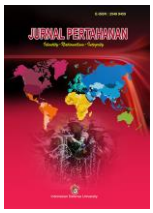
Jurnal Pertahanan

Media Informasi tentang Kajian dan Strategi Pertahanan
yang Mengedepankan *Identity*, *Nationalism* dan *Integrity*
e-ISSN: 2549-9459
http://jurnal.idu.ac.id/index.php/DefenseJournal



STATE ACTION AS AN INDIVIDUAL SECURITY THREAT IN CASE OF CYBERCRIME SECURITIZATION

Miftah Farid Darussalam
Universitas Islam Negeri Alauddin Makassar
Makassar, Sulawesi Selatan, Indonesia
darussalam.farid@gmail.com

Ajeng Ayu Adhisty
Universitas Gadjah Mada Yogyakarta
Sleman, Yogyakarta, Indonesia
ajengayu.adhisty@gmail.com

Article Info

Article history:
Received 23 September 2019
Revised 27 November 2019
Accepted 27 November 2019

Keywords:
Cybercrime,
State Security,
Human Security,
Securitization

Abstract

In the current security concept, there are some changes to the current security object. This is due to the increasingly broad understanding of security objects. This study examines the emergence of cyber issues as a new threat to state security. Cyber actions in the virtual world are developing along with the rapid technology development. Moreover, the state policy on cyber issues is considered as a new threat to individual security. The development of that state security issue is being debated among the theoreticians of international security studies. The concept of securitization explains the phenomenon of cyber issues and receives the attention of many states. Securitization carried out by the United States on Cybercrime issues becomes the initial trigger in viewing cyber actions as a new threat to state security. The object of this paper is more focused on State policy in dealing with cyber threats. Afterward, state policy in facing the cyber threat is seen from the perspective of human security from UNDP. Therefore, there is a debate about the desired security object. State actions to reach state security are then considered as individual privacy security. So, international security now does not only focus on state objects but also on individual, environment, economy, and identity. Thus, every action taken in securing an object does not pose a threat to other security objects.

DOI:
http://dx.doi.org/10.33172/jp.v5i3.589

INTRODUCTION

The international relations phenomenon runs into very advanced development. The development of the International Relations phenomenon provides a challenge for theoreticians and policymakers in adjusting their theories and policies in response to new phenomena. The development of the existing theories in the International Relations study is considered no longer relevant to handle the phenomenon nowadays. The example of developing phenomenon at this time is about International Security. International Security is a complex issue in International Relations. The development of International Security gives criticism for theoreticians to update the existing theories. Issues of International Security has evolved and away from conventional threat issues. According to conventional International Security threats, war is the only international security threat. But, at this time, there is another threat issue besides war, such as environment, economy, and technology issues. It is influenced by the change of the International Security definition. Besides that, the change of the International Security definition runs into shift change objects and the subject of international threats.

Actor and international security developed after the end of the cold war. The shift due to the emergence of many actors who gives a dangerous threat to the State. The actor can be groups or individuals. One of the factors that encouraged the emergence of threats is current technological developments. Current technology developments are able to re-form the strategy and the purpose of International Security Studies (ISS). The new focus formation from ISS caused by the emergence of many actors and a new issue that has become an international threat. Technology developments have an impact on one State weapons and military forces developments to threat another State (Buzan & Hansen, 2009). When a State military using high technology as a defense, the other state will improve that technology as an instrument to anticipating high-tech weapon attacks from the other state. Especially, in developed State that has high technology to create a weapon that produces extensive and large damage. We can see the examples of weapons development from nuclear weapons and drones technology that used to anticipate terrorists in several States today.

At first, the main focus of ISS is having the basic assumption that the big threat caused by a large number of actors too (Buzan & Hansen, 2009). Therefore, when an action endangers the international world, then the actor who gives that threat is also the actor in international scope. However, it is denied through technology development because of the emergence of individual actors who are able to give the threats that have a big impact. This is supported by technology advances that have no clear boundaries in accessing information and giving a threat to the State. The threat that comes from the virtual world can give physical, economic and political impacts (Buzan & Hansen, 2009). Accordingly, when technology developments become a medium to produce the threats, then ISS has to change and shift the strategy and the main focus becomes large. Because actors in cybercrime threats are the abstract actors and difficult to determine.

Technology developments in this era provide obstacles and support for the lives of people in this world. The obstacle experienced by society and State is the issue of security threat which is easier to do through virtual media. It makes crime and threats will be more flexible in staking out the target. The scope in cybercrime is very large and difficult to control, so that, the development of crime through cybercrime also provides a challenge for the state and individuals in dealing with these cyber-actions. Meanwhile, society and the State also get easiness through the development of these technologies. The

influence of technology development gives the easiness to society in achieving very large information and cross-State communication that can be done in an efficient time. From the explanation above, the author wants to explain the issue of international security threats that will become a dilemma between the needs and also the threats to society. The focus in this paper is the object and subject of international security threats on the individuals which are part of the State. The research questions are how does cybercrime become an international security threat today? How can state security become a threat to individual security?

Securitization is the process of an issue that was not a threat before, then becomes a threat issue that must be considered because it can be threatened. Security is a condition that is built in the mind of each individual. In the build-up, the understanding of the meaning of security, need actions that can convince the individual about the threats that will be faced. This securitization process can be described in the speech act (Buzan & Hansen, 2007). Speech is the act of talking about a phenomenon that is starting to be widely discussed when an influential actor participates in discussing the phenomenon, the construction of ideas from the phenomenon has begun to build. Then, when the words about the phenomenon are carried out with an action on the phenomenon, the process of securitization of the phenomenon has been established. A phenomenon can be considered a threat when it has been securitized by the speech act. The process of securitizing a phenomenon is an action to build individual awareness about threats that were not a threat before. Therefore, this securitization process needs an idea and influential actors in the community to convince the phenomenon. In addition, the actions that have been taken by influential actors also become the base for securitizing a phenomenon (Buzan & Hansen, 2007).

The development of International threat issues about cyber gives the theoreticians and State policymakers attention. The skeptical people questioned about the threats caused by the cyber revolution. According to them, threats from cyber actions are not included as international security threats, it is because the impact is not directly and cannot be measured. When a threat does not have a direct impact on the object, the policy in handling the threat will be difficult to realize. Therefore, according to skeptical people, the scope and subjects of cyber threats are very difficult to explain and categorize as international threats (Kello, 2013). Canadian Police College has a definition of understanding the phenomena of cybercrime. In 2009-10 Report and Plans, Public Safety and Emergency Preparedness Canada give an explanation that one of the current threats focuses is the cyber world or virtual world. So, cybercrime is something that will threaten the security of the state. The threats can give an impact on politics, economy, and infrastructure that run by the state through the technology. In addition, technology development becomes an opportunity for cybercrime actors to expand the network and the impact of threats that they are made. Terrorism is one of them, this terrorist organization is able to expand with a very large technology development at this time. Access any information which is owned in a different state and share the information extensively without the real boundaries and obstacles (D.Valiquet, 2011).

There are several parts to understand those cyber actions. Some of those sectors are (Kello, 2013) cyberspace, cybersecurity, malware, and cybercrime. Cyberspace is the scope or the mobile space of some of those cyber actions. Cyberspace can also be interpreted as the concept of cyber action in controlling weaponry through the virtual world.

Cybersecurity is a concept of action to protect computer systems and data integrity from criminal acts through cyberspace. Cybersecurity is also commonly interpreted as an act of a government in protecting every state asset it has. Malware (malicious software) is a term used to describe various forms of software or programs that are hostile, disrupting code (Storlie et al., 2014). Cybercrime is a concept that is used for criminal actions. Such as terrorism, pornography, and increasing weapons of mass destruction. Cyberattack is a concept with actions to attack a group. This is commonly used with the economic and political goals of the group (Kello, 2013).

Some of the impacts caused by cybercrime then take a definition that can describe the cybercrime action. Cybercrime is an act of criminal attack which includes a computer as an object of the crime, or the computer is used as a tool in gathering material components in carrying out the attack. Then from that definition, cybercrime actions can be divided into two categories. The first is Pure Computer, which is the computer that is the object of the crime. This category includes attacks on computers through the network and through the computer system. The attack can be in the form of hacking and spreading viruses through internet networks and computer systems. The second is Computer-Supported Crimes, in this category computers are used as tools to do a criminal action. The crime can be classified as child pornography and the sale of illegal drugs (D.Valiquet, 2011).

METHODS

This article looks at the dynamics of security threats in international relations and uses qualitative methods. Which then compares the concepts of state security and human security. It starts by looking at several defense policy phenomena implemented by the United States. The policy will be assessed from the perspective of securitization and cybercrime concepts. Then, it will be compared with the concept of human security put forward by UNDP. Human security is one of the seven security described by UNDP. This will result in a view of which security priorities should be addressed. In addition, this view will also explain the current shift in the focus of international security. Especially, in assessing the form of threats to the security of a country. The resulting hypothesis is the overlapping of security objects that result from the actions of the State. Overlapping here is seen from the form of State action which is another threat to human security.

RESULTS AND DISCUSSION

The concept of international security still overlaps in explaining and defining a threat. When a phenomenon is securitized, it will become a threat to security. If you want to define the threat you must see the subject and object of the threat. When a phenomenon is seen in the concept of state security, then this phenomenon will become the scope of state security. However, when seeing a phenomenon with individual objects, then this phenomenon will become the scope of the human security concept. Therefore, the debate in international security begins with a criticism of conventional international security which only focuses on the state. In the times and technology development, the issue of international security has also expanded very broad understanding and scope. So, international security now does not only focus on state objects but also on individual, environment, economy, and identity.

Cyber Issues Securitization

Threats about cyber are often challenged by theoreticians who do not believe in these virtual threats. An example of some gaps in the implementation of policies about cybercrime. When a state wants to implement these policies, it needs real operation regarding the threat. Whereas the

cyber action cannot be seen in operational because it only works in the virtual world. However, the impact of these actions can be seen clearly in several fields. The next criticism is about the costs to hold up these actions. The estimated cost needed is very high. Because the development of technology is so fast and there are no limits in its development. In other words, when technology development has increased, higher costs are needed to follow the developments. Besides that, when a state implements a defense action for a cyberattack, it does not rule out the possibility that it will become a weapon in carrying out attacks against other states. So that it is considered very complex in viewing cyber as a security threat today (Kello, 2013). In understanding the phenomena of cybercrime is divided into several actions that are assumed to be threatening. Actions that are believed to be cyber threats to international security such as cyberweapon, malware, cyberattack, cyber exploitation, surveillance or sabotage of sensitive data owned by a state or company. However, the benchmark in operational actions is difficult because they are in a virtual world. Therefore, cyber actions are difficult to measure but can be prevented by securitizing the issue. Theories that explain cyber issues will be a guide for a state to take policies in dealing with cybercrime issues (Kello, 2013).

The explanation about cyber scope so that cyber issues can be one of the focus in contemporary security threats today. Therefore, the action about security not only focuses on the traditional threat. The cyber revolution with technology advances can be viewed in two ways. First, it can be seen as a facility that provides convenience to the interaction and integration of every information in the world. The second, it can be a threat when it is used by a group for criminal action. So that those actions can be categorized into one group. When the action is included in one of the six concepts (cyberweapon, malware, cyberattack, cyber exploitation, surveillance or sabotage of sensitive data owned by a state or company), it will become a threat from one of the corners of a group. This then becomes a weak point for theoretical cyber actions that have no clear boundaries. So that when it is raised as an issue it still does not have full confidence in the existence of the threat. Because it is difficult to say a threat when it becomes an act of defense of a group.

The traditional threat can be interpreted as a security concept that is only focused on military strength. In the Realism approach, State sovereignty is the main focus of a State. This gives an understanding that the main object of the security concept is the State. And its existence is threatened with military power possessed by other countries (Waisova, 2003). The development of subjects and security objects from traditional to contemporary has several links. This is indicated by the use of military weapons that are enhanced with technology. This phenomenon can be regarded as a contemporary threat because, in function, the tool is developing. Although the subject matter, have in common. On the other hand, the impact of these weapons is developing. The development here can be interpreted to be broad or even more specific. Widespread in the sense of the resulting impact causes wider destruction. Meanwhile, specifically, these weapons are capable of certain detection of objects that are considered threatening. So, it can be said that the emerging cyber threat is not a whole new thing. However, in some ways, it is a threat that already exists with certain developments.

The application of the concept of the threat to action is a very subjective assessment. Identification is usually done by policymakers, when a thing that is faced requires more action then it will be determined as a threat to the State (Ritchie, 2011). So, in the study of the concept of security is sometimes seen as a political thing and not objective. Because the referent object is intended only for national

defense. This then raises that the referent object of human security is not achieved. The cyber threat is one of the threats that often provide overlap in implementing policies. Newman (Newman, 2010) argues that in the traditional security concept which focuses military power on territorial integrity is still needed, but in some conditions, it is not able to achieve the welfare of the people within it (Ritchie, 2011).

Cybercrime threat has begun to be considered by the international community in the 1990s. In this case, each state, specially developed state, has given one of its state's security focus to cyber actions taken by certain individuals or groups. This is supported by the draft establishment by the Council of Europe in 1997 regarding actions to deal with cyber actions. The draft establishment has a goal to make it easier for each state to take collective action and cooperation in dealing with cyber actions comes from outside their state ("Adoption of Convention on Cybercrime," 2001). Cybercrime is not the only domestic crime that comes from the internal state. Cybercrime is also able to cross state borders by mediating internet channels that do not have any restrictions. So, when cybercrime has an impact on one state and the actor in another state, it will be difficult for a state to crack down the crimes, because there is a state sovereignty limit that cannot be crossed. It will become an obstacle for a state to face cybercrime if there is no international cooperation that regulates and helps to handle these cyber problems.

Besides that, in 2000, the United States business company was attacked by hackers who stole and falsified information data owned by the business. The action was carried out by Alexei Invanov and Vasiliy Gorshkov, this action unable to be followed up by America. That is because the actors who carry out these actions are in the territory of Russia. Meanwhile, Russia itself does not have cooperation with the United States regarding the handling of cyber actions. Therefore, it is difficult for the FBI to crack down on these actors, except if Russia wants to give the person concerned to get out of the territory of Russia (S.W.Branner, 2007). This is, as explained before, sometimes state actions have limitations in handling these cyber actions. Because the position of each state has its own sovereignty limits. One of the ways to handle it by making a convention to cooperate in the application of national law to deal with cyber actions.

The draft produced by the CEO was then assisted by the United States in securitizing the Cybercrime issue. One of the states that first ratified the draft was the United States in 2001 after the draft was opened to receive a state that would like to cooperate in dealing with these cyber issues. The draft contains several regulations that will be approved by the states that ratified it to apply to their respective national laws. The draft convention in dealing with cybercrime gives every state the right to take action on any deliberate action and violate rights through the computer system as a criminal act which are applied as national law, such as ("Adoption of Convention on Cybercrime," 2001):

a. Get computer access
b. Intercept non-public mission
c. Damaging, deleting, preventing, worsening, and suppressing computer data
d. Obstructs the functioning of the computer system seriously by entering, transmitting data, changing, and destroying computer data
e. Production, sale, procurement for use, distribution or manufacture:
   - Devices designed or adapted specifically to commit violations that have been described above
   - The use of passwords, access codes, or similar data is used for criminal acts
f. Counterfeiting related to computers
g. Cheating related to computers

h. Child Pornography and terrorism. Each of these actions uses a computer as a tool to do criminal actions.

The CEO draft was opened on November 23, 2001, to call on each state to focus on the cyber threat as one of the current international threats. In this convention, 43 states have signed the draft and 21 states have ratified the convention. Some of these countries are Albania, Armenia, Bosnia, and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Hungary, Iceland, Latvia, Lithuania, Netherlands, Norway, Romania, Slovenia, Macedonia, and United States. In this case, some other states outside the European Union were also able to ratify the resulting draft. The other states are also able to invite the states outside Europe to participate in the draft in order to cooperation in handling cyber actions (S.W.Branner, 2007). However, the problem is sometimes developing states do not want to participate in ratifying the draft. That is because the cyber threat is less important for their state. Because the objects of cybercrime are mostly from developed states that have high technology and use a lot of computer systems to regulate the state and the economy. So that, developed states become a target for actors in cybercrime action.

The incidence of threats related to cybercrime or cyberattacks continues to increase in the United States. In the past 6 years, increased crime rates reached 68%. Cyber actions consisting of threats are classified into two parts, that is unintentional threats and intentional threats. Unintentional threats are caused by technical errors or system damage and have an impact on failure in system work. Intentional threats are criminal groups, hackers, espionage and terrorism (Infrastructure, 2009). In this case, President Barack Obama releases a policy that aims to increase the security defense of his state from cyberattack and to create cybersecurity. President Barack Obama's policy strategy is (Infrastructure, 2009) lead through the highest leader, building the nation's digital capacity, sharing responsibility in cybersecurity, establish an incident response agency and share information effectively, encourage innovation, and action plan.

The application of US policy toward cyber phenomena is one of the actions of securitization. In this case, the United States builds the views of its allies and international society that cybercrime is a threat to international security and needs to be addressed. The disadvantage suffered by the United States in economic, social and political sectors makes the cyber phenomenon become a real threat to international security today. The United States is a developed state in the field of technology to conduct speech acts and securitization of cyber phenomena that can attack the state. This can also happen in the other states, especially for a state that does not have advanced technology. The actions of the United States in dealing with cybersecurity, cyber defense, and cyberattacks raise a question about objects that the United States wants to protect. Based on the policy adopted by the President of the United States, the only object to be protected from the threat is the state. In this case, there is a collision of the object protection threat between state and individual. Because the defense carried out by a state can be a threat to individuals who live in the state itself.

State Security Versus Human Security

Human security is a fairly new concept. This concept offers an approach in seeing security from the human aspect as a referent object. Thus, the source of insecurity in this view is everything threatens that exists outside of humans as individuals. Therefore, this approach also considers that the state is also a source of insecurity. Thus, this approach becomes a critique of national security in four aspects; 1) Pay more attention to individuals and communities than the state, 2) Human security threats are state security threats

too, 3) Scope of actor is extended across the state, 4) Achieving human security is not only by protecting humans but also empowering people to protect themselves (Hudson, 2013). The implementation of government policy on national defense raises a debate about the intended security object. In this case, the application of state policy in maintaining its national security can erase human security or individuals who live in it. The security object can be divided into two parts namely, the security object that can be measured and security that cannot be measured. The defense built by the state can have a long-term impact on human or individual security. On a short scale the security built by the state can only have a positive impact on the state but not on individuals.

Government policy in collecting information data about its citizens with the reason to create a defense from external threats can be an individual threat. This can be illustrated when a state centralizes the data center of its citizens' information and can be accessed through the cyberspace is an opportunity for an individual to misuse the information data. Security in terms of privacy is a bridge between data and consumers. Thus, security is something that gives privacy rights to information that can be consumed (Bambauer, 2013). A crime that appears in the information data as transnational crime, such as sending illegal foreign workers to other states. The fraud that is carried out through cyberspace is a threat to individuals and the impact will be affected by individuals. In other words, when the information collected is centralized, it will be easier for actors who do the crimes to get information through the internet and determine the target object. Therefore, state actions sometimes contrary to the security that is being proposed and explained by UNDP about human security.

Human security has seven elements that are related to the concept of Human Security in accordance with UNDP that established in the United Nations. One of those seven-elements is personal security or individual security. Personal security has several issues that will threaten personal security, such as psychological violence in any form, crime, domestic conflict, and human trafficking (United Nations, 2016). Some of those threats are only one part of threats that can threaten personal security. The concept of human security is developed from liberal thinking where each individual has three categories namely, human security, individual development, and individual human rights. Application in the concept of human security is not only implemented by policymakers in government but also promoted and run by international organizations and non-governmental organizations that have networks in various states. The next thought of this approach is about 'freedom from fear' and 'freedom from lack'. UNDP in 1994 tried to provide an understanding of human security, by identifying seven elements which include human security namely, economic security, food security, health security, environmental security, individual security, group security, and political security (Peoples & Vaughan-Williams, 2010).

The threat that comes from Cybercrime's actions is human rights about individual privacy. Privacy is a context that cannot be measured. In some definitions, privacy is a context that can be defined by each individual. Privacy is a power that can only be controlled by oneself. The privacy context then becomes a consideration regarding the security established by a state. When an individual's privacy is eroded by a state's defense policy, then those security threats will still exist.

One of the actions of cybercrime is terrorism which is controlled and mobilized using the reach of the internet and existing computer systems. Because terrorism is not only an action that provides physical threats. However, this action is also able to threaten and provide

terror through virtual media which can then be accepted by every individual in every state in the world. So that terrorism is one of the cybercrime acts that threaten every state and every individual in it.

The threat of terrorism is a phenomenon that has threatened the world since the events of 9/11. The incident then made the issue of terrorism securitized and then it became a focus for all states. Terrorism as an act of 'terrorism' can threaten human psychology who always felt threatened and terrorized by the issue of terrorism. The characteristic of terrorism is the desire to convey a message to a regime or policy with an uncertain object (Buzan & Hansen, 2009). This uncertain object becomes a threat to every individual because they will feel insecure and afraid of terrorism that can occur anytime and anywhere. In this case, the issue of terrorism is not only identical to individual groups, but the state is also able to be labeled as terrorism. This is like what the United States did to identify the states that have nuclear as a state that threatens other states with their nuclear weapons (Buzan & Hansen, 2009).

The issue of terrorism is a threat to every country. The United Kingdom responded to this threat by increasing its surveillance technology. Installation of 440 CCTV in various cities as surveillance in maintaining security. The fear of terrorist attacks then raises a policy that results in a new threat for human security when surveillance technology is installed with the aim of defense from the threat of terrorism, then runs into shifting the goals and felt by the society. The installation of a surveillance camera is considered as a surveillance camera of the daily activities of individuals. The shift of purpose means that CCTV cameras which are supposed to be a defense against terrorism then become a threat to individuals about privacy regarding their daily activities in public areas (S.B.Spancer, 2002).

The technology developments made by the United States on terrorism issues are not different from the United Kingdom. Installation of surveillance cameras in each city and also the collection of individual personal data to handle the entry of terrorist threats into their state. However, this is become a critique of security built by the United States with state objects and sacrifice individual privacy. Besides that, the inspections carried out at the entrance of the United States airport have an impact on individual insecurity on their privacy. The policies adopted by the United States government give an insecure feeling to individuals because they always feel stalked (S.B.Spancer, 2002).

The United States is building a network of surveillance cameras centered on one system. The construction of this system was carried out in the Synchronized Operation Command Complex (SOCC). The construction of surveillance cameras includes 200 cameras in public areas and it will add 200 cameras in several other public places such as shops, hotels, and apartments. In addition, SOCC also forms a network for collecting database and regional traffic system (S.B.Spancer, 2002).

In addition, the FBI team also collaborated with several agencies that had already been established to deal with the issue of cyberattacks. National Cyber-Forensics and Training Alliances (NFCTA) is an organization that was founded in 1997 based in Pittsburgh. This organization changes the view of cyber action into an action that needs attention as a threat to a state. So, at this time the view of cyber actions is a criminal act that originates from domestic but has a transnational or international impact. The United States intelligence agency then collaborated with NFC to deal with the increasingly widespread cyber issue. Because in dealing with a global threat, it is very difficult if only acting individually. Therefore, international organizations are needed to collaborate with other countries to handle this investigation.

United States' actions give a threatening effect on human security in terms of

privacy. Actually, the main goal of the state is handling the terrorist but the national cyber defense policy will provide individual security threats, especially in terms of privacy. Measurable security objects can be achieved in the short term with the application of surveillance cameras. However, security objects that cannot be measured will be sacrificed to achieve security objects that can be measured. According to the concept of human security, when the state security wants to be achieved, it must prioritize human security, that is the individuals who live in it. When human security can be achieved, state security will also be achieved. However, when state security is achieved, it is not certain that the desired human security will be achieved. The definition of human security itself is a condition where an individual feels free from fear (Peoples & Vaughan-Williams, 2010).

Human security is a view that is born from criticism due to the role of the state which too concerned with national interests than human interests. This assumption arises because the concept of human security assumes that the state as an institution fails to guarantee human security. Poverty, crime, prostitution, and etc are still a concern in various states. But for realists, human security can be achieved by seeking national security. So, to create human security, the people in the jurisdiction of the state can express their aspirations to the government. Because the state is able to provide laws and regulations to limit the development of threats that threaten human security. Human security and state security can be interdependent and work in harmony when a state is able to improve the welfare of its society by protecting its national security (Waisova, 2003). However, some countries in this regard still consider that the concept of human security is still just an idea. Which is the concept of human security is divided into two focus namely economic aspects and political aspects (Waisova, 2003).

The security established by the United States through its policies aims to protect its society from the threat of terrorism. However, the practice of implementing defense is only protecting the state from fear with the threat of terrorism that exists. Then, give a new security threat for individuals who feel their freedom eroded by surveillance cameras in various corners of the region. They feel safe from the threat of terrorism with sacrifice their privacy rights that monitored by the state. Safe conditions desired by the United States to be unsafe conditions for citizens, visitors, and the public that monitored in the video and connected in one network and database entered into the system built by the United States. The form of surveillance carried out by the United States is not only in domestic but also with the other states. In an international context, the United States develops cyberweapon Drones which is facilitated by weapons that can be controlled remotely. The drone and can be controlled remotely is facilitated by weapons. The weaponry aims to act directly against acts of terrorism in a country.

In the international context, the use of drones as surveillance equipment can violate international war laws, like *jus ad bellum* and *jus in bello*. *Jus ad bellum* is an international law that explains before the war. Meanwhile, just in bello is a law that regulates the laws of war when the war has occurred (Brunstetter & Braun, 2011). According to the international humanitarian law, reconnaissance carried out by using drones is an espionage action that violates states' sovereignty. Espionage action carried out by a state against another state is a threat to national security. This remote-controlled weapon could not control the impact caused by the weapon. So, it does not rule out the possibility when the weapon is operated, it will threaten the lives of non-combatants around the threat

target. From the explanation above, we can see the actions taken by the United States in dealing with cyber issues by increase cyber defense and cybersecurity in their state. But threats that come not only from outside but can come from within the country as well. When threats come from within the state, then the defense to secure will become an action that creates a new threat. Due to cyber phenomena have unpredictable actors, so that the possibility of threat that could come in the form of attacks from within the state. When the threat handling action is misused and not in accordance with the original purpose, then it will be the new threat for individual security within the state itself.

Seeing the phenomenon faced by the United States regarding gaps between human security and state security brings up a statement from President Bush who said that, freedom and fear of war. Freedom is like the United States and fear is like the Taliban and terrorism. Privacy values are a defense of freedom. Although some security concepts seem to want to help create a sense of security from existing threats. Spancer said don't let something that already exists before, replaced by something in the future (S.B.Spancer, 2002). From the statement above, we can see that the concept of individual freedom about privacy does not replace the concept of security that wants to eliminate fear. Because of that, human or individual security is the main object of a states' security. The concept of security offered should not damage the privacy value held by an individual, especially in the United States. However, in reality, the policies issued by the state cannot be separated from group interests. When the policy is implemented with the aim of dealing with cyber issues, in fact, the security offered threatens the privacy of every individual who lives in. Thus, it is considered less efficient if the main objective of the policy is security. The author agrees with the concept of UK security which uses the concept of "putting people first". In this case, human security is part of the security of the State. Because the State has a duty to provide security for the people who live in it (Ritchie, 2011).

CONCLUSIONS, RECOMMENDATION, AND LIMITATION

The issue of international security is a very complex issue. The approach to international security threats can be seen from the object to be secured. The issues about cyber and cyber threats see individuals as an object of security threats. The policies adopted by the United States are more focused on state security and not really concerned about individual security. It can be seen from the view of the human security concept. When state security has been achieved, does human security can also be achieved. The policy carried out by the United States and supported by European Union in handling Cyber issues seen as securitization carried out by the state. It is because of the position of the United States as a power state and high technology as forming other states' assumptions in the view of cyber as a threat. Then, the action carried out by the United States intelligence agency and also a draft formed by the European Commission is a form of action in dealing with cyber as a very threatening today. Therefore, other states will come to see this as a security threat, even though there is still a debate within the ISS regarding cyber as a threat or not.

In this case, the study of international security is developing more slowly than the phenomenon that occurs. This is reflected when the phenomenon of international threats should be more widespread but the study of international security is still on traditional understanding. So, when the issue becomes wider, awareness about the issue has not appeared because there is no securitization process that raises the issue. The international security development process supported by the phenomenon of

globalization and the very rapid technology development. Therefore, sometimes when a cyber threat becomes an issue that threatens security, it is difficult to distinguish between security measures and needs. As we know, the development of technology and the internet today is very attached to the lifestyle of every individual and state. When something that is very inherent in daily life becomes a threat, it will be difficult to separate it and sort it out in the form of threats and needs.

The concept of international security still overlaps in explaining and defining a threat. When a phenomenon is securitized, it will become a threat to security. If you want to define the threat you must see the subject and object of the threat. When a phenomenon is seen in the concept of state security, then this phenomenon will become the scope of state security. However, when seeing a phenomenon with individual objects, then this phenomenon will become the scope of the human security concept. Therefore, the debate in international security begins with a criticism of conventional international security which only focuses on the state. In the times and technology development, the issue of international security has also expanded very broad understanding and scope. So, international security now does not only focus on state objects but also on individual, environment, economy, and identity.

REFERENCES

Adoption of Convention on Cybercrime. (2001). *The American Journal of International Law*. https://doi.org/10.2307/2674643

Bambauer, D. E. (2013). Privacy versus security. *Journal of Criminal Law and Criminology*.

Brunstetter, D., & Braun, M. (2011). The Implications of Drones on the Just War Tradition. *Ethics and International Affairs*. https://doi.org/10.1017/S0892679411000281

Buzan, B., & Hansen, L. (2007). *International Security: Widening Security*. *SAGE library of international relations*.

Buzan, B., & Hansen, L. (2009). *The evolution of international security studies*. *The Evolution of International Security Studies*. https://doi.org/10.1017/CBO9780511817762

D.Valiquet. (2011). *Cybercrime Issues*. Canada: Parliamentary Information and Research Service (Library of Parliament).

Hudson, N. F. (2013). "Human security." In *Critical Approaches to Security An introduction to theories and methods*. New York: Routledge.

Infrastructure, C. (2009). Cyberspace Policy Review. *Security*.

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*. https://doi.org/10.1162/ISEC_a_00138

Newman, E. (2010). Critical human security studies. *Review of International Studies*. https://doi.org/10.1017/S0260210509990519

Peoples, C., & Vaughan-Williams, N. (2010). *Critical security studies: An introduction. Critical Security Studies: An Introduction*. https://doi.org/10.4324/9780203847473

Ritchie, N. (2011). Rethinking Security : a critical amalysios of the startegic Defence and Security Review. *International Affairs (Royal Institute of International Affairs)*, *87*(2), 355–376.

S.B.Spancer. (2002). Security vs Privacy. In *Denver University Law* (78th ed.). Denver.

S.W.Branner, J. (2007). Cybercrime Havens : Challanges and Sollutions. *Business Law Today*, *17*(2), 48–51.

Storlie, C., Anderson, B., Wiel, S. Vander, Quist, D., Hash, C., & Brown, N.

(2014). Stochastic identification of Malware with dynamic traces. *Annals of Applied Statistics*. https://doi.org/10.1214/13-AOAS703

United Nations. (2016). *Human Security Handbook*. United Nations trust Fund of Human Security.

Waisova, S. (2003). Human Security - The Contemporary Paradigm? *Perspective*, (20), 58–72.