Journal of Social and Political Sciences

Sumarno, Tonny, and Risman, Helda. (2020), The Universal War Strategy in the 5th Generation War in the 4.0 Industry Era (Cyber Threat Case Study). In: *Journal of Social and Political Sciences*, Vol.3, No.4, 1111-1119.

ISSN 2615-3718

DOI: 10.31014/aior.1991.03.04.242

The online version of this article can be found at:
https://www.asianinstituteofresearch.org/

Published by:
The Asian Institute of Research

The Asian Institute of Research *Social and Political Sciences* is a peer-reviewed International Journal. The journal covers scholarly articles in the fields of Social and Political Sciences, which include, but not limited to, Anthropology, Government Studies, Political Sciences, Sociology, International Relations, Public Administration, History, Philosophy, Arts, Education, Linguistics, and Cultural Studies. As the journal is Open Access, it ensures high visibility and the increase of citations for all research articles published. The *Journal of Social and Political Sciences* aims to facilitate scholarly work on recent theoretical and practical aspects of Social and Political Sciences.

ASIAN INSTITUTE OF RESEARCH
Connecting Scholars Worldwide

The Asian Institute of Research
Journal of Social and Political Sciences
Vol.3, No.4, 2020: 1111-1119
ISSN 2615-3718

DOI: 10.31014/aior.1991.03.04.242

The Universal War Strategy in the 5th Generation War in the 4.0 Industry Era (Cyber Threat Case Study)

Tonny Sumarno[1], Helda Risman[2]

[1] Student of Indonesia Defence University. Sentul, Bogor, Indonesia. Email: tonnysumarsono@gmail.com
[2] Lecturer of Indonesia Defense University, Sentul, Bogor, Indonesia. Email: rismancan@gmail.com

Abstract
Currently, the world has entered into the 5th generation war, and this war in the 5th generation can be said to be an invisible war. This war can be interpreted as an information war, an economic war, including cyber warfare. The rapid progress of the development of science and technology today has a very broad impact on various aspects of human life. The threat of cyber attacks that can cripple the stability of national security needs to be watched out for. For this reason, the Indonesian nation must have strategic steps to anticipate all possibilities from the threat of cyber attacks. The research objective in this paper is to identify the potential threat of 5th generation war, analyze cyber threats and cyber attacks in Indonesia and how the Universal War Strategy in dealing with the threat of cyber attacks. This research method uses a qualitative descriptive phenomenology research method, using data sources from some literature and mass media. The research results from the researcher's analysis provide significant results with the conclusion that Indonesia is vulnerable to cyber threats so that it is necessary to equalize perceptions in drafting the concept of defense and security from the threat of cyber attacks.

Keywords: 5th Generation War, Siber Threats, Universal War Strategy

1. INTRODUCTION

War, according to Great Dictionary of the Indonesian Language (KBBI) is the enmity between two countries, which then mobilizes their soldiers to fight using weapons (Kemdikbud, 2019) but war also has a different meaning, so that in essence war can be interpreted as any form of a country's efforts. in exerting all his ability to achieve his goals without relying on military strength alone. The universality of this war is then realized through the mobilization of all national strength and resources to face threats from within and from abroad (Prabowo, 2019). At present, the world has entered into a fifth generation war and this type of war is an invisible war. It can also be said as information warfare, propaganda, economic war including cyber war (Aldinar, 2019). Ex Vice President of the Republic of Indonesia, Try Sutrisno, reminded the Indonesian people that the current threat of war is no longer tangible, the security spectrum is very complicated, and the power base of this war lies in its technological strength. but it has a wider destructive force than physical war, and has an impact on ideological, political, economic, cultural and even defense and security aspects (Taher.A. Pratama, 2019)

Entering the industrial revolution 4.0 era, the development of Information and Communication Technology (ICT) is growing rapidly. The term industry 4.0 was officially born in Germany, in 2011, when the "Hannover Fair" was held. Germany has a development plan policy known as the High Tech Strategy 2020, which aims to keep Germany at the forefront of the manufacturing world, followed by several other countries in realizing the concept of industry 4.0 so that the development of digital technology in various fields develops rapidly (Prasetyo. H, Sutopo. W, 2017). At present, the use of Information and Communication Technology (ICT) has been widely abused by individuals who are not responsible for achieving its goals, but have a broad impact on the life of society, the nation and the country, for example is the misuse of Information and Communication Technology (ICT) to attack government public service sites, use of social medi in the dissemination of radical content and attack the Pancasila ideology.

Based on this phenomenon, researchers are interested in analyzing more deeply, what are the potential threats to this fifth generation war? What types of cyber threats and attacks have attacked Indonesia? and how to implement a universal war strategy in minimizing these cyber attacks? For this reason, the researcher formulated the problem formulation "What is the Universal War Strategy in the Fifth Generation War in the Industrial 4.0 Era" in the Perspective of Cyber Attack Threats?

2. RESEARCH METHODOLOGY

The research methodology used by researchers in analyzing this problem uses descriptive qualitative analysis methodology that emphasizes data collection and analysis of data presentation and facts based on literature study research methods from secondary data with a case study model. A case study model is one type of qualitative research, where researchers conduct in-depth exploration of programs, events, processes, activities, one or more people, researchers collect detailed data using various data collection procedures and in continuo.

3. RESULT AND DISCUSSION

The History in war has recorded that the period of generations of war has started since the first time the world war occurred, precisely since the first world war in 1648-1860. This war in the first generation has formal, orderly, neat and highly upholding knightly values. an example is the Napoleonic wars, when the French expanded into mainland Europe. Then the second generation war (1860-1918). In the 19th century, gunpowder and war machines were discovered, and the war in this second generation emphasized the firepower of the cannon, this method was developed by France in the first world war, the characteristic of the second world war was "The artillery conquers, the cavalry as the attackers and the infantry occupies "the motto that developed in this second generation war is" close and destroy ". Then entering the third generation war period, the characteristics of the third generation war are prioritizing the speed, spontaneity and mental and physical strength of the soldiers, (Rudi, 2011) After a decade, the war that continues is Cold War or intelligence war and espionage, because even though World peace agreements have been signed, but economically and technologically more developed countries are still developing their weapons technology for conventional warfare. Entering the fourth generation of war, there has been a radical change in the norms of war as agreed in the "Westphalia" agreement, namely a return to the culture of past war, namely those involved in conflict are not only state (state actors), but non-state actors as well. involved, using all means to achieve its goals, then in this fourth generation war the term asymmetric warfare appeared, which has been known since the Franco Spanish war in 1823. This asymmetric war has the characteristic of increasingly blurred boundaries of war norms, as agreed. in the Westphalia agreement. The characteristics of this war are transnational, do not know the battlefield and do not differentiate between civilians and military, do not recognize wartime and front lines. examples of this asymmetric war include: the civil war in Syria, the Somali war and the griliary war (Irvan, 2017). How will the next generation of war develop? TNI Commander Marshal TNI Hadi Tjahjanto, SIP said that the current war has entered the fifth generation war, namely cyber war, however conventional war cannot be abandoned (Adminfakta, 2019), the characteristic of this fifth generation war is invisible war, not know the battlefield, there is no physical contact (cyber space), and have a destructive power that is wider than physical war, which has an impact on ideology, politics, economy, socio-culture and even defense and security.

3.1 Potential Threats in the 5th Generation War

The rapidity of science, technology, informatics, mass media, democracy and human rights colors the relationship between countries and their various national interests. This reality in the end has implications for relations between countries in the regional or global scope in the bonds of friendship (amity) but also creates an atmosphere of enmity. Interdependence, security complexity, and rivalry are inevitable. The dynamics of this strategic environment unwittingly give birth to war in a new nature and form. This contemporary war has a very broad battlefield with interconnective and interimplicative aspects with abstract limitations, does not use conventional force, does not declare war, does not cause casualties, but it can paralyze a country (Helda Risman, 2018). Talking about war, of course, is closely related to the word defense and defense itself has a very broad meaning, according to Makmur Supriyanto, defense is the study of how to manage national resources and strength in times of peace, war and after war, in order to face threats from outside and from within the country, both in the form of military threats and non-military threats to territorial integrity, state sovereignty, and the safety of the entire nation in the context of realizing national security (2014, Sept). Then, what kind of threat has the potential to threaten Indonesia in this fifth generation war?

Threat, according to the Indonesian Dictionary (KBBI), is an intention or plan to do something that is detrimental, difficult, troublesome or harms another party. In the context of defense. threats can also be interpreted as efforts carried out through actions or crimes that are thought to endanger the state's order and interests (Kemdikbud, 2020). The dynamics of the development of the strategic environment today have signaled the evolution and transformation of potential strategic threats to state sovereignty and will develop in a multidimensional nature, while in terms of advances in science and technology, it will also influence the form and pattern of war in the future. Although the patterns and forms of irregular warfare, in an asymmetrical form still occur in some areas, conventional warfare technology continues to follow suit. Future wars will consider reducing the impact of damage and casualties among civilians, by applying high-accuracy weapon technology and applying robotic technology to its various weapon systems. The development of this technology will create a network-based war that relies on the advantages of information, as well as being able to carry out warfare in the digital or cyber space. The impact of this war will certainly worry about the world security situation, one of which is cyber crime that knows no boundaries, including biotechnology engineering or nano technology which is very difficult to detect, this technology will also develop in the world of aviation, the manufacture of nuclear weapons, bullets. control and unmanned flying vehicles and even satellites will also be used for national defense. From the aspect of national defense, cyber space will be the fifth domain of the battlefield, in addition to land, sea, air and space battlefields (Indonesian Defense White Paper, 2015).

Security according to Barry Buzan, in his book entitled "A New Pattern of Global Security in the Twenty-First Century" states that security is an effort to pursue freedom from threats and the ability of states and communities to maintain their independent identity and their functional integrity against the forces of change. (Buzan, 1991) Entering the 21st century, the development of Information and Communication Technology has created a variety of changes that are so rapid, the impact of the dynamics of change itself ultimately creates uncertainty, and when viewed from the characteristics of war in this fifth generation, the most potential threat. dominant is the threat of cyber war.

3.2 Threats and Cyber Attacks in Indonesia.

The threat of cyber attack is part of the form of asymmetric warfare (Irregular Warfare). The purpose of which is to destroy the legitimacy and credibility of the enemy and isolate the enemy from the population and external supporters both physically and psychologically, and seek to increase his own legitimacy and credibility in using authority over the same population, so asymmetric warfare is part of irregular warfare, and cyber warfare is part of asymmetric warfare (Anwar, 2020) So in general, the sources of threats that can be identified as potential sources of cyber threats are: Internal and external sources, those involved in intelligence activities, someone / group's disappointment with a policy, those who carry out investigative activities, extremist organizations.

activities of hacktivists, organized crime groups, the existence of competition, enmity and conflict, and the consequences of technology abuse (Kemhan, 2018 Aug).

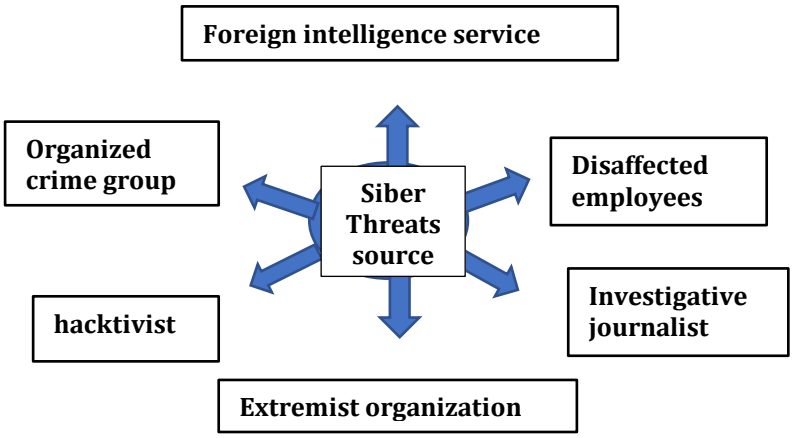

Figure 1: Source of Threats

Today, the understanding of national values has experienced a lot of degradation and shifting due to the presence of cyber space which provides very free access to information. Therefore, an understanding of the values of Pancasila as the ideology of the Indonesian nation must continue to be nurtured in the life of the Indonesian people in order to fortify themselves from negative influences due to the rapid development of technology (Arianto et al., 2020, Agust). Head of the National Cyber and Crypto Agency, Hinsa Siburian stated "Pancasila is the power center of the Indonesian nation", so the fifth generation war will attempt to penetrate the power center of the Indonesian nation (Aldinar, 2019). Sun Tzu, in his book "The Art of War" says that "Reaching 100 victories in 100 battles is not the pinnacle of skill, but conquering enemies without fighting is the highest perfection" (Marsono, 2020). Judging from the characteristics of the fifth generation war and its impact, cyber war is the pinnacle of skill in strategy. So that it can be said that any country that controls cyber technology will easily dominate other countries without having to fight. The forms of cyber threats that often occur today are: advanced persistent threats (APT) attacks, defacement attacks, phishing attacks, malware attacks, cyber intrusion, spam, and abuse of communication protocols (Putra, 2018 Agust). Meanwhile, the trend of threats that will continue to increase is the threat of cyber crime, which covers the banking sector, government agencies, military and police. This cyber crime attacks various websites, blogs, e-mails, social media and various online software based on computers and the internet.

Since 1988, the Indonesian nation has fought cyber wars with other countries several times. This is related to the political and social problems that occur, for example when racial riots occur, Indonesia is fighting in cyber space with hackers from China and Taiwan. In 1999 there were also riots in cyber space between Indonesia and Portugal regarding the East Timor case. Even when there was a "war" with Portugal, attacks occurred to each other to enter the system and be able to delete all data. In addition, on August 6, 2010, Symantek (anti-virus producer Northon) announced that Indonesia was second only to Iran among the 10 countries that experienced the Stuxnet worm attack. Stuxnet is a worm that attacks computers based on windows operations. On November 20 and 23, 2010 the Iranian military officially declared that the Stuxnet worm attacked the Natanz (Iraqi Nuclear Facility), this worm even managed to remote a dangerous explosion in the uranium enrichment center of the nuclear developing country. Israel and the United States are suspected of being the main opponents of Iran's nuclear program. In recent years there has also been a cyber war between Indonesia and Malaysia. The mutual infiltration between hackers of the two countries colored the feud. This action usually occurs when political conflicts or competition between the two countries arise. Even though they did not involve the governments of the two countries, these hackers attacked cyber facilities belonging to the Malaysian and Indonesian governments.

Based on data from the Association of Indonesian Internet Service Users (APJII) in 2017, internet users in Indonesia were estimated to be 143.26 million people, and in the same year, the cyber organization Indonesia Security Inciden Response Team on internet infrastructure (ID-SIRTII) recorded that cyber attacks in 2017 reached 205,502,159, and is expected to continue to increase every year. Of the number of attacks, it was noted that government websites were the highest targets. The government sector is also not spared from cyber crime attacks, this is because the government web sites open full access to all users in the hope that the public will get maximum access, Based on data from the government-owned Go.id Domain incident response statistics from the Director-General of APTIKA In 2016, there was an increase in web attack defenses from 42% to 95%, this shows that almost the entire web was affected by cyber attacks.

Table 1: Insiden respon Domain.Go.Id

INSIDEN	PROSENTASE			
	Triwulan 1	Triwulan 2	Triwulan 3	Triwulan 4
Web Defacement	42.00	66.80	75.00	95.00
Malware	35.00	14.50	2.00	0.00
Phising	17.00	8.90	1.00	1.00
Spam	5.00	9.40	17.00	1.00
Ddos	1.00	0.00	0.00	0.00
Brute Force	1.00	0.00	0.00	0.00
IPR	1.00	0.00	0.00	0.00
Bug	0.00	0.00	4.00	3.00
Data Leaked	0.00	0.00	1.00	0.00

Source: Ditjen APTIKA, Kemenkominfo R.I 2016

This condition needs serious attention, because cyber attacks have attacked all aspects of people's lives, and disrupt the sites of public service facilities and government. The risks faced in dealing with the threat of cyber attack are almost as great as conventional warfare. The use of cyber technology has a very broad impact. The various conditions above illustrate that the impact of cyber threats and attacks on the country being attacked is very large, because it has the potential to threaten the sovereignty and defense of a country (Kemhan, 2018).

3.3 Universal War Strategy in the face of cyber threats and attacks

In the national defense doctrine, it is explained that, the Universal People's War is essentially a total war for all Indonesian people by mobilizing all national strength and resources to uphold state sovereignty, territorial integrity, and national safety from other nations that threaten or occupy the territory of the Republic of Indonesia. The People's War of the Universe is populist, universal and territorial. (Prabowo, 2019 Nov) In other words, that Indonesia's national defense strategy adheres to the Universal War Strategy, a strategy implemented by empowering all national capabilities and assets in maintaining the integrity and sovereignty of the country. Strategy is the art of how to win a war, by using the infrastructure that is owned to achieve goals. In his theory, Carl Von Clausewitz also argued that strategy is the art of using battle to win a war. How is the implementation of the Universal War Strategy in minimizing the impact it causes? viewed from a cyber warfare perspective.

Cyber security and cyber defense are closely related, namely that they are implemented to maintain and maintain confidentiality, integrity and availability of electronic information. Some of the obstacles in building cyber security include: weak understanding of state administrators with the cyber world, cyber crime patterns are developing rapidly, national cyber security governance has not accommodated various problems, low awareness of cyber attacks, weak domestic industry in producing and developing equipment information and communication technology hardware, cyber crime handling is still partial. Currently, the use of Information and Communication Technology (ICT) has entered all aspects of life in the world community. Utilization of

Information and Communication Technology encourages the formation of a community that is connected electronically in a space called cyber space.

The system including the internet network is currently being used to support various activities in various sectors of business, trade, health services, communications and governance as well as the defense sector. The wider and increasing use of Information and Communication Technology, especially through the internet network, is followed by an increase in threat activity. These threats include attempts to break into the confidentiality of information, destroy electronic systems, recruit ISIS members, spread radicalism and various other illegal acts. By paying attention to the above phenomena, cyber space needs to get proper protection in order to avoid potential threats that can harm individuals, organizations and even the state. More special attention is prioritized to the defense sector, security sector and various other public service facilities. Disruptions to the systems contained in strategic and critical infrastructure can cause economic losses, decrease the level of public trust in the government and disrupt public order. This risk is a consideration for the need for cyber defense.

Cyber defense is an effort to tackle cyber attacks that cause disruption to the implementation of national defense. Cyber defense is implemented in stages starting from the scope of individuals, working groups, organizations to the national scale. In Republic of Indonesia Law Number 3 of 2002 concerning national defense, it is stated that state defense aims to safeguard and protect the sovereignty of the state, the territorial integrity of the Unitary State of the Republic of Indonesia and the safety of the entire nation from all forms of threats, both military and non-military threats. From the data and facts mentioned in the above discussion, the strategic step to implement the Universal War Strategy from the perspective of the threat of cyber war is to prepare supporting infrastructure (means) and prepare steps to implement the strategy (Ways).

3.3.1 Preparing Facilities and Infrastructure (Means)

The steps in preparing these facilities and infrastructure begin with the development of the superstructure and infrastructure aspects that can support the implementation of the Universal War Strategy from the perspective of the threat of cyber war.

3.3.1.1 Superstructure Aspect Development

This superstructure development is related to the Indonesian nation's paradigm of understanding cyber defense which has not yet been embedded in the minds of the general public. The government and all components of the nation must begin to transform, the awareness of the understanding of defense that was previously conventional in nature is transformed into cyber defense, which is a new definition of future defense. The threat to Indonesia's territorial sovereignty includes not only the visible dimensions, namely: land, sea, air and space, but also the invisible dimension (cyberspace), because within certain limits, the visible regional sovereignty can be attacked. through sophisticated Information and Communication Technology devices, it is even able to control its operations remotely, such as: electricity, telecommunications, financial or banking systems, and even weapons systems. In addition, in the future, the meaning of sovereignty will be transformed into sovereignty in cyberspace. The transformation agenda on cyber awareness should be carried out by providing education and training to the relevant state apparatus, both policy makers, government, security and defense apparatus at all levels, and the transformation of awareness of cyber security must also have begun to be given to the younger generation through the education system. especially education in the military, defense, security and education in general. The target is the birth of an Indonesian generation with high awareness and sensitivity to cybersecurity.

3.3.1.2 Infrastructure development

Superstructure development must be balanced with adequate infrastructure development. Cyber world requires the availability of sophisticated Information and Communication Technology devices, internet network systems are very important in supporting hacking performance. It is very difficult for a cyber expert to optimize his abilities if it is not supported by a maximum internet network. When compared to other Southeast Asian

countries, such as Singapore, the Philippines, Vietnam, Malaysia and Thailand, the position of the Indonesian state is still far below it. Indonesia's internet access speed is ranked 118, namely 1.5 Mbps. The development of infrastructure assets is not only about increasing internet access, but also the construction of a Cyber Command Center, procurement of sophisticated defense equipment including the construction of servers in the country. Building a cyber security and defense system in the framework of safe guarding the sovereignty of the State cannot be done in a short time, for that it requires stages to make it happen.

3.3.2 Preparing Ways to Implement the Strategy (Ways)

With the fulfillment of the facilities and infrastructure in support of implementing the Universal War Strategy to deal with the threat of cyber war, the next steps that need to be prepared are:

3.3.2.1 Implement Cyber Threat Prevention Measures.

According to Albert W. Steve, to minimize cyber crimes can be done in (3) three ways, namely: prevention, detection and investigation. Cyber crime prevention efforts are an important step because the system must be built with control, both physical and logical access. Physical access control audits are carried out by evaluating the security of physical access to data center locations and alarm systems for unauthorized access to other physical security to hardware, while logical access control can be carried out by evaluating the suitability of passwords with assignment of responsibilities (job description).

3.3.2.2 Implement Network System Security.

Users must be aware that the existing network system needs attention and security, in order to prevent damage to the inside of the system because it is accessed by irresponsible people. System security development must be integrated in the entire system and its sub-systems. With the aim of being able to narrow or close the gaps in access to use by perpetrators. Meanwhile, individual security is carried out using professional anti-virus on personal assets.

3.3.2.3 Establish a Cyber Threat Management Agency.

The Indonesian government initially through the Ministry of Communication and Information of the Republic of Indonesia has formed the IDCERT (Indonesia Computer Emergency Response Team) which then according to the decision of the President of the Republic of Indonesia in collaboration with the National Crypto Agency (BSSN) carries out duties and functions including maintaining and securing information systems and telecommunications networks owned by the government and the public from crime. cyber, including threats and threats of cyber attacks, in addition the National Police institution has also formed a cyber crime unit that carries out its duties and functions to take action against the perpetrators of cyber crimes. Meanwhile, other government agencies that already have cybersecurity handling work units include: Ministry of Defense, Ministry of Foreign Affairs, Ministry of Industry and Trade, Ministry of Education and Culture, Ministry of Research and Higher Education, State Intelligence Agency, National Counterterrorism Agency, Cyber Crypto Agency. State, IPPS, TNI and the National Defense Council.However, given the very rapid development of Information and Communication Technology (ICT) advances, Indonesia needs to make policies that regulate various elements related to cybersecurity in terms of securing internet network systems. According to Lukman Yudho Prakoso's theory on the theory of defense policy implementation, defense policy is closely to Integrative, Interactive, Transparency, Controling and Accountability (IITCA) where in the preparation of defense policy it is necessary to adhere to the principles, namely: Integration of existing national resources (Integrative), there is interactive communication between related entities (interactive), commitment in formulating a transparency system to avoid leakage (Transparency), an entity as a driver force is needed to avoid abuse of authority (Controling), a special system to measure performance accountability that has been implemented (Accountability) (LYP, 2016).

3.3.2.4 Issue a Cyber Crime Act.

In handling cybercrime, legal regulations on cyber crime are required (special regulations for handling crimes in the cyber / internet sector: (Cyber Law). So far, the legal basis for cyber crime in Indonesia uses the Criminal Code (article 362) and legal threats are categorized as minor crimes, while the impact is it can have very fatal consequences. This Law continues to make changes according to the development of Information and Communication Technology (ICT). The Draft Law on Amendments to the ITE Law has been passed into Law Number 19 of 2016 concerning amendments to the Law The ITE Law. The law contains 7 important points that revise the ITE Law, through this new law the government has the authority to cut off access and or order electronic system administrators to cut off access to electronic information that is indicated to have violated the law. provide certainty h law for the public, so that people can be smarter and more ethical in using the internet, so that racial content, radicalism and pornography can be minimized. With the amendment to the new ITE Law relating to cyber crime, it strengthens the role of the government in providing protection from all kinds of disturbances caused by misuse of information and electronic transactions (providing a solid foundation for the government to prevent the spread of negative content on the internet)

3.3.2.5 Organizing the State Defense Program.

In order to revive the sense of nationalism and love for the homeland of the younger generation, organizing a state defense program is one form of implementation of the Universal War Strategy. With the passing of Law Number 23 of 2019 concerning "National Resource Management" by the President of the Republic of Indonesia on October 24, 2019, it can be used as a legal basis for how to implement state defense programs at the Central Government or in the regions. How the technical implementation in the field starting from recruitment, training, rights and obligations as supporting and reserve components is stipulated in Law Number 23. The low level of nationalism and the vulnerability of the influence of foreign ideologies on the younger generation can be minimized by organizing state defense programs from the Central Government to the regions by involving relevant officials and the local Regional Government.

The achievement of superstructure and infrastructure development in designing cyber security and defense systems is followed by stages in efforts to prevent cyber crime and involve all components of the nation, so the goal (Ends) of implementing the universal war strategy in the implementation of cyber war can be achieved.

4. Conclusion

The rapid development of Information and Communication Technology (ICT) in the industrial 4.0 era shows that the dominant potential threat in this fifth generation war is the threat of cyber attacks. The free openness of internet access in Indonesia is one of the opportunities for cybercrime in cyberspace, based on research data and facts, cybercrimes that the government needs to be aware of are the spread of radicalism, attacks on Pancasila ideology and government public service websites. Efforts to prevent and minimize the impact of cyber threats and attacks in Indonesia are carried out by implementing the Universal War Strategy by involving all components of the nation, both government and society. Through socialization and state defense programs from the center to the regions in order to block the movement of cyber criminals, the Universal War Strategy can be applied to support cyber warfare in Indonesia.

References

LYP (2016), "Performance Accountability for Procurement of Goods and Services at the Surabaya Navy Academy", (Desertation). Pp. 170-172

Kemhan (2018). "Strategic Considerations for Cyber Defense in the framework of State Defense ”Dirjenstrahan, p.63

Kemhan (2015) "Indonesian Defense White Paper", Strategic Environment Development. P. 14

Prabowo, J.S (2019) Thought Principles on the Universal War (third edition), Central Jakarta: Center for National Studies and Strategy, p. 43
Sugiono (2013) Management Research Methodology, Qualitative Methodology (1st printing), p. 39, AlfaBeta Bandung
Supriyanto. M (2019) About Defense Science (first edition) Jakarta: Yayasan Pustaka Obor Indonesia, p. 28
Marsono (2020), "Strategy Theory from Various Experts", Defense University Press (printing 1), p. 25
Arianto et al (2020) "The Role of the ITE Law and Cyber Society Ethics" Journal of Defense & State Defense. Vol.10 Number 2
Putra et al (2018), "Cyber Threats in the Perspective of National Defense," Vol 4, No.2
Prasetyo.H & Sutopo.W (2017). Journal of Industrial Engineering, Vol. 13, No.1, Industri 4.0 Study of the Classification of Aspects and Direction of Research Development. Undip Surakarta. p.3
Aldinar (2019). The world enters the fifth generation war. https: //www.dara.co.id/world-enters-war-fifth-generation.html
Adminfakta(2019)5th generation war era, TNI Commander Hopes Soldiers will not fail to understand.Https://faktapers.id/2019/08/era-perang-generasi-ke-5-panglima-tni-hope-soldiers-not -failed /
Anwar (2020). PPT, “Mk. War Theory and Strategy” in Irregular Warfare., Pp. 10-11
Buzan (1991) “A New Pattern of Global Security in the Twenty-First Century” International Relations,67.3 (1991), pp. 432-433.
Helda.Risman(2018),“WarTransformation:“*UniversalWarinaTimeofPeace*” https://www.academia.edu/36382829/transformasi_perang_perang_semesta_di_masa_damai
Irvan (2017) Understanding the fourthgeneration war http://politik.rmol.co/read/2017/05/25/292654/Membentuk-Perang-Generasi- Fourth
The Great Dictionary of The Indonesian Language, "online version 2.8 dictionary". in http // kbbi.web.id / war,
The Great Indonesian Dictionary of Indonesian Language (2020,) "Dictionary online version / online version 3.4", in https://kbbi.kemdikbud.go.id/entri/ancaman
Rudi (2011).A brief history of World War II. https: // rudy- primadi.blogspot.com/2011/04/sejarah-sendek- war-dunia-II_21.html
Taher.A.Pratama (2019) Tri Sutrisno Warns about the dangers of cyberwar to this. https://tirto.id/try-sutrisno-perwarn-bahaya-siber-war-kepada-tni-edVV