



Cybercrime e videogiochi: L'utilizzo di Discord e videogiochi per commettere Cyber-crimini

MATTEO CURCIO*

Come citare / How to cite

Curcio, M. (2025). Cybercrime e videogiochi: L'utilizzo di Discord e videogiochi per commettere Cyber-crimini. *Culture e Studi del Sociale*, 10(1), p-p.60-87

Disponibile / Retrieved <http://www.cussoc.it/index.php/journal/issue/archive>

1. Affiliazione Autore / Authors' information

* Scuola superiore ad ordinamento speciale della difesa (SSOSD), Centro Alti Studi Difesa, Roma, Italia

2. Contatti / Authors' contact

* curmat89@gmail.com

Articolo pubblicato online / Article first published online: Giugno/June 2025



- Peer Reviewed Journal

INDEXED IN
DOAJ

*Cybercrime e videogiochi:
L'utilizzo di Discord e videogiochi per commettere
Cyber-crimini*

Matteo Curcio

Scuola superiore ad ordinamento speciale della difesa (SSOSD), Centro Alti Studi
Difesa, Piazza della Rovere 83, Roma, Italia

curmat89@gmail.com

Abstract

Il mondo del gaming viene spesso presentato come una distrazione innocua, che suggerisce un luogo sicuro dove gli utenti giocano e trascorrono il proprio tempo. Come risultato di questa narrazione, il potenziale comunicativo di questo ambiente deve ancora essere esplorato ampiamente. Discord, un'applicazione creata per il gaming e molto utilizzata dalle comunità di giocatori per facilitare le comunicazioni, è un eccellente vettore per connettere utenti di tutto il mondo. Questo articolo sostiene che Discord, oltre ai suoi usi di intrattenimento, può essere sfruttato per commettere crimini e perpetrare attività illegali. Per illustrare ciò, è stato utilizzato un approccio netnografico per rilevare e analizzare le interazioni sociali all'interno di Discord. I risultati di questa ricerca illustrano come Discord può essere sfruttato in vari modi per commettere un'ampia gamma di crimini in modo sicuro, senza essere scoperti, e come la netnografia si sia rivelata uno strumento efficace per individuarli.

Abstract

The gaming environment is often presented as a harmless distraction, which suggests a safe place where users play and spend their time. As a result of this narrative, the communication potential of this environment has yet to be explored extensively. Discord, an application created for gaming and widely used by the gaming community to facilitate communications, is an excellent vector for connecting users worldwide. This paper argues that Discord, in addition to its entertainment uses, can be exploited to commit crimes and perpetrate illegal activities. To illustrate this, a netnography approach has been employed to detect and analyze social interactions within Discord. According to the findings of this research, Discord can be exploited in various ways to commit a wide range of crimes safely and undetected, and netnography has proved to be an efficient tool for detecting crimes.

Keywords: Discord, Crime, Videogiochi

Introduzione

L'industria del gaming è in continua crescita, e nel 2024 si prevede che raggiungerà i 3,32 miliardi di giocatori in tutto il mondo (Howarth, 2024), ampliando, quindi, il numero di utenti che comunicano quotidianamente attraverso i canali comunicativi forniti da questo ambiente. Discord, fondata nel 2015, è un'applicazione creata per il gaming, che semplifica le comunicazioni vocali e di messaggistica per scopi ludici. Nel corso degli anni questa applicazione ha visto un notevole aumento in termini di entrate e utenti. Nel 2022 la stima segna un totale di 175 milioni di utenti attivi mensili e 19 milioni di server attivi (Curry, 2024). Discord è un'applicazione di facile utilizzo che può essere installata sia su PC che su telefoni, ha una dimensione di pochi Megabyte, è accessibile creando un account e offre diverse funzionalità come illustrato nella tabella 1.

Tabella 1 Funzionalità di Discord

Chat: gli utenti possono chattare con altri utenti tramite messaggi scritti. Invia file: gli utenti possono inviare documenti diretti, immagini o altro per una dimensione totale di 25 MB o 100 MB per la versione Nitro. Condividere file: come altre app di messaggistica, gli utenti possono anche condividere file o collegamenti più grandi con altri. Chiamata: gli utenti possono chiamarsi tra loro senza limiti di tempo. Videochiamata: gli utenti possono videochiamarsi tra loro senza limiti di tempo. Crea un server: gli utenti possono creare un server privato e invitare altri utenti. Unisciti ad altri server: gli utenti possono unirsi a diversi server dedicati a un argomento specifico. Contenuto in streaming/condivisione: gli utenti possono eseguire lo streaming o condividere qualsiasi contenuto live con altri utenti.
--

Gli utenti che accedono a Discord devono creare un account con un'e-mail, accettare i Termini di servizio e utilizzare la propria identità online per spostarsi nella piattaforma. Come tutti i fornitori del settore dei giochi, i Termini di servizio di Discord vietano l'uso della piattaforma per contenuti illegali e cercano di proteggere gli utenti con un certo monitoraggio. I messaggi Discord, ad esempio, vengono

archiviati in un ampio database denominato Cassandra e rimangono a disposizione degli amministratori finché gli utenti non li eliminano; una volta cancellato non è possibile recuperarli. Purtroppo, nonostante gli sforzi dell'azienda per prevenire comportamenti illegali, è estremamente facile sfruttare questa applicazione per commettere diversi reati.

Metodologia

In un mondo complesso e interconnesso come quello odierno, dove la maggior parte delle comunicazioni avviene in contesti virtuali come blog, chat, app di messaggistica e social media, e le comunicazioni mediate dal computer (CMC) rappresentano l'interazione primaria di condivisione di sentimenti ed emozioni (Riffe et al., 2006), è necessario adattare i metodi di ricerca classici al contesto attuale. La ricerca sui videogiochi è ancora lontana dall'aver trovato una metodologia di ricerca unica e funzionale: "Il lavoro condotto nella ricerca sui videogiochi ha sia aspetti cumulativi che trasformativi. Inoltre, è caratterizzato da una multidisciplinarietà e da un'interdisciplinarietà piuttosto eccezionali, che affondano le loro radici da un lato nella complessità e diversità dei suoi argomenti di ricerca, dall'altro nel fatto che la moderna ricerca sui giochi digitali è un fenomeno piuttosto giovane" (Lankoski & Bjork, 2015). La metodologia scelta per questo studio è stata la netnografia: una metodologia recentemente emergente nella ricerca sociale che adatta gli strumenti etnografici e li applica in un contesto digitale. Fondata da Kozinets nel 1995, questa metodologia è stata rivisitata e applicata in molti contesti di ricerca. All'inizio, la netnografia serviva come strumento di ricerca per analizzare i bisogni degli utenti online (Kozinets, 1997, 1998, 1999; Bickart & Schindler, 2001; Catterall & Maclaran, 2002) ma con lo sviluppo di nuove tecnologie, attraverso l'analisi netnografica, i ricercatori possono acquisire nuove prospettive sui servizi tradizionali o esplorare nuovi tipi di servizi digitali (ad esempio, streaming online di intrattenimento, spazio di archiviazione online o giochi online) (Heinonen & Medberg, 2018). L'applicazione di diversi approcci netnografici è stata osservata nel corso degli anni in diversi campi: giornalismo digitale (Aitamurto, 2013), salute (Mudry & Strong, 2013), sport (Gilchrist & Ravenscroft, 2011), geografia (Grabher & Ibert, 2014), videogiochi (Silva et al., 2021; Au & Ho, 2021; Hernandez & Handan, 2014). Questa serie di pubblicazioni dimostra che la netnografia, come approccio metodologico di ricerca, ha un'ampia portata in molte nazioni, lingue e campi (Costello et al., 2017). Di conseguenza, la netnografia non si concentra su un unico approccio ma si adatta invece ai fenomeni studiati. Poiché lo studio mira a illustrare come Discord può essere utilizzata per commettere crimini, è stata adottata l'osservazione diretta e un approccio non partecipativo. Nel dettaglio, sono stati trascorsi tre anni all'interno di comunità virtuali osservando, raccogliendo e classificando i dati seguendo le fasi della netnografia, descritte in Figura 1.



Figura 1 Fasi della Netnografia

Per rispondere alla domanda di ricerca: Discord può essere utilizzato per commettere crimini? il ricercatore deve identificare e selezionare la comunità. Per fare ciò, non è stato possibile randomizzare il soggetto dello studio; ogni comunità di gioco è diversa e possiede caratteristiche uniche. Ad esempio, i giocatori di Fortnite sono relativamente giovani, quindi inclini o vettore di crimini specifici, diversi dalla community di Call of Duty, che è più anziana e con conoscenze diverse. Pertanto, è necessaria una conoscenza preliminare dell'ambiente di gioco per individuare la community più adatta allo studio. In questo caso, per lasciare spazio alla riproduzione ad altri ricercatori, sono stati scelti come soggetti di ricerca dei server pubblici Discord casuali (accessibili a tutti) di alcuni dei videogiochi più famosi. Di conseguenza, la comunità selezionata era la popolazione che partecipa a quello specifico server Discord. Il passo successivo è il coinvolgimento, l'immersione e la raccolta dei dati. È qui che il ricercatore si impegna con la comunità e può farlo in due modi, con partecipazione attiva; pertanto, il ricercatore deve informare gli utenti della sua presenza o non partecipazione. Per questo studio è stato adottato un impegno non partecipativo, poiché quello partecipativo probabilmente non avrebbe prodotto risultati. La fase della raccolta dati è il momento in cui il ricercatore raccoglie i dati; in questo caso sono state prese conversazioni e screenshot come prova del comportamento. Esistono diversi modi per raccogliere dati, ma gli screenshot e le trascrizioni delle chat vocali sono il modo più efficiente nell'ambiente di gioco. Questa fase è anche quella più impegnativa e dispendiosa in termini di tempo, poiché non tutti utilizzano l'ambiente di gioco per commettere crimini e, ovviamente, non viene fatto in bella vista; pertanto, è possibile trascorrere molte ore osservando senza risultati. Dopo che il ricercatore ha raccolto i materiali, è necessario analizzarli, trarre possibili conclusioni e schemi e sollevare alcune nuove domande di ricerca, grazie al processo iterativo. In aggiunta, è stata condotta un'analisi ermeneutica di immagini e conversazioni portando anche qualche caso studio, per evidenziare come questo ambiente potrebbe essere utilizzato per commettere crimini a causa della facilità delle comunicazioni non monitorate. Nell'ultima fase vengono presentati i risultati, che a seconda del ricercatore possono

avvenire in modi diversi. Data la natura dell'argomento, il ricercatore ha rispettato pienamente le norme relative al possesso e alla divulgazione del materiale, andando a censurare e/o modificare possibili informazioni sensibili.

Pedofilia

Le applicazioni per il gaming e i videogiochi online sono un ambiente in continua espansione che coinvolge milioni di giocatori in tutto il mondo, testimoniando una massiccia espansione degli utenti durante la pandemia (King et al., 2020; Guo et al., 2022). Di conseguenza emergono anche delle sfide, tra cui la possibile presenza di pedofili che cercano di sfruttarli per prendere di mira i minori. I giochi online coinvolgono comunità virtuali di giocatori che interagiscono in tempo reale con l'ausilio di diverse applicazioni e questo ambiente può attirare l'attenzione dei pedofili, che cercano di stabilire un contatto con i minori attraverso chat, messaggi diretti o altre forme di comunicazione. Poiché molte piattaforme di gioco consentono un certo grado di anonimato, i pedofili possono atteggiarsi a pari per costruire relazioni con i giovani giocatori. Negli ultimi tempi si è assistito ad un aumento esponenziale di articoli in tutto il mondo riguardanti la pedofilia legata al gaming, dimostrando così che non si tratta di un evento "occasionale" ma di un'attività frequente:

"I videogiochi e le chat online sono 'terreni di caccia' per predatori sessuali, i criminali stanno creando connessioni virtuali con i bambini attraverso piattaforme di gioco e di social media. Un sito popolare avverte i visitatori:" Si prega di fare attenzione." (Bowles & Keller, 2019)

"Gli investigatori sui crimini sessuali su minori della Pennsylvania affermano di essere stati sopraffatti dalle informazioni dall'inizio della pandemia di COVID-19. La task force della contea di Delaware per i crimini sessuali su Internet ha affermato che con più bambini a casa e online, i predatori lo stanno usando a proprio vantaggio. Gli investigatori hanno detto che un uomo del posto stava prendendo di mira dei bambini che giocavano ai videogiochi in streaming. La madre della vittima ha filmato l'incidente. La madre, che non voleva essere identificata, ha incontrato suo figlio mentre giocava ai videogiochi e ha iniziato a spogliarsi. (Pradelli & Mettendorf, 2020)

"I pedofili e le persone cattive trovano un modo per aggirare le cose, tendendo una trappola per i tuoi figli proprio nel tuo salotto", ha spiegato Brian Heins, padre di un giocatore. "Con alcuni giochi, non devi dimostrare quanti anni hai. Basta fare clic su una casella e dire che hai più di 18 anni." (Marrone, 2020)

"Ho arrestato personalmente dei predatori di Internet di oltre 30 anni e ho scoperto che avevano più account Roblox con lo scopo specifico di chattare con bambini di età inferiore ai 10 anni. La funzione di chat può essere disattivata ma raramente viene eseguita poiché i genitori non lo fanno." Non mi rendo conto di quanti predatori di Internet stanno effettivamente dando la caccia ai loro figli in un dato momento." (Jenson, 2023)

Dato il numero di utenti che popolano queste applicazioni, trovare le vittime è facile e i predatori sanno come farlo. Ciò che avviene è essenzialmente un'incitamento attraverso tecniche di ingegneria sociale, che sfruttano le dimensioni interne di queste applicazioni.

Le modalità con cui possono abusare di queste piattaforme per aggredire i minori sono tre:

- Adescamento con uno scambio di denaro/oggetti all'interno del gioco o di servizi (come il power leveling).
- Adescamento mascherando l'identità (fingendo informazioni sull'età, sul sesso, ecc.)
- Ricatto o estorsione

Spesso i pedofili sono essi stessi giocatori, creatori di contenuti o conoscono queste piattaforme attraverso i loro figli. Inoltre, non è raro vedere personaggi famosi arrestati per questi crimini, come rivela un recente caso in Italia e Polonia:

Rimini, abusi su tredicenne: arrestato YouTuber con un milione di follower (Tgcom24, 2023)

"La comunità online polacca è scossa dalle accuse di pedofilia. Gli accusati avrebbero usato la loro fama per abusare sessualmente di giovani ragazze, alcune di età compresa tra i 12 e i 14 anni. Le avrebbero invitate in hotel, le avrebbero intossicate con l'alcol e avrebbero approfittato dei loro disabili." stato. Le rivelazioni scioccanti hanno lasciato scosso il mondo internet polacco, in particolare la comunità di YouTube." (Amokeoja, 2023)

All'interno di Discord, tutti possono muoversi liberamente, chattare e socializzare con altri giocatori. Pertanto, non ci sono limiti alle conversazioni che gli utenti potrebbero avere. È vero che alcuni sistemi cercano di prevenire comportamenti inappropriati, soprattutto nei confronti dei minori, ma non bastano e sono inadeguati (Curcio, 2023).

Vista la natura dell'argomento, la ricerca si è limitata ad indagare l'eventuale presenza di pedofili senza andare oltre, in quanto la normativa attuale impedisce a chiunque di entrare in contatto con tale materiale. Di conseguenza verrà visualizzata solo una parte del materiale trovato. Nelle Figure 2 e 3, alcune chat recuperate dai server Discord relative al gaming evidenziano la presenza di diversi predatori.

*Cybercrime e videogiochi:
L'utilizzo di Discord e videogiochi per commettere Cyber-crimini*



Figura 2 Chat recuperate da Discord

Figura 3 Chat recuperate da Discord

Sfide, istigazioni al suicidio e pianificazione omicidi

Il fenomeno delle sfide e delle istigazioni al suicidio è diventato virale negli ultimi anni, causando numerosi decessi tra gli adolescenti (Henderson, 2023; Levenson & Rubin, 2022). Quando i media riportano un caso di suicidio o di morte, citano i social media come veicolo principale di queste sfide, dimenticando l'intero ambiente di gioco. È vero che queste sfide si realizzano attraverso i social media, ma anche nelle applicazioni correlate ai videogiochi. Quando non esistevano i mondi virtuali, le persone dovevano utilizzare i social media per incontrare o parlare con altri in tutto il mondo, creando una relazione diversa tra gli utenti, come ad esempio sui Social media dove è necessario richiedere l'amicizia o proseguire per chattare. Questo passaggio, nell'ambiente di gioco viene superato perché gli utenti possono interagire direttamente senza barriere. Se una volta era difficile sapere come si comportavano i propri coetanei all'estero perché il sistema di comunicazione rendeva difficile saperlo, ora attraverso queste applicazioni si può interagire con coetanei di altri paesi che possono suggerire di raccogliere una "challenge" non ancora conosciuta. Tra le sfide più famose c'è il gioco "knockout game", praticato ancora oggi, con recenti avvenimenti accaduti in tutto il mondo (Garau, 2023; Moore, 2022), e la blu whale, tornata di recente alla cronaca (Greyman-Kennard, 2023). Oltre a quelle più famose, esiste anche il fenomeno Jonathan Galindo, in cui il personaggio istiga le vittime al suicidio; la sfida Benadryl, che prende il nome dal farmaco a base di Difenidramina (un antistaminico), in cui i partecipanti devono assumere più compresse contemporaneamente per scatenare reazioni allucinogene. E poi, c'è la sfida Momo, simile alla blu whale, dove l'avatar è rappresentato da una donna dai lunghi capelli neri e lo scopo finale è il suicidio. La sfida Kiki, in cui le persone devono saltare fuori da un veicolo in movimento e ballare al ritmo della canzone "In My Feelings", mettendo in pericolo sia la propria vita che quella degli altri. La Fire Challenge, che consiste nel dare fuoco a una persona e vedere quanto resiste, e la sfida dello svenimento, in cui le persone cercano volontariamente di togliergli ossigeno per provocare allucinazioni e svenimenti. Per dimostrare che i videogiochi e le relative applicazioni sono anche un ottimo strumento per diffondere le sfide, la ricerca ha indagato la comunità di alcuni server Discord e mondi virtuali, e i risultati sono visibili nelle Figure 4 e 5.

*Cybercrime e videogiochi:
L'utilizzo di Discord e videogiochi per commettere Cyber-crimini*

Jonathan Galindo#5726 Jonathan Galindo#4991 jonathan galindo#2611 Jonathan Galindo#5426 Jonathan Galindo#2850 Jonathan Galindo/JGC Co-Owner Jonathan Galindos#9208 Jonathan Galindo #6242 Jonathan Galindo#6242 Jonathan Galindo#6556 Jonathan galindo#9593 Jonathan Galindo#6005 Jonathan Galindo#8363	galindo#0784 Jonathan Galindo#0560 Jonathan Galindo#0958 blue whale#3423 Johnathon Galindio#508 jonathan galindo#3526 Jonathan Galindo#4879 Jonathan Galindo#6836 Jonathan Galindo#9387 jonathan galindo#3198	Jonathan Galindo#1287 Jonathan Galindo#8742 Jonathan Galindo#1563 Jonathan Galindo#8974 Jonathan Galindo#5689 Jonathan Galindo#4765 Jonathan Galindo#9043 Jonathan Galindo#8453 Jonathan Galindo#2121 Jonathan Galindo#3945
jonathan galindo#3698 Jonathan Galindo#0958 Jonathan Galindo#6005 Jonathan Galindo#5492 jonathan galindo#6851 jonathan galindo#0235 jonathan galindo#4562 Jonathan Galindo#9593 Jonathan Galindo#8363	Jonathan Galindo#2398 Jonathan Galindo#9424 Jonathan Galindo#4897 Jonathan Galindo#2983 jonathan galindo#0784 Jonathan Galindo#9842 Jonathan Galindo#3781	Jonathan Galindo#8963 Jonathan Galindo#6571 Jonathan Galindo#1782 Jonathan Galindo#3903 Jonathan Galindo#0348 Jonathan Galindo#5163 Jonathan Galindo#2312 Jonathan Galindo#1789 Jonathan Galindo#4560 Jonathan Galindo#3453

Figura 4 Utenti che impersonano Galindo su Discord

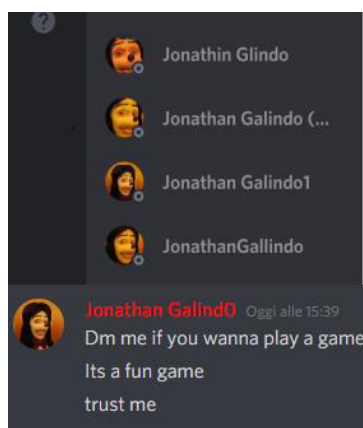


Figura 5 Utenti che impersonano Galindo su Discord

Purtroppo, oltre alle sfide più conosciute, esistono anche sfide meno conosciute perpetrate in gruppi chiusi. Un esempio su tutti è quello del Reiko Trap Harem. Nata nel 2018 dall'idea di un utente chiamato Reiko, questa sfida prevede l'assunzione di ormoni per somigliare il più possibile ad una trappola. Oltre a questa sfida, ce ne sono diverse in cui si prevedono ferite sul corpo, uso di droghe e tentativi di suicidio. Le figure 6, 7 e 8 illustrano parte del materiale recuperato durante la ricerca.

Matteo Curcio

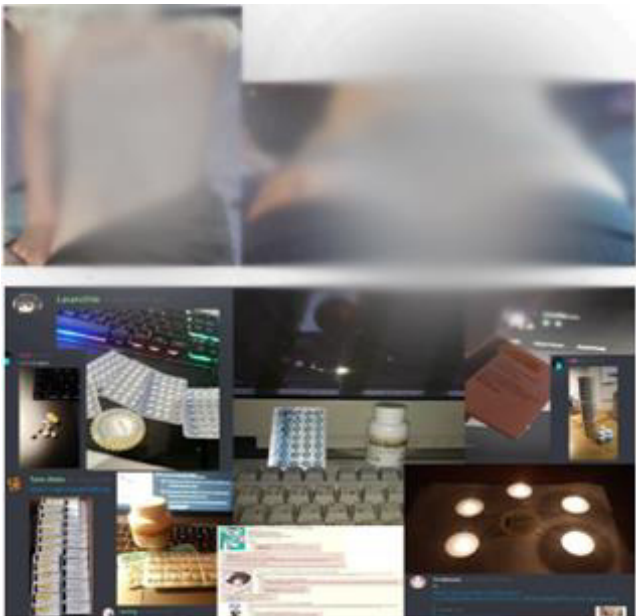


Figura 6 Utenti che partecipano alla challenge

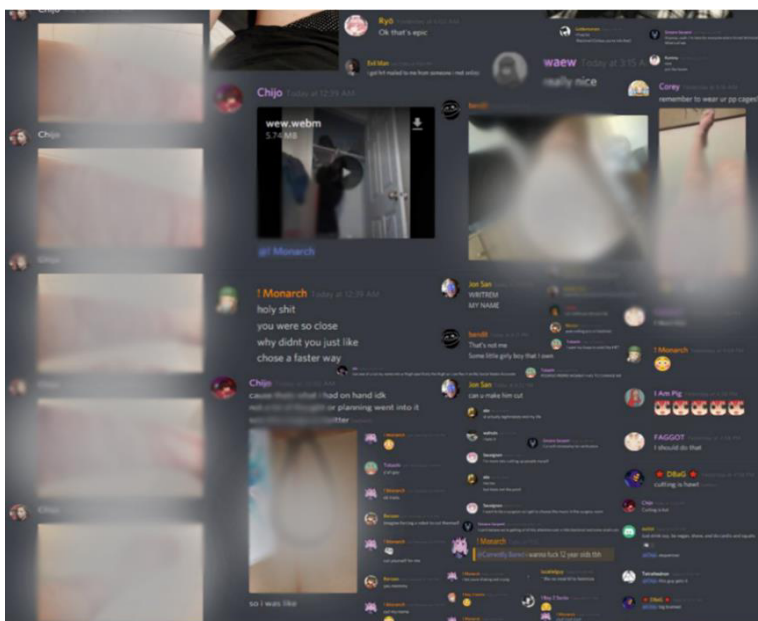


Figura 7 Utenti che partecipano alla challenge

*Cybercrime e videogiochi:
L'utilizzo di Discord e videogiochi per commettere Cyber-crimini*

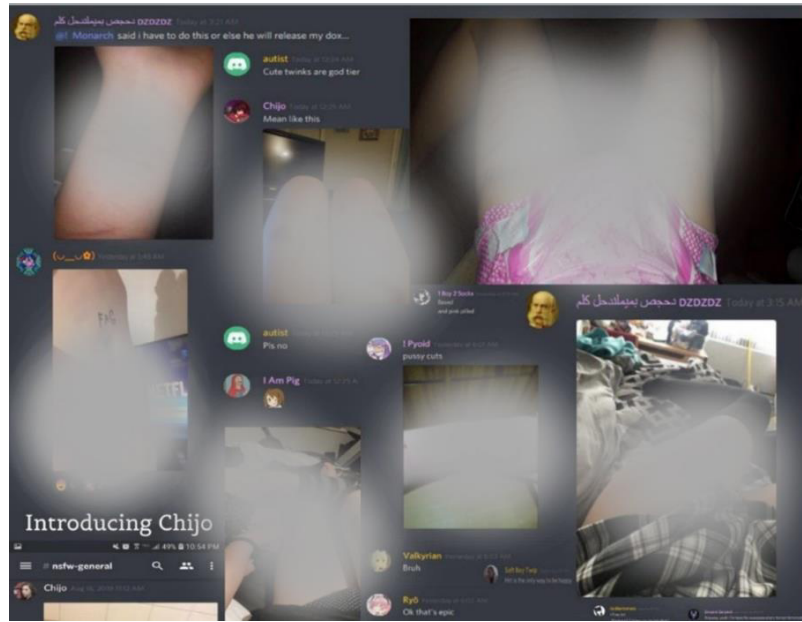


Figura 8 Utenti che partecipano alla challenge

Infine, la ricerca ha scoperto anche alcune chat in cui gli utenti discutevano dell'intenzione di uccidere qualcuno e/o di pianificare una sparatoria a scuola, come illustrato nella Figura 9.

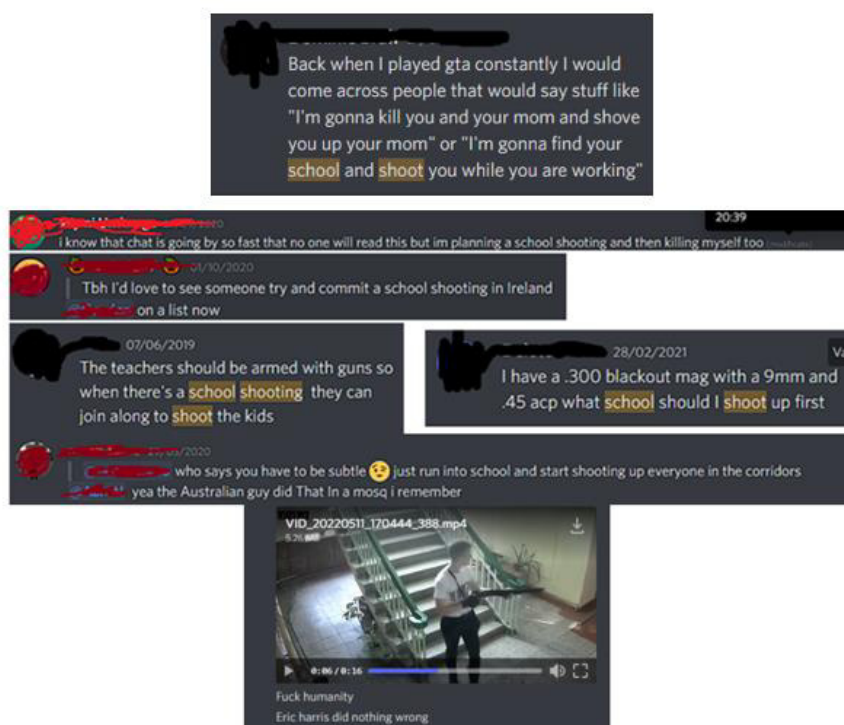


Figura 9 Utenti che pianificano uccisioni

Traffico di droga e armi

L'aumento globale dell'utilizzo delle piattaforme di social media per il traffico illecito di droghe è un fenomeno in espansione. Questa tendenza è alimentata dalla natura dinamica e diversificata del moderno ambiente dei social media (Demant et al., 2019; Moyle et al., 2019; Oksanen et al., 2021). I mercati dei farmaci sui social media condividono una funzionalità di base standard su varie piattaforme. Fungono principalmente da intermediari, collegando gli acquirenti con i venditori e semplificando il coordinamento delle transazioni. Allo stesso modo, i videogiochi e le loro applicazioni vengono utilizzati anche come canale di comunicazione per facilitare le vendite. Un esempio del materiale ritrovato è visibile nella Figura 10.

*Cybercrime e videogiochi:
L'utilizzo di Discord e videogiochi per commettere Cyber-crimini*

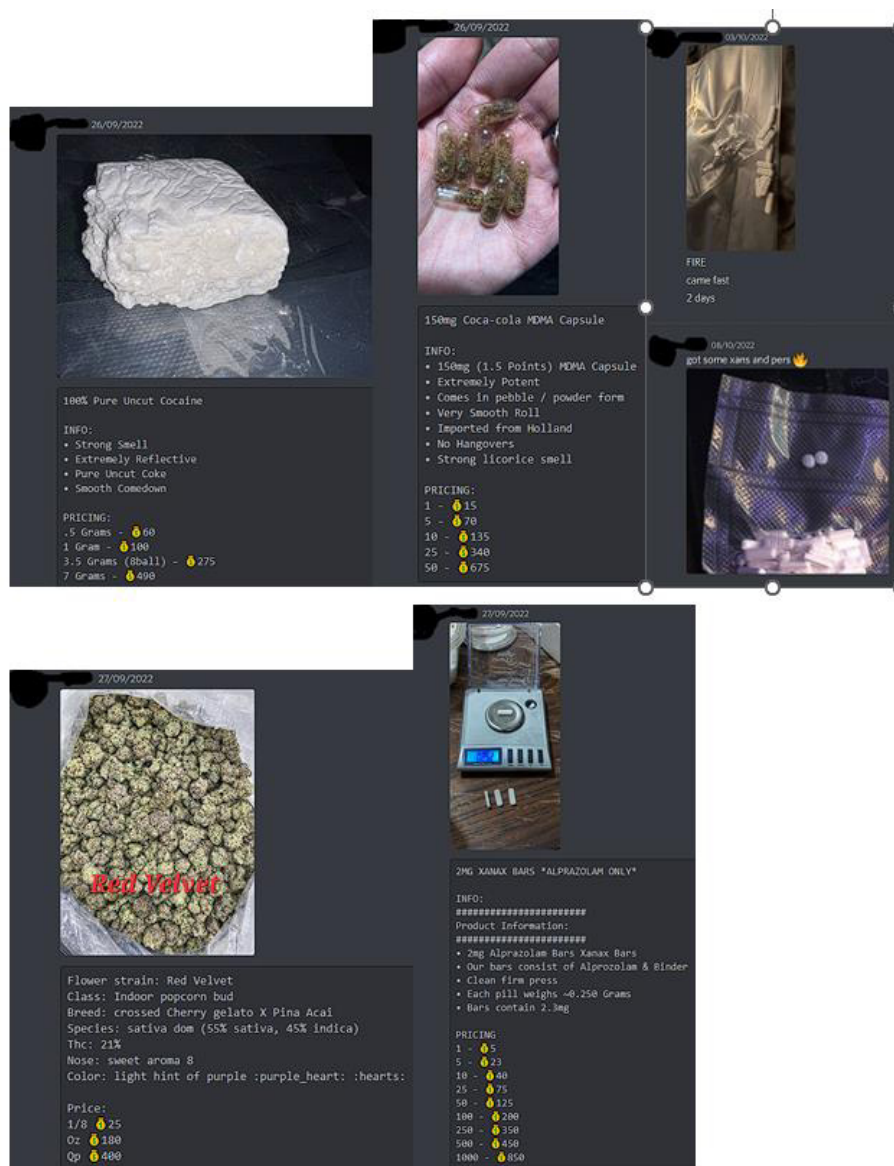


Figura 10 Utenti che vendono droga su Discord

La maggior parte di queste vendite avviene su Discord perché gli utenti sono interessati alla qualità dei beni venduti, che possono essere mostrati solo su applicazioni correlate e non all'interno dei videogiochi stessi. In questo caso, i videogiochi fungono da amplificatore perché i venditori utilizzano le loro funzioni (chat, audio, messaggi privati, ecc.) per offrire i loro prodotti a un pubblico più ampio. Della vendita di droga su questi server si parla in un recente articolo (Van Der Sanden et al., 2022), che evidenzia un caso particolare avvenuto in Nuova Zelanda, in una comunità locale, dove gli utenti utilizzavano queste piattaforme per agevolare il traffico di droga. Oltre ai vari canali di vendita di droga, è stato possibile

osservare anche server in cui gli utenti erano intenti a vendere armi. Questi server hanno una vocazione internazionale, si parla inglese e gli utenti provengono da tutto il mondo, ma il paese più colpito o quello in cui è stato riscontrato il maggior numero di utenti sono stati gli Stati Uniti. Questi luoghi funzionano come un mercato, in cui gli utenti pubblicano immagini delle loro armi e poi si spostano su canali privati per completare gli acquisti. Trovarli non è facile perché spesso sono camuffati sotto falsi nomi, ed è ancora più impensabile poterli scovare senza un legame con il gaming. Molti di questi server sono stati realizzati “sponsorizzando” un videogioco, contenendo al loro interno stanze e canali dedicati a questo tipo di attività. Nelle Figure 11 e 12 sono illustrati alcuni esempi.

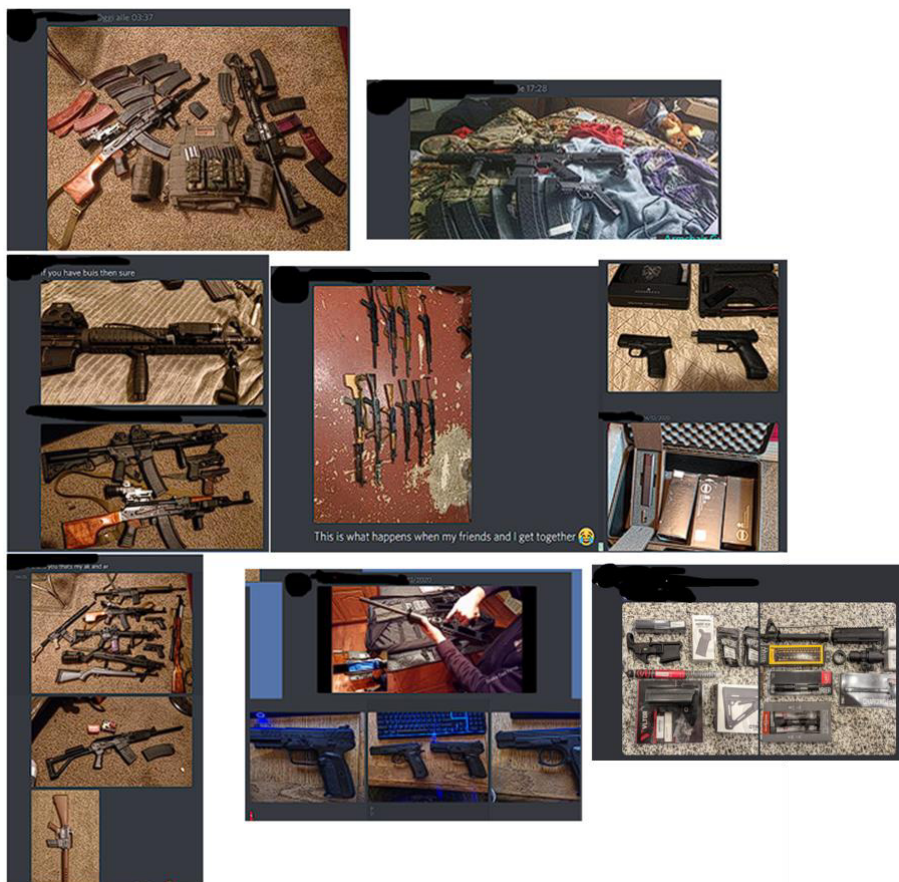


Figura 11 Utenti che mostrano/vendono armi su Discord

*Cybercrime e videogiochi:
L'utilizzo di Discord e videogiochi per commettere Cyber-crimini*

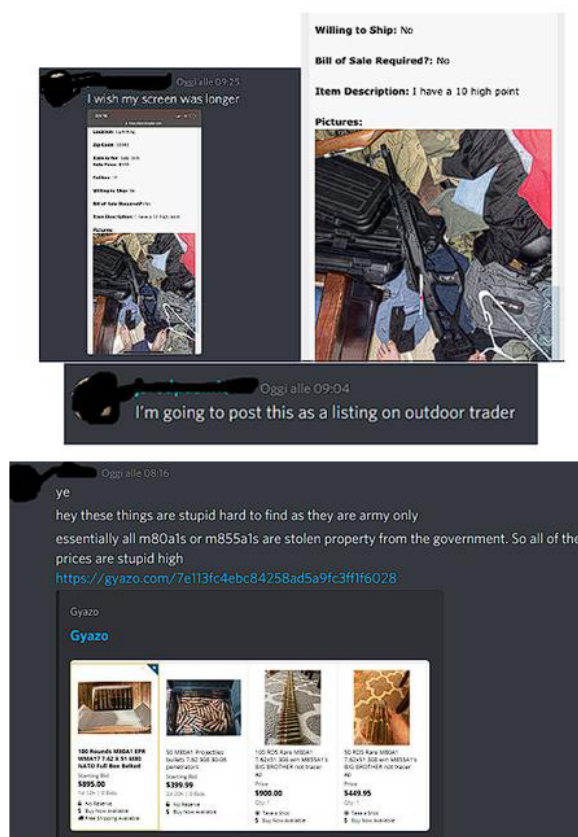


Figura 12 Utenti che mostrano/vendono armi su Discord

Generalmente, gli scambi avvengono localmente tra utenti nelle stesse città mentre raramente avvengono a livello internazionale tramite corrieri privati.

Terrorismo e estremismo di estrema destra

Dopo gli attentati dell'11 settembre 2001, i servizi segreti di tutto il mondo hanno alzato le soglie di allerta e di sorveglianza nell'ambiente digitale. Dal 2008 l'intelligence americana ha iniziato a indagare anche il mondo dei videogiochi, considerandoli un importante veicolo di comunicazione per i terroristi. Un rapporto segreto COMINT redatto per FVEY dal GCHQ è stato trovato tra i documenti rilasciati da Edward Snowden. Questo documento contiene cinque capitoli, ovvero cinque documenti che discutono il potenziale uso improprio di GVE (Giochi e ambienti virtuali) e l'opportunità per le agenzie di intelligence di operare in quel cyberspazio.

"Sappiamo che i terroristi utilizzano molti mezzi di comunicazione ricchi di funzionalità per scopi operativi come e-mail, VoIP, chat, proxy e forum web ed è molto probabile che faranno ampio uso delle numerose funzionalità di

comunicazione offerte da Giochi e ambienti virtuali (GVE) entro il 2010. Con poche eccezioni, la NSA non è nemmeno in grado di riconoscere il traffico, e quindi è impossibile anche solo dire quale percentuale dell'ambiente sia GVE; per non parlare di determinare come gli obiettivi utilizzano le funzionalità di comunicazione dei GVE. Tuttavia, i GVE offrono uno spazio di opportunità SIGINT/HUMINT e sono necessarie ulteriori ricerche per capire uno sfruttamento efficace. Terroristi di Al Qaida sono stati trovati associati a XboxLive, Second Life, World of Warcraft e altri GVE nel traffico di rete PINWALE, nei database TAO e nei dati forensi. Altri obiettivi includono hacker cinesi, uno scienziato nucleare iraniano, Hezbollah e membri di Hamas. GCHQ sta compiendo uno sforzo vigoroso per sfruttare i GVE e ha prodotto moduli di sfruttamento in XboxLive! e World of Warcraft." (Documenti pubblicati da Edward Snowden, nd)

Nel 2011, uno studio canadese (Botnet Analysis Report) ha riportato quanto segue:

"Il terrorismo nel mondo virtuale facilita il terrorismo nel mondo reale: reclutamento, formazione, comunicazione, radicalizzazione, propagazione di contenuti tossici, raccolta di fondi e riciclaggio di denaro e operazioni di influenza. Il rapporto afferma che all'interno dei mondi virtuali, i terroristi hanno modificato i giochi per rendere le truppe alleate il default nemico in modo che potenziali terroristi possano essere reclutati e addestrati. Il rapporto canadese non si ferma qui, aggiungendo che questi giochi sono utilizzati per lo spionaggio sponsorizzato dallo stato. Le chat da giocatore a giocatore e la chat VOIP sono utilizzati per: comunicazioni segrete tra cellule, reti di agenti illegali o clan effimeri o gilde" in MMOG. Questi ambienti consentono ai giocatori di effettuare transazioni con denaro reale (RMT) in mondi virtuali e consentono lo scambio di valuta non regolamentato di crediti virtuali con fondi reali. Il "Gold farming" e il "Power Leveling" sono solo alcuni esempi di operazioni delle organizzazioni criminali che vengono utilizzate per sfruttare queste applicazioni." (Tempesta, 2011)

Sono passati molti anni da quei documenti, ma ancora oggi lo stato dell'arte dimostra che esiste una soluzione ottimale al problema, anzi, è diventato ancora più complesso, dato l'innumerabile numero di mondi virtuali oggi esistenti. Nel 2020, Gilles De Kerchove, capo della Sezione europea antiterrorismo, ha allertato i servizi di sicurezza a livello globale, affermando quanto segue:

"I videogiochi online possono essere utilizzati per propagare ideologie estremiste e persino preparare attacchi", ha detto all'AFP il coordinatore antiterrorismo dell'UE in un'intervista in cui ha sollecitato una maggiore regolamentazione. Ci sono gruppi di estrema destra in Germania che hanno escogitato giochi in cui l'obiettivo è sparare agli arabi, o [al miliardario ebreo americano di origine ungherese George] Soros, o alla signora [la cancelliera tedesca Angela] Merkel per la sua politica migratoria, ecc. " "Questo può essere un modo alternativo per diffondere l'ideologia, soprattutto dell'estrema destra ma non solo, un modo per riciclare denaro... ci sono valute create nei giochi che possono essere scambiate con monete aventi corso legale, ha detto. Può essere una forma di comunicazione. È crittografato. Può anche essere un modo per testare scenari di attacco, ha continuato." (Mondesert, 2020)

In letteratura è possibile trovare anche alcuni articoli interessanti che hanno trattato il legame tra mondi virtuali e propaganda terroristica. “In relazione ai videogiochi e al terrorismo, numerosi giochi affrontano direttamente questioni legate al terrorismo, soprattutto in relazione alla Guerra al terrorismo. Ad esempio, Splinter Cell è un gioco che ruota attorno agli eventi dell'11 settembre, mentre Counter-Strike consente alle squadre di fazioni opposte di assumere il ruolo di terroristi e antiterroristi. Similmente a Counter-Strike, altri giochi come America's Army, Modern Warfare 2 e Medal of Honor: Warfighter consentono ai giocatori di diventare terroristi, il che potrebbe avere alcuni benefici psicologici ed educativi. (Al-Rawi, 2018)

Successivamente si evidenzia come possano effettuare propaganda attraverso queste piattaforme grazie a particolari tecniche di comunicazione. Molte di queste organizzazioni, ad esempio, creano o copiano giochi precedenti, ottenendo una sorta di riformulazione concettuale anche a livello linguistico:

“Nel 2006, il gruppo Al-Qaeda ha apportato modifiche al gioco sparattutto in prima persona (FPS) Quest for Saddam (2003) e ha introdotto un altro gioco chiamato Quest for Bush. L'obiettivo del gioco originale era uccidere i soldati iracheni e catturare Saddam Hussein, mentre Al-Qaeda ha completamente invertito i ruoli dei giocatori. D'altra parte, i videogiochi degli Hezbollah libanesi e della società siriana Afkar Media sono stati utilizzati come mezzi di comunicazione alternativi per offrire ruoli interpretativi contrari alla rappresentazione occidentale tradizionale dei musulmani arabi. In questo modo, i videogiochi forniscono agli attori violenti non statali e alle organizzazioni a loro simpatiche un mezzo per presentare le loro lamentele e mostrare la loro abilità di combattimento in modi che promuovono gli obiettivi strategici delle organizzazioni. Alcuni di questi giochi alternativi includono Quraish e Under Siege, entrambi prodotti da Afkar Media. (Al-Rawi, 2018)

Esiste, quindi, un legame tra terrorismo e Mondi virtuali, che si crea con la duplice connotazione di amico-nemico. È comune trovare videogiochi prodotti da queste organizzazioni, che utilizzano la combinazione amico-nemico per sottolineare ed enfatizzare la differenziazione tra “noi che abbiamo ragione” e “loro, il nemico”. Un nemico spesso rappresentato dall'Occidente, che con i suoi usi e costumi soppianta le tradizioni altrui e distrugge altre terre. Questi Videogiochi vengono utilizzati come strumento di marketing da queste organizzazioni, incluso l'ISIS, che, grazie alle sue abili capacità comunicative, è riuscito a reclutare migliaia di membri in Occidente. Pertanto, queste piattaforme rappresentano un mezzo ideale per la propaganda, grazie alla capacità di raggiungere un numero potenzialmente illimitato di persone. Come nei giochi occidentali, in cui ci sono missioni dove bisogna uccidere i terroristi, i jihadisti hanno ricreato similmente dei videogiochi in cui l'occidente e, in particolare, gli Stati Uniti sono gli obiettivi primari. Oltre alla propaganda, ci sono eventi che riproducono esattamente gli attacchi terroristici avvenuti in passato, come nel caso di "ARMA 3: Takistan life".

In questo VG vengono riprodotti gli eventi dell'11 settembre 2001, gli attentati di Londra del 2005 e gli attacchi Thalyst del 2015. Oltre a questo, nel videogioco potrai imparare a negoziare con i terroristi con varie tecniche di comunicazione, simulare

sessioni di addestramento ed esercitarsi a far esplodere bombe con un detonatore remoto. Da un lato ci sono i VG creati appositamente per la propaganda e il reclutamento, dall'altro queste organizzazioni hanno la grande capacità di infiltrarsi nelle comunità virtuali occidentali. I terroristi religiosi e gli estremisti politici utilizzano i videogiochi quotidianamente ed è spesso possibile trovare un membro dell'ISIS o di qualche organizzazione terroristica mentre giocano. Poiché i Videogiochi occidentali sono più avanzati e sono diventati veri e propri simulatori della realtà, diventano veri e propri mezzi per acquisire nuove conoscenze. Inoltre, le applicazioni e le chat legate ai giochi aumentano lo spazio per la loro propaganda. Questi mondi virtuali vengono utilizzati per scopi terroristici, ma si può riscontrare anche l'estremismo. Un podcast tenuto da Katerina Vittozzi nel Regno Unito mostra come il fenomeno sia dilagante e quanti giovani vengano plagiati e reclutati attraverso queste piattaforme.

“Il signor Bromage ha affermato che i contenuti specifici per bambini utilizzati dall'estrema destra per prendere di mira i giovani online includono videogiochi soprattutto, meme e video. Il bambino di nove anni era stato reclutato dal fratello maggiore che mostrava al fratello minore "videogiochi neonazisti estremi", ha aggiunto. (Vittozzi, 2020)

La strategia utilizzata da questi reclutatori di estrema destra è la stessa dei terroristi; pertanto, videogiochi, meme e immagini di propaganda invitano gli utenti a entrare in spazi virtuali privati. Le ricerche condotte, seguendo e rintracciando diversi utenti in questi mondi virtuali, hanno portato alla luce diverso materiale che dimostra come questi spazi vengano utilizzati per gli scopi sopra menzionati. Gli esempi sono riportati nelle Figure 13,14,15,16,17 e 18.

Sono diversi i casi in cui è stato possibile riscontrare questo fenomeno, ai quali la ricerca ha dedicato anche più tempo in base alla conseguente importanza per la sicurezza nazionale.

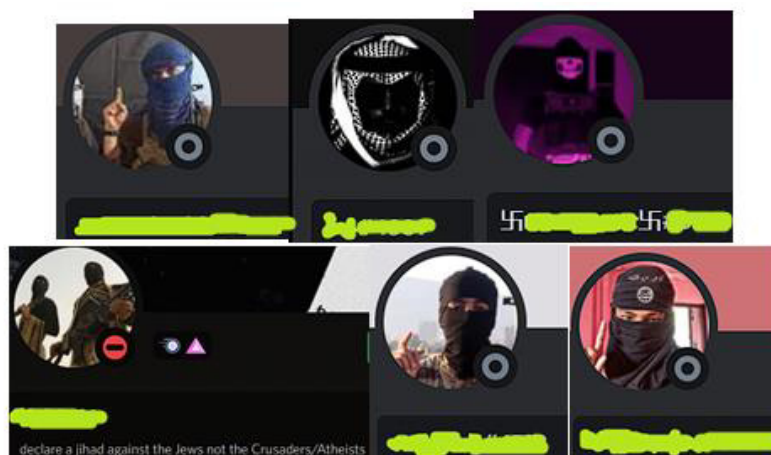


Figura 13 Avatar di Utenti che postano propaganda su Discord

L'utilizzo di Discord e videogiochi per commettere Cyber-crimini

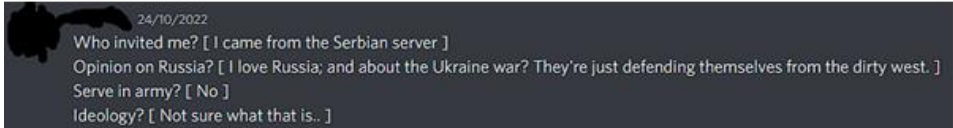


Figura 14 Utenti, che dirigono server in cui viene diffusa propaganda

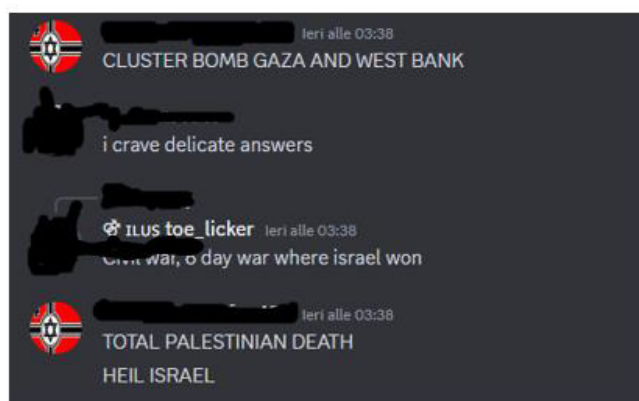


Figura 15 Propaganda during wars

*Cybercrime e videogiochi:
L'utilizzo di Discord e videogiochi per commettere Cyber-crimini*

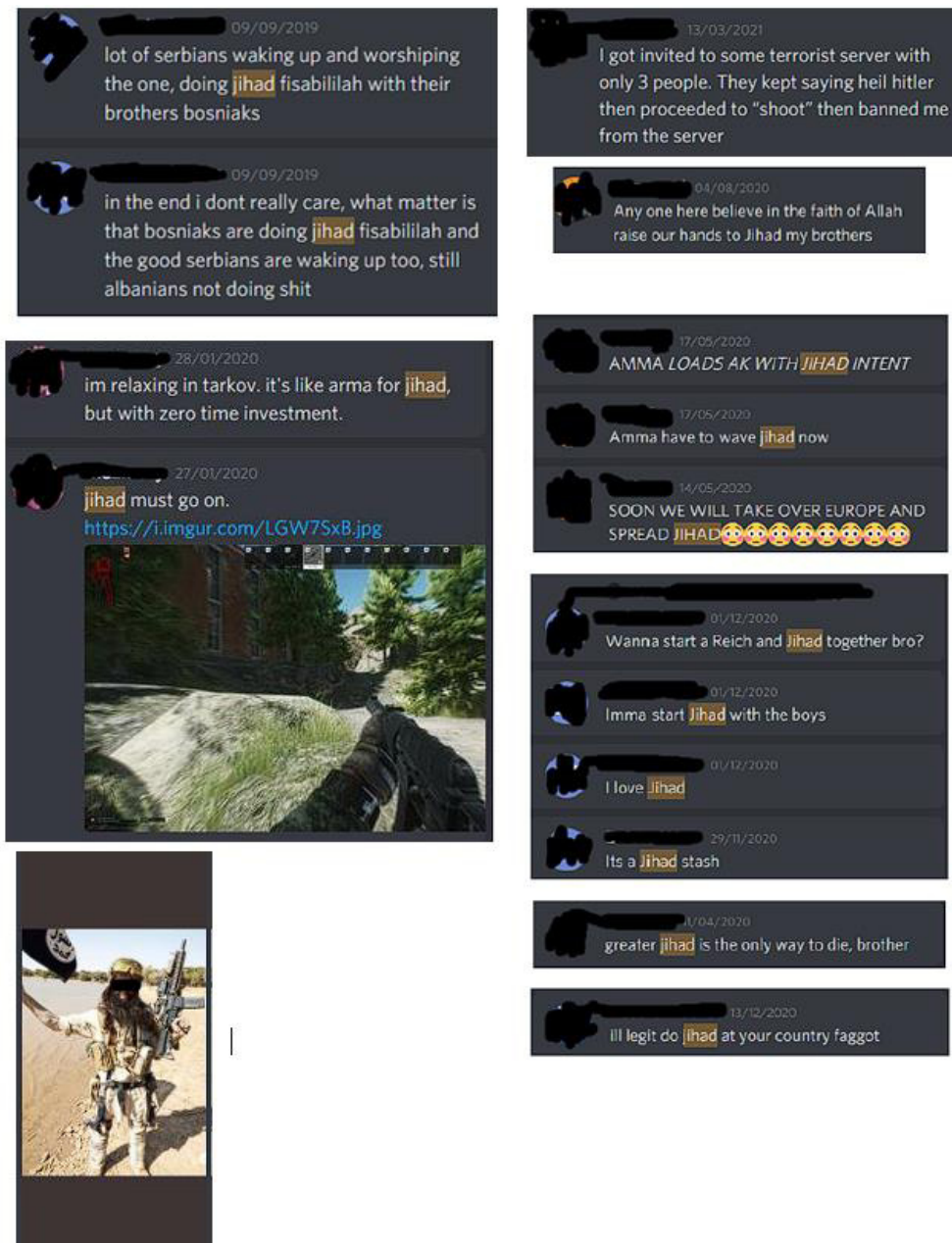


Figura 16 Propaganda

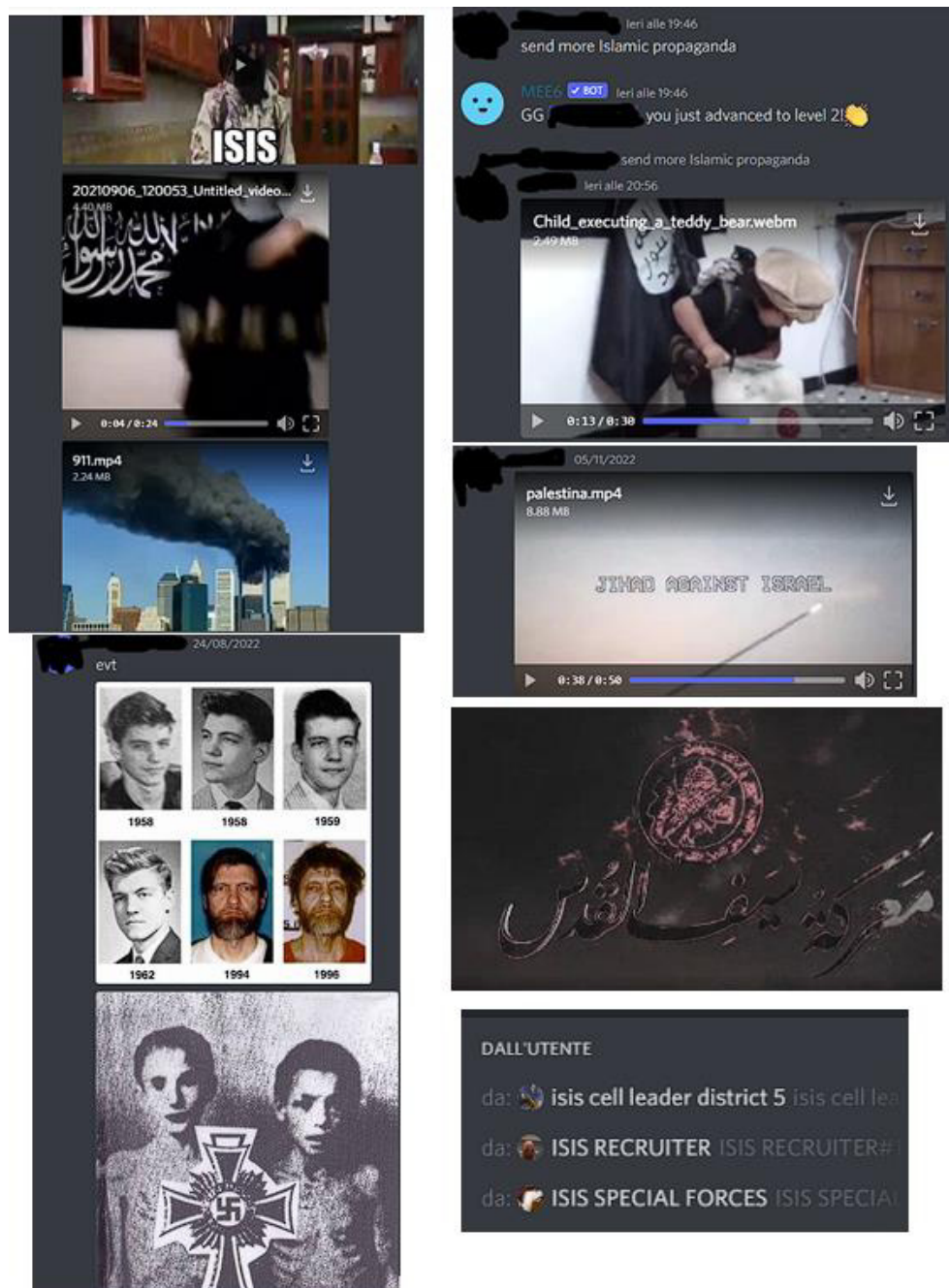


Figura 17 Propaganda

*Cybercrime e videogiochi:
L'utilizzo di Discord e videogiochi per commettere Cyber-crimini*

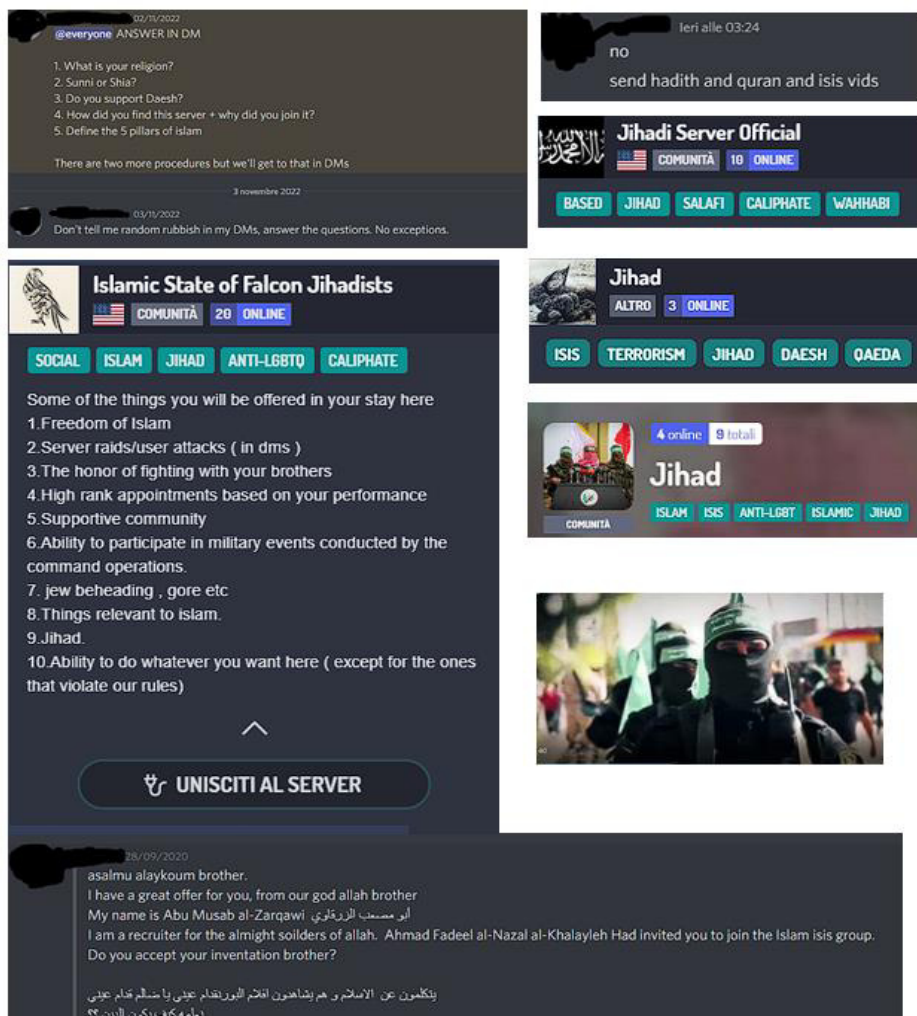


Figura 18 Propaganda

Analisi

Nell'ambiente di gioco, la maggior parte delle comunicazioni avviene tramite chat scritte e vocali, ed è possibile sfruttarle in molteplici modi. Le possibilità di Discord differiscono; non tutti digitano in chat o condividono contenuti su server pubblici ma preferiscono nascondersi in canali privati e condividere i contenuti vocalmente. Anche se i messaggi su Discord vengono archiviati per un certo periodo, le conversazioni non vengono monitorate (Politiche e impegno per la sicurezza | Discord, 2022); pertanto, un auricolare con microfono è l'hardware perfetto per comunicare. Nel corso della ricerca è stata raccolta una grande quantità di materiale; gli screenshot presentati nei risultati rappresentano solo una piccola parte di quel materiale e la maggior parte dei risultati consistono in chat vocali che sono state trascritte e riportate. Analizzando le comunità e il loro comportamento con la netnografia, è stato possibile stabilire un modello esplicativo che evidenzia il flusso comunicativo nell'ambiente di gioco. Il quadro riportato nella Figura 19 illustra tutte

le possibili connessioni che un utente potrebbe intraprendere utilizzando Discord e l'ambiente di gioco. Attraverso i giochi è impossibile scambiare immagini o file; quindi, gli ingaggi avvengono tramite chat vocali o scritte con avatar. Quando un determinato videogioco non possiede funzioni di chat, gli utenti passano a Discord; inoltre, quando la prima interazione tra gli utenti richiede uno scambio di immagini, gli utenti condividono i propri contatti e continuano le conversazioni su Discord. Se non è necessario lo scambio di immagini o file, le conversazioni tra avatar o in Discord possono avvenire all'interno dell'ambiente di gioco. Discord può essere utilizzato contemporaneamente mentre si gioca a un videogioco, diventando un vettore perfetto per raggiungere una popolazione più ampia grazie alla sua stretta connessione con i giochi. L'approfondimento dell'analisi ha consentito di individuare quale server, e di conseguenza quale ambiente di gioco connesso a Discord, sia più adatto ad un reato piuttosto che ad un altro. Nella Tabella 2 sono illustrate quali tipologie di videogiochi erano connesse ai server Discord dove è stato rinvenuto il materiale, e nella Tabella 3 è indicata l'età della community analizzata nei server esposti a quello specifico reato.

Tabella 2 Tipo di videogioco connesso al server Discord e tipologia del server.

	Tipo di videogioco connesso con Discord	Tipologia del Server
Presenza di Pedofili	Battle Royale, MMO, Sandbox, Console related	Pubblico e privato
Sfide e istigazione al suicidio	Battle Royale, MMO, Sandbox, Console related	Pubblico e privato
School shooting - omicidi	FPS, MMO, Battle Royale	Pubblico e privato
Compravendita armi e droga	FPS	Privato
Terrorismo (propaganda, atti), estremismo estrema destra	FPS, MMORPG	Pubblico

Tabella 3 Età media degli utenti colpiti dai reati.

	Server gaming di Discord con un'età <25	Server gaming di Discord con un'età >25
Presenza di Pedofili	80%	20%
Sfide e istigazione al suicidio	80%	20%
School shooting - omicidi	70%	30%
Compravendita armi e droga	30%	70%
Terrorismo (propaganda, atti), estremismo estrema destra	40%	60%

*Cybercrime e videogiochi:
L'utilizzo di Discord e videogiochi per commettere Cyber-crimini*

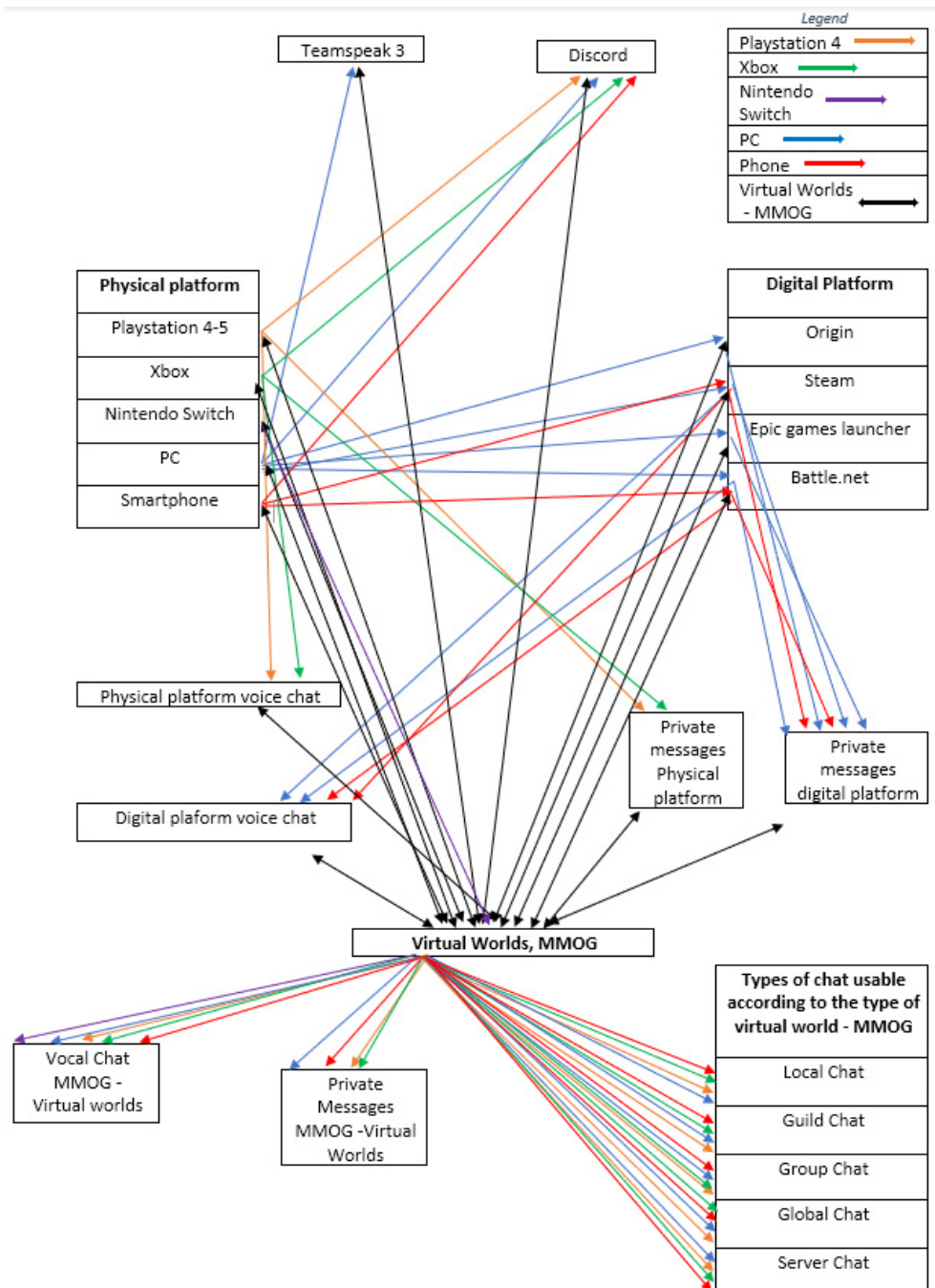


Figura 19 Possibilità di comunicazioni per utenti che utilizzano videogiochi e Discord

Discussione

La possibilità di comunicare senza reale controllo in questa applicazione consente di commettere diversi reati. Inoltre, questo ambiente è diventato il vettore perfetto

per gli utenti che vogliono perpetrare crimini a causa dell'uso globale, della scarsa legislazione e dell'insufficiente conoscenza del settore. I limiti riscontrati e che, comunque, persistono per qualsiasi altro ricercatore sono molteplici:

- Il primo problema è che esistono milioni di server e milioni di comunicazioni passano ogni secondo; pertanto, ciò che è possibile cogliere è limitato solo all'evento concreto connesso alla presenza del ricercatore.

- La maggior parte delle comunicazioni avviene in stanze private o luoghi nascosti, rendendole difficili da intercettare. Inoltre, per alcuni crimini, una stanza nascosta è più sicura di una chat pubblica, mentre una chat pubblica è migliore per la propaganda, poiché potrebbe raggiungere più persone.

- Il comportamento e le relazioni della comunità sono diversi in ciascun server. Ciò rende più complicato quando qualcuno deve studiare questi ambienti. Ci sono alcuni ambienti che si adattano meglio ad alcuni crimini e relazioni piuttosto che ad altri.

- L'unico modo per cogliere possibili spunti è vivere all'interno della comunità e osservare conversazioni ed eventi dal vivo perché tutto viene eseguito in tempo reale. Pertanto, se il ricercatore non è presente in quel momento, è impossibile recuperare quell'evento.

Tuttavia, utilizzando l'approccio netnografico, è stato possibile gettare nuova luce su questo fenomeno, e poiché sono state fatte molte speculazioni sull'ambiente di gioco e sui crimini, il materiale raccolto dovrebbe fornire una migliore visione della questione, che può essere utilizzata come spunto punto per futuri studi su questo problema.

Conclusioni

Con la perenne evoluzione del settore gaming, Discord continua a crescere inesorabilmente. Gli utenti possono accedere a milioni di server in tutto il mondo, ciascuno con regole e funzionalità diverse. Ad oggi nessun sistema è in grado di controllare queste comunicazioni e il sistema di monitoraggio e reporting è piuttosto obsoleto. Al momento, l'unico metodo a disposizione dell'azienda per affrontare il problema è stabilire termini di contratto e regole di condotta per mantenere sicura questa applicazione, ma questo non risolve il problema. Se alcune conversazioni avvengono in canali privati o con una chat vocale, diventa impossibile che gli altri utenti se ne accorgano. Tutto si basa su regole ipotetiche che, il più delle volte, non trovano applicazioni reali. Grazie alle sue funzioni (anonimato, proxy, VPN, account

falsi, ecc.) Discord è diventato il vettore perfetto per commettere crimini. Questa ricerca è stata complessa perché sono state trascorse molte ore senza risultati e non è stato facile scegliere quale server monitorare tra milioni. Inoltre, i messaggi o le conversazioni devono essere catturati immediatamente, poiché i contenuti illegali vengono spesso rimossi rapidamente dai loro autori. Questo studio dovrebbe sollevare preoccupazioni sulla sicurezza relative a Discord e aprire la strada alla costruzione di nuove politiche di sicurezza o strumenti automatizzati con l'aiuto dell'intelligenza artificiale, per migliorare la sicurezza di questa applicazione.

Bibliografia

- Aitamurto, T. (2013). Balancing Between Open and Closed: Co-creation in magazine journalism. *Digital Journalism*, 1(2), 229–251. <https://doi.org/10.1080/21670811.2012.750150>
- Anne-Laure Mondesert. (2020). *EU anti-terror chief warns video games used to spread extremism, prepare attacks* | *The Times of Israel*. <https://www.timesofisrael.com/eu-anti-terror-chief-warns-video-games-used-to-spread-extremism-prepare-attacks/>
- Au, C. H., & Ho, K. K. (2021). The anti-ageing secret of massively multiplayer online game: Managing its lifecycle. *Australian Journal of Management*, 46(4), 652–671. <https://doi.org/10.1177/0312896220981119>
- Bickart, B., & Schindler, R. (2001). Internet Forums as Influential Sources of Consumer Information. *Journal of Interactive Marketing*, 15, 31–40. <https://doi.org/10.1002/dir.1014>
- Bush, D. R. (n.d.). *Reynard Proposers Day IARPA-BAA-09-05 Overview*. 50.
- Catterall, M., & Maclaran, P. (2002). Researching consumers in virtual worlds: A cyberspace odyssey. *Journal of Consumer Behaviour*, 1, 228–237. <https://doi.org/10.1002/cb.68>
- Chambers-Jones, C. (2013). Virtual world financial crime: Legally flawed. *Law and Financial Markets Review*, 7(1), 48–56. <https://doi.org/10.5235/LFMR7.1.48>
- Consalvo, M., & Dutton, N. (2006). Game analysis: Developing a methodological toolkit for the qualitative study of games. *Game Studies*, 6.
- Costello, L., McDermott, M.-L., & Wallace, R. (2017). Netnography: Range of Practices, Misperceptions, and Missed Opportunities. *International Journal of Qualitative Methods*, 16(1), 160940691770064. <https://doi.org/10.1177/1609406917700647>
- Curcio, M. (2023). Cybercrime and Video Games: Exploring children's safety in the gaming environment. *Proceedings of the 2023 European Interdisciplinary Cybersecurity Conference*, 144–148. <https://doi.org/10.1145/3590777.3590801>
- David Curry. (2024). *Discord Revenue and Usage Statistics (2024)*. Business of Apps. Retrieved 9 February 2024, from <https://www.businessofapps.com/data/discord-statistics/>
- Elliott, J. (2013). *World of Spycraft: NSA and CIA Spied in Online Games*. ProPublica. Retrieved 3 October 2022, from <https://www.propublica.org/article/world-of-spycraft-intelligence-agencies-spied-in-online-games>
- Gilchrist, P., & Ravenscroft, N. (2011). Paddling, property and piracy: The politics of canoeing in England and Wales. *Sport in Society*, 14(2), 175–192. <https://doi.org/10.1080/17430437.2011.546518>
- Grabher, G., & Ibert, O. (2014). Distance as asset? Knowledge collaboration in hybrid virtual communities. *Journal of Economic Geography*, 14(1), 97–123. <https://doi.org/10.1093/jeg/lbt014>

- Heinonen, K., & Medberg, G. (2018). Netnography as a tool for understanding customers: Implications for service research and practice. *Journal of Services Marketing*, 32(6), 657–679. <https://doi.org/10.1108/JSM-08-2017-0294>
- Hernandez, M. D., & Handan, V. (2014). Modeling word of mouth vs. media influence on videogame preorder decisions: A qualitative approach. *Journal of Retailing and Consumer Services*, 21(3), 401–406. <https://doi.org/10.1016/j.jretconser.2013.11.003>
- Howarth. (2024). *How Many Gamers Are There? (New 2024 Statistics)*. Exploding Topics. <https://explodingtopics.com/blog/number-of-gamers>
- Irwin, A. S. M., Slay, J., Raymond Choo, K., & Liu, L. (2012). Are the financial transactions conducted inside virtual environments truly anonymous?: An experimental research from an Australian perspective. *Journal of Money Laundering Control*, 16(1), 6–40. <https://doi.org/10.1108/13685201311286832>
- James Titcomb. (2015). *Did Paris terrorists really use PlayStation 4 to plan attacks?* <https://www.telegraph.co.uk/technology/video-games/playstation/11997952/paris-attacks-playstation-4.html>
- Keene, S. D. (2011). Emerging threats: Financial crime in the virtual world. *Journal of Money Laundering Control*, 15(1), 25–37. <https://doi.org/10.1108/13685201211194718>
- Kozinets, R. (1997). I want to believe: A netnography of the X-philies' subculture of consumption. *Advances in Consumer Research*, 24, 470–475.
- Kozinets, R. (1999). E-Tribalized Marketing?: The Strategic Implications of Virtual Communities of Consumption. *European Management Journal*, 17, 252–264. [https://doi.org/10.1016/S0263-2373\(99\)00004-3](https://doi.org/10.1016/S0263-2373(99)00004-3)
- Kozinets, R. V. (1998). On netnography: Initial reflections on consumer research investigations of cyberculture. *Advances in Consumer Research*, 336–371.
- Kozinets, R. V. (2006). Click to Connect: Netnography and Tribal Advertising. *Journal of Advertising Research*, 46(3), 279–288. <https://doi.org/10.2501/S0021849906060338>
- Lankoski, P., & Bjork, S. (2015). *Game research methods: An overview*.
- Mudry, T. E., & Strong, T. (2013). Doing Recovery Online. *Qualitative Health Research*, 23(3), 313–325. <https://doi.org/10.1177/1049732312468296>
- Riffe, D., Lacy, S., Fico, F., Riffe, D., Lacy, S., & Fico, F. G. (2006). *Analyzing Media Messages* (0 ed.). Routledge. <https://doi.org/10.4324/9781410613424>
- Silva, J. P. N., Valadares, G. C., Pedrosa, G., Rezende, D. C., Cappelle, M. C. A., & Assis, F. A. A. (2021). Gender imbalance in MMORPG: The case of World of Warcraft in Brazil. *Feminist Media Studies*, 1–17. <https://doi.org/10.1080/14680777.2021.1973060>
- S.M. Irwin, A., Slay, J., Raymond Choo, K.-K., & Lui, L. (2014). Money laundering and terrorism financing in virtual environments: A feasibility study. *Journal of Money Laundering Control*, 17(1), 50–75. <https://doi.org/10.1108/JMLC-06-2013-0019>
- Van der Sanden, R., Wilkins, C., Rychert, M., & Barratt, M. J. (2022). The Use of Discord Servers to Buy and Sell Drugs. *Contemporary Drug Problems*, 49(4), 453–477. <https://doi.org/10.1177/00914509221095279>