Politea : Jurnal Pemikiran Politik Islam
P-ISSN : 2621-0312
E-ISSN : 2657-1560
Vol. 5, No. 2 Tahun 2022
DOI : 10.21043/politea.v5i2.17369

Cyber-Terrorism of ISIS and The Challenge Towards Global Security

Titis Margiati
Universitas Pertahanan Republik Indonesia, Bogor, Indonesia
titismargiati@gmail.com

Umi Qodarsasi
Institut Agama Islam Negeri Kudus, Jawa Tengah, Indonesia
umiqodarsasi@iainkudus.ac.id

Abstract
Aktivitas terorisme tidak lagi dilakukan secara tradisional, tetapi telah mengadopsi cara yang lebih modern dengan memanfaatkan teknologi informasi. Kelompok teroris bahkan telah meluncurkan proses perekrutan dan penggalangan dana untuk kegiatan teroris melalui media elektronik. Makalah ini bertujuan untuk mengidentifikasi bagaimana ISIS menggunakan dunia maya untuk melakukan aksi terorismenya dan bagaimana inisiatif global untuk mengatasi terorisme dunia maya. Penelitian ini menggunakan pendekatan deskriptif kualitatif. Data penelitian ini diperoleh berdasarkan studi pustaka yang bersumber dari penelitian terdahulu berupa jurnal, buku dan karya ilmiah lainnya yang relevan dengan topik pembahasan. Hasil dari tulisan ini adalah ISIS menggunakan dunia maya untuk beberapa tujuan, antara lain penyebaran propaganda, rekrutmen global, penggalangan dana, publikasi, perencanaan penyerangan, dan kegiatan lainnya untuk meningkatkan eksistensinya. Untuk memerangi terorisme internasional membutuhkan kontra-terorisme yang didasarkan pada kemitraan antara semua tingkat pemerintahan, masyarakat dan sektor swasta. Dalam dunia yang saling bergantung dan mengglobal, kemitraan multilateral, regional, dan bilateral telah terbukti penting untuk mencapai tujuan keamanan global dan kontra-terorisme. Sebagai komitmen terhadap keamanan siber global, PBB membangun kapasitas teknis dan menyiapkan pedoman bagi negara-negara anggota untuk mengantisipasi kejahatan di dunia siber, termasuk terorisme siber.

Kata kunci: ISIS, Keamanan Global, Terorisme Siber.

Abstract

Terrorism activities are no longer carried out traditionally but have adopted a more modern way by utilizing information technology. Terror groups have even launched recruitment and fundraising processes for terrorist activities through electronic media. This paper aims to identify how ISIS uses cyberspace to carry out its acts of terrorism and how global initiatives are to tackle cyberterrorism. This study used a qualitative descriptive approach. This research data was obtained based on a literature review sourced from previous research in the form of journals, books and other scientific works that are relevant to the topic of discussion. The result of this paper is ISIS uses cyberspace for several purposes, including propaganda dissemination, global recruitment, fundraising, publication, attack planning, and other activities to increase its existence. To fights against international terrorism requires counterterrorism that based on partnership between all levels of governments, communities, and the private sectors. In a globalized, interdependent world, our multilateral, regional and bilateral partnerships have proven critical to achieving global security and counter-terrorism objectives. As a commitment to global cyber security, the United Nations builds technical capacity and prepares guidelines for member countries to anticipate crimes in cyberspace, including cyberterrorism.

Keywords: Cyberterrorism, Global security, ISIS

Introduction

The role of technology is increasingly strategic because of its involvement in the arena of asymmetric warfare (Siagian, Budiarto & Simatupang, 2018. Asymmetric Warfare is a model of warfare developed from an unusual way of thinking, and outside the applicable rules of warfare, with a spectrum of war which is very broad and includes *astagatra* aspects (a combination of *trigatra*: geography, demography, and natural resources/natural resources; and *pancagatra*: ideology, politics, economy, social, and culture). Asymmetric warfare always involves warfare between two or more actors, with the salient feature of unequal forces (Dewan Riset Nasional, 2008). Technology has been adopted in various fields and interests to make it easier for user actors to exploit the defense and security vulnerabilities of a country that is asymmetrical targets (Soewardi, 2013). It means, in asymmetric warfare according to strategic interaction theory (strategic interaction) explained by Ivan Arreguin-Toft, if the strategy approach used the same (indirect-indirect or direct-direct), then the actor who stronger will be able to win the war (Toft, 2005). But if approach the strategy used is different (indirect-direct or direct-indirect), then weaker actor will win the war (Toft, 2005). Various forms of threats due to the adoption of technology in asymmetric warfare are hacking of critical infrastructure, information warfare, terror efforts, radicalization, propaganda, and various other forms of cyber threats that have the potential to weaken a country's sovereignty. Asymmetric warfare by utilizing information technology is considered to bring a more serious threat. This is because cyberspace can blur the boundaries between countries (borderless). In addition, threats in cyberspace are dominated by non-state actors such as hackers, non-governance organizations (NGOs), terrorist groups, and certain actors who have interests in the strategic environment. Even in cyberspace, asymmetric actors will easily attack critical sectors in a country if the country does not have sophisticated cyberspace security aspects (Rahmawati, 2017).

Cyberspace according to The International Telecommunication Union (ITU) of the United Nations stated that cyber space is a field (terrain) both physically and non-physically created from the interconnection between computers, computer systems, networks and computer programs, computer data, content data, data traffic, and users or user (Even & Tov, 2012). Based on the statement from ITU, US Military Document defines cyber space as a global domain of various information consisting of a network or networks that are interconnected with information technology infrastructure, networks internet, telecommunications networks, computer systems, and processors (Even & Tov, 2012). In Chinese military studies, cyberspace has been considered an ideological battlefield. For the Chinese Communist Party, cyberspace has presented a threat to the very survival of its people and is almost existential. So in response to this, China seeks to control content and dominate discourse in cyberspace, including through censorship and propaganda strategies which are its internal and external focus (Kania, 2020). Cyber warfare can be interpreted as a war within cyberspace, but in cyber warfare there are different attacks by attacking in a conventional war or other physical war. The main media used in cyber warfare are computers and the internet. The object attacked in cyber warfare is not a physical area, territorial area, or geographical area, but objects in cyberspace controlled by a country (Subagyo, 2015). Cyber warfare is closely related to psychological warfare (Ahluwalia,V.K., 2020). Psychological warfare is an integral element of cyber warfare operations related to cyberspace and electronics. Such a model of war is seen as important to seize the dominance of discourse in future political or military struggles. Cyberspace is like a double-edged sword. It can be a medium that supports the state's strength in defense and security aspects, but at the same time it can open huge potential threats. State sovereignty is increasingly at stake with operations in the cyber world.

Cyberspace as a modern threat to the current generation of war is certainly influenced by various factors, one of which is ideology. Ideology has an important role in influencing today's cyber activity. As it is known that cyber activity is described as all forms of activity that utilize digital technology (Craigen, Thibault & Purse, 2014). The transformation of the use of digital technology since the era of its emergence continues to grow rapidly. Cyberspace has become a domain for movements based on ideological factors. It is undeniable how the narrative of radicalism, provocation of certain ideologies and other forms of threats occur so massively in cyberspace. The interests of cyberspace controlling actors determine cyber activity. In the context of Indonesia, this phenomenon has also become an increasingly serious concern (Budi, Wira & Infantono, 2021). The defense and security system is no longer only focused on military aspects but also on non-military aspects such as cyberspace.

The transformation of cyber activity is formed due to the increasingly massive role of ideology. According to experts, changes in political orientation and ideology are the causes that change the way technology is used. Ideology and perspectives that are believed by most of the community are the determinants of collective action in cyberspace (Holt, Thomas J, 2020). The actors consider that cyber activity is the most effective method for carrying out actions (Gerbaudo, 2017). This condition poses a dilemma, because in the current era of modernization the need for information technology is getting higher, but at the same time the threats are becoming increasingly complex.

In this study, the potential asymmetric threats in question will be focused on the field of terrorism. As it is known that currently terrorism activities are no longer carried out traditionally but have adopted a more modern way by utilizing information technology. Terror groups have even launched recruitment and fundraising processes for terrorist activities through electronic media. This can be seen from the training module "*The Terrorist Handbook*" and the bomb-making module "*The Mujahadeen Positions Handbook*", which have been distributed through the terrorist group's website. As explained above, the researcher is interested in studying how terrorism activities are carried out in cyberspace and how the impact is due to terrorist activities in cyberspace. The researcher carries the title *Cyber-Terrorism and The Challenge Towards Global Security* with two research questions, consist of how ISIS terrorism activity in cyberspace is and what is the challenge of cyber terrorism to global security.

This study used a qualitative descriptive approach. This research data was obtained based on a literature review sourced from previous research in the form of journals, books and other scientific works that are relevant to the topic of discussion, namely cyberspace as a dimension of asymmetric war threats and terrorism activities in cyberspace.

Result and Discussion

Cyber-Terrorism of Islamic State of Iraq and Syria (ISIS)

The Terrorism Act 2000 defines terrorism as the use of threats of one or more acts which include serious violence against a person; serious damage to property; activities that endanger the life of a person or group of people; creates a serious risk to the health or safety of the public or part of the community; and actions designed to disrupt electronic systems. Such actions are designed to influence governments, organizations, or to intimidate the public. Threats are carried out for purposes related to certain politics, religion, ideology, or race (The Crown Prosecution Service, n.d., 2000). The United Nations Security Council resolution 1566 (2004) states that terrorism refers to criminal acts, including against civilians, which are carried out with the intent to cause death or serious bodily injury as well as hostage-taking. The purpose of this terrorist activity is to create a state of terror in a particular community or group of people, to intimidate a population or to force certain governments or organizations to take or not to take certain action (Nations & Rights, n.d., 2004).

Definitions and rules related to terrorism are contained in Law Number 5 of 2018 concerning Stipulation of Government Regulations in Lieu of Law Number 1 of 2002 concerning Eradication of Criminal Acts of Terrorism, terrorism is understood as an act that uses violence or threats of violence that creates an atmosphere of terror or fear widespread, which can cause mass casualties, and/or cause damage or destruction to strategic vital objects, the environment, public facilities, or international facilities with ideological, political or security disturbance motives. Based on several definitions related to terrorism, it can be understood that Terrorism is the use of force or violence against a person, group of people or property that creates an atmosphere of terror or fear in the community with the aim of intimidating and coercing (ICLU, 2018).

Meanwhile, Gibson describes cyberspace as a place that is not real, but its existence can be felt and even become a reality in the mind. More clearly, Gibson defines cyberspace as follows (Nasrullah, 2014) :

> "*a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts – A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding*".

Based on the above definition, it can be concluded that cyberspace is a conceptual space that links all human relationships, data, welfare, and the power manifested through technology. U.S. The Department of Defense defines cyberspace as a global domain in the information environment consisting of a network of interdependent information technology infrastructure, including the Internet, telecommunications networks, computer systems, processors and controllers. (Office of the Joint Chiefs of Staff, 2010). According to Krippendorff (2010) cyberspace results from the collective ability of humans to articulate the possibilities in which technological artifacts are designed, used, and conceptualized (Krippendorff, 2010). Cyberspace according to the Russian-American Cyber Security Summit is described as an electronic medium in which information is created, sent, received, stored, processed and deleted. (Mbanaso & Dandaura, 2015).

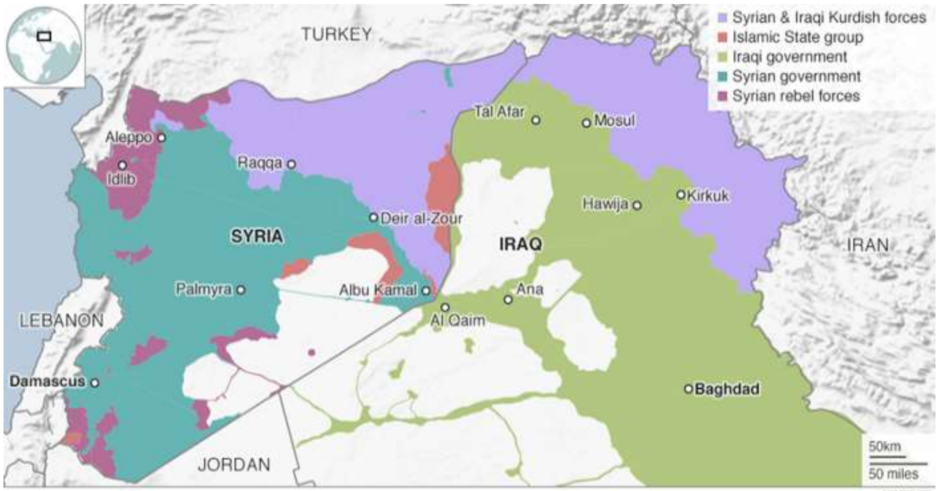
Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear (Plotnek & Slay, 2019). Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not (Weimann, 2004). Cyber terrorism is an activity that involves active or passive action. Active means use the computer to infiltrate the important infrastructure in the country, such as electricity, emergency services, telecommunications, air supply, economy, military, and financial institutions a country which can be fatal. Meanwhile, passive indicates that cyberterrorism can also do recruitment, seeking support, and purpose of propaganda aimed at to spread fear towards global community in cyberspace (Widiyanto, 2017).

The roots of cyber terrorism emerged along with the development of information technology in the early 1990s. Terrorists build networks that are getting stronger with the Internet. This internet then gave rise to the term cyber-terrorism where a group of terrorists use cyberspace (a variety of Internet applications) in carrying out their acts of terrorism. Seib & Janbek (2011) explain that the internet allows the dissemination of information that is fast, low risk, and inexpensive to a variety of constituencies, ranging from potential recruits to potential partners in terrorist organizations. This method prevents them from receiving widespread media attention. Paradoxically, the mass media themselves use the web to find traces and messages about the latest terrorism they carry out that will encourage the emergence of international public opinion. (Sarinastiti & Vardhani, 2017).

Soriano (2008) explains that cyberspace can allow direct communication between terrorists and their public. The Internet not only fills the limitations of mass media, but the Internet also allows them to circumvent several moral rules contained in the mass media and limit their actions, and this is beneficial for their terrorism strategy. As jihadist groups did following the 2003 invasion of Iraq, the Internet not only allows them to avoid operational risks, but allows them to gain access by infiltrating traditional media systems such as Al-Jazeera (Sarinastiti & Vardhani, 2017).

ISIS (Islamic State of Iraq and Syria) is a movement that carries an "ultra-puritan" ideology. On June 29, 2014, ISIS declared itself an Islamic State with a new political entity "caliphate" and appointed Abu Bakr Al-Baghdadi as caliph for Muslims worldwide. ISIS uses Iraq and Syria as regional bases with Raqqah being the center of control of all its oversight activities. The development of ISIS is inseparable from the regional political situation where Middle Eastern countries are undergoing political transitions, democracy, and unfinished revolutionary upheaval (Haryanto, 2015).

The jihadist exploited the chaos, instability and divisions within both Iraq and Syria. IS grew out of what was al-Qaeda in Iraq, which was formed by Sunni militants after the US-led invasion in 2003 and became a major force in the country's sectarian insurgency. In 2011, the group joined the rebellion against President Bashar al-Assad in Syria, where it found a haven and easy access to weapons. At the same time, it took advantage of the withdrawal of US troops from Iraq, as well as widespread Sunni anger at the sectarian policies of the country's Shia-led government. In 2013, the group began seizing control of territory in Syria and changed its name to Islamic State in Iraq and the Levant (ISIS or ISIL) (Al Zor, 2022) . ISIS expansion into Iraq and Syria is shown in the map below:



Source: IHS Conflict Monitor (23 March 2018) BBC

Figure 1. ISIS Spread Across Iraq and Syria (Source : HIS Conflict Monitor – 23 March 2018, BBC) https://www.bbc.com/news/world-middle-east-27838034

Zuhairi Misrawi stated that ISIS was slipping into an atmosphere of democratic transition that was not going well, especially in Iraq and Syria. Zuhairi gave several reasons to justify ISIS, consist of: 1) Western imperialism over the Islamic world in various aspects of life, politics, economy, social and religion; 2) Israel's invasion of Gaza and the West Bank; 3) rejection of the democratic system which he considers as an infidel Western system and can weaken Muslims; and 4) the existence of global inequality and social injustice that ensnares the Islamic world (Haryanto, 2015). There are several things that encourage the spread of ISIS ideology. *First*, there are the theological views and beliefs that are the same as the ISIS group. Some Muslims see the correlation of the ISIS movement with predictions of the rise of the Islamic caliphate in the future. *Second*, ISIS calls for sectarianism against Shia. *Third*, there is a sense of sympathy and feelings of fate as Muslims towards the Syrian people (Rijal, 2017).

Islamic States of Iraq and Syria (ISIS) and The Objective of Cyber-Terrorism

The Internet contributed greatly to revolutionizing movements. Terrorist groups can carry out various activities such as fundraising and training that were previously done face-to-face, now can be done through websites and virtual camps. In studying locations and planning terror or attacks, they use geospatial imagery such as google earth. Potential attacks that present great danger to a country are hacking or cyber-attacks aimed at a country's infrastructure from computers in other parts of the world. Likewise, the Internet has emerged as a dangerous tool for terrorist propaganda and recruitment purposes (Lieberman, 2017).

Most organizations or businesses use social media to promote their products or services to encourage people to stay loyal to their products or services. Terrorist groups have imitated this and have used social media to carry out public propaganda and to get audiences to support their activities (Marcu & Balteanu, 2014). Terror groups usually have multiple accounts to spread their message. In 2016, Twitter removed more than 124,000 user accounts linked to ISIS or found to have spread propaganda from ISIS. Even today, the Terror Group still has a huge influence on the online media. And they seem to immediately create a new account as soon as possible once the old one has been blocked. They regularly create and upload quality and professionally made videos and images to attract and convince social media users that 'Jihad' is the best invitation. On social media accounts, the Terror Group describes its caliphate as a haven for Islamic teachings. ISIS, however, regularly uploads horrific videos of bombings and killings. It was done to spread terror and a message of fear to innocent people. This is also done to perceive that violence as normal and noble for his followers (Ozkaya, 2017).

The use of technology in acts of terrorism is recorded in a journal written by Charlie Winter. In his writings, Charlie revealed that since 2014, ISIS has been actively carrying out propaganda by carrying out the idea of a caliphate. The ease of access to information through electronic means has resulted in victims who are indicated to be exposed to terrorism, regardless of age or background. The example that shows an equally dire impact due to the use of technology for acts of terrorism is the ease with which members of terrorist groups can conduct training. The training module "The Terrorist Handbook" and the bomb making module "The Mujahadeen Positions Handbook", have been distributed through the terrorist group's website (Perwita & Yani, 2005). There are many reasons why terrorists use the power of social media and the Dark Web to support their activities. It all boils down to the fact that social media platforms have a wider following than any other type of media. Therefore, terrorists can easily reach millions and even billions of people very effectively.

The increase in internet access in the African continent and the Middle East has contributed to the increase in ISIS cyber activity. Increasing internet access has further expanded ISIS' reach both in spreading propaganda and recruiting terrorists from various countries (Ward, 2018). Conway (2003) explain that terrorist's use of social media and the Internet to pursue their ideological aims is well documented. This includes terrorist groups such as ISIS who are using the Internet and social media sites, as a tool for propaganda via websites, sharing information, data mining, fundraising, communication, and recruitment. According to Weimann (2004), they using the Internet for psychological warfare, publicity, propaganda, fundraising, recruitment, networking, sharing information and planning (Awan, 2017).

There are many reports stating that many people left their home countries to go to Syria, and Iraq to join ISIS. It is estimated that ISIS has received more than 40,000 foreign national who have mobilized from 120 countries to join as fighters (*Foreign Terrorist Fighters*, n.d.). ISIS fighter from around the world shown in the table below:

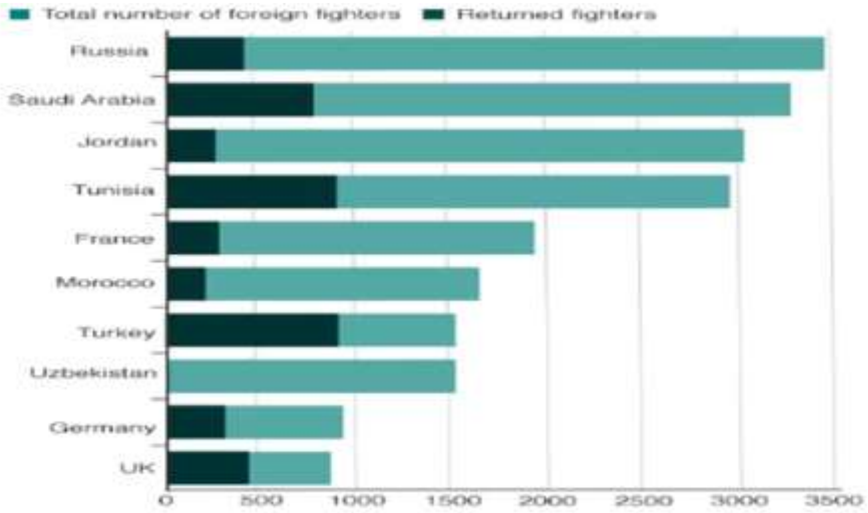


Chart 1. Nationalities of IS Foreign Fighters ((Source : HIS Conflict Monitor – 23 March 2018, BBC) https://www.bbc.com/news/world-middle-east-27838034

ISIS media strategy is louder, consistent, and modern. Starting from the way they frame the news to compiling training manuals that can produce quality propaganda. One of ISIS' main goals is to recruit youth from all over the world to join ISIS. For this reason, ISIS's target media is to indoctrinate them with the propaganda of "benefit" living in the Islamic States. An example of this propaganda is in the narrative in one of ISIS' online magazines "Dabiq", ISIS describes the area it controls as a peaceful, peaceful area, and provides homes for militants. ISIS also strengthens its claim with photos of fighters relaxing over tea, singing in an atmosphere full of brotherhood (Khawaja & Khan, 2016). ISIS has media production companies, that are the al-Furqan Institute for Media Production and the al-Hayat Media Center. Al- Furqan mainly produces CDs, DVDs, posters, pamphlets, and web-related propaganda products. Al-Hayat Media Center targets the Western audiences. It produces the online magazine Dabiq in English, and many other languages. Dabiq Magazine can reach a wider audience because it is produced in various languages (Savitri, 2020).

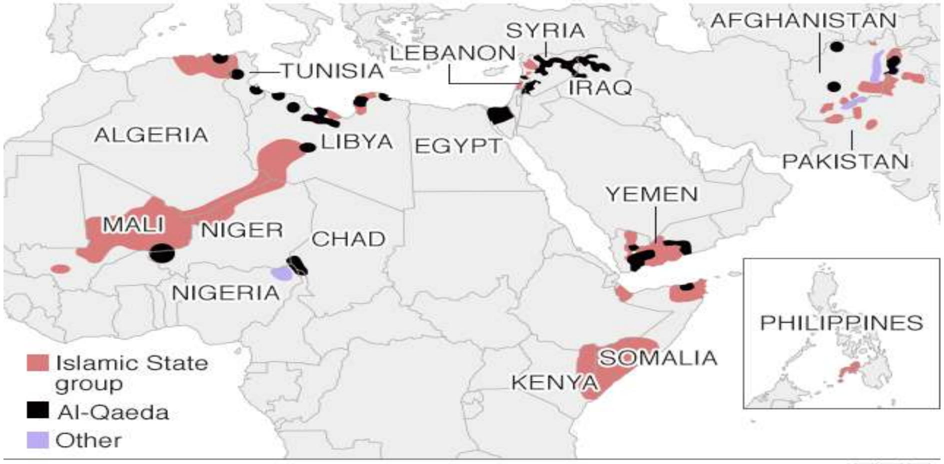
Besides propaganda and recruitment, ISIS also used internet to plan attacks. Terrorists have turned their attention to not only using social media but are also now starting to exploit the use of the Dark Web. They use the Dark Web to complement their activities in addition to what they already do on social media platforms. They use social media to recruit and spread propaganda and use the Dark Web for transactions, and more covert communications such as planning attacks. (Spalevic & Ilic, 2016). There is a Dark Web that specializes in the sale and supply of weapons, ammunition, and explosives. Investigations into the 2015 Paris attacks showed that the guns used for shooting were purchased from a Dark Web store. The supplier was identified as a German citizen operating on the Dark Web under the username DW Guns. This is one of the places where terrorists can buy weapons from the Dark Web (Forbes, 2019). In 2016, former US President Barack Obama said that terrorists had purchased radioactive isotopes from brokers on the Dark Web (Spalevic & Ilic, 2016). In March 2015, ISIS collected several data they take from various sources on the internet and elaborate the data. Then, they create a hit list or a list of targets that are will be attacked explicitly and create 100 data about personnel US military, including photo, physical, address e-mail, and mobile phone number each of them. All this data obtained by hacking multiple military servers, databases, and email every US military personnel at Army, Navy, and Air Force. They also send email to the victim, containing that ISIS will attack individuals the US citizen if known that they were involved in the resistance against ISIS and the resistance against ISIS propaganda in cyberspace (Widiyanto, 2017).

ISIS also uses the internet to raise funds. ISIS gets funding from various sources. These sources are people who have been deceived into beliefs carried out through terrorist propaganda. There is a Dark Web called “Fund the Islamic Struggle without Leaving a Trace” where people can donate anonymously for the so-called “Jihad”. There are rumors that some oil-rich countries in the Middle East and Asia are also key donors of several Islamic-affiliated terrorist organizations (Stergiou, 2016). The Dark Web is a hotbed of illegal activity.

Some of the findings above prove that territorial boundaries cannot be used as a benchmark for categorizing an act of terrorism, because terrorist activities are becoming increasingly massive through cyberspace. After the events of 9/11 which showed the existence of terrorism groups, the world's attention to the issue of terrorism became more serious, especially in the formulation of counter-terrorism strategies. The development of terrorism is increasingly in line with the development of the era due to globalization. Terrorism is even considered as the dark side of globalization, which according to James H. Wolfe is influenced by three main factors, namely rational motivation (factors from rational desire and thinking), psychological motivation and cultural motivation (push that comes from culture) (Vermonte & Wicaksono, 2020).

Cyber-Terrorism of ISIS and The Challenge to Global Security

Chandler and Gunaratna explained that after 9/11 there were three important phenomena in the dynamics of global politics and security. First, the transformation of Al-Qaida. Second, Iraq has become a "land of jihad". Third, the support of Muslim communities in various countries for the narrative of "hate" against the United States and the domination of the West over Islamic society (Rijal, 2017). These three things make the ISIS ideology continue to spread, not only in Iraq and Syria, but also to various countries, especially those with a majority Muslim population. The spread of ISIS ideology in various countries is shown on the map below:



Source: US Office of the Director of National Intelligence BBC

Figure 2. Global Reach of ISIS ((Source : HIS Conflict Monitor – 23 March 2018, BBC) https://www.bbc.com/news/world-middle-east-27838034

Based on evidence found by the US National Counterterrorism Center, since August 2016 IS is reported to have expanded and operated in 18 countries around the world including Afghanistan and Pakistan. In addition, there are also findings that they have "aspiring branches" in Mali, Egypt, Somalia, Bangladesh, Indonesia, and the Philippines. IS also claimed responsibility for various attacks that occurred in several countries such as Egypt, Turkey, Indonesia, France, Germany, US, Finland and Bangladesh. (*Islamic State and The Crisis in Iraq and Syria in Maps*, 2018).

International terrorism is a form of asymmetric warfare. The roots of international terrorism are often related to injustice or inequality in global society so that there are parties who are alienated. Meanwhile, the international system has not been able to provide a democratic solution to this inequality (Ghosh, 2014). Security aspects in globalization are complex and multi-dimensional. It is no longer relevant to use traditional national security boundaries to deal with this terrorism threat. In this era of globalization, where nations have become interconnected and dependent, the threat of theory is no longer a threat to one nation, but a threat to international security. Awareness about this common threat to terrorism emerged after the 9/11 attacks in the United States where terrorists targeted the attack on the World Trade Center as a representation of the economic dimension of globalization and the Pentagon as a representation of the political and military dimensions. In other words, terrorism has placed globalization among its targets (Ghosh, 2014).

Terrorism has changed and is becoming more challenging. With the changing development of globalization and technology, terrorist groups use cyber spaces to carry out attacks, publications, propaganda, recruitment, fundraising and other activities to support the terrorism. Information security is very important for many organizations, including terrorist. The reason for this lies in their malicious activities, so it's clear that they will be confronted with a full-fledged government security force and its troops, who can easily express their intentions through communication interception using sophisticated monitoring equipment. The “Al Qaeda Training Manual” is just one of many proofs of commitment terrorist organizations for secure communications. Among the most important and the most extensive descriptions of this guide are the two lessons that provide guidance on proper use of communications and data protection. Special emphasis on this issue placed in the thirteenth lesson "Writing Secrets and Passwords and Codes" which aims to train would-be members of this terrorist organization for secure data transmission (Bogdanoski & Petreski, n.d.).

To fights against international terrorism requires counterterrorism that based on partnership between all levels of governments, communities, and the private sectors. In a globalized, interdependent world, our multilateral, regional and bilateral partnerships have proven critical to achieving global security and counter-terrorism objectives (*Counter Terrorism*, n.d.). There must be a universal countermeasure and a cosmopolitan approach in the world's struggle against global terror in the 21st century. The emphasis on national sovereignty and the reluctance of states to get involved when the threat does not seem to occur in their homeland will jeopardize cooperation between countries. What will keep us all safe is collective activity directed at new threats such as global terror. Because of the new characteristics of terrorism, and its relationship to globalization, the terrorist threat requires a complex response from transnational cooperation (Ghosh, 2014).

Cyber security is one of the main themes in the debate on the UN security policy system, especially about the threat of terrorism and how the resolutions are issued by the

UN security council. The UN Global Counter-Terrorism Strategy aims not only to “counter terrorism in all its forms and manifestations on the Internet”, but also to a more active approach to “use the Internet as a tool to counter the spread of terrorism.” Cyber security will also continue to be developed in international agendas for international security. Within the United Nations system, the International Telecommunication Union (ITU) has responsibility for the practical aspects and implementation of international cybersecurity. In September 2008, ITU and the International Multilateral Partnership Against Cyber Threats (IMPACT) signed an agreement under which GCA is located at IMPACT's headquarters in Cyberjaya, Malaysia (Bogdanoski & Petreski, n.d., 2008).

The Global Counter-Terrorism Strategy includes several references calling for cooperation in combating the use of ICT for the purposes of terrorism, including in the field of social media. It also supports open internet, and the right to privacy in online activities and in communication surveillance, eavesdropping, and collection. Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights are referenced time and again to anchor human rights responsibilities when dealing with ICT-related activities (Walker, 2019).

As a commitment to global cyber security, the United Nations builds technical capacity and prepares guidelines for member countries to anticipate crimes in cyberspace, including cyberterrorism. Within the ITU, the Cyber Threat Insight Program offers member states two tools to combat cybercrime. HORNET provides technical assistance through a network of strategically placed sensors, which capture data about malware and other attacks, to provide countries with information about threats, so they can better understand and help mitigate them. While the second tool, the Abuse Alert and Reporting Engine, improves the Computer Incident Response Team's ability to collect and analyze data for malicious activity. More broadly, the ITU Global Cybersecurity Index is a survey that measures countries' commitment to cybersecurity, based on five pillars: legal, technical, organizational, capacity building and cooperation (Walker, 2019).

Conclusion

Cyberspace is like a double-edged sword. It can be a medium that supports the state's strength in defense and security aspects, but at the same time it can open huge potential threats. State sovereignty is increasingly at stake with operations in the cyber world. The Internet contributed greatly to revolutionizing movements. The roots of cyber terrorism emerged along with the development of information technology in the early 1990s. Terrorists build networks that are getting stronger with the Internet. This internet then gave rise to the term cyber-terrorism where a group of terrorists use cyberspace (a variety of Internet applications) in carrying out their acts of terrorism. With the changing development of globalization and technology, terrorist groups use cyber spaces to carry out attacks, publications, propaganda, recruitment, fundraising and other activities to support the terrorism.

To fights against international terrorism requires counterterrorism that based on partnership between all levels of governments, communities, and the private sectors. In a globalized, interdependent world, our multilateral, regional and bilateral partnerships have proven critical to achieving global security and counter-terrorism objectives. As a commitment to global cyber security, the United Nations builds technical capacity and prepares guidelines for member countries to anticipate crimes in cyberspace, including cyberterrorism.

References

Ahluwalia, V.K. 2020. *Psychological Warfare: Call out Adversaries' Designs.* CLAWS Journal, Winter 2020

Al Zor, Deir. 2022. *Containing a Resilient ISIS in Central and North-eastern Syria.* International Crisis Group. https://www.crisisgroup.org/middle-east-north-africa/east-mediterranean-mena/syria/containing-resilient-isis-central-and-north

Awan, I. (2017). Cyber-Extrimism : ISIS and The Power of Social Media. *Social Science and Public Policy*, *54*, 138–149. https://doi.org/10.1007/s12115-017-0114-0

Bogdanoski, M., & Petreski, D. (n.d.). 2008. Cyber Terrorism - Global Security Threat. *International Scientific Defence Security Journal*. https://core.ac.uk/download/pdf/35330211.pdf.

Budi, Eko dkk. 2021. *Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0*. Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia Akademi Angkatan Udara, Volume 3, Tahun 2021 hlm. 223-234.

Craigen, Dan dkk. 2014. Defining Cybersecurity. Technology Innovation Management Review, October 2014. http://timreview.ca/article/835

Counter terrorism. (n.d.). Department of Foreign Affairs and Trade of Australian Goverment. https://www.dfat.gov.au/international-relations/security/counter-terrorism/Pages/counter-terrorism

Dewan Riset Nasional (DRN). 2008. *A Thought on Asymmetric Warfare*. Jakarta.

Even, Shmuel dan Tov, Daṿid Siman. 2012. Cyber Warfare: Concepts and Strategic Trends (JSTOR, 2012), hal. 10

Forbes. 2019. *How The Darknet Can Be Used By Terrorists To Obtain Weapons.* Diakses pada 21 November 2022. https://www.forbes.com/sites/nikitamalik/2019/01/15/how-the-darknet-can-be-used-by-terrorists-to-obtain-weapons/

Foreign Terrorist Fighters. (n.d.). United Nations Office on Drugs and Crime. https://www.unodc.org/unodc/en/terrorism/expertise/foreign-terrorist-fighters.html

Gerbaudo, P. (2017). From Cyber-Autonomism to Cyber-Populism: An Ideological Analysis of the Evolution of Digital Activism. *TripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society*, *15*(2), 477–489. https://doi.org/10.31269/triplec.v15i2.773

Ghosh, S. (2014). Understanding Terrorism in the Context of Global Security. *Socrates*, *2*(2).

Haryanto, T. J. (2015). Perkembangan Gerakan ISIS dan Strategi Penanggulangannya (Kasus Perkembangan Awal ISIS di Surakarta). *Jurnal Multikultural Dan Multirelligius, 14*(3).

Holt, Thomas J. 2020. *An Exploratory Analysis of the Characteristic of Ideologically Motivated Cyberattacks*. Political & International Relations Journals, 26 Agustus 2020.

ICLU (Indonesia Criminal Law Update). 2018. *Indonesia's Legal Framework On Terrorism.* Institute For Criminal Justice Reform, Issue No. 3/2018.

Islamic State and The Crisis in Iraq and Syria in Maps. (2018). BBC News. https://www.bbc.com/news/world-middle-east-27838034

Kania, E. B. (2020). The Ideological Battlefield: China’s approach to political warfare and propaganda in an age of cyber conflict. In e. Christopher Whyte. In *Information Warfare in the Age of Cyber Conflict*.

Khawaja, S. A., & Khan, H. A. (2016). Media Strategy of ISIS. *Strategic Studies*, *36*(2), 104–121. https://www.jstor.org/stable/48535950

Krippendorff, K. (2010). The Growth of Cyberspace and the Rise of Design Culture. *Workshop on Social Theory and Social Computing*.

Lieberman, V. A. (2017). Terrorism, The Internett, and Propaganda : A Deadly Combination. *Journal of National Security Law and Policy, 9.*

Marcu, M., & Balteanu, C. (2014). Social Media-A Real Source of Proliferation of International Terrorism. *Annales Universitatis Apulensis: Seroes Oeconomica*, *16*(1).

Mbanaso, U., & Dandaura, E. (2015). The Cyberspace: Redefining A New World. *Bi-Annual Cyber Abuja Conference Centre for Cyber Space Studies*.

Nasrullah, R. (2014). *Teori dan Riset Media Siber (Cybermedia)*. Prenada Media Group.

Nations, O. of the U., & Rights, H. C. for H. (n.d.). 2004. *Human Rights, Terrorism and Counter-terrorism*. UNHCR. https://www.ohchr.org/sites/default/files/Documents/Publications/Factsheet32EN.pdf

Office of the Joint Chiefs of Staff. (2010). *Department of Defense Dictionary of Military and Associated Terms.* https://irp.fas.org/doddir/dod/jp1_02-april2010.pdf

Ozkaya, E. (2017). *The Use of Social Media for Terrorism*. https://www.tmmm.tsk.tr/publication/datr/volume9-2017/03-TheUseofSocial_MediaforTerrorism.pdf

Perwita, B. A. A., & Yani, M. Y. (2005). *Pengantar Ilmu Hubungan Internasional*. PT.Remaja Rosdakarya.

Plotnek, Jordan J & Slay, Jill. 2019. *What is Cyber Terrorism: Discussion of Definition and Taxonomy.* Proceeding of CWAR 2019, Deakin University Centre for Cyber Security and Innovation.

Rahmawati, I. (2017). Analisis Manajemen Resiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defense. *Jurnal Pertahanan Dan Bela Negara*, *7*(2).

Rijal, N. K. (2017). Eksistensi dan Perkembangan ISIS: Dari Irak Hingga Indonesia. *Jurnal Ilmiah Hubungan Internasional*, *13*(1), 45. https://doi.org/10.26593/jihi.v13i1.2670.45-60

Sarinastiti, N. E., & Vardhani, K. N. (2017). Internet dan Terorisme : Menguatnya Aksi Global Cyber-Terrorism Melalui New Media. *Jurnal Gama Societa*, *1*(1).

Savitri, K. (2020). The Islamic State of Iraq and Syria &amp; the Worldwide Web: A Threat to the National Security of Indonesia. *Proceedings of 3rd International Conference on Strategic and Global Studies, ICSGS 2019, 6-7 November 2019, Sari Pacific, Jakarta, Indonesia*. https://doi.org/10.4108/eai.6-11-2019.2297283

Siagian, Lauder dkk. 2018. *The Role of Cyber Security In Overcome Negative Contents to Realize National Information Resilience.* Jurnal Prodi Perang Asimetris, Desember 2018, Volume 4, Nomor 3.

Soewardi, Bagus Artiadi. 2013. *Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia.* Media Informasi Ditjen Pothan Kemhan, Maret 2013.

Spalevic, Z., & Ilic, M. (2016). The Use of Dark Web for the Purpose of Illegal Activity

Spreading. *Ekonomika*, *63*(1).

Stergiou, D. (2016). ISIS Political Economy: Financing a Terror State. *Journal of Money Laundering Control*, *19*(2).

Subagyo, Agus. 2015. *Sinergi dalam Menghadapi Ancaman Cyber Warfare*. Jurnal Pertahanan.

The Crown Prosecution Service. (n.d.). 2000. *Terrorism*. https://www.cps.gov.uk/crime-info/terrorism

Toft, Ivan ArreguinToft. 2005. *How the Weak Wins Wars: A Theory of Asymmetric Conflict* Cambridge: Cambridge University Press, 2005).

Vermonte, P., & Wicaksono, T. Y. (2020). *Karakteristik dan Persebaran Covid-19 di Indonesia : Temuan Awal*. CSIS Indonesia. https://www.csis.or.id/publications/karakteristik-dan-persebaran-covid-19-di-indonesia-temuan-awal

Walker, S. (2019). *Cyber-Insecurities? A Guide to the UN Cybercrime Debate*. The Global Initiative Against Transnational Organized Crime.

Ward, A. (2018). *ISIS's Use of Social Media Still Poses a Threat to Stability in the Middle East and Africa*. RAND Corporation. https://www.rand.org/blog/2018/12/isiss-use-of-social-media-still-poses-a-threat-to-stability.html

Weimann, G. (2004). *Cyberterrorism : How Real Is The Threat?* https://www.usip.org/sites/default/files/sr119.pdf

Widiyanto, B. (2017). Dampak Serangan Virtual ISIS Cyber-Caliphate Terhadap Amerika Serikat. *International & Diplomacy*, *2*(2).