

---

## THE URGENCY OF NATIONAL SECURITY COUNCIL (NSC) IN THE CONTEXT OF CYBER SECURITY AS A SUB SYSTEM OF NATIONAL SECURITY TO PROTECT STATE AND PEOPLE

Sumantri

Universitas Nasional Jakarta

[sumantri11@gmail.com](mailto:sumantri11@gmail.com)

**Abstract** : The 21<sup>st</sup> century, the era of globalization characterized by free fight competition, advanced information and communication technology, and a borderless world has in one side make possibly the entrance of any values of ideology, politic, economy, socio culture, defense and security that can either be threats or challenges for any countries, in the other side democracy and human rights promoted by globalization awakening the universal awareness of human safety from any threat such as war, ethnic cleansing, communal conflict, and other physical and non physical threats. Despite the universal awareness of human safety, insecurity condition and internal political problem of any country will certainly affect the national security.

Keyword : National Security Council, Cyber Security, State, People

### INTRODUCTION

The threats and challenges of security then to be complex and multi-dimensional. Most countries are now strengthening their laws on security as to make their national security system to be adaptive an effective to face multi-dimensional threats and challenges. Though non traditional threats such as non military ones are more potential and factual in recent years, traditional threats such as military threats shall not be ignored. Non traditional threats not only endangering state security but also citizen even **basic values** of a nation which in turn can potentially endangering the state existence. Therefore traditional security concept known as **state security centered** depending upon military power is not sufficient to face multi-dimensional threats so that the concept shifted to **state and people security centered** depending upon the military and non military power (National Power). Security then to be holistic consisting of defense, internal security, public security, human security known as *comprehensive security* demanding collective responsibility, cross sectoral and civil society involvement. Len le Roux defines security as *At national level the objectives of security policy therefore encompass the consolidation of democracy; the achievement of social justice, economic development and a safe environment ; a substantial reduction in the level of crime, violence and political instability. Stability and*

development are regarded as inextricably linked and mutual reinforcing. At international level the objectives of security policy include the defense of the sovereignty, territorial integrity and political independence, and the promotion of regional security (Roux, 1999) . Barry Buzan says “Security is affected by factors in five major sectors: military, political, economic, societal, and environment. A nation can be said to have assured its own security when it is militarily, economically and technologically developed, politically stable and socio-culturally cohesive”(Banyu, 2006). Patrick Garrity says that national security applies most at the level of the citizen. It amounts to human well being; not only protection form harm and injury but from access to water, food, shelter, health, employment, and other basic requisites that are the due to every person on earth. It is collective of the citizen needs –overall safety and quality life –that should figure prominently in the nation’s view of security (Cambone, 1998). Indonesian has his own national security concept as mentioned in the 4<sup>th</sup> paragraph of 1945 Constitution Of The Republic Of Indonesia Preamble.

.....Pursuant to which, in order to form a Government of the State of Indonesia that shall protect the whole people of Indonesia and the entire homeland of Indonesia, and in order to advance general prosperity, to develop the nation’s intellectual life, and to contribute to the implementation of a world order based on freedom, lasting peace and social justice.....

The paragraph indicates three elements of security - state, people and territory. The state (government) is obliged to protect its territory and people (citizen). As to execute its obligation, the state must also protect itself. **State and people centered security** is the spirit of Indonesian national security. Therefore national security concept is to protect either state or people (citizen) from any threat. State security might consist of defense (external security) and home land security (internal security), people security consist of public security and human security (citizen).

Cyber-attack is a recent threat to national security endangering either state or citizen. Cyber-attacks have become increasingly common in recent years. Capable of shutting down nuclear centrifuges, air defense systems, and electrical grids, cyber-attacks pose a serious threat to national security. “Cyber-attack” as “any action taken to undermine the functions of a computer network for a political or national security purpose. A cyber-attack must target a computer network, where a computer network is defined as a system of computers and devices connected by communications channels. Frequently, this connection exists over the Internet, but there are also numerous closed networks, such as the secure networks employed by agencies of government. The concept of a computer encompasses more than a simple desktop or laptop; it also includes the devices that control elevators and traffic lights, regulate pressure on water mains, and are ubiquitous in appliances such as cell phones, televisions, and even washing machines. Cyber-attacks on vital infrastructure are already becoming widespread. The potential for widespread damage

from a cyber-attack grows significantly with the spread of computers to nearly every aspect of human activity. Cyber-attacks are often transnational—run through networks across the world, and used to undermine computer systems in countries. Yet the challenge cannot be met by domestic reforms alone. International cooperation will be essential to a truly effective legal response. New international efforts to regulate cyber-attacks must begin with agreement on the problem — which means agreement on the definition of cyber-attack, cyber-crime, and cyber-warfare. This would form the foundation for greater international cooperation on information sharing, evidence collection, and criminal prosecution of those involved in cyber-attacks — in short, for a new international law of cyber-attack. This global threat may only be effectively met by a global solution—by the international community working together to design a new law for cyber-attacks. States could adopt a clear definition of cyber-attack, cyber-crime, and cyber-warfare in the context of a comprehensive binding treaty, nonbinding declaration, or through independent agreements in anticipation of more broad-based future cooperation (C. Attack, 2011).

There are two Laws among others related to Cyber Security 1) Undang-undang RI Nomor 3 Tahun 2002 tentang Pertahanan Negara (Law No.3/2002 of State Defence) mention that the State defense is to keep and protect the country's sovereignty, the territorial integrity of the Republic of Indonesia (NKRI) and safety all nation and all forms of threats, the threat of military and non-military. Especially non-military threats in cyber space has led to the ability of the state in defense of soft and smart power must be increased in anticipation of cyber war, through a strategy of deterrence, prosecution and recovery of cyber defense, in order to support the implementation of cyber security a national strategy led by the Ministry of Communications and Information Technology (Kementerian Pertahanan Republik Indonesia, 2013); 2) In Undang-undang RI Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Law No.11/2008 of Information and Electronic Transaction) explained that the use of information technology need security in order to maintain the confidentiality, integrity and availability of information. The law in the information in electronic form legally recognized and actions associated with the electronic system, both as providers and as users have a legal responsibility further provided in various legislations. Second Act above gives a mandate to the government agencies, including the Ministry of Defense Republic of Indonesia, to take the steps necessary to safeguard the country's sovereignty, territorial integrity of the Republic of Indonesia (NKRI) and the safety of the nation, including in cyberspace, where the electronic system organized and utilized extensively by the whole society.

Threat of military and non-military. Especially non-military threats in cyber space has led to the ability of the state in defense of soft and smart power must be increased in

---

anticipation of cyber war, through a strategy of deterrence, prosecution and recovery of cyber defense, in order to support the implementation of cyber security a national strategy led by the Ministry of Communications and Information Technology (Sudarsono, 1992).

In Undang-undang RI Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik explained that the use of information technology need security in order to maintain the confidentiality, integrity and availability of information. The law in the information in electronic form legally recognized and actions associated with the electronic system, both as providers and as users have a legal responsibility further provided in various legislations<sup>16</sup>.

Our Parliament has proposed *Cyber Security and Resilience Law Draft* to be discussed by the Parliament to come (2019-2024). The use of information technology with destructive purposes is a threat to national security of a nation and the State. The threat is divided into military and non military threats. The threat of a military nature against national security is a threat to security and defense. Meanwhile, the threat of non-military nature is a threat to the resilience of ideology, politics, economy and social culture of a nation and the State. However advances in technology will sooner or later affect our cultural norms, social institutions of our culture and (in terms of socio-political) decision-making patterns of government policy of our country(Sudarsono, 1992). It is important to bear in mind that to make *Cyber Security and Resilience Law* is not only depending on structural approach “top down” but also “*bottom up*” meaning sociological and cultural approach for Indonesian is pluralistic, participation of institution advocating democracy and human rights, academician, mass media, and business circle. This approach is advisable because cyber-attacks pose a serious threat to ideology, politic, economy, socio culture, defense and security. Coordination and collaboration among the institution of security including cyber security concerned is imperative as to achieve integrated national security system. In this case, Law of National Security and establishing National Security Council (NSC) are urgently needed as the regulator instrument to build integrated national security to face multi -dimensional threats. Mid Term Plan of National Development 2015-2019 mention that in order to build integrated national security system it needs to make National Security Law and to establish NSC by Presidential Decree (RPJMN 2015-2019).

## CONCLUSION

Since the Law of National Security failed to pass , then President by Article 4, Section (1) of Constitution 1945 has his prerogative right to establish NSC of which the functions are as the highest coordination forum of national security chaired by President, National Security Advisor to President, protecting basic values and national identity. NSC can hold

convention led by President to resolve any crucial, crisis or emergency situation (issues) assessed as being strategic for national interest. The President as the Chairman of NSC can invite ministers and head of governmental institution, civil society, academician, expert of all discipline to be the active participant of the convention as long as the function and discipline related closely with the issue being discussed. NSC is a solution to create integrated national security policies in which at the same time to resolve sectoral or partial approach to serious national security threats of both military and non military.

## REFERENCE

- Darmono (2010), Konsep dan Sistem Keamanan Nasional Bagi Bangsa Indonesia, Sekretariat Jenderal Dewan Kethanan Nasional (Wantannas), Jakarta, <http://www.aiendro.info/buku/Buku%20Kamnas%20wantannas.pdf>
- Len le Roux, Defining defence requirements : Force design considerations for the South African National Defence Force, Published In African Security Review Vol 8 No. 5, 1999
- Perwita, Anak Agung Banyu, (2006), Hakekat, Prinsip dan Tujuan Pertahanan-Keamanan Negara, dalam: Mencari Format Komprehensif Sistem Pertahanan dan Keamanan Negara, T. Hari Prihartono (eds.), Propatria Institute, Jakarta
- Patrick Garrity dalam Cambone, Stephen, (1998), A New Structure for National Security Policy Planning,
- The Law of Cyber-Attack (2011), Article (PDF Available) in California Law Review 100(4) • [https://www.researchgate.net/publication/251334352\\_The\\_Law\\_of\\_Cyber-Attack](https://www.researchgate.net/publication/251334352_The_Law_of_Cyber-Attack)
- Muhamad Rizal & Yanyan Mochamad Yani Business Administration Lecturer and Profesor International Relation, Faculty of Social Science & Political Science, Padjadjaran University "Cybersecurity In The Contexts Of Law And National Defence In The Era Asean Community" [https://www.researchgate.net/publication/314489403\\_Cybersecurity\\_Policy\\_and\\_Its\\_Implementation\\_in\\_Indonesia](https://www.researchgate.net/publication/314489403_Cybersecurity_Policy_and_Its_Implementation_in_Indonesia)
- RPJMN 2015-2019, Buku II