NEW AMERICA

Tim Maurer

CYBERSECURITY AND ASIA

September 2015

GLOBAL CYBERSECURITY NORMS AND RESILIENCE PROJECT | CYBERSECURITY INITIATIVE

AUTHORS
Tim Maurer, Director, Global Cybsersecurity Norms and Resilience Project and Head of Research, Cybersecurity Initiative

ABOUT THE GLOBAL CYBERSECURITY NORMS AND RESILIENCE PROJECT
The Global Cybersecurity Norms and Resilience Project pursues research-driven impact in support of these goals. Leveraging its multidisciplinary and diverse network of experts across policy and tech communities, the project aims to provide thought leadership through new, independent research, ideas, and strategies with actionable recommendations at the nexus of international diplomacy, private sector and civil society actors, and security interests. The Global Cybersecurity Norms and Resilience Project feeds into New America's Cybersecurity Initiative, which consists of staff from its International Security Program and Open Technology Institute and addresses both the domestic and international dimensions of cybersecurity.

ABOUT THE CYBERSECURITY INITIATIVE
The Internet has connected us. Yet the policies and debates that surround the security of our networks are too often disconnected, disjointed, and stuck in an unsuccessful status quo. This is what New America's Cybersecurity Initiative is designed to address. Working across our International Security Program and the Open Technology Institute, we believe that it takes a wider network to face the multitude of diverse security issues. We engage across organizations, issue areas, professional fields, and business sectors. And through events, writing and research, our aim is to help improve cybersecurity in ways that work — for the countries, for companies

ACKNOWLEDGEMENTS
Special thanks to the participants at the "Identifying and Sharing Best Practices for Cyber Security" workshop on May 8, 2015, in Seoul, Korea, organized by the Jeju Peace Institute in collaboration and support with the National Security Research Institute. The authors responsible for this text appreciates the thoughtful contributions provided by workshop participants and have used our dialogue as a guide for drafting this paper.

PHOTO CREDIT COVER PHOTO - Shutterstock

Introduction

It was a historic moment. On Friday, December 19, 2014, only a few days before Christmas, President Obama went on television and blamed North Korea for the hack against Sony Pictures Entertainment. It was the first time that a cyber-security incident resulted in a U.S. President publicly accusing a foreign country on live television. Only six months prior, nobody in Washington would have expected that this scenario would be the event that would catapult cyber-security from the obscurity of nerdy discussions onto the highest level of politics and into the living rooms of people busy wrapping presents. It was less of a surprise that one of the parties involved is a country in Asia.

Asia is a microcosm of the complexities of cyber-security worldwide and has been one of the hot spots of cyber conflict. Many of the challenges that have made more significant progress difficult on a global scale also exist in this particular region. It starts with the divergence in Internet access among countries but also includes different approaches regarding how to think about cyber-security in the first place, not to mention the asymmetries that result from different capabilities and degrees of vulnerability. A sign of the region's importance in the broader cyber-security debate is the fact that U.S. Secretary of State, John Kerry, decided to use his visit to Korea in May 2015 to deliver an entire speech titled "An Open and Secure Internet: We Must have Both."[1]

This short paper will outline why and how the Internet has been used for political and military purposes in the region and what is being done to address it. This document therefore focuses on cyber-security as it relates to regional and international security; other dimensions of cyber-security, for example cyber-crime and economic espionage, are outside the scope of this paper.

The Problem: Cyber(in)security as a New Source of Instability

Very few people still doubt that cyber-security has become an important dimension of international peace and security. However, the underlying causes and dynamics remain poorly understood. An unfortunate, negative side-effect of the Internet and the increasing digitalization of infrastructures has been that actors have learned to exploit the technology and to develop malware as a substitute for conventional weapons in some cases and a more powerful tool to expand espionage through signals intelligence. With that said, the new technologies also have a set of unique features that have enabled new types of activity that can undermine international stability and security.

Assistant Secretary of Defense Eric Rosenbach, the Pentagon's principal cyber advisor, provided a good illustration conceptualizing cyber-security within the broader security context, saying "The place where I think it will be most helpful to senior policymakers is what I call in 'the space between'. What is the space between? ... You have diplomacy, economic sanctions...and then you have military action. In between there's this space, right? In cyber, there are a lot of things that you can do in that space between that can help us accomplish the national interest."[2]

In a nutshell, cyberspace inserted a new slice in the Clausewitzian spectrum of war being "the continuation of politics by other means." If we think of international politics as human behavior ranging from cooperative and non-violent to confrontational and violent behavior with the use of force and armed attack being the threshold for the latter, cyberspace added a new segment just underneath this threshold. While it offers new substitutes for conventional tools that cause the same effect – swapping malicious code for a bomb – it also enables entirely novel actions such as manipulating financial data. This is what makes cyber-security a new and unique (manmade) phenomenon in international security

representing a new strategic and, at present, destabilizing effect in international relations as more and more actors are exploring and exploiting these new possibilities.

To be more specific, one of the main reasons intrusions into computer systems are having a destabilizing effect on international relations is because it is much more difficult to tell the difference between reconnaissance and an imminent attack. During the Cold War, the U2 plane over a country's territory did not pose a direct threat because it was built for reconnaissance (which could be used for a future attack), whereas a B-52 bomber was built to attack. In cyberspace, that line is much blurrier. It is much harder to discern whether the plane that's gained unauthorized access into one's space was built for reconnaissance or an attack. In other words, having detected an intrusion it's much harder to know if you are dealing with a U2 or a B-52. This uncertainty carries significant, new risk for mistrust, miscalculation, and accidents.

As a region, Asia is emblematic of all of these trends. It has been a regional hotspot of malicious cyber activity, exploiting the possibilities offered by this new space as part of the broader political conflicts that continue to plague the region. Past incidents range from fairly unsophisticated political hacktivism that has occurred across the continent over the past 15 years[3] to the recent reports about the very sophisticated but failed Stuxnet-like attempt to attack the North Korean nuclear weapons program.[4] Similar to the "hidden conflict" playing out in and through cyberspace in the Middle East,[5] a similar prolonged dynamic can be identified on the Korean peninsula. Here, the low-level web defacements and Distributed Denial of Service attacks have become increasingly complex and accompanied with more serious hacking activity including those targeting financial institutions in the Republic of Korea in 2013.[6] The latter incident is a particularly insightful example of the potential risk of miscalculation due to the attribution problem when it comes to cyber-security: the South Korean government first mistakenly identified China as the source of the malicious activity only to correct later that the Internet Protocol address had been an internal one used by a financial institution that happened to match one registered in China.[7]

International Efforts to Address the Problem

The technologies forming cyberspace are manmade. Cyber-security can therefore be increased by improving the technology. However, the threats emanating from cyberspace are ultimately not the result of the technology itself but how people choose to use the technology. It is therefore primarily a social rather than a technological problem. The incentives to exploit the technology for economic or political gains will only increase in the foreseeable future as more and more people and devices connect to the Internet. For example, over the next five years, an additional two billion people alone are expected to gain access to the Internet. And of the more than five billion people yet to gain access to the Internet, more than half live in just five Asian countries – Bangladesh, China, India, Indonesia, and Pakistan.[8]

The overarching goal of the diplomatic efforts to date has been to agree to norms governing behavior in cyberspace. These discussions can be broken down into three components: norm contestation, norm translation, and norm emergence.

At first, there was disagreement in the international community whether existing international law and norms already apply to cyberspace or if the international community should develop new laws specific to cyberspace. A few countries, China, in particular, were a proponent and promoter of the latter approach. However, in 2013, the UN Group of Governmental Experts comprised of representatives form 15 countries including China, published a consensus report affirming that "international law and in particular the United Nations Charter, is applicable."[9]

In parallel, experts have been investigating how to translate these existing norms to cyberspace. The most comprehensive effort to date is the Tallinn Manual on the International Law Applicable to Cyber Warfare published in 2013. It examines how existing international law governing activity above the threshold of use of force and armed attack could apply to cyberspace. It was

developed by a group of fifteen legal experts under the auspices of NATO's Cooperative Cyber Defence Center for Excellence.

Arguably the most important dimension of the diplomatic efforts focuses on norm development for the types of activities that are currently not covered by existing international law which encompass the vast majority of malicious activity witnessed to date, for example, the targeted hacks of South Korean financial institutions. This area has moved to the center of the cyber-security community's attention and the Tallinn Manual 2.0 expected in 2016 is only one example of an increasing flurry of activity focusing on this issue.[10]

A key stumbling block to more significant progress in this area has been the different approaches to cyber-security overall. Again, the regional dynamics in Asia also highlight the global challenge. Whereas Japan and the U.S. only recently reaffirmed their commitment "to ensure the safe and stable use of cyber space based on the free flow of information and an open internet,"[11] the Chinese government supports the notion of information security as proposed in the International Code of Conduct for Information Security that calls for international cooperation to curb "the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment."[12]

International cyber-security cooperation generally includes both the exchange of information and capabilities. Cyber threat and incident exchange, especially within the critical infrastructure community, has seen limited success due to a set of understandable yet not-insurmountable challenges and barriers. Sharing an incident may reveal weak points within a victim's infrastructure and may cause the victim to be perceived as not capable of maintaining adequate cyber protection. Poor quality information, misaligned economic incentives stemming from reputational risks, privacy concerns, and poor management rank highest in challenges to information sharing, followed by legal barriers related to fear of legal or regulatory action, fear of leaks, norms of rivalry and misaligned economic incentives stemming from group behavior and poor decision-making about investment in security.[13] Barriers to participation in information sharing relationships included lack of advocacy from organizational managers, prohibitions against information disclosure at the organizational and national levels, and a shortage of technical depth and breadth from sharing participants. Issues related to information sharing require a concerted effort on the part of national authorities to understand how to best incentivize organizations to exchange cyber threat and incident data within their relevant communities.

Establishing proven incentives for cyber threat and incident exchange needs to be a top priority for public and private Critical Infrastructure (CI) owners. Their experiences and knowledge are central to the safety and security of their infrastructure and contribute towards national security interests. Another aspect to information sharing that is problematic is how each nations views cyberspace from both a service provided to their population as well as a domain used for military engagement. Information moving between organizations may also be seen as problematic. Moreover, while some countries in Asia exclude discussions over content from cyber-security discussions given their strong commitment to human rights and freedom of expression, other countries view content as an integral part of them. What terms governments use mirrors this divide as highlighted in a document the British government submitted to the United Nations. The document points out that many companies use the term 'information security' but the document highlights that the term "is also used by some countries and organizations as part of a doctrine that regards information itself as a threat against which additional protection is needed."[14]

This difference is one of the reasons a political agreement at a regional or international level on cyber-security has been difficult to reach. The Shanghai Cooperation Organization, for example, has been the incubator for the aforementioned International Code of Conduct for Information Security, which China, Russia, Tajikistan, and Uzbekistan jointly submitted to the United Nations in 2011. Because of its broad definition of information security, among other reasons, the proposal was rejected by other governments around the world, as were calls for an international treaty on cyber-security. The political divisions in Asia are therefore similar to those that exist at the global level while other regions, for example, Europe or countries in the Western hemisphere have a more uniform approach to this issue.

In order to make progress politically, states have therefore been increasingly focused on confidence-building measures during the past five years. Building on existing institutions and mechanisms, namely the Organization for Co-operation and Security in Europe (OSCE) and bilateral channels, there have been several agreements such as the OSCE's Initial Set of OSCE Confidence-building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies that aim to support greater transparency and cooperation among states.[15] A similar effort is being pursued through the ASEAN Regional Forum which has organized a series of workshops on the topic.[16]

Apart from the political process, it is important to note that regional cooperation does exist at a technical level and among law enforcement agencies. For example, in 2013, the national Computer Security Incident Response Teams (CSIRTs) of China, Japan, and Korea met for the first Annual Meeting for Cybersecurity Incident Response. According to the joint statement, "the Parties confirmed that, over the years, they have successfully prevented unnecessary escalation of crises relating to the management of hacking and other critical events concerning China, Japan and Korea."[17] In addition, the Asia Pacific Computer Emergency Response Team (APCERT) is a transnational network of computer security experts in the Asia Pacific region from 27 CSIRTs. APCERT seeks:

"to improve the region's awareness and competency in relation to computer security incidents through:
* Enhancing Asia Pacific regional and international cooperation on information security;
* Jointly developing measures to deal with large-scale or regional network security incidents;
* Facilitating information sharing and technology exchange, including information security, computer virus and malicious code among its members;
* Promoting collaborative research and development on subjects of interest to its members;
* Assisting other CERTs and CSIRTS in the region to conduct efficient and effective computer emergency response;
* Providing inputs and/or recommendations to help address legal issues related to information security and emergency response across regional boundaries."[18]

Hampering international efforts in the region to address cyber-security is the dramatic discrepancies among countries. As a recent report by the Australian Strategic Policy Institute titled Cyber Maturity in the Asia-Pacific Region 2014 points out, the region is "home to some of the world's least networked countries, such as Myanmar (1.1% internet penetration) and Cambodia (4.9%) plus some of the most networked, including South Korea (84.1%) and Japan (79.1%)."[19] And this discrepancy is not limited to Internet penetration rates. It also extends to the maturity of countries' policies and institutions. Cyber-security is a higher priority in some countries compared to others and "capacity and implementation are likely to remain major hurdles for many countries in the region," such as Cambodia, Indonesia, Malaysia, Philippines, and Thailand.[20] India and China have made cyber-security a top priority in recent years but both giants also face significant enforcement limitations.

Conclusion

The Internet has enabled new ways to connect people and machines. It has also opened new avenues for innovation and economic growth. At the same time, it has created new risks that more and more actors are learning to exploit for their own gain. This poses challenges for governments around the world even in regions that have been peaceful and stable for decades with countries that are well developed and the capacities in place to adapt to the changing technological environment.

In preparation for the next workshop in this series, we suggest focusing on three challenges:
1. How is regional stability benefited through information sharing?
2. What is the relationship between CI providers and their national regulatory authorities and security agencies?
3. How should crisis management and transnational cooperation (e.g. cooperation between Korea, Japan and China CERT/CC) be structured for mutual benefit?

In Asia, regional stability is fragile and security can be a daily struggle. Facing the additional stress of having to adapt to a new technological environment, including new vulnerabilities and asymmetric relations, further contributes to the escalatory risk arising from miscalculation in a new context. Mechanisms for co-operation do exist but become easily entangled in the many unresolved political tensions between the countries in the region—even among those that are allies of the U.S. As a result of this dynamic, Asia likely remains a hotspot of cyber conflict, requiring a more concerted effort to improve cyber-security.

Endnotes

1. Kerry, John. 2015. "An Open and Secure Internet: We Must Have Both." Remarks at Korea University. May. 18. <http://www.state.gov/secretary/remarks/2015/05/242553.htm>.

2. Lewis, Jim. 2014. "Cyber Leaders: A Discussion with the Honorable Eric Rosenbach." Center for Strategic and International Studies. Oct. 2. <http://csis.org/event/cyber-leaders>.

3. See, for example, in the context of the political conflict between India and Pakistan as well as between China and Japan over the Senkaku Islands.
Hooper, D. Ian. 1999. "Kashmir-minded Pakistani 'hacktivists' blitz Web sites." CNN.com. Oct. 8. <http://www.cnn.com/TECH/computing/9910/08/pakistani.hack/>. And Muncaster, Phil. 2012. "Chinese hacktivists launch cyber attack on Japan." The Register. Sept. 21. <http://www.theregister.co.uk/2012/09/21/japan_china_attack_sites_senkaku/>.

4. Menn, Joseph. 2015. "Exclusive: U.S. tried Stuxnet-style campaign against North Korea but failed – source." Reuters. May 29. <http://www.reuters.com/article/2015/05/29/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529>.

5. Lewis, James Andrew. 2014. "Cybersecurity and Stability in the Gulf." Center for Strategic and International Studies. Jan. <http://csis.org/files/publication/140106_Lewis_GulfCybersecurity_Web.pdf>.

6. Kwon, K.J, Jethro Mullen and Michael Pearson. 2013. "Hacking attack on South Korea traced to Chinese address, officials say." CNN.com. Mar. 21. <http://www.cnn.com/2013/03/21/world/asia/south-korea-computer-outage/>

7. Kim, Jack and Ju-min Park. 2013. "Cyber-attack on South Korea may not have come from China after all: regulator" Reuters. Mar. 21. <http://www.reuters.com/article/2013/03/22/us-cyber-korea-idUSBRE92L07120130322>

8. Jose, San. 2011. "Global Internet Traffic Projected to Quadruple by 2015" Cisco. June. 01. <http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=324003>

9. United Nations General Assembly. 2013. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of Information Security." UNGA. Jun. 24. <http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98>

10. NATO CCDCOE. "Research." NATO CCDCOE. <http://www.ccdcoe.org/research.html>.

11. Office of the Press Secretary. 2015. "U.S.-Japan Joint Vision Statement" The White House. April. 28. <https://www.whitehouse.gov/the-press-office/2015/04/28/us-japan-joint-vision-statement>

12. Badong, Li and Vitaly Churkin, Sirodjidin Aslov, and Murad Askarov. 2011. "Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General." United Nations General Assembly. Sept. 14. <https://www.ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf>.

13. Robinson, Neil and Emma Disley.2010 "Incentives and Challenges for Information Sharing in the Context of Network and Information Security" ENISA. Sept. 08. <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/incentives-and-barriers-to-information-sharing>

14. United Nations General Assmebly. 2013. "Developments in the field of information and telecommunications in the context of international security Report of the Secretary-General." United Nations General Assembly. Jul. 16. <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N13/397/35/PDF/N1339735.pdf?OpenElement>.

15. Permanent Council. "Decision No. 1106 Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming From the Use of Information and Communication Technology." Organization for Security and Co-operation in Europe. Dec. 3. <http://www.osce.org/pc/109168?download=true>.

16. Freakin, Tobias and Jessica Woodall. 2014. "Cyber confidence building in the Asia-Pacific: three big take-

aways from the ARF." The Strategist. Apr. 09. <http://www.aspistrategist.org.au/cyber-confidence-building-in-the-asia-pacific-three-big-take-aways-from-the-arf/>

17. CNCERT/CC, JPCERT/CC, KrCERT/CC. 2013 "The First China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response." JPCERT/CC. Aug. 09. <https://www.jpcert.or.jp/english/pub/2013/CJK_Joint_Statement2013.pdf>

18. APCERT. 2015. "Mission Statement." APCERT. <http://www.apcert.org/about/mission/index.html>.

19. Feakin, Tobias, Jessica Woodall and Klée Aiken. 2014. "Cyber Maturity in the Asia-Pacific Region 2014." ASPI. Apr. <https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2014/ASPI_cyber_maturity_2014.pdf>.

20. Feakin, Tobias, Jessica Woodall and Klée Aiken. 2014. "Cyber Maturity in the Asia-Pacific Region 2014." ASPI. Apr. <https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2014/ASPI_cyber_maturity_2014.pdf>.