات متباينة متاحة إلكترونيًّا وماديًّا (Alkhunaizi, 2023). وإذا كان المنهج المقدم من أكاديمية الميتافيرس بفرنسا يحتوي على أي مواد تنطبق في محتواها على منطقة الشرق الأوسط وشمال إفريقيا، فإن التعاون بين صُنَّاع السياسات والمعلمين الأوروبيين من ناحية، وصناع السياسات والمعلمين في العالم العربي من ناحية أخرى، من شأنه أن يُوسع التعاليم ويُحسِّن المواد المُقدَّمة للمجتمع.

ونظرًا للتطور السريع الحادث في مجال التقنية، فإنه يجب أن يتواءم هذا التطور أيضًا مع تطور عمليتي التدريس والتدريب، حيث يتعين على قادة العالم العربي ومسؤوليهم المكلفين بإنفاذ القانون، العمل عن كثب مع قطاع التعليم لضمان تقديم برنامج تدريبي مناسب. ويمكن أن تُشَكِّلَ الرياضُ فيما بعد فريقَ عملٍ آخر، مع التركيز على التعليم العام فيما يتعلق بمخاوف الميتافيرس والسلامة، وإجراء هذا التدريب في جميع أنحاء العالم العربي. وعلاوة على ذلك، تقود جهود المملكة العربية السعودية تأسيس أكاديميات ميتافيرس أخرى ومشاركة الدروس المستفادة والنجاحات والاحتياجات المستقبلية مع كلٍّ منها، ولضمان وعي المستخدم، تُعرض اللافتات والشروط والأحكام المشابهة لاتفاقيات المستخدم النهائي، وتُحدد بصورة واضحة في بداية كل جلسة جديدة. ويجب أن تُطالب تطبيقات العالم الافتراضي بعرض لافتات الوصول، التي تحذر المستخدمين من المخاطر المحتملة، وينبغي تنفيذ تدابير أمنية لضمان مشاهدة المستخدمين لمعلومات محو الأمية قبل الوصول إلى منصات الميتافيرس. ويتمثل أحد الجوانب المهمة لهذه الجهود في إنشاء إطارٍ للشروط والأحكام التي تُحَدِّد بوضوحٍ العلاقة التعاقدية، أو عدم وجودها، بين الشركات ومقدمي خدمات الأصول الافتراضية والمستخدمين، حيث يساعد هذا الإطار على توفير الوضوح والحماية لجميع الأطرافِ المَعْنِيَّةِ.



الخاتمة

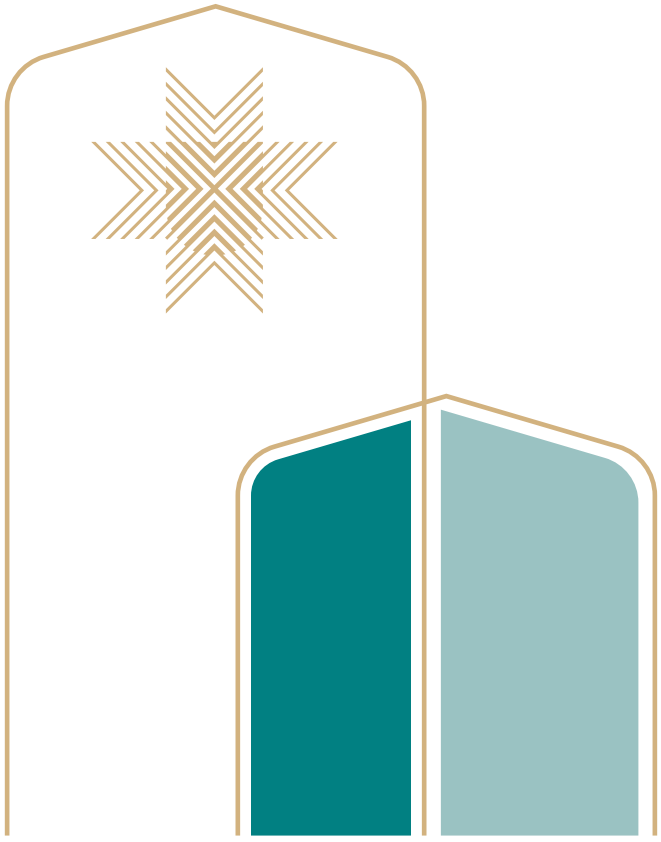
إنَّ تقنيةَ الميتافيرس لا تُمَثِّلُ اتجاهًا عابرًا في مجال التقنية، ولكنها قوةٌ تحويليةٌ تُعيد تشكيل الصناعات والاقتصادات والمجتمعات بصورة سريعة. وتُقَدِّمُ الميتافيرس فرصًا اقتصادية غير مسبوقة، كما اتضح لنا في هذا التقرير، حيث تشير التقديرات أنه بحلول عام 2030 سيجري تقييم محتمل للسوق بقيمة 1.3 تريليون دولار أمريكي. وعلاوة على ذلك، استقطبت هذه الإمكانات الجذابة استثمارات كبيرة من الشركات في جميع أنحاء العالم، لا سيما في الولايات المتحدة والصين، التي تتنافس على الهيمنة في هذه الحدود الرقمية الجديدة. أما بالنسبة للعالم العربي، فتبرز تقنية الميتافيرس باعتبارها وسيطًا للتحول الرقمي الإقليمي، وتضع الدولُ العربيةُ نفسها لجني فوائد هذا التحول النموذجي مع إيلاء قدرٍ من الاهتمام المتزايد بتقنيات الميتافيرس وتحسين الأطر التنظيمية. وقد شهدت منطقة الشرق الأوسط وشمال إفريقيا بالفعل طفرةً في معاملات العملات المشفرة، وهو ما يشير إلى استعداد المنطقة لاعتماد الميتافيرس. وعلاوة على ذلك، تتخذ دولٌ (مثل: الإمارات العربية المتحدة، والمملكة العربية السعودية) تدابيرَ استباقيةً لدمج الميتافيرس في أهداف سياستها العامة، والاستفادة من إمكاناتها في النمو الاقتصادي والسياحة والتعليم والرعاية الصحية.

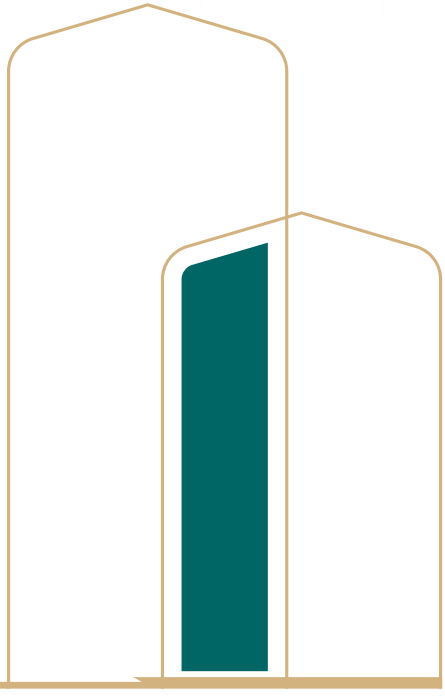
ويؤكد النمو الهائل لقاعدة مستخدمي الميتافيرس أهميتها، نظرًا لوجود أكثر من 400 مليون مستخدم نشط شهريًّا، معظمهم من الشباب، وهو ما يلقي الضوء على أن الميتافيرس تستحوذ استحواذًا كبيرًا على مُخَيِّلة العامة وتجذب انتباههم. ومع الاستمرار المتزايد في اعتماد تلك التقنية، سيكتسب الميتافيرس زخمًا أكبر، وهو ما يدفع حدود التجارب الافتراضية إلى آفاق جديدة. ومع ذلك، فإن الميتافيرس لا يخلو من المخاطر، لما يُقَدِّمُه من فرصٍ وتحدياتٍ على حَدٍّ سواء من منظور الأمن الوطني. ويمكن استغلال إخفاء الهوية والأمن المتصور للمساحات الافتراضية من قِبَل الجهات الفاعلة في التهديد بالجرائم السيبرانية والإرهاب والتجسس. بالإضافة إلى ذلك، يمكن أن تصبح الميتافيرس وكرًا لانتشار المعلومات المضللة والأيديولوجيات المتطرفة؛ لذلك، من الضروري للحكومات والمنظمات وضع تدابير أمنية قوية والتعاون دوليًّا للتخفيف من هذه المخاطر وضمان بقاء الميتافيرس بيئةً آمنةً وموثوقةً.

وَيُعَدُّ تنظيمُ الميتافيرس تحديًا كبيرًا؛ لأنه يتطلب تحقيقَ توازنٍ دقيقٍ بين ضرورات الأمن الوطني وحماية الحقوق والحريات الفردية. ويجب على صُنَّاعِ السياسات التعامل مع القضايا المتعلقة بخصوصية البيانات وسلامة المستخدم وحقوق الملكية الفكرية مع تعزيزِ بيئةٍ تُشَجِّع على الابتكار والنمو الاقتصادي. ويعد التعاون الدولي ووضع معايير مشتركة وأطر قانونية أمرًا بالغ الأهمية للحوكمة الفعالة للميتافيرس.

وعلاوة على ذلك، تَفِي السياساتُ، التي أوصينا بها هنا، بالاحتياجات الخاصة بالتنمية التجارية والاقتصادية وحماية المستهلك وحماية الولايات القضائية الرقمية للدول، باعتبارها سياسات عملية ومعترفًا بها؛ لوعيها بضرورة التعاون الإقليمي من أجل التبني الناضج للميتافيرس وتقنياته المختلطة. ونحن على يقين أن مؤتمر الميتافيرس بجامعة نايف يمكن أن يكون بمثابة نقطة انطلاقٍ لِتَبَنِّي المنطقة العربية لنظامٍ افتراضيٍّ من خلال البناء على اتجاه قائم، حيث يتضمن المؤتمر: التعرف على التحديات والمخاطر التي يشكلها الميتافيرس والتعبير عنها من أجل الاستفادة من فوائده العديدة. وتدرك مثل هذه المؤتمرات أن تحديات الميتافيرس ومخاطره مشتركة، وهو ما يوفر الزخم لتشكيل فريق عمل مسؤول عن تأمين الميتافيرس من قِبَل وزراء الداخلية العرب، وفريق عمل سياسة الميتافيرس التي تتعاون مع الوكالات السيبرانية العربية. ويتسق نطاق كل منها مع المخاطر والفرص المشتركة التي يتعين على الدول العربية اغتنامها ضمن هذا النظام الافتراضي بشكل مشترك. إن دور المعاملات المالية ضمن هذا النظام واسعُ النطاقِ وذو أهمية كبيرة، وهو ما يُحَفِّز التوصية بإنشاء منظمة عربية للأصول الافتراضية لتنظيم وتقنين تبادل الأصول الافتراضية في الميتافيرس. وأخيرًا، تتطلب الطبيعة الديناميكية للتقنيات الناشئة أشكالًا جديدة من محو الأمية الرقمية والافتراضية إلى جانب اعتماد الميتافيرس. وعليه، سيحقق المسئولون الذين يقودون حملات محو الأمية الرقمية والافتراضية، بالتنسيق مع الوكالات السيبرانية، هدفًا مشتركًا يتمثل في: مواكبة نظام افتراضي دائم التغير، ولكنه مستقر بشكل أساسي بطريقة مستنيرة ولصالح الجميع.

وَيُمَثِّلُ الميتافيرس نقلةً نوعيةً لما له من قدرة على إعادة تشكيل الطريقة التي نتفاعل ونعمل ونتصرف بها، بالإضافة إلى قوته التحويلية التي تمتد إلى ما هو أبعد من النظرية والتجريب، مع ظهور تطبيقات واقعية بالفعل في مجالات، مثل: التدريب العسكري والاتصال العالمي. وتكمن جاذبية الميتافيرس في قدرته على إنشاء تجارب رقمية غامرة، وتمكين التفاعلات الاجتماعية الافتراضية، وإحداث ثورة في التجارة الإلكترونية وملكية الأصول. وعلاوة على ذلك، يتضح أنه كلما تطورت التقنيات، استمرت تقنية الميتافيرس في التطور، وهو ما يوفر فرصًا هائلة وتحديات معقدة. ويمكن للعالم العربي أن يكون لاعبًا رائدًا في هذه الثورة الرقمية من خلال تبني إمكانات الميتافيرس وتجنب مخاطرها من خلال التنظيم الفعال. وتحمل الميتافيرس مُعولات الازدهار الاقتصادي، وتعزيز الأمن الوطني، وحدودًا جديدةً للإبداع البشري. والأمر متروك لِصُنَّاعِ السياسات وأصحاب المصلحة والمجتمع ككلٍّ؛ لاغتنام هذه الفرصة وتشكيل مستقبل الميتافيرس بطريقةٍ تُفِيدُ الجميع





المراجع

المراجع

Alobaid, M. (2021, September 3). Intellectual property: A Mena blind spot in a new economic age. PennLaw. https://www.law.upenn.edu/live/blogs/98-intellectual-property-a-mena-blind-spot-in-a-new

Analysis Group. (2020). The Potential Global Economic Impact of the Metaverse. https://www.analysisgroup.com/globalassets/insights/publishing/2022-the-potential-global-economic-impact-of-the-metaverse.pdf

Arab News. (2023, May 18). Metaverse could contribute up to $38 billion to Saudi economy. Arab News. https://www.arabnews.com/node/2305576/media

Argyle, L. P, Busby, E. C., Bail, C., Howe, T., Rytting, C., & Wingate, D. (2023). AI Chat Assistants can Improve Conversations about Divisive Topics. https://doi.org/10.48550/arXiv.2302.07268

Baig, A. I. (2023). Learning in the Metaverse: Challenges, Opportunities, and Threats (Doctoral dissertation, Department of Computing A thesis submitted in partial fulfillment of the requirements for the degree of Masters of Science in Innovative Technologies in Learning (MS ITL) In School of Electrical Engineering & Computer Science (SEECS), National University of Sciences and Technology).

Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021, March). On the dangers of stochastic parrots: Can language models be too big? . In Proceedings of the 2021 ACM conference on fairness, accountability, and transparency (pp. 610-623).

Bjola, C. (2022, February 27). Exploring the Metaverse and Its Implications for Digital Diplomacy. USC Center on Public Diplomacy. https://uscpublicdiplomacy.org/blog/exploring-metaverse-and-its-implications-digital-diplomacy.https://www.thenationalnews.com/business/technology/2022/05/19/middle-east-and-africa-was-region-least-targeted-by-ransomware-attacks-in-2021-study-says/.

Bremmer, I. (2023, June 17). The next global superpower isn't who you think. Foreign Policy. https://foreignpolicy.com/2023/06/17/china-russia-us-multipolar-world-technology

Brown, S. (2022, July 19). What Second life and Roblox can teach us about the metaverse. MIT Sloan. https://mitsloan.mit.edu/ideas-made-to-matter/what-second-life-and-roblox-can-teach-us-about-metaverse

ByBit Learn. (2023, February 22). Metaverse statistics 2023: All the facts & figures you need to know. https://learn.bybit.com/metaverse/metaverse-statistics/

Cabral, A. (2023a, February 10). Xrai glass picks Saudi Arabia as entry point for Middle East expansion. The National. https://www.thenationalnews.com/business/technology/2023/02/10/xrai-glass-picks-saudi-arabia-as-entry-point-for-middle-east-expansion

Cabral, A. R. (2023b, February 7). Meta launches the MENA region's first Metaverse Academy in Saudi Arabia. The National. https://www.thenationalnews.com/business/technology/2023/02/07/meta-launches-the-mena-regions-first-metaverse-academy-in-saudi-arabia/

Chainalysis. (2022). The Chainalysis 2022 Geography of Cryptocurrency Report.

Chesler, J. (2020, December 16). Morocco celebrates inaugural graduation of VR Innovation Academy. EON Reality.https://eonreality.com/morocco-graduation-inaugural

Ciena Corporation. (2022, September). 78% of business professionals are ready for the Metaverse. https://www.ciena.com/about/newsroom/press-releases/78-of-business-professionals-are-ready-for-the-metaverse

Daoud, A. (2022, December 19). The evolution of crypto and Web3 in the Arab world. Fortune Crypto. https://fortune.com/crypto/2022/12/19/evolution-crypto-web3-in-the-arab-world

Deloitte. (2023a). The Metaverse and its potential for MENA. https://scontent-atl3-2.xx.fbcdn.net/v/t39.8562-6/10000000_166618736353611_4640987939387381163_n.pdf?_nc_cat=111&ccb=1-7&_nc_sid=ad8a9d&_nc_ohc=2CwiWBdzx4MAX-jtB4N&_nc_ht=scontent-atl3-2.xx&oh=00_AfCgx__UP-SXX2yk1iehk5kSm2ZYb6kE5TOJV73vRcrSsQ&oe=64C55380

Deloitte. (2023b). Virtual Asset Regulatory Authority (VARA): New Regulatory Framework. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/xe/Documents/financial-services/dme_vara-regulations-Framework.pdf.

Diplo. (2023). Metaverse Diplomacy. DiploFoundation. https://www.diplomacy.edu/topics/metaverse-diplomacy/.

Edwards, B. (2023). OpenAI confirms that AI writing detectors don't work. Ars Technica. https://arstechnica.com/information-technology/2023/09/openai-admits-that-ai-writing-detectors-dont-work/.

Engdahl, S. (2023, June 7). Technology Innovation Institute trains the state-of-the-art Falcon LLM 40B foundation model on Amazon SageMaker. AWS Machine Learning Blog. https://aws.amazon.com/blogs/machine-learning/technology-innovation-institute-trains-the-state-of-the-art-falcon-llm-40b-foundation-model-on-amazon-sagemaker

Ertico and ITS World Congress. (2023). 30th ITS World Congress. ITS World Congress. https://itsworldcongress.com/.

Flanagan, B. (2022, February 1). Saudi Arabia's new metaverse will help design a $500bn city in real life. WIRED Middle East. https://wired.me/technology/saudi-arabias-new-metaverse-will-help-design-500bn-city-irl

Fortis, S. (2023, February 8). Saudi Arabia partners with the Sandbox for future metaverse plans. Cointelegraph. https://cointelegraph.com/news/saudi-arabia-partners-with-the-sandbox-for-future-metaverse-plans

Friedland, A. (2023, July 5). What are Generative Ai, large language models, and foundation models?. Center for Security and Emerging Technology. https://cset.georgetown.edu/article/what-are-generative-ai-large-language-models-and-foundation-models/

Grace, R. (2023, July 7). 5G adoption and its implications in the Gulf States. Middle East Institute. https://www.mei.edu/publications/5g-adoption-and-its-implications-gulf-statesHaddad, J. (2022, July 6). Is Saudi Arabia ready for the metaverse and its related challenges and opportunities? Arab News. https://www.arabnews.com/node/2115146

Han, Y., Zhang, Y., & Vermund, S. H. (2022). Blockchain Technology for Electronic Health Records.

International journal of environmental research and public health, 19(23). https://doi.org/10.3390/ijerph192315577

Harika, M. and Campbell, E. (2022, July 27). Ransomware in the UAE: Evolving threats and expanding responses. The Middle East Institute, Strategic Technologies and Cyber Security Program. https://www.mei.edu/publications/ransomware-uae-evolving-threats-and-expanding-responses.

IBM. (2023). What Is Blockchain Technology? IBM. https://www.ibm.com/topics/blockchain.

Intellectual Property Helpdesk. (2022, June 30). Intellectual property in the metaverse. episode IV: Copyright. European Innovation Council and SMEs Executive Agency. https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/intellectual-property-metaverse-episode-iv-copyright-2022-06-30_en

Joint Counterterrorism Assessment Team. (2021, September 27). Awareness of Illicit Cryptomining-Related Activities May Improve Detection. United States Office of Director of the National Intelligence. https://www.dni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/125s_-_First_Responders_Toolbox_Terrorism_Prevention_Addressing_Early_Risk_Factors_To_Build_Resilience_AgainstViolent_Extremism.pdf

Kosinski, M. (2023). Theory of mind might have spontaneously emerged in large language models. Preprint at https://arxiv. org/abs/2302.02083.

Krishnasamy, E., Varrette, S., & Mucciardi, M. (2020). Edge Computing: An overview of framework and applications.

Kumar, P., Murphy, A., Werner, S., Rougeaux, C., Doppalapudi, P., Zhang, S., & Stearns, R. (2022, October 7). The fight against money laundering: Machine learning is a Game Changer. McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-fight-against-money-laundering-machine-learning-is-a-game-changer

Linganna, G. (2022, August 23). How Metaverse Will Revolutionize the Battlefield. The National Interest. https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/how-metaverse-will-revolutionize

Lu, S., Bigoulaeva, I., Sachdeva, R., Madabushi, H.T., Gurevych, I. (2023, September 4). Are Emergent Abilities in Large Language Models just In-Context Learning? https://arxiv.org/abs/2309.01809.

Luckenbaugh, J. (2022, November 30). I/ITSEC NEWS: Gaming Provides Opportunities, Skills For Military Metaverse. National Defense Magazine. https://www.nationaldefensemagazine.org/articles/2022/11/30/gaming-provides-opportunities-skills-for-military-metaverse.

Mendonca, V., Deuhring, M., and van Diesen, A. (2019). MENA Generation 2030. UNICEF https://www.unicef.org/mena/media/4141/file/MENA-Gen2030.pdf.

Meta. (2022, November 7). The Facebook company is now Meta. https://about.fb.com/news/2021/10/facebook-company-is-now-meta/

Microsoft. (2022, July 20). Microsoft launches HoloLens 2 in the UAE, empowering organizations with the innovation of mixed reality. Microsoft Middle East & Africa News Center. https://news.microsoft.

com/en-xm/2022/07/20/microsoft-launches-hololens-2-in-the-uae-empowering-organizations-with-the-innovation-of-mixed-reality

Microsoft. (n.d.). Introducing Microsoft Mesh: Here can be anywhere. https://www.microsoft.com/en-us/mesh

National Iranian American Council. (2011, December 8). U.S. launches "Virtual" Iran embassy. https://www.niacouncil.org/news/u-s-launches-virtual-iran-embassy/

Ornes, S. (2023). Secret Messages Can Hide in AI-Generated Media. Quanta Magazine. https://www.quantamagazine.org/secret-messages-can-hide-in-ai-generated-media-20230518.

Palmer, D. (2023, May 9). Egypt's largest bank joins the Ripple Network for cross-border payments. CoinDesk. https://www.coindesk.com/business/2021/05/19/egypts-largest-bank-joins-ripple-network-for-cross-border-payments

Peters, J. (2022, December 15). Tim Sweeney wants epic to help build a metaverse that's actually positive. The Verge. https://www.theverge.com/2022/12/15/23511494/tim-sweeney-epic-games-metaverses-positive-dystopian

PRNewswire. (2021, October 19). What might a social metaverse look like in China? Soul App. MarTech Series. https://martechseries.com/social/what-might-a-social-metaverse-look-like-in-china-soul-app-mentioned-by-tsinghua-university-in-its-metaverse-report-could-be-the-answer

Radford, A., Narasimhan, K., Salimans, T., & Sutskever, I. (2018). Improving language understanding by generative pre-training.

Ramos, A. (2022, June). The metaverse, NFTs and IP rights: To regulate or not to regulate?. WIPO Magazine. https://www.wipo.int/wipo_magazine/en/2022/02/article_0002.html

Russo, M., Šrndić, N. & Laskov, P. (2022). Detection of illicit cryptomining using network metadata. EURASIP J. on Info Security 2021 (11). https://doi.org/10.1186/s13635-021-00126-1

Sadeghian, F (2022, October 2). How web 3.0 will transform the Middle East Business Landscape. ZAWYA. https://www.zawya.com/en/opinion/business-insights/how-web-30-will-transform-the-middle-east-business-landscape-mofyib7u

Saleh, A. (2023, May 31). UAE government launches AI-powered Chatbot Platform "U-ask." ZAWYA. https://www.zawya.com/en/smes/technology/uae-government-launches-ai-powered-chatbot-platform-u-ask-d0wt6c14

Sanger, D.E. and Barnes, J.E. (2023, July 29). U.S. Hunts Chinese Malware That Could Disrupt American Military Operations. The New York Times. https://www.nytimes.com/2023/07/29/us/politics/china-malware-us-military-bases-taiwan.html.

Saudi Gazette. (2022, September 14). Saudi Arabia's AI Powerhouse, "mozn" to build world's largest, most effective Arabic ai language models. ZAWYA. https://www.zawya.com/en/business/technology-and-telecom/saudi-arabias-ai-powerhouse-mozn-to-build-worlds-largest-most-effective-arabic-ai-language-models-jwfnjrpb

Saudi Gazette. (2023, May 17). SDAIA launches Allam AI application for Arabic chat. Saudi Gazette. https://saudigazette.com.sa/article/632515

Savitz, E. J. (2023, January 4). Metaverse offers $1 trillion commerce opportunity by late 2025, Accenture says. Barron's. https://www.barrons.com/articles/metaverse-commerce-accenture-51672346692

Shafer, N. (2022, September 15). Cryptocurrency Mining in Lebanon. http://carnegieendowment.org/sada/87924

Shanahan, M. (2023, February 16). Talking About Large Language Models. ArXiv. https://arxiv.org/abs/2212.03551.

Sheffield, S., Davis, M., Smith, P., Masi, K., Colautti, J., & Alhoutti, D. (2022). The Virtual Currency Regulation Review: United Arab Emirates. Charles Russel Speechlys. Lexology. https://www.lexology.com/library/detail.aspx?g=e0015b63-68b2-48dc-bcc3-7a864189308a

Soliman, M. (2022, January 12). The Gulf Has a 5G Conundrum and Open RAN Is The Key To Its Tech Sovereignty. The Middle East Institute. https://www.mei.edu/publications/gulf-has-5g-conundrum-and-open-ran-key-its-tech-sovereignty.

Strickland, E. (2022, February 22). "AI Doesn't Need Our Supervision," IEEE Spectrum, https://spectrum.ieee.org/yann-lecun-ai

Syme, P. (2023, August 23). A Chinese spy used fake LinkedIn profiles to target officials to hand over secrets, report says. https://www.businessinsider.com/chinese-spy-fake-linkedin-profiles-to-offer-money-for-secrets-2023-8.

Tariq, S., Abuadbba, A., Moore, K. (2023, September 10). Deepfake in the Metaverse: Security Implications for Virtual Gaming, Meetings, and Offices. https://arxiv.org/abs/2303.14612.

Technology Innovation Institute. (2023a). Introducing Falcon LLM. Technology Innovation Institute, Abu Dhabi. https://falconllm.tii.ae/

Technology Innovation Institute. (2023b). NOOR: The World's Largest Arabic NLP model. Technology Innovation Institute, Abu Dhabi. https://noor.tii.ae/

Vardanyan, L., Kocharyan, H., Hamulak, O., Mesarcik, M., Kerikmae, T., & Kookmaa, T. (2023). The Unwanted Paradoxes of the Right to Be Forgotten. Masaryk UJL & Tech., 17, 87.

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., ... & Polosukhin, I. (2017). Attention is all you need. Advances in neural information processing systems, 30.

Weimann, G. (2004, December). Cyberterrorism: How Real Is the Threat? United States Institute of Peace. https://www.usip.org/sites/default/files/sr119.pdf.

World Economic Forum. (2023, January 17). A vision for a global collaboration village. https://www.weforum.org/agenda/2023/01/the-global-collaboration-village-davos-2023/

Zawya. (2022, June 27). Arab's first nfts platform in MENA startup UPYO launched in the first of June 2022. ZAWYA. https://www.zawya.com/en/press-release/companies-news/arabs-first-nfts-platform-in-mena-startup-upyo-launched-in-the-first-of-june-2022-do4rmy8f

nauss.edu.sa

nauss.sa

+966 11 246 3444

info@nauss.edu.sa

nauss_sa

+966 11 245 0222