جامعة نايف العربية للعلوم الأمنية
NAIF ARAB UNIVERSITY FOR SECURITY SCIENCES
تأسست ١٩٧٨ Est. 1978

Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

Cybercrimes and Virtual Worlds: A Systematic Literature Review

Curcio Matteo*
Defence Research and Analysis Institute (IRAD),Center for higher defence studies (CASD),Roma,Italy.

CrossMark

Received 26 Sept. 2022; Accepted 07 Nov. 2022; Available Online 05 Dec. 2022

Abstract

With the evolutions of the gaming industry and the increasing number of virtual worlds (e.g., Metaverse), these applications can be an excellent vector to commit cybercrimes. Since this argument is rarely discussed academically, this literature review aims to bring more attention to the topic by assessing the current state of the art and proposing a starting point for future research. The keyword selection process required an in-depth analysis of the terms because "Virtual Worlds" can differ by name, type, and quality, making it more difficult to analyze them. Therefore, specific inclusion/exclusion criteria and a grey literature review were also applied to improve the accuracy and the quality of the results. Findings illustrate that the argument is underestimated, and the lack of knowledge in this academic field created a gap that should be addressed over the years. Therefore, this literature review could be the starting point for future research.

I. Introduction

Digital innovation and the emergence of increasingly complex applications (E.g., Virtual worlds and complex 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 [1]. These numbers along with the evolutions of gaming produced new virtual worlds (see, e.g., Metaverse) that can modify and create new ways of communication. Today, massively multiplayer online games (MMOG) and related applications are standard means of communication between 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 make users completely anonymous and allow them to perpetrate various cybercrimes undetected thanks to their functions.

Scientific literature about the topic is lacking, and the systematic literature review conducted in this research highlights that only ten papers discuss the topic quite superficially. However, even if there are only few academic works of literature, this does not mean that the subject has not been explored; in fact, it is possible to find "classified reports" done by intelligence agencies and released by Edward Snowden [2] that discuss it. Although those reports have no academic relevance, their existence highlights that the problem exists and is extremely complex to investigate. Today, the cyberspace occupied by virtual worlds

Keywords: Cybercrime, MMOG, Virtual Worlds, Games, Systematic Review.

Production and hosting by NAUSS

* Corresponding Author: Curcio Matteo
Email: curmat89@gmail.com

doi: 10.26735/CBBQ4731

likes MMOG and related applications is unknown; every second, millions of undetected communications go through these applications. Vocally or in writing, users worldwide can communicate without barriers and share any content at any moment. Who can control these communications? Who can guarantee that these platforms are not being used to perpetrate cybercrimes? 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. 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.” [2 p. 237]. In particular, as stated by ODNI (Office of the director of national intelligence) [3] 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”. During 2008, Reynard’s focus changed from pattern-based data mining to leveraging expertise in the social science research community to understand MMO behaviors. In April 2009, solicitations for this reoriented Reynard Program were published by IARPA (Intelligence Advanced Research Projects Activity), and more details given as to the intended outcomes of the project. In particular, it would seek “to identify behavioral indicators in VWs [virtual worlds] that are related to the RW [real world] 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” [4]. 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” [2]. In 2021, Gilles de Kerchove, who was the EU counter-terrorism coordinator, stated: “Online video games can be used to propagate extremist ideologies and even prepare attacks, 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, it can be a form of communicating. It’s encrypted. It can also be a way to test attack scenarios.” [5]. Today, those applications remain a question mark; the problem is not well defined and regulated, the issues are not resolved, and the cyberspace of these virtual worlds is still unknown. In this environment, this literature review will be the starting point for conceptualizing the current academic gap for new research projects that want a complete view of this argument.

II. Systematic Literature 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 [6] - [9] 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 a hard endeavour 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[1], a MMO[2],

[1] 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.

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

a digital world[3], a parallel world[4], and many others. Also, investigating such topic, is possible to easily find literature which refers to violence and video games, that is, research which highlights how video games can make people violent: however, this is not the subject of this study. In fact, the topic of this research is related to cybercrimes committed through these platforms (E.g., money laundering in Second Life). 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 of these turned out to be useful 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.

III. Methodology

EBSCOhost was selected as the research database (from previous research[5], this database resulted 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 a variety of names, the keyword selection process has been conducted with an unconventional approach. 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 I (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 = 45.027 results). 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

[3] 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.

[4] 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.

[5] 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.

had an affinity with the topic). The reason to choose the time period (1990-2022) is that prior to 1990, no MMOG or virtual worlds existed.

As presented in Table II, 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.

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, a total of 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.

TABLE I
Keywords

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 II
Results Obtained

	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

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 = 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 Fig. 1 and detailed with the date, author, and a small abstract.

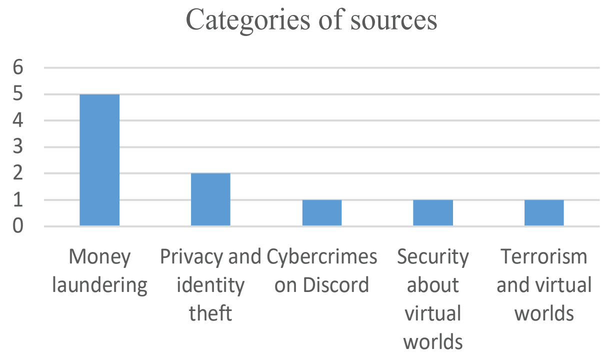


Fig. 1 Categorization.

The papers found are listed below with a brief description:

2004 Identity theft and virtual property. [10]

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

2005 Identity theft and minor crimes. [11]

This paper is similar to the previous one written in 2004, but the crimes discussed are much broader this time. It examines a total of 613 criminal cases 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.

2011 Money laundering. [12]

(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 which explains the risks of these applications by illustrating different examples.

2012 Money laundering. [13]

(Irwin et al., 2012). The purpose of this paper is 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.

2013 Money laundering. [14]

(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.

2014 Money laundering. [15]

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

2015 Affinity to the research topic. [2]

(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 study also includes a thorough analysis of documents that have been uncovered during the years. It offers a comprehensive idea of what problems could arise from these applications and what approach has been taken from intelligence agencies to counter the phenomenon.

2018 Money laundering. [16]

(Chambers-Jones, 2018). Similar to the others that talk about money laundering, this paper analyzes the 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.

2019 Cybercrime app Discord. [17]

(Conway et al., s.d.). 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.

2021 Terrorism and virtual worlds. [18]

(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 does some considerations regarding the Islamic world and their coexistence with these virtual worlds.

IV. 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” [19]. To analyze possible documents that are consistent with the topic, two approaches have been applied:

In the first approach, 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. For the second approach, common research has been done through the internet (Google). In particular: 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".

V. Methodology 1st Approach

Open grey, openAIRE, the FBI vault and the CIA reading room were the chosen research databases. 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 to ensure affinity with the topic, all results were scanned. The findings are illustrated in Table III.

TABLE III
Results Obtained – Grey Review

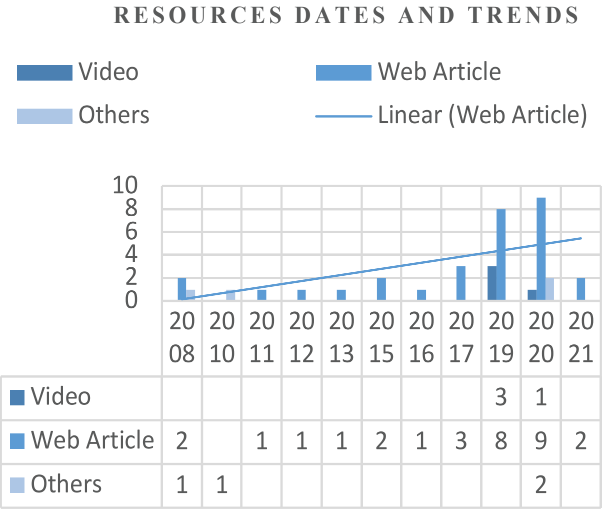
	Open grey	OpenAire	FBI vault	CIA reading room
Video games crime	0	7	0	0
Virtual worlds crime	0	2	0	0
MMOG crime	0	1	0	0
Metaverse crime	0	0	0	0
Online game crime	0	11	0	0
Messaging apps cybercrime	0	0	0	0
Digital world crime	0	17	0	0
Cybercrime video games	0	0	0	0
Virtual worlds cybercrime	0	0	0	0
MMOG 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
MMOG communications crimes	0	0	0	0
Results	**0**	**63**	**0**	**7258**

VI. Methodology 2nd 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 article, 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 dates 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 has occurred. Results obtained with this keyword research were quite a lot, therefore, to reduce the numbers only the primary sources were reported in the results. (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). In Table IV are highlighted the findings. All the sources were also divided by dates and categorization as can be seen in Fig. 2 and Fig. 3.

TABLE IV
Results Obtained – Grey Review

Video	Web Article	Others
4	30	4



	2008	2010	2011	2012	2013	2015	2016	2017	2019	2020	2021
Video									3	1	
Web Article	2		1	1	1	2	1	3	8	9	2
Others	1	1								2	

Fig. 2 Resources by dates and trend.

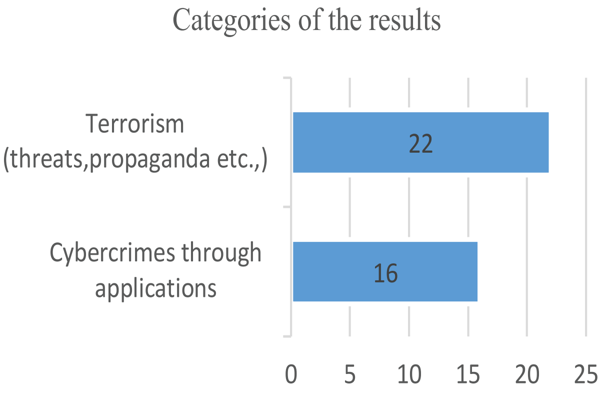


Fig. 3 Categorization of the findings.

TABLE V
MMOG Included vs MMOG not Included in the Keywords

TX	TI	AB	TX	TI	AB
149	0	0	61035	13	309
34	0	0	13352	1	9
18	0	1	116	0	0
39	1	1	1090	0	0
12	0	0	2567	0	1
164	0	2	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

VII. Discussion

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 Table V.

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 Table VI, 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), only twenty-seven 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 ten 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 0,3125 papers per year. If the ten 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 one paper is revealed to be appropriate. The results obtained by this systematic literature review highlight how much this sector is neglected and not studied by academics. This gap in the academic context may become even more significant as virtual worlds develop further. Following this systematic literature review, the grey literature review that was conducted to explore the topic further, highlights different 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 III, 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

TABLE VI
Total Frequency of the Keywords in the Papers

	Papers	%
TX	420629	99.4786
TI	121	0.0287
AB	2083	0.4927
Total	422833	100

VIII. Conclusions

To conclude, the findings of this literature review highlight that in 32 years, only 10 papers have been written about the argument, and the topic has been discussed only superficially. This lack of research leaves behind many questions:

Why have not academics covered the topic? Or why did only a few of them cover a specific issue about the topic superficially? In contrast, why does the "unconventional" grey literature review show the most important results? If the topic has been discussed in “undercover environments”, and local news often talk about it, why is there no public research about the topic?

Given the results of this literature review, it is possible to draw some hypothesis:

-The topic has not been explored due to the lack of knowledge,

-It has been explored in "undercover" environments, and nothing has been published,

-It is hard to develop comprehensive research due to the complexity and lack of studies of these applications,

-There has never been funds and ad-hoc research about the argument by major institutions,

-Many problems keep the argument undiscovered and understudied.

Whatever the correct summary is, the literature review highlights a lack of study regarding the argument in the academic sector which created an impressive gap. With the evolving digitalization and the increasing number of virtual worlds released every year, this systematic literature review raises some concerns about the topic, particularly about the safety of these applications. Since the first virtual world release, nothing has been done to develop knowledge and regulations further. As a result, today, these platforms remain under-regulated, understudied, and unmonitored. The findings demonstrate a considerable gap in the academic field, but that does not involve "unofficial" sources that have proved to be more valuable and accurate. Consequently, if there are only a few scientific papers and it is possible to find different "unofficial" sources that in some way warn about the issue, it reinforces the theory that this argument exists, but academics have not yet explored it. Of course, the reasons could be many, but if the results are further elaborated, it is possible to conclude that a general lack of knowledge of the argument prevented developing further research in this field. According to the FBI Internet Crime Complaint Center (IC3) report on cybercrimes, in 2021 "IC3 continued to receive a record number of complaints from the American public: 847,376 reported complaints, which was a 7% increase from 2020, with potential losses exceeding $6.9 billion. Among the complaints received in 2021, ransomware, business email compromise (BEC) schemes, and the criminal use of cryptocurrency were among the top incidents reported. In 2021, BEC schemes resulted in 19,954 complaints with an adjusted loss of nearly $2.4 billion. [20] The situation pictured above should raise concerns for further research by academics, especially in a field that lacks knowledge but is in continuing evolution (See, e.g., Metaverse). Therefore, editors should encourage more academic research in the field, and practitioners should be more involved in investigating this topic further, even if it is not that easy, given the complexities and difficulties that can be encountered by researching this topic.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] T. Wijman, “Three Billion Players by 2023: Engagement and Revenues Continue to Thrive Across the Global Games Market,” June 25, 2020. [Online]. Available: https://newzoo.com/insights/articles/games-market-engagement-revenues-trends-2020-2023-gaming-report (accessed Sep. 25, 2022).

[2] T. Stevens, “Security and Surveillance in Virtual Worlds: Who Is Watching the Warlocks and Why?,” *Int. Polit. Sociol.*, vol. 9, no. 3, pp. 230–247, Sep. 2015, doi: 10.1111/ips.12094.

[3] US Office of the Director of National Intelligence, “Data Mining Report,” February 15, 2008. [Online]. Available: https://www.fbiic.gov/public/2008/feb/ODNI_Data_Mining_Report.pdf

[4] Intelligence Advanced Research Projects Activity. Broad Agency Announcement?
Reynard Program, IARPA-BAA-09-05, April 21, 2009. [Online]. Available: https://nsarchive.gwu.edu/sites/default/files/documents/3859819/Dr-Rita-Bush-Intelligence-Advanced-Research.pdf

[5] A.-L. Mondesert, “EU anti-terror chief warns video games used to spread extremism, prepare attacks.” Nov. 26, 2020. [Online]. Available: https://www.timesofisrael.com/eu-anti-terror-chief-warns-video-games-used-to-spread-extremism-prepare-attacks/ (accessed Sep. 25, 2022).

[6] D. A. Buchanan and A. Bryman, Eds., *The SAGE handbook of organizational research methods*, LA, USA: SAGE, 2011.

[7] D. J. Cook, “Systematic Reviews: Synthesis of Best Evidence for Clinical Decisions,” *Ann. Intern. Med.*, vol. 126, no. 5, p. 376, Mar. 1997, doi: 10.7326/0003-4819-126-5-199703010-00006.

[8] H. M. Cooper, *Synthesizing research: a guide for literature reviews*, 3rd ed. LA, USA: Sage Publications, 1998.

[9] D. Tranfield, D. Denyer, and P. Smart, "Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review," *Br. J. Manag.*, vol. 14, no. 3, pp. 207–222, Sep. 2003, doi: 10.1111/1467-8551.00375.

[10] Y.-C. Chen, P. Chen, R. Song, and L. Korba, "Online Gaming Crime and Security Issue - Cases and Countermeasures from Taiwan," in *Proc. 2nd Annu. Conf. Priv. Secur. Trust (PST'2004)*, Canada, Oct. 13-15, 2004.

[11] Y. Chen, P. S. Chen, J. Hwang, L. Korba, R. Song, and G. Yee, "An analysis of online gaming crime characteristics," *Internet Res., vol.* 15, no. 3, pp. 246–261, Jul. 2005, doi: 10.1108/10662240510602672.

[12] S. D. Keene, "Emerging threats: financial crime in the virtual world," *J. Money Laund. Control*, vol. 15, no. 1, pp. 25–37, Dec. 2011, doi: 10.1108/13685201211194718.

[13] A. S. M. Irwin, J. Slay, K. Raymond Choo, and L. Liu, "Are the financial transactions conducted inside virtual environments truly anonymous?: An experimental research from an Australian perspective," *J. Money Laund. Control*, vol. 16, no. 1, pp. 6–40, Dec. 2012, doi: 10.1108/13685201311286832.

[14] C. Chambers-Jones, "Virtual world financial crime: legally flawed," *Law Financ. Mark. Rev.*, vol. 7, no. 1, pp. 48–56, Jan. 2013, doi:10.5235/LFMR7.1.48.

[15] A. S.M. Irwin, J. Slay, K.-K. Raymond Choo, and L. Lui, "Money laundering and terrorism financing in virtual environments: a feasibility study," *J. Money Laund. Control*, vol. 17, no. 1, pp. 50–75, Jan. 2014, doi: 10.1108/JMLC-06-2013-0019.

[16] C. Chambers-Jones, "Money Laundering in a Virtual World," in *The Palgrave Handbook of Criminal and Terrorism Financing Law*, C. King, C. Walker, and J. Gurulé, Eds. Cham: Springer International Publishing, 2018, pp. 165–182. doi: 10.1007/978-3-319-64498-18.

[17] M. Conway, R. Scrivens, and L. Macnair, "Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends." Oct. 2019. [Online]. Available: https://icct.nl/app/uploads/2019/11/Right-Wing-Extremists-Persistent-Online-Presence.pdf

[18] D. Trifunović, "Cybersecurity – virtual space as an area for covert terrorist activities of radical islamists," *TEME*, vol. XLV, no. 1, p. 95-109, Apr. 2021, doi: 10.22190/TEME201119006T.

[19] K. Godin, J. Stapleton, S. I. Kirkpatrick, R. M. Hanning, and S. T. Leatherdale, "Applying systematic review search methods to the grey literature: a case study examining guidelines for school-based breakfast programs in Canada," *Syst. Rev.*, vol. 4, no. 1, p. 138, Dec. 2015, doi: 10.1186/s13643-015-0125-0.

[20] L. Mastrangelo, "2021 Internet Crime Report," Mar. 23, 2022. [Online]. Available: https://www.hsdl.org/c/2021-internet-crime-report/ (accessed Sep. 26, 2022).