International Journal of Multicultural and Multireligious Understanding

http://ijmmu.com
editor@ijmmu.com
ISSN 2364-5369
Volume 9, Issue 12
December, 2022
Pages: 162-172

Intellectual Security: Countering Cyberterrorism

Andi Subhan Husain; Ali Muhammad

Department of International Relations, Universitas Muhammadiyah Yogyakarta, Indonesia

http://dx.doi.org/10.18415/ijmmu.v9i12.4167

Abstract

Researchers develop the conception of intellectual security by relating the introductory understanding of cyberterrorism, the difference between cyberterror attacks, and activities supporting. This study uses an inductive approach to formulate a general framework. The data collection technique used is a secondary data that is obtained through literature review from libraries and internet. The result of this study attempts to clarify the distinction between cyberterror attacks and support by examining them in terms of the generalities of confidentiality, integrity, and vacuity. A breach of confidentiality occurs if an unauthorized stoner earnings access to information. A breach of confidentiality is an act of cyberterror support. There are three introductory generalities of intellectual security; As the moderation of human understanding of religious and political issues, understanding deviation and human civilizations; As the harmony between the state and society to save individuals and groups from doctrinal or intellectual that may be the cause of deviations in behavior and thoughts from the right path; As safety of human thought from deviation which leads to maintaining public order. Our study differs from former exploration by offering the conception of intellectual security to fight cyberterrorism. Researchers believe that this conception can be developed further through subsequent study.

K*eywords:* *Intellectual Security; Cyberterrorism; Counter Terrorism*

Introduction

The increase in the number of internet users experienced an increase in messages to approximately 5 billion users marking the unstoppable development of information technology. This figure represents 63 percent of the world's population, which is now estimated at 8 billion people. Technology can make the rich richer and the poor poorer. Information technology is a commodity that is easily distorted. Information can change the way people think and influence political decisions. Even wars can happen or can be stopped with information. Havlíček (2012) says that the world is changing at an unprecedented speed, the conflicts that will occur in the future are full of uncertainty. The "first war on the internet" is believed to be the war in Kosovo that took place in 1998. During the war, governments and non-governmental organizations used the Internet and cyberspace to spread propaganda messages, to slander political and war enemies and to strengthen their positions (Havlíček, 2012). Cyberterrorism is not limited by geographic boundaries. There are no physical barriers, borders or checkpoints for the

perpetrators to cross, which does not endanger their lives, because their actions do not occur in the physical world but in the virtual world. Therefore, cyberterrorism can be carried out remotely from anywhere in the world.

Likewise, according to Kostadinov (2012) during the Kosovo war, the systems of numerous governments and the NATO computers were subordinated to distributed rejection of courtesy attacks and dispatchbombs. The first recordedcyber-attack with a terrorist aspect is believed to have passed in 1998 by the revolutionary group Black Tigers (Kostadinov, 2012). During the war in Kosovo, the authorities and non-governmental institutions started to use the internet to spread information and propaganda, to libel their political and war adversaries and to solicit support for their own positions. Hackers, too, used a fashion for dismembering services of governments to help them from spreading their information, known as distributed denial of service (Havlíček, 2012). Grounded on precedent experience, some would anticipate war opponents to try to shut down the internet as one of the first communication channels, so the opposing parties would not have similar openings to organize. But it was sanctioned NATO policy to keep the internet open (Denning, 1999), so the impacting information could be meetly spread among citizens. It's reported that hundreds of of-mails have been delivered to the mailboxes of United States institutions, potentially forming from the citizens of Serbia for NATO to stop the bombing. still, the credibility of these letters is hovered by the possibility of being faked by the authority.

Why do terrorist groups with political goals choose terror through cyberspace as a non-lethal weapon? Why would they want to limit the amount of bloodshed? It must be understood that terrorists with political goals, using violence as a way to get attention are not the main goal. This idea is neatly expressed in Brian Jenkins' oft-quoted adage that "terrorists want lots of people watching and lots of people listening and not many people dying." The reason terrorists want attention and not death is because their actions are political. They want to achieve what they demand and gain sympathy. As for terrorists who use violence, of course, it cannot be denied, this is done to instill fear and to intimidate. But this violence can go too far. Too much violence, too much death or too much of the wrong kind (children, for example), risks alienating possible sympathizers and making any action against terrorists seem justified. If a group and its political aims are to have any chance of gaining and maintaining legitimacy in the eyes of the world at large, it must not appear to be killing indiscriminately. The use of force must be proportionate to the number of threats (Tucker, 2000). The ambition of a cyberterrorism attack could classify from moneymaking disturbance through the gap of fiscal nets and systems or used in support of a physical attack to bring more distraction and achievable detentions in proper response. Although cyber attacks have caused billions of bones in harm and affected the lives of millions, we've yet substantiation the counteraccusations of a truly disastrous cyberterrorism attack (Committee, 2008). Intellectual, political, and gainful personnels have associated to elevate the terror of cyberterrorism. From an intellectual perspective, two of the full fears of current time are combined in the term “cyberterrorism”. The terror of aimless, furious victimization blends well with the mistrust and outright fear of computer technology (Weimann, 2004).

This study provides a frame for finding the statement of the conception of intellectual security to fight cyberterrorism. We deconstruct varied angles of knowledge as a recourse for cyberterrorism, and for defying them. Cyberterrorism is nearly integrated with change in our intellectual society. The virtual world is a range for knowledge and information, and cyberterrorism is an intellectual activity that surfs in it. Cyberterrorism is a confluence of cyberspace and terrorism and is nearly related to" nonvirtual" terrorist conditioning and global terrorism. Because it takes a network to beat the network, this study intends to lay the foundation for the conception of intellectual security in counter cyberterrorism. This study uses an inductive approach to formulate a general frame. Experimenters develop the conception of intellectual security by relating the introductory understanding of cyberterrorism, the difference between cyber terror attacks and supporting conditioning. Our study differs from former research by offering the conception of intellectual security to fight cyberterrorism. Researchers believe that this conception can be developed further through later examination.

The Cyberterrorism Project

The book edited by Chen, Jarvis, and Macdonald (2014) *Cyber Terrorism: Understanding, Assessment, and Response* is part of the Cyberterrorism Project. The project was founded in 2011 by academics who were then working in the School of Law, College of Engineering and the Department of Political and Cultural Studies at Swansea University. There are four reasons for establishing the project. First, the desire to increase understanding among the scientific and academic community by engaging in original research on the concept, threats posed by, and possible responses to cyber terrorism. The reason for these two projects is to facilitate global networking activities around cyber terrorism and to bring together researchers from different backgrounds with something important to contribute to this discussion. The third is to engage with, and impact on, policymakers, opinion-formers, citizens, and other stakeholders at all stages of the research process, from data collection to dissemination. And, fourthly, trying to do all of the above in a multidisciplinary and pluralist context that draws on expertise from the physical and social sciences. This multidisciplinary emphasis is one that underpins all the work this research team does (Chen et al., 2014).

The book begins with a chapter by Keiran Hardy and George Williams that examines the different legal definitions of terrorism in relation to cyber-attacks. Chapter 2, by Lee Jarvis, Lella Nouri and Andrew Whiting investigates the strategy of terrorism to become a security threat across all spheres of political life, popular culture, and academic debate. Panayotis Yannakogeorgos in Chapter 3 explores the different types of activities that occur in the technical realities of cyberspace. Chapter 4, by Michael McGuire raises the level of threat posed by cyber terrorism. Michael Stohl, in Chapter 5, identifies parallels between contemporary discussions of cyberterrorism and cyberwarfare on the one hand, and older discussions of terrorism and state terrorism on the other. Chapter 6, by Maura Conway, discusses four issues that each reduce the likelihood of cyber terrorism occurring. These issues relate to the cost factor of cyber-attacks; their complexity; their ability to destroy; and their potential for media impact. Chapter 7 by Clay Wilson continues Conway's involvement with the threat posed by cyber terrorism, albeit from a very different angle. In Chapter 8, Tim Legrand brings a public policy perspective to this discussion that focuses specifically on the importance of government responses to cyber terrorism. In Chapter 9, Lord Carlile QC and Stuart Macdonald continue the question of how to respond to cyber-terrorism by focusing on the criminalization of online activities that are preparatory to acts of terrorism. In Chapter 10, Gil Ad Ariely concludes our discussion by outlining the spectrum of available responses in relation to cyber terrorism, distinguishing them according to two dimensions: type and timescale. Conclusion seeks to bring together all the "lessons" learned from the experts. At this point, the answers are few and not really the point. Continuous dialogue to share different points of view and insights is healthy, but it will take time to bridge the differences. Several observations are offered to continue the dialogue (Chen et al., 2014).

In the prominent and influential academic journal Terrorism and Political Violence, that during 2016 and 2017 featured 59 article authors from political science/international relations (English, 2021). James A. Piazza & Ahmet Guler in "The Online Caliphate: Internet Usage and ISIS Support in the Arab World" published in the journal Terrorism and Political Violence, in this article experts argue that the internet has provided wider opportunities for violent extremist groups to do propaganda. and recruiting. In this study, researchers analyzed more than 6,000 individuals in six Arab countries to find whether those who use the internet to follow political news or to express political views are more likely to support ISIS. Researchers found that respondents who got their news online were significantly more likely to support ISIS than those who followed the news on television or print media. In addition, those who use online forums for political expression are also more likely to express support for ISIS. (Piazza & Guler, 2019).

In the article “An Exploratory Analysis of the Characteristics of Ideologically Motivated Cyberattacks” in the Journal of Terrorism and Political Violence, he examines the frequency with which the web is damaged, the factors that distinguish it from other hacking motives, and the extent to which the

correlation reflects research on ideologically motivated physical acts of crime. In this study, we examined approximately 2.4 million US-hosted web breaches from 2012 to 2016 to assess theoretical aspects of routine activity related to target selection and attack methods among ideologically motivated attacks. The findings of this study indicate that the target selection process of ideologically motivated defacers is more purposive and designed to draw attention to their goals, resembling the preferences of target individuals who engage in physical violence to support an ideological agenda (Holt et al., 2020).

Cyberterrorism Definition

"Cyberterrorism" was chased by Barry Collin in the 1980's. The fact that terrorism caused via kinetic force has not been unified yet in the transnational doctrine really impeded determining a proper description for its subcategory, cyberterrorism. In a way, defining cyberterrorism is indeed more delicate because of the image that's naturally intertwined in understanding how certain events do in cyberspace (Kostadinov, 2012). Since also,cyber-attacks have been reproduced. In 2007, a massivecyber-attack passed in Estonia. For nearly 2 months, the websites of authority, several banks, and media endured courtesy rejection attempts (Ottis, 2008). No association affirmed the responsibility for thecyber-attacks, Estonian officers like Foreign Minister Urmas Paet indicted Russia of negotiating the attacks, but both the European Commission and NATO specialized experts were unfit to find believable substantiation of Kremlin participation in the DDoS(Distributed Denial of Service) strikes (Herzog, 2011). On November 24th, 2014, the so- called group Guardians of Peace administered acyber-attack on Sony Pictures Entertainment and blurted particular data of Sony workers and several of the plant's unreleased point flicks. According to Siboni and Siman- Tov(2014) " the purpose of the attack, attributed to North Korea, was to discourage Sony Pictures from releasing amovie, which was concluded as deriding that country's oppressor and portraying the North Korean governance and its leader, Kim Jong- Un, with affront and mockery" (Ottis, 2008).

Cyberterrorism is the illegal destruction or disturbance of digital property to blackjack or force authorities or the humanity into tracking ambitions of a political, religious or ideological nature. As part of terrorism, cyberterror involves the use of data as a armament, system, or target, to achieve terrorist pretensions. Cyberterror exists both outside and outdoors cyberspace and includes the physical destruction of any device, device system or process with an information element. At the smallest common denominator, the information element can be understood to represent a double law. conduct taken to disrupt, deny service, destroy, and tamper with double law are acts of cyberterror. The specific of cyberterror is its capability to take advantage of cheap means to gain disproportionate goods through destruction, declination, scam, corruption, exploitation, and hindrance. Cyberterror can accelerate destructive, or disruptive, action by allowing lesser target content, effect, and effectiveness. Cyberterror can compound or support classical terrorism, or be used as a different form of action in its own right (Nelson et al., 1999).

The term "cyber-terrorism" has come relatively transparent in global accord during last century. It denotes the use of internet for terrorist ambitions, substantially pigmented by political or ideological background. The cyberterrorism itself is the most significant motorist in the matter of reworking the face of moment's terrorism as we know it (Havlíček, 2012). The term terrorist refers to a person who practices terrorism. Terrorists see that they cannot be disdainful to their opponents in current resource explosive warfare, hence they calculate on ways aimed to erode the adversary's moral and corporeal complements (Oprea & Mesnita, 2005). Utmost terrorist acts participate two common features(1) they violation civilians; and(2) they target victims that aren't their true victims, but these victims do impact the target followership(Badey, 1998). Hua and Bapna (2013) define cyberterrorism as an attack carried out by cyber terrorists through information systems to (1) significantly interfere with the political, social or economic functioning of a group or organization of a very important nation, or (2) cause physical violence and/or or cause panic. Hua and Bapna define hackers as individuals who (1) wish to access/modify data, files and resources without having the necessary authorization to do so, and/or (2) wish to block services to

authorized users. Cyber terrorists are individuals or groups who use computing and network technologies to terrorize. (Hua & Bapna, 2013).

The Concept of Intellectual Security

Johnson (2005) in "Maintaining Intellectual Freedom in a Filtered World" aimed at identifying the intellectual security features provided by the Internet to the students in Mankato city in the state of Minnesota, United States. He found that 81% of the students achieved their intellectual security features in terms of freedom of expression via the Internet. Students also achieved intellectual security in terms of freedom of using the internet in education and searching for information that provide them huge amounts of information, thus leading to achieve a kind of intellectual and information security. The researcher also noted that 19% of the students do not care about knowledge and science provided by the internet; rather, they turn to intellectual and moral deviance in their use of the Internet (Johnson, 2005).

Tomlinson, J. (2006) in "Values: The Curriculum of Moral Education" study pointed out the interest of the educational institutions in strengthening intellectual security principles by integrating ethical and cultural values in the educational curriculum in America. The researcher used the analytical approach through addressing a number of studies that tackled intellectual security issue. The study concluded that the school and the teacher lead a major role in strengthening the intellectual security among students through their efforts in spreading the concepts of values and ethics and culture, which are of the educational foundations upon which the curriculum is based (Tomlinson, 2006).

Intellectual security is a relatively modern term, although its content is long-standing in cultural heritage. It has received considerable attention recently. In view of the intellectual, political and cultural developments in the Arab and Islamic world. The First National Conference of Intellectual Security, organized by King Saud University during the period 23-25/5/2009. Al-Reb'i, M. (2009) in "Tthe Role of the Curriculum in Strengthening the Concepts of Intellectual Security among University Students in the Kingdom of Saudi Arabia" examined the role of the curriculum in strengthening the intellectual security concepts among university students in the Kingdom of Saudi Arabia. The study aimed to show the importance of the educational institutions in general and the curriculum in particular, in the formation of the human personality. The study also determined the roles of the school curriculums in explaining, straightening and strengthening the intellectual security concepts among students. The results showed that the role of the curriculum in enhancing intellectual security was moderate; and that the courses that provide the most concepts and information related to intellectual security are those in Education of Islamic Culture (Waswas & Gasaymeh, 2016).

The term "intellectual security" is permanently raised, and the scientific dissertations and studies were abundant about this subject nowadays. That had formed a political, intellectual and security obsession for decision making, toll that became irritating many simple individuals of the community that is because of their exposure to risks of intellectual deviation, which is contradictive to the intellectual security through three domains. The first domain: is using violence against innocents, or at the overcrowded public places. The second domain: is fear of reach of this thinking to the greatest number of people, where intellectual deviation becomes the basis, and the correct moderate thinking is the exception. The third domain: reach of the deviated thinking to the offspring at schools and universities, that forms large extended danger cannot be traditionally confronted (Al-dajah, 2019).

Intellectual security is necessary for every individual in the community and the state, it basically shares in the progress and development of the moderate correct thinking far away from extremism and excessiveness in the trends, practices, and actions. The nation and the state can proceed and become prosperous. Without the intellectual security disorder spreads and the national security disturbs, then that leads to retardation. Intellectual security is the contradictory to the intellectual deviation, and started when Satan deviated and rejected obeying Allah as He ordered him to prostrate to Adam (Peace be upon him). Then, the intellectual deviation was represented since Qabeel killed his brother, Habeel. The Western

World knew terrorist movements, employed violence, because of the intellectual deviation, either in the Christian Religion, or in the Jewish Religion. The religious extremism in Europe led to many wars, the most famous is the war of thirty years between the Catholics and Protestants among the German States, then followed by States of Europe (Wilson, 2009). The same thing in the Islamic Religion, since the Exteriors came in the Day-break of Islam in the First Hijrah Century and waged corruption and killing, so the intellectual security was and is still of humanity preoccupation wherever it was to achieve it and keep it by all means (Al-dajah, 2019).

All along ages the world had witnessed an intellectual deviation at groups believe in deviated and extremist intellectual objectives, either in their religious, or political domains, and the Nazist-National political extremism led to a world war annihilated millions of souls of humans. Also, we do not forget Oklahoma explosions in 1995, and in our modern age incident of September 11th., 2001 had impact on changing the track of international and political relations in the world. The thing that led to destruction, wars, killing, occupation and devastating disorder in many territories of the world, also explosions in Saudi and Jordan. Terrorism is a reality and not only an action, but basically it is an outcome of deviated thinking obliged to be confronted and fought by intellectual, scientific, media and educational institutions; they are responsible for building correct concepts, good human values and fortification of communities against intellectual deviation and bad action. It is evident that intellectual deviation is far from preachings of pure religion, also extremism and exaggeration perhaps could paralyze the movement of the community and the state progress altogether, the thing that demanded states and concerned associations deeply think of restoring intellectual security to its right parth and stability; it is more dangerous from the organized crimes, drugs, community evils or its other diseases. It is a religious, political and a compound social disease, it attempted to extract to itself the legitimacy of working, planning and carrying out, and went persuading itself that it is a right owner and legitimacy, cancelling by that the legitimacy of the state and the nation, and started using its special means to achieve its objectives. The commenced waging corruption on earth through operations of explosion, killing and violating the law, the thing that irritated horror and terror among people (Al-dajah, 2019).

Methodology

This study uses an inductive approach to formulate a general framework. Researchers develop the concept of intellectual security by identifying the basic understanding of cyberterrorism, the difference between cyber terror attacks and supporting activities. The data collection technique used in this research is a secondary data collection technique that is obtained through literature review from libraries and internet. From the book edited by Chen, Jarvis, and Macdonald (2014) *Cyberterrorism: Understanding, Assessment, and Response* was organized under the auspices of the cyberterrorism project. From scientific journals, especially journal Terrorism and Political Violence and Jounal Studies in Conflict and Terrorism. From white paper Center for the Study of Terrorism and Irregular Warfare Monterey, CA. in "Cyberterror: Prospects and Implications"(Nelson et al., 1999). In this research, the researchers obtained data and explained it with descriptive data analysis methods where the concept of intellectual security was developed based on literature of previous studies related to the cyberterrorism project and intellectual security that are relevant to be implemented to counter cyberterrorism.

Result and Discussion

Cyberterrorism Support

The use of information technology by terrorists in carrying out activities supporting cyber terrorism does not include in the definition stated if the information technology is used legally. Whereas these activities can increase the distribution of terrorist messages or increase the efficiency of terrorist groups. So, it is important to explain the difference between cyberterror attacks and support by testing

them through the concepts of confidentiality, integrity, and availability. A breach of confidentiality occurs when an unauthorized user gains access to information. A breach of confidentiality is an act of cyberterror support. A classic example of a breach of confidentiality is obtaining another user's password. A breach of confidentiality is essentially passive. Only when a terrorist group threatens (or implies a threat) some action with stolen information do they cross over to a cyberterror attack an information system integrity violation occurs when information used by the system (either program instructions or data) is altered. This includes changing confidential and direct destruction of data. These modifications can occur while information is within components or when information is in transit between components. Incidents that violate integrity can be categorized as attacks or endorsements. Silent modification of user accounts to allow attackers to access key systems, without threat of action, has no coercive effect. On the other hand, published train routing software modifications intended to generate collisions will intimidate the target audience (Nelson et al., 1999).

Although all cyberterror acts indicate a offense of confidentiality, integrity or accessibility, the knock isn't true. Other illegal acts executed through or against information systems fornon-terrorist ambitions aren't cyberterrorism. Terrorism represents the crossroad of furious felonious exertion and political exertion. The political nature of terrorism is what separates it from other felonious exertion motivated by fiscal gain or particular enmity. In general, spying and felonious exertion don't constitute terrorism, and shouldn't be considered part of cyberterrorism. thus, these types of felonious conditioning are barred from our description, and from this study. The distinction between common felonious exertion and cyberterrorism involves a substantial argentine area – cyberspace conditioning by terrorist groups basically intended to give fiscal support for other operations. This is a real possibility, especially for groups that warrant a guarantor or profit- producing frontal association. also, other authors have argued that the description of terrorism must be expanded to include profitable provocations and conditioning by international felonious associations(TCOs) but that analysis of is beyond the compass of this study (Nelson et al., 1999).

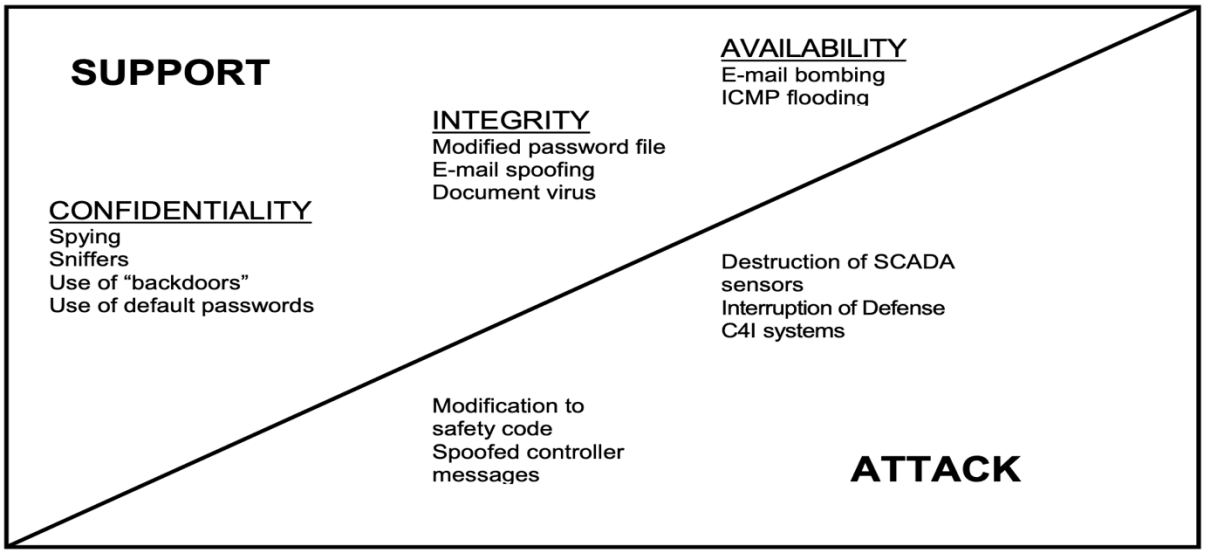

Figure 1. Comparison of Cyberterror Attack and Support

Source: The NPS Institutional Archive (Nelson et al., 1999).

Recognizing that new definitions can be difficult to conceptualize, we provide the following example to help clarify the meaning of cyberterror:

Cyberterror Attack Scenario A aeroplane crash is caused, not by a lemon, but through a palpitation device. The palpitation device was transported on board with a passenger. The intent of the palpitation is to disrupt and permanently loose the information system factors within the aircraft. One disintegrated control process affected by the palpitation was the wharf gear control element. Without the wharf gear in the correct position, among other problems, the aeroplane attempts to land safely but is unsuccessful. However, in this illustration, a lemon were substituted for the palpitation device, If. From this extreme illustration, the argument isn't delicate to make. Examining exemplifications where individualities aren't placed in life hanging (fear producing) situations, however, begins to complicate the description. nonetheless, we argue that the same criteria applied to traditional terrorism should also be applied to cyberterror. formerly again we punctuate the Colombian terrorist bombings of oil painting channels as an illustration where terror, in the life hanging form, fails to develop; but where the incident is indeed distributed as a terrorist act.

We don't dispute the legality of the bombing act in this case. likewise, we employ the same sense when we propose that acyberterror attack be accepted as a form of terrorism (Nelson et al., 1999).

Intellectual Security: Countering Cyberterrorism

The researchers finding at least three basic concepts of intellectual security:

1. Intellectual security as the moderation of human understanding of religious and political issues, understanding deviation and human civilizations.
2. Intellectual security as the harmony between the state and society to save individuals and groups from doctrinal or intellectual that may be the cause of deviations in behavior and thoughts from the right path.
3. Intellectual security as safety of human thought from deviation which leads to maintaining public order, realizing security, tranquility, and stability in political, social, and economic life as well as other elements of national security.

According to the three basic concepts, researchers developed the concept of intellectual security based on literature of previous studies related to intellectual security and theoretical framework that are relevant to be implemented to counter cybercrimes. Some of these studies were also mentioned by Al Osaimi and Al Sufyani (2018). The list of intellectual security concepts is: Islamic ideology, national belonging, cultural belonging, dialogue, positive thinking, human rights, and good citizenship. The implementation of intellectual security in the international environment focuses on preventing deviations from the behavior of the international community, especially on humanitarian issues. In the regional environment, it focuses on strengthening regional sovereignty and harmony, for example on issues of common cultural and historical roots. In the national environment, focusing on domestic policies related to education, social, economic, political and internal state. The implementation of intellectual security in the social environment focuses on the overall conventions, customs, and traditions that influence individual behavior. In the economic environment the focus is on economic issues and the level of individual life. In the political environment the overall focus is on the behavior of the external and internal political systems in general (Al Osaimi & Al Sufyani, 2018).

The development of the concept of handling cyberterrorism by researchers by creating multidimensional solutions through a victim-cantered approach that focuses on prevention. The subject of intellectual security requires social, religious, cultural and political development, uniting the vision and aspirations of the younger generation in society, aiming to limit and then destroy phenomena that are contrary to the values and ideas of a nation. Solutions that can act as self-control and self-monitoring for every human being not to commit cybercrimes are the result of applying religious values that have been implied since childhood. Any type of other solution can be an obstacle to cybercrime, but if every human being feels that God is the controller of every human behavior then there will be no action that is

classified as cybercrime, especially if it is hidden and free in the digital world (Ayeni, 2021). The basis of human control in the form of several references not to commit cybercrimes or not to be deceived by cybercrimes can be identified with the following attitudes: Self-Regulatory (Able to regulate individual self); Self-Control (Able to control every behavior); Self-Monitoring (Able to monitor and monitor crimes that should not be committed).

From the deepened serous studies in this subject, Al- Jihani Studies (1420) from them the called "vision for the Intellectual Security and means of confronting the deviated thinking" (Al-Jihani, pp.245-286), where the concept of intellectual security treated and concluded a comparison between the concept at Moslems from one side and scientists of security and strategy at the west from the other side, for the Jihani clears that the concept at Moslems deeper and more comprehensive for its connection with the divine approach, assuring the significance of intellectual security in the life of Man; because it is clear without vagueness, and it can be reached to the intellectual security aims at protecting the human thinking and his mind, also assures that the intellectual deviation that occurs as a result of dangers that threaten it either internal or external is more dangerous, and must face the deviated or invading thinking, because of its danger on the security of communities and states (Al-dajah, 2019).

This intellectual security can be likened to a vaccine and the threat of cybercrimes such as intellectual deviation, terrorism, and the distortion of their understanding of religious, social and political issues as a virus. Almahaireh (2021) in "The level of intellectual security and its relationship with life satisfaction among mutah university students" also confirms that intellectual security is very relevant in anticipating the increasingly widespread understanding of radicalism and terrorism which leads to the loss of security and stability in various fields of life. This intellectual security is related to life satisfaction and individuals' beliefs about their life, their life situation and what they aspire to be. If a person has a high level of intellectual security, he will achieve satisfaction in life. Therefore, it is necessary to pay attention to the importance of maintaining the level of intellectual security (Almahaireh et al., 2021).

Conclusion

Cyberterrorism continues to cultivate and the strategies used to conduct the communication of terror are also carried out in varied ways. Some groups will hold on to the use of classical terrorist styles and others use chemical, biological, radiological, or nuclear weapons. Another option that terrorists use as armament is cyber terror. The impact that knows no limitations of location and occasion due to cyberterrorism attacks is involved to study more deeply. Cyberterrorism is the unlawful destruction or dislocation of digital property to blackjack or force authorities or societies in the pursuit of pretensions that are political, religious, or ideological. The experimenters chancing at least three introductory generalities of intellectual security as the temperance of mortal understanding of religious and political issues, understanding divagation and mortal societies; Intellectual security as the harmony between the state and society to save individualities and groups from doctrinal or intellectual that may be the cause of diversions in actions and studies from the right path; Intellectual security as safety of mortal study from divagation which leads to maintaining public order, realizing security, tranquility, and stability in political, social, and gainful life as well as other fundamentals of public security.

References

Al-dajah, H. A. (2019). Contemporary Theory of Intellectual Security. *ResearchGate*, *15*(July), 10–22. https://doi.org/10.3968/10733.

Al Osaimi, B. J., & Al Sufyani, D. B. (2018). The Intellectual Security Concepts In The English Textbooks Of The Intermediate Stage In Saudi Arabia:, An Analytical Study. *International Interdisciplinary Journal of Education*, *7*(1), 129. https://doi.org/10.36752/1764-007-001-011.

Almahaireh, A., Alzaben, M., Aladwan, F., & Aljahani, M. (2021). The level of intellectual security and its relationship with life satisfaction among mutah university students. *Journal of Social Studies Education Research*, *12*(3), 28–46.

Ayeni, O. B. (2021). *Branding and Marketing Nigerian Churches on Social Media* (Issue September 2021). Springer International Publishing. https://doi.org/10.1007/978-3-030-77204-8_6.

Badey, T. J. (1998). Defining international terrorism: A pragmatic approach. *Terrorism and Political Violence*, *10*(1), 90–107. https://doi.org/10.1080/09546559808427445.

Chen, T. M., Jarvis, L., & Macdonald, S. (Eds.). (2014). *Cyberterrorism: Understanding, Assessment, and Response*. Springer. https://doi.org/10.1007/978-1-4939-0962-9.

Committee, C. D. (2008). *Cyber securities and Cyberterrorism*. Vardhaman Mahaveer Open University.

Denning, D. E. (1999). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. *Nautilus Institute for Security and Sustainability*. https://doi.org/10.1300/J104v24n01_12.

English, R. (Ed.). (2021). *The Cambridge History of Terrorism*. Cambridge University Press. https://doi.org/10.1017/9781139540902.

Havlíček, J. (2012). Threat of Cyberterrosim. *Association for International Affairs Prague NATO Summit*. https://www.amo.cz/wp-content/uploads/2016/01/PSS-Threat-of-Cyberterrorism-NATO.pdf.

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, *4*(2), 49–60. https://doi.org/10.5038/1944-0472.4.2.3.

Holt, T. J., Lee, J. R., Freilich, J. D., Chermak, S. M., Bauer, J. M., Shillair, R., & Ross, A. (2020). An Exploratory Analysis of the Characteristics of Ideologically Motivated Cyberattacks. *Terrorism and Political Violence*, *34*(7), 1305–1320. https://doi.org/10.1080/09546553.2020.1777987.

Hua, J., & Bapna, S. (2013). The Economic Impact of Cyberterrorism. *Journal of Strategic Information Systems*, *22*(2), 175–186. https://doi.org/10.1016/j.jsis.2012.10.004.

Johnson, D. (2005). Maintaining Intellectual Freedom in a Filtered World. *Learning & Leading with Technology*, *32*(8), 39–41.

Kostadinov, D. (2012). *Cyberterrorism Defined (as distinct from "Cybercrime")*. InfoSec Institute. https://resources.infosecinstitute.com/topic/cyberterrorism-distinct-from-cybercrime/.

Nelson, B., Choi, R., Iacobucci, M., Mitchell, M., & Gagnon, G. (1999). *Cyberterror: Prospects and Implications*.

Oprea, D., & Mesnita, G. (2005). The Information System and The Global Terrorism. *Collaborative Support Systems in Business and Education, International Workshop, October*. ssrn: https://ssrn.com/abstract=906289.

Ottis, R. (2008). Analysis of the (2007) Cyber Attacks Against Estonia from the Information Warfare Perspective. *7th European Conference on Information Warfare and Security 2008, ECIW 2008*, *April*, 163–168.

Piazza, J. A., & Guler, A. (2019). The Online Caliphate: Internet Usage and ISIS Support in the Arab World. *Terrorism and Political Violence*, *33*(6), 1256–1275. https://doi.org/10.1080/09546553.2019.1606801.

Tomlinson, J. (2006). Values: The curriculum of moral education. *Children and Society*, *11*(4), 242–251. https://doi.org/10.1111/j.1099-0860.1997.tb00033.x.

Tucker, D. (2000). *The Future of Armed Resistance: Cyberterror? Mass Destruction?*.

Waswas, D., & Gasaymeh, A.-M. M. (2016). The Role of School Principals in the Governorate of Ma'an in Promoting Intellectual Security among Students. *Journal of Education and Learning*, *6*(1), 193. https://doi.org/10.5539/jel.v6n1p193.

Weimann, G. (2004). *Cyberterrorism: How Real is the Threat?* https://doi.org/10.1080/01296612.2002.11726680.

Wilson, P. H. (2009). *Europe ' s Tragedy: A New History of The Thirty Years War*. Penguin Books Limited.

Copyrights