RSIS COMMENTARY

21 July 2026

Understanding Malign Influence in Video Gaming

Tan E-Reng

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSiS 30

RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 156 – 21 July 2026

Understanding Malign Influence in Video Gaming

By Tan E-Reng

SYNOPSIS

Video games are increasingly recognised as potential vectors for malign influence, but understanding these risks requires looking beyond individual games to the wider ecosystem of platforms, services, and communities that surround them. A broader ecosystem perspective can help policymakers and researchers identify how platform features, communication channels, and moderation practices may create opportunities for harmful activity.

COMMENTARY

A Canadian youth was charged in June 2026 with using Roblox – a popular online game platform that allows users to create and share virtual experiences – to simulate school shootings. In March 2026, the Philippine National Police urged parents to supervise their children's online activities more closely, following a finding that malicious foreign actors were allegedly using in-game communication features to expose minors to extremist ideologies. Closer to home, in January 2026, a 14-year-old Singaporean was issued a restriction order under the Internal Security Act for recreating terrorist attacks on Roblox and Gorebox.

These cases suggest that although gaming-related threats are relatively rare, they are an emerging risk. This is especially true in countries such as Singapore, where video game market penetration is extremely high.

According to research by the European Commission, the NYU Stern Center for Business and Human Rights, and the Swedish Psychological Defence Agency, gamers are universally vulnerable to malign influence activities that can occur both within games and across game-adjacent platforms within the wider video gaming ecosystem. Such activities may include terrorist recruitment, the spread of harmful or hateful ideologies, and sexual exploitation.

Discussions this author had at a December 2025 workshop organised by the United Nations Interregional Crime and Justice Institute (UNICRI) and the Singapore Ministry of Home Affairs covered similar ground, examining how in-game mechanics in games and virtual worlds such as those in Roblox could be exploited to project malicious influence.

Understanding the scale of this risk requires the right analytical tools. However, the existing literature does not appear to offer a unified framework for understanding the mechanics of video games and game-adjacent platforms or for explaining how their specific affordances can enable or exacerbate such harms.

What can be done to bolster the toolkit of analysts studying the potential harms and risks associated with gaming?

Gaming as an Ecosystem

Steps could be taken to provide analysts with a simple yet effective framework for understanding video games and the risks they pose.

This starts with recognising that gaming is an ecosystem. It is important to recognise that the average player's experience includes not only playing the games themselves but also using a network of other services (i.e., game-adjacent platforms) that enhance their overall experience. The games are not the only vector that malicious actors can exploit – chat systems, modifications, forums, private group chats, and other platform-adjacent spaces can all be used to spread misinformation and other online harms.

The following diagramme is a simple illustration of the gaming ecosystem that can help analysts narrow down areas to focus on when a potential risk arises.

In this diagramme, "Video Games" refers to the games themselves. "Immediate Infrastructure" refers to software that directly facilitates the purchasing, organisation, and operation of games for players and provides immediate functionality for player-to-player or player-to-community interaction and communication. Examples include Steam and the Epic Games store. "Peripheral Infrastructure" refers to third-party

software that players use to augment their gaming experience. Examples include messaging applications such as Discord and forum spaces such as Reddit (via gaming-related subreddits).

Understanding the Risk Dimensions

The next step is to understand the risk dimensions when assessing these components of the video game ecosystem and the potential hazards they pose. While video games and their related infrastructure may be complex in their mechanics and operations, a useful way to break down their risk areas is via the following axes: 1) content, 2) communication, and 3) moderation.

Content

Content refers to the material that exists within a game or platform. In the case of games, this could include settings, storylines, overall themes, and imagery used. It also refers to game mechanics – actions that players are allowed to perform within the virtual environment of the game. In the case of immediate and peripheral infrastructure, this could include the types of games that may be hosted and sold on a platform, as well as the types of user-generated content permitted.

Content becomes a concern when it includes questionable, inflammatory, obscene, or hate-mongering elements. This can take the form of hateful symbols and imagery (e.g., swastikas, racist symbols) that can proliferate within games and platforms, particularly on those platforms that permit user-generated assets to be uploaded, displayed, and/or shared. Reports of user-built "concentration camp" structures observed within the game *Minecraft* are an example of such concerns. The terrorist attack simulations recreated by the aforementioned 14-year-old in Roblox are another example.

Communication

Communication refers to the affordances in video games that allow users to interact with one another, often in real time. This could take the form of text-based instant messaging features, voice and/or video chat functionality, and any other means for

users to convey, display, and/or transmit auditory and visual information to one another within the video game itself or on the peripheral infrastructure.

Where direct messaging and communication are permitted, there is a risk of malicious actors using these features to transmit, propagate, and circulate problematic and harmful messages and ideology to other users. In-game chat channels, Discord, and other third-party apps are vectors which malign actors have reportedly exploited to gain access to players, particularly minors.

Moderation

Moderation refers to the mechanisms implemented within a game or service that facilitate the monitoring and reporting of offensive or harmful content.

Where moderation becomes a concern is when a game or platform's moderation policy proves inadequate to manage and curtail the upload and spread of harmful content. Many platforms rely on reactive, community-led informal moderation, which may place a disproportionate onus on parties who might not be suited for moderation roles (e.g., developers, publishers, and users with no experience or interest in moderation).

For example, Steam relies heavily on a community moderation model whose success or failure is structurally dependent on the efforts (or lack thereof) of its community moderators. NexusMods, a popular third-party game modification distribution website, uses a reactive, reporting-based model that places the onus of reporting harmful content on users. Inadequate moderation policies might enable harmful content to emerge and spread unabated.

Implications and Conclusions

Having a unified understanding of how the video game ecosystem works, at its top level and at the more granular level, can help investigators pinpoint specific gaming features and communication tools that may be exploited for harmful activity.

It would also allow teams with different disciplines and expertise levels to operate with a unified understanding when conducting investigations and studies into game-related harms. This is particularly useful for investigators who are not familiar with gaming concepts and cannot readily interview or survey people who are.

This commentary presents a first step towards developing a more unified and streamlined approach to assessing the potential harms arising from the video game ecosystem. This framework should be refined and developed in parallel with the ever-changing gaming industry and the analysts operating within it.

Tan E-Reng is a Research Analyst at the Centre of Excellence for National Security (CENS), at S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. His current research interests encompass the diverse domains of cyber, online harms, disinformation and misinformation, and emerging technologies.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798

Please share this publication with your friends. They can subscribe to RSIS publications by scanning the QR Code below.