SEPTEMBER 2025

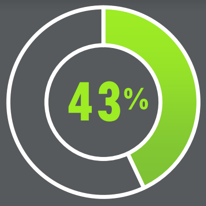
BTAC BULLETIN

BEHAVIORAL SCIENCE | LAW ENFORCEMENT & COUNTERINTELLIGENCE | CYBERSECURITY I EMPLOYEE MANAGEMENT RELATIONS I THREAT ASSESSMENT & MANAGEMENT

ONLINE GAMING

BENEFITS & INSIDER THREAT (InT) RISKS

Online gaming has grown as an avenue for social interaction and cultural engagement among military members, and other cleared personnel. Recent data indicate that over 201 million Americans[1], including service members and veterans, engage in video games, and two-thirds of U.S. gamers spend six to ten hours weekly gaming[1]. While gaming, and related social platforms, can foster positive outcomes—such as relaxation, stress relief, social bonding, and cognitive training—it also poses significant InT concerns. Organizations should consider the risks posed by foreign adversaries, terrorists, and other malicious actors who may seek to exploit these platforms to recruit and compromise trusted insiders and should train personnel in the identification of elicitation techniques through these platforms. By integrating cybersecurity measures on controlled organizational systems, with behavioral threat analysis and promoting awareness of risks and threat vectors, organizations can mitigate insider threats while fostering the use of gaming for training and camaraderie.



43% Of Soldiers reported playing videogames weekly[2]

TRUSTED INSIDERS & GAMING

- **Positive Engagement:** Many cleared individuals find community, stress relief, and peer support through multiplayer games and related platforms.[3]
- **Danger of Exploitation:** Foreign Intelligence Entities (FIEs) and violent groups increasingly use gaming social platforms *(e.g., Discord, Twitch, Steam)* for recruitment, violent content dissemination, and information elicitation.[4]
- **Online Disinhibition:** Individuals in cyberspace may say or do things in games or social platforms that they would not in “real life” situations because they feel less restrained and anonymous.[5]

THREAT VECTORS

- **Social Engineering:** Adversaries can establish trust through in-game chats, guild memberships, and private channels, gradually eliciting sensitive details about work roles or access.
- **Pathways to Violent Ideology:** Terrorist organizations may use multiplayer communities to disseminate ideologically based propaganda and groom potential recruits to violent behavior.
- **Illegal Content:** Encrypted chats and server channels can facilitate the exchange of illicit materials, including child sexual abuse material (CSAM) and contraband, posing legal and security risks.

IDENTIFICATION OF ELICITATION

- **Unusual Online Behaviors:** Rapid shift to encrypted or private gaming servers, particularly with new contacts (e.g., Telegram, WhatsApp).
- **Inquiries About Sensitive Duties:** Probing questions on professional responsibilities, clearance levels, or work location.
- **Foreign Affiliations:** Online profiles/’handles’ showing foreign ties, radical content, or repeated efforts to move discussions off-platform.
- **Suspicious Content Sharing:** Uptick in explicit or illicit content (e.g., sharing violent gore materials or CSAM) through private channels.

InT PROGRAM RECOMMENDATIONS

Policy Additions: Incorporate policies that outline the acceptable use (*and unauthorized disclosure risks)* of gaming, and social forums into existing cybersecurity policies and clarify reporting obligations regarding foreign or extremist contacts on these platforms.

Reporting Protocols: Urge employees to report any suspicious contacts or requests for sensitive information through gaming to security officials to include any gamer “handles.”

Cybersecurity + Cyberpsychology: Utilize integrated cyber literacy training including human behavioral considerations and elicitation techniques associated with this rapidly growing domain (e.g., Discord groups).

Community Awareness Training: Educate personnel on the tactics used by FIEs and malicious actors, especially in gaming communities, to elicit information.

Leverage Positive Aspects: Encourage the responsible use of gaming platforms and related social media forums for relaxation, team-building, and supportive programs (e.g., VA gaming therapies). Seek to avoid labeling video games as strictly “bad” or gamers as being a “problem” and emphasize positive attributes while educating about potential cyber and psychological risks.

[1] Clement, J. (2024, Nov 4). Video gaming in the United States - Statistics & Facts. [2] Orvis, K., Moore, J., Belanich, J., Murphy. J., & Horn D., (2010) Are Soldiers Gamers? Videogame Usage among Soldiers and Implications for the Effective Use of Serios Videogames for Military Training. *Military Psychology,* 22:143-157 Entertainment Software Association. (2022). [3] Video games relieve stress, Foster fun and camaraderie for veterans. VA News. (2023, March 9). [4] Lamphere-Englund, G., & White, J. (2023). The Online Gaming Ecosystem: Assessing Socialisation, Digital Harms, and Extremism Mitigation Efforts. Global Network on Extremism and Technology (GNET). [5] Suler, J. (2004). The online disinhibition effect. Cyberpsychology & behavior, 7(3), 321-326.