INSTITUTE FOR DEFENSE ANALYSES

The Transnational Threat of Radicalization Through the Use of Online Gaming Platforms

Sujeeta B. Bhatt
Janna R. Mantua

September 2022

IDA Document NS D-33269
Log: H 22-000421

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305-3086

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the IDA Systems and Analyses Center under contract HQ0034-14-D-0001. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

For More Information

Sujeeta B. Bhatt, Project Leader
sbhatt@ida.org, 703-578-2719

Leonard J. Buckley, Director, Science and Technology Division
lbuckley@ida.org, 703-578-2800

Rigorous Analysis | Trusted Expertise | Service to the Nation

The Transnational Threat of Radicalization Through the Use of Online Gaming Platforms

Radicalization, Extremism, and Terrorism

An agreed-upon definition of extremism and its associated terms (e.g., terrorism, domestic terrorism, violent extremism, homegrown violent extremism, hate crime) (Schmid, 2011) has been a long-existing challenge for social and behavioral scientists as well as for the law enforcement and intelligence agencies tasked with keeping the public safe from extremist activity. These definitional challenges arise due to the subjectivity associated with categorizing thoughts, beliefs, and actions as extremist. Further, the definition of extremism depends on a number of factors, including the nature of the political system, prevailing political culture, system of values, ideology, personal characteristics, experiences, and ethnocentrism (Sotlar, 2004). In essence, the definition of what is considered extremist is in the eye of the beholder.

Although each term refers to a distinct aspect of the issue, radicalization, extremism, and terrorism are often used interchangeably (and incorrectly) in publications and by the media. Simply put, radicalization is the transformational cognitive-behavioral process by which an individual develops extremist ideologies, beliefs, values, and emotions that are outside of or in opposition to those in mainstream society, which can then lead to extremist actions or behaviors (e.g., an act of terrorism) (Bartlett, Birdwell, & King, 2010; Borum, 2011). It is important to keep in mind that radicalization alone is not indicative of impending violent action as there are far more radicalized individuals in the world than there are individuals who will engage in an act of terrorism (Neumann, 2003). Still, almost all individuals who engage in terrorist acts have gone through a radicalization process (Wolfowicz, Litmanovitz, Weisburd, & Hasisi, 2021).

Extremism refers to those ideologies, beliefs, and convictions that oppose the fundamental values of society, the laws of democracy, and common notions of human rights, often advocating the supremacy of a particular group (racial, religious, political, economic, social, etc.). Additionally, extremism has been used to refer to the methods (though not the specific acts) through which extremist actors try to achieve their aims (Klein & Kruglanski, 2013; Trip, Bora, Marian, Halmajan, & Drugas, 2019). We note that many definitions of extremism erroneously combine ideological motivations with their associated violent actions, effectively blending extremism with terrorism. The academic literature categorizes extremism by the fundamental ideology or motivation for extremist actions and behaviors. Researchers generally agree on four main types of extremist (violent and non-violent) ideologies: left-wing, right-wing, single-issue, and politico-religious. Each category of extremist ideology is associated with a variety of groups and some groups fit into multiple ideological categories. The Aryan Nations could thus be considered both a right-wing and politico-religious extremist group because it was founded on the Christian Identity and white supremacist movement.

While radicalization and extremism target cognitive and behavioral change, terrorism is an expression or manifestation of a violent ideology. Further, while extremism can be expressed through violent or non-violent action, terrorism, by definition, requires violence or the threat of violence. An individual can espouse violent extremist ideology without committing a crime; however, once the threshold of planning, preparation, and/or execution of a criminal act has been crossed, an act of terrorism has occurred (Miller, 2019). The type of terrorism depends on the discrimination between legitimate and illegitimate targets, the degree of force used, the agency of the perpetrator (e.g., state vs. non-state actors), the context of the terrorist act (e.g., domestic vs. international) (Kaplan, 2016), and whether the violent act was committed by an extremist group

or by a single individual who is neither part of a group nor directed by an outside organization. This last categorization makes the distinction between groups and lone-wolf or lone-actor terrorists.

The definitions and typologies of radicalization, extremism, and terrorism used by law enforcement differ from those described in academic literature. In response to the Fiscal Year 2020 National Defense Authorization Act (FY 2020 NDAA), the Federal Bureau of Investigations (FBI), U.S. Department of Homeland Security (DHS), and the Director of National Intelligence (DNI) (collectively known as law enforcement and intelligence agencies, or LEIAs) jointly developed standardized definitions of terminology relating to domestic terrorism and provided typologies of domestic terrorism threats. The LEIAs use the term "violent extremism" because it is the aspect of violence, rather than the underlying extremist ideology or the advocacy of this ideology, that can be prohibited by law. Using this approach, the LEIAs developed a list of domestic threat typologies, including racially or ethnically motivated extremism, anti-government or anti-authority extremism, animal rights or environmental extremism, abortion-related extremism, and other domestic terrorist threats. However, the LEIAs acknowledge that the motivations of actors vary, are nuanced, and can arise from a blend of ideologies (*Strategic Intelligence Assessment and Data on Domestic Terrorism* 2021).

International and domestic terrorism are defined in Section 2331(5) of Title 18, United States Code. Both categories of terrorism include violent acts or acts that are dangerous to human life (including those designed to intimidate or coerce civilian populations, influence governmental policy that would be criminal law violations if committed in U.S. jurisdiction). International terrorist acts take place primarily outside U.S. territorial jurisdiction or are considered transnational due to the manner in which the acts are accomplished, the persons they appear

intended to intimidate or coerce, or the location where the perpetrator resides (or operates from). On the other hand, domestic terrorist acts occur primarily within U.S. territorial jurisdiction and do not include these transnational factors. Under these definitions, a U.S. citizen who is inspired by al-Qaeda (or other internationally based extremist ideology) could be engaging in an act of international terrorism, even if he or she has no actual international ties and carries out an attack on U.S. soil (Sinnar, 2018).

Risk Factors for Radicalization

Radicalization is influenced by a number of factors and as such, there is no single pathway or explanatory theory for radicalization that can apply to all individuals (or groups). Radicalization is not "the product of a single decision but the end result of a dialectical process that gradually pushes an individual towards a commitment to violence over time" (McCormick, 2003). Because it is a dynamic, multi-stage, and multi-faceted process, radicalization is influenced by push, pull, and personal factors in an enabling environment. Push factors include real or perceived factors external to the individual that pushes him/her towards radicalization. Structural, political, and sociological contexts such as a lack of socioeconomic opportunities, marginalization or discrimination, and prolonged or unresolved conflicts are examples of push factors. Alternatively, pull factors are group-level socio-cognitive (or psychological) factors that pull individuals into seeking information, experiences, and other individuals with similar extremist ideologies, pulling him/her towards radicalization. Pull factors can include grievances by groups of individuals who feel oppressed in their communities due to local or national political ideologies, or ethnic/cultural differences. Finally, personal factors are those individual characteristics and psychological and biographical experiences that make some individuals more vulnerable to radicalization. For

example, psychological disorders, personality traits, and traumatic experiences are personal factors that affect the likelihood of radicalization (Cherney, Putra, Putera, Erikha, & Magrie, 2021).

As evidenced by these factors, the drivers of radicalization operate at the level of the individual, group/community, and society, and some drivers can resonate and operate across all three levels. Radicalization is a complex, context-dependent phenomenon that follows an unplanned path that is influenced by sociological, political, ideological, and psychological drivers over time, thus the process of radicalization is neither deterministic nor linear (Cherney et al., 2021). Further, vulnerability to radicalization may develop through small changes that combine to form a larger change (i.e., via a snowball effect) or though small changes that incrementally impact other layers, resulting in larger changes (i.e., in a spiral pattern). Any one or more of these factors can make one more (or less) vulnerable to radicalization and any of these factors can serve as a catalyst for radicalization. The process can be slow, taking place over a lifetime, or it can be quick, triggering real-time efforts to seek information on extremist groups and/or engage extremist activities.

A 2018 report by Allison Smith summarized the findings of four National Institutes of Justice research efforts examining potential risk factors associated with engaging or attempting to engage in terrorism for group-based and lone-actor extremists in the United States (Cherney et al., 2021). Similarly, a 2021 report by LaFree and Schwarzenbach (2021) examined a variety of micro- (i.e., personal or individual) and macro- (i.e., structural/societal) level factors that are associated (both positively and negatively) with radicalization and terrorism. Table 1 summarizes the findings of these two studies, assessing the association of 10 major demographic factors with radicalization

and terrorism.[1] Taking these risk factor as a whole, it seems that individuals with the highest risk of radicalization are young men with radicalized peers (both in person and online), who are un/under employed and single.

Table 1. Micro-level Risk Factors for Radicalization and Terrorism (adapted from Smith (2018) and LaFree and Schwarzenbach (2021)).

Factor	Findings
Gender	Majority of perpetrators of terrorism are male, including lone actors; proportion of women engaging in terrorism is increasing over time (LaFree, Jensen, James, & Safer-Lichtenstein, 2018; Ortbals & Poloni-Staudinger, 2018).
Age	Youth is generally associated with engagement in violent crime, but the average age of those engaging in terrorism is older and spans a broader age range; in the United States. however, younger individuals are radicalized to terrorism (Klausen, Morrill, & Libretti, 2016; Pyrooz, LaFree, Decker, & James, 2017).
Radical Peers	Having (and being in contact with) radical peers (including in social networks) significantly increases likelihood of developing violent extremist ideologies and engaging in terrorism; however, contact with non-violent peers protects against participation in terrorism (Lösel, King, Bender, & Jugl, 2018).
Employment	Most individuals engaged in terrorism were gainfully employed, but lack of stable employment is a strong risk factor for radicalization and engaging in political terrorism, particularly for lone-actors (LaFree & Schwarzenbach, 2021).
Marriage	Relationship between marital status and terrorism is mixed; marriage itself is not a protective factor as spouse is likely supportive of extremist behavior; vast majority of lone-actors were single, lived alone, or socially isolated (Altier, Leonard Boyle, & Horgan, 2021).
Military Service	Findings are mixed – military training serves as a protective factor from some extremist ideologies, but military training is a highly desired expertise for which some extremist groups recruit; there is a 33% likelihood that lone-actors had prior military service (Hafez, 2008; Napolitano, 2009).
Prior Criminal Activity	Pre-radicalization violent and/or nonviolent behavior is the strongest non-ideological predictor of post-radicalization violence; far-right extremists are more likely to engage in crime before radicalization than other ideologies; those engaging in criminal activity before age 18 are more likely than non-juvenile offenders to engage in violent extremist acts after radicalization (Jensen, Atwell Seate, & James, 2020).
Imprisonment	Past incarceration is associated with a higher likelihood of engagement in terrorism; findings increase twofold when individuals radicalized to extremist ideology while incarcerated (LaFree, Jiang, & Porter, 2020).
Ideology	Extreme ideology is associated with a higher likelihood of engaging in extremist actions (including terrorism) and aggressive attitudes and behaviors (Van Hiel et al., 2020).

[1] The researchers examined the relationship of each factor listed with engaging or attempting to engage in terrorism independently. In other words, neither the interactions of the potential risk factors nor the role of a combination of risk factors were examined.

Mental Illness	There is no consensus in the research, but mental illness may combine with other causal factors to produce a pathway to terrorism. This finding is more consistent for lone-actor terrorists (e.g., of far-right extremists who committed homicides, 40% of lone-actor terrorists vs. 8% of other far-right extremists had a reported history of mental health issues) than for other violent actors (Chermak, Freilich, & Suttmoeller, 2013).

Gaming as an Avenue for Increased Radicalization and Extremism

The inter-connectedness that the internet presents in the form of social media and gaming may itself be a catalyst for radicalization. According to statista.com, there were an estimated 3.24 billion gamers across the globe in 2021, making gaming the most profitable sector of the entertainment industry (Clement, 2021). Gaming is a broad and growing industry that is used for educational purposes, to promote physical activity and fitness, or simply for entertainment. The use of gaming increased during the early stages of the COVID-19 pandemic, during which many people could not leave their home for an extended period of time (Blazak, 2022). Due to its size and reach, people around the world are able to use games to interact with each other and to meet new people. In fact, the Pew Research Center found that 57% of surveyed teens reported making a new friend online, and 29% reported having made more than five friends online (Lenhart, 2015). Individuals who play video games (particularly first-person shooter games) are largely male and are of a younger demographic (although the prevalence of females and older individuals playing these games is increasing (Clement, 2021; Wittek et al., 2016; Yee, 2017)). These demographics are notably similar to demographics of individuals most vulnerable to radicalization. Accordingly, there is growing concern that this connectivity through gaming can provide fertile ground for a range of potentially criminal activity. As such, 74% of American adults reported experiencing some form of harassment and 65% reported severe harassment (e.g., physical threat, stalking) while playing online multiplayer games in a survey by the Anti-Defamation League. Further, 53% of the gamers who experienced harassment felt that they were targeted because of their

race/ethnicity, religion, ability, gender, or sexual orientation. In terms of extremism, 23% of adult gamers reported that they had been exposed to white supremacist ideology and 9% to Holocaust denials (League, 2019).

There is evidence that "gamification" within video games or video game-adjacent apps is increasing rates of extremism and radicalization worldwide by both radicalizing new individuals and by virtually bringing already radicalized individuals together. In fact, there is a growing body of literature examining the intersection between online extremism and gaming communities, possible risk factors and vulnerabilities that might make a gamer more susceptible to radicalization, and the gamification of extremism. The goal of the gamification (the inclusion of game elements such as body count/number of kills, badges, leaderboards, or select avatars) in video games is to lead to behavior change such that players are increasingly motivated to play and remain engaged (Steltenpohl, Reed, & Keys, 2018). Gamification could facilitate or accelerate the radicalization process by including pleasure, positive reinforcement, empowerment, competition, and social relatedness within the gaming community (see (Schlegel, 2020b). These elements may increase the likelihood that vulnerable individuals will join games, groups, or chats that are promoting extremist ideologies.

The Centre for Research and Evidence on Security Threats (CREST) recently published a research summary on the gamification of extremist ideologies (O. Brown, 2022). The report noted that Jihadists, such as the Islamic State, have a history of incorporating propaganda into video games. Right-wing extremists, similarly, have both modified mainstream games with far-right ideologies and developed their own video games. For example, in *Jesus Strikes Back: Judgment Day*, players can act out mass murders while using an avatar modelled on Brenton Tarrant (who has been charged with killing 51 individuals at a Christchurch, New Zealand

mosque in 2019) or select avatars such as Adolph Hitler or other current and former leaders associated with nationalist or far-right ideologies. During game play, players select different objectives and setting such that their task is to murder "feminists, gay people and migrants, with levels set in gay nightclubs, news studios and mosques as well as at the US-Mexico border" (Dick, 2019).

In addition to gamification, there are instances of extremist groups using gaming or gaming-adjacent apps (referred to hereafter as gaming apps), such as Discord, Twitch, Steam, and DLive, to engage in extremism-related communications. Due to increased reliability on computer-mediated communication, both domestic and international extremist views are easily shared across the world. For instance, the Institute for Strategic Dialogue (ISD) examined gaming platforms and found public servers in support of far-right political parties and violent neo-Nazi groups (such as the Nordic Resistance Movement and the Misanthropic Division) (Davey, 2021). Although Discord servers were used to host white nationalist/supremacist and neo-Nazi content, it also contained public channels sharing content promoting the Atomwaffen Division and Sonnenkrieg Division. Finally, DLive posters promoted extreme right views and Twitch content focused on conspiracy theories, and misogynistic and white supremacist views. Additionally, some groups have hosted gaming tournaments for recruitment. These events have invited their supporters to attend with the rationale that supporters may invite new members to come to the event (Townsend, 2021). Similarly, The Daily Stormer (a neo-Nazi website) launched its own *Pokémon Go* challenge to identify locations used as battlegrounds by its players and distributing recruitment materials at those locations (Nilan, 2021). There are also examples of extremist groups using gaming platforms or gaming apps to influence (i.e., radicalize) participants into action on behalf of the group. For instance, extremists have modified games,

such as *Counter-Strike, Civilization,* and *Crusader Kings*, to incorporate far right (specifically, white power) ideology into the gameplay. In addition, there was a 2014 movement termed GamerGate during which gamers mobilized en masse to engage in harassment and threaten female journalists with violence. This is seen as a historical moment for the creation of the "alternative right" (Davey, 2021).

Gaming Platform/App Features Facilitate Radicalization and Extremism

There are features inherent to gaming platforms and gaming apps, such as livestreaming, that bolster the use of these technologies for radicalization and extremism. Livestreaming is a novel capability that allows users to instantly broadcast a live video from their phone. Many gaming apps feature livestream capabilities that allow users to broadcast nefarious behaviors. Due to the proliferation of recordings/livestreams of extremist activity at demonstrations and even terrorist attacks (e.g., Tarrant livestreamed his attack in Christchurch), extremists have been able to gamify these recordings, essentially creating an extremist metaverse, or the virtual space within digital environments such as in augmented reality (Schlegel, 2020a). This capability allows extremist activists to promote and support extremist activity without ever leaving their chairs. In fact, Twitch and other gaming chatrooms have been used by extremists not only to disseminate their extremist propaganda and misinformation, but also to allow these individuals to make money by streaming video games and permitting individuals to donate money directly to the streamers (Russonello, 2021). In these cases, individuals can sponsor gamers (with or without similar extremist views) by "gifting" them virtual items within the game. The gamer can then exchange these gifts for cryptocurrency. The FBI reports that the ability to purchase and sell virtual items within games has been used by terrorist organizations to launder funds or transfer funds to individuals planning terrorist attacks (*Awareness Brief: Online Services and Violent*

Extremism, 2014). The regulatory enforcement of these types of financial transactions is still being developed. A challenge is the fact that these types of financial transactions are lucrative revenue streams for smaller and newer streaming and gaming platforms, thus providing incentive for these companies to not engage in content moderation (Network, 2021).

Livestreaming capabilities of gaming and social media apps have created opportunities to easily and efficiently spread extremist messages for radicalization. For example, Brenton Tarrant livestreamed his attack from the vantage of first-person shooter games and the commentary he provided on his actions mimicked gaming language, a format popular in the gaming community ("Extremists' Use of Video Gaming – Strategies and Narratives," 2020). There were 4,000 views of the livestreamed attack before Facebook removed it, but by then it had quickly been copied and shared by Facebook users and had gone viral. Within the first 24 hours after the attack, Facebook removed 1.5 million video copies of the attack and blocked another 1.2 million attempts to upload copies of the video (similarly, YouTube scrambled to remove reposts of the video) (Macklin, 2019). This incident inspired a string of subsequent hate crimes and inspired copycat actors (Dodd, 2019). During the week after the Christchurch attack, there were 89 cases of anti-Muslim hate crimes in the United Kingdom, 85 of which referenced New Zealand, suggesting Tarrant's attack successfully propagated radicalization and violence. In a similar situation, the gaming app Twitch was used on Yom Kippur in 2019 to livestream a shooting at a synagogue in Halle, Germany (Lerman, 2019). This video also quickly went viral with 72,000 views within 5 days of the attack. In a more recent example, assailants livestreamed a targeted attack against African Americans at a Buffalo, NY supermarket on Twitch. Months after the shooting, the video can still be found online (Drew Harwell, 2022).

There are several reasons why livestream videos are difficult to police. In order to discontinue a livestream or to prevent it from going viral, the inappropriate content of the video must be quickly detected. The detection of the content leads to a “hard” consequence (blocking or removing the content) or a soft consequence (flagging, downranking) (Gorwa, Binns, & Katzenbach, 2020). It is not feasible to have humans screening all content that is published or livestreamed, so tech companies are increasingly relying on artificial intelligence (AI) for the detection of inappropriate content. Despite recent advances in AI, the technologies remain inadequate. The broadcast in Buffalo was discontinued only 2 minutes after the first gun shot. Despite this rapid response, watchers of the livestream were able to quickly share and save the video, making it nearly impossible for app regulators to remove all circulating copies. Even if AI advancements were made to improve detection speed, it is not clear that these technologies can stop the proliferation of inappropriate livestreams. This leaves a clear gap for terrorist groups and extremists to exploit.

Chat groups or discussions about extremism are equally as difficult to monitor and police. Because of features inherent to the apps, “dark social” apps, such as Discord, are frequently used to evade monitoring and detection. Specifically, Discord, a voice and text chat platform for gamers, is virtually free of moderation rules and allows users to create anonymous, private, invitation-only chat groups that are invisible to non-users (see (Inés Bolaños Somoano, 2022) for more information). Most features within this app are encrypted, which makes monitoring of activities within the app infeasible. Still, even if the monitoring of chats were indeed possible, extremists find ways to talk about their subject matter without explicitly discussing it. Specifically, extremist organizations use coded language in chats on common gaming platforms like Steam, Roblox, and Minecraft, to discuss their activities. By using seemingly innocuous

words in place of extremist language, chat users can evade algorithms that would otherwise flag the user or chat. Again, even if advanced AI were developed to monitor and detect extremism-related language, the use of coded language can disguise extremism-related language as banal and can evade detection. This solution may not be adequate to stem the problem.

Concerns for the Department of Defense and the Intelligence Community

Radicalization, extremism, and terrorism pose clear national security threats for both the Department of Defense (DoD) and the Intelligence Community (IC), but the LEIAs and DoD must balance national security needs with protections of U.S. citizens under the Constitution. Under current laws and policies, radicalizing others and spreading extremist ideology, even violent ideology, is a protected right. Until a crime or an act of terror has been committed, the LEIAs are unable to monitor and/or arrest domestic terrorist groups. The combination of these two factors may lead to a situation in which radicalization is spreading, but it cannot be detected or monitored. The specific concerns that these threats pose to the DoD and IC, and the limitations of these organizations in confronting these challenges, are discussed below.

The gamification of radicalization and extremism should be a concern to the DoD, particularly in terms of its counterintelligence implications. For example, the social connectedness that video games afford players has direct effects on active duty and reserve personnel (many of whom maintain active security clearances) across the Services. In a 2020 article for the United Service Organizations (USO), DeSimone and Johnson noted that spending time away from family was one of the most significant issues with military life reported by Service members and that gaming served as a mechanism to keep them connected to family and friends at home. Gaming has become such a critical communication tool for Service members that the USO outfits its centers with video games consisting of multiple screens and consoles.

The USO Gaming Community Manager described gaming as "…a new way of socializing [for our military]…" ("It's Not 'Just a Video Game': For Many of Today's Military, It's Their Connection Home," 2020).

Given the popularity of gaming platforms by active duty and reserve personnel across the Services, the gamification of radicalization may pose risks for extremism in the military. For example, USO centers have begun to organize local gaming tournaments and competitions open to USO guests, local civilians, retirees, and veterans. Additionally, the USO is also hosting larger online gaming competitions that are open to the public and livestreamed via Twitch ("It's Not 'Just a Video Game': For Many of Today's Military, It's Their Connection Home," 2020). Although the use of Twitch alone does not indicate an attempt at radicalization, opening the aperture of who is invited to play, which platforms are used for gameplay, and the livestreaming of such competitions may increase the likelihood that such events become an opportunity for extremists to identify targets for radicalization in our active duty forces. The recruitment of Service members to terrorist organizations is a real threat. In his October 13, 2021, Congressional Testimony, Dr. Seth Jones described efforts of domestic extremist groups and networks to recruit active duty personnel, reservists, and veterans. He noted that both left- and right-wing extremist organizations have been successful in their attempts (e.g., the Proud Boys, Oath Keepers, Three Percenters, and the Boogaloo Bois each have current and former military personnel as members) (*Violent Domestic Extremist Groups and the Recruitment of Veterans*, 2021).

The gamification of extremism is also a concern for the IC in regards to national security. Similar to the DoD, the IC also faces counterintelligence risks posed by gaming and gaming-app platforms in terms of radicalization. Current policy poses another challenge for the IC in terms of

addressing radicalization and insider threat issues posed by gaming platforms and apps. Section 702 of the Foreign Intelligence Surveillance Act (FISA) allows the U.S. government to surveil communications of U.S. citizens without a warrant if the principle purpose of the surveillance is to gather "foreign intelligence information." In other words, U.S. citizens can be monitored by the IC if there is a purported association with a foreign terrorist organization. Given these limitations, the IC cannot actively monitor extremism-related communications on gaming platforms or gaming apps unless there is a link between the users and foreign terrorists. Under this law, U.S. citizens communicating about Islamic extremism may be monitored, but U.S. citizens communicating about far-right or far-left extremism may not be. Further, even if monitoring of communications was authorized, encryption prevents the monitoring of communications in many of the gaming platforms and apps. This creates a difficult situation for the IC because illegal or nefarious activity may be happening on a widespread basis, but it cannot be detected or documented.

Both the IC and the DoD may be impacted by the gamification of extremism because many young individuals who are joining the military or the IC may have a history of exposure to—or may have directly participated in—gaming-based radicalization and extremism. As reported by the ISD, the average age of individuals participating in extremism-based communication in gaming apps is 15 (Davey, 2021). Young individuals who join the military or begin working for the IC may have already experienced years of exposure to extremism through gaming. These individuals may be more prone to extremism-related beliefs, or they may have ties to nefarious actors through gaming who wish to take advantage of their position within the DoD/IC for malintent. Furthermore, individuals have begun to self-radicalize more and more due to easy access to

extremist messaging online. Thus, the identification of domestic extremist ideologies—within the general public, the DoD, and the IC—is somewhat of a moving target for LEIAs.

Strategies for Mitigation

Increased Moderation and Surveillance

There are limited means for reducing radicalization and extremism on gaming platforms and apps. There is some evidence to show that moderation can impact extremism-related behavior. Specifically, a study focusing on extremism-related behavior in gaming apps found that apps with a greater degree of moderation exhibited lower rates of extremism-related behavior (Davey, 2021). However, there are two limitations to this approach. First, as mentioned, moderation is difficult because there are ways to evade moderation technologies (e.g., using coded language to avoid algorithms). Second, users who experience moderation can choose to switch to an app with less moderation (of which there are many). App creators would need to actively commit to monitoring communications and reporting nefarious behavior to the proper government authorities in order for this to be effective. It seems unlikely that this will occur on a broad scale.

As mentioned, foreign intelligence information can be monitored under Section 702 of FISA, but domestic intelligence information cannot be gathered. Expanding definitions of terrorism under Section 702 of FISA to include domestic terrorism would allow for broader monitoring of extremism-related communications. However, monitoring private communications could be considered a violation of First Amendment rights related to free speech and/or the right to privacy. If FISA was expanded, a delicate balance would be needed to ensure rights of U.S. citizens are protected.

The DoD and IC may be able to moderate or surveil their own employees to reduce the risk for radicalization and extremism. Federal employees are currently limited in engaging in certain political activities under the Hatch Act. For instance, during duty hours, federal employees are prohibited from engaging in any political acts on social media. While off duty, federal employees are prohibited from using social media to solicit money for political campaigns or from using their position within the government to influence an election. Certain employees, such as certain individuals in the IC, are further restricted in their on- and off-duty activities. The Hatch Act was enacted to prevent federal employees from engaging with "any political organization which advocates the overthrow of our constitutional form of government" (C. Brown & Maskell, 2016). Individuals engaging with extremist organizations that wish to overthrow the government in private chats may be in violation of this principle. The Hatch Act could be expanded or clarified to limit the off-duty activities of federal employees to include private conversations related to radicalization and extremism on gaming platforms or apps.

Security Clearance Process Optimization

New processes could be implemented to ensure individuals who have participated in extremism-related activities online or on gaming apps do not receive a security clearance. Currently, when an individual is undergoing an investigation to obtain a security clearance, they must provide a broad range of information to investigators that will help them determine whether they are suitable to obtain a clearance. Often, investigators will interview friends or acquaintances of the applicant to determine whether they have been involved in activities deemed suspicious. Friends are selected in a geographical manner. In other words, applicants are asked to report the names of friends/acquaintances at each geographic location in which they have lived over a certain period of time. This approach precludes the inclusion of gaming/online-

only friends from being interviewed by investigators. However, online/gaming friends may have insight into potential online extremism-related activities in which the applicant has engaged. Modifying clearance investigation practices to include the interviewing of "gaming friends" could be an avenue for identifying individuals participating in online/gaming extremism-related behaviors prior to their entry into the national security realm.

Individuals applying for a security clearance must report any "close contact" they have with foreign nationals, and individuals holding a clearance must report close foreign contacts on an ongoing basis. Close contact is defined as "close and/or continuing contact with a foreign national with whom you, or your spouse, or cohabitant are bound by affection, influence, common interests, and/or obligation" (*Questionnaire for National Security Positions*, 2016). As previously mentioned, many gamers (over half surveyed) reported making friends online through gaming (Lenhart, 2015). In many cases, it is not possible to verify the identity of gaming/online-only friends. A nefarious actor could claim to be from the United States but may be a foreign national, living either in the United States or overseas. In this case, a foreign contact may not be reported appropriately because the clearance applicant does not realize they have been in close or continuing contact with a foreign national. At best, this will be an oversight on the security clearance application, and, at worse, the foreign contact could be intentionally creating a friendship for the purpose of coercion. To alleviate this issue, security clearance investigators could ask the applicant to share contact information of their close contacts who are gaming/online-only friends in order to verify their identity.

Trainings

Members of both the IC and the DoD regularly complete training courses that provide information to help them identify "insider threats." An insider threat is a malicious threat that

comes from individuals working for or affiliated with the organization (e.g., employees, contractors, or partners). There have been a number of cases in which IC/DoD employees have leaked sensitive information to individuals outside of the organization (e.g., foreign governments, news organizations), the most notable case being Edward Snowden. The trainings that IC/DoD employees complete on insider threat provide information on shared features of previous defectors. For instance, the trainings note that previous defectors are often having financial difficulties or turmoil in their personal life when they conduct the attack. The rationale for training IC/DoD employees about these shared characteristics is that understanding commonalities between these individuals may help with their identification before an attack is committed. In a comparable manner, trainings on what makes individuals vulnerable to extremism (including online/gaming-related extremism) could be implemented. Such trainings would educate IC/DoD employees on what behaviors may be linked to extremism. Increasing awareness of these vulnerabilities could increase the likelihood of detecting these individuals prior to an attack.

Individuals in the IC and DoD also regularly complete training courses on how to have "cyber awareness." Cyber awareness courses are intended to "provide an overview of current cybersecurity threats and best practices to keep information and information systems secure at home and at work" ("Cyber Awareness Challenge 2022," 2022). The training predominantly focuses on avoiding attacks that occur on one's computer/email, such as phishing and whaling. The trainings highlight suspicious behavior that one could encounter when corresponding with a nefarious actor online. However, there are currently no training modules related to keeping oneself safe from gaming contacts. Gaming contacts can easily penetrate one's defenses through social contact and common gaming interests. IC/DoD cyber-awareness trainings could provide

information on how to identify suspicious individuals on gaming platforms or apps and how to protect oneself from malicious actors. Expanding on this training, the IC and the DoD might modify the cyber-awareness training to model simulated cyber-attacks that are often put into action jointly by an organization's information technology and security offices. This real-world training would be game-based, allowing participants to experience the various ways in which extremists and others with nefarious agendas threaten national security via gaming and gaming-app platforms.

Lastly, trainings to specifically reduce radicalization and extremism-related behavior in IC/DoD employees could be implemented. A recently created training with this intent targets users, appropriately, through a videogame (Pisoiu & Lippe, 2022). The videogame has an interactive design through which "characters" with different backstories act as the protagonists of the game. The game displays "alternative narratives" to contradict common extremist beliefs and conspiracy theories. A pilot study of the game in a non-DoD/IC population demonstrated participants had a reduction in extremism-related beliefs as a result of playing the game. This game, or others with a similar theme, may be used to (1) test current extremist views, and (2) reduce extremist behaviors in individuals within the IC and the DoD community.

Conclusions

The current National Terrorism Advisory System Bulletin released by the DHS places the United States in a heightened threat environment due to "threat actors" becoming mobilized by "personal grievances, reactions to current events, and adherence to violent extremist ideologies..." (*Summary of the Terrorism Threat to the United States*, 2022). The level of the threat was determined though DHS' analysis of online forums where posters regularly endorse domestic violent extremist and conspiracy theory-related ideologies and spread disinformation in

order to incite grievances against targeted groups (e.g., the government). They report that "the continued proliferation of false or misleading narratives regarding current events could reinforce existing personal grievances or ideologies, and in combination with other factors, could inspire individuals to mobilize to violence." Although DHS and other LEIAs are doing all they can within the bounds of U.S. policy and law regarding the monitoring of online activity for domestic threats, very little is being done to monitor gaming and gaming-app platforms for extremist messaging and radicalization efforts (Network, 2021). Likewise, preventing and countering radicalization and violent extremism (P/CVE) efforts on gaming platforms are mostly limited to content moderation (done mostly by larger gaming companies) while innovative game-based P/CVE approaches are in their infancy in terms of development and deployment. The lack of adequate regulation of gaming and gaming-app communication platforms by both the gaming industry and security-related agencies combined with the gamification of radicalization by extremist organizations (to include developing financial and fundraising opportunities through such games) allows for the proliferation of social environments that can be exploited for radicalization.

The popularity of gaming and gaming apps will continue to rise. The gamification of radicalization and extremism should be a concern to both the DoD and the IC particularly in terms of its counterintelligence implications. Further, current regulatory policy prevents the LEIAs (to include the DoD) from actively monitoring domestic extremism-related communications on gaming platforms or gaming apps. This creates a problem for the DoD and IC because many young individuals joining the military or pursuing careers in national security may have been exposed to or may have participated in game-based radicalization, making them more susceptible to extremist beliefs and or actions.

That being said, there are a number of avenues for the DoD and IC to address this issue. First, they can work with game and gaming app developers to support and increase moderation and surveillance of these platforms for radicalization and extremist chatter, banning individuals espousing such beliefs. They can also include domestic terrorism in Section 702 of FISA to allow for broader monitoring of extremism-related communications. However, FISA executions using this expanded definition of terrorism would need to ensure the rights of U.S. citizens are protected. The DoD and IC may be able to moderate or surveil their own employees to reduce the risk for radicalization and extremism by expanding prohibited activities under the Hatch Act. Secondly, the DoD and IC can modify the clearance investigation process to include the interviewing of friends made on gaming apps to better understand potential counterintelligence risks posed by these individuals. Expanding the list of individuals included for interviews in clearance investigations could be an avenue for identifying individuals participating in online/gaming extremism-related behaviors prior to their entry into the national security realm. Finally, the IC and DoD can improve on current insider-threat and cyber-awareness training to include the national security risks posed by gaming and gaming apps. Trainings on what makes individuals vulnerable to extremism (including online/gaming-related extremism) could be implemented in order to educate IC/DoD employees on what behaviors may be linked to extremism. Increasing awareness of these vulnerabilities could increase the likelihood of detecting these individuals prior to an attack. Likewise, expanding cyber-awareness training to include modules related to keeping oneself safe from gaming contacts, how to identify suspicious individuals on gaming platforms or apps, and how to protect oneself from malicious actors. This training can also include modules focused on preventing or countering radicalization and violent extremism.

Bibliography

Altier, M. B., Leonard Boyle, E., & Horgan, J. G. (2021). Returning to the fight: An empirical analysis of terrorist reengagement and recidivism. *Terrorism and Political Violence, 33*(4), 836-860.

Awareness Brief: Online Services and Violent Extremism. (2014). Retrieved from https://cops.usdoj.gov/RIC/Publications/cops-w0740-pub.pdf

Bartlett, J., Birdwell, J., & King, M. (2010). The edge of violence: A radical approach to extremism. *Demos*, 5-75.

Blazak, R. (2022). Revisiting the White Boys From Portland to Ukraine: Anomie and Right-Wing Extremism. *American Behavioral Scientist*, 00027642221108940.

Borum, R. (2011). Radicalization into violent extremism I: A review of social science theories. *Journal of strategic security, 4*(4), 7-36.

Brown, C., & Maskell, J. (2016). *Hatch Act Restrictions on Federal Employees' Political Activities in the Digital Age*: Congressional Research Service.

Brown, O. (2022). Right-Wing Extremism Online: Can We Use Digital Data To Measure Risk? Retrieved from https://crestresearch.ac.uk/comment/right-wing-extremism-online-can-we-use-digital-data-to-measure-risk/

Chermak, S., Freilich, J., & Suttmoeller, M. (2013). The organizational dynamics of far-right hate groups in the United States: Comparing violent to nonviolent organizations. *Studies in Conflict & Terrorism, 36*(3), 193-218.

Cherney, A., Putra, I. E., Putera, V. S., Erikha, F., & Magrie, M. F. (2021). The push and pull of radicalization and extremist disengagement: The application of criminological theory to

Indonesian and Australian cases of radicalization. *Journal of Criminology, 54*(4), 407-424.

Clement, J. (2021). U.S. gamers - Statistics & Facts. Retrieved from https://www.statista.com/topics/3070/us-gamers/#dossierKeyfigures

Cyber Awareness Challenge 2022. (2022). Retrieved from https://public.cyber.mil/training/cyber-awareness-challenge/

Davey, J. (2021). Gamers who hate: an introduction to ISD's gaming and extremism series. Retrieved from https://www.isdglobal.org/wp-content/uploads/2021/09/20210910-gaming-reportintro.pdf

Dick, S. (2019). Outpouring of disgust greets sick video game that makes targets of minorities, women and gays. Retrieved from https://thenewdaily.com.au/news/national/2019/03/22/violent-video-game-slammed/

Dodd, V. (2019). Anti-Muslim hate crimes soar in UK after Christchurch shootings. Retrieved from https://www.theguardian.com/society/2019/mar/22/anti-muslim-hate-crimes-soar-in-uk-after-christchurch-shootings

Drew Harwell, W. O. (2022). Buffalo shooting livestream remains available. Retrieved from https://www.washingtonpost.com/technology/2022/05/16/buffalo-shooting-live-stream/

Extremists' Use of Video Gaming – Strategies and Narratives. (2020). Retrieved from https://home-affairs.ec.europa.eu/system/files/2020-11/ran_cn_conclusion_paper_videogames_15-17092020_en.pdf

Gorwa, R., Binns, R., & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society, 7*(1), 2053951719897945.

Hafez, M. M. (2008). Radicalization in the Persian Gulf: Assessing the potential of Islamist militancy in Saudi Arabia and Yemen. *Dynamics of Asymmetric Conflict, 1*(1), 6-24.

Inés Bolaños Somoano, R. M.-W. (2022). Lessons From the Buffalo Shooting: Responses to Violent White Supremacy. Retrieved from https://icct.nl/publication/lessons-from-the-buffalo-shooting-responses-to-violent-white-supremacy/

It's Not 'Just a Video Game': For Many of Today's Military, It's Their Connection Home. (2020). Retrieved from https://www.uso.org/stories/2863-it-s-not-just-a-video-game-for-many-of-today-s-military-it-s-their-connection-home

Jensen, M. A., Atwell Seate, A., & James, P. A. (2020). Radicalization to violence: A pathway approach to studying extremism. *Terrorism and Political Violence, 32*(5), 1067-1090.

Kaplan, J. (2016). Waves of political terrorism. In *Oxford Research Encyclopedia of Politics*.

Klausen, J., Morrill, T., & Libretti, R. (2016). The terrorist age-crime curve: An analysis of American Islamist terrorist offenders and age-specific propensity for participation in violent and nonviolent incidents. *Social Science Quarterly, 97*(1), 19-32.

Klein, K. M., & Kruglanski, A. W. (2013). Commitment and extremism: A goal systemic analysis. *Journal of Social Issues, 69*(3), 419-435.

LaFree, G., Jensen, M. A., James, P. A., & Safer-Lichtenstein, A. (2018). Correlates of violent political extremism in the United States. *Criminology, 56*(2), 233-268.

LaFree, G., Jiang, B., & Porter, L. C. (2020). Prison and violent political extremism in the United States. *Journal of quantitative criminology, 36*(3), 473-498.

LaFree, G., & Schwarzenbach, A. (2021). Micro and macro-level risk factors for extremism and terrorism: Toward a criminology of extremist violence. *Monatsschrift für Kriminologie und Strafrechtsreform, 104*(3), 184-202.

League, A.-D. (2019). Free to Play? Hate, Harassment, and Positive Social Experiences in Online Games. Retrieved from https://www.adl.org/free-to-play

Lenhart, A. (2015). Teens, Technology and Friendships. Retrieved from https://www.pewresearch.org/internet/2015/08/06/teens-technology-and-friendships/

Lerman, R. (2019). AP Explains: Streaming of German synagogue attack on Twitch. Retrieved from https://abcnews.go.com/Technology/wireStory/ap-explains-twitch-streaming-site-shooting-66190772

Lösel, F., King, S., Bender, D., & Jugl, I. (2018). Protective factors against extremism and violent radicalization: A systematic review of research. *International journal of developmental science, 12*(1-2), 89-102.

Macklin, G. (2019). The Christchurch Attacks: Livestream Terror in the Viral Video Age. Retrieved from https://ctc.westpoint.edu/christchurch-attacks-livestream-terror-viral-video-age/

McCormick, G. H. (2003). Terrorist decision making. *Annual Review of Political Science, 6*(1), 473-507.

Miller, G. D. (2019). Blurred Lines. *Perspectives on Terrorism, 13*(3), 63-75.

Napolitano, J. (2009). *Statement by U.S. Department of Homeland Security Secretary Janet Napolitano on the Threat of Right-Wing Extremism*.

Network, G. a. E. R. (2021). State of Play: Reviewing the Literature on Gaming & Extremism. Retrieved from https://drive.google.com/file/d/1WEq4OjtqZYdltAB0SK46M88gFF863jWs/view

Neumann, P. R. (2003). The trouble with radicalization. *International affairs, 89*(4), 873-893.

Nilan, P. (2021). *Young people and the far right*: Springer.

Ortbals, C. D., & Poloni-Staudinger, L. (2018). *Gender and Political Violence*: Springer.

Pisoiu, D., & Lippe, F. (2022). The name of the game: Promoting resilience against extremism through an online gaming campaign. *First Monday*.

Pyrooz, D. C., LaFree, G., Decker, S. H., & James, P. A. (2017). Cut from the same cloth? A comparative study of domestic extremists and gang members in the United States. *Justice Quarterly*.

Questionnaire for National Security Positions. (2016). Retrieved from https://www.opm.gov/forms/pdf_fill/sf86/

Russonello, G. (2021). Twitch, Where Far-Right Influencers Feel at Home. Retrieved from https://www.nytimes.com/2021/04/27/us/politics/twitch-trump-extremism.html

Schlegel, L. (2020a). Jumanji Extremism? How games and gamification could facilitate radicalization processes. *Journal for Deradicalization*(23), 1-44.

Schlegel, L. (2020b). Making extremism fun? The potential role of gamification in radicalization processes. Retrieved from https://modus-zad.de/blog/making-extremism-fun-gamification-extremism/

Schmid, A. P. (2011). *The Routledge handbook of terrorism research*: Taylor & Francis.

Sinnar, S. (2018). Separate and Unequal: The Law of Domestic and International Terrorism. *Mich. L. Rev., 117*, 1333.

Sotlar, A. (2004). Some Problems with a Definition and Perception of Extremism within a Society. *Policing in central and Eastern Europe: Dilemmas of contemporary criminal justice*, 703-707.

Steltenpohl, C. N., Reed, J., & Keys, C. (2018). Do others understand us? Fighting game community member perceptions of others' views of the FGC.

Strategic Intelligence Assessment and Data on Domestic Terrorism (2021).

Summary of the Terrorism Threat to the United States. (2022). Retrieved from https://www.dhs.gov/sites/default/files/ntas/alerts/22_0607_S1_NTAS-Bulletin_508.pdf

Townsend, M. (2021). How far right uses video games and tech to lure and radicalise teenage recruits. Retrieved from https://www.theguardian.com/world/2021/feb/14/how-far-right-uses-video-games-tech-lure-radicalise-teenage-recruits-white-supremacists

Trip, S., Bora, C. H., Marian, M., Halmajan, A., & Drugas, M. I. (2019). Psychological mechanisms involved in radicalization and extremism. A rational emotive behavioral conceptualization. *Frontiers in psychology, 10*, 437.

Van Hiel, A., Onraet, E., Bostyn, D. H., Stadeus, J., Haesevoets, T., Van Assche, J., & Roets, A. (2020). A meta-analytic integration of research on the relationship between right-wing ideological attitudes and aggressive tendencies. *European Review of Social Psychology, 31*(1), 183-221.

Violent Domestic Extremist Groups and the Recruitment of Veterans, (2021).

Wittek, C. T., Finserås, T. R., Pallesen, S., Mentzoni, R. A., Hanss, D., Griffiths, M. D., & Molde, H. (2016). Prevalence and predictors of video game addiction: A study based on a national representative sample of gamers. *International journal of mental health and addiction, 14*(5), 672-686.

Wolfowicz, M., Litmanovitz, Y., Weisburd, D., & Hasisi, B. (2021). Cognitive and behavioral radicalization: A systematic review of the putative risk and protective factors. *Campbell Systematic Reviews, 17*(3), e1174.

Yee, N. (2017). Beyond 50/50: Breaking Down The Percentage of Female Gamers by Genre. Retrieved from https://quanticfoundry.com/2017/01/19/female-gamers-by-genre/

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED *(From–To)*
September 2022	FINAL	

4. TITLE AND SUBTITLE

The Transnational Threat of Radicalization Through the Use of Online Gaming Platforms

5a. CONTRACT NUMBER
HQ0034-19-D-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Bhatt, Sujeeta B.
Mantua, Janna R.

5d. PROJECT NUMBER
STDPD

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Institute for Defense Analyses
Systems and Analyses Center
730 East Glebe Road
Alexandria, VA 22305-3086

8. PERFORMING ORGANIZATION REPORT NUMBER

IDA Document NS D-33269

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Institute for Defense Analyses
Systems and Analyses Center
730 East Glebe Road
Alexandria, VA 22305-3086

10. SPONSOR/MONITOR'S ACRONYM(S)

IDA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited (28 November 2022).

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The use of online games to interact with others around the world and meet new people has been rapidly increasing with the development of relevant technology (e.g., cloud adoption and access, 5G wireless technology). Individuals who play video games are largely male and are of a younger demographic. These are the same demographics of individuals most vulnerable to radicalization. There is growing concern that this connectivity through gaming can provide fertile ground for a range of potentially criminal activity and radicalization. Extremist organizations are leveraging the "gamification" of extremism to both radicalize new individuals and virtually bringing already radicalized individuals together, leading to an increased spread of extremist ideology worldwide. A growing body of literature has focused on possible risk factors and vulnerabilities that might make a gamer more susceptible to radicalization as well as on the gamification of extremism. The gamification of extremism poses clear national security threats for both the Department of Defense (DoD) and the Intelligence Community (IC), particularly in terms of its counterintelligence implications. In order to address this concern, the DoD and IC can develop policies for moderating gaming and gaming app platforms for Federal employees and Service members, optimize the security clearance process to account for online gaming relationships, and modify current counterintelligence and cybersecurity training for Federal employees and Service members.

15. SUBJECT TERMS

Counterintelligence (CI); countering violent extremism (CVE); DoD and Gaming; Online Gaming; radicalization

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Buckley, Leonard J.
Uncl.	Uncl.	Uncl.	SAR	31	19b. TELEPHONE NUMBER *(include area code)* 703-578-2800

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18