Security Update
August, 2019

DILEMMA OF CYBER SECURITY REGULATION

Ali Asghar, MA.Pol
Dr. Awaludin Marwan, SH, MH, MA

The Center for National Security Studies
Bhayangkara University of Jakarta Raya

Profil

The Center for National Security Studies (Puskamnas) Bhayangkara University of Jakarta (UBJ), is a strategic think thank which actively contribute to advice the government, academia, society, and media concerning national and international security policy. We conduct a research, training, advocacy, academic publication, conference, and other academic activities in regards with the issue of terrorism, security, conflict resolution, human rights, rule of law and democracy. Hereby, we release a security update to give an insight to public sphere.
We have some researchers with widely multidisciplinary approach and academic background.

Problems and Political Challenges

Indonesia stands in 41st of global rank from the 2018 cyber security index. Despite Indonesia received a high-level ranking of cyber security from 175 countries,[1] cyber incidents in Indonesia still leave many problems. According to ID.CERT, cybercrime incidents recorded amount of 8.053 intellectual property right offence cases, 4.233 spam cases, network incident 2.700 network incident cases, 1.761 malware cases, 1.063 phishing/ spoofing, and so on from May-June 2018.[2] Furthermore, from March-April 2018, ID.CERT reports the cybercrime incidents that are still high. Herewith, intellectual property right offences contain 10.553 cases, spam comprises 5.256 cases, network incident composed of 2.501 cases, malware contain 1.149 cases and so forth.[3]

As described above, we can analyse that cybercrime incidents are frequently happened in Indonesia. Cyber security is demanded to be increased its security system. Whilst the booming of digital economy in Indonesia is growing up with the increased e-commerce, financial technology, social media, start-up, and so on, cyber security desires to be provided to secure this growth digital economy. However, Indonesia government does not have yet cyber security regulation. Herewith, the regulatory making process to cyber security regulation needs to be realised. So far, Indonesian government has only the electronic information and transaction (Law No. 11 of 2008). In the contemporary digital era, at least data protection act as well as the cyber security regulation is required to shield the country and their citizens.

Cyber security system is demanded, not only to protect from cyber-attack within the home country, but also to secure from cyber war and establish cyber defence. For instance, in 2009, the shocked news concerning illegal interception telecommunication which have targeted Indonesian President Susilo Bambang Yudhoyono (SBY). This illegal interception had also targeted vice-president and other senior ministers. This case is problematic on how the cyber security system should be paid attention to.

The draft of cyber security regulation has created. This draft contain preparation of creating cyber defence, cyber audit, certification, oversighting throughout electronic information system of government institutions, and so on. Some problems arise. One example, the Indonesian National Cyber Security Centre (BSSN) has a bit problematic authority to handle cyber security issue. First, the issue of cyber security may become a broad area which needed to analyse from multidisciplinary approach and many stakeholders. The aims of strengthening cyber security is required to empower democracy and economic growth. However, due to some authorities equipped in the Indonesian National Cyber Security Centre (BSSN) such as military password or secret code, this body seems to be an anxiety of its position. Cyber security centre from comparative law approach is normally taken by government officials who mainly do not have military task. Moreover, the chairman of the Indonesian National Cyber Security Centre (BSSN), mostly comes from ex-military general such as Major-General Djoko Setiadi and Lieutenant-General Hinsa Siburian. This situation may restrain the quality standard of this body to improve. The development of cyber

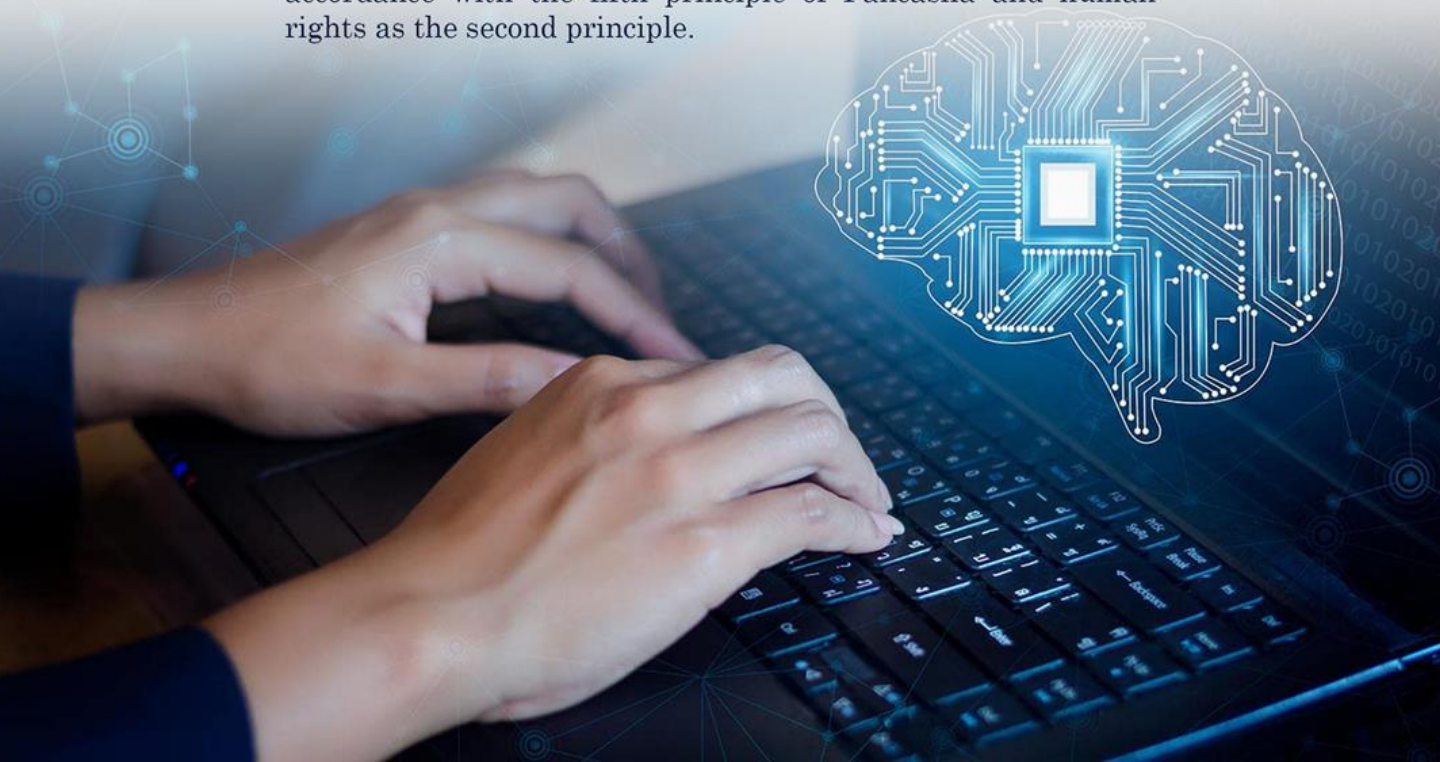
security body mush be flexible, responsive and innovative. Second, the design of cyber regulation should consult to public, especially scholars, media, human rights activists, etc. This regulation has already submitted into the Indonesian Parliament to be discussed. Hence, the draft of cyber security regulation, public should pay attention.

Global Cybersecurity Index (GCI) 2018. ITU Publications., p. 68
Laporan Dwi Bulan III 2018 (Two Monthly Report III 2018), p. 8
Laporan Dwi Bulan II 2018 (Two Monthly Report II 2018), p. 8

Analysis

Cyberwar may suffer citizens which taken down banks, e-commerce, ministries' website, e-governments, smart-cities, and many other things. Cyberwar as well-known defined cyberwarfare was occurred in Estonia, Georgia, Iran, and North Korea. The case of Iran in 2010 was delineated on how American cyber army attacked and damaged Iran's nuclear program (Karnouskos, 2014; Matrosov et al, 2010). In 2008, cyberattack also brought many Georgia's electronic system that taken down for 24 hours (AFCEA, 2008). Currently, every country has prepared to defence their electronic system from cyberwar. At least, every government has also devised cyber defence system from cybercrime.

If Indonesian government needs a cyber security regulation, they have to prepare which based on rigorous and comprehensive academic research. In the main consideration, as other regulations do, Pancasila as the ground of legal source should be mentioned. According to Law No. 12 of 2011 concerning the establishment of regulation is stated that Pancasila as the main source of Indonesian legal system. Moreover, cyber security is related to enhancing social justice in accordance with the fifth principle of Pancasila and human rights as the second principle.



Besides the basic philosophy of legal consideration, the draft needs to mention the urgency of growing digital economy and enhancing digital start-ups. If the consideration is only security aspect, people and private sector may not be interested in. According to Temasek and Google's research in 2018, Indonesia is the biggest digital economy growth, with 25 trillion USD can be reached in 2018 and it will achieve until 100 trillion USD in 2025.[4] Unfortunately, this cyber security regulation concerns too much on security audit in accordance with the ISO 27001. Of course, international standard for cyber security is demanded. However, the ISO 27001 has some problems in practice. This system is too expensive for small and medium-sized enterprises. At the same time, this system is criticized by some activists concerning issue of 'digital imperialism.' Indonesia need to have their own system to information technology audit and secure their society through digital means. Herewith, research and development is required by the universities and the collaboration with persistent stakeholders. Furthermore, the cyber security regulation should stimulate societal participation of people in politics and government decision making process.

From theoretical viewpoint, security is not only about military matter, but also ideological, social and economic. Furthermore, integrated security policy which defined existential threats and emergency action.[5] Cyber security strategy should contain integrated cyber security policy and reform to multi- approaches. Military approach is the traditional way to establish a national security.

[4]Temasek and Google, E-Conomy SEA 2018, 2018

[5]Barry Buzan. Rethinking Security after the Cold War. 1997. Nordic International Studies Association, SAGE Publications.

Recommendation

1

1. The draft of cyber security regulation is a new draft of law which already sent in the Indonesian Parliament. This draft should contain an academic substance which based on scientific research. Furthermore, this draft also need to be consulted towards public, media, scholars, industries, and so on;

2

2. We need to have an autonomy cyber security system which does not only refer to international standard such as ISO 27001. Rigorous and serious research should be prioritized in order to have Indonesian own system besides the fulfilment of international standard;

3

3. Indonesian Cyber Security Centre may become a democratic and innovative institute when the composition of this centre is not dominated by military figure. Indonesian government need to have distinguished cyber security system between civilian and military.