Insignia Journal of International Relations
Vol. 10, No. 2, November 2023, 214-227
P-ISSN: 2089-1962; E-ISSN: 2597-9868

Analysis of the Australian Government's Security Strategy in Countering Potential Threat of Terrorist Groups through Cyber Terrorism Instruments

Suci Cantika
Department of International Relations, Universitas Tanjungpura
E-mail: e1111201045@student.untan.ac.id

Annisa Umniyah
Department of International Relations, Universitas Tanjungpura
E-mail: e1111201052@student.untan.ac.id

Abstract

This paper discusses the strategies adopted by Australia in dealing with and overcoming the violent acts of Cyber Terrorism. Since the terrorist attack on September 11, 2001 in the United States, countries in the world have assumed the existence of terrorist groups as a global threat. Globalization has enabled the terrorist groups to transform conventional media in the cyber world into the infamous cyber terrorism which they use as a propaganda instrument for recruitment, providing logistics, training, forming paramilitaries, planning, carrying out attacks, hiding, and funding. This paper discussed the concept Australian national security which has developed beyond military. The concept of security according to the non-traditional approach is emphasized on the security interests of non-state actors (non-state actors). The present research used descriptive qualitative research, employing literature review or library research for data collection. The results found that the Australian government remains vigilant against cyberterrorism through law enforcement and international cooperation. The Australian government has stipulated the Criminal Code Act 1995 part 5.3 to fight against the acts of terrorism. In addition, to increase domestic skills in cyberspace, The Australian government also establish Australia's Cyber Security, through which the Australian Cyber Security Centre (ACSC) founded Joint Cyber Security Centres (JCSCs), AustCyber, the Australian Cyber Security Growth Network, and the Cyber Security Cooperative Research Centre. and. Australia is also committed to supporting and maintaining international mechanisms that promote stability and to working with partners on a voluntary basis to prevent and respond to threats, including cyber terrorism.

Keywords: Australia, cyber terrorism, national security

Abstrak

Artikel ini menganalisis strategi yang dilakukan oleh Australia dalam menghadapi dan menanggulangi aksi kekerasan Cyber Terrorism. Sejak terjadinya serangan oleh kelompok teroris pada tanggal 11 September 2001 di Amerika Serikat, negara-negara di dunia beranggapan bahwa keberadaan kelompok teroris merupakan ancaman global. Kehadiran globalisasi telah mentransformasikan penggunaan media konvensional ke dalam dunia cyber oleh kelompok teroris, yaitu penggunaan internet yang dikenal dengan istilah cyber terrorism*. Adapun aktivitas teroris yang memanfaatkan jaringan siber yaitu sebagai instrumen propaganda, perekrutan, penyediaan logistik, pelatihan, pembentukan paramiliter, perencanaan, pelaksanaan serangan, persembunyian, dan pendanaan. Dalam membahas tulisan ini, digunakan konsep keamanan nasional yang dalam perkembangannya tidak lagi hanya berkutat pada militer. Dalam pendekatan nontradisional, konsep* *keamanan ditekankan pada kepentingan keamanan aktor non-negara. Dalam tulisan ini, penulis menggunakan metode penelitian kualitatif dengan tipe deskriptif. Peneliti menggunakan tinjauan literatur atau riset kepustakaan sebagai teknik pengumpulan data. Hasil penelitian menunjukkan bahwa pemerintah Australia tetap waspada dengan menegakkan hukum dan kerja sama internasional dalam menghadapi* cyber terrorism*. Beberapa strategi yang dilakukan oleh pemerintah Australia adalah melalui undang-undang tentang pemberantasan tindakan terorisme yang terdapat pada Criminal Code Act 1995 pada bagian 5.3. Pemerintah Australia juga membuat Australia's Cyber Security, melalui strategi ini Australia Cyber Security Centre (ACSC), mendirikan Joint Cyber Security Centres (JCSC), AustCyber, Australian Cyber Security Growth Network, Cyber Security Cooperative Research Centre, dan peningkatan kemampuan di dunia maya. Tidak hanya pada keamanan dalam negeri, Australia juga berkomitmen untuk mendukung dan mempertahankan mekanisme internasional yang mempromosikan stabilitas dan bekerja sama dengan mitra secara sukarela untuk mencegah dan merespons ancaman, salah satunya terorisme siber.*

Kata kunci: *Australia, cyber terrorism, keamanan nasional*

INTRODUCTION

The development of terrorism as a form of transnational crimes encourages countries in the world to improve their country's security. Since the 9/11 terror attack in the United States, making countries, the world consider that the existence of terrorist groups is a global threat. The infamous 9/11 terror attacks was one in four organized suicide attacks targeting the Washington DC and New York regions (Sindi, 2016). The United States President, George W. Bush immediately took action to combat this act of global terrorism through his foreign policy War on Terror (Payani, 2016). The doctrine of "global war on terrorism" initiated by the United States, drove international community opinion that the Al-Qaeda terrorism network was fully responsible for the attack. According to Sukma in Hardiana et al. (2014), the US response to terrorism was the beginning of the establishment of a world political order marked by increasing non-traditional security threats (especially in the form of terrorism) and US hegemony as a single superpower.

The 9/11 attacks that shocked the world made Australia strengthen its national security to prevent similar casualty. Australia became one of many countries that focused on the existence of terrorism groups in responses to terrorism in the United States. The Australian Government, the Prime Minister Howard, proved this by increasing security against global terrorist attacks through Speech Acts. Howard delivered a speech act addressed to the Australian Parliament to carry out the alliance and activation function of Article IV of the ANZUS Agreement to assist and support war actions against terrorism (Ansari, 2019). Despite having zero cases related to terrorism at that time, the Australian Government stepped forward to mitigate terrorist groups.

Before 9/11, Australia did not have specific national laws for handling acts of terrorism. Therefore, Australia adopted to the UK's Terrorism Act 2000 due to UK’s long history of dealing with terrorist attacks. Afterwards, the Australian government (2023) enacted around 60 laws in response to the 9/11 attack. In Septem-ber 2014, Australia raised its terrorism threat level for the first time since 2000 because of concerns that some Australian citizens joined terrorist groups and were involved in the conflicts in Iraq and Syria (Anton, 2022). The

Australian Govern-ment perceived this could lead to attacks and terror to its nation by extremist groups from abroad; accordingly, terrorist laws and multivarious collab-orations with other countries to eradi-cate terrorism groups were in place. In 2022, Australia lowered its terrorism threat level from highly probable to possible, but there remained possibility of terror attacks by individuals or groups.

In the modern era, terrorist groups take advantage of advances in technology and information of the cyber world as an instrument in expanding terrorist networks (Halida, 2021). There are two main characteristics in modern terrorism: threat or violence and social goals (Madjid, 2021). The terrorists use threats or violence to force the government to grant their demands. Social purposes drive the terrorist group attacks, for example to prove their existence as a big, threatening group. In other word, without socio-political motivation and a vast offline and cyber networks, a crime is simply a crime, not terrorism. The internet has enabled terrorism propaganda to outlive and outspread the terrorists who have been imprisoned or dead without a trace (Sarinastiti & Vardhani, 2018). This further confirms that acts of terrorism are not simply threats to particular countries, but rather, a security issue with countries in the international world. The transformation of the use of conventional media in the cyber world by terrorist groups is known as cyber terrorism.

According to Dorothy Denning (in Weiman, 2004), cyber terrorism can be defined as an attack or a threat via the computer network or information network which aims to intimidate and pressure the government and people and has political or social interests. Cyber terrorism has become a modern issue that requires countries to actively prevent and overcome the expansion of terrorist networks. Initiated by Barry C. Collin in 1980s, cyber terrorism referred to hacking actions that can lead to quite massive disruption and damage. This action is then influenced by other factors such as ideology, religion and politics, ultimately aiming to influence, intimidate, and put pressure on the government. Furthermore, Collin mentioned that cyber terrorism is a new threat because it combines two elements: cyberspace and terrorism. Therefore, virtual threats using sophisticated technology for spreading propaganda are the core of cyberterrorism. Using media sophistication, the potential attacks could be multiple times greater.

Cyber terrorism in Australia can drive disruptions in both domestic realm and multilateral relationship. The resulting chaos could have domino effect from mass damage to disruption of domestic stability and e-commerce businesses. According to Holmes (in Latuheru and Irwansyah, 2019), "any medium which encloses human communication in an electronically generated space could be a form of cyberspace. Cyberspace is vital for Australia because it influences country's economy and security of the country. The Australian government (2020) anticipates the poten-tial terror from radical groups, both traditionally and through cyber terrorism because the important data and information of multifarious infrastructure is interconnected and therefore susceptible to be penetrated by cyberterrorism.

However, the Australian government has not thoroughly regulated cyber terrorism in international realm. Other regions have implemented regulations regarding cyber terrorism, such as the ASEAN convention on countering terrorism and the international convention on eradicating terrorist bombings.

National Security

Changes in the dynamics of international relations have in turn encouraged countries to modify their security system and strategy. The contributing factors to these changes are the development of globalization, advances in technology and information, trends in conflict between countries, the rapid flow of information and increasingly complex threats. These factors make countries reorganize their national security systems to protect and enable national interests. Since national security translates into the welfare of society, protecting the societal security will allow countries to achieve national security (Simorangkir, 2020).

According to Barry Buzan in A'raf (2015), the concept of security has undergone a broad evolution of meaning and developed over time. Etymologically, security is derived from Latin "securus" (se+cura) which means free from danger, free from fear. Security is a portmanteau of ‘se’ (without) and ‘curus’ ("uneasiness"), so securus means liberation from uneasiness, or a peaceful situation without any risks or threats. In this case, Buzan mentions five main aspects in defining security, namely military security (weapon management for defensive and offensive purposes), political security (the stability of the state organization, the ideology that gives legitimacy to the government), economic security (access to resources, finance and markets that support the country welfare), societal security (acceptance to traditional patterns of language, culture, religion, identity, nationality and customs), and environmental security (preservation and maintenance of environment to support human survival).

However, in its development, the threats against countries are no longer only about the military. Threats to human security in other aspects such as infectious diseases, natural disasters, environmental damage and others have seen an upward trend (A'raf, 2015). It is evident that security is not merely protecting the territory of the state but also guarantee citizen security as well as economy and cyberspace.

Considering the unavoidable nature of national security threats in cyberspace, it is imperative for the government to stipulate relevant regulations and policies in cyber laws to protect the safety and security of the country by means of, including but not limited to, military (use of weapons), economy, diplomacy, cooperation. Cyber law is the legal basis for the state to take actions for violations that occur. In an increasingly connected digital era, cyberspace security is very important.

Research Methods

In this study, researchers used descriptive qualitative research methods. Qualitative research is a research method used in a scientific context to explore the phenomena or issues experienced by the subject of the research in the form of actions, behaviors, motivations and perceptions described through the form of words and language (Moleong, 2017). Literature review or library research was applied to collect data. Then, to test the validity of the data, the researcher applied credibility testing to understand the phenomena as the target of the present research.

RESULTS AND DISCUSSION

Cyber Terrorism as an Instrument of Terrorist Groups

The utilization of cyber networks by terrorist groups is motivated by several rationale. The first is the relatively cheaper cost incurred than direct attack using weapons (traditional methods). Cyber space can save budget because all it takes is a gadget or a computer set and internet network. This is considered effective because with minimal costs it can reach individuals in various countries, which is a benefit for terrorism groups to launch their cyberattacks. Secondly, cyber networks enable the perpetrators to carry out discreet mission with fake identities and stealthy actions. Next, cyber networks allows the perpetrators to reach multiple levels of society due to convenience and direct access provided by the existence of digital communication and information technology. This can facilitate cyber terrorism activities to target both the community and the government. Fourth, cyber spaces enable high flexibility for its users to carry out activities regardless of time and space without having to physically relocate. In addition, the perpetrators also do not require special physical training. Lastly, cyberspace enables cyber terrorism to impose greater impacts than traditional attacks, for example as a tool to raise funds and seek support from various parties. For example, the group founded by Abu Musab Al-Zarqawi from the Al Qaeda faction in Saudi Arabia almost never had any direct contact with mass media because they primarily communicate in the cyberspace, thus keeping them from mass media attention. Paradoxically, the mass media use the internet to track Al Qaeda network and spread message about their latest terrorism in order to drive international public opinion (Soriano in Sarinastiti and Vardhani, 2018).

Some characteristics of cyber terrorism in general are intimidation or coercion, using murder and destruction to facilitate certain goals. Victims are not their main target but only as a tool to induce fear to others. The target of terror acts is determined while working in secret but with publicity as a goal. The message conveyed is clearly reflected in the action although the perpetrator does not declare himself personally, the motivation of the actor by strict idealism, the use of information technology and computers as instruments.

According to Petrus R. Golose in Bambang A.S. & Fitriana (2017), there are nine terrorism activities that utilize cyber networks, namely propaganda instruments, recruitment, logistics providers, training, paramilitary formation, planning, carrying out attacks, hiding, and funding. Below is the elaboration of each activity.

First, propaganda instrument according to Jacques Ellul in Bachtiar et al. (2016) is a set of methods used by organized groups who want to lead active or passive participation in their actions to a mass number of individuals who are united through a process of psychological manipulation and coordinated with the organization. Cyber space allows perpetrators to disseminate their influence without having to meet their targets in person. Cyber terrorism as a propaganda tool is intended to make the targets understand the terrorist ideology spread on the internet in order to gain support and further strengthen the terrorist network through fear.

Second, recruitment is activities carried out through spreading terrorism and radicalism to attract people to join the terrorist groups. The third activities made possible by cyber space to support cyber terrorism is logistic providers. It means that the cyber space is a tool utilized by terrorist groups to access various necessities in carrying out attacks, such as weapons and explosives.

Training is the fourth activities carried out in cyber space where the terrorist groups upload videos, photos, and various other documentation or content as training materials. Fifth, paramilitary formation is enabled by cyberspace that allows the terrorists group to spread calls and invitations to mobilize weapons and other vital needs. The formation of paramilitaries will strengthen the groups and extend their fearmongering the international community.

Planning is the sixth activity in the cyberspace which also marks a crucial stage in cyber terrorism. The perpetrators who will carry out terrorist attacks utilize the internet and technology networks to develop strategies and tactics and to communicate with each other to set the agenda and disseminate information. By planning, terrorist acts can be more focused and are more likely to succeed, especially for large-scale terrorism.

Seventh, the affordances of attack by cyber space in addition to weaponry, can imbue fear, anxiety, and panic to the victims. These attacks aim to strengthen the existence of the terrorist group. Terrorist attacks that use weapons are usually launched at critical points and crowded places such as mosques, churches, streets, banks and historical places. It aims to show off the strength of this terrorist group so that people will fear them and the government is coerced to take actions.

The eighth activity that cyberspace has enabled the terrorists to do is hiding. The perpetrators who carry out attacks, at some point, will run away or hide. In this case, the use of the internet network is to eliminate the traces and any identifiers of the perpetrators. Cyber terrorists usually create fake accounts that are so hard to reveal that the government instructs the police agency to track down the perpetrators of cyber terrorism.

At last, cyber space is the enabler of funding activities of terrorists to generate income from both domestic and foreign sources that are connected to other terrorist networks. Terrorist groups will usually attract the attention and incite people to join their group. Then, a distorted understanding and information will be circulated to these people in order to captivate them with words to participate in terrorist activities. People on the internet who perceive the terrorist propaganda to be true, will not hesitate to give sizeable financial support. Therefore, many terrorist groups spread their propaganda on the internet, run sophisticated online campaign to get the attention of the international community to generate more funding which could be in form of crypto. In 2020, the Al-Qassam, Al-Qaeda, and ISIS terrorist groups collected funds to finance their group activities (source).

Terrorism in Australia

Terrorism has become one of Australia's concerns. The Australian Home Minister must be definite in labelling a group as a terrorist group that must be eradicated and banned from Australian territory. There are some aspects to consider prior to this, such as whether the group is involved in acts of terrorism, upholds terrorism ideology, threatens the security of the Australian, and belongs to the list of terrorist groups established by the United Nations or like-minded countries (Nedim, 2023).

Based on Australian National Security, there are 29 terrorist groups included in the official list of terrorism groups, including Abu Sayyaf, a violent extremist group originating from Sunni Islam. Established in 1991, Abu Sayyaf aims to establish an Islamic state. Much of the group's funding is generated from ransom payments from kidnappings. Australia has officially incorporated the Abu Sayyaf group into the list of terrorism groups that must be eradicated since November 14, 2002. The other group is Al-Qa'ida, which is a Sunni Islamic terrorist group. Al-Qa'ida is often associated with Abu Sayyaf group because both are assumed to form alliances. Like Abu Sayyaf, the Al-Qa'ida group seeks to establish an Islamic caliphate and perceive Australia and the US stand in their dream of Islamic caliphate. Al-Qa'ida was formed by Osama Bin Laden and Abdullah Azzam in 1998. Another terrorist group in the eye of the Australian government is the Jama'at Mujahideen Bangladesh, a Sunni Islamic terrorism group based in Pakistan. the Jama'at Mujahideen Bangladesh carried out terrorist attacks in the Jammu and Kashmir regions to seize them under the authority of Pakistan. Australia added the Bangladesh Jama'at Mujahideen group as a terrorist group that must be eradicated on June 9, 2018. The next group is National Socialist Order (NSO), which is a violent and racist extremist group formed in the United States in 2015 by Brandon Russell. The NSO group seeks to introduce a national socialist and accelerationist ideology by inviting the use of violence aimed at establishing a white tribal state. Australia has included NSO as an official list of terrorist groups on February 18, 2022. Hamas is another group that was officially included as a terrorist group by Australia on March 4, 2022. Hamas is a violent extremism group that enforces its ideology and religion. Founded in 1987, Hamas group combines Palestinian nationalist and Sunni Islamic goals. In 2006, Hamas participated in Palestinian elections and succeeded in overthrowing the Palestinian Authority by taking control of Gaza in 2007. The goal of the Hamas terrorism movement is to liberate the Palestinian state by establishing an independent Palestinian state that uses Islamic principles and destroys Israel.

In addition to these 5 terrorism groups, are Hurras Al-Din, Hizballah, Hay'at Tahrir al-Sham, Boko Haram, Al-Shabaab, Jaish E- Mohammad, Jama'at Nusrat Al-Islam Wal Muslimin, Kurdistan Workers Party (PKK), and many others that have been officially included by the Australian Government as dangerous terrorism groups. These terrorist groups have never committed acts of terrorism directly in Australia, but Australia has made anticipations by establishing regulations and forming cooperation with other countries to eradicate these terrorist groups.

Reflecting on the magnitude of the potential threats arising from cyber terrorism, the Australian government also responded by implementing policies to secure the country's cyber assets, particularly by warding off negative impacts on private businesses in Australia and trusts in Australian ICT (Australian Government, 2020).

In this case, the Australian government has involved several parties in mitigating the threat of cyber terrorism. As the main party, the Australian federal government has four responsibilities. The first is to establish, implement, and enforce laws, regulations and policies regarding cyber security. Second, it must participate in global cyber security to improve coordination and cooperation in handling cyber threats. Next, it provides public policy as a tool to investigate cybercrime activities. The last is to provide references, recommendations and operational capabilities to identify and detect cyber threats. The role of every stakeholder from all levels determines the success of a country and the international community in minimizing and limiting the development of terrorism (Wattimena & Arifin, 2018).

The next parties are the state and territory governments. In addition to carrying similar responsibilities to those of the federal government, the state and territory governments focus more on members of their own territories. In most jurisdictions, cyber security for individuals and corporations is the domain of the police force in a particular area. Police departments focus more on the identification, investigation, and prosecution of cyber criminals. The responsibility of state and territory governments is to educate people, especially young adults and children about cyber threats and how to address them.

The third party the Internet Space Provider (ISP) that enables internet services for every traffic and transaction regardless of the legal or illegal status. ISPs have the responsibility to provide a secure line of communication for their users. For this reason, ISPs have a very important role in maintaining internet services in Australia to prevent illegal traffic and transactions.

The last party is the owners and administrators of Information and Communication Technology (ICT), both individuals and corporates. This group has an important role because of their ability to implement cyber security systems in their own facilities. If each of them has implemented a robust cyber security system, malicious software will not easily spread across systems.

In this regard, cybersecurity has presented many challenges that countries including Australia must face. Cybersecurity is part of civil security as cyberspace is connected through the internet which is also used by civil society.

In 2014, the threat of extremism attacks by terrorist groups was put under the terrorism category by the Australian Government due to the concerns of Australian citizens who were fighting against terrorist groups abroad, especially in Iraq and Syria. At that time, several terrorist attacks occurred in Australia, such as stabbing by Abdul Numan Haider who planned to join forces with ISIS. There were also five men who were arrested in connection with a terrorist incident in 2015. Another attack was committed by a private named Yacqub Khayre, who was a member of ISIS and Al-Qaeda terrorists. These threats were enough to remind

Australian citizens that among them stood the members of terrorist groups like ISIS and Al-Qaeda.

However, in November 2022, the Australian Security Intelligence Organization lowered the threat level of terrorism in Australia from probable to possible (Yunus, 2022). This is because there has been a decrease in the risk of terrorism attacks in Australia for almost a decade.

Despite no physical terrorism attacks in Australia these days, the Australian Government remains vigilant by enforcing laws and international cooperation in dealing with terrorism. One form of terrorism that Australia must be aware of is cyber terrorism. This is because cyber terrorism can threaten Australian security and data.

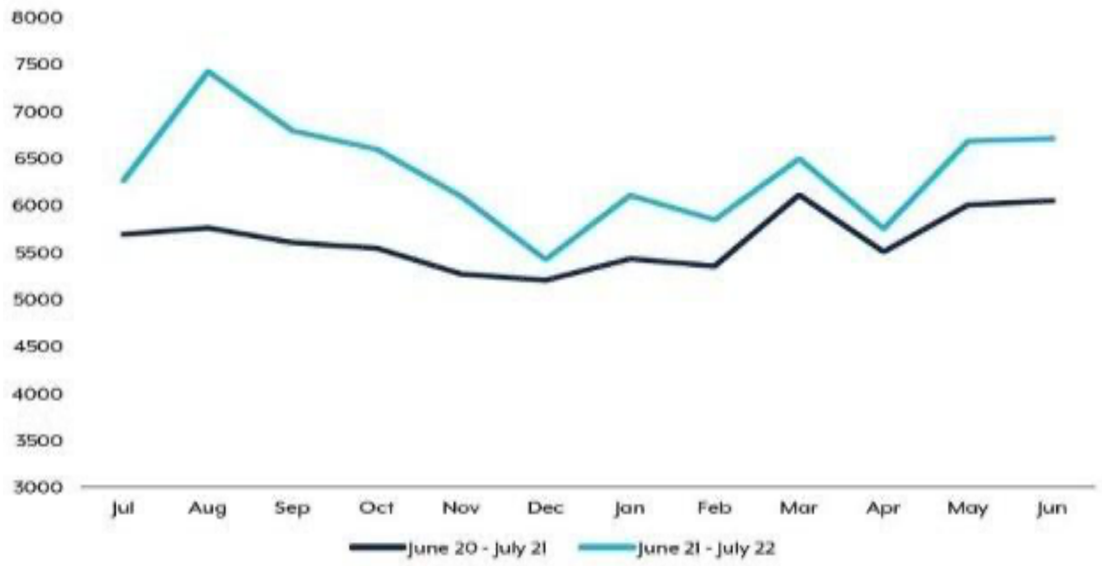
The potential for cyber terrorism today is high. The ease of accessing the internet and the rapid development of advanced technology have made cyber terrorism more widespread. In Australia, there is a high number of the population that use the internet, and this figure keeps increasing every year.

Table 1.
Internet Users in Australia

Year	Number of Users
2018	88%
2019	87%
2020	88%
2021	89%
2022	91%

Source: Hughes, 2023

Table 1 shows that the internet usage in Australia is very high. Almost all Australians use the internet in their daily lives and the number increased gradually until it reached its peak in 2022 where 91% of the populations were the internet users. It drives the Australian Government to impose stricter policies to protect the privacy and personal data of its citizens. The most common acts of cyber terrorism are hacking and cybercrime. The perpetrators of cyber terrorism will usually steal personal data for the benefit of their group, and therefore, cyber terrorism-based crimes are important to mitigate by the Australian Government. Terrorists who use the internet can impose fatal impacts, if not handled properly. While rarely causing casualties, cyber terrorism crimes can drive chaos in a country when data and information theft takes place.



Source: Australian Cyber Security Center, 2022.

Figure 1.
Cyber Crime Reports in Australia

Table 2 demonstrates general data to illustrate the number of cyber-crimes in Australia, including acts of cyber terrorism. Based on the Australian Cyber Security Center data above, between 2021 and 2022, there were over 76,000 cases of cybercrime or at least an increase of 13% from the previous year in Australia.

Australian Government's Strategy to Counter the Threat of Cyber Terrorism

Cyber terrorism in the form of cybercrime and hacking cannot be considered as a simple threat. It can be a very big threat if it causes disruption in the national security of a country. The theft of personal data and information from residents, companies, organizations, and even countries can disrupt domestic stability. Therefore, the Australian Government establishes various strategies in dealing with cyber-based threats such as cyber terrorism.

The initial strategy is the stipulation of the Criminal Code Act 1995 in Part 5.3. Mitigating threat of terrorism cases that include cyber terrorism, the Australian Government has long made a law on countering acts of terrorism contained in the criminal code act 1995 in part 5.3 (Federal Register of Legislation, 1995). The anti-terrorism law focuses on aspects like terrorist offenses, terrorist organizations, prevention of terrorist financing, restraining orders, foreign attacks and recruitment offenses. In order to prevent terrorism financing, the Australian Transactions Reports and Analysis Center (AUSTRAC) will monitor bank accounts and money circulation. If financial transactions are detected in any of terrorist group listed by the Australian government, their bank account will be frozen and the person holding the account will be charged. In addition, a person in Australia can be suspected as a terrorist if he or she commits various acts of terrorism, such as deliberately committing terrorist acts, planning terrorist acts, providing funds for terrorist acts, and facilitating terrorist elements. Thus, if proven to have done the above, the person will be sentenced to life imprisonment in accordance with Australian regulations on countering terrorism in the criminal code act 1995 in part 5.3.

Second, Australia's Cyber Security. The next step taken by the Australian Government in dealing with the threat of cyber terrorism is to create a cyber security strategy. In 2016, Australia created the 2016 Cyber Security Strategy. At that time, the Australian Government was faced with the challenges of the advancement of the digital era so it was imperative to extend their security system to online realm. To smoothly implement the strategy, the Australian Government invested $230 million to strengthen the cybersecurity foundation in Australia, encourage private investment in the domestic cybersecurity industry, and make Australia a regional cybersecurity leader. The 2016 cybersecurity strategy was successful as proven by achievements such as the opening of the Australian Cyber Security Centre (ACSC) and the establishment of Joint Cyber Security Centres (JCSCs AustCyber, the Australian Cyber Security Growth Network, and the Cyber Security Cooperative Research Centre. In addition, increasing cyber skills is in the ballpark of this series of achievement.

Then in 2020, the Australian Government wanted to further improve cybersecurity by implementing the Cyber Security 2020 which received an investment of $1.67 million. fighting cybercrime, protecting Australian Government data and networks, strengthening partnership cyber security, protecting critical infrastructure and services, and blocking malicious activities in cyberspace. More importantly, however, the Cyber Security 2020 is a response to threats to Australian networks on June 29, 2020 when the Australian PM announced that sophisticated state-based cyber actors targeted Australian organizations, governments, industries, infrastructure operators, and others stakeholders. To overcome this, the Australian Cyber Security Center (ACSC) worked with major Australian telecommunications providers and Google companies to protect Australia and its citizens from malicious cyber activities.

Third, The Lombok Treaty is a Security Cooperation between Australia and Indonesia in 2016 in order to improve both countries' security against cyber terrorism crimes while strengthening defense cooperation, transnational crime law enforcement cooperation, intelligence cooperation, maritime security cooperation, and others (Department of Foreign Affairs and Trade, 2023). All these measures were achieved by information sharing, mutual assistance in border and immigration security, and improvement in law enforcement and national security cooperation to counter terrorism.

Fourth, Australia's international involvement. Cyber terrorism as an international-scale terrorism is able to threaten the stability of world peace and security directly or indirectly. Therefore, handling cyber terrorism should engage not only national laws but also the collective efforts of the international community.

Furthermore, when referring to Barry Buzan's concept of national security, protecting national security translates into preserving access to related resources, finance and markets that support the welfare of the country (the economic security). Therefore, the reinsurance program coverage by APRC was established. This program focuses on commercial property, subject to some coverage exclusions outlined in regulation (including for computer crime). The mission of this program is to assure the market that claims will be paid in the event of terrorism in Australia. APRC is a public finance company backed by an Australian government guarantee.

The Australian Government is responsible to uphold international laws and norms of the state behavior relating to cyber space. Australia will continue to encourage people to act responsibly in online domain, and this includes complying with existing international and domestic laws. This is done by the government to ensure that Australia is not seen as a target. Australia's Cyber Security Strategy 2020 states that, "We work to actively prevent cyberattacks, minimize damage, and respond to malicious cyber activity directed against our national interests. We deny and deter, while balancing the risk of escalation. Our actions are lawful and aligned with the values we seek to uphold, and will therefore be proportionate, always contextual, and collaborative. We can choose not to respond."

In other words, Australian government works hard to strengthen country's cyber security. To ensure national security, the Australian government cooperates with international partners and is committed to supporting and maintaining international mechanisms that promote stability and to working with partners voluntarily to prevent and deal with various cyber threats, including cyber terrorism in cyberspace. Australia also contributes to international cyber forums such as the International Organization for Standardization and the International Telecommunication Union that develop international standards that contribute to a safer cyber space for all countries. The Australian Government has also committed to a seven-year program worths $34 million for cyber cooperation program involving government, industry, civil society and academia. Collaborating with Papua New Guinea for four years, Australia improves the cyber security framework, and teaming up with India in a four-year partnership worths $12.7 million.

CONCLUSIONS

The events of 9/11 have made countries around the world is a wake-up call that the acts of terrorism can destabilize their country. In the current era of globalization, technology has become increasingly sophisticated and almost all international communities use technology and actively use the internet, including terrorist groups. Terrorism activities that have utilized technology and the internet and are based in cyberspace are known as cyberterrorism.

Australia, being a developed country with advanced technology, can potentially become a target of cyber terrorism activities. This is because 91% of Australian citizens use the internet it is imperative for the government to ward off hacking and terrorism acts in order to protect the privacy and personal data of its citizens, as well as national documents and information, organizations, and companies in Australia to prevent further chaos in the country. In an effort to deal with the threat of terrorism, including cyber terrorism, Australia has made various strategies and established laws against terrorism known as the Criminal Code Act 1995 in Part 5.3. Other strategies include creating a cyber security strategy and conducting cyber security and defense cooperation with other countries.

REFERENCES

A'raf, A. (2015). Dinamika Keamanan Nasional. *Jurnal Keamanan Nasional*, *1*(1), 27–40.

Ansari, R. (2019). Politik Sekuritisasi Kontra-Terorisme Global Australia Pasca 9/11 Hingga Terpilihnya Kembali Perdana Menteri Howard. *Jurnal Asia Pacific Studies*, *3*(2), 171-180.

Australia Cyber Security Centre. (2022). "Annual Cyber Threat Report July 2021-June 2022." Accessed from https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022.

Australian Government. (2023). "Australia'sCounter-Terrorism Laws." Accessed from https://www.ag.gov.au/nationa l-security/australias-counter-terrorism-laws.

Australian Governments. (2020). "Australia's Cyber Security Strategy 2020." Accessed from https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

A.S, B..A.A. & Fitriana, I. (2017). Cyberterrorism: An Asymmetric Communication Challenge for National Defense. *Jurnal Komunikasi*, *2*(1), 1-15.

Bachtiar, Y. A., Perkasa, D.H. & Sadikun, R. (2016). The Role of Media in Propaganda. *Komunikologi: Jurnal Ilmiah Ilmu Komunikasi*, *13*(2), 78-89.

Dina, H. A. I. (2021). Aksi Cyber-Terrorism di Amerika Serikat dalam Perspektif Keamanan Global. *Global & Policy*, *9*(2), 130-134.

Department of Foreign Affairs and Trade. (2023). "Agreement Between Australia and the Republic of Indonesia on the Framework for Security Cooperation. " Accessed from http://www.austlii.edu.au/au/other/dfat/treaties/ATS/2008/3.html.

Federal Register of Legislation. (1995). "Criminal Code Act 1995." Accessed from https://www.legislation.gov.au/Details/C2019C00043.

Hardiana, I. M. Y., Sushanti, S., & Fasisaka, I. (2014). Kerjasama Kontra-Terorisme antara Australia dengan Indonesia dalam Menanggulangi Ancaman Terorisme di Indonesia (2002-2008). *DIKSHI (Diskusi Ilmiah Komunitas Hubungan Internasional)*, *1*(2), 1-15.

Hughes, C. (2023). "Internet User As A Percentage Of The Total Population Australia 2015-2022." Accessed from https://www.statista.com/stat istics/680142/australia-internet-penetration/#:~:text=The%20share%20of%20the%20Australian,22%20million%20subscribers%20in%202022.

Latuheru, M. N., & Irwansyah, (2019) Aplikasi Traveloka Sebagai Bentuk Konstruksi Sosial dalam Dunia Siber. *Jurnal Kajian Media*, *3*(2), 79-88.

Madjid, Y. R. (2021). Cyber Terrorism Challenges: The Need for Global Mutual Legal Assistance for Universal Criminal Jurisdiction. *Yustisia Journal of Law*, *10*(3), 388-414. https://doi.org/10.20961/yustisia.v10i3.

Moleong, L. J. (2017). *Metode Penelitian Kualitatif.* Bandung: PT. Remaja Rosdakarya.

Nedim, U. (2023). "Which Groups Does Australia List as Terrorist Organizations?" Accessed from https://www.nationalsecurity.gov.au/what-australia-is-doing/terrorist-organisations/listed- terrorist-organisations.

Payani, N. L. B. (2016). Pengaruh Serangan 9/11 Terhadap Perkembangan Dinamika Keamanan Internasional. *Andalas Journal of International Studies*, *5*(1), 28-41.

Sarinastiti, E. N. & Vardhani, N.K. (2018). Internet dan Terorisme : Menguatnya Aksi Global Cyber-Terrorism New Media. *Jurnal Gama Societa*, *1*(1), 40-52.

.

https://doi.org/10.22146/jgs.34048

Simorangkir, B. (2020). Expanding the Agenda for National Security Studies: Politics, Law and Strategy. *Jurnal Diplomasi Pertahanan*, *6*(3), 47-57.

Sindi, H. Q. (2016). Analisis Perilaku Kejahatan Terorisme Osama Bin Laden. *Journal of International Relations Universitas Diponegoro*, *2*(4), 93-98. https://doi.org/10.14710/jirud.v2i4.13413

Sukoco, A., Syauqilah, M. & Ismail, U. A. (2021). Media, Globalisasi, dan Ancaman Terorisme. *Journal of Terrorism Studies*, *3*(2), 1-15. https://doi.org/10.7454/jts.v3i2.1039

Wattimena, R.A.A. & Arifin, B. (2018). Beyond Terrorism: A Comprehensive Approach to Understanding and Countering Terrorism. *Mandala Journal of International Relations*, *1*(1), 38-55.

Weiman, G. (2004). "Cyberterrorism How Real Is The Threat?" *United States Institute of Peace*. Accessed from https://www.usip.org/sites/default/files/sr119.pdf.

Yunus, S. (2022). "For First Time Since 2014, Australia Lowers Terror Threat Level." *Tempo*. Accessed from https://dunia.tempo.co/read/1661970/pertama-kali- sejak-2014-australia- menurunkan-tingkat-ancaman-teror.