E-ISSN : 2963-4946
Vol. 2 No. June 09, 2024
Asian Journal of Social and Humanities
https://ajosh.org/

Cyber Warfare Is The Newest Challenge To Support Indonesian National Resilience

Dwi Imroatus Sholikah, Tegar Harbriyana Putra, Mohammad Fauzan Hidayat
Universitas Boyolali, Indonesia
E-mail: d.imroatus@gmail.com, tegarharbriyanaputra@gmail.com, fauzanhidayat@gmail.com

***Correspondence:** d.imroatus@gmail.com

KEYWORDS
cyber warfare; international law; national security

ABSTRACT
Cyber operations began to attract attention in international law in the late 1990s, in 1999 the United States Naval War College held the first major legal conference on this issue. In the aftermath of the attacks of September 11, 2001, transnational terrorism and subsequent armed conflict shifted attention from topics to large-scale cyber attacks. Operations occurred in Estonia in 2007 and against Georgia during its war with the Russian Federation in 2008, as well as cyber incidents such as the targeting of Iran's nuclear facilities with the Stuxnet Worm in 2010. Cyber warfare is included in organized crime and terrorism as one of the level one threats. This research aims to explore the novel and evolving field of cyber warfare, a critical aspect of modern warfare that operates exclusively in the virtual realm of cyberspace. This research is normative in nature, using a conceptual approach and statutory regulations to answer. Conclusion is Synergy in facing the threat of cyber warfare is a must for Indonesia. Relevant parties such as the Ministry of Defense, TNI, BSSN and others must be able to protect against the threat of cyber warfare for Indonesia's resilience.

Introduction

In this modern era, everything in various aspects of life is dependent on technology which is developing very rapidly, from the line of work to the world of shopping which is all online (Schmitt, 2014). But without realizing it, unimaginable threats are circling the cyber world, recently a lot of cyber threats have occurred. Not just cyber crime. Now cyber warfare has developed, which is known as war in cyberspace without physical or conventional war (Alfian, 2018). The domain of cyber warfare is in cyberspace, those who attack are people who are information technology experts who do not have to come to the country that will be attacked. The area that was attacked was not a physical area, territorial area or geographic area, but a virtual world area. Common battlefields in physical warfare are war on land, war at sea, war in the air and war in space. However, for cyber warfare, the area is in cyberspace (Andress & Winterfeld, 2013).

Political dynamics in the world are increasingly complex and diverse, thus affecting the domestic political constellation of each country. Every country in the world is currently increasing awareness of various threats in the form of conflicts between countries and domestic conflicts between countries which endanger the national security of each country (Andrews et al., 2012). In addition, globalization has encouraged technological development so that various threats of conflict and war between militias and governments and between large and small countries are increasingly complex regarding facilities and infrastructure. This happens because of the use of information and communication technology, especially cyberspace, which then leads to the threat of cyber war (Cyber Warfare) (Barkawi, 2011).

According to UNTERM, cyber warfare is a military action that utilizes technology to damage/destroy a target's information to gain military and business advantage (Green, 2015). Meanwhile UNICJRI defines cyber warfare as "any action by a nation-state to penetrate another nation's computer networks for the purpose of causing some kind of damage". The definition given by UNICJRI is similar to the definition given by Richard Clarke, namely that it is an action by a state actor to penetrate another country's computer network with the aim of causing damage that cannot be avoided and has extraordinary impacts. An example is the Wannacry virus ransomware attack on a hospital in Hollywood which resulted in crippling access to healthcare for patients being treated (Carr, 2012). Another example of a cyber attack on the Israeli internet occurred during the military attack on Gaza in 2009. The most famous was in 2010 where the United States used Stuxnet to attack Iran's nuclear installation at Natanz which caused the destruction of machines used to separate uranium and caused significant losses. significant and there are many more examples of cyber warfare resulting in physical damage (Andersen & Kragh, 2011).

There are still many people who think that the impact of cyber warfare does not have a significant impact, that is a big mistake. Therefore, this research is intended to provide an understanding of cyber warfare as a method of state warfare, the position of cyber warfare according to international law and how terrible it would be if this were allowed to continue without clear regulation and protection from each country arising from cyber warfare (Wang & Wang, 2004). This. Cyber warfare is included in the military scope to protect civilian assets, internet freedom requires military intervention to protect against cyber attacks, especially to protect civil government bodies or individuals. This cyber war also cannot be equated with conventional war, therefore international legal regulations are needed to regulate cyber war issues raised by cyber warfare as a new model of war (Robinson et al., 2015).

This research aims to explore the novel and evolving field of cyber warfare, a critical aspect of modern warfare that operates exclusively in the virtual realm of cyberspace. As technology advances at an unprecedented pace, the threat landscape in cyberspace has expanded beyond cybercrime to encompass state-sponsored cyber warfare. Unlike traditional warfare, cyber warfare involves sophisticated attacks orchestrated by skilled IT experts, targeting not physical territories but rather the digital infrastructures and information networks of nations. The novelty of this study lies in delving into the intricacies of cyber warfare as a method of state aggression, examining its implications under international law, and highlighting the urgent need for clear regulations and protections. By shedding light on these aspects, the research aims to enhance understanding among policymakers, military strategists, and the international community about the potential catastrophic impacts of unchecked cyber warfare.

Ultimately, this study seeks to advocate for robust legal frameworks and defensive strategies to mitigate the threats posed by cyber warfare, safeguarding global security and stability in an increasingly interconnected world.

Research Methods

This research is normative in nature, using a conceptual approach and statutory regulations to answer. A conceptual approach is used u to respond to cyber warfare as a new method of warfare in this modern era. The legal approach is used to describe cyber warfare in terms of international law and the formation of national law for the benefit of national security in Indonesia (Bernard, 2017).

Results and Discussions

Cyber Warfare as a New Method of War

The attack method in cyber warfare is different from conventional warfare. Where the domain of cyber warfare is in cyberspace, which not many people are aware of or know about. The ICRC also issued a similar definition in its publication entitled "The Evolution of War". The ICRC defines it as military operations via computers and networks to damage or destroy an enemy (Sanjaya et al., 2022). There are several differences between conventional war and cyber warfare. Attacks in cyber warfare can be carried out by anyone in a militia corps because the tools needed are very easy and cheap. There is no need to buy weapons, even if there is a lot of time, the attacks carried out can be unknown/anonymous (the party does not known). The following are attack methods in cyber warfare:

1. Vandalism

Where this attack is carried out to damage web pages (Deface), or use a denial of service attack, namely destroying the resources of another computer. Deface is often in the form of propaganda such as political messages that can be distributed over the internet via email, instant messages or text messages.

2. Information collection

It is a form of collection of confidential and sensitive information from individuals, competitors, other government groups and enemies in the military, political and economic fields. The method used is illegal exploitation via the internet, networks and/or computers in other countries. Where confidential information that is not protected safely and well will become a target for public consumption and can even be easily changed.

3. Sabotage

Sabotage is a military activity that uses computers and satellites to determine the coordinates of the location of enemy equipment which has a high risk of interference. Sabotage can take the form of intercepting information and disrupting communications equipment so that energy sources, water, fuel, communications and transportation infrastructure all become vulnerable to disruption. Sabotage can take the form of malicious software hidden in computer hardware.

4. Attacks on the Electric Network

This attack on the electricity network could take the form of a blackout of the electricity network so that it could disrupt the economy and divert attention to the opponent's military attack which is taking place simultaneously which results in the network stopping and so on. This attack uses a Trojan horse-type program to suddenly control electrical infrastructure (Basholli, 2022).

In his book, Igor Bernik, entitled Cybercrime and Cyber warfare, describes several types and techniques of cyber warfare:

"Using the techniques of cyber warfare at the state level is usually aimed at obtaining information on the economic, political, cultural and military situations in another country-the target-or for specific offensive and defensive operations in cyberspace. In the first case, countries most often achieve the objects through espionage, and in the second case, these are carried out through actions in cyberspace that are similar to military activities (Cunningham & Touhill, 2020)

However, cyber warfare does not fall only within the competence of states, but is also used by corporations or those organizations, which need information for which they do not have authorized access for their survival, development and competition. New guidelines and needs for information, as well as knowledge related to it, will be increasingly dictated by aggressive competition and lagging organizations."

As a cyber warfare attack activity, it consists of six components as follows:

1. Psychological, which will have an impact on the opponent's mental condition, such as propaganda or dissemination of information to influence people's decision making, where the internet is the right tool to carry out this attack.
2. Electronic warfare, this includes disabling access to information needed by opponents such as those carried out by terrorists, hackers and states.
3. Military deception is similar to traditional forms of warfare in that opponents are misled about true military capabilities.
4. Physical cyber warfare, physical attacks on information systems.
5. Protection measures to protect information systems, the aim is to have a system that cannot be paralyzed by opponents.
6. Information attack, misuse or destruction of information.

Information attack operations involve the collection of confidential information, unauthorized access to information systems, creating security gaps in them. Meanwhile, this kind of formation battle has two basic forms, such as deceiving the opponent to attacking the computer network and disrupting or destroying the opponent's information (Akimenko & Giles, 2020). Refers to the rules in international law of armed conflict or war as a conflict that contains violence. When viewed from the definition above, cyber attacks can be categorized as the use of armed violence if the impact of the attack or use of cyber warfare methods has an impact similar to conventional war. This argument can refer to the International Court of Justice that armed violence must be based on correct arguments.

Articles 2 (4) and 51 of the UN Charter collectively state that states can take self-defense measures when armed violence attacks their sovereign territory. Using the arguments of Articles 2 (4) and 51 of the UN Charter will raise new questions, to what extent is a country's sovereignty in cyberspace? Tallin in rule 1 states that a country has the authority to exercise control over all cyber infrastructure and cyber activities within its sovereign territory (Schmitt, 2012). So when a cyber attack occurs, it is categorized as an armed attack on a country's infrastructure and cyber activities, the country has the right of authority to defend itself and this is the answer to whether cyber warfare can be considered a "war" and justified in the international community.

Cyber warfare Current challenges and potential future threats

In looking at actions, cyber warfare can include offensive actions, defensive actions, or preventive actions. By this explanation, this includes the dissemination of offensive information via computers or computer networks (Andress & Winterfeld,

2011). Cyber war is a war that has no clear boundaries or actors, so many of the existing laws and regulations do not help. Acts of war or states of war are usually assigned to recognized states and combatants. However, in this case, cyber war can be carried out by states, state agents, non-state actors, international groups, or groups of people who have interests or even by one individual (Cornish, et al., 2010).

In accordance with the principle of non-intervention, states must not intervene directly or indirectly in the internal affairs of another state, including by means of icts." The 2015 UNGE report applies the charter as a whole, the group notes the inherent right of each state to take action consistent with international law and as recognized in the charter. Unge 2021 report on the use of Information and Communication Technology (ICT) risk management, and in accordance with the United Nations (UN) charter, countries in their international relations must refrain from threats or use of violence against the territorial integrity or political independence of a country or in other ways that are not in accordance with the objectives.

Applicable principles of international law, including, where applicable, the principles of humanity, necessity, proportionality and distinction. The failure to agree on international law is partly due to disagreements regarding the application of International Humanitarian Law. It noted that International Humanitarian Law only applies in situations of armed conflict. This recalls the applicable principles of international law including, where applicable, the principles of humanity, necessity, proportionality and distinction noted in the 2015 report. However, further study is needed.

International law relating to cyberwarfare jus ad bellum article 24 (use of force) UN Charter Article 51 (self-defense) exceptions to the use of cyber force authorized by the UN Security Council, self-defense in response to cyber armed attacks authorizing cyber operations in the area humanitarian intervention such as the use of armed strike force of temporal and quantitative necessity and proportionality.

Cyber warfare is where all actions are carried out deliberately and coordinated with the aim of disrupting state sovereignty. Cyber war can take the form of terrorist attacks (cyber terrorism) or espionage (cyber espionage) which disrupt national security. Cyber attacks have the following characteristics:

a) Intentional
b) Active activities
c) Large scale

The targets of cyber attacks are aimed at individuals, the general public, organizations, certain communities that are cyber crimes, vital objects of national infrastructure, very important physical infrastructure systems where if these systems are not functioning or damaged, it can have an impact on weakening the nation's defense or security and economy. The impact of cyber attacks can take the form of:

a) Functional disorders
b) Remote system control
c) Misuse of information
d) Riots, fear, violence, chaos, conflict
e) As well as other very detrimental conditions that can result in destruction.

The existence of cyber threats should be of concern to everyone the right in Indonesia to better protect Indonesia's defense system. As is known, the Indonesian defense system is a universal defense system with the main component being the TNI and the supporting components being the people. In this context, the universal defense system contained in Law 3 of 2022 concerning National Defense must be able to be interpreted

as a universe that is not only physical, but also non-physical, especially digital and cyberspace.

Conclusion

Technological developments have resulted in methods of war that continue to develop and advance. Previously, war only occurred on land, sea and air, now war has developed in space and cyber space. The war that takes place in space and cyber space requires clear rules, defenses to counter threats from cyber warfare and ready human resources. Synergy in facing the threat of cyber warfare is a must for Indonesia. Relevant parties such as the Ministry of Defense, TNI, BSSN and others must be able to protect against the threat of cyber warfare for Indonesia's resilience.

References

Akimenko, V., & Giles, K. (2020). Russia's cyber and information warfare. *Asia policy*, *15*(2), 67–75.

Alfian, M. (2018). Penguatan Hukum Cyber Crime di Indonesia dalam Perspektif Peraturan Perundang-Undangan. *Kosmik Hukum*, *17*(2).

Andersen, P. H., & Kragh, H. (2011). Beyond the inductive myth: new approaches to the role of existing theory in case research. In *Rethinking the case study in international business and management research*. Edward Elgar Publishing.

Andress, J., & Winterfeld, S. (2013). *Cyber warfare: techniques, tactics and tools for security practitioners*. Elsevier.

Andrews, L., Higgins, A., Andrews, M. W., & Lalor, J. G. (2012). Classic grounded theory to analyse secondary data: Reality and reflections. *Grounded Theory Review*, *11*(1).

Barkawi, T. (2011). From war to security: Security studies, the wider agenda and the fate of the study of war. *Millennium*, *39*(3), 701–716.

Basholli, F. (2022). Cyber warfare, a new aspect of modern warfare. *International Scientific Journal Security & Future, Publisher: Scientific Technical Union of Mechanical Engineering Industry-4.0*, *5*(2), 72–75.

Bernard, H. R. (2017). *Research methods in anthropology: Qualitative and quantitative approaches*. Rowman & Littlefield.

Carr, J. (2012). *Inside cyber warfare: Mapping the cyber underworld*. " O'Reilly Media, Inc."

Cunningham, C., & Touhill, G. J. (2020). *Cyber warfare-Truth, tactics, and strategies*. Packt Publishing Birmingham, UK.

Green, J. A. (2015). *Cyber Warfare*. Taylor & Francis.

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & security*, *49*, 70–94.

Sanjaya, B. R., Efrianti, D., Ali, M., Prasetyo, T., Mukhtadi, M., Widasari, Y. K., & Khumairoh, Z. (2022). Pengembangan Cyber Security dalam Menghadapi Cyber Warfare di Indonesia. *Journal of Advanced Research in Defense and Security Studies*, *1*(1), 19–34.

Schmitt, M. N. (2014). The law of cyber warfare: Quo Vadis. *Stan. L. & Pol'y Rev.*, *25*, 269.

Wang, H., & Wang, S. (2004). Cyber warfare: steganography vs. steganalysis. *Communications of the ACM*, *47*(10), 76–82.