Cyber terrorism and its role in the outbreak of international crisis

Abedalrzag Aldalbeeh, Ahmad Alsharqawi

Cyber terrorism and its role in the outbreak of international crisis

Abedalrzag Aldalbeeh*

Prince Al-Hussein bin Abdullah II Academy for Civil Protection,
Al-Balqa Applied University, Jordan
Email: adlabeeh@gmail.com
*Corresponding author

Ahmad Alsharqawi

Faculty of Law,
Applied Science Private University, Jordan
Email: Ahmad_alsharqawi29@hotmail.com

Abstract: Cyber-terrorism is an important issue that concerns the local and international communities. Terrorist acts have developed due to the evolution of societies and the scientific and technological progress that societies are witnessing, where they have developed in terms of style and concepts. Therefore, cyber-terrorism has become one of the sources of threat and outbreak of the crisis, whether local, regional or international. One of the most important reasons for developing the concept of cyber-terrorism is the technological revolution. Despite the many advantages offered by the age of technology in facilitating human life, it has become a fertile environment for terrorists to spread their extremist ideology, thus causing. Therefore, this study came to explain the phenomenon of cyber-terrorism and its role in the outbreak of crisis through social media and electronic programs.

Keywords: cyber; terrorism; crisis; technological; revolution; social media; electronic.

Biographical notes: Abedalrzag Aldalbeeh is the Vice Dean of the Academy of Prince Al-Hussein bin Abdullah II for Civil Protection, in addition to the practical experience in the field of public prosecution and police work for a period of 28 years. He is an Assistant Professor and legal researcher with many books and research. He holds a PhD in Public Law and International Law, and he has many experiences in the field of teaching in Jordanian universities and international participations in the USA, as well as in workshops and conferences at an international level. His academic experience in the field of teaching exceeds seven years.

Ahmad Alsharqawi obtained his Master of Laws (LLM) in General Law, with merit from the University of Leicester in 2017. He completed his undergraduate degree in Law (LLB – 4 year course) at Applied Science Private University in 2015, with excellent with honour. Meanwhile in 2015, he has been called to the Jordan Bar Association. He is a part of the law firm's litigation department that

he is currently working at in Amman and his main area of focus is commercial law, public, criminal and civil law whilst also having considerable experience in family law.

---

1   The introduction

In the modern era, the international community faces many security threats characterised by their continuous change and development and the widening scope of their impact, not limited to harming the security of specific actors but extending to affect global security in general. Perhaps the most prominent of these contemporary security threats, the most recent and the most widespread, is the cyber threats. Cyber threats have become so complex that it has become difficult to limit them or develop tight strategies to fully confront them, especially with their multiple forms and sources and rapid and continuous development.

Just as the internet and modern technology mechanisms have played a major role in achieving the progress of countries and communication between peoples and the development of a huge number of fields, where cyberspace has become a new space in which various human activities are practised, whether, at the level of individuals or states, we find that these developments on another level have led To the emergence of new security threats no less serious than traditional security threats. Therefore, confronting these threats has become a top priority for the security policies of countries and international organisations, especially with the expectation of a surge in technological developments in the coming years, with which the danger of these threats will grow.

1.1   The importance of studying

The importance of this study is highlighted in clarifying the importance of the role of cyber-terrorism in helping to erupt international crises, as the phenomenon of cyber-terrorism is a recent phenomenon that has become widely used by terrorist organisations and individuals. Therefore, the researcher directed to study all aspects related to the phenomenon of cyber-terrorism and its role in the outbreak of the crisis in order to clarify the role of cyber-terrorism in the occurrence of crisis and thus try to address this phenomenon in order to avoid the occurrence of the crisis.

1.2   The study problem

The problem of this research lies in (what is the role of cyber-terrorism in the outbreak of the crisis and the extent to which it is possible to address such a phenomenon to mitigate the occurrence of international crisis).

1.3   Objectives of the study

This study aims to clarify the concept of cyber-terrorism and its compatibility with the concept of traditional terrorism, clarify the concept of crisis and identify its most

important features, and explain how to reduce the phenomenon of cyber-terrorism in the outbreak of the crisis.

1.4   Study methodology

In this study, we will rely on the descriptive analytical approach by describing cyber-terrorism through a statement of its concept, pillars, and characteristics and clarifying the role of cyber-terrorism in the outbreak of the crisis.

1.5   Study plan

This study has been divided into the following investigations and demands:

- The first topic: what is cyber-terrorism?

- The first requirement: defining cyber-terrorism, its pillars and characteristics.

- The second topic: the nature of the crisis.

- The first requirement: the definition of the crisis.

- The first topic.

- The nature of cyber terrorism:

In order to clarify the role of terrorism in the outbreak of international crisis that takes place through electronic programs, we must first clarify the nature of cyber-terrorism through its definition and statement of its pillars and characteristics, and in the following manner:

The first requirement: defining cyber-terrorism, its pillars and characteristics.

In this requirement, we try to explain the concept of terrorism in general and cyber-terrorism in particular, and then explain its pillars and characteristics in order to demonstrate the extent to which the concept of traditional terrorism is compatible with the concept of cyber-terrorism as follows:

2   Section one: the concept of terrorism

2.1   First: the concept of traditional terrorism

Terrorism means the language/(by terrorism) 'is the illegal use of violence supported for a political goal' (Alwan, 2001). It means (to terrorise) his fear. It is said that he terrorised people with his strength and his help, that is, his strength and his help made people fear him, and he means (Terrorist: a person who resorts to terrorism to establish his authority, and terrorist rule: one of the types of rule that is based on terrorism and violence, which groups or governments resort to' (Al-Munajjid in Language, 2011).

We note from the previous definitions that the definitions unanimously agree on an important thing: the terrorist act is irresponsible and illegal behaviour. This crime would raise fear and panic among people, and this behaviour could be adopted either by a group or government with political goals and objectives (Abu Issa et al., 2019).

Technically, there are multiple definitions of terrorism. Some of them define it as "every violent act, the illegal use of force, incitement to it, or a threat to it by one country to another, and it is based on assaulting lives or funds, threatening their security and stability, exposing them to danger, trying to interfere in their affairs, imposing control over them, and hegemony under the names of different states that violate their sovereignty and the rule of law in order to reach certain goals and objectives by which they achieve their own interests" (Mohammed, 2011).

Some define terrorism as "the illegal use of violence or the of it by an individual, group, or state against an individual, group, or state that results in terror that exposes human lives to danger or threatens basic freedoms and whose purpose is to pressure groups or the state to change its behaviour towards a subject" (Helmy, 2004).

Terrorism is also defined as "an act issued by an attacker of an innocent person that causes him to fear, terror and panic, whether by carrying out acts of violence such as killing, sabotage or threatening, and for any reason, political, financial, religious, sexual, or personal aggression for psychological and social reasons, and this act may be issued by An unjust authority or a state that occupies a people or is issued by a group or an individual, so every act that this description or definition applies to is terrorism, regardless of who is doing it, whether an individual, a state, or a group".

Through the definitions presented, we note that there is no agreement on a definition of the concept of terrorism because the concept of terrorism is not confined to a specific framework. After all, it can be committed within the internal framework of a state or the international framework between two or more states. Moreover, there may be political motives or other motives. This crime does not have a specific target, which a person, group or organisation may commit.

Therefore, we can say that terrorism (any act or act characterised by violence, force and threat of it, in violation of the law and issued by the state or a person or group motivated by the state towards another state or group or directed against its vital facilities, to incite terror and intimidation in this state or group or sabotage or destruction of the property of the victim's state).

2.2 Second: the concept of cyber-terrorism

The crime of cyber-terrorism is a type of crime whose origin is due to the circumstances and environment in which this crime is committed.

Cyber-terrorism: what concerns us in this study is to explain the concept of cyber-terrorism, so that this type of terrorist crime differs from other crimes of traditional terrorism, as it is the use of information resources such as a computer, information network, information system or the internet, in order to intimidate or to force others, for example, illegally entering the computer system in a hospital in order to change the quantities, components and medical syringes for patients or a patient, which leads to creating a lethal dose and thus leads to the killing of patients, for example (Al-Amoush, 2006). We note that there is no unified or stable definition of cyber-terrorism. Every trend has tried to define this crime according to its perspective of this crime. Some have defined cyber-terrorism as "aggression, intimidation, or physical or moral threat emanating from countries or groups or individuals unjustly use information resources and cyber-means of various forms of aggression and corruption against a person in his religion, psyche, honour, mind or money" (Al-Ajlan, 2015).

Others define it as "unlawful attacks or threats of attacks against computers, networks or cyber-ally stored information directed in order to retaliate, blackmail, coerce or influence governments or the international community as a whole to achieve humiliating political, religious or social goals, and thus to call someone He is a terrorist on the internet, not just a hacker. Moreover, his attacks must lead to violence against people or property or at least cause enough harm to spread fear and terror" (Bashir, 2014).

Through the preceding, we note that despite the many advantages of the cyber-network revolution and the misrepresentation of information that facilitates its access to millions of people at one time, in addition to that, it constitutes a wide field for terrorists with experience to exploit the information network to achieve their goals in many areas such as transferring and exchanging information and directing Threats, cyber-messages, affecting navigation systems, changing the course of transportation lines, whether by land, air, or sea, or cutting electricity, water and telephone lines (Al-Marri, 2005).

Here, we conclude by reviewing the concept of terrorism, whether traditional or cyber-, that the two concepts are compatible together, as they have the same nature of sabotage and destruction, as well as threatening and sabotage of property and inciting a state of panic, and also have the same goal.

However, the simple difference between them is the means that they use. The means in conventional terrorism are physical weapons, and their tools are people or members of a particular country. In contrast, the means in cyber-terrorism are information technology, the information network, the internet, and computers. Its users may be civilians affiliated with the state or under its supervision. Alternatively, we invite them to believe it or ordinary people or organisations.

3   Section two: the elements of cyber-terrorism crime

Through the preceding definitions of cyber-terrorism, we find that cyber-terrorism, like all other crimes, has an Actus reus and a Mens rea. This can be clarified as follows:

1   Actus reus: Actus reus in cyber-terrorism crimes has many and different forms, and it is achieved by the availability of the possibility of perpetrating the act, which is (the use of an information system, the information network, or a computer). The means used to commit terrorist acts (Ayyad, 2008).

    (And the criminal outcome) that is, the use of violence or threat (behaviour) leads to one of those results, which is to spread terror among people, endanger their security, cause damage to the environment or national resources, or lead to disruption of the provisions of the constitution and laws (Al-Huwaidi, 2011). (and the causal relationship) so that there is a link between the criminal behaviour and the criminal result, that is, the harm resulting from the crime results from the conduct of the act.

2   Mens rea: the terrorist crime is intentional, and it cannot be committed by mistake. Also, two elements are required for its occurrence, namely (knowledge and will). Knowledge is through the offender's knowledge of the elements of the crime, i.e., knowledge of what he did and the means used in that (Abu Issa et al., 2020). Knowledge must be available when the offender enters. To the information network and the establishment of a site that facilitates carrying out terrorist acts, as well as its

intentions to commit this terrorist act without coercion, as the general intent is not sufficient for the establishment of Mens rea in the crimes of cyber-terrorism (Al-Huwaidi, 2011). So, the perpetrator's intention, who uses information technology, must be present to sign or threaten to perpetrate a terrorist act; otherwise, the crime will not occur (Al-Zoubi, 2010).

We note from the preceding that cyber-terrorism has two cornerstones represented by the use of information systems or the information network in order to commit terrorist acts to cause damage to people and their property, and a moral corner represented by the knowledge of the offender that he is committing a terrorist act and the will to commit such an act.

4   Section three: characteristics of international cyber-terrorism

Several characteristics distinguish this crime from other crimes, namely:

Cyber terrorism crimes are characterised by being difficult to prove. This feature is considered one of the most important distinguishing characteristics of these crimes from other crimes, especially the traditional ones. It is due to the ease of concealing the features of the crime and getting rid of its traces. As this crime requires expertise to reveal it and this hinders the investigator's work, as well as its reliance on deception in its commission and misleading in identifying its perpetrators, and also depends on the peak of intelligence and skill in committing it (Bashir, 2014).

The Jordanian legislator has criminalised cyber-terrorism according to paragraph (E) of Article 3 of the Anti-Terrorism Law which considered the following acts as being of the prohibited terrorist acts: (using the information system, internet or any publishing means or media, creating a website for facilitating the performance of terrorist acts or supporting a group, organisation or society performing acts, promoting their ideas, financing them or otherwise committing any act cathat would endanger the Jordanians or their properties to be exposed to the risk of aggressive or retaliatory acts) (Abu Issa et al., 2020).

4.1   The second topic: the nature of the crisis

There is much crisis facing society, either periodically or randomly. Looking at these crises, we find that they have caused many losses and damages to the individual and society in the past, which worsened in terms of social, political, economic, and administrative terms. It is no secret to anyone that the exposure of society to crisis randomly and continuously at the same time threatens development, whether in its Actus reus or human aspect, as the crisis of all kinds cause losses in facilities, public facilities, property and human and natural wealth. All these losses reduce opportunities for progress in the development path as they directly affect or indirectly affect society's human wealth and what it represents as a basic pillar of the development movement (Mohammed, 2005).

The crisis is considered unpleasant because they make you feel an unstable and sudden change, making you feel confused and anxious, and perhaps impulsive and hasty decisions that make things worse (Mahmoud, 2010).

In the past decades, crises have caused great losses and severe economic damage, affecting the lives of hundreds of organisations around the world. These crises are undoubtedly major obstacles to the development and development of these organisations. Addressing such a crisis requires that crisis management be included in development plans. For countries and organisations alike, relying on a well-developed knowledge base and awareness of decision-makers.

The crisis has become an anticipated event for all organisations in this era of changes and developments. Whenever the organisation can adapt to these changes, it can deal with crises steadily and in balance.

From this standpoint, the importance of studying crisis stems from an attempt to classify, analyse and evaluate crisis according to the probability of occurrence, the severity of the danger and the degree of control by society, all to face potential crisis through a perception of the risks that can occur as a result of environmental changes or human errors, and given the continued existence of the factors causing different crisis types, it must prepare plans to prepare to face these crises and try to lay the foundations and principles for predicting them or limiting their destructive effects in case it is difficult to make predictions.

4.2   The concept of crisis and crisis management

There have been many definitions that deal with the concept of crisis as a direct result of the rapid and successive internal and external environmental changes in which organisations operate, whether they are production or service, which leads to the occurrence of crises that require organisations to manage them efficiently and effectively to reduce their negative results and benefit from their positive results (Sami, 2013).

Some of them defined the crisis as "a critical and decisive moment related to the fate of the administrative entity that is affected by it, and a problem that represents a severe difficulty for the decision-maker that makes him deeply confused, so that any decision he takes becomes within a circle of uncertainty, lack of knowledge, mixing causes with results and the successive collapse that increases the degree of the unknown. In developments that may result from the crisis" (Mahmoud, 2010).

It is defined (Mitroff, 1991): "it is the process that includes five basic stages, which are the discovery of early warning signals, preparation and preparedness to prevent crisis, contains danger, reduce negative effects, increase the positives, restore activity, and in the end learn and gain experience".

The term crisis management is closely related to public administration. Crisis management is a purposeful activity based on research and obtaining the necessary information that enables the administration to predict the locations and directions of the expected crisis and create the appropriate climate to deal with it by taking the necessary measures to control and eliminate the expected crisis. or change its course in favour of the organisation (Bundy, 2017).

The science of crisis management is one of the modern human sciences that have increased in importance in our time, which has witnessed many condensing variables very strange to the point of miracles, whether at the international, regional or national level. The organisation and its ability to generate revenues and preserve its individuals and employees against various risks (Mahmoud, 2010).

Hence, we conclude that crisis management is:

> "The set of administrative preparations and efforts being made to confront or limit the devastation caused by the crisis."

Alternatively, it is the art of managing control by raising the efficiency and capacity of the decision-making system, whether at the collective or individual level, to overcome the elements of a heavy bureaucratic mechanism that is unable to cope with events and successive variables and surprise, and to bring the organisation out of its state of slack and relaxation.

Alternatively, it is the process of preparing and evaluating the organised and regular internal and external problems that seriously threaten the company's reputation, its profitability or its survival in the market (El-Refaie et al., 2021).

Alternatively, is the ability to manage the company before, during and after the crisis.

Hence, we know the concept of crisis management in line with the nature of the current study in the field of cyber-terrorism, which is "an unusual situation that is outside the scope of control and control in the state system so that it threatens the security and stability of the state by an individual or a specific organization through the information network".

5 Conclusions

Through his presentation on the topic of cyber-terrorism and its role in the outbreak of the international crisis, the researcher reached several important results and recommendations, namely:

First, the results:

- Through the definitions presented, we note that the concept of traditional terrorism is consistent with the concept of cyber-terrorism, but what distinguishes it from other traditional terrorist crimes is the means used to execute the crime. The cyber-means of terrorism is the internet and information systems.

- Cyber-terrorism has the same characteristics and pillars as traditional terrorism.

- The researcher also reached an important conclusion, which is that cyber-terrorism is one of the reasons for the outbreak of the crisis in the modern era.

6 Recommendations

The researcher recommends the need to reduce the phenomenon of cyber-terrorism by strengthening the role of control over the information network so that the terrorist cannot reach individuals and groups, especially since terrorist groups and organisations can promote their criminal ideas through social media and sow terror and panic in the hearts of people.

References

Abu Issa, H., Alkseilat, A. and Alrefaie, A. (2020) *The Cyber Terrorism Crime in Jordanian Law*, Vol. 13, pp.136–147.

Abu Issa, H., Ismail, M. and Aamar, O. (2019) 'Unauthorized access crime in Jordanian law (comparative study)', *Digital Investigation*, Vol. 28, DOI: 10.1016/j.diin.2019.01.006.

Al-Ajlan, A. (2015) 'Cyber-terrorism', *The First International Conference on Combating Information Crimes ICACC*, published on the Dar Al-Manzmah website, Saudi Arabia-Riyadh, p.52.

Al-Amoush, A. (2006) *Reasons for the Spread of Terrorism in this Century*, Naif Arab University for Security Sciences, Saudi Arabia.

Al-Huwaidi, O. (2011) *Combating Terrorist Crimes*, Wael House for Printing and Publishing, Jordan.

Al-Marri, J. (2005) *National Security/Terrorism/Organized Crime/Espionage/Rumor/Sabotage*, Dubai Police Academy, Dubai.

Al-Munajjid in Language (2010) Dar Al-Fiqa for Printing and Publishing, Beirut.

Alwan, F. (Ed.) (2001) *General International Dictionary*, Lebanon edition 1, p.180, Dar Al-kotob Al-Ilmiyah, Beirut.

Ayyad, S. (2008) *The Use of Information Technology in the Fight Against Terrorism*, Dar Al-Fikr University, Egypt.

Bashir, H. (2014) *Cyber-Terrorism in Light of the Cyber Revolution and its Applications in the Arab World*, Arab Center for Research and Studies, Egypt.

Bundy, J. (2017) 'Crises and crisis managed integration', *Journal of Management*, Vol. 43, No. 6, p.2, Arizona State University.

El-Refaie, A.M., Aldalbeeh, A. and Alsharqawi, A. (2021) 'The extent of bound or unbound United Nations security council by law', *Journal of Legal, Ethical and Regulatory Issues*, Vol. 24, No. S4, pp.1–7.

Helmy, N. (2004) *International Terrorism*, Arab Renaissance House, Cairo.

Mahmoud, J. (2010) *Crisis Management*, Dar Osama for Publishing and Distribution, Jordan.

Mitroff, I. (1991) *C: Programs Framework and Services*, Centre for Crisis Management, pp.13–15.

Mohammed, H. (2011) 'International terrorism and its repercussions on global peace and security', *Research Journal of the College of Islamic Education*, Vol. 11, No. 1, pp.267–292, University of Mosul, Iraq.

Mohammed, S. (2005) *Crisis and Disaster Management between a Theoretical Concept and pracTical Application*, Ain for Human and Social Studies and Research, Cairo.

Sami, S. (2013) *A Proposed Model for the Relationship between Knowledge Management and Crisis Management*, PhD thesis, Faculty of Commerce, Ain Shams University.