التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

VIDEO GAMES: A RECRUITMENT TECHNIQUE IN THE HANDS OF TERRORISTS

PUBLISHED BY: STUDIES AND RESEARCH DEPARTMENT

3
TERRORISM ISSUES
Mar. 2023

TERRORISM ISSUES

A monthly publication issued by the Islamic Military Counter-Terrorism Coalition

---

VIDEO GAMES:
A RECRUITMENT TECHNIQUE IN THE HANDS OF TERRORISTS

PUBLISHED BY; STUDIES AND RESEARCH DEPARTMENT

Over the past century, the world has witnessed an accelerated information and technology revolution, which contributed rapidly and significantly to the development of electronic services in all forms and in all sectors, including both the government and private sectors. This revolution has also contributed to changing the way of living of societies, starting from customs, practices and behavior up to the ladder of values and lifestyles, thus leading to abandonment of many social values and customs established in our societies. As a result, the process of socialization confronts a number of influences that affect the upbringing of generations. Electronic culture particularly is now playing a major role in shaping values and forming cultural and civilizational identities.

We should not forget that the world has become a small village based on its permanent connection to the Internet. As a result, each and every country is now required to protect its individuals, institutions, capabilities and civilization from the effects of this unlimited Internet openness, and every individual should now realize the benefits of information technology. However, we cannot simultaneously deny the multiple risks underlying the large-scale permeation of this technology into our societies. This requires the society and government institutions to endeavor to prevent and reduce these risks.

The wide spread of video games has led to a significant development in the personality of children and youth. They have started to adopt various intellectual and behavioral values and trends based on the things they learn from these games, which are now competing with the role of the family in building the thought and personality of the players. This led to the emergence of a kind of social upbringing that is not compatible with the customs and traditions of the society.[1]

Undeniably, this is the current situation that we experience in our societies. These games constitute an important source of social upbringing because of their direct impact on the behavior of individuals and societies. Therefore, we must pay attention to how much time children and youth spend with these games.[2]

In light of the role played by video games, we notice that children and youth are an easy target for recruitment by terrorist groups because they do not possess a high culture that could enable them to distinguish between correct and extremist ***takfiri*** (excommunicational) thought. This makes them an easy prey to persuade and more prone to embrace false ideas, and these groups can thus instill misleading concepts and beliefs in their minds to recruit them through such games. In other words, when children and youth play these games that contain scene of wars,

explosions, killing, destruction, violence, and terrorism, they would be directly affected, as these games make them so mentally programmed that these scenes become familiar to them, and they even become enthusiastic to implement what they have just seen.

For these reasons, many countries have sought to take measures and precautions to combat cyberterrorism. These efforts, however, require more procedures and measures to stand in the face of this dangerous weapon due to its diverse sources, aspects, and purposes. It can be said that cyberterrorism is the terrorism of the future, an imminent danger that has multiple forms and divers methods and fields. The more we devise new and modern ways to combat cyberterrorism, the more diverse its methods and fields grow.

Cyberterrorism

The term "cyberterrorism" appeared in the 1980s and its definition was limited to those attacks in which computers were used against the economies and governments of countries. With the beginning of the 1990s, the meaning of this concept expanded, especially with the increasing growth of the Internet and its clear use in the Arab Spring, as well as its importance in the mechanics of international relations.

Definition of Cyberterrorism

There is no standard definition of cyberterrorism, as the term has several meanings. The phenomenon of electronic or digital terrorism (Cyberterrorism) refers to a negative culture and another type of terrorism as a result of technological development and the information revolution, where the Internet and technological tools are used for purposes of destruction, vandalism, and theft.

Cyberterrorism is defined as material or moral aggression, intimidation, or threat through using electronic means by countries, groups, or individuals across cyberspace; it also refers to a situation where cyberspace becomes a target of such aggression, affecting its peaceful use.[3] Cyberterrorism is also defined as the use of digital technologies to intimidate and subjugate others, or as an attack on information systems for political, economic, social, ethnic, sectarian, or intellectual motives.

Cyberterrorism is also defined as a material or moral act of aggression, intimidation, or threat through using electronic means and tools by countries, groups, or individuals against a person by targeting his religion, his own self, his honor, his mind, or his money, unjustly and in various forms of corruption.[4]

Forms of Cyberterrorism

The forms of cyberterrorism can be counted as follows:[5]

- Using electronic platforms by terrorists to communicate and coordinate with their aides and financiers and to give them orders via the Internet to carry out terrorist operations;
- Creating websites dedicated to launching media campaigns against countries that they wish to intimidate, by showing images and video clips of hostages and captives and their executions, by spreading rumors aimed at destabilizing the security and economy of the target country or group, or by organizing demonstrations and acts of sabotage directed at the target country;
- Hacking only for the purpose of tampering and vandalism, as psychological studies of the personalities of these hackers indicate that they suffer from mental illnesses that push them to revolt against society or institutions and lead them to commit acts of tampering and sabotage;
- Seizing other people's funds or personal files; hacking into an individual's computer, which is deemed as theft of that person's private property; and utilizing modern technology tools to obtain private information of individuals or institutions and extorting these victims by threatening to publish such information online if they do not respond to their demands;
- Electronic indoctrination by mobilizing supporters of and sympathizers with these terrorists and with their principles, methods and means in order to recruit new terrorists through social media platforms and chat rooms in video games.

Video Games

The emergence of video games dates back to the beginnings of the computer industry. These games made use of the available software capabilities to simulate true and virtual reality with their various elements and effects, which opened wide interaction areas for human education, entertainment and

recreation. It also prompted specialized companies to develop hardware and software for these games in order to promote cultural and social awareness.

The recent years have witnessed a wide spread of video games selling places, and gaming centers and halls in various shapes, sizes and types. This spread was matched by an increasing demand by children and young people to acquire these games. These electronic devices and games quickly spread in homes, clubs, and gaming centers. Worthy of note is that these games often rely on speed of attention, concentration, and thinking.[6]

As electronic devices developed and increased in number, the games associated with them also expanded. They followed a tactical sequence, starting with speed and excitement games, such as car racing, then conflict between animals, all the way to games on wars between countries, gangs and militias, which included military tactics and use of light and heavy military equipment such as war games and military games, as well as destruction, killing, theft and looting games. Thus, with the rapid advancement of technology, video games have become welcomed and accepted by gamers of different age groups, especially in light of the excitement and suspense they contain.

At the same time, games have now become out of control. Even more, children and young people have started to participate in manufacturing or programming them. More importantly, these games now instill a certain social content into children and young people, perhaps at the expense of the social content of the society, which may lead to loss of loyalty to their community and weaken their social ties. Even worse, these video games may provide deviant social values that contribute to making these gamers real enemies of their homeland.[7]

Types of Video Games

There are many types of video games; they are divided as follows:

- Games built on a story or a cartoon character; these are very useful;
- Intellectual games, namely software that relies on imagination, quick-wittedness, memory and mental activity;
- Games that rely on war strategy and require making plans; this is an advanced type of games that requires intellectual maturity; and
- Games that depend only on the struggle for survival; this type is marked by violence and leads to dull-mindedness and distraction, as it depends on killing, destruction, sabotage, and a feeling of ecstasy.[8]

The danger of the spread of video games stems from the absence of any law prohibiting their sale to children. In addition, some children illegally download these games from the Internet through foreign or Arab websites. They also develop the game to introduce strategic planning based on cooperation between a group of players, for example to rob a bank or a shop. They also introduce other elements, such as wearing masks, concealing personalities, encouraging killings, robbing people of their money and property, and disrespecting security laws and regulations.

The negative side of video games mainly lies in the fact that these games address serious topics such as violence, sex, and disregard for the other. Only a few games are designed for harmless edutainment or specific educational purposes, while other game designs seek to stereotype the recreational needs of young people. These latter games race to transform virtual vices, namely killing, violence, fraud and lies, into highly attractive entertainment products targeting age groups that are not able to resist these threats due to their poor awareness and understanding during their early receptive and formative years.[9]

Relationship between Violence in Video Games and Cyberterrorism

Our findings indicate that many video games contain different models of repetitive violent personalities and behaviors. Children and youth imitate these models without expressing any form of criticism or condemnation, which could maintain the prevailing social opinion that deems violence as a reprehensible social behavior that must be stopped and resisted.

This problem coincides with the remarkable absence of the family role in controlling video games and the emergence of new social classes based on differences in informational use and awareness of potential risks, especially if we take into account the level of cultural awareness among many segments of society. This would certainly reduce any perceived

risks of video games in general.[10]

Video games promoted by terrorist organizations may be considered as an organized process for recruiting children and youth. Most of these games employ different forms and types of guns, pistols, daggers, swords, theft, destruction, seizure of others' money and property, and dissemination of terror and fear in the hearts of others. These actions destroy the normal innate nature of children and young people and take them into a far-distant environment that encourages violence, killing, destruction and hatred of others.[11] They also increase sectarian and ethnic fanaticism, raise children to disrespect security rules and regulations, and develop weak social responsibility, all of which are considered as anti-good citizenship values.

The damage resulting from some video games is no longer limited to the violence that exists within the world of such games, but rather extends to misleading young people and urge them to join terrorist organizations. Members of these organizations communicate by voice with players in the world of online video games to manipulate their ideas and mislead them. Likewise, a number of video games have also been used for communication between members of terrorist groups to carry out terrorist operations. In that case, members join a virtual electronic battle in a particular game and plan and communicate in that world away from the eyes of direct observation because the servers for those games are distributed all over the world. Terrorist organizations try to contact and mislead players in various ways such as voice or text chat. We cannot rule out the fact that children and adolescents may be affected by such attempts and may wish to experience the adventures taking place in the world of violent video games outside their homes. This could translate into their being lured by these terrorists and falling victim to such attempts.

Relationship between Aggressive Behavior in Video Games and Cyberterrorism

Children's practice of violent video games can increase their aggressive thoughts and behaviors. These games may thus become more harmful than violent movies on television or the cinema because they are characterized by interaction between the child and the game and require the child to identify with the aggressor that instills in their hearts the idea that killing is acceptable and enjoyable.

The risks of these violent games lie in the continuous reinforcement of killing and destruction behavior and other aggressive practices. Sometimes, winning the game is contingent on practicing a greater amount of destruction and bloodshed. To be able to do so, the player is taught ways of complete loyalty to and total engagement in the time and place of the virtual game. This would push him afterwards to exercise the violent solutions available to him when dealing with people and when trying to overcome any obstacles or impediments that prevent him from scoring the required number of points to reach the last level of the game. In this way, rewards and incentives are granted to the gamer in exchange for killing and destruction activities throughout the game's time. Accordingly, the child finds himself in the middle of a closed circle of violence and aggressive behavior, as well as reactions that praise and reward his violent behavior. This makes the person who is better at using violence and aggression than others the successful winner of the game.[12]

The design of video games and their various options rewards players, especially youngsters and gamers who favor of adventure and violence games, and opens up before them new areas to learn violent solutions and aggressive behavior in conflicts and competitions. This practice could endanger the lives of young people, as it puts aggressive thoughts front and center. Young people, just like children, play and learn at the same time, especially when they learn tricks and implement plans related to aggressive behavior.

Terrorist groups may take advantage of these games and actively seek to recruit new members, especially from among children and youth. For example, video games that glorify martyrdom can play an influential role in attracting the interest of potential suicide bombers in the future. Terrorist groups may also use video games for educational purposes to spread cyberterrorism through inviting children and youth to steal houses, money and vehicles as well as to commit crimes of bank robbery, bombing and murder.[13]

Violence in these games turns gradually into a familiar aggressive act and behavior to which

gamers resort as an alternative when the time is ripe for fighting and the door of conflict opens in the reality of social life. These games also instruct children and young people on the techniques, arts and tricks of committing crimes, and develops in them the mental abilities, skills, and methods of violence and aggression that drive them to commit terrorist acts, or even make them willing to become members of terrorist organizations.[14]

Video Games: A Recruitment Technique for Terrorist Groups

Terrorists make large-scale use of online games to spread extremist ideology, false beliefs, and misconceptions that facilitate the task of recruiting new members in terrorist organizations, whether as members or as lone wolves to carry out suicide operations. For this purpose, terrorist organizations model their own video clips intended for recruitment and merge them into video games. In this way, these groups have been able to spread large-scale propaganda and increase their publicity through quick and effective means. This phenomenon has become a global threat in recent years as terrorists have been able to reach larger audiences through such methods, which may have contributed to an observed increase in the recruitment of more terrorists around the world and a significant growth in the number of terrorist attacks, especially attacks carried out by lone wolves and sleeper cells.[15] Due to this trend, many terrorist groups have allocated much of their resources and their capabilities to the online world, and particularly to video games, which has made it even more challenging for law enforcement agencies to track and intervene with terrorist activity. Many law enforcement agencies thus recommend for security professionals and experts to stay up-to-date on cybersecurity materials and for government officials to consider the effects of violent video games on players when drafting public policy; with such counterterrorism measures, terrorists may be more easily apprehended despite their familiarity with modern technology.

The Internet has opened new opportunities for terrorists to operate incognito without security oversight, spread their poisonous messages and ideas to their target groups, motivate and train their followers, fundraise, and facilitate the planning of their terrorist attacks.[16] The most important aspect that these terrorists rely upon is interactivity, which has widened the circle of communication through the Internet and eliminated geographical borders caused by location distance and security obstacles, allowing people to instantly connect with each other around the world without control or limits. Although this development has stimulated social and economic growth, many media and social platforms – like Facebook and other media platforms – also profit from content that arouses great emotions and stirs sympathy with the published content, such as images or videos depicting violence and bloodshed. Sensitive information psychologically activates divergent emotions in people, which functions to create global discussions and greater engagement on social media. This increases the views of a post and the comments below it, thus making the social platform involved more powerful and popular, and this platform will oftentimes continue to boost or neglect to take down the content for their economic gain. Regardless of the attention it tends to draw in, what should be happening instead is the total and immediate ban of violent and disturbing content.[17] This is a concerning dilemma that states must address first through legal changes before allowing the counterterrorism community to tackle online terrorism and extremism.

In addition, the proliferation of the COVID-19 pandemic has induced many people to spend more time on the Internet from home, which has increased their risk of exposure to extremist content, radicalization, and being involved in violence.[18] These circumstances have granted terrorists a large pool of vulnerable targets susceptible to their methods of radicalization. In particular, people have recently been seeking entertainment sites and video games as a way to partake in a virtual world where they are able to interact with people from all over the world and belong to a virtual community. The increased popularity of gaming and its ability to reach a large and diverse audience has therefore served to attract extremist organizations looking to recruit more fighters and loyalists to prepare them to initiate acts of violence without having physical ties to terrorist activity.[19]

These platforms broadcast international online

video game streaming service where individuals are allowed to live stream audio and video of them playing video games. Although meant to share gaming experiences with others, some individuals utilize chat rooms to spread their polarizing and violent political beliefs about controversial issues.[20] Furthermore, first-person shooter video games have been and are currently being investigated for their potential influence in the desensitization of individuals to violence, and in general the promotion of violence. The University of North Carolina at Chapel Hill in the United States conducted a study in which they discovered that terrorist groups have been found to alter their recruitment strategies to reflect violent video games in order to make joining their groups more appealing to potential recruits. The researchers involved found that Islamic State (ISIS) professional-grade propaganda and recruitment videos copy popular computer games, most notably Call of Duty. "First Person Shooter (FPS) games like these are played by hundreds of millions of people, generally under age 35 and 90 percent male, which is a key target demographic for Islamic terrorist organizations. It was discovered that ISIS videos often mimic or lift footage and imitate editing styles, common features, and sequences in detailed ways that only regular gamers may fully recognize. This includes footages that instigate terrorist activities like "how the weapon the shooter is holding appears in the shot, the progression from lighter to heavier weapons, the use of drone footage clips, and the way graphics and titles are used".[21] The researchers did not conclude that video games were directly linked to the radicalization of players, but rather that terrorist groups such as ISIS have tailored their recruitment strategies to be similar to those in Call of Duty and FPS games by showing first-person shooter media in their recruitment videos.[22] It is important to note that video game manufacturers do not promote the utilization of violence, but rather seek profit. However, terrorist organizations such as ISIS have become aware of the popularity of first-person shooter games, and thus determined that by using FPS game techniques, they could reach a larger audience when trying to recruit new members.

It is important to note that ISIS is also known to encourage violence against young children using several methods of technology-related entertainment. Specifically, ***Huroof*** is an educational application that asks kids to match Arabic letters to pictures of bombs, weapons, tanks and many other military symbols.[23] Children are generally extremely naive and vulnerable but also quick to learn new material. Therefore, ISIS's method of targeting this demographic through entertainment will most likely create a new generation of strong-willed fighters faithful to ISIS's cause, without any regard to moral values or the destruction that violence creates. This prediction needs to be addressed at the international level, and measures must be taken to ensure that these children receive the education they require as opposed to tactics of desensitization by an extremist organization.

Terrorist groups like ISIS are not the only actors to increase their focus on video games and other online platforms. Smaller, less sophisticated terrorist organizations have been inspired by ISIS's recruitment strategies and have begun utilizing these techniques as well. The research team at the University of North Carolina at Chapel Hill also evaluated the elements within these FPS inspired recruitment techniques and compared them based upon their production values. The study found that the previously discussed video game strategy "was expanded to cover about 50 points of assessment ranging from technical production values to storyline, camera technique, editing craft, and so on." With this grading scale, the researchers concluded that the typical ISIS video was produced at a similar level to a professionally produced corporate video.[24] The utilization of these types of techniques for recruitment makes it evident that terrorist organizations are becoming increasingly more sophisticated. They are adapting their recruitment strategies to the interests of their target demographic so that they can tailor their recruitment campaigns to be appealing to them. Terrorist organizations are willing to learn, practice, and utilize various skills that individuals external to their group may not perceive to be a threat. It is also important to consider that with the increased popularity of such tactics, terrorist organizations could be competing amongst one another to improve their recruitment strategies and reach a greater

number of potential recruits. Their efforts to further familiarize themselves with potential recruits and to attract as many followers as possible signifies that the threat of online terrorism will continue to exponentially increase and to adapt to the popular preferences observed in this modern day and age.

While it may be perceived that the utilization of these recruitment techniques by terrorist organizations is negative, the increased prevalence of recruitment techniques by video games can help law enforcement agencies identify terrorist organizations. They had stated that "studying propaganda videos can help track the spread of sophisticated production values and [help] develop detailed 'aesthetic fingerprints' that could be used to identify teams and organizations producing such material."[25] By studying the videos produced by extremist organizations, law enforcement agencies and government officials can work together to publicly condemn these practices and to warn individuals on the domestic and international level to practice hypervigilance when engaging with unknown individuals on online platforms. Exposing these sophisticated techniques via the news, printed sources, and word of mouth can also help individuals to understand what methods terrorists are relying upon today so that they can identify terrorist activity and report it if they come across it. Agencies, organizations and companies must also increase funding for cybersecurity divisions or personnel in order to improve existing cybersecurity measures designed to scan the Internet for language or images related to extremism. It is paramount that they also collaborate with Big Tech personnel to ensure that such large companies are involved in this process, which may hold both accountable in adhering to their efforts to protect the public from such methods.

It is possible to notice a turning point in the fight against online radicalization, which sees many group-chat apps banning extremist and violent communities from their platforms. For example, Discord – a popular group-chatting app originally created for gamers – removed groups that are organized around violence and extremist ideologies.[26] This is important because it shows that social platforms have the power and the ultimate control over everything that happens within them. Identifying violent content is a complex process, but it is possible. Banning all communities that incite and promote violence could serve to send a warning message to all those who intend to create their own extremist group.

The Counterterrorism Group (CTG) will continue to monitor and analyze violent content posted on both large and smaller online platforms and will continue to produce reports intended to identify key actors and new techniques to be read by agencies, organizations and companies. CTG's Crime Team will stay up to date on the most recent developments in privacy laws for violent video games and will ensure that the necessary analysis-oriented connections are being drawn to ensure that extremist organizations are not taking advantage of possible loopholes or violating public policy. The Crime Team will additionally prioritize gathering intelligence information indicative of terrorist radicalization processes from widely used media platforms such as Twitch, which currently reports around 140 million unique visitors every month.[27]

Cybersecurity

Just like regular security forces are aimed at protecting physical property and people from criminal or terrorist activity, cybersecurity protects computer systems, end-user applications, the users of those systems, and the data they store. Cybersecurity is aimed at preventing cybercriminals, hackers, or others from accessing, damaging, disrupting, or modifying IT systems and applications.

The Importance of Cybersecurity

As human society goes digital, all aspects of our lives are facilitated by networks, computer and other electronic devices, and software applications. Critical infrastructure including healthcare, financial institutions, governments, and manufacturing, all use computers or smart devices as a core part of their operations. A vast majority of those devices are constantly connected to the Internet.

Hackers have a greater incentive than ever to find ways to infiltrate those computer systems, for financial gain, extortion, political or social motives (known as hacktivism).

Over the past two decades, cyberattacks were launched against critical infrastructure in all

developed nations, and countless businesses suffered catastrophic losses. There are over 2,000 confirmed data breaches globally each year, with each breach costing over $3.9 million on average.[28] Security breaches and threats can affect nearly any system including:

Communication: Phone calls, emails, text messages, and messaging apps can all be used for cyberattacks.

Finance: Naturally, financial institutions are a primary target for attackers, and any organization processing or dealing with bank or credit card information are at risk.

Governments: Government institutions are commonly targeted by cybercriminals, who may obtain private citizen information or confidential public data.

Transportation: Connected cars, traffic control systems and smart road infrastructure are all at risk of cyberthreats

Healthcare: Anything from medical records at a local clinic to critical care systems at a national hospital are vulnerable to attack.

Education: Educational institutions, their confidential research data, and information they hold about students or staff, are at risk of attack

In the vast majority of these systems, websites and web applications are a gateway for attackers. They are exposed to the public Internet, and commonly connected to sensitive back-end systems, representing a weak link in the organization's security strategy.[29]

Principles of Cybersecurity

The primary objective of cybersecurity is to protect data. The security community commonly refers to a triangle of three related principles that ensure data is secure, known as the CIA triad:[30]

Confidentiality: ensuring sensitive data is only accessible to those people who actually need it, and are permitted to access according to organizational policies, while blocking access to others.

Integrity: making sure data and systems are not modified due to actions by threat actors, or accidental modification. Measures should be taken to prevent corruption or loss of sensitive data, and to speedily recover from such an event if it occurs.

Availability: ensuring that data remains available and useful for its end-users, and that this access is not hindered by system malfunction, cyberattacks, or even security measures themselves.

Role of Cybersecurity in Protecting the Gaming Industry

The gaming industry is the largest entertainment industry worldwide, with a market worth of more than $197 billion in 2022. The COVID-19 pandemic has caused an enormous 26% surge in growth in 2019 and 2021, as users attempted to break up the monotony of lockdowns and stay close to friends and family. This large and growing industry where cash and data are exchanged online is a draw for nefarious actors.[31]

Gamers tend to trust gaming software with sensitive personal information, allowing them to spend either real money or cryptocurrencies in exchange for in-game valuables. Both types of data are valuable and draw hackers to steal them. Hackers have different methods that they will commonly use to intercept data that can be resold online or to divert transactions into their accounts. Some hackers may attempt to find and take advantage of security vulnerabilities to disrupt gameplay. These service interruptions may cause damage to a game or a company's reputation, costing them financially.

It is thus important to adhere to cybersecurity protocols to prevent the risks of data disruption and currency theft from in-game transactions, stop cyberattacks on gaming software, and halt malware infections on users' devices.

Cyberthreats Facing the Gaming Industry

Cyberthreats come in different forms depending on what the hacker tries to achieve and where weaknesses may lie in gaming software. Following is a description of some common cyberthreats and how they affect gamers.

In-game cheats and mods

A game mod is a game hack that integrates cheating software into the game itself. While this is possible for any game, this type of cyberthreat is most common for small compact game clients like mobile games. It is also relatively common for Windows PC games.

Mods require specialized coding knowledge to be created. Typically they require not only knowledge

of programming language but also knowledge of compilers and machine code since raw source code is generally not available for use. Mods are sold to users for profit to give them an edge in the game. Especially in massively multiplayer online (MMO) games, the actions taken by mods will affect and frustrate legitimate users who may quit the game, leaving their subscriptions. The game developers must close loopholes used by hackers to create mods. Removing these loopholes ensures that mods take too much time to build to be profitable.[32]

PII Leaks

Personally identifiable information (PII) leaks are a type of cyberattack where valuable personal information is collected and either used or sold. Data can be collected in different ways, including manipulating the forms in a game to collect personal information, attacking data stores holding this information for game users, or taking advantage of developer errors causing exposure of data. Collected data may include emails and passwords, credit card information, device information, and other personal and sensitive data.

Mobile games are a particular draw for database leaks since games will often collect data automatically rather than via forms. Studies estimate that 14% of iOS and Android apps using cloud storage are vulnerable to issues that expose PII. In 2022 Neopets revealed that a data breach was in place for 18 months, exposing the personal information of more than 69 million users.[33]

Phishing Attacks

Phishing attacks attempt to gain personal information or payments. The attacker will send a message posing as a trusted individual or service requesting personal information. Once collected, information can be sold or used for ransom demands.

Phishing is one of the most widespread cyberattacks used on gamers. Over one year, one security solution detected more than 3.1 million phishing actions in online games, generally targeted at acquiring user credentials to take over gaming accounts. Games targeted include big titles, where a website offering generation of in-game rewards was set up to collect credentials.

Game accounts often have access to payment information which can then be stolen, or if the gamer is one of many who reuses passwords, the hacker may be able to use credential stuffing on other sites to steal more valuable information. Credential stuffing is a cyberattack method where stolen credentials are used to breach other systems.[34]

DDoS attacks

A distributed denial-of-service (DDoS) cyberattack aims to overwhelm regular server traffic, slowing or blocking legitimate connections. These attacks can be lobbied against game servers, blocking connections for many users, or targeted against personal devices disrupting a single user. The motivation behind each of these cyberattacks is different and requires different data.

DDoS attacks on individuals cause the user's online gaming system to become slow and unplayable. This is generally done to gain a competitive advantage over the attacked user. The attacker requires the IP address of the individual, which can be acquired with malware. DDoS cyberattacks on online gaming platforms like PlayStation Network and Xbox Live leave users unable to play networked games. In 2104, a hacker group took down both PlayStation and Xbox networks.[35]

Malware

Some computer and mobile games pose a significantly more severe danger to users' online and personal security because of hackers or bad developer security. Devices may become infected with malware (malicious software) intending to steal data after downloading the wrong file or an infected program.

Downloaded games can become infected with malware when a hacker injects malicious code into a legitimate game, or if he manages to create a fake application that is simply a shrouded virus. This is especially common when downloading games from unsafe sites. Minecraft is one of the most malware-infected PC games after malware was detected on over 3 million computer devices between 2020 and 2021.[36]

Protecting Games from Cyberattacks

Cyberattacks become successful when there are failures in cybersecurity in gaming software or when users are tricked into giving away valuable information. Game developers should understand

the importance of including cybersecurity when developing and maintaining games to ensure that data is kept safe and that the game continues to function expectedly. Including cybersecurity protocols in all aspects of the game and observing game data reduces the risk of successful cyberattacks.

Building a Cybersecurity System into the Game Development Process

Security should be one of the priorities considered when designing and building software. Code reviews and design discussions should include identifying security loopholes and potential exploits so they can be closed before writing code or putting code into production. It is necessary to apply best practices to game development, like practicing threat modeling and running static analyses.

Monitoring Games in Production

Relevant monitoring data should be collected from the software. This data can be exported to an observability tool to detect security issues. When dynamic alerting and automated incident response is available, teams can respond to cyberthreats quickly, which would reduce affected users.[37]

Secure Authentication Methods

It is crucial to ensure that any stored passwords are protected and encrypted. Authentication methods should be secure using methods like two-factor authentication to protect against cyberattacks, as follows:

Providing a Secure Infrastructure

Infrastructure in gaming includes databases, networking, and servers (cloud or local) that run code. Code should use principles of least trust to limit the scope of any attacks through servers. Place protection on endpoints against DDoS attacks, so that the game experience is not interrupted. Ensure that databases are encrypted and secure, especially upon storing personal information. Wherever possible, separate data into different storage locations so breaches are limited in scope.

Running security exercises

Run security exercises against your game to identify potential attack vectors. Pen testing and red teaming are valuable exercises to find and close security vulnerabilities in production.

Engaging users

Engage with users where possible to educate them about phishing attacks and ensure clear communications about the data which your game could request from them. Inform them when phishing attempts are known to be occurring, so they are less likely to be caught. Encourage users to utilize strong passwords and inform them to avoid reusing passwords across different applications.[38]

References:

1. Maha Hosni Al Shahrouri (2008) (In Arabic). Video Games in the Era of Globalization: Pros and Cons. Cairo: Dar Al Maysara, p. 26.
2. Shahba Jassim Al-Hamdani (2011) (In Arabic). Violence in Video Games with Aggressive Behavior among Primary School Students. MA Dissertation. Tikrit University in Iraq: College of Education.
3. Adel Abdul Sadiq (2015) (In Arabic). Cyberterrorism: A New Pattern and Different Challenges. Arab Center for Cyberspace Research, 14th Year, Issue no. 52, p. 92.
4. Aysar Muhammad Attia (2014) (In Arabic). The Role of Modern Mechanisms in Reducing Emerging Crimes and Ways to Confront Electronic Terrorism. Scientific Forum entitled "Emerging Crimes in light of Regional and International Changes and Transformations" held on 2-4/9/2014, Amman, Hashemite Kingdom of Jordan.
5. C. A. Anderson & K. E. Dill (2000). "Video Games and Aggressive Thoughts, Feelings, and Behavior in the Laboratory and in Life". Journal of Personality and Social Psychology, p. 78 .
6. J. R. Linder & D. A. Walsh (2004). "The Effects of Violent Video Game Habits on Adolescent Hostility, Aggressive Behaviors, and School Performance." Journal of Adolescence1) 27).
7. Fatima Youssef Al-Qalini (1995) (In Arabic). "Cultural Media Risks for Children: A Study of Negative Dimensions of Emerging Games on the Egyptian Child". Third Annual Conference entitled "Children between Risk and Addiction," Cairo.
8. Dalia Mahmoud Baklawa (2009) (in Arabic). "Role of Educational Video Games in Developing Creative Thinking". Electronic Training and Human Resources Development Conference, Cairo, August 12-13.

9. C. A. Anderson (Ed.) (2004). "Violent Video Games: Specific Effects of Violent Content on Aggressive Thoughts and Behavior". Advances in Experimental Social Psychology, Vol. 36.
10. Farid Al-Saghiri (2013) (in Arabic). "Video Games: Relationship between Youth Practice and Violence". Journal of Studies and Research. Algeria, University of Djelfa, p. 11.
11. A. B. Spinks & A. K. MacPherson (2006). "Quantifying the association between physical activity and injury in primary school-aged children". *Pediatrics*, 1 July.
12. Khaled Abdo Al-Sarayrah (2008) (in Arabic). *Impact of Electronic Publishing on Libraries and Information Centers*. Amman: Kunooz Al Marefa.
13. Peter Grabowski (2006). "PC Crimes: Global Dimensions in Internet Networks and their Social and Security Effects". Security Research and Studies Center, 6-8 November 2006, UAE, 1st Edition.
14. "Middle East – The resurgence of the Islamic State in Syria and Iraq". *Global Risk Insights*, February 2021. Available at: https://globalriskinsights.com/2021/02/middle-east-the-resurgence-of-the-islamic-state-in-syria-and-iraq/
15. Eric Young (2016): "Terrorism, Media, and the Rise of the Internet". In J. K. Wither and S. Mullins (Eds.): Combating Transnational Terrorism. Sophia: Procon.
16. Eric Young (2016): "Terrorism, Media, and the Rise of the Internet". In J. K. Wither and S. Mullins (Eds.): Combating Transnational Terrorism. Sophia: Procon.
17. "The Role of Video Games and Online Platforms in Terrorist Radicalization and Recruitment". Available at: https://www.counterterrorismgroup.com/post/the-role-of-video-games-and-online-platforms-in-terrorist-radicalization-and-recruitment
18. "COVID-19 and Terrorism in the West: Has Radicalization Really Gone Viral?". Just Security, March 2021. Available at: https://www.justsecurity.org/75064/covid-19-and-terrorism-in-the-west-has-radicalization-really-gone-viral/
19. "Jumanji Extremism? How games and gamification could facilitate radicalization processes". Journal for Deradicalization, 2020. Available at: https://journals.sfu.ca/jd/index.php/jd/article/view/359/223
20. Twitch streamer Destiny loses partnership for "encouraging violence", Ginx, September 2020. Available at: https://www.ginx.tv/en/twitch/twitch-streamer-destiny-loses-partnership-for-encouraging-violance-against-protesters
21. "How 'Call of Duty' Is Transformed Into a Call for Jihad". Homeland Security Today, August 2019. Available at: https://www.hstoday.us/subject-matter-areas/counterterrorism/how-call-of-duty-is-transformed-into-a-call-for-jihad/
22. "How 'Call of Duty' Is Transformed Into a Call for Jihad". Homeland Security Today, August 2019. Available at: https://www.hstoday.us/subject-matter-areas/counterterrorism/how-call-of-duty-is-transformed-into-a-call-for-jihad/
23. "Jumanji Extremism? How games and gamification could facilitate radicalization processes," Journal for Deradicalization, 2020. Available at: https://journals.sfu.ca/jd/index.php/jd/article/view/359/223
24. "How 'Call of Duty' Is Transformed Into a Call for Jihad". Homeland Security Today, August 2019. Available at: https://www.hstoday.us/subject-matter-areas/counterterrorism/how-call-of-duty-is-transformed-into-a-call-for-jihad/
25. "How 'Call of Duty' Is Transformed Into a Call for Jihad". Homeland Security Today, August 2019, https://www.hstoday.us/subject-matter-areas/counterterrorism/how-call-of-duty-is-transformed-into-a-call-for-jihad/
26. "Group-Chat App Discord Says It Banned More Than 2,000 Extremist Communities", NPR, April 2021. Available at: https://www.npr.org/2021/04/05/983855753/group-chat-app-discord-says-it-banned-more-than-2-000-extremist-communities?t=1617718575660
27. "Twitch Usage and Growth Statistics: How Many People Use Twitch in 2021?" BackLinko, January 2021. Available at: https://backlinko.com/twitch-users
28. "Cybersecurity". Available at: https://www.imperva.com/learn/application-security/cyber-security/
29."Cybersecurity". Available at: https://www.imperva.com/learn/application-security/cyber-security/
30."Cybersecurity". Available at: https://www.imperva.com/learn/application-security/cyber-security/
31. "Gaming Industry: The Need For Cybersecurity (Protocols)". Available at: https://coralogix.com/blog/gaming-need-cyber-security/#:~:text=Cybersecurity%20protocols%20are%20necessary%20to,malware%20infections%20on%20users'%20devices
32. "Gaming Industry: The Need For Cybersecurity (Protocols)". Available at: https://coralogix.com/blog/gaming-need-cyber-security/#:~:text=Cybersecurity%20protocols%20are%20necessary%20to,malware%20infections%20on%20users'%20devices
33. "Gaming Industry: The Need For Cybersecurity (Protocols)". Available at: https://coralogix.com/blog/gaming-need-cyber-security/#:~:text=Cybersecurity%20protocols%20are%20necessary%20to,malware%20infections%20on%20users'%20devices
34. "Good game, well played: an overview of gaming-related cyberthreats in 2022". Available at: https://securelist.com/gaming-related-cyberthreats-2021-2022/107346/#:~:text=One%20of%20the%20most%20widespread,account%20credentials%20or%20financial%20information
35. "DDOS Attacks: How to Protect Yourself from the Political Cyber Attack". Available at: https://coralogix.com/blog/ddos-attack-political-cyber-attack/
36. "The Most Malware-Infected Games of 2023: Protect Yourself". https://vpnoverview.com/internet-safety/malware/malware-infected-games/
37. "How do Observability and Security Work Together?" Available at: https://coralogix.com/blog/observability-security-work-together/
38. "What is Red Teaming in Cyber Security? The Complete Guide". https://coralogix.com/blog/red-teaming-cybersecurity/