Council of the European Union

Brussels, 6 July 2020
(OR. en)

9066/20

LIMITE

CT 46
JAI 520
COSI 106
CATS 45
ENFOPOL 152
COPEN 166
DIGIT 46
TELECOM 98
HYBRID 14
CYBER 104
IND 82

NOTE

From:	EU Counter-Terrorism Coordinator
To:	Delegations
Subject:	Online gaming in the context of the fight against terrorism

INTRODUCTION

While not a threat in and of itself, online gaming[1] can be an enabler of terrorist and other criminal activity[2]. Gaming platforms are increasingly being used not only for playing online games, but also as social media platforms[3] and chat rooms[4] and are using virtual cryptocurrency[5].

[1] Online games are video games that are played through computer networks, in particular the Internet. Such games have enjoyed enormous growth in recent years and are commonplace, both on the leading gaming platforms, such as PCs and game consoles (e.g. Sony's PS4, Microsoft's Xbox One or the Nintendo Switch) and on mobile devices such as tablets and cell phones. The design of e-games is variable and can range from basic, cost-free and browser-based online games to fee-based games with advanced gameplay and sophisticated graphics and audio elements. E-gaming also covers various genres, ranging from sports, strategy games and first-person shooter (FPS) formats, to massively multiplayer online games (MMOGs). Online gaming should be distinguished from online gambling. Cloud gaming, a type of online gaming that uses remote servers to stream on the user's device, is becoming increasingly important. E-sports, i.e. sports competitions played in the form of videogames, are also gaining popularity.

[2] The phenomenon is not limited to the field of terrorism. Through its sustainable democratization and its opportunities for concealment from public authorities online gaming has a broader impact on Internet-facilitated crime (e.g. child grooming, online money laundering, etc.).

[3] For example, Steam (owned by the Valve Corporation) is the largest digital distribution platform for PC games ($4.3 billion in revenue in 2017) and provides a social platform for PC gaming. It currently has 95 million monthly users and is still mostly unmonitored. As a result, the platform has gained popularity among violent extremists, since various users and groups glorify Nazi, racist, anti-Semitic, homophobic or otherwise hateful content.

[4] All major online video games (e.g. World of Warcraft, League of Legends), video-gaming platforms (e.g. Playstation

The gaming industry is rapidly growing, with over two billion players around the world, global revenue of several billion dollars ($135 billion in 2018) and the involvement of major actors such as Sony, Microsoft, Activision Blizzard, Nintendo and Electronic Arts (EA)[6]. Other gaming-related activities, such as the use of gaming-related apps (e.g. Discord[7]) and live streaming of video games with millions of viewers (e.g. on Twitch)[8], have also grown considerably in recent years. Major tech companies are investing increasingly in the video games industry. In November 2019, Google launched its cloud-gaming service called Stadia[9], while Amazon has created its own video game developer[10].

The Chinese video game industry is currently the world's largest market for video games; it includes major gaming companies like Tencent and NetEase, which are increasingly looking for opportunities to expand internationally[11].

According to the Interactive Software Federation of Europe (ISFE), the EU video games market was worth EUR 21 billion in 2019, with 54% of EU citizens playing video games.

Network, Xbox Live and Steam) and live-streaming platforms (e.g. Twitch) feature in-game voice communication and chat rooms. Alternatively, players can use external gaming chat apps (e.g. Discord and Mumble) that support text chat and video chat, which further facilitates exchanges between gamers.

[5] Nearly all online games have a virtual currency. The most popular ones, such as Fortnite and World of Warcraft, have robust secondary markets, where in-game currencies can be exchanged for real money.

[6] The video-gaming industry is very competitive and continually growing. There are over two billion gamers across the world (26% of the world's population). According to Forbes the industry as a whole earned over $135 billion in revenue in 2018.

[7] Discord is a free voice, video and text chat application, which was originally created for gamers but then evolved into a generic platform hosting different communities. Launched in 2015, Discord is divided into communities named "servers", which include text channels and voice channels. Each "server" is dedicated to a different topic. Discord allows users to share files, videos and music.

[8] Major gaming live-streaming services include Twitch (owned by Amazon), Facebook gaming and YouTube gaming, plus the broadcasting of gameplay footage is widespread on other platforms.

[9] Stadia is a service offering some 20 games including big-budget blockbusters for use on PCs and/or home consoles subject to a monthly subscription fee.

[10] In 2014, the Amazon group announced its intention to develop games. Amazon Game Studios is focusing entirely on the development of online games and mobile games designed specifically to develop synergies with Twitch (which belongs to the same group). Amazon and Amazon Game Studios are also developing cloud-gaming projects.

[11] In almost 20 years, China has established itself as the world's largest video game market. In 2018, there were 620 million gamers in China, and the gaming industry brought in 30 billion dollars of revenue. The Tencent Games division of Tencent Holdings is the world's largest gaming company by revenue (46% of China's market share and 10% of the global market share in 2018). Other major gaming companies include NetEase, Perfect World, Shunrong and Shanda. The Chinese government strictly regulates the Chinese gaming industry (e.g. games need approval and there are measures to protect minors) and foreign gaming companies are forced to form partnerships with local companies if they want to bring games to the Chinese market. In recent years, the Chinese gaming companies have been trying to position themselves on the international market and have been investing aggressively in foreign video game developers. In 2017, Tencent bought the US gaming developer Riot Games, the company behind the famous game 'League of Legends', for $400 million. The company also owns minority and majority stakes in many other video game companies (e.g. 5% in Ubisoft, 5% in Activision, and 80% in Supercell).

Online gaming has so far not been the focus of EU counterterrorism (CT) efforts, such as the EU Internet Forum or initiatives to remove terrorist content online, combat terrorist financing and prevent radicalisation. However, this is starting to change: The 2020 Strategic Orientations on a coordinated EU approach to prevention of radicalisation identified online gaming and radicalisation as a new priority. INTCEN provided a paper on online-gaming in the context of right-wing violent extremism and terrorism[12]. The EU Internet Referral Unit (EU IRU) at Europol has followed the issue since 2016 and is providing Member States with analysis, especially in the context of jihadi terrorism.

Gaming platforms are not supervised in the same way as major social media platforms like Facebook or cryptocurrencies like Ethereum[13]. As a result, they operate in a kind of vacuum and so are at risk of abuse by terrorists and other criminals.

This note will first seek to clarify the threats posed by the use of gaming for terrorist purposes, before examining existing measures to address this and concluding with some recommendations for the way forward, including possible mitigation measures.

Online gaming can enable four main terrorist activities: **i) content propagation, radicalisation and recruitment; ii) communication, iii) combat training and iv) money laundering and terrorist financing.** Each one of them is looked in details below.

I. ONLINE-GAMING COULD BE MISUSED FOR TERRORIST PURPOSES

1. Content propagation, radicalisation and recruitment

Gaming platforms, video games, related apps and live-streaming services have a strong social media dimension; they have a similar reach but are less well known than the mainstream social media companies. As a result, terrorists can use gaming platforms to spread propaganda and recruit new members even when they have been banned on mainstream social platforms.

[12] EEAS (2020) 00685 of 15 June 2020.
[13] Policymakers have increased their focus on how violent extremists can use cryptocurrencies to commit financial crimes and on how they exploit mainstream social media platforms to promote their narratives. As a decentralised computing platform for cryptocurrencies, Ethereum falls within the scope of the 5th Anti-money laundering Directive which also tackles terrorist financing risks linked to the anonymous use of virtual currencies. Mainstream social media companies (e.g. Facebook, Google, Microsoft) have implemented a variety of voluntary measures to detect and remove terrorist content.

Right-wing violent extremists (RWVEs) are firmly anchored in the online gaming community[14], while the presence of Islamist terrorists can also be observed, albeit to a lesser extent[15]. For example, Anders Bering Breivik actively shared his propaganda with people he met through online video games[16].

However, it remains difficult to identify the exact scale of the presence of terrorists and violent extremists and the modus operandi of **terrorist** '**groomers' on these platforms. Further investigation is therefore needed**[17].

Considering the volume of toxic content and the presence of violent extremists on online gaming platforms, **these platforms could in future replace other social networks as the preferred channel for terrorist propaganda and recruitment**[18].

Three factors make gaming platforms particularly attractive locations for recruitment and the dissemination of violent propaganda:

[14] RWVEs have proven to be particularly 'technology savvy', adapting and taking advantage of the rapidly changing variety of online tools. As a result, they have also used online gaming to promote their ideology, intimidate the audience or radicalise and recruit new members. The gaming community is international, and RWVEs can use it to network on a global scale. 'Gamergate' was an uncoordinated, misogynistic and 'anti-liberal' troll movement that emerged in 2016 and was initially directed against the gaming industry. However, it rapidly became a symbol for the uninhibited spread of right-wing violent extremist ideas in the predominantly male online culture.

[15] (1) Mobile games have been mentioned in the online chatter of Da'esh supporters, who suggested the use of in-game chats to reach out to online communities of users for recruitment and incitement of lone actor types of attacks. (2) In recent weeks, invitation links to the application Discord have been detected by the EU Internet Referal Unit in pro-Da'esh channels and groups across different platforms, such as Hoop and Rocket. Da'esh supporters appeared to have started creating a limited number of servers on Discord, representing unofficial supportive Dae'sh media outlets. One of them, the "#Akbar-Media", shared links to video releases by other Dae'sh supportive media outlets, as well as links to official propaganda such as the Dae'sh weekly magazine al-Naba. This server disappeared from the platform a few days after its creation. (3) In Europe, a 14-year-old Austrian boy was contacted by Da'esh sympathisers online in 2014, and downloaded bomb-making plans on his PlayStation. This was detected by the authorities and he was sentenced to two years in prison.

[16] For example, prior to his attacks, he sent his manifesto to a Dutch gamer. See: Waterfield, B. (26.7.2011). Norway: Anders Behring Breivik used online war games as 'training', https://www.telegraph.co.uk/news/worldnews/europe/norway/8663329/Norway-Anders-Behring-Breivik-used-online-war-games-as-training.html .

[17] A 2019 'Anti-defamation League' report on the social interactions and experiences of video game players in the US was able to establish that 23% of American online gamers were exposed to violent extremist white supremacist ideology in online games, while 8% of players were exposed to positive views concerning the activities of Da'esh. Free to Play? Hate, Harassment, and Positive Social Experiences in Online Games. (not dated), https://www.adl.org/free-to-play.

[18] The Munich shooter *David Sonboly* was active on the gaming platform Steam, where he gathered more than 4000 gaming hours using the first-person shooter 'Counter Strike' and regularly engaged in forums that glorified mass shootings and anti-Muslim propaganda.

Firstly, **there is a huge target audience for radicalisation on gaming platforms, especially among young people, who tend to be more vulnerable to radicalisation and recruitment.** According to the latest Eurobarometer report on 'Europeans' attitudes towards cybersecurity', published in January 2020, **online gaming represented 25% of all online activities in the EU**, while **51% of 15-24 year olds were playing online games** (this number decreases with age)[19]. While most adults today have not grown up around online gaming, the youth of today are the adults of tomorrow. The proportion of players is therefore bound to increase. Even if vulnerability is generally assumed to decrease with maturity, the emergence of isolated cases with exploitable weaknesses cannot be excluded. In the future, this phenomenon will experience sustainable democratisation. The current context of the global COVID-19 pandemic and the associated lockdown measures, with millions of young people at home, could be an additional fertile ground for online terrorist recruiters.

Many popular video games involve violence and war, which appeals to players who could be attracted to violent extremist messages. The predominant player-base of violent video games is young men, who may be socially isolated or disenfranchised, and drawn to violence for those reasons. Violent extremist groups can manipulate feelings such as resentment, isolation or an identity crisis to radicalise these individuals. Accordingly, the psychological profiles of these gamers can make them prone to radicalisation.

Secondly, **gaming platforms, related apps and streaming services provide an ecosystem that is suitable for spreading violent propaganda**. Some gaming platforms offer sizeable social networking services, which enable gamers to search for, and interact with other users and groups that advertise violent extremist ideologies. The level of anonymity on these platforms is very high, and the players can identify themselves using avatars and profiles. Certain video games require players to team up and communicate with strangers. Radical groups can use this to 'troll'[20] (e.g. use racial slurs to 'test the waters') and initiate contact with potential recruits[21].

[19] Survey and report by Kantar Belgium at the request of the European Commission, Directorate-General for Migration and Home Affairs. The figures from this Eurobarometer survey of a sample of the population are slightly lower than the data provided by the Interactive Software Federation of Europe (p. 2).
[20] 'Trolling' (or 'flaming') can be defined as abusive Internet behaviour aiming to antagonise other gamers online by deliberately posting inflammatory, irrelevant, offensive or other disruptive comments and content.
[21] They then address vulnerable or interested players' problems, give them structure and identity and gradually bring them closer to their ideology. It has been reported that right-wing violent extremists first use racial slurs to test and desensitise potential recruits, and later use popular topics such as military history or Nordic mythology to spark further interest.

Once trust is built, recruiters can lure them onto less well monitored message boards and share more violent extremist material, thereby intensifying the indoctrination[22]. Radicalisation can also occur on gaming-related live-streaming platforms (e.g. Twitch) or gaming-related communication apps (e.g. Discord). Additionally, online gaming enables the development of anonymous and close ties with co-players. This situation provides all the benefits and none of the drawbacks of in-person radicalisation[23], which could create a **radicalisation creep**, with violent extremist views becoming normalised over time.

Indeed, **radicalisation through e-gaming creates powerful echo chambers similar to those found on Facebook or other platforms, but with the added components of regular interaction with one's fellow players** and the emotional bonding that occurs through dopamine releases during the high-pressure activity of fast-paced gaming. For socially-isolated gamers, **gaming echo chambers are social media echo chambers on steroids**.

Thirdly, in connection with the spread of online terrorist propaganda, various terrorist groups are increasingly exploiting popular elements from video games and the gaming culture to to appeal to younger generations, to normalise their message as well as to desensitize users to violence. For instance, Da'esh has spread 'memes' and propaganda videos designed to evoke shooter games like Call of Duty and Grand Theft Auto, which are particularly popular with young male gamers – the key target group for terrorist recruitment[24]. Additionally, a number of user-generated content (UGC) banners supportive of Da'esh have been inspired by the "Assassin's Creed" videogame series[25].

[22] Kamenetz, A. (2018, November 5). Right-Wing Hate Groups Are Recruiting Video Gamers. https://www.npr.org/2018/11/05/660642531/right-wing-hate-groups-are-recruiting-video-gamers
[23] Gamers grow closer to recruiters, while remaining isolated from people who could help them question the increasingly radical views presented to them, or who might provide them with a social alternative to interacting with violent extremist individuals.
[24] Dauber, C. E., Robinson, M. D., Baslious, J. J., & Blair, A. G. (2019, June). 'Call of Duty: Jihad – How the Video Game Motif Has Migrated Downstream from Islamic State Propaganda Videos', https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2019/issue-3/02--dauber-et-al..pdf.
[25] According to the EU IRU.

In that context, **the concept of 'gamification' of terrorist violence**[26] — which is the transfer of popular in-game elements into reality — is an increasing trend. Da'esh propagandists have used allusions to videogames in interviews and tweets[27] and have also shared propaganda videos of combat scenes that were filmed with helmet cameras and thereby recall the first-person perspective of first-person shooter games. The attacks in Oslo, Utøya, Christchurch and Halle are further examples of gamification of terrorism. In all these instances, the terrorists were actively involved in the gaming community, and their attacks were inspired by it[28]. The perpetrators of Christchurch and Halle attacks respectively broadcasted their killings in a live stream (Facebook Live and Twitch), adopting the first-person shooter perspective often found in video games. The attacker in Halle even tried to create and perform game-like achievements during his attack[29]

To summarise, given the advantages that the e-gaming community offers to violent extremists and the growing popularity of gaming across the world, **the EU should engage with, hold accountable and work with the online gaming industry similarly to mainstream social media with regard to violent extremist content propagation, radicalisation and recruitment**.

2. Communication

Gaming communication services allow terrorists to connect in a mostly secure setting, even when 'on the move', through gaming chat apps[30].

[26] Gamification can be defined as the use of game design elements like aesthetics, competition, levels and rewards in the 'real life' context. The goal is to encourage a behaviour change.
[27] During a BBC interview in June 2014, a Da'esh fighter declared that his new life was better than Call of Duty. In a tweet, Da'esh propagandist Junaid Hussein announced: 'You can sit at home and play call of duty or you can come and respond to the real call of duty', Can You Hear Your Call of Duty? The Gamification of Radicalization and Extremist Violence. (2020, March 17). https://eeradicalization.com/can-you-hear-your-call-of-duty-the-gamification-of-radicalization-and-extremist-violence.
[28] Ebner, J. (2020, February 14). 'Dark ops: Isis, the far-right and the gamification of terror', https://www.ft.com/content/bf7b158e-4cc0-11ea-95a0-43d18ec715f5.
[29] 'Achievements' are typical in video games. They are in-game attainments and a way of comparing yourself to other players in the game of getting a higher score, while they simultaneously serve as 'game instructions', encouraging other players to copy them. In his manifesto, Stephan Balliet (the attacker from Halle) formulated possible 'real life' achievements, e.g. the first achievement for his attack in Halle, which he called 'No Way Back', was to upload the manifesto to the Internet. This ironic tone is not uncommon for achievements in the gaming scene. He also mentions other possible 'achievements' like killing Jews each time with different weapons, using grenades, burning down a synagogue and a mosque, killing a communist, killing people with a sword or a nail bomb. But in the fora of the far-right gamer scene, Balliet is mocked for his failure and the 'low score' he achieved in the stream, while other terrorists like the Christchurch perpetrator Brenton Tarrant are praised for the fatality achieved in their attacks. Fröhlich, A., 10.10.2019, https://www.tagesspiegel.de/politik/der-anschlag-von-halle-rechtsterrorismus-inszeniert-wie-ein-computerspiel/25103584.html .
[30] E.g., the League of Legends app, 'LoL Friends' or gaming-related communication apps such as 'Discord'.

Online gaming enables extensive communication (through text, voice and video chat). While terrorists are already verifiably using encrypted digital communication tools (e.g. Telegram), there is concern that they could also misuse the communication tools provided through gaming to exchange information and further elude investigations. A 2016 analysis by the EU IRU on the potential use of gaming consoles such as the Sony PlayStation by jihadi groups highlighted that challenges related to the investigation of terrorist communications on gaming consoles concerned the use of voice over IP (VoIP) technologies. Additionally, the frequent reference to guns and violence being an integral part of these games make it harder to identify potential threat profiles automatically.

The majority of these gaming communication systems are encrypted[31], as the gaming industry knows that users generally demand strict privacy protection. Popular video game platforms like PlayStation Network or Xbox Live, as well as popular gaming-related apps like Discord or Mumble, offer encrypted text, audio and video chats. The type of encryption and more generally the security levels for communication can vary from one gaming platform to another. However, instead of using more secure end-to-end encryption, most of these gaming communication systems use less secure encryption protocols. In that regard, the majority of these gaming platforms offer their players mechanisms to report content, which can later be identified and removed by the operator[32].

In 2018, Sony provided the FBI with data retrieved from the PS4 console of an alleged terrorist[33]. This data also included the suspect's decrypted communication history, which suggests that the current encryption protocols of at least some leading gaming platforms provide scope for cooperation between such platforms and law enforcement officers in specific cases. Major gaming platforms seem to be able to access their users' messages and communication data, even when these are encrypted.

[31] Data encryption occurs when sent text or data is converted into a code (called 'ciphertext') that can only be decrypted by those who have the correct key. There is a distinction between symmetric and asymmetric encryption as different keys are used for encryption and decryption.
[32] E.g. the free voice, video and text chat application application Discord. Although this operator does not monitor the content of the communication of its users, it nonetheless decided to remove several, previously reported white nationalists and Nazi servers in 2018. This was after receiving public pressure for its lax monitoring of violent extremist content. The app Discord removed several reported white nationalist and Nazi servers in 2018. Discord is vulnerable to hijacking by violent extremists. Three factors can explain that vulnerability: (1) the chat provided by Discord to its users is private and only works with an invitation to enter into chat groups, which makes them imperceptible for non-users of Discord; (2) Discord allows a high degree of anonymity for its users; (3) the administrators of the chat groups can set their own moderation rules.
[33] In 2018, Sony shared information with the FBI on a PlayStation 4 user suspected of planning to leave the US to join Da'esh in the Middle East. This is the first time Sony provided gaming-related data after receiving an official government order.

Another aspect of the problem is that gaming communication is less in the limelight and that law enforcement might have prioritised the surveillance of more conventional telecommunication systems. Often terrorist and violent extremist groups and actors, therefore, use these less moderated, less regulated and more anonymous gaming communication systems as a teaser to later share more radical content on alternative more secured platforms.

It is essential for law enforcement officers to be able to access terrorist and other criminal communications lawfully, including such communications on gaming platforms. It would be interesting to compare the experiences of Member States on whether, and, if so, to what extent lawful interception of communications is applied in this context and to hear their experiences with regard to cooperation with gaming platforms.

3. Virtual combat training

E-gaming can support the training of fighters in two ways, by: (1) desensitising them to violence and (2) giving them the know-how (mission planning, equipment, tactics, etc.) to prepare and carry out military-style operations.

Many video games actively glorify brutality and may even serve as instructional guides on how to inflict pain[34]. Other games take the dangerous step of placing players in the shoes of terrorists[35]. **Terrorist groups have also created their own games aimed at glorifying violence and rallying players to their cause by fighting a specific enemy** (e.g. the US, the Israeli Defense Forces, ethnic minorities, etc.)[36].

Although some psychologists deny there is a causal relationship between violent video games and a propensity to violence, others suggest that prolonged exposure to violent video games can lead to aggressive thoughts and behaviour, psychological instability and lack of empathy[37]. In any event, by using video games in their propaganda, terrorists want to capitalise on desensitisation to violence to fuel the radicalisation and recruitment process.

---

[34] Games such as 'Splinter Cell' and '24: The Game' both have lengthy and realistically simulated torture interrogation components.
[35] One example, from very many, is 'Counter-Strike', where the player goes through missions as a terrorist. Meanwhile, 'ARMA 3' provides the ability to engage in-depth with the terrorist psyche, investing significant time in developing terrorist characters, creating one's own motives and defending them against other players.
[36] The right-wing violent extremist news portal *the Daily Stormer* released its modification of the first-person shooter game Doom 2 which lets the player fight against a Jewish World Conspiracy. The Hezbollah developed the video games Special Forces (2003) and Special Force 2: Tale of the Truthful Pledge (2006), which allow players to impersonate the Hezbollah and fight against the Israeli military.
[37] Kühn, S., Kugler, D., Schmalen, K. *et al.*, 'Does playing violent video games cause aggression? A longitudinal intervention study', *Mol Psychiatry* 24, 1220–1234 (2019). https://doi.org/10.1038/s41380-018-0031-7.

Certain first-person shooter games allow players to gain **a non-negligible knowledge base and skill set regarding mission planning, tactics, equipment and methodologies**[38]. At his trial, Anders Behring Breivik declared that he played video games such as 'Call of Duty: Modern Warfare' and used them as training simulation to prepare for his attacks[39]. Furthermore, the 9/11 Commission reports that attackers used flight simulator video games 'to increase familiarity with aircraft models and functions, and to highlight gaps in cabin security'[40]. On the other hand, video games and their overly simplistic and unrealistic nature cannot be expected to prepare individuals accurately for combat. They do not provide training on aspects such as muscle memory, physical fitness and comprehensive military know-how, which are fundamental in executing military-style operations.

Some experts warn that this is likely to change with advances in augmented and virtual reality (AR/VR), which will provide better tools for physical training and preparation for fighting[41]. Such technologies would give terrorists the ability to substantially raise their combat readiness while removing the risk factor associated with in-person training sessions (i.e. the need for travel, physical presence, etc.). The exponential technological progress is likely to offer additional opportunities.

4. Money laundering and terrorist financing

Online gaming has enabled the emergence of virtual economies, allowing virtual items and in-game currencies to be traded within a game, whilst in certain instances these can even be exchanged for real money outside the video game.

[38] E.g., *Call of Duty* lays the groundwork for physical training of individuals in how to position, cooperate with teammates and attack targets during combat. The primary focus of *Delta Force: Xtreme 2* is on designing the appropriate mission plan and correctly equipping one's team to achieve an objective.
[39] Pidd, H. (2012, April 19). Anders Breivik 'trained' for shooting attacks by playing Call of Duty.https://www.theguardian.com/world/2012/apr/19/anders-breivik-call-of-duty
[40] The National Commission on Terrorist Attacks Upon the United States (also called 'the 9/11 Commission') is an independent, bipartisan commission, established through US Congress legislation, which wrote a full and complete account of the circumstances surrounding the 11 September 2001 terrorist attacks in the United States. https://govinfo.library.unt.edu/911/report/911Report.pdf
[41] Virtual reality (VR) is the use of computer technology to immerse a user entirely in a digital world. Augmented reality (AR) projects digital information into the real world. The Automated Serious Game Scenario Generator for Mixed Reality Training (AUGGMED) creates scenarios allowing officers to practice fighting terrorists and rescuing hostages.

While money laundering via online gambling has been addressed and largely neutralised, *inter alia* through the Second and Third EU Money Laundering directives and follow-up regimes (due to high vigilance vis-à-vis service providers and tighter controls), online gaming has not received the same attention and supervision.

E-gaming remains a relatively unsupervised and — in some aspects — unregulated industry, which, given the advanced economic systems present in leading games[42], high player-counts[43], and the increasingly strong links to the real economy, makes it vulnerable to money laundering.

The laundering of money via e-gaming is rendered even easier by the fact that:

1. The Fifth EU Anti-Money Laundering Directive (5AMLD) explicitly states that currencies used exclusively for use in gaming environments do not fall under its scope;
2. In-game currencies which can be easily converted into cryptocurrencies or even standard currencies are growing in number;
3. Hiding one's identity while laundering money via online games is relatively easy to accomplish with only basic IT skills.

Consequently, gaming virtual currencies are attractive for money laundering and terrorist financing purposes as they enable money to be transferred across borders quickly, easily and almost invisibly. The concealment of flows can be facilitated by the multiplication of microtransactions. This context is particularly favorable for the financing of "low-cost" terrorism.

Virtual currencies can be divided into convertible/non-convertible and centralised/decentralised currencies. According to the Financial Action Task Force (FATF), virtual currencies in online gaming are, in theory, centralised and non-convertible. 'Non-convertible' means that they cannot be exchanged for fiat currency and must remain attached to a specific virtual environment (e.g. FIFA points, WOW Gold).

[42] The majority of online games have their virtual economy, in which players exchange virtual goods. Massively Multiplayer Online Games (e.g. WOW) in particular have enabled the emergence of complex virtual communities whose virtual economic activity is tied to the real economy. The idea is to acquire in-game currency and later sell it for real-world money. (E.g., in 2001, a region in the online role-playing game EverQuest, Norrath, was found to have the 77th highest GNP per capita in the world - it is located squarely between Bulgaria and Russia.) (http://news.bbc.co.uk/2/hi/sci/tech/1899420.stm).

[43] Free games have become the most lucrative business model in the gaming industry (https://www.forbes.com/sites/ilkerkoksal/2019/11/08/video-gaming-industry--its-revenue-shift/). Instead of paying to get to play the game, gamers get free access but have to pay for additional in-game content (e.g. items, abilities or upgrades). Fortnite has an estimated 250 million players, who spent $84.67 on average for additional content. In 2018, the game earned $2.4 billion (https://www.businessofapps.com/data/fortnite-statistics/).

'Centralised' means that a single administrator (the developer) controls the system and determines its rules and procedures. However, the FATF views non-convertible virtual currencies as 'not necessarily static' since they can be exchanged on unofficial, parallel secondary markets[44]. As a result, previously non-convertible virtual currencies such as in-game currencies and items become convertible and have real value.

Popular games such as Fortnite, Call of Duty, Counter-Strike and Overwatch are ideal targets for money laundering. All have large player-bases, enable easy trading of in-game currencies and high-value items, and have robust secondary online markets for these assets, making them easily transferable into fiat currency.

Recent reports document the use of gaming for money laundering. In 2018, Valve (Steam) declared that almost all of the micro-transactions carried out in the very popular Counter-Strike Global Offensive game were part of money laundering operations, while in the same year research suggested that criminals across the world abused Fortnite's virtual economic system[45]. In this context, a standard method to launder money works as follows: a criminal purchases in-game currency/item (e.g. WoW gold) with a pre-paid or stolen card. He or she then sells the in-game currency/item via a third-party platform, often at prices below market value to attract customers[46]. As a result, the money used (fiat currency or cryptocurrency) is 'cleaned' and transferred to the criminal's bank account or virtual wallet. Neither the seller nor the buyer is ever even aware of the other's identity. This is made even more effective if the purchase and sale of in-game currencies is performed using cryptocurrencies (e.g. Bitcoin), or when multiple accounts are used for micro-laundering purposes (thus avoiding the attention of game moderators, law enforcement officials or financial institutions, so that no suspicious activity reports (SARs) are submitted). Other popular methods of laundering money include the abuse of so-called 'loot boxes' and convertible in-game currencies[47].

[44] In-game currencies and items are resold on third party fora (e.g. Ebay, specialised websites, and the Dark Web).
[45] The Independent revealed, with the help of cybersecurity company Sixgill, that criminals were using Fortnite and its V-bucks to launder 'dirty money'.
[46] Anton Moiseienko, Kayla Izenman (2019), 'Gaming the System: Money Laundering Through Online Games', RUSI Newsbrief, Centre for Financial Crime and Security Studies, AML/CTF.
[47] Loot boxes contain a random assortment of weapons and skins, both valuable and not, that a player can obtain during matches with other players. To open loot boxes, players first must buy a key using real money. Loot boxes and keys can be traded between players in the **Steam marketplace**, one of the largest online gaming retailers. Criminals will use illegal funds to acquire them and trade them with other accounts. A criminal may launder its illicitly obtained money through a game that utilises convertible in-game currency by creating numerous separate accounts using fictitious IDs and funding those accounts with his/her money.

It is difficult to estimate the amount of money that is laundered through video games every year[48]. According to experts, it may be rather limited, as money launderers prefer microtransactions to avoid the suspicion of the developer[49]. Although the amount of money laundered through video games currently represents only a small fraction of the estimated total of USD 1.5 trillion laundered every year, the growing popularity of gaming could make video games a more significant laundering tool in the future[50].

In the past, successful counterterrorism finance measures have reduced terrorists' access to fiat currencies. Terrorists may, as a result, increasingly decide to use virtual currencies to sustain their activities. So far there have been a few instances of jihadist and right-wing violent extremist and terrorist groups using virtual currencies for financing (e.g. Bitcoin fundraising by Hamas in 2019[51]). However, there is no evidence that terrorist groups have used online gaming platforms for their financial transactions and it seems that more conventional forms of financing (e.g. cash) still predominate. More generally, the insufficiently-regulated gaming economies offer potential for future abuse by terrorists, who could transfer and withdraw money almost untraceably.

In short, video game currencies are not very different from cryptocurrencies, apart from the fact that in-game currencies can be more easily confiscated. As there is little qualitative difference between them, however, in-game currencies pose near-identical risks in terms of money laundering to their cryptographic equivalents. Moreover, while the CFT (countering the financing of terrorism), UBO (ultimate beneficial owner), and AML (anti-money laundering) regulations have progressed in scope, **money laundering through video gaming remains unaddressed and could therefore gain significantly in popularity.**

[48] It is difficult to know how popular this method of laundering really is. A methodology employed by an expert relied on combing through popular hacker fora searching for certain key terms. His findings showed that hackers had, according to their own testimony, laundered money in this way. He was, however, unable to quantify the amount. https://www.pcgamer.com/how-microtransactions-and-in-game-currencies-can-be-used-to-launder-money/.
[49] Siggia, S. (2020, January 21). Online Video Games: Regulatory Overview. https://www.acamstoday.org/online-video-games-regulatory-overview.
[50] Although it is difficult to assess the amount of money laundered through video games, the cybersecurity firm Sixgill established that the popular online game Fortnite had become a money-laundering haven. Sixgill observed that in two months, on eBay alone, more than EUR 283 000 euros of virtual items had been exchanged to launder money. https://www.numerama.com/business/456880-comment-fortnite-serait-utilise-pour-blanchir-de-largent.html.
[51] During an online fundraising campaign carried out in January 2019, the armed wing of Hamas asked its supporters to make donations through the digital currency Bitcoin via a two-minute video on the al-Qassam Brigades website, which showed step-by-step instructions in Arabic for avoiding the traditional financial system and donating cryptocurrency. https://www.reuters.com/article/us-crypto-currencies-hamas/hamas-shifts-tactics-in-bitcoin-fundraising-highlighting-crypto-risks-research-idUSKCN1S20FA

II. CURRENT REGULATORY ENVIRONMENT, VOLUNTARY ENGAGEMENT AND LAW ENFORCEMENT AND JUDICIAL CHALLENGES

Online games have not yet been a focus for EU counter-terrorism policies, so gaming operators may not be strongly engaged in fighting terrorist abuse. At the same time, certain aspects of the long-overlooked gaming sector are raising challenges for law enforcement and judicial authorities.

1. Content propagation, radicalisation and recruitment have not yet been the subject of dialogue between the EU and the gaming industry, and the online gaming sector has so far not been involved in voluntary cooperation through the EU Internet Forum, on the basis of which specific major hosting service providers (HSPs)[52] have already committed to detect and remove violent and terrorist content on their platforms[53]. While some of the providers participating in the Forum also play an important role in the gaming industry (e.g. Microsoft, Apple and Amazon), the largest gaming companies (such as Sony, Valve and Discord) are still absent from it.

In June 2020, representatives from the SIRIUS Project[54] team within the EU IRU participated in the meeting of the Games Network Roundtable, organized by the UK National Crime Agency (NCA). This outreach activity represents an initial step in the engagement with over 20 companies in the games sector industry.

[52] According to the draft proposal, a HSP is a 'provider of information society services consisting in the storage of information provided by and at the request of the content provider and in making the information stored available to third parties'.
[53] After the terrorist attack in Christchurch, New Zealand launched the Christchurch Call for Action initiative which brought together government leaders and online platforms. Following this initiative, the Commission established an EU Crisis Protocol connected to the EU Internet Forum. Its goal is to enable Member States and online platforms to act rapidly and in a coordinated way to prevent the spread of terrorist content online in the event of a terrorist attack.
[54] Europol created the SIRIUS project - spearheaded by Europol's European Counter-Terrorism Centre and European Cybercrime Centre, in close partnership with Eurojust and the European Judicial Network - in October 2017 as a response to the increasing need of the law enforcement community to access electronic evidence for internet-based investigation. It aims to help investigators cope with the complexity and the volume of information in a rapidly changing online environment, by providing guidelines on specific OSPs and investigative tools; and sharing experiences with peers, both online and in person, to make the process for data requests faster and more effective. The knowledge products developed in the framework of the SIRIUS Project are disseminated via the restricted SIRIUS page on the Europol Platform for Experts, which counts with over 4200 users from all EU Member States.

In order to create a clear and harmonised legal framework to address the spread of terrorist content online, the Commission submitted a proposal for a Regulation in September 2018, which would oblige HSPs to take additional measures and to cooperate more closely with Member State authorities on combating terrorist content online. The scope of the definition of HSPs, as phrased in the Commission proposal, would also include **certain major online gaming platforms (e.g. Playstation Network, Xbox live and Steam)**. Thus, many of the above-mentioned, online-gaming-related actions that can incite terrorism would fall under the scope of 'terrorist content online'; this may help close a regulatory gap relating to terrorist risks resulting from online gaming platforms. However, certain gaming communication services, such as in-game chats, would not fall within the scope of the Regulation.

Illegal hate speech on online gaming platforms should be another priority, since the line between illegal terrorist content and illegal hate speech can be fluid, and the two types of comment are often found together. In May 2016, the Commission launched the Code of Conduct to counter illegal hate speech online. Several IT companies signed this code and strengthened their precautions in this area[55]. As the only representative from the gaming sector, Microsoft participated in the initiative with its gaming services Xbox Live and Mixer, a live-streaming app. Thanks to improved human moderation of hate speech in chats and forums, over 20 million pieces of content were removed from these two platforms in 2019 alone[56].

The vast majority of online gaming platforms have their own terms of service, rules and community standards which, in theory, ban violent and extremist speech. However, gaming companies' practices regarding removal and enforcement remain very variable and opaque, and they do not prevent violations comprehensively. The identification of illegal content represents a technical challenge, as hundreds of millions of players, using several different languages, use platforms such as Xbox Live, PlayStation Network and Steam every month. Therefore, closer and sustained dialogue and cooperation between government and the gaming industry will be essential in the future. Enforcement measures could also be explored.

[55] All IT companies who signed the Code now have terms of service, rules or community standards prohibiting users from posting content inciting violence or hatred against protected groups. They have also significantly increased the number of employees monitoring and reviewing the content.
[56] INFORMATION NOTE - Assessment of the Code of Conduct on Hate Speech online - State of Play - European Commission - Brussels, 27 September 2019

The gaming industry needs to recognise the importance of this issue and adopt a more comprehensive and proactive strategy, which could, for example, include new and robust analytical tools, more precise guidelines for platforms, and other proactive measures (e.g. monitoring suspicious changes in gaming patterns and reporting them, where necessary, to the authorities).

2. Another challenge for law enforcement and judicial authorities concerns access to in-game communication data, which are commonly encrypted. In the absence of EU-wide legislation on encryption and cross-border access to e-evidence, access to this data still represents a challenge for law enforcement. Investigators rely on cooperation with the gaming developer in order to obtain the evidence needed to prosecute and convict terrorists. In particular in cases of non-cooperation special investigation techniques are also relevant.
It is important to know to what extent authorities have focused on online gaming communication channels. So it would be helpful compate the different approaches that law enforcement and judicial authorities in the Member States have adopted towards online gaming, obtaining evidence and related challenges, including encryption.

3. As regards money laundering and terrorist financing, the EU has not focused so far on screening of in-game economic transactions[57]**. The Fifth AMLD excludes in-game virtual currencies that can only be used in a specific gaming environment.** According to the current EU definition, virtual currencies are 'digital representations of value' which are accepted as a means of exchange by natural or legal persons and which can be transferred, stored and exchanged electronically[58]. **The Fifth AMLD** also regulates providers engaged in services enabling exchange between virtual currencies and fiat currencies, as well as custodian wallet providers[59]. Certain convertible in-game currencies, i.e. those (like the Linden Dollar) that can be exchanged for fiat currency, could therefore fall within the scope of this Directive.

[57] The monitoring has been limited to issues such as gambling. Some regulators in Member States tackled 'loot boxes' that are sold in video games as they can be considered as a form of gambling. After investing real funds, players get the opportunity to randomly win in-game items, which can be seen as a form of gambling.
[58] The Fifth Anti-Money Laundering Directive (AMLD5) considers that 'virtual currencies' represent a digital representation of value that is not issued or guaranteed by a central bank or a public authority. Therefore, it is not attached to a legally-established currency and does not possess the legal status of a currency or money.
[59] Entity providing services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies.

In comparison, the definitions of virtual assets[60] and virtual asset service providers in the FATF standards (adopted in June 2019) are more extensive.

The question remains as to whether in-game currencies that are traded on unofficial secondary markets should also be considered as virtual currencies as they are de facto convertible. Online gaming platforms should, as a whole category, be considered as, and therefore regulated like virtual asset service providers[61] (VASPs) since they enable trading in *de facto* convertible in-game currencies.

So far, game developers have self-regulated and punishments have taken the form of bans, but with no legal consequences. Considering the success of video games and current forecasts, it appears likely that money laundering through these channels will gain in popularity. Gaming operators should be encouraged to take more responsibility and additional measures. As the AML policies are not applicable, the authorities are currently entirely dependent on operators' voluntary cooperation. So given the observed, increased threat of money laundering in video games, it would be important to make this sector comply with AML standards. An extension of the current EU legal framework on AML/CTF should therefore be envisaged.

III. RECOMMENDATIONS

1. Engage with gaming platforms, video game live-streaming services and gaming apps in the EU Internet Forum (EUIF)

The nexus between **online gaming and terrorism should be addressed in the context of the EUIF**. The EU should engage the main gaming platforms like Valve corporation (Steam), Sony, Microsoft, Nintendo and Apple, as well as video game live-streaming services like Amazon (Twitch), Facebook and YouTube and gaming communication apps (Discord) in a dialogue.

[60] Virtual assets (FATF glossary) are a digital representation of value that can be digitally traded or transferred, and can be used for payment or investment purposes, and that does not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.
[61] According to the FATF, a '*Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i. exchange between virtual assets and fiat currencies; ii. exchange between one or more forms of virtual assets; iii. transfer of virtual assets; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset*'.

This would enable a comprehensive assessment of terrorist abuse of online gaming and assist the development of new strategies and measures to prevent abuse. The objectives should be to step up voluntary cooperation and increase the accountability of companies providing e-gaming.

The EU should also **address the presence of illegal hate speech on gaming platforms** with gaming companies. Ideally this could happen in one combined dialogue with the gaming platforms.

Companies should be invited to communicate their strategies and the measures (AI tools, reporting mechanisms, etc.) they are implementing with respect to terrorist content online, illegal hate speech and terrorist financing.

The EU IRU is well placed to support these public-private partnership efforts, including with analysis, and to promote outreach activities to companies in the industry, raise their awareness in relation to the abuse of their services and to provide them the relevant support to tackle such issues.

Finally, the gaming community should be more involved in the fight against terrorist abuse of online gaming. It would be necessary to launch an **awareness campaign among gamers** and to promote the use of reporting mechanisms.

2. Set up a technical dialogue between experts on law enforcement and judicial challenges relating to online gaming

Technical issues for law enforcement need to be further examined, including in-game communication and encryption, and potential related difficulties with regard to lawful access to data, including interception. While Europol and Eurojust could facilitate such an EU internal dialogue with law enforcement and judicial authorities from the Member States, for example in the context of the existing exchanges on encryption, **technical exchanges with the e-gaming industry would also be important**. Exchanges among EU law enforcement regarding special investigation techniques related to gaming could also be considered.

Through the SIRIUS Project, the EU IRU will continue to support EU law enforcement in the process to request cross-border access to electronic evidence from gaming companies as to allow the investigation and prosecution of crimes facilitated by the abuse of these platforms.

The **EU IRU intends to develop tailored guidelines and training modules for law enforcement and judicial authorities**[62]**, focusing on lawful access to electronic data from gaming companies.** This will follow an approach already in place with companies in other sectors and provide relevant information to support Member States authorities to submit cross-border data disclosure requests[63].

3. Examine further trends and issues with regard to online gaming and terrorism

It would be useful for INTCEN and Europol through its Innovation Hub and the EU IRU, as well as the Commission through the Radicalisation Awareness Network (RAN)[64], to further **examine the extent of terrorist presence and use of online gaming for radicalisation and recruitment purposes**. The available data is limited in this area, so additional knowledge would be very valuable in the fight against terrorist abuse of online gaming. The EU IRU will continue to share its findings on these issues with Member States and the Commission as part of its commitment to the EUIF.

In this context, a first exploratory RAN meeting in the autumn 2020 will bring together communication experts, youth/exit workers, industry representatives, researchers and law enforcement/police officers to further examine how violent extremists use video-gaming platforms to radicalise and recruit new members.

In addition, the Commission could **launch research** to assess the impact of violent video games on terrorist activities in the broader sense (e.g. desensitisation to violence, combat training, sympathy with terrorists, and use of AR and VR games for combat training purposes) under its Horizon 2020/Horizon Europe research and innovation programme, the Internal Security Fund or other relevant instruments. The trend of 'gamification' of terrorism and the resulting implications (e.g. for radicalisation and recruitment) should also be examined in more depth.

[62] In the context of the SIRIUS Project and in partnership with Eurojust
[63] For instance, guidelines and training material will include information in relation to the datasets that are collected by each specific company, contact details of the legal entities that control such data, specific requirements of each company in relation to governmental requests and other relevant best practices in this regard.
[64] The RAN factbook of October 2019 on far right extremism, which mentions gaming - https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/ran_fre_factbook_20191205_en.pdf

4. Assess AML/CFT risks in relation to online gaming and explore measures

In its **next report** on the risk of money laundering and terrorist financing affecting the internal market and cross-border activities, the **Commission could assess the risks of money laundering and terrorist financing in the context of online gaming**. This should enable the identification of existing weaknesses and measures to address them.

Since money laundering via gaming involves global-scale activities, exchanges with key international partners such as the USA are also important. Furthermore, the EU should align its AML/CTF legislation with the FATF standards on virtual assets. In that context, the Commission could review the current AML/CTF framework and assess ways to tackle more effectively the challenges posed by in-game currencies and by gaming platforms that operate as **virtual asset service providers.** In that context, exchanges with Member States and private actors from the industry would be valuable.

5. Policy discussion

Given the wide range of terrorist abuses that are enabled by online gaming (radicalisation and recruitment, money laundering and terrorist financing, as well as encrypted communications), it would be useful for further discussions on this issue to take place in the relevant Council preparatory bodies, such as the Working Party on Terrorism (TWP).