The 2015 Northeast Asia Regional Young Leaders Security Seminar

A conference report, table-top exercise, and regional security primer

Edited by Brad Glosserman and Julia Gardner

PACIFIC FORUM CSIS

YOUNG LEADERS

Issues & Insights
Vol. 16-No. 14

Seoul, Korea
July 2016

Pacific Forum CSIS

Based in Honolulu, the Pacific Forum CSIS (www.pacforum.org) operates as the autonomous Asia-Pacific arm of the Center for Strategic and International Studies in Washington, DC. The Forum's programs encompass current and emerging political, security, economic, business, and oceans policy issues through analysis and dialogue undertaken with the region's leaders in the academic, government, and corporate areas. Founded in 1975, it collaborates with a broad network of research institutes from around the Pacific Rim, drawing on Asian perspectives and disseminating project findings and recommendations to opinion leaders, governments, and members of the public throughout the region.

The Young Leaders Program

The Pacific Forum Young Leaders program is a global community of emerging experts who have demonstrated interest in and aptitude for Asia-Pacific regional affairs. We seek to ensure that bridges between East and West grow stronger and peace prevails in the Asia-Pacific region and do this by bringing together several generations of experts in Asian affairs at Track 1.5 and Track 2 dialogues. We groom these next-generation leaders and help them to realize their potential through scholarship, mentorship, and partnership. Members – more than 1,000 in number, from more than 60 countries – are professionals and students from a wide range of fields, including government, academia, the private sector, the military, and think tanks, all between the ages of 25 and 35. Since the program was launched in 2004, 1,114 spaces have been offered at YL programs in 19 different countries. The Young Leaders program operates with the generous support of a number of individuals, think tanks, nongovernmental organizations, and foundations. For further information on the Young Leaders Program and how to get involved, please visit our website: http://csis.org/program/young-leaders-program or contact youngleaders@pacforum.org

Table of Contents

Acknowledgements

The Pacific Forum CSIS and I would like to acknowledge the support of several people and institutions that made this meeting and its products possible. We would first like to thank SK Group and its Chairman Choi Shin Won, whose support provided us with a beautiful conference venue in Seoul and a memorable experience for all. We would also like to point out the generous assistance of SKC staffer Lim SooJi, whose kindness, tireless effort and keen attention to detail made our meeting possible. I am also indebted to Young Leaders Program team members Sarah Henriet (assistant director) and Petra Kubalkova (fellow) who supported me and this meeting in myriad ways over the last two years.

We are tremendously grateful to the Embassy of the United States in Seoul and Ambassador Mark Lippert for giving us several hours of his time and sharing his wisdom. His team expertly facilitated the appearance and we recognize how fortunate we were to have had the chance to dialogue with Ambassador Lippert, a true practitioner of Northeast Asia diplomacy.

Thanks are especially due to the United States Japan Foundation whose support provided the means to bring American and Japanese Young Leaders to the table in Seoul to discuss these important issues. USJF is also supporting this publication and we are grateful for the opportunity to share our experiences with a wide audience. We must also thank Beijing Foreign Studies University, particularly Dean Li Yonghui and Professor Li Yongcheng, for bringing this meeting's first delegation from the People's Republic of China. Your support of our program and your participation in the meeting were invaluable.

Thank you to John Warden, Jim Platte, and Jenny Jun for their expert contributions and leadership in writing and managing the table-top exercise, and to Tristan Volpe for his analysis in the enclosed report. Thank you to the Young Leaders who participated as presenters and moderators: Seukhoon Paul Choi, Guanpei Ming, James Platte, Akira Igata, Yu Harada, Jenny Jun, Tong Zhao, and Jina Kim. We would also like to thank the senior expert reviewers who helped lend credence to the TTX by offering their critique of the scenario, particularly Jor-Shan Choi.

Finally, thank you to all the Young Leaders and alumni who attended the meeting in Seoul. They are to be credited for their creativity and intellectual contributions. We would also like to thank the Sasakawa Peace Foundation, the Japan-US Friendship Commission, the Kelly Fellowship Endowment, the Korea Foundation, and the Worldwide Support for Development/Dr. Haruhisa Handa Fellowship for their continuous support for our program and for providing us with the ability to bring Young Leaders to participate in these important conversations.

Julia Cunico Gardner
Director, Pacific Forum CSIS Young Leaders Program

Message from CHOI Shin Won
(Chairman & CEO of SK Networks Co. ltd)

I'd like to extend my special thanks to Pacific Forum CSIS President Ralph Cossa for giving me the opportunity to host the 2015 Northeast Asia Regional Young Leaders Security Seminar. I also wish to thank officials from the US Embassy Seoul, US-Japan Foundation, Beijing Foreign Studies University, and all the speakers and panelists for supporting the discussion of this Seminar. This is the second Young Leaders Security Forum hosted by SK, and I am pleased to see that in just one year, the Dialogue has expanded to include Young Leaders from the People's Republic of China. I welcome all of you to South Korea and I thank you for your passion and commitment to the region.

Northeast Asia is one of the most dynamic regions in the world, surrounded by tremendous opportunities but also difficult challenges. Distrust and historical tensions continue to affect politicians and pose a barrier to effective leadership, but 2016 has been marked by a significant milestone: the ROK-Japan Comfort Women Deal. Although the agreement was followed by much criticism, it is meaningful in that the two governments are trying to move past this sensitive issue and seek public support to do so. On a less positive note, North Korea continues to threaten the stability of the region. This calls for more coordinated cooperation among the ROK, US, Japan, and China – collaboration is the only way to cope with these continuous provocations and promote regional peace and security.

In this forum, the next-generation leaders gathered together and had a heated debate about the challenges and opportunities of the quadrilateral relationship. Young Leaders discussed a wide range of important issues – from the perceived ROK shift toward China and countries' expectations of Japan, to the role of China and the US in the region and multilateral collaboration on cyber, space, and nuclear issues. I was very impressed by the findings and the engagement level of the Young Leaders. This quadrilateral dialogue gave our next-generation thinkers an opportunity to understand each country's perspective and to establish a strong network of young Asia security experts. It is crucial to provide a safe venue for our Young Leaders to discuss innovative solutions to our region's challenges, and I sincerely hope they will always remember the value this Forum has offered.

As a member of Pacific Forum CSIS, I will pay consistent attention to training young professionals and do my utmost to contribute to ROK-US-Japan-PRC relations. I will be looking forward to your continued growth and development.

Thank you very much.

SK Group

SK Group is the second largest conglomerate in South Korea. It changed its name from Sunkyoung Group to SK Group in 1997. SK Holdings ranked 57th in the 2013 Fortune Global 500. SK Group has more than 70,000 employees who work from 113 offices worldwide. While its largest businesses are primarily involved in the chemical, petroleum, and energy industries, it also has South Korea's largest wireless mobile phone service provider, SK Telecom, and provides services in construction, shipping, marketing, local telephone, high-speed Internet, and the wireless broadband service WiBro. SK has further broadened its range of business to semiconductors, merging Hynix into SK Hynix, the world's second largest memory semiconductor manufacturer.

SK Networks Co. ltd

SK Networks Co. ltd, one of the affiliates of SK Group, was founded in 1953 which signaled a new start for the Korean economy which had been in a slump following the devastation of the Korean War. It was formerly known as 'Sunkyong Textiles', the forerunner of current SK Group. It had begun its operations by repairing 20 old weaving machines damaged during the war but succeeded to make tremendous growth and transformed into an export-leading company. In 1976, the company was awarded the 'USD 100 Million Export Tower and was officially designated as a general trading company by the Korean government. SK networks has continued to make development and expand into various business fields that it now carries out a broad range of businesses. It trades globally in chemicals, steels, coal and other high value-added products. It also distributes petroleum products to gas and LPG stations via nationwide network. Meanwhile, it operates as a prestige lifestyle provider of car-life services, ICT distribution, fashion, other high-quality consumer goods, and high-end services through clubhouses, restaurants, and hotel operations. SK networks is continuing to cater to the needs of its customers by offering best products and services, and by strengthening its primary competitiveness in its existing core businesses. In addition, it will develop and foster new growth engines such as the Car-Life service, consumer goods, and hotel service businesses.

Introduction

by Julia Gardner

The Northeast Asia Regional Young Leaders Security Seminar, which took place November 8-11, 2015 at the Sheraton Walkerhill in Seoul, Republic of Korea, is the only Pacific Forum CSIS Young Leaders meeting that does not rely on "senior experts" for wisdom, and thus depends on the experience and opinions of Young Leaders and their thoughtful engagement. We expect them to challenge assumptions and prove they have something to say.

The meeting convened November 9 at the picturesque Aston House, where US-ROK Wisemen's Council meetings took place in the early to mid-1990s; these sessions helped shape ROK-US relations then, just as we hope Young Leaders meetings will shape relations in the future. The first panel explored opportunities and challenges facing regional cooperation in Northeast Asia and featured presentations by senior Young Leaders from Japan, the United States, and the People's Republic of China, and it was moderated by a senior Young Leader from the Republic of Korea (ROK). The question and answer session exposed the volatility of the historical issues between Japan and the ROK and China, but the Young Leaders were able to agree to disagree and move forward amicably. The second panel assessed the evolving threats posed by the Democratic People's Republic of Korea and included presentations by senior Young Leaders from the US, China, and ROK, and was moderated by a Japanese Young Leader. The discussions introduced issues of traditional and nontraditional security, such as cyber and nuclear security and disaster relief, that laid the foundation for the later table-top exercise (TTX). Several presentations highlighted the need for Japan and the ROK to take the lead on security cooperation in Northeast Asia, since they have the most to gain and lose in the event of a crisis.

The Honorable Mark W. Lippert, US Ambassador to the ROK, and SK Chairman Choi Shin Won addressed the group over lunch. They discussed the importance of giving voice to the next generation of security experts, and applauded Pacific Forum's efforts to do so, and the role of the US in regional security in Northeast Asia. Young Leaders engaged in a robust question and answer session with Ambassador Lippert on issues relevant to the US-Korea relationship, the presence of US military forces around the world, and the situation with North Korea.

Monday afternoon kicked off the TTX that divided the Young Leaders into country groups (US, Japan, China, and ROK) and presented them with a scenario that involved nuclear accidents in Japan and Korea, possibly caused by cyberattacks. With limited information, the groups had to identify their first five actions, the first five messages they would deliver, and what they expected and hoped the other countries would and would not do. The TTX exposed fundamental differences in perceptions of attribution and intent, and the subsequent ability to deliver a proportional response. Tristan Volpe writes in his enclosed analysis that, "a key implication from the TTX is that the challenges faced by the Young Leaders in assigning attribution and devising a proportional response are not unique to digitally enabled attacks on critical infrastructure.

Rather, these are problems that countries have long had to address with covert action in general…how should the victim respond in the absence of a clear-cut *casus belli*?" Volpe's analysis and the TTX country reports that follow present each team's response to the crisis and to one another, and the obstacles they faced reaching a solution. Two items worth noting are: the China team was comforted by the Japan team's reluctance to react aggressively to the DPRK and saw this as an introduction to future China-Japan cooperation, and the ROK, China, and Japan teams were confident they could have direct, trilateral coordination without US involvement.

As you will read in the enclosed reports, the core competencies for both participating in and analyzing this exercise can be divided into six topics: cyber security, conventional threats from the Democratic People's Republic of Korea (DPRK), regional cooperation and improving HA/DR capability in Northeast Asia, Northeast Asia Regional Security Architecture, nuclear safety and security, and China's role in Northeast Asia. The second half of this publication is an exploration of these six areas that includes suggestions for further research and reading on the subjects. The authors have demonstrated interest and expertise on the subjects and have provided a solid foundation on which to build greater familiarity with these areas. We hope that by providing this foundation research, we give our table-top exercise and our conference a longer shelf-life and we hope that others run this scenario in their own groups.

The Pacific Forum CSIS Young Leaders program is built on the premise that establishing expertise and a network of young Asia security experts will pay dividends for peace in future years when they are able to discuss contentious issues in times of crisis with people they already know. This meeting, more than any other, provides a venue for that mission. We hope that readers will be inspired by the Young Leaders' diplomacy and scholarship presented here and will walk away with a renewed sense that peace and security in Northeast Asia will be in good hands.

Table-top Exercise

Move 1

It is October 2016. Tensions between North and South Korea ebb and flow with the historical cycle of North Korean provocation, North-South talks, and a temporary resolution to the crisis of the moment. Economic relations between the US and its allies remain strong, while trade between China and the Republic of Korea has expanded since the passing of an ROK-China free trade agreement. Thousands of Chinese tourists visit Korea and Japan each year, further deepening ties. Korea and Japan still struggle to forget their past, but have increased political-military cooperation.

On October 5, President Xi arrived in Seoul to meet with ROK President Park to discuss the China-ROK economic relationship. On the morning of October 6, Xi travelled with President Park to Busan to tour Korean manufacturing and shipping facilities.

Shortly after the 8:00AM shift change at the Kori Nuclear Power Plant (approximately 40 km north of the Port of Busan), unit 1 (Kori-1), Korea's oldest commercial nuclear reactor, experienced an unexpected and rapid rise in temperature. The reactor automatically performed an emergency shutdown, but the reactor temperature continued to rise due to an apparent failure of both the primary and emergency cooling systems. The site manager ordered that the other three units at Kori be shut down, and all efforts focused on stabilizing unit 1. Fearing a meltdown in unit 1, Korea Hydro & Nuclear Power (KHNP) officials notified the Nuclear Safety and Security Commission (NSSC) and the Blue House of the situation. By 1:30PM, Presidents Park and Xi were evacuated to a safe location in Seoul. KHNP officials briefed local media, and the Blue House said that all measures were being taken to stabilize the reactor and ordered a 20 km evacuation zone around Kori.

Shortly after 2:00PM, unit 1 of the Sendai Nuclear Power Plant in Kyushu, Japan also experienced an unexpected shutdown but did not lose emergency cooling to the reactor core. Since the Fukushima accident, the Japanese public remains distrustful of nuclear power and has already started to panic. It has only been slightly more than a year since Sendai went back online, and the Japanese people have little willingness to endure another nuclear disaster. An evacuation around Sendai has not been ordered. Kyushu Electric Power, Sendai's owner, is investigating the situation, and Japanese authorities are on standby in case reactor conditions degrade. While the two incidents appear to be similar, international intelligence agencies are thus far unable to explain their cause or whether they are related.

Overnight, staff at Kori were still unable to adequately restore cooling, and ROK officials ordered the reactors' vents opened. While the venting prevented potential explosions within the reactors, it results in a release of radioactive gas into the atmosphere, and the reactor's operators conceded that a partial meltdown certainly has occurred. Twenty-four hours into the nuclear accident, Kori-1 remains unstable,

and there are rumors circulating online and in the media that other nuclear facilities could suffer similar fates.

1) What are the first five actions you recommend in response to this emergency? (in order of priority)
2) What are the five messages that should be delivered (by whom, to whom, about what, and in what order?)
3) What do you expect from the other countries in the region? What do you want them to do/say? What do you not want them to do/say?

Intel update (move 1B)

Thirty-six hours after the start of the Kori-1 nuclear accident, international investigators and the US and ROK intelligence services each confirm that the information technology systems were hacked. Meanwhile, police in Busan detained a Kori plant worker who confessed to inserting infected USB drives into plant systems one month ago. The worker is a defector from North Korea and claims that North Korean agents in Busan blackmailed him by saying that his family in North Korea would be executed if he did not follow their orders. He also claims that he did not know what was on the USB drives or what would happen after he inserted them, and he has not heard from the North Korean agents in the last three weeks. There also are rumors in the South Korean media claiming that the attack was aimed to mark the occasion of North Korea's first nuclear test in October 2006 and to punish the international community for UN Resolution 1718, which imposed sanctions on the DPRK and caused their recent famine and economic hardship.

KHNP has resorted to temporarily pumping seawater into Kori-1 to cool the reactor while continuing to vent gas and working to restore the reactor's cooling systems. Sendai-1, on the other hand, has remained stable since shutting down, and the primary cooling system is operating. Japanese officials say that the incident was caused by a mechanical failure, and with no indication of a cyber attack at Sendai, the incidents at Kori and Sendai occurring on the same day appears to have been a coincidence.

Move 2

Since we have now confirmed this incident was a DPRK cyber-attack against Korea, we now know that North Korea has increased its capacity in cyberspace and has used an infected USB drive to deposited malware targeting Industrial Control Systems (ICS) similar to the functions of the Stuxnet virus. Intelligence agencies have found the source code for Stuxnet available for purchase in the darkweb and have concluded that the DPRK has successfully learned how to code one.

North Korea decries the results of the intelligence investigation and says, "results of the 'investigation' is another extremely ridiculous charade staged by the Park Geun-hye puppet group in a bid to hurt the dignity of the DPRK, steadily tighten

the ‘sanctions’ against it, harm and suffocate it in conspiracy with her US and Japanese masters, much upset by the might of the Republic advancing by leaps and bounds toward a strong and prosperous nation.” The DPRK begins to hold rallies against the US, ROK, and Japan and their “Anti-DPRK smear campaign.” Troops on the North Korean side of the border are mobilized and ready for action against the South. On the morning of October 21, shots are fired between the North and South Korean militaries at the DMZ. Both sides accuse the other of having fired first. There are reports of DPRK casualties and one ROK soldier was hospitalized in critical condition. The DPRK maintains innocence, and their public statements have emphatically denied all allegations of wrongdoing.

KCNA reports, “It is the age of science and technology. As a swollen balloon is bound to break, any lie is bound to be brought to light no matter how hard one may try to make it sound plausible. Availing ourselves of this opportunity, we sternly warn the US and Japanese authorities and riff-raffs, their poor lackeys, to act with discretion. The world will clearly see what dear price the group of traitors will have to pay for the clumsy ‘conspiratorial farce’ and ‘charade’ concocted to stifle compatriots.”

1) What are the first five actions you recommend in response to this emergency? (in order of priority)
2) What are the five messages that should be delivered (by whom, to whom, about what, and in what order?)
3) What do you expect from the other countries in the region? What do you want them to do/say? What do you not want them to do/say?

Developing global norms for cyber-enabled covert action

By Tristan Volpe

The table-top exercise at the 2015 Northeast Asia Regional Young Leaders Security Seminar presented Young Leaders with an international security problem that vexes government policymakers today. The exercise exposed fundamental differences about how Young Leaders representing the United States, China, Japan, and the Republic of Korea (ROK) assigned attribution for a purported North Korean cyber-attack on a ROK civilian nuclear reactor, and what constituted a proportional response to such an operation.

In particular, three important nodes of agreement and disagreement emerged during the Table-top Exercise (TTX):

1. *Attribution* – The US, ROK, and Japan teams all shared largely the same requirements for attributing the cyber-attack to North Korea, while the China team disagreed with these assessments, and demanded a much stronger burden of proof.
2. *Response* – The US, ROK, and Japan teams also agreed that the North Korean attack warranted a stern response, although the Japanese representatives were hesitant to take military action that would increase the risk of regional conflict. Again, the China team vehemently opposed the use of force as a retaliatory measure against the North Koreans, and pushed for action instead at the United Nations.
3. *Vulnerability* – The US, ROK, and Japan triangle was particularly worried about mutual shared vulnerability to further cyber-attacks, and took actions during the TTX to deter additional transgressions. China's apparent lack of concern about its own vulnerability to cyber operations surprised many participants.

These contrasting positions point towards two more general themes from the TTX. First, as discussed in detail below, the cyber-attack signified a new tool employed by the North Koreans, but it was not a revolution in covert action. The nodes of agreement and disagreement during the TTX reflected this critical point. Second, the lack of shared ground between the China team and the US-ROK-Japan triangle over the full spectrum of issues—from how to attribute a cyber-attack to an intentional actor to the most appropriate mode of response—should be addressed in future TTX scenarios.

On initial consideration, the source of these agreements and disagreements during the TTX seemed to stem from the digital nature of the North Korean operation. Cyber capabilities can be notoriously difficult to attribute to a specific country or actor, and provide an opportunity for a rogue military commander or individual "hacker" to launch an operation without government authorization. Unlike conventional or nuclear weapons, moreover, the intended costs and damage of cyber operations can be difficult to estimate with high confidence. As a result, the Chinese and US teams frequently disagreed about whether the North Koreans had actually launched a cyber-attack on the ROK, and developed different policy responses to dealing with the situation.

Yet a key implication from the TTX is that the challenges faced by the Young Leaders in assigning attribution and devising a proportional response are not unique to digitally-enabled attacks on critical infrastructure. Rather, these are problems that countries have long had to address with covert action in general. How does a government definitively prove that another country authorized and launched an attack when the capabilities employed can be plausibly denied or spoofed by a third party? If attribution for a covert operation cannot be established, how should the victim respond in the absence of a clear *casus belli*?

As the Seoul TTX made clear, these are not easy questions to answer in peacetime, let alone a contested geopolitical environment in the wake of a nuclear accident. But government stakeholders and public analysts can better plan for these potential situations by viewing cyber capabilities as a new instrument to accomplish age-old objectives of covert espionage and sabotage against a range of targets, including critical infrastructure. Cyber capabilities do not create a revolutionary new set of challenges when it comes to dealing with covert action. However, as the TTX drove home, the diffusion of cyber instruments to new actors such as North Korea requires a frank conversation about appropriate norms of international behavior.

Consider the crux of the disagreement over attribution that set the China country team apart from the United States and ROK teams. In the scenario, a human agent gained tailored onsite access and delivered the digital payload to sabotage the industrial control systems of the ROK nuclear reactor. The cyber dimension seemed to introduce a new attribution challenge, as the China team demanded concrete proof that this act was an official North Korean military operation. But as a counterfactual, what if the North Korean saboteur physically caused the reactor to shutdown instead of employing a cyber-package? The China team probably would still have demanded additional proof that this agent was acting on behalf of an order from Pyongyang. The North Koreans, of course, could still maintain plausible deniability.

Over the last few years, however, a handful of high-profile incidents generated concern over how "cyber-capabilities" or "hacking" might blur the line between classic covert action and the next phase of digitally enabled sabotage. In 2007, the US government demonstrated that hackers could physically destroy a power plant with just 21 lines of malicious code. The infamous 2010 Stuxnet exploit took out Iranian enrichment centrifuges by gaining control of standard computer control systems used by industries around the world. In December 2014, hackers associated with North Korea gained access to the networks of nuclear facilities in South Korea, and copied sensitive design and blueprint information from the servers. More recently, two power distribution enterprises in Ukraine claimed that hackers had comprised their networks and shutdown power to more than 80,000 customers. As the Young Leaders in the TTX found out, the spread of information technology opens up a range of vulnerabilities for the safe and secure operation of nuclear energy facilities.

The nuclear community has long been aware of the general threat posed by information technology. Within the domain of strategic nuclear policy, for instance, the US government has invested considerable resources into assessing and responding to a

cyberattack on strategic command, control, and intelligence capabilities that could leave Washington blind and unable to give orders during a conflict. Yet the prevalence of antiquated legacy systems in civilian nuclear facilities meant the nuclear energy industry lagged behind the digital revolution by decades. But with many of these pre-digital systems reaching the end of their life cycles, the community of operators, experts, and policy makers who deal with nuclear safety and security is rapidly coming up to speed on the risks of introducing information technology into nuclear facilities.

Not all cyber operations or hacks against the nuclear energy industry pose the same level or type of risk to the general population. The next phase of covert operations is likely to use a combination of human agents and digital payloads to threaten the confidentiality, availability, and integrity of information technology systems at nuclear facilities.

Confidentiality refers to protecting and keeping secret sensitive nuclear data from espionage and data theft. The 2014 North Korean hack against South Korean nuclear facilities is a prime example. The attack could have been an exercise to gather information as a means to pinpoint digital or physical vulnerabilities in the reactor, but the operators did not gain control of the facilities. Beyond attacks on physical infrastructure, malicious actors may want to access sensitive nuclear data to jumpstart an illicit nuclear weapons program. In general, the nuclear industry faces strong incentives to defend its networks against these sort of "cyber spying" operations to maintain control over intellectual property. Encryption schemes can go a long way to protecting sensitive digital information from being used by malicious actors, but there are a number of key vulnerabilities in current networks.

Availability means keeping critical network services running at all times. This is a huge risk for nuclear facilities with digital technology. If a software patch to a reactor's control systems caused them to shut down, operators need to have redundant controls to avert a core meltdown. A more malicious hacker could devise ways to turn a reactor into a nuclear-fallout generating weapon against the local population. Indeed, there are a handful of conceivable scenarios where this could fit into an overall political-military strategy.

Integrity is the least understood and most dangerous problem for the nuclear industry. As one leading information security expert put it, the issue is assessing "whether the software and critical data within the network and systems are compromised with malicious or unauthorized code or bugs." With a confidentiality breach, the hacker might learn valuable information about a facility or nuclear technology. But with an undetected integrity attack, hackers gain control over the facilities themselves. Last fall, James Clapper, the director of national intelligence, underscored that the biggest threat is "cyber operations that will change or manipulate electronic information in order to compromise its integrity instead of deleting or disrupting access to it." In other words, an operator of a nuclear reactor may not be able to trust the information visible on the digital screen.

The information security community is engaged in a digital arms race to develop effective solutions to these three distinct risks. For example, encryption locks might thwart espionage, but do little if a hacker has compromised the entire system. Integrity defenses in development are more akin to an active alarm system that detects unauthorized modifications and intrusions. As the nuclear industry catches up with the digital revolution, the nuclear security community should continue its efforts to fully integrate technical and policy developments from the information security community. Beyond these nuclear specific discussions, the Seoul TTX underscored the need for government leaders to develop new norms of appropriate behavior for covert action with cyber instruments.

Summary of the Chinese team

By Yongcheng Li, Xiao Kang, Meng Li, Suo Wang,
Guanpei Ming, Hongzhou Zhang, Yizhe Xie and Tong Zhao

The Table-top exercise provided a great opportunity for teams from the United States (US), Republic of Korea (ROK), Japan and People's Republic of China (China) to exchange ideas and better understand each other.

In the first move, the Chinese team focused on two priorities: identification of the nature and cause of the tragedy, and second, avoiding escalation. The Chinese team was in the beginning divided on what should be done first, to define the cause and nature of the attack or to ensure the safety of our president, who remained in the ROK. However, after careful scrutiny, we were confident with the security efforts made by the ROK team, so we agreed to prioritize identification. To that end, we recommended the establishment of a trilateral nuclear power cooperation mechanism among China, South Korea, and Japan, to offer help to the ROK in their investigation into the truth behind the situation, thus making a solid basis for the next cooperative response. Second, we prioritized the avoidance of escalation and war as possible reactions to the tragedy. By escalation we meant a trend that might lead to inter-state military exchanges and conflicts. For the Chinese team, this was best done by encouraging an international investigation to not only uncover the nature of the attack, but also to help calm leaders and people and avoid hasty and emotional actions.

The Chinese team sought to convey to our partner teams that the peace and stability of the Korean Peninsula has always been the core goal of China's peripheral diplomacy. We were happy to see a productive relationship between China and South Korea written in the scenario. However, the Chinese team was worried about possible irrational actions from the DPRK that might undermine the ROK-US alliance and cause tit-for-tat reactions that might go out of control. Therefore, we recommended that the DPRK government not act in ways that could undermine the interest of China, the peace on the peninsula, and the security and safety of nuclear power facilities and plants.

The top five actions that the Chinese team took were: first, we condemned any action from any individual, organization or country aimed against critical infrastructure resources, particularly nuclear facilities. While we noticed that there is evidence suggesting that North Korea could be linked to the attack, we urged all parties involved to refrain from labeling this as a state-sponsored event until further investigation is done. Second, we emphasized that all countries must remain calm and avoid any provocative actions that could lead to the escalation of the crisis. In particular, we requested that North Korea cooperate with the international investigators to provide necessary evidence. Third, we began investigating our own critical infrastructure, particularly nuclear facilities, to eliminate any security threats, and we increased our cyber-monitoring efforts. Fourth, we raised our national security alert level and mobilized necessary military assets, especially in Northeast China and the Yellow Sea, in case of any unexpected military contingencies. Last, we emphasized that China is willing and ready to provide technical assistance, manpower, and other means of assistance to ensure a

peaceful resolution of the current crisis, and we called immediately for a six-party or four-party meeting to solve the crisis through diplomatic and peaceful means. We also stressed that attention has to be paid to ensure the safety of the damaged nuclear plants, and that we are willing provide assistance to South Korea and Japan.

At the same time, messages needed to be sent. First, the Chinese team recommended that the Chinese UN ambassador call an urgent meeting at the UN Security Council to discuss the crisis in the Korean Peninsula, and establish a comprehensive international investigation team. Second, we sent a private message through our ambassador to the North Korean government, urging North Korea to stop military actions near the border and to refrain from any provocative actions. We requested that the North Korean authorities cooperate with international investigators and provide all necessary evidence, and we encouraged the North Korean government to share all necessary information with us. If the North Korean government does not cooperate, we would reconsider economic ties such as the supply of critical resources and military agreements, including the possibility of reconsidering the renewal of our military mutual defense agreement. Third, the Chinese team encouraged President Xi to hold a teleconference with South Korean President Park. The message said that, "We feel very shocked and saddened as a result of the attacks on South Korean Nuclear facilities, we send our deepest sympathy to those who suffered from the attack, and we are willing to provide assistance. As matter of fact, we are also victims, thus we share the feelings of the South Korean people. We want to make it clear that we condemn any actions against critical infrastructure, we hold it strongly that any person, organization or even a nation which commit this crime must be held accountable and punished. We believe that this has to be done through the UN Security Council, however, and military retaliation is not a desirable option." Fourth, President Xi called President Obama through a hotline to say that, "China and the United States should work together to ensure peace and stability in East Asia. Our top priority should be avoiding the escalation of the crisis and preventing war." Last, the Chinese team assured the Chinese people that we have conducted thorough safety checks at all of our nuclear facilities and they are in good condition. The Chinese team worked with all parties involved to ensure the peace and stability of the Korean Peninsula. We agreed to provide timely updates on the development of the situation and urged fellow citizens to remain calm, and not to trust or spread rumors.

In the second move, the attack was linked to the North Korean government, and probably backed by the North Korean regime. As a result, the Chinese team expected strong reactions and/or retaliation from the United States, South Korea, and to a certain extent, Japan. The Chinese team's biggest concern was that any military actions could lead to a full-scale war or even nuclear war. Therefore, our priorities remained similar to those from move one: first, prevent war or further escalation of the conflict and stress the need for further investigation to buy more time to solve this crisis through diplomatic means. Second, we needed to make it clear that China had nothing to do with this attack and China was not involved or briefed by North Korea. Third, we felt it was important that China show support to South Korea and urge South Korea to remain calm, and fourth, ensure that China talks with the United States via the highest available communication channel.

Surprises and Lessons learned: During the exercise, two things surprised us; the overestimation by US, ROK, and Japan teams of China's ability to influence the DPRK, and the gap between the US team's military readiness and the ROK team's steadiness. China does not have much power or influence to direct or stop the DPRK's behavior. China and the DPRK signed a bilateral Mutual Aid and Cooperation Friendship Treaty on July 11, 1961; Article II of which stipulates that "*the Contracting Parties undertake jointly to adopt all measures to prevent aggression against either of the Contracting Parties by any state. In the event of one of the Contracting Parties being subjected to the armed attack by any state or several states jointly and thus being involved in a state of war, the other Contracting Party shall immediately render military and other assistance by all means at its disposal.*" However, after China established diplomatic relations with the ROK in the early-1990s, the China-DPRK relationship became more uncertain. China and the DPRK have disagreed over denuclearization of the Peninsula, and this has hindered relations between them. On the second item that surprised us, there is a critical difference between the ROK team's strategic rationality and the US team's military preparedness. When the ROK team said it was necessary to find out whether the cyber-attack was DPRK state-sanctioned behavior or a non-state actor's plot, we appreciated the strategic rationality of avoiding hasty judgment. At the same time, the US team's stress on the necessary military deployment and preparation for further damage and accidents reminded us that great powers think differently than weaker powers.

We expected Japan to follow the lead of the United States to favor military actions against North Korea, and to fulfil its obligation under its alliance with the US However, the Japan team's position was similar to that of the Chinese team. It stressed the need for all countries to remain calm and prevent further escalation of conflict. We were impressed by the lack of militarization in their actions responding to the crisis, which we viewed as a welcome example of the peaceful transformation of the Japanese people. Thus, we feel that China and Japan could increase cooperation and play facilitating roles to bring peace and stability back to East Asia in times of crisis on Korean Peninsula.

The most important thing we learned from the exercise was how significant cooperation is in cyber security and how this valuable asset could be developed among nations. Rules and principles based on international consensus and legitimacy form the basis for cyber cooperation, but unfortunately, rules and principles have been absent for many years. We also learned that proper communication style and correct vocabulary are as important as having an open and honest communication and mistakes can easily undermine prospective cooperation.

We hope the cooperation of the US, China, Japan, and ROK will lead to an effort to set rules and principles to guide the successful management of cyber security issues.

Summary and analysis of the Republic of Korea (ROK) team

By Paul Choi, Jina Kim
Julia Jungmin Oh, Gibum Kim, Nahee Kim,
Diana Jea Hyun Lee, Sung Hyo Kim

Throughout the TTX, the ROK team focused on encouraging regional cooperation and support as well as tailoring our response to prevent further conflict between the DPRK and the ROK. During Move 1, our primary focus was placed on ensuring the safety of the affected facilities and adjacent area, as well as other nuclear facilities and critical infrastructure in the ROK. As we went into Move 2, our team decided to demonstrate a more aggressive response against North Korea to prevent prolonged escalation and additional provocations by North Korea.

For our messaging, the ROK team divided the audience by country to tailor our messages to their key interests and concerns. This step was critical to mitigate public concern and tension in the region. To minimize economic impact, the ROK team communicated key points (relating to public health and safety in particular) in a straightforward way. Close coordination with ROK government agencies and domestic media, as well as other countries was essential. Although we checked the security around the region and nuclear power plants, arranged alternative destinations for the incoming vessels and flights, and focused on minimizing negative economic impact, some participants from other countries wanted a clearer emphasis and more detailed measures to ensure stable economic activities as part of our message.

Messages from other teams were close to what we expected. It was interesting to observe China's expectation for Japan to not "overreact." While the Japanese team was cautious about possible SDF deployment in the region and exercised restraint in dealing with the situation outside of Japan, China repeatedly urged Japan to refrain from using military means that could aggravate tension in the region. The fact that China referred to Japan's military action as an "overreaction" showed the degree of concern and sensitivity on the Chinese side. The Korean team shared a similar concern. However, as we thought that mentioning these concerns could upset Japan, the ROK team chose not to communicate them and instead emphasized close intelligence sharing between the ROK and Japan, and civilian support and assistance with damage control over the accident at the nuclear facility.

Prior to Move 2, the ROK team decided that until we knew whether this attack was planned and conducted by the DPRK, it would be premature to publically attribute it to the DPRK. For this reason, we assessed that any military action in response at this stage should not be encouraged. However, after Move 2, our team's focus expanded from damage control to countermeasures against the DPRK's cyberattack and armed provocation. We also noted the unprecedented nature of such a cyberattack by the DPRK on the ROK's critical infrastructure, which could have led to a more severe crisis.

Awareness of the consequences of failing to meet the public's expectations of the ROK government was also an important factor in our decision. This reflected 20 years of

experience in South Korea when unpopular decisions were met with large-scale demonstrations and sometimes prolonged anti-government sentiment, such as in the reaction to the Sewol Ferry incident or DPRK provocations. Our team also discussed the Korean public's unique perception of North Korean provocations; over the past few decades, the Korean public has become more desensitized to North Korean provocations than people in other countries. A growing number of the public also think that the DPRK's continued provocations, despite the ROK's efforts to engage in a dialogue and bring peace, indicate a failure to give a strong, proportional, timely, and effective ROK response. In light of this analysis, our group decided to take stronger actions despite previous ROK policy measures or expectations from other countries. This is not to say that past decisions by the ROK were neglected. We went through previous interactions between the ROK and DPRK to see what measures are likely to enable the DPRK to acknowledge its actions and bring the North Koreans back into a dialogue.

The primary goal throughout the scenario was de-escalation. There were, however, diverse opinions within our team as to the degree of proportional response against the DPRK. We concluded that having been "soft" in response to past DPRK provocation may have encouraged reckless behavior and that the recent hardline policy of the ROK has been working well. Recognizing the importance of managing this crisis in a manner that would not trigger escalation or a full scale war, the ROK team decided that it was important to demonstrate a will to act against any future provocations and send a strong message that armed provocations will no longer be tolerated. After calculating the risks and possible reaction from North Korea, as well as what we could expect from other countries, our team decided to carry out a ROK-led surgical strike on one of the nonnuclear military facilities in the DPRK. Our team determined that targeting a cyber operations facility was not ideal as we did not see any meaningful impact on the DPRK's cyber capability. We also expected robust military support from the US, including the deployment of US strategic assets as a deterrent. To ensure the success of the military operation and to de-escalate the situation, we encouraged close cooperation among the US, Japan, China, and the ROK, especially concerning intelligence, surveillance, and reconnaissance (ISR) support and attribution regarding the cyberattack.

When the ROK team presented our response, other country teams were surprised. Some participants from other teams felt that the ROK decision was very "rational." Although our team did expect other countries to be surprised by such an aggressive response, the US was surprised by our decision to strike a nonnuclear military facility in DPRK as a de-escalatory measure. All teams had a shared understanding of the importance of cooperation concerning the North Korean threat and the Chinese, Japanese, and Korean teams seemed comfortable with direct, trilateral coordination without US involvement.

One of the differences in perspective the exercise highlighted was the Chinese team's understanding of the importance of proving culpability. The stark difference in interpretation between China and the US showed how conflicting opinions may hinder cooperation in responding to North Korean provocations among the four countries and the rest of the international community. It was also interesting that the Chinese team was

willing to consider aggressive, non-kinetic measures to signal to the DPRK that China is willing to reconsider its military commitment to DPRK if such provocations continue. However, it seemed that other countries were hoping for a more proactive response and cooperation from China to pressure North Korea. As most participants recognized, this TTX showed us the importance of having a better understanding of the North Korean regime and their people for better analysis and prediction before a crisis and better cooperation during a crisis.

Summary and analysis of the Japan team

By Yu Harada, Shino Hateruma, Yoshifumi Ide,
Akira Igata, Amane Kobayashi, Tatsuya Sakurai-Jyc Liu,
Takehiro Masutomo, Yoko Mori, and Rie Takezawa

In Move 1 of the table-top exercise (TTX), the Japan team began by reflecting on the lessons learned from the Fukushima nuclear accident and decided to utilize several new mechanisms that have been installed since 2011 to respond to the crises developing at home and abroad.

The Japan team's primary concern was to deal with the situation at Sendai nuclear power plant. First, the Japan team convened the Emergency Situations Minister Meeting at the National Security Council (NSC), which was established in 2013. Responses to the crises were discussed at the NSC: the prime minister pledged to keep the domestic populace updated about the situation; all information about the crisis was to be provided in Korean, Chinese, and English languages; the Japanese government took full responsibility to evacuate Chinese/Korean citizens in Kyushu if necessary, etc. The team discussion concentrated on the importance of providing accurate information in a timely manner to minimize mass fear and anxiety about the nuclear crises.

Second, the Japan team utilized the Alliance Coordination Mechanism, which is stipulated in the Guidelines for Japan-US Defense Cooperation and was established in November 2015 to institutionalize intelligence-sharing with the US. Since no similar information-sharing mechanism exists between Japan and the Republic of Korea (ROK), the Japan team asked for the establishment of a hotline with the ROK. Furthermore, the Japan team decided to share information with the Chinese team as needed to avoid misperception and to help reduce tension.

Third, the Japan team ordered the Self-Defense Forces (SDF), especially the Central Nuclear Biological Chemical Weapon Defense Unit, and the Japan Coast Guard, particularly the units stationed in Kyushu or Chugoku region, to prepare for possible deterioration of the Sendai nuclear power plant.

In Move 1B of the simulation, the intelligence update confirmed with near certainty that the shutdown of the Sendai plant was due to a mechanical failure with no indication of a cyberattack. This left the Japan team with the possibility of further investigation revealing the shutdown to be in fact connected to a North Korean cyberattack. However, given the circumstantial evidence and the Sendai power plant being under control, the team moved to the consideration of the situation on the Korean Peninsula.

In dealing with the potential meltdown of the Kori plant located near Busan, the Japan team asked Japanese residents in the affected area to stay calm and follow directions from the Korean government. Since it is about 250km between the closest Japanese territory (the Tsushima Island) and the Kori plant, no further actions were taken vis-à-vis residents of the Japanese territory.

In Move 2, after North Korea's involvement in the cyberattack was revealed, the Japan team assessed the severity of the current situation. Since the ROK's noncombat countermeasures against North Korean provocations in past years had failed to prevent the cyberattack on Kori, the Japan team expected the ROK and the US teams to take severe military actions.

From the Japan team's perspective, it was critically important to minimize the risk of a North Korean attack on Japanese territory while simultaneously deescalating the crisis in the Korean Peninsula. To fulfil this goal, the Japan team reached consensus that it would support retaliatory measures by the ROK and the US teams for deterrence purposes but hope to limit these measures from leading to regime change in North Korea.

Facing the possibility of military retaliation, the team considered whether Japan can apply the new security legislation, passed by the Diet in summer 2015. The team unanimously concluded that the situation in Kori did not amount to a situation that satisfied the three conditions for Japan to exercise its right of collective self-defense. However, this situation could fall under "the situation that substantially affects Japan (*jyuuyou eikyo jitai*)," which enables Japan to give rear-end support.

With limited proactive policy options available, Japan not only placed its critical infrastructure on high alert, including all the nuclear power stations, but also proceeded with the preparation for deploying the Ballistic Missile Defense system to defend against possible attacks by North Korea.

The Japan team considered dispatching SDF to the Sea of Japan/East Sea to evacuate Japanese citizens living in the Busan area. Should that happen, we would clarify our intention to deal only with the crisis in the Korean Peninsula including the crippled Kori plant to avoid misperception and unexpected clashes with neighbors, China in particular.

In the Move 1 plenary, the Japan team expected the ROK and the US teams to react assertively, yet, the ROK team's response was more moderate while the US team demonstrated a more aggressive and proactive policy than expected. After the plenary discussion, the Japan team became wary of the China team's reaction because it mentioned concern about the proactive roles that the SDF may take.

The Japan team strongly condemned North Korea's aggression. The team sought to bring the case to the UN Security Council to exert economic sanctions against North Korea, in coordination with the ROK, China, US, and Russia. Making use of Japan's technological advantage, the Japan team wanted to take the initiative in establishing new institutions in the UN to deal with cyberattacks to contribute to building countermeasures to respond to future crises and to show Japan's commitment to regional stability without use of force.

Throughout the exercise, the Japan team realized that Japan and the ROK lack an effective cooperation mechanism. As the radioactive materials released from Kori Nuclear Power Plant could damage Japanese soil and waters, it was crucial for the Japan

team to obtain information from the ROK promptly. Similarly, sharing Japan's experience and know-how in addressing nuclear disasters with the ROK would be helpful. While bilateral cooperation was essential to deal with the threat of North Korea, the team had a difficult time identifying appropriate institutional channels for cooperation between the two countries.

The Japan team was concerned about Japan's vulnerability to cyberattacks. In the TTX, the Japan team discussed how much technical assistance and logistical support Japan can and should offer as Japan could experience a similar attack simultaneously and cyber-related capabilities usually contain classified information. Hence, we recognized the importance of setting up a government-to-government level cyber cooperation framework prior to crisis. For this purpose, Japan and the ROK should always keep the dialogue channel open despite difficult political circumstances in which the two leaders are unable to hold talks.

Summary and analysis of the US team

By Wrenn Yennie Lindgren, Maile Plan, Crystal Pryor,
Grant Schneider, Tristan Volpe, and Christopher Whyte

In the first move, the group discussed options for providing Japan and Korea assistance, given the US experience of providing unique US capabilities in response to the Fukushima disaster. First, we immediately agreed to offer assistance in the event of a potential humanitarian crisis to both South Korea and Japan. At this time, the situation in Japan did not seem as dire, and so our focus was on South Korea. Second, we discussed assistance on intelligence-gathering and analysis. The United States has unique capabilities in this regard and can deploy additional assets to the region in relatively short order. At this stage, we had no information on the potential threat vector vs. the scenario being two unrelated (if highly coincidental) accidents, but we immediately began an investigation. Third, we discussed the nature of US messaging in the wake of this crisis/potential crisis. There is a great deal at stake current regional security relationships, on the Korean Peninsula, and given the nature of a potential non-accident involving nuclear facilities.

The team also discussed logistical considerations. Though the initial discussions were designed to support our partners in crisis response, investigation, etc., the US team had to consider the position of its current regional assets and commitments to treaty partners. Rushing resources to help with an evacuation or with crisis investigation in a short period would divert forces from their regular assignments.

The first intelligence update offered information that seemed to implicate North Korea. This update changed the tenor of our discussions as we began to think more broadly about the national security implications of such an attack. We began by focusing on how regional actors, such as China and North Korea, might respond to evidence that attributed the attack to the DPRK. That the delivery method involved a defector presented a weak link muddying the waters with regard to North Korean (and, possibly, Chinese) state responses. Without a strong case for attribution that North Korea was the perpetrator, the China team would be unlikely to support North Korea. The US team saw it as essential to ensure that North Korea understood the gravity of the situation, as well as the seriousness with which actions were taken by the US team.

We discussed possible actions by the South Korean government. We agreed that understanding how the South Koreans might respond would be essential for any major policy decisions regarding next steps. Finally, we discussed the changed nature of the situation. Though partners' responses would inevitably focus on the specifics of the situation, we noted that such an attack set a very serious precedent; it would be the first cyberattack that could lead to loss of life. This apparent attack not only crossed the "use of force" threshold for cyber, but also produced a nuclear incident. It was clear that the nature of the alliance/international community response would play a role in norm creation and maintenance regarding interstate cyber security.

With these considerations in mind, we discussed certain actions that might be taken immediately to continue steps already taken and strengthen our support for the Korean and (secondarily) Japanese governments. The team was surprised by the initial reticence demonstrated by the Korean team in considering a military response.

In the second move, the DPRK responded to the situation as anticipated: it denied culpability for the attack. The denial arguably made a response more difficult because we could not pursue standard diplomatic and military channels. We looked to what we did in the first move as a foundation for next steps. As we assessed our actions and messages, we realized there was not much we would dramatically change. Our main focus was on the impending crisis on the peninsula and how to deter further DPRK provocation. To that end, we wanted to send a strong message to the ROK that we would stand by our ally and our alliance commitment. One aspect of this was to emphasize the seriousness of the cyberattack, and declare the attack as "unprecedented" and "crossing a red line." Furthermore, although the cyberattack was not itself a kinetic weapon, it created a "low-yield nuclear weapon," which had serious implications.

Our group discussed how the US would react if something similar happened in our country, but we concluded that this was ultimately the ROK's security issue and we had to be careful not to overstep another country's sovereignty and security protocols. Therefore, we wanted to support the ROK and not take the lead on its response to the DPRK.

The China team did not seem to think that a cyberattack on a nuclear facility that could lead to civilian casualties was a cause for war or the involvement of the military, which we think was why our Move 1 military posturing shocked them. Therefore, in Move 2, we wanted to reassure China that we were not mobilizing or using our military without the ROK's consent because we did not want China to think that the US was unilaterally moving into the Korean Peninsula and ignite the same miscalculation as in the Korean War. The US team wanted to be clear that we were not leading but supporting. We discussed the possibility of Chinese troops moving into the Korean Peninsula if US troops were seen moving into North Korea, so to prevent any further misunderstanding with China, we wanted to continue our mil-to-mil communication. However, even though we wanted to assure China that we are not war-mongers, we also had to maintain military readiness to assure South Korea of our commitment to it. Although discussions entertained a variety of nonmilitary options, our presentation to the other countries came across as military-heavy, focusing on the DPRK's crossing a "red line" when it came to its attack on critical (nuclear) infrastructure.

Lessons learned

During the exercise, the US team ran into several unexpected challenges. The first was how quickly the ROK team would request US involvement. Several members of the US team believed that the ROK would ask for immediate retaliation against North Korea. ROK officials have indicated that the tempo and promptness of a US military response to aggression underpins the credibility of extended deterrence. Instead, the ROK team

requested time to conduct due diligence on attribution for the cyberattack. The US team learned that while promptness demonstrated a strong commitment to the alliance relationship, it was only welcome after the ROK solved the attribution problem.

The second challenge resulted from a realization that alliance structures complicate decisions. The US team dealt with the issue of overstepping or under-stepping alliance commitments, particularly, regarding South Korea's expectations. With an exercise involving two major alliance structures (US-ROK and US-Japan), we were concerned about competition over resources/attention – although resolution of the nuclear problem in Japan meant that this concern faded in the second round. The delegation spent time discussing values, interests and commitments, especially vis-a-vis our allies.

The third challenge stemmed from a perception gap between the US and China teams over whether the North Korean action crossed the "use of force" redline. One of the most interesting aspects of the exercise was that the intended effect of the cyber operation – a nuclear reactor meltdown – eliminated ambiguity on the US side about the nature and magnitude of the attack: it was a clear act of war comparable to a failed attempt to detonate a low-yield nuclear device in South Korea. Several members of the US team believed that this created a small opening to work with China because both countries had recently agreed that cyber operations against critical infrastructure, most notably nuclear energy reactors, should be off-limits. Yet the China team dodged the issue by focusing instead on attribution, which quickly devolved into ad hominem attacks on the reliability of national intelligence communities.

As a result, the US team learned that it would be useful to establish clear parameters for attribution of cyber-attacks in advance of a crisis. For example, if a rogue commander or proxy actor within North Korea really did launch the attack, as the China team claimed, should the national leadership and military still be held accountable for these actions? This is a tricky yet critical issue for the United States to explore with China.

Lastly, it became clear that we (and US stated policy) do not know what an appropriate proportional response is to cyberattacks. For example, is kinetic retaliation to a cyberattack appropriate? Our delegation reached no agreement as to taking the "nuclear option" – i.e,; responding with nuclear weapons if deemed necessary – off the table, or if it should be taken off at all. Some members of our delegation were of the opinion that we should not remove any potential method of dealing with the crisis, while others thought that, especially due to North Korea's potential nuclear capability, that we should state from the outset that we were *not* considering nuclear retaliation to North Korea's cyberattack. China seemed to differ the most from our position in terms of what is appropriate when a cyberattack results in kinetic force and/or casualties. Meanwhile, the ROK and the United States seemed to agree that a cyberattack that resulted in civilian casualties can and possibly should warrant a proportional kinetic response.

Cyber Security

By Yu Harada, Jenny Jun,
Grant Schneider, and Christopher Whyte

Presentations

The focus of the cyber discussions was North Korea's organization of cyber operations. The US speaker focused on the Sony hack and government entities within North Korea that house the country's cyber capabilities, sharing her recent research on the unique and unprecedented nature of the Sony hack, as well as its effects on the international community.

The presenter argued that the Sony attack occurred in the context of North Korea's strategic operational environment. As in the past, North Korea has relied upon asymmetric and irregular means to sidestep the conventional military deadlock on the Peninsula. As such, she argued that North Korea views cyber capabilities as a relatively low-cost and low-risk way to threaten the security of conventionally superior states. Additionally, cyber means allow North Korea to project power far beyond its borders and its conventional military capabilities.

The presenter believed two main actors could house North Korea's cyber capabilities: the Reconnaissance General Bureau and the General Staff Department. She argued that North Korea's cyber-attacks are the result of top-down, carefully planned attacks on specific chosen targets. She also argued that the North Korean information technology base is not as primitive as many think.

Simulation

The simulation centered on a number of issues: the unprecedented nature of the attack and the lack of reliable evidence and attribution. Given the seriousness with which all countries take nuclear safety, an attack on a nuclear power reactor is a particularly egregious act. Attacks on civilian nuclear power plants could have long lasting – potentially centuries – effects on civilian populations. As such, most states would see such attacks as in violation of international law. All groups struggled with how to deal with such an attack, given the lack of real world examples. While cyber-attacks have occurred, none have directly threatened large civilian populations. The simulation provided an opportunity to think through their country responses, as well as hear other participants' views and reactions to their own group's views. Without agreed understanding or historical examples, the United States team and its allies (the teams from South Korea and Japan) struggled with the appropriate response, both within their own teams and collectively. The China team also struggled with its response, understanding that an attack on a South Korean nuclear reactor could lead to radioactivity being released into the environment and spreading to China. On the other hand, the China team was forced to weigh such an event against its historic alliance with the likely, although unconfirmed, aggressor in North Korea.

Participants also had to weigh responses based on imperfect information. Teams had to assess the potential for further changes in the simulation, as well as historical precedents such as North Korea's previous cyber-attacks, to decide whether they believed North Korea was responsible for the attack. The China team raised the possibility of rogue elements acting without the sanction of senior leadership, further complicating states' abilities to take decisive cooperative action.

Participants were also interested in finding ways to increase transparency in an effort to come to a common understanding of what had occurred to resolve the crisis. Given the lack of concrete information, as well as difficulty in sharing information due to mistrust among states, participants were unable to devise new ways to solve this problem. Agreement focused mainly on the understanding that such attacks would be extremely serious and would have deleterious effects on stability in Northeast Asia.

Suggested readings for further learning

There is a lack of reliable open-source information on North Korea's political and military apparatus as well as technical difficulties in tracking cyber activity readily attributable to the North Korean state. Adding to these difficulties is the fact that very little attention has been given to North Korea's cyber operations in the English-language media and academic circles before the November 2014 Sony incident. Thus, much of the existing analysis in both academia and the technical community is in Korean, focusing on incidents that occurred in South Korea. Another barrier derives from the relative paucity of North Korea-related incident response data in the US compared to that of other threat actors. This limits the ability to conduct in-depth case studies as well as the compilation of a larger data set to analyze patterns in behavior from technical data. Because North Korea has traditionally targeted the South Korean government and civilian organizations much more frequently than US entities, more data is available in South Korea than anywhere else. Given these difficulties, much more work needs to be done to gain a comprehensive understanding of North Korea's cyber operations, one that probably requires an interdisciplinary approach.

There are a number of valuable English-language works for those seeking an introduction to the topic. There is an even more expansive set of literature for those interested in learning more about North Korea's military or state conflict in cyberspace, and some technical analysis on North Korean cyber activity. A good approach would use multiple sources in different disciplines to gain a balanced understanding on the topic.

Introductory readings on North Korea's cyber operations

- Jun, Jenny, Scott LaFoy and Ethan Sohn, *North Korea's Cyber Operations: Strategy and Responses.* CSIS, Landham, MD: Rowman & Littlefield, 2015.
- Haggard, Stephan and Jon R. Lindsay, "North Korea and the Sony Hack: Exporting Instability through Cyberspace," *East-West Center*, 117 (2015).
- Mansourov, Alexandre Y, "North Korea's Cyber Warfare and Challenges for the US-ROK Alliance." KEI Academic Paper Series, Korea Economic Institute of America, 2014.

- Murauskaite, Egle, "North Korea's Cyber Capabilities: Deterrence and Stability in a Changing Strategic Environment," *38 North*, Sept. 12, 2014.
- HP Security Research. "Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape." HP Security Briefing, August 2014.
- Feakin, Tobias. "Playing Blind-Man's Buff: Estimating North Korea's Cyber Capabilities." *International Journal of Korean Unification Studies* 22, no. 2 (2013).

Introductory readings on North Korea's military

- Cordesman, Anthony H. *The Korean Military Balance.* Washington, DC: Center for Strategic and International Studies, 2011
- Bermudez Jr., Joseph S. "A New Emphasis on Operations against South Korea?" 38 North Special Report, US Korea Institute at School of Advanced International Studies (SAIS), 2010.
- Gause, Ken E. *North Korean Civil-Military Trends: Military-First Politics to a Point.* Carlisle, PA: Strategic Studies Institute, 2006.
- Mansourov, Alexandre Y., ed. *Bytes and Bullets: Information Technology Revolution and National Security on the Korean Peninsula.* Honolulu, HI: Asia-Pacific Center for Security Studies, 2005.
- Minnich, James M. *The North Korean People's Army: Origins and Current Tactics.* Annapolis, MD: US Naval Institute Press, 2005.
- Bermudez Jr., Joseph S. *The Armed Forces of North Korea.* London: I. B. Tauris, 2001.

Introductory readings on conflict in cyberspace

- Lindsay, Jon R. and Erik Gartzke, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies,* 24:2 (2015) 316-348.
- Valeriano, Brandon, and Ryan C. Maness, *Cyber War and Cyber Realities: Cyber Conflict in the International System.* Oxford University Press, 2015.
- Zetter, Kim. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York: Crown, 2014.
- Healey, Jason, and Karl Grindal, eds. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.* Vienna, VA: Cyber Conflict Studies Association, 2013.
- Libicki, Martin C. *Brandishing Cyberattack Capabilities.* The Rand Corporation, 2013.
- Libicki, Martin C. *Crisis and Escalation in Cyberspace.* The Rand Corporation. 2012.
- Rattray, Gregory and Jason Healy. "Categorizing and Undertanding Offensive Cyber Capabilities and Their Use." National Research Council. Proceedings on a Workshop on Deterring Cyberattacks. Washington, DC: The National Academies Press, 2010.
- Nye, Joseph S. Jr., "Cyber Power," Belfer Center for Science and International Affairs, 2010.
- Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security,* Washington, DC: National Defense University, 2009.

Technical analysis of North Korean cyber activity

- "North Korea," in *2015 Global Threat Report,* Crowdstrike, Jan. 18, 2016. 31-34.
- Jiang, Genwei, and Josiah Kimble. "Hangul Word Processor (HWP) Zero-Day: Possible Ties to North Korean Threat Actors," FireEye Blogs, Sept. 9, 2015.
- Baumgartner, Kurt. "Sony/Destover: Mystery North Korean Actor's Destructive and Past Network Activity: Comparisons with Shamoon and DarkSeoul." SecureList. Dec. 4, 2014.
- Tarakanov, Dmitry. "The 'Kimsuky' Operation: A North Korean APT?" SecureList, Sept. 11, 2013.
- Symantec Security Response. "Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War." Symantec Official Blog, June 26, 2013.
- IssueMakersLab, "South Korea Identified Who's Behind the Cyber Attack," Press Release, April 10, 2013.
- Sherstobitoff, Ryan, Itai Liba, and James Walter. "Dissecting Operation Troy: Cyberespionage in South Korea." McAfee White Paper, March 20, 2013.

Discussion questions

There were at least three points of controversy regarding cyber security: (1) the attribution problem, (2) how to set a threshold for a cyber-attack, and (3) what constitutes a proportional response.

In cyberspace, specifying sources of attack is difficult since identities can be easily disguised and attacks often leave no trace. This well-known concern, called the attribution problem, was one of the most controversial issues in the TTX.

Since the scenario simply mentioned "a DPRK cyber-attack against Korea," the China team questioned the DPRK government's responsibility for the cyber-attack. It claimed further international investigation was needed to conclude that the attack had been conducted by the DPRK government, while other teams concluded that the DPRK government was responsible. The ROK team argued the problem/threshold was clear and the DPRK government must understand that the attack against the aged Kori Nuclear Power Plant unit 1 (Kori-1) would pose a high risk of a meltdown. The US team supported the ROK team's view, arguing that the crash of Kori-1's computer system could not be achieved without the DPRK government's well-organized preparation.

The China team raised another controversial issue: the DPRK's *intention* to attack the Kori-1. The China team repeatedly claimed that since the intention was not clear, there was a risk of overestimating the severity of the situation. It highlighted the necessity of grasping the DPRK's intention before next steps could be taken. The ROK and US teams objected to the China team's claim, the US team arguing that regardless of intention, the DPRK government could not escape responsibility since DPRK agents were involved in the attack.

The second disputed point in the TTX was whether the DPRK's cyber-attack reached the armed attack threshold that invoked the ROK's right of self-defense. According to International Group of Experts of Tallinn Manual, cyber-attacks resulting in injury or death of persons, or damage or destruction of properties could qualify as an armed attack; theft, intelligence gathering or disturbance of non-essential services by using cyber means would not qualify. In addition, an operation cannot be considered intentional merely by looking at the nature of the attack but instead must assess the scale and effects of the attacks.

There are reasons to conclude that the DPRK's attack against Kori-1 was well over the threshold. First, the attack was against critical infrastructure that provides an essential service and underpins Korean society. Second, the attack caused a massive loss of life and property, damaging a vital facility. Third, radiation was released into the atmosphere and a partial meltdown occurred. For these reasons, the attack was beyond a disturbance of service and it could be regarded as an armed attack that would, in turn, invoke the ROK's right of self-defense.

This view was shared among the ROK, US, and Japan teams, while the China team took a different view. The China team thought it was premature to discuss the ROK's right of self-defense and maintained that the first priority was to accumulate evidence indicating the DPRK government's direct involvement.

The third point of controversy was how to proportionally respond to cyber-attacks. Participants in the TTX agreed that cyber-attacks should be met with retaliatory cyber-attacks, which would comply with the necessity and proportionality criteria required by international humanitarian law. However, the issue becomes more complicated when the opponent state lacks facilities or systems which are suitable targets for cyber-retaliation. In the TTX, it seemed that there were no suitable targets for cyber-retaliation in the DPRK, and the ROK team chose to conduct a limited conventional weapon strike. This decision raised the question whether the ROK team's response was excessive. Preparing for escalation, the ROK team asked the US team to move strategic assets near the ROK. The China team insisted that such movements were an overreaction and worried they would make the situation worse. Thus, the TTX highlighted a difficulty in achieving a consensus on proportional and appropriate responses to cyber-attacks.

Further reading

- Rid, Thomas and Ben Buchanan (2015) "Attributing Cyber Attacks" *Journal of Strategic Studies*, February, Vol. 39, Issue 1, p. 4-37.
- Lindsay, Jon R. (2014) "The Impact of China on Cybersecurity: Fiction and Friction," *International Security* 39, No. 3, p. 7–47.
- Boebert, W. Earl (2011) 'A Survey of Challenges in Attribution', in Committee on Deterring Cyberattacks (ed.), Proceedings of a Workshop on Deterring Cyberattacks (Washington DC: National Academies Press), p. 51–2.
- Waxman, Matthew C. (2011) "Cyber-Attacks and the Use of Force," *The Yale Journal of International Law* 36.

- Tsagourias, Nicholas (2013) "Cyber Attacks, Self-Defense and the Problem of Attribution," *Journal of Conflict & Security Law* 17, p. 229–44.
- Roscini, Marco (2014) *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press).
- Mansourov, Alexandre (2014) "North Korea's Cyber Warfare and Challenges for the US-ROK Alliance," Korea Economic Institute of America, Academic Working Paper Series.

Conventional threats from the Democratic People's Republic of Korea (DPRK)

By Yoshifumi Ide, Akira Igata, Gibum Kim, Sung Hyo Kim, and Tong Zhao

North Korea's conventional capabilities and its threats were not the primary subjects of the 2015 Northeast Asia Young Leaders Regional Security Seminar. Instead, presentations, discussions and the following TTX all focused on North Korea's growing capabilities regarding its nuclear weapons program, delivery vehicles, and cyber warfare, which are mostly classified as nonconventional threats. However, the DPRK's conventional military capabilities were a critical factor that affected the South Korean group's discussions during the breakout sessions. In general, talks among other groups about North Korea's conventional threat mostly touched upon its missile development and the security threat it poses to neighbors.

During the TTX, before deciding the moves in response to the alleged North Korean action, the South Korea team had to consider the DPRK's conventional threat capability to anticipate how the DPRK would respond to US-ROK countermeasures and to avoid unnecessary conflict escalation. It is assumed that North Korea will continue to develop its conventional military capabilities alongside asymmetric ones such as nuclear weapons and long-range missiles. Artillery and rockets deployed by the North Korean army are heavily concentrated along the Demilitarized Zone (DMZ) between the two Koreas. Their primary target is Seoul. Thus, there is a danger of North Korean artillery shells raining down on the city to inflict damage, including massive civilian casualties.

The DPRK's missile development and deployment is, and will continue to be, the greatest conventional security threat to neighboring countries. The conference participants addressed the challenge of North Korean long-range missiles, but the DPRK's deployment of transporter erector launchers (TELs) and short-to medium-range nonnuclear-tipped missiles are formidable threats to all nearby countries, not just South Korea. A considerable part of North Korea's investment in its missile program is presumed to have gone to short-range missiles, which would likely be used in regional conflicts. As pointed out by the China team, the DPRK's possession of such short-to medium-range firepower implies that it does not need to use nuclear weapons to deter an armed attack from its southern border or the US-ROK alliance, as long as it does not attack them first. Japan's nuclear power plants near the Sea of Japan (East Sea) while currently inactive could become targets of DPRK missiles, which would complicate Japanese calculations in a conflict. However, the strategic downside for North Korea, and even China, is that the US, ROK, and Japan are highly likely to strengthen security cooperation in the face of an increasing DPRK conventional threat. Options for bilateral or trilateral military cooperation are deploying advanced weaponry, adopting reinforced countermeasures, or conducting joint military exercises near the Korean Peninsula. Improved bilateral or trilateral military cooperation among the three countries aimed at deterring and countering a North Korean threat could threaten the security interests of other states, especially China. The recent controversy over deployment of the Terminal High Altitude Area Defense (THAAD) system to South Korea shows how messy things

could become, irrespective of the understanding of the potential of such military platforms and the intentions relevant states have.

The DPRK's cyber warfare capability was also discussed as an emerging threat that needs more attention. The unpredictability of cyberattacks, their potential to inflict severe damage without much cost, and the difficulty of conducting a proportional response to such hostilities were core reasons why cyber threats are considered a serious concern. Many conference participants worried that cyber-attacks could be a prelude to massive conventional military aggression. It was noted that more innovative instruments are needed to counter new types of hostilities that use cyber capabilities. The scenario in the TTX reflects the dangerous potential of these attacks and the shortcomings of regional states dependent on conventional means of retaliation.

Lastly, discussions during the meeting were a stark reminder of divisions when responding to North Korean threats. While the US, Korea, and Japan teams favored tougher measures in the face of North Korean provocations – even though the three diverged when assessing exactly how harsh they should be – the China team argued that coercive policy toward the DPRK would not achieve denuclearization. This proves that effective countermeasures against North Korean conventional capabilities require thinking not only about beating DPRK capabilities *per se*, but also coordinating better with regional countries.

Suggested readings

- Cha, Victor. *The Impossible State: North Korea, Past and Future* (New York City: Ecco Press, 2013)

This is a close examination of the nature and identity of the DPRK regime viewed from various angles. A comprehensive understanding of North Korea's past and current affairs ranging from high politics, economic policies to military development and cultural shift is helpful in analyzing and predicting North Korea's conventional military capability development.

- Cordesman, Anthony H., and Ashley Hess. *The Evolving Military Balance in the Korean Peninsula and Northeast Asia* (Washington, D.C.: Center for Strategic & International Studies, 2013)

This is a comprehensive summary of the security strategies, military spending, military modernization, conventional, and asymmetric force posture and development trends of states in Northeast Asia, with emphasis on North Korea. Despite being slightly dated, readers acquire in-depth knowledge of security matters on the Korean Peninsula to better understand the dynamics of inter-Korean security relations and regional affairs.

- Kydd, Andrew H. *Trust and Mistrust in International Relations* (Princeton, New Jersey: Princeton University Press, 2007)

A country should adopt policies that avoid another country's worst fears. Restraint will encourage other countries to act similarly. This book argues that reassuring other countries and guaranteeing them some benefit, is in a state's best interest.

- Office of the Secretary of Defense. *Military and Security Developments Involving the Democratic People's Republic of Korea 2013* (Washington, D.C.: Office of the Secretary of Defense, 2014)

A concise summary of security threats posed by the DPRK, compiled for an annual report to Congress. Basic, but helpful in understanding the situation on the Korean Peninsula.

- Scobell, Andrew, and John Sanford. *North Korea's Military Threat: Pyongyang's Conventional Forces, Weapons of Mass Destruction, and Ballistic Missiles* (Carlisle, Pennsylvania: The Strategic Studies Institute, 2007)

This is an authoritative and comprehensive review of North Korea's conventional military and WMD capabilities. Despite being a little dated, it remains a good summary of North Korea's conventional military structure.

Discussion questions

1. Given the need to balance deterrence of DPRK attacks with minimizing the risks of escalation, is there an asymmetrical yet proportional response to low-intensity conventional DPRK aggression that will serve as a better countermeasure than a symmetrical conventional attack? (This year's TTX was a comparable, but essentially opposite case: a DPRK nontraditional attack triggered a conventional response by the ROK and the US).

2. How can the two Koreas avoid small-scale exchange of fire or military incidents along the Korean Demilitarized Zone (DMZ) and the Northern Limit Line (NLL) in the Yellow Sea (West Sea) from escalating, undermining stability more broadly as a consequence?

3. How have recent efforts by both the ROK and Japan to strengthen political and military cooperation affected DPRK military decisions? As there are UN rear bases in Japan that could be mobilized under the UN Command when armed conflict breaks out in the Korean Peninsula, and the transformation of Japan's military posture, how would the DPRK respond to ROK-Japan security cooperation beyond information sharing?

4. Has military and diplomatic trust between DPRK and China diminished in any meaningful degree due to DPRK provocations? What would trigger a substantial change in Chinese attitude and policy toward the DPRK, and how far will China go regarding sanctions should the DPRK pass the tipping point? What is the tipping point for China?

5. What is the DPRK's worst case, assuming that it continues to develop nuclear weapons and long-range missiles? What would cause the worst case to occur? Would the DPRK come to the negotiating table in such a desperate situation and give up its nuclear program, or would it self-destruct?

6. The DPRK's current strategy is believed to stress and maintain numerical superiority in conventional arms inventory and force posture to offset ageing equipment. While South Korea has had technical superiority over North Korean forces for almost two decades, the DPRK's heavy investment in missiles and artillery complicates the balance between the two militaries. Neither side is close to full-spectrum dominance and this

delicate balance limits fast conflict escalation. If both Koreas agree to establish new confidence-building measures in the midst of ongoing tensions, what is the easiest place to start?

Suggestions for future research

1. The development, deployment, and employment of military drones by North Korea and its military implications.

2. The utility and efficacy of existing sanctions on DPRK military capability development and arms trade.

3. Factors that impact the quality of the conventional DPRK threat, in particular, ROK psychological warfare (propaganda tactics). Do different operations demoralize DPRK forces (i.e., blasting anti-DPRK rhetoric or K-pop through loudspeakers across the DMZ, balloon campaigns to scatter propaganda leaflets on DPRK, sending propaganda over radio broadcasts) and how much?

4. DPRK leadership goals and scenarios that could lead to achieving them. Neighboring countries have adopted both appeasement and hardline policies to cope with threats from the DPRK and ensuing instability. To reassure North Korea and start confidence-building, which could lead to arms control, we need a better understanding of the DPRK regime's goals, strategy, and logic. Depending too much on "deterrence" could provoke other neighboring countries and fuel a security dilemma.

5. DPRK investment in conventional forces development. Assessments of arms control and disarmament agreements as well as comparative research of the conditions shaping past cases and the Korean Peninsula.

Regional cooperation and improving HA/DR capability in Northeast Asia

By Zhang Hongzhou, Xiao Kang, Amane Kobayashi, Meng Li, Rie Takezawa, and Wrenn Yennie-Lindgren

This paper focuses on the challenges of regional HA/DR (Humanitarian Assistance/Disaster Relief) cooperation in Northeast Asia, from the perspectives of Japan, South Korea, China, and the US, using two recent earthquakes as examples. The 2011 Tohoku earthquake in Japan and 2008 Sichuan earthquake in China showed that sharing relevant information and preventing mistrust and misperception between providers and recipients of aid are critical for effective HA/DR operation. In Northeast Asia, however, historical and territorial conflicts undermine cooperation, particularly for the recovery of critical infrastructure. To ensure and improve regional HA/DR capability, Northeast Asia must institutionalize a regional HA/DR cooperation mechanism to minimize mistrust and misperception and maximize efficiency and effectiveness of operations.

Defining HA/DR

HA/DR (Humanitarian Assistance/Disaster Relief) is defined as humanitarian assistance operations, including: disaster relief, rehabilitation, food assistance, foreign consequence management (for chemical, biological, radiological, nuclear, and high-yield explosives), displaced civilian support, and logistical and technical support. "Disaster relief" in HA/DR has a wider strategic concept that includes manmade disasters such as civil war or destruction of critical infrastructure. HA/DR is currently considered a nontraditional security mission/operation involving the cooperation of governments, NGOs, and military personnel.

Summary of the table-top exercise (TTX) scenario, focusing on HA/DR issues

The table-top exercise at the Northeast Asia Regional Young Leaders Security Seminar presented a complex set of potential HA/DR issues. The TTX involved a scenario where nuclear power plants in both South Korea and Japan malfunctioned. Groups deliberated issues such as evacuation, preventing radioactive contamination, and supplying basic needs. The teams' initial reactions to the scenario varied but the possibility of an impending humanitarian crisis on the Korean Peninsula was a common point of discussion. For instance, the US team discussed civilian assistance to mitigate radiation and to aid in possible evacuations. A potential humanitarian crisis spurred by the fall of the North Korean regime was also discussed, as well as the possibility of "nuclear refugees" in both South Korea and Japan. These HA/DR issues must be kept in mind throughout each stage of the TTX and alliance structures would likely play a key role in response. Another crucial part of prepping for HA/DR issues involves informing – and reassuring – concerned publics. All teams considered this and communicated overall scenario developments to their country's citizens. While preparation and response points for addressing HA/DR issues developed with each move in the scenario, it did not become necessary to put them into action.

Japan: Tohoku earthquake disaster and response

On March 11, 2011, a 9.0 magnitude earthquake occurred 81 miles east of Sendai, Japan. The Tohoku area in eastern Japan suffered devastating damage from the earthquake and from the 10m tsunami that followed. The tsunami affected coastal cities and crippled the Fukushima Daiichi nuclear power station, which caused the meltdown of reactor cores and a hydrogen explosion that released radioactive material. The March 11, 2011 disaster was a challenge for the Japanese government as it was the first time the government faced a multifaceted and cascading disaster.[1] Though Japan had experienced several severe earthquakes, the disaster relief for the Tohoku earthquake was especially difficult as it was the first large-scale disaster involving multiple prefectures since World War II. In widespread areas, roads were shut down and communications were severed, paralyzing many local governments. The central Japanese government was especially important in coordinating multi-layered disaster relief operations. In the event of a nuclear accident, the Japanese government can convene the Emergency Situations Ministerial Meeting at the National Security Council (NSC) and declare "Article 16: Establishment of Nuclear Emergency Response Headquarters" of the Act on Special Measures Concerning Nuclear Emergency Preparedness.[2] This enables a single governmental organization to conduct information and intelligence gathering, and crisis management, including communication with foreign governments. However, the domestic mechanism for inter-ministerial cooperation and public-private partnerships for disaster management did not work efficiently, and there was no capacity to accept and coordinate foreign assistance. As a result, Japan had limited ability to accept aid or support.

The crisis revealed gaps in accident preparedness, especially planning for nuclear emergencies, within the Japanese government and with the plant operator Tokyo Electric Power Company (TEPCO). As the situation at the nuclear power plant worsened, many countries offered material resources and expert advice on how to stabilize the nuclear reactors and the spent fuel pools. The Obama administration dispatched a team to resolve the crisis, but the collaboration was disorganized, and created mistrust and misperception between the two governments. With each government working with different information, the analysis of the situation and the solutions proposed were different. Japan faced for the first-time the challenges of receiving foreign assistance and the importance of creating an operational framework for responding to a nuclear accident.

Operation Tomodachi, undertaken by the US military and the Japan Self-Defense Forces (JSDF), supported the disaster relief effort. This response was notable not only for its scale but also its extensive and complex management. The cost of intervention can be high and encompasses a large number of workers and equipment. In *Operation Tomodachi*, costs came to $90 million and involved 24,000 US service members, 189 aircraft, and 24 ships.[3] The destruction of essential infrastructure and large-scale

[1] National Bureau of Asian Research, *Chronology of Operation Tomodachi*, March 11–April 8, 2011, http://www.nbr.org/research/activity.aspx?id=121

[2] Japanese Ministry of Justice, Japanese Law Translation Database System, http://www.japaneselawtranslation.go.jp/law/detail_main?re=2&vm=02&id=106

[3] Moroney, Jennifer D. P., Stephanie Pezard, Laurel E. Miller, Jeffrey Engstrom, Abby Doll (2013) *Lessons*

displacement of the people affected by the disasters remains a challenge. In addition to the US, 163 countries and 43 international organizations provided medical or financial support or relief. Research has identified areas where response challenges persist, such as the restoration of evacuees' livelihoods[4] and ensuring gender equality in post-disaster decision-making (Saito 2012).

China: HA/DR and the Sichuan earthquake

During the first stage of recovery after the 2008 Sichuan earthquake, four international earthquake disaster relief teams participated in search and rescue from Russia, Korea, Singapore, and Japan.[5] Those four countries have close relationships with the Chinese national earthquake disaster relief team (China International Search & Rescue Team, CISRT), had trained together and shared perceptions and experiences. China first held an international earthquake drill in 2006 and 17 teams, including those from the ROK, Japan, and the US, participated. Trust among countries responding might have been strengthened by frequent communication and cooperation. Another reason for the successful cooperation during the Sichuan earthquake may be the "professional to professional" cooperation mechanism. During the Sichuan earthquake, the teams invited to help were professional HA/DR forces belonging to specific government departments or NGOs; the teams took civilian aircraft to the earthquake area and carried only rescue equipment. The teams focused on rescuing survivors and other humanitarian jobs and complied with the overall arrangements of the Chinese government. Given the sensitivity of Northeast Asian countries – a result of history and geopolitics – to the behavior of the US military and that of their neighbors, repair of this kind and avoiding military involvement could minimize the mistrust and maximize the goodwill between the countries in this region.

In addition, the 2008 Sichuan earthquake in China provided valuable lessons on addressing food security challenges. Immediately after the earthquake, tens of thousands of displaced survivors were living in makeshift tents or on the streets and faced shortages of food. With the massive inflow of rescue forces, the food shortage became an even bigger challenge. The Chinese government, NGOs, individual volunteers, and the international community in the later phase began to provide emergency food relief to affected areas. However, most of the food supplies were nonperishable, with little fresh food and little consideration for the dietary and nutritional needs of diverse types of people. As a result, children and infants were sometimes provided the same food as adults. Nutrient deficiency became a serious issue, particularly for infants and the wounded. The Chinese government and international agencies such as UNICEF worked together to introduce complementary food supplements. For instance, UNICEF provided vitamin A capsules and nutritional supplements to 150,000 children and women in the aftermath of the earthquake, helping to combat the risk of acute malnutrition. Shortly after, the China

---

from Department of Defense Disaster Relief Efforts in the Asia-Pacific Region, RAND Cooperation. http://www.rand.org/pubs/research_reports/RR146.html.

[4] Mosneaga, Ana. (2015) "Restoring Livelihoods after Disasters: The Case of Fukushima's Nuclear Evacuees," *Policy Brief*, No.2, United Nations University Institute for the Advanced Study of Sustainability, http://i.unu.edu/media/ias.unu.edu-en/news/10502/UNU-IAS-Policy-Brief-No.-2-2015.pdf.

[5] In the end, a total of 166 countries and 16 international organizations provided funding or aid to China.

Centre for Disease Control developed a national nutrition security plan that aims to ensure that nutrition considerations are central elements of future emergency operations in China. A few months later, in October 2008, with assistance from the US Department of Agriculture's (USDA) Foreign Agricultural Service (FAS) and Global Child Nutrition Foundation (GCNF), China began to develop an efficient nutrition-based feeding program for schools in the earthquake-affected areas as a model.

China's experience shows that efforts to achieve food security must be multidimensional, and cooperation with the international community is critical. This cooperation will be even more necessary in the scenario of a nuclear power plant meltdown in South Korea. Unlike China, which has a high degree of food self-sufficiency, South Korea is heavily dependent on food imports. Fear of radiologically contaminated food means the public avoids consuming food not only from directly affected regions but surrounding areas as well. This could result in huge food supply gaps, which can only be filled by imports and international cooperation. China and Japan, owing to similar food culture and physical proximity, can play a critical role in helping South Korea during a crisis. Moreover, there is a need to establish a Northeast Asia Emergency Food Reserve. The United States, the biggest food exporter in the world, has an important role to play. The US commitment to ensuring a stable food supply to South Korea during a crisis will help prevent panic-buying and speculation in South Korea.

As it can take three to five years to rebuild the agricultural sector after a big disaster, ensuring food security has to be a long-term goal and commitment. After the earthquake in 2008, it was estimated that the agricultural sector in Sichuan province suffered $6 billion in losses. A significant portion of crops could not be harvested because of a shortage of labor as a result of deaths and injuries in farming families. These losses would occur in South Korea in a nuclear accident, and it could take decades for agricultural production to recover. Therefore, long-term support from the national government and the international community is needed to rebuild food production systems and to ensure that there is a food supply for affected regions.

US HA/DR strategy, particularly in the Asia-Pacific region

Events in the Asia-Pacific have focused attention on disaster response and recovery over the past 15 years. Large-scale disasters have both challenged and propelled collaboration on bilateral and multilateral levels. The United States plays an important role in ensuring that the peace and stability of East Asia is maintained through its alliance structures and active diplomacy. The US has been key in responding when disaster strikes, as well as in disaster preparedness and post-disaster relief. This section addresses the United States' humanitarian assistance/disaster relief (HA/DR) strategy, with a particular focus on activities in the Asia-Pacific.

Asia is a disaster-prone region, with a notable share of the world's earthquakes, tsunamis, floods, typhoons, and volcanoes. In addition to these physical threats, health threats challenge HA/DR efforts. Recently, pandemics such as MERS or Zika have reminded planners that health disasters do not discriminate geographically and that addressing these threats requires close international coordination and cooperation. Both

immediate disasters and disaster trends that are more diffuse in space and time such as droughts, epidemics, and global changes (sometimes called "chronic disasters") are often transnational in nature. In 2004, the Indian Ocean tsunami claimed the lives of over 230,000 people from 14 countries. This disaster not only set precedents by initiating domestic, bilateral, and multilateral frameworks for responding to disaster, but it also showed the international nature of a disaster in a globalizing world. The US has played a supporting, and at times coordinating, role as states in a region encompassing the globe's largest economies and populations are confronted by disasters and engage in "drought diplomacy," "earthquake diplomacy," and "tsunami diplomacy."[6]

The US military is often the primary responder to large-scale disasters. Although disaster relief is not a primary mission or area of expertise for the military, it reinforces and tests the interoperability and habits of cooperation within alliance structures. Military HA/DR has been at the forefront of US responses to disaster in the Asia-Pacific; the most recent example is the US-Japan response to *Typhoon Haiyan* in the Philippines in November 2013.[7] The joint capabilities of US Forces Japan (USFJ) and the Japanese Self-Defense Force facilitated disaster response by coordinating communications, logistics and access capabilities, reconnaissance of the missing, and medical care. The US government is actively engaged in initiatives to increase disaster response capacity by leveraging comparative advantages of allies and partners in the Asia-Pacific. The US-Japan response to *Typhoon Haiyan* is a testament to the benefits of such collaboration. In addition to the US and other government response mechanisms, assistance from aid agencies and nongovernmental organizations contribute to and complement immediate and ongoing relief efforts.

The US ability and willingness to come to the aid of disaster-struck countries and regions has been an important reinforcement of alliance mechanisms, as it provides an opportunity to build trust and to capitalize on unique capabilities to ensure the best response. Continued coordination and studies on best practices/approaches help states to prepare for the next disaster. One of the most well-known examples of US HA/DR in the Asia-Pacific was *Operation Tomodachi*. 2016 marks five years since the triple disaster hit Japan and offers an opportunity to reflect on how far bilateral cooperation and coordination on HA/DR has come and how it can be enhanced in the Asia-Pacific. While *Operation Tomodachi* has been lauded and deemed "a model for American disaster response efforts" abroad[8], assessments of the response to the Fukushima nuclear crisis have been mixed. Five years on, there are still tens of thousands of displaced "nuclear refugees" and the accumulation of radioactive water on the site remains a concern.[9] A

[6] Kelman, Ilan. (2012) *Disaster Diplomacy: How Disasters Affect Peace and Conflict*, Routledge, Abingdon, U.K.

[7] Other major US HA/DR operations in the Asia-Pacific region include: Cyclone Nargis in Burma (2008), the Padang earthquake in Indonesia (2009) and monsoon floods in Pakistan (2010).

[8] See Wilson RK (2012) "Operation TOMODACHI: A Model for American Disaster Response Efforts and the Collective use of Military Forces Abroad" *Journal of Defense Management* 2:108.

[9] Roberts, David and Norman Neureiter, "Five Years After Fukushima," *Foreign Affairs*, Feb. 16, 2016, https://www.foreignaffairs.com/articles/japan/2016-02-16/five-years-after-fukushima; Soble, Jonathan, "Fukushima Keeps Fighting Radioactive Tide 5 Years After Disaster," *The New York Times*, March 10, 2016, http://www.nytimes.com/2016/03/11/world/asia/japan-fukushima-nuclear-disaster.html

series of powerful earthquakes in Kumamoto in southern Japan in spring 2016 have reminded the Japanese of the fragility of communities, especially those located in close proximity to nuclear plants, and the need for concerted efforts in relief support.[10]

While enhancing HA/DR in the Asia-Pacific merits a report of its own[11], effective channels of communication and information sharing are arguably the most crucial elements for fast and efficient disaster response efforts. In addition to constantly updating and testing organizational response mechanisms, ensuring that there are established points of contacts and people with prior experience with disaster response, and collaborating with specific, established counterparts facilitate communication and response efforts. By seeking bilateral and multilateral cooperation and coordination on HA/DR in the Asia-Pacific, the US helps to enhance response capacity and the maintenance of a stable security environment within the region and beyond.

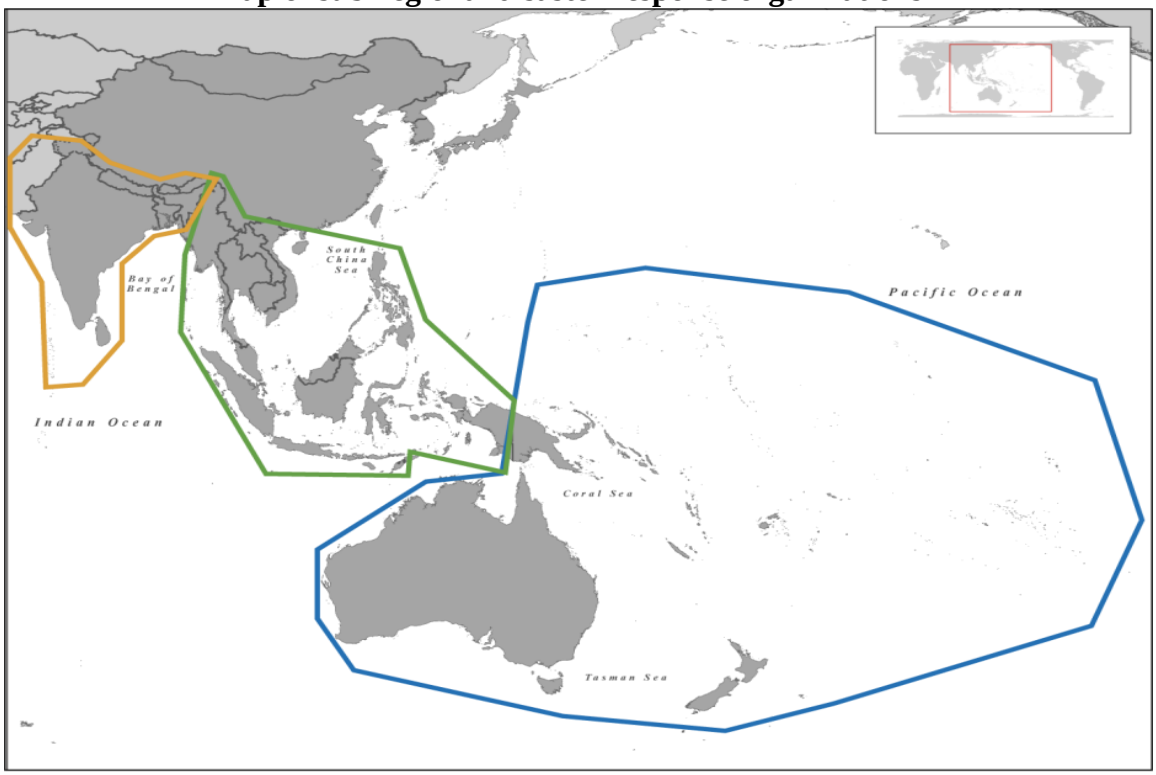
Discussion questions

The TTX and case studies of regional HA/DR cooperation in Northeast Asia pose difficult questions. First, how can counterparts share information and intelligence, particularly about critical technologies and infrastructure such as nuclear power plants? How can we prepare for deploying troops, ships, or aircraft for HA/DR?

Second, how can the region establish effective cooperation mechanisms? While international disaster relief frameworks are becoming well organized (as shown in the map below of sub-regional disaster response organizations in the Asia-Pacific), there is no institutionalized cooperation mechanism for HA/DR among China, ROK, Japan, the DPRK, the US, and Russia. During the TTX, facing severe nuclear accidents in the ROK, both the ROK and Japan teams could not decide what to request/respond for nuclear disaster relief.

[10] Soble, Jonathan, "New Sense of Fragility in Japanese Town Struck Twice by Quakes," *The New York Times*, April 17, 2016, http://www.nytimes.com/2016/04/18/world/asia/japan-earthquake.html
[11] For one recent and comprehensive report, see: Moroney et al. (2013).

Map of sub-regional disaster response organizations[12]



ASEAN Member States:
Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Singapore, Thailand, Viet Nam.

SAARC Member States:
Bangladesh, Bhutan, India, Maldives, Nepal, Pakistan, Sri Lanka.

SPC Member States:
Australia, The Cook Islands, The Federated States of Micronesia, Fiji, Kiribati, The Marshall Islands, Nauru, New Zealand, Niue, Palau, Papua New Guinea, Samoa, The Solomon Islands, Tonga, Tuvalu, Vanuatu.

Suggestions for future research

Comparative studies of Asia-Pacific regional HA/DR cooperation would be beneficial. Identifying best practices and lessons learned in Southeast Asia[13] or South Asia would have implications for Northeast Asia. The ASEAN Agreement on Disaster Management and Emergency Response (AADMER),[14] South Asian Association for Regional Cooperation (SAARC) Natural Disaster Rapid Response Mechanism (NDRRM)[15] and UN's International Search and Rescue Advisory Group (INSARAG),[16]

[12] UN OCHA, http://www.unocha.org/publications/asiadisasterresponse/images/figure3.png
[13] Centre for Non-Traditional Security Studies at Rajaratnam School of International Studies in Singapore briefs on ASEAN's regional capacity for disaster response operations. http://reliefweb.int/sites/reliefweb.int/files/resources/NTS-Bulletin-March-2015.pdf
[14] The ASEAN Agreement on Disaster Management and Emergency Response, http://www.ahacentre.org/about-aadmer
[15] South Asian Association for Regional Cooperation, http://saarc-sadkn.org/ndrrm.aspx

could be references. As the Chinese saying goes, *"A near friend is better than a far-dwelling kinsman."* It is critical for the cooperative and effective regional HA/DR mechanism to build trust, share relevant information, and prevent misperceptions between providers and recipients of aid.

Sources and suggested readings/sources

- Annie Isabel Fukushima, Ayano Ginoza, Michiko Hase, Gwyn Kirk, Deborah Lee and Taeva Shefler, *Disaster Militarism: Rethinking US Relief in the Asia-Pacific*, Institute for Policy Studies, March 2014.
- Fargo, Thomas B., Noboru Yamaguchi, Ryo Sahashi, Kei Koga and Alison Szalwinski, *Preparing for Future Disasters: Strategic Assistance and the US-Japan Alliance*, The National Bureau of Asian Research, 2015.
- Gregson, Wallace C., *Disaster Response Operations, Resilience, and Regional Stability in Asia*, The National Interest, June 19, 2015, http://nationalinterest.org/feature/disaster-response-operations-resilience-regional-stability-13146.
- The Independent Investigation Commission on the Fukushima Nuclear Accident "The Fukushima Daiichi nuclear power plant station disaster, investigating the myth and reality" Routledge, 2014, New York
- Kelman, Ilan, *Disaster Diplomacy: How Disasters Affect Peace and Conflict*, Routledge, Abingdon, UK, 2012.
- Moroney, Jennifer D. P., Stephanie Pezard, Laurel E. Miller, Jeffrey Engstrom, Abby Doll, *Lessons from Department of Defense Disaster Relief Efforts in the Asia-Pacific Region*, RAND Cooperation, 2013.
- Mosneaga, Ana, "Restoring Livelihoods after Disasters: The Case of Fukushima's Nuclear Evacuees", *Policy Brief*, No.2, United Nations University Institute for the Advanced Study of Sustainability, 2015, http://i.unu.edu/media/ias.unu.edu-en/news/10502/UNU-IAS-Policy-Brief-No.-2-2015.pdf.
- Sakai, Minako, Edwin Jurriëns, Jian Zhang, Alec Thornton eds, *Disaster Relief in the Asia Pacific: Agency and Resilience*, Routledge, 2014.
- United Nations Office for the Coordination of Humanitarian Affairs, International Humanitarian Architecture, http://www.unocha.org/publications/asiadisasterresponse/InternationalHumanitarianArchitecture.html#Regional%20intergovernmental%20organizations%20and%20forums
- United Nations University, Fukushima Global Communications Programme, http://fgc.unu.edu/en/
- US Army Support to Humanitarian Assistance and Relief Operations, http://www.army.mil/standto/archive/issue.php?issue=2012-01-03.
- Wilson RK (2012) "Operation TOMODACHI: A Model for American Disaster Response Efforts and the Collective use of Military Forces Abroad" *Journal of Defense Management* 2:108.

[16] International Search and Rescue Advisory Group, http://www.insarag.org/

Northeast Asia Regional Security Architecture

By Julia Jungmin Oh, Shino Hateruma, Yoko Mori,
Tatsuya Sakurai-Jyc Liu, Nahee Kim, and Shuo Wang

Northeast Asia does not have discrete regional security architecture. Despite numerous interrelated traditional and nontraditional security issues – North Korea's nuclear proliferation, disputed maritime claims in the East and South China Seas, territorial disputes and historical issues largely between China, Japan, and South Korea, terrorism, disaster relief, cyber-attacks, climate change, and energy – there is a considerable gap in motivation and trust, resulting in a lack of momentum to establish an institutionalized security architecture.

Some point to the Six-Party Talks or the Shanghai Cooperation Organization as successful Northeast Asia-led multilateral regional security architectures, but no institution like the European Union or ASEAN exists. Some argue that US alliance relationships with Japan and the Republic of Korea render such an organization unnecessary or stand in the way of its creation.

Key to establishing a common regional security architecture is clarification of the issues: nuclear safety and nonproliferation may be of shared concern. On issues such as dealing with North Korea or how to regulate nuclear energy, cooperation is pursued through organizations such as the Asia-Pacific Regional Cooperative Agreement (RCA) or the Asia Nuclear Safety Network (ANSN), the International Atomic Energy Agency (IAEA), the World Association of Nuclear Operators (WANO), and even the United Nations.

Dialogue among Young Leaders in Seoul demonstrated that each country had different interests in regional cooperation and mutual distrust toward each other; there was even doubt whether Northeast Asian countries had a shared goal.

The next section explores obstacles to the creation of a regional security architecture. Mistrust is one of them. It also presents insights on sustainable security structures in Northeast Asia. The third section identifies future research topics on this issue and suggested readings.

Northeast Asian regional security architecture

What hinders cooperation in the region? National security is increasingly comprehensive in nature. Core concepts include commonality, universality, and cooperative concerns. China has demonstrated its commitment to regional security mechanisms through participation in multilateral organizations such as the Six-Party Talks, the ASEAN 10+1 and 10+3, Shanghai Cooperation Organization, and ASEAN Defense Ministers Meeting-Plus. Yet, China’s commitment to a cooperative relationship with Northeast Asian countries is hindered by its worries about the US-Japan and US-Korea military alliances, and a lack of trust. Opinion polls reveal alignments and

divergences among these countries. A 2015 Japan-US-China-ROK joint opinion poll shows for example that while the US and Japan share national security interests, China has the biggest perception gap with Japan.

During the Seoul dialogue, participants noted that the situation on the Korean Peninsula directly impacts Northeast Asian security; indeed, the Korean Peninsula is the most urgent problem and the toughest challenge for security cooperation in Northeast Asia. Teams from China, Japan, South Korea, and the US tried to coordinate to ensure stability when a crisis occurred on the Korean Peninsula. But the four country teams had different interpretations of the conflict as well as competing interests and approaches to intervention. Other country teams believed that China would be a close "friend" of the DPRK and expected that the DPRK would share secrets with Beijing. While the China team was concerned that some actors would "overreact," others wanted China to be more resolute in its response to the DPRK's provocation.

Distrust is rife. The confrontation between North Korea and the United States has contributed to regional instability and led to tensions between China and the US. In 2002, President George W. Bush said North Korea was a member of the "Axis of evil" and called on the world to impose strong sanctions on it. China opposed coercion against the DPRK and still does. In our exercise, the China team preferred that the world embrace the DPRK and encourage it to reform as China has. Although the China team claimed to be doing its utmost to restrain North Korea, other teams considered China to be too lenient. This led to tension between them and China. There is also significant distrust toward Japan. During the TTX, the China team emphasized that other country teams should "not overreact," a sign of suspicion toward Japan and South Korea. The Korea team was concerned about the prospect of Japanese military interference and responded by asking for help only in sharing intelligence. Japan's legacy of atrocities during World War II still hinders efforts to establish a Northeast Asia security mechanism.

Historical and territorial issues have hindered cooperation on security matters, especially between South Korea and Japan. Both governments have tried to reduce tensions, but the gap in the two countries' positions on apology, politics, and other heated controversies makes it hard to move forward. Discord between South Korea and Japan gives the US an even more central role in Northeast Asia security architecture. The US is a dialogue facilitator and could be an arbitrator if conflict deepens.

Another obstacle to multilateral cooperation is strong bilateral tendencies in Northeast Asia. The US has been a critical partner for Japan and South Korea, and each country's alliance with the US has been critical to its security. Since the Korean War, South Korea has depended on the US for national security. Economic ties strengthened the bilateral relationship. A similar process ties the US and Japan together. Even China has an interdependent economic relationship with the US. It is difficult to reach a consensus on establishing a multilateral security mechanism without breaking with the bilateral mindset.

The absence of regional multilateral security mechanisms has led to suspicion, fear, and hostility among nations. TTX participants noted that a lack of information led to fear of escalation which dominated the discussion. To better understand the intentions of each country, security dialogues are needed.

China needs to be empowered as a trustworthy regional power. A security mechanism requires a set of rules that apply equally to all countries. These standards should be determined by all participants and fit the region's security environment. They should not be directed against any party, and must restrict every country equally. A security mechanism should provide a platform for consultation, dialogue, and cooperation among equals. The dialogue in Seoul made clear that the region is too disparate for this level of cooperation. Even trying to define a crisis revealed discord between the countries in Northeast Asia.

China's rise is altering regional dynamics, creating opportunities and causing problems. The US and China have conflicts over many issues but seek to coexist and cooperate when they can. China is being encouraged to follow international norms and stand firm against North Korea's provocations to bring about meaningful change in the region. China is vital to regional security cooperation. Therefore, building confidence among South Korea, China, and Japan is a precondition to a cooperative relationship to deal with security issues. But the China team concluded that the United States and Japan fear that China's rapid rise would culminate in an "Asian version of the Monroe doctrine," one that will exclude the US from a role in Northeast Asian affairs.

While South Korea's dependence on the US has traditionally aligned its national interests with those of the US, in recent years, South Korea has developed an increasingly close economic relationship with China which forces it to balance economic and security interests. Arguments over whether South Korea should join the US-led TPP trade deal or the Chinese-backed RCEP are signs of the competing tugs the ROK faces.

Some argue that closer ties between South Korea and China disturb the balance of power in the region. An alternative view suggests that South Korea's engagement of China is a way to strengthen regional security, especially when dealing with North Korea and could be the first step toward Northeast Asian multilateralism. South Korea is trying to diversify mechanisms to pursue its national interests by empowering China as a regional power. South Korea wants China to be more accountable when North Korea provokes. At the same time, deepening economic ties with China and Japan can be developed into a more political and diplomatic relationship. From there, Northeast Asia can lay a foundation for a cooperative relationship; this process resembles that of the EU, which originated as an economic community.

Economic partnership does not mean an alignment in security views, however. As North Korea's Jan. 6, 2016 nuclear experiment shows, China maintains existing relations with North Korea. South Korea responded to China's lukewarm reaction to pressuring Pyongyang by stressing the need to accept deployment of the Terminal High Altitude Area Defense missile (THAAD) system. China counters that this harms its security

interests and complicates regional peace and stability. Thus far, South Korea's attempt to change regional security dynamics has not had a significant impact on regional security.

For some, this disagreement is proof that security cooperation between South Korea, Japan, and China is impossible due to fundamental differences in national interests. In particular, they assert that as long as the US fears the rise of China and the two countries cannot find a workable compromise, China will continue to use North Korea to balance US influence in the region.

Nevertheless, the effort to find common ground to establish a regional cooperation mechanism must continue. Northeast Asian countries should arrange talks to minimize misconceptions, find solutions, and work together on regional security. Nuclear and related technologies are critical in Asia because of increasing energy demands resulting from rapid economic development. While Northeast Asia continues to depend on nuclear energy, there are concerns about the safe use of nuclear energy. In addition, there are worries about security at nuclear facilities: attacks on them can cause serious damage to nearby areas and neighboring countries. While there are a variety of regulations to promote nuclear safety and safeguards in Northeast Asian countries, but there is no regional institution that promotes nuclear safety cooperation.

The diversity of economic and technological achievements throughout Asia makes it difficult to set a single standard for all countries. Furthermore, concerns about proliferation can inhibit discussions about nuclear safety cooperation, which would tackle issues like nuclear proliferation resulting from the spread of technologies such as uranium enrichment and spent fuel-reprocessing.

The Top Regulators Meeting (TRM) held since 2008 between China, Japan, and South Korea is one platform for discussing nuclear safety cooperation in Northeast Asia. It includes a limited number of countries, but the discussion could evolve to provide a vision for security cooperation. For instance, following President Park's 2014 Northeast Asia Peace and Cooperation Initiative (NAPCI) (part of her *Trustpolitik* agenda), TRM+ was proposed; it would expand to include the United States, Russia, France, IAEA, with the hope for more discussion on nuclear safety and cooperation in the region.

NAPCI will have limited impact due to the larger shadow cast be security concerns. Leaders will have strong perspectives and it will be difficult to expect this mechanism to promote sustainable regional cooperation on nuclear safety. However, NAPCI recognizes the importance of involving significant players in the region to discuss hard security issues and build robust cooperation. Thus, the TRM+ discussion could forge a realistic and multilateral mechanism that focuses on building a broad safety culture, with stronger regulations for developed and developing countries in the region.

Suggestions for future research and reading

- Scrutinize the function and effectiveness of security frameworks and reorganize or unify them if necessary. There are too many regional groups and meetings Northeast

Asia should concentrate on productive meetings, not dispersing resources. A comparative study of the EU and ASEAN would help identify the kind of meetings and regional organization that are needed.

- Renew the commitment and engagement of leading countries. The US, China, Japan, and Korea countries are major players in the region and their commitment and leadership is required. South Korea showed its determination to push regional security by launching NAPCI. The US can hold joint exercises in the region to strengthen mil-mil relations. Japan is actively promoting capacity-building. Those efforts will be more consistent if undertaken under the same framework. Getting China to take part is critical; Beijing should play a more important and responsible role. Removing distrust should be a focus (e.g., identifying common threats, common interests and areas in which all four countries can cooperate with each other).

- Strengthen hotline network for unexpected event such as unplanned encounters at sea, natural disasters, and nuclear power plant accidents. Northeast Asia remains one of the world's flashpoints. Since problems will persist, hotlines can be set up and secured among all parties and a code of conduct can be developed to prevent accidents. A Multilateral Crisis Management system would be a good first step toward a regional security organization.

Conclusion

When we ask if all the countries in Northeast Asia share a goal, the divergence of interests is plain. Although the North Korea nuclear issue is a top concern, and regional and global frameworks have been addressing the issue, it seems that little has been accomplished. It is probably because each country seeks a different outcome. South Korea, Japan and the United States see a denuclearized North Korea differently than China does. Establishing an efficient regional framework is not a goal, but a process. Northeast Asia regional cooperation will not occur unless countries share the same goal and work to the same end. It is important to be united on regional interests, and realize that such cooperation can advance national interests.

Even when Northeast Asian countries agree on threats that does not mean that perceptions are the same: priorities probabilities differ. The TTX demonstrated that countries have different assessments of odds and outcomes. Many contingencies, including attempted attacks, natural disasters, and manmade disasters could happen to any country. Geographical proximity means that when crisis occurs, no single country can escape danger. To commence effective regional cooperation, it is beneficial to share assessments of risks and potential damage caused by contingencies.

Many factors impede progress on Northeast Asian regional cooperation. There is concern about the balance of power, mutual distrust, differing perceptions of history, territorial disputes, and all are magnified by domestic politics. While South Korea, Japan and the US expect China to play a more cooperative role when engaging North Korea,

China criticizes these countries for counterproductive measures. Given the diversity of perspectives and interests, regional cooperation is extremely difficult.

But while national interests appear to be divided, threats are shared. Although forging a cooperative security mechanism remains beyond reach, countries should seize opportunities to move forward. Progress will be slow, but effort must be continuous.

Suggested readings

- Jen Pearce, "HADR and China-US Military Cooperation," *The Diplomat*, July 28, 2014, http://thediplomat.com/2014/07/hadr-and-us-china-military-cooperation/
- Republic of Korea, Ministry of Foreign Affairs, *Northeast Asia Peace and Cooperation Initiative,* http://www.mofa.go.kr/ENG/North_Asia/res/eng.pdf
- Haejin Kim, "Northeast Asia, Trust and the NAPCI," *The Diplomat*, Dec. 18, 2015, http://thediplomat.com/2015/12/northeast-asia-trust-and-the-napci/
- Takeshi Yuzawa, "The Roles of Regional Security Institutions in the Era of Power Shift: The Implications for Japan-China Relations," The Tokyo Foundation, http://www.tokyofoundation.org/en/topics/japan-china-next-generation-dialogue/roles-of-regional-security-institutions

Nuclear safety and security

By Diana Lee, Jim Platte, Crystal Pryor, and Tristan Volpe

In the "second nuclear age," Northeast Asia has become the heart of nuclear safety and security concerns – including nuclear safeguards and proliferation. In this era, it is more difficult for the United States to assure its allies in Northeast Asia due to a rapidly shifting regional security environment.[1] As states possessing nuclear weapons, China and North Korea present important security concerns. Assurance is challenging despite strong US alliances with the Republic of Korea (ROK) and Japan.

North Korea's recent cyber-attacks, nuclear tests, and ballistic missile tests pose triple threats to the region. North Korea is thought to have 10-20 nuclear warheads and is developing more, and may soon be able to strike the western US with a ballistic missile.[2] Some believe that North Korea's cyber-attacks pose a threat even greater than its nuclear activities.[3] Even critical infrastructure previously thought to be safe from attack, like nuclear power plants, is understood to be at risk.[4]

North Korea also poses a major proliferation risk. The US government found that North Korea has shared nuclear materials with Libya and Syria, and has collaborated with Iran on missile development.[5]

Nuclear security has received increased attention in recent years due to the series of Nuclear Security Summits (NSS) that began in 2010 in Washington. The fourth (and seemingly final) Nuclear Security Summit was held in Washington after being held in Seoul in 2012 and The Hague in 2014. The Obama administration led this effort and pushed for multilateral cooperation to strengthen nuclear security worldwide, particularly on securing nuclear materials.

Our table-top exercise involved a North Korean cyber-attack on a nuclear facility in South Korea. This learning module addresses nuclear security and safety with regard to this exercise from three different dimensions – cyber security, nonproliferation export controls, and the US-ROK alliance. Our discussion, questions, and suggestions for further reading should contribute to what must be a multidimensional approach to ensuring nuclear safety and security in Northeast Asia.

---

[1] David Santoro and John K. Warden, "Assuring Japan and South Korea in the Second Nuclear Age," *The Washington Quarterly* (spring 2015).
[2] Zachary Keck, "Assessing the North Korea Nuclear Threat," *The Diplomat* (May 1, 2015).
[3] Jon E. Dougherty, "Defector: N. Korea prepared to unleash advanced hacker army on its enemies," Nationalsecurity.news (Sept. 9, 2015), http://www.nationalsecurity.news/2015-09-09-defector-n-korea-prepared-to-unleash-advanced-hacker-army-on-its-enemies.html.
[4] "What can we learn from the South Korea cyber nuclear hack?" Chatham House (March 17, 2015), http://cyber-and-nuclear-security.blogspot.co.uk/2015/03/what-can-we-learn-from-south-korea.html.
[5] Manyin et al., "North Korea: Back on the State Sponsors of Terrorism Lists?" Congressional Research Service (January 2015).

Critical nuclear infrastructure and information security: unpacking the risks

Over the last few years, a handful of high-profile incidents – more commonly known as "cyber-attacks" or "hacking" – generated growing concern over how information technology might impact critical infrastructure such as power plants and nuclear reactors. In 2007, the US government demonstrated that hackers could physically destroy a power plant with just 21 lines of malicious code. The infamous 2010 Stuxnet exploit took out Iranian enrichment centrifuges by gaining control of standard computer control systems used by industries around the world. In December 2014, hackers associated with North Korea gained access to the networks of nuclear facilities in South Korea and copied sensitive design and blueprint information from the servers. More recently, two power distribution enterprises in Ukraine claimed that hackers had compromised their networks and shut down power to more than 80,000 customers. As these examples underscore, information technology opens up a new range of challenges for the safe and secure operation of nuclear energy facilities.

The nuclear community has long been aware of the threat posed by information technology. Within the domain of strategic nuclear policy, for instance, the US government has invested considerable resources into assessing and responding to a cyber-attack on strategic command, control, and intelligence capabilities that could leave Washington blind and unable to give orders during a conflict. Antiquated legacy systems in civilian nuclear facilities means that the nuclear energy industry lagged behind the digital revolution by decades. With many of these pre-digital systems reaching the end of their life cycles, however, the community of operators, experts, and policymakers who deal with nuclear safety and security is rapidly coming up to speed on the risks of introducing information technology into nuclear facilities.

Not all cyber operations or hacks against the nuclear energy industry pose the same level or type of risk to the general population. This primer explains three distinct threats to nuclear facilities: confidentiality, availability, and integrity.

Confidentiality refers to protecting and keeping secret sensitive nuclear data from espionage and data theft. A 2014 North Korean hack against South Korean nuclear facilities is a prime example. The attack could have been an effort to gather information to pinpoint digital or physical vulnerabilities in the reactor, but the hackers did not gain control of the facilities. Malicious actors may also want to access sensitive nuclear data to jumpstart an illicit nuclear weapons program. In general, the nuclear industry has strong incentives to defend its networks against these "cyber spying" operations to maintain control over intellectual property. Encryption schemes can go a long way in protecting sensitive digital information from being used by malicious actors, but there are a number of key vulnerabilities in current networks.

Availability means keeping critical network services running at all times. This is a huge risk for nuclear facilities with digital technology. If malicious code enters a reactor's control systems and causes a shutdown, operators need to have redundant controls to avert a core meltdown. Hackers could also devise ways to turn a reactor into a

fallout-generating weapon against the local population. Indeed, there are a handful of scenarios where this unique capability could fit into a political-military strategy.

Integrity is the least understood and most dangerous problem for the nuclear industry. As one leading information security expert put it, the issue is assessing "whether the software and critical data within the network and systems are compromised with malicious or unauthorized code or bugs."[6] With a confidentiality breach, the hacker might learn valuable information about a facility or nuclear technology. But with an undetected integrity attack, hackers gain control over the facilities themselves. Last fall, James Clapper, the director of national intelligence, underscored that the biggest threat is "cyber operations that will change or manipulate electronic information in order to compromise its integrity instead of deleting or disrupting access to it." In other words, an operator of a nuclear reactor may not be able to trust the information on the digital screen.

The information security community is engaged in a digital arms race to develop effective solutions to these three distinct risks. For example, encryption locks might thwart espionage, but do little if a hacker has compromised the entire system. Integrity defenses in development are more akin to an active alarm system that detects unauthorized modifications and intrusions. As the nuclear industry catches up with the digital revolution, the nuclear security community should continue its efforts to fully integrate technical and policy developments from the information security community.

The table-top exercise and presentations during the Seoul Young Leader's meeting showed the potential threat to nuclear facilities posed by offensive cyber operations. North Korea's improving cyber capabilities makes that threat more real in Northeast Asia. North Korea's hacking of Sony and of South Korea's nuclear reactor operator, Korea Hydro and Nuclear Power (KHNP), in 2014 was discussed, and the table-top exercise proposed an even more extreme North Korean cyber-attack that crippled South Korea's oldest nuclear reactor, Kori-1.

The cyber-attack in the table-top exercise was conducted by North Korean agents introducing a USB drive into the air-gapped control systems of Kori-1. In December 2014, South Korean Minister of Trade, Industry and Energy Yoon Sang-jick stated that, in addition to the North Korean cyber-attack, a worm had been removed from air-gapped KHNP control systems, and the worm likely got into the systems inadvertently through the use of unauthorized USB drives.[7] Thus, the table-top exercise used real-world vulnerabilities, even in air-gapped nuclear reactor control systems.

---

[6] Mike Gault, "The CIA Secret to Cybersecurity that No One Seems to Get," Wired.com (Dec. 20, 2015), http://www.wired.com/2015/12/the-cia-secret-to-cybersecurity-that-no-one-seems-to-get/.

[7] "What can we learn from the South Korea cyber nuclear hack?" Chatham House Project on Cyber and Nuclear Security (March 17, 2015), http://cyber-and-nuclear-security.blogspot.co.uk/2015/03/what-can-we-learn-from-south-korea.html.

Proliferation risks in Northeast Asia

North Korea's bad behavior around nuclear material broadly poses great risks. North Korea conducted its fourth nuclear test on Jan. 6, 2016. The international community has been highly skeptical of North Korea's claims to having successfully tested a hydrogen bomb, but the event heightened regional security concerns. North Korea is also a chief proliferator of weapons of mass destruction (WMD) in Northeast Asia.[8] Unless the international community aggressively pursues preventative practices to immobilize North Korea's nuclear proliferation efforts, the denuclearization process will prove even more difficult.

North Korea will continue developing and testing WMD for its national security and defense as part of its two-track policy of military and economic development (the *byungjin* line).[9] The continued testing of advanced weapons technology is itself a grave issue, exacerbated by uneven implementation of sanctions and export controls by China and the United States and its regional allies, including South Korea. North Korea's efforts to improve and develop its nuclear program as well as other WMD will continue to challenge global nonproliferation efforts. Nuclear nonproliferation expert Mark Fitzpatrick notes that "the US and its allies can be expected separately to apply the kind of financial sanctions that were seen to be effective in persuading Iran to accept limits on its nuclear programme."[10] With North Korea, financial sanctions may open a channel for negotiations, which can be effective in the short term, but restricting weapons trade at borders with tight trade regulations will prevent North Korea from further proliferation.

A.Q. Khan's notorious proliferation network revealed in 2005 that nuclear weapons-relevant technologies were transferred to Libya, North Korea, and Iran. Through this network, North Korea obtained centrifuge parts for its uranium-enrichment program. When Libya declared its nuclear program in 2004, questions were raised as to whether the recovered containers of uranium hexafluoride came from North Korea. Discovery of Khan's network encouraged the international community to enhance national export control systems, including through UN Security Council Resolution 1540. Countries across Asia are increasingly producing and exporting sensitive technologies, and the entrepôt countries such as Myanmar, Malaysia, Singapore, and Taiwan also serve as transshipment hubs for materials.

One way to improve nonproliferation efforts is for Asian countries to harmonize export controls to the greatest extent possible. Although a region-wide export control regime like that of the European Union is probably too ambitious, the more Asian countries can agree on which proliferation-sensitive items should be controlled and to

[8] "Proliferation Challenges in Northeast Asia and South Asia," IISS conference proceedings (Sept. 4, 2014), http://www.iiss.org/en/events/eu%20conference/sections/eu-conference-2014-4706/special-sessions-6020/special-session-8-d1b3.
[9] Manyin et al., "North Korea: Back on the State Sponsors of Terrorism Lists?" Congressional Research Service (January 2015).
[10] Mark Fitzpatrick, "North Korea - Nuclear bombs and bombast," IISS Voices (Jan. 6, 2016), https://www.iiss.org/en/iiss%20voices/blogsections/iiss-voices-2016-9143/january-671d/north-korea---nuclear-bombs-and-bombast-10b4.

what destinations, the more effective the controls will be. Yet it is not enough for countries to simply have the legal infrastructure to monitor and control sensitive exports and transshipments. The devil is in the *implementation* of export control legislation. Outreach and cooperation is necessary in the implementation of both sanctions and export controls, including monitoring, enforcement, customs/port control, internal compliance programs, transit and transshipment. Those countries with more developed export control systems – Japan, the United States, and now the ROK – have a special interest in and obligation to conduct outreach. Joint statements between Singapore, Hong Kong, and Japan in 2004 on information sharing, conducting outreach activities, and encouraging other Asian countries to introduce stringent export control systems were important steps in this direction. China must also be brought on board since, "Longstanding China-North Korea economic ties enable North Korean entities to conduct business comfortably in China."[11] Mark Hibbs of the Carnegie Endowment for International Peace notes that North Korea gets much of its dual-use equipment and materials from China. China's continued supply of dual-use technologies to North Korea poses major WMD risks.[12]

In sum, to successfully initiate the denuclearization process, the international community should make a unified effort to reinforce nonproliferation measures preventing North Korean attempts to transfer weapons, parts, technologies, and knowledge in or out of the country. Countries trading with North Korea need to strengthen import/export measures and tighten border security against illicit movements. Governments and NGOs need to discuss barriers to nonproliferation controls, not only on tangible technologies but intangible ones including knowledge transfer.

Nuclear security and the US-ROK alliance

South Korea has strongly supported the NSS process and even hosted the second round in Seoul in 2012. While the Nuclear Security Summit process focuses on wider multilateral cooperation, cooperation between Seoul and Washington on the NSS process is indicative of the allies' shared interests in a broad range of nuclear issues, including safety, security, nonproliferation, and deterrence. The United States provides extended deterrence assurances to South Korea as part of the military alliance between the two countries, and other bilateral and multilateral agreements address cooperation on safety, security, and nonproliferation. The primary bilateral treaty that governs nuclear cooperation between South Korea and the United States is known as the 123 Agreement, and Washington and Seoul signed a new 123 Agreement in June 2015. The new 123 Agreement "…functions as a load-bearing beam, supporting the entire infrastructure of US-ROK nuclear partnership."[13]

[11] Stephanie Lieggi, Robert Shaw, and Masako Toki, "Taking Control: Stopping North Korean WMD-related Procurement," *Bulletin of the Atomic Scientists* (September/October 2010).
[12] Armin Rosin and Mark Hibbs, "How North Korea Built Its Nuclear Program," *The Atlantic* (10 April 2013), http://www.theatlantic.com/international/archive/2013/04/how-north-korea-built-its-nuclear-program/274830/.
[13] Scott Snyder, Toby Dalton, and Miles Pomper, "The Future of US-ROK Nuclear Cooperation," James Martin Center for Nonproliferation Studies (March 27, 2015), http://www.nonproliferation.org/the-future-of-us-rok-nuclear-cooperation/.

A key aspect of the new 123 Agreement is the creation of a new High-Level Bilateral Commission that will facilitate cooperation on "…shared objectives such as spent fuel management, assured fuel supply, promotion of cooperation between our nuclear industries, and nuclear security."[14] Working groups will be formed to address each of these issue areas, and the High-Level Bilateral Commission will be led by the ROK vice minister of foreign affairs and the US deputy secretary of energy.[15]

The new 123 Agreement builds on strong relationships between the US Nuclear Regulatory Commission (NRC), the Korean Institute of Nuclear Safety (KINS), and the Korean Nuclear Safety and Security Commission (NSSC). These three organizations regularly share "…advice on regulation and maintenance of protocols that are critical to the safe operation of nuclear reactors."[16] In addition to safety, the NRC also is responsible for regulating physical security, cyber security, and safeguards at US nuclear facilities and can assist South Korean authorities in these areas. The NRC also likely would provide advice to and support for ROK emergency responders, nuclear reactor operators, and nuclear regulators in case of a significant nuclear accident in South Korea, similar to how the NRC provided crucial support to Japanese authorities after the Fukushima nuclear accident in 2011.

The new 123 Agreement and the High-Level Bilateral Commission will give the allies a formal mechanism to discuss nuclear security after the Nuclear Security Summit process concludes. While the NSS process has focused on the physical security of nuclear materials, the discussions and table-top exercise conducted at this meeting demonstrated the need to address cyber security at nuclear facilities and the nexus between nuclear safety and security. Even though the United States and South Korea have relatively robust cooperation on nuclear issues, our meeting highlighted the need to strengthen regional cooperation on nuclear safety and security.

One attempt at building stronger regional nuclear cooperation is South Korean President Park Geun-hye's Northeast Asia Peace and Cooperation Initiative (NAPCI), which aims to build trust among regional actors, namely South Korea, Japan, China, and the United States, through dialogue on nontraditional security issues, such as disaster relief, nuclear safety, environmental protection, public health, energy security, cybersecurity, and transnational crime. After strengthening regional cooperation in these nontraditional security areas, NAPCI dialogue would expand to include traditional hard security issues.[17]

---

[14] White House.

[15] Toby Dalton, Scott Snyder, and Miles Pomper, "How South Korea Can Take Advantage of Nuclear Cooperation With the United States," Carnegie Endowment for International Peace (April 22, 2015), http://carnegieendowment.org/2015/04/22/how-south-korea-can-take-advantage-of-nuclear-cooperation-with-united-states.

[16] Scott Snyder, Toby Dalton, and Miles Pomper, "The Future of US-ROK Nuclear Cooperation," Carnegie Endowment for International Peace (30 March 30, 2015), http://carnegieendowment.org/2015/03/30/future-of-US-rok-nuclear-cooperation.

[17] Lee Sang-Hyun, "The Northeast Asia Peace and Cooperation Initiative (NAPCI): A Vision toward Sustainable Peace and Cooperation in Northeast Asia," *The Asan Forum*, The Asan Institute for Policy

NAPCI proposed to expand the Top Regulators Meeting (TRM) – a regular information exchange meeting between nuclear regulators in China, Japan, and South Korea established in 2008 – to the TRM+, which would include other regional actors such as the United States, Russia, and Mongolia. The TRM+ began meeting in 2013 but needs more time to better define the new mechanism's purpose, mandate, and desired outcomes. The fact that the TRM has now lasted longer than the Six-Party Talks gives reason to hope that regional cooperation on nuclear safety is improving. In addition to NAPCI's inclusion of nuclear safety, regional cooperation on nuclear security could be promoted through better coordinating activities at the nuclear security centers of excellence that were established during the Nuclear Security Summit process in Japan, South Korea, and China.

Nuclear issues play a large role in the US-ROK alliance, and the US team demonstrated this during the table-top exercise by steadfastly supporting its South Korean ally during the nuclear accident caused by the North Korean cyber-attack. The Nuclear Security Summit process, the new 123 Agreement, and NAPCI are all positive steps to encourage regular dialogue on these issues, but all actors must work to maintain and strengthen cooperation.

Discussion questions

1. Are existing bilateral cooperation mechanisms sufficient to address nuclear security issues, including both physical and cyber security?
2. How can the United States best support South Korea in the event of a nuclear accident at a South Korean nuclear facility? In addition to support from the Nuclear Regulatory Commission (NRC) and other civilian agencies, what should US military forces do?
3. What role do nonproliferation export controls have to play in the region? Can they be effective if only certain countries practice them but not others?

Research questions

1. What concrete steps can the nuclear security community take to integrate technical and policy developments from the information security community?
2. What entities might target South Korean or US nuclear facilities, and what are the current or projected future capabilities and intentions of those entities? How can US and ROK authorities improve cyber security at nuclear facilities?
3. Can lessons from the US and Japanese response to the March 11, 2011 Fukushima Daiichi nuclear accident be applied to the US-ROK alliance?

Studies (Dec. 15, 2014), http://www.theasanforum.org/the-northeast-asia-peace-and-cooperation-initiative-napci-a-vision-toward-sustainable-peace-and-cooperation-in-northeast-asia/.

Further reading

- Toby Dalton, "Nuclear Governance: South Korea's Efforts to Strengthen Regimes and Frameworks for the Safe and Secure Use of Nuclear Energy," *Middle-Power Korea: Contributions to the Global Agenda*, Council on Foreign Relations, June 2015. http://i.cfr.org/content/publications/attachments/Middle-Power%20Korea_Dalton.pdf.
- Park Younwon, "Securing Nuclear Safety in Northeast Asia: ROK Proposal on Northeast Asia Nuclear Safety Mechanism," *NAPSNet Special Reports*, Nautilus Institute, 4 May 2015. http://nautilus.org/napsnet/napsnet-special-reports/securing-nuclear-safety-in-northeast-asia-rok-proposal-on-northeast-asia-nuclear-safety-mechanism/.
- Caroline Baylon, Roger Brunt, and David Livingstone, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, Chatham House Report, September 2015. https://www.chathamhouse.org/publication/cyber-security-civil-nuclear-facilities-understanding-risks
- "Cyber Survival," *MIT Technology Review*, Business Report, January 2016. https://www.technologyreview.com/g/cyber-survival/?sort=recent
- Stephanie Lieggi, Robert Shaw, and Masako Toki, "Taking Control: Stopping North Korean WMD-related Procurement," Bulletin of the Atomic Scientists, Feature, September/October 2010. http://csis.org/files/attachments/130828_Stopping%20N.%20Korea%20WMD%20Procurement.pdf

China's role in Northeast Asia

By Youngcheng Li, Guanpei Ming, Takehiro Masutomo,
Maile Z. Plan, and Yizhe Daniel Xie

The rise of China is one of the most important events shaping Northeast Asia. China surpassed Japan as the largest economy in the region in 2010 and its economic weight is exceeded only by that of the United States. This dynamism propelled double-digit growth in military spending, the most investment in clean and renewable energy, and triggered assertiveness in territorial disputes with Japan, Vietnam, and the Philippines. Under Xi Jinping's leadership, Beijing is more confident and more willing to participate in world affairs than before. With increasing capability and willingness, China is poised to contribute greatly to economic development and peace-building in Northeast Asia.

The 2015 Young Leaders Security Seminar in Seoul tackled several topics that addressed China's role in Northeast Asia. These included, but are not limited to, China's role in solving territorial disputes, energy security, regional peacebuilding, and regional economic cooperation. China can play an active and constructive role in the region; the four sections that follow address each topic.

China's role in Northeast Asian territorial disputes

Northeast Asia is a diverse region made up of many different cultures, social and political systems, development levels, ideologies, and religious beliefs. Security cooperation requires greater understanding and flexibility as well as new approaches to institution-building. A mature and systematic East Asian security cooperation mechanism will bolster development in this area.

Northeast Asia is "characterized by 'strategic diversity' where a number of unresolved territorial disputes threaten to undermine the very source of regional prosperity: maritime trade."[1] China has multiple overlapping territorial claims with its neighbors in the East and South China Seas: Beijing and Tokyo both claim the Diaoyu/Senkaku Islands, and China and five other Southeast Asian countries struggle over ownership of South China Sea islands. The disputes not only involve economic factors but also have strategic significance. "Control of the surrounding waters enhances the strategic position of the state in possession of the islands and may contribute to establishing naval primacy."[2] Tensions are also rising in Northeast Asia. "Rivalries and difficult relations are nothing new in a region marked by competing nationalisms,

[1] "Territorial Disputes in Northeast Asia," *China Policy Institute Blog*, accessed Dec. 29, 2015, http://blogs.nottingham.ac.uk/chinapolicyinstitute/2014/10/13/territorial-disputes-in-northeast-asia/.
[2] Elena Atanassova-Cornelis, Ramon Pacheco, and Eva Pejsova, "Pride and Prejudice: Maritime Disputes in Northeast Asia," *ISSUE* 23 (April 2015): 8.

historical antagonism, a legacy of past invasions and occupations, and territorial disputes."[3]

The islands called Diaoyu by China, Senkaku by Japan, could lead to conflict between China and Japan. These are uninhabited islands and rocks located east of China, northeast of Taiwan, and west of Okinawa. Japan controls these islands but China and Taiwan both claim sovereignty over them. China thinks the Diaoyu and its affiliated islands "are an inseparable part of the Chinese territory. Diaoyu Dao is China's inherent territory in all historical, geographical and legal terms, and China enjoys indisputable sovereignty over Diaoyu Dao."[4] China asserts that the Treaty of Shimonoseki ceded the islands to Japan as part of Taiwan and that they were returned to China under the provisions of World War II, as laid out in the 1943 Cairo Declaration, the 1945 Potsdam Declaration, and the 1951 San Francisco Peace Treaty.

Japan counters that "there is no doubt that the Senkaku Islands are clearly an inherent part of the territory of Japan, in light of historical facts and based upon international law. Indeed, the Senkaku Islands are under the valid control of Japan. There exists no issue of territorial sovereignty to be resolved concerning the Senkaku Islands."[5] Japan also maintains that the "Treaty of Shimonoseki was not applicable to the Senkaku/Diaoyu, since Japan had incorporated the islands into its territory as *terra nullius* (no man's land) in January 1895, i.e., before the end of the war, and after conducting surveys confirming that no government control over these territories existed."[6] Given the tense bilateral relations between China and Japan, it is unlikely that this dispute will be resolved soon. Beijing's declaration establishing an ADIZ in the East China Sea in 2013 increased concern in Japan.

These disputes cannot be understood without considering the conviction of many in Northeast Asia that "once it becomes strong, China will attempt to reestablish its historical role as the center of Asian culture and politics."[7] Countries with territorial disputes with China are worried that Beijing will be more assertive in its foreign policies. China has assured its neighbors that its economic rise is not a threat to peace and security. Former President Hu Jintao, for example, asserted that China will try to settle all territorial disputes with its neighbors by peaceful means and stated that "China will continue its practice of settling all disputes with its neighbors over territory, territorial

[3] Evans J. R. Revere, "Whither Northeast Asia? Managing Tensions and Avoiding Conflict in a Troubled Region," *The Brookings Institution*, 1, accessed Dec. 30, 2015, http://www.brookings.edu/research/opinions/2013/12/02-managing-tensions-northeast-asia-revere.
[4] "Diaoyu Dao, an Inherent Territory of China," accessed Dec. 31, 2015, http://english.cntv.cn/20120925/106168.shtml.
[5] "Senkaku Islands," *Ministry of Foreign Affairs of Japan*, accessed Dec. 31, 2015, /region/asia-paci/senkaku/index.html.
[6] Atanassova-Cornelis, Pacheco, and Pejsova, "Pride and Prejudice," 9.
[7] Harry Harding, *China and Northeast Asia: The Political Dimension* (University Press of America, 1988), 47.

waters and marine rights and interests through friendly negotiation, and play a constructive role in the solution of regional hotspot issues."[8]

Territorial disputes pose one of the biggest challenges in Northeast Asia. All countries should make greater efforts to solve these disputes. As Northeast Asian countries have been slow to develop a regional security mechanism and institution, China should lead in establishing confidence and trust among countries. While the US is geographically distant from Northeast Asia, it has a strong presence in the region, especially through its alliances with Japan and Korea. "The nature and form of Sino-US relations have become critical variables for Northeast Asian security."[9] It would be a mistake to conclude that the impact of these territorial disputes is restricted to Northeast Asia, and it is equally important to emphasize the role of the US in these disputes. But as China becomes a hub for flows of global capital, it will likely rely on soft power and cultural governance rather than overt military aggression to support its territorial claims.

China's role in Northeast Asia: energy security

Energy security is a great concern in Northeast Asia, especially since China, Japan, and South Korea all import large quantities of petroleum and liquefied natural gas. Each country is seeking ways to decrease its dependence on imported fuel, such as using nuclear energy and developing clean energy sources for power and electricity. China is leading the world in clean energy investments, and its economy, financial prowess, and growing geopolitical clout provide it with an opportunity to lead the region in energy security.

There are several ways to do this. First, China can play a role in establishing nuclear energy security norms. As demonstrated in the Seoul TTX, cyber-attacks on South Korean's nuclear infrastructure led disagreement on whether it constituted an armed attack and the appropriate way to respond. The US and South Korean teams agreed that cyber-attacks on South Korea's nuclear power plants led to a meltdown that could have resulted in nuclear fallout and civilian casualties, and was equivalent to a kinetic (nuclear) attack on its soil. This type of unprecedented attack therefore warranted a kinetic response on the attacker. China did not think such an attack warranted a kinetic response. Although the International Convention for the Suppression of Terrorist Bombings explicitly states that cyberattacks on critical infrastructure are illegal,[10] there is no precedent for an appropriate response. For example, the recent cyber-attack on Ukraine's electric grid, allegedly by Russia, is the first of its kind and the response to

[8] "Settlement of Territorial Disputes through Peaceful Means CHINA US Focus | CHINA US Focus," accessed Dec. 31, 2015, http://www.chinausfocus.com/peace-security/settlement-of-territorial-disputes-through-peaceful-means/.
[9] Chen Jimin, "Solving the Northeast Asia Security Dilemma," *The Diplomat*, accessed Dec. 30, 2015, http://thediplomat.com/2013/05/solving-the-northeast-asia-security-dilemma/.
[10] David Fidler, "Cyber Norm Development and the Protection of Critical Infrastructure," *Council on Foreign Relations* (July 23, 2015), http://blogs.cfr.org/cyber/2015/07/23/cyber-norm-development-and-the-protection-of-critical-infrastructure/, accessed December 2015.

such an attack would be unprecedented and uncertain.[11] Therefore, defining rules and regulations on responses would be an important step toward normalizing how countries view cyber-attacks on critical infrastructure, including nuclear facilities. China, Japan, South Korea, and even North Korea would benefit from established and publicly declared norms regarding cyber-attacks to decrease miscalculation. Any country violating these norms or international laws would understand the consequences of undertaking such actions.

Second, China can facilitate advances in solar, wind, biofuel, or water-derived energy sources. China, Japan, and South Korea are all pursuing clean energy initiatives. China has significant investments in hydropower and is developing electric and hybrid car technologies.[12] Japan is investing heavily in biofuels for its commercial aviation industry,[13] especially as the country is expected to host the 2020 Olympics.[14] South Korea is expanding its solar industry market to meet its pledge to cut greenhouse gas emissions by 30 percent by 2030.[15] While each country has its own plans, it may be more efficient if the region worked together on clean energy goals. Each country can play a role in creating a regional green energy economy with its many renewable projects. China can play a bigger role because of its vast capital and willingness to spend on clean energy initiatives. This type of collaboration and specialization can enable financing, construction, exports and imports, as well as developing safety standards for the region and the industry in general.

Third, China, Japan, and South Korea have been moving away from coal and toward liquefied natural gas (LNG), which produces only half the greenhouse gas emissions and deadly particulates as coal. Many view LNG as a stepping stone or bridge away from coal and toward cleaner, renewable energy. As shipments of LNG increase in Northeast Asia, the region will need to develop more infrastructure projects and improve security in ports and at sea. China can help finance more LNG infrastructure and establish security protocols for LNG shipments along with Japan and South Korea. Although the Society of International Gas Carrier and Terminal Operators (SIGTTO) and the Society for Gas as a Marine Fuel (SGMF) published the "Standards and Guidelines

[11] Eric Geller, "Ukraine says Russia launched a cyberattack that hit its electrical grid," *The Daily Dot* (Dec. 31, 2015), http://www.dailydot.com/politics/ukraine-russia-energy-grid-cyberattack-investigation/, accessed December 2015.
[12] "China sees a competitive edge in green cars," *Business Insider* (Sept. 11, 2015), http://www.businessinsider.com/r-from-big-to-strong-china-sees-competitive-edge-in-green-cars-2015-9, accessed December 2015.
[13] "ANA to use Euglena jet fuel made from green algae at Japan plant," *The Japan Times* (Dec. 1, 2015), http://www.japantimes.co.jp/news/2015/12/01/business/corporate-business/ana-use-euglena-jet-fuel-made-green-algae-japan-plant/#.VoWZ4RUrKUl, accessed December 2015.
[14] "Boeing, Japanese Aviation Industry Unveil Biofuel 'Roadmap' to 2020 Olympics," *PR Newswire* (July 8, 2015), http://www.prnewswire.com/news-releases/boeing-japanese-aviation-industry-unveil-biofuel-roadmap-to-2020-olympics-300110743.html, accessed December 2015.
[15] Ian Clover, "South Korea announces $1.94bn clean energy plan," *PV Magazine* (July 18, 2014), http://www.pv-magazine.com/news/details/beitrag/south-korea-announces-194bn-clean-energy-plan_100015778/#axzz3vvxQCWyx, accessed December 2015.

for Natural Gas Fueled Ship Projects",[16] no international law sets standards on LNG ships or ports. Industry standards and strict compliance have created a strong regulatory safety framework that ensures that LNG facilities are in a safe operational environment,[17] but China can push a regional or international standard for all LNG shipments into the region to create still safer conditions.

Energy security is key to Northeast Asia's future and China should push regional collaboration to expand and improve clean energy infrastructure.

China's role in economic cooperation

The table-top exercise highlighted the growing number of visitors between China, Japan, and ROK, and the plenary touched on the importance of economic interdependence among the three countries in a security crisis. There is more room for economic cooperation among these Northeast Asian countries in trade and finance.

Trade within Northeast Asia is growing.[18] The total amount of trade among China, Japan, and South Korea amounted to more than $600 billion in 2014, more than triple the amount in 2000.[19] Among these three bilateral trade relationships, the trade volume between Japan and China is greatest, although the trade growth rate has been declining. Trade between China and Korea has recently gained momentum. Experts foresee that the volume and amount of China-Korea trade will soon surpass that of China-Japan trade.

Rivalry between China and Japan often limits regional economic cooperation, however. China and Japan agreed on financial cooperation in 2011, including promotion of the direct use of their respective currencies in bilateral trade, but cooperation halted due to the Senkaku/Diaoyu dispute. Meaningful economic partnership between China and Japan is not foreseeable in the short term. China appears to sense it can achieve greater influence over the region as its economy grows. Seeking a win-win situation with Japan may better serve Chinese interests and help it become 'the' regional leader.

China, Japan, and South Korea along with ASEAN countries have established the Asian Bond Fund (ABF) and initiated the Asian Bond Market Initiative (ABMI). These initiatives reaped an early harvest as bond markets in the region grew steadily. Moreover, three Northeast Asian countries led the creation of the Chiang Mai Initiative and regional surveillance unit, the AMRO. The former evolved into Chiang Mai Initiative

[16] "Standards and Guidelines for Natural Gas Fuelled Ship Projects," LNG Ship Fuel Safety Advisory Group, http://www.sgmf.info/media/5637/standards-guidelines-natural-gas-fuelled-v5k1.pdf, accessed December 2015.
[17] "LNG & Safety," International Group of Liquefied Natural Gas Importers, http://www.giignl.org/about-lng/lng-safety, accessed December 2015.
[18] "Country Report," *Ministry of Commerce of the People's Republic of China*. http://countryreport.mofcom.gov.cn/record/view110209.asp?news_id=43691, http://countryreport.mofcom.gov.cn/record/view110209.asp?news_id=42573, accessed January 2016
[19] "Statistics," *Japan Customs*. http://www.customs.go.jp/toukei/suii/html/y5.pdf, http://www.customs.go.jp/toukei/suii/html/y4.pdf, accessed January 2016

Multilateralisation (CMIM), but the mechanism has never been activated and the latter is understaffed.

In 2010, the year China's economy surpassed that of Japan, the two countries competed for the top position in the AMRO. Both China and Japan have signed currency swap agreements with other Asian countries, suggesting the two regional powers favor a unilateral approach, rather than strengthening multilateral institutions. It will be important to see who will replace AMRO's current director Nemoto Yoichi because it will hint at the future of regional economic cooperation.

Further cementing this financial rivalry, China has begun promoting its own initiatives. Previously, the Asian Development Bank (ADB) was the only multilateral development bank in the region. The Japan-initiated ADB was established in 1966 and its nine heads have all been former high-ranking Japanese officials. In 2013, Chinese President Xi Jinping announced the establishment of the Asian Infrastructure Investment Bank (AIIB). The AIIB has attracted 57 founding members including countries such as South Korea and Australia, and 20 more members are expected to join.[20] Japan has not joined, despite China's vigorous invitation[21] because the Japanese government regards it as a challenge to the ADB and is skeptical about the transparency of the AIIB. Prime Minister Abe announced a $110 billion development initiative for Asia, which was widely regarded as a form of competition with the AIIB. South Korea, on the other hand, fully supports the AIIB and reportedly will assist in the issuance of the new bank's bonds.

Given its status as the region's largest exporter, China has become central in drawing the blueprint for regional economic integration. China led "ASEAN+1" Free Trade Agreements (FTAs) by signing the China-ASEAN FTA in 2002. Recently, China has pursued more ambitious deals such as China-Australia and China-South Korea FTAs, which came into force in December 2015. According to the ADB, China has signed or launched negotiations on 22 FTAs. Although Japan's diplomatic ties with China and South Korea soured in recent years, at a trilateral Summit in November 2015, the three leaders vowed to push trilateral FTA negotiations. Separately, China and ASEAN agreed to upgrade their FTA in the same month.

China's attitude toward the Trans-Pacific Partnership (TPP) remains ambiguous.[22] Reformers in China favor accession to TPP to promote economic reform at home.[23]

---

[20] "Up to 20 countries Waiting to Join China-Led AIIB, President-Designate Says," *Wall Street Journal*, Sept. 19 2015. http://www.wsj.com/articles/up-to-20-countries-waiting-to-join-china-led-aiib-president-designate-says-1442666572, accessed January 2016.

[21] "China offered Japan No.2 post at new bank," *Nikkei Asian Review*, April 15 2015. http://asia.nikkei.com/Politics-Economy/International-Relations/China-offered-Japan-No.-2-post-at-new-bank, accessed January 2016.

[22] "MOFCOM Spokesman comments on the conclusion of TPP negotiations," *Ministry of Commerce of the People's Republic of China*, Oct. 8, 2015. http://english.mofcom.gov.cn/article/newsrelease/policyreleasing/201510/20151001132863.shtml, accessed January 2016.

[23] "China Has No Reason to Fear the TPP," *Caixin Online*, Oct. 14 2015. http://english.caixin.com/2015-10-14/100862832.html, accessed January 2016.

Observers believe China has set up four Free Trade Zones (Shanghai, Tianjin, Fujian, and Guangdong) to prepare for possible accession to the TPP. But Beijing has also promoted the Regional Comprehensive Economic Partnership (RCEP). Furthermore, Xi Jinping called for accelerating negotiations for the China-backed Free Trade Area of the Asia Pacific (FTAAP) during the 2014 APEC meeting he hosted in Beijing.

To lead the region, China must implement difficult economic reforms, in particular reforms of State-Owned Enterprises (SOEs), if it wants to join TPP. Because a prerequisite for RCEP and FTAAP is conclusion of the China-Japan-South Korea FTA negotiations, China has to coordinate with Japan.

Taiwan poses particular problems for regional economic cooperation.[24] Taiwan's President-elect Tsai Ing-wen announced her willingness to join TPP in the next round. Although Taiwan is an important part of the supply chain in Northeast Asia, it is often left out of Asia's economic integration. Because of the "China factor," Taiwan has concluded only 8 FTAs and did not take part in large-scale FTA negotiations such as TPP or RCEP. As is the case of WTO accession, if China joins or considers joining TPP, Taiwan's likelihood of the accession would be higher. Therefore, how China deals with Taiwan is an interesting test for the Northeast Asian economic integration.

China is also promoting internationalization of the renminbi. According to SWIFT, the RMB overtook the Japanese yen to claim fourth place among the world's payment currencies.[25] The IMF also decided to include the renminbi in its Special Drawing Rights (SDR) in 2015. In addition to Hong Kong, financial centers such as Singapore, London, Luxembourg are vying to become the main RMB offshore market. Japanese Finance Minister Aso Taro recently said that Tokyo would like to build a renminbi clearing bank in Tokyo.[26] Japan missed the opportunity to internationalize the yen in the 1980s and 1990s and seeks more international use of yen today as intra-regional trade grows. Thus, there might be a chance for a win-win situation for China and Japan by promoting internationalization of both the renminbi and yen.

China's leading role in East Asian peace efforts

China is one of the leading forces pushing for a regional security architecture in East Asia. President Xi Jinping's regional peace strategy prioritizes two pillars: a "New Type of Major Power Relations" between China and the US, and the pursuit of regional peace through development. The China-US New Type of Major Power Relationship focuses first and foremost on peace, defined as "no conflict, no confrontation," which means no war, and no cold war. The South China Sea territorial disputes are the most challenging issues. China sees the China-US strategic relationship as the anchor of

[24] "China Factor Awaits Next Taiwanese President on FTAs," *Newsweek Japan*, Dec. 24, 2015. http://www.newsweekjapan.jp/stories/world/2015/12/ftatpp.php, accessed January 2016.
[25] "Renminbi overtakes Japanese yen as global payments currency," *Financial Times*, Oct. 6 2015. http://www.ft.com/intl/cms/s/0/bb54b4f0-6bf2-11e5-aca9-d87542bf8673.html#axzz3vcT7EBpN
[26] "Finance Minister Aso calls for setting up of RMB clearing banks in Japan," *Jiji.Press*, Oct. 10 2015. http://www.jiji.com/jc/zc?k=201510/2015101000087, accessed January 2016.

regional peace and has been pushing and pulling China-US relations in a peaceful direction, despite perceived provocations.

Peace through development is an important concept in China and Chinese leaders invariably put peace and development together, stressing their separate significance and their effects on each other. President Xi sees development as "the key" to global governance. FTAs with countries like ROK and Australia, and RCEP are efforts to promote peace through development. The "one road and one belt" initiatives and the AIIB are China-led initiatives that aim at helping countries in East Asia and beyond share benefits and facilitate regional peace.

Unlike the United States, which plays a role as pacifier through offshore balancing, China has been implementing two missions to ensure peace in East Asia is maintained: managing China-US relations by a "New Type of Major Power Relationship" and helping regional countries realize economic growth as an alternative to political violence. China's peace pillars are equal parts idealistic and realistic: idealistic because diplomatic compromise is very hard and realistic because peace is the best and most reasonable approach to interstate disputes.

Conclusion

Northeast Asia faces many challenges and China can play an active and constructive role by leveraging its economic power and political influence. In territorial disputes, China can play a lead role in confidence and trust building; in energy security, it should promote regional collaboration to expand and improve clean energy infrastructure; in peace building, Beijing is introducing the "New Type of Major Power Relationship" and helping regional countries to realize economic growth; in economic cooperation, China is designing and constructing regional financial and economic frameworks through trade deals (like RCEP), currency swaps, the Asian Bond Initiative, RMB internationalization, and the AIIB.

Discussion questions

1. What should China do after North Korea's fourth nuclear test in January 2016 and is there any way China can persuade North Korea to return to the discussion table?
2. Do we need international laws and standards for LNG shipments if there is an industry standard?
3. How should China deal with Taiwan's FTA policy?
4. How can China avoid repeating the failure of the internationalization of the Japanese yen? Is cooperation possible between Japan and China to promote the use of local currencies?

Suggestions for future research

1. What impact will China's economic slowdown have on its foreign policy and the security and economy of Northeast Asia?
2. How do China and Japan view each other's intentions in the region? Are they doomed to be rivals?
3. How should China and Japan avoid future conflict?
4. How can Northeast Asian countries establish a security cooperation mechanism and what should the US role be?

Suggested readings

1. "Currency and Contest in East Asia: The Great Power Politics of Financial Regionalism" by William W. Grimes
2. "Taiwan and Regional Trade Organizations: An Urgent Need for Fresh Ideas" by Kevin G. Nealer and Margaux Fimbres
3. "Asian Infrastructure Investment Bank in the Evolving International Financial Order" by Masahiro Kawai. http://spfusa.org/wp-content/uploads/2015/07/AIIB-Report_4web.pdf
4. "China Has No Reason to Fear the TPP." http://english.caixin.com/2015-10-14/100862832.html

APPENDIX A

CHOI SHINWON, CHAIRMAN OF SKC
PRESENTS THE
NORTHEAST ASIA REGIONAL YOUNG LEADERS SECURITY SEMINAR
SHERATON GRANDE WALKERHILL, SEOUL
NOVEMBER 8- 11, 2015

PARTICIPANT BIOGRAPHIES

Mr. Seukhoon Paul CHOI (ROK) is a Strategist for the United Nations Command/ROK-US Combined Forces Command/US Forces Korea. In this capacity, he serves as an advisor to Senior Leaders on the regional strategic environment and alliance management. Previously, he served as a Research Associate in the program on US-Korea Policy at the Council on Foreign Relations. He was also a non-resident James A. Kelly fellow at the Pacific Forum CSIS; a consultant to the Center for US-Korea Policy at The Asia Foundation; visiting scholar at Fudan University in China; a lecturer at the Korea Military Academy in South Korea, and an officer in the ROK Army. He has conducted research on base politics and the US-ROK alliance at the East-West Center and for the Reischauer Center at SAIS. He has an MA in International Cooperation from Seoul National University GSIS, and a BA in Philosophy, Politics & Economics from the University of Pennsylvania.

Mr. Yu HARADA (JPN) is a Research Fellow, Policy Studies Department at the National Institute for Defense Studies (NIDS), Japan Ministry of Defense. His research focuses on maritime security; especially South China Sea related issues, and cyber security. He earned an MA in International Relations from Graduate School of Global Studies, Sophia University, and a BA in International Relations from Sophia University. His recent publications in English include "Failure of Japan's Foreign Policy to Secure the Sea Lines of Communication: Disputes over the Straits of Malacca and Singapore in the 1970s" (journal article, 2013) and "Dispute over Governance of Cyberspace" (NIDS Commentary, 2015).

Ms. Shino HATERUMA (JPN) is a PhD student in international studies at Waseda University's Graduate School of Asia-Pacific Studies. Her current research focuses on conditions of the closure of US military bases overseas and her research interests are in regional security of the Asia-Pacific. She previously served as a researcher of the Regional Security Policy Division, in the Executive Office of the Governor, for the Okinawa Prefectural Government from July 2013 to March 2015. During that period, she had researched US policy regarding its overseas bases as well as security issues in the Asia-Pacific region. Before serving in Okinawa, Shino worked as a researcher for the Research Institute for Peace and Security, a Tokyo-based think tank.

Mr. Yoshifumi IDE (JPN) is a Master's student at the Graduate School of Asia-Pacific Studies, Waseda University doing research in international security that focuses on psychological explanations of decision-making in foreign policy in Northeast Asia. Previously, he graduated from Faculty of Law, Seikei University in March 2014, having spent a semester at the Faculty of Social Science, University of California, San Diego in 2012. He is politically active in Japan's Liberal Domestic Party chapter in Kanagawa Prefecture, where he is involved in LDP policies such as tax reform, revision of the constitution, and others as a political intern. Yoshifumi has also travelled widely in Asia, Europe, and Northeast America, visiting more than 20 countries.

PARTICIPANT BIOGRAPHIES

Mr. Akira IGATA (JPN) is an Aoi Global Scholar at Cambridge University, an SPF Resident Fellow at Pacific Forum CSIS, and a PhD student at the Department of Law, Keio University. He received his undergraduate training at Georgetown University (one-year exchange program, Heiwa Nakajima Foundation scholar) and International Christian University (Chris-Wada scholar). He received his MA in political science (international relations) from Columbia University (Japanese government fellowship scholar). He was a recipient of the security studies fellowship from the Research Institute for Peace and Security (2010-2012) and has been involved in several projects of the Rebuild Japan Initiative Foundation. He notably contributed, as a researcher, to The Fukushima Daiichi Nuclear Power Station Disaster: Investigating the Myth and Reality (Routledge, 2014) and wrote the chapter entitled, "The Gulf War and Japan's National Security Identity" (forthcoming, co-authored with Michael J. Green), for a book on Japan's "lost decades."

Ms. Jenny JUN (USA) is a co-author of the forthcoming Center for Strategic and International Studies (CSIS) report titled *North Korea's Cyber Operations: Strategy and Responses*. Her current research interests include cyber warfare, asymmetric warfare, and security issues in East Asia. She is currently researching the role of cyber warfare in military decision cycles through a summer research grant with Georgetown's Security Studies Program (SSP). Prior to her graduate studies, she was a cybersecurity consultant at Delta Risk LLC, where she focused on international cybersecurity policy and information sharing mechanisms. Jenny is a MA candidate at Georgetown University's Security Studies Program. She graduated magna cum laude from Georgetown University School of Foreign Service in International Politics with a certificate in Asian Studies, and has published articles at *CSIS Korea Chair Platform*, *38North*, and *Yonsei Journal of International Studies*. She currently serves as the President of Sejong Society, a young professional organization focused on Korea studies affiliated with the US-Korea Institute at SAIS.

Dr. Xiao KANG (PRC) is an Associate Professor at the School of International Relations and Diplomacy, Beijing Foreign Studies University. His research interests are global governance and China's diplomacy, geopolitical economy and regional governance, comparative politics and comparative political economy. His most recent publication is *"Global Governance about Climate Change and China's Economic Transformation: Perspective of Internalization of International Norms,* World Book Publishing Company, 2014".

PARTICIPANT BIOGRAPHIES

Mr. Gibum KIM (KOR) is a program officer in the Office of the Vice President for Research and the Center for Foreign Policy and National Security at the Asan Institute for Policy Studies. Prior to joining the Asan Institute, he was an intern researcher at the International Policy Studies Institute Korea. He has also worked as a professional researcher at the Research Institute for Language and Information at Korea University. He earned both an MA and a BA in Political Science at the College of Political Science and Economics, Korea University. His research interests include East Asian regional security, multilateral security cooperation, weak states, and human security.

Dr. Jina KIM (ROK) is an Associate Research Fellow at the Korea Institute for Defense Analyses and holds a PhD in International Relations from the Fletcher School of Law and Diplomacy at Tufts University. Her research areas include US-North Korea relations, nuclear nonproliferation, and Northeast Asia security. She provides advice to the ROK Ministry of Defense, Joint Chiefs of Staff, and Ministry of Foreign Affairs on security environment and inter-Korean relations. She taught seminars on humanitarian intervention at Yonsei University and nuclear nonproliferation at Tufts University. Previously, she worked for the Korean National Assembly, UNESCO, and BBC. Her recent publication includes "UN Sanctions as an Instrument of Coercive Diplomacy against North Korea," in The Korean Journal of Defense Analysis (2014), The North Korean Nuclear Weapons Crisis (2014), "US Rebalancing toward Asia Revisited: Implication to US-China Competition," in Maritime Security and Governance (2014), "Sources and Objectives of DPRK Foreign Policy," in The North Korea Crisis and Regional Responses (2014), The North Korean Military Secret Report (co-authored, 2013), "An Analysis of Political Instability in the DPRK," in The Korean Journal of Defense Analysis (2013) and many others.

Ms. Nahee KIM (ROK) is a recent Master's degree graduate from the Graduate School of International Studies, Yonsei University, Korea, where she focused on development cooperation and trade & economic development. She was also a Research Assistant in the field of international security. Previously, she interned at Asia-Pacific Centre of Education for International Understanding under the auspices of United Nations Educational, Scientific and Cultural Organization (UNESCO) and Korea Trade-Investment Promotion Agency (KOTRA). She has an interest in developing cooperative relations in the Asia-Pacific region and political economy dynamics of Northeast Asia. She received her BA in Human Ecology from Seoul National University, Korea.

PARTICIPANT BIOGRAPHIES

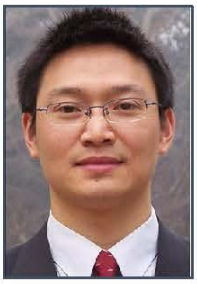
Mr. Sung Hyo KIM (ROK) Sung Hyo Kim is an intern at Liberty in North Korea and Gonggam. He has been assisting the operation of various empowerment programs at Liberty in North Korea for North Korean refugees in South Korea, and has conducted research on public interest issues and human rights issues at Gonggam. Previously, Sung Hyo served as an Air Force Interpreting Officer (1st Lieutenant) at the Republic of Korea Ministry of National Defense, Joint Chiefs of Staff, and Air Force Operations Command for three years. During his military service, Sung Hyo worked with various senior military and government leaders, as well as scholars from both Korea and the United States on bilateral security initiatives, including issues related to the transition of wartime operational control between the ROK and US armed forces, UN Command, combined military exercises, and regional cooperation for North Korean issues. Sung Hyo graduated from Carleton College with a BA in Cinema and Media Studies. He was born and raised in Gwangju, South Korea. He is fluent in Korean, English, and is conversational in Japanese.

Mr. Amane KOBAYASHI (JPN) is a PhD candidate at the Graduate School of Media and Governance, Keio University where he is also a Research Associate at the Global Environmental System Leaders Program. He received his BA in Policy Management (2009) and his MA in Media and Governance (2011) at Keio University. Previously, he was a Research Fellow at University of Nairobi, Kenya (December 2014 to April 2015). His current research focuses on the impact of the climate change on the international security, especially in the Middle Eastern and African countries. He is also interested in the security cooperation in Northeast Asia, and the role of regional collaboration, particularly towards the disaster risk reduction, regional energy security and peace operations. He has previously researched on the politics and economy of the Middle Eastern and North African countries, and served as an Advisory Expert for Japan International Cooperation Agency for the project on reconstruction and development of the industrial sector in post conflict Libya during 2013 to 2014.

Ms. Jea Hyun (Diana) LEE (ROK) is a recent graduate from the Middlebury Institute of International Studies at Monterey with Master's Degree in Nonproliferation and Terrorism Studies, and regional focus on the Northeast Asia, and the Korean Peninsula. At the institute, Diana studied strategic trade controls of nuclear weapons and weapons of mass destruction, drones policy, and forecasting proliferation risks in Southeast Asia. She was a graduate research assistant at the James Martin Center for Nonproliferation Studies, and co-authored on an article entitled, "Tracking Growth in Dual Use Commodities in Southeast Asia". Currently, Diana serves as an intern at Women In Trade-Northern California (WIT-NC), and as a member of the Young Leaders Program at Pacific Forum CSIS.

PARTICIPANT BIOGRAPHIES

Mr. Meng LI (PRC) is a Lecturer at Beijing Foreign Studies University (BFSU). He is in a joint PhD training at the graduate school of Chinese Academy of Social Science (CASS) and Law School of Tohoku University, Japan where he is an Assistant Researcher of Research Center for Gender Equality and Multicultural Conviviality. His research focuses on regional governance and decentralization. He has published papers on this topic and presented his research at international meetings. He was awarded the "Academic Newcomers Award" from Chinese Ministry of Education in 2013. Presently, he is leading a research program named "Research of decentralization and regional governance in Policy overlapping area."



Dr. Yongcheng LI (PRC) is an Associate Professor of International Relations at Beijing Foreign Studies University. He received his PhD in International Relations at Renmin University of China in 2005. He spent the 2010-11 academic year as a visiting scholar at the University of Chicago, under the sponsorship of Professor John Mearsheimer. He has written extensively about western IR theories and international security issues, and has published two books (in Chinese): *Myths of Hegemony* (2007, which won the 2nd class Prize of Beijing Awards for Distinguished Works of Philosophy and Social Sciences 2008), and *The Logic of Intention: US and China's Soft Security Environment* (2011). Currently, he is working on a book about China's international leadership in the perspective of peace and development strategy. He has also written dozens of articles that have appeared in Chinese academic journals like *Foreign Affairs Review*, *Journal of International Politics* and English Journal *International Journal of China Studies* (Malaysia).

Mr. Tatsuya Sakurai-Jyc LIU (USA) is an International Studies Ph.D. Candidate at Waseda University (Tokyo) as a Japanese-government fellowship scholar (MEXT). Tatsuya holds an MA in International Studies & Diplomacy from the School of Oriental and African Studies (SOAS), University of London, and a BA in International Affairs from the George Washington University. Hailing from the Pacific-island of Guam, he considers himself a Guamanian-at-heart who beyond his current research on the influence of the periphery in the Arctic and Asia-Pacific, esp. in-regards to roles, powers, and security affairs, was involved in the fashion-industry (P.R.), contemporary art consultancy, as well as formerly being an ethics-fellow with the Carnegie Council in New York City.

Mr. Takehiro MASUTOMO (JPN) is a Research Associate at the Centre on Asia and Globalisation, Lee Kuan Yew School of Public Policy, National University of Singapore. His research interests include competition between China and Japan in Southeast Asia, China-ASEAN relations and Japanese business presence in the region. He holds a Master's degree in Pacific International Affairs from IR/PS, UC San Diego (2010) and a Bachelor's degree in Sociology from Kwansei Gakuin University (2008). Takehiro was a Beijing-based researcher at Caixin Media (2010-2014) where he wrote analysis and in-depth news articles on economic and political affairs in Northeast Asia using Chinese language.

PARTICIPANT BIOGRAPHIES

Ms. Guanpei MING (PRC) is a PhD candidate in the Department of Political Science at the University of Hawaii at Manoa. She is a former Vasey Fellow at Pacific Forum CSIS. Guanpei received a BA in English and Economics from the Nanchang University of Aeronautics, an MA in International Politics from Peking University, and an MBA from the Seoul School of Integrated Science and Technologies. Her research has been funded by the Konosuke Matsushita Memorial Foundation, the University of Hawaii Foundation, and the Calebe Foundation. Guanpei is also a graduate of the Middlebury College Hebrew Language School, where she was a Kathryn Davis Fellow and learned to speak Hebrew.

Ms. Yoko MORI (JPN) is a Researcher at the Political Affairs Section of the Consulate-General of Japan in Honolulu. She holds a Master's Degree in Development and Security from the University of Bristol in United Kingdom. In graduate school, she conducted research about human security in order to find out how improving living standards could affect to promoting peace and stability. Her current interests are Japan-US security cooperation and security environment in East Asia, diplomatic and security policy of Japan and US military base in Okinawa.

Ms. Julia Jungmin OH (ROK) interned for one year in separate research roles for the Korea Economic Institute of America, in Washington DC, and the United Nations Office for Disarmament Affairs, in New York City. While completing her MA, she also contributed to the Centre for Science and Security Studies in London and NK News, a North Korea–focused news and information service. Julia recently worked for the Korean government in London as a Marketing Assistant Manager for the Korea Trade-Investment Promotion Agency. As a fellow, she joined the National Bureau of Asian Research in Washington DC. She holds a BA in Communications from the University of Delaware and an MA in International Relations from the Department of War Studies at the King's College London, where her thesis focused on the role of North Korea's nuclear weapons program in domestic propaganda. She has native fluency in English and Korean.

Ms. Maile PLAN (USA) is a Vasey Fellow, and is researching East Asian Security issues, including maritime security in Southeast Asia, Chinese foreign and military policy, nuclear deterrence, and the arms industry. She earned her MA in security studies from Georgetown University where she focused on Chinese security and East Asian regional issues (including study abroad in Taiwan). Previously, Maile worked as a legislative correspondent for US Senators Brian Schatz and Daniel K. Inouye in their Washington DC offices where she contributed to the foreign relations, defense, energy, and trade policy issue areas. She also studied abroad in Beijing while pursuing her Bachelor's degree in Asian Studies from Whitman College.

PARTICIPANT BIOGRAPHIES

Dr. James E. PLATTE (USA) is an Adjunct Lecturer in the Department of Political Science at Merrimack College and a non-resident Sasakawa Peace Foundation Fellow with Pacific Forum CSIS. He specializes in energy security, nuclear proliferation, and East Asian politics. He recently completed a visiting fellowship at the East-West Center in Washington DC, where his research focused on nuclear safety cooperation in Northeast Asia, and his SPF fellowship research analyses US-Japan civil nuclear cooperation. He received his PhD in International Relations from the Fletcher School of Law and Diplomacy. His dissertation was a comparative study of nuclear fuel cycle decision making in India, Japan, and South Korea, for which he conducted research in all three countries. He also studied Japanese nuclear policy as a 2012-13 Council on Foreign Relations International Affairs Fellow in Japan. Previously, he was a 2011-12 Stanton Nuclear Security Predoctoral Fellow at the Harvard Kennedy School and worked as a counterproliferation analyst for the US Department of Defense from 2008 to 2010. He holds an MA in Science, Technology and Public Policy from the Elliott School of International Affairs and an MS and BS in nuclear engineering from the University of Michigan.

Ms. Crystal PRYOR (USA) is a Political Science Ph.D. Candidate at the University of Washington, where she focuses on International Relations and Security Studies. Her dissertation is on strategic trade controls, for which she has conducted fieldwork in Japan, US, and Europe. Crystal holds a BA in International Relations from Brown University (2004), a Master's degree in Political Science from the University of Tokyo (2009), and a Master's Degree from the University of Washington (2012). Crystal has public sector experience working at the US Embassy in Tokyo (2008-2010).

Mr. Grant SCHNEIDER (USA) is a Foreign Affairs Officer in the Bureau of Arms Control, Verification and Compliance at the US Department of State. He is responsible for supporting the development and implementation of cyber stability and arctic policy. Previously, he led the Bureau's public affairs office where he led the Department's media efforts on the removal and destruction of the Syrian chemical weapons program, as well as on numerous nuclear, space and missile defense issues. He has also served as a speechwriter to Under Secretary Rose Gottemoeller. In 2014 he represented the US as a United Nations Disarmament Fellow. He was also a 2010 Nuclear Scholar at the Project on Nuclear Issues at the Center for Strategic and International Studies. He received his BSFS from Georgetown University and his MA from The George Washington University.

PARTICIPANT BIOGRAPHIES

Ms. Rie TAKEZAWA (JPN) is a Doctoral student at the Department of Law, Hitotsubashi University. Her areas of interests are international peace operations, including Japan's decision-making and policy regarding its contributions. Previously, Rie was a Research Associate of the Rebuild Japan Initiative Foundation, a Tokyo-based think-tank, where she contributed in analyzing various issues within Japan's crisis management systems. She was also a senior visiting researcher of The Keio Research Institute at SFC, researching the regional cooperation on disaster management and emergency response in the Asia-Pacific. She received her MA in media and governance, and BA in policy management from Keio University.

Dr. Tristan VOLPE (USA) is a Stanton Nuclear Security Fellow and an Associate in the Nuclear Policy Program at the Carnegie Endowment for International Peace, where his research focuses on the use of nuclear technology as a bargaining chip in world politics. Prior to working at Carnegie, Tristan was a Lawrence Scholar at Lawrence Livermore National Laboratory (LLNL). He remains a Visiting Scientist at LLNL's Center for Global Security Research. Tristan received a PhD in Political Science from the George Washington University and a BA in Political Science from the University of California, Los Angeles.

Mr. Shuo WANG (PRC) is a Master's student at Beijing Foreign Studies University with a major in diplomacy. His Bachelor's degree is from Beijing University of Technology in Business Japanese. Previously, he worked for the Ministry of Human Resources Social Security of the People's Republic of China.

Mr. Christopher WHYTE (USA) is a PhD candidate in the School of Policy, Government and International Affairs at George Mason University. His research focuses on the impact of emerging information & communications technologies across a range of international security issues, including information (cyber)security topics, transnational subversion, and crisis bargaining with a focus on East Asia. He has work published or forthcoming in International Studies Quarterly, Strategic Studies Quarterly, Comparative Strategy, International Relations, New Media & Society, Foreign Policy, The National Interest, and Diplomat. Previously, he has worked at several foreign policy think tanks and consultancies in research roles, including Center for a New American Security, Cato Institute, Center for the National Interest, and Wikistrat.

PARTICIPANT BIOGRAPHIES

Mr. Yizhe (Daniel) XIE (PRC) is a PhD candidate focusing on economic, political and security issues of Asia-Pacific with the Japanese government Monbukagakusho Young Asian Leaders Program at Graduate School of Asia Pacific Studies, Waseda University. Daniel's research interests include international trade and finance, the rise of Asia and China, Sino-Japan relations, Inter-Korea relations, China-Japan-Korea-US quadrilateral relations, and Asian integration and regionalism. He also has a broad work experience in business & finance and journalism across the region including Industrial Bank of Korea Securities, SK Corporation in Seoul, Goldman Sachs in Beijing and Sumitomo Corporation, Deloitte in Tokyo and, CNN, Voice of America and Televisión Española. And his articles on current affairs appeared in the newspaper, magazines and policy forum in China, Korea, Japan, Hong Kong, Vietnam and Australia. He obtained a double degree BA in International Studies and BA in Business Administration from Korea University, MA in International Relations (concentration on international economics) from Waseda University, and he speaks fluent Chinese, English and Korean, and is conversational in Japanese.

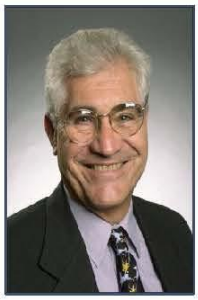
Ms. Wrenn YENNIE-LINDGREN (USA) is a Junior Research Fellow at the Norwegian Institute of International Affairs (NUPI). She specializes in the politics and foreign policy of Japan, regional diplomacy in East Asia, and traditional and non-traditional security issues in the Asia-Pacific region. She holds Master's degree in International Policy Studies from Monterey Institute of International Studies, and Asian and African Studies Master's degree from the University of Oslo. She was a visiting graduate student at Waseda University's Graduate School of Asia Pacific Studies (GSAPS) in Tokyo from 2009-2010. Previously, Wrenn held research positions at the Centre for Asian Security Studies at the Norwegian Institute of Defense Studies (IFS), United Nations University–Tokyo, the US Embassy–Tokyo and the James Martin Center for Nonproliferation Studies in Monterey, CA. She co-authored the 2013 article "Coming into the cold: Asia's Arctic Interests," Polar Geography 36(4), 253-270 with Elana Wilson Rowe and Per Erik Solli and independently authored "Energizing Russia's Pivot: Japan-Russia energy relations, post-Fukushima and post-Ukraine," NUPI Policy Brief, 28 January 2015.

Mr. Hongzhou ZHANG (PRC) is an Associate Research Fellow with the China Programme at the S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore. His main research interests include China and regional resources security, fishing policies and maritime security. He has contributed papers to peer reviewed journals such as the *Pacific Review, WIREs Water, the Copenhagen Journal of Asia Studies, Harvard Asia Quarterly, the ISPI Analysis* and *Southeast Asia Studies,* edited volumes, RSIS Working papers and Policy Reports. He has also contributed Op-Ed articles to major newspapers and magazines in the Asia-Pacific, such as the *YaleGlobal Online, the Diplomat, ChinaDialogue, the Global Times, Today, Lianhe Zaobao, the Nation, the Jakarta Post* and *Fair Observe*r. He has presented his work at events organized by *Cambridge University, Center for Naval Analyses (CNA), National University of Singapore, Copenhagen Business School, Tsinghua University, China's Academy of Social Sciences, University of Copenhagen , Foreign and Commonwealth Office of UK, Skoll Global Threats Fund, Sydney University, International Institute for Strategic Studies* and others.

PARTICIPANT BIOGRAPHIES

Dr. Tong ZHAO (PRC) is an Associate in Carnegie's Nuclear Policy Program based at the Carnegie–Tsinghua Center for Global Policy. His research focuses on strategic security issues, including nuclear arms control, nonproliferation, missile defense, strategic stability, and China's security and foreign policy. Previously, Tong was a Stanton Nuclear Security Fellow with the Managing the Atom Project and the International Security Program at the Belfer Center for Science and International Affairs at Harvard University. He has held a number of other positions, including as a non-resident WSD-Handa Fellow at Pacific Forum CSIS and working for the Office of Foreign Affairs of the People's Government of Beijing Municipality. He currently serves on the Executive Board of the International Student/Young Pugwash.

Staff and Observers



Mr. Ralph A. COSSA (USA) is President of the Pacific Forum CSIS. He is a member of the ASEAN Regional Forum Experts and Eminent Persons Group, as well as a founding member of the Steering Committee of the Council for Security Cooperation in the Asia Pacific (CSCAP). Mr. Cossa is a political/military affairs and national security specialist with more than 30 years of experience in formulating, articulating, and implementing US security policy in the Asia-Pacific and Near East–South Asia regions. He served in the US Air Force from 1966 to 1993, achieving the rank of colonel. He last served as Special Assistant to the Commander in Chief of the US Pacific Command. Previously, Mr. Cossa served as Deputy Director for Strategic Studies at the National Defense University's Institute for National Strategic Studies and earlier as a National Security Affairs fellow at the Hoover Institution at Stanford University. Mr. Cossa holds an MS in Strategic Studies from the Defense Intelligence College, an MBA from Pepperdine University, and a BA in International Relations from Syracuse University. He sits on the boards of the Center for Strategic and International Studies, the Pacific and Asian Affairs Council, and Worldwide Support for Development, and was awarded an honorary doctorate from the University of Cambodia.

Ms. Julia Cunico GARDNER (USA) is the Director of the Pacific Forum CSIS Young Leaders Program and was a 2014 resident Kelly fellow. She is a recent graduate of Columbia University's Master in Negotiation and Conflict Resolution program. Previously, she worked as associate director for programs at the Korea Economic Institute (KEI) in Washington, D.C., managing the logistics for hundreds of KEI events and coordinating the internship program. Following her tenure at KEI, she joined the Columbia University team of Nobel Laureate Economist Joseph Stiglitz as special assistant, where she was responsible for coordinating his speaking engagements, travel, teaching, and writing. Her areas of interest include Korean peninsula security; environmental conflict; and climate change. Ms. Cunico received her BA in politics and Asian studies from Fairfield University in Connecticut.

PARTICIPANT BIOGRAPHIES

Mr. Brad GLOSSERMAN (USA) is an Executive Director of the Pacific Forum CSIS. He oversees all aspects of Pacific Forum activities, including conferences, fellowships, publications, and administration. He is coeditor of Comparative Connections, the Pacific Forum's triannual journal and writes, along with Pacific Forum president Ralph Cossa, the regional review. He is also the coauthor, with Scott Snyder, of *The Japan-South Korea Identity Clash* (Columbia University Press, 2015), a study of national identity in Japan and South Korea and its impact on US alliances. Prior to joining the Pacific Forum, Mr. Glosserman was a member of the Japan Times editorial board. He holds a JD from George Washington University, an MA from Johns Hopkins University, and BA from Reed College.

Ms. Petra G. KUBALKOVA (USA) is a Young Leaders Fellow at the Pacific Forum CSIS and a PhD student at the Department of Political Science at the University of Hawaii, Manoa focusing on international relations and security studies. Her research encompasses substantive analysis of global politics, and the interlinking relations among East-Asia and US foreign policy. Her research interests include political theory, coercive diplomacy, cross-strait relations and East-Asia security studies. She holds a BA from the University of California, Berkeley in Political Science and a Master's in Public Administration from the University of Hawaii, Manoa.

Mr. John K. WARDEN (USA) is a Senior Fellow at the Pacific Forum CSIS where he works on East Asia security issues including US alliances, Japan's island disputes, extended deterrence, and nonproliferation. He received his MA in Security Studies from Georgetown University, where he also served as a research assistant and as editor-in-chief of the Georgetown Security Studies Review. Previously, he worked as a program coordinator and research assistant at the Center for Strategic and International Studies, contributing to projects on nuclear deterrence, arms control, and US alliances. He served as executive director for working groups on US-Russian arms control and US-China nuclear dynamics, managed a project on the US nuclear posture, coordinated the US-Japan-ROK Track II Trilateral Dialogue on Nuclear Issues, and twice directed the Nuclear Scholars Initiative, including editing the accompanying journals. Mr. Warden has published articles in Proceedings Magazine, PacNet, Infinity Journal, The National Interest, and The Diplomat. He earned his BA in Political Science and History from Northwestern University.