Advances in Social Science, Education and Humanities Research, volume 225
International Conference on Business, Economic, Social Sciences and Humanities (ICOBEST 2018)

Foreign Policy of The United States of America in Addressing China's Cyberpower

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

Yanyan Mochamad Yani
International Relations Department
Universitas Padjadjaran
Bandung, Indonesia
yanyan.mochamad@email.unikom.ac.id

Arry Bainus
International Relations Department
Universitas Padjadjaran
Bandung, Indonesia
Arry.bainus@email.unikom.ac.id

***Abstract*— The purpose of this research is to analyze the strategy of US foreign policy in the face of Chinese cyber power. To answer the problem of research, researchers use qualitative research design. Researchers use primary sources in the form of official state documents and secondary sources in the form of interviews with US foreign policy experts, and through journals, dissertations and related research. The enmity of the United States and China in cyberspace has become a prominent issue in the bilateral relations of both countries. The latest developments of the United States are seriously issuing its Foreign Policy formulation to virtual space following a number of Chinese behaviors in virtual space that affect the United States National Interest. The different interpretations of the cyberspace, leading these two countries to a mutual interaction. The United States puts more cyber security as a priority in its foreign policy with the increasingly aggressive actions of China in achieving its goals as a cyber power country. Based on the data analysis, the researchers conclude that the US foreign policy strategy in dealing with Chinese cyber power tends to use leadership strategy, in which the United States utilizes the dominance of cyber capability to suppress Chinese cyber power in a persuasive way. The strategy chosen by the United States is to take advantage of government channels and involve non-government channels to strengthen the level of trust and stability of both countries in the virtual space.**

Keywords*— *Foreign Policy, Cyberpower, cyberwar, US-China

I. INTRODUCTION

Cyber priorities in US foreign policy were further strengthened by the release of the "International Strategy for Cyberspace" document in 2011 [1] and "The Department of Defense (DoD) Cyber Strategy" in 2015 [2]. There are important statements in the US defense strategy. China's cyberpower development has become a major concern of the US. Even China is one of the countries that is very detrimental to the US due to the acts of data theft he did. Therefore the US needs to prepare its foreign policy to deal with Chinese cyberpower.

Some research results that also examined the cyber relationship between the United States and China, namely Ghazi-Tehrani [3] conducted a dissertation research, entitled "Regulating Cyberspace: An Examination of U.S. - China Relations ". Ghazi-Tehrani's research emphasizes the regulation of international law regarding cybersecurity by taking case studies of relations between the United States and China. Ghazi-Tehrani tried to answer the impact on the relations between the two countries and how cyberspace should be regulated by adapting the latest cybercrime theories including non-cyber criminology theories that had developed before. Subsequent research was made by Kluver [4] with the title "US and Chinese Policy Expectations of the Internet". the emphasis of this research is more on the Chinese side, namely the actual impact of the internet on governance and political change in China. Meanwhile the cyberpower variable in this study refers to several previous studies as well. Spade [5] examines the growth of Chinese cyberpower, its knowledge and the offensive, defensive and exploitative capabilities of China's computer network operations and compares China's capabilities with the cybersecurity capabilities of the US. From these comparisons Spade was then able to underline the degree to which Chinese cyberpower must be addressed as a threat to US national security. Meanwhile research on cyberpower was also developed by military institutions. Wentz et al [6], cyberpower from a military perspective. While Nye, Jr. [7], wrote cyberpower as a force in the future. Meanwhile, research on cyberpower was also carried out by Jordan [8] and Betz [9].

II. METHOD

This research use qualitative method. Researcher have recorded and investigated objects, symptoms, or events and facts that explain how cyber interests are applied in US foreign policy. Answering why Chinese cyberpower is seen as a threat to national security for the US. especially in dealing with, as well as reviewing the data strategy can be in the form of documents and phenomena obtained by researchers considering in this study, researchers have collected data that shows this research both obtained through documents and information from informants obtained in the data collection to be examined and checked and will be the main data source.

Data sources included in the secondary data in this study the authors use news from various newspapers, magazines, and documents. Regarding newspaper news, the magazine carried out content analysis by the researchers themselves, then understood the results that were able to provide an understanding of US foreign policy in dealing with Chinese cyberpower. To obtain primary data in this qualitative research, the authors used informants consisting of two categories, namely key informants and supporting informants who were chosen purposively based on their activities that could explore their experiences.

III. RESULTS

A. China's Cyberpower Development and The United States Interest's

For China, in cyber issues, the main priority of their strategy is the drive to realize social stability and national security. The two main points are Chinese interests above all. At the same time, control of access to information is part of a process that has long been carried out since the Chinese state was established [10]. Therefore, in addition to domestic interests, China needs an international environment that provides guarantees for information and cyber. That is what makes China take steps related to their international strategy. Chinese strategies are more about taking advantage of the economic side than military strategies that have the potential to make other countries alert and feel threatened.

In March 2017, the Chinese government released a document on the strategy of international cooperation in cyberspace / ISCC. As a basic goal of international exchanges and cooperation in cyberspace, China sets six strategic objectives in the ISCC document [11], namely:

1) Protecting sovereignty and security;
2) Develop a system of international rules;
3) Promote good internet governance;
4) Protecting the rights and interests of legitimate citizens;
5) Promoting digital economic cooperation;
6) Building a cyber cultural exchange platform

China's cybersecurity strategy consists of three main driving components, namely economic, political and military, and foreign policy behavior that strives actively and confidently to promote its ideas, China shows an effort to convince the international community to adapt to Chinese values in network security. With more involvement in the international community, China is trying to signal that the country is a responsible actor and can be invited to work together on technology issues. China has expressed its desire to behave in cyberspace, although some countries consider it to be an on-the-surface attitude and only as a jargon to prevent noise from other international actors [12].

Understanding Chinese cyber structures and strategies is not an easy task. China has not made a comprehensive approach to cyber issues in the form of strategies that clearly outline the country's cyber objectives and implementation. This has created a lot of uncertainty for the domestic environment China itself and for outsiders the complex hierarchy, the Chinese command structure and various defense documents are very confusing. Although China does not seem to object to a certain level of mystery, a move that suggests that they increase the desire to manage their cyber operations more efficiently at an early stage can be seen from the making of "Central Internet Security and Information Leading Group (CISILG)" in which President Xi Jinping directly as decision maker and person in charge to determine China's cyber strategy. This is also a good example of how Chinese people understand cyber as something that is highly integrated with society, and does not separate it from the general flow of government. Admittedly, the challenges arising from a typical approach such as cyber have great potential to influence the activities of the Western world in cyberspace for a number of reasons.

B. United States Cyberspace Strategy

Despite tending to a defense strategy from cyber attacks and increasing internal capabilities, the United States has an international strategy related to cyberspace, mainly because cyber networks are now well-known throughout the world so that it is impossible to focus only on domestic capabilities. After releasing a national strategy for handling cybersecurity in 2003, in May 2011 the White House released the International Strategy for Cyberspace and stated: "The United States will work internationally to promote 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 US citizens or the global community. The United States focuses on seven important areas that are actually interrelated and require collaboration from government, international partners, and existing private sectors. Seven international cyber priority areas of the United States [1]:

1) Economy: Promotes an innovative and open market
2) Protecting Our Network: Improve the security, reliability and robustness 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

Virtual world or cyberspace is a world that is very important in all sectors of American society. In the government, trade, academia, and private life sectors, cyberspace in the United States has supported hundreds of trillions of transactions. Power grid services, water systems, health services, law enforcement, and emergency calls are just one of several important roles of cyberspace for citizens. Meanwhile, communication, research and development, collaboration of educational institutions and the private sector, military command and control, intelligence work, and government administrative work are important roles of cyberspace for the United States government. Just like China, cyberspace is very important in the global network of the United States military, whether from everyday conversation to the issue of military operations.

However, the internal capabilities of US cyberspace are not the best in the world. In terms of individual access, the United States is only ranked 28th with 84% of individual

access to the internet. In terms of internet connectivity speed, the United States is under South Korea, France, Britain and Japan. In terms of government security and supervision, the cyber infrastructure of the United States is also not free from attacks. In a series of exercises to test US cyber vulnerability, in 1997, a team from the National Security Agency managed to break the power grid and emergency response system in nine cities in the United States, and even gain access to 36 DOD internal networks and send fake messages that spread confusion and distrust through the chain of command. The vulnerability of the US cyber system has the potential to bring negative consequences to these important sectors. Attacks on the banking system, for example, can cause economic panic and damage the stock market. An attack on a credit card has the potential to cause a loss of 35 billion US dollars. Attacks on public service sectors such as electricity and telephone can weaken the life of a region. This is coupled with the strength of China's cyber which is suspected of having a reconnaissance network and network maps that can be moved to attack and paralyze military command and infrastructure.

The White House itself has categorized cybersecurity in five levels of threat, 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 have implications at the national level, as well as threats that have the potential to touch global levels. All threats at the 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. Firstly, the activity of securing cyberspace is a national effort. Second, the principle of protecting privacy and civil liberties. That is, the United States government considers that abuse of cyberspace is a violation of the privacy and freedom of citizens. This is a contradictory norm against Chinese government strategies that use the internet as a propaganda tool and exercise control that makes its citizens do not have complete freedom in exploring cyberspace. Third, the principle of force regulation and market. Government regulation will not be the main system in securing cyberspace. Broader regulations that mandate how all corporations must regulate their information systems may only interfere with the success of the effort by creating an unsuccessful approach to cybersecurity.

With these principles, 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. 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 globally connected networks, protecting intellectual property rights, including protecting commercial trade secrets from theft, and encouraging superior and safe engineering standards 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 aggressively formulating an effort to punish international cyber criminals. In the military field, the United States strives to realize a safe and trusted military network.

The United States also focuses on the values of openness and innovation in the internet world. This includes supporting civil society based on freedom of expression and assembly. For this reason, the United States strives to increase cyber quality and technical and security capacity, and to create programs and assistance for other countries in need.

IV. DISCUSSION

A. United States Responses Towards China Cyberpower

The United States has a different national interest in cyberpower with China. In this first part, the author attempts to analyze this further by observing the clash of paradigms and policies of the United States in information technology and their relationship with Chinese actions. The policy in question is actions that are directed to the objective conditions and actors (both government and non-government) that are outside the territorial territory of the United States that they are trying to influence. These actions are expressed in the form of goals, commitments and / or directions stated explicitly, and those carried out by government representatives acting on behalf of the state or sovereign community.

The paradigm held by China regarding the internet and cyberpower has differences with the US paradigm. This difference not only leads to a different direction for internet development, but in some cases causes conflicts of interest between China and the US, China sees the internet and directs the development of its cyberpower on two main things. First, China developed communication technology to strengthen the efficiency of government organizations. Second, China wants to use communication technology to maintain the legitimacy of the Communist Party. That knowledge collides with US assumptions that are more inclined to assumptions related to information technology and its relationship with political communication. The US assumes that information technology and democracy share the same paradigm, namely the free flow of information. This compatibility causes the US to assume that information technology is a strategic component of China's political transformation.

The US hopes that China will become a more open and democratic government. That assumption is the guideline for China's foreign policy. The US responds by making policies that encourage the development of the internet and incorporating information technology-based companies into Chinese society. International organizations on human rights, several multinational companies, and academics try to provide Chinese citizens with free access, even though it must be "cat-mouse" with the Chinese government.

Even so, some academics consider the US has failed in responding to China's interests and strength over its cyberpower. Multinational companies such as Yahoo eventually have to submit to the Chinese government's request to censor and give control to the Chinese government. This indicates that US interests regarding democratic values cannot be carried out at a practical level in China.

B. Unites States Strategy in Addressing China's Cyberpower

The US strategy in dealing with cyber attacks is related to its foreign policy. According to Jones [13], policies are often interpreted in two forms, (1) policy as design and (2)

policy as practice. Policy as a design is something that is deliberately designed to achieve certain goals. In this context, a country's foreign policy becomes a plan of action. Whereas seen from the meaning of policy as a practice, the policy is actions made to solve technical or practical matters that arise in the international system. In this context foreign policy can be interpreted as an action itself.

A. Strategy through the First Track

The first path refers to government actors when completing the political process peacefully. This pathway is a strategy carried out from country A to country B in sharpening relations between countries with their respective national interests [14]. Reference [15] stated that China has always been the concern of the United States government. The question that continues to emerge is whether China will and has an obsession to become hegemonic in cyberspace. That is, whether China has an obsession to have the ability to choose their own path consistently without having to play roles regulated by other countries. Some ways China has done to dispel the hegemony of the United States. China, for example, began building fiber optic cables that connect directly from Asia to Europe to prevent sending data to lines based in the United States.

The strategy adopted by the United States against China is to initiate a joint agreement to improve cybersecurity. Finally, on September 24-25 2015, Xi Jinping and Barack Obama made a joint agreement on cybersecurity. The meeting between the two countries became very meaningful after a few years before the relations between the two countries were colored with mutual criticism in the matter of cybercrime. This agreement agreed not to hack each other's private companies for commercial gain and other adverse cyber activities. In essence, China and the United States agree with each other to jointly [15]:

1) Provide timely responses to requests for information and assistance regarding dangerous cyber activities.
2) Refrain from being involved or intentionally / consciously supporting theft of intellectual property.
3) Pursuing efforts to promote state behavior norms that are appropriate in cyberspace in the international community, andEstablish a high-level joint dialogue mechanism to combat cybercrime and related issues.

Based on the agreement in the agreement, especially the fourth point, since 2015 the two countries have consistently held high-level dialogues continuously to continuously improve the cybersecurity agreement of both countries (see Table 1).

TABLE I. U.S. - CHINA HIGH LEVEL JOINT DIALOGUE ON CYBERCRIME

Desember 2015: *First U.S – China High Level Joint Dialogue on Cybercrime*
Juni 2016: *Second U.S – China High Level Joint Dialogue on Cybercrime*
Desember 2016: *Third U.S – China High Level Joint Dialogue on Cybercrime*
April 2017: *Fourth U.S – China High Level Joint Dialogue on Cybercrime*

We can see from the continuity of high-level dialogue carried out by the United States and China, the authors analyze that the approach of dialogue by the United States to China is quite successful. Indirectly the agreements produced can bind China's behavior in cyberspace.

2. Strategy through the Second Track

The second path indicates an activity involving non-governmental actors or professionals between the two countries, without considering whether there is a third party presence or assistance in the discussion The main objective of this pathway is to encourage communication, understanding and collaboration towards problem solving.

Just like the first line, the second route is taken because of the problems of spying on each other and recriminating between the United States and China. But this is not easy because China itself thinks that the United States has companies, groups, and important discoveries related to the internet that it cannot run even longer. Internet management groups based in the United States such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Engineering Task Force (ETF) are included as targets of sources of Chinese jealousy of US technological progress. ICANN is a non-profit company that serves to regulate aspects of domain registration on the internet, while ETFs are open membership organizations that promote general internet standards. The United States itself, as previously explained, responds to the advancement of information technology by making multinational companies based in the United States to enter the Chinese market. In market competition with China, the United States has advantages in software technology. China is trying to lift the internal market by promoting the doubling of technical standards in Chinese products to please Chinese companies themselves. China is trying to get their companies to compete with the hegemony of the best US companies such as Cisco, IBM, Google, Qualcomm, Intel, Apple, Oracle, and Microsoft. China's efforts make Chinese companies superior or at least able to compete in hardware issues, while for software, US companies are still superior. Hardware devices such as router from Huawei, Xiaomi mobile phones, and ZTE mobile phones can make quite a lot of money. But to win in the software market, China must have the ability to find and update devices on a computer, while in terms of research and development, US companies have a larger budget and are still strong competitors. Therefore, one problem that often arises is the US accusation that China is eyeing research data from products that have been patented by US companies.

The difficulty in resolving the problem between China and the US originated from the term freedom which was understood and practiced differently. Freedom here can be seen as individualistic freedom, which emphasizes the freedom of users as long as it does not endanger other users. Freedom here can also be interpreted in the context of the

community, where each community adapts to the framework of certain rules and norms. Freedom can also be seen in the context of the country or company, namely how the state controls the internet by blocking pornographic content or radical thinking, for example, or companies use the internet for their economic interests. The difference and the breadth of the context make freedom of internet a very difficult goal to realize. A different paradigm of cyber war between China and the US shows that cyber worlds and different free characters create conflicts of interest.

Even so, technological progress raises its own expectations for the United States government. The US responds to China's cyber progress by continuing to encourage technology-based multinational companies in the United States to enter the Chinese market. The United States hopes that the internet will make China have a democratic value and protect the freedom of internet in its country. But the advancement of Chinese technology is considered to be in an act that is detrimental to the United States. China is able to hack military sites, public space sites and multinational companies' sites and steal research data from there. The data is then used to develop domestic enterprises in China. To try to overcome this, the United States carries out an action strategy through two channels, namely the interstate and professional paths. The strategy of the United States to develop China that is more free in arguing and overcoming China's cyber attacks with peace agreements has still not been fully achieved. China has never wanted to acknowledge cyber attacks on China. Negotiation through the second path which is felt to be more informal will also be more useful if it finally shows the results to the first line negotiations by determining concrete steps. However, the first and second paths provide at least opportunities for each of them to know their respective points of view regarding cyber attacks.

V. CONCLUSION

Addressing China's cyber attacks there are two main lines chosen by the United States, namely through government channels and through professional or non-state channels. The first path refers to intergovernmental efforts to bring together the relations between the two countries with their respective national interests. This first path strategy is of course not very easy because China and the United States have conflicting interpretations in understanding the cyber world. While the United States assumes that information technology and democracy have the same paradigm, namely the flow of free information. China instead developed information technology to strengthen the efficiency of government organizations and maintain the legitimacy of the Communist Party. Whereas the second path is the United States' strategy to use non-government actors in this case like multinational companies based in the United States to enter the Chinese market. In the face of developing Chinese cyberpower that tends to use aggressive actions in the cyber world, The United States tends to use the Confrontation strategy in its foreign policy to China. Although in general the United States is still considered to have superior cyber capability, the United States chooses persuasive measures and bargains with China. The choice of this strategy is very evident from the US foreign policy which continues to pressure the Chinese government not to carry out cyber attacks on the country and on the other hand the US is also very intensely inviting China to agree on "rules of common play" in the cyber world and encourage American internet-based companies Unions can negotiate with the Chinese government so they can enter and hegemony in China.

ACKNOWLEDGMENT

Ministry of Research, Technology and Higher Education of The Republic of Indonesia which has provided scholarships and grants on 2017 for this research.

REFERENCES

[1] Department Of Defense, "Departement of Defense Strategy for Operating in Cyberspace", Washington: Departement of Defense, 2011.
[2] Department Of Defense, "Departement of Defense Cyber Security", Washington: Departement of Defense, 2015.
[3] Ghazi-Tehrani, Regulating Cyber Space: An Examination of U.S. – China Relations. Irvine: University of California, Doctor of Philosophy in Criminology, Law & Society, 2016, Disertasi diperoleh melalui Proquest Number: 10125391.
[4] Randolph Kluver, U.S and Chinese Policy Expectations of the Internet, *China Information*, Volume XIX (2), 2005, pp. 229-324.
[5] J. M. Spade, *China's Cyber Power and America's National Security* [Strategy Research Project], Philadelphia: U.S. Army War College, 2011.
[6] Franklin D. Kramer., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and national security*, Potomac Books, Inc., 2009.
[7] Joseph S. Nye, Jr., The Future of Power. New York: PublicAffairs™, 2011.
[8] Tim Jordan., *Cyberpower: The Culture and Politics of Cyberspace.* New York: Routledge, 1999.
[9] David Betz, Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed, Journal of Strategic Studies, 35:5, 2012., pp. 689-711.
[10] N. Inkster, *China's Cyberpower*, London & New York: Routledge for The International Institute for Strategic Studies, 2016.
[11] SCIO, *International Strategy of Coorporation on Cyberspace*, Beijing: The State Council Information Office of The People's Republic of China, 2017.
[12] Amy Chang., "*Warring State: China's Cyber Strategy*", Center for a New American Security, 2014.
[13] R. Jones, *Analyzing Foreign Policy: An Introduction to Some Conceptional Problems*, London: Routledge Kegan Paul Ltd, 1970.
[14] sL. Diamond, J. McDonald., Multi-Track Diplomacy: A Systems Approach to Peace, 3rd Edition, Connecticut: Kumarian Press, Inc, 1996.
[15] S.W. Harold, M.C.Libicki, A.S. Cevallos., Getting to Yes With China in Cyberpsace, Santa Monica: RAND Corporation, 2016.