29th
ASIA-PACIFIC
ROUNDTABLE
1 - 3 JUNE 2015, KUALA LUMPUR, MALAYSIA

ISIS MALAYSIA

ASEAN-ISIS

PS 5 (c)

PLENARY SESSION FIVE
2 JUNE 2015

DEBATE: "CYBER CONFLICT IS SIMPLY A QUESTION OF WHEN, NOT IF"

by

Prof Dr Motohiro TSUCHIYA
Professor, Graduate School of Media and Governance,
Keio University
Japan

SPONSORS

UEM

The Embassy of
The People's Republic of China
in Malaysia

Konrad
Adenauer
Stiftung

JAPANFOUNDATION

NEW ZEALAND
FOREIGN AFFAIRS & TRADE

Cyber Conflict is Simply a Question of When, Not If

Motohiro Tsuchiya
Keio University
taiyo@sfc.keio.ac.jp

PLEASE DO NOT QUOTE:
This is for a debate session at the 29th Asia-Pacific Roundtable only.

Cyber Warfare Depends on Definitions

It is widely recognized that the possibility of cyber conflicts depends on how we define conflict. Thomas Rid argued "Cyber War Will Not Take Place."[1]BrandonValerianoand Ryan Maness pointed out that there have been quite few cases of real cyber warfare so far.[2]However, we cannot decisively deny the future possibilities of conflicts occurring. Very few scholars of international relations foresaw the collapse of the Soviet Union in 1991, the Al Qaeda terrorist attacks on September 11, 2001, and, indeed, the rise of Islamic State in 2014. While the results of electionsin developed countries would appear to berelatively predictable, the result of the UK general election of May 2015 surprised many political science scholars. Predictions regarding the future remain contingent on many factors that we cannot completely grasp.

In this sense, the position presented in this paper can be little morethat a statement of an uncertain future. Despite all the uncertainties and intangibles, it seems impossible to deny the higher possibility of cyber conflicts emerging in the near future. As several documents released by the United States Department of Defense have pointed out, operational domains are expanding from the traditional land, sea, and airdomains to outer space and cyberspace. Different from the other four domains, cyberspace is an artificial domain that simultaneously impinges on, overlapswith, and connects those four domains. Cyberspace, if you like, has become a kind of nervous system that

[1] Thomas Rid, *Cyber War Will Not Take Place*, London: Hurst and Company, 2013.
[2]BrandonValeriano, and Ryan Maness, "The Fog of Cyberwar: Why the Threat Doesn't Live Up to the Hype,"*Foreign Affairs*, November 21, 2012.

increasingly seems to ever more intimately connect human and machineactivities. Should we expect conflicts to arise in any, or any combination, ofthe other four domains, it would be quite natural that the nervous connective system between them will also be targeted.

It is less probable to see cyber conflicts that are boxed in cyberspace and that have serious impacts. There are numerous cyber incidents that arise on almostan everyday basis, but they do not cause human losses or physical damage. Take, for example, the First Web War, which involved Estonia in 2007, which was based on DDoS (Distributed Denial of Services) attacks. Such methods were used in the attacks against the U.S. and the Republic of Korea (ROK) in 2009, and against Japan in 2009, and there are many other examples. Cyber espionage cases are almost countless. FireEye, an American security company, disclosed cyber operations such as APT 1, APT 28, and APT 30. Other companies have also revealed cyber operations such as Dragonfly, Putter Panda and DarkHotel. Both Sony Pictures Entertainment and J.P. Morgan Chase lost confidential information in 2014.If we were to name these issues in all their varieties as"Cyber Conflicts," then we can indeed logically say that cyber conflicts are already prevalent. However, the intention of this debate probably goes beyond a specific interpretation of such cyber operations and activities.Such activities, in all their diversity, can be labeled cyber "operations,"rather than cyber "conflicts."

So, beyond this, are there any possibilities of cyber conflicts that go beyond our notion of the rubric of cyber operations?If we assume that cyber conflicts remainboxed in cyberspace, then, probably no. If we assume, however, cyber conflicts combined with physical or kinetic methods, very probably yes. Combinations of cyber and kinetic attacks will have higher probabilities of occurringin the near future. Some cases have set a precedent for such combination attacks. They wereSyria in 2007, Georgia in 2008, and Iran in 2010.

Protection of Critical Infrastructures

Looking back at the history of information, technology and communication before the Internet, telecommunications infrastructures were always under attack in wartime emergencies. During World War I,for example, German submarine cables were cut except for one that connected Sweden, which was a neutral county at that time. However, this last cable was also tapped by the United Kingdom, which was predominantly in control of the world's telegraphic cable systems at the time. In fact, wiretapping of German communications led to the Zimmermann-Depesche incident in 1917, in which a message sent by German Foreign Minister Arthur Zimmermann to persuade Mexico to start a war against the U.S. was intercepted and its encryption was broken. The revelation of the message led the U.S. to join World War I on the side of the UK.In addition, attacks against telecommunicationssystems were also seen during World War II. There were submarine cables in the Pacific Ocean, which were laid by Germany. Japan took them over following the defeat of Germany at the end of World War I. However, those cables were also targeted during World War II. For example, Palau in the Pacific used to be connected to a submarine cable, but the connection was lost during World War II, and it has yet to have been reestablished to this day.

Until the 1960sit was relatively easy to identify which country owned a given communication infrastructure, which then comprised of assets such as telegraphic/telephone cables, artificial satellites and other components. However, the privatization and liberalization of telecommunications markets that started in 1980s has made it increasingly more difficult to identify nationality of such infrastructures. As it became ever more risky for one company alone to invest in a submarine cable system, operators have gradually worked towards pooling risks and resources and formed consortiums to build and lay submarine cable systems. A situation has developed in which the protection of communications infrastructures has gone beyond the more traditional scope of national security. In 1989, for example, the first optic fiber submarine cable was laid between the U.S. and Japan, heralding the explosion of bandwidth demand that has developed over the last 20 years, which has accelerated the need of operators to build more cables. The growing popularity of the Internet and digital technologies has, concomitantly, created a deep level of societal dependence on such technologies. Telephone systems technology hasmoved from analog to digital circuits, and postal services are increasinglybeing substituted by the use of e-mail. Mail order businesses have rapidly transferred into online shopping services. Most financial transactions are now made online. Both government-related and medical services are increasingly utilizing digital technologies. Even if they are not connected to the Internet directly, many services are adopting the use of Internet protocols.

Therefore, combination attacks of cyber and kinetic methodshave the increasing potential to cause increasingly serious levels of damage and collateral effects in today's digitally connected society and economy. Digital technologies require electric power, so that attacks against power generation and transmission systems will have serious impacts. The original idea of the Internet was to provide an alternative communications network that was designed to survive a nuclear attack. The Internet today might survive a few or several attacks against its architecture, and we would be able to communicate even with some delays. Nevertheless, today's financial transactions are completed in a millisecond (1/1,000 second) or a microsecond (1/1,000,000 second). In a situation where traffic is forced to be rerouted around the world to avoid a disconnected point, a financial company will lose its competitiveness. If it happens in a country, the country will lose its competitiveness and trust. If it happens in many points of the world at the same time, the international economic system might collapse.

Japan is a maritime country that is composed of four main islands, the Okinawa islands and other small islands. Ninetynine percent of Japan's international telecommunications traffic passes through submarine cables. Australia is a continent, but its distant location from other continents makes it depend on submarine cables,which connect it to the global economy. The U.S. might be a continental country with its large land mass and oil and other natural resources, but, as James Kurth argues, the U.S. economy needs the world economy more than the world economy needs the U.S. economy.[3]In that sense, the U.S. is also dependent on communications infrastructures. In today's digitalized global economy, the protection of communications infrastructures has become critical and is one of the top security agendas.

Cyber Deterrence

It was said that deterrence in cyber security was impossible. The attribution

[3]James Kurth, "Migration and the Dynamics of Empire," *The National Interest*, no. 71, Spring 2003, pp. 5-16.

problem,which makes it extremely problematical to identify real attackers hiding in the clouds of the Internet,makes it difficult to set up a situation to deter a first strike. But some of recent discussions point out that cyber deterrence is working, at least among nation states. Jason Healey said that deterrence "is actually keeping an upper threshold to cyber hostilities."[4]Even if we see some signs of combination attacks, a cyber total war has not yet broken out between the U.S. and other countries including China, Russia, Iran, and North Korea. On May 8th, the Chinese and the Russian governments agreed to not launch cyber attacks against each other.[5]

Furthermore, the Group of Governmental Experts (GGE) under the first committee of the United Nations General Assembly has been discussing international norms, confidence building measures (CBMs) and capacity building for the past several years. Cyberspace Conferences in London (2011), Budapest (2012), Seoul (2013) and The Hague (2015) also discussed similar issues. Cyber security is becoming one of the major diplomatic issues to be discussed among governments. In that sense, it seems that the possibilities of a cyber "Pearl Harbor" have been greatly reduced.

However, if you take up a realist position in international relations theory, there are always possibilities of cyber conflicts. Kenneth N. Waltz, a leading scholar of structural realism, once pointed out that analysis of actors such as human beings and nation states is insufficient to understand real reasons for wars.[6]In addition to the characteristics of actors, we need to understand structures of international systems that plunge political leaders into thinking of war options. Hindsight always tells us that any reason for starting a war is ridiculous, but,sometimes, political leaders make irrational decisions to avoid personal or organizational disgrace. We still cannot discard the possibilities of a cyber Pearl Harbor attack. Rather, one could be even imminent.

[4] Jason Healey, "Commentary: Cyber Deterrence Is Working: Dynamics Are Similar to the Cold War Nuclear Standoff," *Defense News*<http://www.defensenews.com/article/20140730/DEFFEAT05/307300017/Commentary-Cyber-Deterrence-Working?odyssey=nav%7Chead > July 30, 2014.

[5]Olga Razumovskaya, "Russia and China Pledge Not to Hack Each Other," *Wall Street Journal*<http://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/>May 8, 2015.

[6] Kenneth N. Waltz, *Man, the State, and War: A Theoretical Analysis*, New York: Columbia University Press, 2001.

Japan’s National Security in Cyber Space

The National Diet of Japan passed the Cyber Security Basic Act in early November 2014. In Japan, aBasic Act usually sets mid-term and long-term policy directions. The 2014 Cyber Security Basic Act was designed to fulfill the policy goals set by the 2013 Cyber Security Strategy. One of them was to strengthen the roles and functions of the NISC. The NISC used to be an acronym of the National Information Security Center. The Basic Act changed NISC into theNational center of Incident readiness and Strategy for Cybersecurity. The Information Security Policy Council (ISPC) was also reorganized as the Cyber Security Strategy Headquarters (CSSH). Both of the NISC and the CSSH gained more authority. Japan is stepping up its state of readiness regarding cyber security.

Cyber security these days includes defense, offense and exploitation. Exploitation refers to unusual ways of using technologies and architectures beyond their original intentions. Exploitation can therefore refers to, for, example, military commands accessing enemy systems to look for vulnerabilities, dig security holes, penetrate systems, and implant cyber weapons for future operations. Low-intensity cyber conflicts are taking place even in peacetime. Japan is subjected to more attacks in cyber space than in any and all of the other four operational domains, and needs to invest more to defend its social systems and infrastructures.

The Japanese term “joho” includes data, information, and intelligence. Joho security is one of the most necessary policy items in the Japanese government. The Constitution of Japan does not allow the overseas dispatch of troops and restrictsthe use of force, and offensive weapons. Bolstering intelligence, surveillance and reconnaissance (ISR) is the key to improve Japan’s national security. That is why Japan needs to strengthen its focus on joho security, both inside and outside cyber space.

Japan is assuming that a cyber conflict might break out today, tomorrow, or anytime in the near future. Japan’s headache in terms of cyber security focuses on the 2020 Tokyo Olympics. How we can defend the nation before, during, and after the Olympics is now a

Japan's top-priority cyber security agendas. Japan welcomes an international alliance to promote better cyber security.