Jurnal Kajian Peradaban Islam
OPEN ACCESS
JKPIs , Pages 19 – 21, Vol. 3, No. 1, 2020
E-ISSN: 2654-3974
www.jkpis.com

Review

The Rise of Cyber Warfare

Andrian Willyan Djaja[1]*

[1]*Marine Geological Institute, Bandung, Indonesia*

ARTICLE INFO

Keywords
Democracy, cyber war, politics, ideology

***Correspondence**
asepwong@yahoo.com

Article History
Received 28 March 2019
Accepted 31 December 2019
Published on-line 25 January 2020

ABSTRACT

A war in cyber domain has been already started, and its impact is quite devastating. Dangers arisen from the new kind of war ranged from economic disaster such financial accounts shutted or locked, technological problems, for example personal computer hacking and thievery of important data, also includes hacking into a country's defense system and its use for personal benefit of a country or organization. The recent rise of 5G technology increases the possibility of these dangers to happen in real world. China currently holds the best 5G technology in the world in the hands of its leading company, Huawei. Heated politics between the US and China makes the possibility for China to use its technological advantage against its Western rivals and the whole world becomes very big. The US and its allies will definitely be retaliating against China with their own cyber weaponry, resulting in a large scale cyber warfare.

1. INTRODUCTION

International competition in arms between United States of Amerika (USA) and Russia with its ally of China, and, Iran, certainly has military dimension and has already reached levels where it can affect many people's daily life. Military aircraft contest has taken place several years before, resulting in USA put China's military development into successive watch. China, on the other hand, has also using power projection in Taiwan Strait using its anti access/area denial (A2/AD) capabilities, preventing US ships to come any closer to aid their allies.

The contest between these great powers already reached nuclear issue. At this point, North Korea has entered the stage. The decade-long struggle between USA and North Korea regarding the latter's nuclear development rises concerns in all the world : what will happen if nuclear war breaks out between these states ? Not to forget that Russia and China have their own nuclear arsenals. Even though China still maintain its 'no first strike' policy, there's no guarantee that it will not break into nuclear struggle involving China and its rivals.

Drone attacks also shines a new chapter. Trump administration has been mentioned as 'orders more drone strikes than Obama administration', noted specially in Middle East theatre (Edelman, 2019). Small drone swarm scenario has been considered as future war scenario. Drone has also considered to replacing soldier attacks or manned aircraft, since it's safer with less expensive.

Aside these strategies, another strategy has arisen in its place in geopolitical arms contest. Also, it took place not in our domain, but in cyber realm. Although not resulting in direct deaths, cyber attacks may deal a great damage to infrastructures such as power plant, resulting in power shutdown in public services such hospital or government offices. Deaths may occur from such situation, but it's intended result might be panic or chaos in the target state. Another effect comes from cyber mess has economical impact such bank rush by massive money lost.

Another impact by cyber strike is information stealing. Sensitive information stealing by hackers can be devastating, such as government policy or money savings in a bank. Even personal information theft such Facebook password can be troublesome. It increases chances for account hacking, bank saving theft, etc. In military context, sensitive information stolen can be about secret projects or latest armored vehicle development.

The situation is worsened by the birth of 5G technology, which is able to connect to many kinds of devices such robots or drones, and also able to stream big amounts of data in high speed (Craven, 2017). This 5G and its abilities provides an ideal environment for hackers to steal data from many institutions such as bank or governmental offices. If Julian Assange is still stealing data, then he might be enjoy using 5G network to take or send data to his computer(s), considering he has many (Segan, 2019).

Currently, the highest ability in the world to use 5G network is held by Huawei, a Chinese telecommunication company **(**Chang, 2019. The arrest of Huawei deputy chairwoman Meng Wanzhou on December 1st, 2018, although by financial fraud

charges, was suspected as (actually) a part of technological warfare between the US and China. Although Huawei denied these accusations, it is believed that Huawei did able to acquire these abilities to steal informations of secret government projects and world trades.

In addition, Australia has also banned 5G gadgets produced by Huawei and ZTE, also a Chinese telecommunication company. Huawei was also charged in stealing trade secrets. Meng Wanzhou also indicted to have affiliation to Iran, added as to list of reasons for her arrest. Huawei was also charged in intellectual property theft, such it's employee dismembering Tappy, a T-Mobile robot, and walked away carrying its arm. Allegations also came from Cisco, an American tech giant, for Huawei to stole its source code for routers.

It's not stopping now. Beijing had been known for stealing African Union secrets from 2012 to 2017, using certain application or device installed in Huawei gadgets donated by China to the organization. In other words, thievery of sensitive information or intellectual property is not a theory, but a reality we should start to face.

2. RESEARCH METHOD

This review was based on literature study through at least 5 websites containing recent news about politics and defense technologies around the world. Analysis was done based on the facts collected from the literatures, considering consistent facts found in the articles. Conclusion was done based on these facts after analysis completed.

3. RESULTS AND DISCUSSION

One of the greatest danger in this war of technology is in the 5G technology. Considering the rumors about 5G network were true, then none of us are free from the danger the 5G inflicted, for example, personal data theft (such as PIN number, should it kept in the phone), e-mail password, or even important information such latest result in meeting with an oil company.

5G network also offers remote capabilities to everyday devices such as autonomous vehicles or drones, even smartphones. A hacker might try using any smartphone to send an inappropriate message to his/her colleague, such porn picture/message or flirty text message. The same kind of action might be done to the victim's social media, for example Twitter or Facebook.

The danger list by cyber war keeps getting longer. Virus threat also comes, spreading to personal computers through e-mail opened in smartphones or external devices. There's no telling how many viruses may come at a time, considering the amount of data the 5G can bring. This means the threat of viruses or malwares such as WannaCry will increase.

It should be kept in mind, however, that not only China possess the ability to wave cyber attacks through 5G network; the US is actually able to do the same. However, China as mentioned before is leading the world in 5G technologies, portrayed in this case by Huawei, although it cannot be said that the US is unable to do the same.

It should be noted as well that cyber warfare was born through international (ideological) competition between world's superpowers. It can be said that cyber warfare is another form of war in modern era, a new kind of war waged beside conventional land, air, and sea warfare or the unconventional psychological war, but the same motive : to take control of the world in the name of capitalism or socialism (whichever the state uses).

If, or when, China does the cyber attack against its rivals, the attack will certainly be returned, assuming China's rivals have the ability to fight back. The activity of sending cyber attacks between states at this point can be called a cyber warfare. The problem is that cyber network and activities are not limited only between certain countries or states, but able to reach the entire world. The effects of cyber warfare ranges from computer network and internet shut down, financial system damage, a mess in public transportation, into damage in a country's defense system such air defense system. These effects will affect the entire world into chaotic situation, without any sign if it will ever stop.

3.1. Political Consequences

The danger of hacking is not limited to personal accounts such e-mails or social media. It is possible that hackers might get a try to remotely control US nuclear command center, for example. From there, hackers might turn to cyber terrorist, by accessing US nuclear control system, they launch a nuclear missile into US' rival such as Russia, igniting (first) nuclear war.

It is also possible to hack even satellites, to steal information or to spread virus or jamming certain communication line. If the satellite is linked to some weapon system, it is also possible to steal the use of the weapon system for a country's benefit, for example to disable the system whenever it is going to be used.

Not to forget that lately, world leaders uses social medias to communicate with the world. For example, Venezuelan self-proclaimed leader Juan Guaido states their opinions regarding latest situation in the torn-apart country using Twitter (Lyons, Ho, & Durkin, 2019). It is not hard, or rather usual, for a hacker to hack some figure's Twitter account and states some words by his own, not the figure's. The result is sometimes more heated situation leading to chaos or even civil war.

Capitalizing political statements can also be used to divide an alliance of several countries, or to alienate certain target country from its allies. China might will use this to make a crack between NATO countries, in an example. In reverse, the US can also use false statements to make a rift between Kim's North Korea and Xi's China, or even with Putin's Russia or Rouhani's Iran.

3.2. Economic Consequences

Cyberattacks might have economic impact as well. If cyberattacks are pointed to financial institutions (such as banks, to create a massive loss of money, for example), then an economic chaos is inevitable. Sudden poverty might happen, leading to mental illness to those who experienced it. Business collapses, money exchange value deteriorates, such also leads to economic breakdown and people chaos.

Another scenario might involve certain virus or malware (or ransomware) such WannaCry which locks certain accounts or files then offers for ransom in BitCoin. Cyber warfare might turn such situation or action into common action, which in turn will make sharp increase in cybercrime. Many people will lose their money in the process, which might also leads to another chaos, especially if the hacker is in another country that makes it hard to catch.

For a state that became hostage in cyber warfare, the state might be forced to do the attacker's bidding. If the US cannot retaliate against China's cyber campaign, then China will force US to do, for example, release Meng Wanzhou from her imprisonment, and make way for Huawei to open US branches and sell more products of Huawei in US market, defeating US' own

products such Apple phones. That way, China trample over US economy, and become leading country in the world. Such scenario is no impossible at all, although the US cyber capabilities are well-known as well.

If the scenario is reversed, the US is winning the cyber realm, then China will be forced, for example, to disarm its nuclear weapon system along with its control system. The US will also force China to pull some of its 5G equipment and limit the sale in several countries, opening path for the US to win international market.

A question might rise : what about the third side, the spectator state, which might also became the victim in cyber war ? Will the US or China, or the whole warring states, care about the victims ? Historically, no war victims ever being cared by either socialist or capitalist state. Both care only for the victim state if it is willing to accept the winner's terms. Current cases of Iraq, Syria, or even Rohingya people proves this statement.

4. CONCLUSION

A new kind of war, the cyber warfare, has started already. In theory, cyber activities don't take lives, although in reality it is proven otherwise. However, there's no telling what consequences might come, despite what's already mentioned above, due to secular paradigm that doesn't give limit to what a person or an institution might do. The consequences might be even worse, bringing impact to our daily life, where we can no longer feel safe when connected to the internet or network.

The cyber war might just begun, and it can get any worse at anytime. Unfortunately, there's no safe from this war, for it is not know any limit such distance or ammo. Even the latest antivirus or antimalware will not guarantee any safety at all from any threat might come. We can only prepare for the worst by regularly checking our accounts, and when it comes, then chaos might not far behind.

References

Chang, G. G. (2019, February 14). How Chinese Theft Becomes a Global Menace. *The American Conservative.* Retrived from https://www.theamericanconservative.com/articles/how-chinese-theft-is-becoming-a-global-menace.

Craven, C. (2017, October 20). Key Elements for 5G Networks. *Cdx central.* Retrived from https://www.sdxcentral.com/5g/definitions/key-elements-5g-network.

Edelman, L. (2019, January 28). Trump has this one right: China's 5G is a real national security threat. *Globe Staff.* Retrived from ttps://www.bostonglobe.com/business/2019/01/28/trump-has-this-one-right-china-real-national-security-threat/5Y8dVFUBkAY4Ud3LENemSO/story.html.

Lyons, K., Ho, V., & Durkin, E. (2019, February 24). Guaidó: military should disown leader who burns food in front of the hungry – as it happened. *The Guardian.* Retrived from https://www.theguardian.com/world/live/2019/feb/23/venezuela-brazil-border-aid-live-news-latest-updates.

Segan, S. (2019, January 3). What is 5G?. *PCMag Asia.* Retrived from https://sea.pcmag.com/cell-phone-service-providers-products/15385/what-is-5g.