Insignia Journal of International Relations
Edisi Khusus, Januari 2021, 32-47
P-ISSN: 2089-1962; E-ISSN: 2597-9868

Internet Governance Forum Analysis on Artificial Intelligence in Cyber Security

Faishal Ihsan
Department of International Relations, Universitas Jenderal Soedirman
Email: faishal.ihsan@gmail.com

Nuriyeni K. Bintarsari
Department of International Relations, Universitas Jenderal Soedirman
Email: nuriyeni.bintarsari@unsoed.ac.id

Abstract

This research examines the way the Internet Governance Forum (IGF) discusses Artificial Intelligence (AI) in the cyber security field. The discussion focuses on 2016, 2017 and 2018 periods. This article utilizes two concepts; cyber politics and internet governance. IGF believes that AI can be regulated collectively with solid frameworks and clear regulations. This in turn will maximize the security aspect of cyber security, which will be cheaper and more efficient in the era of internet freedom and technology rapid development. The paradox in AI lies in the breach of data privacy, which contradicts the goal of cyber security itself, i.e. to protect user's privacy and sensitive data away from any kind of unauthorized access. Framework cooperation based on mutual recognition of the importance of security within governments, private sectors, technical community and civil society can address privacy and cyber security concerns without undermining the open, free and secure nature of the internet. Hence, a stable and reliable cyber security focused on data protection will provide and preserve trust in cyberspace, and will eventually bring socioeconomic growth, innovation and education advancement.

Keywords: artificial intelligence, Internet Governance Forum, cyber security

Abstrak

Penelitian ini mengkaji bagaimana Internet Governance Forum (IGF) membahas Artificial Intelligence (AI) atau kecerdasan buatan di bidang keamanan siber. Pembahasan difokuskan pada periode 2016, 2017 dan 2018. Artikel ini menggunakan dua konsep; politik dunia maya (cyberpolitics) dan tata kelola internet (internet governance). IGF memandang bahwa AI dapat diatur secara kolektif melalui kerangka kerja yang kokoh dan regulasi yang jelas. Hal ini pada akhirnya akan memaksimalkan aspek keamanan siber yang semakin murah dan efisien di era kebebasan internet dengan perkembangan teknologi tumbuh pesat. Paradoks dalam AI terletak pada pelanggaran privasi data, yang bertentangan dengan tujuan keamanan dunia maya itu sendiri, yaitu untuk melindungi privasi pengguna dan data sensitif dari segala jenis akses yang tidak sah. Kerangka kerja sama ini didasarkan pada pengakuan timbal balik akan pentingnya keamanan di dalam pemerintah, sektor swasta, komunitas teknis, dan masyarakat sipil yang dapat mengatasi masalah privasi dan keamanan dunia maya tanpa merusak sifat internet yang terbuka, bebas, dan aman. Karenanya, keamanan siber yang stabil, andal dan berfokus pada perlindungan data akan memberikan dan memelihara kepercayaan masyarakat di dunia maya, dan pada akhirnya akan membawa pertumbuhan sosial ekonomi, inovasi, dan kemajuan pendidikan.

***Kata kunci**: Internet Governance Forum, keamanan siber, kecerdasan buatan*

INTRODUCTION

Internet, or Interconnected Network (Vedantu, 2020) is an electronic communication network which connect computer networks with computer facilities throughout the world (Merriam-Webster, 2019). As a result, computer, wire network, servers, satellite and

gadgets in a massive number are interconnected one another and allow information and transaction to travel through the internet, reviving rapid development in all sectors on the earth. The US Department of Defense is the first institution to initiate the implementaton of the internet as a strategic means of communication for exchanging data through Advanced Research Projects Agency Network (ARPANET) in 1960s (Featherly & Gregersen, 2016).

The penetration of internet use in the society will keep on increasing and show its impacts in all sectors of our life, such as education, sociocultural aspects, economic aspects, and national and international securities (Soewardi, 2013: 31). The data on estimated internet users show that in June 2020, out of around 7,796,949,710 inhabitants of the earth, almost two third of them or around 4,833,521,806 have accessed the internet. Asian population is ranked 1st in terms of the number of internet users, followed by Europeans and Americans, including North America, Caribbean and Latin (Internet World Stats, 2020). An example of how the internet changes the society is in the case of shopping activity, where in 2020 it is predicted that around two billions of the world population actively use the internet for shopping purpose (NodeGraph, 2020).

In October 2018, around five exabyte (5 Eb, or equal to five billion gigabyte (5,000,000,000 Gb) or 0.005 zettabyte) data pass through the internet, or around 40,000 movies each lasted for 2 hours (Sample, 2018). However, in 2020, it is estimated that the data transaction in the internet has reached a greater amount than in 2018 at 40,000 Exabyte (Eb) or equal to 40 trillion Gb or 40 Zb (Petrov, 2020). This number will keep on increasing as the number of internet users and variation of online activities such as online shopping, applied by no less than two billion population, increase (NodeGraph, 2020).

The formation of a massive communication link between internet users leads to a separate imaginary known as cyberspace (Soewardi, 2013: 31). As quoted from Businessdictionary.com, cyberspace is an imaginary, virtual and intangible form of internet activities—including human mind (the activity of thinking, imagining, and discussing). It is imaginary since it consists entirely of data manipulation and information, rather than a representation of physical forms. Cyberspace is an imaginary environment formed from interactions not only by humans, but also interactions between software and hardwar, internet service, technology and, of course, network (CSRC NIST, 2020).

The higher the internet users and technology advancement, the more urgent the need for a security system to be integrated into the internet-based data management in all services in institutions and companies is. This attempt is called cyber security, a set of commands used to protect various forms of penetration attempts into the system which aims at taking and damaging the data (NHS Digital, 2017: 2-3). This is based on the presence of new crimes in cyberspace as a form of proction attempts from cyber attacks; the attacks directed to the system—either organized or not based on material motives, destruction, data theft or political ones through the internet as its spreading media (Rouse, 2019).

Two forms of cyber attack are phishing and malware. Phishing is operated by disguising oneself as an institution or a person, generally through email (electronic mail), spreading links or media which contain commands to destroy or steal the target data (Rouse, 2019). Meanwhile, malware is a program or file, usually containing malicious programs such as viruses, trojan and spyware spread over the internet or

stayed in a computer and other devices (Rouse, 2020).

Cyber attack occurs all the time. Around 30,000 sites in the internet are attacked each day. Around 60 percent of companies around the world have been attacked at least once at a different intensity and extent (Bulao, 2020). However, some cases are too massive that the cases are publicly known.

In 2007, a hacker (a person who attempt to penetrate a system or a target) attacked the sites of Estonia parliament, ministries, banks, and media when their government rejected the Russia's proposal to relocate the Bronze Soldier Tallinn, a memorial monument of World War II owned by the Russia in Tallinn, current Estonia's capital (Smith, 2017: 2).

In 2008, the Royal Bank of Scotland's network system was hacked and this caused a leak of access to PIN information and replication of their ATM cards. In only 24 hours, 10 million US dollar had been withdrawn in 49 cities throughout the world, requiring the bank to ask for FBI's help for tracing the case (Henry, 2009).

The January 12, 2010 attack became one of cyber attack cases that attract the international world's attention. Google announced a massive attack to their infrastructure system in China. The investigation conducted by Google revealed that this attack was associated to the Chinese People's Liberation Army (PLA). This attack affected not only Google, but also other companies such as Adobe, Northrop Grumman, Juniper Networks and even Dow Chemical. As a result, the personal data and sensitive contents, including the Chinese human rights activists were leaked (Varma, 2010, p. 3), causing the US-Chinese diplomatic relations to heat. This attack was later known as the Operation Aurora (Matthews, 2019).

The three cases are merely a fragment of the many cyber attack cases with varied tensions occuring in the cyberspace. The attempt to secure a company's site and application requires substantial costs. The technology innovations bring with them great ease and cost efficiency in the security attempts. One of this innovations are artificial intelligence (AI).

AI is placed as a potential technology to facilitate a system security attempt, in both local and greater systems such as companies, areas and countries. The conventional system security such as the use of password is considered slow and ineffective. Thus, the presence of AI is deemed capable of improving the performance entirely and the cyber security system from many threats (Wirkuttis & Klein, 2017). It works not only at micro level, but also expands to include the formulation of national security and state policy making.

Back to cyber security issue, in International Relations (IR) it is a relatively new discipline and will continue to develop. Scientists still cannot formulate and answer the great question on the involvement of actors in the universal system which accomodate the rhythm and flow in cyber security (Nadella, 2018), legal regulations for the perpetrators, and bias between civil and military societies (including army) which is still debatable. For example, the perpetrator of stuxnet attack which attacked the military security system was launched by non-military group (Valeriano & Maness, 2018). The participation of various global actors gave birth to many forums aiming to articulate the framework of of cyberspace security. IGF or Internet Governance Forum is one of them, a discussion platform with a discussion forum agenda through a multi-stakeholder perspective (IGF, 2014).

Through IGF, experts, technicians, governments, private sectors and even civil groups from around the world gather at the same level to discuss,

exchangeinformation to achieve the same understanding to maximize the potential, minimize the risks and articulate the attempts to secure the cyberspace. For this reason, the writer through this article wish to analyze how IGF apply AI as a solution in cyber security which can then be a recommendation.

Research Method

In this research, the authors used qualitative method. Qualitative research is used to investigate the object naturally, where the researcher serves as the key instrument (Sugiyono, 2013). The source of data used as a reference are secondary data and were compiled from various form, comes from books (including e-book), journals, and articles in the websites. The authors downloaded the articles as one of source from the IGF site in which able be accessed freely and legally. The rest, other data collected discuss artificial intelligence, global governance, cyberspace and cyber security, and diplomacy in the artificial intelligence age. The forms of source used here called secondary data. Furthermore, the data are then used to support each other.

Theoretical Framework

Cyberpolitics Concept

The international world in cyberspace is increasingly interconnected without physical geographic boundaries and this gives birth to new dynamics in a great number; individuals have a new form of freedoms and greater participation in their own state and global political processes; the state has a medium to provide their social services, even new forms of influence and repression; the continued growth of internet users results in an increasingly complex international system and forms a new global society; the increasing international interactions by a variety of international organizations and actors bring about new forms of dynamics, including, for example, in the decision-making process (Choucri, 2013).

This form of communication eventually give births to the term cyberpolitics, which is defined as an attempt and form of communication which include such activities as who, gets what, when and how something can happen which takes the cyberspace medium as new arena in the international world (Indrawan, 2019). One of the motivations in cyberpolitics is, of course, protection from threats. For example, as the result of 9/11 attack, the US used the cyberspace as a medium for their propaganda attempt for the eradication of all terrorism movements through media to other entities and countries, in addition to using more coercive policies (Choucri, 2013).

The process of identifying threats colllectively will result in better preventive attempts in order to protect credential data and information (Rahmawati, 2017: 55-56). Deeper knowledge and understanding need to involve the thoughts through business, education and social interaction perspectives (Llorente, 2018: 3).

Internet Governance Concept in Global Governance

The keyword Global Governance (GG) means governing without government. In its management, it has no sovereign authority like a state. Almost all political processes and structures which exceed a state's boundaries, regardless of their scope, content and context, are included in the study of global governance (Dingwerth & Pattberg, 2006). During the 1990s internet development, some organizations attempted to play a role in the internet and created a "commone climate" which was then termed Internet Governance (IG) (Mueller, et al., 2007: 237).

IG consists of two words; internet and governance. Internet refers to a

system of global communication transition, using the Internet Protocol (IP) as the main technique of the communication system. Governance has something to do with the participation of governmental and non-governmental processes in a system (Kurbalija, 2014).

According to the Internet Governance Project, a site dealing with internet research and policy, IG refers to the rules, policies, standards and practices which coordinate and form a global cyberspace. When the internet connectivity produced a new form of innovative services, capability, sharing and cooperating systems, it also causes crimes, abuse, excessive surveillance, and even unprecedented social conflicts. IG is a process where its participatition solves the conflicts, problems and developing workable orders. IG itself is related to the digital world and applicable for anyone related to and involved in the internet world (Kurbalija, 2014).

An order through a territorial national institution might not capable of handling nor analyzing every dynamic occuring within the cyberspace. There is a need for a well-managed order, transnational cooperation between standard developers, network operator, service providers, internet users, government, and international organization. Keohane and Nye called this phenomenon as "transnational activity, making the society more sensitive to one another, hence influencing in policy coordination, where it will increase bureaucratical contacts between government sub-units, thus multilaterally, it will create a chance for international organizations to create significant roles in global politics (Ozgercin, & Weiss, 2014: 2), and therefore IG becomes a concept related to GG.

The state's role in IG, in addition to participating in international forums, is to apply policies limited to its boundaries, such as online gambling policies, national intellectual property protection, and content censor and internet access blocking. As reported by the Freedom House in 2013, China, Cuba and Iran were the three countries with lowest internet freedom ranks or it could be said that the governments of these three countries implemented tight regulations in cyberspace and internet access (Masters, 2014).

RESULT AND DISCUSSION

AI in Cyber Security and International Relations

Dr. Greg Corrado, a researcher and Director of Augmented Intelligence Research Google in the US defined AI as a collaboration of arts and sciences in a machine which generated a helpful intelligence that allowed this machine to have the ability to learn how to process, identify, clarify and previously given abstract data and commands efficiently (Pauwels, 2019: 1-6).

AI collects billions of either structured or unstructured data from various sources as the basis for identification and analysis of documents and threats, such suspicious behavior in a site, problematic IP addresses and dangerous dcouments shared through the internet. Furthermore, AI will make a curated recommendation to minimize or recover from the threats (IBM, 2019).

AI currently plays a role in international politics, particularly diplomation (Horowitz, 2018). The relations between AI and diplomacy can be explained in three points; AI as a topic of diplomacy (political policy agenda related to AI which is wider than economic, business and security oriented to democracy, human rights and ethics), AI as a tool of diplomacy (AI which supports the continuance and implementation of a diplomat's duties and their diplomacy functions) and AI as a factor which makes up the enviornment where the diplomacy is implemented (AI has massive potential

as a technology which determine the international pattern and order) (Bjola, 2018).

Competitions between countries have entered a new arena currently, where AI becomes the potential factor to make a country more powerful in their security and economy by considering the following four issues. First, having the right and adequate data. Mostly to perform the AI function, an algorithm require many sources of data to function well. Owning data are highly important to perform the national and international missions and policies which employ AI. Second, talents with AI ability. Countries need to make and prepare the humans with a good capacity in running AI. AI revolution comes from the AI run by highly skilled humans. Third, AI-oriented organization. Both organizations, institutions, and business sectors must be prepared for the transition to AI era and a country should support to make itself capable of being independent and competing with other countries. Fourth, public-private cooperation. Countries with their policies should cooperate with private sector to improve the innovations and talents in AI and technology fields (Katte, 2018).

Former Alphabet CEO, Eric Schmidt and former Vice Secretary of Defense of the US, Robert Orton Work equate competition between countries in the world in technology advancement and AI to US-Soviet Union during the Cold War. The difference is that the competition during this AI era is far more intense. The US and China are currently leading in AI. Currently, China leads in terms of research and journal publications on AI; more than 41,000 within 2011-2015 period. The US within the same time frame was at the second place by publishing more than 25,500 journals and articles on AI. Japan ranked 3rd (around 11,700) and England at the fourth place (10,100). According to Scopus, a database system containing abstracts and citations from various multiple disciplines, despite publishing the most, China's publications have lower quality than those from the US (Baker, 2017).

China in 2017 stated their amibition to be the global leader in AI and technology in 2030. One of the strategies is by consistently developing AI to make it more and more efficient, fast and stable. The advancement made by the US into the competition arena, especially in the studies of AI development and integration in the US's military security and armed force (Congressional Research Service, 2019). However, if a comparison is to be made, while China is currently in the first place for the largest internet users in the world (829 millions per December 2018) and has 1,011 AI companies in 2018, the US still ranks first in terms of their number of AI companies in the world, i.e. 2,028 in the same year (Holst, 2019). About 252 companies running their businesses in NLP in the US, compared to 92 China's companies. For semiconductor, processor and robotics, China is still below Japan and South Korea as the global leaders. This phenomenon leads to international cooperation and competition at the same time (Deloitte China, 2020: 14-15).

The cooperation in cyberspace needs new understanding, approach, development and management from multiple international actors. In their role, a state has a consideration for both their own and international greater goods (bilateral, regional and global). Meanwhile, for NGOs, despite the fact it is made by the state and has certain interest, yet the issue brought up remain as the organization views it. NGOs in the international world plays the of an actor who; consolidate other actors and apply new norms, pressure countries to participate in and conform with the collective understanding or agreement, maintain communication and one understanding, faciliate mediation

between conflicting actors and improve the prospect in solving a problem (Choucri, 2012).

On Internet Governance Forum (IGF)

IGF is an open dialogue platform attended by various scientific disciplines, entities and various countries gathered at one level to articulate and formulate potential utilization of, minimize problems with and secure the cyberspace. Villa Le Bocage Palais des Nations, City of Geneva, Switzerland is the home to the IGF secretariate office.

Through dialogue, the IGF has some influence on the attempt to improve cooperation and involvement of multi-stakeholders in assessing policies, fostering innovation, equity, multilingualism and multiculturalism, resilience, security and stability in internet governance from the participant countries (including developing and developed countries) and organizations and private companies. Nevertheless, IGF does not produce any policy nor agreement, rather all participants contribute to the formulation of thoughts and analysis of various policies and phenomena and generate a list of recommendations to be published and downloadable for free from their site (IGF, 2019).

IGF was born under the decision of the United Nations Secretary-General to make an advanced forum discussing such topics as issues requiring attention from the international community, such as internet use, local contents, spam and cyber security from the previous forum, Working Group of Internet Governance (WSIS) which was organized twice; Geneva, Switzerland (2003) and Tunis, Tunisia (2006).

All fundings for IGF activities are supported by voluntary contributors from various stakeholders, governments, including the host country. The IGF Secretariat manages the collected funds, and it is then managed by the United Nations Department of Economic and Social Affairs (UNDESA) with an adjustment to the procedures of the UN auditing policies and all details will be displayed in the audit report. Finland, Switzerland, the United States, the Netherlands, Germany, England, Japan and Portugal, are among the donor countries. The donors from private sectors include Tides Foundation, AT&T, Google, China Energy Fund Committee, Microsoft Corp and the Walt Disney Company (IGF, 2019).

IGF was held for the first time in 2006 in Athens, Greece. Each year, IGF has one big theme as its main focus of discussion which is different from the previous years. The writer tries to analyze IGF in 2016, 2017 and 2018 because in those three years AI began to develop.

IGF's Analysis of AI in Cyber Security

IGF in 2016

The 11th IGF meeting or IGF 11 was organized in Jalisco, Mexico on December 6-9, 2016 with the Mexican Government and the UN as its hosts. More than 2,000 delegates from 123 countries attended this forum.

Enabling Inclusive and Sustainable Growth was the major theme and it focused on how the internet could support and assisted the 2030 Agenda for Sustainable Development Goals (2030 SDGs) policy through a collective work after one year of being inaugurated.

Source: Assembly of European Region, 2020.

Figure 1.
Sustainable Development Goals

SDGs are an agenda formulated by the UN General Assembly in October 2015, a series of actions devoted to the humans, the planet and prosperity—including global reinforcement to face and alleviate poverty which has been a global problem. SDGs have 17 points and 169 targets to be achieved in thirty years focusing on three aspects; economic, social and environmental. These 17 points in the SDGs include; (1) no poverty, (2) zero hunger, (3) good health and well-being, (4) quality education, (5) gender equality, (6) clean water and sanitation, (7) affordable and clean energy, (8) decent work and economic growth, (9) industry, innovation and infrastructure, (10) reduced inequalities, (11) sustainable cities and communities, (12) responsible consumption and production, (13) climate action, (14) life below water, (15) life on land, (16) peace, justice and strong institutions, and (17) partnerships for the goals.

AI was not the main focus during IGF 11 discussion. As can be seen in the official document, AI is only mentioned three times in the opening section (p. 9) and discussion of IoT (pp. 64 and 130). According to IGF 11 in the opening, issues like standardization, interoperability, security and protection of personal data in cyber security require global cooperation and collaborative work. This was then discussed during the IGF 11 agenda. This was what was then discussed during IGF 11.

A tension occurs in cyber security, i.e. the conflict between the government and the wider community, especially activists and journalists on the use of encrypted data. Encryption is a technology that converts information or electronic signals into a secret code in a system of series of letters, numbers or symbols that cannot be understood or used using merely normal tools (Cambridge Dictionary, 2020). A paradox emerges when the needs confront the reality. For example, government requires data for the investigation of a case, yet the required data cannot be accessed without the owner's consent because it has been encrypted. This IGF 11 emphasizes the importance of establishing a framework regarding cyber security and national security, public security, corporate security, and personal security need to be identified. National security concerns threats to the wider community and the sovereignty of a country. Corporate security deals with infrastructure and intellectual property. In regard to communities such as NGOs, cyber security

is present for the defense of human rights and data confidentiality. Personal security includes personal identity, reputation and property. This will facilitate a more targeted and focused risk management. However, until the forum session is over, no policy can be used as a parameter. Security also includes physical support infrastructure that is stable and strong from various threats.

Seven points can be drawn from the official documents during IGF 11; (1) the government needs to understand its responsibility to secure internet infrastructure without having to resort to extreme measures such as closing internet access in certain areas, (2) clear regulations are needed to govern the government involvement in data access, (3) collective work between the government, private sector and state legal institutions, (4) despite the global internet domain, specific geographic approach (local and regional) is needed in considering cyber security practices, (5) educational incentives in using the internet properly are very necessary, especially in the school education curriculum system, (6) obsolete computers and other devices need regular upgrades, and (7) cyber security and internet governance initiatives should be built on the basis of democratic and multi-interest principles, ensuring that the participation of all actors as a whole are real and accountable.

IGF in 2017

The 12th IGF meeting or IGF 12 was held in Geneva, Switzerland on December 18-21, 2017 with the Swiss Government serving as the host and attended by more than 2000 delegates from more than 142 countries.

Shape Your Digital Future! is the main theme to continue the formulations from IGF 11 regarding collective work to achieve the 2030 Agenda for Sustainable Development. How AI affects the world's technology and its role in the dissemination and regulation of information, big data and IoT is a discussion in IGF 12. How AI affects the world's technology and its role in the dissemination and regulation of information, big data and IoT is discussed in IGF 12.

IGF 12 views that reliable and trustworthy cyber security is an open place for anyone for peace, stability, prosperity to avoid militarization and to ensure that the state does not make it a place for weaponry competition and this will stimulate IGF 12 growth in internet technology that helps escalate business and the economy and increase wealth. Using encryption for data security will create a sense of trust and security. All of these will be built into a framework between all entities; government, technicians, private sector and society. Poor cyber security threatens the growth of internet technology. Its vulnerability also increases users' distrust which will hinder growth, investment and innovation processes as well as efforts to recover and overcome threats.

Currently, the challenges in ensuring cyber security can be divided into four; infrastructure, trade, protection and law. The infrastructure aspect relates to the stability of the system in repelling attacks based on the quality of physical infrastructure which is consistently monitored and continuously developed. The second aspect is trade where the internet is used in the economic sector. Strong rules and frameworks ensure that all entities use the internet and its potentials to the fullest without neither fear nor objection in cross-border transactions and labor, thus creating a cyber security that supports business, transaction and financial functions and potentials.

Thirdly, data protection and alleviation of privacy issues must be the goal of all cyber security policies, practices

and regulations of law. According to the Privacy International, an organization engaged in information privacy advocacy from London, England, some countries in the world still do not have adequate frameworks and regulations. Large projects still need to protect sensitive and vital data such as population registration numbers, health registers and biometrics from data theft and leakage threats. The fourth aspect is law. A good cyber security contributes to the protection of human rights, democracy and law supremacy. However, certain security measures have the potential to become a serious threat to democratic values, particularly during the moment the government is tightening the internet control rules, such as easing encryption, blocking internet access and certain sites and weakening critical public campaigns and activist aspirations.

IGF 12 emphasizes that the discussion on AI will take a long time because it is a very broad subject. The fact that AI is seen as a machine that has initiative and is out of control is considered as the negative side of AI. On the positive side, the use of AI for developing countries, such as in the medical sector, will help them achieve the points in the 2030 Agenda.

The Organisation for Economic Co-operation and Development (OECD) through the IGF explains the steps to guide the development of AI collectively through the OECD AI Principles. This principle was created by around 50 members of various professionals and experts from various countries as well as leaders, academics, scientists, business people and civil activists. Through this principle, the OECD tries to apply standards for practical and flexible AI to keep up with innovation development. OECD complements these principles with standards in areas such as privacy, cyber security risk management and behavior in running a business.

The OECD AI Principles recommendations identify five points of complementary value-based principles for governing AI more reliably; (1) AI must benefit humans across the planet by promoting inclusive growth, sustainable development and prosperity, (2) AI systems must be designed in a way that respects the rule of law, human rights, democratic values and diversity and includes appropriate safeguards, for example, enabling human intervention where needed to ensure a fair society, (3) transparency and responsible disclosure should be present around AI systems to ensure that people understand the outcomes of the AI base and can challenge them, (4) AI systems should function in a strong, secure and safe manner throughout their life cycle and potential risks should be continuously assessed and managed, (5) organizations and individuals developing, using or operating AI systems must be responsible for their functions in accordance with the principles above.

IGF in 2018

The 13th IGF meeting or IGF 13 was held in Paris, France, on November 12-14, 2018 with the French Government and the UN Educational, Scientific and Cultural Organization (UNESCO) serving as its host, and it was attended by more than 3,000 delegates from 143 countries. Around 62 percent of the participants attended IGF activities for the first time. The Internet of Trust was the major theme at IGF 13 to continue to support the 2030 Agenda.

The writer finds that the theme this time was decided based on three issues, i.e. cyber security, trust and privacy security. This was different from IGFs 11 and 12 which have not escalated these three issues. Customer trust greatly determines how a company will continue to run in the future because both companies and institutions stored customer track record data and their behavior for service improvement

purposes (Menand, 2018). For this reason, the issue of trust in cyber security was raised in IGF 13.

Concerns will continue to arise in society about emerging technologies[1] which are associated with ethical and security issues. Understanding how AI algorithms in cyber security work becomes a technical solution in reducing the negative impact of the open and transparent nature of the internet by means of interoperability of regulations, policies and laws by various countries and global institutions. AI still requires a lot of transparency in its data processing to allow the wider community to understand how AI works and enable the public to participate in its development. The global community consciously use the values of norms and human rights as values and the basis for how emerging technologies are present and accepted by the public, and vice versa.

Emerging technologies refer to both newly present and under-development technologies (Winston & Strawn, 2020). Satya Nadella, Chief Executive Officer (CEO). Microsoft said that emerging technologies refer to three technologies; edge computing, artificial intelligence and mixed reality (Christou, 2019). Everyone can be involved to promote, adopt and adapt these emerging technologies through education, development, and training. Technical skills and public policies can reduce anxiety and skepticism over emerging technologies. Anticipatory steps need to be taken collectively by the government, business actors and mass media organizations using a comparison between the spreading media and the truthful news and utilizing the potential of social media to attract user participation in filtering biased and ambiguous content and information.

For example, does the term fake news actually means the news is invalid and unjustifiable or is it just political interests and opposition. Using AI, the government can adopt an effective and automated monitoring and content identification procedure. In partnership with partners, the government implements a digital literacy program in the curriculum to increase public digital awareness. The private sector provides transparent information to customers, filtering provocative advertisements and prioritizing the validity and authenticity of information. Representatives of civil society and NGOs evaluate laws and government regulations they deem inappropriate on political, ethical and human rights perspectives.

People with disabilities have a higher level of vulnerability to cyber security threats. More often than not, the internet, system devices, applications and computer hardware or smartphones are not designed to meet the needs of people with disabilities. Using AI, various applications such as Google with its Google Disability Support launches the Accessibility Help feature to help people with disabilities interact using smartphones and the internet. Other technology vendors are expected to follow Google's step.

Children, refugees, migrants and victims of human trafficking need strict data protection. Using blockchain—an algorithm on how large amounts of data form one space and how that data is shared and used (Gupta, 2017)—and AI will accelerate processes that support humanitarian efforts such as funding, aid distribution, applications for providing identity document assistance, data collection and verification to avoid duplication of data and marking locations. In the era when AI exists, the legal framework for refugee digital rights needs to be evaluated and adopted as quickly as possible by all strategic actors.

Biometric data is the privacy data inseparable from the track record of a person's life, including people with disabilities and refugees. The risk of being misused by irresponsible parties is very high. The safe and privacy-respecting use of biometrics requires collaboration between experts, practitioners and other actors with diverse backgrounds such as technicians, business people, governments, philosophers, gender experts and related individuals.

According to Marina Kaljurand, the chairman of GCSC, the government has a legal and ethical responsibility in ensuring cyber stability (safe, stable and equitable cyber access for all), policy initiatives, control of the proliferation of cyber weapons and commitment to the 2017 Call to Protect The Public Core of the Internet forum.

Developing a cyber-security strategy requires an approach from multiple fields of work and disciplinaries. Each stakeholder has their own responsibilities, and they must be complementary to each other. IGF 13 provides the best practices regarding the internet governance by implementing a collaborative model that promotes agility, transparency and trust in sharing valid information and promoting a collaborative framework to enhance initiatives. A public-private partnership governance should allow the government and Internet Service Providers (ISP) to gather resources and knowledge to handle various key aspects of cyber security by taking into account both socioeconomic and human rights aspects.

In IGF 13, the following eight recommendations for strategic roles in the internet governance era were formulated: (1) Stimulating innovation for the benefit of all; (2) Providing a way to highlight and disseminate information on innovation; (3) Avoiding risks and threats arising from the development of emerging technologies; (4) Ensuring that applicable business or government practices do not slow down either research nor development activities; (5) Being careful if AI is used as a method of making decisions; (6) Providing ethical guidance related to health, defense, cyber security and use of privacy; (7) Creating an inclusive technology climate, facilitating access to skills and knowledge; (8) Facilitating conversations between relevant stakeholders, including technology activists and users, to discuss ways to balance innovation and potential risks through policy formulation.

AI in IGFs 11, 12 and 13

According to IGF, AI refers to a series of theories, methodologies, approaches and practices in which computer systems are assigned tasks. These tasks involve not only solving mathematical or astronomical calculations, but also scanning and facial recognition, identifying and matching data with biometrics and so on. Knowing in detail and comprehensively how the AI process is quite impossible, making the public anxious and suspicious of AI.

The writer sees that the AI issues discussed in the IGF focuses on data privacy and encryption. To run AI, massive amounts of data are needed. These data are gathered and collected (blockchain) as fuel for AI. Data incompleteness leads AI to results that tend to be discriminatory, biased in dealing with gender and sexual problems, contradicting norms and ethics, and even defective, because it will process every data available to it.

However, the stored data reap paradox, because not all data can be used for all purposes. Cyber security is actually a series of systems and frameworks that serve to protect computer infrastructure and systems and personal data from being stolen by parties who use the data for harmful purposes, such as sabotage, phishing and theft of financial and personal health data. Much of this data is

traded for commercial purposes and is threatening or intimidating in nature, such as online money lending services by accessing all data on numbers stored on the borrower's smartphone as access to pressure borrowers to pay loans by calling these numbers (CNN Indonesia, 2020) and some even deliberately spreading out photos of borrowers without permission to intimidate them (Ratriani, 2019). Contradictory interests of government, if it requires sensitive data for solving certain criminal cases but the data cannot be accessed because it is encrypted such as biometric data.

Organizations, governments, companies, and individuals who develop AI must be responsible for the development, innovation and operation of it, including its transparency and education to users on how they make AI better with their data, ensuring their data is safe and ready for all risks. Because after all, public trust and strong interactions are built, bringing the domino effects from various sectors. People use the internet to do business, communicate and transact across borders. AI makes things, such as shipping goods and opening stores online, easier, better, and more efficient. Guaranteed security in cyber security stimulates better and more competitive socio-economic and political growth than during the first industrial era. Today, data is considered a superior force. Any actors capable of taking full control of data, hold greater power and potential than others.

Regulations on AI and cyber security must govern universally the framework for protecting infrastructure and data, economy, privacy, human rights and democracy (freedom). Government needs to understand that the problem of bias in AI and cyber security vulnerabilities is not the task of individuals or groups, rather it is a collective task for the government, organizations, companies, and individuals, including judges, civil rights activists and law activists. Government and AI activists must stimulate, guarantee and educate all actors from various lines.

CONCLUSION

IGFs 11, 12 and 13 view AI in cyber security as a strategic and paradoxical technology. It is strategic because using AI, activities would be more effective and efficient, even in decisions under critical situations, such as making decisions in war, recession or data collection on refugees. Using AI, attempts and frameworks in securing cyberspace are increasingly efficient, by identifying suspicious movements and behavior in the security system in an automated manner. The paradox in AI lies in the use of privacy data, which contradicts the purpose of cyber security, i.e. protecting privacy and sensitive data from unauthorized uses or without the user's knowledge. A collective framework between institutions, governments, companies, organizations and individuals makes AI more transparent and data protection and encryption would be more oriented to human rights, including freedom, democracy, non-discrimination, gender equality in security measures. This will allow the creation of a cyber security which is oriented towards stimulating socio-economic growth, public trust, advances in education and innovation.

REFERENCES

Bjola, Corneliu. (2019). "Diplomacy in the Age of Artificial Intelligence." Retreived from http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/ari98-2019-bjola-diplomacy-in-the-ageof-artificial-intelligence.

Bulao, Jacquelyn. (2020). "How Many Cyber Attacks Happen Per Day in 2020?" Retrieved from https://techjury.net/blog/howmany-cyber-attacks-perday/#gref.

Choucri, Nazli. (2013). "Cyberpolitics in international relations." Retrieved from http://cis.mit.edu/publications/newsletter/cyberpoliticsinternational-relations.

Christou, Luke. (2019, 25 Februari). "Satya Nadella: These are the technology trends set to "change the landscape of computing"." Retrieved from https://www.verdict.co.uk/satyanadella-mwc-technology-trends/.

Congressional Research Service. (2019). "Artificial Intelligence and National Security." Retrieved from https://fas.org/sgp/crs/natsec/R45178.pdf.

NHS Digital. (2017). "An Introduction to Cyber Security." Retrieved from https://www.digitalsocialcare.co.uk/latest-guidance/an-introduction-to-cyber-security/.

Deloitte China. (2019). "Global Artificial Intelligence Industry White Paper." Retrieved from https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/technology-mediatelecommunications/deloitte-cntmt-ai-report-en-190927.pdf.

Dingwerth, Klaus & Pattberg, Philipp. (2006). "Global Governance as a Perspective on World Politics." Retrieved from https://www.researchgate.net/publication/260121396_Global_Governance_as_a_Perspective_on_World_Politics.

Featherly, Kevin & Gregersen, Eric. (2016). "Arpanet: United States Defense Program." Retrieved from https://www.britannica.com/topic/ARPANET/.

Horowitz, Michael C. (2018). Artificial Intelligence, International Competition, and the Balance of Power. *Texas National Security Review, 1*(3), 36-57.

IBM. (2019). "AI for cyber security." Retrieved from https://www.ibm.com/security/artificial-intelligence.

IGF. (2014). "The Global Multistakeholder Forum for Dialogue on Internet Governance Issues." Retrieved from http://intgovforum.org/multilingual.

IGF. (2016). "Best Practice Forums (BPF) Cybersecurity." Retrieved from https://www.intgovforum.org/multilingual/content/bpf-cybersecurity-2016.

IGF. (2017). "Best Practice Forums (BPF) Cybersecurity." Retrieved from https://www.intgovforum.org/multilingual/content/bpfcybersecurity-2017.

IGF. (2018). "Best Practice Forums (BPF)." Retrieved from https://www.intgovforum.org/multilingual/content/bpf-cybersecurity-2018.

Internet World Stats. (2020). World Internet Usage And Population Statistics 2020 Year-Q2 Estimates. Retrieved from https://www.internetworldstats.com/stats.html.

Katte, Abhijeet. (2018, 16 August). "Artificial Intelligence is a key to future international relations dynamics." Retrieved from https://analyticsindiamag.com/artificial-intelligence-is-a-key-tofuture-international-relations-dynamics/.

Kurbalija, Jovan. (2014). "An Introduction to Internet Governance." Retrieved from http://www.diplomacy.edu/.

Llorente, R. V. (2018). "A Digital Geneva Convention? The Role of the Private Sector in cyber security." Retrieved from

http://www.lse.ac.uk/ideas/publications/updates/cyber security

Masters, Jonathan. (2014, 23 April). "What Is Internet Governance?" Retrieved from https://www.cfr.org/backgrounder/what-internet-governance.

Matthews, T. (2019, 8 Januari). "Operation Aurora – 2010's Major Breach by Chinese Hackers." Retrieved from https://www.exabeam.com/information-security/operationaurora/.

Mueller, Milton., Mathiason, John., Klein, Hans. (2007). The Internet and Global Governance: Principles and Norms for a New Regime. *Global Governance Journal, 13*(2), 237-254.

Nadella, Satya. (2018). *Hit Refresh.* Yogyakarta: Penerbit Bentang.

Smith, B. (2017). "Transcript of Keynote Address at the RSA Conference 2017 - The Need for a Digital Geneva Convention." *Microsoft Corporation*, 1–15. Retrieved from https://mscorpmedia.azureedge.net/mscorpmedia/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf.

Ozgercin, Kevin V., & Weiss, Thomas G. (2014). The Evolution of Global Governance. Retrieved from https://www.eolss.net/SampleChapters/C14/E1-35-03-04.pdf.

Pauwels, Eleonore. (2019). *The New Geopolitics of Converging Risks: The UN and Prevention in the Era of AI.* United Nations University Centre for Policy Research. Retrieved from https://collections.unu.edu/eserv/UNU:7308/PauwelsAIGeopolitics.pdf.

Petrov, Christo. (2020, September). 25+ Impressive Big Data Statistics for 2020. Accessed from https://techjury.net/blog/bigdata-statistics/#gref.

Rahmawati, I. (2017). Analisis Manajemen Resiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defense. *Jurnal Pertahanan & Bela Negara, 7*(2), 51-66.

Rouse, M. (2020). Malware (malicious software). Retrieved from https://searchsecurity.techtarget.com/definition/malware.

Rouse, M. (2019). Phishing. Retrieved from https://searchsecurity.techtarget.com/definition/phishing.

Sample, Ian. (2018). What is the internet? 13 key questions answered. Retrieved from https://www.theguardian.com/technology/2018/oct/22/what-isthe-internet-13-key-questionsanswered/.

Soewardi, I. A. (2013, Maret). Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia. Retrieved from Media Informasi Ditjen Pothan Kemhan: https://www.kemhan.go.id/pothan/2014/04/19/perlunyapembangunan-sistempertahanan-siber-cyber-defenseyang-tangguh-bagi-indonesia.html.

Sugiyono. (2013). *Memahami Penelitian Kualitatif.* Bandung: Alfabeta**.**

Valeriano, Brandon, & Maness, Ryan. (2018). International relations theory and cyber security: Threats, conflicts, and ethics in an emergent domain. Retrieved from https://www.researchgate.net/publication/326845990_International_relations_theory_and_cyber_security_Threats_conflicts_and_ethics_in_an_emergent_domain.

Winston & Strawn. (2020). What is the Definition of Emerging Technology?. Retrieved from https://www.winston.com/en/legal-glossary/emergingtechnology.html.

Wirkuttis, Nadine & Klein, Hadas. (2017). Artificial Intelligence in cyber security. *Cyber, Intelligence, and Security, 1*(1), 103-119.