Intermestic: Journal of International Studies
e-ISSN.2503-443X
Volume 7, No. 1, November 2022 (298-315) doi:10.24198/intermestic.v7n1.14

THE IMPORTANCE OF GLOBAL EFFORT TO SECURE SPACE SECTOR FROM CYBERATTACK

Antonia Rahayu Rosaria Wibowo[1*]

[1]**Badan Riset dan Inovasi Nasional**
*email: arosariawibowo@gmail.com

Abstrak

Penggunaan internet telah berkembang dengan cepat sejak tahun 1990an. Hal ini telah membawa baik perkembangan dalam kehidupan maupun tindak kriminal pada ruang siber. Serangan siber telah memengaruhi banyak sektor termasuk sektor antariksa. Sektor antariksa rentan terhadap serangan siber sebab banyak teknologi manusia bergantung pada sektor antariksa. Aktor di balik serangan siber tidak dapat diidentifikasi secara individu berdasarkan lokasi geografis sehingga diperlukan upaya global. Pentingnya upaya global untuk mengamankan sektor antariksa dari serangan siber didiskusikan dalam makalah ini. Makalah ini menggunakan metode deskriptif dan teknik kajian pustaka untuk mengumpulkan data. Data terkait serangan siber pada sektor antariksa dan upaya mengamankannya dari serangan siber dikumpulkan dari jurnal akademis dan dokumen organisasi internasional. Data tersebut kemudian dianalisis menggunakan teori global governance. Hasil analisis menunjukan bahwa upaya global untuk mengamankan sektor antariksa dari serangan siber penting sebab serangan siber merupakan masalah transnasional dan sektor antariksa menghubungkan infrastruktur modern secara global.

Kata Kunci*: sektor antariksa; serangan siber; upaya global*

Abstract

The use of internet has grown massively since 1990s. It has brought both life improvement and criminal activities in cyberspace. The cyberattack has affected most sectors including space sector. The space sector is vulnerable to cyberattacks because a lot of human technologies depend on it. The actors behind it cannot be identified as an individual based on geographical location, so that, global effort is needed. The importance of global effort to secure space sector from cyberattacks is discussed in this paper. This paper used the descriptive method and library research techniques to collect data. Data about cyberattack on space sector and efforts to secure them were collected from academic journals and international organizations' documents. Then, they were analyzed using the global governance theory. The result shows that global effort to secure space sector from cyberattack is important because it is a transnational problem, furthermore space sector connects modern infrastructures worldwide.

Keywords: cyberattack; global effort; space sector

Introduction

The use of the internet has grown massively since the 1990s. This growth is accompanied by the development of digital technology. The development of digital technology makes people's lives easier and faster. In the past, when people wanted to transfer some money, they had to go to the bank or Automated Teller Machine (ATM) center. Nowadays, they can transfer from their homes using internet banking or mobile banking. This technology advances can save a lot of time because people do not need to walk or drive to the bank or ATM center. Besides, due to the development of digital technology, people get interconnected. It seems there is no more border among people. For example, Indonesians can directly connect to foreigners on different continents through social media. Throughit, people can chit-chat, share images, and make face-to-face video calls. Because of the massive development of digital technology which makes people interconnected, most people's interactions happen in cyberspace, hence cyber interactions live and exist hand in hand with physical interactions.

Although it brings a lot of benefits, technology and cyber activities also create criminal activities. Phishing, ransomware, malware, and social engineering are four types of criminal activities in cyberspace (Sheth, Boshale & Kurupkar, 2021: 247). Those four activities consist of manipulating people through phone calls, distributing fake communication, hijacking personal data and computer systems, and using destructive software. Unfortunately, these criminal activities do not only affect personal things. They also affect the government. There are some cases when a destructive virus attacks the financial documents of a certain economic system or disrupts a country's stock market (Li & Liu, 2021: 2). This condition leads to that country's instability. One sector that is also affected by cyber-criminal activities is the space sector.

Space sector is a vulnerable sector. It can be easily attacked by a hacker which brings chaos to the economy and military system. There are three groups of weak points which make the space sector vulnerable. They are the satellite, the ground station, and the end-user (Rajagopalan & Porras, 2015: 2). One example is a hacker can attack satellites or an operator of many satellites which connect to point-of-sale credit card systems, inventory management, or video conferencing services. By attacking satellite systems which connect credit card systems, for example, the economic activities which need credit cards will be disturbed. The economy is an important sector for people and countries, by disturbing its system, the hacker can create chaos. Using cyber technology to attack the satellite is easier than attacking an e-commerce company (Falco, 2018: 2-3).

Besides the attack on the economic system, cyber technology has been used in other systems which depend on the space sector. The cyberattack has targeted several sectors, such as transportation, banking, energy, telecommunications, air, sea, and land navigation, distress detection, and GNSS timing. There were four examples of the cyberattack on the space sector that occurred in the 2000s. The two first examples were Landsat 7 in 2007 and Terra EOS in 2008 experienced cyber interference when hackers achieved the required steps to assume Command & Control but did not issue commands. Another example, the US National Oceanographic and Atmospheric Agency was denied space-based information for 48 hours in 2014 and the US Maritime Administration reported the first GPS spoofing attack against over 20 ships in the Black Sea in 2017 (Plattard & Smith, 2021: 6).

Considering the vulnerability of the space sector to the cyberattack, it is important to find a suitable method to secure the space sector. The actors behind the cyberattack cannot be easily identified as certain individuals (Rajagopalan & Porras, 2015: 4), they can be an unknown group of people. Moreover, the actors cannot be limited by geographical borders (Li & Liu, 2021: 2), they can live anywhere without specific nationality and geographical location. Because cyberattack is borderless, therefore global effort is needed. The importance of the global effort to secure the space sector from the cyberattack is discussed in this paper.

The topic of this paper is important because there is no research on international efforts to create cybersecurity for the space sector. There was comparative research on cybersecurity awareness in 2020 which took Israel, Poland, Slovenia, and Turkey as examples. The research examined the relationship between cybersecurity awareness, knowledge, and behavior with protection tools among individuals in those four countries (Zwilling et al., 2020). The objective of the research is the national phenomena in those four countries. Yet the research does not discuss the space sector and international efforts to combat cyberattack on the space sector.

There was also research on cybersecurity and politics in 2019. This research discussed the driver of technology, politics, and science which have an influential role in the evolution of cybersecurity politics and its study (Cavelty & Wenger, 2019). This research only discusses political elements behind the cybersecurity issues. It does not discuss cybersecurity on space assets and international politics. Another research on international response and cybersecurity provided the initial baseline for representing and tracking institutional responses to the changing of international landscape, both real and virtual (Choucri, Madnick & Ferwerda, 2014). This research only gives a theoretical baseline and does not touch the space sector. Three previous studies cited here do not discuss cybersecurity in the space sector. There is only one research discussing international response toward cybersecurity. However, it does not discuss the space sector.

Based on the introduction above, this paper wants to question the importance of the global effort to secure the space sector from cyberattack. There are three realities to bear in mind. First, it is a fact that a lot of human technologies depend on the space sector. Second, the development of information technology creates a massive number of cyberattacks besides its benefits and the cyberattack is also experienced by the space sector. Thus, the space sector which supports a lot of human technologies is also vulnerable to cyberattack. Third, cyberattack is a transnational problem which needs global effort to be maintained. However, there is no research that discusses the global effort to secure the space sector from cyberattack. Realizing these facts, this paper seeks to analyze the importance of the global effort to secure the space sector from cyberattack using the global governance theory. After the analysis, this paper can give new insight into the existing research by exploring the international effort to combat cyberattack on the space sector.

Global Governance Theory

According to Zürn in his book entitled *A Theory of Global Governance: Authority, Legitimacy, and Contestation*, global governance refers to the exercise of authority across national borders as well as consented norms and rules beyond the nation-state, both of them justified with reference to common goods or transnational problems (Zürn, 2018: 3-4). That definition shows that there is another authority above the national authority. This authority can be in a form of norms and rules which are applied at the international level. Further, Zürn mentioned five points to be understood about global governance's definition. First, global governance refers to a pluralization of governance actors; second, global governance contains agreed norms and the exercise of authority; third, the exercise of the authority and the declaration of the agreed norms are followed by a communicative act; fourth, global governance's definition does not prejudge its social purpose; fifth, not all global governance arrangements need to be applied to the whole globe (Zürn, 2018: 4-5).

Global governance system consists of patterns of authority relationships which produce conflict, contestation, and resistance. As other systems, the global governance system consists of some actors. They are states, transnational institutions, and also citizens. Every actor brings different norms and rules. As the interaction of the actors goes on, the interaction of different norms and rules also goes on. The interaction produces transnational and international regulations and other governance activities such as agenda setting, monitoring, adjudication, and enforcement (Zürn, 2018: 6). Those outputs are referred to global common goods and are expected to get a minimal level of compliance pull (Zürn, 2018: 6) from states and societies. The outputs do not always create benefits and agreements among countries. They sometimes create costs and disagreements.

Global governance system is based on three normative principles that qualify sovereignty. First, the justification of global governance needs not only states but also societal actors and individuals. Both sovereign states and societal actors who have the rights to address international authorities can justify global governance. Second, global governance aims for the achievement of global common good. In order to achieve a global common good, the national authority and societal actors' autonomy is less preferred than global regulations. Third, there is a generalized belief in international authority. When states and societal actors respect obligations that may be different from their own interests, and these are justified according to the global common good and individual rights, the system is no longer anarchical (Zürn, 2018: 7-8). These three normative principles show that international regulations or global governance has higher hierarchy than national sovereignty.

Global governance can get special authority because of three reasons. First reason is states will be willing to renounce their sovereignty only in very special circumstances. Second reason is that the authority of global governance does not come before the birth of states. It comes after the birth of states. Third reason is that global governance authority targets states which have more resources than other international organizations. These show that the authority of the global governance system is a reflexive relationship. The characteristic of a reflexive relationship is it is not based on the command, but on the request or demand. The reflexive relationship makes countries delegate some of their authorities to the higher system in order to achieve the common good. The higher system is the global governance. Global governance hopes that its recommendation will be followed by countries because they have agreed to delegate some of their authority for the common good (Zürn, 2018: 9-10).

Research Method

This paper used the descriptive method and library research technique to collect the data. Data about cyberattacks on the space sector and efforts to secure the space sector from them were collected for this paper from academic journals and international organizations' documents from 2014-2021. For answering the question above, the data were analyzed using global governance theory. Global governance theory is chosen to analyze the global effort to secure the space sector from cyberattack because this theory emphasizes the importance of authority that is exercised beyond national borders. Also, this theory highlights the international authority beyond national authorities. It is suitable to analyze cyberattack due to its transnational characteristic. Analysis was conducted by matching the data with variables mentioned in the global governance theory.

Cyberattack on Space Asset

Cybercrime can be defined as any crime that is committed using a computer or network, or hardware device. The computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime. Cybercrime can be divided into two categories with different characteristics. Cybercrime type I is characterized as a single attack from the perspective of the victim. For example, the victim unknowingly downloads a Trojan horse which installs a keystroke logger on his or her machine. Then, the victim might receive an e-mail containing what claims to be a link to a known entity, but in reality, is a link to a hostile website. Some examples of this type I cybercrime are phishing, theft or manipulation of data or services via hacking or viruses, identity theft, and bank or e-commerce fraud. Cybercrime type II is characterized as an ongoing series of attacks, involving repeated interactions with the target. For example, the target is contacted in a chat room by someone who, over time, attempts to establish a relationship. Eventually, the criminal exploits the relationship to commit a crime. Some examples of cybercrime type II are cyberstalking and harassment, child predation, extortion, blackmail, stock market manipulation, complex corporate espionage, and planning or carrying out terrorist activities (Nassau County, n.d.).

For the context of space assets, Secure World Foundation defines cyber capabilities as a broad set of different tools and techniques aimed at exploiting ever-changing vulnerabilities in each layer of the infrastructure that underpins space access. Next, Secure World Foundation mentioned that cyberattack requires access, vulnerability, malicious payload, and a command-and-control system. There are four categories of cyberattacks on space assets.

a. The risks to global supply chain security posed by the increasing use of faulty or counterfeit microelectronics and materials produced abroad have been well-documented.
b. Cyberattacks which directed against the links between satellites and ground control stations.
c. Attacks on terrestrial C2 or data relay stations.
d. Cyberattacks against the user segment of a space system, often the terminals or devices used to receive or process a satellite signal (Secure World Foundation, 2021: 9_2-9_7).

In the research entitled The Vacuum of Space Cyber Security, Falco mentioned that cyberattack can target satellite systems. First, it can target IP satellite communication. A hacker can detect IP addresses from satellite internet users and then create an IP connection from the stolen IP address. It can disturb and damage the end-user’s operation. Second, it can attack Global Positioning System (GPS) satellites. This system relies on satellites to triangulate specific positions on earth. Introducing noise into the receiver spectrum of the GPS satellite can create failure in the GPS receiver which makes the reading become inaccurate. Third, it can attack government satellites and ground space systems. A hacker can use the public internet to reach government satellites. After reaching the satellite system, the hacker can compromise satellite imagery, stunt the transmission of imagery or exfiltrate images (Falco, 2018: 6-7).

Besides Falco's research, Kwok in his article in 2021 entitled The Growing Threat of Cybercrime in The Space Domain wrote that in 2007 Sri Lanka's Tamil Tiger rebel group hijacked an Intelsat satellite in order to broadcast a propaganda which represented Tamil's minority population who fought against Sri Lankan military power. The Tamil Tiger used a Ku-band transponder to broadcast political messages for over a year (Kwok, 2021: para. 3-4). This event shows that space assets are vulnerable. It can be easily attacked in cyberspace. After it is hijacked, it will be used to fulfill the hacker's interest and it might disturb the legal government.

The current trend of space activities is space commercialization. Information technology is needed for commercialization. Information technology and massive development of satellites which create the advancement of communications, transmissions, electronics, computing, artificial intelligence, and a large amount of data procession make space assets more vulnerable to cyberattack. A cyberattack can disrupt satellites and become an effective space weapon. It can promulgate space warfare (Pražák, 2020).

Due to its vulnerability, space assets are able to be the target of cyberwarfare. Cyberwarfare is possibly becoming a large challenge because cyber capabilities are easily accessible. They can also be developed and deployed faster and cheaper compared to other counter-space capabilities. Their development is also supported by the presence of many independent hackers. Eventually, cyberwarfare can create massive disruption and damage to space systems (Rajagopalan, 2019: 9). The techniques used in a cyberattack on space assets can be in a form of direct attack on the data or the systems which use data, satellites which are linked to cyber nodes, landlines which link ground stations to terrestrial networks, user terminal which links satellites, and antennas on satellites or ground stations (Rajagopalan, 2019: 9).

Securing Space Sector from Cyberattack

A United Nations resolution 75/36 in document A/RES/75/36 noted that there are rapid advances of technology in space systems. The use of technologies could have positive or negative impacts on international security, seeking to understand how states behave in the light of this development (United Nations, 2020: 2). This resolution shows that the United Nations, as the multilateral platform, realizes both the positive and negative impacts of the technological development used in the space system. This resolution calls the states to use the technologies for maintaining international stability and security and requests states to avoid and mitigate potential impacts on peace and security arising from the lack of transparency and miscommunication of the technological development which could lead to miscalculation or contribute to arms race (United Nations, 2020: 2). The technological development includes the development of cyber capabilities which can bring negative effects to the space system. The negative effects of cyber capabilities used in space systems were elaborated in the previous part of this paper.

As explained above, due to its vulnerability, it is important to make the space sector resilient toward cyberattacks. There are three considerations to make the space sector irrepressible. They are prevention, mitigation, and resiliency. First, prevention refers to several techniques to prevent attackers from successfully directing an attack against a space system. Second, mitigation refers to the complexity of modern cyber-intensive systems, such as typical space ground systems and prevention strategies. Third, resiliency refers to strategies that help the mission survive by ensuring some level of service from IT components that may be under duress from attackers (Llansó & Pearson, 2016: 3). For achieving this space sector resiliency, global effort is needed. According to Livingstone & Lewis, an international coherent approach is needed to overcome complex and internationalized cybersecurity problems.

Furthermore, Livingstone & Lewis mentioned that policy requirements, governance, management, and inclusiveness are needed to establish space cybersecurity.

a. “The policy requirements should ideally meet the needs of all concerns, among others the millions of end users, individual scientists, the corporate sector and the military. The policy should also address technical, political, economic and social interests, and combine the tactical with the strategic approach.

b. The governance should adopt and apply policies which enable legitimate users of space-related capability while increasing the costs for illegitimate users. The governance should also use a collective approach, involving as many legitimate stakeholders as possible and practical. Then, the governance should base itself on a self-governing and lightly regulated effort by a wide range of legitimate users of space capability.

c. Management is related with the ability to manage threats and risks on cyberspace and create security-by-design and pre-emptive risk mitigation controls with the flexibility and resilience to handle emergencies as the threats and risks develop.

d. Inclusiveness is related with the actors involved on the governance. In order to secure space sector from cyberattack, the international governance should involve analysts, policy makers, technical experts, and users because all of them can give intellectual contributions in the discussion of how to create security for space sector" (Livingstone & Lewis, 2016: 25-27).

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies 1967 or known as the Outer Space Treaty is the first multilateral policy to secure space assets. As a treaty, it is also the first legal multilateral agreement on outer space. It was produced to protect outer space and to guarantee its peaceful uses. The purpose to protect outer space is clearly stated in Article III and Article IV of the Outer Space Treaty. Article III mentions that all states which explore and use outer space, including the Moon and other celestial bodies, should conduct their activities in following international law to maintain international peace and security and promote international cooperation and understanding. Article IV mentions that States must not place objects carrying nuclear weapons or any other kinds of weapons of mass destruction around the Earth's orbit, on the Moon, and on other celestial bodies. Article IV also forbids the establishment of military bases, installations and fortifications, the testing of any type of weapons, and the conduct of military maneuvers on celestial bodies (United Nations, 2002).

Besides the policy, real action to secure the space sector from cyberattack has to be implemented. Two examples of securing the space sector from cyberattack are cited here. Those examples are taken from telemedicine and space information networks. Telemedicine involves the fusion of healthcare information and Information and Communication Technology (ICT), various new services, and networked medical devices. This facility needs health information exchange, therefore, security management is important. Telemedicine can be categorized into five types: videoconference-based patient consultations, multimedia transmission to provide remote services, remote home care, remote training of patients or health professionals, and online medical counseling and health information sharing. Then, there are seven telemedicine security threats areas: users or patients, telemedicine devices, home networks, gateway devices, internet, telemedicine system, and telemedicine service provider. Security threat assessment and analysis should be performed for the seven areas in order to find appropriate security guidelines and measures (Kim, Choi & Han, 2020).

Space Information Networks (SINs) is a network infrastructure which uses satellites, stratospheric air-ships, Unmanned Aerial Vehicles (UAV), and other platforms as carriers to acquire, transmit and process spatial information in real-time. It is a hybrid network system that interconnects spatial satellite networks, modern communication networks, terrestrial ad-hoc, and internet. The threats of SINs can be divided into three types: natural threats, environmental threats, and mission threats. First, natural threats caused by natural factors like interference from space electromagnetic radiation and severe natural climates. Second, environmental threats caused by system operating environment failures like power outages or downtime. Third, mission threats caused by organizations or individuals for various goals and motivations like malicious cyberattacks. They include force destruction, destruction or interference for communication channels, information theft and destruction for entire networks. Basic security and efficiency requirements like data integrity, confidentiality, truth, availability, and non-repudiation should be fulfilled in order to avoid those security threats. SINs security issues should be investigated from the routing issues and anomaly detection issues. There are four types of routing issues: SINs routing types, single-layer routing, multi-layer routing, and intelligent routing-based machine learning (Zhuo, et al., 2021).

Two research above investigated how to secure space assets from cyberattack. The policy combined with the technical research is hoped to create effective security protocols to secure space assets. Since cyberattack cannot be restricted by national borders or geographical location, international or global policy is needed. The International Multilateral Partnership Against Cyber Threats (IMPACT) is the cybersecurity executing arm of United Nations special agency, International Telecommunication Union (ITU). ITU is a special agency of the United Nations which deals with international connectivity in communications networks by providing global radio spectrum and satellite orbits, developing technical standards that ensure networks and technologies interconnect, and improving access to ICTs to communities around the globe. Seeing these works of ITU, it can be seen that ITU deals with the space sector to ensure the communication is available worldwide. In order to face cyber threats worldwide, ITU creates IMPACT. According to the IMPACT Fact Sheet provided by ITU, IMPACT has four centers: Global Response Center (GRC), Center for Policy & International Cooperation, Center for Training & Skills Development, and Center for Security Assurance & Research.

> "Global Response Center (GRC) evolves as the centralized threat coordination and analysis center in collaboration with its research and operational partners. Through its partnership with leading cyber security vendors, academic research networks and the governments, GRC provides the global community (especially the government sector) with visualization of emerging threats, near real-time aggregated threat information and a collaboration platform for helping governments to mitigate the threats through effective collaboration tools. Center for Policy & International Cooperation creates a platform for various stakeholders to come together and collaborate to share knowledge, skills, expertise, resources and technology for the benefit of its partner countries. Center for Training & Skills Development gives world-class training in the field of cybersecurity. IMPACT has developed its own specialized training program like forensics, malware analysis, and network investigations. Center for Security Assurance & Research enhances a government's cyber security posture through its offerings, namely the IMPACT Government Security Scorecard (IGSS) and CIRT-Lite. Both solutions were developed by IMPACT and its industry partners to bridge the need for governments to ramp up on their cyber security capabilities in light of the increasing number of cyber threats and managing governance, risk and compliance frameworks. This division also assists partner countries and members to improve their security posture through vulnerability assessment and penetration tests" (International Telecommunication Union, 2022).

Besides IMPACT, at the international level, the United Nations has a Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. This group realizes that harmful ICT activity against critical infrastructure that provides services domestically, regionally or globally has become more serious, especially malicious ICT activity affecting critical information infrastructure, infrastructure providing essential services to the public, the technical infrastructure essential to the general availability or integrity of the internet and health sector entities. Vulnerabilities in operational technology and in the interconnected computing devices, platforms, machines or objects that constitute the Internet of Things are not exploited for malicious purposes has become a serious challenge. So, this group has agreed on the voluntary, non-binding norms of responsible state behavior which can reduce risks to international peace, security and stability. The norms say that:

> *a.* "States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;

b. If there is an ICT incident, states should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment, and the nature and extent of the consequences;

c. States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;

d. States should consider to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;

e. States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions, protection and enjoyment of human rights on the internet, General Assembly resolutions on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;

f. States should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;

g. States should take appropriate measures to protect their critical infrastructure from ICT threats;

h. States should respond to appropriate requests for assistance by another state whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another state emanating from their territory, taking into account due regard for sovereignty;

i. States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;

j. States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

k. States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity" (United Nations, 2021).

Analysis

The Outer Space Treaty 1967, IMPACT, and GGE are three international or multilateral efforts to protect outer space. The Outer Space Treaty, as the oldest among those three, does not specifically mention cyberattack on space assets. It is because in 1967 the relations and interactions in cyber space were not massive in the past. This treaty discusses how to protect outer space under the general purpose which is exploring outer space for peaceful purposes. On the other hand, the newest initiatives, IMPACT and GGE, address cyber security on space assets issues. They can be analyzed using global governance theory as follows.

The initiative to create IMPACT and GGE above suits four points of global governance theory mentioned by Zürn in 2018. First, global governance refers to a pluralization of governance actors. This point is suitable with the fact that both IMPACT and GGE are multilateral initiatives. Since they are multilateral initiatives, there are plural actors in those initiatives. Second, global governance contains agreed norms and the exercise of authority. The agreed norms on responsible state's behavior in using ICT initiated by GGE suits this point. Third, the exercise of the authority and the declaration of the agreed norms is followed by a communicative act. The communicative act of responsible states behavior is shown by the continued discussion conducted by GGE on the topic of responsible state behavior in cyberspace in the context of international security. Moreover, the facilitation provided by IMPACT through its four centers also shows the communicative act after the initiation of IMPACT. Fourth, not all global governance arrangements need to be applied to the whole globe. GGE and IMPACT as global governance arrangements are only applied on the cybersecurity issue. IMPACT is more specific because it is applied only on the telecommunication technology which is based on the space sector.

IMPACT and GGE also match with three normative principles of global governance. First, it needs not only states but also social actors and individuals. It is clear from the areas of facilitation provided by IMPACT which need technical experts. GGE also consists of experts and it is clearly shown by the name of the group. Second, the purpose of global governance is the global common good. The common good behind the initiation of IMPACT and GGE is securing the global community from cyber threats. Third, if the global common good is the purpose, the national interest and individual authority are less preferred than the global interest. Through IMPACT and GGE's norms, countries should cooperate with each other to mitigate the impacts of cyber threats. Countries are also asked to exchange information, become transparent, and encourage responsible actions in using ICT technologies. Moreover, if there is an ICT related incident or a request from another country whose critical infrastructures are affected by malicious ICT conducts, a country should be cooperative in giving related information and other assistance needed to achieve international cybersecurity.

The analysis using variables as mentioned in the global governance theory above shows that global effort plays an important role in creating cybersecurity. Both GGE and IMPACT as multilateral initiatives involve national governments and experts to create norms, conduct research, provide training, and other efforts needed to create cybersecurity. These two initiatives show that global effort is important to create cyber security. GGE members realize that cybersecurity has a significant contribution to international security. The group agrees that an open, secure, stable, accessible, and peaceful ICT environment is essential for all and requires effective cooperation among countries to reduce risks to international peace and security (United Nations, 2021: 6). This statement shows that effective cooperation is a must to create cybersecurity. In particular in the space sector, IMPACT with its four centers provides an academic research network, platform to share knowledge, skills, expertise, resources, and technology, training programs, and security assurance for ITU members.

Moreover, the policy to secure the space sector from cyberattack should be focused on the protection of critical national infrastructure, a “bottom-up”, concerned with computer and network security, information security, and assurance. The policy should also be based on an agreed set of operational and strategic principles, with four objectives. First, to turn the intersection of space and cyberspace from a permissive, ungoverned environment into a self-governing network. Second, to raise the costs of use by illicit actors.Third, to encourage a comprehensive and inclusive understanding of cybersecurity across the user community. Fourth, to facilitate and assure legitimate use of the ICT infrastructure supported by space technologies (Livingstone & Lewis, 2016: 29).

The policy which should be based on an agreed set of operational and strategic principles is suitable for the global governance theory. Global governance theory mentions that the interaction among various actors creates interaction among different norms and rules. This interaction produces transnational and international regulations and other governance activities such as agenda setting, monitoring, adjudication, and enforcement (Zürn, 2018: 6). The agreed norms on responsible states behavior initiated by GGE is also the result of interaction among various actors. It is also a bottom-up initiative because it was produced based on the informal consultative meetings of the group with countries members and through a series of consultations held in collaboration with regional organizations (United Nations, 2021: 6).

According to Livingstone & Lewis (2016), an international coherent approach is needed because cybersecurity is a complex and internationalized problem. This approach requires various actors including nation-states, expert groups which have good technical capabilities, and individuals. The policy also needs to be coherent to create common good for all nations and people which is to create secure cyberspace. Space sector cannot be excluded from cyberspace because it is a vulnerable sector. It becomes more vulnerable in this modern era when all systems are interconnected through space technology, like satellite communication. Second, the space sector is vulnerable because a lot of modern systems, like the economy, military, navigation, and transportation, depend on space technology. As mentioned in the global governance theory, sovereign states agree to delegate some of their authority to the international government on special conditions. The special condition is when the global common good is needed in facing transnational issues including cyberattack.

Conclusion

The space sector is vulnerable to cyberattack, so it must be secured. In order to secure the space sector from cyberattack, a global effort is needed. The importance of global effort to secure the space sector from cyberattack is related to the fact that cyberattack is a transnational problem. The policy and governance to secure the space sector from cyberattack should include various actors among other nation states, expert groups, and individuals. Next, the policy should be based on the agreed set of operational and strategic principles which accommodate the interest of all actors involved. The policy aims to change the ungoverned cyber environment into a governed cyber network. By establishing a governed cyber network, it will be more difficult or costly for hackers to enter the network. Moreover, the establishment of a governed cyber network can give comprehensive and legitimate rules to all the network's members. Legitimate global governance can share rules and norms to be followed by all actors who play a certain role in space activities and give them legal authority to secure space activities from cyberattack.

The International Multilateral Partnership Against Cyber Threats (IMPACT) and Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security are two global efforts to create cybersecurity. IMPACT works in the telecommunication field which relies on the space sector. It provides practical actions needed to protect telecommunication technology from cyberattack. Meanwhile, GGE focuses on the norms that should be followed by countries in using ICT in order to create cybersecurity. Cybersecurity can contribute to international security and peace. GGE creates general norms on how to be responsible in using ICT and it can be applied also to the space sector.

This paper has analyzed two global efforts to create cybersecurity in the space sector. The analysis conducted using global governance theory shows that global efforts are important to create cybersecurity. This paper has given new insight on cybersecurity in the space sector by analyzing international efforts to combat cyberattack. This paper gives new knowledge to the existing research which focuses on the national policy to combat cyberattack and the political issues behind them. This paper also gives a new perspective by discussing cybersecurity in the space sector. Since information technology develops very fast, this topic is still important for research. The robust development of technology including cyber capabilities in the space sector is still important to be examined. It is because more advanced development will bring more opportunities and challenges. The dynamic between opportunity and challenges brought by cyber capabilities in the space sector can be investigated from some perspectives among others international security, regional or multilateral geopolitics, and human rights perspectives.

References

Cavelty, M. D., & Wenger, A. (2019). Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science. *Contemporary Security Policy*, 1-28. https://doi.org/10.1080/13523260.2019.1678855

Choucri, N., Madnick, S., & Ferwerda, J. (2014). Institutions for Cyber Security: International Responses and Global Imperatives. *Information Technology for Development*, No. 20 (2): 96-121. http://dx.doi.org/10.1080/02681102.2013.836699

Falco, G. (2018). The Vacuum of Space Cybersecurity. *AIAA SPACE Forum*, 1-14. https://doi.org/10.2514/6.2018-5275

International Telecommunication Union (ITU). (2022). *IMPACT: International Multilateral Partnership Against Cyber Threats*. Paris.

Kim, D. W., Choi, J. Y., & Han, K. H. (2020). Risk Management-Based Security Evaluation Model for Telemedicine Systems. *BMC Medical Informatics and Decision Making*, No. 20 (106): 1-14. https://doi.org/10.1186/s12911-020-01145-7

Kwok, A. (2021). *The Growing Threat of Cybercrime in the Space Domain*. Retrieved January 25, 2022, from https://www.eastasiaforum.org/2021/09/09/the-growing-threat-of-cybercrime-in-the-space-domain/

Li, Y., & Liu, Q. (2021). A Comprehensive Review Study of Cyber-attacks and Cyber Security; Emerging Trends and Recent Developments. *Energy Reports*, 1-11. https://doi.org/10.1016/j.egyr.2021.08.126

Livingstone, D., & Lewis, P. (2016). *Space, the Final Frontier for Cybersecurity?* London: Chatham House The Royal Institute of International Affairs.

Llansó, T., & Pearson, D. (2016). Achieving Space Mission Resilience to Cyberattack: Architectural Implications. *AIAA SPACE Forum*, 1-12. https://doi.org/10.2514/6.2016-5604

Nassau County: SPiN Security/ Police Information Network. What is Cyber Crime? Retrieved July 26, 2022 from https://www.wantagh.li/spin/what_is_cyber_crime.pdf

Plattard, S., & Smith, A. (2021). Reducing Vulnerabilities of Space Activities: A Call for Coordinated Leadership at the Global Level. *Journal of Space Safety Engineering*, 1-8. https://doi.org/10.1016/j.jsse.2021.08.003

Pražák, J. (2020). Dual-use Conundrum: Towards the Weaponization of Outer Space? *Acta Astronautica*, 187: 397-405. https://doi.org/10.1016/j.actaastro.2020.12.051

Rajagopalan, R. P., & Porras, D. A. (2015). Cyber Arms Race in Space: Exploring India's Next Steps. *ORF Issue Brief*, No. 113: 1-8.

Rajagopalan, R. P. (2019). Electronic and Cyber Warfare in Outer Space. *UNIDIR*, No. 3: 1-18.

Secure World Foundation (SWF). (2021). *Global Counter Space Capabilities.* Washington, DC.

Sheth, A., Boshale, S., & Kurupkar, F. (2021). Research Paper on Cyber Security. *Contemporary Research in India*, Special Issue: 246-251. https://www.researchgate.net/publication/352477690

United Nations (UN). (2002). *United Nations Treaties and Principles on Outer Space*. New York.

United Nations (UN). (2020). *Reducing Space Threats through Norms, Rules and Principles of Responsible Behaviors*. New York.

United Nations (UN). (2021). *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. New York.

Zhuo, M., et al. (2021). Survey on Security Issues of Routing and Anomaly Detection for Space Information Networks. *Nature*, 11(22261): 1-18. https://doi.org/10.1038/s41598-021-01638-z

Zürn, M. (2018). *A Theory of Global Governance: Authority, Legitimacy, and Contestation.* Oxford: Oxford University Press.

Zwilling, M., et al. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, 2-16. https://doi.org/10.1080/08874417.2020.1712269