POLICY, LAW, NOTARY AND REGULATORY ISSUES (POLRI)
Volume 2 ISSUE 1 (2023)

PROXY WAR IN THE ERA OF GLOBALIZATION IN INTERNATIONAL LAW PERSPECTIVE

I Putu Bagus Arya Krisna[1*], I Wayan Novy Purwanto[2]
[1,2] International Law Specialization Program, Faculty of Law, Universitas Udayana
E-mail: [1)] krisnabagusarya@gmail.com, [2)] novy_purwanto@unud.ac.id

Abstract

Along with the development of science and technology, there has also been a shift in the form of war which we know is synonymous with military force, firearms and artillery explosions. Marked by the emergence of Proxy War as a new style in the world of war. The absence of direct involvement and the existence of competition between the great powers between the parties is one of the characteristics of the Proxy War itself but the Proxy War itself still has an impact that is as dangerous as a normal war, because Proxies can be formed from within/outside the country which makes it be difficult to detect. This paper aims to find out how Proxy War exists in historical developments and to see and understand Proxy War in the present which is very closely related to cyber warfare. The method used was a normative legal research method whose research focuses on the relationship between norms and predicts their development in the future. The findings showed that proxy war as a new style of warfare creates its own worries. Because the close link between Proxy War and Cyber War can cause national instability in a country. If propaganda that occurs in cyberspace is spread widely and systematically, this has the potential to cause riots within a country.

Keywords: *Cyber Warfare, National Instability, Proxy War*

1. INTRODUCTION

When we hear the word "war," it immediately brings to mind images of conflict, brutality, and carnage. It cannot be denied that since the beginning of human civilization, war has colored the history of the development of life on earth, both the wars that occurred during the kingdom era and the wars that have raged in the modern era. War itself is a form of interaction that is formed from the relationships that occur between humans. Not infrequently differences in interests, a sense of dissatisfaction and disputes between the parties are a number of factors that suggest a war occurs.

We have heard many stories that have been engraved in the dark history of our civilization about wars that have claimed many human lives for various reasons, both economic, social, political, territorial disputes and other disputes that cannot be resolved through deliberation. Etymologically, war has a meaning, namely physical and non-physical action or hostile conditions carried out by means of violence and other uses of force that occur between two or more human groups in order to fight over a goal.

Meanwhile, Karl Von Clausewitz in Nurwulansari et al. (2022) expressed his opinion regarding the definition of “war as a struggle on a large scale intended by one party to subdue its opponent in order to fulfill its will”. From some of the meanings that have been conveyed above, it can be understood that war is something that is synonymous with violence and the use of force to achieve a goal.

Along with the development of the times and technology, we are now in the era of globalization where the exchange of information has become so easy and there have been various shifts in the aspects of human life that are now completely modern, so it also

happens in the form of the war itself. Today, war is no longer visible to the naked eye, no longer synonymous with the use of weapons and violence but still has the same destructive impact as the conventional war we know.

This is what became known as a proxy war. It may still sound foreign to most people's ears, but this proxy war is currently happening in the midst of an international audience. Proxy War itself has the following meaning “A proxy war is a conflict inflicted by a major power or powers that do not become involved in it directly. Often, proxy wars involve countries fighting their opponents’ allies or helping their allies fight their opponents” (Hidayat, 2017).

Thus, the above understanding about "proxy war" refers to a conflict that occurs between a large power or more that are indirectly involved in it (Dalimunthe et al., 2022). Often, proxy wars involve countries fighting allies of their enemies or helping their allies against their enemies. From the above understanding it can be seen that there is an element of indirect involvement, this is what makes proxy wars difficult to see with the naked eye but has an impact that is just as dangerous as other wars.

Especially the internet which is now a means of connectivity that connects people from all over the world. Etymologically the internet comes from the word Interconnection and Networks. The internet itself is defined as “a network of networks that connects computers all over the world” (Syafrizal, 2020).

Even though the presence of the internet as a means of connectivity brings a variety of positive impacts, of course, behind all this, there are various negative impacts that can be detrimental and have a damaging impact. In the development of cyber law itself, the term Cyberspace is known, which is a space for long-distance conversations to take place. not in the phone, but in the intangible space that is out there (Nugroho et al., 2020).

In connection with proxy wars, cyberspace or the internet itself is a medium that can be used by parties who have an interest (state or other entity) to form proxies to achieve predetermined goals. This could have started with the spread of anti-government narratives, radicalism, and the spread of certain ideologies through cyberspace.

Therefore, Cyber Law has an important role in preventing undesirable things from happening, because after all the damage that arises from within is more difficult to see than the damage that is visible from the outside. As such, this research will be oriented towards the existence of Proxy War in the Cyberwarfare era in the perspective of International Law and its preventive efforts.

Based on the background that has been explained, writing paper aims to find out the importance of cyberlaw in the era of proxy wars and to know and understand proxy wars in more depth which will be studied in the perspective of International Law.

2. RESEARCH METHODS

The writing method used to compile this scientific journal was a normative law research method in which the subject matter of the study was law conceptualized as norms or rules that apply in society and become a reference for society itself. Normative legal research was also known as doctrinal legal research, as stated by Hutchinson that doctrinal legal research in broad outline was research on regulations governing certain categories, analyzing the relationship between regulations, explaining areas that experience obstacles, and even predicting future developments (Muhajirin & Maya, 2017).

3. RESULTS AND DISCUSSION

3.1. Social Media as A Proxy War Catalyst and Preventive Efforts on A National Scale

Looking back to find out and understand the history and development of something is one method that is often used to get more comprehensive information about a problem. Likewise in the context of understanding Proxy War. In providing a classification of a war that can be categorized as a proxy war, we can see from the existence of several elements which include:

1) There is a party that becomes a proxy (State / Non-State Actor)
2) There is a strategic goal
3) The existence of an indirect involvement (indirect involvement) (Mumford, 2013)

Some of the elements above can of course be used as a measure to classify a war/conflict as a Proxy War.

How then can social media be said to be one of the catalysts for Proxy War in the era of globalization? before examining further, the term catalyst used in writing this scientific journal has the meaning of "something that causes change and causes new events or accelerates an event". Seeing the fact that the number of social media users in Indonesia continues to increase from year to year makes social media one of the platforms that is very vulnerable to being infiltrated by the interests of proxies. This is based on survey results quoted from APJII (Association of Indonesian Internet Service Providers) which recorded in 2017 which noted that 143,26 million Indonesians actively used the Internet and 87,13% of the total are active social media users who have various age ranges.

The trend of social media in Indonesian society certainly has both positive and negative impacts simultaneously. Ease of access to information is expected to be one of the driving factors for human resource development in Indonesia, but the spread of fake news (hoaxes) and the use of social media as a tool to divide the nation must also be watched out for as having a potentially high negative impact.

The government as the holder of authority must participate in creating a safe and peaceful life for the nation and state, in this case as a preventive measure for the disintegration of the nation, the government forms a legal product which we know as Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions, or better known as the ITE Law which was issued in response to the government's response to the rapid progress of access to information technology, has become one of the legal instruments that provides restrictions regarding activities that may and may not be carried out in cyberspace. As referred to in the summing up of articles 27 – 37 of the ITE Law, it can be seen that there are limits set by the government in terms of Information Technology.

The spread of radicalism through social media, the existence of divisions caused by differences of opinion both related to politics and religion are several things that are very vulnerable and have the potential to form proxies that damage from within. The right to freedom of opinion is regulated and protected by the constitution, but what is happening now is not an argument based on logical reasons and scientific references but rather hate speech and provocation. Segregation occurs on social media in the name of one group and another, which then develops into a growing dichotomy in society. This is a particular concern because several things that have happened recently have the potential to disintegrate the nation due to differences in political choices and religious matters.

3.2. Cyber Warfare in International Law

Seeing the relationship between Cyber Warfare and Proxy War, we can depart from the explanation previously described that there has been a shift in the characteristics of war which are now no longer closely related to armed contact and military force, which is also supported by the rapid development of technology and the rapid exchange of information on a massive basis on the internet.

As explained in the previous section regarding Proxy War including its definitions and elements, this section will focus on Cyber Warfare and its existence in the Proxy War era. The term "Cyber Warfare" may sound unfamiliar to some people, in Indonesian, while this term also known as "Cybernetic War". In KBBI or Indonesian Dictionary, Cybernetics means the science of communication and supervision, especially with regard to comparative studies of automated surveillance systems.

The full definition of Cyber Warfare is put forward by UNTERM (United Nations Multilingual Terminology Database) that "Cyber Warfare is The offensive and defensive use of information and information systems to deny, exploit, corrupt or destroy an adversary's information, information based processes, information systems and computer based networks while protecting one's own. In this case, such actions are designed to achieve advantages over military or business adversaries" (P. A. Prasetyo, 2020).

If freely translated, the provisions above can be interpreted as an act of using information and information systems both offensively and defensively to prevent, utilize, damage and destroy the opponent's information, or processes based on information systems and computer-based networks. This action was designed to gain both military and business advantages.

Meanwhile, the United Nations Interregional Crime and Justice Research Institute (UNICJRI) provides a simpler definition of Cyber Warfare, namely "Any action by a nation-state to penetrate another nation's computer networks for the purpose of causing some sort of damage" (B. Prasetyo, 2022). This definition is simpler without losing the meaning that there is an element of action taken to penetrate a country's computer-based network system with the aim of causing damage.

Referring to the data compiled by The Center for Strategic International Studies (CSIS), cited by Naufal Herdanto (2022) estimates that between May 2006-June 2011 there were at least 78 significant cyber incidents, some of which resulted in successful attacks on government agencies, defense and technology companies with estimated losses of millions of dollars.

In order to provide evidence that Cyberwarfare has an important role in the Proxy War era, we can look at the case of the Stuxnet virus attack in 2012, which is a virus designed by computer scientists from the United States and Israel with the aim of slowing down the Uranium repair system at Nuclear facilities in Iran and to paralyze Iran's nuclear arsenal.

Directly related to Cyber Warfare, the importance of regulating Cyber Crime is of particular concern to the international community. Cyber Crime itself was defined at the 10th UN Congress in Vienna in 2000 as:

1) Any action taken by means of an electronic device that targets computer security systems and processed data (in a narrow sense).
2) Any illegal action carried out with the intention of or related to a computer system or network, including criminal acts such as illegal possession, provision or distribution of information through a computer system or network.

The international legal instruments that are relevant to Cyber Crime which are used as a reference in writing are the 2001 Convention on Cybercrime initiated by the Council of Europe (European Union) in Budapest. This convention can be said to be one of the effective efforts in the context of International Law because this convention acts as a Legally Binding Hard Law for the parties. The 2001 Convention on Cybercrime was drafted to form harmonization of International Law into the National Law of the countries that ratified this convention. This is strengthened by the existence of provisions to implement the provisions of the Convention into the Criminal Law of each country that ratifies it, as well as providing formal legal provisions in investigative procedures, investigations and prosecution. As well as the provisions on Extradition and Mutual Assistance in Part III of this convention, making the 2001 Convention on Cybercrime one of the instruments of international law that was successful in forming Legal Harmonization, especially in the realm of Cyber Crime.

Definitively, there is a difference in the meaning between proxy war and cyberwarfare where in general a proxy war is a power competition between 2 or more parties that occurs without the direct involvement of the parties. Meanwhile, cyber warfare is generally defined as the use of a computer system or network as a means to launch an attack on a computer network from a country or other institutions and entities.

Both Proxy War and Cyber warfare have correlations that are quite relevant in writing this scientific journal. Because with the special characteristics of a Proxy war that allows no direct contact between conflicting parties, this makes these feuds now occur in cyberspace. By starting with simple things as a trigger of more complicated problems that have a damaging impact and disturb the stability of the country.

The importance of harmonization of international legal products into Indonesian national law, especially in the realm of cyber law in order to prevent the occurrence of unlawful acts in cyberspace, can be used as an alternative to form a preventive and repressive effort related to cybercrime. Bearing in mind that every country has the same international legal responsibilities from all forms of cyber operations that impact other countries (International Group of Experts at NATO Cooperative Cyber Defence Centre of Excellence, 2013). This is strengthened by the role of international organizations such as the ITU (International Telecommunication Union) which established the ITU Toolkit for Cybercrime Legislation as a guide for countries to draw up legal regulations related to cybercrime.

Until now, international legal instruments have only provided recommendations or the Rule of Guidance regarding the preparation of legal regulations relating to cybercrime. Clearly, this is inseparable from the jurisdiction of the state in relation to all actions that occur within its jurisdiction where a state is obliged to take firm action against all criminal actions based in cyberspace as long as the action occurs within the territory of a country or has a direct impact on the security and stability of the country concerned. .

Regardless of the role of international organizations, the role of the government, especially as regulators, is very important in realizing harmonization between international legal instruments and their application in national legal products, bearing in mind that the stability and security of the country in the era of globalization are not only vulnerable to visible threats but also vulnerable to threats that invisible, such as Proxy War, which uses social media as a medium for forming proxies. Hence, the role of the state is very important in preventing the formation of proxies from the development of radical understandings and narratives that are provocative of the safety and stability of the state.

4. CONCLUSION

Based on the findings, it can be concluded that Proxy Wars is a real form of a shift in the world of war. It is marked by the absence of direct involvement from the proxy maker as a big power that appoints or forms other parties, both state actors and non-state actors as an extension to achieve the strategic goals of the proxy maker himself. In the current age, Proxy War is often used by parties who want to take advantage indirectly from the occurrence of national instability in a country. Technological developments and the rapid exchange of information have now become a medium for parties aiming to form proxies from within the country with the aim of triggering national instability. As a result, public awareness and the role of government are very important in forming regulations related to cyberspace in order to prevent national disintegration that occurs as a result of efforts by foreign powers to undermine the national life of a nation.

Hence, it is extremely vital for there to be a high level of public knowledge of the presence of unseen dangers that occur as attempts by foreign powers in order to avoid conflicts in the life of the country and the state. Besides, it is hoped that the government's role in forming regulations that are oriented towards technological development, as well as updating the national cyber system can be the first step in preventing the entry of propaganda and foreign powers that can affect the stability of the country by contributing to the importance of filtering information that is widely circulated in society.

REFERENCES

Dalimunthe, S. R., Pujawati, S. A., & Sitorus, A. S. A. (2022). Technical Security In Ite Law And Copyrights Of Devices And Systems. *POLICY, LAW, NOTARY AND REGULATORY ISSUES (POLRI)*, *1*(2), 27–36. https://doi.org/10.55047/polri.v1i2.124

Hidayat, S. (2017). Proxy War And Indonesia's National Security: Victoria Concordia Crescit. *Jurnal Pertahanan & Bela Negara*, *7*(1), 1–22.

International Group of Experts at NATO Cooperative Cyber Defence Centre of Excellence. (2013). *Tallin Manual on International Law Applicable to Cyber Warfare*. Cambridge University Press.

Muhajirin, M., & Maya, P. (2017). *Pendekatan praktis: metode penelitian kualitatif dan kuantitatif*. Idea Press.

Mumford, A. (2013). Proxy warfare and the future of conflict. *The RUSI Journal*, *158*(2), 40–46.

Naufal Herdanto, R. (2022). *Kebijakan Cyber Security Terhadap Keamanan Negara: Studi Kasus Australia Pada Tahun 2010-2020*. UPN" Veteran" Yogyakarta.

Nugroho, C., Sos, S., & Kom, M. I. (2020). *Cyber Society: Teknologi, Media Baru, dan Disrupsi Informasi*. Prenada Media.

Nurwulansari, N., Suwarno, P., Syamsunasir, S., & Widodo, P. (2022). Strategi Pemerintah Dalam Menghadapi Proxy War Sebagai Salah Satu Penyebab Gerakan Separatisme di Indonesia. *Jurnal Kewarganegaraan*, *6*(2), 2518–2528.

Prasetyo, B. (2022). Kesiapan Oeprsi Cyber Warfare Markas Besar TNI Angkatan Darat 2018. *Strategi Pertahanan Darat (JSPD)*, *8*(2), 72–100.

Prasetyo, P. A. (2020). *Penggunaan Kapabilitas Cyberwarfare Tiongkok dalam Menghadapi Cyber Superiority Amerika Serikat*. UNIVERSITAS AIRLANGGA.

Syafrizal, M. (2020). *Pengantar jaringan komputer*. Penerbit Andi.