CENTRO ALTI STUDI DIFESA
SCUOLA SUPERIORE UNIVERSITARIA

UNIVERSITÀ DEGLI STUDI DI SALERNO

Dottorato di Ricerca in

Scienze dell'Innovazione per la Difesa e la Sicurezza

XXXVII CICLO

TITOLO DELLA TESI

Cybercrimes and Virtual worlds: from theory to practice.

SETTORE SCIENTIFICO-DISCIPLINARE: INFO-01/A, GIUR-09/A, ECON-07/A

PRESENTATA DA: MATTEO CURCIO

COORDINATRICE DEL DOTTORATO: Prof.ssa Paola Adinolfi

Tutor:
Prof.ssa Valeria Eboli

Firmato il 11/10/2024 alle 16:53da
VALERIA EBOLI

Co-tutor:
Gen.B.A. Alberto Surace

Firmato Digitalmente da/Signed by:
ALBERTO SURACE
In Data/On Date:
lunedì 14 ottobre 2024 12:34:10

ANNI ACCADEMICI: 2021/2024

INDEX

Glossary

AR- Augmented Reality

DS- Discord

VR- Virtual Reality

VG/VGs - Video game/s

MMOG/MMOGs - Massively Multiplayer online game/s

MMORPG/s - Massively Multiplayer online role play game/s

AI - Artificial intelligence

TS - Team Speak

SM - Social Media

GVE - Games and Virtual Environments

VW- Virtual worlds

Disclaimer

This work is the result of research activities conducted within virtual worlds in the gaming environment and Metaverse. This research requested the author to recover different types of material: audio, chats, pictures, and events within these platforms. In accordance with current legislation and international regulations, the author conducted his research in full respect of privacy and the law, censoring material deemed unpublishable, and/or any information that could harm others. As a result, some information and/or events the researcher witnessed could not be published, and therefore, no evidence of such events has been preserved.

1. INTRODUCTION

This doctoral thesis aims to bring to everyone's attention a phenomenon that, according to the systematic review, has yet to be studied sufficiently but can emerge as a problem for national and public security as will be illustrated in the following chapters. Digital innovation and the emergence of increasingly complex applications (E.g., Virtual worlds and complex Massive multiplayer online games MMOG) have profoundly changed the global scenario in terms of communication. In 2023, the gaming sector is expected to surpass 3 billion online users, about 40% of the world population (Wijman, 2020). These numbers, along with the evolution of gaming, produced new virtual worlds (see, e.g., Metaverse[1]) that can modify and create new ways of communication. Today, MMOG and related applications are standard means of communication among users; however, their structures are complex, unpredictable, and may raise safety concerns. These applications, in fact, can provide a fertile ground for different cybercrimes. Unlike social media (SM) or applications like Telegram, MMOG makes users completely anonymous and therefore may potentially allow them to perpetrate various cybercrimes remaining undetected, thanks to their functions. In recent years, with the advent of the metaverse, several institutional reports have raised concerns, highlighting that it could be fertile ground for mafias and criminals, forgetting, however, that the metaverse is the last of the thousands of virtual worlds that exist. It is true that with new technologies (AR-VR, blockchain, etc.), the metaverse stands out from other virtual worlds in terms of innovations, but it is not the only one capable of posing threats. Today, the term "metaverse" refers to two concepts: the metaverse conceived by Zuckerberg, that is a reality still in development, and the metaverse understood as a virtual world that everyone can create independently[2] (Bhatt, 2023). Both are virtual worlds, but while the first is yet an undefined entity, the metaverse as a virtual world has much deeper origins: the gaming world. Approximately twenty years ago, the first massively multiplayer online games appeared in the market, characterized by an open world and an alternative virtual reality, which implemented concepts from real life (e.g.: Second Life, the Sims) and are found today in the metaverse. Today's narrative neglects all of this, identifying the metaverse as the only virtual world capable of causing threats to national and public security, forgetting that thousands of other virtual worlds can also be maliciously exploited (Vanolo, 2021; Marler et al., 2023). Over the years, some rumors have emerged regarding the possible involvement of gaming as a threat to national security (Klippenstein, 2024); however, the problem has never been thoroughly

[1]An example of Metaverse can be found here: https://decentraland.org/

[2]The metaverse conceived by Zuckerberg is a concept that materializes with meta. However, this does not imply that meta is the only metaverse available; it is a concept that expands and produces new metaverses, whether or not they are related to gaming or industries. To date, different companies create thousands of metaverses, and it is possible to make one in just a few steps thanks to various providers around the web.

investigated at an academic level. The only accessible material about the matter is a classified report found among the documents released by Edward Snowden, which refers to intelligence activities conducted within these virtual worlds as early as 2008[3]. Therefore, are virtual worlds a problem for national and public security? How many virtual worlds exist, which one can represent a threat and how can they be illegally exploited? These questions represent the basis of the research path to investigate such virtual worlds to bring new knowledge and demonstrate that they can become an excellent tool for cybercriminals. Therefore, the main objective of this thesis is to demonstrate that virtual worlds can be used as a vector to commit different cybercrimes, can become a problem to national security, and tries to develop new knowledge and solutions for this problem. The methodology adopted for this research is netnography, combined with OSINT techniques. After an introduction to the topic, the results of a systematic review and an analysis of material found will be illustrated. Then, a contribution in terms of a solution to the problem will be proposed.

1.1 Towards virtual worlds: A brief history of the gaming environment

The early Seventies are called the years of the creation of the first virtual worlds, in which the foundations for creating alternative realities began to be laid. At this historical moment, the Internet is less developed than it is today, and everything is managed through ARPAnet, which is the precursor of the contemporary Internet[4]. The seventies were also the period in which some minds began to develop the idea of a more complex gaming network. 1977 marks the birth of one of the first consoles, the Atari 2600. Moreover, in those years, precisely in 1978, the Multi-User Dungeon (MUD) idea was born thanks to Roy Trubshaw and Richard Bartle (Sloane, 2000). The possibility of letting multiple users play simultaneously, creating connections between them in a parallel world, therefore begins to emerge. Given the significant development of the Internet in the 1980s, VGs began to develop multiplayer modes, and new consoles began to appear, such as the Commodore 64 (1982) and the first commercial MMOG created by Kelton Flinn and John Taylor -

[3]Among the documents published by Edward Snowden, it is possible to find a document classified as "top secret", which includes five intelligence searches carried out within virtual worlds linked to gaming.

[4]"Development of ARPANET began in 1966. Several standards were developed. Network Control Program (NCP) would handle communication between hosts and could support the first commands, Telnet and File Transfer Protocol (FTP). The first message sent over ARPANET happened on Oct. 29, 1969. Charley Kline, who was a student at the University of California Los Angeles (UCLA), tried to log in to the mainframe at the Stanford Research Institute (SRI). He successfully typed in the characters L and O, but the computer crashed when he typed the G of the command LOGIN. They were able to overcome the initial crash, however, and had a successful connection that same day. The first permanent connection between UCLA and SRI was put into place on Nov. 21, 1969. Two more universities joined ARPANET as founding members on Dec. 5, 1969. These were the University of California, Santa Barbara and University of Utah School of Computing. ARPANET grew rapidly in the early 1970s. Many universities and government computers joined the network during this time. In 1975, ARPANET was declared operational and was used to develop further communications technology. In time, several computers in other countries were also added using satellite links." (Wright, 2021)

Island of Kesmai (1985) (Radoff, 2010). After the launch of the first video game that could be used for 12 dollars an hour, through a service that allowed up to one hundred players to connect called CompuServe, the network service moved in parallel, and the Internet finally arrives (1983) (Zimmermann, 2022). The Eighties saw a slow progress with the launch of other consoles, such as Nintendo in 1983 and SEGA in 1987, and an increasingly connected network (from a thousand connected computers in 1984 to a hundred thousand in 1989) (Roser, 2024). In the 1990s, the first graphic MMOGs were born as slightly superior models capable of including a more complex graphic interface. Neverwinter Nights and Meridian 59 archetype were the first third-person graphic MMOG launched in 1991 (Bainbridge, 2004). In 1996, ten million computers were connected to the Internet, a race that will not slow down, and by 1999 will reach two hundred million users worldwide (Peterson, 2003). At the same time, the term MMOG was born, coined by Richard Garriott, the creator of Ultima Online, in 1997, inspired by the term used two years earlier by Dale Addink: MMO (Steed & Oliveira, 2010). From that moment, the term has been used to describe all those video games (VGs) that allow interaction between users, such as Meridian 59, Tibia, Ultima Online, and others. These video games are called the first generation of MMOGs. At this stage, many VGs are developed around the world, and the United States played an important role in the sector with the launch of "EverQuest," followed by South Korea with the launch of "Nexus: The Kingdom of the Winds," which already had one million subscribers in those years. Their success will lead the industry to understand the market's potential. At the beginning of the 2000s, an important transition occurred for the gaming industry: Introducing new MMOGs called the second generation. Between 2000 and 2010, the gaming industry saw the birth of hundreds of VGs that could make the most of the progress of the Internet, which in those years had almost two billion connected users worldwide. The new MMOGs allow users to play with unknown people worldwide, interacting and sharing experiences with them. Consoles also keep pace with this development, introducing various VGs incorporating new functions, including connecting to the Internet. The progress described leads to what is commonly defined as the current generation of MMOGs, which saw the light in 2010 and remains today. The VGs of this generation are by far the most developed in graphics and functionality, as they offer unique capabilities thanks to the complexity with which they are created. Their introduction brought numerous benefits to the gaming world and created a more dangerous market than previous generations. If previously there was a fixed cost to play these video games and the gaming experience ended once a hypothetical level was exceeded, today, this generation has introduced a parallel world inhabited by real users, with a completely alternative economy and reality. The introduction of MMOGs introduced several innovations that were difficult to imagine before their creation: from the Seventies to the Nineties,

VGs were single-player only, and the user could only interface with the Artificial Intelligence. From the nineties onwards, with the birth of MMOGs, the new parallel realities enabled the user as the protagonist. Before this, the most complicated challenge a user could face was defeating the machine. In contrast, today, users who play an MMOG are catapulted into an alternative reality where the character is the user himself. Consequently, the user finds himself having to face a reality specifically created to be shaped: he is the protagonist of the story, and he decides its course and who to be. These differences highlight that video games are not all the same, and different virtual worlds exist that can be played but also exploited.

1.2 Defining virtual worlds – mapping the gaming environment

'Virtual Worlds' is a term widely used to describe a computer-simulated environment (Bartle, 2003) populated by users' avatars who can interact and communicate with each other (Kaplan & Haenlein, 2009). An individual who enters a virtual world experiences sensory stimulation provided by a computer-simulated environment, which enables them to manipulate elements of the modelled environment and, as a result, experience a sense of presence (Singhal & Zyda, 1999). Furthermore, users inside these virtual worlds can communicate through text, graphical icons, visual gestures, sound, and rarely, through touch, voice commands, and balance senses. Among the first to be provided, these definitions have changed in response to technological advancements and the evolving gaming industry. In current literature, it is possible to identify two of the latest and most accurate definitions that describe virtual worlds. Richard Bartle (2015) proposes the subsequent concept:

"A virtual world is something with the following characteristics:

- It operates using an underlying automated rule set - its physics;
- Each player represents an individual 'in' the virtual world - that player's character;
- Interaction with the world takes place in real time - if you do something, it happens pretty much when you do it;
- The world is shared - other people can play in the same world at the same time as you;
- The world is persistent - it's still there when you are not; It's not the real world".

While Nevelsteen (2018) suggests that virtual worlds can be described as follows:

- "A simulated environment where many agents can virtually interact with each other, act and react to things, phenomena and the environment;

- Agents can be zero or many human(s), each represented by many entities called a virtual self (an avatar), or many software agents;
- All action/reaction/interaction must happen in a real-time shared spatiotemporal nonpausable virtual environment;
- The environment may consist of many data spaces, but the collection of data spaces should constitute a shared data space, one persistent shard".

These concepts, as well as elaborated by different authors (Bell, 2008; Castronova, 2005), are intended to provide a common ground toward a definition. However, an accepted definition has not yet been developed. Today, media and academics use the term virtual world to indicate different applications (video games, social media, applications, etc.), and it is often used interchangeably with many acronyms (virtual reality, digital world, MMORPG, etc.). In this environment, the idea of a virtual world is not well defined; most of these definitions are labels used to designate 'some virtual space,' and the linguistic register generally used indicates different meanings. Are all virtual worlds the same? What type of virtual worlds exists? Which main characteristics constitute a virtual world in the gaming environment? Are all the video games virtual worlds? Taking the aforementioned definitions as a starting point, this chapter aims to develop a comprehensive and accurate classification for virtual worlds in the gaming environment based on their structure and typology.

1.2.1 The meaning of Virtual

Virtual is a word often used to describe a place that does not exist physically: something created by computer technology and appearing to exist but not existing in the physical world (Cretu, 2022). Also, it can be considered as anything that is mediated by or brought to existence through a digital game (Bösche & Kattner, 2011); It is something that has no place in reality, does not exist in reality, but is designed in the mind (Tuncer, 2020); Not physically existing as such but made by software to appear to do so (Alam, 2021). The word *Virtual* is also interpreted as images of real places and objects (Almeida, 2008); Any activities that occur online (Shelby-Caffey et al., 2021); Interactions that are done online (Amponsah et al., 2021); And an environment simulated by electronic networks for reasons of economics, convenience, or performance (Switzer, 2008). Therefore, looking at the previously mentioned definitions along with others (Gesche, 2009; O'Connor, 2012; Lange, 2008; Benjamin, 2015), it is possible to summarize that *Virtual* is something that exists as a simulated experience without physical properties.

1.2.2 The meaning of World

World is a term that encompasses many meanings and is interpreted differently according to reference theories. For those scientists who study the universe, the world is the totality of space and time (Zeilik & Gregory, 1998; Mittelstraß, 2005; Sandkühler & Borchers, 2010), while for phenomenology philologists, the world incorporates the perceptions and experiences that surround an object (Smith, 2018), making the world becomes the horizon of all the horizons (Embree, 1996). In the history of philosophy, this word has also been conceptualized in different ways:

Plato: 'The world that appears to our senses is in some way defective and filled with error, but there is a more real and perfect realm, populated by entities (called 'forms' or 'ideas') that are eternal, changeless, and in some sense paradigmatic for the structure and character of the world presented to our senses' (Kraut, 2022).

Eugen Fink: 'The world is the totality of the inner-worldly things that transcends them (Halák, 2016). It is itself groundless, but it provides a ground for things. It therefore cannot be identified with a mere container. Instead, the world gives appearance to inner-worldly things, it provides them with a place, a beginning and an end (Homan, 2013). The definition of Heidegger, which discusses the 'Being-in' concept in the world, is also important: 'What is meant by 'Being-in'? Our proximal reaction is to round out this expression to 'being-in' 'in the world,' and we are inclined to understand this being-in as 'Being in something' as the water is in the glass, or the garment is 'in' the cupboard. By this 'in' we mean the relationship of being which two entities extended 'in' space have to each other with regard to their location in that space. Being-present-at-hand-along-with in the sense of a definite location-relationship with something else which has the same kind of being, are ontological characteristics which we call 'categorial' (Heidegger, 1962).

In brief, summarizing the definitions above, it is possible to state that the world consists of an *interactive, shared, spatial and temporal* dimension populated and shaped by entities where experiences are mediated through physical bodies.

1.2.3 The current debate

The current scientific literature does not define precisely what can be considered virtual worlds and what is not; instead, it tries to define what is a virtual world. In a three-page paper written by Schroeder, the outcome is that virtual worlds are 'environments that people experience as ongoing

over time and that have large populations which they experience together with others as a world for social interaction' (Schroeder, 1980). Consequently, in his paper, online gaming and Massively Multiplayers Online Role-Playing Games (MMORPGs) were not considered virtual worlds but rather a subset of them. In 2008, in a five-page work, Bell identified a definition for virtual worlds that later would become the most cited: 'A synchronous, persistent network of people, represented as avatars, facilitated by networked computers.' (Bell, 2008) This work also presents the five characteristics that a virtual world must have to be so-called, and in this case, contrary to the previous one, it is stated that MMORPGs are virtual worlds[5]. Among these, a more recent article by Girvan gives another definition of virtual worlds: 'Shared, simulated spaces which are inhabited and shaped by their inhabitants who are represented as avatars. These avatars mediate our experience of this space as we move, interact with objects and interact with others, with whom we construct a shared understanding of the world at that time' (Girvan, 2018). Therefore, she argues that MMORPGs are not virtual worlds but can exists within them. The first two works present their argumentation without methodology as they are brief essays, while the last one offers a conceptual framework for what is intended to be a virtual world based on previous literature. In different research (Boulos et al., 2007; Stevens, 2015; Keene, 2011; Chambers-Jones, 2018), virtual worlds are used as a synonym for MMORPGs, while as previously seen, many others do not think that they should be considered virtual worlds. There are, therefore, two fundamental problems arising from this framework: All the literature that has been presented is controversial as there is no agreement on what virtual worlds are, and none of these clearly defines what a virtual world is: besides a few hints that can be found in the work of Bartle, the literature only focuses on the characteristics that virtual worlds should possess. Consequently, the following elaboration is the author's work.

1.2.4 Video Games essential characteristics

Although video games are different among each other, they all possess specific essential characteristics:

- Online: as a result of the nature of online video games, players can interact with other players and engage in cooperative and/or competitive activities;
- Offline: players, in this case, cannot interact with any others and can only play the game as it is;

[5]In the paper, the author states the following: Environments that are virtual worlds include MUD-1, Neverwinter Nights, Second Life, World of Warcraft, and the upcoming Hello Kitty Online. Therefore, since Neverwinter, Second Life, and Word of Warcraft are MMORPGs, that category is included in virtual worlds.

- Single player: in a single-player game, the player can only interact with the virtual environment proposed, completing different activities;
- Multiplayer: players can interact with others locally or online in a series of activities proposed by the video game.

These four elements are the common ground for every video game, and they can establish relationships between them:

A single-player video game can be - online and offline, a multiplayer video game can be - online and offline, therefore, a video game can be online and/or offline, single-player and/or multiplayer. These elements constitute the first layer of the reference theory of this study.

1.2.5 Video game Categories

Each video game can be classified into categories, that is, the macro container in which video games are collocated and constitute the second layer of the framework elaborated by the author:

- Video games

This label is given to video games without much specification, but it should be correctly used to indicate a video game that does not possess other characteristics. For example, the correct allocation should refer to single-player or multiplayer video games without access to the internet (retrò games, simulation games, etc.).

- Video games online

These video games grant access to a wide area of gameplay thanks to the internet. It allows players to simultaneously play together or against and interact in a specific environment. Moreover, these games do not always need to be bought physically but can be accessed by the sole internet.

- MMOG

Massively multiplayer online games represent the latest frontier in gaming. These video games differ mainly in the number of players; a dedicated server can host thousands of players who interact, fight and cooperate. In addition, they feature a persistent open virtual world.

- MMORPG

Massively multiplayer online role-playing games are the same as MMOG but incorporate role-play.

Video games Typologies

Typologies are the gaming style of a video game, and they can be declined as follow:

- MOBA

(Multiplayer Online Battle Arena): players control a certain character who fights against other players; the game's goal is to win against the opposing team by destroying the enemy's core.

- FPS - TPS

(First person shooter - Third person shooter): is a video game where players play on specific maps and perform various actions, such as eliminating other players or the AI.

- RTS

(Real-Time Strategy): is a video game where players maneuver units of populations, armies and build their world in real-time.

- RPG - ARPG

(Role Play Games - Action Role Play Games): video games where a player creates a character and controls it in a world that can be fantasy or realistic.

- Action and Adventure

This video game allows players to play an immersive experience with the character created inside a world, elaborated for gaming purposes.

- Survival

In these video games, players must survive against something or someone. The environment can be realistic or fantasy.

- Horror

These video games often collide with the survival ones, but they can also be pure horror.

- Battle Royale

In these games, people fight to victory in a pre-determined word/map.

In addition to these typologies, there are many more, but only a few have been reported. These Typologies are the third layer of the theory.

1.2.6 Video games Dimensions

As a result of the analysis of these virtual worlds, it was possible to determine that these environments consist of three different dimensions, according to the author.

- Environment Dimension: This dimension includes the internal environment of video games, specifically the map and the world. The world is the macro container where the video game

is set (e.g., Tyria is the world of Guild Wars 2, like Azeroth is the world of World of Warcraft), while the map represents a place inside the world. On the map, it will be possible to find different locations and spaces. The 'Time' is also considered part of this dimension. The environment must be persistent.

- Economic Dimension: In this dimension, all the economic interactions between the subjects who populate the videogame to satisfy their needs are included. Therefore, an economy regulates the video game using virtual currency.
- Social Dimension: This dimension contains all the social interactions that occur between users (e.g., chats-parties)

These dimensions always present inside a virtual world constitute the fourth layer of the framework.

1.2.7 Combining the Layers

In this section, a Venn diagram illustrates the logical relationships among the elements listed above. This diagram was developed by Jhon Venn in the 1880s and is frequently used to illustrate logical relationships between sets.

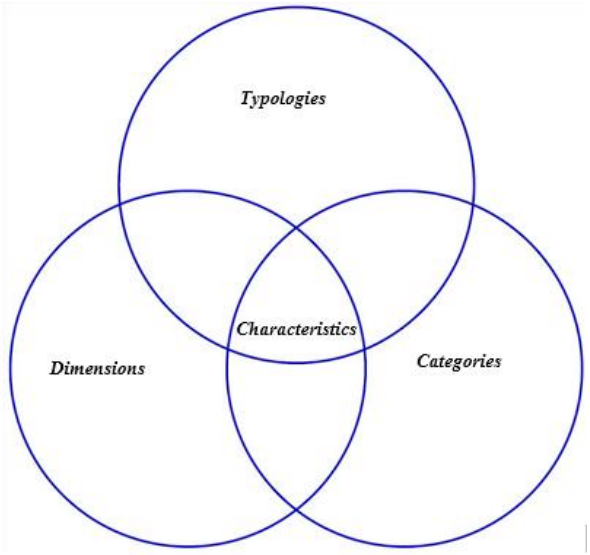

Figure 1: A Venn Diagram representing the layers. Elaborated by the author.

The Diagram illustrates a close interdependence among the four layers, with the 'characteristics' being the common thread that connects them all. These layers comprehend different specifications and serve as a categorization for determining which video game can be categorized as a virtual world. Therefore, a new framework can be developed to determine which video game is a virtual world.

1.2.8 A new conceptual framework

When can video games be considered a virtual world, and why? Moreover, what makes a video game a virtual world? Connecting all the points discussed above, it is now possible to develop a new approach that can help to categorize virtual environments correctly. To determine if a video game is a virtual world is sufficient to follow the layers illustrated in Figure 2 and connect the points.

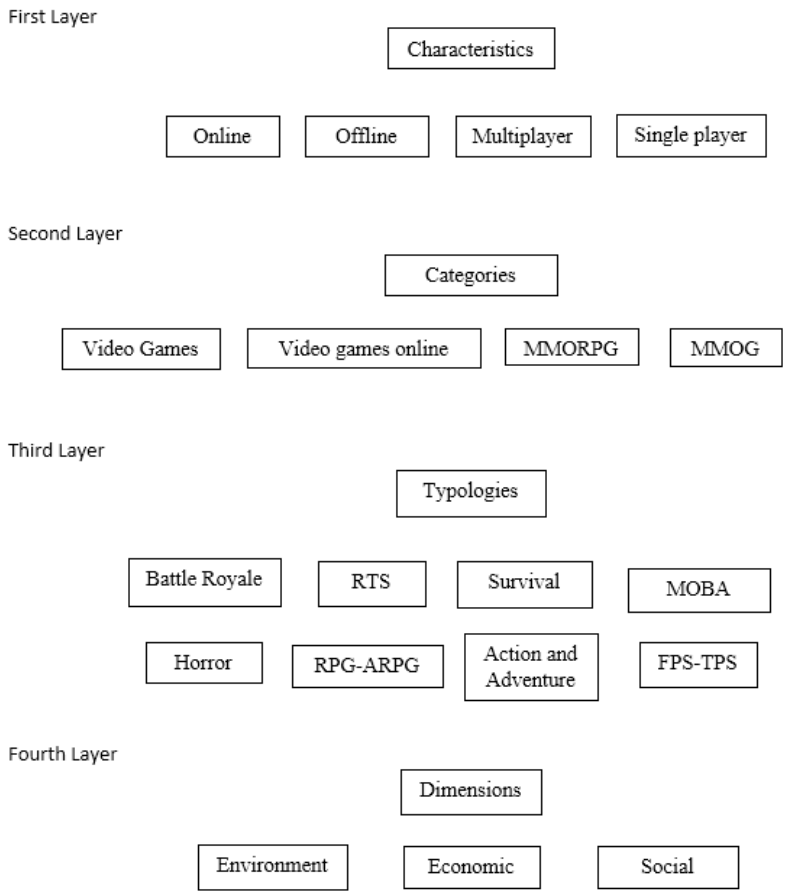

Figure 2: The full scheme. Elaborated by the author.

Therefore, in determining which video game or environment is a virtual world, the first step is to start from the first layer and categorize the object, then move to other layers according to the object characteristics. In detail, using an example, the process (Figure 3) would be as follow:

Is Fortnite a virtual world?

- First step: Define the characteristics of the video game; in this case, it is multiplayer and online.

- Second step: determine in which category this game falls. In this case, Video games online.
- Third Step: Define the typology of the video game: Battle Royale.
- Fourth Step: Are all the dimensions present? In this case, Fortnite does not possess all these dimensions. There is the social, but it does not contain the environment and economic one.

Therefore, according to this scheme, Fortnite is not a virtual world.

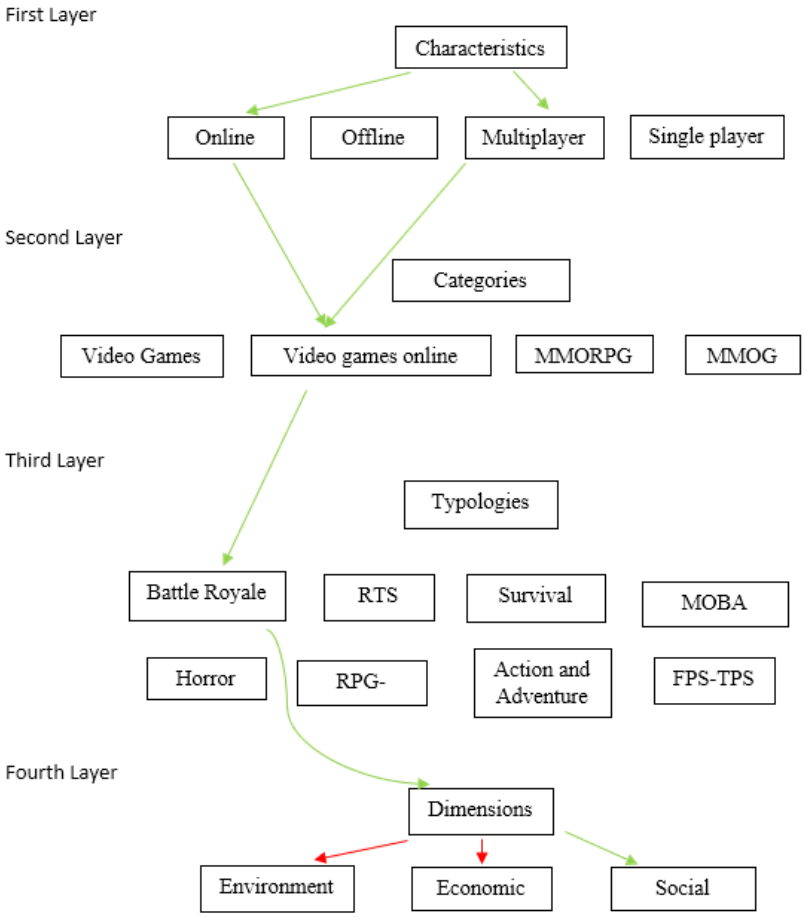

Figure 3: The steps to take to determine the nature of the video game. Elaborated by the author.

To be classified as a virtual world, a video game that reach the fourth layer, must include all three dimensions without exception. A video game that stops before the end is not considered a virtual world. Without further instructions, this scheme can be used for every video game and gaming-related content. As a result, the findings show that it is possible to determine whether a video game is a virtual world and what is the fundamental characteristic that makes it a virtual world.

1.2.9 Towards a Definition of virtual world in the gaming environment

According to Bartle (2015) and Nevelsteen (2018) definitions mentioned above, a virtual world must possess several characteristics to be considered such. These characteristics are the basics for

every virtual world, but neither they nor others in the current literature have developed a clear pattern to determine whether a video game can be considered a virtual world. Also, many works do not consider MMORPG or other kinds of video games virtual worlds. Consequently, this framework argues that a virtual world in the gaming environment can be correctly determined by following this scheme and that the variables that allow identification are the dimensions. Considering, therefore, the definition of Bartle as a basis, a virtual world in the gaming environment can be declined as follows:

- It must operate under underlying automated rules, its physics.
- Players are represented by an avatar, that is the player character.
- All the interactions in video games considered virtual worlds happen in real time.
- A video game that is also a virtual world must have an environmental dimension: a world, a location, and a time that can be shared; other people play in the same world simultaneously.
- The environment dimension is persistent and will always be there.
- A video game considered a virtual world must have an economic dimension regulating the video games and the users' daily life.
- A video game that is a virtual world must possess a social dimension where users interact.

Consequently, a virtual world in the gaming environment is:

A shared interactive open world populated by avatars governed by environmental, economic, and social dimensions.

In this regard, different virtual worlds exist because of their differences in categories and typologies, but the dimensions remain the inalienable cornerstone for a virtual world. Considering the literature cited above, it is evident that the interpretation of these environments is controversial, but the data collected and analyzed during the years inside these environments allowed the creation of a new framework. According to the scheme developed based on these results, video games can be classified according to specific characteristics, and even though the scheme may be criticized and interpreted in various ways, it provides the only theoretical starting point currently available. In addition to clarifying which video games can be considered virtual worlds, this study also indicates that each MMORPG is a virtual world since its structure reflects the real world but is situated in a fictional setting. The tests conducted show that every MMORPG currently on the market, old or new, reaches the bottom of the scheme, consolidating the theory that MMORPG represents the ideal virtual world. In conclusion, not all video games are virtual worlds, not all gaming environments represent a virtual world, and it is possible to have different virtual worlds determined by categories

and typologies. Also, in some cases, a few applications resemble a virtual world but are not considered one.

1.3 Understanding virtual worlds: A look inside MMOGs.

The most important aspect MMOG introduced, which then gave rise to the acronym, is the number of players that can be contained in a server communicating with each other. If previously VGs could contain a few hundred people connected simultaneously, today, we have moved on to several hundred thousand people connected in real-time. Depending on the peculiarities of each company producing the individual VG, all these users will be hosted on dedicated servers, which can be distinguished based on language, continents, or a single server capable of hosting anyone. These flows of people serve to create the alternative reality and economy that will govern the virtual world. In the alternative reality of MMOG, the economy created within them, and the economy of the real world intertwine, creating a unicum. To understand what alternative reality means or how virtual worlds work, an MMORPG called Guild Wars 2 will be used as an example. To enter any virtual world, the first thing to do is to create an avatar/character that will represent the user within the virtual world. Each VG or Metaverse will make character creation available to the user based on its characteristics. Sometimes, there is no character creation, and the users must use a character already prepared by the AI, to which the users will only have to assign a nickname. Therefore, every virtual world user will possess a nickname and an avatar/character.

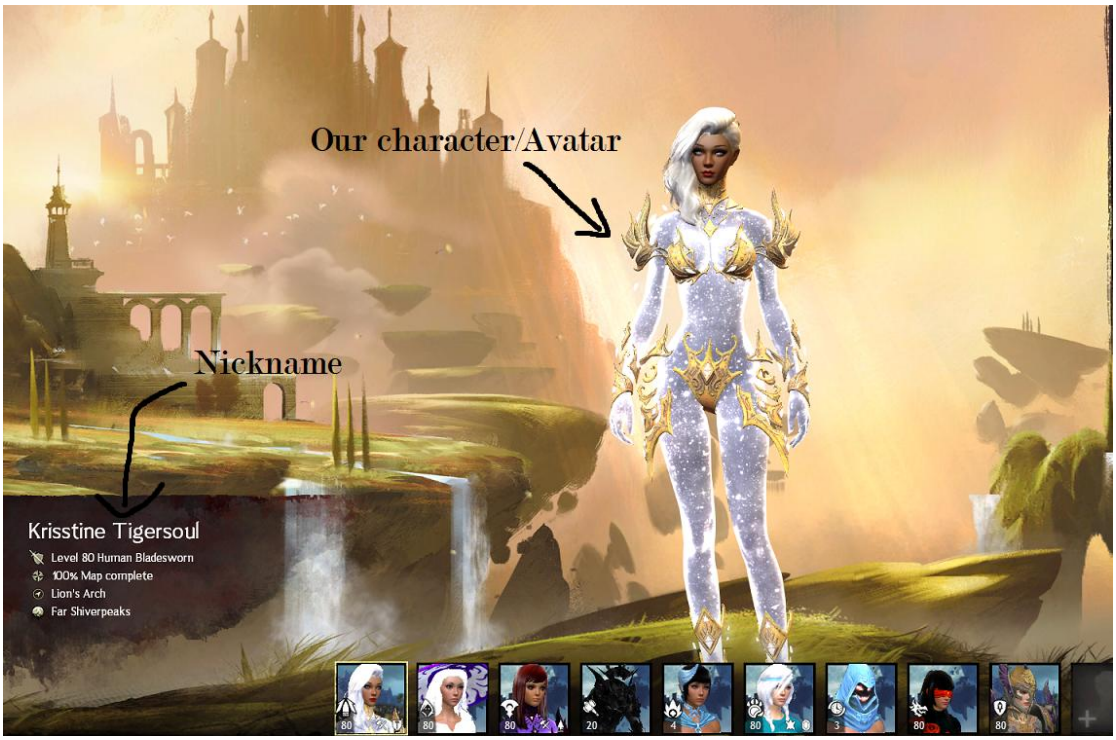

Figure 4:Avatar/character that will represent the player in the world of GW2. Elaborated by the author.

As shown in Figure 4, this is the character created that will allow the user to enter the world of Guild Wars 2. In this case, the character is female and has been assigned a female nickname. Since GW2 is a fantasy MMORPG, it is also possible to choose the race (in this example, human) and make a male.

As previously mentioned, each virtual world has an environmental dimension where players can move and interact. The map shown in Figure 5 illustrates Tyria[6], the world of Guild Wars 2.

[6]The map is cut off to the south because it was impossible to report it in its entirety for space reasons.

Figure 5: "Guild Wars 2" - World Map: Tyria. Elaborated by the author.

Tyria is not a freshly generated map but rather the world that players are placed in, so like the real world, it is always alive, and time flows as it does on Earth. So even when a user with his character logs out, it continues to live and will keep moving forward. In Figure 6, the created character is now inside the VG, and it is possible to notice the presence of other avatars connected. In the game, the character will be free to move and interact with other users and the world around him. This freedom creates two peculiarities that are the basis of all virtual worlds: communication and the alternative economy.

Figure 6: Character inside GW2. Elaborated by the author.

1.3.1 Communication within MMOGs.

Within virtual worlds, communication is a fundamental element in the interaction between users, which helps the execution of game actions, but not all virtual worlds host the same functions; each has different characteristics and contains various methods of communication. However, MMORPGs are the most complete ones that offer users the most significant possibilities. Communication methods can be divided into two macro-categories:

● classic chat: a chat that allows users to write and contact other players.

● voice chat: a chat that allows users to talk to other players.

The classic chat can be divided into different subgroups, which can be used according to the needs of the players. In most virtual worlds, especially MMORPGs, there will be:

- Server chat: It is a chat where what is written is visible to all the people present on the server, i.e., to all those players who play that game and who have chosen to play on that specific server (e.g., Europe or America - server name).
- Group Chat: It is a chat that works only when a group is formed, and only its members can read what is written. Group chat includes all those chats in which two or more people participate.
- Private chat: It is a private chat between two players; the exchange of messages is bi-directional, and what users write to others can only be visible to the recipient and the sender.

- Local chat: It is a chat that can be used by the character at any time and is visible to everyone within a certain radius of the player's position on the map.
- Guild chat: It is a chat that can only be used by members of a clan or guild (in MMORPGs and other VGs, users are often grouped into guilds or clans), and what is written is visible only to their members.
- Global chat: It is a chat where anyone can read what is written. (This is typically a chat in VGs that do not have servers divided by user region).

Along with various text chats, voice chats are also available in VGs. They can be accessed within the VGs or through related applications, which will be explained later. Unlike text chats, voice chats do not have subcategories and are used for communication through headphones and microphones.

1.3.2 The alternative economy of MMOGs.

Based on the virtual world a user has entered, he will have to deal with the economy present within it, which is closely connected to the real world. In every virtual world, an internal currency governs it, so all exchanges and/or transactions occur thanks to a specific currency tied to that VG. The currency will have fictional names or be based on reality, but it is strictly connected to the real currency, which will differ from the user's country of origin. Returning to the previous example made with GW2, the following pictures will demonstrate how this currency system works.

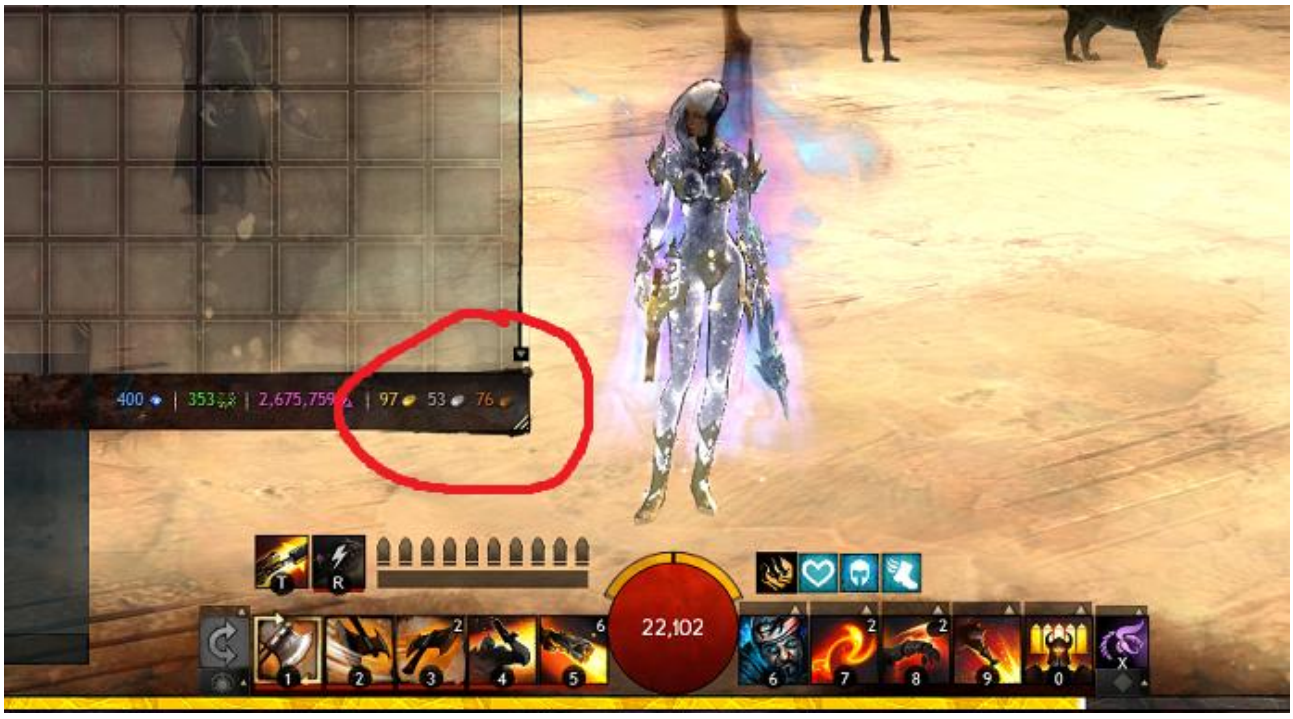

Figure 7: GW2 in game currency. Elaborated by the author.

Figure 7 shows the character's internal GW2 currency, highlighted in red, amounting to 97 gold, 53 silver, and 76 coppers. This currency is used to buy various objects within the VG from other players and from the game Marketplace. As stated before, this currency is interconnected with real ones as companies aim to generate income with their VG and, consequently, introduce an alternative marketplace created directly by them, where items are sold in exchange for real currency. In GW2, the virtual currency that can be purchased with actual money is known as gems. In Figure 8, it is possible to see the amount of gems that can be bought by spending euros. This currency, once purchased, will have the same function as the in-game currency but will allow the user to customize their gaming experience with premium items and/or other benefits.

Figure 8: Amount of Gems obtainable with Euro. (inside GW2) Elaborated by the author.

In addition, it is possible to convert the gems with the internal currency of the VG and vice versa, as shown in Figure 9.

Figure 9: Gems to gold conversion.in GW2. Elaborated by the author.

Both elements showed in this section introduce some of the peculiarities of virtual worlds, which will be further explored in subsequent chapters concerning their exploitation in cybercrime.

1.4 Gaming related applications

Applications related to video games are platforms created to facilitate communication between players that enable functions similar to those of a virtual world, even though they are not. These applications can be divided into two categories:

- Directly associated;
- External.

The first category concerns those applications created by the same company that produces the virtual world and which are opened simultaneously or, in any case, before the virtual world's launch. These applications function as a warehouse containing everything a user has downloaded, such as VGs and the friends list. Not all are the same; some offer different functions, but in general terms, the possible functions are interaction via both vocal and written chat, purchasing and/or exchanging currency. The second category consists of applications that are not integral parts of virtual worlds but are opened separately by the user. The functions are comparable to instant messaging programs, with some differences. Among the most used directly associated applications, there are:

- EA (formerly Origin);
- Steam;

- Epic Games launcher;
- Battlenet;
- Others like GOG galaxy, itch.io, Xbox (beta), Uplay, Bethesda launcher.

In detail, taking steam as an example, in Figure 10, it is possible to notice:

1. The username at the top left that represents the user;
2. At the bottom right, the "friends and chat" section.

Clicking on any friend in the friend list will open chat functions, which will be either vocal or written.

Figure 10: Friendlists and Chat options in Steam. Elaborated by the author.

Consequently, for each directly associated application, the user can take advantage of these functions remaining outside the virtual world but still in close connection. In fact, the avatar, account, or username used on these platforms represents the user within the virtual world. However, the situation is different with external applications, which require further elaboration. Unlike those listed previously, these applications are not part of virtual worlds nor integrated into them; therefore, users need to download such applications like any other software and use them simultaneously. These programs were created to facilitate communication within VGs and virtual worlds, with functions that are often more convenient and faster than those of virtual worlds. Among them, two stand out in particular for the number of users who use them and their functions: Discord and Teamspeak. Discord, founded in 2015, is an application created for gaming, which

makes voice or chat communications easier for gaming purposes. Over the years, this application has seen a significant increase in revenue and number of users. In 2021, it was estimated to have 140 million monthly active users and 13.5 million active servers (Curry, 2020). Discord is a friendly user application that can be installed on PCs or Phones, has a download size of 67MB (But 1 GB of Free space is needed), is accessible by creating an account, and offers different functionalities, as illustrated in Table 1.

Chat: Users can chat with other users through written messages.
Send files: Users can send direct documents, images, or others for a total size of 8MB, or 100 MB for Nitro version.
Share files: Like other messaging apps, users can also share bigger files or links with others.
Call: Users can call each other without a time limit.
Videocall: Users can video call each other without a time limit.
Create a server: Users can create a private server and invite other users.
Join other servers: Users can join different servers dedicated to a specific topic.
Stream/Sharing content: Users can stream or share any live content with other users.

Table 1: Discord Functionalities. Elaborated by the author.

Users who access Discord must create an account with an email, accept the Terms of Service, and use its online identity to move into the platform. Like all the gaming industry providers, the Terms of Service of Discord prohibits using the platform for illegal content and tries to protect the users with some monitoring. Discord messages, for example, are stored in an extensive database named Cassandra and remain available to the admins as long as the users do not delete it; once deleted is not possible to retrieve it. When a fake or real account has been created, within Discord, any user can start creating private servers among the options available. In this case, for purely informational purposes, a private server will be created to illustrate its functionality.

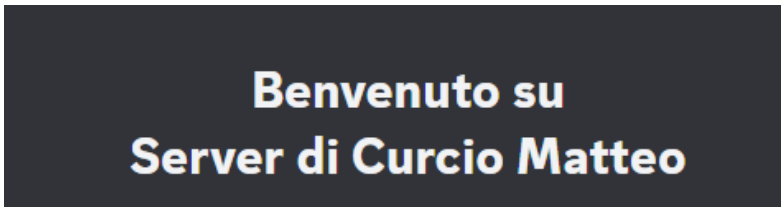

Figure 11: Opening messages of the private server created in Discord. Elaborated by the author.

After creation, a welcome message will appear, as illustrated in Figure 11, and the user can now navigate inside it[7]. Many options are available to the users, including creating additional private rooms equipped with passwords and containing voice or classic chat.

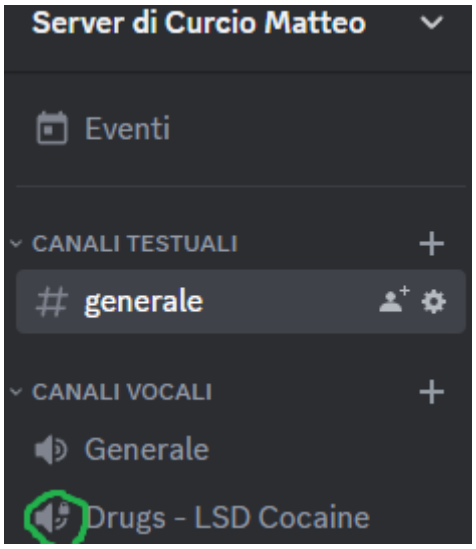

Figure 12: Example of channel created within the Discord server. Elaborated by the author.

In Figure 12, it is possible to observe a channel created within the server, and the icons illustrated indicate a voice closed channel that requires a password. Therefore, it is possible to enter the server only by invitation, in the channel with a password, and communicate only vocally, without chatting. These possibilities create potential security risks and questions: Who monitors these conversations and the interactions in these channels? While some messages can be recovered through Cassandra, no method can record the conversations through Discord, and unfortunately, despite the efforts of the company to prevent illegal behavior, it is extremely easy to exploit this application to commit different crimes, as will be illustrated in the following chapters. Another application that is not very well known but used in large numbers is Teamspeak, which offers similar solutions to the one previously analyzed. Unlike Discord, TS can only be used from a PC and was also created to facilitate competitive communications between players and is not to be considered a messaging application. To use Discord, the users need to create an account, while for TS, that step does not exist; the users need to download it, and it is ready to use[8]. Once downloaded, the user will find himself in front of the screen illustrated in Figure 13:

[7]The server's name corresponds to the author of this thesis to facilitate understanding, but it is possible to call the server in any way and change it at will.
[8]Today, a more recent version of Teamspeak is in beta, which requires registering an account but not replacing version 3, the current one. The new version lends itself to being very similar to Discord.

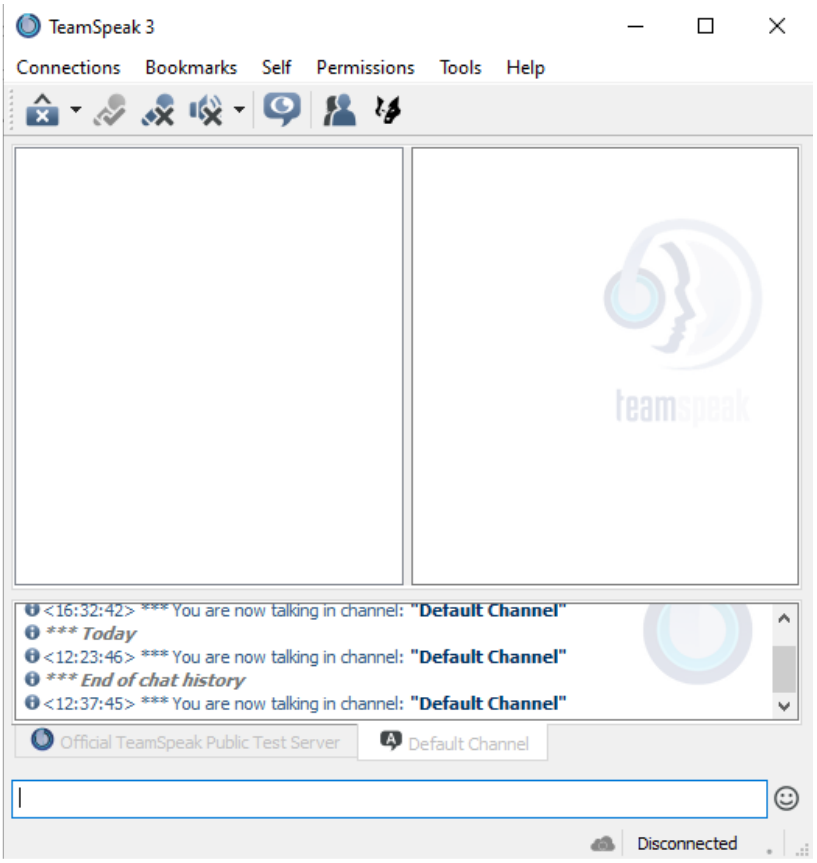

Figure 13: TeamSpeak Home page. Elaborated by the author.

By clicking on Connections, it will be possible to choose a nickname and connect to public or private servers, characterized by further rooms, which are protected or not by password. Furthermore, in TS, a list of geolocalized servers is scattered worldwide, where a user can access them without constraints.

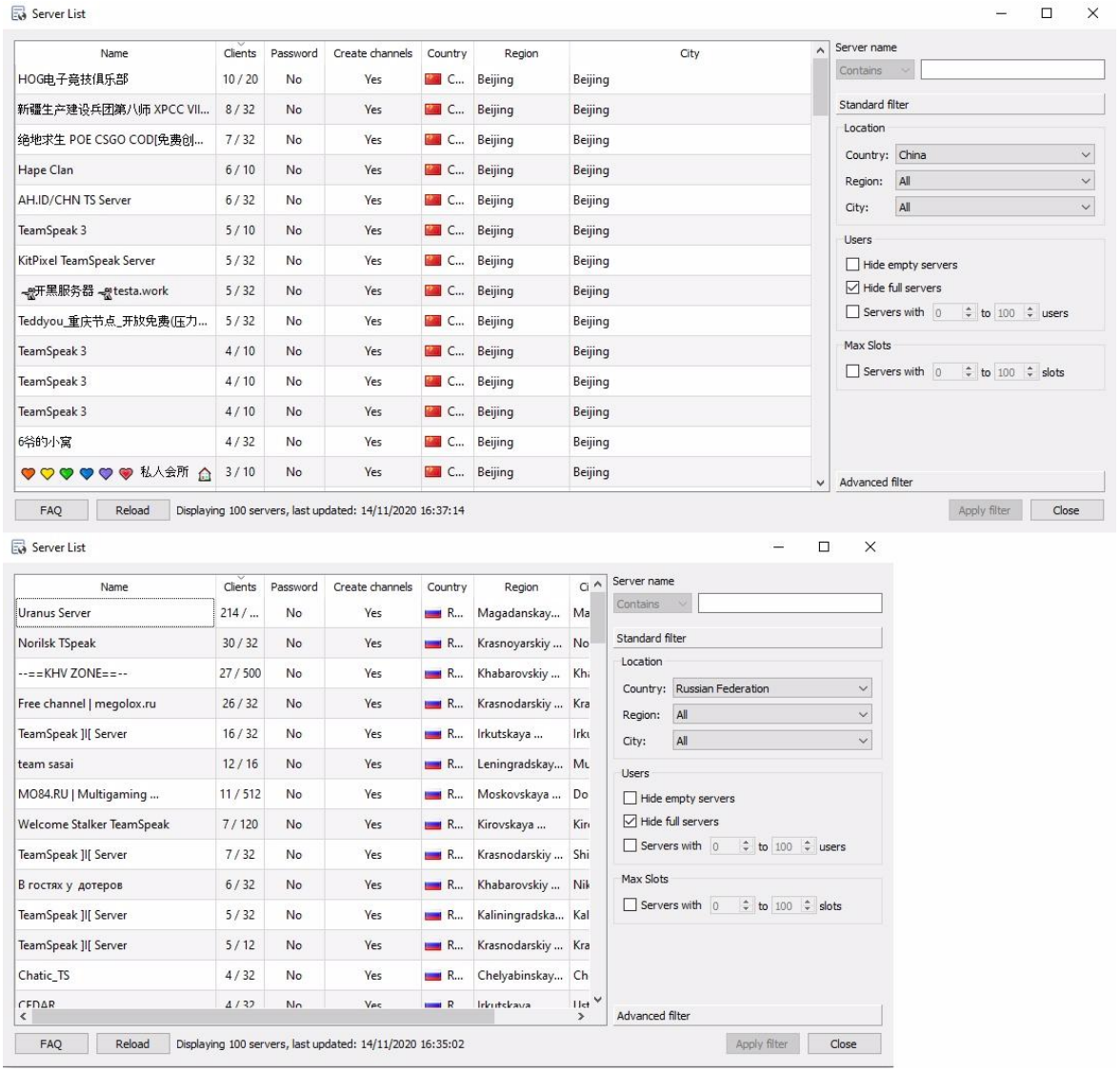

Figure 14: Part of the lists of Russians and Chinese servers. Elaborated by the author.

Figure 14 shows a part of the list of servers in China and Russia, with the related options, therefore equipped or not with passwords, and how many users there are on each server. Once inside the server, as with Discord, users can create additional rooms protected by passwords and accessible only to those who own them. There are private and public servers, and sending messages is possible even though it is not a messaging application. Furthermore, the possibility of recording what happens within personal channels has recently been added. In conclusion, TS, despite being a little-known tool, is widely used to communicate with users worldwide and can be used for non-gaming purposes.

1.5 The Metaverse

In 1992, Neal Stephenson defined in the book Snow Crash the Metaverse as a virtual world where users create and interact through avatars (Stephenson, 1992; Grimshaw, 2015). Today, after Zuckerberg's announcement (Milmo, 2021), the Metaverse has become a household word, but there still exists a lot of confusion about the term and its implications; the media confuses the word "Metaverse" with "the Metaverse",[9] and institutions often do not grasp its real potential. "The Metaverse" has at least two meanings, a bit like the term "Web." We can speak of it as a new platform, understood as that digital space where the experience is virtual, three-dimensional, immersive, and with (limited) kinetic and tactile possibilities. But it can also be spoken of as a specific metaverse (note the lowercase m) different from another: imagine the metaverse of a fashion house and the metaverse of an FPS (First-Person Shooter) game. In short, just as there is the Web and there are websites, there is the Metaverse and the "metaverse sites". Anyone trying to build the Metaverse probably refers to the ambition of providing *the* interface to the Metaverse and its metaverses. A bit like building *the* browser to access the Web" (Floridi, 2022). The Metaverse aims to become the future virtual world based on augmented and virtual reality, implementing technologies such as NFT and blockchain. However, as seen previously, it is not the only one, and the foundations from which it starts are those of a classic virtual world. But how does it work? Today, there are many metaverses on the market, each with its own rules, and for this example, the sandbox metaverse will be illustrated. The sandbox is a virtual world similar to MMOGs like Roblox and Minecraft, characterized by pixelated graphics.

[9]The metaverse is what Zuckerberg announced, a project about an interconnected virtual world. When we refer to the metaverse, we are talking about this. Different is when we talk about metaverses, which can be considered subgroups or by-products of the metaverse. They reflect characteristics of the metaverse but are specific and created by companies or individuals. For example, there are currently more than 160 metaverses of different societies. (https://insidetelecom.com/how-many-metaverses-are-there/) So, in the end, we have "The Metaverse," which is the idea of Zuckerberg and other Metaverses that encompass the same characteristics but are applied in different contexts.

Figure 15: Avatar created to enter the metaverse. Elaborated by the author.

Entering the Metaverse, it will be necessary to create an avatar, as illustrated in Figure 15. Once the character has been created, the user will be able to navigate the map of that Metaverse, illustrated (only partially) in Figure 16.

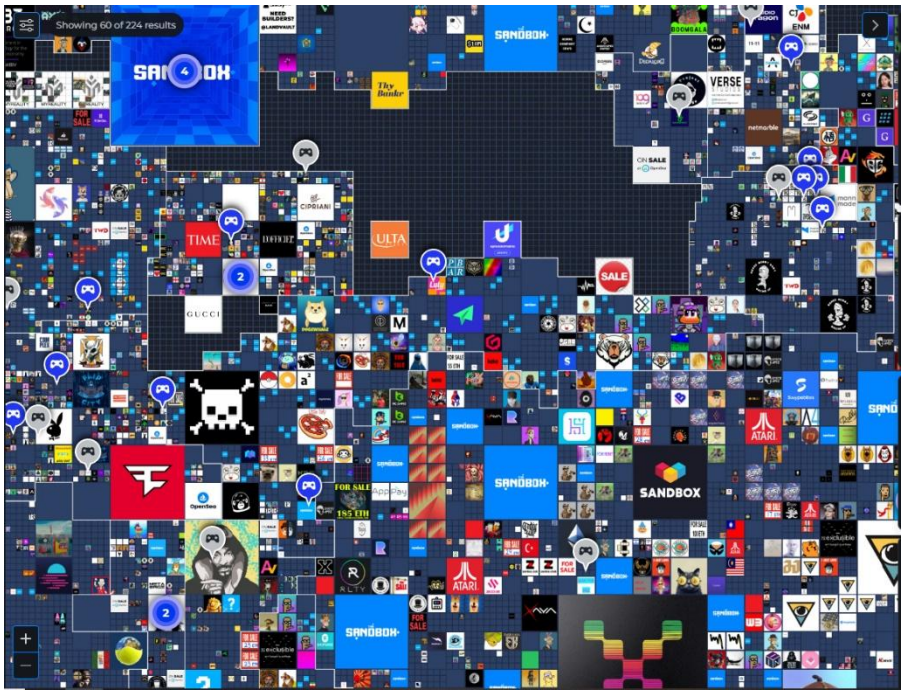

Figure 16: The Sandbox Map. Elaborated by the author.

In the image, it is possible to notice a grid map with different realities inside the squares that correspond to different metaverses. For example, clicking on one of those squares will open the area description and, for some, the "play" option. Once clicked, the user will enter that space, as illustrated in Figure 17.

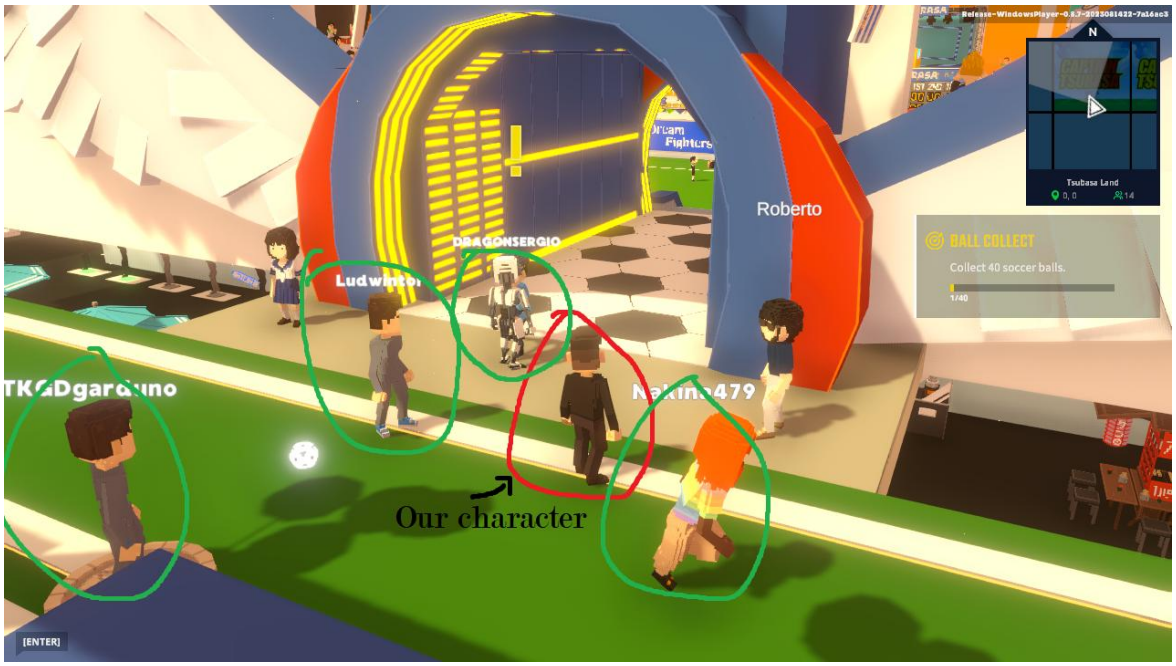

Figure 17: The user's avatar inside a square resembling football activity in Sandbox. In green circles, other users. Elaborated by the author.

This Metaverse is reminiscent of what was previously illustrated, that is, some video games, which also represent virtual worlds, but the difference that the Metaverse brings is augmented reality. With that example, Metaverse seems more like a video game, and one would not appreciate the potential of an augmented reality visor, but there are metaverses where this logic changes. For example, the metaverses used via Spatial.io are completely different. To access them, as with all other virtual worlds, it is necessary to create an avatar, and users can also do this via the camera, which will take a photo and recreate an avatar as faithfully as possible. Once users have the avatar, entering the Metaverse is very simple, and if the users also wear an augmented reality device, the experience will be closer to a real virtual world.

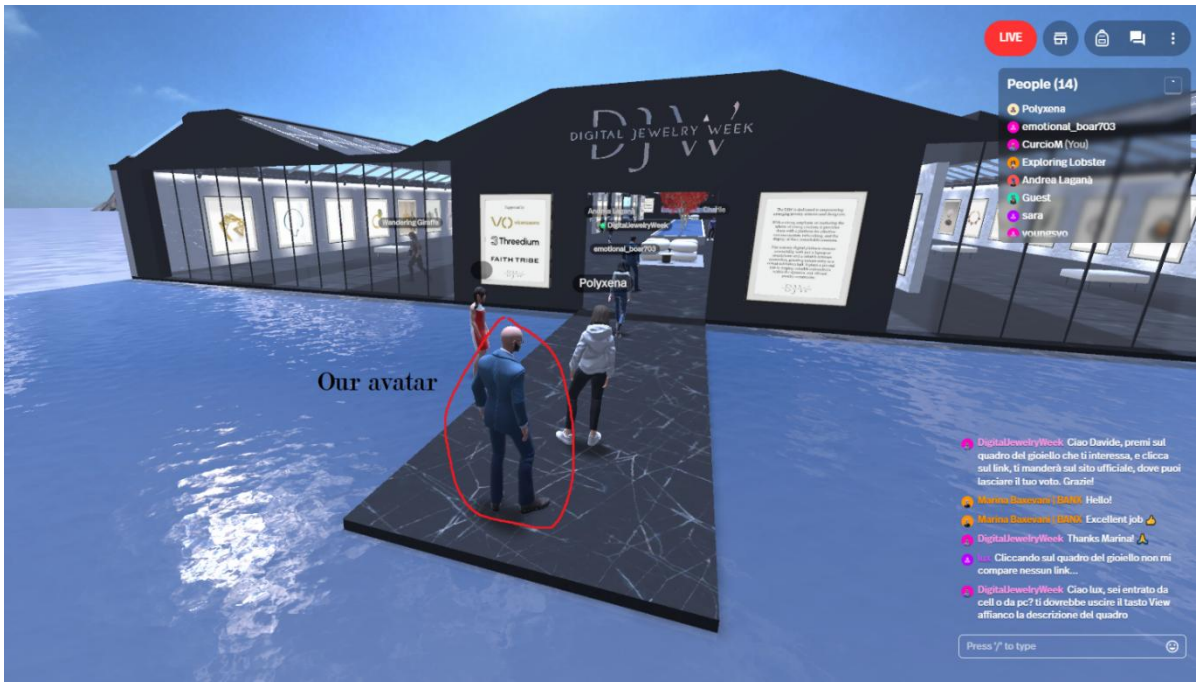

Figure 18: User Avatar inside the metaverse –DJW. Elaborated by the author.

In Figure 18, the avatar is inside a metaverse created especially for an event called Digital Jewelry Week, which is a jewelry exhibition. All interested people can comfortably enter the Metaverse from home and view the exhibition without having to be there physically, and with an augmented reality viewer, everything will recall an experience very similar to reality. Inside it is then possible to exploit NFT, blockchain technology to buy/sell and exchange currencies, just as if the user were inside a shop, or commit different cybercrimes[10]. In conclusion, it is possible to have many metaverses, each with its characteristics varying in reality, but all sharing logic that arises from the VGs and which are modulated and innovated. Therefore, the metaverses are virtual worlds that can be divided into typologies, but to be such, they must respect the dimensional and interactive standards set out previously.

1.6 The relationships between virtual worlds and digital/physical platforms

All video games, virtual worlds, and metaverses are accessed via physical platforms, such as computers, consoles, and mobile phones. However, not all these physical platforms offer the same

[10] [1] Zhou, Y., Tiwari, M., Bernot, A., & Lin, K. (2024). Metacrime and cybercrime: Exploring the convergence and divergence in digital criminality. Asian Journal of Criminology, 19(3), 419-439.
[2] Pandey, P. (2024). Bits and Bytes Betrayal: Unravelling the Dark Threads of Cybercrime in the Metaverse. In Security and Privacy in Smart Environments (pp. 120-148). Cham: Springer Nature Switzerland.
[3] Awadallah, A., Eledlebi, K., Zemerly, J., Puthal, D., Damiani, E., Taha, K., ... & Yeun, C. Y. (2024). Artificial intelligence-based cybersecurity for the metaverse: research challenges and opportunities. IEEE Communications Surveys & Tutorials.

options concerning digital platforms and communication. As part of the research, an in-depth study was conducted regarding the communication possibilities between users in this environment to summarize users' possibilities when interacting. Figure 19 shows the results of the analysis.

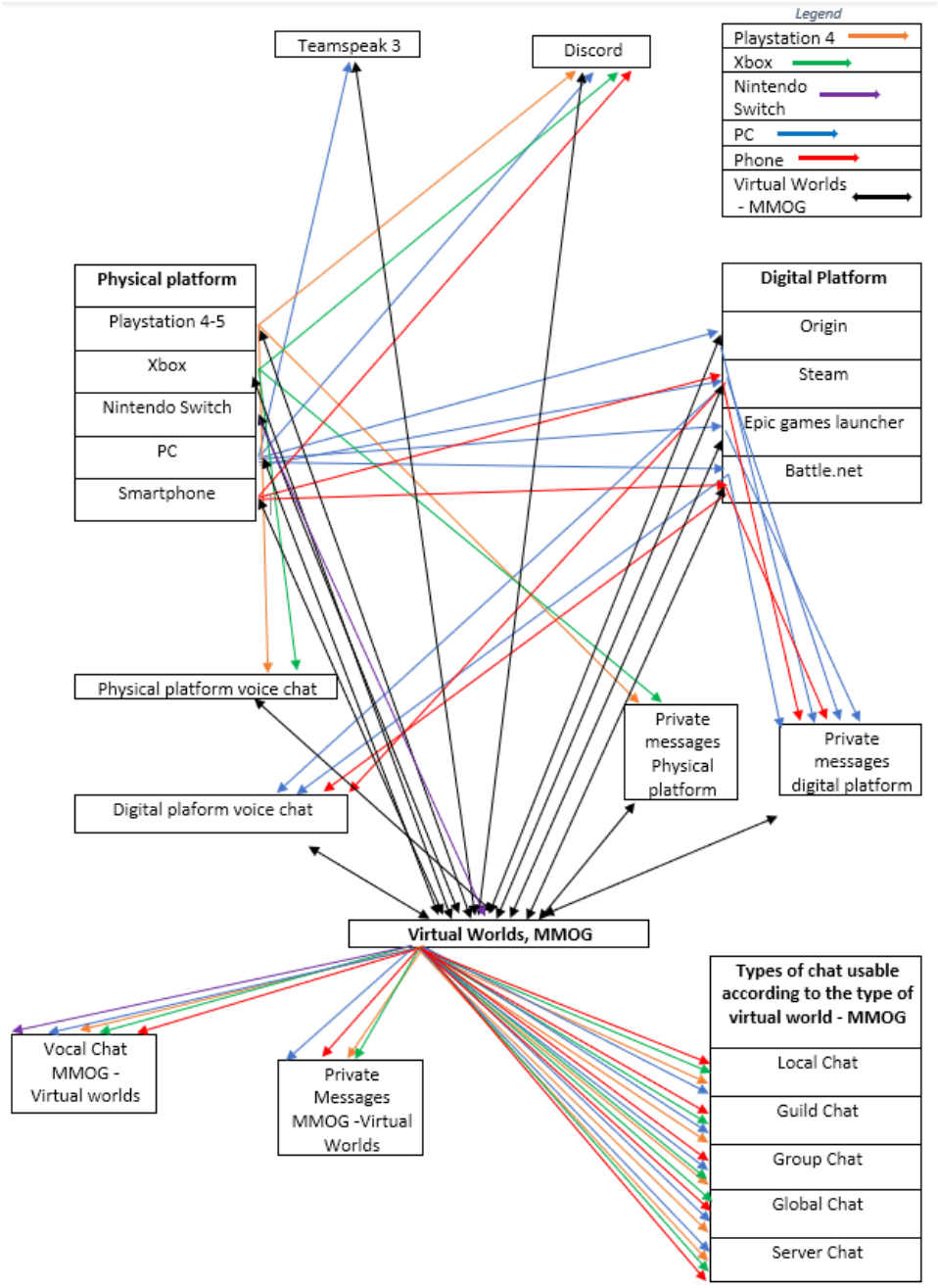

Figure 19: Model that represents the flow of possible communication within the gaming environment. Elaborated by the author.

The arrows indicate the user possibilities and taking the PlayStation 4 as an example:

• One ends on Discord;

• One ends on the "private messages via physical platform";

• One ends on the "voice chat via physical platform".

After that, there is the MMOG discriminant. The black arrow is bi-directional; therefore, it means that MMOGs are the factor that increases or changes communication possibilities. Once an MMOG has been installed on the PS 4 there will be the following functions:

• Voice chat;

• Private messages;

• The chats provided by each type of MMOG.

All of this refers to a single user using the PlayStation 4. Each combination can be paired or used individually. In this case, the user will have 6 (+5, depending on the type of chat used within the MMOG) possibilities to use these communications. This flow creates a quantity problem because it is impossible to know which platform is used to communicate in a given moment if more than one is used, and if the user is moving between some of them. There's also the problem of alternative identity, amplified in MMOGs compared to VG-related applications. A user can be different people at the same time on multiple platforms. For example, a user can call themselves Matteo on Fortnite, Goofy on Discord, and Franco on TS, to which the VGs identity will be added. Furthermore, in some platforms, the possibility of changing the user nickname exists, making things more complicated under a security lens. The companies producing some of these platforms would be able to trace the user who misuses these platforms via chat, but the process is complex and must be done independently. For example, some users can be reported through community or user reports. However, this is all the manufacturing companies can do; the conversations are not monitored (Good, 2020), and often, even the chats are not kept. In short, if a user uses one of these platforms outside of its purposes, other users or company employers must catch him at the exact moment or hope another user reports the incident. However, as illustrated above, this is not feasible currently, as users intending to communicate on these platforms for other purposes know well how to avoid this and exploit specific functions (such as secret rooms, passwords, and VPNs) to conceal themselves.

2. CYBERCRIME AND VIRTUAL WORLDS

Today, the cyberspace occupied by virtual worlds like MMOGs and related applications is unknown; millions of undetected communications go through these applications every second. Vocally or in writing, users worldwide can communicate without barriers and share any content anytime. Who can control these communications? Who can guarantee that these platforms are not being used to perpetrate cybercrimes? And how these platforms can be maliciously exploited? As illustrated in Edward Snowden documents, there has been a lot of interest by the intelligence agencies in these virtual worlds, and different projects were launched secretly (Singel, 2008). One of these projects is named "Reynard": “a seedling effort to study the emerging phenomenon of social (particularly terrorist) dynamics in virtual worlds and large-scale online games and their implications for the Intelligence Community” (Stevens, 2015). In particular, as stated by the Office of the Director of National Intelligence (ODNI) (Reynard "will seek to identify the emerging social, behavioral, and cultural norms in virtual worlds and gaming environments," the findings from which would be applied "to determine the feasibility of automatically detecting suspicious behavior and actions in the virtual world." (ODNI, 2008). In 2008, Reynard shifted its focus from pattern-based data mining to utilizing social science research community expertise to gain insight into Massively multiplayers online games (MMO). In April 2009, announcements about the revamped Reynard Program were released by the Intelligence Advanced Research Projects Activity (IARPA), and more details were given on the project's intended outcomes. In particular, it would seek "to identify behavioral indicators in virtual worlds (VWs) that are related to the real world (RW) [] characteristics of the users," whether these be individuals or groups. Research areas might include "Avatars and Representation, Communication, Things That Avatars Do, Group Formation and Dynamics, Money and Economics, and Cultural Differences" (IARPA, 2009). At a meeting of possible Reynard partners, researchers and defense contractors were told that it was "highly likely that persons of interest were using virtual spaces to communicate or coordinate" (Stevens, 2015). In addition to video games, in recent days, the Metaverse has also been the subject of a report in which Interpol considers it to be at high risk of cybercrime (Kartit et al., 2022) as well as targeted by Europol that proposed a study regarding law enforcement (European Union Agency for Law Enforcement Cooperation, 2022). Furthermore, Discord recently caught the attention of intelligence agencies after some users reported that an American soldier leaked secret material through the platform (Shane Harris et al., 2023). In this contest, virtual worlds remain a question mark, and despite several reports worldwide suggesting that they can become potentially dangerous, there are no studies on the matter nor solutions that can contain the phenomenon to date. Consequently, this chapter intends to highlight the seriousness of the problem, illustrating the results obtained from the

systematic review and some examples of cybercrime that can be perpetrated, found during the research.

2.1 Cybercrime Definition and legal frameworks

For this research, it is important to define cybercrime, which is commonly used but lacks a universally accepted definition. According to many authors (Black et al., 2019; Viano, 2017; Donalds&Osei-Bryson, 2019), it is impossible to find a definition everyone can agree on today. In addition, the Prefix "Cyber" is constantly being used for anything related to the Internet, like "Cybershopping, Cybersurfing" or illicit activities like "Cyberterrorism and Cyberbullying" (Yar& Steinmetz, 2019). At an international level, there are several attempts to define this term over the years, from the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders that defines it as:

1. "Any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them."

2. "Any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network".

Another contribution emerges from the preamble of Council of Europe Cybercrime Convention held in 2001[11], that say: “Action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct” (Convention on Cybercrime, 2001). In 2007, the European Commission defined cybercrime as: "criminal acts committed using electronic communications networks and information systems or against such networks and systems" (European Commission, 2007), and later in 2013, the Cybersecurity Strategy of the European Union defined cybercrime as: "a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target" (Cybersecurity Strategy of the European Union, 2013). Today, the UN is still discussing a possible definition of cybercrime as the Budapest Convention[12] remains at a standstill, not finding a broad consensus (Bannelier&Lostri, 2024). Furthermore, the taxonomy created by these reports does not find configurations accepted by all but attempts to specify and categorize the type of cybercrime and the

[11]ETS 185 – Cybercrime (Budapest Convention), 23.XI.2001, opened for signature in Budapest, on 23 November 2001 and it entered into force on 1 July 2004. As of April 2023, 68 states have ratified the convention, including Italy.
[12] https://rm.coe.int/1680081561

action committed. Consequently, the definition used most often by institutions and academics today is very generic: “cybercrime is a crime or criminal activity that uses or targets a computer or a computer network”. However, the U.S. Department of Justice (DOJ), in the 1989 manual where computer crime is defined, has a very interesting categorization not included in other documents. “In its elaborations on the subject, DOJ divides computer crime into three categories: 1) crimes in which computer hardware, peripherals, and software are the target of a crime; the criminal is obtaining these objects illegally; 2) crimes in which the computer is the immediate "subject" or "victim" of a crime, i.e., the crime consists of attacks on a computer or a system, destruction or disruption of which is the damage caused; and 3) crimes in which computers and related systems are the means or "instrument" by which ordinary crimes are committed, such as theft of identities, data, or money or the distribution of child pornography” (Inc, 2023). For this research, the interpretation that fits the most is the one given in point 3. Consequently, taking this definition as a guideline by combining it with the most recent adopted by actors at an international level, cybercrime in this work will be defined as:

A criminal activity in which computers and related systems are the means or "instruments" by which crimes are committed.

Where "related systems" also involve physical and digital platforms, Virtual Worlds, Video Games, and related applications.

Cybercrime, as a rapidly growing global phenomenon, requires a global and collaborative legal response. Frameworks established by international law and European law provide essential mechanisms to address cybercrime, including cooperation, regulation and harmonization of criminal laws. However, most current frameworks do not have a specific focus in virtual worlds. If "online environments" or something about the metaverse is sometimes mentioned, there is no framework that specifically focuses on cybercrime in virtual worlds, but rather on more technical problems, which fall under cybersecurity, which although being a cybercrime is different from the type of cybercrime mentioned here. Below are some of the most well-known frameworks:

International Legal Frameworks

The Budapest Convention on Cybercrime (2001)[13].

The Council of Europe Convention on Cybercrime, commonly referred to as the Budapest Convention, is widely regarded as the first comprehensive international treaty aimed at addressing

[13] https://www.coe.int/en/web/cybercrime/the-budapest-convention

the challenges posed by cybercrime. The Convention seeks to harmonize national laws and foster international cooperation to combat cybercrime effectively. It defines various offenses, including illegal access to computer systems, illegal interception, and data-related offenses, and establishes procedural measures for the investigation and prosecution of such crimes. One of the most significant provisions of the Budapest Convention is its emphasis on international cooperation. It facilitates the provision of mutual legal assistance, enhances extradition processes, and establishes frameworks for police collaboration across member states, thus ensuring efficient and coordinated responses to cybercrime incidents. While the Convention has garnered considerable global support, with over 65 countries as parties, there remain some notable exceptions, including certain EU member states.

The United Nations (UN) Convention on Cybercrime (Proposed)[14].

While a universally ratified global cybercrime treaty is yet to be realized, the United Nations has been active in addressing the issue under the auspices of the UN Office on Drugs and Crime (UNODC). The ongoing discussions surrounding a potential UN Convention on Cybercrime are aimed at developing international standards for legal cooperation, jurisdictional matters, and capacity-building in the criminal justice sector to tackle cybercrime. These efforts underscore the importance of a unified international approach in addressing the borderless nature of cybercrime.

OECD Guidelines on Cybercrime[15].

The Organisation for Economic Co-operation and Development (OECD) has also been instrumental in addressing cybercrime through initiatives such as the OECD Guidelines for Protecting Consumers in the Global Market. These guidelines advocate for stronger international cooperation and the adoption of best practices in the regulation of cyberspace to protect consumers and combat cybercrime.

European Legal Frameworks

Directive 2013/40/EU on Attacks Against Information Systems[16].

The EU Directive 2013/40/EU, commonly referred to as the Directive on Attacks Against Information Systems, is a critical legislative instrument in the European legal landscape designed to

[14] https://www.unodc.org/unodc/en/cybercrime/convention/home.html
[15] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.osce.org/files/f/documents/a/8/534684.pdf
[16] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013L0040

criminalize cyberattacks. It encompasses a broad range of offenses, including illegal access to information systems, illegal interception of data, and the manipulation of data.

The Directive places an emphasis on harmonizing criminal laws across the EU, ensuring that cybercrime offenses are met with consistent penalties and that member states are equipped with the necessary tools to investigate and prosecute cybercriminals. This harmonization is essential for enhancing cross-border cooperation within the EU, particularly as cybercrime often involves actors spanning multiple jurisdictions.

General Data Protection Regulation (GDPR) (EU Regulation 2016/679)[17].

The General Data Protection Regulation (GDPR), while primarily concerned with data protection, plays a crucial role in mitigating cybercrime. It imposes stringent requirements on organizations to implement robust cybersecurity measures to safeguard personal data. In the event of a data breach, the GDPR mandates rapid notification to supervisory authorities and affected individuals within 72 hours, thus promoting transparency and accountability in the handling of personal information.

Additionally, the GDPR incentivizes the use of encryption and pseudonymization techniques to minimize the impact of data breaches, further enhancing cybersecurity measures. The regulation also imposes significant penalties for non-compliance, with fines reaching up to 4% of global turnover or €20 million, whichever is higher, thereby underscoring the financial risks associated with cybercrime and data breaches.

Directive 2016/1148/EU on Security of Network and Information Systems (NIS Directive)[18].

The NIS Directive (Directive 2016/1148/EU) is a pivotal EU regulation designed to strengthen the security of network and information systems across the European Union. The Directive requires operators of essential services and digital service providers to adopt cybersecurity measures, conduct regular risk assessments, and report significant incidents to national authorities.

[17] https://eur-lex.europa.eu/eli/reg/2016/679/oj
[18] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148

The NIS Directive further fosters cross-border collaboration within the EU, enabling member states to share information and best practices in cybersecurity, thereby enhancing the collective resilience of EU member states against cyber threats.

EU Cybersecurity Act (Regulation 2019/881)[19].

The EU Cybersecurity Act provides a comprehensive framework for improving cybersecurity standards within the EU. It strengthens the role of the European Union Agency for Cybersecurity (ENISA) and introduces an EU-wide cybersecurity certification scheme for ICT products, services, and processes. By establishing a uniform standard for cybersecurity practices, the Cybersecurity Act enhances the protection of critical infrastructure, businesses, and individuals against cybercrime.

European Arrest Warrant (EAW)[20].

The European Arrest Warrant (EAW) is a significant tool for combating cross-border cybercrime within the EU. It simplifies and accelerates the process of extraditing individuals who have committed cybercrimes in one EU member state but are located in another, thus ensuring swift justice for cybercriminals and minimizing the risk of safe havens within the EU.

Directive 2011/93/EU on Combating the Sexual Exploitation of Children[21].

The Directive 2011/93/EU focuses on the protection of children from sexual exploitation, including via online platforms. It criminalizes the production, possession, and dissemination of child sexual abuse material, which is often facilitated through digital means. This Directive enhances the EU's ability to combat the distribution of such material online and encourages collaboration between law enforcement agencies to dismantle child exploitation networks operating in cyberspace.

The Digital Services Act (DSA) and Digital Markets Act (DMA)[22]

The Digital Services Act (DSA) and Digital Markets Act (DMA) represent recent EU regulatory efforts to impose greater accountability on digital platforms, which are frequently used to facilitate cybercrime. These regulations include provisions aimed at reducing the spread of illegal content, enhancing platform transparency, and ensuring that platforms take responsibility for user safety.

[19] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881
[20] https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/european-arrest-warrant_en
[21] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0093
[22] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

While these Acts primarily focus on market regulation and consumer protection, they also have broader implications for cybersecurity and the prevention of cybercrime by increasing platform accountability in the face of growing online threats.

2.2 Systematic Review

Today, the complexity of virtual worlds and the lack of research in this field have created an academic gap that makes it difficult to understand "what" has been written about this argument. To conduct a thorough systematic literature review that would fit this complex field of study, the methodology illustrated by other authoritative research (Buchanan &Bryman, 2011; Cook, 1997; Cooper, 1998; Tranfield et al., 2003) turned out to be the best choice. The primary purpose of the following systematic literature review is to identify possible academic contributions that have covered the research topic (Cybercrimes in Virtual Worlds). In this review, selecting keywords has been quite challenging not only because virtual worlds are called in many different ways but also because there is no official "name" that distinguishes them. For example, a virtual world can be called a video game, a game, a MMOG, a MMORPG[23], a MMO[24], a digital world[25], a parallel world[26], and many others. Also, investigating such topics makes it possible to easily find literature on violence and video games, that is, research highlighting how video games can make people violent. However, this is different from the subject of this study. Infact, the topic of this research is related to cybercrimes committed through virtual worlds, where computers are the meaning of which crimes are committed. Nevertheless, the most challenging part of this systematic review was the scanning: Many results appeared to be good with the selected keywords, but after a rigorous selection, only a few were valuable and coherent. In addition to the systematic literature review, a grey literature review has been conducted to extend the possible findings. The latter will have two different methodologies adopted to improve the review further. For this study, EBSCOhost was

[23]MMORPG (massively multiplayer online role-playing games) is always a MMOG but with different properties. The main difference is in the video game's content: a MMORPG differs from an MMOG because it combines elements of role-playing games (RPGs) with the gameplay of multiplayer online gaming worlds. These words are often used to identify virtual gaming worlds, and both are correct.

[24]MMO is used to indicate a MMOG; there is no substantial difference, and it is used to shorten the word massively multiplayer online games.

[25]Digital worlds refer to online places where you can interact with other users and complete different actions, like chatting and meeting. Nowadays this word is increasingly used to describe everything that refers to virtual space. Therefore, a digital world can be a video game or a parallel world, and this is why the word is often used to replace "video games" or "MMOG" because it can still refer to those digital worlds. For example, a digital world can be Second Life, but second life is also an MMORPG. Today, this word is often used as
synonym and cannot be said to be wrong, perhaps too vague or imprecise. Moreover, digital worlds do not necessarily have to refer to video games; in fact, another example of digital worlds are all those applications related to MMOGs
(E.g., Discord, Teamspeak) and the Metaverse.

[26]Parallel worlds are often used to define those virtual worlds in which real life is reflected with the digital one. For example, Second Life is an MMORPG, a digital world, but it can also be defined as a parallel world because several factors make a simple video game or virtual world a digital projection of the real world. For example, in these parallel worlds, like the Metaverse, it is possible to perform actions that are performed in real life through an avatar. Also, parallel worlds are often used to indicate applications that make things more realistic than other definitions.

selected as the research database (from previous research[27], this database resulted in the one with the most resources). Peer-reviewed English academic contributions were considered (Articles, Books, Books chapters, Proceedings etc..). The period set for this research was from 1 January 1990 to 1 January 2022. Since the mentioned virtual worlds are known under various names, the keyword selection process has been unconventional. An extensive set of words comprehending several concepts was first used to identify all possible documents referring to virtual worlds and cybercrimes. Subsequently, to increase the accuracy of this process, other keywords were chosen based on more specific issues; for instance, a keyword was selected along with a crime (e.g., Terrorism video games). Finally, a few interesting keywords were added to the selection in a mix of terms that could have produced some results. The selected keywords, presented in Table 2 (one word plus the combinations of words), were used to identify contributions in which the keywords appeared throughout the whole text (TX). (e.g., Keyword: (video games crime) searched in the TX of all contributions available = 45.027results). Within the previous result, the selected keywords were searched in the Title (TI) and Abstract (AB), assuming that their presence would ensure affinity and relevance. (E.g., Keyword: (video games crime) searched in TI and AB from the initial 45.027 contributions gives these results: 27 of them contain the keyword in the TX and 371 the keyword in the AB). To ensure more affinity, all relevant contributions containing the selected keywords in the TI and AB were scanned to verify their coherence with the subject. (E.g., the 27 contributions with the keywords present in the TI were scanned by reading their abstract, while the 371 contributions with the keyword in the AB were scanned by reading them). This process has been repeated for each keyword. All the remaining contributions that resulted in having some affinity from the previous procedure were again scanned by reading their abstract. (E.g., from the past procedure, the total amount of contributions was:121 with keywords present in the TI and 2083 with keywords present in the AB. These contributions were scanned by reading their AB to ensure they had an affinity with the topic). The reason to choose the period (1990-2022) is that prior to 1990, no MMOG or virtual worlds existed. As presented in Table 3, the results obtained are:

• 422833 contributions that contain the selected keywords.

• 121 contain the keywords in the TI.

• 2083 contain the keywords in the AB.

[27]Before using EBSCOhost, other search databases were briefly tested by using some keywords for comparison to see which database offered the most results. The research databases tested were: JSTOR, Google Scholar, and ProQuest. After this small research, EBSCOhost was the one offering the most results, and so it was chosen.

All the contributions in which the keywords were present in the TI and AB were scanned to verify their coherence and affinity. From this process, 27 papers were found to be appropriate. After careful readings, 6 more papers were removed from this pool as they were not academic. In detail:

• One of these was a thesis.

• One of these was a periodic article.

• Two of these were website notices.

• Two of these were duplicate results.

Video games crime	Cybercrime video games	Terrorism video games	Terrorism virtual worlds	Gamification terrorism video games
Virtual worlds crime	Virtual worlds cybercrime	Terrorism online apps	Terrorism metaverse	Discord app crime
MMOG crime	MMOG cybercrime	Terrorism MMOG	Money laundering video games	Gaming chat crime
Metaverse crime	Metaverse cybercrime	Money laundering virtual worlds	Money laundering online apps	MMOG communications crime
Online game crime	Online game cybercrime	Money laundering metaverse	Money laundering MMOG	Digital applications crime
Messaging apps cybercrime	Messaging apps crime	Murders video games	Murders MMOG	Murders online apps
Digital world crime	Digital world cybercrime	Murders metaverse	Murders virtual worlds	

Table 2: Keywords

	Keyword in the TX	**Keyword in the TI**	**Keyword in the AB**
Video games crime	45027	27	371
Virtual worlds crime	42499	25	207
MMOG crime	164	0	2
Metaverse crime	102	0	2
Online game crime	44956	6	153
Messaging apps cybercrime	5436	0	7
Digital world crime	63794	11	441
Cybercrime video games	5854	0	4
Virtual worlds cybercrime	3573	3	21
MMOG cybercrime	12	0	0
Metaverse cybercrime	12	0	1
Online game cybercrime	44956	6	153
Messaging apps crime	625	0	2
Digital world cybercrime	8639	8	149
Terrorism video games	15701	5	75

Terrorism online apps	7544	0	4
Terrorism MMOG	39	1	1
Money laundering virtual worlds	8098	3	39
Money laundering metaverse	26	0	0
Murders video games	13334	11	86
Murders metaverse	27	0	0
Murders online apps	4533	0	0
Terrorism virtual worlds	19905	1	43
Terrorism metaverse	37	0	1
Money laundering video games	5042	0	1
Money laundering online apps	4537	0	0
Money laundering MMOG	18	0	1
Murders MMOG	34	0	0
Murders virtual worlds	13352	1	9
Gamification terrorism video games	116	0	0
Discord app crime	1090	0	0
Gaming chat crime	2567	0	1
MMOG communications crime	149	0	0
Digital applications crime	61035	13	309
Results	**422833**	**121**	**2083**

Table 3: Results Obtained

In the end, 21 academic papers were identified as suitable as they contained necessary keywords; however, even if these papers, at first reading, appeared to be appropriate, it was necessary to adopt "inclusion" and "exclusion" criteria to determine their relevance.

Inclusion criteria:

• Consistency with the main topic (the paper contains questions and discusses important aspects related to the research).

• Illustrates at least one crime that can be perpetrated through the illicit use of virtual worlds.

• In the text, MMOG is cited in relation to cybercrimes (virtual worlds or video games).

• MMOG-related applications in connection with cybercrime are mentioned in the text.

• It describes, even superficially, a problem related to the improper use of these platforms (anonymity, VPN, multiple identities).

Exclusion criteria:

• Inconsistency with the research project (does not question a topic inherent to the research project, does not discuss the topic).

• It does not illustrate any crime perpetrated through the illicit use of virtual worlds.

• No keywords are mentioned in connection with cybercrime and misuse of the platforms.

• No MMOG related applications are mentioned.

• Cybercrime is not described as a result of the misuse of virtual worlds (It describes platforms as the tool that causes the problem when instead platforms are the means by which crimes are perpetrated. E.g., using a PlayStation and a violent video game, you can develop violence is inconsistent with the project. E.g., Laundering money through the platform, using secret in-game chats to communicate and commit crimes = consistent). Based on these criteria, out of 21 papers, 10 had some affinity with the topic. Furthermore, the papers were catalogued in Figure 20 and detailed with the date, author, and a small abstract.

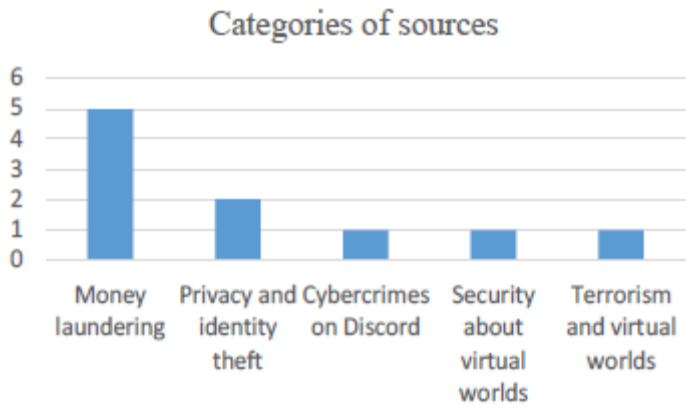

Figure 20:Categorization.

The papers found are listed below with a brief description:

Identity theft and virtual property.

(Chen et al., 2004) The paper highlights different crimes committed through MMOG in Taiwan. It focuses on identity theft, virtual property, and privacy violations. It is very short but gives some good hints on what could happen on these platforms.

Identity theft and minor crimes.

(Chen et al., 2005) This paper is similar to the previous one written in 2004, but the crimes discussed are much broader this time. It examines 613 criminal cases that happened through these platforms, giving a good explanation. It mainly focuses on theft and some other minor crimes but is a paper that is valuable and offers excellent perspectives.

Money laundering.

(Keene, 2011). The purpose of this paper is to highlight emerging threats in cyberspace, with particular reference to financial crime in the virtual world, which have real life implications; it also recommends ways by which the threat may be mitigated. The paper discusses different financial

crimes, including money laundering. It is an interesting paper explaining these applications' risks by illustrating different examples.

Money laundering.

(Irwin et al., 2012). This paper aims to examine different verification procedures implemented by MMOGs platforms and providers to determine if the transactions are truly anonymous. In addition, the study is conducted to search if the identities of those who may wish to use that environment to conduct money laundering or terrorism financing are covered and not identifiable.

Money laundering.

(Chambers-Jones, 2013). This paper highlights how the absence of laws in virtual worlds permits several crimes, including money laundering. It explains how virtual currencies work and what it is possible to do through these applications. Also, it compares different legal legislations to explain how the system is flawed.

Money laundering.

(S.M. Irwin et al., 2014). This paper is similar to the one written in 2012 but focuses explicitly on "financing terrorism activity through money laundering." The interesting findings show that it is possible to finance that activity in these virtual worlds. Furthermore, the paper experiment was conducted in different MMOG, producing positive results.

Affinity to the research topic.

(Stevens, 2015). This paper is the most accurate as it grasps the main problem of these applications. Virtual worlds, as explained, are completely law-free environments and are unmonitored. The studyalso includes a thorough analysis of documents uncovered during the years. It offers a comprehensive idea of what problems could arise from these applications and what approach has been taken by intelligence agencies to counter the phenomenon.

Money laundering.

(Chambers-Jones, 2018). Similar to the others about money laundering, this paper analyzes virtual currencies and the exploitable functions these applications have. It also gives some idea of what is possible to achieve in private rooms with fake accounts.

Cybercrime app Discord.

(Conway et al., 2019) This paper discusses how it is possible to use gaming-related applications to spread far-right extremist ideology and recruit people. It also brings many examples regarding a specific application called Discord, which has been used multiple times to commit cybercrimes.

Terrorism and virtual worlds.

(Trifunović, 2021). This paper discusses how it is possible to use virtual spaces as a territory to perpetrate covered terrorist activities. It develops interesting conclusions by showing different case studies that illustrate how it is possible to conduct illicit activities. Also, it considers the Islamic world and its coexistence with these virtual worlds.

2.2.1 Grey Literature Review

"Grey literature is an extensive, though complex, source of information. The 'Luxembourg definition' offers a widely accepted description for grey literature as 'that which is produced on all levels of government, academics, business and industry in print and electronic formats, but which is not controlled by commercial publishers, e.g., where publishing is not the primary activity of the producing body" (Godin et al., 2015). To analyze documents that are consistent with the topic, two approaches have been applied: In the first one, different research databases were consulted to identify possible documents that fit the argument. In particular, the open grey, openAIRE, the FBI vault, and the CIA reading room were scanned to find possible results, while common research has been done online (Google) for the second approach. In detail, sites, videos, and web articles were explored. The methodology adopted for the first approach of this grey literature review is the same as the standard literature review; the only option changed is the database, scanning for "other research documents" rather than "peer-reviewed articles." Therefore, Previous inputs (E.g., English language, time period) were applied for databases such as open grey and openAIRE, changing only one option regarding contributions. Instead of searching for peer-reviewed articles, only "other research products" were scanned. Previously selected keywords were applied, and all results were scanned to ensure affinity with the topic. The findings are illustrated in Table 4.

	Open grey	**OpenAire**	**FBI vault**	**CIA reading room**
Video games crime	0	7	0	0
Virtual worlds crime	0	2	0	0
MMOG crime	0	1	0	0
Metaverse crime	0	0	0	0
Online game crime	0	11	0	0
Messaging apps cybercrime	0	0	0	0
Digital world crime	0	17	0	0
Cybercrime video games	0	0	0	0
Virtual worlds cybercrime	0	0	0	0
MMOG cybercrime	0	0	0	0
Metaverse cybercrime	0	0	0	0

Online game cybercrime	0	0	0	0
Messaging apps crime	0	0	0	0
Digital world cybercrime	0	2	0	0
Terrorism video games	0	5	0	160
Terrorism virtual worlds	0	0	0	3691
Terrorism online apps	0	0	0	30
Terrorism metaverse	0	0	0	0
Terrorism MMOG	0	0	0	0
Money laundering video games	0	0	0	10
Money laundering virtual worlds	0	0	0	182
Money laundering online apps	0	0	0	3
Money laundering metaverse	0	0	0	0
Money laundering MMOG	0	0	0	0
Murders video games	0	0	0	87
Murders MMOG	0	0	0	0
Murders metaverse	0	0	0	0
Murders virtual worlds	0	0	0	2154
Murders online apps	0	0	0	12
Gamification terrorism video games	0	0	0	0
Discord app crime	0	0	0	110
Digital applications crime	0	18	0	467
Gaming chat crime	0	0	0	352
Results	**0**	**63**	**0**	**7258**

Table 4: Results Obtained Grey literature review first approach.

For the second approach, Google was selected as the research database. The keywords selected are the ones previously used. All documents, audio, and video were searched in English, and all the findings were scanned and given appropriate categorization. First, the keywords were used on Google, and then the results were scanned by different categories, such as video, web articles, and other documents. The most common sources found on the web are articles written by some tech-field experts and different videos about the topic that date back to the documents released by Edward Snowden. Since then, the material obtainable is some local news and videos about the argument, with most of them being warnings released after a dangerous event. The results obtained with this keyword research were quite a lot; therefore, only the primary sources were reported to reduce the numbers. (E.g., If different sources repeat the same news, only the first has been indicated. In this case, if the findings are 25000 results talking about the same issue, the amount reported will be "one" since all other results are discussing the same content). Table 5 highlights the findings. All the sources were also divided by dates and categorization, as can be seen in Fig. 21 and Fig. 22.

Video	Web Article	Others
4	30	4

Table 5: Summary of the results

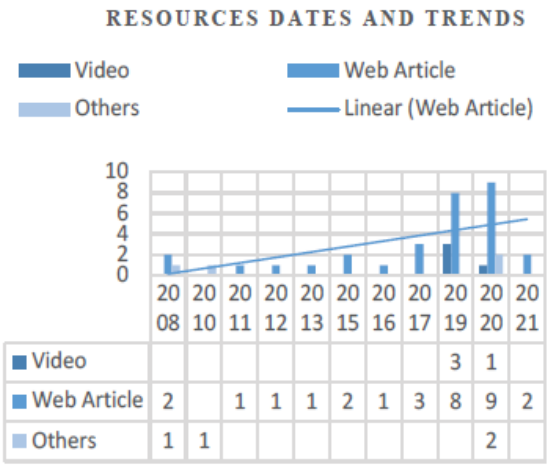

Figure 21: Resources by dates and trend.

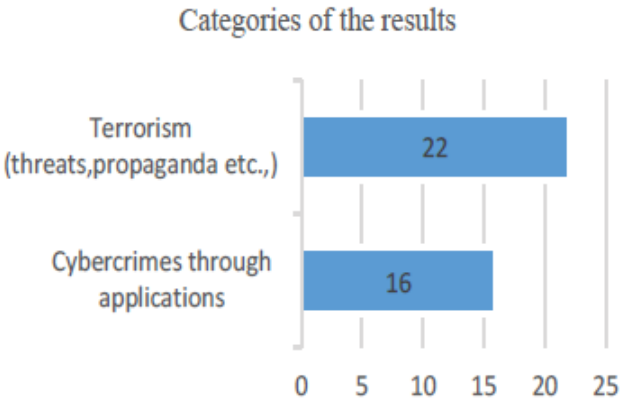

Figure 22: Categorization of the findings.

- **Video 1.**

(Deputies Warn Parents about Discord App Potential Dangers, 2019). The video highlights how this gaming application raises concerns among deputies in the US. This application has been used multiple times to commit crimes, and it offers many possibilities to communicate undetected. It also brings attention to this application's potential by clarifying different important aspects, particularly how crimes can be easily committed without detection.

- **Video 2.**

(Cybercriminals Are Doing Big Business in the Gaming Chat App Discord, 2021). This video explains the possible exploitations of Discord. This application can be used to perpetrate different crimes, and it offers some unique features, such as user anonymity, the possibility of hiding inside private channels to conversate, and file transfers. These characteristics make Discord more attractive to the users who want to exploit this kind of platform.

- **Video 3.**

(We Need to Tackle Domestic Terrorism like We Do Foreign Threats, Expert Says CBS News, 2021). In the video, the participants discuss the problem of domestic terrorism that has been quite frequent in the US. This phenomenon is also perpetrated through gaming applications, spreading very fast. However, as highlighted in the video, the problem is that there are no resources, and it is impossible to predict these events, so the issues remain open.

- **Video 4.**

(Teen Accused of Making Death Threats on Gaming Platform, 2021). This video shows a sheriff who talks about discord and highlights how difficult it is for police to contact the provider of this application. Even with a subpoena sent to the agency, it tooks four days to respond. Also, the event discussed in the video has been reported to local police, but many of these events go unnoticed. An issue that also raises more concerns.

- **Web Article 1.**

(Shachtman, 2008). This article talks about the research of Dr. Dwight Toavs, highlighting how it is possible to use MMOG to perpetrate terrorist attacks.

- **Web Article 2.**

(*Singel, 2008).* This article talks about the Reynard project, an undercover operation being done by intelligence agencies to discover terrorists in online gaming environments.

- **Web Article 3.**

(Storm, 2011). This article is similar to the previous one and discusses the Reynard project and some events that occurred in Michigan.

- **Web Article 4.**

(Pidd, 2012). This article discusses the case of Anders Breivik[28] and explains the issue that gaming platforms could have on people.

[28] Anders Breivik is the author of the Utoya massacre, where he killed 69 and the bombs that killed 8 people in Oslo. In his 1,500-page manifesto, "2083: A European Declaration of Independence," terror suspect Anders Behring Breivik, who is now in custody, writes in detail about how he used Activision's *Call of Duty: Modern Warfare 2* game and Blizzard Entertainment's *World of Warcraft* game to help him prepare for the attack. Eighty-five people were killed when Breivik allegedly gunned down campers at an island retreat disguised as a law enforcement officer and an additional seven were killed from a bomb he allegedly set off at a government building in the capital.*"I just bought Modern Warfare 2, the game. It is probably the best military simulator out there and it's one of the hottest games this year. ... I see MW2 more as a part of my training-simulation than anything*

- **Web Article 5.**

(ProPublica, 2013). This article discusses what NSA and CIA have done to analyze these platforms. The article is based on the documents released by Edward Snowden and makes some appreciable considerations.

- **Web Article 6.**

(Tyers et al., 2015). This article explains various doubts regarding the ISIL Paris attacks, questioning if gaming platforms were behind it.

- **Web Article 7.**

(Greenwald, 2015). This article describes how Osama Bin Laden could have used video games to train terrorists and subordinates. It also highlights how some video games could be used for that purpose, as they reproduce realistic content.

- **Web Article 8.**

(Dave Grossman, 2016). This article explains how video games platforms can modify people's behavior and teach them how to perpetrate crimes. It is not the best fit for this review, but it highlights some significant issues encountered during most cases: the distinction between fantasy and reality.

- **Web Article 9.**

(Al-Awsat, 2017). This article brings attention to the CIA documents about Osama Bin Laden, highlighting that he could have been using gaming platforms.

- **Web Article 10.**

(Zilber, 2017). This article is superficial, but it does confirm that everyone could use these platforms, even terrorists and other persons like Osama Bin Laden.

- **Web Article 11.**

(Swearingen, 2017). This article explains one of the methods exploited in virtual worlds (Gold Farming). A practice that many bots and agencies could use to launder money.

- **Web Article 12.**

(Makuch, 2019). The article describes what a Californian congressman said during a meeting. On that occasion, a topic that is a major issue on these platforms was brought up: the far-right extremism and racism spreading on these applications.

- **Web Article 13.**

---

else. I've still learned to love it though and especially the multiplayer part is amazing. You can more or less completely simulate actual operations." (Gaudiosi, n.d)

(Griffin, 2019). This article discusses an Oklahoma case of prostitution that has been perpetrated through the Discord application.

- **Web Article 14.**

(Qureshi, 2019). This article highlights some discord features and explains how it has been used in two cases: The Albion school and Bianca Devins.

- **Web Article 15.**

(Lamoureux, 2019). This article discusses the case of a group of gamers that have assisted to a murder case through Discord and tried to track it down.

- **Web Article 16.**

(The "gamification" of Domestic Terrorism Online, 2019). This article illustrates the phenomenon of gamification and radicalization spreading in online environments.

- **Web Article 17.**

(Brewster, 2019). This article illustrates how hackers and criminals do business through the Discord application.

- **Web Article 18.**

(Freile, 2019). This article discusses the case of Albion school and Bianca Devins and introduces a new case and different considerations.

- **Web Article 19.**

(Staff, 2019). Again, this article brings attention to the Discord platform, where a teenager has been reported making threats.

- **Web Article 20.**

(Mondesert, 2020). This article reports the speech of Gilles the Kerchove (EU anti-terrorism chief) that warns about virtual worlds dangers.

- **Web Article 21.**

(Vamshi, 2020). This article illustrates how cybercriminals are targeting users through the discord application.

- **Web Article 22.**

(Govind, 2020). This article illustrates a case where ten people were sentenced to prison for sexual exploitation through Discord.

- **Web Article 23.**

(CecliaD'Anastasio, 2020). This article illustrates the case of BOTs that exploit virtual worlds currencies to launder money.

- **Web Article 24.**

(Cory Shaffer, 2020). This article illustrates the case of a man that was threatening to steal weapons and start an uprising.

- **Web Article 25.**

(Vittozzi, 2020). This article illustrates how terrorists and extremists recruit people through video games platforms. Also, it highlights how the phenomenon is spreading.

- **Web Article 26.**

(Croft, 2020). This article is interesting because it reports an important statement made by Sony in which they say that they will not be able to listen or monitor users' conversations.

- **Web Article 27.**

(Good, 2020). This article talks about Sony and their statement about recording vocal chats and makes some considerations.

- **Web Article 28.**

(Stuff.co.nz, 2020). Again, this article talks about a case in New Zealand, where people constantly used the app Discord to buy and sell drugs.

- **Web Article 29.**

(Roebuck, 2021). This article illustrates that some users who participated in the Capitol Hill assaults used gaming platforms such as Discord.

- **Web Article 30.**

(Shukla, 2021). This article is one of the most interesting; it brings to the attention the work of Indian intelligence in discovering some terrorist accounts that were using that kind of application.

- **Others 1.**

(*S1E8: How Are Terrorists and Violent Extremists Using Gamification?* 2020). This Podcast found on the internet explains the role of gamification in virtual worlds.

- **Others 2.**

(*Combating Robot Networks*, 2010). This is an unclassified report made in 2010 by a Canadian defense research center. The report highlights different risks and challenges that are present in virtual worlds.

- **Others 3.**

(Online gaming in the context of the fight against terrorism, 2020). This is a public report made by EU Counter-Terrorism Coordinator to different delegations. Superficially, this report brings attention to virtual worlds, as they are a potential risk for national securities.

- **Others 4.**

(Office of the director of national intelligence, 2008). This is a small part of the Reynard project unclassified document. It explains the scope of the project and why it has been launched.

This systematic literature review highlights different important aspects. First, it is possible to notice that different results were obtained according to the keywords modification. For example, when the main keyword was used (E.g., MMOG) the research database produced very poor results, while if the spectrum was broadened to more comprehensive terms (E.g., instead of using precise words like MMOG, more general words were used, like "virtual worlds"), there was a higher response, as detailed in Figure 23.

MMOG as part of the Keywords.

TX	TI	AB
149	0	0
34	0	0
18	0	1
39	1	1
12	0	0
164	0	2

MMOG not present in the Keywords.

TX	TI	AB
61035	13	309
13352	1	9
116	0	0
1090	0	0
2567	0	1
8098	3	39
26	0	0
13334	11	86
27	0	0
4533	0	0
19905	1	43
37	0	1
5042	0	1
4537	0	0
12	0	1
44956	6	153
625	0	2
8639	8	149
15701	5	75
7544	0	4
102	0	2
44956	6	153
5436	0	7
63794	11	441
5854	0	4
3573	3	21
45027	27	371
42499	25	207

Figure 23: Comparison of Keywords

These results highlight the limited coverage of academic literature regarding the topic "MMOG" in the current academic literature. From the total pool

- 416 papers have "MMOG" present in the TX.
- 1 paper has "MMOG" present in the TI.
- 3 papers have "MMOG" present in the AB.

Besides one, these papers were also not connected with the research topic because the term "MMOG" was associated with the sociological issue of video games and not with the possible misuse of these platforms. Continuing with the observations, it is possible to note that the most results given with the selected keywords were in the TX, while a small amount was in the TI and AB. As illustrated in Figure 24, most papers have in their TX one of the 34 keywords selected, and only 0,5% show the presence of the keywords in the TI and AB. Another interesting consideration is the general overview that resulted from the research database. After rigorous reading and the application of inclusion and exclusion criteria, the gap increased: from a pool of 2204 papers (2083 +121), 27 were selected, and after the criteria application, only 10 were left. This proceeding highlights how scarce is the academic literature about the argument: From 1990 till 2022, only 10 papers discuss some of the issues of these virtual worlds, and five focus on a specific topic (money laundering). In 32 years, peer-reviewed English-language papers about this topic are equal to 0,31 papers per year. If the 10 papers are deeply investigated, the conclusion is that only four of them discuss the argument covering only a small part of the issue. In total, if further clarifications are to be made, only 1 paper is revealed to be appropriate.

	Papers	%
TX	420629	99,4786
TI	121	0,0287
AB	2083	0,4927
Total	422833	100

Figure 24: Total frequency of the keywords in the papers.

Following this systematic literature review, the grey literature review conducted to explore the topic further highlights important aspects. For the first approach, it is possible to notice that no reliable sources were found even if there were many results in the CIA reading room. The main reason is that the words "Terrorism" and "Murders" found in CIA documents are not related to the content but are generally mentioned in the sources. As reported in Table 4, an interesting factor is that the

FBI vault and the Open grey database have no resources, and OpenAire only shows 63. Once again, these poor results highlight the total absence of records regarding this topic. Different instead are the results of the second process. In this case, it is possible to observe that from millions of results, different sources were found. Unlike previous results, the situation given by these findings is different; in some way, all of these sources discuss the topic, or some specific aspects related to it. Further considerations can be made by watching the dates of the resources; most of the "news" and "video" are recent, meaning that the problem is relevant today and is being discussed "unofficially." In support of this, some of the latest "news" present on the web quote the speech of high institutional level persons (E.g., Gilles De Kerchove, EU Counter- Terrorism Coordinator) or have reported direct quotes from former FBI agents (E.g., Dan Woods, FBI). All of the sources obtained with this methodology can be considered reliable as they report direct quotations from institutional authorities and actual events.

2.3 Methodology

In a complex and interconnected world like today, where most communications occur in virtual contexts such as blogs, chats, messaging apps, and social media, and computer-mediated communications (CMC) are the primary interaction of sharing feelings and emotions (Riffe et al., 2006), it is necessary to adapt the classic research methods to the current context. Research in video games is still far from having found a unique and functional research methodology: “The work conducted in games research has both accumulative as well as transformative aspects. In addition, it is characterised by rather exceptional multidisciplinarity and interdisciplinarity, which is rooted on the one hand in the complexity and diversity of its research subjects, as well as on the fact that modern scholarship of digital games is a rather young phenomenon” (Lankoski&Bjork, 2015).The methodology chosen for this study was netnography: a recently emerging methodology in social research that adapts the ethnography tools and applies them in a digital context. Founded by Kozinets in 1995, this methodology has been revisited and applied in many research contexts. In the beginning, netnography served as a research tool for analyzing the needs of online users (Kozinets, 1997, 1998, 1999; Bickart& Schindler, 2001; Catterall&Maclaran, 2002) but with the development of new technology, through netnographic analysis, researchers can gain new perspectives on traditional service or explore new types of digital service (e.g., online streaming of entertainment, online storage space or online gaming) (Heinonen&Medberg, 2018). The application of different netnography approaches has been observed over the years in a variety of fields: Digital journalism (Aitamurto, 2013), health (Mudry& Strong, 2013), sport (Gilchrist & Ravenscroft, 2011), geography (Grabher&Ibert, 2014), video games (Silva et al., 2021; Au &Ho, 2021; Hernandez &

Handan, 2014). This raft of publications demonstrates that netnography, as a methodological research approach, has a wide reach across many nations, languages, and fields (Costello et al., 2017). Consequently, netnography does not focus on a single approach but instead adapts to the phenomena studied. As the study aims to illustrate how these virtual worlds can be used to commit crimes, direct observation and non-participatory approaches have been adopted. In detail, three years have been spent inside virtual communities observing, collecting, and classifying data following the steps of netnography, described in Figure 25.

Figure 25: Steps of Netnography.

The research focus comprehends the research topic the researcher intends to investigate and the research questions: Can video games, virtual worlds, and the gaming environment be exploited to commit crimes? Which crimes can be perpetrated? Moreover, how can we fight the phenomenon?

The successive step is where the researcher has to identify and select the community. This step is challenging as each virtual world is unique and requires different steps. In the first instance, creating different accounts, one for each video game/virtual world and application the researcher intends to investigate, is necessary. Then, the researcher must download the application, create its avatar, and play it to understand the game mechanics and community habits. It is not enough to play in the virtual world for a few hours, but for each contest, the suitable timeframe is when the users reach the "end game[29]" and have mastered the mechanic; therefore, each virtual world may require

[29]In virtual worlds, but especially MMORPGs, the end game consists of the final content of that particular world. This means those who have achieved it will have complete access to the world, including unlocking specific functions.

different timescales. Once reached this point, the researcher has mastered the virtual world enough to identify users in guilds, groups, communities, friends, and locations like maps, words, cities, etc. When the different communities have been identified, the researcher can select which one best suit its research purpose (By using OSINT-COMINT-HUMINT analysis, different hints can appear during gameplay about some users). The successive step is engagement, immersion, and data collection. Here is where the researcher engages with the community, and this can be done in two ways: with active participation, therefore, the researcher must inform the users about its presence; or in a non-participatory mode. For this research, non-participatory engagement has been adopted, as an active participation would probably produce no results[30]. Instead, the immersion step has been done with a participatory approach. Finally, the data collection is where the researcher gathers the data; in this case, conversations and pictures were taken as proof of the behavior. There are different ways to collect data, but screenshots and transcriptions of vocal chats are the most efficient way to collect them in this environment. This stage is also the most challenging and time-consuming, as not everyone uses the gaming environment to commit crimes, and of course, users are not doing this in everyone's eyes; therefore, many hours could be spent observing without results. After the researcher has gathered the materials, it is necessary to analyze them, draw possible conclusions and patterns, and raise some new research questions, in a iterative process. A hermeneutical-multimodal and linguistic analysis of pictures and conversations was conducted to highlight how this environment is used to commit crimes because of the ease of unmonitored communications. In the last stage, the findings are presented, which can be done differently according to the researcher. All processes have been adapted to the nature of the research object, "gaming environment," as Kozinets suggested in 2006, and integrated with previous methodological works published in the gaming environment, in particular, the works of Consalvo& Dutton, 2006 – (Game analysis: Developing a methodological toolkit for the qualitative study of games,) and (Game Research methods of Lankoski&Bjork, 2015). Moreover, OSINT-COMINT, and HUMINT techniques were used along with netnography to reach a wider result. Due to the topic's nature, the researcher fully complied with the regulations regarding the possession and disclosure of the material.

2.4 Pedophilia

Virtual worlds and online video games are an ever-expanding environment involving millions of players worldwide, witnessing massive user expansion during the pandemic (King et al., 2020; Guo

[30]In the engagement phase, it was deemed appropriate not to reveal the identity as it would have changed the behavior of the communities observed. Let's imagine that any law enforcement agent warns everyone before taking an undercover operation; we can deduce that this operation would lead to nothing, exactly like in this case. Revealing the identity would have prevented results.

et al., 2022). As a result, challenges also emerge, including the possible presence of pedophiles seeking to exploit them to target minors. Pedophilia is considered to be a mental disorder where an individual seeks sexual gratification from children (APA Dictionary of Psychology, 2018), and in many jurisdictions, this phenomenon is a crime regulated by various penal codes. The law may vary according to the country, but in general terms and with the necessary exceptions to the various penal codes, it is considered a crime when an adult performs any sexual acts with a child under their age of consent. The age of consent is different depending on the country, as do the penalties imposed on those who commit the crime. Therefore, to be defined as a crime, looking at various penal codes, such as the Italian (Codice Penale Art. 609 quater, 1996) and Californian (Californian Penal Code art 288, 1982) ones, for example, it is considered a crime when an adult commits any sexual act with a minor under 14 years of age (age of consent). This also includes any form of sexual abuse perpetrated via computers (Polizia Di Stato, 2021). Online games involve virtual communities of players interacting in real time with the aid of different applications, and this environment can attract the attention of pedophiles, who seek to establish contact with minors through chats, direct messages, or other forms of communication. Since many gaming platforms allow a certain degree of anonymity, pedophiles can pose as peers to build relationships with young players. Recently, there has been an exponential increase in articles worldwide about pedophilia linked to gaming, thus demonstrating that it is not an "occasional" event but a frequent activity:

"Video Games and Online Chats Are 'Hunting Grounds' for Sexual Predators, Criminals are making virtual connections with children through gaming and social media platforms. One popular site warns visitors, "Please be careful." (Bowles & Keller, 2019)

"Pennsylvania Child sex crime investigators say they're overwhelmed with tips since the start of the COVID-19 pandemic. The Delaware County Internet Crimes Against Children task force said with more kids at home and online, predators are using it to their advantage. Investigators said a local man was targeting kids playing streaming video games. The victim's mother captured the incident. The mother, who didn't want to be identified, walked in on her son while he played video games and began undressing." (Pradelli&Mettendorf, 2020)

"Pedophiles and bad people, they find a way around things, setting a trap for your kids right in your living room," explained Brian Heins, a father of a gamer. "With certain games, you do not have to prove how old you are. You just click a box and say you are over 18."(Brown, 2020)

"I have personally arrested 30-year-old plus internet predators and found that they had multiple Roblox accounts for the specific purpose of chatting with kids under the age of 10. The chat feature can be turned off but is rarely done as parents don't realize how many internet predators are actually hunting their kids at any given time."(Jenson, 2023)

Given the number of users who populate these virtual worlds, it is effortless to find victims, and predators know how to do it. What happens is essentially an enticement through social engineering techniques, which exploit the internal dimensions of these virtual worlds.

The methods with which they can abuse virtual worlds to attack minors are three:

- Enticement with an exchange of money/items inside the game or services (like power leveling[31]).
- Enticement by masking the identity (pretending about age, sex, etc.).
- Blackmailing or extorting.

Often, pedophiles are gamers themselves, content creators, or know about these platforms through their children. It is also not uncommon to see famous people arrested for these crimes, as a recent case in Italy and Poland reveals:

Rimini, abuse of a 13-year-old: YouTuber with one million followers arrested (Tgcom24, 2023).

"Poland's Online Community Rocked by Pedophilia Allegations. The accused individuals allegedly used their fame to sexually abuse young girls, some as young as 12 to 14 years old. They would invite them to hotels, intoxicate them with alcohol, and take advantage of their impaired state. The shocking revelations have left the Polish internet world, especially the YouTube community, shaken." (Amokeoja, 2023).

Inside virtual worlds, everyone can move freely, chat, and socialize with other players. Therefore, there are no limits about the conversations the users could have. Is it true that some systems try to prevent inappropriate behavior, especially towards minors, but are not enough, and as will be shown later, are inadequate. Not only can chats be exploited, both vocal and written, but it is also possible to witness behaviors that recall pedophilia, as in Figure 26, where an avatar of a 7-year-old girl has been "raped."

[31]It is the process of raising a character's level in the shortest possible time. Often, this is done by users who have reached the final stages of a VG. This is often done in exchange for money or favours.

Figure 26: An avatar of a 7-year-old girl being raped on Roblox. Image recovered from https://ph.theasianparent.com/gang-raped-on-roblox.

Due to the nature of the topic, the research could merely investigate the possible presence of pedophiles without going further, as the current legislation prevents anyone from getting in touch with that material (Codice Penale Art. 600 quater comma 3, 2021). Consequently, only part of the material found will be displayed. In Figures 27 and 28, some chats recovered from Discord servers related to gaming highlight the presence of different predators.

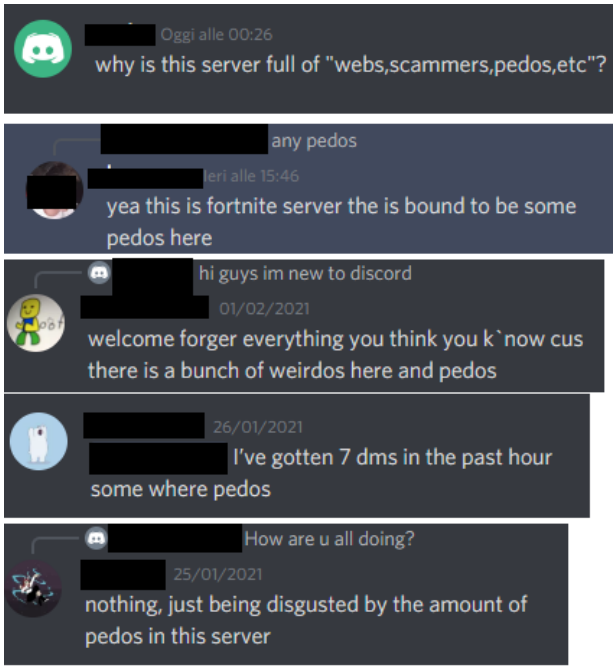

Figure 27: Example of chats collected in Discord Server. Elaborated by the author.

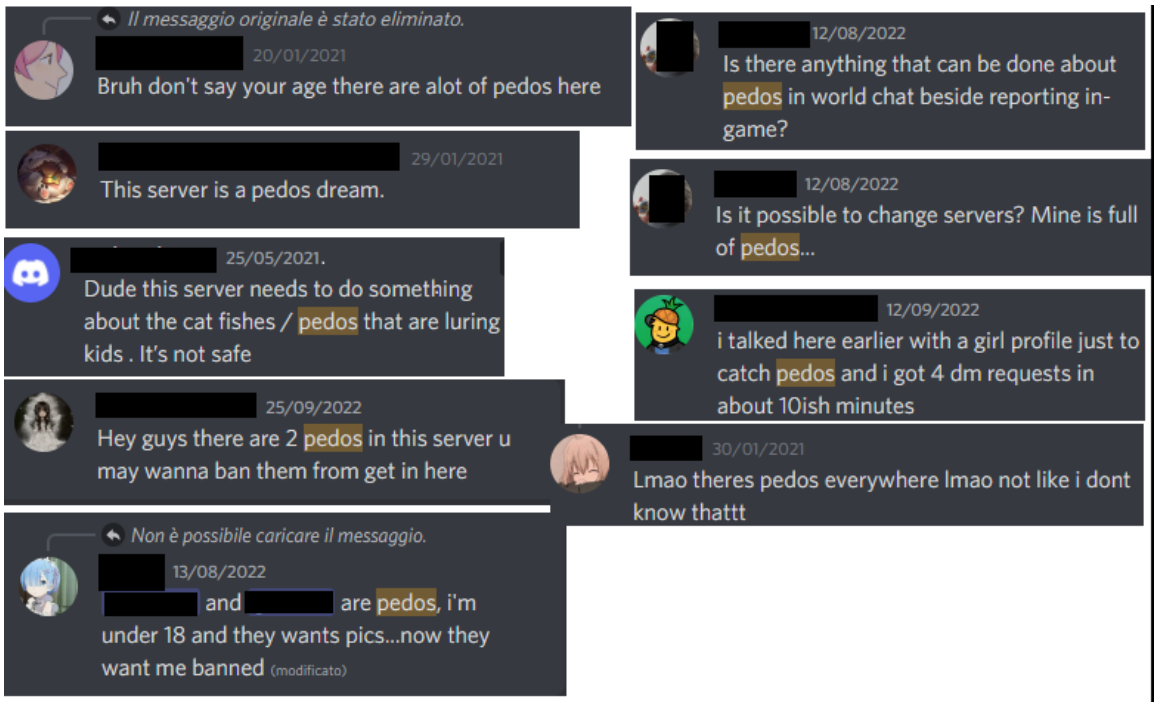

Figure 28: Example of chats collected in Discord Server. Elaborated by the author.

Analyzing virtual worlds, it is possible to stumble in different communities where this phenomenon is more radicated, and generally, this applies to all those video games and/or related application servers where the average age is very low, such as Fortnite, Roblox, and Minecraft.

2.5 Money Laundering

Money laundering is the process by which the proceeds of crime are put through a series of transactions, which disguise their illicit origins, and make them appear to have come from a legitimate source (Graycar&Grabosky, 1996). At a legal level, money laundering is a crime defined by various conventions, such as that of the UN in Vienna in 1988[32] and that of the Council of Europe in 2005[33].As illustrated by the systematic review, in virtual worlds, money laundering has been investigated in several publications. In particular, the book "Virtual Economies and Financial Crime" by Clare Chambers-Jones (2012) highlights the problem very well, describing different

[32]United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. Signed 1988, entered into force on November 11, 1990. As of June 2020, there are 191 Parties to the Convention, including Italy. Money laundering has been addressed in the UN Vienna 1988 Convention Article 3.1 describing Money Laundering as: "the conversion or transfer of property, knowing that such property is derived from any offense(s), for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in such offense(s) to evade the legal consequences of his actions." https://www.unodc.org/romena/en/money-laundering.html

[33] Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, The Convention was opened for signature in Warsaw on 16 May 2005 and entered into force on 1 May 2008. There are 39 signatories and 28 party, including italy. https://rm.coe.int/168008371f

mechanisms that can be exploited to launder money. “As Kevin Sullivan states in his anti- money laundering training materials, ‘the virtual world with little regulation or observation by law enforcement is fertile ground and ripe with opportunity for the criminal element’. He continues to bemoan the lack of adequate regulation in virtual worlds. In the virtual world there is negligible means of monitoring financial activity, sparse due diligence, paltry customer identification rules, nor any mandatory forms or reports to complete” (Chambers-Jones, 2012). This lack of regulation and control described years ago is still relevant today, as demonstrated by the new regulations that the institutions adopt[34][35]. In the world, the financial regulation strategy for virtual worlds aims to combat the illegitimate use of cryptocurrencies, NFTs, and the blockchain, completely forgetting the gaming sector, which includes virtual currencies that are different from those mentioned in the documents. Furthermore, the content of the documents focuses almost exclusively on the Metaverse, considering it the only virtual world in existence. Virtual worlds within gaming are governed by the so-called TOS (terms of service) and EULA (end users license agreements), which establish guidelines of conduct that users must follow and regulate digital currency. For example, EULA article 4 of the VG Fortnite, created by Epic Games, which regulates game currency and content, mentions the following:

“Neither Game Currency nor Content are redeemable for money or monetary value from Epic or any other person, except as otherwise required by applicable law. Game Currency and Content do not have an equivalent value in real currency and do not act as a substitute for real currency. Neither Epic nor any other person or entity has any obligation to exchange Game Currency or Content for anything of value, including, but not limited to, real currency. You agree that Epic may engage in actions that may impact the perceived value or purchase price, if applicable, of Game Currency and Content at any time, except as prohibited by applicable law. You may not transfer, sell, gift, exchange, trade, lease, sublicense, or rent Game Currency or Content except within the Software and as expressly permitted by Epic.” (*Fortnite End User License Agreement*, 2023)

In general terms, this type of EULA is similar for almost all virtual worlds in which a virtual currency exists, and as can be seen, companies try to protect themselves by remarking in these licensing agreements that in-game currency has no real-life counterpart or value, but what happens is very different. It is true that companies expressly prohibit users from making improper use of virtual currency, but it is a deterrent that does not prevent users from carrying out illicit activities. Figure 29 represents the Fortnite virtual currency, V-BUCKS, with its relative price in real currency. Therefore, if a user wants to buy 1000 V-BUCKS, he will need to spend 8,99 euros.

[34] Eu Strategy for Virtual Worlds: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3718
[35] Uae Strategyhttps://www.tamimi.com/law-update-articles/virtual-currencies-real-world-regulation/

Figure 28: FortniteV-buck in game shop. Elaborated by the author.

Continuing the research and sticking to what the EULA establishes, on the internet, it should not be possible to find digital currency for sale and/or sites that sponsor this currency; instead, by simply typing "Fortnite v-bucks buy" into Google, it is possible to have 15 million results, which contain thousands of sites for exchanging and/or selling this currency as shown in Figure 30.

Figure 29: Fortnite V-buck on sale on www.z2u.com. Elaborated by the author.

This site and all the others are public and, therefore, accessible to all users. However, in addition to sponsored websites, many private exchanges are managed by companies that do not sponsor this activity, conducting them more secretly. Nevertheless, how do these activities develop? These activities are portrayed in two different ways:

1) private users that exchange and sell currency in exchange for services or money,

2) companies that have built a truly lucrative currency system through bots.

The first case is not relevant like the second, as it is less structured and complex. Every private user can replicate that model on any portal, as illustrated in Figure 31, where users sell currency and gaming accounts via eBay.

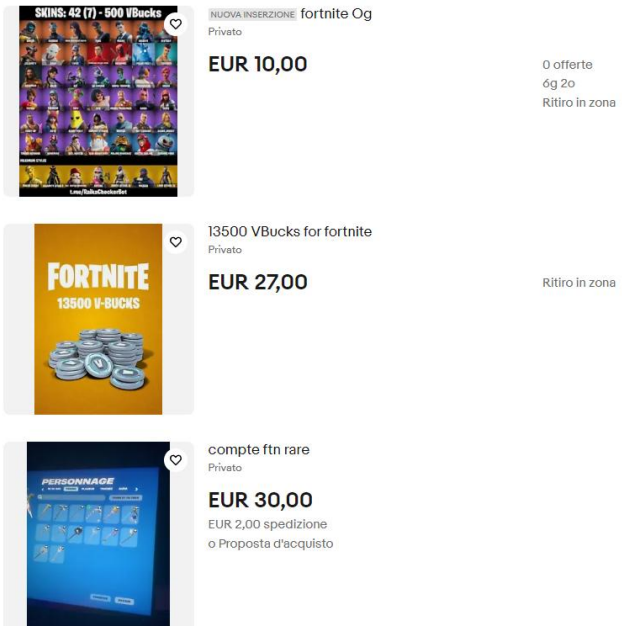

Figure 30: Users selling accounts/V-buck on ebay. Elaborated by the author.

The second case, however, deserves more attention and concerns the criminal organizations that use bot farmers and gold sellers. The latter use worldwide factories created by "anonymous users," with fake websites without traceable content. Their job consists of creating accounts and, consequently, avatars who, thanks to macros (preset keys that allow the character to perform specific actions in the game), "farm" (acquire) the currency within the game to resell it for real currency. Trying to perform some research will reveal thousands of sites like the one reported in Figure 32 and 33:

Figure 31: A Website featuring in-game currency sales for real money in gw2. Elaborated by the author.

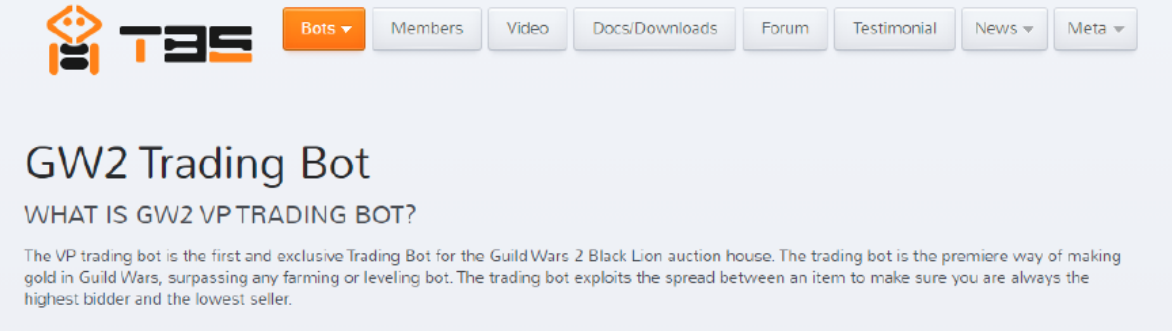

Figure 32: A site that promotes bot systems for currency farming. Elaborated by the author.

This mechanism manifests within virtual worlds with bots exploiting chats to offer services. Sometimes, a global chat is used, while other times, more sophisticated bots send private messages directly to users so as not to be banned so quickly. The gaming companies ban these bots when caught; however, it is not enough, as it is true that the bots will be banned, but after a few minutes, they return, and this process is repeated for millions of bots. Figure 34 illustrates how this mechanism appears inside three different virtual worlds.

Figure 33:Bots that spam the sale of currency for real money. Elaborated by the author.

This illegal system is a worldwide phenomenon with infinite possibilities: “There’s no limit to money creation, says Michael Morrison, an Edinboro University of Pennsylvania economics professor who wrote his dissertation on the World of Warcraft economy. In the real world, money is created through a federal reserve. Historically, the limit was how much gold was in the ground. In World of Warcraft, currency continues to grow with play. The more people play, the more hours played, the more money is in the system and the more inflation you see. More organized botters sell

the in-game money or high-level characters they obtain to players in exchange for cash on third-party websites. On Loknar's server, 100 gold goes for $4.79, while 1,000 gold goes for $47.73. (No bot-makers or gold sellers agreed to an on-the-record interview for this article.)" (D'anastasio, 2020). It is, therefore, clear that these platforms, despite the various regulations seen previously, are perfect territory for perpetrating money laundering. "Virtual environments continue to be an ideal environment for criminals to launder money, as there are very few checks to ensure whether financial transactions are legitimate. Furthermore, criminals are able to hide behind the anonymity of the avatars they create, making identification difficult." (Keene, 2011) Consequently, how is money laundering carried out in practice on these platforms? Figure 35 illustrates the entire process.

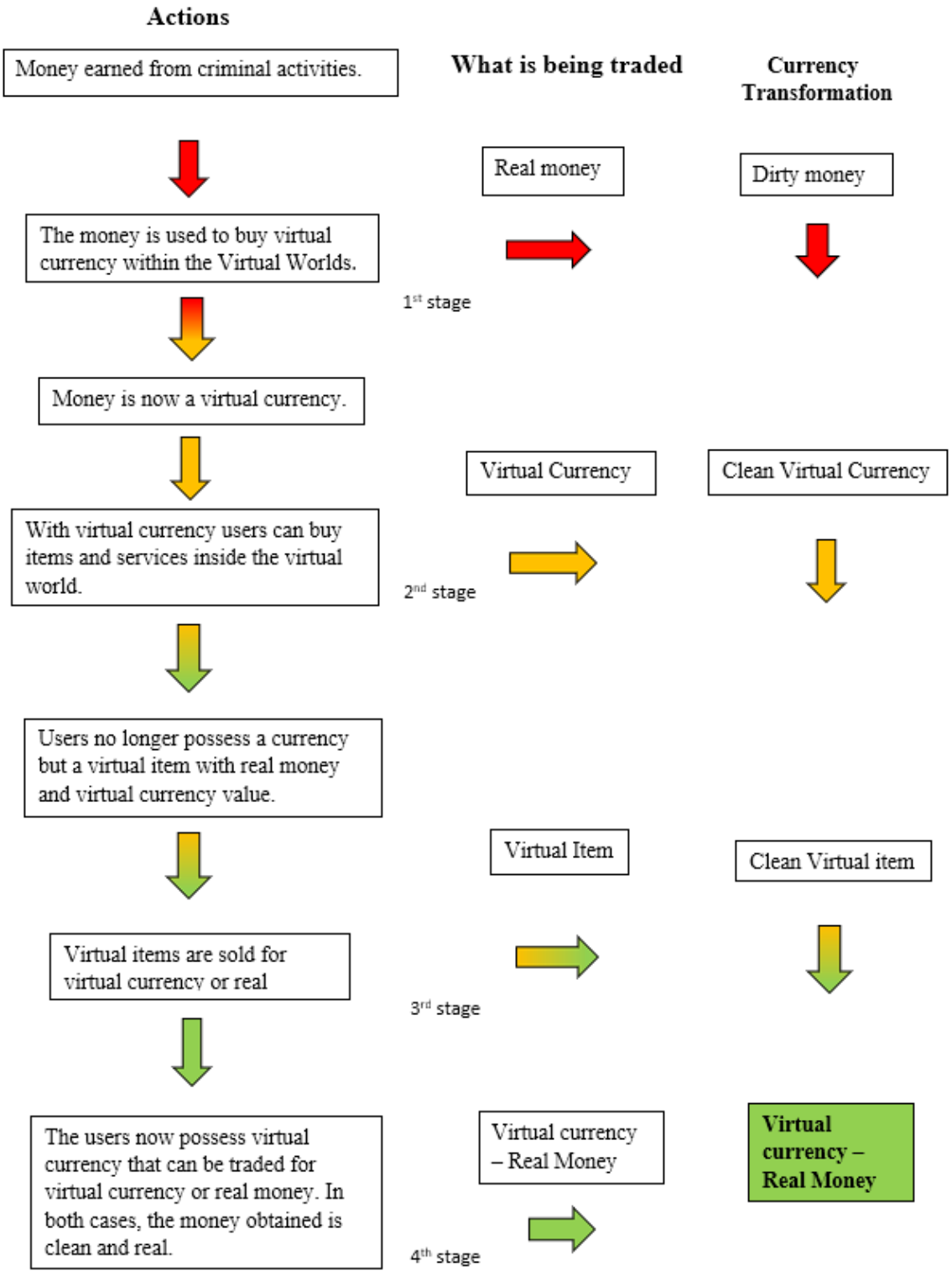

Figure 34: Money Laundering System in Virtual Worlds. Elaborated by the author.

The flow illustrated in the scheme is made up of different stages representing both steps and difficulty tracing the phenomenon. In the first step, it is not easy to hypothesize possible money laundering behind a transaction, but it is still possible. Between the second and third steps, the chances of tracing the transactions and the phenomenon become equal to 0. At the same time, it is

impossible to identify money laundering between the third and fourth steps. This is because the initial capital no longer corresponds to money but to a currency and objects/services, which makes it impossible to understand their origin at the time of purchase. This scheme may also have variations because with the arrival of the Metaverse and Non-fungible Tokens (NFTs) the problem becomes more acute, adding a parallel layer including cryptocurrencies and NFTs. The procedure will be the same, with minimal variations relating to the virtual world's content. Therefore, this proposed scheme illustrates a new system to launder money not defined in previous literature, highlighting the simplicity with which users or criminal organizations worldwide can carry out this process. Returning to the TOS and EULA seen previously, it is clear that these are insufficient deterrents to prevent money laundering on these platforms. "Virtual world economies are 'all very normal and mundane. They have work, business, societies, commodities just as we do on Earth. However, Castronova continues to state that, 'given further thought . . . virtual economies may be anything but normal'. By this he means that in the real world, governments control the prices of goods, through supply and demand and price control. In cyberspace, this is one of the major differences." (Chambers-Jones, 2012). This problem is exacerbated today by the fact that since the 1990s, there has been no regulation and/or law about this phenomenon[36]. For this reason, it is necessary to think of other, more innovative solutions to engage with this phenomenon.

2.6 Internet Challenges, suicide instigations, homicide planning

The phenomenon of challenges and suicide instigations has gone viral in recent years, causing numerous deaths (Henderson, 2023; Levenson& Rubin, 2022) among teenagers. When the media reports a case of suicide or death, they cite social media as the primary vehicle for these challenges, forgetting the entire gaming environment. Is it true that these challenges are carried out via social media, but also in virtual worlds. When virtual worlds did not exist, people had to use social media to meet or speak to others worldwide, creating a different relationship between users, as on SM, it is necessary to request friendship or follow up to chat. This step is overcome in virtual worlds and the gaming environment because users can interact directly without barriers. If once it was hard to know how one's peers were behaving abroad because the communication system made it difficult to find out, now through virtual worlds, one can interact with peers from other countries who can

[36]For example, for article 648-bis (Italian penal code), the necessary requirement is the use of bank accounts; here, no one uses current accounts. Furthermore, the proceeds must come from a non-negligent crime; these are normal transactions that can be carried out in this context. The same goes for legislative decree no. 125 of 4 October 2019, implementing the EU anti-money laundering directive 2018/843. They do not apply to this type of case: both legislations refer to cryptocurrencies or tokens/currencies that do not fall within this category. And they also aim to regulate the platforms or providers of these services. Other regulations fall within these rules and therefore are ineffective in this environment.

suggest taking up a challenge not yet known. Among the most famous challenges, there is the knockout game, which is still practiced today, with recent events occurring worldwide (Garau, 2023; Moore, 2022), and the Blue Whale that has been recently returned to the news (Greyman-Kennard, 2023).In addition to the most famous, there is also the Jonathan Galindo phenomenon, in which the character instigates victims to commit suicide; the Benadryl challenge, which takes its name from the drug based on Diphenhydramine (an antihistamine), where participants must take multiple tablets at the same time in order to trigger hallucinogenic reactions. The Momo challenge similar to the Blue Whale, where the avatar is represented by a woman with long, black hair, and the ultimate aim is suicide. The Kiki challenge, where people must jump out of a moving vehicle and dance to the song "In My Feelings," endangering both your own life and the lives of others. The Fire Challenge, which consists of setting a person on fire and seeing how long they resist, and the pass-out challenge, where people voluntarily try to take away oxygen in order to cause hallucinations and fainting. To demonstrate that virtual worlds and related applications are also an excellent tool for spreading challenges, the research investigated the community of some Discord servers and virtual worlds, and the results are visible in Figure 36 and 37.

Figure 35: A list of users impersonating Jonathan Galindo on Discord. Elaborated by the author.

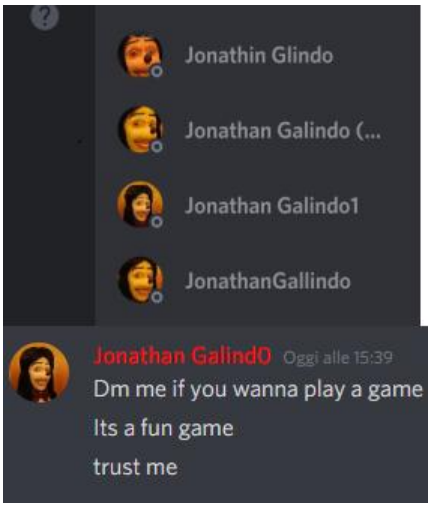

Figure 36: Users impersonating Jonathan Galindo on Discord. Elaborated by the author.

Unfortunately, in addition to the more well-known challenges, there are also less well-known challenges perpetrated in closed groups only in virtual worlds. An example above all is that of the Reiko Trap Harem. Born in 2018 under the idea of a user called Reiko, this challenge involves taking hormones to resemble a trap[37] as much as possible. In addition to this challenge, there are several ones in which wounds on the body, drug use, and suicide attempts are expected. Figures 38, 39, and 40 illustrate some of the material recovered during research.

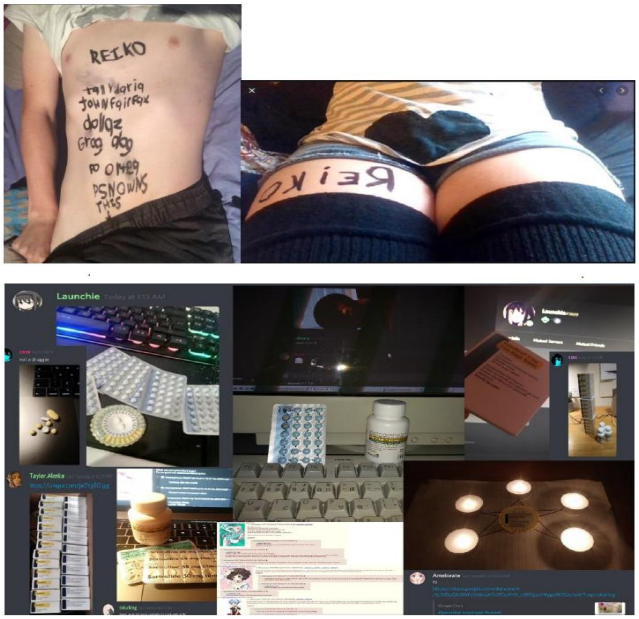

Figure 37: Users perpetrating challenges on Discord. Elaborated by the author.

[37]"Traps" are girls with an almost flat body, without muscles but with much energy, a stereotype in many Japanese manga depictions.

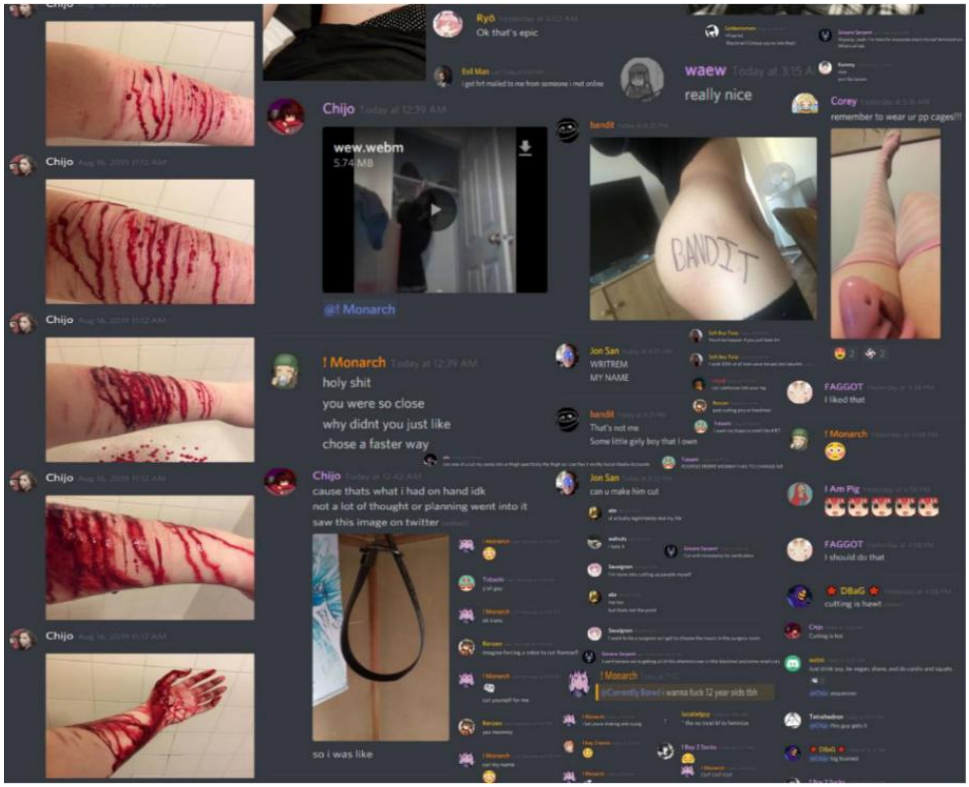

Figure 38: Users perpetrating challenges on Discord. Elaborated by the author.

Figure 39: Users perpetrating challenges on Discord. Elaborated by the author.

Lastly, the research has also uncovered some chats where users were discussing the intention to kill someone and/or plan a school shooting, as illustrated in Figure 41.

Figure 40: Users talking about school shooting on Discord. Elaborated by the author.

2.7 Weapons and drugs trading

The global rise in the utilization of social media platforms for the illicit trade of drugs is a burgeoning phenomenon. This trend is fueled by the dynamic and diverse nature of the modern social media environment (Demant et al., 2019; Moyle et al., 2019; Oksanen et al., 2021). Social media drug markets share a standard core functionality across various platforms. They primarily serve as intermediaries, connecting buyers with sellers and streamlining the coordination of transactions. Similarly, virtual worlds and their applications are also used as a communication channel to facilitate sales. An example of the material found can be seen in Figure 42.

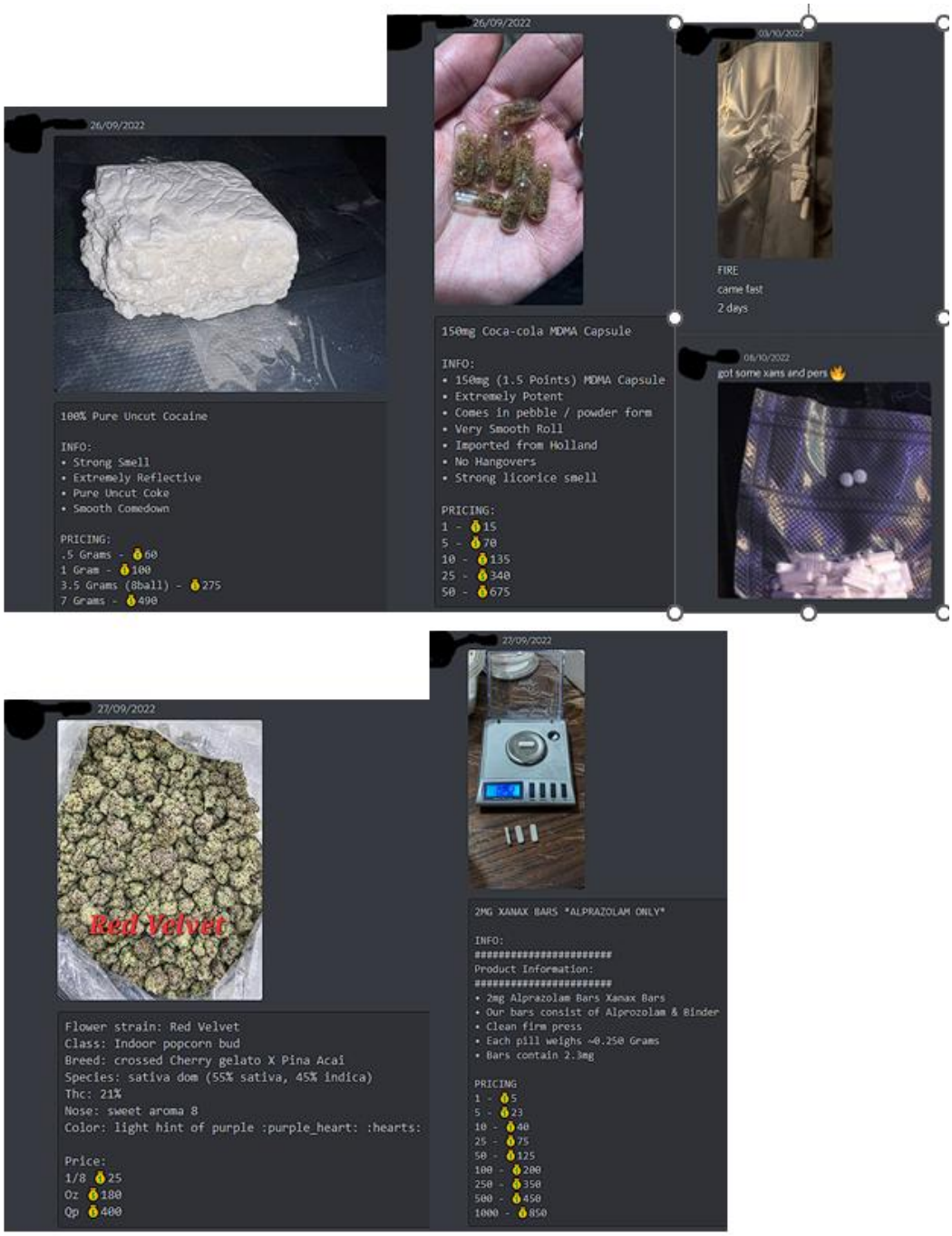

Figure 41: Users selling drugs on Discord. Elaborated by the author.

Most of these sales occur in applications related to virtual worlds because users are interested in the quality of the goods sold, which can only be shown on related applications and not within virtual worlds. In this case, virtual worlds act as an amplifier because sellers use their functions (chat, audio, private messages, etc.) to offer their goods to a broader audience. The sale of drugs on these servers is mentioned in a recent article (Van Der Sanden et al., 2022), which highlights a particular case that occurred in New Zealand, in a local community, where users used these platforms to facilitate drug trafficking. In addition to the various channels selling drugs, it was also possible to witness servers where users were intent on selling weapons. These servers have an international

vocation, English is spoken, and users come from all over the world, but the most affected country or the one in which the most number of users was found was the United States. These places function like a marketplace, with users posting images of their weapons and then moving to private channels to complete purchases. Finding them is not easy because they are often disguised under false names, and it is even more unthinkable to be able to find them without a connection to gaming. Many of these servers were created by "sponsoring" a video game, containing rooms and channels dedicated to this type of activity within them. In Figure 43 and 44 are illustrated some examples.

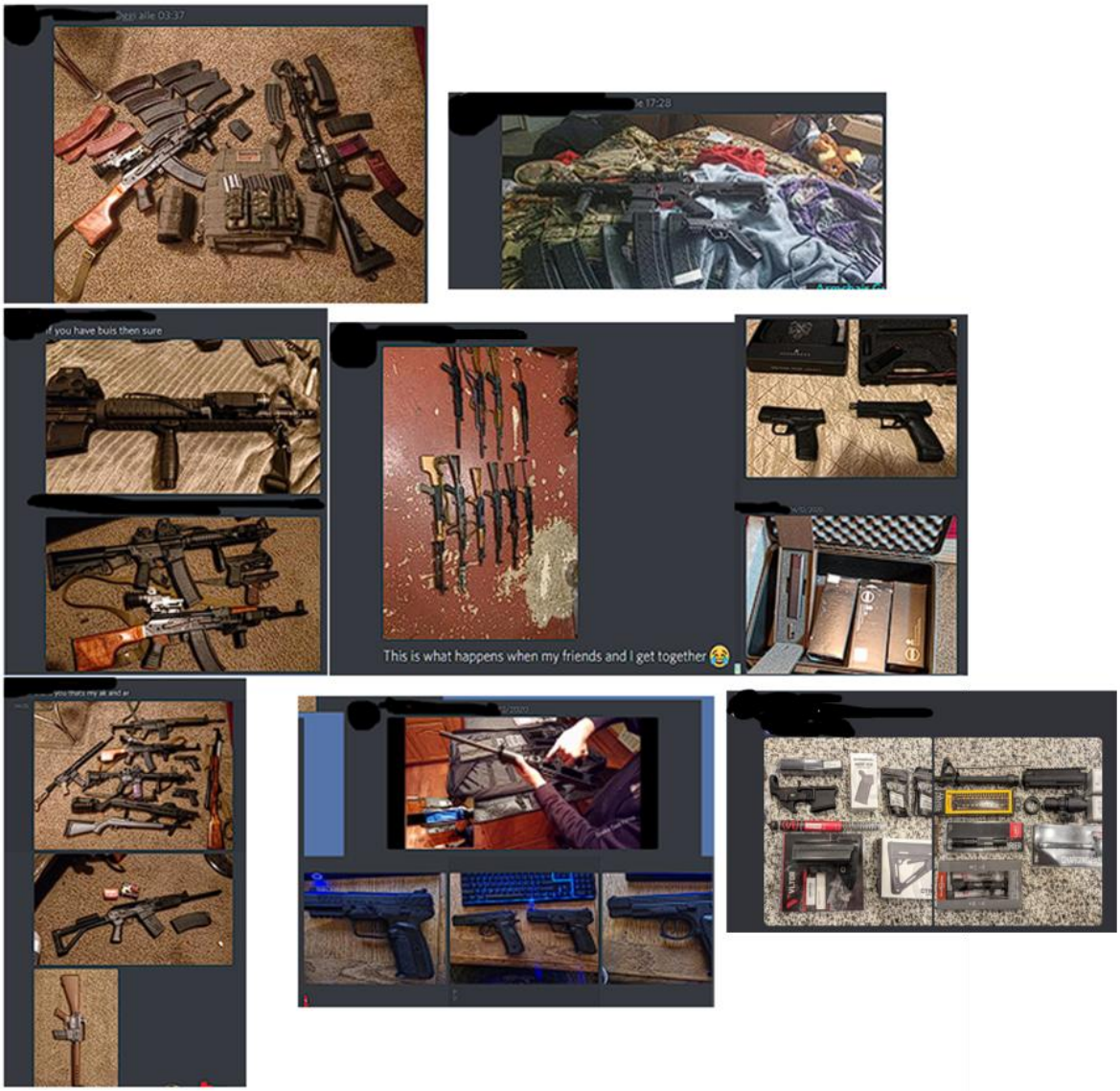

Figure 42: Users showing/trading their weapons on Discord. Elaborated by the author.

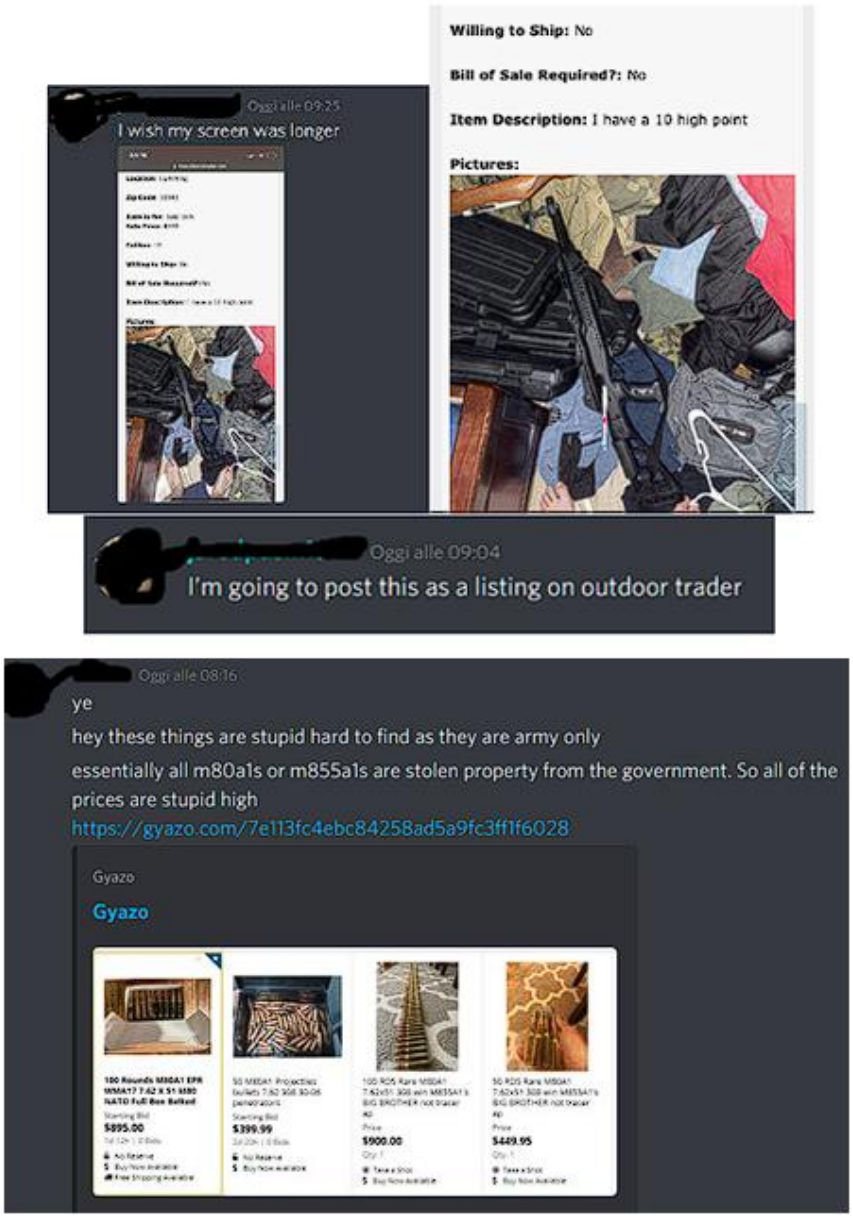

Figure 43: Users showing/trading their weapons on Discord. Elaborated by the author.

Generally, trades occur locally between users in the same cities while rarely taking place internationally via private couriers.

2.8 Terrorism and Right-Wing extremism

After the attacks of September 11, 2001, intelligence agencies around the world raised the alert and surveillance thresholds in the digital environment[38]. Since 2008, American intelligence has also begun investigating virtual gaming worlds, considering them an important communication vehicle

[38]After the attack on the Twin Towers on September 11th, the United States, as well as many countries in the world, have implemented many security measures at both a physical and cyber level, thus raising the levels of surveillance and security. Some information can be found here: https://www.cfr.org/timeline/how-911-reshaped-foreign-policy https://www.brookings.edu/articles/how-technology-and-the-world-have-changed-since-9-11/

for terrorists. A secret COMINT[39] report made for Five Eyes (FVEY)[40] by the Government Communications Headquarters (GCHQ)[41]has been found among the documents released by Edward Snowden. This document contains five chapters, which are five papers that discuss the potential misuse of Games and Virtual Environments (GVEs) and the opportunity for intelligence agencies to operate in that cyberspace.

"We know that terrorists use many feature-rich Internet communications media for operational purposes such as email, VoIP, chat, proxies, and web forums and it is highly likely they will be making wide use of the many communications features offered by GVEs by 2010. With a few exceptions, the National Security Agency (NSA) can't even recognize the traffic, and therefore it is impossible to even say what percentage of the environment is GVE; let just determine how targets are using the communications features of GVEs. However, GVEs offer a SIGINT/HUMINT opportunity space, and more research is needed to figure out effective exploitation. Al Qaida terrorist target selectors and GVE executables have been found associated with XboxLive, Second Life, World of Warcraft, and other GVEs in PINWALE network traffic, TAO databases, and in forensic data. Other targets include Chinese hackers, an Iranian nuclear scientist, Hizballah, and Hamas members. GCHQ has a vigorous effort to exploit GVEs and has produced exploitation modules in XboxLive! and World of Warcraft." (Edward Snowden Released Documents, nd)

In 2011, a Canadian study (Botnet Analysis Report) reported the following:

"*Virtual world terrorism facilitates real world terrorism: recruitment, training, communication, radicalization, propagation of toxic content, fund raising and money laundering, and influence operations. The report claims that inside virtual worlds, terrorists have modified games to make Allied troops the default enemy so would-be terrorists could be recruited and trained. The Canadian report doesn't stop there, adding that these games are used for state-sponsored espionage. The player-to-player text and VOIP chat are used for: covert communication between cells, illegal agent networks or the ephemeral clans' or guilds' in MMOG. These environments allow players to conduct real-money transactions (RMTs) in virtual worlds and permit the unregulated currency exchange of virtual credits for real funds. Gold farming' and power levelling' operations of criminal organizations are some of the novel means of exploiting the medium. The encrypted exchange of zero-day network exploits is present as is the out-of band control and tasking of bot-nets."* (Storm, 2011)

[39]Communications Intelligence

[40] The Five Eyes (***FVEY***) is an Anglosphere intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States.

[41]Uk's intelligence

Many years have passed since those documents, but even today, the state of the art demonstrates that there is no solution to the problem, and indeed, it has become even more complex, given the innumerable number of virtual worlds that exist today. In 2020, Gilles De Kerchove, the head of the European Counter-Terrorism Section, alerted security services globally, stating the following:

"*Online video games can be used to propagate extremist ideologies and even prepare attacks, the EU's anti-terrorism coordinator told AFP in an interview in which he urged more regulation. You have extreme-right groups in Germany that have come up with games where the aim is to shoot Arabs, or [Hungarian-born US Jewish billionaire George] Soros, or Mrs. [German Chancellor Angela] Merkel for her migration policy, etc." "That can be an alternative way to spread ideology, especially of the extreme right but not only them, a way to launder money… there are currencies created in games that can be exchanged for legal tender, he said. It can be a form of communicating. It's encrypted. It can also be a way to test attack scenarios, he continued*." (Mondesert, 2020)

In literature, it is also possible to find some interesting articles that have dealt with the link between virtual worlds and terrorist propaganda. "In relation to video games and terrorism, a number of games directly deal with terror-related issues, especially in connection with the War on Terror. For example, Splinter Cell is a game that revolves around the 9/11 events, while Counter-Strike allows teams from opposing sides to take the role of terrorists as well as counter-terrorists. Similar to Counter-Strike, other games like America's Army, Modern Warfare 2, and Medal of Honor: Warfighter allow players to become terrorists, which could have some psychological and educational benefits." (Al-Rawi, 2018).

This study focuses on the language and communication created by terrorist organizations. Subsequently, it is highlighted how they can carry out propaganda through these platforms thanks to particular communication techniques. For example, many of these organizations create or copy previous games, obtaining a sort of conceptual re-frame also at a linguistic level:

"In 2006, Al-Qaeda group made changes to the first-person shooter (FPS) game Quest for Saddam (2003) and introduced another game called Quest for Bush. The goal of the original game was to kill Iraqi soldiers and capture Saddam Hussein, whereas Al-Qaeda completely reversed the players' roles. On the other hand, video games by the Lebanese Hezbollah and Syrian Afkar Media company were used as alternative media outlets to offer playing roles that were contrary to the mainstream Western representation of Arab Muslims. In this way, video games provide violent non-state actors and organizations sympathetic to them with a means of presenting their grievances and displaying their fighting prowess in ways that advance the organizations' strategic goals. Some of these

alternative games include Quraish and Under Siege, which were both produced by Afkar Media." (Al-Rawi, 2018).

There is, therefore, a link between terrorism and Virtual worlds, which is created with the dual connotation of friend-enemy. It is common to find VGs produced by these organizations, which use the friend-enemy combination to underline and emphasize the differentiation between "us who are right" and "them, the enemy." An enemy often represented by the West, which, with its habits and customs, supplants the traditions of others and destroys other lands. These VGs are used as a marketing tool by these organizations, including ISIS, which, thanks to its skilled communication skills, has managed to recruit thousands of members in the West (Ham-Kucharski, 2022). Therefore, these platforms are an ideal means for propaganda, thanks to the ability to reach a potentially unlimited number of people. Figures 45 and 46 illustrate some examples of propaganda.

Figure 44: Pictures recovered from Al-Rawi, and Dauber et al papers.https://www.tandfonline.com/doi/full/10.1080/09546553.2016.1207633

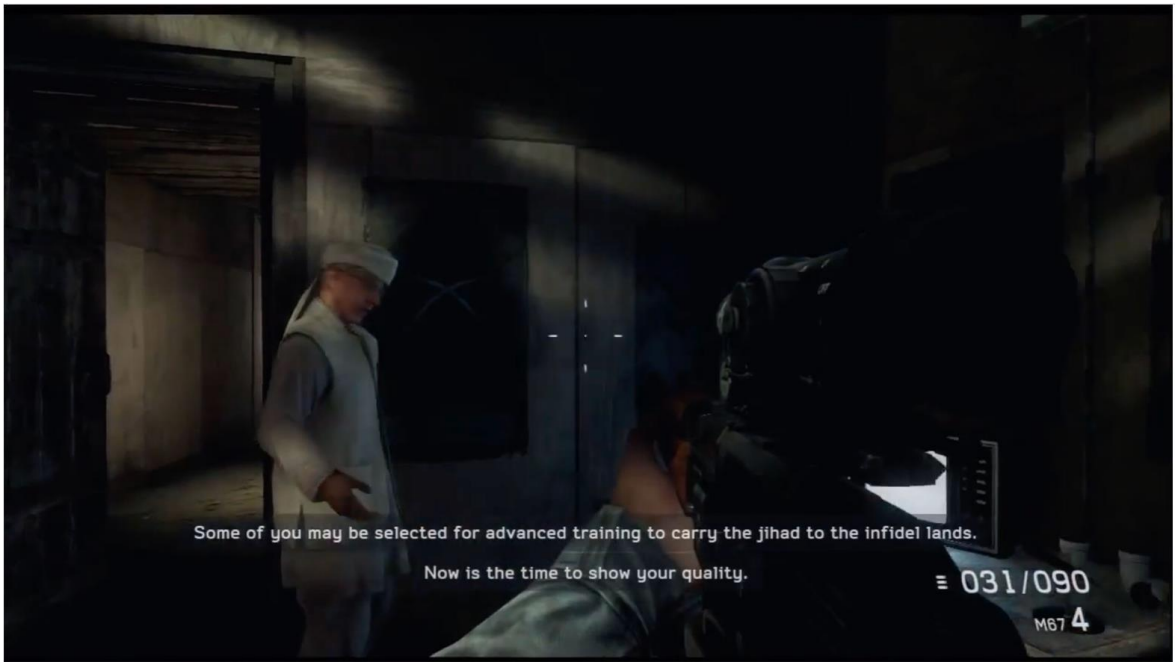

Figure 45: Propaganda inside Medal of Honor warfigther - Mission#2. Image recovered from Salvador Miranda article: https://thehmm.nl/the-simulated-real/.

As with Western games, in which there are missions in which you have to kill terrorists, the jihadists have similarly recreated VGs in which the West and, in particular, the United States are the primary targets. In addition to propaganda, there are events that exactly reproduce terrorist attacks that occurred in the past, as in the case of "ARMA 3: Takistan life". In this VG, the events of September 11, 2001, the London attacks of 2005, and the Thalys attacks of 2015 are reproduced[42]. In addition to this, in the VG, you can learn to negotiate with terrorists with various communication techniques, simulate training sessions, and practice detonating bombs with a remote detonator. On the one hand, there are VGs created specifically for propaganda and recruitment, while on the other, these organizations have the great ability to infiltrate Western Virtual communities. Religious terrorists and political extremists use regular VGs on a daily basis, and it is often possible to find a member of ISIS or some terrorist organization while playing VGs. Comments like those in Figure 47 are very common and demonstrate how the VGs favored by these organizations are Western ones and no longer those created by themselves. As Western VGs are more advanced and have

[42]The September 11 attacks were a series of airline hijackings and suicide attacks committed in 2001 by 19 terrorists associated with the Islamic extremist group al-Qaeda. It was the deadliest terrorist attack on U.S. soil; nearly 3,000 people were killed.https://www.britannica.com/event/September-11-attacks.
London bombings of 2005, coordinated suicide bomb attacks on the London transit system on the morning of July 7, 2005. At 8:50 AM explosions tore through three trains on the London Underground, killing 39. An hour later 13 people were killed when a bomb detonated on the upper deck of a bus in Tavistock Square.https://www.britannica.com/event/London-bombings-of-2005.
On 21 August 2015, a man opened fire on a Thalys train on its way from Amsterdam to Paris. Four people were injured, including the assailant. French, American and British passengers confronted the attacker and subdued him.https://en.wikipedia.org/wiki/2015_Thalys_train_attack.

become real simulators of reality, they become real means of acquiring new knowledge. Furthermore, gaming-related applications and chats increase the space for their propaganda.

Figure 46: Extract of an image posted on Discord with a link to a YouTube video and a comment as an example.

These virtual worlds are used for terrorist purposes, but extremism can also be found. A podcast held by Katerina Vittozzi in the UK shows how the phenomenon is rampant and how many young people are plagiarized and recruited through these platforms.

“Mr Bromage said the child-specific content being used by the far-right to target youngsters online included shoot 'em up video games, memes and videos. The nine-year-old boy had been recruited by his older brother who showed his younger sibling "extreme neo-Nazi video games," he added.” (Vittozzi, 2020)

The strategy used by these far-right recruiters is the same as that of terrorists; therefore, video games, memes, and propaganda images invite users to enter private virtual spaces. Figure 48 provides an example.

Figure 47: First picture recovered from the correspondent KaterinaVittozzi. (https://news.sky.com/story/sharp-rise-in-children-investigated-over-far-right-links-including-youngsters-under-10-12131565), Second picture Recovered from the correspondent Julia Alexander (https://www.polygon.com/2018/2/28/17061774/discord-alt-right-atomwaffen-ban-centipede-central-nordic-resistance-movement). Examples of propaganda.

The research conducted, following and tracing different users in these virtual worlds, has brought to light different material that demonstrates how these spaces are used for the aforementioned purposes. Examples are reported in Figure 49,50,51,52 and 53.

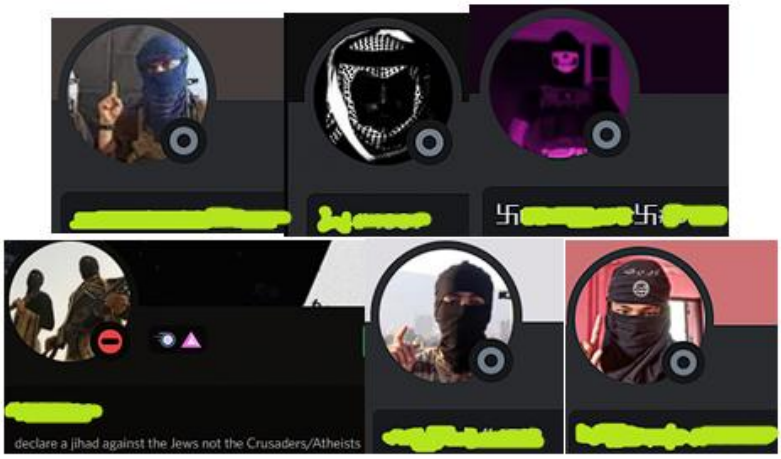

Figure 48: Avatar of users doing propaganda. Elaborated by the author.

Figure 49:Different propaganda servers on Discord. Elaborated by the author.

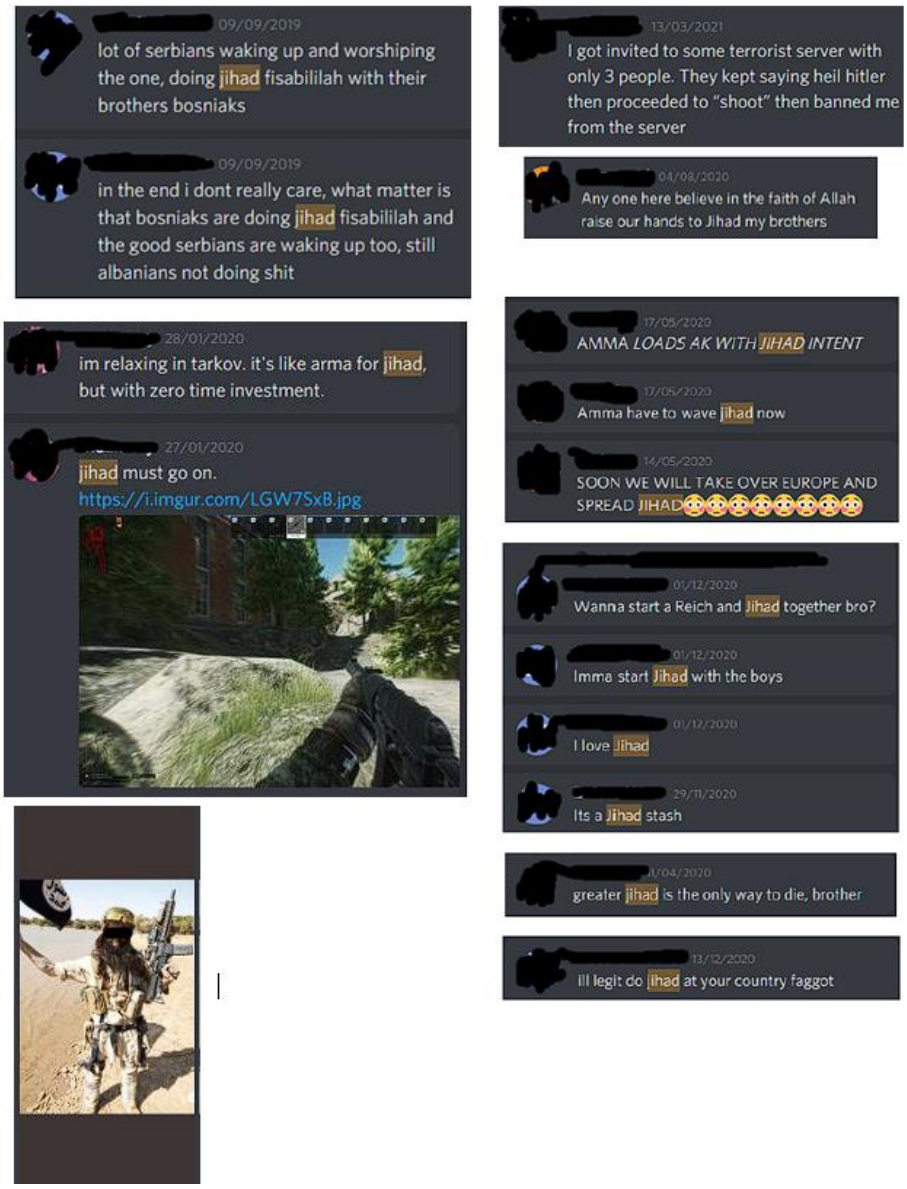

Figure 50: Extremisms and propaganda on Discord. Elaborated by the author.

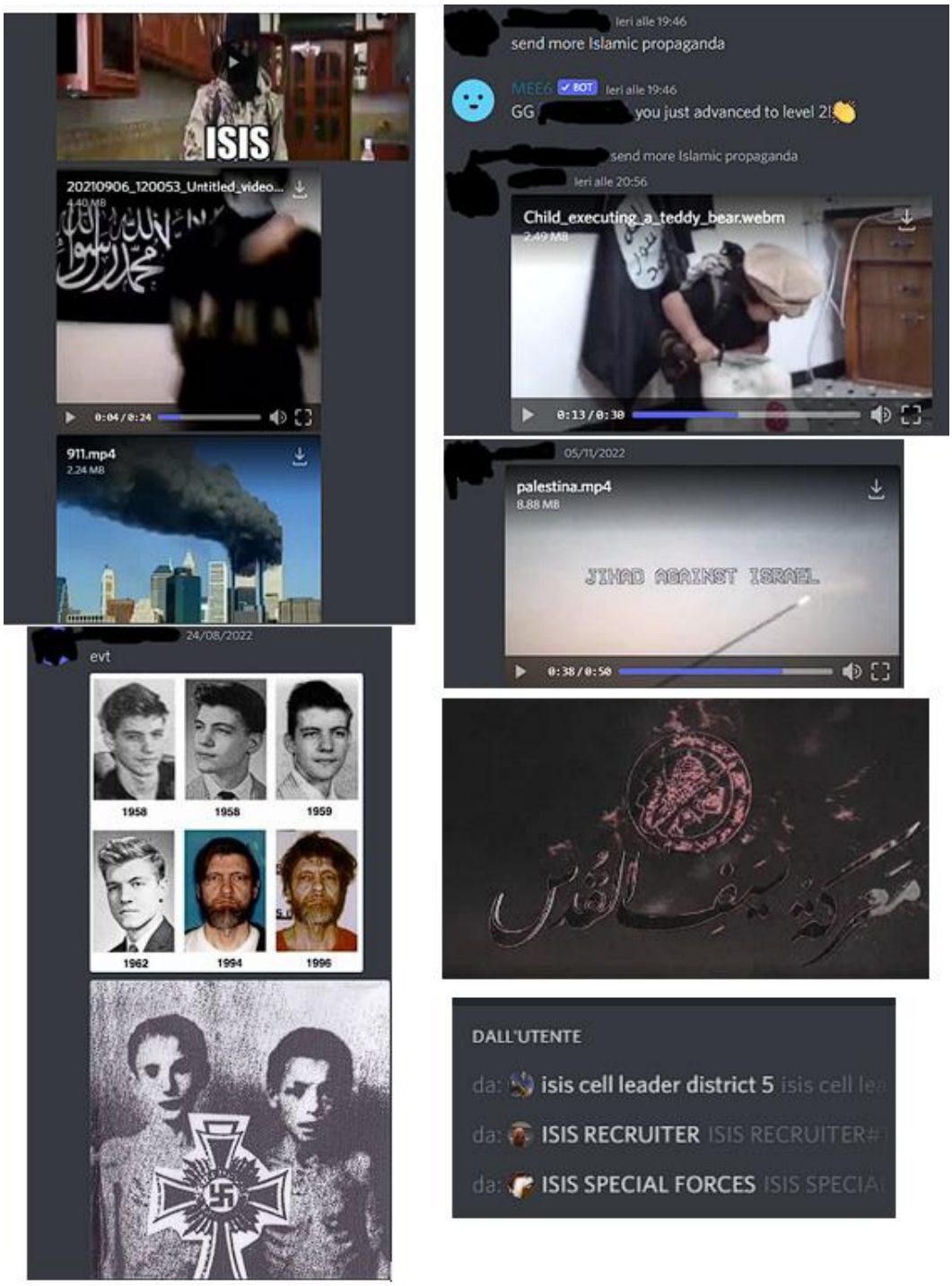

Figure 51: Extremisms and propaganda on Discord. Elaborated by the author.

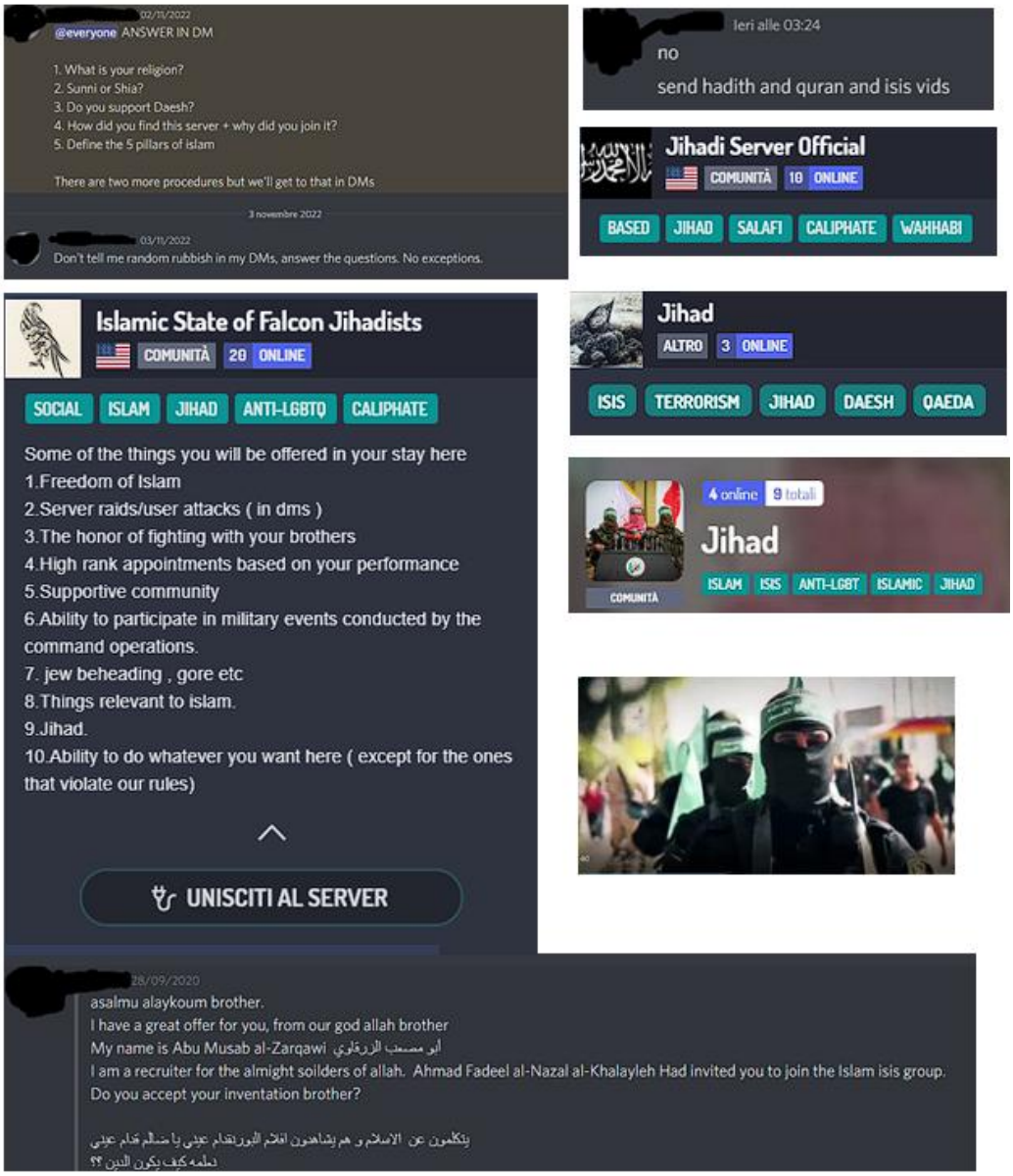

Figure 52: Extremisms and propaganda on Discord. Elaborated by the author.

There are several cases in which it has been possible to find this phenomenon, to which research has also dedicated more time based on the resulting importance of national security.

2.9 Children's safety in the gaming environment

Thanks to the internet, online gaming allows connecting with millions of players worldwide, increasing users' communication possibilities. While on the one hand, this innovation has undoubtedly brought many benefits for players, and an enticing market (E.g., Esports) has also increased the risks children can be exposed to while accessing these applications (UNICEF, 2020; Weru et al., 2017).Video game companies have taken preventive measures to mitigate the risk of exposing children to explicit or illegal content (Epic Games, 2023; Riot Games, 2023). However,

these efforts have not prevented the risk (Krossbakken et al., 2018). Children in the gaming environment can move freely through the multitudes of chats that video games offer without limitations and engage with anyone from anywhere. According to the Nations Interregional Crime and Justice Research Institute (UNICRI) report on gaming (UNICRI, 2022), grooming increased by 70% from 2017 2018 to 2020 2021; in the US, 59% of kids aged between 12 and 17 have experienced cyberbullying, and CSAM (Child sexual abuse material) also increased significantly. These studies suggest that efforts to prevent children from being harmed in the gaming environment have been insufficient. Most of the research conducted in this environment also does not correctly target gaming platforms (Faraz et al., 2022) but focuses on social media chatting platforms (Al-Garadi et al., 2019; Jevremovic et al., 2021), which are completely different from the gaming environment. More recently, new applications of AI to predict and counter predator behaviors against children have been proposed in different publications (Preuß et al., 2021; Agarwal et al., 2022). However, the chats examined were taken from social media, not gaming platforms. The difficulty of analyzing video games is that no datasets are available, and research in these environments is still far from having found an effective methodology (Lankoski&Bjork, 2015). Most social interactions in the gaming environment are a combination of verbal and written messages, which creates many difficulties when the AI has to distinguish between a chat referring to the content of a video game rather than a user. For example, if a user is typing, "I will f**k him hard," the AI would probably detect abusive language. However, it needs to find out if this sentence was directed to a user or in-game content, creating inaccurate outcomes. Furthermore, technologies have yet to prove they can successfully target vocal messages and prevent inappropriate behavior in the current state of the art, complicating the situation. Given this scenario, the research has explored this aspect in depth, reviewing the current child protection measures on these platforms and comparing them with the results of a survey conducted among 330 children under 18. Through awareness campaigns, governmental and nongovernmental organizations guide parents in monitoring children's behavior on these platforms with different annual reports (Cook et al., 2021; WHO, 2022; Childline, 2022). Although useful, these reports are little observed, and therefore, they prove ineffective. The risks that children can face in these virtual worlds are multiple: from predators who actively roam these platforms (Wilcock, 2024) to scam attempts by abusing the naivety of children, blackmail, and sexual harassment (Kavenagh, 2023). Cyberbullying (Stopbullying.gov, 2021), hate speech (Costa et al., 2021), far-right recruitment (Koehler et al., 2023). To ensure children's safety in the gaming environment, different approaches are primarily used today:

Age classification systems for Online Games:

The classification system attempts to classify the content of videogames according to different criteria and match them to appropriate age groups.

PEGI from Europe (PEGI, 2023) is an age classification system used by 38European countries, which rates video games according to content.

ESRB from America (ESRB,2023) is a classification system that provides information regarding the content of video games and rates them accordingly.

USK from Germany (USK, 2023) is the official rating system in the country, as Germany does not officially recognize PEGI. The system works like PEGI.

GRAC/GCRB from South Korea (GRAC/GCRB, 2023) rates video games according to the content, and it is very similar to others but with some differences.

ACB from Australia (ACB, 2023) rates video games according to the content but slightly differs from other systems.

RARS from Russia (RARS, 2023) rates video games similarly to other systems but is broader.

IARC Global (IARC, 2023) is a standard age classification method for video games.

Depending on the country, certain elements in the game are given more or less weight than others, but everyone strives to achieve the same result or that of categorizing a video game as accurately as possible. The aim of giving an appropriate age for the in-game content is to preserve a safe environment for children, but this system continues to be ignored, becoming irrelevant (Hollett et al., 2022).

Parental control on Online Games:

In order to keep children safe, some gaming platforms offer parental control, a feature that enables parents to limit their children's activity. Through filtering, parents can observe the children's activity in gaming, block communications with strangers, and monitor their in-game activities. However, this system, widely used today by most of the famous gaming platforms (Fortnite, Roblox, Minecraft), has not proven successful, as different news indicates increased offenders in this environment and children being harmed (Hoose, 2020; Goldenberg, 2021; Blankley, 2023). In addition, according to different reports, including ISFE (Interactive Software Federation of Europe), parental control reveals that awareness and use of parental control are insufficient among parents (Videogames Europe, 2018; Taylor, 2018; Guttmann, 2023). Parental control is also a feature only available on some gaming platforms, and each one can differ in its functions, leaving some without

this security system. Furthermore, to work, parental control must be activated by the parent or the user who uses the video game. Unfortunately, this only sometimes happens due to a lack of knowledge or limitations.

AI for children's safety in Online Games:

Other attempts to curb possible offenders and protect children in this environment have been made with AI. For example, Negobot (Laorden et al., 2013), a bot that aims to analyze chats to identify individuals who try to hunt kids, has been proposed and tested. However, this bot does not intervene directly in live chats during gameplay but can only be used on pre-established and/or retrieved datasets. Like Negobot, other automated tools were tested or developed conceptually without success (Zambrano et al., 2017; Zuo et al., 2018). More specifically, these tools were not tested or created for the gaming environment but on datasets of chats recovered from social networks.

Legislation and Regulations Applicable to Online Games:

Additionally, UNICEF presented a comparative study in 2019 showing how some articles of the Convention on the Rights of the Child can also apply to children in gaming environments (UNICEF, 2019). Furthermore, the International Telecommunication Union launched an initiative in 2008 (COP), with the latest upgrade occurring in 2020, where the set of guidelines was adjusted to the increasing threats online for children (COP, 2020). The illustrated approaches highlight the intention to safeguard children in the gaming environment, but today's results are not very encouraging. Not only, as seen previously, have crimes increased, but the complexity with which these virtual worlds evolve and are built has made the systems in use obsolete. With Web 3, the Metaverse, and new emerging technologies (Blockchain), which encompass gaming features (avatars, chat interactions, etc.), the threats are escalating, making it difficult to control access and develop an adequate safeguarding policy for children in such an environment.

This research, as an integral part of the thesis work, was conducted with a survey composed of 13 questions regarding the gaming experience online that has been administered to 330 participants. The participants were selected from gaming platforms, Discord servers related to gaming, and local schools. Gaming platform participants were recruited through in-chat advertising; the video games where the people were selected include Fortnite, Call of Duty, Minecraft, Roblox, GuildWars 2, League of legends, and World of Warcraft. The advertising consisted of messages posted in chat by

the researcher inviting users to participate in the questionnaire with the relevant link. For participants of game-related Discord servers, a message inviting users to take part in the questionnaire was posted in the chat by the researcher with the permission of server's moderators. As for the local school, the participants were recruited with the help of the principal, who allowed the questionnaire to be distributed in the classes and the parents of the youngest children to be briefly interviewed. The participants' ages ranged from 6 to 17, with a gender distribution that was not gathered, but the sample was quite balanced. For the younger ones, the survey was administered with a parent, which helped and answered some questions. The questionnaire was anonymous, and no data or information regarding who compiled the survey was collected. The survey results were analyzed with SPSS, and the survey questions are available as Appendix.

Of the 330 participants, 313 completed the survey. Of the 313 answers, 253 play video games online, while 58 do not. SPSS was used to analyze the results of the 253 answers, and the findings revealed the following:

• 35.2% of the users mostly played Battle Royale games, followed by 28.5% for FPS, 22.1% for Others, and 14.2% MMOG/MMORPG. More details are presented in Figure 54.

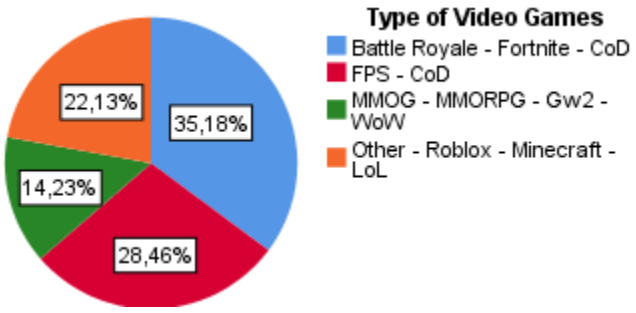

Figure 53: Most played video games, according to the survey. Elaborated by the author.

• 67.2% of users reported informing their parents about their in-game activities.

• 56.5% of users stated that their parents do not monitor their in-game activities, 34% are unaware if their parents are monitoring, and 9.5% confirm that there is a sort of monitoring.

• 72.7% of the users are not aware of what parental control is.

• 91.3% of the users declared that their parents are unaware of the parental control features.

• 88.1% of the users confirm that their parents do not activate parental control while they play video games.

• 72.3% believe that activating parental control and limiting the conversations with other users would create an unpleasant gaming experience.

• 84.2% of the users received threats or direct insults during gameplay, of which 70% reported they had received them from time to time. Figure 55 illustrates the type of threats reported in the survey.

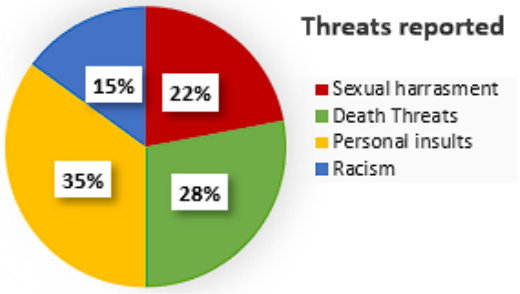

Figure 54: Threats reported in the survey. Elaborated by the author.

• Respectively 47.4 % of the users declared to have witnessed criminal behavior in chat, and 49% in vocal chat. Figure 56 illustrates the type of crimes reported in the survey.

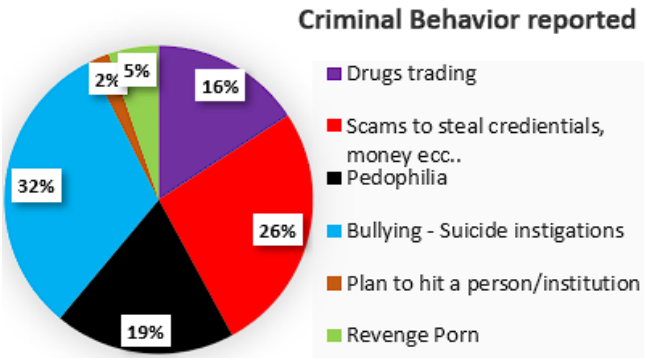

Figure 55: Criminal behavior reported in the survey. Elaborated by the author.

Further analyzing the data with SPSS, the analysis highlights the following critical aspects; Starting from the age of 8, increasing number of children declared to be harassed or threatened during gameplay, with the peak being reached between 12 and 17 years old. Figure 57 illustrates the contingency table with the children's answers.

		Duringyourplaytimehaveyoueverwitnessedanycriminalbehavi_A	
		No	Yes
Whatisyourage	6	4	0
	7	13	0
	8	12	5
	9	15	5
	10	13	7
	11	9	9
	12	11	14
	13	13	14
	14	16	18
	15	7	21
	16	14	9
	17	6	18
Total		133	120

Figure 56: Contingency table with relative answers. Elaborated by the author.

Most of the crimes in the chats were witnessed by children aged 12 to 17, as reported in Figure 58.

		Haveyoueverreceivedthreatsordirectinsultsduringgameplay	
		No	Yes
Whatisyourage	6	4	0
	7	5	8
	8	3	14
	9	4	16
	10	2	18
	11	4	14
	12	0	25
	13	5	22
	14	3	31
	15	3	25
	16	5	18
	17	2	22
Total		40	213

Figure 57: Contingency table with relative answers. Elaborated by the author.

And, as the age of the children increase, there is more knowledge of parental control in children, but it does not influence the knowledge of their parents or their activations. In a general overview, the results indicate that this environment is not always safe for children; there is a lack of monitoring of these platforms by gaming companies, and all this is accompanied by a lack of knowledge of the monitoring tools that are made available. As seen before, this brief study about the safety of

children confirms that gaming is really dangerous for children. The reviews of the current protection systems in this environment remark the efforts of gaming companies and agencies to provide a safe place for children, but they also proved inefficient. Additionally, the results obtained from the survey illustrates that most of the parental control features enforced by gaming companies are not used or not known by the users. Some of the safety measures offered in the gaming environment by parental control often prevent users from communicating with others, limiting users from experiencing a complete gaming experience. Gaming online requires users to communicate to achieve complex challenges (Like Raids, Competitive Matches, etc.), and parental controls developed by gaming companies limit this function, thus making the gaming experience unsatisfactory. Most respondents highlighted that their parents are unaware of this function, and the majority declared that activating it would prevent them from enjoying the video game.

3. CLASSIFICATIONS AND DATA ANALYSIS

The following chapter aims to analyze the data collected during the research and combine them to categorize virtual worlds based on cybercrime risk. First, however, it will present two important elements that helped in the categorization: the presence of alternative servers and the language used in these virtual worlds.

3.1 The alternative servers

A further obstacle that must be dealt with is having alternative servers that retain the same properties of the original virtual world but are hosted by private individuals or small parallel companies. Usually, by playing a VG like Grand Theft Auto (GTA) you can connect online and interact with other players. By doing so, users are subject to the rules and control of the game manufacturer. Over the past few years, many companies allow the user to create a private server parallel to a specific VG (for example, GTA), managing all its aspects: users can decide to invite other specific users or make it public, establishing their own rules. No one can enter the server without owner's permission. There are many servers like that worldwide, and they are rather populated. This introduces an additional level of difficulty in the case of any investigation. When users enter an original virtual world, large companies, for better or worse, manage to provide any data with some mandate in these servers; however, this becomes impossible because they are self-managed. As a result, they become a coveted space suitable to perpetrate possible illegal activities. Some examples are showed below:

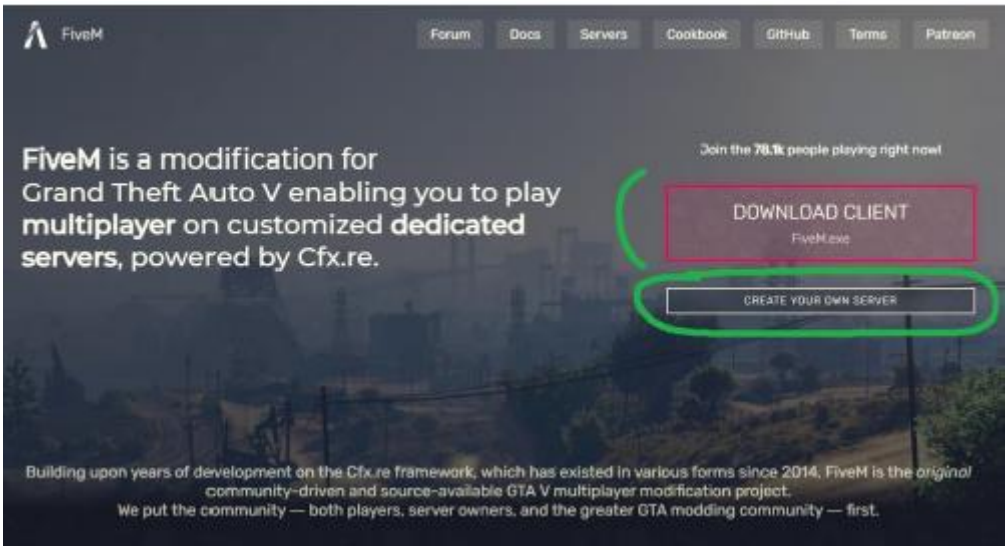

Figure 58: example of private servers (FiveM), offered by cfx.re. Recovered from https://fivem.net/.

Figure 59 shows the example of FiveM; By clicking "CREATE YOUR OWN SERVER," all the paid options will appear to allow users to create their own private server. If users have their own original version of GTA, once they open the game, they will be able to select their server and enter it. The owner and any other administrators will establish the rules, and users will be able to enter by invitation with the credentials received unless the server is made public. Figure 60 shows a list of private servers:

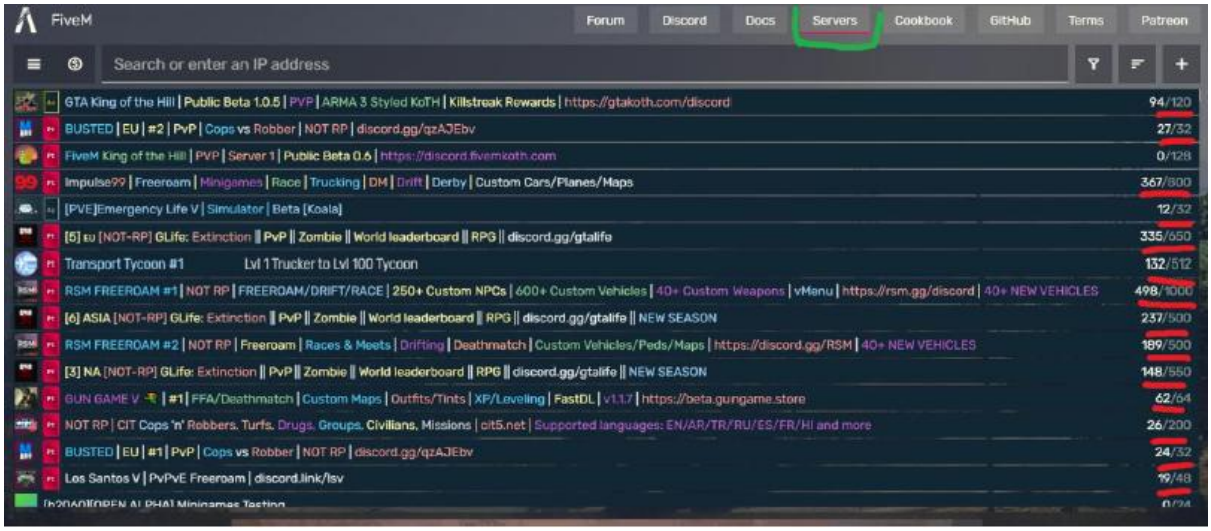

Figure 59: Server lists on FiveM. Recovered from https://fivem.net/.

The number of users connected to that specific server is highlighted in red. The amount of these servers is significant, and there is not a single company, but there are several, each with different types of hosting service. In Figure 61, it is possible to see Nitrado servers for another type of VG: Ark survival evolved. Also, in this case, the list is full of servers and users.

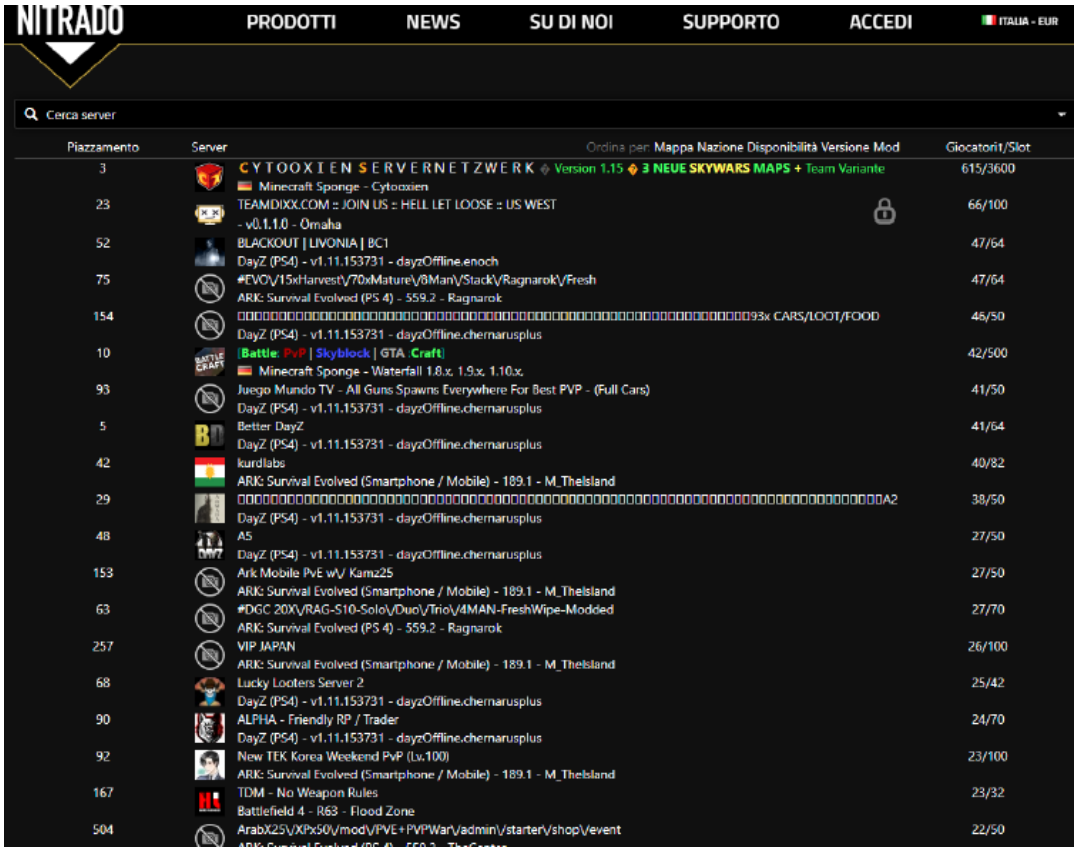

Figure 60: List of Nitrado Servers for Ark Survival Evolved. Recovered from https://server.nitrado.net/usa/toplist/index.

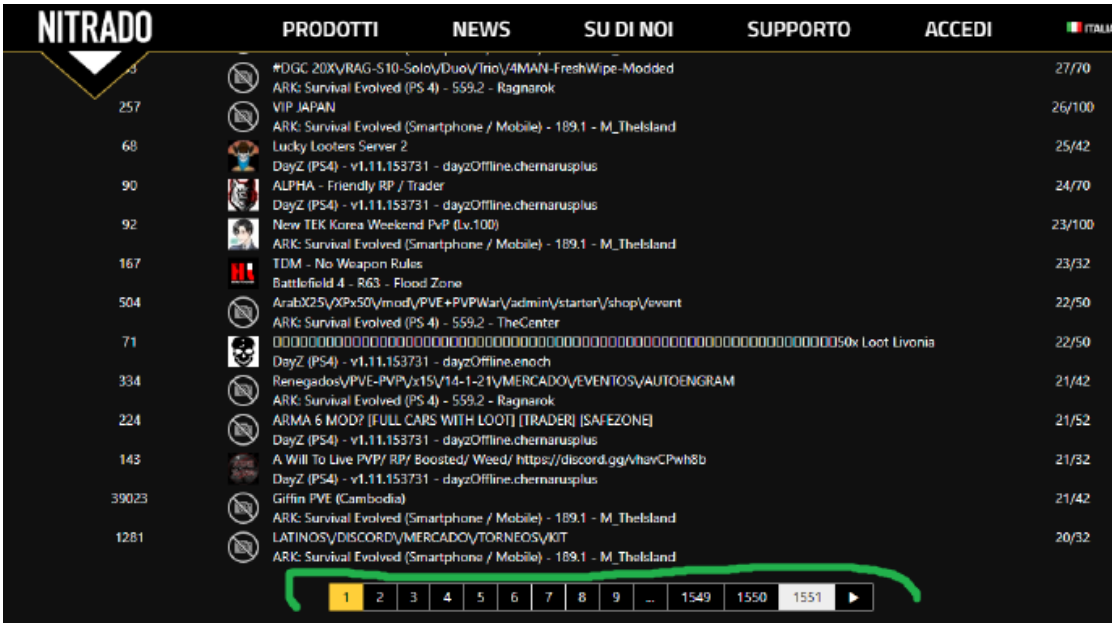

Figure 61: Servers list Nitrado. Recovered from https://server.nitrado.net/usa/toplist/index.

Figure 62 lists 1551 pages; in each page, 24 servers are displayed, so it is possible to count more than 37000 servers for a single game. In each server users can communicate without control. Consequently, the official MMOG managed by the manufacturing company is not the only source

of the problem[43]. Furthermore, communications take place both in written and oral form, which makes it almost impossible to intercept the content or trace it once the chat has ended. There are potentially infinite possibilities for undetected communication.

3.2 Communities and language

Virtual worlds are populated by users worldwide who interact among each other using a language typical of those who visit these platforms. Each virtual world is different and form communities organized into smaller parts, such as guilds and legions, through the functions specific to the virtual world. Consequently, three fundamental layers can be identified. The first includes the community that populates the entire virtual world according to the category (MMORPG), the second comprises the community created around the specific video game, and lastly, the third consists of the community created within it. For example, taking an MMORPG on the market, such as "Aion", the overall population is categorised of a first level consisting of users who typically populate that category of VG, who will therefore have characteristics and specifications typical of those who populate mmorpgs, then the one that is formed around the VG itself, and finally the one that is created inside the VG. Figure 63 shows the visual example.

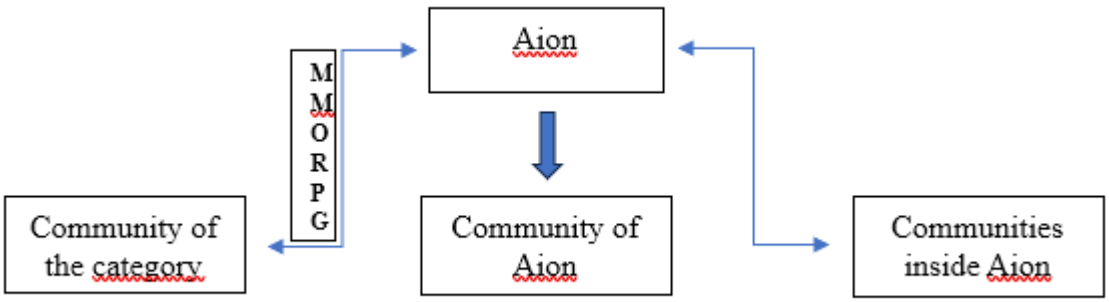

Figure 62: Layers of the communities created for each virtual world.

Obviously, if the virtual world of reference changes, the consisting layers also change. This system, therefore, generates further dynamics: the community layer of a category does not exclude interfacing with other virtual worlds; for example, an individual can be a regular user of

[43]Some companies offer the possibility of creating a server for an original game, just as a private individual can create his server and game with complete autonomy. ES. Ark Survival Evolved is a video game managed by Wildcard Studio. Therefore, it controls and manages the servers. As seen in the images above, however, another company may recreate the possibility of creating and managing servers in total autonomy for a specific video game, in this case, Ark Survival Evolved. So, we will have the original game and the copy. Like the original, this copy can produce thousands of servers, which have nothing to do with the original.

MMORPGs and also FPS; therefore, these layers are not mutually excluding, since they categorize communities for better knowledge. Consequently, a user can be part of multiple different communities. So why is it useful to categorize the type of community? In virtual worlds, each community has different characteristics in terms of language and knowledge. Going into more detail, a community linked to a category of MMORPG-type VG will certainly have a different attitude and language from those who frequent FPS. In the same way, a community that is born around a specific virtual world will have a different jargon from those who frequent another, and even more evident will be the difference between communities that are born within these virtual worlds, where the languages and attitudes are completely different in respect to the other categories. Furthermore, as explained in Figure 64, there is a behaviour and a language common to all users of virtual worlds, which constitutes a general macro level possessed by all users in these platforms.

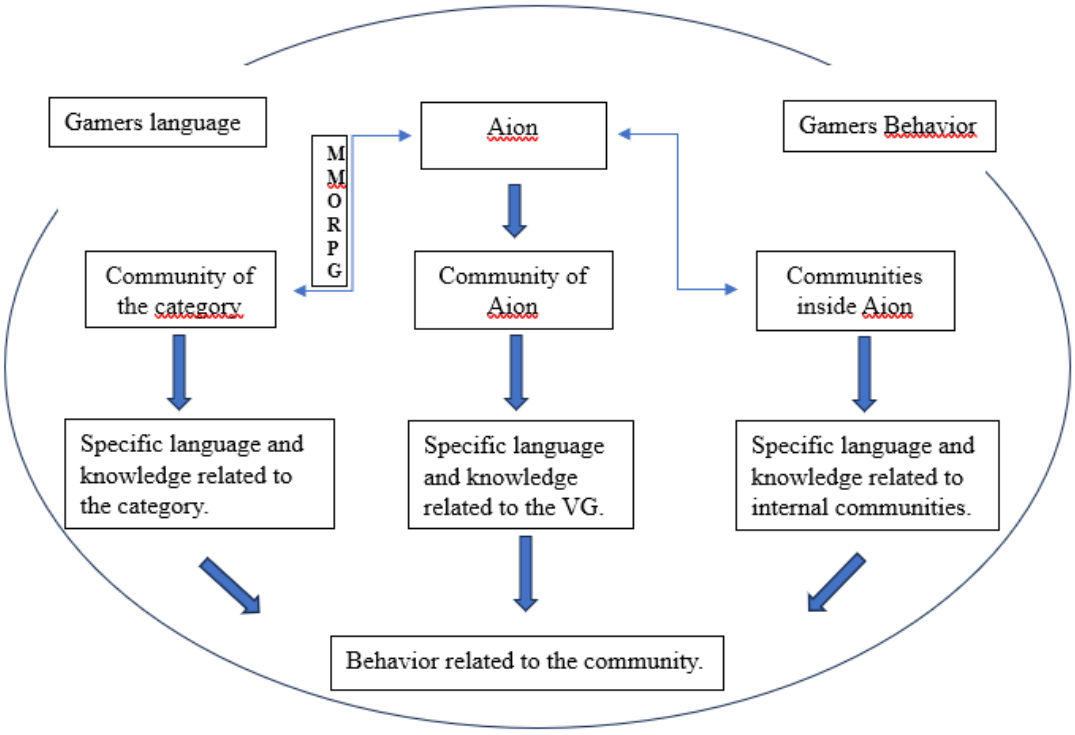

Figure 63: Complete categorization of communities.

Therefore, categorizing communities becomes a way to target the element of interest during the research and intelligence phase. This is a first step that could help targeting, although, like all things, it is not without exceptions. In fact, itis not always true when we go down to the micro level and, therefore, try to identify a single user. This is because, as highlighted previously, a user can be skilled in mastering a language and behaviors adaptable to any virtual world that would grant him

access to different communities, making him a difficult target. Since each community has a different language and behavior, an analysis is needed to understand their peculiarities. When a community that frequently plays MMORPGs is observed, for example, on Discord, they will have a common jargon, which reflects terms specific to the virtual world category and more specific when talking about VG. The same happens for a community that plays FPS and so on. This gives life to a series of typical words these communities use to communicate. Considering a fantasy-MMORPG virtual world, the communities will therefore use jargon relating to the category, which combines with that specific to the virtual world. Below is an example created with the words recovered during research and the jargon of gw2 recovered from the specific wiki.

Jargon MMORPG specific[44]*:*

- AoE = Area of effect (n.) is used to define an ability that allows you to perform an area attack. The area is delimited based on the type of spell used. Therefore, if a skill is defined as AoE, it will create damage in a certain area and can hit multiple enemies.
- Aggro = 1. (v.) refers to a hostile mob that has noticed a player and is actively trying to attack him; 2. (n.) refers to the amount of "hostility" the player has generated on the mob. In the typical combat strategy, the fighter tries to draw as much aggro away from weaker players like healers and mages as possible.
- Ava = abb. of “Avatar”.
- Alt = abb. of “alternate.” Typically, a fantasy MMOG player creates multiple characters and, usually, Alts are secondary characters that are used to complete missions or other things.
- BAM = abb. of “Big Ass Monster." Typically refers to very strong bosses within the MMOG or really strong players.
- Bind = (n.) In many MMOGs the Bind is the point at which a player has bound his character to that specific point on the map. Bind points often correspond to predetermined structures or locations in maps and are safe locations. At this point the user always has a teleportation tool available to return to that point where he binded.
- BoE = abb. of “Bind on Equip.” They are objects that are often linked to a specific character, the only one capable of using it. Once used that object will no longer be usable by others. Furthermore, the item can be traded/sold as long as no one has equipped it yet.

[44] For the full List, visit the Annex.

- BoP = abb. of “Bind on Pickup”. They are objects that bind to the character as soon as they are collected/looted from the terrain/mob that has been defeated. The item can no longer be traded or sold after a character has picked it up.
- Brt= abb. of “Be right there.” It simply means “I'll be right there”.
- Btw = abb. of “By the way”. Self-explanatory.
- Buff = (n.) spell that increases attributes of some kind.
- …. Continue in the Annex

To these general terms, which refer to a jargon used generally for all MMOGs, the language of the specific MMOG, which in this case is GW2, shall be added.

GW2 Jargon[45]*:*

- AA: Auto Attack Pressing 1 over and over to auto-attack or letting the auto-attack chain run through without button press.
- AB: Auric Basin A zone in Heart of Maguuma, part of the Heart of Thorns expansion.
- AC Ascalonian Catacombs: A dungeon in Plains of Ashford.
- ACArrow cart: A siege weapon used in World versus World.
- AFK: Away from keyboard The player is not actively playing, but remains logged in.
- Akili Event: Defend Akili while he recalibrates mirrors around the Astralarium.
- Alac Alacrity Renegade: A support build for the Revenant using the Renegade specialization which provides Alacrity for the group.
- AotJ: Ashes of the Just The epilogue skill of the Tome of Justice from the Firebrand specialization.
- AP Achievement points: Points awarded for completing achievements.
- AP Aetherpath: A specific path of the dungeon Twilight Arbor.
- AP Assassin's Presence: A Revenant Master trait in the Devastation line.
- AR Agony Resistance: Resistance to the Agony found in Fractals.
- Arah: The Ruined City of Arah A dungeon located in Cursed Shore. Also refers to the event chain allowing access.
- AT Automated Tournament: The daily and monthly automated Structured PvP tournaments.

[45] For the full list, visit: https://wiki.guildwars2.com/wiki/Abbreviations#W or the Annex

- AG / Axe / Axemaster Kill AxemasterGwyllion: It refers to the event in Verdant Brink during Night and the Enemy.
- BK Black Kiter:Literally means black kiter, this is the same as Oil Kiter in the Deimos raid encounter.
- BC Black Citadel: The charr capital city in Ascalon.

It is clear that for every virtual world, there is an excessively large glossary of words, which allows users to speak in code and, above all, in closed environments, where only those who are part of certain communities can understand the meaning. Therefore, if the virtual world changes with a military-type fps, the communities will use jargon that includes military terms, including knowledge relating to weapons, ammunition, and so on. However, why is all this important and useful to categorize? In 2008, a Pentagon researcher at the Director of National Intelligence Open-Source Conference in Washington presented the possible threats that can arise in these virtual spaces, as illustrated in Figure 65 through 72:

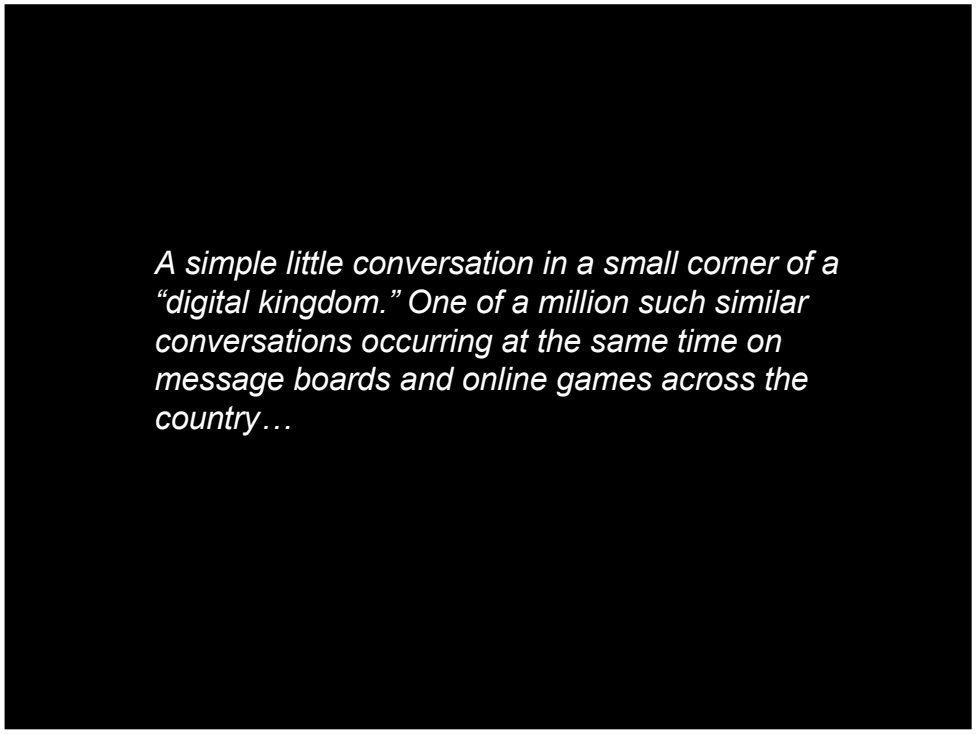

Figure 64: Dr.Toavs Presentation recovered from DNI Open Source Conference 2008 Panel: Making Use of Emerging Media Sources Emerging Media: Its Effect on Organizations Dr. Dwight Toavs Information Resources. - ppt download (slideplayer.com)

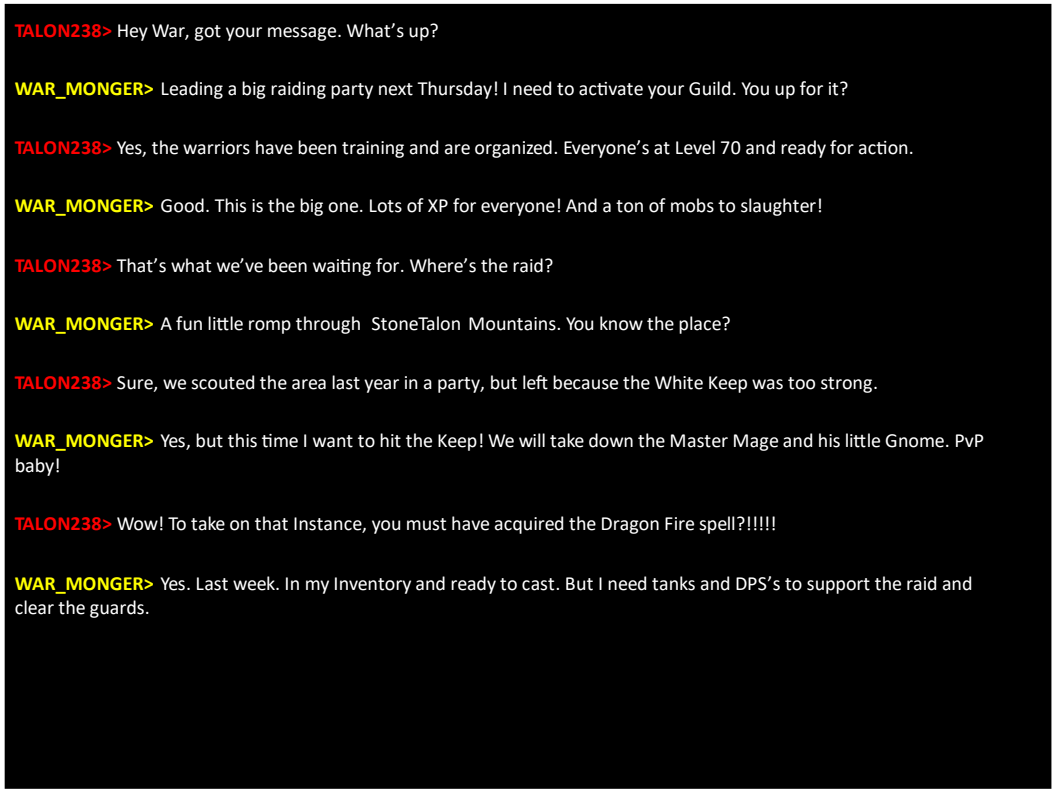

Figure 65: Dr.Toavs Presentation recovered from [DNI Open Source Conference 2008 Panel: Making Use of Emerging Media Sources Emerging Media: Its Effect on Organizations Dr. Dwight Toavs Information Resources. - ppt download (slideplayer.com)]

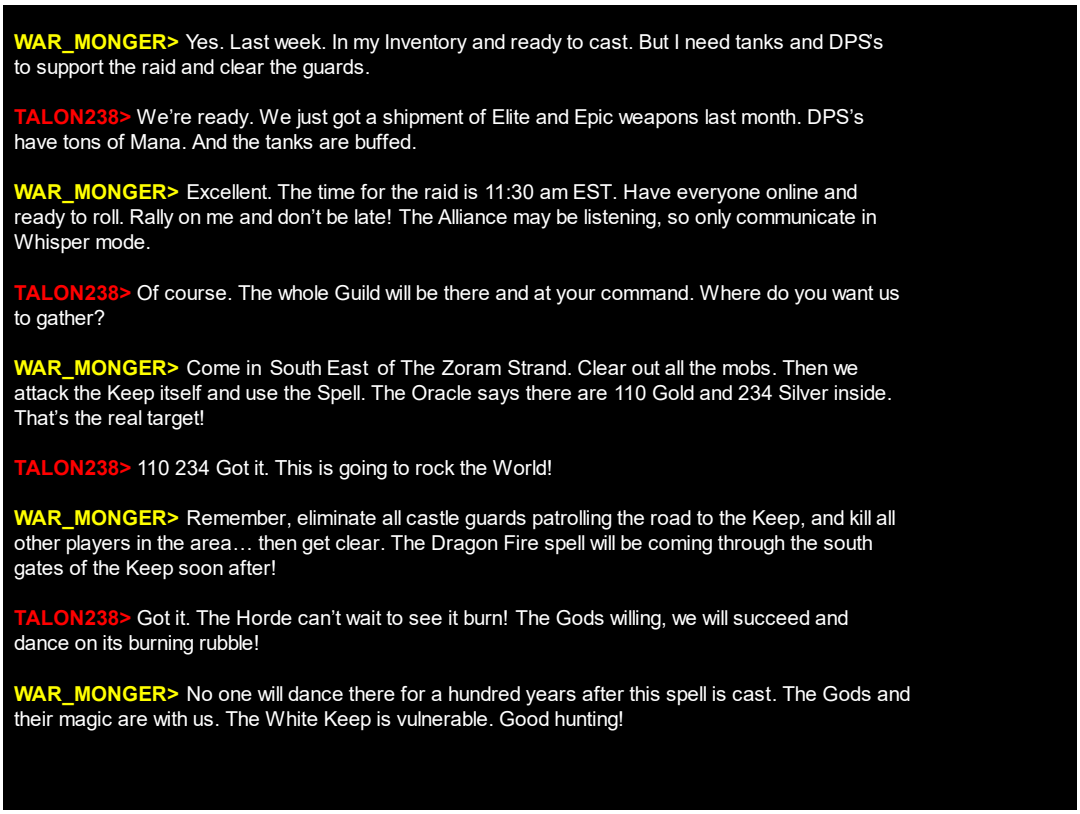

Figure 66: Dr.Toavs Presentation recovered from [DNI Open Source Conference 2008 Panel: Making Use of Emerging Media Sources Emerging Media: Its Effect on Organizations Dr. Dwight Toavs Information Resources. - ppt download (slideplayer.com)]

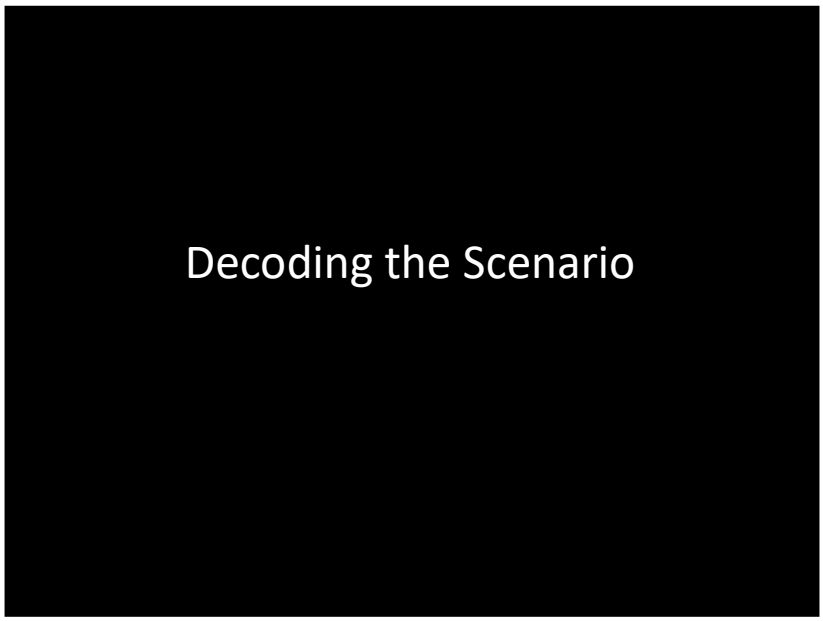

Figure 67: Dr.Toavs Presentation recovered from [DNI Open Source Conference 2008 Panel: Making Use of Emerging Media Sources Emerging Media: Its Effect on Organizations Dr. Dwight Toavs Information Resources. - ppt download (slideplayer.com)]

Figure 68: Dr.Toavs Presentation recovered from [DNI Open Source Conference 2008 Panel: Making Use of Emerging Media Sources Emerging Media: Its Effect on Organizations Dr. Dwight Toavs Information Resources. - ppt download (slideplayer.com)]

Figure 69: Dr.Toavs Presentation recovered from [DNI Open Source Conference 2008 Panel: Making Use of Emerging Media Sources Emerging Media: Its Effect on Organizations Dr. Dwight Toavs Information Resources. - ppt download (slideplayer.com)]

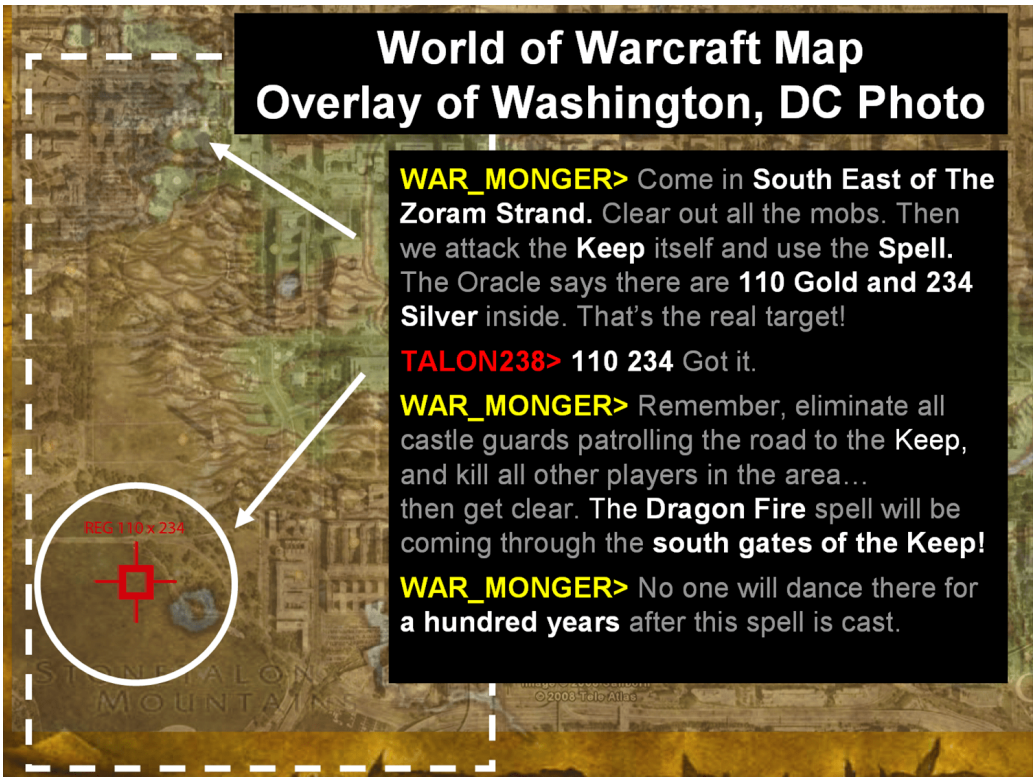

Figure 70: Dr.Toavs Presentation recovered from [DNI Open Source Conference 2008 Panel: Making Use of Emerging Media Sources Emerging Media: Its Effect on Organizations Dr. Dwight Toavs Information Resources. - ppt download (slideplayer.com)]

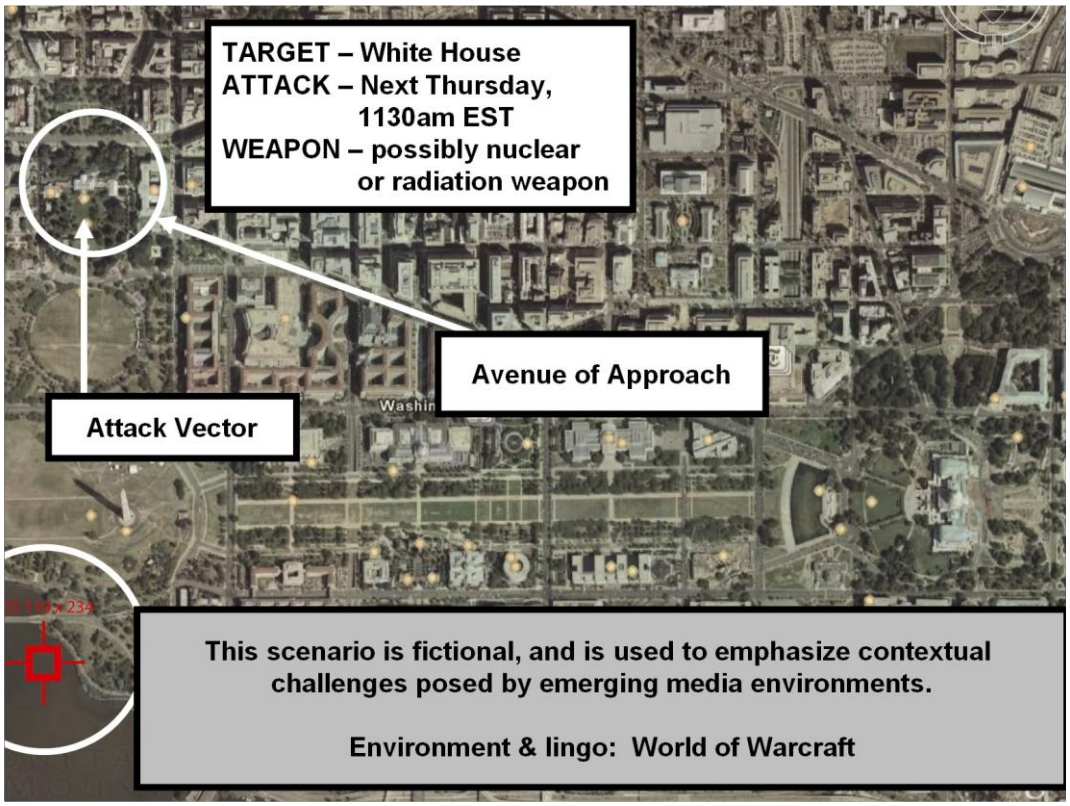

Figure 71: Dr.Toavs Presentation recovered from [DNI Open Source Conference 2008 Panel: Making Use of Emerging Media Sources Emerging Media: Its Effect on Organizations Dr. Dwight Toavs Information Resources. - ppt download (slideplayer.com)]

This scenario is fictional, but it is useful to understand how dangerous the use of coded language can be for national security. Therefore, the classification of communities and languages serves to understand the peculiarities of the users who inhabit these virtual worlds and becomes an important piece for understanding how to Handle the phenomenon. Naturally, this lexicon is often used in conjunction with normal language and becomes clear that given the number of different jargon and virtual worlds that exist, keeping track of the entire lexicon becomes impossible. Another important factor concerning communities, particularly users, is age. If it is true that there are no age limits and anyone can access these virtual worlds, understanding what type of users frequents a particular virtual world can provide further elements of interest. For example, there are some virtual worlds where the average age is very low, while others have a higher average. For example, Minecraft, Fortnite, and Roblox are populated by younger users. In contrast, Call of Duty, Diablo 4, and GW2 see a population of users with a higher average age. Why is this important? Depending on the type of user, there will be different languages used, availability of money, and knowledge. This, therefore, could be a predictor of the type of crime that maybe committed in a certain virtual world rather than another. Consequently, understanding who populates a particular virtual world and outlining their specifics helps in the identification process and serves as an essential element for

what will be showed in the following chapter, namely the categorization and analysis of virtual worlds.

3.3 Virtual Worlds categorization

As shown previously, not all virtual worlds are the same, since they have different characteristics and peculiarities, each with its specifications. This introduces further research questions that the following analysis and categorization aim to answer. Which virtual world is more dangerous than another? Which virtual world is best suited for the possible perpetration of a certain crime? And why? To answer these questions, it is necessary to combine and categorize the previous elements to offer a complete overview. As shown in Chapter 1.6 in Figure 19, users within virtual worlds have a wide range of possibilities to communicate, and each of these can occur at the same time under different profiles. For example, the same user can simultaneously speak vocally on Discord and chat in a virtual world being two distinct avatars. Therefore, it is essential to determine which kind of virtual world is best exploitable to commit a certain type of crime rather than another. To do that, the methodology used to categorize/classify the material have been done with the following steps:

- The first step is to categorize the virtual environment following the approach highlighted in Chapter 1.2.8
- The second step is to analyze the communication possibilities of the virtual world that have been identified following the example of Figure 19 of Chapter 1.6

These two steps are the first part of the categorization analysis, which can be identified as a *general* step.

Once the virtual world and its related communications that can be exploited have been identified, specific aspects of this virtual world must be evaluated further. Therefore, to arrive at an optimal categorization, the following steps were followed.

- The third step is to evaluate the age of the players who populate the aforementioned virtual world (it can be done directly, as in this case, by asking the age during regular gaming sessions, or they can be identifiable through some specialized sites[46])
- The fourth step is where the community and the typical language of users who live inside the virtual world are analyzed, as illustrated in Figure 64.

[46] An example of a site that collects statistical data on some video games, including age. https://explodingtopics.com/blog/fortnite-stats

- The fifth step is to analyze the spaces and functions inside the identified virtual world. This includes, for example, the number of maps, locations, rooms, and other specific elements of that virtual world.
- *Additional step: Merge the information found with netnography on applications related to virtual worlds to strengthen the results*[47].

These steps can be defined as *specific*, as they analyze aspects of the identified virtual environment. Consequently, following the steps listed previously, a practical example of what has been done to categorize virtual worlds based on crime can be summarized as follows:

Example: What crime can be committed on and how dangerous is Fortnite?

First Step: Categorize the virtual environment following the approach highlighted in chapter 1.2.8.

Fortnite is a battle royale video game online.

Second Step: analyze the communication possibilities of the virtual world that have been identified following the example of Figure 19 of Chapter 1.6

Fortnite can be played from: Consoles, PC, and phones. Can be used together with Discord and Teamspeak. Can use the messaging function of digital platforms (Epic Games). Can use vocal and written chat inside the game.

Third Step: Evaluate the age of the players who populate the aforementioned virtual world.

Fortnite is populated by users with a very low average age.

Fourth Step: Analyze community and language of that specific virtual world.

The Fortnite community is reflected in other battle royale games, as is the language, which is characterized by typical and specific jargon and is a classic one used by teenagers. It is considered simple, not complex, but rather elementary.

[47] This is optional but used here to reinforce the results obtained from this methodology. For example, suppose a high risk for a particular crime is obtained with this methodology for a specific virtual world. In that case, it is also possible to compare the results obtained by investigating the Discord servers related to that virtual world to confirm it.

Fifth Step: Analyze the spaces and functions inside the identified virtual world.

Fortnite, a battle royale game, is designed with a user-friendly approach. Its spatial complexity is minimal, featuring a main map with various modes. Additionally, it offers the option to create private maps. The game includes a shop and a unique 'gift to friends' function. It operates on its own alternative currency, VBUCKS, but does not incorporate an in-game economy, further simplifying its structure.

Additional Step: Compare the results with related applications.

These collected data were then summarized and evaluated using Table 6 which assigns the risk.

STEP	SCORE	CRIME SCORES
1	**Characteristics** Offline: 0 Singleplayer: 0 Online: 1 Multiplayer: 1 **Categories** Videogames: 0 Videogames online: 1 MMORPG:1 MMOG:1 **Typologies** All typologies: 1 **Dimensions** Environment: 1 Economic: 1 Social: 1	**Minimum score for a remote chance of a crime occurring:** **5** **Grade C** **Minimum score for a medium chance of a crime occurring:** **9** **Grade B** **Minimum score for a high chance of a crime occurring:** **12** **Grade A** **Minimum score for the maximum chance of a crime occurring:** **15+** **Grade S** **For the pedophilia category only, the score must reach:** **9 for grade B,** **11 for grade A,** **and 13 grade for S.**
2	**Communications possibilities:** Irrelevant: 0 1-2: 1 3-4: 2 5+: 3	
3	**Age of users (average):** Irrelevant: 0 1-18: 3 18-30: 2 30+: 1	
4	**Community and language complexity:** Irrelevant: 0 Simple: 1 Average: 2 Complex: 3	
5	**Spaces and functions complexity:** Irrelevant: 0 Simple: 1 Average: 2 Complex: 3	

Table 6: Summary table for assigning scores. Elaborated by the author.

The following table 7 groups together some of the most famous virtual world investigated, categorized according to the peculiarities seen previously, to determine their risk.

Table Legend:

• Grade S: Maximum probability that the phenomenon occurs.

• Grade A: High probability that the phenomenon will occur.

• Grade B: Medium possibility that the phenomenon occurs.

• Grade C: Remote possibility of the phenomenon occurring.

MMOG/ MMORPG/FPS, Virtual worlds	Pedophilia	Money Laundering	Internet challenges, suicide instigations	Weapons and drugs trading	Terrorism: Acts	Terrorism: recruitment and propaganda
Guild wars 2	C	S	S	S	S	S
League of Legends	B	C	B	C	C	C
Fortnite	S	A	A	C	C	A
DiabloIII-IV	C	B	C	C	C	C
Teamfight Tactics	C	C	C	C	C	C
Counter strike G.O.	C	B	C	A	B	A
Rust	C	C	C	C	B	C
Ark	C	B	C	C	B	C
Genshin Impact	C	C	C	C	C	C
Minecraft	S	B	A	C	A	A
Roblox	S	B	A	C	A	A
Blade and Soul	C	S	C	C	A	A
PUBG	C	C	C	B	B	B
Apex legends	C	B	C	B	B	B
Call of Duty	C	A	C	S	S	S
Valorant	C	B	C	C	C	C
Word of warcraft	C	S	S	S	S	S
Escape from Tarkov	C	C	C	A	A	A
Overwatch	C	C	B	B	B	B
Black Desert	C	S	C	A	S	S
Rainbow Six Siege	C	B	C	B	B	B
Path of Exile	C	B	C	B	A	B
Dayz	C	B	C	A	A	A
Runescape	C	S	B	A	A	B
Sea of Thieves	C	C	C	B	B	C
Heroes of the storm	C	C	C	C	C	C
Arma III	C	C	C	S	S	S
GTA V	B	A	A	A	S	S
Metin2	C	A	C	C	B	B
Aion	C	A	C	C	B	B

Table 7: Probability that a particular crime related to the virtual world will occur. Elaborated by the author

This table is not exhaustive because thousands of virtual worlds should be analyzed and categorized, but what is of interest for this research is the method that determines which virtual world could be the vector of a specific crime rather than another.

For example, Guild Wars 2 obtained the following results:

Guild Wars 2	C	S	B	A	S	S

- The chance that an event of pedophilia will occur is remote. This is because GW2 users have a high average age, making it hard to find children.
- Money laundering is an event that can easily occur as the structure of MMORPG/MMOG allows users to exploit the alternative economy and digital currency.
- Internet challenges and suicide instigations are phenomena that can occur in every virtual world, but here, the chance is not so high, but it can occur within the lower average age users.
- Weapons and drug trading can occur as that virtual world allows the exploitation of many chats and places, including some very safe ones.
- Terrorism acts, recruitment, and propaganda can easily be perpetrated as the infinite places and the number of users offer an ideal place to dive deep into some communities and spread ideology.

Now, comparing the example with another virtual world, such as Fortnite, it is possible to notice some differences:

Fortnite obtained the following results:

Fortnite	S	A	A	C	C	A

- The chance that an event of pedophilia will occur is an event that can occur daily. This is because Fortnite users have a really low average age, making it a perfect ground for predators.
- Money laundering is an event that can easily occur, not thanks to the structure of the VG, but thanks to high populations that trade their virtual currency for real money.
- Internet challenges and suicide instigations are phenomena that can occur in every virtual world, but here, the chance is pretty high as most of the users are very young.
- Weapons and drug trading is an event that can barely occur since the age of the users is very low, and they are not predisposed to have money for drugs, much less for weapons.

- Terrorism acts are rare because the VG structure does not allow much space to reproduce real scenarios, and the conditions it offers are not real but somewhat fictional. On the other hand, recruitment and propaganda can easily be perpetrated as the infinite places and the number of users offer an ideal place to dive deep into some communities and spread ideology.

This classification highlights how not only do the virtual world create the necessary conditions for the perpetration of a crime, but also the users who populate or use that virtual world. Also, comparing the data recovered from Discord, illustrated in Table 8, the categorization appears somewhat similar to what has been found on that platform. Where there are communities with low average age, there is much more presence of predators and crimes such as incitement to suicide, challenges, etc., while a higher age corresponds to more complex crimes.

	Gaming Discord server with average age of <25	**Gaming Discord server with average age of >25**
Presence of pedophiles	80%	20%
Internet challenges and suicide instigation	80%	20%
School shooting, challenges - planning homicides	70%	30%
Buying/selling weapons and drugs	30%	70%
Right-wing extremism, terrorism recruiting, acts, and propaganda	40%	60%

Table 8: Average age of the users affected by the crimes. Elaborated by the author.

Therefore, as a general rule, is it possible to identify what type of crime can be perpetrated in a given virtual world? Indeed, it is more appropriate to identify virtual worlds which are riskier than others and which can lead to a certain type of crime, even if a specific pattern cannot be rigorously defined. This is because, although it is possible to categorize and analyze what has been found during the research, there are too many possibilities for exploiting these platforms, and no one is prohibited from using virtual worlds considered to be of little risk to perpetrate more complex crimes. Generally speaking, even if it would be less possible, some communications and events may be implemented through virtual worlds that are less known and/or considered safer from a purely scientific point of view. It follows that the categorization illustrated in table 9, and table 10 regarding the material found on Discord, which in some way confirms the categorization, maybe used if taken into account that it cannot always be considered completely true or reliable.

Table Legend:

- Effective
- Somewhat effective
- Not effective

Typologies and categories	Pedophilia	Money Laundering	Internet challenges, suicide instigations	Weapons and drugs trading	Terrorism: Acts	Terrorism: recruitment and propaganda
FPS	Not effective	Not effective	Not effective	Effective	Effective	Effective
RTS	Not effective	Not effective	Not effective	Somewhat effective	Somewhat effective	Not effective
MOBA	Effective	Effective	Effective	Not effective	Not effective	Somewhat effective
RPG	Somewhat effective	Somewhat effective	Somewhat effective	Not effective	Somewhat effective	Not effective
Battle Royale	Effective	Somewhat effective	Effective	Somewhat effective	Somewhat effective	Effective
MMOG/MMORPG	Somewhat effective	Effective	Somewhat effective	Effective	Effective	Effective
Metaverse	Somewhat effective	Effective	Somewhat effective	Effective	Effective	Effective

Table 9: Categorization of typologies and categories of virtual worlds in relations to the crime. Elaborated by the author.

	Type of Game connected to Discord	Typology of the server
Presence of pedophiles	Battle Royale, MMO, Sandbox, Console related	Public and Private
Internet challenges and suicide instigation	Battle Royale, MMO, Sandbox, Console related	Public and Private
School shooting –challenges- planning homicides	FPS, MMO, Battle Royale	Public and Private
Buying/selling weapons and drugs	FPS	Private
Right-wing extremism, terrorism recruiting, acts, and propaganda	FPS, MMORPG	Public

Table 10: Video game type connected to the Discord server, and typology of the server. Elaborated by the author.

In conclusion, each virtual world has characteristics that make it unique and subject to exploits. However, thanks to the years spent within these virtual worlds and the material recovered, it was possible to categorize and analyze the most recurring behaviors, including the methodology and techniques used by users to perpetrate cybercrimes. However, as the images and tables demonstrate, this does not solve the problem; on the one hand, it shows that it is possible to perpetrate crimes on these platforms in complete freedom, but on the other, it highlights how complex it is to establish with certainty where a crime could occur. Given the vastness of these virtual worlds, the answer could be found anywhere, even in what is often underestimated and not considered. Indeed, no terrorist would carry out propaganda in a virtual world where there are no users and certainly would not use a chat where everyone reads to carry out an attack. Therefore, to address the problem, it is necessary to think differently.

4. TOWARDS A SOLUTION

The relevant possibility of exploitation that these platforms offer, the unquantifiable number of communications occurring through them, and the lack of monitoring require developing new and innovative solutions to prevent unwanted phenomena. This chapter will consider possible solutions that could be developed and implemented to tackle the criminal use of these platforms. Such proposals may help in the general effort with which national security and intelligence agencies fight cybercrimes in virtual worlds.

The first solution is the possibility of issuing “privileged accounts” to law enforcement and security services, which would have specific access and powers over these applications, to be used for investigative purposes only. These accounts would take over the functions of the Game Master,

who, supported by the necessary IT tools, would guarantee adequate monitoring to the law enforcement agencies. This means that the staff who use an account of this type must be able to navigate these virtual worlds, knowing their peculiarities.

Another solution is that of a “content blocking” system that uses algorithms to prevent content judged to be “unsuitable and dangerous” (e.g., censorship, Time Out). In some virtual worlds, it is possible to activate this feature as an optional option, but it cannot prevent complex linguistic forms. For example, it can censor the word “Fuck" but not “F4ck” and so on. A blocking system of this type could be efficient thanks to artificial intelligence; training the AI tool with specific datasets would allow it to resort to more important censorship. However, this would leave the vocal part of these virtual worlds uncovered, as it would not be able to block their content. Shifting attention to the legal side, today, there is no regulation over these virtual worlds, and it seems difficult to create one, given that companies around the world govern each virtual world without any particular limitation. In the current framework, several institutions attempt to regulate virtual worlds, such as the EU[48], which has proposed an initiative that can regulate virtual worlds such as the metaverse, focusing on opportunities and future implementations with a European Commission's Inquiry on Virtual Worlds and AI On 9 January 2024[49] and an EU Parliament's Regulatory Approach to Virtual Worlds The European Parliament's statement of 17 January 2024[50]. Attempts are also being made to regulate the world of online gaming, with systems that protect children from online content and some safety recommendations to video game companies[51]. It is important to note that the current attempts to regulate virtual worlds and online gaming, while commendable, have their limitations. They primarily focus on their use for companies and development opportunities, without adequately addressing potential issues of cybercrime and malicious use. Therefore, this could translate into an opportunity for a new national regulation that norms their use. From this perspective, an implementation that tries to overcome anonymity would be effective. In detail, the use of these virtual worlds should only take place through verified documents. (E.g., ID card) and/or digital fingerprints that would allow law enforcement agencies to track down who is hiding behind an avatar and consequently insert limitations on the accounts of those who have not verified their identity, preventing them from using chats and voice functions. Moreover, a standardization of age-based user profiles can be introduced. For example, children aged 10-15 shall only be able to perform certain actions within these applications, but not others. Therefore, they will not be

[48]https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13757-Virtual-worlds-metaverses-a-vision-for-openness-safety-and-respect_en
[49]https://www.taylorwessing.com/en/insights-and-events/insights/2023/10/navigating-the-legal-labyrinth-of-virtual-worlds
[50]https://www.taylorwessing.com/en/insights-and-events/insights/2023/12/deciphering-the-future
[51]https://tremau.com/regulating-online-gaming-challenges-and-future-landscape/

exposed to propaganda content, challenges, etc. While these tools appear valid, it is also clear that they would require immense work, both at national and international level, perhaps causing more problems than benefits. Furthermore, given that there are millions of uncontrolled conversations every second from every part of the globe, it is unlikely to think that finding a solution in the current legislative framework is possible. It follows that a solution should necessarily go beyond the established patterns, addressing a problem that today threatens the national security of every country. Therefore, the solution elaborated below does not consider privacy regulations, GDPR, and all those regulations that effectively tries to protect users online. This is because the main objective of the thesis is to demonstrate that in virtual worlds, it is possible to commit various crimes and, as a secondary objective, provide an innovative tool to address the problem, which must necessarily be developed alongside of current legislation, pending the regulation regarding its possible use, which is solely up to political decision-makers. Given the infinite possibilities virtual worlds can offer, developing an intelligence tool that can oversee all the conversations made through those applications is necessary. It is almost impossible to intervene directly in every virtual world, or even at a linguistic level, given the complexity of the coded language. It is also true that each user needs an internet connection to access virtual worlds, a keyboard/joystick to chat, and a microphone to speak. Therefore, the innovation that would allow law enforcement to tackle the problem more effectively would be to intervene directly on users' peripherals. Such a tool would work similarly to anti-cheat software used in most virtual worlds. The software would activate automatically on the device when the application or virtual world is opened. While anti-cheat software monitors "not permitted" programs (e.g., macros, cheats, hacks) on the client side, such software would intervene similarly. Once any virtual world or related application has been launched, the background software would start automatically, affecting the devices used by the users. Therefore, it would monitor both written chats and voice messages within the applications, recording the user's actions through the peripherals. However, it is clear that this process would give rise to further problems, such as how and by whom it would be installed, whether it would be mandatory, and whether legislation would be needed. Consequently, two options can be pursued: the first is to create ad hoc legislation that allows different monitoring of these virtual worlds and implies installing software of this type. However, the problem here is how to address this issue globally. Assuming that some action is taken in Europe, it is not certain that the same will be done in other parts of the world, and this would, therefore, only partially solve the problem, covering only those states adhering to the law. Alternatively, for national security, it is possible to adopt specific measures for each country by implementing a protocol through ISP providers that directly apply software of this type. However, here we fall into what is today defined as "spyware," and therefore, further problems regarding

privacy, GDPR, etc., would arise again. Therefore, the issue of implementing any monitoring software remains difficult, even if today the producers themselves are slowly trying to stem the problem with single individual actions, but without great success.

The following example shows how the software would work:

Suppose a user X opens "World of Warcraft" on his PC. In that case, the software starts automatically in the background, recording the user's actions by connecting to the peripherals (keyboard, joystick, and headphones). The operation would resemble that of a keylogger, which hackers use today to commit cyber-attacks by stealing credentials.

The millions of chats collected in real time are automatically saved in an external cloud[52], forming a database of conversations. At this point, a generative linguistic artificial intelligence add-on will analyze (always in real-time) the conversations, categorizing them according to an algorithm and assigning them a score equivalent to the danger they pose. The following step is the manual verification by an analyst who will confirm or not the result provided by the tool, thus possessing all the information necessary to trace it back to the user. In all virtual worlds, the user who chats and/or speaks has a username and a unique ID, which remains in the company databases. Once a dangerous chat has been found, the user is traced back to where he connects from, and if necessary, if he uses the masking tool, his chronological data, such as payments and/or logins or logoffs kept by the company can quickly be recovered. Figure 73 illustrates how the tool works. Since, in general terms, the crimes committed are perpetrated (as illustrated by the material found) in a fairly common language, the AI software will be trained with NLP techniques, which will also include a glossary typical of these virtual worlds. Furthermore, given that many virtual worlds are also accessible from the mobile phone, this tool can be modulated for other applications that use that device as a platform (e.g., Whatsapp, Telegram). Consequently, even if the software was born with the idea of monitoring chats in virtual worlds, it is still possible to make it usable for messaging apps since the tool's function is to monitor chats that take place via devices. As a result, phones remain a viable target for the application since it is necessary to use a keyboard to send messages. Consequently, even if the software was born with the idea of monitoring chats in virtual worlds, it is still possible to make it usable for messaging apps since the tool's function is to monitor chats via devices. As a result, phones remain a viable target for the application since it is necessary to use a keyboard to send messages. For example, if a person opens any virtual world on the phone, the software will automatically detect it and start monitoring the chats. Likewise, this function can be

[52] For greater security, the cloud should be managed by national government agencies or under license from the software manufacturer.

used without opening a virtual world, as the vital operation of the software is to monitor the device's chats. Therefore, this alternative would be possible with a simple modulation of the software, with obviously all the limitations foreseen in its use.

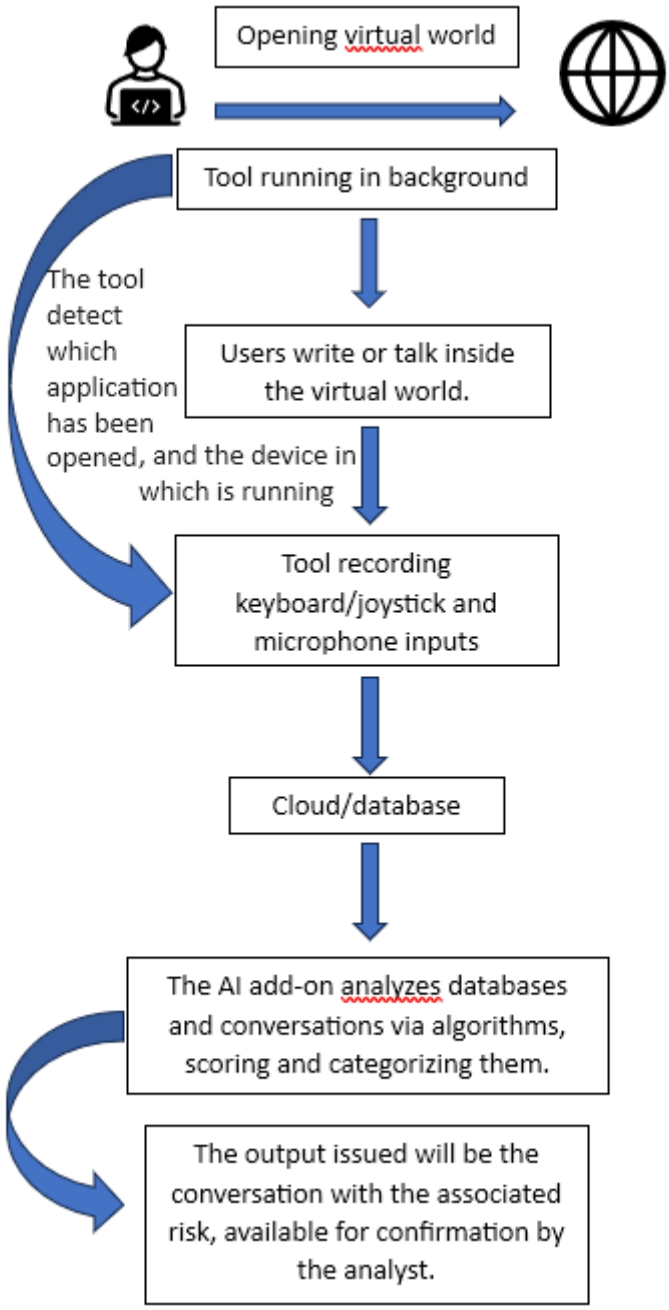

Figure 72: Tool processes. Elaborated by the author.

It is clear that the application of such a tool will lead to the deprivation of users' privacy in these virtual worlds, but since that would be a tool intended for government and police agencies, particular functions could be disabled, such as preventing the view of all the conversations in the

database, but only those reported by the AI. In this way, all users could chat and speak peacefully, and only when the AI reports a suspicious conversation can it be viewed. Therefore, the proposal of this research suggests that, instead of relying on rules that should be international and could, in any case, be circumvented, the approach would be based on monitoring the media used to interact in VWs: essentially, the internet connection and peripherals. This could happen with dedicated SWs that can record the communication flow through these peripherals and an AI machine capable of analyzing and categorizing the data. These SWs would act as an intelligence tool. Therefore, their use should be regulated by sector laws. They could be injected by state authorities autonomously, being invisible to companies and users. These state authorities should equip themselves with technical skills to develop and manage these tools and adequate know-how concerning the virtual world to be monitored. Such monitoring activity should be connected to any consequent pre-emptive (police forces) activities involving both national and foreign intervention (therefore, international legislation should be updated). The proposed solution requires a significant investment of resources and a legal framework that allows intelligence and police forces to use it. This is not easy, considering that the manufacturing companies are scattered worldwide and have no intention of limiting access to these platforms. It is the same problem faced today with Telegram and other private applications, which do not grant data or make intercepting messages possible. However, considering that virtual worlds, thanks also to the Metaverse, will eventually be a daily reality involving everyone, the sooner the change arrives, the better safety in using these virtual worlds will be guaranteed.

5. CONCLUSION

In recent years, some companies have attempted to implement remedies against possible illegal activities with limited success. The most recent example that left the entire American intelligence administration astonished, namely the great leak of top-secret NATO files, disclosed via the Discord application by a US soldier (Shane Harris et al., 2023). Based on this case, a documentary entitled The Discord Leaks was also made[53]. In the series, many experts asked themselves several questions: Why wasn't it blocked before? How could it happen that top-secret file travel on a gaming application? Fortunately, someone snitched and reported everything in this case, but how many other things are running on these platforms, and we do not know the content?

These questions were some of those that this research had asked itself, and they join the others that the research attempted to answer, demonstrating that it is possible to use virtual worlds to commit illegal activities, offering an alternative and efficient communication tool, even in times of war and/or bans.

Despite being extremely current, the research topic has little academic study and exploration, as demonstrated by the systematic review. This is because the environment in which the research is carried out is challenging and only sometimes produces results; much depends on the researcher's skills and knowledge of the virtual environment. Furthermore, the data is not always easy to find since everything happens in real-time, and therefore, the researcher must be present at the exact moment in which an illicit activity is being perpetrated. These problems pose many challenges to those studying cybercrime in virtual worlds, since many hours of research may not bring results.

Thanks to the data gathered and analyzed from this research, it was possible to produce the following outputs:

- A risk assessment: it could be determined which virtual worlds and related applications are greater risk than others, in correlation to a certain crime,
- How these platforms can be exploited,
- Analyze the community and criminal behavior/language,
- The possible creation of an artificial intelligence monitoring software.

One of the problems encountered during the research is certainly the non-participation of companies; despite repeated requests for data access, and interviews with companies in the sector, a

[53] https://www.imdb.com/title/tt30442234/

negative response was always received, and the research was never looked upon favorably. Clearly, who would want to hear that certain types of material travel in their applications?

In conclusion, Virtual worlds (VWs) are conducive to criminal activities: VWs, like other online platforms, offer anonymity, virtual currencies, and specific places, making them attractive for cybercrime activities. The absence of physical presence and the ease of creating multiple identities further exacerbate these issues, creating a breeding ground for criminal behavior. VWs require vigilant oversight and regulation: Just as in the physical world, VWs need governance to ensure safety and security. Without adequate oversight, these digital environments can become havens for exploitation and abuse. Regulation is essential to establish boundaries, protect users' rights, and maintain a level playing field for all participants. To effectively regulate VWs, it's crucial to have clear rules and appropriate technological tools. Rules set the legal framework, defining what constitutes acceptable behavior and outlining consequences for violations. However, rules alone may not suffice. Technological tools such as content moderation algorithms, user verification systems, and encryption protocols are needed to enforce these rules effectively to prevent abuses. This research aimed to highlight the possibility that virtual worlds offer concerning cybercrime and a strategic framework for tool development. In summary, addressing the challenges of crime in virtual worlds requires a multi-faceted approach that combines legal frameworks, technological innovations, and ongoing research efforts.

6. BIBLIOGRAPHY

ACB. (2023). Homepage [Other]. Australian Classification. https://www.classification.gov.au/

Agarwal, N., Ünlü, T., Wani, M. A., & Bours, P. (2022). Predatory Conversation Detection Using Transfer Learning Approach. In G. Nicosia, V. Ojha, E. La Malfa, G. La Malfa, G. Jansen, P. M. Pardalos, G. Giuffrida, & R. Umeton (Eds.), Machine Learning, Optimization, and Data Science (pp. 488–499). Springer International Publishing. https://doi.org/10.1007/978-3-030-95467-3_35

Aitamurto, T. (2013). Balancing Between Open and Closed: Co-creation in magazine journalism. Digital Journalism, 1(2), 229–251. https://doi.org/10.1080/21670811.2012.750150

Alam, S. (2021). Evolution of Malware in the Digital Transformation Age [Chapter]. Handbook of Research on Advancing Cybersecurity for Digital Transformation; IGI Global. https://doi.org/10.4018/978-1-7998-6975-7.ch013

Al-Awsat. (2017). Was Bin Laden a Fan of Video Games? https://english.aawsat.com/node/1073006

Alexander, J. (2018, February 28). Discord is purging alt-right, white nationalist and hateful servers. Polygon. https://www.polygon.com/2018/2/28/17061774/discord-alt-right-atomwaffen-ban-centipede-central-nordic-resistance-movement

Al-Garadi, M. A., Hussain, M. R., Khan, N., Murtaza, G., Nweke, H. F., Ali, I., Mujtaba, G., Chiroma, H., Khattak, H. A., & Gani, A. (2019). Predicting Cyberbullying on Social Media in the Big Data Era Using Machine Learning Algorithms: Review of Literature and Open Challenges. IEEE Access, 7, 70701–70718. https://doi.org/10.1109/ACCESS.2019.2918354

Almeida, J. M. F. de. (2008). Virtual Informatics Museum [Chapter]. Encyclopedia of Networked and Virtual Organizations; IGI Global. https://doi.org/10.4018/978-1-59904-885-7.ch236

Al-Rawi, A. (2018). Video games, terrorism, and ISIS's Jihad 3.0. Terrorism and Political Violence, 30(4), 740–760. https://doi.org/10.1080/09546553.2016.1207633

Amokeoja, O. (2023, October 5). Poland's Online Community Rocked by Pedophilia Allegations. BNN Breaking. https://bnn.network/arts/polands-online-community-rocked-by-pedophilia-allegations/

Amponsah, S., Aheto, S.-P. K., Anapey, G. M., & Kwapong, O. O. (2021). Arrangements for Online Engagements of Distance Learners in the Wake of the COVID-19 Pandemic [Chapter]. Re-Envisioning and Restructuring Blended Learning for Underprivileged Communities; IGI Global. https://doi.org/10.4018/978-1-7998-6940-5.ch012

Andronico. (2021, January 28). Discord is the one app you need to be using—Here's what you need to know. CNN Underscored. https://www.cnn.com/2021/01/28/cnn-underscored/discord-app/index.html

APA Dictionary of Psychology. (2018). APA Dictionary of Psychology. https://dictionary.apa.org/

Au, C. H., & Ho, K. K. (2021). The anti-ageing secret of massively multiplayer online game: Managing its lifecycle. Australian Journal of Management, 46(4), 652–671. https://doi.org/10.1177/0312896220981119

Bainbridge, W. S. (Ed.). (2004). Berkshire encyclopedia of human-computer interaction. Berkshire Pub. Group.

Bannelier & Lostri. (2024). So Close, So Far: UN Committee Tasked With Cybercrime Convention Hits Snooze. Default. https://www.lawfaremedia.org/article/so-close-so-far-un-committee-tasked-with-cybercrime-convention-hits-snooze

Bartle, R. (2003). Designing Virtual Worlds (p. 768).

Bartle, R. A. (2016). MMOs from the Inside Out. Apress. https://doi.org/10.1007/978-1-4842-1724-5

Bell, M. (2008). Toward a Definition of "Virtual Worlds". Journal of Virtual Worlds Research; Vol 1, No 1: Virtual Worlds Research: Past, Present and Future, 18. https://doi.org/10.4101/jvwr.v1i1.283

Benjamin, G. (2015). "Virtual Reality" Reconsidered [Chapter]. Handbook of Research on Digital Media and Creative Technologies; IGI Global. https://doi.org/10.4018/978-1-4666-8205-4.ch009

Bhatt, T. (2023, October 11). Types of Metaverse: An In-Depth Exploration. Intelivita. https://www.intelivita.com/blog/types-of-metaverse/

Bickart, B., & Schindler, R. (2001). Internet Forums as Influential Sources of Consumer Information. Journal of Interactive Marketing, 15, 31–40. https://doi.org/10.1002/dir.1014

Black, A., Lumsden, K., & Hadlington, L. (2019). 'Why Don't You Block Them?' Police Officers' Constructions of the Ideal Victim When Responding to Reports of Interpersonal Cybercrime (pp. 355–378). https://doi.org/10.1007/978-3-030-12633-9_15

Blankley. (2023, January 10). Law enforcement warns of 'alarming' spike in online exploitation of children. The Center Square. https://www.thecentersquare.com/national/article_8002e888-9131-11ed-9b41-9b82d461d195.html

Bösche, W., & Kattner, F. (2011). Field Report: Using a Violent Multiplayer Game as a Virtual Classroom for a Course on Violent Video Games [Chapter]. Handbook of Research on Improving

Learning and Motivation through Educational Games: Multidisciplinary Approaches; IGI Global. https://doi.org/10.4018/978-1-60960-495-0.ch035

Boulos, M. N. K., Hetherington, L., & Wheeler, S. (2007). Second Life: An overview of the potential of 3-D virtual worlds in medical and health education. Health Information and Libraries Journal, 24(4), 233–245. https://doi.org/10.1111/j.1471-1842.2007.00733.x

Bowles, N., & Keller, M. H. (2019, December 7). Video Games and Online Chats Are 'Hunting Grounds' for Sexual Predators. The New York Times. https://www.nytimes.com/interactive/2019/12/07/us/video-games-child-sex-abuse.html, https://www.nytimes.com/interactive/2019/12/07/us/video-games-child-sex-abuse.html

Brewster, T. (2019). Discord: The $2 Billion Gamer's Paradise Coming To Terms With Data Thieves, Child Groomers And FBI Investigators. Forbes. https://www.forbes.com/sites/thomasbrewster/2019/01/29/discord-the-2-billion-gamers-paradise-coming-to-terms-with-data-thieves-child-groomers-and-fbi-investigators/

Brown. (2020, February 11). Predators at Play: How kids can be targeted through online gaming. WCIV. https://abcnews4.com/news/local/predators-at-play-how-kids-can-be-targeted-through-online-gaming-02-12-2020

Buchanan, D. A., & Bryman, A. (Eds.). (2011). The SAGE handbook of organizational research methods (Paperback ed). SAGE.

Californian Penal Code art 288. (n.d.). Law section. Retrieved 2 April 2024, from https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=288.&lawCode=PEN

Castronova, E. (2005). Synthetic Worlds: The Business and Culture of Online Games. Bibliovault OAI Repository, the University of Chicago Press.

Catterall, M., & Maclaran, P. (2002). Researching consumers in virtual worlds: A cyberspace odyssey. Journal of Consumer Behaviour, 1, 228–237. https://doi.org/10.1002/cb.68

CBS Mornings (Director). (2019, August 21). We need to tackle domestic terrorism like we do foreign threats, expert says. https://www.youtube.com/watch?v=ureqmS-zHFU

Cecilia D'anastasio. (2020, June 20). Bot mafias have wreaked havoc in World of Warcraft Classic. Wired. https://arstechnica.com/gaming/2020/06/bot-mafias-have-wreaked-havoc-in-world-of-warcraft-classic/

Chad pradelli, Cheryl Mettendorf. (2020, December 11). Pandemic predators: Authorities say child sex crime tips are up since start of COVID outbreak. 6abc Philadelphia. https://6abc.com/geoffrey-hines-upper-darby-pa-sex-crime-video-games-pennsylvania-delco/8670338/

Chambers-Jones, C. (2012). Virtual Economies and Financial Crime: Money Laundering in Cyberspace. Edward Elgar Publishing. https://doi.org/10.4337/9781849809337

Chambers-Jones, C. (2013). Virtual world financial crime: Legally flawed. Law and Financial Markets Review, 7(1), 48–56. https://doi.org/10.5235/LFMR7.1.48

Chambers-Jones, C. (2018). Money Laundering in a Virtual World. In C. King, C. Walker, & J. Gurulé (Eds.), The Palgrave Handbook of Criminal and Terrorism Financing Law (pp. 165–182). Springer International Publishing. https://doi.org/10.1007/978-3-319-64498-1_8

Chen, Y., Chen, P. S., Hwang, J., Korba, L., Song, R., & Yee, G. (2005). An analysis of online gaming crime characteristics. Internet Research, 15(3), 246–261. https://doi.org/10.1108/10662240510602672

Chen, Y.-C., Chen, P., Song, R., & Korba, L. (2004). Online Gaming Crime and Security Issue—Cases and Countermeasures from Taiwan. Proceedings of the 2nd Annual Conference on Privacy, Security and Trust (PST'2004), Collection / Collection : NRC Publications Archive / Archives des publications du CNRC.

Childline. (2022). Online gaming | Childline. https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/online-gaming/

Codice Penale Art. 600 quater comma 3, 2021. (n.d.). Art. 600 quater codice penale—Detenzione o accesso a materiale pornografico. Brocardi.it. Retrieved 2 April 2024, from https://www.brocardi.it/codice-penale/libro-secondo/titolo-xii/capo-iii/sezione-i/art600quater.html

Codice Penale Art. 609 quater. (n.d.). Art. 609 quater codice penale—Atti sessuali con minorenne. Brocardi.it. Retrieved 2 April 2024, from https://www.brocardi.it/codice-penale/libro-secondo/titolo-xii/capo-iii/sezione-ii/art609quater.html

Combating Robot Networks. (n.d.). 195.

Commission of Europe. (2007). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE COMMITTEE OF THE REGIONS. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF

Consalvo, M., & Dutton, N. (2006). Game analysis: Developing a methodological toolkit for the qualitative study of games. Game Studies, 6.

Convention on Cybercrime. (2001). Convention on Cybercrime. Refworld. https://www.refworld.org/legal/agreements/coe/2001/en/90189

Conway, M., Scrivens, R., & Macnair, L. (2019). Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends. 24.

Cook, D. J. (1997). Systematic Reviews: Synthesis of Best Evidence for Clinical Decisions. Annals of Internal Medicine, 126(5), 376. https://doi.org/10.7326/0003-4819-126-5-199703010-00006

Cook et al. (2021, September 30). Understanding child safety and video gaming with GameTrack. Ipsos. https://www.ipsos.com/en-uk/understanding-child-safety-and-video-gaming-gametrack

Cooper, H. M., & Cooper, H. M. (1998). Synthesizing research: A guide for literature reviews (3rd ed). Sage Publications.

COP. (2020). Child Online Protection | ITU COP Guidelines. ITU-COP Guidelines. https://www.itu-cop-guidelines.com

Cornish, S. (2020, December 13). Gang members robbing and assaulting people using online app to buy drugs. Stuff. https://www.stuff.co.nz/national/123668754/gang-members-robbing-and-assaulting-people-using-online-app-to-buy-drugs

Cory Shaffer, cleveland com. (2020, May 12). Cleveland man planned to ambush law enforcement to steal weapons for armed uprising, feds say. Cleveland. https://www.cleveland.com/court-justice/2020/05/cleveland-man-planned-to-ambush-law-enforcement-to-steal-weapons-for-armed-uprising-feds-say.html

Costa, S., Mendes Da Silva, B., & Tavares, M. (2021). Video games and gamification against online hate speech? 10th International Conference on Digital and Interactive Arts, 1–7. https://doi.org/10.1145/3483529.3483679

Costello, L., McDermott, M.-L., & Wallace, R. (2017). Netnography: Range of Practices, Misperceptions, and Missed Opportunities. International Journal of Qualitative Methods, 16(1), 160940691770064. https://doi.org/10.1177/1609406917700647

Cretu, V. (2022). The Role of Spiritual Communication and Care During the COVID-19 Pandemic [Chapter]. Basic Communication and Assessment Prerequisites for the New Normal of Education; IGI Global. https://doi.org/10.4018/978-1-7998-8247-3.ch002

Croft. (2020, October 14). Sony: 'We Do Not Record' PS4 Party Chats. Push Square. https://www.pushsquare.com/news/2020/10/sony_we_do_not_record_ps4_party_chats

Curcio, M. (2023). Cybercrime and Video Games: Exploring children's safety in the gaming environment. European Interdisciplinary Cybersecurity Conference, 144–148. https://doi.org/10.1145/3590777.3590801

Dauber, C. E., Robinson, M. D., Baslious, J. J., & Blair, A. G. (2019). Call of Duty: Jihad – How the Video Game Motif Has Migrated Downstream from Islamic State Propaganda Videos. Perspectives on Terrorism, 13(3), 17–31.

David Curry. (2023, January 9). Discord Revenue and Usage Statistics (2023). Business of Apps. https://www.businessofapps.com/data/discord-statistics/

Demant et al. (2019). Technology-facilitated drug dealing via social media in the Nordic countries | www.emcdda.europa.eu. https://www.emcdda.europa.eu/drugs-library/technology-facilitated-drug-dealing-social-media-nordic-countries_en

Donalds, C., & Osei-Bryson, K.-M. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. Computers in Human Behavior, 92, 403–418. https://doi.org/10.1016/j.chb.2018.11.039

Elliott, J. (2013, December 9). World of Spycraft: NSA and CIA Spied in Online Games. ProPublica. https://www.propublica.org/article/world-of-spycraft-intelligence-agencies-spied-in-online-games

Embree, L. (1996). Encyclopedia of Phenomenology. Kluwer Academic Publishers.

Epic Games. (2023). Controllo parentale. https://safety.epicgames.com/it/parental-controls

ESRB. (2023). ESRB Ratings | Entertainment Software Ratings Board. ESRB Ratings. https://www.esrb.org/

European Union Agency for Law Enforcement Cooperation. (2022). Policing in the metaverse: What law enforcement needs to know : an observatory report from the Europol innovation lab. Publications Office. https://data.europa.eu/doi/10.2813/81062

Faraz, A., Mounsef, J., Raza, A., & Willis, S. (2022). Child Safety and Protection in the Online Gaming Ecosystem. IEEE Access, 10, 115895–115913. https://doi.org/10.1109/ACCESS.2022.3218415

Floridi, L. (2022). Metaverse: A Matter of Experience. Philosophy & Technology, 35(3), 73. https://doi.org/10.1007/s13347-022-00568-6

Fortnite End User License Agreement. (n.d.). Epic Games' Fortnite. Retrieved 27 November 2023, from https://www.fortnite.com/eula?lang=en-US&sessionInvalidated=true

FOX 35 news. (2019, October 25). Teen gamer arrested after posting violent threats, sheriff says [Text.Article]. FOX 35 Orlando; FOX 35 Orlando. https://www.fox35orlando.com/news/teen-gamer-arrested-after-posting-violent-threats-sheriff-says

Freile. (2019). Violent New York criminal cases tied to popular gaming app. https://eu.democratandchronicle.com/story/news/2019/11/11/discord-gaming-app-albion-middle-school-threat-bianca-devins-islamberg-rochester-utica-ny/2560441001/

Garau. (2023, January 21). Il pugno al volto e la fuga: Cos'è il 'knock out game', la sfida dei balordi. ilGiornale.it. https://www.ilgiornale.it/news/cronaca-locale/pugno-volto-nel-bar-e-fuga-si-teme-knockout-game-2107759.html

Gaudiosi, J. (n.d.). Norway Suspect Used Call Of Duty To Train For Massacre. Forbes. Retrieved 13 March 2022, from https://www.forbes.com/sites/johngaudiosi/2011/07/24/norway-suspect-used-activisions-call-of-duty-to-train-for-massacre/

Gesche, A. (2009). Adapting to Virtual Third-Space Language Learning Futures [Chapter]. Handbook of Research on E-Learning Methodologies for Language Acquisition; IGI Global. https://doi.org/10.4018/978-1-59904-994-6.ch032

Gilchrist, P., & Ravenscroft, N. (2011). Paddling, property and piracy: The politics of canoeing in England and Wales. Sport in Society, 14(2), 175–192. https://doi.org/10.1080/17430437.2011.546518

Girvan, C. (2018). What is a virtual world? Definition and classification. Educational Technology Research and Development, 66(5), 1087–1100. https://doi.org/10.1007/s11423-018-9577-y

Godin, K., Stapleton, J., Kirkpatrick, S. I., Hanning, R. M., & Leatherdale, S. T. (2015). Applying systematic review search methods to the grey literature: A case study examining guidelines for school-based breakfast programs in Canada. Systematic Reviews, 4(1), 138. https://doi.org/10.1186/s13643-015-0125-0

Goldenberg, S. (2021, July 26). FBI warns predators are targeting children playing video games. Https://Www.Cleveland19.Com. https://www.cleveland19.com/2021/07/26/fbi-warns-predators-are-targeting-children-playing-video-games/

Good, O. S. (2020, October 16). PS5 won't actively monitor or listen to your voice chat, Sony says. Polygon. https://www.polygon.com/2020/10/16/21520174/ps5-voice-chat-recording-moderation-sony-playstation-5-ps4

Govind. (2020, October 1). 10 sentenced to prison for child exploitation enterprise & conspiracy— Biometrica Systems, Inc. https://www.biometrica.com/10-sentenced-to-prison-for-child-exploitation-enterprise-conspiracy/

Grabher, G., & Ibert, O. (2014). Distance as asset? Knowledge collaboration in hybrid virtual communities. Journal of Economic Geography, 14(1), 97–123. https://doi.org/10.1093/jeg/lbt014

GRAC/GCRB. (2023). GAME RATING and ADMINISTRATION COMMITTEE. https://www.grac.or.kr/english/

Graycar, A., & Grabosky, P. (n.d.). Money laundering in the 21st century: Risks and countermeasures.

Greenwald. (n.d.). Bin Laden Might Have Trained Terrorists With a Video Game. PCMAG. Retrieved 26 December 2023, from https://www.pcmag.com/news/bin-laden-might-have-trained-terrorists-with-a-video-game

Greyman-Kennard. (2023, September 27). Parents be warned: 'Blue Whale' suicide game returns. The Jerusalem Post | JPost.Com. https://www.jpost.com/health-and-wellness/article-760706

Griffin, D. (n.d.). Operation Velvet Fury Targets Illicit Oklahoma Massage Parlors. Retrieved 26 December 2023, from https://www.news9.com/story/5e35bab9fcd8ef694720c947/operation-velvet-fury-targets-illicit-oklahoma-massage-parlors

Grimshaw, M. (2015). The Oxford handbook of virtuality. Oxford university press.

Grossman, L. C. D. (2016, November 18). Are Video Games Teaching Children to Kill? Literary Hub. https://lithub.com/are-video-games-teaching-children-to-kill/

Guo, Z., Wang, H., & Xie, C. (2022). Covid-19's Impact on the Gaming Industry and Countermeasures. 726–730. https://doi.org/10.2991/aebmr.k.220405.121

Guttmann. (2023). Parental control over children's media time U.S. 2019-2020. Statista. https://www.statista.com/statistics/232345/parental-control-over-childrens-media-consumption-in-the-us/

Halák, J. (2016). Beyond Things: The Ontological Importance of Play According to Eugen Fink. Journal of the Philosophy of Sport, 43(2), 199–214. https://doi.org/10.1080/00948705.2015.1079133

Ham-Kucharski, A. (2022). Respawning Jihadist: ISIS Recruiting Through Online Gaming Communities. Student Work. https://pdxscholar.library.pdx.edu/is_student/2

Heinonen, K., & Medberg, G. (2018). Netnography as a tool for understanding customers: Implications for service research and practice. Journal of Services Marketing, 32(6), 657–679. https://doi.org/10.1108/JSM-08-2017-0294

Hernandez, M. D., & Handan, V. (2014). Modeling word of mouth vs. media influence on videogame preorder decisions: A qualitative approach. Journal of Retailing and Consumer Services, 21(3), 401–406. https://doi.org/10.1016/j.jretconser.2013.11.003

Hollenbeck. (2019, January 15). Deputies warn parents about Discord app potential dangers. ABC Action News Tampa Bay (WFTS). https://www.abcactionnews.com/news/region-pinellas/deputies-warn-parents-about-discord-app-potential-dangers

Hollett, R., Tomkinson, S., Illingworth, S., Power, B., & Harper, T. (2022). Evidence that digital game players neglect age classification systems when deciding which games to play. PLOS ONE, 17(2), e0263560. https://doi.org/10.1371/journal.pone.0263560

Homan, C. (2013). The Play of Ethics in Eugen Fink. Journal of Speculative Philosophy, 27(3), 287–296. https://doi.org/10.5325/jspecphil.27.3.0287

Hoose, B. (2020, June 16). Predators and Gaming: What's a Parent to Do? Plugged In. https://www.pluggedin.com/blog/predators-and-gaming-whats-a-parent-to-do/

Hornsby. (n.d.). What Heidegger Means by Being-in-the-World. Retrieved 14 August 2022, from https://royby.com/philosophy/pages/dasein.html

IARC. (2023). IARC ratings for mobile and digitally delivered games from International Age Rating Coalition. https://www.globalratings.com/

Inc. (2023). Computer Crimes. Inc.Com. https://www.inc.com/encyclopedia/computer-crimes.html

Iprofess. (2009). Toons and Terrorism.

Irwin, A. S. M., Slay, J., Raymond Choo, K., & Liu, L. (2012). Are the financial transactions conducted inside virtual environments truly anonymous?: An experimental research from an Australian perspective. Journal of Money Laundering Control, 16(1), 6–40. https://doi.org/10.1108/13685201311286832

Jennifer Henderson. (2023, September 8). Teen Death After Spicy 'One Chip Challenge' Raises Alarm. https://www.medpagetoday.com/popmedicine/cultureclinic/106242

Jenson. (n.d.). Pedophiles Hunt Kids in Popular Gaming Apps: Roblox, Minecraft, & Fortnite | Defend Young Minds™. Retrieved 27 October 2023, from https://www.defendyoungminds.com/post/pedophiles-hunt-kids-online

Jevremovic, A., Veinovic, M., Cabarkapa, M., Krstic, M., Chorbev, I., Dimitrovski, I., Garcia, N., Pombo, N., & Stojmenovic, M. (2021). Keeping Children Safe Online With Limited Resources: Analyzing What is Seen and Heard. IEEE Access, 9, 132723–132732. https://doi.org/10.1109/ACCESS.2021.3114389

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001

Kaplan, A. M., & Haenlein, M. (2009). The fairyland of Second Life: Virtual social worlds and how to use them. Business Horizons, 52(6), 563–572. https://doi.org/10.1016/j.bushor.2009.07.002

Kartit, D., Howcroft, E., & Howcroft, E. (2022, October 27). Interpol says metaverse opens up new world of cybercrime. Reuters. https://www.reuters.com/technology/interpol-says-metaverse-opens-up-new-world-cybercrime-2022-10-27/

Kavenagh. (2023). Child Sexual Exploitation in Online Gaming | UNICEF East Asia and Pacific. https://www.unicef.org/eap/blog/child-sexual-exploitation-online-gaming

Keene, S. D. (2011). Emerging threats: Financial crime in the virtual world. Journal of Money Laundering Control, 15(1), 25–37. https://doi.org/10.1108/13685201211194718

King, D. L., Delfabbro, P. H., Billieux, J., & Potenza, M. N. (2020). Problematic online gaming and the COVID-19 pandemic. Journal of Behavioral Addictions, 9(2), 184–186. https://doi.org/10.1556/2006.2020.00016

Klippenstein, K. (2024, March 9). The Feds Are Coming for “Extremist” Gamers. The Intercept. https://theintercept.com/2024/03/09/fbi-dhs-gamers-extremism-violence/

Koehler, D., Fiebig, V., & Jugl, I. (2023). From Gaming to Hating: Extreme-Right Ideological Indoctrination and Mobilization for Violence of Children on Online Gaming Platforms. Political Psychology, 44(2), 419–434. https://doi.org/10.1111/pops.12855

Kozinets, R. (1997). I want to believe: A netnography of the X-philes’ subculture of consumption. Advances in Consumer Research, 24, 470–475.

Kozinets, R. (1999). E-Tribalized Marketing?: The Strategic Implications of Virtual Communities of Consumption. European Management Journal, 17, 252–264. https://doi.org/10.1016/S0263-2373(99)00004-3

Kozinets, R. V. (1998). On netnography: Initial reflections on consumer research investigations of cyberculture. Advances in Consumer Research, 336–371.

Kozinets, R. V. (2006). Click to Connect: Netnography and Tribal Advertising. Journal of Advertising Research, 46(3), 279–288. https://doi.org/10.2501/S0021849906060338

Kraut, R. (2022). Plato. In E. N. Zalta (Ed.), The Stanford Encyclopedia of Philosophy (Spring 2022). Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/spr2022/entries/plato/

Krossbakken, E., Torsheim, T., Mentzoni, R. A., King, D. L., Bjorvatn, B., Lorvik, I. M., & Pallesen, S. (2018). The effectiveness of a parental guide for prevention of problematic video gaming in children: A public health randomized controlled intervention study. Journal of Behavioral Addictions, 7(1), 52–61. https://doi.org/10.1556/2006.6.2017.087

Lakomy, M. (2019). Let's Play a Video Game: Jihadi Propaganda in the World of Electronic Entertainment. Studies in Conflict & Terrorism, 42(4), 383–406. https://doi.org/10.1080/1057610X.2017.1385903

Lamoureux, M. (2019, August 2). How a Group Of Gamers Tracked Down a Quadruple Murder Suspect. Vice. https://www.vice.com/en/article/kz4ezn/how-a-group-of-gamers-tracked-down-a-quadruple-murder-suspect-menhaz-zaman

Lange, P. G. (2008). Terminological Obfuscation in Online Research [Chapter]. Handbook of Research on Computer Mediated Communication; IGI Global. https://doi.org/10.4018/978-1-59904-863-5.ch033

Lankoski, P., & Bjork, S. (2015). Game research methods: An overview.

Laorden, C., Galán-García, P., Santos, I., Sanz, B., Hidalgo, J. M. G., & Bringas, P. G. (2013). Negobot: A Conversational Agent Based on Game Theory for the Detection of Paedophile Behaviour. In Á. Herrero, V. Snášel, A. Abraham, I. Zelinka, B. Baruque, H. Quintián, J. L. Calvo, J. Sedano, & E. Corchado (Eds.), International Joint Conference CISIS'12-ICEUTE´12-SOCO´12 Special Sessions (pp. 261–270). Springer. https://doi.org/10.1007/978-3-642-33018-6_27

Levenson, M., & Rubin, A. (2022, July 6). Parents Sue TikTok, Saying Children Died After Viewing 'Blackout Challenge'. The New York Times. https://www.nytimes.com/2022/07/06/technology/tiktok-blackout-challenge-deaths.html

Makuch. (2019). Congressman Shames Blizzard for Letting Nazis Run Wild in "World of Warcraft." https://www.vice.com/en_us/embed/article/mb7b9q/world-of-warcraft-has-a-rape-problem?utm_source=stylizedembed_vice.com&utm_campaign=3kxw4b&site=vice

Marler, T., Abdurahaman, Z. F., Boudreaux, B., & Gulden, T. R. (2023). The Metaverse and Homeland Security: Opportunities and Risks of Persistent Virtual Environments. RAND Corporation. https://www.rand.org/pubs/perspectives/PEA2217-2.html

Mastrangelo, L. (2022, March 23). 2021 Internet Crime Report. Homeland Security Digital Library. https://www.hsdl.org/c/2021-internet-crime-report/

Matteo, C. (2022). Cybercrimes and Virtual Worlds: A Systematic Literature Review. Journal of Information Security and Cybercrimes Research, 5(2), Article 2. https://doi.org/10.26735/CBBQ4731

McLaughlin, J. (2023, September 13). UN debates how to define cybercrime. NPR. https://www.npr.org/2023/09/13/1199324577/un-debates-how-to-define-cybercrime

Milmo, D., & editor, D. M. G. technology. (2021, October 28). Enter the metaverse: The digital future Mark Zuckerberg is steering us toward. The Guardian. https://www.theguardian.com/technology/2021/oct/28/facebook-mark-zuckerberg-meta-metaverse

Miranda. (2019, May 2). The Simulated Real: Roleplaying Terrorism in Gaming. The Hmm. https://thehmm.nl/the-simulated-real/

Mittelstraß, J. (Ed.). (2005). Enzyklopädie Philosophie und Wissenschaftstheorie. J.B. Metzler. https://doi.org/10.1007/978-3-476-00134-4

Mondesert, A.-L. (2020). EU anti-terror chief warns video games used to spread extremism, prepare attacks. https://www.timesofisrael.com/eu-anti-terror-chief-warns-video-games-used-to-spread-extremism-prepare-attacks/

Moore. (2022, August 22). Sickening video shows man knocked out by stranger in NYC mall. https://nypost.com/2022/08/22/sickening-video-shows-man-knocked-out-by-stranger-in-nyc-mall/

Moyle, L., Childs, A., Coomber, R., & Barratt, M. J. (2019). #Drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs. International Journal of Drug Policy, 63, 101–110. https://doi.org/10.1016/j.drugpo.2018.08.005

Mudry, T. E., & Strong, T. (2013). Doing Recovery Online. Qualitative Health Research, 23(3), 313–325. https://doi.org/10.1177/1049732312468296

Nevelsteen, K. J. L. (2018). Virtual World, Defined from a Technological Perspective, and Applied to Video Games, Mixed Reality and the Metaverse. Computer Animation and Virtual Worlds, 29(1), e1752. https://doi.org/10.1002/cav.1752

O'Connor, E. (2012). Practical Considerations When Using Virtual Spaces for Learning and Collaboration, with Minimal Setup and Support [Chapter]. Handbook of Research on Practices and

Outcomes in Virtual Worlds and Environments; IGI Global. https://doi.org/10.4018/978-1-60960-762-3.ch018

Oksanen, A., Miller, B. L., Savolainen, I., Sirola, A., Demant, J., Kaakinen, M., & Zych, I. (2020). Social Media and Access to Drugs Online: A Nationwide Study in the United States and Spain among Adolescents and Young Adults. The European Journal of Psychology Applied to Legal Context, 13(1), 29–36. https://doi.org/10.5093/ejpalc2021a5

Patterson. (2019, October 21). Cybercriminals are doing big business in the gaming chat app Discord—CBS News. https://www.cbsnews.com/news/cybercriminals-are-doing-big-business-in-the-gaming-chat-app-discord/

PBS News. (2019, August 4). The 'gamification' of domestic terrorism online. PBS NewsHour. https://www.pbs.org/newshour/show/the-gamification-of-domestic-terrorism-online

PEGI. (2023). | Pegi Public Site. https://pegi.info/

Peterson, M. (2003). Maps and the Internet (pp. 1–16). https://doi.org/10.1016/B978-008044201-3/50003-7

Pidd, H. (2012, April 19). Anders Breivik 'trained' for shooting attacks by playing Call of Duty. The Guardian. https://www.theguardian.com/world/2012/apr/19/anders-breivik-call-of-duty

Polizia Di Stato. (2021, January 25). Pedofilia on-line che cos'è? Polizia Postale. https://www.commissariatodips.it/approfondimenti/pedofilia-online/pedofilia-on-line-che-cose/index.html

Preuß, S., Bley, L. P., Bayha, T., Dehne, V., Jordan, A., Reimann, S., Roberto, F., Zahm, J. R., Siewerts, H., Labudde, D., & Spranger, M. (2021). Automatically Identifying Online Grooming Chats Using CNN-based Feature Extraction. In K. Evang, L. Kallmeyer, R. Osswald, J. Waszczuk, & T. Zesch (Eds.), Proceedings of the 17th Conference on Natural Language Processing (KONVENS 2021) (pp. 137–146). KONVENS 2021 Organizers. https://aclanthology.org/2021.konvens-1.12

Qureshi et al. (2019). What is Discord? What to know about gamers' messaging platform after Albion school threat. Democrat and Chronicle. https://www.democratandchronicle.com/story/news/2019/07/16/discord-what-know-gamers-messaging-platform-instagram-4-chan-bianca-devins-death-utica-ny-teen/1742315001/

Radoff. (2010, May 27). History of Social Games. https://web.archive.org/web/20100527090108/http://radoff.com/blog/2010/05/24/history-social-games/

RARS. (2023, December 31). Russian Age Rating System. Rating System Wiki. https://rating-system.fandom.com/wiki/Russian_Age_Rating_System

Reynard. (n.d.). Retrieved 2 April 2024, from https://www.iarpa.gov/research-programs/reynard

Riffe, D., Lacy, S., Fico, F., Riffe, D., Lacy, S., & Fico, F. G. (2006). Analyzing Media Messages (0 ed.). Routledge. https://doi.org/10.4324/9781410613424

Riot Games. (2023, March 4). VALORANT Voice Evaluation Update. https://playvalorant.com/en-us/news/announcements/valorant-voice-evaluation-update/

Roebuck, J. (2021, January 19). Authorities will 'never take me alive,' Harrisburg woman told social media after stealing Nancy Pelosi's laptop, FBI says. Https://Www.Inquirer.Com. https://www.inquirer.com/news/riley-williams-nancy-pelosi-laptop-capitol-arrests-pennsyvania-harrisburg-discord-20210120.html

Roser, M. (2024). The Internet's history has just begun. Our World in Data. https://ourworldindata.org/internet-history-just-begun

S1E8: How are terrorists and violent extremists using gamification? (2020, May 13). https://open.spotify.com/episode/2yTDYIDPDVGMf1MBJME59c

Sandkühler, H. J., & Borchers, D. (Eds.). (2010). Enzyklopädie Philosophie: In drei Bänden mit einer CD-ROM (2., überarb. und erw. Aufl.). Meiner.

Schroeder, R. (1970). Defining Virtual Worlds and Virtual Environments. Journal For Virtual Worlds Research, 1(1). https://doi.org/10.4101/jvwr.v1i1.294

Shachtman, N. (2008). Pentagon Researcher Conjures Warcraft Terror Plot. Wired. https://www.wired.com/2008/09/world-of-warcra/

Shane Harris And Samuel Oakford. (2023, April 13). Discord member details how documents leaked from closed chat group. Washington Post. https://www.washingtonpost.com/national-security/2023/04/12/discord-leaked-documents/

Shelby-Caffey, C., Jafari, S., & Munguia, M. R. (2021). What the Flip: Embracing Flipped Learning as a Mediated Approach in Teacher Education [Chapter]. Shifting to Online Learning Through Faculty Collaborative Support; IGI Global. https://doi.org/10.4018/978-1-7998-6944-3.ch014

Shukla. (2021). ISIS using 'Discord', 'Rocket Chat' messenger, security agencies alert govt. DNA India. https://www.dnaindia.com/india/report-isis-using-discord-game-rocket-chat-messenger-indian-security-agencies-alert-government-2866005

Silva, J. P. N., Valadares, G. C., Pedrosa, G., Rezende, D. C., Cappelle, M. C. A., & Assis, F. A. A. (2021). Gender imbalance in MMORPG: The case of World of Warcraft in Brazil. Feminist Media Studies, 1–17. https://doi.org/10.1080/14680777.2021.1973060

Singel. (2008). U.S. Spies Want to Find Terrorists in World of Warcraft | WIRED. https://www.wired.com/2008/02/nations-spies-w/

Singhal, S., & Zyda, M. (1999). Networked virtual environments: Design and implementation. ACM Press/Addison-Wesley Publishing Co.

Sloane, S. (2000). Digital fictions: Storytelling in a material world. Ablex Pub.

S.M. Irwin, A., Slay, J., Raymond Choo, K.-K., & Lui, L. (2014). Money laundering and terrorism financing in virtual environments: A feasibility study. Journal of Money Laundering Control, 17(1), 50–75. https://doi.org/10.1108/JMLC-06-2013-0019

Smith, D. W. (2018). Phenomenology. In E. N. Zalta (Ed.), The Stanford Encyclopedia of Philosophy (Summer 2018). Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/sum2018/entries/phenomenology/

Staff, A. (2019, October 25). Teen-aged Florida gamer accused of making violent, disturbing threats. Https://Www.Mysuncoast.Com. https://www.mysuncoast.com/2019/10/25/teen-aged-florida-gamer-accused-making-violent-disturbing-threats/

Steed, A., & Oliveira, M. F. (2010). Networked graphics: Building networked games and virtual environments. Morgan Kaufmann.

Stephenson, N. (1992). Snow crash. Bantam Books.

Stevens, T. (2015). Security and Surveillance in Virtual Worlds: Who Is Watching the Warlocks and Why? International Political Sociology, 9(3), 230–247. https://doi.org/10.1111/ips.12094

Stopbullying.gov. (2021, April 7). Cyberbullying and Online Gaming [Text]. https://www.stopbullying.gov/cyberbullying/cyberbullying-online-gaming

Storm, D. (2011, April 13). Intelligence agencies hunting for terrorists in World of Warcraft. Computerworld. https://www.computerworld.com/article/2471127/intelligence-agencies-hunting-for-terrorists-in-world-of-warcraft.html

Swearingen. (n.d.). Steve Bannon's 'World of Warcraft' Gold Farming Inspired Him. Retrieved 26 December 2023, from https://nymag.com/intelligencer/2017/07/steve-bannon-world-of-warcraft-gold-farming.html

Switzer, J. S. (2008). Successful Communication in Virtual Teams and the Role of the Virtual Team Leader [Chapter]. Handbook of Research on Virtual Workplaces and the New Nature of Business Practices; IGI Global. https://doi.org/10.4018/978-1-59904-893-2.ch004

Taylor. (2018, September 14). UKIE: Only 19% of parents set and enforce screen time limits for their children. GamesIndustry.Biz. https://www.gamesindustry.biz/digital-school-house-only-19-percent-of-parents-set-and-enforce-screen-time-limits-for-their-children

Tgcom24. (2023, October 25). Rimini, abusi su un 13enne: Arrestato youtuber da un milione di follower. Tgcom24. https://www.tgcom24.mediaset.it/cronaca/youtuber-arrestati-abusi-13enne-rimini_71792376-202302k.shtml

Titcomb. (2015, November 16). Did Paris terrorists really use PlayStation 4 to plan attacks? The Telegraph. https://www.telegraph.co.uk/technology/video-games/playstation/11997952/paris-attacks-playstation-4.html

Tom Wijman. (2020). Three Billion Players by 2023: Engagement and Revenues Continue to Thrive Across the Global Games Market. Newzoo. https://newzoo.com/insights/articles/games-market-engagement-revenues-trends-2020-2023-gaming-report

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. British Journal of Management, 14(3), 207–222. https://doi.org/10.1111/1467-8551.00375

Trifunović, D. (2021). CYBERSECURITY – VIRTUAL SPACE AS AN AREA FOR COVERT TERRORIST ACTIVITIES OF RADICAL ISLAMISTS. TEME, 095. https://doi.org/10.22190/TEME201119006T

Tuncer, I. (2020). Customer Experience in the Restaurant Industry: Use of Smart Technologies [Chapter]. Handbook of Research on Smart Technology Applications in the Tourism Industry; IGI Global. https://doi.org/10.4018/978-1-7998-1989-9.ch012

UNICEF. (2019). The online gaming industry and child rights. UNICEF-IRC. https://www.unicef-irc.org/article/1926-the-online-gaming-industry-and-child-rights.html

UNICEF. (2020). UNICEF publishes recommendations for the online gaming industry on assessing impact on children | UNICEF. https://www.unicef.org/partnerships/unicef-publishes-recommendations-online-gaming-industry-assessing-impact-children

UNICRI. (2022). UNICRI :: United Nations Interregional Crime and Justice Research Institute. https://unicri.it/Publication/Gaming-and-the%20Metaverse

USK. (2023). For Business. Unterhaltungssoftware Selbstkontrolle. https://usk.de/en/

Vamshi, A. (2020, November 13). Here Comes TroubleGrabber: Stealing Credentials Through Discord. Netskope. https://www.netskope.com/blog/here-comes-troublegrabber-stealing-credentials-through-discord

Van Der Sanden, R., Wilkins, C., Rychert, M., & Barratt, M. J. (2022). The Use of Discord Servers to Buy and Sell Drugs. Contemporary Drug Problems, 49(4), 453–477. https://doi.org/10.1177/00914509221095279

Vanolo. (2021). Edizioni-Machiavelli-Metaverso-e-Sicurezza-Nazionale.pdf. https://www.strategicstudies.it/wp-content/uploads/2021/12/Edizioni-Machiavelli-Metaverso-e-Sicurezza-Nazionale.pdf

Viano, E. C. (Ed.). (2017). Cybercrime, Organized Crime, and Societal Responses. Springer International Publishing. https://doi.org/10.1007/978-3-319-44501-4

Videogames Europe. (2018). Research: Majority of parents control child's in-game spending. VIDEOGAMES EUROPE. https://www.videogameseurope.eu/news/research-majority-of-parents-control-childs-in-game-spending/

Videos. (2019, October 25). [Collection]. FOX 35 Orlando; FOX 35 Orlando. https://www.fox35orlando.com/video/618965

Vittozzi. (2020). Sharp rise in children investigated over far-right links—Including youngsters under 10. Sky News. https://news.sky.com/story/sharp-rise-in-children-investigated-over-far-right-links-including-youngsters-under-10-12131565

Weru, T., Sevilla, J., Olukuru, J., Mutegi, L., & Mberi, T. (2017). Cyber-smart children, cyber-safe teenagers: Enhancing internet safety for children. 2017 IST-Africa Week Conference (IST-Africa), 1–8. https://doi.org/10.23919/ISTAFRICA.2017.8102292

What is cybercrime? Definition from SearchSecurity. (n.d.). Security. Retrieved 2 April 2024, from https://www.techtarget.com/searchsecurity/definition/cybercrime

WHO. (2022). What works to prevent online violence against children? Executive summary. https://www.who.int/publications-detail-redirect/9789240062085

Wijtman, T. (n.d.). Three Billion Players by 2023: Engagement and Revenues Continue to Thrive Across the Global Games Market. Newzoo. Retrieved 25 September 2022, from https://newzoo.com/insights/articles/games-market-engagement-revenues-trends-2020-2023-gaming-report

Wilcock, M. (2024, January 18). 5+ Video Games Where Predators Target Kids. Gabb. https://gabb.com/blog/predators-on-video-games/

Wright. (2021). What is ARPANET and what's its significance? Networking. https://www.techtarget.com/searchnetworking/definition/ARPANET

Yar, M., & Steinmetz, K. F. (2019). Cybercrime and Society (3rd ed.). SAGE Publications Ltd. https://www.perlego.com/book/1431897/cybercrime-and-society-pdf

Zambrano, P., Sanchez, M., Torres, J., & Fuertes, W. (2017). BotHook: An option against Cyberpedophilia. 2017 1st Cyber Security in Networking Conference (CSNet), 1–3. https://doi.org/10.1109/CSNET.2017.8241994

Zeilik, M., & Gregory, S. A. (1998). Introductory Astronomy & Astrophysics. Saunders College Pub.

Zilber, A. (2017, November 3). Bin Laden played video games like Counter-Strike and Super Mario Bros. Mail Online. http://www.dailymail.co.uk/~/article-5045111/index.html

Zimmermann, K. A., & published, J. E. (2022, April 8). Internet History Timeline: ARPANET to the World Wide Web. Livescience.Com. https://www.livescience.com/20727-internet-history.html

Zuo, Z., Li, J., Anderson, P., Yang, L., & Naik, N. (2018). Grooming Detection using Fuzzy-Rough Feature Selection and Text Classification. 2018 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), 1–8. https://doi.org/10.1109/FUZZ-IEEE.2018.8491591

ANNEX

Jargon MMORPG specific:

- Camper = (n.) Usually, this term indicates a person who "camps" (stops) a certain place or point on the map. This is often done while waiting for the spawn of a boss or an important mob. It is also used in FPS to criticize the behavior of certain players, who wait around the corner and are ready to kill other players as soon as they cross the threshold.
- Cash Shop = (n.) syn. Item shop, is the shop with items and more, which can be purchased with real and/or game currency.
- Craft = (n.) Ability to create objects.
- Crit = (n.) Refers to the critical hit or chance of scoring a critical hit.
- CC = abb. of “Crowd Control”. It refers to skills, spells, spells and everything that can somehow gain control over the opponent, such as paralysis, stunning etc.
- Dmg = abb. of “damage”, i.e. the damage that can be caused.
- Dps = abb. of “Damage per second”, the damage caused every second. Dd = abb. of "Damage dealer", i.e. the user in the group who deals with causing damage.
- Dot = abb. of “damage over time”, continuous damage. Debuff = (n.) is the opposite of Buff, i.e. a spell that removes any increased statistics.
- Dkp = (n.) is a scoring system developed by MMOG players, used above all by guilds to distribute any loot, based on participation and contribution given to the guild. There are different types of Dkp.
- Dupe = abb. of “Duplication”, in this case it is used when you want to copy or duplicate a certain object.
- Exp/xp = abb. of “Experience”, i.e. the experience acquired during the game.
- Farm/Farming = (v.) In the context of MMOGs it indicates the action with which a player accumulates resources/objects within the game. Often the farming process is also considered as a repetition of that process. (E.g. “let's go farm that area”, “then let's farm those monsters”).
- Ftw = abb. of “For the win”, means “for the victory”.
- Gank = (v.) is used to describe when a player has been overwhelmed and killed by a very large and numerous groups. Example: “Man I got ganked by Techs”, in this case it properly means that the player was killed and overwhelmed by the Techs, who can be a guild of players, NPCs or other. GM = abb. by Game Master. This figure is used by employees of

many MMOG companies. This account allows you to have typical developer functions and, therefore, all the powers. This figure has complete control of the game, with the ability to temporarily and permanently ban a player from that game.

- Griefer = (n.) is a title given to players who enjoy ruining other people's games. There are different types of ways you can do this; for example, it is possible that a high level in a certain MMOG will go to areas where there are low level players and start killing them for no reason. Or, in competition, a griefer is someone who goes away from keyboard (AFK) during a competitive game or engages and trolls the game voluntarily.
- Guilds = (n.): groups of people with private access and communications.
- Gtg = abb. of "Got to go" and "good to go", which, depending on the context, mean "I have to go" and "that's fine" respectively.
- Heal = (v.) is used to refer to all healing spells.
- Hot = abb. of "Healing over time". As with Dot spells, Hot is identical but deals with healing rather than damage.
- HP = abb. of "Health Points". It is the scale by which the life of a monster, NPC or any other participant of an MMOG is measured.
- Imho = abb. of "In my humble opinion".
- Inc = abb. of "Incoming", used to describe an imminent attack or danger.
- Iap = abb. of "In app purchase", which refers to micro-transactions.
- Irl = abb. of "In real life".
- Iirc = abb. of "If I remember correctly".
- Instance = sin. dungeons, specific places where you enter in groups of people or individually.
- Jk = abb. of "just kidding".
- Kite = (v.) is used in regard to a game mechanic. It consists of luring a mob behind you, trying to make your companions attack. Often, in this case, the lured mob is unable to keep up with the player, so it is slowed down or prevented from moving, making the target easy prey.
- KoS = abb. of "Kill on Sight"; is used when there are problems with other factions or enemies within the game.
- KS = abb. of "Kill Stealing", it means stealing the killing from someone. For example, if a player fired 10 bullets and did not kill his opponent, he will certainly have left him with little health. The kill stealer is the one who arrives later and thanks to the Last Hit kills the enemy. As a result, the user who was denied the kill will say that that was a KS.

- LD = abb. of “Link Dead”, generally used for players who have disconnected due to lag or connection.
- LFG = abb. of “Looking For a Group”, used to find other players.
- LFM = abb. of “Looking ForMore” or “looking for members”, depending on the context.
- LFT = abb. of “Looking For a Team”.
- LOM = abb. of “Low On Mana”, used when players are in a shortage of mana, which is used to be able to use abilities.
- LOS = abb. of “Line Of Sight”, also used for FPS, often indicates the range in which a certain ability can be used. Also used to see if it is possible to attack with a specific ability and you have a free or obstructed visible field.
- Loot = (n.) is the drop that is left by mobs when they are defeated. Medding/Med = (v.) used to describe the situation in which a user is recovering something, which can be health or mana or stamina points. E.g. “wait don't go, I need to med”.
- Mod = abb. of “modification”, it can be used both as a verb and as a noun. In the first case it means that someone is modifying something, while in the second it refers to add-ons from third-party programs that increase or strengthen the game's performance (e.g. macros). In FPS the term "full mod weap" indicates a weapon completely modified and modded for your needs.
- MT = abb. of “Mistell”, used when typos occur.
- Mule = (n.) (possible translation of “mule”) characters usually used in these MMOGs as alts, but which have a different function. While alts are used to retrace the game and do other things, mules are characters that are stationed in points deemed "useful" by the user. For example, to avoid having to travel to different cities, you can place a mule, so as to have everything you need at hand once logged in with that character.
- Nerf = (n.) is a term used by players often in a controversial way. A nerf occurs when the power of something in the game (an item, an ability, etc.) is reduced. Players often request this change or complain after it happens.
- Newbie = syn. noob. Corresponds to a new player in the game or that he is bad at the game.
- Ninja/Ninjaing = The term can be used depending on the different MMOGs, but in general, the term indicates a user who purposely steals loot from other players, even though he doesn't need it. So, if assassins use leather armor in an MMOG, a knight won't have to steal leather armor. If he does so and steals that item from within the group, he is considered a ninja looter.
- Nuke = (n.) describes an ability that deals enormous damage, generally found in wizards.

- Omw = abb. of “On my way”, means “I'm coming”.
- OOC = abb. of “Out OfCombat”, a user/character who has exited combat.
- OOM = abb. of “Out OfMana”, when the character is without mana
- OST = abb. of “Original Soundtrack”, refers to the different MMOG soundtracks.
- Ownz/owned = (adj.) generally used when you completely destroy an opponent in a competition.
- Pat = abb. of “patrol”. In fantasy MMOGs it is possible to have NPCs called pats, who have a precise movement pattern. The usage in the sentence is as follows: “wait for the pat”.
- PK = abb. of “Player Killing”, used to describe a user who kills other players.
- Pker = (n.) is a user who plays with the primary purpose of killing other players.
- Port = abb. of “Teleport” (Ex. Can you take yourself to the city?).
- Power level = loc. it is an unfair practice, where often a high-level player helps low level players, thus making that player grow faster.
- Proc = abb. of “Programmed random occurrence”; it is generally used to describe additional damage or a greater chance of improvement than normal. For example, if you are about to craft a weapon from +4 to +5, hopefully this step will work, so you can go from +4 directly to +6. Or if you have a 20% chance to do critical damage with an ability, hopefully the damage done is 20% greater.
- PUG = abb. of “Pick Up Group”, it is a group of players assembled at that moment for a quest or other objectives.
- Pull = (n.) technique used to start a fight, where a player is expected to make the aggro of the mobs be on him, so as to bring them closer to him and allow his group to attack from a safe side.
- PC = abb. of "Price Check", often used in chat to find out the opinions of the community regarding the price of an object or other.
- PM = abb. of “Private Message”.
- Quest = (n.) mission that a player must complete.
- QQ = used as a direct insult to another player who complains about something in the game or about a defeat.
- Raid = (n.) used to organize assaults on a mob or boss within the game. Regen = abb. of “Regeneration”, the regeneration of something.
- Rekt = is a slang term for the word wrecked, used to describe someone who has been dramatically destroyed (e.g. “you just got Rekt so hard bro”).

- Respec = (see) often in certain Fantasy MMOGs it is possible to use this function, which allows you to reset something, from skills to the entire character, and then return to the starting point, changing some elements.
- Rez = (n.) indicates a resurrection.
- RMT= abb. of “Real Money Trade”; means the sale of virtual currency or items for real currency. In fact, it is also often used as an acronym for Real Money Transfer.
- Roll = (n.) often used for a dice roll, which assigns a random number to a player. The score higher or lower than the agreed one will win the prize. RNG = abb. of "Random number generation", is often used as a synonym for luck.
- Root = (n.) often used to describe an ability that can immobilize the enemy.
- Souldbound = (n.) is a mechanically controlled object, which once acquired can no longer be traded. Only one player will be able to use it for the entire life of the object.
- Spawn = (n.) is intended as a point of birth or departure. Spawn is often considered the point where a boss or a certain mob must spawn, or a point on the map where players spawn.
- Spec = abb. of “Specification”, often in video games it is used to ask and describe which build/skill you have chosen.
- Stun = (n.) is a crowd control, which immobilizes the enemy for a short time. So a stunned enemy is immobilized.
- Tank = 1. (v.) indicates the act with which a player attracts the aggro of a mob towards him and tanks the damage, therefore it is the player in charge of taking the damage from that mob. 2. (n.) is the one who is generally better able to resist blows because he is more robust and therefore has a better constitution.
- Twink = 1. (v.) is the act of giving some currency or a valuable object to nabbis. 2. (n.) is a character who has better gear/equip than he might have if he were to play alone. So, he is often helped and geared by characters who pass him items
- Wipe = (see) means that the entire party or group must die.
- WTB = abb. of “Want ToBuy”.
- WTS = abb. of “Want ToSell”.
- WTT = abb. of “Want ToTrade”.

Jargon GW2 specific: can also be found at this site
https://wiki.guildwars2.com/wiki/Abbreviations#W

- Bag Bag of Loot: 1) A ground item, appearing at a player's feet, containing a defeated enemy's loot in World vs World. 2) A negative term for bad WvW enemies, hinting on the spoils they'll leave, also see previous meaning.
- Bal / Ball Ballista: A siege weapon in World vs World.
- BL Borderlands: Often prefixed with the specific world or color of the Borderlands, e.g. TCBL for Tarnished Coast Borderlands, GBL for Green Borderlands or HBL for Home (your server's current color) Borderlands.
- BS Banner: Slave/Support Warrior with banners.
- BT Boon Thief: Thief with boon build.
- BU Backup: A person to step in and complete a particular task or role, only if the original person in charge can't do it.
- CA Celestial Avatar: The Druid profession mechanic.
- CA Conjured Amalgamate: The first boss in the Mythwright Gambit raid wing.
- Cata Catapult: A siege weapon used in World vs World.
- Cap Capture a point: Fully capture a Capture point, either from neutral or enemy team color to friendly team color. Usually used in Structured PvP.
- CD Cooldown: The time it takes for a skill to be ready to use again. Referred to as Recharge.
- Condition damage per second A build based on condition damage with the main task to deal high damage.
- CF Chest farming: Exploring the Silverwastes with a group of people to collect as many Lost bandit chests as possible.
- CFB Condition Firebrand: Refers to a dps variant for Firebrand.
- Champ Champion: A very difficult enemy, intended for a group, indicated on its portrait by a gold outline with crossed swords.
- ChronoChronomancer: The mesmer elite specialization in Heart of Thorns.
- Claw / Jormag Claw of Jormag: One of the many champions of Jormag in Frostgorge Sound that spawns a Dragon Chest upon its defeat.
- CM Caudecus's Manor: A dungeon in Queensdale.
- CoE Crucible of Eternity: A dungeon in Mount Maelstrom.
- CoF Citadel of Flame: A dungeon in Fireheart Rise.

- Com / Comm / Commi / Cmdr Commander: See also Tag / Taco / Pin / Dorito.
- Condi Condition: Damage over time or control effect.
- CoZ Champion of Zommoros: Refers to the title gained from completing all achievements in the Mythwright Gambit raid wing, also known as Regulars on the Tour.
- CPS Condition Phalanx Strength: A warrior build that shares might and deals condition damage.
- CQB / CQFB Condition Firebrand: A Guardian build that shares quickness and deals condition damage. See also CFB and QB.
- CS Cursed Shore: Refers to a champion and event farm with a designated commander in Cursed Shore.
- CS / Split Continuum Split: Refers to the Chronomancer profession mechanic Continuum Split.
- DD Damage Dealer: The role describing a person focusing on dealing damage.
- DD / DAR Daredevil: The thief elite specialization in Heart of Thorns.
- DD Demon's Demise: Refers to the title gained by completing the achievement The Real Raiders of Tyria.
- DE / DED Deadeye: The thief elite specialization in Path of Fire.
- DF Dragonfall: A zone in Path of Fire, part of the Living World Season 4 episodes
- DecapDecapture a point: Neutralize an enemy Capture point but leave it at neutral without being fully captured. Usually used in Structured PvP.
- DH Dragonhunter: The guardian elite specialization in Heart of Thorns.
- Disc Discord:AVoip program for communication.
- DoDDefier of Doubt: Title awarded after successfully completing the Challenge Mode in Sunqua Peak Fractal. Used in Fractals of the Mists Looking For Group to demand that the player has this title.
- Additionally, a group may look for DPS players, which means they are looking for players whose primary group role is dealing direct damage to the enemy.
- DR Diminishing returns: Anti-farm code implemented to prevent bots and exploits from disrupting the economy and gaining an unfair advantage over legitimate players.
- DR Divinity's Reach: The human capital city in Kryta.
- DRM Dragon Response:MissionDestroyer fighting instanced mini-missions released as part of The Icebrood Saga chapter 5, Champions.
- DS Death Shroud: Refers to the necromancers profession mechanic.

- DS Dragon's Stand: Refers to the explorable zone in the Maguuma Jungle and its respective meta event.
- DSD Deep sea dragon: The Deep sea dragon's official name is currently not known, so players have invented a variety of nicknames for it. See Common terms for others.
- DT Dry Top: A high-level zone found in Maguuma Wastes, accessed through BrisbanWildlands.
- DwD Dances with Demons: Title given upon completing Sunqua Peak Fractal on Challenge Mode with no members of your party dying.
- EA Empower Allies: A Warrior Master trait in the Tactics line.
- EB / EBg Eternal Battlegrounds: The central map in World vs World. Location of Stonemist Castle.
- Ecto Glob of Ectoplasm: A max-level crafting material, only acquired by salvaging rare or better level 68+ items.
- EleElementalist: One of the eight core professions which wears light armor.
- Engi Engineer: One of the eight core professions which wears medium armor.
- EoD End of Dragons: Referring to the third Guild Wars 2 expansion, End of Dragons.
- EotM Edge of the Mists: A sort of overflow map for World vs World. Events grant rewards and achievements but do not count toward the Mist War score.
- EotN Eye of the North: An upgradable base for The Icebrood Saga living story arc.
- EXP Experienced: Often seen in LFG (such as fractals) where a group wants an experienced player who knows the fractal.
- F&P / P+F Fractal Potion & Food: Often found in the LFG when looking for fractals or dungeons. Players in this group are expected to use potions and food for their run.
- FA Fresh Air: An Elementalist trait.
- FB Firebrand: The guardian elite specialization in Path of Fire.
- FGS: Fiery GreatswordAnElementalist elite skill.
- FotM / Fractals / Fracs: Fractals of the Mists A dungeon in Lion's Arch.
- FC Full Clear: Commonly seen in the raid lfg when people want to clear an entire raid wing.
- Frogs Kill Cotoni and Huetzi: Refers to the event in Verdant Brink during Night and the Enemy.
- Gar / Garri Garrison: The large central keep in a World vs World borderland.
- GH Guild hall: Guild halls are areas designed for guilds.

- GH Mordant Crescent Great Hall: Refers to the Sunspear Uprising meta event in the Domain of Istan.
- GM Guild Mission: Guild activity which members can do together. Rewards the participants with Guild Commendations.
- Golem / Alpha / Omega Siege Golem: A mobile siege weapon in World vs World.
- Gor / GorsGorseval the Multifarious: The second boss in the Spirit Vale raid wing.
- GPH Gold per hour: The amount of gold earned by some farming method if all loot is converted to gold.
- GotL Grace of the Land: A Druid Grandmaster trait.
- GS Greatsword: A two-handed melee weapon used by Warriors, Guardians, Rangers, Mesmers and Reapers.
- GW / GW1 Guild Wars: The original Guild Wars installment. Sometimes inaccurately used to refer to Guild Wars 2, if the 1 is omitted.
- HB / HFB Healbrand / Heal Firebrand: Refers to a support variant for Firebrand.
- HK Hand Kiter: Refers to a specialized role used in the Deimos encounter in Bastion of the Penitent.
- HoloHolosmith: The engineer elite specialization in Path of Fire.
- HoT Heart of Thorns: Referring to the first Guild Wars 2 expansion, Heart of Thorns.
- HotM Heart of the Mists: The main hub for Structured PvP.
- HotWHonor of the Waves: A dungeon in Frostgorge Sound.
- HP Hero Point: A character currency used to progress characters through training skills and traits.
- HS / HSc Heal Scourge: Refers to a support variant for Scourge
- IAS Increased Attack Speed: See Quickness, Dual Wielding, Malicious Sorcery.
- ICD Internal Cooldown: Used mainly for trait and skill systems, and indicate that a particular trait/skill enters an internal cooldown before producing its effect.
- IMS Increased Movement Speed: See Movement Speed.
- Ini / Init Initiative: The skill cost mechanic for thieves.
- IP Internet Protocol: Each instance/shard of every zone in the world has its own unique IP address, which can be determined by typing /ip.
- JP Jumping puzzle: A platforming puzzle with a chest reward at the end.
- KC Keep Construct: The third encounter in the Stronghold of the Faithful raid wing.

- KP Kill proof: Often used in high level fractal and raid LFGs; usually items unique to the content, such as a decoration token or unique gear.
- LA Lion's Arch: One of Tyria's cities, which connects all other major cities together.
- Lab / Laby Mad King's Labyrinth: Refers to the map available during the Halloween holiday event, the Mad King's Labyrinth.
- Largos Twin Largos (Nikare and Kenut): The second encounter in the Mythwright Gambit raid wing.
- LB Longbow: A ranged weapon used by Warriors, Rangers and Dragonhunters.
- LD Legendary Divination: Item acquired from bosses in Path of Fire raids, used in the creation of the legendary ring Coalescence.
- LF Life force: Resource pool for Necromancers.
- LFR Looking For: Raid Poster is looking to join a raid.
- LI Legendary Insight: Item acquired from bosses in Heart of Thorns raids, used in the creation of legendary armor.
- LNHB Leaves No Hero Behind: Refers to the title gained from completing the T4 Shattered Observatory CM fractal without a single party member dying. Usually seen/wanted in Fractal LFG's to show a players' experience.
- LS / LW Living World: Refers to the Living World update structure between expansions.
- LT Lieutenant: A "rank" inside a Squad with elevated permissions. Can only be assigned by the squad's Commander.
- Mat Kill the wyvern matriarch: Refers to the event in Verdant Brink during Night and the Enemy.
- Mats Crafting material: Materials used in Crafting.
- Matt Matthias Gabrel The final boss of Salvation Pass.
- Maw The Frozen Maw: The meta event and world boss event in Wayfarer Foothills that takes place every two hours.
- MC Mystic Coin: Refers to Mystic Coins which are often used as an alternative to Coins.
- Meta Meta event: Refers to dynamic events that take place in a certain map.
- Meta Metagame: The most appropriate builds of the moment. Simply put, it refers to the most effective group composition and specializations of the classes making up that group.
- MF Magic Find: Attribute that increases chance of higher-quality loot from defeated foes.
- MF / Forge Mystic Forge: An interactive object in certain places around Tyria and the Mists used to acquire and gamble with various recipes.

- MO Mursaat: Overseer 2nd boss of the Bastion of the Penitent raid wing.
- MO Mike O'Brien: Co-founder and former president of ArenaNet.
- MP Mastery point: An endgame progression element available in any one of the expansions.
- MS Meteor Shower:Elementalist fire staff skill with a large radius and long recharge.
- Necro Necromancer: One of the eight core professions which wears light armor.
- Node Resource node: A gathering location to mine, harvest, or chop to acquire ore, cooking materials, or wood.
- Obby / Obsi / Obi Obsidian Shards: A rare crafting material which is needed for Ascended equipment and Legendary weapons.
- OOC Out of Combat: Mainly used so party members can heal or teleport/revive at a waypoint.
- OP / Op Overpowered: Used to describe something too powerful.
- Pala Palawadan, Jewel of Istan: Meta event in the Domain of Istan.
- Pat Kill the Wyvern Patriarch: Refers to the event in Verdant Brink during Night and the Enemy.
- PBAoE Point Blank Area of Effect: Refers to area of effect attacks that are centeredaround the player, sometimes referred to as player-based area of effect.
- PHIW Play How I Want: A tag for groups where players are not required to run (popular) meta classes. (see meta)
- PI Perfect Inscriptions: A Guardian Grandmaster trait that improves their Signets and share the passive effects with their team.
- PoF Path of Fire: Referring to the second Guild Wars 2 expansion, Path of Fire.
- PoI Point of interest: The points of interest (little squares) that are required for map completion. Alternatively, a former show about the game.
- Port Portal Entre: A mesmer skill which is used to teleport people from one place to another nearby.
- Pot Potion: A consumable which grants effects that are helpful against specific type of NPC enemy.
- PPK Points Per Kill: Points awarded towards war score per enemy players killed in World vs World.
- PPT Points Per Tick: Points awarded towards war score every 5 minutes for locations controlled in World vs World.

- Pre-event: Events that are part of an event chain and lead to a particular, sought after event. Pre is rarely used for precursor weapons.
- PS Phalanx Strength: A build-defining Warrior Grandmaster trait in the Tactics line.
- PU Prismatic Understanding: A build-defining Mesmer Grandmaster trait in the Chaos line.
- PvD / PvDoor: Player versus Door Players attacking gates with their weapon skills in World versus World to break them faster.
- PvX Player versus anything: A PvX player is a player who enjoys doing both PvE and PvP. Similarly, a PvX guild is a guild which does both PvE and PvP.
- QB / QFB Quickness Firebrand: Refers to a support and dps hybrid variant for Firebrand.
- QQ / Rage / Salt Crying / Lashing out: Used for pointing out sore losers or players complaining about events, battles or teammates.
- QtP / Q2 / Qadim2 Qadim the Peerless: The third boss of The Key of Ahdashim raid wing.
- r / r? ready Used in chat for ready checks, on occasions where the game does not provide a built-in ready tool.
- Rec / Recs Recommended Fractals: Refers to a set of daily fractal achievements.
- Ren Renegade: Refers to the Path of Fire elite specialization for the Revenant profession.
- Rep Represent Representing a guild.
- Rev Revenant: A profession introduced in and available by owning Heart of Thorns.
- Rez / Res Revival: Refers to the act of reviving a player from downed or defeated state.
- RI Righteous Indignation:AnWvW NPC effect that grants invulnerability against damage of all sources and provides a significant damage boost.
- RI Righteous Instincts: A Guardian Grandmaster trait that significantly increases critical chance and generates might. Used in opposition to Perfect Inscriptions. See also PI.
- RIBA Red-Indigo-Blue-Amber: A casual-oriented Silverwastes event farming method referring to the order of event-tagging.
- River River of Souls: The second encounter in the Hall of Chains raid wing.
- RLF Raid looking for: Poster is looking to fill specific spots in an already mostly complete raid group.
- Rota, rot Rotation: A sequence of actions performed by players to achieve a desired outcome. Often a skill sequence.
- RP Role Playing: Where players act out their character's attitude, actions and speech within the game setting.

- RR Righteous Rebel: Often used to indicate a variant of a condition Renegade build which will provide alacrity
- SAB Super Adventure Box: An 8-bit platformer inspired mini-game.
- Sab Sabetha the Saboteur: The third boss in the Spirit Vale raid wing.
- Sam Samarog 3rd: boss of the Bastion of the Penitent raid wing.
- SB / Behe Shadow Behemoth: Epic nightmare boss in Queensdale, that appears on a fixed schedule.
- SB Short bow: A ranged weapon used by Rangers, Thieves and Renegades.
- SBr / SPB Spellbreaker: Warrior elite specialization featuring dual daggers, interrupts, and heavy boon removal.
- SlbSoulbeast: Ranger elite specialization featuring mainhand dagger and pet merging.
- SE Sorrow's Embrace: A dungeon in Dredgehaunt Cliffs.
- SH / Desmina Soulless Horror: The first boss in the Hall of Chains raid wing.
- Sloth Slothasor:1st boss of the Forsaken Thicket raid wing.
- SM / SMC:Stonemist Castle The main fort in the Eternal Battlegrounds.
- sPvP: Structured PvPPvP mode which allows competition on an even footing. Available in the Heart of the Mists.
- Stab Stability: Boon that prevents players from being affected by hard crowd control effects.
- Statues /Statues of Grenth: The third encounter in the Hall of Chains raid wing.
- StM Seize the Moment: A Chronomancer major Grandmaster trait that provides quickness for each clone shattered.
- Sup(s) Supply: A currency that allows a player to construct siege, deploy a trap (environmental weapon), or repair a damaged gate or wall.
- SW Silverwastes: Refers to activities in Silverwastes - typically either doing meta events, doing meta bosses, or a Lost Bandit Chest train. Often accompanied with XX%, indicating how far along the map is towards the meta boss events.
- SW Sword Weaver: A Weaver build wielding a sword.
- T T1 / T2 / T3 / T4 Tier #: One of the 4 difficulty tiers in the Fractals of the Mist.
- TA Twilight Arbor: A dungeon in Caledon Forest.
- Tag/Tagging: Refers to the act of dealing an increment of damage or achieving some minimum amount of credit towards a mob kill or objective credit.
- Tarir: Referring to the meta event in Auric Basin which involves the defense of the Exalted city of Tarir.

- TaV Twice as Vicious: The Soulbeast minor Grandmaster trait that increases your damage and condition damage after disabling an ennemy.
- TC Tarnished Coast: A World in North America.
- TC Twisted Castle: An encounter in the Stronghold of the Faithful raid wing.
- TD Tangled Depths: A zone in Heart of Maguuma, part of the Heart of Thorns expansion.
- Teq / Taco Tequatl: The world boss Tequatl the Sunless.
- TIS The Icebrood Saga: Refers to the fifth Living World season.
- TM Treasure Mushroom: Events in HoT maps that have a daily rare chance of rewarding Invisible Boot Box.
- TP Trading Post: An in-game tool for buying and selling loot, accessed by default with O.
- TP Teleport/TP to Friend Portal Entre: Teleport to Friend or skills with similar mechanics.
- Train / KTrain Train: A great amount of players using the strength of numbers to achieve a task with little difficulty.
- Karma: Train (capturing camps/objectives/towers/keeps in WvW or EotM in a cycle to acquire a constant stream of karma, experience, and loot)
- Champion: Train (circling a set amount of places where Champions spawn to kill them efficiently for loot, or swarming an event to make more of them spawn)
- or sometimes Fail: Train (staying at a place farming an event or an event chain that restarts faster or is more lucrative when failed).
- Treb Trebuchet: A siege weapon used in Player vs Player and World vs World.
- Trio Protect the caged prisoners: The 2nd encounter in the Salvation Pass raid wing, which contains 3 individually weaker bosses.
- TT Triple Trouble: Referring to the Three-Headed Wurm world boss.
- UF / UFE: Unstable Fractal Essence Item acquired from completing Nightmare Fractal, Shattered Observatory Fractal, or Sunqua Peak Fractal with challenge mode active.
- UM Unbound Magic: Refers to the Living World Season 3 global map currency Unbound Magic.
- VB Verdant Brink: Refers to the explorable area in the Maguuma Jungle and often its associated meta events.
- VG Vale Guardian: The first boss in the Spirit Vale raid wing.
- VW Vinewrath: Refers to the boss of the meta event that follows The Breach in the Silverwastes.
- Vet Veteran: Refers to a veteran rank NPC, indicated by a bronze border on its portrait.

- VitV Voice in the Void: Refers to the title gained from completing all achievements in the Hall of Chains raid wing, also known as Silencer.
- VM Volatile Magic: Refers to the Living World Season 4 global map currency, Volatile Magic.
- W1 / W2 / ... / W7 Wing #: Commonly seen in the raid lfg to refer to one of the raid wings based on the order released.
- WB World boss: A special kind of event that gives a daily reward at the end of an event chain culminating in the battle against a powerful enemy.
- WP Waypoint: Allows fast-travelling across the map.
- WvW World versus World: A form of Player versus Player that pits three worlds against each other in a weekly match.
- Yak / Dolly Dolyak: An animal in Tyria. Most commonly used to refer to supply caravans in World vs World and The Silverwastes.
- Zerg / (Map-)BlobZerg: Massive group of players. A zerg is any group above 10-15 players, Blobs are generally maxed out squads of 40-50 ppl, or more.
- Zerk / ZerkerBerserker's: A widely-used stat combination improving purely direct damage attributes (power, precision and ferocity), or a character wearing such equipment.