

Worldwide / Cyberspace: Probable use of videogames by China and Russia for intelligence operations against the United States

Chinese and Russian actors could recruit agents for disruption and intelligence collection operations for ideological and monetary reasons, with first contact established through videogames. We assess with probable certainty that Chinese and Russian agents will use video games during election season to recruit for disruption and intelligence collection operations. China is known for recruiting human assets with access to highly classified information, while Russia has a past of inciting real-life actions from internet communities. Chinese video games can be used to spy on the American population and gain vital intelligence, both from SIGINT operations and through human sources recruited in these games.

- Videogames have already been used to recruit terrorists, and this, since at least 2015, as some of the terrorists involved in the Bataclan attacks were recruited through the PlayStation Network since it is “more difficult to keep track of than WhatsApp” according to the Belgian federal home affairs minister,¹ and allows malicious actors to avoid “governments eavesdropping on those forms of communication”.
- Videogame communities meet on dedicated forums, some of which have additional message boards for topics not relating to gaming. 4Chan is a prime example of this, with message boards dedicated to gaming and others about domestic and international politics. A player looking to connect with others can easily get wrapped up in other message boards which adversaries can use to recruit operatives. The DNI has referred to this as “gamification” when adversarial parties use “gaming motivational techniques” to encourage violence outside of the gaming environment.²
- War Thunder and other games have exploited their realism and attention to detail as a marketing tool, boasting about players having access to simulated weapons from the 1920s to the early 2000s for battles. In recent times, players on forums dedicated to this game have used “sensitive or classified information” to settle debates about military equipment³ as reported by military blog Task and Purpose.
- Gaming content has gained popularity recently, leading to platforms like Twitch emerging which allow users to live stream themselves in real-time playing games and reacting to them. The January 6th riots and assault on the capitol were live-streamed by some of the rioters for others to cheer on in the text chat, with a lot of them actively using the “pog-champ” emote which was later banned. These disruption operations could be live streamed to generate propaganda and incite violence.

China desires to remain competitive against the United States and other Asian powers through the modernization of the People’s Liberation Army (PLA) at the lowest cost, while Russia seeks to undermine American democracy and the electoral process by any means necessary. In the wake of the next election,

¹ Paul Tassi, “How ISIS Terrorists May Have Used PlayStation 4 To Discuss And Plan Attacks,” *Forbes*, November 14, 2015, <https://www.forbes.com/sites/insertcoin/2015/11/14/why-the-paris-isis-terrorists-used-ps4-to-plan-attacks/?sh=24deb97e7055>.

² Director of National Intelligence, “Terrorist Exploitation of Online Gaming Platforms,” *First Responder’s Toolbox*, October 24, 2023, https://www.dni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/144s_-_First_Responders_Toolbox_-_Terrorist_Exploitation_of_Online_Gaming_Platforms.pdf.

³ Joshua Skovlund, “Sensitive Documents Showed up on War Thunder Forums. Again.,” *Task & Purpose*, December 19, 2023, <https://taskandpurpose.com/news/leaked-bradley-documents-war-thunder-forums-again/>.

adversaries could use these platforms to coordinate disruptions around polling sites, especially in key areas by “gamifying” the operation⁴.

- Russian electoral interference has been seen in the past with the 2016 election on social media reports David Sanger⁵ and more recently by Iran with Operation Endless Mayfly as studied by Gabrielle Lim⁶.
- Adversaries could try to recruit personnel with access to technical details to give away information under the guise of discussing game realism. Thinkers report that Chinese tech giant Tencent has invested in or bought some of the largest gaming companies, responsible for worldwide titles like “Fortnite” and the communications platform Discord⁷. We could see efforts by the MSS to try to recruit American personnel through video game platforms, especially if they are interested in military-themed ones like War Thunder and Digital Combat Simulator.
- We are likely to see new counterintelligence cases surrounding the loot box mechanic, as it stimulates the same part of the brain responsible for gambling and purchasing behavior.⁸ Payments to sources would likely not be done through physical exchanges but by trading in-game items and digital currencies that “do not meet anti-money-laundering standards”⁹, according to the DNI, and can be immediately laundered. As Chinese video games dominate the market and offer a lot of microtransactions, the MSS can get the data to spot and assess someone who has many lower-tiered items for very few higher-tiered ones.

If China and Russia achieve their goals, American military technology could be compromised due to leaks of technology, and independent actors could try to disrupt the electoral process leading up to November 2024. We assess an increased risk of leaks of information for both monetary and ideological reasons, with initial contact established through video games. American service members are known to access videogame platforms and classified information and have, in the past, leaked such documents on social exchange sites like Discord.

- Documents on American support for Ukraine surfaced on the official Minecraft Discord server in March 2023 before making their appearance in 4Chan message boards and telegram channels in

⁴ Director of National Intelligence.

⁵ David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, First paperback edition (New York: Broadway Books, 2019).

⁶ Gabrielle Lim et al., “Burned After Reading: Endless Mayfly’s Ephemeral Disinformation Campaign,” *Citizenlab.Ca*, May 14, 2019, <https://citizenlab.ca/2019/05/burned-after-reading-endless-mayflys-ephemeral-disinformation-campaign/>.

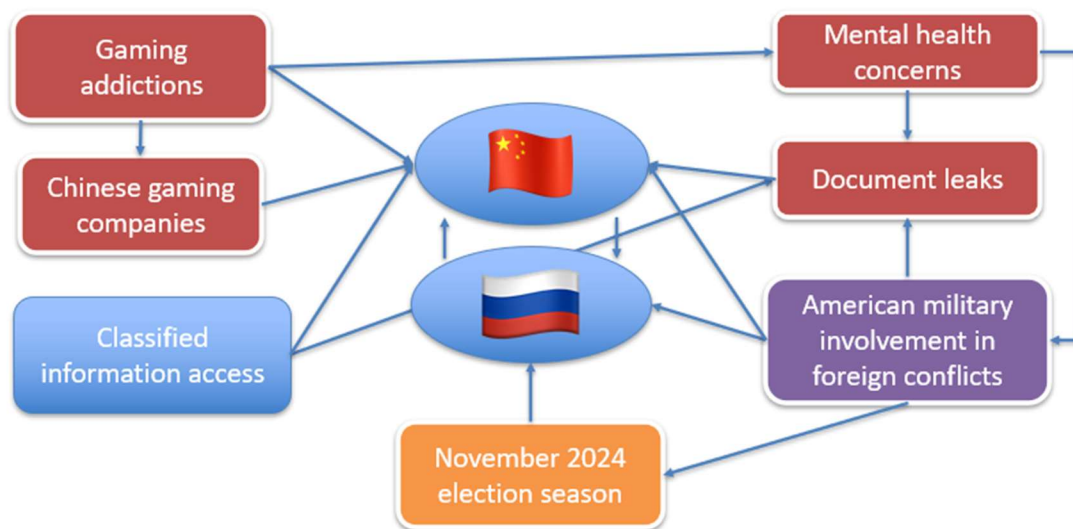
⁷ Dave Aitel and Jordan Schneider, “If You Play Videogames, China May Be Spying on You,” *Center for a New American Security*, October 28, 2020, <https://www.cnas.org/publications/commentary/if-you-play-videogames-china-may-be-spying-on-you#:~:text=Yes%E2%80%94China%20is%20already%20using,games%20to%20conduct%20intelligence%20operations.>

⁸ Xiaowei Cai, Javier Cebollada, and Mónica Cortiñas, “A Grounded Theory Approach to Understanding In-Game Goods Purchase,” ed. Jarosław Jankowski, *PLOS ONE* 17, no. 1 (January 27, 2022): e0262998, <https://doi.org/10.1371/journal.pone.0262998>.

⁹ Director of National Intelligence, “Terrorist Exploitation of Online Gaming Platforms.”

April, containing “maps and casualty figures”¹⁰. Just like for the War Thunder forums, this was posted to try to “win an argument” according to the Guardian¹¹. Given the current political context surrounding American involvement in the Middle East and Ukraine, recruitment of American service members by adversaries could focus on these key issues.

- According to a study from the Center for a New American Security on ten thousand soldiers, 51-59% of younger enlisted played video games frequently, which directly affected “aggression, sleep deprivation, and mental health” of junior enlisted to a greater degree.¹² This mental health crisis and connection to the internet was particularly evident during the Aaron Bushnell case when an Airman set himself on fire “while yelling ‘Free Palestine’”¹³ and was broadcast all over news channels like CNN.



1 Intersection of multiple issues, creating a concern for National Security

¹⁰ Matthew Loh, “Leaked Pentagon Documents Appeared on a ‘Minecraft’ Discord Server Weeks before Officials Knew about a Breach: Report,” *Business Insider*, April 12, 2023, <https://www.businessinsider.com/pentagon-document-leaks-origins-appeared-minecraft-discord-server-report-2023-4>.

¹¹ Harry Davies and Manisha Ganguly, “Up to 50 UK Special Forces Present in Ukraine This Year, US Leak Suggests,” *The Guardian*, April 11, 2023, <https://www.theguardian.com/uk-news/2023/apr/11/up-to-50-uk-special-forces-present-in-ukraine-this-year-us-leak-suggests>.

¹² Elizabeth Howe, Elena LoRussa, and Emma Moore, “Esports and the Military,” *Center for a New American Security*, August 3, 2021, <https://www.cnas.org/publications/reports/esports-and-the-military>.

¹³ Casey Gannon, Jennifer Hansler, and Rashard Rose, “US Airman Dies after Setting Himself on Fire Outside Israeli Embassy in Washington,” *CNN*, February 26, 2024, <https://www.cnn.com/2024/02/25/politics/man-sets-himself-on-fire-israeli-embassy-washington-dc/index.html>.