Metawars: Projecting Future Conflicts in Virtual Domain

By Oleg Abdurashitov

ITSS Verona Magazine, Vol. 2, n. 2

Fall/Winter 2023

Metawars: Projecting Future Conflicts in Virtual Domain

Oleg Abdurashitov

To cite this article: Oleg Abdurashitov, *Metawars: Projecting Future Conflicts in Virtual Domain,* ITSS Verona Magazine, Vol. 2, no. 2, Fall/Winter 2023.

Keywords: Metaverse, Cybersecurity, Metawars, Cyberwarfare

ITSS Verona website: https://www.itssverona.it/itss-magazine

LinkedIn: https://www.linkedin.com/company/itss-verona/

Instagram: https://instagram.com/itss_verona?igshid=YmMyMTA2M2Y=

Published online: December 29th, 2023

Abstract: While study of conflicts in Metaverse may lack immediate practical interest due to its current infancy stage and the overly optimistic predictions about its imminent future, it is crucial to consider the trajectory of the Metaverse as it evolves into a digital subset of the real world. This prompts a critical inquiry into the potential scenario wherein conflicts originating in the physical or digital realm might extend their reach into the virtual space. This paper delves into the evolving concept of the Metaverse, drawing parallels with the development of cyberspace as a military domain. Not only the trajectory of cyberspace understanding bears similarities to the nascent Metaverse, the Metaverse itself may be considered a subset of cyberspace. Applying the analytical frameworks developed for cyberwarfare this paper focuses on the likelihood of major conflicts in Metaverse (or Metawars) to understand how such conflicts may arise and what they may look like. In exploring the likelihood of future "Metawars", the paper analyzes prerequisites for virtual wars, tools and tactics available to combatants, and the constraints of the virtual environment itself. This analysis aims to expand the comprehension of this new environment and calls for a proactive approach to prevent or mitigate the impact of future conflicts within the virtual landscapes.

The author would like to thank Fadli B. Sidek (Singapore), a cybersecurity researcher and Metaverse enthusiast, for his invaluable input and commentary.

Despite the recent setbacks in the development of the Metaverse, including massive losses in Meta's (NSDQ: META) VR arm Reality Labs[1] and plummeting prices of virtual land[2] on Web 3.0 platforms, the vision of a global Metaverse continues to promise an unparalleled immersive experience that over time will redefine the way we work, play, rest, and live. However, one aspect of human behavior that the discussion of Metaverse seems to omit is the human or societal drive to resolve conflicts through violence, individual or collective. Some debates are taking place around the former - for instance, the issue of cyberbullying or stalking has gained some attention due to unpleasant experiences of early adopters of the Metaverse . Nonetheless, the case of collective scalable violence that we may call 'Metawars' remains a largely unexplored area.

The lack of practical interest is at least understandable due to Metaverse currently being at the infancy stage with overly-optimistic predictions of its near future conveniently forgotten. However, if Metaverse will continue to evolve as yet another digital subset of the real world, one may question whether one day it will have potential for conflicts existing in the physical realm to spill over into the digital space.

In today's cyberspace, a large part of ongoing cyber conflict remains intrinsically connected to the geopolitical, historical, social, or territorial grievances in the real world. For instance, the advanced persistent threat (APT) groups' targeting often reflects political interests of their state sponsors[3], and attempts at information warfare are in line with broader political or

[1] Jonathan Vanian, Ariel Levy, "Meta lost $13.7 billion on Reality Labs in 2022 as Zuckerberg's metaverse bet gets pricier", *CNBC*, February 02, 2023 https://www.cnbc.com/2023/02/01/meta-lost-13point7-billion-on-reality-labs-in-2022-after-metaverse-pivot.html.

[2] Jessie A Alice, "$707 Million Investment in Metaverse So Far in 2023 Despite Metaverse Land Collapse" *Blockchain News*, Jul 04, 2023, https://blockchain.news/news/707-Million-Investment-in-Metaverse-So-Far-in-2023-Despite-Metaverse-Land-Collapse-bfa9ffb0-d8a6-4ee0-90ab-6122bf70077e.

[3] "Advanced Persistent Threat (APT) Groups & Threat Actors," Mandiant, accessed November 26, 2023, https://www.mandiant.com/resources/insights/apt-groups.

military objectives of the competing states[4] or non-state actors, like terrorist groups or hacktivists collectives.

There is, of course, little history or geography in today's Metaverse, as there are no states, ethnic identities, or history to speak of, and hence potential conflict along these lines seems unlikely. In addition, unlike in an anarchic structure of international relations where no single hegemon can set the rules, in a centralized Metaverse, like one embraced by Meta Inc., commercial entities have god-like powers in establishing what is possible and permissible in the virtual spaces they create and own. The competing vision of a decentralized Metaverse, powered by the Web 3.0 ethos where no single owner will be able to define the rules of the game, allows somewhat greater autonomy in terms of asset creation, trading and ownership. However, it is yet to take shape, and whether its rules would allow any organized confrontation remains to be seen.

Nonetheless, one cannot rule out that a major conflict may still take place even in the walled gardens of digital Eden. Conflicts are not only natural - they may well be desirable. As social media and gaming companies, the major proponents of immersive experiences, know all too well, conflict brings 'user engagement,' the one key metric that the companies' management teams swear by.

As demonstrated by increasingly hostile and tense interactions between individuals on social media it could be only a matter of time before users seeking their own tribe turn against a perceived 'other.' A decade ago the inventor of the term 'metaverse,' sci-fi author Neil Stephenson, envisioned a major war between players of an online game (MMORPG) based on the colors of their avatars' outfits, independent of the historical narrative developed by the game creators[5]. Something similar could likewise occur in the Metaverse.

[4] Council of Foreign Affairs, *Cyber Operations Tracker*, https://www.cfr.org/cyber-operations/
[5] Neal Stephenson, Reamde. 2011, Harper Collins

The potential for conflict is even more ripe in the current version of Metaverse, since one of its defining features is its mimicking the offline realm. As real-world organizations, including national embassies and international bodies, build their own digital replicas in a virtual environment, it is foreseeable that some existing conflicts could find their way into Metaverse. Even if this somewhat sterile virtual environment reduced the existing tensions - for example, by grouping various users within their own social bubbles and curbing their access to other segments or by heavily policing the speech and actions acceptable - Metaverse virtual communities may remain as prone to conflict as communities in the real world.

Just like nations and collectives in the real world, these digital communities would be 'constructed' through their members establishing language, history, worldviews, artistic endeavors, and behavioral patterns that are different from other communities[6]. No matter how arbitrary, imaginary, or plain ridiculous these differences might be to a casual observer, they would be very real for the group members, virtual or not. These differences could become even more pronounced in digital environments (as for many users and creators of multiplayer games, avatars and skins are key both to self- and group-identification), and which could in turn create a potential for organized groups of users to engage in activities targeting other users or communities. Once such concerted actions are conducted on a significant scale - and scaling is what digital technology does best - we may consider that the first Metawars have begun

Having established the potential for spillover of existing conflict into Metaverse or formation of a new conflict between the recently-established virtual communities is at least plausible, we now need to turn to the question of what means of warfare may be available to the opposing parties. Provided that Metaverse will itself remain an evolving environment, we have

[6] Thiesse, A.-M., & Norris, S. (2003). How Countries are Made: The Cultural Construction of European Nations. *Contexts*, *2*(2), 26–32.

to acknowledge that the only short answer to this question is that we don't yet know. Nonetheless, some observations can be made by looking at how such capabilities evolved in cyberspace.

Cyberspace shares its fundamental characteristics of a man-made multilayered domain with Metaverse, which in turn could be seen as a subdomain (or a by-product) of cyberspace, largely relying on the same technological backbone. Just like the Metaverse, cyberspace was not built with the domain's militarization in mind. In fact, cyberspace was not 'built', but rather evolved as common protocols and growing processing capabilities allowed explosive growth of interconnected digital systems. It is only through this evolution and expansion of cyberspace that security analysts and military planners of the 1990s and 2000s came to see potential ways of leveraging this unique domain for military purposes.

Here we may argue that Martin C. Libicki's definition of three key layers of cyberspace - physical, syntactic, and semantic, roughly representing hardware, software, and information[7] - would be still applicable to Metaverse. Libicki acknowledged that cyberspace - unlike other spaces or operational domains - has the unique characteristic of being a man-made construct, in essence a virtual medium. While the three layers are interconnected, cyber incidents mostly take place on the syntactic - or software level with the ultimate aim to disrupt or corrupt the semantic layer (or information that computers and humans rely on to make decisions). Similarly, the Metaverse can be viewed as a continuation, or rather expansion of Libicki's semantic level of cyberspace.

In case of conflict in Metaverse, the attacks on the first two levels would likely employ the tools already available for cyber operations, such as physical attacks on infrastructure or malware targeting equipment (ranging from servers to end-user peripherals) or seeking to destroy

[7] Martin C . Libicki, *Cyberdeterrence and Cyberwar*. RAND Corporation. Santa Monica CA, 2009, 12-13.

or leak data of individual users or communities. Exploitable vulnerabilities abound in any software or hardware, and it is only a matter of time until we learn of successful attacks against the underlying infrastructure of Metaverse. In terms of execution, such attacks would be largely indistinguishable from traditional cyberattacks with little to nothing Metaverse-specific about them.

In turn, the syntactic level of Metaverse - and that in fact is the very immersive user experience of Metaverse itself - presents a somewhat different case, because it is supposed to be, well, immersive. What we know so far is that users of Metaverse will have the ability to interact with objects and each other, but the nature of such interactions is highly dependent on the platform's architecture. Hence the means available to potential Metaverse combatants would be mostly the same means available to all users. To date, that leaves us with a rather limited ecosystem of 3D avatars, virtual objects and pre-programmed interactions between them.

What can we make of these means in terms of potential military uses in case of conflict in Metaverse? Following from Martin C. Libicki suggestion that conflicts in cyberspace must be analyzed on the domain's own unique terms, what are the potential instruments in Metaverse that could be used to inflict significant, even violent damage, on a competing group operating in the same environment?

At first glance, these options today seem very limited. Both centralized and decentralized visions of Metaverse generally lack tools for violent confrontation, and thus acquiring capabilities for conflict in Metaverse is constrained by its very architecture. While at some point the Metaverse developers may introduce 'weapons' to all or some users, it is likely that those would be only available in some specially designed areas rather than in Metaverse at large. The *Ready Player One*-like environment with an array of weaponized artifacts available at all times

and in all settings may not only be years or decades away technologically - it may go against the very business logic of Metaverse as a place for social and commercial activity.

Thus on the semantic (or cognitive) level of the Metaverse, we are mainly looking at the potential weaponization of social and economic mechanisms within the Metaverse itself. In the area of social interactions, the Metaverse seems to offer opportunities to engage in psychological warfare and disinformation campaigns. These can range from stalking or harassing selected high-profile individuals or groups, to targeting places of economic and social importance by either denying access to these or overtaking them, akin to a group of like-minded insurgents storming the virtual Capitol.

From the perspective of economic warfare , we must take into account that in its current incarnation the Metaverse will only host a limited number of users and 'spaces' on a single server and thus competition for finite resources may well become a prerequisite to various forms of conflict. Collectively, a group of like-minded individuals may have a greater ability to purchase a greater share of 'space' or build a greater number of virtual 'real estate' potentially limiting options available to other groups. Also, one such group could constrain another group's ability to produce economic value, for instance by declining to purchase or sell virtual products or properties, effectively imposing economic 'sanctions.'

On a spatial level, the 'spaces' offered in today's Metaverse(s) are finite and often measured in virtual 'square kilometers,' thus making the tactics of blockades and displacements an attractive form of potential conflict. For example, a group large enough could attempt to deny a competing group access to important places of social and economic activity - like virtual marketplaces, meeting areas, or portals to other parts of the metaverse - by purchasing 'land' around them and building various high-rise buildings blocking strategic locations of the other

groups. While these ‘virtual’ barriers may well be permissible enough to allow some ‘infiltration’ through the defenses, they may nonetheless effectively block a larger number of users from accessing the area in question and thus limit other groups’ ability to expand and develop in the same virtual environment.

Finally, we may consider that by exploiting software vulnerabilities or undocumented functionalities, organized groups may acquire capacities that in some sense could be considered ‘weapons’. For instance, exploiting an access management system purchased on the Dark Web could allow a certain group to restrict the ability of other groups or individuals to enter the Metaverse altogether. Alternatively, through insider attacks on platform owners, as in the case of centralized Metaverse, an aggressor may acquire internal ‘policing’ capabilities such as blocking groups or users or deleting their data - and that means their very existence - from Metaverse.

This activity would likely happen behind the scenes of Metaverse and involve groups of hackers tinkering with the platform's code. However, seemingly little prevents these hackers from 'repackaging' software exploits as Metaverse artifacts (basically any virtual object users can interact with), such as a magic spell expelling a selected group from the area or a super grenade destroying virtual properties. This is especially plausible in the decentralized Metaverse, with its greater freedom to produce and sell virtual assets without supervision. Regardless, once such tools or services become available, competing groups will be incentivized to enter a virtual arms race.

Finally, today’s Metaverse is years or even decades away from having a palpable kinetic effect on its users. It would take dramatic leaps in technology, such as haptics, as well as far greater adoption of Metaverse, for the real and the virtual worlds to become truly inseparable. Kinetic impact is considered prerequisite to crossing the ‘threshold of violence’ that researchers

such as Thomas Rid define as the critical factor in defining something as 'war.'[8] It is safe to say that we are years, if not decades, away from a world where attacks in Metaverse could have significant consequences beyond its realm. Nonetheless, assuming that competing groups will naturally form within the Metaverse and seek out ways to harm each other on a significant scale, the platform owners may need to start thinking about how to manage such conflicts in the future and what preventative measures should be built into the Metaverse's fabric. 'Metawars' may lack the drama and damage of the real world conflicts, but like other wars, they will have a long-term destructive effect on the economic and social development potential of this new environment.

Conclusion

The Metaverse, while a novel, uncertain, and ambiguous concept as it is today, shares the key characteristics of a man-made domain with cyberspace. It thus can be approached with the same analytical apparatus developed over the decades of cyberspace turning into an expansive and complex battlefield of hacking attacks and information operations conducted by a plethora of actors.

While the Metaverse may never become as all-encompassing as cyberspace, which permeates every single aspect of modern society, the development trajectory of the domain's understanding may be reminiscent of the latter. From this point of view, the appearance and expansion of conflicts in Metaverse is not only likely but somewhat logical. Exploring what those future Metawars may look like would not only help to better understand its specifics - it may help to develop tools and solutions to prevent them, or at least limit their impact on the inhabitants of the future virtual worlds.

[8] Thomas Rid (2012) Cyber War Will Not Take Place, *Journal of Strategic Studies*, 35:1, 5-32.

Bibliography

"Advanced Persistent Threat (APT) Groups & Threat Actors." Mandiant. Accessed November 26, 2023. https://www.mandiant.com/resources/insights/apt-groups.

Alice, Jessie A. "$707 Million Investment in Metaverse So Far in 2023 Despite Metaverse Land Collapse." Blockchain News, July 04, 2023. https://blockchain.news/news/707-Million-Investment-in-Metaverse-So-Far-in-2023-Despite-Metaverse-Land-Collapse-bfa9ffb0-d8a6-4ee0-90ab-6122bf70077e.

Council of Foreign Affairs. "Cyber Operations Tracker." https://www.cfr.org/cyber-operations/.

Libicki, Martin C. Cyberdeterrence and Cyberwar. RAND Corporation. Santa Monica, CA, 2009.

Rid, Thomas. "Cyber War Will Not Take Place." Journal of Strategic Studies 35, no. 1 (2012): 5-32.

Stephenson, Neal. Reamde. 2011. Harper Collins.

Thiesse, Anne-Marie, and Sigrid Norris. "How Countries are Made: The Cultural Construction of European Nations." Contexts 2, no. 2 (2003): 26–32.

Vanian, Jonathan, and Ariel Levy. "Meta Lost $13.7 Billion on Reality Labs in 2022 as Zuckerberg's Metaverse Bet Gets Pricier." CNBC, February 02, 2023. https://www.cnbc.com/2023/02/01/meta-lost-13point7-billion-on-reality-labs-in-2022-after-metaverse-pivot.html.