Hadtudományi Szemle
15. évfolyam (2022) 3. szám 183–195. • DOI: 10.32563/hsz.2022.3.12

József Sáfrán[1]

Digital Terrorism: Communication through Online Video Games

Abstract

We interact nowadays through the internet in many different ways, we are socially connected to this network. Of course, this has its dangers, as many individuals or groups operating illegally also have access to these opportunities and use them to support their own activities. Online gaming is based on the hobby of many people including terrorists: to connect and play together online. In the world of online video games, there have been several cases of terrorists or organised criminal group members using data game software to achieve their own ends. Therefore, defence organisations have been monitoring this unconventional world for more than a decade. It is worth examining exactly how terrorist organisations can exploit this form of entertainment. The information society has brought with it a proliferation of video games, which has led to a significant acceleration in communication.

This study examines how different terrorist organisations or organised criminal groups use online video games to communicate. We will examine how they can exchange information, organise different activities, disseminate their propaganda and recruit. This article focuses on video games that can be played online and are mainly publicly available, as these are the programs that can be quickly accessed by the web and many other players. We are not dealing with games with single player only mode, as it would require a completely different way of analysis, and in online video games the communication factor is one of the primary factors in their use.

Keywords: *video games, online jihad, online gaming, ISIS, terrorism*

[1] Research assistant, University of Public Service Lőrincz Lajos Department of Administrative Law, e-mail: safran.jozsef@uni-nke.hu

1. Introduction

The internet is no longer just a technology, but a social phenomenon that has given rise to a multitude of genres that are different from the usual forms of communication and opportunities. The wealth of possibilities is nowadays the reality and medium through which significant social interactions and identity formation take place at its layers.[2] For this reason, the processes of comprehensive and cognitive communication cannot be left out of the virtual space, including the sector of online video games.[3] From a functional perspective, it is worth examining how terrorist organisations (and sometimes the organised crime groups) are able to use online video game communication at a theoretical level and what cases we know of where it has been used in practice.

The essence of online video games is that players can play with or against each other over the internet and engage in various interactions. There are many ways to communicate during games: written, verbal or non-verbal messages.[4] Each communication type has its own advantages and disadvantages, and the ways in which it can be used may vary from platform to platform.[5] Interpersonal communication can take many forms in a given piece of software, and the more signalling it includes, the more colourful and meaningful the communication.[6] It is important to highlight again that communication is an essential, central part of the online video games.

The aim of this study is to present the communication possibilities of different groups and individuals that pose a threat to security in the online gaming space. In my research, I will analyse only software that can be played online, and I will not analyse games with a single player only mode, as this analysis would require a completely different approach, and the communication factor is not the primary factor in their use. The relationship between terrorist and extremist groups within online video games through communication is the subject of my study. Research on the relationship between video games and criminal groups is still evolving, most research comes from the United States of America.[7] These studies mostly focus on the behaviour of violent extremists in cyberspace and the rise of digital terrorism.

[2] Steven L. Thorne – Ingrid Fischer: Online Gaming as Sociable Media. *ALSIC: Apprentissage des Langues et Systèmes d'Information et de Communication,* 15, no. 1 (2012).

[3] We distinguish between multiplayer games and online video games. Multiplayer games are video games that allow more than one players to join in – although they can also include a single-player mode. This can be done locally, on a single machine, connected to a local network or over the internet. Online video games can also be multiplayer games, but only over the internet, or only with multiplayer functionality available or included in the options. For the purposes of our analysis, the study of online video games is our primary interest, as it is important for terrorist organisations to use them to conduct their communications covertly, hidden and over distance.

[4] Non-verbal messages are mostly game-specific. The most common are emojis, which can be pictures expressing moods, states, moving images, videos (e.g. League of Legends, DOTA2). It is also possible to express a message with the character itself, using different postures and facial expressions (e.g. Dark Souls series, Fortnite).

[5] Anton Westerlund: *Using Video Communication in Online Multiplayer Games. The effects of adding a video chat overlay on the game experience in online multiplayer video games – a quasi-experimental design.* Linnaeus University, Bachelor Thesis in Media Technology, 2021. 4–5.

[6] Westerlund: op. cit.

[7] Maura Conway: Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research. *Studies in Conflict and Terrorism,* 40, no. 1 (2017). 77–98.

The article will demonstrate that terrorists can use these areas, which are less focused on by defence services, for information exchange, either overtly or covertly. Beyond these basic aspects, the possibilities for recruitment and propaganda will be presented. The article will describe the security implications and dangers of communication within online video games, and open a space for dialogue on this less studied but important area for the future information society. For this reason, it also deals with possible data collection for national security services. The focus of the research will not be on games made by extremist groups for specific communication, propaganda or training purposes, as these require separate investigation, but on popular, widely accessible programmes made by profit-oriented companies.

2. Forms of communication in online video games

The communication environment provided by online video games enables a unique social interaction between users. Like online chat rooms, online video games provide a social space for similar individuals to form friendships and close relationships that can be exploited by terrorist organisations. Online video games thus contribute to internet-based social opportunities, while much of it is well documented.[8]

We distinguish between internal and external means of communication, as well as written or voice-based forms of communication. The focus of this study is on game software that is accessible to the general public and is not designed for a specific purpose, such as propaganda or training.

Within online video games, one way of communicating is through written chat. This is especially common for games played on a computer, laptop or mobile phone, as games on consoles are usually played with a controller (although Nintendo Switch in handheld mode is somewhat capable of touch typing) and it is more distracting than slow typing (using a touchpad or pressing letters and numbers on the screen). This detracts from the gaming experience and distracts attention, and it is less common on consoles than on devices with a keyboard that allow much faster typing.[9] Most games include an open chat room for everyone, as well as smaller rooms for specific communities, clans, guilds, etc., and the possibility to chat privately.

An increasingly popular communication channel is voice over internet protocol (VoIP), which is built into games. VoIP uses computer networks, along with the global internet, to transmit digitised voice messages. In a study, Caplan Williams and his colleagues investigated how voice communication in online video games strengthens the relationship and trust between players. They found that the added verbal cues eliminate anonymity and add depth and openness to the conversation, which can bring participants closer together. Therefore, VoIP communication allows for a higher

[8] Malcolm R. Parks – Kory Floyd: Making Friends in Cyberspace. *Journal of Computer-Mediated Communication,* 1, no. 4 (1996). 80–97.

[9] Xiaofei Lu: Automatic Measurement of Syntactic Complexity in Child Language Acquisition. *International Journal of Corpus Linguistics,* 14, no. 1 (2009). 3–28.

quality game between people playing cooperatively or against each other.[10] In games, not only can verbal communication take place between two people, but they can also form guilds or rooms where they can talk to several people at the same time. Of course, some software does not link communication between several individuals to guilds, it is possible to interact with each other in the game by means of a pool, so communication can be initiated directly or random. When entering multiplayer rooms, it is important that they are simple and easy to use, so as many users as possible can make contact in them. Thanks to fast servers and search algorithms, the ability to quickly play and collaborate with others to achieve a common goal has evolved.

Sony released an update for PlayStation 4 in 2015 that allowed text to be converted to sound (read aloud), buttons to be rearranged and a larger font. The Tobii eye-tracking peripheral allows you to control what happens on the screen by moving your eyes. All of these examples show us that the possibility has been further increased for more people to play the game the way they want, increasing the community in all directions.[11]

A lot of research has been done on how the proportion of players is distributed. We can see that there is now a minimal gender gap, with almost as many women as men. Thanks to the internet, people often come into contact with people from other countries, build relationships, understand each other better and even develop sympathy for each other, which some groups are able to use to their advantage.[12]

3. Security monitoring opportunities

Online video games are extremely complex and – although they have been present in the entertainment industry since 1980 – a huge business, but often marginalised as a specific product of the media. However, it is an undeniable fact that video game entertainment is becoming less of a stratified activity, thanks in large part to the proliferation of mobile games. Moore's law says that the number of online virtual spaces doubles every two years. The number of virtual gamers is estimated to be at least 10 million a day, many of them playing up to 30 hours a week. The growth of digital games has followed this strong interest, with developers now writing programs in virtually every style and genre.[13] One of the most popular of these online games is World of Warcraft (WoW), the first online video game to have been specifically monitored by the national security services (as far as we know now from public documents). WoW is a Massively Multiplayer Online Role-Playing Game (MMORPG), and also a very complex game in which success can only be achieved by cooperating with others. What makes it different from other video games, apart from the cooperative aspect, is that it is explicitly based on teamwork or interaction with other

[10] Dmitri Williams – Scott Caplan – Li Xiong: Can You Hear Me Now? The Impact of Voice in an Online Gaming Community. *Human Communication Research,* 33, no. 4 (2007). 427–449.

[11] Stanley Pierre-Louis – Susanna Pollack: Video Games Are Transforming How We Communicate with Each Other – And They Could Fix a Range of Other Global Issues too. *World Economic Forum,* 10 December 2019.

[12] Entertainment Software Association: *2019 Essential Facts About the Computer and Video Game Industry.*

[13] Julie M. Sykes – Jonathon Reinhardt – Steven L. Thorne: Multiplayer Digital Games as Sites for Research and Practice. In Francis M. Hult (ed.): *Directions and Prospects for Educational Linguistics.* New York, Springer, 2010. 117–135.

users. Communication can take place through text, voice and non-verbal means.[14] Our information about the monitoring comes from documents leaked by Edward Snowden in 2013: the first activity dates back to 2007, when the National Security Agency (NSA), Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI) and other intelligence agencies started analysing and processing communications on WoW and Microsoft's Xbox Live. NSA agents investigated suspicious elements in the Games and Virtual Enviroment (GVE), as intelligence sources claimed that al-Qaeda fighters were using the game for propaganda, recruitment, training and communication. From the virtual world, intelligence agents were able to retrieve not only chat logs, but also the targets' friendship lists, guildmates, geographical locations and personal data. With this information, the hackers were able to plant spyware on the appropriate computers. WoW was run over the internet, specifically on Battle.net servers, communicating with computers in different locations, making it easy to map. The Government Communication Headquarters (GCHQ), in partnership with the NSA, attempted to integrate mapping modules into the World of Warcraft and Xbox Live servers, and the integration was completed by February 2008. The main targets were terrorists, but they did not want to ignore the new games that were coming out. It can be concluded that HUMINT has become part of the constant presence, information gathering, analysis and processing in virtual games. The intelligence community of the United States developed methods and strategies for collaboration. Looking at Snowden's documents, we know of one successful operation in 2008: in this specific case a website was discovered where stolen credit card details were being traded.[15] After the WoW incident, gaming companies started to collaborate much more with the national security agencies, but this did not mean that everything could be checked fully. The easiest part of backtracking is to check the chat logs in a game, but the terrorists also know this, thus they are trying to find new or mixed methods, and to not stay for too long in the same "internet location". The other problem is that even if an agency has the name or internet history of a terrorist, it is still difficult to monitor the traffic. In a shooting game, for example, terrorists can shoot at the wall and form letters from the bullet holes left behind to send a message to the person they are playing with.

4. Technical aspects of encrypting communications on personal computers and consoles

In the aftermath of 13 November 2015, the world was shocked by the terrorist attack on Paris, planned and carried out by ISIS, which claimed 127 lives and injured more than 300 people. It was initially suspected that the terrorists may have communicated with each other using PlayStation 4 devices. The Belgian Interior Minister Jan Jambon said in an interview that it was very difficult for their services to decode

[14] T. L. Taylor: *Play Between Worlds: Exploring Online Game Culture.* Cambridge, Mass., The MIT Press, 2006.
[15] Kyle Orland: Snowden Leak Examines Gaming as a Terrorist Propaganda and Training Tool. *Ars Technica,* 12 September 2013.

communications via the PlayStation 4.[16] The PS4 voice communication software was the primary suspect in the terrorist attack. It uses IP-based voice technology, which was relatively difficult to trace.[17] The U.S. media jumped on the Sony PlayStation case for a few days. In the end, Sony was not prosecuted in the case because it could not be proven to have been one of the perpetrators of the attacks. In fact, the terrorists only communicated with each other using disposable phones. The perpetrators were in fact using disposable phones, but the vulnerability of the consoles and their use by terrorists immediately attracted even more media and national security attention.

The protection of the PlayStation 4 was very good, but it was almost impossible for most of the high-tech national security services to hack it. The PS4 uses the Transport Layer Security (TLS) protocol, which uses symmetric encryption (AE256-CBC) and 2048-bit asymmetric (RSA) encryption keys, which most experts believe one of the best encryption systems in the world. The PS4, on the other hand, uses three suboptimal encryption settings, which could be described as a gap in its security, as it allows either national security organisations or terrorist organisations to successfully hack into it. Until recently, PlayStation used TLS version 1.0 instead of the more secure 1.2, which was considered secure but also crackable. The certificates used by PS4 are old and used SHA-1. Larger services, and groups with more substantial financial backing, could easily break it if they forced a hash collision. Thanks to this, they can even intercept conversations and read messages. Another problem is that double-encryption techniques, although supported by Sony's cloud system, are not supported by the console itself. It also works extremely well against national security services and other criminals. Thus, agencies with extensive surveillance powers, if they were to record all PS4 chats today, could decrypt the text of the messages in the future if they were able to obtain Sony's secret key (either through a court order or through coercion).[18] As can be seen from the above, although the PS4 of a generation ago was relatively well protected, it was far from perfect. However, it can be said that investing in hacking is probably not worthwhile for terrorists, either individually or as a group, as it is much cheaper and they can use it for activities that are more useful from their point of view.

The PlayStation 5, which has been released in 2020, is no exception to the number of consoles that ethical hackers have tried to hack since its release. In November 2020, the Fail0verflow hacking team successfully obtained not only all the root keys for the PS5, but also for the other new generation consoles. The root keys are symmetric and can be encrypted and decrypted. The root key for the set-top box requires special hardware, according to expert engineers, but the hacking team has denied this and claims that the data was obtained solely through software. This allows them to access almost anything inside the state-of-the-art and supposedly better encrypted console, a cautionary tale that threats are not only present on computers in the classic

[16] Alan Hope: Brussels Is 'Weakest Link' in Europe's Fight against Terrorism. *The Bulletin,* 13 November 2015.

[17] Nate Anderson: CSI: Xbox – How Cops Perform Xbox Live Stakeouts and Console Searches. *Ars Technica,* 01 October 2012.

[18] David Holmes: Paris Attacks: What kind of Encryption Does the PlayStation 4 Use, Anyway? *Security Week,* 09 December 2015.

way.[19] Other terrorist organisations will eventually be able to decrypt the PlayStation 5 firmware, which will open up possibilities for them to install third-party software (e.g. encryption, cloaking) or run other additional services. There have already been examples of jailbreaking games on rival console Microsoft's Xbox 360. Hackers were able to flash the console without much difficulty and then copy the games obtained from pirated sources to disk. This allowed various organisations to make huge profits on the black market, while Microsoft was put at a disadvantage.[20]

The year 2014 marked a turning point in the history of online video games and jihad, when the Islamic State began an intensive online campaign. The intense operations, known as cyber warfare, evolved into a new type of challenge with huge backing from professional individuals and groups. The use of entertainment software as supporting software for games has different elements than the activities of the late 2000s.

Although they started making AAA games instead because they realised they were being watched, it is unlikely that they have stopped, but they are spreading propaganda very much through modding. Direct propaganda has been transformed into their own, mainly by modding games, which makes it easier and more covert for terrorist organisations to get on their side and train.

One of the most active online organisations is the Islamic State. They have stolen the code of a lot of existing game software and modified it to their liking. Not only do they have a large active membership, but also a large number of cyber proxies, mainly working on social media and trying to lure users into games. They continue to communicate mainly in the products of game manufacturers, as their financial resources do not allow them to write programs of the quality of the leading game development companies in the world. Of course, they have their own development, but the quality and seriousness of their work does not even approach that of the world's leading developers. According to some reports, they have no intention of developing anything other than the aforementioned mods or lower quality games of their own, as this is extremely time-consuming and costly.[21]

5. Methods of use that compromise safety

The U.S. Department of Homeland Security has long been concerned about the dangers posed by online video games. The interaction that takes place in them has not escaped their attention, and they have identified three ways in which terrorist groups are trying to radicalise mainly young users:

[19] Interestingly, although with reservations, the Fail0verflow team said that consoles are no longer worth hacking as they are almost identical in functionality to desktop computers. The statement may mainly refer to the financial gain mentioned in the article, but when considering the potential for any criminal on the internet to choose the least conventional and conspicuous solution to achieve their goals we may have doubts. For more information see Aroged: Fail0verflow Hackers Hinted at Hacking the Playstation 5 Encryption System. *Aroged,* 08 November 2021.

[20] Derek Black: Hacker Obtained PS5 Encryption Keys that Will Allow Pirating Games. *World Stock Market,* 08 November 2021.

[21] Miron Lakomy: Let's Play a Video Game: *Jihadi* Propaganda in the World of Electronic Entertainment. *Studies in Conflict and Terrorism,* 42, no. 4 (2017). 383–406.

They look for groups where people are present for fun, and they approach them pretending to have a common interest.

They look out for individual users who may be lost in real life, looking for their place, their company and a community to belong to.

They look out for people who are looking for information about heritage, traditions or ideologies associated with a particular radical group within video games, or who have a visible interest.[22]

Terrorist propaganda and recruitment activities actively target users in the ways listed. When targeting individuals who are susceptible to their ideology and marginalised, playing video games can exploit their weaknesses, their loneliness, their need to belong. To do this, they specifically segregate gender, social groups, age groups or ethnicities. Their hacking activities are not negligible either, as they are able to covertly enter games and download chat logs of individual players, which they can use to analyse the person, assess their network of contacts and plan their next steps. Although the proportion of the sexes playing video games is levelling out, in general, terrorists still target young men, who prefer more violent and shooter games. Psychological reasons for this include the desire to have similar experiences, the conversion of real-life failures into success in the virtual space, the desire for power and fame, and possibly an interest in learning about the real environment of combat. These can be complemented by stress relief, anger release or a desire to do something for society.[23] The exploitation of real or perceived negative experiences[24] by teenagers makes it even more dangerous for terrorists to find a weakness. The creation of their own games is also a major trend in this direction. Identification with violent games has led ISIS to produce similar programmes, which are popular not only with young people of the Muslim faith but also with other children, so producing such games and diverting them from other games can boost their recruitment.[25]

6. Terrorist and criminal groups exploit video game players

For the purposes of our topic, it is important to note that various terrorist organisations also produce their own video games in their backyard. These mainly target teenagers and young adults. For example, Hezbollah has tried to promote and legitimise the war against Israel, especially among gamers in Europe and North America, with its Special Force and Special Force 2 games. There is also the Quest for Bush game, which is linked to al-Qaeda, and in a children's game the ultimate goal is to kill President George W. Bush. The Night of Bush Capturing has the same objective, but the latter game focuses specifically on the online, cooperative part and is aimed more at children themselves, who are growing up in the terrorist "spirit". These games also offer young generations the chance to try out what it feels like to follow the aims of a different ideology by taking on the role of a terrorist. In their own games, they can use forums,

[22] Department of Homeland Security: *Strategic Framework for Countering Terrorism and Targeted Violence.* 2019.
[23] Matthew Hall: This Is Our Call of Duty: How ISIS Is Using Video Games. *Salon,* 01 November 2014.
[24] The phenomenon known as cyberbullying only reinforces this trend.
[25] Ahmed Al-Rawi: Video Games, Terrorism, and ISIS's Jihad 3.0. *Terrorism and Political Violence,* 30, no. 4 (2016). 745.

chat rooms and other communication channels even more freely. These sites make it easier for curious young people to get their political or ideological questions asked, to put their views against each other. Anonymity is also preserved, we are talking about programmes with a lot of professional protection, which can be a challenge even for national security services. We have seen repeated examples, particularly for recruitment in Iraqi areas, of people switching to private email or chat after time spent in the game, perhaps even meeting in person. After meeting in person – this can happen also in small groups – they can talk about politics more explicitly.[26] Terrorist organisations profile their ideal candidate in a similar way to national security services. Games can provide information on the "candidate's" Arabic language skills and knowledge of Islamic teachings. In particular, the best candidates are sought out in a hurry outside the games, as it is in their vital interest to have them join up as quickly as possible.[27] But it is not only terrorist organisations that have discovered cheap and relatively protected recruitment opportunities: according to several U.S. reports, Mexican drug cartels (especially the Sinaloa Cartel) are targeting young people (mostly aged between 11 and 14) on online platforms, asking them to perform small tasks – such as smuggling drugs, equipment and money – in exchange for a few hundred dollars. In one case, a man named George offered to a young player 2,000 dollars to bring 60 kg metamphetamine through the Mexican border in Arizona. They had met in Grand Theft Auto Online, and after a couple of games and chats they started to meet personally in Phoenix, and also started to talk on Snapchat.[28] Another case took place in the game Free Fire, where scouts were recruited for the northern border of Mexico. Several cartels are also reported to operate and recruit through Call of Duty, Gears of War and Grand Theft Auto V. In several cases, the recruiters have taken advantage of the victims' armed and violent nature, mainly consisting of young boys. They were promised that they would get guns and do things like in the games, only they would earn money additionally. The duped youngsters were then given fake tickets to their destinations. The percentage of recruitment in Mexico that takes place in online games remains a mystery. Another problem could be that the children who are lured are themselves spreading the propaganda to their fellow children. The above case also shows that the cartels are directly targeting children in the online space.[29]

Internet propaganda and marketing play a major role in the psychological development and socialisation of children, who may be more easily persuaded to commit violent acts or suicide bombings as adults. In addition to video games, online videos, books and newspapers are also known to be used as vehicles. They are trying to get children out of the world of online games, which are not controlled by terrorist organisations, as soon as possible and into platforms they control themselves. These are usually interactive sites, forums or monitored chat rooms where they can communicate more freely and safely. This allows them to reach young people in a more

[26] Carl Miller – Shiroma Silva: Extremists Using Video-Game Chats to Spread Hate. *BBC News,* 23 September 2021.
[27] Homeland Security Institute: *Recruitment and Radicalization of School-Aged Youth by International Terrorist Groups.* Final Report. 23 April 2009. 58–59.
[28] Thomas Brewster: How Mexico's Real Life Cartels Recruit Drug Mules on Grand Theft Auto Online. *Forbes,* 24 January 2022.
[29] The Associated Press: Mexico: Drug Cartels Recruiting Youths through Video Games. *ABC News,* 20 October 2021.

direct and comfortable environment. Many of these sites are hosted by Western providers, such as Yahoo![30]

In the digital age, many children are growing up using technology and this means that they are also playing games from a relatively early age. Terrorist organisations are already trying to implant their ideology and views in the minds of the youngest age groups, and they have to resort to different approaches than in the case of their adolescent counterparts. Al-Qaeda in the Islamic Maghreb (AQIM) have changed their strategy to specifically target children under 14. In order to spread their radical ideology, they lure children approached online into their self-developed games, which are extremely primitive, lightweight and technologically underdeveloped, but offer a sure sense of achievement. An example of this is the 2013 game Muslim Mali, in which you have to fight under the banner of AQIM and shoot down French planes. Such games, which offer easy success, can play an important role in radicalising children and encouraging them to join a terrorist organisation in the future.[31]

As we have seen, there are many ways in which terrorists and other criminal organisations can exploit the potential of online video games for communication. To illustrate their potential and the ideal forms of communication, we can summarise the utilisation of the online video games in the following table:

Table 1: Communication forms and effectivity of disguising real intention (with legend)

Utilisation of the online video games for communication	Risk of use
Verbal communication	
Written communication	
Non-verbal communication (gestures, emojis, etc.)	
Spreading propaganda	
Recruiting	
Advertising own games	

	Useful, hard to track
	It can be used, but it requires effort and has its dangers
	Useful, but easy to track, high risk of being caught

Source: Compiled by the author.

[30] The Associated Press (2021): op. cit.

[31] Nick Robinson – Joe Whittaker: Playing for Hate? Extremism, Terrorism, and Videogames. *Studies in Conflict and Terrorism,* 11 January 2021. 3–4.

7. Summary

As part of the information society, online games are creating a new and dangerous theatre of war. The digital world of online video games represents a small part of society, yet this sector of communication has been made so unique that it requires specific studies from a security perspective.

The aim of propaganda is to influence opinion in order to achieve a social, political or economic objective. Terrorist groups use propaganda mainly to spread their ideology and for recruitment. Most analyses and studies focus on the path of normal individuals playing video games towards extremist views. Games provide a recruitment opportunity for terrorist and criminal organisations and are used as a tool to strengthen their groups and views. At the same time, a game can also serve to persuade and motivate their membership.[32]

As we can, terrorist and organised crimes groups use the communication through online video games for general communication (verbal, written and non-verbal form), for spreading propaganda, to recruit new members and to advertise their own products.

Defence organisations should not ignore the world of online video games that are available to everyone, regardless of the fact that since 2014, the trend has been to lure people into proprietary or modified games. They have started to train their officers and government workers to protect players. We have to be aware of the new and changing challenges in the other forms of entertainment industry too, and have to continue the adaptation of the new approaches for the digital world. A good example is the internet itself, where without proper regulation, any entertainment product – whether it is a game, film, series, book, magazine, comic book or any other product available for purchase – that disseminates propaganda can be easily accessed by children and adults alike.

Further research on this topic is important for our security, so it is worth exploring the recruitment opportunities, self-produced programmes, training and educational opportunities for online video games. Another important area of research could be offline games. The most common example are the simulators, which ones are designed to reproduce reality as realistically as possible and can therefore be particularly useful for training purposes (e.g. piloting aircraft, weapons handling) – something that has been introduced by the army in several countries, but unfortunately also by organisations that threaten our security.

References

Al-Rawi, Ahmed: Video Games, Terrorism, and ISIS's Jihad 3.0. *Terrorism and Political Violence,* 30, no. 4 (2016). 740–760. Online: https://doi.org/10.1080/09546553.2016.1207633

Anderson, Nate: CSI: Xbox – How Cops Perform Xbox Live Stakeouts and Console Searches. *Ars Technica,* 01 October 2012. Online: http://arstechnica.com/

[32] Robinson–Whittaker (2021): op. cit.

tech-policy/2012/01/searches-and-xbox-live-stakeouts-how-cops-investigate-consoles/
Aroged: Fail0verflow Hackers Hinted at Hacking the Playstation 5 Encryption System. *Aroged,* 08 November 2021. Online: www.aroged.com/2021/11/08/fail0verflow-hackers-hinted-at-hacking-the-playstation-5-encryption-system/
Black, Derek: Hacker Obtained PS5 Encryption Keys that Will Allow Pirating Games. *World Stock Market,* 08 November 2021. Online: www.worldstockmarket.net/hacker-obtained-ps5-encryption-keys-that-will-allow-pirating-games/
Brewster, Thomas: How Mexico's Real Life Cartels Recruit Drug Mules on Grand Theft Auto Online. *Forbes,* 24 January 2022. Online: www.forbes.com/sites/thomasbrewster/2022/01/24/mexican-cartels-recruit-drug-mules-on-grand-theft-auto-online/?sh=20072acb69f6
Conway, Maura: Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research. *Studies in Conflict and Terrorism,* 40, no. 1 (2017). 77–98. Online: https://doi.org/10.1080/1057610X.2016.1157408
Department of Homeland Security: *Strategic Framework for Countering Terrorism and Targeted Violence.* 2019. Online: www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf
Entertainment Software Association: *2019 Essential Facts About the Computer and Video Game Industry.* Online: www.theesa.com/wp-content/uploads/2019/05/2019-Essential-Facts-About-the-Computer-and-Video-Game-Industry.pdf
Hall, Matthew: This Is Our Call of Duty: How ISIS Is Using Video Games. *Salon,* 01 November 2014. Online: www.salon.com/2014/11/01/this_is_our_call_of_duty_how_isis_is_using_video_games/
Holmes, David: Paris Attacks: What kind of Encryption Does the PlayStation 4 Use, Anyway? *Security Week,* 09 December 2015. Online: www.securityweek.com/paris-attacks-what-kind-encryption-does-playstation-4-use-anyway
Homeland Security Institute: *Recruitment and Radicalization of School-Aged Youth by International Terrorist Groups.* Final Report. 23 April 2009. Online: www.eccnetwork.net/sites/default/files/media/file/2009-recruitment-and-radicalization.pdf
Hope, Alan: Brussels Is 'Weakest Link' in Europe's Fight against Terrorism. *The Bulletin,* 13 November 2015. Online: www.xpats.com/brussels-weakest-link-europes-fight-against-terrorism
Lakomy, Miron: Let's Play a Video Game: *Jihadi* Propaganda in the World of Electronic Entertainment. *Studies in Conflict and Terrorism,* 42, no. 4 (2017). 383–406. Online: https://doi.org/10.1080/1057610X.2017.1385903
Lu, Xiaofei: Automatic Measurement of Syntactic Complexity in Child Language Acquisition. *International Journal of Corpus Linguistics,* 14, no. 1 (2009). 3–28. Online: https://doi.org/10.1075/ijcl.14.1.02lu
Parks, Malcolm R. – Kory Floyd: Making Friends in Cyberspace. *Journal of Computer-Mediated Communication,* 1, no. 4 (1996). 80–97. Online: https://doi.org/10.1111/j.1083-6101.1996.tb00176.x
Miller, Carl – Shiroma Silva: Extremists Using Video-Game Chats to Spread Hate. *BBC News,* 23 September 2021. Online: www.bbc.com/news/technology-58600181

Orland, Kyle: Snowden Leak Examines Gaming as a Terrorist Propaganda and Training Tool. *Ars Technica,* 12 September 2013. Online: http://arstechnica.com/gaming/2013/12/snowden-leak-examines-gaming-as-a-terrorist-propaganda-and-training-tool/

Pierre-Louis, Stanley – Susanna Pollack: Video Games Are Transforming How We Communicate with Each Other – And They Could Fix a Range of Other Global Issues too. *World Economic Forum,* 10 December 2019. Online: www.weforum.org/agenda/2019/12/video-games-culture-impact-on-society/

Robinson, Nick – Joe Whittaker: Playing for Hate? Extremism, Terrorism, and Videogames. *Studies in Conflict and Terrorism,* 11 January 2021. Online: https://doi.org/10.1080/1057610X.2020.1866740

Thorne, Steven L. – Ingrid Fischer: Online Gaming as Sociable Media. *ALSIC: Apprentissage des Langues et Systèmes d'Information et de Communication,* 15, no. 1 (2012). Online: https://doi.org/10.4000/alsic.2450

Sykes, Julie M. – Jonathon Reinhardt – Steven L. Thorne: Multiuser Digital Games as Sites for Research and Practice. In Francis M. Hult (ed.): *Directions and Prospects for Educational Linguistics.* New York, Springer, 2010. 117–135. Online: https://doi.org/10.1007/978-90-481-9136-9_8

Taylor, T. L.: *Play Between Worlds. Exploring Online Game Culture.* Cambridge, Mass., The MIT Press, 2006. Online: https://doi.org/10.7551/mitpress/5418.001.0001

The Associated Press: Mexico: Drug Cartels Recruiting Youths through Video Games. *ABC News,* 20 October 2021. Online: https://abcnews.go.com/International/wireStory/mexico-drug-cartels-recruiting-youths-video-games-80691749

Westerlund, Anton: *Using Video Communication in Online Multiplayer Games. The effects of adding a video chat overlay on the game experience in online multiplayer video games – a quasi-experimental design.* Linnaeus University, Bachelor Thesis in Media Technology, 2021. Online: www.diva-portal.org/smash/get/diva2:1580454/FULLTEXT01.pdf

Williams, Dmitri – Scott Caplan – Li Xiong: Can You Hear Me Now? The Impact of Voice in an Online Gaming Community. *Human Communication Research,* 33, no. 4 (2007). 427–449. Online: https://doi.org/10.1111/j.1468-2958.2007.00306.x