asean studies program

Discussion Report Talking ASEAN Webinar on

Cybersecurity and Geopolitical Crisis: Lessons Learned from Taiwan

Jakarta, November 17th 2022

Introduction

The Habibie Center (THC) convened the 6th Talking ASEAN Webinar on 17 November 2022. Entitled **"Cybersecurity and Geopolitical Crisis: Lessons Learned from Taiwan,"** the webinar invited three speakers—**Bart Hogeveen** (Head of Cyber Capacity Building – International Cyber Policy Centre, Australia Strategic Policy Institute), **Ardi Sutedja** (Chairman, Indonesia Cyber Security Forum (ICSF)), and **Tzeng Yisuo** (Assistant Research Fellow, Institute for National Defense and Security Research, Taiwan)—and was moderated by **Mabda Haerunnisa Fajrilla Sidiq** (Researcher of ASEAN Studies Program, The Habibie Center).

The objectives of the webinar were to: (a) assess the development of the cyber dimension within the global security discourse; (b) discuss the cyber security dimension within the geopolitical crisis in the Indo-Pacific; and (c) gain insight into Taiwan's measures and policies in managing cyber security and the risks resulted from strategic cyber competition in the region.

This discussion report summarized the key points of each speaker, as well as the following questions and answers session.

PRESENTATION FROM THE PANELIST

Tzeng Yisuo
(Assistant Research Fellow,
Institute for National Defense and
Security Research, Taiwan)

Dr. Yisuo Tzeng focused on how Taiwan drew lessons from the Ukraine war and Chinese military exercises surrounding Taiwan in August 2022. These two events served as enabling accelerators for Taiwan to get ready to enhance digital resilience in coping with the situation. To be more specific, Dr. Tzeng, addressed the relationship between geopolitical crisis and cyber security in Taiwan, and the measures taken by Taiwan to address the geopolitical risk to cyber security.

Dr. Tzeng highlighted three takeaways from the Russia-Ukraine war. The first one was the importance of secure backup in space due to numerous attacks on communication satellites. The second takeaway was the importance of sustainable internet due to physical damage to the backbone of the internet system, power supply outage, and the possibility of underseas line sabotage. He then mentioned that maintaining sustainable internet was a difficult task, especially in relation to power supply in the case of the Russia-Ukraine war. In the case of Taiwan, the undersea line was critical for communication. Dr. Tzeng indicated that China had a digital experiment submarine using a robot that could damage the Taiwanese sea cable line. Lastly, there was also a need to ask for help from the international community. For instance, Ukraine requested the Internet Corporation for Assigned Names and Numbers (ICANN) to remove the Russia LTD from the top-level domain which failed and it actually was not a good move. Taiwan had been worried that China might do the same and might try to control the chip export to Russia in the future. Moreover, Russia had started to face a shortage of advanced chips and it could create serious impacts on battlefield management. A similar consequence would also be applicable to China since the US had also initiated high-tech cooperation with Taiwan.

Taiwan had learned that a resilient internet was an important aspect in order to survive, considering constant cyber-attacks, including attacks on the political infrastructure. The most concerning attack was deep-seated in futuristic advanced persistent threat (APT). Thus, Taiwan would always expect that a substantial attack would happen. Moreover, Taiwan would have to be ready with safe storage to recover the internet system and have backup data in order to run the system normally. The backup system, including the hardware, had to be in a secure physical space, for example in a cave or hardened physical shelter. Taiwan had been taking this effort seriously since the Russia-Ukraine war and sped up the preparation. In Taiwan, the strategic thinking went along the lines that cyber security should be considered as a national security issue and Taiwan had been adopting a whole government approach to cope with malicious cyber-attacks. However, those preparations still would not be sufficient and efficient to tackle digital problems.

Furthermore, Taiwan was also aware that Border Gateway Protocol (BGP) was also an issue. Taiwan had established the Ministry of Digital Development and Minister Audrey Tang had been advocating for a heterogeneous network to maximize Taiwan's digital resilience. Regarding the backup system and the data, Taiwan learned from Ukraine to have a cloud data center located abroad. Even though there were still political and technical issues to be resolved, Taiwan believed that they would find solutions soon.

With regard to the lessons learned for Taiwan, there had been many discussions on costly undersea cable protection. In order to achieve cyber resilience, Taiwan would have to equip itself with an expensive system and repair undersea cables. Thus, Taiwan had been trying to build up the capability to repair undersea cables by itself. Furthermore, Taiwan also had four reception stations on the land and tried to enhance the physical protection from potential malicious sabotage by spies called fifth column troops. Besides, Taiwan had several rehearsals and employ tabletop exercises first to identify gaps and problems. Then, the government would figure out a way to fix it and put it to test the live exercise. For a bigger scope of the clean network, Taiwan joined the initiative of the US clean network. Thus, more undersea cables were connected in Taiwan compared to Hongkong since Hongkong had been under the tight control of the national security act.

To sum up, resilience matters but it cannot be built overnight. In addition, it is also important to have a high availability storage of satellite communication for strategic communication to the outside world and to the people.

PRESENTATION FROM THE PANELIST

Bart Hogeveen
(Head of Cyber Capacity Building - International Cyber Policy Centre, Australia Strategic Policy Institute)

Mr. Hogeveen touched upon three particular issues, namely reflection on the current security environment and the roles of cyber, the current International settings in governing cyberspace at the level of the United Nations (UN), and the development of cyber security in the world. Before he started his presentation, Mr. Hogeveen congratulated President Jokowi, as a chair of G20, for his achievement in getting a communique. G20 leaders agreed to tackle the devastating effect of COVID-19 on the global economy, society, and political security. The G20 summit also touched on several issues on climate change, poverty reduction, SDGs, and also Russia-Ukraine war that had adversely impacted the global economy and how the G20 leaders subscribed and deployed the strongest possible terms to the aggression by Russia against Ukraine. Furthermore, the communique was essential to uphold international law and a multilateral system that would balance and bind together developing, emerging, and developed economies.

In the absence of a proper structure within the ASEAN framework, there had been an annual forum called the ASEAN Ministerial Conference of Cyber Security. This forum was initiated in 2018 under Singapore Chairmanship. The latest event was held in October 2022 and it discussed issues on strengthening the rules of space and multilateral order in cyberspace as a collective responsibility of all the ASEAN leaders and all the ASEAN ministers responsible for cyber security. They also discussed the rules of the road which required deliberate and consistent effort. Mr. Hogeveen believed that this initiative was an important marker for ASEAN on how it would stand on cyber security and how that would relate to both economic security and international peace and security issues.

Regarding the cyber security environment, recent trends of the international security climate indicated that cyber-security was not in good condition. There had been a growing incident of cyber-attacks from 2015 onward by state-sponsored cyber operations. Moreover, there were more than 100 significant state-sponsored cyber operations in 2022. These attacks were based on the understanding that if states could exploit vulnerabilities in the system, it could compromise the integrity of the system. As a result, it would affect our sense of security, including how businesses and individuals would use the digital system or digital economy.

Looking from the context of international peace and security, cyber could be seen based on its usage, such as: (1) cyber was used for espionage purposes within certain boundaries; (2) there was evidence that cyber was used as part of military operations in the Middle East; (3) the degradation of the communication network for ISIS in Syria; and (4) there were stand-alone cyber operations where states were involved in very particular niche operations either to stop another stack from developing certain capabilities or for financial gain. Moreover, it was also important to take note of the domestic space, given that all countries had

been in the business of developing national cyber security capabilities, done by security forces, military, or police intelligence services. Generally, cyber was acknowledged as a part of national defense, national economy, and broader strategic outlook.

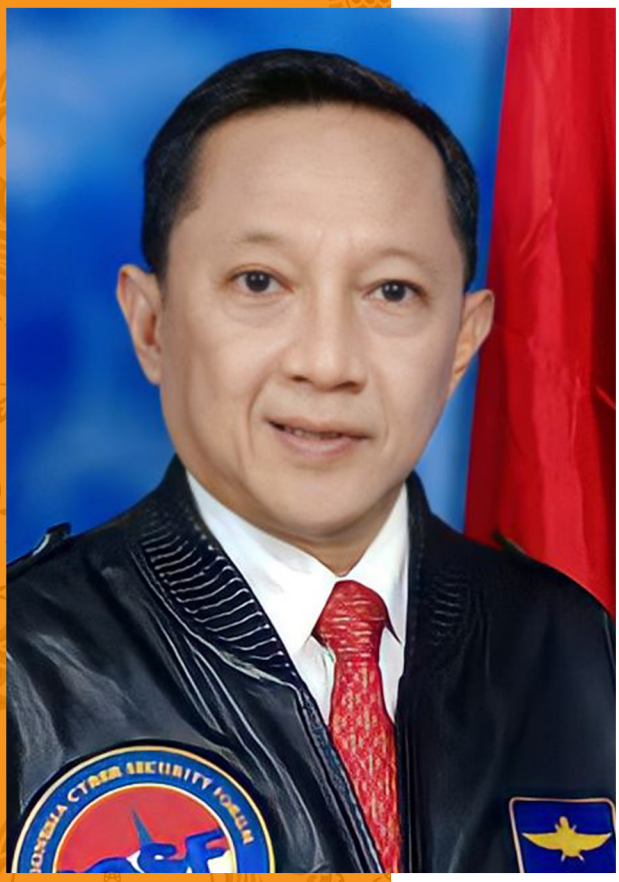
Furthermore, there were several efforts undertaken for the last 20 years at the UN. The Russian Federation put the cyber topic on the agenda of the UN General Assembly in 1998 and both the US and Russia were acknowledged to have established their first cyber unit for military operations in the same year. Over the years, the UN member states managed to agree and disagree on many things regarding cyber issues. However, there were many important things to note. From 2004 onwards, the UN member states had agreed on four main items. Firstly, international law would be applicable in cyberspace, a principle generally acknowledged by all UN member states, including the five permanent members of the UN Security Council. This principle referred to the UN Charter and would be applied to all countries dealing with cyberspace. Secondly, there was an agreement called norms of responsible state behavior in cyberspace. There were eleven voluntary norms that described what states should and should not be doing in cyberspace. One of them stated that a country should be involved in international cooperation and debates at the diplomatic level in terms of police cooperation, search cooperation, and computer emergency response teams (CERTs) of different nations. The most contentious issue was the issue of attribution, holding another state responsible for cyber accidents, and the norms said that any party should not jump to a conclusion.

Besides, there were also two really important things to highlight. Every state had a responsibility that their territory should not be misused for international wrongful action. It meant that states should exert governance of what had happened in their internet domain at a national level. There was a positive duty for a country to protect its critical infrastructure in their countries because it was crucial when an incident occur somewhere else, their infrastructure would not be inadvertently affected by the incident. In the context of international peace and security, the attacker could distinguish between legitimate targets and non-legitimate targets.

Furthermore, two other items called an agreement to engage in confidence-building measures, including sharing policies, conducting dialogues, and having a point of contact directory. It was also essential to have a collective and global effort to support nations in building cyber security and cyber capabilities. Those initiatives had been in the works for almost 20 years and it had been reaffirmed recently. Moreover, there had been a few attempts to differentiate the initiatives from the original agreements. The debates had been ongoing in terms of how to make some of the agreements more specific and tangible for states to operationalize, implement and demonstrate how they would comply with and observe these current agreements.

Mr. Hogeveen also highlighted how this issue would be dealt with in the Indo-Pacific. It was striking to see that all the nations have developed certain cyber capabilities within government and the security services of government. For example, countries like Australia, the US, China, and India established defense cyber agencies. Japan announced the establishment of a cyber-self-defense force unit in 2022, Singapore established a digital and intelligence service with a clear role in intelligence and cyber defense of the nation, Malaysia established its cyber command and a cyber warfare regiment in 2019, the Armed Forces of the Philippines established a cyber group, Vietnam had a cyber operations command, and Indonesia had the military cyber unit. These developments signified that all countries had capabilities within their security forces. In some countries, the militaries had started to conceptualize how they would use cyber in national defense, both in interstate and domestic contexts. Mr. Hogeveen saw that most global developments where national cyber capabilities were being used for internal purposes, including content control and interference with the networks and surveillance. In other words, in a relatively short period, cyber security has been leveled up from the local level to the international level and recognized as a domain of international peace and security in geopolitics. In terms of diplomatic statements, there was still a significant diversion between what states said and what they did in practice. For instance, the non-alignment movement was still calling for the demilitarization of cyberspace and did not acknowledge that cyberspace was a domain for political and military activities.

PRESENTATION FROM THE PANELIST



Ardi Sutedja
(Chairman, Indonesia Cyber Security Forum (ICSF))

Mr. Ardi Sutedja started his presentation by highlighting the rapid changes in geopolitics and how they have influenced global decisions that created disruptions towards cyber security. He then described the cognitive domain in cyberspace as one of the most disturbing aspects of cyber disruption that could affect both government and consumers' minds in the long run. This disruption would influence how people would act and respond. Furthermore, echoing the previous speakers, Mr. Sutedja stated that cyber disruption had become a national security matter because it would be related to human life and business continuity, including everything that people do daily.

The word 'cyber' had been highly correlated with everything digitized. However, understanding the matter would require a helicopter view and a good perspective. The historical factor would be one of the factors in understanding how technology evolved, the future technology that would come into the pipeline, and the weaknesses of the technology. The second factor would be geopolitical. Indonesia had been a part of global geopolitical influences and had been experiencing disruptions, not only in political matters but also in technology selection. There are many technologies available in the world but only a few had been available in Indonesia. Moreover, the development of technology in Indonesia not only came from the technology companies but also from the state actors to push the use of technology.

Cyber disruptions had been a real source of threats and risks, however, people have never been prepared to face the risk of cyber disruptions. Thus, it would be challenging if we faced more extensive cyber disruptions in the future. In the case of Indonesia, the government had been aware of the threats and the risk, however, Indonesia still had various issues in catching up with other neighbors, such as Singapore, Taiwan, and Australia. Indonesia recently established the first cyber security agency called National Cyber and Crypto Agency (Badan Siber dan Sandi Negara/ BSSN) in 2017. Besides, the government had been trying to catch up by discussing cyber security in bilateral and multilateral settings. These efforts aimed to enhance the country's knowledge in overcoming cyber disruptions.

Concerning cyber warfare as the sixth domain, the cognitive dimension would be important to be discussed because three layers of aspects were being targeted. The hardware and software aspects were often discussed in many fora, however, the discussions on the cognitive aspect (users and personas) were still lacking. In fact, this aspect had affected many people in the US, Europe, and Indonesia. Indonesia was also prone to various methods of attack and hacking and had been experiencing the same form of attacks that occurred globally.

Mr. Sutedja continued his presentation by explaining the global political distrust as the root cause of cyber disruption that had increased after the conflicts in Eastern Europe.

Moreover, global conflict and tensions outside Europe remained high, contributing to cyber disruptions, for instance, the China-Taiwan-US and the semiconductor crisis that disrupted the global value chain of electronic devices. The last thing that also caused the cyber disruption was the emergence of new state actors and players post the Cold War era, both in the real world and virtually. For many years, countries like the US, China, Russia, Israel, Iran, the UK, NATO, and its allies had been known as the leading global actors. Nevertheless, all these countries were also trying to survive and manage the cyber threats they faced.

Mr. Sutedja also mentioned social engineering as a critical aspect of capturing cognitive disruption. Thomas Sowell defined social engineering as the art of replacing what would work with what would sound good. The old paraphrase had currently been used to deceive people using technology through content engineering. In the long run, people would be led to believe something that they were not supposed to believe. Human beings became the weakest link in everything in the world. Thus, improving human capability should be the priority. In this context, Indonesia had been experiencing a shortage of good talents in cyber security. This condition forced Indonesia to catch up with countries already in an advanced state of human capital development.

There are different aspects of social engineering techniques, and it would be important to understand the terms used to describe the techniques of social engineering. Mr. Sutedja believed that social engineering in the cognitive dimension was dangerous and disruptive because it could alter people's minds, beliefs, sensitivity, and mindsets. Social engineering was everywhere and came in various forms. It has already entered the policy-making circles within the government, physical domain, and almost everything people do has been penetrated by social engineering. In other words, no single person or institution is immune to social engineering. For instance, all the big 500 companies have gone through these experiences in various forms that caused financial loss. Social engineering had also crippled economies worldwide and made it a national security issue.

Furthermore, the impact of social engineering consisted of four main aspects, namely physical, psychological, financial impacts, and unknown vulnerabilities. For example, a different data breach happened in Indonesia almost every month that opened the weakness of our cyber defense. The main objectives of cyber-attack were to obtain all personally identifiable information (PII) from computer systems, cell phones, consumer gadgets, and other things used to communicate among families and within the workplace. This data could be extracted to identify the activities and weaknesses of society.

Subsequently, Mr. Sutedja argued that cyber disruptions could not be abolished through regulations. For instance, Western countries

still became victims of cyber disruptions even though they had implemented very strict rules and regulations. Thus, the global community should look elsewhere for weaknesses and find collaborative ways to close the gap. Moreover, cyber disruption was never in a single form. Cyber-attacks had become increasingly sophisticated and require more time and effort to mitigate.

Mr. Sutedja then explained the cyber security disruption cycle. Cyber-attack started with espionage. It occurred when hackers are trying to infiltrate any network. It also applied to social engineering by looking for weaknesses to penetrate and study the target. After that, they would influence the target after gathering all the information. Thus, to mitigate cyber risk, it would be vital to identify the weaknesses, the key players, the insiders, criminal organizations, and the hackers.

There is also a new approach called "zero trust", which would be embedded in every individual. The concept of zero trust is a long-forgotten mindset that has actually been taught for many years by our parents. Unfortunately, due to the development of technology, people tend to forget about the basic teaching of not trusting strangers. People used to build fences around our homes to prevent thieves or bad people from trespassing our houses. Ironically, following the development of technology, the mindset had changed. Recently, the thief or bad people have already been inside our houses through technology. Handphones, setup boxes, and other technological appliances used daily could be weaponized.

Mr. Sutedja ended his presentation by touching upon the cyber-attack response management. It is important to emphasize to the victims that no one would judge them and they should focus more on how to respond given the circumstances. It is also an important task for the computer emergency responses team to respond to the incidents and are equipped with the full team. Overcoming cyber-attacks is not only a task for computer or technology experts, it would require multidisciplinary expertise. Mr. Sutedja also underlined that tackling global challenges and cyber-attacks would be a collective responsibility. It should not be the sole responsibility of the government, but it would also be the responsibility of the private sector, experts, and the communities in order to find a solution that can manage the crisis.

QUESTION AND ANSWER SESSION

Questions

Marina (The Habibie Center):

Question for Mr. Sutedja, in Indonesia's context, which still needs to continue improving its cyber security, what are key elements that Indonesia should improve to achieve cyber resilience as preventive and mitigation efforts?

Responses

Ardi Sutedja (Chairman, Indonesia Cyber Security Forum):

Based on his experience working with the Ministry of Communication and Information Technology, human talent development was one aspect that would need improvement. This aspect should be done and planned carefully because catching up involves the development of proper human talent to manage potential vulnerabilities.

The next aspect that would need to be addressed was understanding various weaknesses, more complex threats, and the influx of new technology to the market. For instance, many technologies were not indigenous to Indonesia and were created by third parties that were still technically unknown. Additionally, the existence of regulations behind the development and growth of technology could become one aspect where global leaders could collaborate to get everybody on the same page. However, the challenges would be difficult because of generation and knowledge gaps.

Bart Hogeveen (Head of Cyber Capacity Building – International Cyber Policy Centre, Australia Strategic Policy Institute):

Mr. Hogeveen highlighted the fact that not a single country in ASEAN was starting from scratch, some countries already had decent capabilities and existing infrastructure. In a country like Indonesia, there were debates and discussions on cyber security among non-governmental communities that would not be found in the reference of government communique or policy documents. It showed the resilience of the community at large.

In addition, all Southeast Asia member states had national cyber security centers, especially Indonesia. Over the last couple of years, we had seen a few national computer emergency response teams (CERT) being merged into national cyber security centers, including Vietnam CERT and Malaysia CERT. After they transformed into national cyber security centers, their roles signified from the initial core role of dealing with incidents that affected government networks to be an institution that would give advice to businesses, companies, and communities across economies. Indeed, some parts of the world struggled in the early stages. That happened also in Indonesia

and Australia, where everything was concentrated in the capital city and struggling to reach small and medium enterprises (SMEs). It was still challenging to make SMEs aware of their vulnerabilities and risks, especially to give them real advice to improve their security without telling them to go to a costly cybersecurity company to solve their issues. Mr. Hogeveen identified them as the challenges worldwide and required regional cooperation within ASEAN and its neighborhood. The big question for Indonesia would be, whether Indonesia had a proper understanding of what was really happening. Some rumors did not give us a real image of what was happening. Thus, it would be crucial to get a proper understanding of what was happening and to what extent businesses would be affected, the trends and what were the real issues that we were confronted with.

Questions

Herawati (The Habibie Center):

Question for Dr. Yisuo Tzeng, how has Taiwan engaged the private sector in ensuring cyber resilience? And how has it benefited from its domestic ICT companies?

Responses

Dr. Yisuo Tzeng (Assistant Research Fellow, Institute for National Defense and Security Research, Taiwan):

Since 2014, Taiwan has had a national priority to focus on developing the cyber security industry, not just for our nation's security concern but also to develop another automation of high-tech industry. At first, there were huge barriers in other countries, but then all private sectors figured out the ways. Many SMEs had no experience in reporting to the incident report center. However, attacks on social engineering were frequent, and almost all workers from the private sector, government, and think tanks were highly targeted. In this matter, individual training or education would be the key to cyber security, particularly in prevention and for precaution. This effort would be the best way to mitigate the damage and it had become the consensus in Taiwan. At first, the Taiwanese government raised awareness regarding cyber-attacks, security threats, and disinformation threats from China. Dr. Tzeng argued that Taiwan was well noted not only for strong cyber-attacks but also for the misinformation campaign from China.

Questions

Fara (Audience from YouTube):

How do you see the role of the social media industry or social media companies influencing the global cybersecurity landscape?

Responses

Bart Hogeveen (Head of Cyber Capacity Building – International Cyber Policy Centre, Australia Strategic Policy Institute):

The question showed the tendency of how the West had been looking at the problem from a technical lens. In contrast, other countries looked at it more comprehensively through the lens of ICT security, not cyber or information security. For the last couple of years, we had seen a convergence of perspectives on the whole idea of the misuse of the information environment. For example, the cognitive element was seen as a problem and a potential threat to cohesion in our society. The things being said and pushed by outside forces and sometimes orchestrated or industrialized on our social media platforms become a real concern that had been widely acknowledged. However, the global community would still need to find the right balance between freedom of expression and the responsibility of technology companies, particularly social media platforms. It would also be crucial to determine the company's responsibilities and what the government could do to manage the matters.

An interesting phenomenon occurred after the Christchurch attack in New Zealand, where an extreme-right shooter attacked a few mosques in New Zealand which was live-streamed on one of the social media platforms. That was one of those trigger moments where everyone realized that we could not stay in this usual conundrum of saying that the social media companies were responsible for those attacks. The government did not touch the area. In fact, it has real-life effects and the government should do something about it. Thus, the G20 or the G7 at the time agreed that social media companies and governments would need to work together to ensure that those kinds of extremely bad things would not happen again. It also led to a recognition that some of the concerns in countries like Indonesia, Malaysia, and Vietnam had been taken more seriously that disinformation and the spread of hatred and extremism online could become a national security issue and must be addressed. The question is how to address the problem responsibly without infringing on human rights and privacy and without interfering with the integrity of the networks.

Ardi Sutedja (Chairman, Indonesia Cyber Security Forum):

Mr. Sutedja had been using the internet since the connectivity was received from the telephone line with only 14.4 bps, which was very low. However, the early adopters of the internet had

unwritten ethics and a shared understanding called netiquette that they had to obey and respect. Unfortunately, people tended to ignore these ethics nowadays and believed the internet was a free space to do anything they want. On the other hand, people who developed the internet technology did not expect the misuse or abuse of the internet. Thus, these problems were not being properly taught and no one was doing anything to mitigate them through a regulatory approach. However, bear in mind whatever is published on the internet, the digital footprint would stay and not be erasable, including some of the disturbing content on the internet. Thus, all the tech companies and all the players would have to come to an understanding that regulating the internet would not necessarily mean violating human rights. The interest of the public and public safety must be put at the front because if we ignored all these issues, the internet would create a new, unexpected conflict. Awareness must be built for the users of the internet and the tech companies. In addition, everyone who was involved in technology would have to be involved in figuring out these problems because it was not a country-centric issue. Indeed, this problem was a global issue that would have to be discussed in order to avoid bigger problems in the future.

Yisuo Tzeng (Assistant Research Fellow, Institute for National Defense and Security Research, Taiwan):

Mr. Tzeng considered Taiwan a unique case because Taiwan treated disinformation as a national security issue. Then it followed by unexpected consequences that the government in Taipei brought all the giant tech platforms into the line to comply with the government for the fact check. Most importantly, Taiwan had been in consultative democracy with a divided society as any democracy normally would. Subsequently, people only picked what they would want to listen to and believe what they would want to believe. Thus, we needed to have a multi-stakeholder approach instead of just a government approach in dealing with cyber security risks. In dealing with disinformation campaigns and all these content fact checks, Taiwan went for a whole society and incorporated civil society groups. In Taiwan, different kinds of civil society groups with different partisan alignments exist. Thus, the government organized multiple fact-check agencies and those agencies would have to build up their credibility.

Over the years, the government, private sector, and civil society groups would gradually work with three to four big fact-check agencies that earn societal trust to deal with social engineering and malicious content. Since Taiwan was a democratic country, the government could not really regulate the content because of ethics. However, the government had several rules to deal with disaster emergencies when disinformation might cause loss of life or harm human life. In addition to that, the government used a multiple-stakeholder approach or the whole society approach to deal with fact-checking. These efforts had made Taiwan, according to some countries, become the best practice for the matter. In most of the world, disinformation or the malicious content of those hateful speeches that might cause death was something that people in Taiwan need to gravel with and improve. Nevertheless, Taiwan still had a lot of insight to share with each other.

Questions

Greg (Audience from YouTube):

Throughout 2022, several cyber incidents occurred in Indonesia that caught wide attention. What lessons can be learned from them and do you think the Indonesian government had started to tackle those problems? Someone says that the Indonesian government was more concerned about domestic issues than external threats. Would you agree, and if yes, would that be the same mindset in the cyber field?

Responses

Ardi Sutedja (Chairman, Indonesia Cyber Security Forum):

Mr. Ardi Sutedja reminded the audience that he was not speaking on behalf of the Indonesian government. However, he believed in the concept of a collaborative approach to managing the issues that people would face on a daily basis. The collaborative approach would not only be the responsibility of one single entity in the government or the private sector. It would have to be done in concert with all our abilities.

He disagreed with the statement that said the Indonesian government had only been focusing on domestic issues. In reality, the government had been doing a lot in the international arena. The Ministry of Foreign Affairs had been having various international discussions on cyber issues, including at the UN level and with international partners. In addition, the Indonesian government also worked with similar organizations in various countries. Given many constraints, especially the shortage of experts and the talent gap, the Indonesian government had been doing its best. It would be a long process for Indonesia and the world and require patience and understanding to face this issue and the incidents.

Questions

Luthfy Ramiz (The Habibie Center):

Question for Mr. Sutedja dan Mr. Hogeveen. If ASEAN were to put forward one priority to accelerate cooperation in the cyber security aspect, what should it be? How do you see Indonesia's ASEAN Chairmanship 2023 would fare in cybersecurity issues? Especially as you mentioned before, Singapore, during its 2018 chairmanship, greatly invested much effort in this regard.

Responses

Bart Hogeveen (Head of Cyber Capacity Building – International Cyber Policy Centre, Australia Strategic Policy Institute):

In regard to Indonesia's roles as the chairman of ASEAN and the chair of the Asia Regional Forum, it should ideally be built on what Indonesia cared about in terms of cyber security or information security and what Indonesia can share based on its strength. Related to the previous question on what Indonesia had learned from a series of cyber security incidents over the past year where there were a few data breaches earlier this year, which instantly pushed forward a data security law that had been in the parliament for a long time. Looking at data breaches and how the government dealt with them, both on the regulatory side but also on what would the government do in making sure that government entities and data enterprises or private enterprises would employ proper data security or information security standards as a way of doing their utmost to make sure that identical personal data from citizens would be in place. Mr. Hogeveen believed that would definitely be a role for ASEAN to play. It should not be political enough to be too sensitive and not step on anyone's toes. That would build the ASEAN together and where they could really make an effort which would also be connected to the idea of the integrated digital market that the ASEAN Member States had been pushing.

Ardi Sutedja (Chairman, Indonesia Cyber Security Forum):

It would be a good opportunity for Indonesia to play a big role in shaping cyber security in the region. Being the largest country in ASEAN with a big market and large-scale infrastructure development had been a privilege for Indonesia. For instance, Indonesia succeeded in putting cyber security into discussion during the G20 meetings where Mr. Sutedja was part of the digital economy working group, especially in promoting cross-border data exchange. This effort would need to be continued in Southeast Asia and start to work collaboratively among the members.

Indonesia had been working with Australia on certain issues, including managing the incidents and organizing training about the pipeline. Indonesia had also been working with the US and China and would be open to working with other countries with an honest approach to curtail and manage the risks. Cybersecurity should not be a country-centric issue and would require global collaboration. Thus, Indonesia would be better off if more partners engage in working and enhancing knowledge sharing.

Questions

Mabda (The Habibie Center):

Understanding that Indonesia itself had been such an active player in the multilateral settings, how had Taiwan played its diplomatic approach in making sure that it would be able to engage other actors in ensuring cyber security, especially at the global level? As Mr. Tzeng mentioned before, Ukraine requested to pull Russia out of the top-level domain (TLD) in the previous year. Also, there was a similar accident between Taiwan and China.

Responses

Yisuo Tzeng (Assistant Research Fellow, Institute for National Defense and Security Research, Taiwan):

Taiwan did not treat cyber security as a simple diplomatic issue and did not stress internet sovereignty because it would be a matter of global cyberspace governance. Even though Taiwan was not a member of ICANN or UN, Taiwan followed every rule and norm adopted by these two global organizations. However, if any programs or regulations had been perceived as best practices, Taiwan is willing to share and contribute to international cybersecurity development.

Closing Remarks

Ardi Sutedja (Chairman, Indonesia Cyber Security Forum):

Internet and its technology were evolving, thus regulation would not be the only answer to tackle cyber security issues. The key solution to this problem would be understanding what we had been facing from the highest point of view. Thus, we all would need to learn more, communicate more, and work collaboratively with partners in the world because the internet had been everybody's domain. In the internet era, people tended to talk more without communicating, which would make people lose their ability to see the internet from a helicopter view.

Yisuo Tzeng (Assistant Research Fellow, Institute for National Defense and Security Research, Taiwan):

The internet belonged to the average global citizen. Thus, everybody should sit down and talk to figure out what it would mean to have internet or digital sovereignty. There had been confusion that digital sovereignty raised by the European Union differed from other countries' internet sovereignty. Taiwan had encountered confusion, and digital sovereignty could be a good topic for further discussion and debates to give people a place to state their voices and emphasize that

digital sovereignty would not be up to a single entity.

Bart Hogeveen (Head of Cyber Capacity Building – International Cyber Policy Centre, Australia Strategic Policy Institute):

Two things that stood out were the idea that we still would need to work on, for example, the checks and balances of certain entities that had the authority to engage in cyber security issues, such as the government, private sector, and also the broader community. The more stakeholders engaged in this debate, it would scrutinize the regulation and its implementation. That being said, Mr. Hogeveen would like to see more conversations on this matter in public. Moreover, the issue of multi-stakeholder engagement was often used as a throwaway term. Thus, we must reinvent the whole idea and definition of multi-stakeholder engagement in cyber security issues.

The new idea should transfer the political-military in the international security domain where communities and companies should have a proper place to speak to share their key concerns and key responsibility for saving and securing online space.

asean studies program

ABOUT ASEAN STUDIES PROGRAM

The ASEAN Studies Program was established on February 24, 2010, to become a center of excellence on ASEAN related issues, which can assist in the development of the ASEAN Community by 2015. The Habibie Center through its ASEAN Studies Program, alongside other institutions working towards the same goal, hopes to contribute to the realization of a more people-oriented ASEAN that puts a high value on democracy and human rights.

The objective of the ASEAN Studies Program is not merely only to conduct research and discussion within academic and government circles, but also to strengthen public awareness by forming a strong network of civil society in the region that will be able to help spread the ASEAN message. With the establishment of ASEAN Studies Program, The Habibie Center aims to play its part within our capabilities to the ASEAN regional development.

ABOUT TALKING ASEAN

Talking ASEAN is a monthly public dialogue held at The Habibie Center in Jakarta. Covering a wide array of issues related to ASEAN, Talking ASEAN addresses topics of: Economic Integration, Socio-cultural, & Democracy, human rights and regional peace, among others. Featuring local and visiting experts, Talking ASEAN is one of a series of twelve dialogues regularly held each month and open to a target audience consisting of ASEAN officials, foreign ambassadors & diplomats, academics, university students, businesses, and the media.

PROJECT SUPERVISOR: Mohammad Hasan Ansori (Executive Director) & Julia Novrita (Director for Program and Development) | **RESEARCHERS:** Marina Ika Sari, Luthfy Ramiz, Herawati, Mabda Haerunnisa Fajrilla Sidiq | **FINANCE & ADMINISTRATION:** Dewi Isma Rikya Ikhsan, M. Sohib | **LAYOUT & DESIGN:** Mayka R. Asnawiyah

ASEAN Studies Program - The Habibie Center

The Habibie Center Building - Jl. Kemang Selatan No.98, Jakarta 12560
Tel: 62 21 781 7211 | Fax: 62 21 781 7212 | Email: thc@habibiecenter.or.id

www.habibiecenter.or.id

facebook.com/habibiecenter @habibiecenter