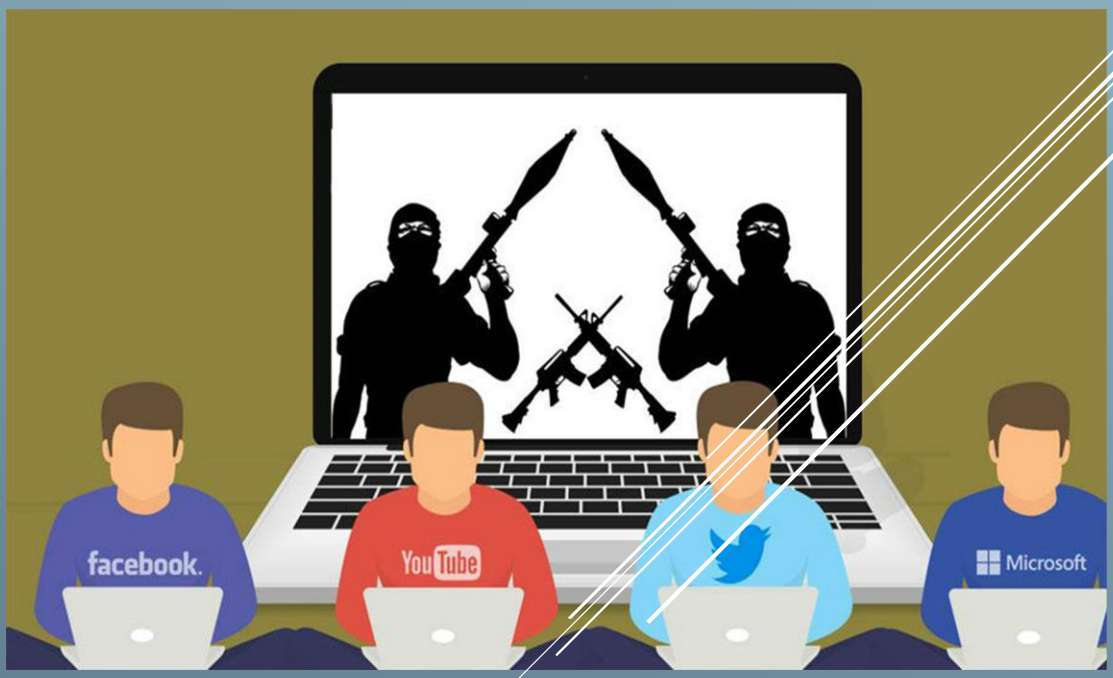


# Cyberterrorism: The Silent Danger

**Prepared by: Zainab Saleh  Edited by Muhammad Al-Badawi**

**ECHRD**

**February 2023**

# Cyberterrorism: The Silent Danger

**Egyptian Coalition for Human Rights and Development (ECHRD)**

**It is an initiative launched by the Forum for Development and Human Rights Dialogue (FDHRD) consisting of 500 associations and development organizations in 9 governorates that aims to enhance the human rights situation in Egypt, strengthen partnerships and exchange experiences.**

**The NGOs participating in the initiative are distributed in 9 governorates: Cairo, Gharbia, Beheira, Alexandria, Beni Suef, Sohag, Luxor, Qena and Aswan.**

**Facebook:**

**https://www.facebook.com/profile.php?id=100090569196942**

## Introduction

Crime started with the emergence of humankind and began to develop accordingly, becoming a behavior inherent to human nature, which made it take on different dimensions and forms. Among these crimes is terrorism, from which human societies have suffered throughout history. This suffering has increased in the modern era because of the scientific and technological development witnessed by the world, which led to the emergence of a huge information revolution that included most aspects of life. This includes crimes in general and terrorism in particular, where the first generation of terrorism with a nationalist nature appeared in the late nineteenth century. The second generation of it appeared to have an ideological nature during the Cold War by including conflicts between the Western and Eastern camps. In conjunction with technology and the information explosion, a third generation of terrorism appeared under the name "cyberterrorism" as a new threat to societies as they are using modern technology to launch terrorist attacks to spread fear and terror.

Cyberterrorism is considered one of the most heinous and dangerous crimes committed via the Internet and threatens the world. It exploits the information arena or cyberspace by creating terrorism accounts on multiple websites to spread extremism and terrorism in the world, communicate among its members on how to penetrate and destroy websites, spread viruses, spy on countries to reveal their secrets and blackmail them to achieve terrorist purposes, obtain funds for their terrorist activities, and destroy the infrastructure of countries. The contemporary form of terrorism is considered the cyber version of terrorism. In terms of organization, it is transnational and multinational, does not share a national or nationalist issue but rather a political or religious ideology, and aims to achieve the greatest material and human losses in a very short period of time and at lightning speed, using very advanced digital weapons. Modern technology is the most lethal weapon used by the cyber terrorist in carrying out his attacks on international peace and security. Cyberspace is a fertile field for communication among them and preparation for their destructive actions.

Due to all the dangers and threats posed by cyberterrorism to the whole world, most countries, whether Western or foreign, have sought to combat the dangerous crime that accompanied the misuse of modern technologies. Therefore, we will discuss the issue of cyberterrorism through several axes, namely the definition of cyberterrorism and its origin, identifying ways of using the Internet in terrorist acts, clarifying the

role of social networking sites in spreading extremist ideology among young people, why extremist groups use social media sites, clarifying terrorist groups' recruitment methods of youth through social media sites, social networking sites, identifying how electronic games are exploited in terrorism and recruitment, clarifying what the game of "Salil al-Sawarim/Clashing of the Swords." is, explaining the impact of electronic games on the growth of terrorist behaviors among young people and children, identifying mechanisms to confront the phenomenon of youth recruitment into terrorist groups, identifying international and Arab efforts to combat cyberterrorism, and presenting some recommendations to address this threat to the entire world.

## ➢ Definition of Cyberterrorism and Its Origins

The first use of the term cyberterrorism was in the eighties of the last century, and the treatment of that term was limited to referring to those attacks in which the computer is used against the economy and the government of the United States, then this concept expanded with the beginning of the nineties, which witnessed an increasing growth of the Internet and its use and the conditions experienced by the Arab world in early 2011, and drew attention to the importance of the electronic field in the movement of international relations, especially with its role in mobilization, mobilization and organization of protests, which ravaged the rule of a number of Arab systems.

Specialists and researchers have not settled on an approved definition of terrorism, as well as the definition of electronic terrorism, as there are several definitions of the term electronic terrorism that has recently emerged, and the phenomenon of electronic or digital terrorism (Cyber Terrorism) is a term that refers to a negative culture and another type of terrorism as a result of technological development and the information revolution, where the Internet and technical tools are exploited for demolition, sabotage and theft..

It is defined as aggression, intimidation or physical or moral threat issued by states, groups or individuals against a person in his religion, himself, honor, mind or money without the right to use information resources and electronic means of various types of aggression and forms of corruption. On the other hand, it is every act or behavior adopted by the individual to acquire a negative culture and anti-citizenship values from the electronic games environment that contributes to increasing violence and aggressive behavior and perpetuates terrorism.

Cyber terrorism is a new formulation of conventional terrorism, redefined in line with technical development, and the digital space has been used as a field of terrorism, and has been defined as high-impact illegal attacks, or the threat of attacks using computers and computerized systems by non-state activists on computers, networks or electronically stored information, to intimidate, retaliate, blackmail, coerce or influence governments, peoples or the entire international community; Specific political, religious, or social goals. To be considered an online terrorist and not just a hacker, attacks must result in violence against people or property or at least cause enough harm in order to spread fear and terror.

We conclude from the previous definitions that cyberterrorism differs from conventional terrorism in its characteristics, means, scope and impact. It relies mainly on modern technology, harnesses the means of communication and information networks to achieve its goals and objectives, and uses cyberspace as a field for its wars and conflicts. This is a very important matter that confirms that modern means of communication, although aimed at facilitating people's lives and serving societies and their institutions that aim to serve humanity, may be used badly and harmfully if we avoid the ethical and value dimensions.

## ➢ Ways of Using the Internet in Terrorist Acts

**Confidential Preparatory Communications**:

The primary function of the Internet is to facilitate communication, and terrorists are very sophisticated in exploiting communication technologies to communicate with each other anonymously when planning terrorist acts. Terrorists may use a simple-creative email account to message in a "virtual mailbox." This means writing messages without sending them, leaving behind minimal electronic traces, and can be viewed on any internet-connected device around the world by multiple individuals who know the password for that account.

There are also many advanced technologies that make it more difficult to detect the identity of recipient or content of the original message transmitted over the Internet, as encryption tools and anonymization software are available on the Internet and can be easily downloaded. These tools allow, inter alia, hiding the IP address that distinguishes and locates each device used to access the Internet, encrypt traffic data of the sites accessed, or all these actions together. Steganography can also be used, i.e. hiding messages in pictures.

**Using the Internet to obtain funding and financial support:**

The interactive and immediate nature of the Internet and its ability to reach different categories of individuals around the world, these features help extremist and terrorist groups to use the Internet to access sources of funding and financial support, which appears in several forms followed by the websites of these groups:

**Solicit donations, aid and funding directly from site visitors:**

The group indicates a bank account number or online payment.

It may adopt the idea of carrying out electronic activities of a commercial nature through its sites, such as providing services for purchasing and downloading electronic books, audio and video recordings, etc. etc. in return for payment of a fee.

Sometimes it adopts the method of the commercial broker to obtain a commission, by providing referrals on its site to other commercial sites, and benefits from a percentage of the fees collected by those sites for each commercial transaction made through them.

**Using electronic commercial activities indirectly:**

Extremist and terrorist groups may employ Internet service providers (ISPs) to get the material support they need.

**Organizing charity to bring in the required funding:**

The websites of extremist and terrorist groups also organize charitable activities and works, such as humanitarian relief committees, which they promote by announcing their humanitarian goals to attract the sympathy and donations of members of the public, and then use this funding to support their terrorist activities. In the case of extremist and terrorist groups that use Islam as their cover, they defraud the feelings of Muslims who commit to paying zakat imposed in the Holy Quran, as well as alms, so that charitable and humanitarian activities sponsored by them and in need of donations are announced through Islamic websites and through religious slogans that favor them and urge cooperation with them.

**Reducing security risks to extremist and terrorist groups:**

If extremist and terrorist groups find themselves in constant pursuit of security by the security authorities and authorities, then they find a safe haven for them - to some extent - represented in virtual groups on the Internet, where individuals of the same intellectual and ideological affiliation from all over the world share information and

opinions virtually. Through the Internet and away from reality, which represents a dimension of high importance for these groups, especially in light of the security prosecutions against them. All in all, it can be concluded that the greater the degree of breadth and complexity of the structure of the extremist group, the greater the importance and strength of the role that information technology plays in the coordination, planning and decision-making process within it, and that information technology and exchange of communication allow extremist groups more power and global spread while giving it the greatest possible degree of security to carry out its activities.

**Using the Internet to mobilize and recruit targeted youth:**

Extremist and terrorist groups use the Internet to gain the sympathy and support of others, especially youth, and to try to recruit them and obtain their assistance and support for their terrorist activities, and they achieve this goal through various mechanisms such as:

- Employing interactive communication channels on the Internet, such as electronic forums, chat rooms and mailing lists, in attracting and recruiting youth by integrating them into a directed dialogue on specific topics raised by the group to serve its orientations.
- Provide information that may be needed by those wishing to join or support the group. Easily and quickly, and across a variety of modes.

It is noticeable that the websites of extremist and terrorist groups with an Islamic reference seek in this regard to draw a mental image that helps them attract youth based on consolidating the idea of cohesion, and belonging to one organized and strong entity. This may come in an attempt to exploit the currents of isolation, alienation, confusion and loss of identity that have spread among youth in their favor, as they give the young man the impression through their media messages on the site - that by joining them he finds his lost self in the midst of a safe, strong and coherent company. At the same time, it offers religious scruples to demonstrate the soundness of its position, the strength of its argument and its logic in the terrorist activities and acts it adopts.

## ➢ The Role of Social Media in Spreading Extremist Ideology among Youth

Social media has contributed to the dissemination of a range of negative behaviors among youth that have made them vulnerable to so-called intellectual stalemate and

lack of acceptance of the other and has also contributed to the dissemination of a culture of fraud among members of one community and thus become a fertile soil and a growing environment for the dissemination of extremist terrorist ideology. This is because of its rapid ability to spread, as well as its ability to influence and steal minds and provoke emotions in its young users through two key elements of influence: (Enthusiastic rhetoric- exploitation of international events) against Muslims around the world "Islamophobia" and endeavor to hold Arab Governments accountable by directing pressured and hostile rhetoric and seeking to incite against these Governments by making sure that they are able to use today's information infrastructure and virtual technology, characterized by easy communication between individuals without censorship and the difficulty of controlling the content provided through social media sites also weak content provided through traditional media and official government websites, This paved the way for extremist terrorist groups to attract a large number of youth to them on social media.

## ➢ Reasons Why Extremist Groups Use Social Media Platforms

- The ability to provide interesting and attractive content on social networking sites.
- The possibility of using artistic elements capable of attracting attention, such as audiovisual and kinetic effects used through images and videos that they publish on social networking sites.
- Work on the use of language and words used by youth in their speeches, with the addition of a set of influential words such as "jihad" and "just Islamic rule" without complications in the language of dialogue, which motivates youth to adopt inflammatory and violent ideas and behaviors without realizing the consequences of embracing such ideas.
- The availability of the element of confidentiality and the absence of censorship of the content provided through the cyberspace called social networking sites.
- Ability to communicate with a large fan base easily.
- Reduced costs used to stream content on social media.
- Easy access to information.
- Young people are increasingly using social networking sites.
- The possibility of obtaining financing from unknown parties in a way that is difficult to trace.
- Terrorist groups rely on social networking sites to spread their extremist actions among the ranks of young users who are good at using this type of

technology, and take advantage of the gap generated by youth who grew up within Western societies on a range of methods to spread their ideas on social networking sites.

## ➢ Methods of Youth Recruitment by Terrorist Groups through Social Media Platforms

Extremist terrorist groups work to attract youth, with their attractive media strategy, through which they can obtain the sympathy of many with these groups, where youth of different ages and at different levels of scientific and academic interests are targeted through the use of social networking sites, luring them and then recruiting them into those terrorist groups across countries and continents, so it will be clarified how terrorist groups use them through social networking sites to recruit youth and join them. The spread of terrorism and extremism is as follows:

1- Image-making: by disseminating information and ideas among current and potential supporters of extremist terrorist groups, and countering the enemy's negative propaganda, by publishing news of battles and creating an attractive image of daily life. In addition to spreading ideas that are used in propaganda, such as exalting the desire for martyrdom and celebrating it as a path to paradise, and promoting a culture of martyrdom, it also often involves efforts aimed directly at making jihad an attractive view for a younger audience.

2- Polarization processes: where social networks are used for recruitment, whether through intermediaries, or by sending messages to the accounts of terrorist groups through Facebook and Twitter accounts, or the person is communicated electronically through a relative or friend from within those groups who invites him to join them, and provides him with the required instructions, and music "White Power" and superior computer games are also used online that are provided through websites and virtual communities to specifically target youth in an attempt to arouse their interest in the movement with the aim of employment, the increasing popularity and sophistication of computer games are being used by extremist elements on the Internet to attract potential new recruits, targeting primarily youth, and here the growing development of these games and their potential as a tool for propaganda and recruitment should not be ignored..

3- Formation of the recruitment cell: Terrorist groups form a "recruitment cell", whose mission is to entice the targets, as the cell members rely on a specific code during their speech and each word has a different meaning to choose new young recruits in armed organizations, away from the old traditional steps that relied on mosques, and the target is attracted after knowing his psychological state, and

then the focus is on issues: Monotheism, loyalty, and the importance of ruling by the Qur'an and Sunnah, and the assertion that jihad is the solution, followed by planting extremist ideas in the mind of the targeted youth, then pushing him to listen to everything that makes him sad by using sad audio speeches on YouTube and listening to enthusiastic songs, and then doing what we can call "hypnosis", depending on the idea that Islam in society is an Islam far from the truth, and this is what ISIS does when recruiting many individuals".

4- Focused intellectual nutrition: After the targeted young person goes through concentrated intellectual nutrition, he will find himself with a change of attitudes, driven or invited to search for the "virtuous society" portrayed by social networks, by publishing pictures, films and wills that narrate with influential melodies the biographies of youth who participated in "jihad" and the dignities that happened to them and comparing them to the great conquerors.

5- The executive stage: The executive stage (process) of the formation of extremist thought and direction, and then the actual joining of extremist terrorist groups, can be distinguished as follows:

- **First**: Injecting extremist thought by digging up books and fatwas and showing the strictest interpretations of the texts, and inflicting them on the facts of the times and then issuing judgments, and at this stage the young man is in the stage of reflection and selection.
- **Second**: Assisting in the choice, which is a stage through which influences are used to push the confused person to form a situation.
- **Third**: Congratulating on knowing the truth and promoting ideas when there are signs of conviction in ideas.
- **Fourth**: Actual joining of the organization under the slogan of guidance, commitment and seeking paradise.
- **Fifth**: Engaging in operational roles, which is the main goal of all these efforts.

By tracking the activities of terrorist and extremist groups, we notice their reliance on the "persuasive approach", which leads those who engage in it and touch their whims to the arms of these groups, a supporter in support of their theses, or an executive member who surrenders to the instructions of the leaders of the group that attracted him, and in order to understand the process of transferring information and ideas from sources - leaders - instigators to the rest of the members and supporters, it is necessary to distinguish the scientific leadership hierarchy and understand the

nature of the roles and strength of commitment of each group in the system of extremism, and how instructions are transmitted to youth groups. Via Social Media.

The Internet is packed with sites where terrorists can communicate securely away from the eyes of governments and cannot be monitored at all. This is evident in many of the programs and apps that terrorists use to communicate with each other. Most of these programs cannot be monitored or monitored. If the government can know and monitor a particular program, it is easy to use other, more sophisticated programs.

However, there are other apps like Facebook and Twitter that terrorists use to promote their ideas.

- Facebook is one of the most widely used social media outlets to recruit extremists and terrorist organizations often create Facebook groups whose thesis focuses on an essentially human idea, as the number of members of this group increases, terrorist material is gradually developed in a way that does not reprehend or condemn such acts. At the same time, Facebook's policy is not violated, and the organization's members are then directed directly to sites or forums linked to terrorist organizations. Members can be recruited through Facebook in this way and in fact, Facebook is not just used to promote terrorists' ideas. However, it is more widely used to destabilize States and undermine their prestige. This is evident in videos broadcast on Facebook and YouTube from burning, drowning and beheading, it’s all meant to sow fear in people's hearts to show the power of terrorists. The Internet is a way of streaming videos, and you can find millions of views of these videos.

## ➢ How Electronic Games Are Exploited in Terrorism and Enlistment

Electronic video games were able to achieve a great spread by playing them on a chord that immersed players in an alternative and experimental reality to build their identities, but terrorists and extremists took advantage of this point to recruit "fuel" for their wars, and take advantage of these platforms to plan their heinous operations, and communicate with each other.

When video games first appeared, the main goal behind the industry was to have fun entertainment, tackling stories and novels that movies could not provide with the same realism and degree of interaction. Over time, the video game industry has evolved into one of the largest industries in the world, but as with any invention or technology, there is a bad side that bad guys can take advantage of in destroying

innocent lives, as the Australian Federal Police recently called on parents to follow what their children are doing online, warning that they have evidence indicating that extremist terrorist groups are targeting gaming platforms to recruit teenagers. Police said in a statement that these extremist groups are exposing youth to dangerous content, including reposting real terrorist incidents on electronic gaming platforms. Police said extremist content on gaming platforms had become a "serious concern" for law enforcement. They explained that popular games in which players were able to create scenarios that may be bloody, and record them for others, so that they are shared on the Internet and social networking sites. They warned that what is happening in Australia is not a new trend for terrorist and extremist organizations, as numerous reports have indicated that terrorists and armed groups use multiparty online video games to plan armed attacks. Using these games, terrorists can use a secure "chat" line and talk to their partners from around the world about their next plan, without any fear of revealing their identity.

Terrorists often focus on first-person shooters because of the realism they provide. In addition, when compared to other means of communication, gaming platforms provide a secure environment for communication compared to even phone calls, texts, and encrypted messages. What makes it easier for terrorists to carry out their criminal tasks is the difficulty of determining the IP address on gaming platforms compared to, for example, mobile phones. Through the use of video games, terrorists will not have to talk or exchange written messages, which makes the task of the security authorities difficult, as it is enough for them to pass hidden messages among themselves through the games they play, such as writing the details of the operation in the scenes of a number of games in a cunning way, such as shooting at a wall.

Today, almost all gaming platforms come equipped with capabilities that allow everything to be recorded, which could make it easier for intelligence agencies to track terrorists and suspects, based on the history of conversations they have had on gaming platforms, if laws are passed that enable law enforcement agencies to access that information. Similar to single-use phone manufacturers who have been accused of facilitating the communication of criminals, the same will apply to video game manufacturers, who may concede to the security services by providing data that simplifies the task of monitoring the accounts of suspects in a world where terrorists have mastered devising ways to evade the grip of security.

Since games are one of the essential elements of popular culture, and since extremist organizations constantly seek to use references and tools derived from public culture, it is not surprising that video games are used by extremist organizations for various purposes, including indoctrinating children, appealing to a wide audience, facilitating radicalization and interactively building their ideal reality. A group of extremist organizations have developed their own games or modified existing ones.

ISIS is the most notorious group for using gaming language, including the visual style of "first-person shooting" games. ISIS used video game images and actual games to serve its goals. By launching an educational app called Horouf that aims to teach children the Arabic alphabet by encouraging them to match letters with military equipment such as tanks and bombs, the group sought to pave the way for radicalization at the earliest possible age for young users. ISIS has also consistently used visual images of popular video games. For example, they have extensively used footage shot with high-resolution cameras mounted on helmets and scenes taken from toys, such as Call of Duty, in their propaganda videos.

They supposedly developed their own game, Salil al-Sawarim, though it's still unclear whether they have launched the game yet. Although the use of video games is linked to, and part of, the discourse on online extremism, it has so far received little attention compared to other factors that contribute to facilitating radicalization. It can be said that games-related research, in this context, is still in its infancy.

## ➢ What Is Salil Al-Sawarim Game

In 2014, the Islamic State in Iraq and the Levant (ISIL) launched a new electronic game called "Salil al-Sawarim", which is full of scenes of missions against international forces formed by the United States to eliminate its strongholds. The jihadist media platform, the media arm of ISIS, announced that there are versions of other electronic games to raise the morale of the jihadists, train children and young adolescents to fight the West, and throw terror in the hearts of opponents of the state, explaining that the content includes all the military tactics of the organization against its enemies, as the game begins with warning the United States against striking its strongholds and war on them. The media platform stressed that what appears in electronic games of skills and behavior of cartoon characters such as jihad and sacrifice, exists indeed on the ground and in the arenas of jihad.

The promo of the game, which was published, begins with a warning message, which reads, "Those games that you produce, we commit the same actions on the

battlefields". After this, the CD of the game appears, which contained the image of a masked cartoon mujahid, and behind him destruction and traces of an explosion, and the name of the game "Salil Al-Sawarim". The promo contained, instead of music, a jihadist anthem with the same name of the game calling for fighting. The promo divided the game according to the tactics known about "ISIS", where characters similar to ISIS fighters carry out their work with ambushes to blow up military vehicles, others specialized in sniping, and a third fighting commando style and attacking military facilities with knives and silencer pistols.

The stages of the game go through the attack of the Iraqi army and then the American forces. With each successful mission of the game, the cartoon characters launch shouts and takbeers with crying and hugs of joy for victory. The cartoon characters also kill their victims by shooting and slaughtering, in a simulation of what the organization's fighters do in reality. There is no doubt that the target of this game are young adolescents who are attracted by such games, as happened with the game "Call of Duty", which achieved the highest sales globally, especially as it develops their desire to experience these feelings on the ground and practice the experience of carrying weapons and killing in reality and not in the virtual world. It can be said that the production of a game such as "Salil Al-Sawarim" would contribute to recruiting more young men into the ranks of the organization.

The use of electronic games in psychological propaganda, promotion of ideas and polarization is not new. For example, an American company has produced a game called "Splinter Cell". It revolves around the attacks of the eleventh of September. Another game called Counter Strike has also been produced. It allows the player to play the role of anti-terrorist and the role of terrorist as well. This game has been prepared in this way based on in-depth psychological studies. Moreover, in 2006, al-Qaeda produced a game called "Quest for Bush" in which the player kills American soldiers and captures and kills George Bush. Hezbollah, as well, has spread some of its beliefs through video games such as "Quraish" and "Under Siege".

## ➢ The Effect of Electronic Games on The Growth of Terrorist Behaviors Among Youth and Children

The interest in the impact of electronic games on children and youth lies in the fact that this recreational practice has nowadays consumed more youth time than any other practice. Given the relationship of this practice to violence and terrorism, we find that many electronic games contain different models of characters and repetitive violent behaviors that young children embody without showing any form of criticism

and condemnation that may maintain the survival of the dominant social opinion that sees violence as a reprehensible social behavior that must be prevented and resisted.

Electronic games leave negative effects on the child's character building due to the violence they are exposed to and the programs they contain. The nature of entertainment that characterizes these games has a major role in attracting them to it strongly, which leads to great neglect of their personality, psychological needs and noble goals that they should aspire to. In addition to that, these electronic games do not give weight to the faith or the values in our Arab world and its customs, traditions and civilized values that we should teach children about and adhere to. This coincides with the noticeable absence of advisory and guiding roles for parents with regard to playing electronic games and the emergence of new social classes based on the difference in the use of entertainment information and awareness of the potential dangers of the great encroachment of electronic entertainment, especially if we take into account the high level of alphabetic and informational illiteracy for many groups of society. This reduces the sense of the dangers of virtual reality among parents in general. It leads to a kind of idleness and unjustified tolerance towards electronic games, as the role of the family seems small and meager in control and supervision. This reflects a great deal of lack of awareness among parents, of the serious educational effects that could result from this free use of electronic games. Most electronic games take different forms and types of guns, pistols, daggers, swords, theft, destruction, seizure of money and property of others, spreading terror and fear in the hearts of others. These acts destroy the instinct of normal children and youth and is far from their environment, and turn them into an environment that encourages violence, killing, destruction and hatred of others, and increases sectarian intolerance. It upbrings the children to disrespect the rules and regulations of security and with weak social responsibility, all of which are anti-citizenship values. What electronic games promoted by suspicious organizations brings, is a real destruction of the instinct and innocence of a normal child and an alarming load of violence received by the child.

We are facing a real crisis of communication, whereby the electronic game turns into a tool for deepening alienation and a means of isolation and introversion by distancing children from themselves and their reality. Most of the dialogues that take place when they play killing and adventure games, tend to express belonging to new social groups that are real in reality, inspired by their ideals, values and cultural references from the culture of violence, war and destruction. It is not based on the principles of honor, freedom, justice and tolerance as much as it calls for force,

opportunism and control. It educates children and adolescents not to adhere to the system or work with it. It instills in them negative attitudes towards the preservation of public and private property and these values perpetuate terrorism.

The harm of some electronic games is no longer limited to the violence that exists within their world, but rather it extended to misleading youth to join terrorist organizations, where members of organizations reach out vocally with players in the online world of electronic games to manipulate their ideas and try to mislead them. Some electronic games are also used to communicate between members, where members join a virtual fight in a game allowing them to plan and communicate away from the eyes of direct observation, as the servers of those games are distributed all over the world. Organizations try to contact players in different ways before chatting by voice or text and trying to mislead them. It is not far off that children and adolescents are affected and wish to experience what is happening in the world of violent e-games outside their homes, which translates into them being victims of such attempts. Many studies confirm that electronic games and their networks have become a primary target for terrorist groups and an outlet to unload the wishes of murder and assassination, as they do not have adequate surveillance and security protection. Some studies have also concluded that the risks posed by playing electronic games are raising the child's awareness of violence, aggression and terrorism.

Children playing violent electronic games can increase thoughts, behaviors and aggression in children and adolescents. These games may be more harmful than violent films on television or cinema because they are characterized by interaction between them and the child, and require the child to assume an aggressive personality, which instills in children that killing is acceptable and fun. Analysis of some studies showed that scenes of violence in violent computer games contributed to an increase in violence among children, as young children who watched violent footage on television or cinema or played violent video games showed aggressive games and behavior.

Social media sites have dealt with the phenomenon of the market ~~invasion~~ being invaded, in some Arab countries, especially in Saudi Arabia, by a group of the latest versions of electronic games that target the minds of children. Specialists considered that it represents an irremediable danger~~.~~ They explained that the tapes of these games belong to major international companies with three aspects: Sexual overtones, religious abuses, intellectual delinquency. It~~, targeting~~ targets the age groups (7-35

years) ~~age groups~~, and ranges from sports to adventures and war games. Specialists have revealed that anonymous groups have targeted children and youth for three goals: the spread of homosexuality, violence and terrorism. The dangers of violent electronic gaming lie in the continuous promotion of killing, destruction and other aggressive practices, so that winning the game is conditional on exercising greater destruction and bloodshed. This is done by teaching the player the means of full loyalty and integration at the time and place of the virtual game. This then prompts him to exercise the violent solutions available when dealing with people and passing the obstacles that stand in the way of obtaining the required number of points to reach the final ranks in play, where rewards and incentives are given for killings and destruction that extend throughout the game. The child then finds himself in a closed circle of acts of violence and aggressive behavior, and reactions that reward this behavior, and is given to everyone who succeeds in doing it. That is, it is the person who is best able to use violence and aggression, is the one who wins the game, and is considered a success.

The use of a reward-system for the use of violence in the design of electronic games and their varied technical options opens up for players, especially youth and those who prefer adventure games and violence the most, new areas for learning the practice of violent solutions and aggressive behavior in tendencies and competitions that can interfere with youth's lives. It is a practice that puts aggressive ideas at the forefront because youth, as well as children, play and learn at the same time. This is even more evident when they practice tricks, and implement aggression-related plan. Terrorist groups may exploit these games and strive to recruit new members, especially children and youth. Cyber games that glorify martyrdom, can play an influential role in attracting the interest of future suicide bombers. Moreover, terrorist groups may use electronic games for educational purposes to broadcast cyberterrorism by calling on children and adolescents to steal homes, money and vehicles as well as bank robberies, bombings and killings. Violence under these games gradually turns into a familiar act and aggressive behavior, which one resorts to instead of any other alternative approach, when the time comes for conflict and conflict opens up in the reality of social life. This supports anti-citizenship values such as the loss of human rights, the marginalization of their self-identity and national identity, disrespect for other opinion, lack of coexistence with others, the undue destruction and abuse of property. It also teaches children and adolescents the methods, arts and tricks of crime and develops in their minds the abilities and skills of violence and aggression that perpetuate terrorism.

## ➢ Mechanisms To Confront the Phenomenon of Enlisting Youth into Terrorist Groups

The absence of technological awareness and the absence of the purpose of using the Internet and social networking sites, which is characteristic of our youth today, is a key driver of the youth's indifference to dealing with caution, and publishing personal data and information about themselves without realizing the seriousness of this matter. This in turn may lead to their permanent feeling that they are far from the threat of terrorism, because they feel that their data is of no value to anyone. Thus, any change in the reality of youth's use of social networking sites may require the work of many procedures and mechanisms to confront their recruitment into terrorist groups, including:

**1-** Spreading technological awareness of how to deal with social networking sites and computers, training youth on their safe use, and introducing them to how to maintain the confidentiality of data and secure their sites, e-mail and computer that they use to connect to the Internet against attempts to hack them.

**2-** Educating youth on how to benefit from the Internet in their field of study and interest, and specifying the purpose of using it.

**3-** Introducing youth to the danger of cyberterrorism, and how they can fall prey to it without their knowledge.

**4-** Preparing media-qualified security cadres, enabling them to formulate clear, influential and credible media messages, through which they can confront the lies spread by the websites of terrorist groups.

**5-** Launching religious sites on social networking sites and networks that address the other, according to concepts based on noble human contents and reflect the concept of the Islamic religion as a means to close the door for those groups that take religion as a cover to hide behind, and who are far from religion.

**6-** Activating the role of scholars and intellectuals to carry out the task of combating destructive ideas that lead to terrorist acts.

**7-** Developing a sense of duty and patriotism among youth, opening areas of work and creative thinking and not rejecting the other.

**8-** Developing means of persuasion and argument aimed at removing the religious cover on terrorism.

**9-** Developing the priorities of development programs for the benefit of youth, by formulating a new strategy to deal with employment.

10- Adopting comprehensive media programs aimed at developing public national awareness and confronting fallacies and tendentious ideas that negatively affect youth.

11- The security services must also contribute to supporting the media at all levels, through the flow of important security information that helps uncover many of the mysteries and means used by terrorist groups to win over youth and recruit them.

12- The need for Arab media cooperation to invest in various media outlets, especially social networks, because of their presence and great influence in this era and employ them to achieve and maintain intellectual security, and to enhance the exchange of information related to media affairs.

13- Directing national, regional and international efforts focus to analyzing social media actors and discovering their profiles and activities. It should further explore ways in which terrorist groups use social media sites.

14- Contemplating how to access extremist content on social networking sites such as Twitter, YouTube, Facebook and Instagram and block it permanently, because if left, the level of viewership would increase. This is what may make young followers of those sites eventually engage in promotional activity to join extremist terrorist networks.

15- Social networks represent a new set of uses over the Internet that pose a series of challenges to the security community. While these networks provide new opportunities for interaction and socialization between users, the huge amount of information generated, exchanged and redistributed by users requires the adoption of new tools and techniques of research, analysis and data security on the Internet.

## ➢ International and Arab Efforts to Combat Electronic Terrorism

**Efforts of the United Nations (UN):**

The UN is making active efforts to combat cyberterrorism in order to prevent any attempt by cyberterrorism against the security of the state and its personnel. Its efforts are demonstrated through its Congress on Crime Prevention and Criminal Justice, as well as the conferences of the International Association of Penal Law, which are held every five years. The UN, through its bodies and agencies, is endeavoring to develop the legislative framework for this emerging criminal phenomenon. The seventh Milan Congress (1985) was a breakthrough in this regard, as it emphasized the use of scientific and technological developments in the face of this criminal phenomenon related to computers. At the Ninth Congress by the UN in

Cairo (1995), it was emphasized that the dangers of technology must be addressed, and that coordination and cooperation between States must be ensured. At the Tenth Congress on Crime Prevention in Budapest, cybercrime was considered a new pattern of crimes developed with necessity of working to reduce piracy.

The UN General Assembly, in its session (56/285) held on (31 January 2002), approved a resolution calling for the use of Information and communications technology (ICT) for development. This came after a series of international resolutions to alert the world public opinion and develop awareness of the dangers of these crimes. The UN General Assembly issued Resolution No. (45/95) on (14/12/1990) which relates to sensitive data, meaning any information that leads to racial discrimination or discrimination in general between human beings, such as information about race, color, political opinions, philosophical opinions, …etc.

On April 12, 2000, the UN signed a convention against the misuse of criminal technology, due to the increase in crimes committed via the Internet and the problems they raise. The Convention stressed the need to strengthen, coordinate and cooperate among states in combating the misuse of information technology for criminal purposes.

In 2010, the Security Council warned in Resolution 1963, expressed " g concern at the increased use, in a globalized society, by terrorists of new information and communication technologies, in particular the Internet, for the purposes of the recruitment and incitement as well as for the financing, planning and preparation of their activities". In 2015, Resolution 2255 was more comprehensive of the ways in which terrorists use the Internet in their terrorist activities, as it included "concern at the increased use, in a globalized society, by terrorists and their supporters of new information and communications technologies, in particular the Internet, to facilitate terrorist acts, as well as their use to incite, recruit, fund, or plan terrorist acts".

At the Twelfth UN Congress on Crime Prevention and Criminal Justice in (2010), was held in Salvador, Brazil from 19-12 April 2010 under the title Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World. The agenda consisted of eight items, including cybercrime, and international cooperation in combating this crime.

The UN Charter did not explicitly criminalize the use of information as a terrorist tool within what is known as cyberterrorism, but the spirit of the Charter is consistent with the criminalization of its use as a violation of what is stated in the Charter regarding "the threat or use of force against the territorial integrity or political

independence of any state". Taking into account that the Charter came to combat armed conflicts, and considering that cyberterrorism and the use of information warfare fall within the aggression, this type of terrorism is incompatible with international sovereignty. It threatens international relations by using force against the territorial integrity or political independence of states, which is incompatible with the purposes of the UN.

We conclude that the UN, in the context of combating cyberterrorism, cybercrimes and the digital space, has taken three axes:

- Alerting of the dangers of new forms of terrorism, spreading and developing international awareness through a series of efforts.

- Ensuring freedom of expression and the free exchange of information, ideas and knowledge on the Internet, with the necessity of monitoring the Internet in order to maintain international peace and security.

- Developing comprehensive scientific strategies to confront and combat the dangers of cyberterrorism on the ground.

**2014 African Union Convention on Cyber Security and Personal Data Protection**

This Convention was concluded with the approval of the Presidents of the African Union (AU) and entered into force with the ratification of 15 countries. It came to address the Internet-related problems on the African continent such as e-commerce, data protection, cyber-terrorist crimes, and cybersecurity. This Convention allows member states to enact national laws under this Convention to combat cyber-terrorist crimes.

Article (18) of this Convention protects data owners. They have the right to be informed, before their data is shared with third parties. Article (25/3) also put stipulations on cybersecurity and human rights, where the Convention's cybersecurity sections protect human rights and governments must guarantee in new laws the African Charter on Human and Peoples' Rights and other fundamental rights such as freedom of expression, the right to privacy and the right to a fair trial. Article (26/1) focused on society's culture of cybersecurity. The text of the article (28/2) came to strengthen the rule of law from cybersecurity norms, as well as insist that governments sign the mutual legal assistance agreements, in order to establish international standards for the effective exchange of data. The Convention also prohibited the use of computers to abuse a person for reasons of race, religion, ethnic

or religious national origin or political opinion. (15) of the 54 Member States must refer to the Convention in its provisions. Then the laws implementing the Convention must be passed in each member state and published on the Internet.

**Arab conventions to combat electronic terrorism:**

**Arab Convention on Combating Technology Offences (2010):**

Arab efforts to combat cybercrime reached the signing of an Arab convention to combat ICT crimes at the end of the year (2010), which aims to strengthen cooperation between Arab States in the fight against cyberterrorist crimes. The Convention consists of (43) articles, including (21) articles under criminalization, and (8) procedural articles relating to the rights of the authorities, the collection of information, the tracking of users, the seizure of materials stored on personal computers and technical devices. Chapter IV consists of (14) articles regulating cooperation between member states in the exchange of users' information, where the scope of application of this Convention is regional. The Convention contained substantive provisions of criminalizing acts constituting IT offences, including hacking and interception, assault on data integrity and intellectual property, misuse of information technology means, forgery, fraud, pornography, information technology crimes related to cyberterrorism, money laundering, drugs and human trafficking, weapons, and illegal use of credit tools and electronic documents, as well as tougher penalties for technical crimes committed by means of information technology. Article 11 of this Convention provides for the willful and undue harm to beneficiaries and users with the intention of fraud to achieve interests and benefits. In addition to criminalizing acts of producing, displaying, distributing, encrypting, publishing, buying, selling or importing pornographic or immoral sites by means of information technology; Gambling, incitement to prostitution, debauchery and crimes of public morality have been criminalized, in addition to assaulting the sanctity of the private or family life of individuals or defamation, insult, and defamation of reputation through information technology.

Article 15 of the Arab convention on information technology also includes crimes related to terrorism by means of information technology, including the following:

1. Dissemination and advocacy of the ideas and principles of terrorist groups.
2. Financing of and training for terrorist operations, and facilitating communication between terrorist organizations.
3. Dissemination of methods to make explosives, especially for use in terrorist operations.

4. Spreading religious fanaticism and dissention and attacking religions and beliefs.

**- Model Arab law on combating offences related to information technology systems, 2004:**

Arab States' efforts to keep well-informed of technological and informatics developments in the world have been guided by the promulgation of a unified Arab model law to combat IT crimes. The League of Arab States, through the Technical Secretariat of the Council of Arab Ministers of Justice, has adopted the so-called Model Arab law on combating offences related to information technology systems; It was adopted by the Council of Arab Ministers of Justice at its nineteenth session as adopted by the Council of Arab Ministers of the Interior at its twenty-first session, this law consists of 27 articles. According to this law, the following acts may be criminalized, and are considered cyberterrorism offences if they affect legally-protected interests:

- Unlawful entry for the purpose of cancelling, deleting, destroying, creating, damaging, altering or reposting personal data or information.

- Obstruction, disruption, or deliberate disruption by any means through the information network or an automated computer device, and accessing the service or devices, software, data sources or information.

- The use of the information network or an automated computer and the threat or extortion of another person in its judgment to induce him to do or refrain from doing an act, even if such act or abstinence is lawful.

- The use of the information network or an automated computer device and its provisions in accessing, without right, credit card numbers or data, etc. in order to be used to obtain the data or funds of others.

- -Production, preparation, transmission, or storage that would prejudice public order or public morals through the information network or one of the automatic computer devices.

- Establishment or publishing a website on the information network or an automated computer or other computer with the intention of human trafficking or facilitating its handling.

- The establishment or dissemination of a website on the information network or an automated computer and other devices to a terrorist group under camouflage names

to facilitate communication with its leaders and members, promote or finance ideas or disseminate how incendiary or explosive devices or any tools used in terrorist acts are manufactured;

- Unjustly accessing a site or system, directly or through the information network, an automated computer, etc. with a view to obtaining data or information affecting the internal or external security of the state or its national economy, or with a view to eliminating, destroying or damaging such data or information or to transmitting ideas that cause it.

**- The League of Arab States' efforts to combat cyberterrorism:**

The League of Arab States, as an Arab regional organization, has addressed illicit activities committed through information technology. Its Charter does not explicitly provide for combating terrorism and related branches, but article (2) clarified the purpose of the League as "the strengthening of the relations between the member-states, the coordination of their policies in order to achieve co-operation between them and to safeguard their independence and sovereignty". This necessarily intersects with the violations and disturbance of power and the rule and sovereignty of states through exposure to information systems associated with sovereign institutions, as well as the possibility of exploiting and employing sensitive information against the interests of Arab target States. This calls for Arab States to confront such terrorist activities through cyberspace. This trend was confirmed by Article 3 of the Charter when the Council of the League was tasked "to decide upon the means by which the League is to cooperate with the international bodies to be created in the future in order to guarantee security and peace". Attacks on the information systems adopted by Arab States' official institutions, attempts to destroy or damage them, and the spread of terror and incitement against the existing regime through mechanisms of cyberterrorism may be regarded as aggression in accordance with the norms of international law and the UN Charter.

The interest of the League of Arab States seems to be lagging behind in field work. It began in the year 1983, the Arab joint efforts in combating terrorism by reaching the Arab security strategy approved by the Council of Arab Ministers of the Interior, which included the need to preserve the security of Arab citizens from aggressive attempts at terrorism and sabotage directed from within and outside the country. Within the framework of the security plan, the Organized Crimes Committee was formed and dealt with cyberterrorism crimes at its first meeting.

The League of Arab States' efforts to address illicit activities through electronic technology resulted in the adoption by the Council of Arab Ministers of resolution No. (229 1999) On the promulgation of the Unified Arab Penal Code as a Model Arab Law. The most notable monitoring of efforts at the level of the League of Arab States in addressing cyberterrorism and cybercrime is the adoption of this Law by the Council of Arab Ministers of Justice, which included a chapter on infringement of persons' rights resulting from informatics.

Arab attempts and efforts continue to fill the legislative vacuum in existing criminal laws. In order to confronting this type of crime, the League of Arab States allocated the twelfth meeting of the Commission on Emerging Crimes, which was established in 2007, on the topic "Credit card forgery"(2009). The General Secretariat of the League of Arab States has prepared a draft Arab convention on computer crime in implementation of the recommendation of the eleventh meeting of the Commission on Emerging Crimes; the discussion was held by a joint committee of the Arab Ministers of the Interior and Justice. So far, several meetings were held to finalize the draft in light of the member states' observations. It is important to note that so far these efforts have not been crowned with the adoption of this agreement.

## ➢ Recommendations

- ✓ The need for parents and teachers to monitor children and youth when they use information technologies, especially the Internet, to ensure the safety and legitimacy of use, and guide and inform them of the issue as it is related to the security of the homeland and the citizen, so there is no room for tampering and sabotage.
- ✓ The attention of the family, including the parents, and the regular and continuous monitoring of their children, avoiding them playing electronic games that contain violence, which may lead to trauma for children or imitation of violence in real life.
- ✓ The dissemination of educational and cultural games suitable for children and reducing violent games needs to be encouraged, provided that cultural and media institutions assume this task along with the Ministry of Education.
- ✓ Programmers, innovators and educational thinkers must design and program electronic games that take into account the educational, cultural and educational aspects of the formation of children and youth, to the same extent that they are keen on presenting the elements of suspense, entertainment and excitement.
- ✓ Governments should cooperate with the organizations responsible for social networking sites to monitor and identify accounts affiliated with terrorist groups and work to prevent their spread on social networking sites.
- ✓ The need to hold conferences, seminars, workshops and panel discussions on the phenomenon of terrorism in general and electronic terrorism in particular to identify its sources, methods, causes, motives and risks and develop effective solutions to confront it and limit its spread
- ✓ Governments begin to identify and put in place serious steps to develop religious discourse in order to resist the ideas that terrorist groups seek to spread.
- ✓ Arab efforts need to be unified towards setting strict regional legislation to combat cyber-terrorism crimes.
- ✓ The sponsoring of a national project to produce Egyptian electronic games to confront terrorism and cultivate national values among youth.

## Conclusion

The Internet is an interactive network that in record time has made a cross-border impact and to increase the intensity and speed of globalization and mutual influences at different levels, so that any interaction occurring in any region of the world leaves its impact in other regions. With non-state actors increasingly relying in their external movements on combining soft and hard power tools, the reliance on this network has increased. This made terrorist groups not depend solely on military force to achieve their objectives. They have resorted to the widespread use of means of communication, media, the Internet and websites and propaganda for their ideas and movements and also for material and moral support, and as a new tool to spread their extremist ideas and beliefs.

Through the above, it can be said that the Internet, social networks and electronic games play a role that negatively affects society if it is employed in a particularly negative manner, especially if it is employed by terrorist groups to spread ideas of extremism. The most dangerous is the use of such sites and networks to attract and recruit youth into terrorist groups and to engage and deceive them. This report monitored the relation between terrorism and globalization, and the use of technology as a tool that has brought extremist terrorist organizations to a global level. This has facilitated their spread and the adoption of their terrorist ideas and practices by many youths.