International Journal of advanced humanities Research" (IJAHR)
Online ISSN: - 2812-5940
https://ijahr.journals.ekb.eg/

Cyberspace and Organized Crime: The New Challenges of the 21st Century

Dr Atif Ali

PMAS Arid Agriculture University,

Rawalpindi, Pakistan

atif.alii@yahoo.com

Abstract
The Occidental Societies are becoming increasingly vulnerable to cybernetic attacks due to their heavy reliance on computer and electronic systems and network fraud. Additionally, the Internet is an easily accessible medium through which any individual, while maintaining their anonymity, can perform a difficult act of linking virtually undetectable and difficult to smuggle, let alone achieve high-impact, striking directly and surprising the adversary. Therefore, the network is becoming "that ideal place" for delinquents and terrorists to carry out their official actions and activities. Although they have taken their battle to cyberspace, so have states beginning to employ this means to attack their enemies. Hence, cybercrime, cyber terrorism, and cyber warfare have become three major threats that seem to haunt Western societies. Therefore, in this article, we discussed the use of the network, terrorists, criminals, and the security of states, and the measures taken to avoid these attacks and activities crime as far as possible.

Keywords— cyber terrorism, cybercrime, cyber war, cyber-attacks, Internet, network, and web.

Introduction

Information and Communication Technology (ICT) is generating an unprecedented revolution since cyberspace is becoming a meeting point for millions of people, thanks to its flexibility in use and a large amount of information that is being made available to netizens. Undoubtedly, this contributes to the fact that the network is reaching an enormous repercussion, to the point that there are already many who dare to affirm that its appearance has marked a before and after in the era of information and communication. What's more, today, everything seems to be interconnected: security, defense, commercial, energy, health, communication, transportation, banking, lighting systems, librarians, etc. [1] in such a way that we are facing a hyper connected world, where the network is a crucial element for the most advanced societies, although, in reality, it is for all those who have joined the train of the digital age. In any case, we are projecting our work online; But not everything is positive since cyberspace also favors the emergence of new problems and threats that will have to be faced. So much so that it is becoming more and more frequent for news to come to light about some illicit activity that has occurred on the Internet. The point is that the true scope of the problem has not yet been assessed. Many consider that a cyber-attack is something related to science fiction or reserved for action movies. The reality seems to be quite another. Although up to now there has been no action that has seriously affected the systems or institutions of any country, there is no doubt that we can all be victims to the extent that we carry out some usual activity, such as buying goods in supermarkets that set their prices in barcodes, that is, electronically, we use telephones with electronic cards, we use the Internet, etc., and what is more serious, we may not know it. For this reason, in this article, we have decided to analyze what activities criminals and terrorists are carrying out in cyberspace to determine if they will pose a new challenge to society and what measures are being taken to counteract these new dangers [2].

Related Work

What is Cybercrime and Cyber terrorism?

Cybercrime encompasses a variety of economic crimes, including computer fraud, theft, counterfeiting, computer hacking, computer espionage, sabotage, computer extortion, commercial piracy and other intellectual property crimes, invasion of privacy, distribution of illegal and harmful content, incitement to prostitution, and other morally reprehensible attitudes, and organized crime. Unlike other types of crime, cyber-crime uses cyberspace to carry out its criminal activities. Thus, cybercrime can be understood as those criminal activities carried out with the help of communication networks and electronic information systems or against such networks and systems.

By contrast, cyber terrorism is distinct from cybercrime, although some believe the two are synonymous. They undoubtedly have a connection, as cyber terrorists frequently commit criminal acts on the Internet, but their motivations and desired outcomes are quite different. Cyber terrorism is the fusion of cyberspace and terrorism, defined as "the way terrorism uses information technologies to intimidate, coerce, or harm social groups for political or religious purposes." Thus, evolution occurs due to substituting weapons, bombs, and missiles for a computer capable of planning and executing attacks that cause the greatest damage to the civilian population [3].

Passive use of the Internet by terrorist groups

There has not yet been a cyber-attack that has caused great damage or human losses, that is, none that can induce us to proclaim the start of a cyber-terrorist attack, since so far, only traces of visits or attempts to access strategic infrastructures, but without major consequences. Computer attacks have been limited, in most cases, to collapse the website services of institutions or companies, disable communication systems (e.g., Gulf War, 1991), counter-reporting, or stealing information (e.g., USA, 2009). As a result, we can say that they have been passive network users up to this point [4].

The use of the network by terrorist groups

Terrorist groups mainly use the network to finance themselves, recruit new members, train the different cells, communicate, coordinate and carry out actions, find information, ideologically indoctrinate, promote their organizations and develop a psycho-warfare. The logic against the enemy (Weimann, 2004a) [5].

a) Financing

Terrorist groups are using the network, like other organizations, to finance themselves. In it, they have found a new means of raising funds for the cause. For this reason, terrorists are using their web pages to solicit donations from their supporters. For example, the website of the Irish Republican Army (IRA) contained a page where visitors could do donations with their credit cards; Hamas has raised money through the website of a Texas-based charity, the Holy Land Foundation for Aid; Chechen terrorists have published online the number of bank accounts in which their supporters could make their contributions. But they are also using the Internet to extort money from financial groups, transfer money, make financial transfers through offshore banks, la-var and steal money, use electronic money (cyber cash) and smart cards (smart cards), make sales. Fake products, or perpetuate different scams through spam emails, etc. [6].

b) Psychological warfare

Cyberspace is being used to conduct what is referred to as "psychological warfare." Numerous examples exist of how they use this uncensored medium to disseminate false information, threaten, or distribute images of their attacks. Videos of hostages being tortured, pleaded with, and murdered, such as Americans Nicholas Berg, Eugene Armstrong, Jack Hensley, British Kenneth Bigley, Margaret Hassan, or South Korean Kim Sun Il, have done nothing but reinforce Western societies' sense of helplessness [7]. Thus, the groups can project an internal image of vitality, strength, and determination, and their messages have a global reach. Simultaneously, they have devoted themselves to disseminating images, texts, and videos about the attacks Muslims face in the hope of inciting rebellion and armed struggle, attempting to achieve referred to as "delegated frustration," that is, rebellion against injustice suffered by others, but also to boost the morale of the comb. This is intended to undermine the US and its allies' morale and foster a sense of vulnerability in these societies [8].

c) Recruitment

The network is used to recruit members, just as some individuals use it for advertising their services. To begin, just as "commercial headquarters track visitors to their websites to create consumer profiles," terrorist organizations collect information about users who visit their headquarters. Then they contact those who appear to be the most enthusiastic about the organization or the most qualified to work there"; second because terrorist organizations maintain websites that detail how to carry out Jihad. Thirdly, those responsible for recruiting members frequently visit Internet cafes and chat rooms searching for young people interested in joining the cause. Fourth, the network enables many people to self-identify as terrorists. While it is true that the vast majority of recruitment occurs through friendship and personal treatment, jihadist circles recognize that the Internet facilitates this work as well [9].

d) Interconnection and communication

Furthermore, the Internet is providing them with cheap and efficient means of interconnection. Through the network, terrorist leaders can maintain relationships with members of the organization or another without physically meeting. So much so that messages via email have become the main communication tool between factions scattered worldwide. However, it should be mentioned that terrorist groups use very different techniques to avoid the interception of their messages, among which the stenography should be highlighted.2, encryption3 and the red traffic lights4. But they also hang messages on the private corporate server of a predetermined company for operatives/receivers to retrieve and then delete the

Communiqué without leaving any trace; or manipulate electronic pages of private companies or international organizations to create attached files with propaganda, or hide data or images on websites with pornographic content. Although among all the methods they use, the most creative is establishing communications through email accounts with user names and shares passwords. Thus, the terrorists communicate the keys through drafts, messages, or drafts once the keys have been agreed upon. The form of communication is simple. The sender writes a message in that account and does not send it but files it in the draft, and the recipient, which may be in another part of the world, opens the message, reads it, and destroys it, preventing it from being intercepted. Access to mailboxes is done from public Internet cafes, so it is impossible to know who has accessed a specific computer [4, 5].

e) Coordination and execution of actions

But terrorists not only use the network to communicate but also to coordinate and carry out their actions. Coordination is achieved through fluid communication through the Internet, and the execution may imply from an attack destructive enough to generate a fear comparable to that of physical acts of terrorism or any other action that affects the population differently, but that they are just as effective, as can be the mass sending of emails or the spread of a virus throughout the network. Such is the attraction it presents to terrorists that it has even been said that terrorists had a training ground in different countries intended solely for the training of operational members in matters of penetration of computer systems and cyber warfare techniques [10].

f) Source of information and training

Another role that the Internet plays in terrorism is being an inexhaustible source of documentation. The network alone offers nearly a billion pages of information, much of it free and of great interest to terrorist groups, since they can learn a variety of details about their possible targets (maps, schedules, precise details about its operation, photographs, virtual visits, etc.), the creation of weapons and bombs, action strategies, etc.

g) Propaganda and indoctrination

The Internet significantly expands the window of opportunity for groups to advertise as much as they want, as, before the Internet, hopes for publicity for their causes and actions were contingent on gaining the media's attention. Additionally, the fact that many terrorists have direct control over the content of their messages creates new opportunities for them to shape their own and their adversaries' perceptions. As a result, propaganda from groups labeled as "terrorists" has become widespread

on the Internet. The Irish Republican Army (IRA), the Colombian National Liberation Army (ELN), the Revolutionary Armed Forces of Colombia (Farc), the Shining Path, Hezbollah, and even the Ku Klux Klan all have websites on the network. However, in addition to official pages, terrorist groups are using forums to express their views publicly and thus interact with other website visitors [11]. Prominent members of terrorist organizations frequently register in these forums, and to avoid the inconveniences associated with their official websites' "instability," they use these platforms to publish new communications and links to new materials. As a result, these forums are frequently subject to a variety of "security" measures. For instance, it is common to locate input passwords to avoid overloading them. The network's presence of criminals and criminals Cybercrime is the fraudulent use of the Internet to obtain money, block web pages for political purposes, and spread malware, among other things.

Obtain money fraudulently

Perhaps the most common online scams are mail spoofing and web spoofing. The first is a procedure through which it is intended to impersonate a user's email or create supposedly true emails from a domain to send messages as if they were part of that identity. For example, it is increasingly common to find in our emails messages from banking entities, which have an electronic mail address that We usually identify with: name@bbva.es or name@cam.org.In these messages, the presumed clients usually receive the following information: "This message was sent automatically by our server to verify their email address. To validate your email address, please click on the link below". In this way, they obtain your email address and data, but it is also common for mail spoofing to be used as a social engineering ploy to request the number of credit cards from certain unsuspecting users who think that the origin of the message is supposedly derived from the very company of which they are customers [7].

Another phenomenon related to this aspect would be cyber squatters, individuals or companies that register domains associated with brands, companies, or institutions to profit by reselling them to their rightful owner. Another issue is phone calls, a fraud between the computer's modem and the Internet provider. This process is usually carried out through a local node so that the telephone rate to pay corresponds to a local call. Hence, the fraud inadvertently diverts the call from the local node to other, much more expensive commercial prefixes. Another issue is cyber sex, one of the most profitable businesses on the Internet since the freedom of access and the supposed anonymity contribute to this fact. Sex on the Internet is not penalized as long as it complies with all legal requirements. The problem is that this becomes illegal when we refer to child pornography or the sale of sex without consent through the Internet, or when customers are deceived into believing that

access to the contents of their pages is free when they are a fee-two for a high-cost line [12].

Another place frequented by cybercriminals is the sub-bass portals, from which a wide assortment of products and services is offered. The problem is that in most cases, these products can be fake or, a buyer purchases them, but they are never delivered, that is, paying without receiving anything in return. On other occasions, the purchase of products is made with fake cards, and then the products are sold at very low prices, with which the benefits are very high. This fraud dynamic requires a structure capable of obtaining cards for purchases, infrastructure for receiving products, and subsequent sales channels for objects originating from fraud; that is, a minimum organizational structure. The sale of pharmaceutical products is another permissible space for fraud. In Pakistan, the marketing of drugs is prohibited over the Internet; however, it is becoming more and more frequent to go to this medium to obtain a series of products that can only be acquired under medical pre-registration. But cybercriminals are also using the Internet to sell narcotics and create real thematic markets on drugs with very diverse information; provide, under a price, information on all kinds of illegal activities such as the weaknesses of alarm and anti-theft systems, tricks on how to open a car, break into a house, circumvent security systems, etc.; offering to enter the systems or computers of companies or institutions to steal, manipulate or damage data in exchange for money; steal information and then sell it to the highest bidder; create forums dedicated exclusively to the purchase/sale of stolen data, such as credit card numbers and other elements related to fraud, to mention a few cases [13].

i) Block web pages

It consists of entering the websites of institutions, organizations, companies, or governments to paralyze them for a certain time to generate chaos, confusion, and uncertainty. Perhaps the best known was the one carried out by Estonia on April 27, 2007, when the official pages of several Estonian departments, those of the Government and those of the ruling Reform Party, were paralyzed by computer attacks from abroad. At the same time, the systems of some banks and newspapers were blocked for several hours by a series of Distributed Denial of Service (DDoS) attacks. A similar event occurred just after Russia pressured Estonia to withdraw from the streets of Tallinn, a monument from Soviet times. Hence, the Estonians will accuse the Russian Government of being behind these attacks, although the Kremlin always denied its involvement in the matter. But also those that occurred during the war between Russia and Georgia. They had the consequence that different pages government websites were compromised, with continuous denial of service attacks distributed against other government pages, resulting in the migration of certain sites to posting services in the United States, even a group of pro-Russian cyber

activists provided help on their official page to empower Internet users with tools to perform distributed denial of service attacks, provide a list of Georgian pages vulnerable to SQL injection, and publish a list of Georgian politicians' email addresses for targeted attacks and spam5 [11].

***j) Spread* malware**

The amount of malware and the evolution of its infection and propagation techniques have increased considerably in recent years. Let's not forget that when we talk about malware, we can refer to a virus, a Trojan horse, a backdoor, spyware, or a worm. In addition, other attacks can be derived from malware, such as Distributed Denial of Service (DDoS), distribution of spam email, the spread of viruses and worms to other networks, phishing sites, expansion of botnets (networks of compromised teams), electronic banking, pharming, and driving fraud, among many others (Fuentes, 2008: 4). The solution has been antivirus, but in the face of them, hackers develop more and more and more complex viruses, some practically undetectable, like rootkits. This has created an endless spiral of action-reaction between hackers and software companies [9, 11].

k) Launder money

The typology of mules is very diverse and has undergone a significant evolution. In the beginning, the organized gangs were sent to the different countries where they operated, gang personnel with various false identities and with each of them and in different entities and branches, they opened bank accounts to receive the money of their victims. Subsequently, they transferred gang members to mule catchers, among natural immigrants from the countries where the head of the organized gang was located. The captors were dedicated to offering certain profits to those who were willing to collaborate. In addition, they were given the necessary instructions, including to face police action, with credible alibis, such as receiving income from inheritances from friends of their country, remitted to avoid the fiscal action of your Government, or income from marital separations of friends to avoid control of the spouse. Mules linked to the world of drugs were willing to offer their accounts for the meager earnings that would allow them to acquire new doses of drugs [10].

Nowadays, without neglecting these procedures, they have opted for deception. This consists of sending emails to many users proposing a financial collaboration for a company operating in the country. The earnings will be a percentage based on what you receive in your account, and they ensure that you can earn amounts up to € 3,000 with exclusive dedication. The coverage of the companies is very diverse, and many of them credible, such as the case of the marriage agency of women from eastern countries, who move to the country of the "mule," and when they get married, the alleged spouse pays services through income to the financial partner or

mule. Such is the activity of capturing mules through deception techniques, that has been created around him networks of criminals specialized in the subject, capable of designing deceptions, accompanied by the necessary technological infrastructure, such as web pages simulating companies or legal businesses, capable of obtaining lists of users who attend, contributing their CVs, to job portals, and capable of launching campaigns aimed at these users selected for deception, that the mule recruitment function is also beginning to be offered as a service for the world of organized crime [7]. In any case, the function of the mule is none other than to receive the money from the fraud in your checking account and send it, prior communication, via a money transfer company, to a third recipient. Such as web pages simulating companies or legal businesses, capable of obtaining lists of users who attend, contributing their resumes, to job portals, and capable of launching campaigns directed at these users selected for deception, that the function of attracting mules, it is also being offered as a service to the world of organized crime. In any case, the function of the mule is none other than to receive the money from the fraud in your checking account and send it, prior communication, via a money transfer company, to a third recipient. Such as web pages simulating companies or legal businesses, capable of obtaining lists of users who attend, contributing their resumes, to job portals, and capable of launching campaigns directed at these users selected for deception, that the function of attracting mules, it is also being offered as a service to the world of organized crime. In any case, the function of the mule is none other than to receive the money from the fraud in your checking account and send it, prior communication, via a money transfer company, to a third recipient. that the function of recruiting mules is also beginning to be offered as a service for the world of organized crime. In any case, the function of the mule is none other than to receive the money from the fraud in your checking account and send it, prior communication, via a money transfer company, to a third recipient. that the function of recruiting mules is also beginning to be offered as a service for the world of organized crime. In any case, the function of the mule is none other than to receive the money from the fraud in your checking account and send it, prior communication, via a money transfer company, to a third recipient [10, 12].

How to try to reduce the dangers of the network?

It is proving extremely difficult to find effective solutions to stop all those activities related to cyber terrorism and cybercrime. The first solution would be to disconnect the computer from the network, although this seems impossible in the face of societies that have become more and more hyper connected. The second is to identify the vulnerabilities and identify the existing and potential dangers that these weaknesses allow. This can only be achieved with cyber intelligence6. The problem that arises is that the Internet has no borders and illegal content circulates from one

country to another in milliseconds; In addition, there is little or no regulation of cybercafés, phone booths, public computer rooms, libraries, educational centers, popular Internet access machines and others where, anonymously, people can connect and carry out illegal activities. The same occurs with free wireless networks within reach of computers with connections capable of connecting to those networks with the anonymity of no belonging to the authorized group. But these are not the only difficulties police officers face when conducting investigations online. For example, when potential criminals know that a machine is compromised because it is accessible through a connection, they can turn it into a virtual work station to navigate through its address without being detected; or when they use the cache machines of some communication providers to optimize their performance since they guarantee the anonymity of users to commit crimes [13].

The problem is that most of the laws aim to protect the improper use of the network; some even foresee the creation of specialized bodies that protect the rights of citizens, but little else. However, to avoid these possible legal deficiencies, they classify a large number and variety of computer crimes. Now the Convention on Cybercrime has contents of diverse nature, such as, for example. These intrusion crimes include criminal offenses against the confidentiality, integrity, and availability of data and computer systems, patrimonial crimes (falsifications and fraud via the Internet such as phishing and pharming) [12].

The third possible solution is to provide yourself with means of security, although always considering that there is the possibility that they will be violated. The fourth solution is to get ahead of any criminal act by controlling information systems such as Echelon, Enfopol, Carnivore, and the Dark Web. The first was created in the 1970s by the US but was later joined by Great Britain, Canada, Australia, and New Zealand. Its initial objective was to control the military and diplomatic communications of the Soviet Union and its allies. But at present, it is being used to locate terrorist plots and drug trafficking plans, political and diplomatic intelligence. Its operation involves locating innumerable electronic interception stations on satellites and other points to capture the communications established by radio, satellite, microwaves, mobile telephones, and fiber optics. These received signals are then processed by a series of supercomputers called "Dictionaries" and have been programmed to search for specific patterns in each communication, be they addresses, words, or even verifications. This project aims to detect certain words considered "dangerous" for the United States' national security or the countries participating in the project. The problem the program is facing is information saturation; for its part, "Enfopol is the European version of a communications control system. It is trying to impose its rules on all European fixed and mobile telephony operators so that the European secret police have full access to their clients' communications and information on the numbers dialed and the numbers from which they can be reached.

Calls, all without the need for a court order" . In the case of the Internet, "providers must provide" a back door "so that they can penetrate freely through private systems, "But it is still more demanding for crypto. It is requested that only this type of service be allowed as long as it is regulated by a "trusted third party," which must automatically deliver when requested: the complete identification of the user of a password,

The third is a system that has been designed by the Federal Bureau of Investigation (FBI) to capture those email messages that are suspected of containing useful information for the agency. It is even speculated that it can spy on the user's hard drive who is considered suspicious and, without leaving a trace of its activity. For this, a chip is placed in the computers of Internet service providers to control all electronic communications that take place through them; so when it finds a suspicious word, it reviews all the email data that circulates through that person's computer, tracks the visits they make to web sites and the chat sessions in which they participate. This, together with the control of IP addresses and connecting phones,

The fourth is a project developed by the University of Arizona's Artificial Intelligence Laboratory that employs techniques such as "spiders" and analysis of links, content, authorship, opinions, and multimedia to locate, catalog, and analyze extremist activity online. The Write print, one of the tools developed in this project, automatically extracts thousands of multilingual, structural, and semantic features to determine who creates "anonymous" content online [14]. To the extent that you can examine a comment posted on an Internet forum and compare it to other writings found on the network, and additionally, by analyzing these characteristics, you can determine with greater than 95% accuracy if the author has previously produced others. As a result,8. However, the Dark Web also employs sophisticated page-tracking software and thread spiders to discuss search and other content and locate hotspots for terrorist activity on the Internet.

The fifth possible solution is the establishment of government agencies designed to combat potential cyber-attacks. In this sense, it should be mentioned that many governments are creating Information Security Offices to combat cybercrime, cyber terrorism, and cyber war legally. For example, Germany has just created the Federal Office for Information Technology Security (BSI), which will become a kind of data surveillance center for government agencies; Japan has formed an anti-terrorist team made up of some 30 computer specialists and a person in charge of the Government Security Office [15].

The sixth solution is the proposal made by some American researchers to create Internet 2. A separate network from the commercial Internet, linking laboratories and universities worldwide and developing systems for transmitting the information at large speeds and through fiber optics (Sánchez Medero, 2009)9. But unlike the

commercial Internet, Internet 2 will be highly regulated, and a Federal Communications Commission or the Government itself will accept only "appropriate content." In addition, the guidelines and proposals being made by both the EU and the US for data retention will allow absolute regulation of the network (Waston, 2007). In this way, Internet 2 will not escape government control and, therefore, be less permissible for criminal actions [16].

How are all these actors preparing to carry out their actions in cyberspace?

Directed their actions. There is no doubt that all these actors are preparing to increase their presence on the Internet since it is a medium that provides them with superior advantages over the traditional ones. Thus, more and more criminals are becoming familiar with this new technique and are transferring their activities to cyberspace. Terrorist groups and cybercriminals are turning to former communist ideology countries or countries like Pakistan or India to hire computer experts who are seduced by those who can pay for their services at a good price, regardless of the purposes for which they are. At the same time, they are trying to get their members to adapt to using the tools of the digital world since their organizations and activities are being transferred to a large extent to the network. They all have been endowed with a team of people dedicated solely to thinking and finding a way to continue perpetuating and carrying out new attacks, newer and more difficult to counter [17].

Discussion

In today's cybercrime era, hackers hacking computers for fun or fame is no longer the norm. The rise of the digital economy has changed the criminal landscape. Organized crime groups are increasingly focusing on lucrative and risk-free cyberspace operations rather than traditional criminal activities. On the other hand, new types of criminal networks dedicated solely to e-crime have already emerged.

Online criminal networks often consist of multi-skilled, multi-faceted criminals. These gangs are not structured like traditional gangs. These networks are formed "stand-alone" because members rarely meet in person and lack virtual communication with other colleagues. In addition to the complex structure, close allies only have access to core operations, making it difficult to detect and infiltrate organized cybercrime groups.

The networks may have tens to several thousand members and may be linked. Any virtual criminal network is typically run by a small group of skilled online criminals who don't commit crimes but act as entrepreneurs. The network's top members share spamming, infected machine control, and information exchange duties. Due to their wealth, some "elite" criminal organizations are closed and do not participate in online forums. So they don't need to outsource or be integrated into other groups.

It has always been difficult to combat cybercrime due to the sheer number of users, the global nature of the Internet, and decentralized architecture. And they will continue to be one step ahead of politicians and law enforcement agencies.

To detect, investigate, and prevent e-crime perpetrated by organized criminal groups, cross-sector cooperation is required on a national and international level. Combating organized cybercrime requires a thorough understanding and a proactive approach. Some countries lack the tools to combat organized cybercrime, whether due to technical or legal constraints. Countries must work together to resolve this global issue. No country can be secure in the global ICT network alone, which all must understand.

Without a global strategy to combat organized cybercrime, the situation is likely to worsen. As ICT networks and opportunities develop, criminal organizations will benefit from the full range of tools and models available to legal sectors. Due to the availability of information, organized groups can commit fraud and promote and automate it. Opportunistic criminals would thus be linked to established crime networks.

Without a global strategy to combat organized cybercrime, the situation is likely to worsen. As ICT networks and opportunities develop, criminal organizations will benefit from the full range of tools and models available to legal sectors. Due to the availability of information, organized groups can commit fraud and promote and automate it. Opportunistic criminals would thus be linked to established crime networks.

Cybercrime has evolved into a sophisticated criminal enterprise with elusive syndicates. Organize criminal groups would control certain cybercrime enterprises, constantly seeking new technological solutions and new markets to exploit. As a result, criminal gangs will likely dominate the cybercrime ecosystem shortly.

Because the Internet is borderless, the problem of organized cybercrime is truly global, as no single country can guarantee security. The issue can only be resolved by long-term solutions involving both national and international coordination.

Conclusions

Anonymity, rapid information flow, high impact, low risk, low cost, and undetectable are all attributes of the Internet that make it ideal for cybercrime and cyberterrorism. However, despite notable exceptions such as the UAE, North Korea, and China, shutting down or suppressing the Internet is the only truly effective and efficient solution. Another option is to identify the flaws and the threats they enable, then wait and see what happens. Other solutions proposed here, such as communication control systems, agencies, and cyber soldiers, are currently ineffective. While they can help detect cybercriminals and cyberterrorists, they cannot control or prevent their network activity. Also, no matter how diligently

security agencies or state secretariats work, it is impossible to secure computer systems completely.

The Internet is becoming a more important tool for both cybercriminals and cyberterrorists. Terrorist groups are relocating their diffuse organizations to cyberspace to dilute their influence in an area that appears difficult to counter; they are thus using the network to finance themselves, recruit, train, communicate, coordinate, and

However, as we've seen, terrorists are passively using the network. But not for cybercriminals. In any case, we believe both will increasingly rely on cyberspace to perpetuate and execute their plans. According to McAfee's annual report, a "cyber cold war" is brewing. Hence, cybercrime and cyberterrorism are two of the most serious threats facing the 21st century. This new threat affects us all, starting with routine activities like shopping at supermarkets that use barcodes or electronic pricing. For example, we may be victims of computer fraud or man-made regulations that raise call costs. Moreover, we may be unaware of victims of an illegal act due to technologies right now. As a result, victims include large multinational corporations, banks, governments, everyday citizens, consumers, and users.

References

[1]. Zhao, H. (2021). Cyberspace & sovereignty. https://doi.org/10.1142/12027.

[2]. Fishwick, M. W. (2021). Cyberspace. *Popular Culture*, 140-143. https://doi.org/10.4324/9781315865355-30.

[3]. Owen, T. (2020). CyberTerrorism: Some insights from Owen's genetic-social framework. *Rethinking Cybercrime*, 3-22. https://doi.org/10.1007/978-3-030-55841-3_1.

[4]. Sandler, T. (2018). Role of terrorist groups. *Terrorism*. https://doi.org/10.1093/wentk/9780190845841.003.0003.

[5]. Weimann, G. (2004). Cyberterrorism: How real is the threat? (Vol. 31). United States Institute of Peace.

[6]. Brennan, A. M. (2018). The network-based structure of transnational terrorist groups. *Transnational Terrorist Groups and International Criminal Law*, 21-32. https://doi.org/10.4324/9781315264981-2.

[7]. Jones, sir Kenneth Lloyd, (Sir Ken), (born 13 June 1952), global counter terrorism, policing and cyber security consultant, since 2015; Defence and security adviser, British Embassy, Washington DC, 2013–14. (2009). *Who's Who*. https://doi.org/10.1093/ww/9780199540884.013.250305.

[8]. Cole, A. (2017). All of us are vulnerable, but some are more vulnerable than others: The political ambiguity of vulnerability studies, an

ambivalent critique. *The Politics of Vulnerability*, 110-128. https://doi.org/10.4324/9781315180519-8.

[9]. Luiijf, E. (2014). New and emerging threats of cyber crime and terrorism. *Cyber Crime and Cyber Terrorism Investigator's Handbook*, 19-29. https://doi.org/10.1016/b978-0-12-800743-3.00003-7.

[10]. Defining the workforce and training array for the cyber risk management and cyber resilience methodology of an army. (2020). *Proceedings of the 19th European Conference on Cyber Warfare*. https://doi.org/10.34190/ews.20.114

[11]. Hunt, J. (2011). The new frontier of money laundering: How terrorist organizations use cyberlaundering to fund their activities, and how governments are trying to stop them. *Information & Communications Technology Law*, *20*(2), 133-152. https://doi.org/10.1080/13600834.2011.578933.

[12]. Child pornography in the digital age. (2012). *Illegal Immigration and Commercial Sex*, 175-192. https://doi.org/10.4324/9780203044551-8.

[13]. Wasielewski, A. (2021). From city space to cyberspace. https://doi.org/10.5117/9789463725453.

[14]. Ballardini, R. M. (2019). AI-generated content: Authorship and inventorship in the age of artificial intelligence. *Online Distribution of Content in the EU*, 117-135. https://doi.org/10.4337/9781788119900.00015.

[15]. MITRĂ, S. (2020). The structure of cyber attacks. *International Journal of Information Security and Cybercrime*, *9*(1), 43-52. https://doi.org/10.19107/ijisc.2020.01.06.

[16]. Mohsin, K. (2021). The internet and its opportunities for cybercrime – Interpersonal cybercrime. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3815973.

[17]. Bozkurt, S. (2021). Stepping out into cyberspace. *Women in Transition*, 204-221. https://doi.org/10.4324/9780367771638-17.