29th ASIA-PACIFIC ROUNDTABLE

Cyber Conflict is Simply a Question of When, Not If

Motohiro Tsuchiya

THE APR SERIES
E-Monograph

Cyber Conflict is Simply a Question of When, Not If

Motohiro Tsuchiya

The APR Series
E-Monograph

INSTITUTE OF STRATEGIC AND
INTERNATIONAL STUDIES (ISIS) MALAYSIA

Published by
Institute of Strategic and International Studies (ISIS) Malaysia
1 Persiaran Sultan Salahuddin
PO Box 12424
50778 Kuala Lumpur
Malaysia
www.isis.org.my

The views and opinions expressed in this book are those of the author and may not necessarily reflect those of ISIS Malaysia.

Cyber Conflict is Simply a Question of When, Not If

Cyber warfare depends on definitions[1]

It is widely recognised that the possibility of cyber conflicts depends on how we define conflict. Thomas Rid argued, "Cyber war will not take place."[2] Brandon Valeriano and Ryan Maness pointed out that there have been quite few cases of real cyber warfare so far.[3] However, we cannot decisively deny the future possibility of conflicts occurring. Very few scholars of international relations foresaw the collapse of the Soviet Union in 1991, the Al Qaeda terrorist attacks on 11 September 2001, and, indeed, the rise of the Islamic State in 2014. While the results of elections in developed countries would appear to be relatively 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 more than 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 air domains to outer space and cyberspace.[4] Different from the other four domains, cyberspace is an artificial domain that simultaneously impinges on,

[1] This paper was presented in the debate session at the 29th Asia-Pacific Roundtable (APR) organised by ISIS Malaysia on 2nd June 2015.

[2] Thomas Rid, *Cyber War Will Not Take Place*, London: Hurst and Company, 2013.

[3] Brandon Valeriano, and Ryan Maness, "The Fog of Cyberwar: Why the Threat Doesn't Live Up to the Hype," *Foreign Affairs*, 21 November 2012.

[4] United States Department of Defense, *Quadrennial Defense Review*, http://www.defense.gov/qdr/, February 2010.

overlaps with, and connects those four domains. Cyberspace, if you like, has become a kind of nervous system that increasingly connects human and machine activities in an intimate way. Should conflicts arise in any of the 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. Numerous cyber incidents arise on almost an everyday basis, but these do not cause human losses or physical damage. Take, for example, the First Web War, which involved Estonia in 2007, based on Distributed Denial of Services (DDoS) attacks. Such methods were used in the attacks against the United States and the Republic of Korea in 2009,[5] 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,[6] APT 28,[7] and APT 30.[8] Other companies have also revealed cyber operations such as Dragonfly,[9] Putter Panda,[10] and DarkHotel.[11] Both Sony Pictures Entertainment and JP Morgan Chase lost confidential information in 2014. If we were to name these issues in all their varieties

[5] Motohiro Tsuchiya, “Cybersecurity in East Asia: Japan and the 2009 Attacks on South Korea and the United States,” in Kim Andreasson (ed.) *Cybersecurity: Public Sector Threats and Responses*, Boca Raton, FL: CRC Press, 2012, pp. 55–76.

[6] Mandiant, “APT1: Exposing One of China’s Cyber Espionage Units” Mandiant http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf, 2 March 2013 (accessed on 22 May 2014). Mandiant was merged with FireEye.

[7] FireEye, “APT28 — A Window Into Russia's Cyber Espionage Operations?” FireEye https://www2.fireeye.com/apt28.html (accessed on 13 July 2015).

[8] FireEye, “APT30: The Mechanics Behind a Decade Long Cyber Espionage Operation,” FireEye https://www2.fireeye.com/WEB-2015RPTAPT30.html (accessed on 13 July 2015).

[9] Symantec, “Emerging Threat: Dragonfly / Energetic Bear — APT Group,” Symantec http://www.symantec.com/connect/blogs/emerging-threat-dragonfly-energetic-bear-apt-group (accessed on 13 July 2015).

[10] CrowdStrike Global Intelligence Team, “CrowdStrike Intelligence Report: Putter Panda,” CrowdStrike http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf, June 2014 (accessed on 18 June 2014).

[11] Kaspersky Lab, “The Darkhotel APT: A Story of Unusual Hospitality,” Kaspersky Lab https://securelist.com/blog/research/66779/the-darkhotel-apt/ (accessed on 13 July 2015).

as "cyber conflicts," then we can logically say that cyber conflicts are already prevalent. However, the intention of this debate[12] 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? The answer is probably no if we assume that cyber conflicts remain boxed in cyberspace. However, if we assume that cyber conflicts combined with physical or kinetic methods, then the answer is probably yes. Combinations of cyber and kinetic attacks will have higher probabilities of occurring in the near future. Some cases have set a precedent for such combination attacks. They were Syria 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, the telecommunications infrastructure was 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 country at that time. However, this last cable was also tapped by the United Kingdom, which was predominantly in control of the world's telegraph cable system 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 United States was intercepted and its encryption was broken. The revelation of the message led the United States to join World War I on the side of the United Kingdom. In addition, attacks against the telecommunications system was also seen during World War

[12] See footnote 1.

II. There were submarine cables in the Pacific Ocean laid by Germany. Japan took over them 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 be reestablished to this day.

Until the 1960s, it was relatively easy to identify which country owned a given communication infrastructure, which consists of assets such as telegraph/telephone cables, artificial satellites and other components. However, the privatisation and liberalisation of the telecommunications market that started in the 1980s have made it increasingly more difficult to identify the nationality of such infrastructure. 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 have gone beyond the traditional scope of national security. In 1989, for example, the first optic fiber submarine cable was laid between the United States and Japan, heralding the explosion of bandwidth demand that has developed over the last 20 years. This has accelerated the need for 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 has moved from analog to digital circuits, and postal services are increasingly being 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 utilising 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 methods have the increasing potential to cause serious levels of damage and collateral effects in today's digitally connected society and economy. Digital technologies require electric power hence attacks against power generation and transmission systems will have serious impacts. The original idea of the Internet was to provide an alternative communications network 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. 99 per cent of Japan's international telecommunications traffic passes through submarine cables. Australia is a continent, but its distant location from other continents makes it dependent on submarine cables to connect to the global economy. The United States might be a continental country with its large land mass and oil and other natural resources, but, as James Kurth argues, the US economy needs the world economy more than the world economy needs the US economy.[13] In that sense, the United States is also dependent on communications infrastructures. In today's digitalised 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 problem, which makes it extremely problematic to identify

[13] James Kurth, "Migration and the Dynamics of Empire," *The National Interest*, No. 71, Spring 2003, pp. 5–16.

real attackers hiding in the clouds of the Internet, makes it difficult to set up a situation to deter a first strike. But some 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."[14] Even if we see some signs of combination attacks, a cyber total war has not yet broken out between the United States and other countries including China, Russia, Iran, and North Korea. On 8th May 2015, the Chinese and the Russian governments agreed to not launch cyber attacks against each other.[15]

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 reduced.

However, if one takes 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.[16] 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

[14] 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, 30 July 2014.

[15] 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/, 8 May 2015.

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

us that any reason for starting a war is ridiculous, but, sometimes, political leaders make irrational decisions to avoid personal or organisational disgrace. We still cannot discard the possibilities of a cyber Pearl Harbor attack. Rather, one could be even imminent.

Japan's national security in cyber space

The National Diet of Japan passed the Cyber Security Basic Act in early November 2014. In Japan, a basic 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 the National center of Incident readiness and Strategy for Cybersecurity. The Information Security Policy Council (ISPC) was also reorganised as the Cyber Security Strategy Headquarters (CSSH). The NISC and the CSSH have 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. 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 encounters more attacks in cyber space compared to 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 restricts the 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 one of Japan’s top-priority cyber security agendas. Japan welcomes an international alliance to promote better cyber security.

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

Motohiro Tsuchiya is Professor at the Graduate School of Media and Governance in Keio University. Prior to joining the Keio faculty, he was Associate Professor at the Center for Global Communications (GLOCOM), International University of Japan. He was an expert member of the Information Security Policy Council (ISPC) of the Japanese government from 2009 to 2013. He authored *Cyber Security and International Relations* (Chikura Shobo, 2015, in Japanese), *Cyber Terror* (Bungeishunju, 2012, in Japanese), and co-authored more than 20 books, including *Cybersecurity: Public Sector Threats and Responses* (CRC Press, 2012, in English). He earned his BA in Political Science, MA in International Relations, and PhD in Media and Governance from Keio University.

INSTITUTE OF STRATEGIC AND INTERNATIONAL STUDIES (ISIS) MALAYSIA

The Institute of Strategic and International Studies (ISIS) Malaysia was established on 8 April 1983 as an autonomous, not-for-profit research organisation. ISIS Malaysia has a diverse research focus which includes economics, foreign policy, security studies, nation-building, social policy, technology, innovation and environmental studies. It also undertakes research collaboration with national and international organisations in important areas such as national development and international affairs.

ISIS Malaysia engages actively in Track Two diplomacy, and promotes the exchange of views and opinions at both the national and international levels. The Institute has also played a role in fostering closer regional integration and international cooperation through forums such as the Asia-Pacific Roundtable (APR), the ASEAN Institutes of Strategic and International Studies (ASEAN-ISIS), the Pacific Economic Cooperation Council (PECC) and the Network of East Asian Think-Tanks (NEAT). ISIS Malaysia is a founding member of the Council for Security Cooperation in the Asia-Pacific (CSCAP) and manages the Council's Secretariat.

As the country's premier think-tank, ISIS Malaysia has been at the forefront of some of the most significant nation-building initiatives in the nation's history. It was a contributor to the Vision 2020 concept and was consultant to the Knowledge-Based Economy Master Plan initiative.

INSTITUTE OF STRATEGIC AND INTERNATIONAL STUDIES (ISIS) MALAYSIA
No. 1, Persiaran Sultan Salahuddin,
P. O. Box 12424, 50778 Kuala Lumpur, MALAYSIA

Tel : +603 2693 9366
Fax : +603 2691 5435
+603 2691 3210
Email : info@isis.org.my
Web : www.isis.org.my

Institute of Strategic and
International Studies (ISIS) Malaysia

ISIS_MY