The Challenges of Civil-Military Cooperation in The Face of Cyber Threats in Indonesia

Tommy Mandala Putra, I Wayan Midhio, Deni D.A.R
Republic of Indonesia Defense University, Indonesia

***Abstract*—Non-military threats in the era of globalization are so complex, cybercrime is a threat that must be considered by all groups, including the government, military and society. The existence of cyber threats requires strengthening civil-military cooperation to deal with them. In this research, the writer wants to knowwhat are the challenges ahead for civil-military cooperation in dealing with cyber threats in Indonesia. Methods of data collection using literature review. The results of the research are cyber threats at the civilian level. The government has regulated matters relating to activities in cyberspace through laws and regulations. At the military level, cyber defense has been established to deal with cyber threats. It can be said that civil-military cooperation has been carried out by using their respective powers. And another form of cooperation is civilians supporting the military in defending the country's sovereignty and participating in various threats.**

***Keywords*—Non-military threats, civil-military cooperation, cyber**.

I. INTRODUCTION

In the current era of globalization, non-military threats are more complex in their impact on countries in the world. Non-military threats such as terrorism, ideological propaganda, drug abuse, exploitation of natural resources and cybercrime have a direct impact on all elements of the state. These threats are more real than military threats such as territorial violations, aggression, invasions and others. Law Number 3 of 2002 concerning National Defense is a sense of security and peace of the Indonesian people within the Unitary State of the Republic of Indonesia (NKRI) which has regulated to defend the sovereignty of the Republic of Indonesia from various threats.

To deal with various threats, the increase in cooperation between members of the military and civilians, seen since 1990, needs to be increased more efficiently. The function of military units is not only to protect state security from traditional threats, but also to support peace and help reduce problems in society. (Sutisna et al. 2018). Civil-military cooperation will have a significant positive impact in dealing with various threats. In addition, civil-military cooperation also demonstrates that civil-military relations are an inseparable unity.

At a global level, currents that are happening all over the world today have brought the world to an era of information and communication technology development so as to create an all-digital era or digital world. In this case, the development of computer technology and the internet has become a new means for countries in the world to be used as a tool to carry out various penetrations, influences and infiltrations into various countries so that it is very encouraging for the world to develop complex, diverse and pluralistic developments. Through globalization, each country can pass through one country to another without any dominant state control and control. (Purwanto 2010)

Current and future global challenges indicate that the world cannot be separated from political and economic uncertainty. On the strategic side, there is a "shifting military power" from weapons of mass destruction to the intensity of dissemination of advanced technology, both manned and unmanned, which is operationalized in unconventional asymmetric warfare. Also present is a new war mandala in information technology, namely increasing competence of hackers (Cyber Armies), popularly known as Cyber War. In the face of various dynamics of change occurring globally for Indonesia, there is only one step that can be taken collectively in response to protect the country, namely shoulder-to-shoulder cooperation between civilians and the military. (Sjafrie S 2015)

The challenges of civil-military cooperation in the future will be more complex with globalization which has spread to all elements. In the industrial revolution 4.0, cyber threats are a special concern that must be anticipated and fought together. The shift of cyber threats, cybercrime into cyber warfare (cyber warfare) will change the traditional pattern of society to become technologically literate but can increase failure in carrying it out. Because the misuse of technology will have an impact on crimes that can destroy themselves. It is also a state threat that can weaken state security.

The Check Point Software Technologies report shows that cyberattacks in Indonesia occur seven times more than the world average with the government and military, manufacturing and banking sectors being the three sectors most affected by cyberattacks. (Abid 2021). Cyber threats in the military are important to study because the military has an important role in maintaining national sovereignty and defense. With the existence of strong civil-military cooperation going forward, it is hoped that cyber threats can be resolved. Therefore, the author is interested in studying how the challenges of civil-military cooperation will be in dealing with cyber threats in Indonesia, which are so complex due to changes in globalization.

Research methods

The methodology used in this research is a literature study approach. Literature study or literature can be interpreted as a series of activities related to the methods of collecting library data, reading and taking notes and processing research materials. (Antar and Supriyadi 2016). Literature review or literature study is an activity that is required in research, especially academic research whose main purpose is to develop theoretical aspects as well as aspects of practical benefits. (Sukardi 2013).

In literature research, there are at least four main characteristics that the author needs to pay attention to. (Antar and Supriyadi 2016). including: First, that the writer or researcher is dealing directly with text or numerical data, not with direct knowledge from the field. Second, the library data is "ready to use" meaning that the researcher does not go directly to the field because the researcher is dealing directly with the data sources in the library. Third, that library data are generally secondary sources, in the sense that researchers obtain materials or data from second-hand sources and not original data from first-hand data in the field. Fourth, that the condition of the library data is not limited by space and time.

Based on the foregoing, the data collection in this study was carried out by reviewing and/or exploring several journals, books, and documents (both printed and electronic) as well as other sources of data and/or information deemed relevant to the research. or study.

II. RESULTS AND DISCUSSION

Cooperation Theory

Cooperation is a form of social interaction. (Landsberger 2011) Cooperation is a group process in which members support and rely on each other to achieve a consensus. (Thomas and Johnson 2014) cooperation is a grouping that occurs among living things that we know. Cooperation can remove mental barriers due to limited experience and a narrow perspective. So, you are more likely to discover your own strengths and weaknesses, learn to respect others, listen with an open mind, and build cooperative agreements. By working together small groups will be able to overcome various forms of obstacles, act independently and with a full sense of responsibility, rely on the talents or thoughts of each group member, trust others.

So cooperation can be said to be a process where a person or group interacts with each other having the same goals and achievements in an activity. Cooperation will make it easier for a person or group to carry out a vision and mission that will be faced. With the cooperation of one goal. Then an activity or thing to be carried out can be passed easily.

Civil-military cooperation is a step in achieving common goals at the level of the interests of the state and society. Cooperation can increase the close relationship of a goal to strengthen the vision and mission to be achieved. In this study, civil-military cooperation is to deal with non-military threats such as cyber threats. Cyber threats need a complete solution in dealing with what will happen. Civil-military has a composition that can solve this problem.

Civil Military Cooperation in Indonesia

The United Nations (UN) in 2004 through the United Nations Humanitarian Civil-Military Coordination (UN-CM Coord) issued a Civil-Military Coordination Officer Field Handbook issued by the United Nations Office for the Coordination of Humanitarian Affairs (OCHA) with the European Commission Department of Humanitarian Aid. Meanwhile, coordination or cooperation between civil and military in Indonesia has been carried out, but there is no fixed procedure/doctrine and also not structured, such as CIMIC (NATO) or CMCoord (UN). (Satrio, Wayan Midhio, and Dar 2018).

Civil-military cooperation aims to maximize positive effects and minimize negative effects. (Sutisna et al. 2018). In times of peace, the cooperative relationship between civilian and military is cooperation, the interaction of civil-military relations becomes very close and becomes one, it can be seen that there is a merger so that both civilian and military work together in one organization.

When facing a complex emergency situation, a liaison or liaison from both the civilian and military parties is formed with a structure that is adapted to an operation at hand. (Sutisna et al. 2018)

The division of civil and military tasks is divided into three categories Un-Ocha (2015) namely Direct Assistance in peacetime the military can provide direct assistance to the community; Indirect Assistance sometimes the task of the military is just to help and finally Infrastructure Support provides general services in humanitarian activities. This provides an explanation of the core principles of implementing humanitarian assistance, namely Humanity, Neutrality, Independence, and Impartiality.

Civil-military cooperation can be said to be effective collaboration in various activities. Especially in the development of globalization which is constantly changing and full of uncertainty. Civil-military cooperation will greatly impact the policy process and the strength of the state's defense from various threats. Today Indonesia's cyber threats continue to increase every month, this becomes important for the military as a state security factor in preventing the entry of crime, especially in cyberspace. Military professionalism will depend a lot on what will happen.

There are 2 (two) categories of military professionalism in theory. (Effendy 2008). First, Huntington's old professionalism made the military only a means of state defense without being involved in the country's political affairs. Second, new professionalism by Stephan is defined as a form of military professionalism that involves itself in the

socio-political life of the country. (Widiyanto and Dian Hikmawan 2019).

In Indonesia, civil-military cooperation has been built since the reform era, the dynamics of civil-military cooperation since the reformation can be said to go up and down, depending on the situation. However, recently civil-military cooperation is getting closer due to several factors. One of the things that makes the civil-military close is the dynamics of globalization which cannot be predicted by anyone. Puts all the elements together and becomes one. Therefore, the civil-military becomes increasingly close and can have the same goal in defending state sovereignty and national defense.

The Challenge of Facing Cyber Threats in Indonesia

National defense is organized by the government and prepared early with the national defense system through efforts to build and foster the capability and deterrence of the state and nation as well as overcoming any threats. (Tek Oki 2015). The state defense system in the face of military threats places the TNI as the main component, supported by reserve components and supporting components. In dealing with non-military threats, placing government institutions outside the defense sector as the main element that is adapted to the form and nature of the threat, supported by other elements of the nation's power. (Tek Oki 2015).

In facing the dynamics of global development, civil-military cooperation has many challenges that must be done. One of them is cyber threat and cybercrime. Cybercrimes will have an impact on state stability and a threat to state sovereignty from a technological perspective. Data from the National Cyber and Crypto Agency (BSSN) (2021) in January-May 2021 there were approximately 448 million cases of cyberattacks. The next three months in August saw 440 million cyberattacks. The total from January-August was 888,711,736 million cyberattacks. If you look at the data, cyberattacks continue to increase from month to month. This is a threat to the state in the cyber security system.

Cyber threats are important because over time the threats are growing. In the virtual world, for example, has given birth to cybercrime. Cybercrime is a type of transnational crime, because it involves actors from two or more countries, the victim can be from more than one country, the modus operandi is in cyberspace using computers and the internet, and the evidence is in the form of electronic evidence, so it requires a process. modern and sophisticated law enforcement. Cybercrime can attack various sites, blogs, emails, social media, and various other computer software so that it is very dangerous for various companies, banks, government agencies, as well as the military and police based on computers and the internet online. (Subagyo 2015).

Malware attacks are the most common in cyberattacks, disrupting service availability (denial of service) and trojan activity. These threats include attacks of a technical nature as well as attacks of a social nature such as spreading false news or hoaxes. Various cyberattacks that occurred in Indonesia have a big task in dealing with various crimes in cyberspace. Cyber threats as well as cybercrimes will be a challenge for the state in strengthening security in the field of communication and information technology. Therefore, it is important for the government to immediately improve security in the field of information technology.

The government has regulated matters relating to activities in cyberspace through laws and regulations. Cyberattack according to national law is seen as a crime and is in the domain of national security (authority of law enforcement officers / police). In addition, there is also Law no. 11 of 2008 concerning information and electronic transactions (ITE) essentially regulates cybercrime, e-commerce, copyrights & consumer protection and unfair competition. The crimes regulated in this law are very diverse, ranging from crimes related to internet technology activities such as abuse of access, interception, entering computer systems or electronic systems illegally, to committing crimes in the form of destruction, alteration, omission and manipulation of electronic data information. (Permanasari 2018).

In a more specific regulation, a cyberattack is formulated in the Minister of Defense Regulation No. 82 of 2014 as "All forms of actions, words, thoughts, whether intentionally or unintentionally by any party with any motive and purpose, carried out in any location, which are targeted at electronic systems or their contents (information) or equipment that relies heavily on technology and natural networks of any scale, on vital and non-vital objects in the military and non-military scope, which threatens the sovereignty of the state, territorial integrity and national safety". These cyberattacks can occur when the intensity and scale of cyber threats increases and changes from a potential threat level to a factual one. (Permanasari 2018).

This is generally in the form of actions aimed at entering, controlling, modifying, stealing or damaging or destroying or disabling information systems or assets. This action can take the form of cyber warfare which is carried out intentionally and coordinated with the aim of disturbing state sovereignty or in the form of cyber violence, which is carried out unintentionally, passively and on a small scale. (Permanasari 2018).

In order to strengthen civil-military cooperation in facing the challenges of cyber threats, it is necessary to design an integrated cyber defense strategy to secure national interests and national defense. The demands of the TNI now and in the future are to be consistent in maintaining the military's code of honor while developing intellectualization and the profession to achieve interoperability on the scale of military missions and mutualistic interactions with civilian capabilities. (Sjafrie S 2015).

Cyber defense is a comprehensive form, meaning

that it does not only strengthen cyber security infrastructure but also includes strategies, policies, research and collaboration with various parties related to cyber security, which are not limited to state entities such as international organizations, cyber security companies. (Setiyawan n.d.).

With cyber defense, it is hoped that cyber threats and crimes can be controlled and resolved, as well as an effort to tighten civilian positions in using information technology. In using technology, civilians are sometimes uncontrolled, which results in gaps where the interests of other countries and the community are not known. Therefore, through cyber defense, it will strengthen civilian and military control to jointly safeguard state sovereignty from various cyber threats and civil-military cooperation as the main force in dealing with threats.

The challenge in the future, civil-military cooperation will be more complex, because technological advances are increasingly sophisticated and dynamic. The military as the subject of national defense will always face various dynamics of cyber threats. Therefore, development in the regulatory aspect needs to be structured in such a way, so that access by other parties can be controlled. Military mastery and skills in the aspects of information and communication technology need to be developed, so that they have the ability to protect their own infrastructure, are able to carry out reconnaissance and observation of opposing party's data or information as well as being able to manipulate data or information (cyber defense and cyberattack capabilities). (Khalimatus, Diyah, and Tri Vinata 2016)

For civilians, the effort to deal with cyber threats is to support the military in defending state sovereignty and participating in various threats. The form of civil cooperation is to support everything related to the state, especially for the military. With the involvement of civilians as state objects, civil-military cooperation can be said to have worked and can face various cyber threats in the current era.

III. CONCLUSION

Civil-military cooperation in dealing with various non-military threats, especially cyber threats, is a strategic step in the era of technology and information development. Various cybercrimes have been committed in Indonesia in various ways. Civil-military cooperation is more about where the role of the military as the subject of state defense uses its power in dealing with threats. Cyber defense can be said as a step to defend the country from cyber threats. Civilians represented by government institutions certainly support the existence of cyber defense. Thus, cyber threats in Indonesia can be minimized and can be faced together.

REFERENCES

[1] Antar, Pengetahuan, and Pustakawan Supriyadi. 2016. "Community Of Practitioners: Solusi Alternatif Berbagi." Lentera Pustaka 2(2): 83–93.

[2] Effendy, Muhadjir. (2008). Profesionalisme Militer: Profesionalisasi TNI. Malang: UMM Press

[3] Khalimatus, Nur, Sa ' Diyah, and Ria Tri Vinata. 2016. Rekonstruksi Pembentukan National Cyber Defense Sebagai Upaya Mempertahankan Kedaulatan Negara. http://nasional.kompas.com/.

[4] Permanasari, Arlina. 2018. Terorisme Siber, Perang Siber & Hukum Humaniter: Tantangan Bagi Kerangka Hukum Indonesia Tentang Pertahanan Siber.

[5] Purwanto, Adi Joko. 2010. Peningkatan Anggaran Militer Cina Dan Implikasinya Terhadap Keamanan Di Asia Timur. https://www.researchgate.net/publication/321239577.

[6] Satrio, Giri, I Wayan Midhio, and Deni Dar. 2018. Strategi Kerjasama Sipil Dan Militer Bidang Pembangunan Infrastruktur Daerah Dalam Rangka Memperkuat Pertahanan Negara (Studi Di Provinsi Jawa Barat).

[7] Setiyawan, Anang. Penguatan Kerjasama Cyber Defense Asean Guna Menghadapi Ancaman Cyberwar.

[8] Sjafrie S. 2015. Kerjasama Sipil Dan Militer. www.dmc.kemhan.go.id.

[9] Subagyo, Agus. 2015. 5 Sinergi Dalam Menghadapi Ancaman Cyber Warfare Synergy In Facing Of Cyber Warfare Threat.

[10] Sutisna, Sobar et al. 2018. Kerjasama Sipil-Militer Dalam Tanggap Darurat Kebakaran Hutan Dan Lahan Di Provinsi Riau Tahun 2014. http://www.dw.com/id/indonesia-.

[11] Widiyanto, Andika, and M Dian Hikmawan. 2019. "Implementasi Rencana Aksi Nasional Bela Negara Berdasarkan Instruksi Presiden Nomor 7 Tahun 2018 Oleh Dewan Ketahanan Nasional Republik Indonesia." JSPG: Journal of Social Politics and Governance 1(2).

[12] Undang-Undang Nomor 3 Tahun 2002 Tentang Pertahanan Negara

[13] https://katadata.co.id/sortatobing/indepth/619750dd61e6a/pertahanan-siber-indonesia-jadi-tugas-penting-panglima-tni-baru

[14] https://www.kemhan.go.id/2015/06/05/sinergi-sipil-militer-dapat-tercapai-dengan-pemahaman-yang-jelas-tentang-peran-masing-masing.html