CYBER WARFARE: NATIONAL SECURITY IN DEALING WITH CHANGING METHOD OF WAR

by Maskun -

Submission date: 04-Jan-2022 09:03PM (UTC+0700)
Submission ID: 1737414377
File name: 22371-77217-1-PB.pdf (342.83K)
Word count: 4643
Character count: 25126

Kanun Jurnal Ilmu Hukum
Vol. 23, Issue 3, (December, 2021), pp. 477-490.

CYBER WARFARE: NATIONAL SECURITY IN DEALING WITH CHANGING METHOD OF WAR

Maskun & Azhar Risaldy Rum

Faculty of Law, Universitas Hasanuddin
Perintis Kemerdekaan Street Km. 10 Tamalanrea, 90245
E-mail: maskunmaskun31@gmail.com; Phone Number: +62-8114107094

Received: 24/08/2021; Reviewed: 26/11/2021; Accepted: 30/12/2021.

DOI: https://doi.org/10.24815/kanun.v23i3.22371

ABSTRACT

The purpose of this research is to identify cyber warfare as a model of War, its position in the perspective of international law, and the steps taken by the state in minimizing losses arising from cyber warfare. This research is normative research using conceptual and statute approaches to answer the problems in this research. The analysis used is content analysis. The study results indicate a need for a common understanding of cyber warfare as a new model of war agreed upon by countries in practice. Normative cyber warfare in international law has to be applied universally. The periodic simulations of cyber defense and artificial intelligence are needed in minimizing the losses caused by cyber warfare. The recommendation is to formulate a definition of cyber warfare universally agreed upon and the state's agreement on the meaning of cyber warfare in international law perspectives.

Key Words: cyber warfare; national security; war methods.

INTRODUCTION

War, or in modern terms known as armed conflict, is a familiar and unavoidable phenomenon in the history of humankind. The argumentation is that War has become a form of problem-solving when there is a conflict between 2 or more parties. In its development, War has undergone various evolutions. This change, of course, cannot be separated from multiple technological developments that have occurred while humans have been on earth (Bernard, 2016). It can be proven wherein the ancient kingdom, the warriors who fought still used sharp weapons at close range, which began to appear as firearms used today.

Developments indeed continued to occur until the 2000s, the International Committee of Red Cross (ICRC) began to introduce to the world a new method of warfare called cyber warfare (Rain Liivoja, 2016). This method of warfare is carried out in cyberspace and apart from various weapons

that have physical damage. In essence, this cyber War no longer uses known conventional weapons such as firearms and explosives but uses cyber operations through computers and networks. Thus, cyber warfare should no longer cause significant damage and losses, as conventional wars do.

This view can be considered entirely wrong because, in practice, it turns out that cyber operations, whether carried out in the context of cyber warfare or not, can have a tremendous physical impact. Some examples can be seen in 2017. There was an attack by the wannacry ransomware virus against a hospital in Hollywood which resulted in the paralysis of the provision of health access to patients being treated (Ragan, 2021). Another example is the cyber attack on Israel's internet infrastructure that occurred during the military attack on the Gaza Strip in 2009 (Pfeffer, 2021). The most famous in 2010 where the United States used Stuxnet to attack Iran's nuclear installation at Natanz, which caused the destruction of the machine used to separate uranium and caused significant losses and many more examples of cyber operations that caused physical damage (ICRC, 2021).

The extraordinary losses suffered by countries and affected by this cyberattack prove that several countries are currently less prepared to face attacks through computer networks. It is also possible that there are still many parties who feel that cyberattacks do not significantly impact their government's activities, including the allocation of resources to increase defense against cyber attacks. Therefore, the focus of this paper is to provide an understanding of cyber warfare as a new method of warfare for countries, the position of cyber warfare according to international law, and the preventive measures to minimize losses arising from cyber warfare activities.

In the literature study, several previous articles that described cyber warfare were as follows: First, Cyberwar: The Next Threat to National Security and What to Do About It (Clarke, 2010). This study places cyberwar about national defense interests, and at the same time, provides an opportunity for the government to take military actions to protect civilian assets. This study also

confirms that internet freedom requires military intervention to protect against cyber-attacks primarily directed at civilian agencies or individuals.

Second, the position of Cyber Warfare in International Law (Angel Tampubolon, 2018). This study focuses on the role of cyber warfare in the broader context of international law. This study also emphasizes that cyber warfare cannot be equated with conventional war. The regulation of the international legal regime is urgently needed to regulate cyber warfare issues that have not been regulated by international law.

Both Clarke and Angel Tampubolon's research differs from this study. This study aims to share knowledge about cyber warfare, which is currently not standardized, so the need for international law is urgently needed and equipped with preventive steps to reduce losses caused by cyber warfare as a new war model.

RESEARCH METHODS

This research is normative, using a conceptual approach and legislation to answer existing problems (Marzuki, 2016). A conceptual approach is used to respond to cyber-warfare as a new form of War. A statutory approach is used to elaborate on cyber warfare in the provisions of international law. This study's two types of normative approaches are qualified as primary and secondary legal materials. The analysis used in this study is content analysis to find the right formula for describing this study's problems (Marzuki, 2016).

DISCUSSIONS AND ANALYSIS OF RESULTS

1) Cyber Warfare as a form of War

Cyber warfare is a form of development in cyberspace, such as cybercrime, cyber vandalism, or cyber espionage, where all work in cyberspace. The term "cyber warfare" has been interpreted differently by several groups of people. "Cyberwarfare" is a way or method of fighting using cyber

operations that are directed or used in the context of armed conflict. Richard Clarke and Knake define cyber warfare as a war in which the attackers consisting of war militias use cyber operations against their enemies to damage, disrupt, or destroy enemy computer systems (Clarke and Knake, 2010). The ICRC also issues a similar definition in its publication entitled "The evolution of war." The ICRC defines it as a military operation through computers and networks to damage or destroy the enemy (ICRC, 2016).

In essence, there are two critical points; the first is computers and networks, and the second is the *mens rea* of the attacker to disrupt and reduce the enemy's military capacity. Broadly, it can be distinguished several points to differ between conventional War and cyber warfare, as followings: (1) Attacker in cyber warfare can be carried out by anyone in a corps of militia because the tools needed are very quickly accessible and inexpensive; (2) Attackers in cyber warfare can be carried out anonymously (Unknown/identifiable parties); (3) Does not require much energy; (4) Cyberwarfare occurs in the virtual world (Soewardi, 2013).

It is essential to understand that not all cyber operations carried out in cyber warfare are to attack or "offensive cyber operations." Some are included in "defensive cyber operations," such as the use of intelligence, surveillance, and reconnaissance (ISR) systems that allow for planning and preparation for further military operations.

The difference between cyber warfare and activities in other cyberspace such as cyber crime, cyber espionage, cyber vandalism, of course, cannot be avoided. Starting with cyber vandalism, destructive activities, or entering a website without political goals or any profit to be achieved but based on pleasure (Cyberwire, 2021). It is different from cyber espionage. This activity is an action by a party to take or spy on the opposing party's information with a specific purpose, usually motivated by bringing down other countries and other political goals (Maskun, 2020). Lastly is cybercrime, that the main targets of operations carried out in cyber warfare are networks, software, to the hardware of a computer.

Kanun Jurnal Ilmu Hukum
Vol. 23, Issue 2, (August, 2021), pp. 477-490.

The attack's primary purpose is to paralyze, damage, or destroy the enemy's computer system, so in other words, it can be concluded that the purpose of this cyberwar is to paralyze the activities of other countries' governments based on computers and the internet. Therefore, the "victims" of cyber warfare are governments or companies. Cybercrime, on the other hand, is a conventional crime committed in cyberspace (theft, pornography, and fraud) and not a few where someone's data is the goal of cybercrime which is now known as hacking. Cybercrime targets are also generally individuals. What is quite prominent in cybercrime is that the perpetrators are dominantly individual, and the legal domain is criminal.

The description above explains and states that although cyber warfare is carried out in the same domain as other cyber activities, namely cyberspace, there are fundamental differences between them, so they cannot be equated. An important question is whether carrying out a "war" in cyberspace is justified? or whether "cyber warfare" is essentially a war. It is necessary to look at what and the terms of War itself.

Referring to the rules that already exist in international law, armed conflict or War is defined as a conflict that has an element of "violence" and escalates into the use of armed violence (use of force), and this does not require a formal declaration beforehand (Gandhi, 2001). Through his instrument-based approach, Jean Pictet (1990) states that a cyber attack can be categorized as "the use of armed violence" if the attack's impact or the use of cyber warfare methods has an effect similar to that which can be achieved by using conventional weapons. This argument can refer to the International Court of Justice in its decision on Nicaragua v. United States (ICJ, 1984) that the use of armed violence must be postulated on the correct arguments. Therefore, the ICJ's decision that the United States violated the principle of non-use force because the United States had violated the sovereignty of Nicaragua by assisting the opposing forces in overthrowing the legitimate government.

Another analysis to answer the question mentioned above is when countries can respond to cyber-attacks. It can be seen in Articles 2 (4) and 51 of the United Nations Charter, which collectively states that states can take an act of self-defense when elements of armed violence attack their sovereign territory. Using the arguments of Articles 2 (4) and 51 of the UN Charter will raise new questions, namely the existence and extent of a country's sovereignty in cyberspace. Tallinn, in rule 1, states that a country has the authority to exercise its control over all cyberinfrastructure and cyber activities within its sovereign territory (Schmitt, 2012). Thus, when a cyber-attack is categorized as an armed attack on a country's infrastructure and cyber activities, the state has the authority to defend itself, and this is the answer to whether cyberwar can be considered a "war" and is justified in the international community.

2) Cyber Warfare in International Law Framework

War has traditionally been regulated by international law through various conventions. These rules do not prohibit War but limit War, such as restrictions on the use of certain weapons, prohibition of attacks on specific objects and individuals, treatment of militias who cannot fight, and use of symbols. Restrictions on the action in War had existed long before World War 1 occurred. At that time, ancestral customs and teachings in religion became the primary source of a soldier's behavior in War. This series of rules regarding War is known today as humanitarian law.

On the other hand, activities in cyberspace have also been regulated in international law, specifically in the 2001 cybercrime convention initiated by the Council of Europe (CoE). Even though a regional organization formed it, Article 36 states that other countries outside the CoE can bind themselves to the convention. Through this convention, governments worldwide have begun to intensify themselves to formulate rules regarding activities in cyberspace on a national scale.

The thing that needs to be underlined from the previous description is that humanitarian law or the law of War only regulates traditional War or kinetic warfare. Meanwhile, looking at the

cybercrime convention, it can be found that cyberwar is not included in it. It concludes that the rules that specifically talk about cyberwarfare do not exist until now.

Tallinn Manual on international law applicable to cyber warfare is a guide formed by world legal experts and involves various relevant parties such as USCYBERCOM, NATO, and ICRC (Schmitt, 2012). This Tallinn Manual comprehensively explains how current international law applies in a cyberwar situation. Many cyberwar issues are answered in the Tallinn Manual, some basic things such as the definition of cyber War itself and state sovereignty in cyberspace. These two things are one of several reasons for the absence of legal rules regarding cyber warfare precisely.

On the other hand, there are still gaps in the Tallinn Manual itself. One example is the combatants' issue in cyber warfare, as it is known that the combatant parameters have been set in existing international humanitarian law. In that case, it is found that 2 of the four requirements are not met, namely carrying weapons openly and using signs that can be seen from a long distance, where all the conditions should be met collectively. For example, such as "hackers", which are generally individuals or groups from civilians who use technology to carry out cyberattacks during cyber wars, can these hackers become targets of attacks in cyberwars? These issues regarding the status of combatants have not been answered by the Tallinn Manual comprehensively.

Another drawback is also the existence of non-international cyber wars. One of the conditions in categorizing a non-international armed conflict is that part of the territory of the attacked country has been controlled by the rebellious party (Ghandi, 2001). Does this mean in the context of cyber warfare that the rebels have taken over part of the entire infrastructure or cyber activity by a country? It is still a question.

It is important to remember that this Tallinn Manual is not a new law but a guide, and from this, it can be concluded that this Tallinn Manual has no binding legal force for countries. Two instruments have binding legal force for states, international treaties, and international security

council resolutions in international law. First, of course, the Tallinn Manual does not fall into the Security Council's Resolutions category. However, to test whether the Tallinn Manual falls into another category, namely international treaties, it is necessary to look at the definition of the international treaty itself. Using the Vienna convention on treaty law, it can be found in Article 2 explaining that "Treaty means an international agreement concluded between States in written form and governed by international law, whether embodied in a single instrument or two or more related instrument and whatever its particular designation."

It can be concluded that the state forms international treaties. In contrast, the Tallinn Manual is developed by experts, so that the Tallinn Manual is not included in the category of international agreements. The exciting question now is, what if there is a cyberwar when there is still a legal vacuum regarding cyber warfare rules. In this regard, the ICRC once answered that if this method of cyber warfare produces an impact similar to that caused by War or conventional weapons, then the same provisions apply to conventional weapons.

The International Court of Justice, in its Advisory opinion on the legality of the threat or use of nuclear weapons in 1996, also supports this argument stating that one of the advantages of humanitarian law is that it can be applied to all types of War and weapons, including in the future (ICJ, 1996). The most crucial point is that cyber warfare is legal as long as civilians and objects are not the targets of the attack.

It is related to one of the doctrines in humanitarian law contained in the 1899 Hague Convention, namely the Marten Clause Doctrine. This clause states that when humanitarian law has not regulated a specific problem that occurs in the world, the applicable provisions must refer to the principles of international law, which are formed from humanitarian law, the customs of countries, and the conscience of the people.

3) State Steps in Dealing with and reducing the damage caused by Cyber Warfare

Some examples of cyberattacks that have had a reasonably severe impact, as mentioned above, show the possibility that the target country or object is not ready to face this attack model, especially when the target is attacked suddenly. However, in the end, cyberwar is a series of cyberattacks directed at both military objects and state infrastructure. In dealing with or reducing the impacts of cyber wars, it is necessary to protect from common cyber attacks.

The methods that can be applied by both the state and an agency in preparing themselves for the upcoming cyber attacks are as follows:

a. Periodic simulation and Improvement of the Quality of Human Resources in the Field of Cyber Defense

In 2010, the United States carried out a simulation called Cyber ShockWave which demonstrated the conditions during a cyberwar as realistic as possible (Chertoff, 2010). The results showed that America was not ready to attack with this model. The United States then conducted a simulation of being given a cyber storm exercise initiated by the Cybersecurity and Infrastructure Security Agency (2020), a form of exercise to test national defense from digital espionage attacks. Suppose the United States or other developed countries can conduct simulations to test their national defense readiness from the possibility of facing cyber-attacks. In that case, the vital question to consider is how prepared countries or agencies have never carried out simulations or improvements in their cyber defense systems?

The simulation carried out by the United States can be an example for other countries in the world facing the upcoming cyberwar. The simulation results will reflect the readiness of these countries to face cyber-attacks. This simulation can also be carried out with other countries through international cooperation. Nevertheless, of course, several points need to be considered in determining the effectiveness of the simulation, both if it is carried out independently or in collaboration. First, the frequency with which the simulations are carried out has become a standard

agreement that technology develops rapidly over time. The simulation results carried out by America in 2010 will not be so effective when there is a cyberwar in today's era. It is, of course, by looking at the increasingly sophisticated tools and programs that already exist, giving rise to the potential of a new cyberattack model. So, to support the effectiveness of this simulation, countries need to do it as often as possible.

Second, the technology used. Simulations about cyber warfare or cyber-attacks will not be very effective when the tools used to run the simulation cannot support achieving the goals. Of course, this will be an additional burden for countries in ensuring the technology they have is the latest and most up-to-date. Of course, it will be a challenging task for countries that do not have sufficient financial capacity. Third, the capability of human resources. The third point is quite closely related to the second point. Even sophisticated technology will not bring out its maximum potential when used by untrained hands. The training of these users is critical in increasing defense both during cyber warfare and from common cyber attacks.

In the end, the results of this simulation will significantly depend on the country's capabilities and intentions. Through the simulations carried out, governments will be able to assess in real and detail which parts of their cyber defense need to be improved.

b. Artificial Intelligence System (AI) in Improving Cyber Defence

Artificial intelligence (AI) cannot be avoided when discussing the development of technology and cybernetics. AI is defined as a system that simulates human intelligence in acting and making choices (Frankenfiled, 2021). This intelligence is generally used to solve complex problems and takes a long time because AI can create solutions in a short time. AI acts independently and does not require human intervention once it is operated, and through various activities, the AI learns and develops itself as if it were human by nature.

The development of AI in its use on the battlefield has been going on for a long time now. However, AI systems for war purposes are only embedded in a combat robot and have not yet

reached the point where AI has penetrated to carry out cyberattacks through cyberspace. In 2017, a group of AI experts gathered in California at a conference and proposed 23 principles, which are now known as Asilomar AI principles (Mahbub, 2017).

Some of the discussions centered on how beneficial it is to use AI to identify and protect against computer attacks by detecting and responding automatically to such attacks. Not to mention a dilemma when this AI system is used otherwise to carry out cyberattacks, which means these attacks have the potential to be even harder to contain and harder to track. It is another dilemma for countries that do not have access to the latest technology.

Several agencies that have tried to implement AI systems in their cyber systems include IBM/Watson, Juniper Networks, and Balbix. With the hope that AI can increase cyber defense and minimize the potential damage caused by a cyber attack. However, keep in mind again that on the other hand, cybercriminals, hackers, or other agencies and parties can also use this AI system to defeat these defenses and at the same time go undetected. It is where the term "AI Conundrum" comes in. With the development of AI, making it possible to implement it in cyber defense is not impossible, so companies and agencies that want to use it need to increase awareness of the shortcomings that this new technology will bring.

CONCLUSIONS

Cyber warfare is not something new and impossible again; practices in the field have proven that the potential for replacing conventional War is genuine, especially with the technology that supports cyber warfare. However, there are still no clear and specific international rules governing cyber warfare, so customary War laws are still in effect today. Therefore, every party, be it companies or the state, needs to prepare themselves by increasing their cyber defense to ward off or reduce the impact of a cyber-attack. Periodic simulations to improve the capabilities of technology

information personnel and implementing systems in cyber defense are tangible steps to minimize cyber-attacks.

REFERENCES

Books

Marzuki, P. M. (2016). *Penelitian Hukum*, (ed. Revisi), cet ke-12, Jakarta, Prenada Media Group.

Maskun, et al. (2020). *Korelasi Kejahatan Siber dan Kejahatan Agresi Dalam Perkembangan Hukum Internasional*. Makassar: Nas Media Pustaka.

Pictet, J. (1990). *The Principles of International Humanitarian Law*. Geneva: Henry Dunant Institute.

Richard, A. C., Knake, R. (2010). *Cyber War The Next Threat to National Security and What to Do About it*. United States of America: HarperCollins.

Journal Articles

Bernard, V. (2016). Tactics, Techniques, Tragedies: A Humanitarian Perspective on the Changing Face of War. *International Review of the Red Cross*, *97* (900): 1513.

ICRC. (2016). The Evolution of Warfare. *International Review of the Red Cross*, *97* (900): 1513.

Michael, N. M. (2012). International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. *Harvard International Law Journal Online*, *54* (12): 14-37.

Liivoja, R. (2016). Technological Change and the Evolution of the Law of War. *International Review of the Red Cross*, *97* (900): 1513.

Artiadi, S. B. (2013). Perlunya Pembangunan Sistem Pertahanan, Siber (Cyber Defense) yang Tangguh bagi Indonesia, *Media Informasi Ditjen Pothan KEMHAN*, *1* (3): 31-35.

Research Report

ICJ. (1984). *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. the United States of America), Jurisdiction and Admissibility*, *Judgment,* ICJ Reports. The Netherlands: The Hague.

ICJ. (1996). *The legality of the Threat or Use of Nuclear Weapons, Advisory Opinion July 8, 1966*, ICJ Rep. 1996. The Netherlands: The Hague.

Thesis

Tampubolon, A., Eliva, K. (2018). *Kedudukan Cyber Warfare dalam Hukum Internasional*. Thesis. Surabaya: Faculty of Law, Universitas Airlangga.

Internet Resources

Chertoff. Michael. (2010, March 15). *Cyber ShockWave Exposed Missing links in US Security*, Retrieved August 16, 2021, from https://gcn.com/articles/2010/03/15/commentary-chertoff-cyber-shockwave.aspx.

Cybersecurity and Infrastructure Security Agency. (2020, August 10). *Cyber Storm 2020: After-Action Report*, Retrieved August 20, 2021, from https://www.cisa.gov/sites/default/files/publications/Cyber_Storm-2020_After-Action-Report_01052021_Final.pdf

Cyberwire. (2019, November 8). *Cyber Vandalism*, Retrieved August 15, 2021, from https://thecyberwire.com/glossary/cyber-vandalism.

Frankenfield. Jake. (2021, March 8). *Artificial Intelligence (AI)*, Retrieved August 16, 2021, from https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp.

Gandhi. M. (2001, November, 11), *Notes and Comments Common Article 3 of Geneva Convention, 1949 in the Era of International Criminal Tribunals*, Retrieved August 14, 2021, from http://www.worldlii.org/int/journals/ISILYBIHRL/2001/11.html.

ICRC. (2015, August 15) *Iran, Victim of Cyberwarfare*, Retrieved August 14, 2021, from https://casebook.icrc.org/case-study/iran-victim-cyber-warfare.

Amri, M. (2017, October 3). *Ahli Teknologi Bikin Agama Baru Bertuhanakan Kecerdasan Buatan*, Retrieved August 20, 2021 from https://tekno.tempo.co/read/1021681/ahli-teknologi-ini-bikin-agama-baru-bertuhankan-kecerdasan-buatan/full&view=ok.

Pfeffer. A. (2019, November 8). *Israel Suffered Massive Cyber Attack During Gaza Offensive*", Retrieved August 14, 2021, from https://www.haaretz.com/1.5065382.

Ragan. S. (2016, February 15). *Ransomware takes Hollywood Hospital offline, $3.6M demanded by attackers*, Retrieved August 19, 2021, from https://www.csoonline.com/article/3033160/ransomware-takes-hollywood-hospital-offline-36m-demanded-by-attackers.html.

CYBER WARFARE: NATIONAL SECURITY IN DEALING WITH CHANGING METHOD OF WAR

ORIGINALITY REPORT

4%	3%	2%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.whatconvention.org Internet Source	<1%
2	calhoun.nps.edu Internet Source	<1%
3	Submitted to Mount Kenya University Student Paper	<1%
4	Submitted to American Public University System Student Paper	<1%
5	Submitted to King's College Student Paper	<1%
6	dspace.gazi.edu.tr Internet Source	<1%
7	Matthias Vanhullebusch. "The Law of International Humanitarian Relief in Non-International Armed Conflicts", Brill, 2022 Publication	<1%
8	www.collectionscanada.gc.ca Internet Source	<1%

9	www1.umn.edu Internet Source	<1%
10	A Erna Mustafa, Arman Arman, St Nurani Sirajuddin, Nurdwiana Sari Saudi. "Social status relationship to purchase of tedong bonga for the Community Toraja Tribes", IOP Conference Series: Earth and Environmental Science, 2019 Publication	<1%
11	ceje.ch Internet Source	<1%
12	legal.un.org Internet Source	<1%
13	ndl.ethernet.edu.et Internet Source	<1%
14	Albert Olagbemiro. "Cyberspace as a Complex Adaptive System and the Policy and Operational Implications for Cyberwarfare", International Journal of Cyber Warfare and Terrorism, 2015 Publication	<1%
15	hdl.handle.net Internet Source	<1%

Exclude quotes	On	Exclude matches	< 5 words
Exclude bibliography	On		