Advances in Social Science, Education and Humanities Research, volume 391
International Conference on Business, Economic, Social Science, and Humanities – Humanities and Social Sciences Track (ICOBEST-HSS 2019)

American Foreign Policy in Cyberspace

Dewi Triwahyuni
Departemen Hubungan International
Universitas Komputer Indonesia
Bandung, Indonesia
dewi.triwahyuni@email.unikom.ac.id

***Abstract*—The purpose of this study is to comprehensively understand the importance of cyberspace in US foreign policy. Cyberspace is very crucial in all sectors of life in the United States. Cyberspace provides information distribution and is a vital communication medium, both for government, trade, academia, and the private sector. Dependence on the cyber world results in exploitation of the fragility of the US cyber. It has the potential to provide an opportunity for opponents to gain important knowledge such as plans, capabilities, and US military operations. In certain cases, opponents can disrupt communications and people's civil or economic infrastructure. To answer the problem of research, the researcher uses qualitative methods to analyze deeply the priorities of cyberspace for the United States, especially in its foreign policy.**

Keywords— United States, Foreign policy, Cyberspace

I. INTRODUCTION

Currently, the US foreign policy in cyberspace is an international scene. The United States foreign policy is one of the most dynamic foreign policies in the world. As a strong country, the United States believes in itself in choosing politics or policies against the world. Various American policies to solve problems in cyberspace today often get criticism by the American community itself and the world community in general [1]. This study examines how America makes cyberspace as a priority in its foreign policy.

There are a number of studies that have been done previously which encourage the making of this research. Hallams has explored how the internet and media technology play an increasingly important role in changing US public diplomacy programs [2]. Hallam came to the conclusion that it was important for the United States to make changes to its Foreign policy in dealing with the situation of the digital revolution [2].

Meanwhile, Segal highlighted the ongoing cyber conflict between the United States and China. Segal sees the fragility of international norms governing cyberspace as having an impact on relations between the two countries [3]. The situation of the void of international norms was also examined by Jeffrey. He stressed the importance of international cooperation in dealing with cyber problems that occur [4]. While research conducted by Pawlak said the United States is a country that is very supportive of the establishment of international norms that can shape the behavior of countries in the cyber world [5].

II. METHOD

The method used in this research is a qualitative method. Researchers have made observations on research objects, observing symptoms, events, and facts about changes that occur in the United States foreign policy in the field of cyberspace. Researchers obtained data by studying the US foreign policy documents and analyzing various policy priorities from year to year so that researchers can understand the differentiation that occurs. The researcher conducted interviews with several key informants and supporting informants. The informants are experts in foreign policy.

III. RESULTS

Although the United States has always been seen as a strong country that has high technology and innovation, the United States is not the foremost country in matters of internet access and connectivity [7, 5]. Research from the International Telecommunication Union places the United States at 28 in individual access to the internet, which is 84 percent. The speed of internet connectivity in the United States is not at the forefront. The United States is behind South Korea, France, Britain, and Japan.

Meanwhile, the spread of the use of information technology and computer networks which later became the center of US strategy also caused its problems. Dependence on cyberspace results in the exploitation of the fragility of the United States. This has the potential to provide an opportunity for opponents to obtain important knowledge such as plans, capabilities, and military operations of the United States. In certain cases, opponents can even disrupt communication and disrupt the civil and economic infrastructure of the community. The protection of vital U.S. interests in cyberspace requires adjustments to the applications of all aspects of U.S. power [6].

Network connections in the United States ride the United States internet for civilians. Internet service providers are private telecommunications companies. These companies own and operate almost all of the United States cyberinfrastructure, such as cables, servers, routers, and other devices that connect cyberspace. The Supervisory Control and Data Acquisition (SCADA) system is a system that runs the United States' cyber-physical infrastructure which includes electricity, water and communication infrastructure. SCADA control is in domestic control but connected to the global internet.

In terms of security and government oversight, the American cyberinfrastructure has not been properly regulated and supervised. In 1997, the Department of Defense held an exercise called the Eligible Receiver. The

training is to see the extent of the vulnerability of cyber United States. In the exercise, the Department of Defense formed a team of 35 people from the National Security Agency to simulate cyber attacks against the United States.The United States Placing Security in cyberspace as one of the country's national security priorities we can see from various formulations of strategies and policies regarding the security of cyberspace that has been issued by the government of the United States (see Table I).

Only by using the system available on the internet, the team from the National Security Agency succeeded in doing a number of things, such as (1) breaking the electricity grid and emergency response systems in nine cities in the United States; (2) gain access to the 36 DOD internal network and send fake messages that spread confusion and distrust through the chain of command. In 1999, another NSA team, Zenith Star, managed to hack into the SCADA control system that regulates electricity to the United States military base and then disrupts the 911 emergency system [8, 32].

The training and experiments above show that hackers have a high ability to be able to turn off electricity, prevent response to emergency calls, and obstruct command and control in civilian and military areas [5, 32]. Therefore, in 2009, the President of the United States Barrack Obama stated that "No official single oversees cybersecurity policy across the federal government, and no single agency has the responsibility or authority to match the scope and scale of the challenge. When it comes to cybersecurity, federal agencies have overlapping missions and do not coordinate and communicate as well as they should with other private sectors [5, 31]". The cybersecurity priorities outlined in the various strategic documents (Table I) are actually the elaboration of the United States national strategy book (National Security Strategy / NSS) which is published every four years, as a policy line under the ruling administration. Even cyber is added as one of the threats of attacks that must be prevented and resisted to become US national security besides missile and terrorist attacks [11, 7].

TABLE I. LIST OF UNITED STATES GOVERNMENT DOCUMENTS ON CYBERSECURITY

Year	Institution	Documents
2003	The White House	The National Strategy to Secure Cyberspace
2011	The White House	International Strategy for Cyberspace
2011	The Department of Defense (DoD)	Department of Defense for Operating in Cyberspace
2013	Executive Office of The President of The United States	Administration Strategy on Mitigating the Theft of U.S. Trade Secrets
2015	The Department of Defense (DoD)	The Departement of Defense Cyber Strategy

Source: from several references

Other evidence that cybersecurity is very significant for the United States can be seen from the special expenditure plan for cyber power in the upcoming 2019 budget year which has been planned since the previous 5 years, which is included in the 2014 United States Defense Report (QDR). US cyber strategies for 2019 can be seen in Table II. the following [9, 41]:

TABLE II. CYBER MISSION FORCES PLANS FOR FY2019:

1	13 National Mission Teams (NMTs) with 8 National Support Teams (NSTs)
2	27 Combat Mission Teams (CMTs) with 17 Combat Support Teams (CSTs)
3	24 Service CPTs
4	26 Combatant Command and DOD Information Network CPTs

Awareness of the importance of cyberspace security is getting stronger in President Trump's leadership. In December 2017, the White House just released the National Security Strategy (NSS) of the United States of America under Trump's presidential administration. This document lists 5 priority actions that must be taken to safeguard the security of the United States in the cyber era [12,12-14]. Priorities for these actions include:

1) Identify and Prioritize Risk. In order to maintain infrastructure security, the United States sees risks from six main areas: national security, energy, and power, banking and finance, health and safety, communication and transportation.
2) Build a defensible Government Network. Strengthening the security of government agency networks including improving the ability to provide safe and uninterrupted communication.
3) Deter and Disrupt Malicious Cyber Actors. The United States will prioritize the precautionary principle before important infrastructure is attacked. The United States will also invite allies and friendly countries to jointly fight cybercrime.
4) Improve Administration Sharing and sensing. Improvements to capabilities provide protection against civil rights and privacy. Intergovernmental cooperation is also strongly encouraged by the government of the United States, as well as cooperation with private institutions.
5) Deploy layered defenses. It is because cyber threats move globally through communication networks, the United States Government must work with the private sector to be able to see and monitor cybercrime activities at the network level.

Meanwhile, to maintain peace, the United States strengthens the capabilities of the military, the basis of the defense industry, nuclear power, space, intelligence and cyberspace itself. In the future the United States believes cyber attacks will be the main character of the Global conflict. Therefore, the United States will strengthen cyberspace through improving attribution, accountability, and response; enhance cyber tools and expertise; improve integration and agility [12, 31-32].

In partnership with other countries, the United States Department of State leads efforts to promote open, operational, safe and reliable information and communication infrastructure that supports local and

international trade and encourages freedom of expression and innovation. To be more effective in advancing all of the interests of the United States in cyberspace, then on February 2011 under the Department of Foreign Affairs, the Office of the Coordinator for Cyber Issues (S/CCI) was opened as follows [10]:

1) Coordinating the State Department's diplomatic involvement on cyber issues
2) Serve as a liaison department to the White House and federal departments and agencies on these issues
3) Give advice to the secretary and deputy secretary on cyber issues and engagements
4) Acting as a liaison for public and private sector entities in cyber problems
5) Coordinate the work of regional and functional bureaus within the departments involved in this field

Although it tends to be a strategy of surviving cyber-attacks and increasing capabilities from within, the United States has an international strategy related to cyberspace, especially since cyber networks are now classified throughout the world so it is impossible to focus solely on domestic capabilities. After releasing a national strategy to deal with cybersecurity in 2003, in May 2011 the White House released International Strategy for Cyberspace [10] which generally stated the following objectives:

> *"The United States will work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce strengthens international security, and fosters free expression and innovation. To achieve that goal, we will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace".*

In the document, the United States affirms that the country continues to take action to help build and maintain an open, safe and trusted network both at home and abroad, both for citizens of the United States or the global community. The United States focuses its strategy on seven important areas that are actually interrelated and require collaboration from the government, international partners, and existing private sectors. The seven areas are economy, protection of networks, law enforcement, military, internet governance, international development, and internet freedom [10]. United States international cyber priority:

1) Economy: Promoting innovative and open markets
2) Protecting Our Network: Improve the security, reliability, and resilience of global networks
3) Law Enforcement: Extends the collaboration of law enforcement and legal regulations
4) Military: Preparing for the 21st security challenge
5) Internet Governance: Promote effective and inclusive internet governance structures
6) International Development: Building capacity, security, and prosperity through international trade
7) Internet Freedom: Supports the creation of privacy and fundamental freedom

IV. DISCUSSION

The White House categorized cybersecurity in five threat levels, namely threats to small businesses or home users, threats to large companies, threats to important sectors and infrastructure (such as government or universities), threats to national issues and vulnerabilities implicates at the national level, as well as threats that have the potential to touch the global level. All threats at these five levels are possible because of the interconnected network.

In carrying out its strategy, the United States has important principles as the basis of their strategy. First, cyberspace security activities are a national effort. Second, the principle to protect privacy and civil liberties. in other words, the United States government considers the abuse of cyberspace as a violation of the privacy and freedom of citizens. Third, the principle of forced regulation and markets. Government regulations will not be the main system for securing cyberspace. Broader regulations that mandate how all corporations must regulate their information systems can only disrupt successful efforts by creating less successful approaches to cybersecurity.

Fourth, the principle of accountability and responsibility. The point is that the government's strategy or policy focuses on information infrastructure that is more resilient and reliable. Fifth, the principle encourages flexibility, namely flexibility in the ability to respond to cyber-attacks and handle existing vulnerabilities. Sixth, based on long-term plans and awareness that the act of securing cyberspace is an ongoing process, as technology continues to develop and new vulnerabilities continue to emerge from the process.

V. CONCLUSION

Based on the principles stated above, the United States developed international strategies covering seven important areas, namely economics, protection of networks, law enforcement, military, internet governance, international development, and internet freedom. This strategy is the basis of the United States in issuing the foreign policy. In economic activity, the United States' international strategy is centered on the goal of promoting open and innovative international markets, such as maintaining a large market environment that encourages technological innovation in a globally connected network, protecting intellectual property rights, including protecting commercial trade secrets from theft, and encouraging superior technical standards and safe from experts. The United States also encourages discussion on cyber issues and how countries should behave. In the field of law enforcement, the United States is intensively in formulating an effort to punish international cybercriminals. In the military field, the United States seeks to realize a safe and trusted military network.

REFERENCES

[1] B. David, "Cyberpower in strategic affairs Neither Unthinkable nor Blessed," The Journal of Strategic Studies Vol.35, No.5, pp.689-711, October (2012).
[2] E. Hallams, "Digital diplomacy: the internet, the battle for ideas & US foreign policy", CEU Political Science Journal Vol. 04, pp.538-74, (2010).
[3] Segal. Adam M, "Cyberspace: The New Strategic Realm in US-China Relations", Strategic Analysis Vol.38 No.4, pp 577-581, (2014).
[4] H. Jeffrey, "U.S. International Policy for Cybersecurity: Five Issues That Won't Go Away", Journal of National Security: Law & Policy, Vol.4 No.1, pp.197.
[5] Pawlak. Patryk, "Capacity Bulding in Cyberspace as an Instrument of Foreign Policy", Global Policy Vol.7 Issue 1, February (2016).
[6] M. D. Young, "National Cyber Doctrine: The Missing Link in the Application of American Cyber Power", Journal of National Security Law & Policy, Vol. 4, pp.173-196, (2010).
[7] Pernik, Wojtkowiak, & Verschoor-Kirss, "National Cyber Security Organisation: United States", Tallian, Estionia, NATO Cooperative Cyber Defence Centre of Excellence, (2016).
[8] Spade. J. M, China's Cyber Power and America's National Security [Strategy Research Project]. Philadelphia: U.S. Army War College, (2011).
[9] United States Quadrennial Defense Review (QDR), US Departement of Defense, (2014).
[10] United States National Security Strategy, The White House, 2011
[11] United States National Security Strategy, The White House, 2015.
[12] United States National Security Strategy, The White House, 2017.