May 2023

Perspective
EXPERT INSIGHTS ON A TIMELY POLICY ISSUE

TIMOTHY MARLER, ZARA FATIMA ABDURAHAMAN, BENJAMIN BOUDREAUX, TIMOTHY R. GULDEN

The Metaverse and Homeland Security

Opportunities and Risks of Persistent Virtual Environments

Interest in and development of the emerging "metaverse" has grown markedly, raising questions around what it entails and why it is relevant for a variety of social, economic, and security issues. The answers to these questions can have significant implications for the U.S. Department of Homeland Security (DHS).

Regardless of precise definitions, metaverses offer both opportunities and potential threats for DHS and for society more broadly.[1] However, an emerging technology, such as the metaverse, can often reflect a *technology push*, whereby products are first developed in the private sector simply with an eye toward exciting new capabilities and profits, rather than responding to a *technology pull* that reflects specific user needs (Marler, 2022). This can obfuscate threats and opportunities and stifle appropriate management. Although a multifaceted technology might, in fact, respond to specific needs, it might also still have aspects that emerge without aligning to any goal. This, of course, can foster innovation, but it can also result in hollow hype (Jones, 2022; Vinsel and Funk, 2022). The metaverse is no exception. As various technologies and capabilities associated with metaverses mature, users

RAND CORPORATION

and policymakers will need to understand those technologies' and capabilities' impact and to ask, "So what?" What are the implications of metaverses for DHS's mission, and can they help respond to specific needs?

To be sure, virtual environments—arguably, the crux of metaverses—have been maturing for decades. Virtual reality (VR) can be traced back to the 1960s, with early work on head-mounted displays (Sutherland, 1968) and much seminal work following throughout the 1980s (Card, 1977; Conn et al., 1989). Stephenson (1992) first coined the term *metaverse*, and many authors, such as Cline (2011) popularized the concept. Most recently, of course, the term made headlines when Facebook announced a name change to Meta (CNET, 2021), thus heightening the term's popularity and recognition. Then, additional companies offering related capabilities also borrowed the term,[2] and the metaverse took on a life of its own. For example, Nike is preparing to offer virtual Nike-branded sneakers and apparel, which has significant implications for the "business" of the metaverse (Golden, 2021). Disney pitched the idea of a metaverse as the next evolution of "storytelling without boundaries" (Milmo, 2021). Consequently, potential various regulatory and policy issues are surfacing (Tusk, 2022). However, all the publicity can make it difficult to discern between, on the one hand, practical and impactful capabilities that could foster valuable opportunities or considerable threats and, on the other hand, relatively unvaluable or even irrelevant hype.

Abbreviations

AR	augmented reality
DHS	U.S. Department of Homeland Security
IoT	internet of things
SLTT	state, local, tribal, and territorial
VR	virtual reality

Such confusion can affect public discourse, not to mention individual users and customers. Furthermore, it can affect policy decisions. How are metaverses relevant to various organizations, and what does a metaverse entail? Leveraging opportunities and mitigating threats require that potential confusion be mitigated as early as possible.

Two ways to help avoid empty hype are to (1) clearly describe relevant technologies and thus facilitate coherent discussion and (2) map technologies and capability development to underlying needs (and threats). Although definitions, characteristics, and issues will likely change over time, laying out a starting point for discussion, based on common terms, or at least standardizing the current and anticipated capabilities, can help facilitate efficient communication. Furthermore, it can be helpful to ensure that capability development and subsequent management align with underlying needs. Open exploratory development and research can be beneficial, but being cognizant of how emerging technologies map to organizational mission sets can help decisionmakers leverage current capabilities most effectively.

This Perspective briefly explores these two mitigating strategies for DHS, focusing on opportunities and threats derived from the metaverse. First, we briefly explore existing definitions and descriptions of metaverses. Given the inadequacy of these definitions, we lay out key characteristics of a metaverse. Then, we conduct a basic and high-level mapping between these characteristics and DHS mission sets, thus confirming the significance of metaverses to the department. We then highlight specific opportunities and

A metaverse is a persistent and digital environment, potentially informed by real-world sensors, that someone can enter and assume a persona, interact with others, have affordances and agency, perhaps modify the environment itself, and then leave.

threats that DHS might want to consider. Certainly, this kind of analysis should be continuous as technologies and issues change, and this Perspective does not provide an exhaustive analysis of the metaverse. Rather, it introduces key characteristics and considerations for DHS, which might deserve further study and analysis.

What Is a Metaverse?

To discuss and manage the metaverse, one must understand what it entails. As we explain, a metaverse is generally a persistent and digital environment, potentially informed by real-world sensors, that someone can enter and assume a persona (or multiple personas), interact with others, have affordances and agency, perhaps modify the environment itself, and then leave. Nonetheless, a succinct and distinct definition can be elusive in the literature (Chowdhury and Marler, 2022), and a precise definition can change over time and vary depending on the users. Committing to a singular, static, universal definition as technology matures can be detrimental to discussions of emerging technology. However, having a common and foundational set of characteristics can help facilitate coordinated discussion, answer policy questions, and inform anticipated benefits or dangers. Some form of a base definition is necessary to scope initial discussions. Thus, the intent here is not necessarily to codify a permanent definition for *metaverse* but rather to offer relevant key defining characteristics. Ultimately, we discuss how metaverses could affect DHS, so here we focus on practical implications.

It is important to distinguish between what is *necessary* to form a metaverse and what *could become* an aspect or characteristics of a metaverse going forward. We focus on the most-critical and -impactful aspects of a metaverse.

Originally, Stephenson (1992) provided the first definition of metaverse in the novel *Snow Crash* as a VR-based successor to the internet, describing it as a potential "escape"—albeit a potentially unhealthy one—from a dystopian society, with some degree of addictiveness. Huddleston (2021) argued that the metaverse was still intended as an escape and thus reflected many of the origi-

nal characteristics, including digital avatars, VR goggles, gaming communities, spending on virtual belongings, and encrypted electronic currency. In many respects, *Snow Crash* was predictive (Robinson, 2017). However, in today's context, there is not necessarily a dystopia, and the metaverse need not replace the internet but rather provide a new front end or expansion.

Following Stephenson's work, multiple authors have offered specific definitions, but those definitions can vary to the point of stifling rather than fostering coordinated discussion (Ball, 2021; Park and Kim, 2022; Smart et al., 2007). Such companies as Microsoft also offer their own differing definitions of *metaverse*, often slanted to suit their own needs and thus reflecting only the private sector (Roach, 2021).[3] In the face of many disparate definitions, Ball (2021) noted that "we should not expect a single, all-illuminating definition of the 'Metaverse,'" especially when the metaverse is emerging and technology-driven transformation can be organic and unpredictable. Consequently, Park and Kim (2022) offered an extensive taxonomy of terms and components. However, although this taxonomy is comprehensive, it can be unwieldy for identifying practical opportunities, threats, and policies.

Key Metaverse Characteristics

- Virtual
- Networked to facilitate interaction between users
- Persistent and accessible
- Dynamic, ephemeral, and editable
- Informed by real-world data
- Defined by people involved in its development and use

Aside from the context of its initial use, the etymology of the word *metaverse* offers some insight into a potential consistent definition, suggesting a new, transformative, and comprehensive universe (Merriam-Webster Dictionary, undated). But what does *metaverse* mean in more-practical terms?

Key Characteristics

Although there might not be a common and succinct definition,[4] through a series of structured discussions, a panel of RAND Corporation researchers with expertise in such diverse areas as engineering and social sciences identified key characteristics that can be useful when determining opportunities, threats, and challenges. A key foundational aspect is that of a generated **virtual environment**. A metaverse necessarily involves virtual representation of agents and various digital assets. With respect to this particular characteristic, it is important to remember that there is not just one metaverse, a point that can be confused by discussing the idea of *the* metaverse. There could be many virtual environments that qualify as metaverses. A metaverse certainly need not involve VR or augmented reality (AR) to be impactful; a metaverse need not involve (or be limited to) a three-dimensional geographic representation of reality. Arguably, a virtual environment could have many more conceptual dimensions, but here we try to stay grounded in the most-pervasive, -practical, and -impactful aspects.

Although a metaverse can be accessed by a single user, one aspect that offers a variety of benefits and risks is that a metaverse is **networked and facilitates interaction among users**. It can be accessed by many disparate users in differ-

ent locations both synchronously and asynchronously. Like first-person interactive games, metaverses include distinct aspects of social media, whereby groups of users can interact and can affect the space in which they interact. It is just these first two aspects—virtual environment with interacting users—that is captured in published definitions (Cambridge Dictionary, undated; Oxford English Dictionary Online, undated). However, although these characteristics are foundational, they are insufficient for characterizing today's metaverses.

What departs from traditional multiplayer games with a metaverse is the combination of persistence and variability. On one hand, a metaverse is **persistent**; it is a virtual environment that users can revisit at different times. There can be recurring access. There is a persistent presence of the virtual environment but not necessarily of the participants who visit that environment. Yet, a metaverse can change; it is **dynamic, ephemeral, and editable**. Creators and users can alter a metaverse. They can change various aspects and virtual entities, and these changes are visible and available to returning users.

Although it is not necessarily a defining characteristic, an element that has potentially significant repercussions is the link between the virtual environment and **real-world data**. Although this Perspective focuses on an assessment and the implications of current capabilities, going forward, sensors and thus data from the real world could increasingly inform and contribute to metaverses. This link between the virtual and real worlds can be facilitated by various forms of interaction beyond just the common visual sense (e.g., haptic or even smell).

Finally, a metaverse can be defined in part by the **people involved in it**, as well as the outcomes of the actions of these participants. That is, a metaverse is established or specified not just by virtual entities but by the actual developers, users, policymakers, and stakeholders. As Harkavy, Lazzarin, and Simpson (2022) notes, "community ownership is the piece of the puzzle that aligns network participants—builders, creators, investors, and users—to cooperate and strive for a common good."

Most of the defining characteristics noted above can fall on a spectrum. For example, metaverses might vary in the degree to which they persist or to which a user can edit them. Nonetheless, considering these elements can inform a common understanding of what a metaverse is. In general, a metaverse combines today's internet, multiplayer games, increased interconnectivity and interoperability (i.e., the internet of things [IoT]), and possibly immersion (e.g., VR, AR), persistence, and emergent and dynamic editability.

Relevance to the DHS Mission Set

With this understanding of *metaverse* in mind, we have conducted a preliminary survey of DHS mission sets and exemplary needs. This is based on publicly available literature and material published on DHS websites. We then compared these needs with the primary characteristics outlined in the previous section. The goal was to identify opportunities and risks that the metaverse brings for DHS.

In general, DHS develops and implements strategies that ensure safety and security of the United States' land,

people, and economy. It focuses on tasks that align with its six core missions (DHS, 2023):

- Counter terrorism and homeland security threats.
- Secure U.S. borders and approaches.
- Secure cyberspace and critical infrastructure.
- Preserve and uphold the nation's prosperity and economic security (DHS, 2022a).
- Strengthen preparedness and resilience.
- Champion the DHS workforce and strengthen the department.

After mapping DHS mission sets to characteristics of the metaverse, we found that almost all the characteristics pertain to most of the six mission sets. For example, metaverses could be used to train the DHS workforce or track terrorist communications within a virtual environment. If one considers a metaverse a virtual world, able to reflect much of the physical world, then this conclusion is not unexpected. Many of the things that happen in the physical world might happen in a metaverse.

These DHS mission sets inform specific needs, so in addition to reviewing missions, we conducted a basic review of exemplary DHS needs related primarily to science and technology, to investigate the extent to which these needs align with metaverse characteristics. This comparison between primary needs and metaverse characteristics is provided in the appendix and summarized in the table. Although this analysis is not exhaustive, it does illustrate the relevance of metaverses to DHS missions, and it helps unpack which particular areas might require a different approach from what DHS might have used in the past and what new capabilities that do not exist in the physical world will be leveraged in the virtual world.

Exemplary DHS Needs Mapped to Key Metaverse Characteristics

	Metaverse Characteristic				
DHS Need	Is Virtual	Facilitates Interaction	Is Persistent and Accessible	Is Dynamic, Ephemeral, and Editable	Is Informed by Real-World Data
Reconfigurable areas for testing and evaluating operational concepts	x	x	x	x	x
Planning tools for risk assessment and emergency response		x	x	x	x
Visualization, training simulation, and process and threat modeling	x	x	x	x	x
Interoperable methods for incorporating IoT sensors into city services			x		x
Information on domestic extremism and tools to communicate threats and counter disinformation		x			x

Opportunities and Threats for DHS

This section highlights areas in which DHS might want to leverage characteristics of a metaverse, as well as areas in which metaverses could present new or intensified threats and risks. Opportunity areas include research, outreach, preparedness, and training, while threats include misinformation and disinformation, abuse, organized violence, cybersecurity threats, and a set of ethical and equity issues pertaining to DHS's activities in the metaverse. There are existing analogues to these opportunities and threats, but the metaverse could augment them and make them more complex, requiring new capabilities and careful consideration of DHS's role. As DHS considers increased presence in metaverses, it must consider these opportunities and threats together. This will help ensure that the department plays a positive role in the new environment and is ready to respond to augmented threats, rather than playing a role associated with surveillance, civil-liberty violations, and inequity that can decrease public trust and support.

Opportunities

Metaverses can provide a variety of opportunities for DHS to improve its existing mission execution and service delivery.

Research and Intelligence

As a potentially expansive set of virtual worlds, metaverses will include many opportunities for DHS to monitor possible threats and gather evidence to help secure the United States. Digital information from metaverses might assist DHS in both preventing real-world criminal attacks and investigating them afterward.

Many DHS mission areas require detailed understanding of what people do and how they interact. The computerized nature of metaverses could provide chances to conduct various types of research, such as measuring usage and demand across a wide variety of areas. This could help DHS allocate resources and refine processes in ways that maximize service delivery and human security. For example, many metaverse interactions could be public, with users expressing themselves not just privately to trusted associates but to the world at large. DHS might find it useful to monitor this discourse, to identify emerging themes relating to shifts in values, such as the heightened interest in diversity and inclusion, or to identify actual threats, such as those posed by white nationalist organizations.

Outreach and Information Dissemination

Metaverses present opportunities for DHS to communicate about a variety of security issues. Most visions of the metaverse posit it as a shared, persistent, virtual space that is both information-rich and relatively open, or at least highly interoperable. This could provide an environment in which DHS and other organizations with an interest in safety and security can engage people in constructive ways. This could take the form of expanded versions of the "If you see something, say something" campaign. It could also involve interactive programs and outreach that target events and locations where security messages are particularly likely to be useful or need to be delivered emergently. These engagements might take forms beyond traditional messaging, such as virtual environments that simulate a day in the life

of a DHS official, or virtual DHS presences that offer an environment conducive to building trust and collaboration with key communities. A metaverse could provide a new venue for recruiting DHS workforce. It might also provide a tool for engaging with witnesses or soliciting public assistance.

Preparedness

Preparedness is likely to be a particularly rich area for DHS engagement in metaverses. Current materials on earthquake and tsunami preparedness, for example, use mostly text and static images to communicate the hazards of these phenomena and encourage people to keep appropriate supplies of nonperishable foods and fresh water, as well as go bags and other points of preparedness. A metaverse-based preparedness simulation could allow people to experience a simulated earthquake and see the damage it can cause, as well as examine the contents of a go bag. People could participate in evacuation drills from their homes or neighborhoods, as well as public venues, with most of the other evacuees being simulated. This would allow users to gain experience with evacuation without the need for massive coordination. Similar principles might apply across the variety of situations in which DHS has an interest in enhancing preparedness. In general, virtual environments and simulations can reduce risks of injury, reduce costs, facilitate repetitions, and allow for more-effective and -objective after-action reviews.

Training

Many characteristics of metaverses are advantageous for training. Virtual environments, in particular, can be useful for DHS agents and other security personnel in training for catastrophic events, including terrorist attacks and natural disasters, such as fires, hurricanes, and earthquakes. Large-scale exercises can be extremely expensive to conduct, requiring the coordination (and transportation) of large numbers of people and often the temporary closing of the venue involved. Training in a metaverse could avoid these problems, allowing an arbitrary number of personnel to train in a realistically crowded environment, in which the majority of people are operated as computer simulations. Such training could be useful in public venues, such as sports stadiums and schools, as well as larger landscapes, such as fire-prone neighborhoods or difficult-to-patrol borderlands. In addition, training in a metaverse could be safer than real-world on-the-ground training, especially for first responders potentially involved in life-threatening situations. Furthermore, virtual environments provide opportunities for additional feedback and after-action reviews, not to mention data on performance.

There might be a large up-front cost for DHS to create the "digital twin" assets for preparation and training, but there could be a good return on DHS investment, especially if these assets could be highly multiuse, in which, for example, the same virtual stadium could be used for event planning, security drills, maintenance work, and advertising.

Threats

DHS faces a variety of threats and challenges related to existing cyberspace and internet technologies, including misinformation, abuse, organized violence, and cybersecurity (Rudman et al., 2021). Unfortunately, many of these same challenges could persist in metaverses, further

As DHS seeks to leverage opportunities and deal with threats, it should ensure that its response aligns with ethical and equity considerations.

challenging DHS capabilities. Moreover, metaverses could give rise to new technological characteristics and increased complexity, with attendant effects on human users, thus having implications for DHS capabilities and authority. As DHS seeks to leverage opportunities and deal with threats, it should ensure that its response aligns with ethical and equity considerations, including the full list of values that DHS professes.

Misinformation and Disinformation

The rapid dissemination of online misinformation already poses serious risks to key DHS missions, such as the Cybersecurity and Infrastructure Security Agency's role in election security or the Federal Emergency Management Agency's role in emergency response, and these challenges might only increase with widespread adoption of metaverses. Narrative content in a metaverse might be disseminated through multisensory dimensions, thus perhaps more powerfully working on the psychological enablers, such as confirmation bias, that build credence in false information.[5] The metaverse also brings the possibility of multisensory deepfakes that could be used to falsely imitate American leaders or others in order to seed pernicious ideas designed to destabilize American institutions and polarize the public.[6] Just as in existing social media, deliberate misinformation campaigns might seek to target underserved and marginalized communities to foster mistrust in government institutions, except now in a different form (e.g., a highly realistic avatar representing what seems to be a leader or policymaker). In addition, with the extensive spread of misinformation, users might even view metaverses as totally fake, in which nothing is to be trusted, including important information that DHS seeks to disseminate (e.g., notices related to an oncoming hurricane or other disaster).

An additional complexity of misinformation in a metaverse is that much of the content might be fleeting and ephemeral—more like in-person social conversations rather than data that are permanently stored in algorithmic feeds for a wide audience to observe. As stated by one Meta executive, "The metaverse will constitute a shift towards live, speech-based communication that will often feel as transient as face-to-face conversations" (Clegg, 2022). As a result, it might be harder for DHS and even metaverse platforms themselves to track the spread of false and misleading information and to identify key content creators and disseminators. This analytic challenge could also make it harder for the U.S. government to act against misinformation campaigns coordinated by foreign states. Even getting a handle on the scope of the misinformation challenge could be a problem, and, as we discuss in more detail, DHS

will need to consider carefully how it monitors activity in metaverses to ensure that it understands the challenges while still protecting civil liberties and privacy.

Abuse and Harassment

DHS's homeland security missions, such as U.S. Immigration and Customs Enforcement's missions to combat child exploitation, might be affected by new forms of harassment and abuse that could take place in the metaverse and that will further stretch DHS capabilities. The internet has already enabled forms of sexual and other abuse especially against women, and there is a risk that metaverse platforms could further enable child exploitation, sexual abuse, and sex trafficking (Sum of Us, 2022). Indeed, there are already reports of sexual abuse and harassment in still-nascent metaverses (Basu, 2021). Some metaverse platforms have sought to create barriers to certain forms of abuse (for instance, Horizon World's personal boundary developed after reports of sexual harassment [Sharma, 2022]), but the problems persist and might be particularly pronounced for women, children, and people of color. A more immersive social experience could also expand the potential for confidence schemes that tend to prey on the elderly and others who are new to the technology or are otherwise socially vulnerable.

It will be important that DHS develop effective and safe engagement to understand the forms of abuse that might occur in the metaverse. DHS will need to be prepared for victims to come forward with new kinds of harms that might not have an equivalent in the physical world. The effects that abuse and harassment experienced in metaverses could have on outcomes in the physical world are understudied. Some evidence suggests that the heightened sense of reality users experience in metaverses means that adverse experiences in metaverses will have *greater* psychological impacts than the same experiences in the real world (de Vries, 2011). However, others might argue that metaverses provide space for the constructive outlet of behavior that would be deemed incontestably abusive in the physical world (for instance, the sort of activities players undertake in violent video games, such as Fortnite).

Organized Violence

One of DHS's core missions is preventing and responding to organized violence and terrorism, and the metaverse could provide a new venue for such violence or organizational efforts. As with existing social media platforms, the metaverse will provide a forum for radicalizing people, recruiting terrorists, enabling organizations to plan and coordinate attacks, and inciting widespread violent attacks.[7] Just as virtual environments help simulate the real world and provide DHS with interactive planning capabilities and information dissemination opportunities, they can also provide powerful planning and training environments for terrorist and other organized criminal attacks. Attacks might themselves take place in metaverses, which could itself affect people's well-being or even evolve into real-world violence.

Furthermore, just as a metaverse could provide a potential recruiting tool for DHS, so too could it help various terrorist organizations recruit new members. DHS will need to be prepared to engage with emerging virtual communities to ensure that it can effectively stay attuned to these types of threats in a way that reflects the department's legitimate role and with the protection of civil liberties.

The emergence of metaverses as persistent environments, in which people have possessions that can be purchased with real money and used across environments, has the potential to create a new class of property crimes.

Cybersecurity

DHS has a lead role in strengthening cybersecurity resilience, and the metaverse could become a front line for various kinds of cybercrime and consumer fraud that expands on the existing forms of this criminality in the existing internet. In addition, the emergence of metaverses as persistent environments, in which people have possessions that can be purchased with real money (likely based on blockchain technology) and used across environments, has the potential to create a new class of property crimes. Investigation of such crimes is likely to require a skill set different from that of traditional police work or cybersecurity as currently practiced.

An additional cybersecurity issue for which DHS will need to be prepared is the possibility that state, local, tribal, and territorial (SLTT) governments or critical infrastructure owners and operators might themselves use metaverses for service provision or preparation of many kinds. If SLTTs and critical infrastructure providers become more dependent on metaverses for training or other activities, new vectors for malicious attacks could emerge. DHS will need to be prepared for the cybersecurity challenges that arise in these metaverse applications and potentially provide guidance on best practices or even response to metaverse cyber incidents.

Ethics and Equity Issues

Potential challenges with ethics and equity might be pervasive across many threats. The challenges noted above suggest a role for DHS in being prepared for, monitoring, and responding to potentially harmful effects on the homeland stemming from the metaverse. However, DHS will need to be mindful of its core ethical values because its responses to these challenges might themselves raise important legal, ethical, and equity issues. According to its stated priorities for 2022, DHS will "Advance Diversity, Equity, Inclusion, and Accessibility (DEIA) in our workforce and protect the privacy, civil rights, civil liberties, and human rights of the communities we serve" (DHS, 2023a). DHS will need to ensure that these values are advanced in the metaverse.

DHS will need to carefully consider its legal authority (relating to ethics and equity issues) to analyze and engage

in a metaverse. Insofar as there are legal questions or perceived barriers to effective response to challenges, DHS might need to seek clear authorization or resources from Congress. Already DHS has faced questions from Congress and civil-liberty organizations about its legitimate role in responding to challenges of misinformation on the existing internet (Lorenz, 2022). So DHS will need to proceed carefully in clarifying and scoping its role. It will need to ensure that it has the capabilities to respond to issues, and it will need to build appropriate partnerships and oversight mechanisms to prevent overstepping of its authority and ensure the protection of civil liberties.

As DHS grapples with emerging challenges by monitoring and analyzing users' activity in metaverses, it should undertake legal and ethical reviews of what information is collected and how it is managed. In these and other activities, DHS will have to be particularly mindful about how its use of metaverses, or response to emerging challenges, will affect civil liberties, especially the implications for personal privacy and freedom of speech. Just as with current social media and mobile phone app technology, there might be a variety of new analytic and predictive platforms readily available on the open market that can assist DHS in tracking suspects or metaverse users (Burke and Dearen, 2022). However, given concern from Congress and others, DHS will need to be careful about how it leverages these tools to surveil Americans and will need to be deliberate about the equity implications of predictive analytic technology or other emerging surveillance technologies.

The problem of inequity is already a major challenge in the metaverse (DallasKidd, 2022; Dick, 2021), and DHS will need to be thoughtful about how its approach to metaverses will itself have implications for users' equity. For instance, it will need to consider when its activities might not reach underserved or marginalized communities or whether its metaverse surveillance and enforcement unfairly target members of those communities.

DHS would benefit from working to address challenges in accordance with its ethical values. This could include considering the public's perception of DHS's role in the metaverse and building trust and support from stakeholders, such as private industry, members of Congress, and civil society organizations (Boudreaux, Yeung, and Steratore, 2022). Stakeholder consultation will be important to ensure that DHS can develop and leverage its partnerships to track threats and respond most effectively. Engagements with these groups will also help DHS ensure that marginalized communities can voice their concerns about misinformation, abuse, inequity, and other threats that might arise.

Conclusion

Despite the increasing discussions about and use of metaverses, commonly agreed-upon defining characteristics can remain elusive. Consequently, there is risk of developing capabilities that do not necessarily respond to underlying needs, and management and coordination of the consequent technologies can be challenging. In response, this Perspective offers a baseline for discussions about the metaverse, noting past fundamental definitions and outlining key characteristics. It provides a basic and initial crosswalk between DHS missions and needs on the one hand and metaverse characteristics on the other.

For technologies to be impactful, they must align with objectives and goals, and we contend that metaverses do, in fact, align with DHS mission sets (and certain specific

needs) in many ways. The metaverse is relevant to DHS. However, as with any organization facing emerging technologies, DHS could benefit from being proactive rather than reactive. DHS could consider further analysis to leverage opportunities and mitigate threats *before* metaverses become more prevalent and mature.

The discussion in this Perspective suggests some future considerations for DHS that might help ensure that it is ready for the more-widespread promulgation and use of the metaverse:

- **Understand the technology, opportunities, and challenges.** DHS can continue to analyze the metaverse, paying close attention to the ways the relevant technologies are developing and are being used, so that it is prepared to identify opportunities to advance its mission while conducting risk analysis to identify potential harms. DHS could consider the existing opportunities and threats of the internet and add the extended capabilities that the metaverse provides. Using this past analysis of the opportunities and threats of the internet provides a starting point for lessons learned and does not require a completely clean slate.

  DHS can also consider world-building techniques, robust decisionmaking, and other forward-looking methods to identify possible future states of the metaverse and its role in society so DHS can be prepared for the variety of technological trajectories. This Perspective provides a brief overview, but more research and analysis will be necessary by specific components to understand the metaverse today and how it will likely evolve.

The metaverse is relevant to DHS.

- **Assess DHS capabilities, policies, and roles.** With a better understanding of the metaverse, DHS can determine how to engage within it to leverage opportunities and respond to threats. The department can determine what capabilities it needs, including specific metaverse technologies, such as simulation tools, workforce and personnel, or new helpful policies or authorities. DHS will need to work across the U.S. government and with SLTTs to ensure that there is a consistent approach and that differing capabilities can be most effectively leveraged.
- **Build trust and partnerships.** DHS will not be able to effectively engage in the metaverse alone; rather, it will need support from key partners. DHS should work with private-sector entities to understand their plans for developing the metaverse, and DHS can work with these companies to help foster interoperability that will make it easier for DHS to collaborate with SLTTs and other operational partners. In fact, interoperability is a key implicit theme in considering responses to metaverse-related technologies. There is not just one metaverse, and the community and collaborative benefits of metaverses (or any virtual environments) magnify as various environments link or coordinate. This requires interoperability between data, policies, graphical

rendering engines, and more. With respect to DHS, this can affect collaboration between state and local governments, international partners, and critical infrastructure owners and operators. With relevant organizations, such as the Metaverse Standards Forum (undated), industry is laying the foundation for this integration, but more work is needed on technical capabilities and incentives for successful collaboration.

In considering these three broad efforts, DHS could collaborate with critical infrastructure owners and operators, SLTTs, and others through new types of stakeholder engagement and empowerment. This could help the department understand how others will be using the metaverse and thus provide appropriate guidance or support. Ethics and equity reviews should be done as a standard matter, but these efforts will also help DHS gain public support. The department could work with representatives from different political viewpoints to ensure that its role in the metaverse is perceived as legitimate. DHS could also conduct public perception research, such as surveys or focus groups, to better understand how the public sees metaverse activities and to shape a role for DHS that can build public trust. Just as technologies should align with the needs of organizations, organizations could work better to understand the needs of end users across public sectors.

Appendix: Exemplary DHS Needs Mapped to Metaverse Characteristics

The table provides our crosswalk between DHS needs and metaverse characteristics.

Aligning DHS Needs with Metaverse Characteristics

DHS Need	Metaverse Characteristic
Enriched first responder and law enforcement training experiences with flexibility to train under a variety of conditions (S&T, 2021)	• Ability to create virtual worlds informed by real-world data • Ability for a large number of users to share synchronized simulations in real time • Ability to change and edit worlds • Use of AR and VR to create immersive experiences
Improved digital indoor mapping tool for first responders	• Ability to build virtual environments with real-world data • Interoperability with the IoT for real-time updates
Improved capabilities for response, characterization, and remediation of radiological and nuclear incidents (e.g., modeling how radioactive material is dispersed to enable first responder preparedness) (S&T, undated-b)	• Ability to create planning and training simulations • Ability to simulate models of radioactive materials' spatial distribution in virtual environments based on real-world data

Aligning DHS Needs with Metaverse Characteristics—Continued

DHS Need	Metaverse Characteristic
Reconfigurable areas for testing and evaluating several operational concepts (S&T's Maryland Test Facility is an example of such a facility [S&T, 2023b])	• Ability to create dynamic and editable virtual worlds • Ability to facilitate interaction
New technologies and standards to assist law enforcement with cyberattack and cybercrime prevention and investigation (DHS, 2022b)	• Ability to be defined by people involved in its development and use
Information on domestic extremism, radicalization, and other topics, as well as tools to communicate threats and counter disinformation (S&T, 2022)	• Ability to communicate with many users in real time • Ability to access publicly available data for information-gathering
Accurate planning tools for risk assessment and emergency response	• Ability to build virtual environments with potential real-time updates
Accurate position, navigation, and timing capabilities for the critical infrastructure sector with minimal intentional or unintentional disruption	• Ability to build virtual environments with real-world data • Interoperability with the IoT for real-time updates
Research on open, interoperable methods for incorporating IoT sensors into city services (S&T, undated-c)	• Ability to build virtual environments with real-world data • Interoperability with the IoT for real-time updates
Technology solutions to operate and respond in remote maritime locations (S&T, undated-a)	• Ability to build virtual environments informed by real-time data
Immersive visualization, process modeling and gaming and predictive threat modeling (S&T, 2023a)	• Ability to create virtual worlds informed by real-world data • Ability for large number of users to share synchronized simulations in real time • Ability to change and edit worlds • Use of AR and VR to create immersive experiences
A forum to connect and engage the participants in homeland security enterprise with experts in modeling and simulation	• Ability to interact with multiple users within the virtual space • Ability to connect with users globally
Technical oversight for emergency evaluation of crowd dynamics and crowd flow	• Ability to build virtual environments informed by real-world data • Ability to interact with multiple users within the virtual space
Safety and security for U.S. financial systems	• Ability to create and use digital currency, ownership of virtual assets, investments, and other tools

NOTE: S&T = Science and Technology Directorate.

Notes

[1] Technically, there can be many metaverses, but the common use of the term *metaverse* tends to refer to the overall concept or idea.

[2] Examples of such companies are Sensorium (Sensorium AG, undated), Roblox (Roblox, undated), Microsoft (Microsoft, undated), and Niantic (Niantic, undated).

[3] Also see, for example, Meta (Meta, undated) and Roblox (Bronstein, 2021).

[4] The Oxford English Dictionary provides a definition (Oxford English Dictionary Online, undated), as does the Cambridge Dictionary (Cambridge Dictionary, undated). However, these definitions differ, and they do not address the myriad capabilities in use and in the literature describing what a metaverse entails and how it can be used. As of this writing, neither McMillian nor Merriam-Webster provided a definition of *metaverse*.

[5] Although there is some research on the psychological implications of VR, there are not yet robust studies that analyze the implications for users' beliefs or dispositions.

[6] Deepfakes are convincingly realistic, computer-generated depictions of events that did not actually occur—including statements by political leaders.

[7] These are long-standing concerns, as discussed in Don et al. (2007).

References

Ball, Matthew, "Framework for the Metaverse," *The Metaverse Primer*, June 29, 2021.

Basu, Tanya, "The Metaverse Has a Groping Problem Already," *MIT Technology Review*, December 16, 2021.

Boudreaux, Benjamin, Douglas Yeung, and Rachel Steratore, *The Department of Homeland Security's Use of Emerging Technologies: Why Public Perception Matters*, RAND Corporation, PE-A691-1, 2022. As of April 2, 2023: https://www.rand.org/pubs/perspectives/PEA691-1.html

Bronstein, Manuel, "The Future of Communication in the Metaverse," Roblox, September 2, 2021.

Burke, Garance, and Jason Dearen, "Tech Tool Offers Police 'Mass Surveillance on a Budget,'" Associated Press, September 2, 2022.

Cambridge Dictionary, "metaverse," undated.

Card, Orson Scott, *Ender's Game*, Tom Doherty Associates, 1977.

Chowdhury, Swaptik, and Tim Marler, "The Metaverse: What It Is and Is Not," *Inside Sources*, June 19, 2022.

Clegg, Nick, "Making the Metaverse: What It Is, How It Will Be Built, and Why It Matters," May 18, 2022.

Cline, Ernest, *Ready Player One*, Crown Publishers, 2011.

CNET, "Everything Facebook Revealed About the Metaverse in 11 Minutes," video, October 28, 2021.

Conn, C., Jaron Lanier, Marvin Minsky, Scott S. Fisher, and A. Druin, "Virtual Environments and Interactivity: Windows to the Future," *ACM SIGGRAPH Computer Graphics*, Vol. 23, No. 5, December 1989.

DallasKidd, Sean, "3 Ways to Tackle the Metaverse and Its Promise of Equity," *Forbes*, February 17, 2022.

de Vries, Katja, "Avatars Out of Control: Gazira Babeli, Pose Balls and 'Rape' in Second Life," in Serge Gutwirth, Yves Poullet, Paul De Hert, and Ronald Leenes, eds., *Computers, Privacy and Data Protection: An Element of Choice*, Springer, 2011.

DHS—*See* U.S. Department of Homeland Security.

Dick, Ellysse, "Risks and Challenges for Inclusive and Equitable Immersive Experiences," Information Technology and Innovation Foundation, June 1, 2021.

Don, Bruce W., David R. Frelinger, Scott Gerwehr, Eric Landree, and Brian A. Jackson, *Network Technologies for Networked Terrorists: Assessing the Value of Information and Communication Technologies to Modern Terrorist Organizations*, RAND Corporation, TR-454-DHS, 2007. As of April 2, 2023: https://www.rand.org/pubs/technical_reports/TR454.html

Golden, Jessica, "Nike Is Quietly Preparing for the Metaverse," CNBC, updated November 2, 2021.

Harkavy, Elizabeth, Eddy Lazzarin, and Arianna Simpson, "7 Essential Ingredients of a Metaverse," a16zcrypto, May 6, 2022.

Huddleston, Tom, Jr., "This 29-Year-Old Book Predicted the 'Metaverse'—and Some of Facebook's Plans Are Eerily Similar," *Make It*, updated November 3, 2021.

Jones, Benjamin, "The Social Value of Science and Innovation Investments and Sources of Breakthroughs," *The Reporter*, No. 1, March 2022.

Lorenz, Taylor, "How the Biden Administration Let Right-Wing Attacks Derail Its Disinformation Efforts," *Washington Post*, May 18, 2022.

Marler, Tim, "Beware the Allure of Training Technology," *Defense News*, May 18, 2022.

Merriam-Webster Dictionary, "meta," undated.

Meta, "What Is the Metaverse?" webpage, undated. As of April 2, 2023: https://about.meta.com/what-is-the-metaverse/

Metaverse Standards Forum, homepage, undated. As of April 2, 2023: https://metaverse-standards.org

Microsoft, "Microsoft Mesh," homepage, undated. As of April 2, 2023: https://www.microsoft.com/en-us/mesh

Milmo, Dan, "A Whole New World: Disney Is Latest Firm to Announce Metaverse Plans," *The Guardian*, November 11, 2021.

Niantic, homepage, undated. As of April 2, 2023: https://nianticlabs.com

Oxford English Dictionary Online, "metaverse," undated.

Park, Sang-Min, and Young-Gab Kim, "A Metaverse: Taxonomy, Components, Applications, and Open Challenges," *IEEE Access*, Vol. 10, January 13, 2022.

Roach, John, "Mesh for Microsoft Teams Aims to Make Collaboration in the 'Metaverse' Personal and Fun," Microsoft, November 2, 2021.

Robinson, Joanna, "The Sci-Fi Guru Who Predicted Google Earth Explains Silicon Valley's Latest Obsession," *Vanity Fair*, June 23, 2017.

Roblox, homepage, undated. As of April 2, 2023: https://www.roblox.com

Rudman, Mara, Rudy deLeon, Joel Martinez, Elisa Massimino, Silva Mathema, Katrina Mulligan, Alexandra Schmitt, and Philip E. Wolgin, "Redefining Homeland Security: A New Framework for DHS to Meet Today's Challenges," Center for American Progress, June 16, 2021.

Science and Technology Directorate, U.S. Department of Homeland Security, "Maritime Safety and Security," fact sheet, undated-a.

Science and Technology Directorate, U.S. Department of Homeland Security, "Radiological/Nuclear Response and Recovery Research and Development," fact sheet, undated-b.

Science and Technology Directorate, U.S. Department of Homeland Security, "Smart City Interoperability Reference Architecture," fact sheet, undated-c.

Science and Technology Directorate, U.S. Department of Homeland Security, "First Responder Capabilities," fact sheet, c. April 2021.

Science and Technology Directorate, U.S. Department of Homeland Security, "Public Safety and Violence Prevention," webpage, last updated September 7, 2022. As of April 16, 2023: https://www.dhs.gov/science-and-technology/public-safety-and-violence-prevention

Science and Technology Directorate, U.S. Department of Homeland Security, "Modeling and Simulation Technology Center," webpage, last updated January 12, 2023a. As of April 2, 2023: https://www.dhs.gov/science-and-technology/MS-TC

Science and Technology Directorate, U.S. Department of Homeland Security, "The Maryland Test Facility (MdTF)," webpage, last updated February 22, 2023b. As of April 2, 2023: https://www.dhs.gov/science-and-technology/maryland-test-facility

Sensorium AG, "Sensorium Galaxy," homepage, undated. As of April 2, 2023: https://sensoriumgalaxy.com

Sharma, Vivek, "Introducing a Personal Boundary for Horizon Worlds and Venues," *Meta Quest Blog*, February 4, 2022.

Smart, John, Jamais Cascio, Jerry Paffendorf, Cory Bridges, Jochen Hummel, James Hursthouse, and Randal Moss, *Metaverse Roadmap: Pathways to the 3D Web—A Cross-Industry Public Foresight Project*, Metaverse Roadmap, 2007.

S&T—*See* Science and Technology Directorate.

Stephenson, Neal, *Snow Crash*, Penguin Books Limited, 1992.

Sum of Us, "Metaverse: Another Cesspool of Toxic Content," May 2022.

Sutherland, Ivan E., "A Head-Mounted Three Dimensional Display," *Proceedings of the Fall Joint Computer Conference*, Part I, December 1968.

Tusk, Bradley, "Regulating the Metaverse(s)," January 31, 2022.

U.S. Department of Homeland Security, "Preserve and Uphold the Nation's Prosperity and Economic Security," webpage, last updated March 1, 2022a. As of April 18, 2023: https://www.dhs.gov/preserve-and-uphold-nations-prosperity-and-economic-security

U.S. Department of Homeland Security, "Cybersecurity," webpage, last updated November 2, 2022b. As of April 2, 2023: https://www.dhs.gov/topics/cybersecurity

U.S. Department of Homeland Security, "2022 Priorities," webpage, last updated February 3, 2023a. As of April 26, 2023: https://www.dhs.gov/priorities

U.S. Department of Homeland Security, "Mission," webpage, last updated February 26, 2023b. As of April 26, 2023: https://www.dhs.gov/mission

Vinsel, Lee, and Jeffrey Funk, "Blinded by the Hype," *Open Mind*, June 23, 2022.

Acknowledgments

We would like to thank Emma Westerman and Kelly Klima of the Management, Technology, and Capabilities Program for their oversight and direction. In addition, we are grateful for insightful review and feedback from Kyleanne M. Hunter. Finally, we would like to thank our quality assurance reviewers, Todd A. Richmond and Osonde Osoba, for their valuable feedback.

About the Authors

Tim Marler is a senior research engineer at the RAND Corporation and leads the VR and AR thrust for RAND's Tech and Narrative Lab. His work revolves around modeling and simulation with a focus multiobjective optimization, human systems, training simulators and virtual environments, VR and AR, advanced manufacturing, and emerging technology. He has a Ph.D. in mechanical engineering.

Zara Abdurahaman is an assistant policy researcher at RAND. She has a background in electrical and electronic engineering, and her interests are disruptive technology, equity, diversity, and ethics. Her research at RAND has included computer game design and simulation on racial equity policy analysis, equity-centered methodological framework design, and risk assessment on emerging technology. She is a doctoral candidate in the Technology Applications and Implications Stream at Pardee RAND Graduate School.

Benjamin Boudreaux is a policy researcher at RAND working in the intersection of ethics, emerging technology, and human security. His current research focuses on the ethics of artificial intelligence and on social media policy issues. He teaches ethics in theory, policy, and practice. Prior to joining RAND, Boudreaux was a diplomat in the U.S. Department of State's Cyber Policy office, where he worked to promote security, stability, and human rights in cyberspace, and led the department's cyber operations portfolio. Boudreaux holds a Ph.D. in philosophy.

Tim Gulden is a senior policy researcher at the RAND Corporation. His research focuses on modeling complex systems in the context of data, as well as more-general policy analysis, including cost/benefit analysis, organizational design, and cybersecurity policy. His Ph.D. is in public policy.

About This Perspective

The metaverse is an emerging concept and capability supported by multiple underlying emerging technologies, but its definition and key characteristics can be unclear. Thus, its relevance to some organizations, such as the U.S. Department of Homeland Security (DHS), can be unclear. This, in turn, can lead to unmitigated threats and missed opportunities.

This Perspective provides an initial analysis of the meaning of *metaverse* and its relevance to DHS. It summarizes critical aspects of a metaverse, DHS's overarching needs, and an initial analysis of how various risks and opportunities stemming from metaverses align with DHS mission sets.

This work was completed in 2022. This research was conducted using internal funding generated from operations of the RAND Homeland Security Research Division (HSRD) and within the HSRD Management, Technology, and Capabilities Program.

About the RAND Homeland Security Research Division

Funding for this research was provided by gifts from RAND supporters and income from the operation of HSRD. HSRD operates the Homeland Security Operational Analysis Center, a federally funded research and development center sponsored by DHS. HSRD also conducts research and analysis for other federal, state, local, tribal, territorial, and public- and private-sector organizations that make up the homeland security enterprise, within and outside the Homeland Security Operational Analysis Center contract. In addition, HSRD conducts research and analysis on homeland security matters for U.S. allies and private foundations.

For more information on HSRD, see www.rand.org/hsrd.

www.rand.org