MARCH 2016

STRATEGIC RESILIENCE

A U.S.-Japan Alliance Action Plan for All-Hazard Emergency Management

Sachiko Kuno and Michèle Flournoy
Co-Chairs, The Evermay Dialogue

Patrick Cronin and Maki Fukami
Main Contributors

[S&R] Foundation
Inspiring Innovation, Empowering Excellence in Art, Science and Social Entrepreneurship

IIGR International Institute of Global Resilience

Center for a New American Security

About the Authors

Dr. Sachiko Kuno is the President and CEO of the S&R Foundation in Washington, D.C. Dr. Kuno and Dr. Ryuji Ueno founded the S&R Foundation for the purposes of supporting talented individuals with high aspiration and great potential in science, art and social entrepreneurship areas, especially those who are furthering the international cultural collaboration. Dr. Kuno is also the Founder and Managing Member of S&R Technology Holdings, LLC and was the founding CEO of Sucampo Pharmaceuticals, Inc. in Bethesda, MD. She currently serves as the Board of Director on numerous organizations including Johns Hopkins Medicine, Maureen and Mike Mansfield Foundation and Strathmore Hall Foundation, and as the Advisory Board on THIS for Diplomats at Meridian International Center.

Michèle Flournoy is Co-Founder and Chief Executive Officer of the Center for a New American Security (CNAS). She served as the Under Secretary of Defense for Policy from February 2009 to February 2012. She was the principal advisor to the Secretary of Defense in the formulation of national security and defense policy, oversight of military plans and operations, and in National Security Council deliberations. She led the development of DoD's 2012 Strategic Guidance and represented the Department in dozens of foreign engagements, in the media and before Congress. Prior to confirmation, Ms. Flournoy co-led President Obama's transition team at DoD.

Dr. Patrick M. Cronin is a Senior Advisor and Senior Director of the Asia-Pacific Security Program at the Center for a New American Security (CNAS). Previously, he was the Senior Director of the Institute for National Strategic Studies (INSS) at the National Defense University, where he simultaneously oversaw the Center for the Study of Chinese Military Affairs. Dr. Cronin has a rich and diverse background in both Asian-Pacific security and U.S. defense, foreign and development policy. Prior to leading INSS, Dr. Cronin served as the Director of Studies at the London-based International Institute for Strategic Studies (IISS). At the IISS, he also served as Editor of the Adelphi Papers and as the Executive Director of the Armed Conflict Database. Before joining IISS, Dr. Cronin was Senior Vice President and Director of Research at the Center for Strategic and International Studies (CSIS).

Dr. Maki Fukami is the only organization management scientist who has studied emergency management in Japan. She has undertaken extensive fieldwork in the Japanese Fire Service and Coast Guard for more than 10 years and is currently the International Association of Emergency Managers (IAEM) Japan Council President and the Global Board member. She established the International Institute of Global Resilience (IIGR) to promote the professionalization of emergency management internationally and globally in 2012. IIGR has done many innovative projects with partners both in the United States and Japan and received the Chairman's Award from IAEM for exceptional efforts to establish a strong partnership between Japanese emergency managers and their colleagues globally in 2013.

Acknowledgements

This report is the final product of the Evermay Dialogue, a collaborative research effort of the S&R Foundation, the International Institute of Global Resilience (IIGR), and the Center for a New American Security (CNAS). The project was made possible through the generosity of the S&R Foundation, both in the form of a grant but also in the use of Evermay for meetings.

Many people were critical to this collaborative effort and final report. The Co-Chairs wish to thank the Embassy of Japan, including especially His Excellency Kenichiro Sasae, Japan's Ambassador to the United States. They also wish to thank people critical to prompting the idea of an Evermay Dialogue, particularly Takeshi Yamawaki, American General Bureau Chief of The Asahi Shimbun, and Dr. David Asher, CNAS Adjunct Senior Fellow for Strategy and Statecraft. They are also extremely grateful to all S&R Foundation staff members who supported this project. We are also especially grateful to Dr. Maki Fukami, Founder, President, and CEO of IIGR, as well various staff members and associates who participated in the dialogue.

Key CNAS contributors to this project were Dr. Patrick M. Cronin, Senior Advisor and Senior Director of the Asia-Pacific Security Program, and Hannah Suh, Program Coordinator. May others played a role in either the meetings or this final report or both, including: Shawn Brimley, Alexander Sullivan, Phoebe Benich, Harry Krejsa, Melody Cook, Maura McCarthy, Mary Gladstone, John Gudgel, Daniel Brown, Paul Giarra, Sak Sakoda, and Andrew Saidel.

Cover Photos: Faced with a number of potential homeland hazards – from natural disaster and terrorism to cyber and humanitarian and military contingency – Japan and the United States must strengthen each other's strategic resilience in order to prevent catastrophic national failure. Pictured on the cover from left to right: Ground Zero following the September 11, 2001, attacks; the devastation of Meulaboh, Sumatra, Indonesia, following the 2005 tsunami; a real-time map of cyberattacks; and a U.S. Navy lieutenant providing humanitarian aid as part of Operation Tomodachi following the 2011 tsunami and earthquake that struck Japan. (U.S. Navy/Chief Photographer's Mate Eric J. TIlford; U.S. Navy/Photographer's Mate 1st Class Bart A. Bauer; Flickr/Christiaan Colen; and U.S. Marine Corps/Gunnery Sgt. Leo Salinas)

STRATEGIC RESILIENCE

A U.S.-Japan Alliance Action Plan for All-Hazard Emergency Management

S&R Foundation is a non-profit organization that supports emerging creatives and works with its partners to encourage social, scientific and artistic innovation. S&R promotes cultural and personal development by nurturing these highly talented individuals' ability to enrich society with the fruits of their hard work and dedication.

International Institute of Global Resilience's (IIGR) mission is to help strengthen the readiness and professionalism of the emergency management community worldwide through training, education, consulting, and research. The primary focus of IIGR is on Japan, a key friend and ally of the United States. The two main goals of IIGR are: (1) to help strengthen emergency management and disaster resilience in Japan and the United States through mutual learning; and(2) to work to improve Japan–U.S. cooperation in disasters, including cooperation on humanitarian assistance/disaster relief (HA/DR) in the Asia Pacific Region.

FOREWORD

DR. SACHIKO KUNO AND MICHÈLE FLOURNOY
CO-CHAIRS OF THE EVERMAY DIALOGUE

A nation's strategic resilience should not be taken for granted. It takes forethought, expertise, and hard work to withstand and reduce the ill effects of the myriad natural and human-made disasters that threaten an increasingly complex and interconnected world. Crisis management has never been so challenging, and the lines of authority and responsibility between national security and homeland security are increasingly difficult to distinguish. One way to stay ahead of the curve is to adapt existing institutions and partnerships, including the U.S.-Japan alliance, to assist national and multinational thinking and preparation about crisis management. More than ever, national governments need to come together to share best practices, improve training and readiness, and conduct effective responses. Major allies such as the United States and Japan need to leverage their existing security apparatus to hedge the risks that might arise from a broad variety of challenges.

It is the question of how the alliance might improve strategic resilience and crisis management that spurred us to initiate the Evermay Dialogue. Since the end of 2014, the Center for a New American Security (CNAS) and the International Institute of Global Resilience have conducted quiet expert dialogues at the Evermay estate, the Georgetown headquarters of the S&R Foundation in Washington. The Evermay Dialogue thus refers to the series of five quarterly gatherings that the two of us co-chaired to examine emergency management and strategic resilience from the vantage point of the United States and Japan.[1]

The inaugural Evermay Dialogue in December 2014 discussed the broad subject of current emergency management strategies and systems in Japan and the United States, with an eye toward identifying opportunities for strengthening national preparedness and crisis response. Each subsequent discussion in 2015 gathered 20 to 40 experts to consider one of four types of major contingency: natural disaster (March), terrorism (June), cyberattack (September), and local military escalation (December). While the discussions were conducted off-the-record, a roster of those who participated in one or more meetings in the series is attached at Appendix A. This all-hazards approach to crisis management was devised to identify the essential building blocks for a new framework to think comprehensively about resilient responses to major crises. While the dialogue focused on the U.S.-Japan alliance, the aim was to derive lessons for both national and collective action, not just by the allies but potentially other partners as well.

The Evermay Dialogue identified a number of key ideas that deserve official consideration. Among the most important and useful actions highlighted in this report, the following five steps in particular merit serious study by governments:

- Initiate an official U.S.-Japan working group on strategic resilience.
- Institutionalize an annual U.S.-Japan crisis management exercise modeled on defense war-game experience.
- Focus on cyberspace cooperation to ensure alliance connectivity across civil-military domains, with a particular emphasis on risks to the integrity of information.
- Establish an operational U.S.-Japan alliance command structure that allows for all-of-government information-sharing and cooperation.
- Create a training program on strategic communications for national and local governmental officials, first responders, and appropriate private-sector and civil-society actors likely to find themselves on the front lines of reporting information in the midst of different crises.

These and other actions should become part of an alliance-plus framework that adapts existing institutions for future needs. There is no way to fully predict when disaster will strike, but it seems certain that decision-makers will never be sufficiently prepared to deal with the full spectrum of crises that might arise. Learning and doing together, through the alliance, can offer cost-effective returns for both nations and for helping other countries and actors, too.

Dr. Sachiko Kuno is President and CEO of S&R Foundation and the Honorable Michèle Flournoy is Co-Founder and CEO of the Center for a New American Security.

Key Judgments

Strengthening the strategic resilience of the United States and Japan is an imperative that the two nations should do more to advance jointly. Faced with myriad potential major homeland hazards, ranging from natural disaster and terrorism to cyber and humanitarian and military contingency, decisionmakers need to apply renewed urgency and focus on the measures most likely to stave off catastrophic national failure and buy down risk on a wide array of future threats.

The concluding section amplifies the following **10 recommendations** that together constitute an alliance action plan:

1

Initiate an official U.S.-Japan working group on strategic resilience. Officials in Washington and Tokyo should adopt a process to create a comprehensive strategic resilience plan of action. As a first step, an official discussion mirroring the unofficial Evermay Dialogue might underscore the benefits of adding an alliance "catastrophic health insurance" plan on top of existing national capabilities. Furthermore, an official forum for outlining a new strategic framework under changing strategic circumstances would be able to build on existing levels and areas of cooperation while also indicating areas for potential alliance growth.

2

Institutionalize an annual U.S.-Japan alliance crisis management exercise modeled on defense war-game experience. Such exercises are meant to be not necessarily prescriptive, but provocative and suggestive. This technique is also invaluable in establishing mutual understanding where fundamental experiences and thinking among participants may be somewhat different. To move from planning to action, the alliance should not wait for a detailed plan of action to be agreed upon before starting more active cooperation on crisis management.

3

Create an alliance series of authoritative after-action reports. This will entail collecting data from major crises confronted by each or both nations. Going forward, both Japan and the United States need to do a better job of collecting data when crises occur and then scrupulously internalizing the results of after-action reports.

4

Create a training program on strategic communications for national and local government officials, first responders, and appropriate private-sector and civil-society actors likely to find themselves on the front lines of reporting information in different crises. Effective strategic communication is essential in any crisis and includes both technical and organizational solutions. Technically, this means developing the capability for communicating past the failure of established infrastructures, providing for civil and military power and connectivity.

5

Identify ways to break down some of the highest hurdles to achieving a unity of effort and effect. Together, the U.S.-Japan alliance can share innovative ways for interconnecting complex government at all levels as well as incorporating the private sector and civil society. Doing so is good governance and could be the difference between crisis and disaster when the time comes.

6

Consider actionable ways the alliance can translate shared best practices and requirements into improved disaster preparedness. This would include: understanding critical infrastructure; developing a new approach to risk assessment, safety standards, and redundancy before critical infrastructure and other systems are built or overhauled; developing realistic risk assessment and disaster preparedness guidelines; establishing authorities and responsibilities in advance for prevention, defense, and recovery; and implementing the guidance on a steady-state basis through training, compliance, and a culture of safety.

7

Determine ways to deliver assistance and speed recovery during and after major disasters. For instance, officials should ensure that policies, training, processes, and resources reflect how much will be driven by and reliant on the response of local communities and individuals, and how much by central governments. This is an evolving government-citizen understanding that has emerged in both Japan and the United States from great calamities. There should be no surprises regarding who will be responsible, because, like the aftershock of an earthquake, a tragedy can reassert itself unexpectedly at a moment's notice.

8

Focus cooperation in the relatively new realm of cyberspace on ensuring alliance connectivity across civil-military domains, and with a particular emphasis on risks to the integrity of information. A cyber 9/11 appears still a distant more than an immediate threat, and yet cyber vulnerabilities are significant and growing. Preparing for them as an alliance is an urgent need for the United States and Japan. Current cyberthreats compromise one or more aspects of the triad of information confidentiality, availability, and integrity. Of particular concern, because of the difficulty of detection, are integrity attacks in which data are altered or manipulated.

9

In the context of crisis management – but not only in that context – establish an operational U.S.-Japan alliance command structure that allows for all-of-government information-sharing and cooperation, preferably as part of the Five Eyes intelligence arrangement, but at least in parallel with it. The United States and Japan might work on this as part of a trilateral forum with Australia – in particular should a joint submarine project move forward – as well as with South Korea.

10

Alliance managers need to help crisis managers dealing with homeland security consider how humanitarian and military contingencies could pose serious challenges to homeland peace and security, and vice versa. These are not separate portfolios; however, governments organize around particular responsibilities. A deteriorating security environment in Northeast Asia and around Japan includes a range of risks arising from the Korean Peninsula. Potential maritime tensions with China might affect civilian populations in Japan's home islands and, through them, Japan's ally the United States. Such contingencies are important to consider in part because they reveal the obstacles to bureaucratic politics that otherwise prevent integrated whole-of-government and whole-of-society solutions.

An All-Hazards Approach to Emergency Management

Disaster is inevitable, but the level of resilience can vary broadly depending on the foresight and commitment of decisionmakers acting before a crisis. Five years after the Great East Japan Earthquake triggered a deadly tsunami and nuclear meltdown, a decade after Hurricane Katrina laid waste to parts of coastal Mississippi and Louisiana, and nearly 15 years after al Qaeda hijacked civilian aircraft to destroy the World Trade Center towers in Manhattan, natural disaster, terrorism, and other crises threaten the strategic stability and resilience of the United States, Japan, and other highly developed nations. Although crises come in all varieties and sizes, these countries' crisis management systems, plans, and responses are sure to be taxed time and again in the coming years. This report aims to highlight some of the unlearned lessons of the past to inform with new urgency and focus the kinds of steps that might better improve national and societal resilience in the face of myriad hazards.

Government often fails to meet public expectations when dealing with major crises. For instance, regarding the nuclear meltdown of March 2011, one Japanese report understatedly concluded that "the policymaking of the Japanese government and Japan-US coordination in response to the Fukushima crisis was not implemented smoothly."[2] The bipartisan congressional committee investigating the preparation for and response to Hurricane Katrina damningly named its report *A Failure of Initiative.* The committee wondered "why government at all levels failed to react more effectively to a storm that was predicted with unprecedented timeliness and accuracy."[3] The 9-11 Commission similarly opened its own comprehensive report: "September 11, 2001, was a day of unprecedented shock and suffering in the history of the United States. The nation was unprepared."[4]

In the wake of 9/11, Katrina, Fukushima, and other crises in both the United States and Japan, it is clear that both allies can gain much from each other in strengthening their individual and collective resilience to national strategic contingencies. The Evermay Dialogue was created to explore lessons and identify an action plan for improving future crisis management.

Former CNAS Chairman of the Board and Secretary of the Navy Richard Danzig argues that preparing for "all hazards" is the most intelligent way to ensure resilience in the face of so many types of potential crisis.[5] In the context of focusing on current emergency management strategies and systems in Japan and the United States, he avers that the two countries could both benefit by moving away from national systems and toward a more integrated alliance framework and set of standards. The United States and Japan, and perhaps other nations, could bolster crisis management by enhancing four types of cooperative behavior:

- **Engage in mutual learning:** Use the two cultures and systems to inject new approaches, applied in innovative ways.
- **Broaden alliance cooperation:** Bring together more and different actors, as security is not simply a narrow military construct or gathering of alliance managers, but the provenance of numerous governmental and nongovernmental actors.
- **Provide material provision:** Think of practical and physical ways each country can help the other buttress crisis management and resilience.
- **Leverage the U.S.-Japan relationship for crisis management:** The U.S.-Japan alliance is widely perceived as achieving high degrees of effective and operational integration. Less obvious is the progress toward more integrated crisis management and resilience. The two allies should actively expand this dimension of the relationship while simultaneously seizing opportunities in which crisis stressors intensify and strengthen the countries' bonds (much as happened after the March 2011 triple disaster in Japan).

Integrating two very different national approaches is easier said than done, but the chances of averting future disasters can be better improved by working together than going it alone. The United States and Japan each has a distinctive system, culture, and bureaucratic organization for responding to crises, particularly those affecting the homeland. But diversity can be an asset. For instance, Japan has fewer legal obstacles to nationally unified domestic crisis response than does the United States. Similarly, the United States has tremendous capacity to respond to crises around the globe. Thinking through each country's approach and the strengths and weaknesses of each system can yield new

ways to improve crisis management for both. Moreover, the process of doing so may facilitate crisis response collaboration with other partners as well.

The U.S. approach to crisis, particularly domestic disasters, is long evolved and complex. At the first meeting of the Evermay Dialogue, the current U.S. crisis management strategic culture was described in terms of 10 characteristics:

1. The United States is challenged by constitutional and legal authorities that give state and local governments a large role in responding to crises.
2. The United States strives for unity of effect more than unity of effort.
3. The country uses planning to overcome bureaucratic politics.
4. The United States plans for complex events – the maximum of maximums – with no-notice exercises.
5. It leverages what is ubiquitous, such as smartphones and social media.
6. America focuses on delivering capacity for survivors, not just for responders.
7. The country seeks to be expeditionary, not reactive and top-down.
8. It tries to buy down risk on future threats.
9. The United States encourages others to adopt similar standards and systems.
10. It seeks to overcome "crisis entitlement," or that the nation is over-reliant on government and under-reliant on community and individual citizens.

The lessons of strategic resilience can be characterized as a tussle between the science and the creative art of crisis. Both dimensions must be improved upon and integrated to achieve the most effective response possible. For example, a scientific approach to crisis management might delineate a single type of crisis (say, natural disaster) or even an individual crisis (such as the Great East Japan Earthquake or Hurricane Katrina); a more creative dimension, however, might seek to identify an all-hazards approach that is optimally prepared for different categories of crisis.

Japan and the United States could both benefit by moving away from national systems and toward a more integrated alliance framework and set of standards.

The latter approach may advocate *building in* resilience, or what Nassim Nicholas Taleb has called "anti-fragility," so that systems not only survive but actually become stronger in response to severe challenges.[6] Other "scientific" or at least top-down assessments of predictability, frameworks for response, national command and control, or central directives, etc., can be contrasted with more elastic and local ideas of agility and improvisation, community response, local situational awareness, and persuasion. The following chart offers some of the contrasting themes that emerged out of the first Evermay Dialogue.

These broad insights and themes, especially the notion of seeking a more holistic system for dealing with a wider spectrum of hazards, require thinking through past and future crises in order to synthesize ideas useful for multiple contingencies. The rest of this report briefly distills discussions of the Evermay Dialogue on terrorism, cyberattack, humanitarian crisis and military conflict. It then concludes with a prospective action plan for the United States, Japan, the alliance, and other partners.

Crisis Management as a Balance of Scientific and Creative Approaches

SCIENTIFIC	CREATIVE
Single Crisis Event	All-Hazards Approach and Anti-fragility
Predictability	Agility and Improvisation
National Framework	Community Response and Self-Reliance
National C4ISR	Local Situational Awareness
Central Directives	Persuasion
IT and Systems Integration	Collaborative Information-Sharing
Institutional "Silos of Excellence"	Whole Community
Emergency	Individual Empowerment
Best Practices	Wise Investments and Implementation
Disaster Stressors	Bonding (or Fragmenting)
Political Costs and Constraints	Education in Aftermath and Marketing Crisis Readiness

01 CHAPTER

Terrorist Attacks

Terrorist Attacks

Terrorism has evolved in waves over the past century or more, but it seems one of the more durable threats that modern nations will have to grapple with over the coming decades. Nearly 15 years after the worst such attacks on American soil, the United States remains as vigilant and concerned about homeland terrorism and attacks on American citizens, property, and interests abroad as at the beginning of the new millennium. Lone-wolf and homegrown (though foreign-inspired) attacks, such as the one in San Bernardino, Calif., that killed 14 innocents and injured an additional 22 people in December 2015, reinforce the notion that acts of terrorism can come from diverse actors with access to lethal means. The so-called Islamic State of Iraq and the Levant (ISIL) is of particular concern at present. The ISIL-related terror attacks that left 130 dead in Paris last November are only the largest of multiple international assaults in recent months, and they were preceded by the sensational January 2015 mass murder spree centered on the Charlie Hebdo satirical magazine office. The resurgence of terror attacks conducted or inspired by ISIL and al Qaeda or their local affiliates is also posing a growing threat in Asia and even Northeast Asia. If ISIL can brutally behead innocent Japanese civilians on camera, as it did last year, then ISIL-inspired actors with access to lethal means could wreak havoc on Japanese civil society in the future. As the 9/11 Commission report suggested for the United States, Japan, France, and many other nations, preparations for a major terror attack are almost certain to be inadequate.

Democracies preparing for potential terror attacks require more than the British slogan "Keep calm and carry on." Although such a plucky public attitude certainly would not hurt, governments should focus on better preparing for the detection, early response, assistance, law enforcement, and recovery elements of an attack. Unfortunately, even despite past experience with such attacks, there is no guarantee that governments are getting better at preventing or responding to them. Beginning in the 1970s, the re-emerging phenomenon of terrorism has revealed that government is not well-organized to confront it. Throughout the years, a number of committees and agencies have been created to combat terrorism. The attacks on 9/11 fundamentally altered the perception of plausibility; the question was no longer "will this happen" but "can you prove that this will not happen again?"

The attacks on September 11, 2001, altered the perception of the plausibility of such a terrorist attack and shifted the focus on threat analysis from the adversary's capabilities and intentions to the target's vulnerability. (Flickr)

This led to a shift in threat analysis. Traditional threat analysis assesses the adversary's capabilities and intentions. Since 9/11, this changed, to an assessment of the target's vulnerability. Vulnerability-based analysis is legitimate for analyzing consequence but does not evaluate threat and instead becomes part of the threat assessment. The result is that threats become seen as inevitabilities, which in turn seem imminent. An unfortunate and unintentional byproduct of such vulnerability-based analysis is threat advocacy, with individuals championing protection again their threats as most deserving of funding. Furthermore, if officials are discussing scenarios, terrorists begin talking about such scenarios, resulting in a feedback loop.

Terrorism profoundly affects resiliency and the national psyche. Resilience implies at least a certain degree of closure, but in the case of terrorism, that luxury has been denied. Major terrorist events have enormous psychological impact on individuals and society, and governments – whose primary function is to protect the community – typically respond by overpromising, for example by claiming that they will eliminate any risk of future attack. However, this erodes a realistic appraisal of risk and a healthy stoicism. Leaders should instead ask, when they think about resilience, what they can do to reassure the individual, community, and society.

The concepts of security and resilience manifest themselves differently locally, nationally, and internationally. People adopt a different role at home as opposed to the Capitol, and the public's relationship with fear differs as well due to what local governments can do to deal with a threat compared with the federal government. These differences extend to the organization of each. National security is centralized and top-driven, whereas homeland security is decentralized, transactional, and bottom-driven. Yet the American public still expects both local and federal governments during crises to be top of what is happening.

Leaders should instead ask, when they think about resilience, what they can do to reassure the individual, community, and society.

One World Trade Center symbolizes the resilience of the American public. While the United States has taken positive steps in building resilience by planning for broader, capability-based planning, there is still room for improvement. (Port Authority of New York and New Jersey)

The United States is achieving progress in some areas yet falling short in others. In terms of positive actions the country is taking, the government, private sector, individuals, think tanks, and nongovernmental organizations (NGOs) are all contributing to building resilience. In the past 20 years, there has been a shift from planning for specific events to broader, capabilities-based planning, developing core capabilities that can be used to address any event that may occur. Furthermore, businesses have removed stovepipes separating physical threat planning from cyberthreats and interdependency. Overall, industry and government are beginning to understand the importance of trends and how they can manage risks.

One Evermay Dialogue participant and leading expert on crisis management suggests that the United States can improve in at least 10 ways:

1. Increase public trust.
2. Reduce legislative and regulatory barriers to responding to an event.
3. Provide more concise guidance.
4. Achieve better situational awareness.
5. Mobilize resources to deal with the crisis after the fact.
6. Foster better innovation in the private sector.
7. Develop more useful metrics for effectiveness.
8. Take responsibility.
9. Focus on how to mitigate vulnerability.
10. Create greater resilience among interdependent supply chains.

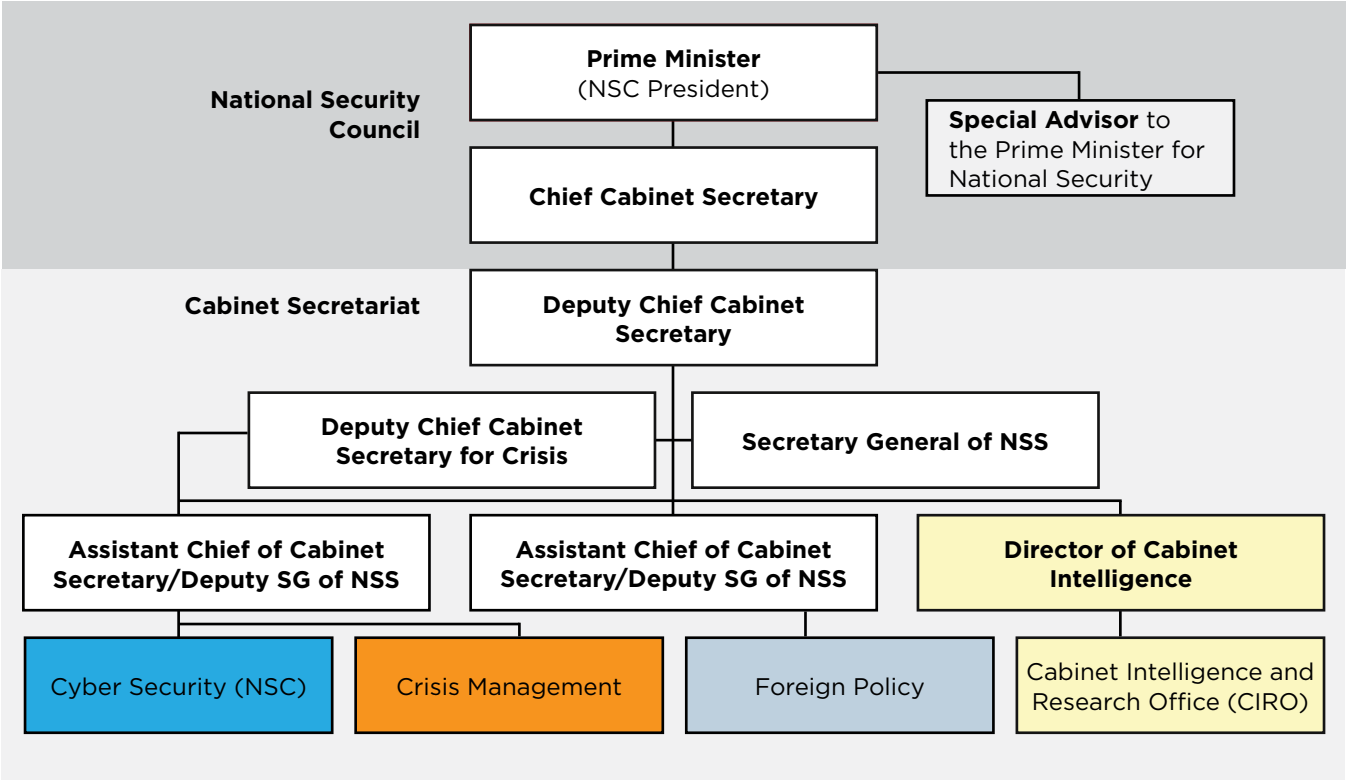
Japanese responses to terror attacks also face numerous hurdles. If a terrorist attack were to occur inside Japan, local police and fire departments would be the first responders. The Japan Self-Defense Forces (SDF) would respond only if requested, and that request could be slow or delayed if first responders were unaware of the scope of the threat. Japan's interagency approach to a domestic terrorist attack creates potential bureaucratic obstacles to a swift and effective response. The issue of synthesizing the information that comes in at the central government level and pushing it back out again still exists and affects the relationship between police authorities and local municipalities. Although it has been more than two decades since the 1995 sarin gas attack by Aum Shinrikyo on the Tokyo subway, the Japanese government still has yet to adequately assess what it did right, what it did wrong, and what it can improve upon. As those who responded to that attack are increasingly in or facing retirement, the opportunity to learn fully from past experience is disappearing.

[In Japan] sharing information across elements of the government and beyond has always been a challenge, especially at the nexus of police and national security.

Until the March 2011 Great East Japan Earthquake (also known as the Great Tōhoku Earthquake and as Japan's "3/11") and subsequent tsunami and nuclear meltdown, Japan had an almost mythical notion of being able to provide 100 percent safety. It almost seems as though the Japanese public discourse avoids contemplating worst-case scenarios. The dynamics between politicians and the bureaucracy are very different from the U.S. system. While theoretically, politicians should respond to the public's needs, in reality, the bureaucracy takes over and leaves politicians in the dark. Sharing information across elements of the government and beyond has always been a challenge, especially at the nexus of police and national security. Recent organizational changes under the Abe administration no doubt put Japan's crisis managers in a better position than they would have been to deal with potential terror attacks. Yet the unpredictability of terrorism means that major international events hosted by Japan, including the G-7 meeting in May 2016 and the 2020 Olympics, might not constitute the only high-risk targets. Even so, such events provide an opportunity to further improve crisis management preparation, information-sharing, and cyber resilience.

The notable lack of after-action reports on the 1995 sarin gas attack makes the Japanese government seem ambivalent. There are also cultural differences with respect to the idea of safety, including the considerable protection surrounding the White House compared

Organizational Chart of Japan's National Security Secretariat (NSS)



with Japan's executive residence at the Sori Daijin Kantei. The United States can improve in making after-action reports more publicly releasable and hold bilateral or joint exercises, especially with Tokyo on crisis preparedness. While there may be a willingness to perform a truthful after-action reporting, actually dissecting the findings and recommendations is an undertaking in itself. For Japan, 3/11 made the government realize and begin to expose its vulnerabilities. The United States and Japan should share their experiences and expose their vulnerabilities to each other. By cooperating and engaging in the 3/11 incident study together, each will benefit from the findings.

Japan's new National Security Secretariat is modeled after the British National Security Council, given the similar parliamentary systems. The secretariat comprises four ministers: the prime minister, chief Cabinet secretariat, foreign minister, and defense minister. The secretariat serves as the control tower of diplomacy and defense, giving guidance to the ministries. However, should a terror attack occur in Japan, the National Security Secretariat would share responsibility in coordination but would not be the leading national actor in managing all crises. The limited role in dealing with terrorism was visible during the January 2015 hostage crisis, in which ISIL captors ultimately beheaded two Japanese civilians. The division of labor could introduce potential confusion in the event of a larger attack on the homeland.

02 CHAPTER

Natural Disasters

Natural Disasters

Of all the crises considered in the Evermay Dialogue, few are as guaranteed as natural disasters. The issues of prevention and preparation, response, and recovery are well-developed. In seeking to tap into some of the rich experience in thinking about and dealing with natural disasters, the Evermay Dialogue channeled expert discussion into three categories: actions that should be taken before any disaster, those taken during an unfolding crisis, and those after the immediate response in order to facilitate long-term recovery.

Before a Disaster: Steady-State Preparation Processes

Improving disaster preparedness starts with developing a new approach to risk assessment and safety standards before critical infrastructure and other systems are built. Some who have dissected the decisions that led to the Fukushima crisis noted that the design basis for the nuclear facility did not contemplate a tsunami of the size that resulted from the Great Tōhoku Earthquake – but only because some arbitrary constraints were placed on both initial and subsequent analyses. Probabilistic risk assessments are a more promising method for guiding design basis and evaluating the risk of "beyond-design-basis events."

A second, related task is to develop realistic risk assessment and disaster preparedness guidelines and to update them regularly. Guidance needs regular updating not least because of the importance of incorporating the latest scientific findings on all-hazards risks, especially for highly complex systems such as nuclear facilities. Much of this can be done within departments and agencies, but experience underscores the importance of creating scientific advisor positions at senior levels that can appropriately coordinate and synthesize these efforts.

Probabilistic risk assessments are a more promising method for guiding design basis and evaluating the risk of "beyond-design-basis events."

The next component of disaster preparedness efforts is to implement the guidance on a steady-state basis through training, compliance, and a culture of safety. In the aftermath of nuclear accidents in both the United States and Japan, governmental reviews have revealed lapses in these efforts. Moreover, all training needs to be realistic, modeling the type of uncertainty that attends real-life disasters.

To ensure effective coordination across the diverse agencies that may be responsible for responding to a complex disaster, it is important to build interoperability. Throughout the U.S. 3/11 response, White House efforts to coordinate among U.S. agencies such as the Nuclear Regulatory Commission (NRC) and the National Oceanic and Atmospheric Administration (NOAA) were hampered not only by bureaucratic silos but also by technical barriers in modeling and other scientific functions.

Another point of general consensus among those involved in Japan's March 2011 crisis is the difficulty of effective risk communication to the public, especially when media are being less than helpful. This challenge points to the need for standard operating procedures (SOPs) for risk communication for bureaucrats and training for senior leaders. For instance, it would be useful for agencies to develop and maintain a network of scientists and experts who could be mobilized in the event of a crisis to comment in media and avoid the kind of sensationalism that can hamper government responses.

Another point of unanimous agreement was the vital need to lay down a flexible physical infrastructure for disaster response in advance, especially since natural disasters can cause material damage of a much greater scope and scale than can other types of national strategic contingencies. This includes pre-positioning materiel and basic necessities for immediate dispatch to affected areas. It also includes a communications infrastructure that has enough redundancy and mobility to surge capacity into blackout zones and provide key situational awareness.

Finally, the United States, Japan and other nations must prepare to do all this together, rather than just separately. In an interconnected world, this socializes the risk of major disasters across states. Such preparation may

include joint training where possible but should at least include high-level bilateral agreements on mechanisms and procedures for joint responses to disasters. U.S. efforts to assist Japan after March 2011 were hampered because all the SOPs for responding to a foreign disaster were geared toward aid-receiving countries. Likewise, although over the past decade the U.S. government has increasingly considered the issue of foreign consequence management for nuclear accidents, there were no specific plans to help Japan. The connective tissue of the U.S.-Japan alliance helped overcome the lack of specific disaster planning, but that cannot be counted on with most nations or with respect to every type of national strategic contingency.

In an interconnected world, joint disaster preparation socializes the risk of major disasters across states.

While the participants in the Evermay Dialogue identified a number of clear steps to be taken to prepare for disasters, they also underlined the technical and political difficulty of planning for the unthinkable on a consistent basis. After all, it is an immense and enduring challenge to create a more effective all-hazards approach in the face of complex crises such as 3/11, particularly when such events happen so rarely.

The March 11, 2011, earthquake and tsunami and resulting meltdown of Fukushima Dai-ichi devastated the northern region of Japan. (Getty)

During an Unfolding Crisis: Decisionmaking and Implementation Under Uncertainty

The challenges of responding to an unfolding disaster, particular one as complicated and destructive as the 3/11 triple disaster, are twofold: making the best possible decisions under conditions of extreme uncertainty and ensuring effective implementation of those decisions by diverse stakeholders and participants in complex disaster responses.

Both aspects of disaster response require governments to be prepared to adopt ad hoc processes that can break down silos and cut through red tape. For example, once it was clear that Fukushima Dai-ichi was melting down, Japan and the United States had to decide and agree upon the proper radius for the evacuation zone around the facility. Competing advice emerged from different pockets of scientific knowledge within the bureaucracy. Japan could have used a "science coordinator" position to referee among agencies, evaluate the information coming in, and advise political decisionmakers. At the bilateral level, an ad hoc Joint Liaison and Coordination Meeting process was formed – informally named the "Hosono process," after the able politician Goshi Hosono, who was thrust into the role of Fukushima troubleshooter. The Hosono process convened agencies such as the NRC and Department of Energy from the United States and Japan's Foreign Ministry and Nuclear and Industrial Safety Agency in order to make decisions outside normal bureaucratic bailiwicks.

Similarly, the implementation of those decisions required the creation of several special-purpose formations, including the U.S.-Japan joint task force created for Operation Tomodachi, which saw SDF helicopters flying off the aircraft carrier USS *Ronald Reagan*. The U.S. Agency for International Development (USAID)/ Office of Foreign Disaster Assistance's Disaster Assistance Response Team (DART) played a critical role in facilitating U.S. support for Japan. In addition to the expertise and training of its own members, DART is empowered to pull resources from across the U.S. government outside normal bureaucratic channels, thus greasing the wheels of the nation's response.

Another key determinant of effective emergency management is tailored, responsive risk communication to the public – ideally enabled by pre-existing guidelines and training as outlined above. In this context, "tailored" refers to the need to balance transparency with other downside risks: Had the Japanese government announced the possibility of a Fukushima meltdown immediately after the crisis (when, indeed, the status of the reactor's cooling systems was very much in doubt), it may well have precipitated mass panic and a paralyzing, unplanned evacuation of metropolitan Tokyo that would have had global economic repercussions. But later on, risk communication needs to be accurate, as transparent as possible, and responsive to the public.

During the weeks and months after 3/11, Japanese officials made a point of doing press briefings every day and answering every question put to them, even it if meant marathon six-hour sessions. Several lessons emerged over time. First, it is wise to provide a bottom line upfront and then proceed to all the details. Second, with a rapidly unfolding, uncertain situation one is obliged to communicate risks in bands of probability; when one acknowledges the worst possible outcome and then proceeds to one's own assessment, it creates trust with the media and the public and makes the overall message more effective.

In terms of concrete actions, repairing transportation and communications infrastructure is especially important to facilitate an effective disaster response. Pre-positioned supplies can be rushed to affected areas through air power and other (often scarce) mobile resources at the outset, but roads must be

Sailors scrub the flight deck of the USS *Ronald Reagan* to prevent potential radiation contamination while providing assistance off the coast of Japan during Operation Tomodachi. (U.S. Navy/ Mass Communication Specialist 3rd Class Kevin B. Gray)

Following the 2011 Tohoku earthquake and tsunami, U.S. armed forces collaborated with Japan Self-Defense Forces to provide emergency response disaster relief through Operation Tomodachi. (U.S. Marine Corps/Lance Cpl. Steve Acuff)

repaired quickly to transport supplies at scale. Similarly, restoring communications and sensors within the affected area will reduce pervasive uncertainty and ease the response effort overall.

Finally, it is worth highlighting an often underappreciated facet of crisis response: The greatest health consequences to affected populations are mental as much as physical, so when medical resources are deployed forward, they must include capabilities to address mental health.

Contemplating the management of such extraordinary disasters in the "before" and "during" phases calls to mind President Dwight D. Eisenhower's famous dictum: "Plans are worthless, but planning is everything." That is to say, any plan is less important than the skills and capacity of staffs to conduct planning. Furthermore, guidelines should not be rigid scripts, but rather general precepts and toolkits to assemble the right responses to unique situations. This includes the ability to accommodate improvisation and emergent behaviors within the bounds of prudence. In a word, governments must be – often against their nature – adaptive. But in the 21st century, it is imperative that nongovernmental actors also improve their ability to plan on their own and in coordination with governments.

After the Crisis: Facilitating Long-Term Recovery

In the aftermath of a disaster, how does one assess when the situation has passed from "during" the crisis to "after"? Like the aftershock of an earthquake, a tragedy can reassert itself unexpectedly at a moment's notice. Thus, many of the principles that should be applied during a crisis must continue long after the period of most acute danger. Similarly, many actions necessary to meet the unique requirements of long-term recovery need to be set into motion as soon as disaster strikes.

One of the signal demands for both short-term disaster relief and long-term rebuilding is the effective delivery of aid, both in the form of domestic government resources and the outpouring of international support that often accompanies high-profile tragedies. Donors may wish to send money but not know where to create lasting impact. This requires public-private partnerships. The U.S.-Japan "Partnership for Reconstruction" announced by then-Secretary of State Hillary Clinton, which later developed into the Tomodachi Initiative, provides an effective model for this type of effort. On the private side, it helps to have umbrella organizations for nongovernmental entities wishing to contribute, such as Japan Voluntary Organizations Active in Disaster (JVOAD), formed in 2014 in response to 3/11 and based on the U.S. National VOAD (NVOAD).

Public education is crucial for any societal approach to resilience and risk reduction. Indeed, education is so important that the maturity of a country's public disaster resilience education is one of the only accurate barometers for its true emergency management capability. It stimulates advance planning, catalyzes new advocacy for resilience, creates a receptive audience for crisis communications, and provides a framework for emergent behaviors that are crucial for responses to dynamic challenges. Education can create the type of local resilient capability that can effectively link up with centralized resources. International cooperation requires adopting educational frameworks that can bridge societal gaps. Southeast Asia, for instance, has achieved good results in part because countries there are more receptive to using a common English vocabulary. Northeast Asian countries, by contrast, remain loath to use a second language to discuss disaster-related issues.

There is some evidence that the U.S. and Japanese governments are taking steps to reform their disaster preparedness approaches. Standards such as the National Health Security Preparedness Index educate the public and create accountability for states. In response to Hurricane Katrina, the Federal Emergency Management Agency (FEMA) reorganized itself to be more responsive in a bottom-up framework. FEMA was once a check-writing organization that waited for local authorities to "pull" or request assistance before taking action. It subsequently became a "push-pull" organization that dispatches pre-assembled resources at the outset of a disaster in order to meet local requests with greater flexibility and timeliness.

Education is so important that the maturity of a country's public disaster resilience education is one of the only accurate barometers for its true emergency management capability.

On Japan's part, it is doing more to create public-private partnerships and increase international coordination on disaster response. The foundation of JVOAD represents the kind of disaster preparedness constituency that can create political progress in support of better approaches. JVOAD, in partnership with the Tomodachi Initiative, also helps create U.S.-Japan connectivity on these issues. In addition, Japan is playing a greater role in R3ADY Asia-Pacific (formerly the APDR3 Network), a disaster resilience organization launched under the aegis of the Asia-Pacific Economic Cooperation (APEC) forum. The R3ADY network espouses many of the same principles as those raised during the Evermay Dialogue.

The United States and Japan should build upon these steps by deepening bilateral cooperation on disaster preparedness issues. As alliance military assets are also vulnerable to a number of potential disasters in Japan, the U.S.-Japan alliance is a natural starting point for this type of cooperation. However, ultimately the approach must involve the whole of government in addition to public-private partnerships.

03 CHAPTER

Cyberattacks

Cyberattacks

Unlike planning for natural disasters that usually have global precedents, it is a whole other challenge trying to prepare for a major cyberattack that has not yet been experienced. Indeed, predictions of cyber calamities – from the Y2K "Millennium Bug" to a potential cyber 9/11 – may only serve to further desensitize officials and publics alike to the very real dangers lurking because of society's heavy dependence on cyberspace and networked systems. Through the Evermay Dialogue, though, experts were able to advance critical thinking on this important subject.

A Mutual Recognition of Cyber Vulnerabilities

While officials speak of a "new threat landscape," many see cyber espionage and the theft of intellectual property as possibly among the greatest threats to U.S. national security. Current cyberthreats compromise one or more aspects of the triad of confidentiality, availability, and integrity. However, confidentiality attacks, such as the breach of records at the Office of Personnel Management (OPM), are running out of confidential data not already exposed. Availability attacks, like those that occurred at Sony Pictures Entertainment and the Sands Casino, can destroy data and deny employees and customers access to services. Integrity attacks, or those where data are maliciously altered, are of particular concern due to the difficulty in knowing when data have been manipulated. Concerns about the manipulation of data through cyberspace also have been expressed by the U.S. director of national intelligence.[7]

Current cyberthreats compromise one or more aspects of the triad of confidentiality, availability, and integrity.

The National Center of Incident Readiness and Strategy for Cybersecurity (NISC) in Japan is seeing increasingly more sophisticated cyberattacks. Targeted emails or "spearfishing" attacks against government agencies have increased from 139 in 2013 to 264 in 2014. Suspicious emails containing malware have more than doubled, from 381 in 2013 to 789 in 2014. Malware infection reports in government agency systems have more than tripled, from 500 in 2013 to 1,700 in 2014. In May 2015, the Japanese Pension Service was hacked, leading to 1.25 million cases of personal data being leaked. This breach, along with the passage of new cybersecurity legislation in late 2014 (Basic Act on Cybersecurity), was the catalyst for the release of a new Japanese cybersecurity strategy in September 2015.[8]

It is possible to consider four types of threat actors: nation-state teams, criminals, "hacktivists," and, to a far lesser extent, terrorists. Nation-states have the most sophisticated cyber capabilities, and the greatest state threats to Japanese and U.S. national security come from China, Russia, Iran, and North Korea. These nation-state adversaries sometimes employ proxies to carry out cyberattacks, but countries with fewer cyber capabilities can still hire cyber mercenaries or acquire more sophisticated weapons. However, state use of cyber weapons should still tend to be consistent with the state's foreign policy, and those actors that have more advanced cyber capabilities are likely to better understand escalation dynamics.

China has been gathering cyber intelligence and preparing the battlefield since the mid-1990s, obtaining much of its information using open sources. Chinese cyber strategy embraces the ambiguity of cyberspace and the ease of cyberattack. Beijing believes that high-tech adversaries such as the United States are highly vulnerable and that China is not. A private cyber company, FireEye, is tracking more than 20 China-based cyber teams, with a smaller number in Russia, Iran, North Korea, and Syria.[9]

The Chinese teams are arguably the most aggressive, but some believe that Russia's cyber offensive capabilities are more advanced. Russian cyberattacks are often directly in support of Moscow's kinetic air and ground operations, such as has occurred in Ukraine over the past two years.

Yet the traditional security paradigm of state-versus-state threat is certainly less applicable when it comes to cyberspace. Individuals are now being empowered, and private companies may matter more than governments in cyber response. The private sector generally has the most capabilities, handles many more attacks, and has the most talent. Given that the private sector owns most of the infrastructure related to the Internet, it is hardly surprising that a majority of intrusions and offensive cyber technology resides in private companies and organizations.[10] Some former senior officials think that the private sector should in fact be the lead actor in cybersecurity, as supported by the government. Regarding individual empowerment among private, young, tech-savvy folks, "force" is devolving from being just a state-monopolized activity. It is now MIT versus the state, and there needs to be greater understanding between "the geeks and the wonks." For example, the increasing levels of cybercrime imply the need for greater awareness of criminal activities and consequences, including prosecuting individuals who plan and carry out cyberattacks. However, there is a shrinking gap between what is technically possible and what is socially acceptable, and for many techies hacking is a game.[11]

After a power outage during Hurricane Sandy in 2012 caused a blackout throughout Manhattan. While critical infrastructure has traditionally been deemed off-limits, the potential for future attacks is increasingly likely. (Reuters)

In a 2014 CNAS report, Richard Danzig wrote that the "beginning of wisdom about cyber systems is to understand that vulnerability is inherent in the technology."[12] There are four key types of cyber vulnerabilities: flaws in software, weaknesses in components procured through the global supply chain, errors caused by humans, and an over-reliance on private-sector platforms. Over time a good deal of existing software has proved badly flawed, riddled with defects that can be exploited.

Part of the challenge is the nature of cyberspace itself. Cyber has its own space that transcends other areas. With cyber it can sometimes be difficult to identify the cause of a failure, and thus one has to be careful with using the term "cyberattack" since it has certain connotations and ramifications. This attack uncertainty characteristic is a genuine policy quandary, as the cross-border nature of cyberattacks only complicates the challenge of attribution and response. Because of the multitude of vulnerabilities available to be exploited, that offense has an advantage over defense. To riff off an axiom usually associated with terrorism, the attacker only needs to be right once; the defense needs to be right every time.

Imagining a Major Cyber Crisis

Many experts view cyber espionage and theft of intellectual property as a greater immediate threat to the national security of the United States, Japan, and other allies than that of large, catastrophic cyberattacks. The future could well hold the potential for catastrophic attacks on interconnected critical infrastructure, however, and planning for them may be as important as for any similar disaster.

There are three sets of actors that have the potential to implement a cyber 9/11. The first is a terrorist group, though this is highly unlikely since such groups typically lack the level of target knowledge and technical sophistication to carry out a critical infrastructure attack. If they did implement such an attack it would likely be as a proxy with the support of a nation-state, or through the use of critical-infrastructure insiders. The second possible threat is from North Korea or another third-tier actor that in a crisis goes beyond what it has done in the past and threatens key assets, such as the financial system or electrical grid. However, the United States is more worried about other types of threats from such actors, including the use of chemical or nuclear weapons. The third threat is from nation-states with first-tier cyber capabilities such as China or Russia, which might use cyberattacks as a way to gain a strategic advantage. Rogue nation-states such as North Korea or Iran could also pose similar threats, although most states have better ways to go about pursuing their interests.

There is international consensus that critical infrastructure is off-limits and should never be attacked. But the world may be approaching a crisis point, and future attacks may be increasingly likely if not inevitable. Critical infrastructure is generally considered off-limits, but all cyber-sophisticated countries are actively doing intelligence preparation of the battle space (IPB) that includes gathering information on others' critical infrastructure systems and possibly even implanting logic bombs into those systems.

Several interesting and plausible cyber crisis scenarios can be posited that would involve a response from the United States, Japan, and other allies. These include potential tensions and conflict in the East China Sea, an issue that is analyzed in the next section of this report. Another scenario involves Taiwan, as the January election of the main opposition candidate, Tsai Ing-wen of the Democratic Progressive Party, raises new concerns about whether cross-strait relations might become a renewed source of regional- and major-power tensions. Cyber might be used broadly to disrupt or degrade Japanese or Taiwanese networks and slow the ability of the United States to offer an effective or timely response. Furthermore, there could be more targeted cyberattacks aimed at the supervisory control and data acquisition (SCADA) systems that control the critical infrastructure that supports military operations, including electrical power. Likewise, adversaries might attempt to combine electronic and physical attacks or launch a major strike against the U.S. electrical grid. There is concern about the convergence of cyber and physical systems and a possible catastrophic attack involving the emerging Internet of Things (IoT). Finally, there is also concern, at least in Japan, that a major attack could be launched during the 2020 Tokyo Olympic and Paralympic Games.

So far there has not been an attack with significant harm to critical infrastructure. However, past performance is not necessarily an indicator of future threat. The cyberattack against Sony was a significant wake-up call. And officials are beginning to take seriously questions such as, "What would we do if there is an attack on Wall Street?"

Preparing for Cyber Scenarios

The question is not whether to do more to prevent cyber disasters but where to place priorities and on what scale of investment in time and money. Most argue for a focus on better cyber defense, reduction in cyber dependencies, and the development and use of technology, policy, law, organizations, strategy, and response doctrine to mitigate cyber risk. In particular, there is a need for the private sector to play a larger and more effective role and to find ways to improve public-private information-sharing. Of course, this is easier said than done, especially given the difficult debate already taking place over encryption. While some in the government want the private sector to ensure data access to law enforcement, most of the private sector argues that such industrial back doors would only shift business to non-U.S. companies.

Focus and Dependence Reduction: One prescriptive solution is to see the world of cyber vulnerabilities in terms of *risks* and not *threats*. This implies the willing use of scarce resources to protect what is needed most and the willingness to incur losses in some places. However, unlike in the nuclear era, cyber risk is not completely understood, partly because it is constantly changing. Government officials are acutely aware about the cyber dependence of military and critical civilian infrastructure alike, and both the United States and Japan need to consider ways to reduce these dependencies or mitigate their effects.

Technology: Curiously, when it comes to improving cybersecurity and averting major disaster, few see technology as the main panacea – but several important technological steps could be taken to mitigate those risks. To be sure, the adoption of automated machine-to-machine standards, including Structured Threat Information Expression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII), might speed the sharing of vulnerability and threat information. Furthermore, a key prescription to reducing risk might be to implement third-generation cyber defense predictive and behavioral capabilities. For example, the entertainment community is able to very accurately predict opening-weekend box office revenue and the dollar impact that a Sony-like cyberattack can have on potential audience behavior. However, there is no technological "silver bullet" that will solve the cyber problem. Instead, there needs to be a comprehensive assessment of doctrine, strategy, law, and organization.

Law and Policy: Much of the policy and law risk-reduction discussion involved ways to improve cyber-threat and incident information-sharing between the public and private sectors. Most critical infrastructure in both the United States and Japan is owned by the private sector, and there is a significant gap in proactive information-sharing between the public and private sectors that needs to be bridged. But information-sharing between the private sector and government is complicated. From an industry perspective, it is not clear what the government brings to the table. Yet there are legal and policy tools that can be used to spur public-private action; these include tax rebates, regulation, insurance and liability protection, and class-action litigation.

Organization and Strategy: The Department of Defense (DoD) has made significant progress in implementing *The DoD Cyber Strategy*[13] (April 2015). It has organized its cyber command and built out a cyber mission force (CMF) of 6,200 military, civilian, and contractor support personnel. The strategy also clarifies the functional relationship among federal agencies (including DoD and the Department of Homeland Security) on cyber activities, looking at creating a whole-of-government approach to dealing with cyber emergencies. Japan's NISC has both policy and operational aspects. The operations center monitors Japanese government networks and also is responsible for information-sharing with critical infrastructure sectors. Japan's September 2015 *Cybersecurity Strategy* emphasizes the protection of cyber-physical systems (including IoT systems), with a special focus on reducing the risk of a major cyber-related event during the Tokyo 2020 Olympic and Paralympic Games.

Response Doctrine: There is a general consensus that thresholds and rules of engagement are necessary to create firebreaks from escalation. Further, there is general agreement that most countries with cyber capabilities understand that restraints are necessary and that there are implicit norms on what lines should not be crossed. However, questions remain about what types of cyberattacks constitute a use of force and could potentially trigger the right to self defense.

The United States at least needs to establish parameters for what is acceptable and what is not. This includes thresholds for state-versus-state cyberattacks and state-versus-private-entity cyberattacks. When thresholds are understood and then violated, the United States should push back using sanctions or other

means. Japan is still in early stages of threshold debate, but that response would likely depend on the level of damage and the perceived need for self defense. Laws legitimize responses, including what the American Bar Association calls "comprehensive incident response," more commonly referred to as "hacking back."[14] However, cyber response to a cyberattack is not always effective, and sanctions or other types of response might be more efficient. This is why DoD seeks in its cyber strategy to develop a full spectrum of response options.

Attribution and Deterrence: Deterrence plays a key role in an adversary's calculus, and developing a high level of attribution is key to deterrence success. However, there appears to be a deterrence deficit. For example, when dealing with the Chinese, cyber actions appear to lack credibility with Beijing. To be taken more seriously, the United States and its allies may need to use more economic power to change behavior and bring cost-benefit analysis into the debate. The April 2015 executive order authorizing targeted sanctions can change the Chinese cost-benefit calculation and, subsequently, Chinese behavior, but only if it is used. Unfortunately, reports that the Obama administration might apply additional cyber sanctions have not come to fruition.

While attribution is difficult, most experts believe it is improving. There have been significant advances in private-sector intelligence, technology, and the use of open-source imagery, and this is enabling private firms such as Mandiant (in the United States) and Kaspersky Lab (Russia) to do high levels of attribution. However, many believe that the United States needs to be more transparent about its attribution capabilities if it is to parlay those improvements into stronger deterrence against cyberattack.

Role of the Private Sector: Throughout the discussion, regular references were made to the importance of private-sector companies as the primary targets and responders to cyberattacks. Private companies often have more sophisticated tools and higher levels of technical expertise versus their government counterparts. However, the level of cybersecurity and information-sharing implemented by private firms is a business decision. Corporate executives and boards want to know if they are overspending, underspending, or spending on the wrong stuff. They require a cost-benefit analysis and clear return on investment in order to be willing to make cybersecurity investments, and a business case or market motivation for participating in information-sharing. Companies are worried about liability and regulatory issues and want immunity when sharing information with the government. Furthermore, there is a growing distrust in government with regard to how far companies will cooperate; the heated debate over encryption is a case in point.

ENCRYPTION DEBATE

Unbreakable encryption is another potential obstacle to an effective law-enforcement response. In the wake of the Edward Snowden leaks, leading technology companies have concluded that "[t]he solution to government surveillance is to encrypt everything." Since then, companies have significantly expanded the use of encryption in their products – both with respect to "data at rest" on mobile devices and "data in motion" as it travels across the Internet.

Increasingly, the companies themselves often do not retain a key to the encrypted devices or messages. This means that even if a judge approves a search warrant the companies may be physically unable to comply.

In the United States, Apple is now battling the Department of Justice over whether Apple can be forced to help the government penetrate an encrypted iPhone used by one of the San Bernardino terrorists. Overseas, the United Kingdom, France, and China have passed or are considering legislation that would require companies to break encryption for law enforcement. Technology companies argue that "backdoors" in encryption will weaken cybersecurity for all users. Law enforcement counters that many companies' business models require them to retain access to unencrypted data – Google, for instance, scans the contents of Gmail messages in order to target advertising – and that these business models are widely considered secure.

Whatever the resolution, this global debate will have significant implications both for cybersecurity and for law enforcement's ability to respond to national-security threats, including cyber threats.

The key recommendations to strengthen states' ability to manage future cyber-related crises primarily focus on conducting cyber exercises and developing international partnerships and norms.

The United States and Japan need to think systematically and learn from previous disasters such as Fukushima. There are at least two key lessons learned from 9/11 and Hurricane Katrina that can be applied to managing future cyber-related crises. The first is the importance of professional relationships in managing a crisis. Counterparts who know each other and have worked together through long-term interagency or alliance relationships are better able to collaborate under crisis conditions. The second lesson is the importance of exercises in preparing for potential catastrophic events. Exercising for catastrophic cyber events means the participants need to break the system and figure out what went wrong. The United States and its allies need country-to-country, sector-to-sector, and company-to-company exercises to stay ahead of the curve. Cyber realism should be injected into all military exercises, and recommendations to do so were made for bilateral exercises between Japan and the United States in preparation for the 2020 Olympic Games. Such exercises should include simulations of cyberattacks on critical infrastructures, such as the electrical grid, and involve both public- and private-sector leadership.

An actual attack on Japan, even one that was difficult to attribute, using cyber and terrorist attacks, could sow fear nationwide and change the public confidence in government and the alliance.

Another series of recommendations involved the establishment of international cyber partnerships and norms. Cyber provides a new area for alliance cooperation. First, as the 2015 U.S.-Japan Defense Guidelines highlight, there is a clear recognition of the importance of additional cyber cooperation between the United States and Japan. This includes establishing specific cyber guidelines and commitments in the policy area and identifying ways to better cooperate in cyber operations. For instance, there is significant scope for considering a new command and control mechanism, as well as a need for continuous guideline updates after U.S.-Japanese consultation. Second, the United States and Japan (as well as others) need to establish a better framework for alliance sharing of information and technology. The United States has been hesitant to share its best cyber technologies with allies even while there is a broad-based recognition of the need to rely increasingly on international partners. More generally, the United States also needs to establish cyber norms and advance the development of international law dealing with cyberspace, although one obstacle is that most cyberattacks are aimed at the private sector rather than governments. Even so, more can be done through bilateral and multilateral agreements.

Resilience is a key theme of both the 2015 *DoD Cyber Strategy* and the Japanese government's 2015 *Cybersecurity Strategy*. There is ample scope and need for greater leadership from both government and society when it comes to cybersecurity. Companies must understand that this is a national security issue, and the nation needs more political will to look at the cyberthreat more conscientiously. But it is vital also to think through software design and make it more resilient. Furthermore, there needs to be more incentive for the private sector to assure the resiliency of its critical systems. Ultimately, it is difficult to maneuver in cyberspace, and the United States and its allies need better models for how to organize and respond as an international community to cyber-related disasters.

04 CHAPTER

Humanitarian and Military Contingencies in Northeast Asia

Humanitarian and Military Contingencies in Northeast Asia

Crisis managers need to consider how humanitarian and military contingencies could pose serious challenges to homeland peace and security. A deteriorating security environment in Northeast Asia and around Japan includes a range of risks arising from the Korean Peninsula, as well as potential maritime tensions with China that might reverberate within Japan's home islands and through them to Japan's ally the United States. Such contingencies are important to consider in part because they overcome the obstacles to bureaucratic politics. That is to say, examining crossover conflict and humanitarian events that could spill over onto homeland security avoids the pitfall of creating more monochromatic analysis for either law enforcement or the military, but not for the whole of government or whole of society.

The Korean Peninsula

The Korean Peninsula is of vital interest to Japan and the U.S.-Japan alliance. In the aftermath of a fourth nuclear test in January 2016, perhaps the most plausible source of conflict might entail the use or threatened use of missiles that are potentially nuclear-armed against Japan. Even a threat to bomb a U.S. base inside Japan would rapidly escalate tensions and put civil society on edge. An actual attack on Japan, even one that was difficult to attribute, using cyber and terrorist attacks, could sow fear nationwide and change the public confidence in government and the alliance. A more effective nuclear deterrence strategy on the part of North Korea would be to develop land-based solid fuel systems capable of attacking Japan.

But let us place this possible scenario in context with a discussion of North Korean motives for its nuclear weapons program. Generally, there are three uses for Pyongyang: maintaining peacetime coercion, preventing forcible reunification, and preventing all-out war. With respect to peacetime coercive use, North Korea has historically resorted to provocations to undermine the U.S.-South Korean alliance and U.S. regional credibility. The United States and its allies in Northeast Asia can neither afford to be intimidated by every North Korean capability, nor to take them too lightly. But while nation-

A famine in North Korea could result in a humanitarian crisis with the potential to lead to regional conflict. (AP/Kathy Zellweger)

The United States, Japan, and South Korea are ill-prepared for the case of a massive outflow of refugees from North Korea, not unlike the migrant and refugee crisis overwhelming Europe.

al security officials in Seoul, Washington, and Tokyo seek to find the right balance, public opinion might shift quickly out of fear or uncertainty. For instance, if the U.S. forces based in Japan were to respond to North Korea's threat, then Japan would instantly become a target. As one Japanese strategist asked, under those circumstances, would most Japanese be willing to "trade Tokyo for Seoul"? Of course, it is not just nuclear weapons that might instigate a crisis. In the context of a discussion on crisis management, the main takeaway may be to consider local civil order and national psychology in thinking through different possible scenarios. Similarly, information-sharing on missile defense, extended deterrence, and contingency plans among the three countries becomes essential for finding a way through possible crises.

Sudden change on the peninsula as a result of civil unrest or the collapse of the Kim family dynasty could either trigger or result from a massive humanitarian crisis. The exact triggers that would cause a societal breakdown are unknown, but the situation is certainly potentially unstable inside North Korean society. Moreover, even a seemingly benign development leading to Korean unification might unleash powerful unintended consequences that could create regional conflict or humanitarian crisis. Just as information-sharing is important for potential missile and nuclear threats, so, too, is it vital for helping policymakers to enact operational mechanisms ahead of time to collaborate and coordinate an allied response in the initial hours after a collapse. Efforts to reverse the previous decline in Seoul-Tokyo relations, including the positive steps taken by President Park Geun-hye and Prime Minister Shinzo Abe in December 2015, provide a foundation on which to proceed in 2016 and beyond. The United States can continue to play an encouraging role in developing practical progress that meets the interests of all parties.

Humanitarian and Refugee Crises

A Famine or Health Crisis: Humanitarian and refugee crises are also possible on the Korean Peninsula, and these less kinetic threats to stability could well bedevil crisis managers. The United States lacks firsthand experience and consequent understanding of the connection between famines and geopolitical calculations. In some historical circumstances, famine is not the result of failed policy, but rather of intentional policies designed to facilitate regime objectives, which instead point to an enduring regime rather than an unstable one (such as Cambodia, and Stalin's likely targeted famine against the Ukrainian population). However, the Chinese famine under Mao Zedong was certainly unintentional, and in North Korea one major consideration (and part of the evidence suggesting that any famine there is indeed unintentional) is that North Korea has the largest land army in the world as a proportion of its population (47 percent). Thus, a significant portion of the military force would undoubtedly have relatives who would be affected by the famine. A North Korean famine would, however, likely disproportionately affect those without political connections to provide access to critical food supplies, but the overall effects would certainly be too large to be intentional.

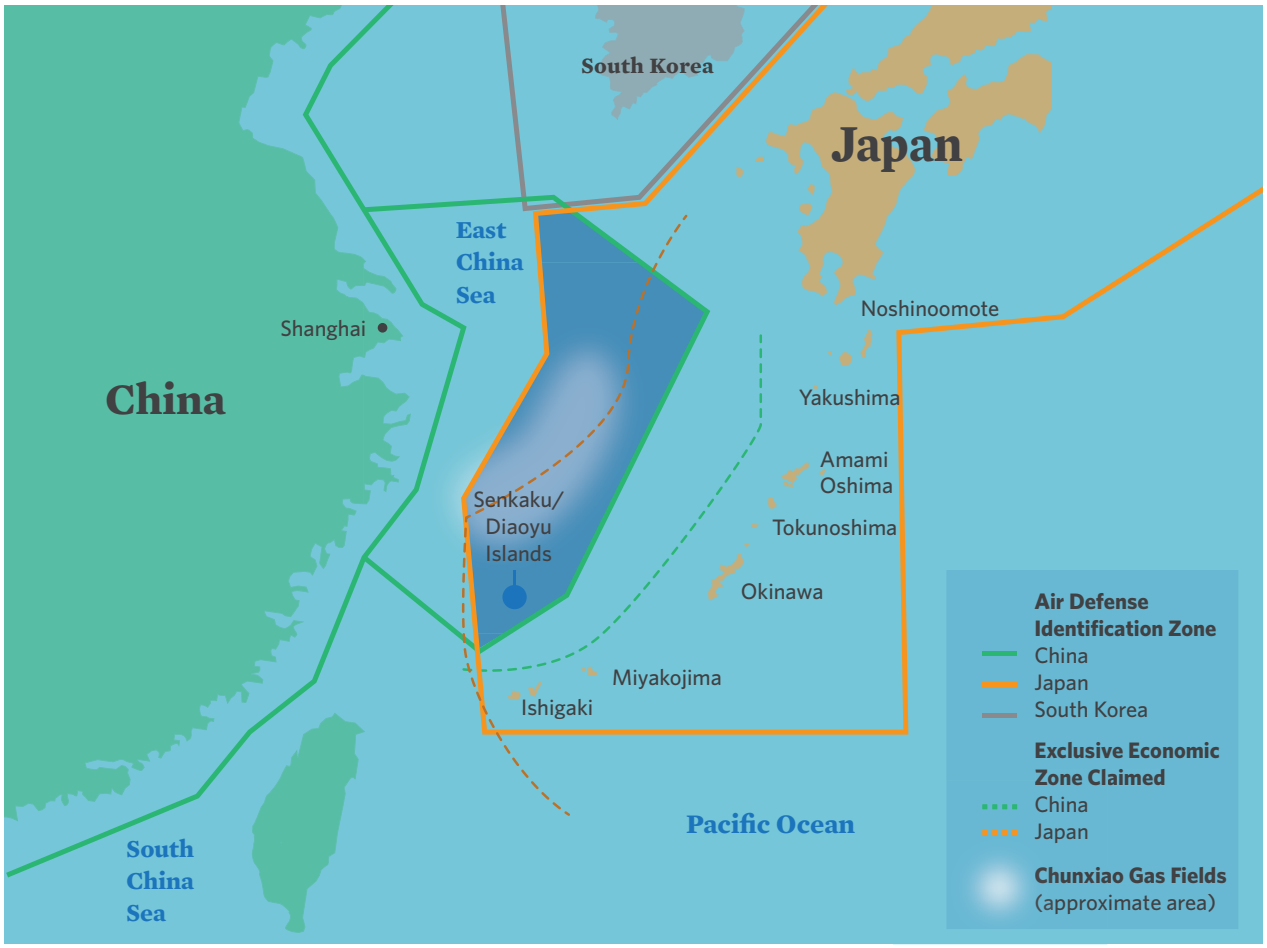
A new agricultural or health crisis could precipitate collapse of the regime in North Korea. Famine is not just absence of food; it is about access to food. Famines are not events, but processes.

A new agricultural or health crisis could precipitate collapse of the regime in North Korea. Famine is not just absence of food; it is about access to food. Famines are not events, but processes (they take place over time; it took two years to build up to the crisis in 1997; warning signs can be observed). Food production is a fragile system; an agricultural problem could precipitate a food security issue. Famines are frequently accompanied by large-scale population movements. There is evidence of a coup plot in 1994, likely precipitated by huge death rates in the northeast, suggesting that famines could be a catalyst for regime change. The United States, South Korea, Japan, and others should be tracking the food situation and population movement as indicators of possible regime stability issues (direct relation between food security and provocative actions).

A Refugee Crisis: The fear of being inundated with refugees remains one reason why China and other neighbors fear instability in North Korea. Yet refugees from North Korea would be unlikely to overrun China, Japan, and South Korea given existing border controls. In addition, both the U.S.-Korean alliance and the international community could implement specific mitigation efforts within North Korea to keep the majority of the population from leaving while also helping to build it back up. South Korea is legally obligated to take refugees, but it may wish to manage migration, such as through camps/criteria for determining entry and limiting the overall number entering at a time. In any event, there are barriers to refugee flow: China would likely restrict illegal refugees and establish camps or zones; this would also enable a Chinese military presence in the North; the heavily mined demilitarized zone (DMZ) to the south, and possible South Korean military action, would limit refugees streaming in that direction; North Koreans may stay put if resources are provided; and generally people escape to safer parts of their own country and become internally displaced persons rather than flee to a different country.

The only factors likely to spark a mass exodus in the event of a governmental collapse would be unmitigated violence, all-out civil war, or widespread starvation. To prevent a refugee exodus in the event of a crisis, the United States and its allies would need to undertake efforts immediately to assist North Koreans inside the country and avoid protracted displacement or long-standing camps that become breeding grounds for armed action. Support from the international development community and investment from other countries would also be needed. Focusing on providing assistance within North Korea requires coordinated planning by both NGOs and outside governments. North Korea is vulnerable to floods and the effects of climate change, but NGOs can map out aid distribution and design mitigation efforts. Additionally, any contingency planning should involve human rights groups. North Korea holds well over 100,000 political prisoners, which the government has ordered to be exterminated in the event of a major crisis. The international community has an obligation to rescue these prisoners/abductees, and planning for that should be included in any crisis response. The Kim family is expected to flee the

Overlapping Jurisdictions in the East China Sea



An insight from the Evermay Dialogue is that while there is growing emphasis on potential conflict in the East China Sea, the more important consideration may be alliance coordination over a contested peacetime competition, as Japan is increasingly concerned about overlapping Air Defense Identification Zones with China, for example. (Sources: Wire agencies, BBC, Yonhap News, and Réseau International.)

country along with key leaders fearing reprisals; preparations for a North Korean collapse need to include plans for bringing them to justice. The United Nations Development Assistance Framework offers a general approach that is valuable in this regard. By including human rights goals into this framework as it negotiates its on-the-ground country assistance program, the United Nations can describe the priorities and actions necessary to achieve stability and development.[15]

From a Japanese planning perspective, there is a good possibility that North Korean boat people could provide a pretext for multinational navy-to-navy cooperation among the United States, South Korea, and Japan. But Japan is not concerned with large numbers of refugees in the early stages of a crisis fleeing to Japan because it is much easier to get to South Korea or China. However, the Japanese *are* more concerned with long-term refugees and immigrants. Some 120,000 North Koreans may have relatives in Japan or some connection to Japan from the orchestrated abduction programs stemming from the 1960s. But a better way of helping these people is by building up North Korea from the inside. From the U.S. perspective, the question is whether and to what extent Japan will be proactive in responding before and during a Korean crisis. Even a few refugees could cause a public communications issue in Japan, sowing confusion and preventing Japan from marshaling the resources to act together with its allies.

Military Crises

Military crises in Northeast Asia center on North Korean scenarios but also increasingly on the possibility of tensions escalating in the East China Sea with China. Regarding Korea, the United States has focused on the prospect of a North Korean attack, a provocation that escalates out of control, or potential civil war or regime collapse. But the United States and South Korea have done more planning than preparation, and the planning with Japan lags what is needed. On top of traditional planning, more must be done to keep pace with changing threats in cyberspace. At the same time, Japan should consider liaisons to U.S. military commands.[16] It is critical to improve Japanese-South Korean relations for advancing intelligence-sharing, training, military interoperability, and anti-submarine warfare capabilities, among other dimensions of military readiness. To mitigate a variety of risks, the allies should implement better tripartite (U.S./Japan/South Korea) coordination, larger-scale involvement by Japan in Foal Eagle exercises, and joint planning processes. To better prepare for a North Korean crisis scenario, Japan and the United States need to resolve differences over the use of U.S. bases and entice Japan into true collective self-defense commitments. The United States should help Japan develop state-of-emergency preparations and develop resistance to North Korean propaganda that constantly threatens Japan because of its hosting of U.S. bases.

The United States also must prepare for possible evacuation of U.S. citizens in South Korea (currently more than 100,000 Americans). Evacuation sends a strong political signal, and with the 7th Fleet sure to be heavily involved, timing must be carefully and appropriately determined.

East China Sea Contingencies: One insight to emerge from the Evermay Dialogue is that despite the increasing focus on potential conflict in the East China Sea over the Senkaku Islands (which the Chinese call the Diaoyutai), the more important consideration may be alliance coordination over a contested peacetime competition. To be sure, Japan has become increasingly concerned about the defense of its southwest island chain, overlapping Air Defense Identification Zones with China, and growing Chinese naval and law-enforcement activity in the East China Sea. The reaffirmation of a strong alliance with the United States reinforces deterrence against aggression. But China's nibbling or salami-slicing strategy has not totally eased a simmering crisis from growing. China prefers the use of nonlethal force and pressure to achieve objectives and control engagements.

This is not to say the risk of conflict in the East China Sea is trivial. There are many local incidents possible that could trigger escalation, particularly if one incorporates the potential of unplanned and brash actions on the part of young commanding officers on scene in any situation. Washington needs to develop nonlethal activity response mechanisms, shape public policy and mass opinion to keep nationalism from taking over, encourage the status quo of the Senkakus so as not to trigger a Chinese response, and consider that a North Korean provocation might be actions taken by proxy on behalf of China.

The East China Sea is very important to the United States and Japan than the South China Sea due to significant consequences, including the potential for direct conflict – such as over Taiwan or the Senkakus. These dynamics are exacerbated by the fact that the East China Sea constitutes home waters for both Japan and China, with both the People's Liberation Army Navy (PLAN) and the Japan Maritime Self-Defense Force (JMSDF) continually operating in those waters. Moreover, the East China Sea region includes the only routes to get to China's six largest ports, thus holding both great strategic and economic significance. In addition, the most convenient way for China to get to the high seas is to cross Japanese waters, ensuring constant interaction between PLAN and JMSDF. The East China Sea consequently sees large amounts of submarine and air traffic, increasing the possibility of midair collision or potentially violent encounters.

Though Taiwan has been on the geopolitical back burner for the past eight years, there is new potential for cross-strait flare-ups if the newly elected Democratic Progressive Party government makes moves toward Taiwanese independence. The United States and Japan need to re-engage in serious planning for this contingency; though not the most likely, it would certainly constitute the most serious such contingency.

In the Senkakus, Japan would have the lead in any potential contingency, but the United States would play key support roles. Adequate contingency planning will need to resolve multiple outstanding stumbling blocks to smooth U.S.-Japan response integration. There is disagreement between the two countries as to what constitutes Japanese sovereign airspace, current combined U.S.-Japan planning is immature, and such integration should be developed further based on NATO or other models.

A similarly critical concern will be avoiding unnecessary escalation in the event of contingencies with China. Managing a crisis will necessarily involve effective engagement with China while simultaneously determining how willing the United States and Japan are to deter escalation. The two allies should not consider triggers or provocations in such a crisis as independent events, but rather evaluate them in the context of the three countries' relations and histories. The United States and Japan will have to determine how to differentiate between localized incidents and indicators of broader Chinese plans, how to evaluate Chinese actions at different scales, and how China continues to change the geopolitical status quo without overt war. In the latter case, the more Beijing does so, the more it is achieving its objectives.

Moreover, the United States and Japan should consider the different pitfalls and threats that are still inherent in both explicitly crisis and noncrisis scenarios. A military incident, or overt crisis, could arise out of a collision of submarines or aircraft, quickly and without notice. The United States should be as concerned, however, with *non*crisis scenarios. If peacetime competition continues apace, it is more likely that China would prevail over time than if its interests and those of the United States and Japan came into conflict in an overt crisis. Examples of such peacetime coercion include Chinese "rights protection" operations, including incursions into Japanese territorial waters by or alongside ostensibly private commercial vessels. Japan and the United States need to devote more time and effort to these kinds of noncrisis scenarios, particularly since they are not currently part of the conversation. Japanese air forces are overstretched as a result of scrambling so many sorties in response to Chinese incursions and will need to determine more efficient means of confronting them. The two allies should also engage in more joint patrols and intelligence-gathering operations, even though doing so in the South China Sea may introduce new hazards for which the alliance must be fully prepared. Finally, the United States and Japan should seek to develop a long-term road map to encourage China to eventually accept Japanese sovereignty over Senkakus.

Alliance Actions

To better prepare for crisis management and resilience in the face of myriad humanitarian and military contingencies in Northeast Asia, there are a number of steps that the United States and Japan should consider.

First, each country should separately and then together create a more whole-of-government approach to planning for crises. Natural disasters have highlighted response and recovery capabilities, and the SDF have become trained to react to non-military crises. Strategic communications are also important, not least with respect to a large regional power such as China. There is also a need for more systematic means of strategic communications to connect strategic and operational levels of collaboration. Finally, tactical actions relate to strategic messages; therefore, even individual captains affect national objectives.

Second, alliance integration needs to occur in command and control and at an operational level. Each ally should step up consultation over roles and mission-sharing, such as clearly identifying "spear" and "shield" forces in a strategic buildup and how they would work together. This might be done more easily by a possible joint U.S.-Japan combatant command. The United States should also welcome Japan into a Five Eye-type arrangement for intelligence-sharing. This might begin with routine video teleconferences at the director or assistant secretary level to coordinate contingency

An official forum for outlining a new strategic framework under changing strategic circumstances would be able to build on existing levels and areas of cooperation, while also indicating future areas for potential alliance growth.

planning. The two nations can also implement an internship-level arrangement to learn how each force operates. Additionally, Japanese SDF should increasingly use U.S. bases in Japan during exercises. In short, the alliance needs to be integrated at a command-and-control and operational level.

Third, the alliance needs more red-teaming and war-gaming scenario planning, including with an annual major war game. Scenario planning is a vital part of the military planning process, and it needs to be part of a larger alliance crisis management preparatory process. Leaders across governments and societies need to be exposed to new processes and scenarios while confronting uncomfortable situations. They need to walk through the various possibilities, with an objective of addressing each plausible scenario while also including other allies and partners as appropriate. For instance, the United States enjoys a parallel military relationship with Japan and South Korea, but not Taiwan because of political sensitivity.

Conclusion: 10 Critical Steps Toward an Alliance Action Plan

The U.S. -Japan alliance should initiate a comprehensive effort to advance crisis management. It is commonplace to note that no single country can manage the most important international security challenges. A corollary to this presumption is that no one country can manage major natural disasters that affect the homeland. In the age of electricity and societal connectivity, the systems that sustain civilization have never been more vulnerable. Both natural and human-made crises threaten the resiliency of advanced modern democracies such as the United States and Japan. As U.S.-Japan alliance managers contemplate taking the alliance to a higher degree of integration, both bilaterally and with other regional partners due to changing strategic circumstances, there is a gap between alliance planning and full-spectrum crisis management. Furthermore, as the allies plan to step up integration with respect to command and control, situational awareness, and operations, there is a natural overlap and mutual reinforcement between alliance national and homeland security cooperation, and humanitarian assistance and disaster relief. Over the next several years, Washington and Tokyo should leverage the economies of this overlap and take concrete steps to strengthen the strategic resilience of each country when confronting a variety of potential crisis scenarios.

Even a preliminary bilateral crisis management net assessment depends upon good data. In fact, the United States and Japan have plenty of data regarding past crises, but the information is held separately, in dispa-

> ***Counterparts who know each other and have worked together through long-term interagency or alliance relationships are much better able to collaborate under crisis conditions.***

rate forms, and has never been brought together in any coherent way. Collecting, normalizing, and consolidating this data is no easy task, but any organized approach to considering the challenges and requirements of future crisis management will depend upon comparing what has happened in the past with what might happen in the future. This data-driven approach is how to best consider risk, identify shortfalls and overlaps, make tradeoffs, and set priorities among competing crisis management requirements.

Accordingly, officials in the United States and Japan need to take more initiative to advance joint solutions and systems that support the strengthening of strategic resilience on both sides of the Pacific. Faced with myriad potential major homeland hazards ranging from natural disasters and terrorism to cyber and humanitarian and military contingency, decisionmakers need to apply renewed urgency and focus on the measures most likely to stave off catastrophic national failure and buy down risk on a wide array of future threats. The measures described in this report are selected from the extensive in-depth expert dialogue regarding both past experience and current crisis management planning that was chartered by this project. Above all else, newfound energy can be found through tightening the crisis management aspect of the already successful security alliance. But the lessons and insights of this collaboration can apply equally to other countries, especially as the United States and Japan seek to build closer security cooperation with key allies such as South Korea or to assemble a loose network of Indo-Pacific countries through building connectivity in the form of a common operating picture.

1. Initiate an official U.S.-Japan working group on strategic resilience. Officials in Washington and Tokyo should adopt a process to create a comprehensive strategic resilience plan of action. As a first step, an official discussion mirroring the unofficial Evermay Dialogue might underscore the benefits of adding an alliance "catastrophic health insurance" plan on top of existing national capabilities. Furthermore, an official forum for outlining a new strategic framework under changing strategic circumstances would be able to build on existing levels and areas of cooperation, while also indicating future areas for potential alliance growth. There are, after all, numerous reasons to adopt an alliance approach to strategic resilience. First, a comparative approach can help each ally identify new ideas and approaches to managing crises in innovative ways. Second, an official alliance forum for crisis management can expand U.S.-Japan cooperation, bringing together more and different actors; in so doing, there might be a growing appreciation that security is not simply a narrow military construct but the provenance of a host of national, local, and nongovernmental actors. Third, serious consideration of alliance scenarios and potential shortfalls in capacity, organization, and imagination will stimulate thinking about necessary new capabilities, institutions, and protocols. Fourth, allies can take advantage of an increasingly operational alliance to extend capabilities useful for a range of homeland security challenges, and vice versa. In particular, there is nothing quite like a real-world crisis, such as during the 3/11 triple disaster in Japan, to transform stressors into stronger alliance bonds. Fifth, effective information-sharing at all stages will be a bedrock requirement. Even without excessive intrusion into the internal affairs of the other ally, each country can identify potential ways to provide the other with material and other assistance in the midst of a wider range of contingencies. Finally, as Operation Tomodachi demonstrated, organizing for effective command and control must be thoughtful and forehanded in order to maximize the effectiveness of national and alliance crisis response capabilities.

2. Initiate an annual U.S.-Japan alliance crisis management "future data" exercise modeled on defense war-game experience. Such exercises are meant to be not necessarily prescriptive, but provocative and suggestive. This technique is also invaluable in establishing mutual understanding where fundamental experiences and thinking among participants may be somewhat different. To move from planning to action, the alliance should not wait for a detailed plan of action to be agreed upon before starting more active cooperation on crisis management. Toward that end, the alliance could initiate an annual exercise or simulation modeled after successful defense gaming exercises, including those conducted at the U.S. Naval War College and other gaming centers. But these crisis management exercises would be centered on scenarios affecting the homeland and engaging a multitude of governmental and nongovernmental actors. Each year could focus on a different hazard and scenario to cover far more than the canonical military scenarios that receive most attention with the national security establishments of the United States and Japan. These exercises might run the gamut from simple tabletop discussions to the extensive use of advanced models and simulations. Advances in big data, artificial intelligence, and cyber simulations will allow for creative alliance simulations on an entirely higher level of sophistication than those conducted in the past, even at a national level.

Together, the U.S.-Japan alliance can share innovative ways for interconnecting complex government at all levels as well as incorporating the private sector and civil society.

The United States and Japan can think systematically about and learn from previous disasters such as Fukushima. For instance, there are at least two key lessons learned from the 9/11 attacks and Hurricane Katrina that can be applied to managing future cyber-related crises. The first is the importance of professional relationships in managing crisis. Counterparts who know each other and have worked together through long-term interagency or alliance relationships are much better able to collaborate under crisis condi-

tions. The second lesson is the importance of exercises in preparing for potential catastrophic events. Exercising for catastrophic cyber events means working to failure in a controlled laboratory, workshop, or field environment in order to simulate the system breaking down and then figuring out what went wrong in order to establish solutions for what can be fixed in advance, and the ability to work through and restore failures that cannot be prevented. Country-country, sector-sector, and company-company exercises are needed to stay ahead of the curve. Cyber realism must be injected into all military exercises, and recommendations were made for bilateral exercises by Japan and the United States in preparation for the 2020 Olympic Games. Such exercises should include simulations of cyberattacks on critical infrastructures, such as the electrical grid, and involve both public- and private-sector leadership.

There should be no surprises regarding who will be responsible, because, like the aftershock of an earthquake, a tragedy can reassert itself unexpectedly at a moment's notice.

3. Create an alliance series of authoritative after-action reports. This will entail collecting data from major crises confronted by each or both nations. Likewise, both Japan and the United States need to do a better job of collecting data when crises occur, and then scrupulously internalizing the results of after-action reports. While there may be a willingness to perform a truthful after-action reporting, actually dissecting the findings and recommendations is an undertaking in itself. The United States and Japan should share their experiences with each other and expose their vulnerabilities. For Japan, 3/11 made the government realize and expose its vulnerabilities. Both the United States and Japan will benefit from the findings of the incident study, so the two countries should cooperate and engage in it together.

4. Create a training program on strategic communications for national and local governmental officials, first responders, and appropriate private-sector and civil-society actors likely to find themselves on the front lines of reporting information in different crises. Effective strategic communication is essential in any crisis and includes both technical and organizational solutions. Technically, this means developing the capability for communicating past the failure of established infrastructures, providing for civil and military power and connectivity. Extensive experience and continuing experimentation resources can be drawn upon to consider new solutions and additional requirements. Organizationally, those who will communicate will have to be selected in advance and prepared for their duties. This will include having the organizations available and able to provide relevant, tailored, and timely information to communicate; sufficient personnel to communicate around the clock; and ways to communicate to a broad variety of audiences (including opponents and non-state actors). These technical and organizational effects are crucial to crisis management: As John F. Kennedy during the Cuban missile crisis and George W. Bush during Hurricane Katrina discovered, official communications can either ameliorate or exacerbate a crisis, and the political and strategic effects can be serious and long-lasting.

5. Identify ways to break down some of the highest hurdles to achieving a unity of effort and effect. Successful crisis management is like conducting an orchestra: There is no better approach than practice, practice, practice, and this requires all of the musicians on stage. For instance, this would mean bringing in more science advisors into planning and implementation, and successfully integrating government, corporate, and academic policy and technical experts with the strategy and resource planners who are needed to fashion a response to nuclear disasters and cyberattacks, respectively. Together, the U.S.-Japan alliance can share innovative ways for interconnecting complex government at all levels as well as incorporating the private sector and civil society. Doing so is good governance and could be the difference between crisis and disaster when the time comes.

6. Consider actionable ways the alliance can translate shared best practices and requirements into improved disaster preparedness. This would include: understanding critical infrastructure; developing a new approach to risk assessment, safety standards, and redundancy before critical infrastructure and other systems are built or overhauled, in order to design out critical design flaws and single points of failure; developing realistic risk assessment and disaster preparedness guidelines, and updating them regularly; establishing authorities and responsibilities in advance for prevention, defense, and recovery; and implementing the guidance on a steady-state basis through training, compliance, and a culture of safety.

7. Determine ways to deliver assistance and speed recovery during and after major disasters. For instance, officials should ensure that policies, training, processes, and resources reflect how much will be driven by and reliant on the response of local communities and individuals, and how much by central governments. This is an evolving government-citizen understanding that has emerged in both Japan and the United States from great calamities. There should be no surprises regarding who will be responsible, because, like the aftershock of an earthquake, a tragedy can reassert itself unexpectedly at a moment's notice. Thus, many of the principles that should be applied during a crisis must continue long after the period of most acute danger. Similarly, many actions necessary to meet the unique requirements of long-term recovery need to be set into motion as soon as disaster strikes, and planned for long in advance. One of the signal demands for both short-term disaster relief and long-term rebuilding is the effective delivery of aid, both government resources and the outpouring of international support that often accompanies high-profile tragedies.

8. Focus cooperation in the relatively new realm of cyberspace on ensuring alliance connectivity across civil-military domains, with a particular emphasis on risks to the integrity of information. A cyber 9/11 appears still a distant more than an immediate threat, and yet cyber vulnerabilities are significant and growing. Preparing for them as an alliance is an urgent need for the United States and Japan. Current cyberthreats compromise one or more aspects of the triad of information confidentiality, availability, and integrity. However, confidentiality attacks, such as the breach of records at the Office of Personnel Management, are running out of confidential data that have not already been exposed. Availability attacks, like those that occurred at Sony Pictures Entertainment and the Sands Casino, can destroy data and deny employees and customers access to services. Of particular concern, because of the difficulty of detection, are integrity attacks in which data have been altered.

9. In the context of crisis management – but not only in that context – establish an operational U.S.-Japan alliance command structure that allows for all-of-government information-sharing and cooperation, preferably as part of the Five Eyes intelligence arrangement, but at least in parallel with it. The United States and Japan might work on this as part of a trilateral forum with Australia – in particular should a joint submarine project move forward – as well as with the Republic of Korea (South Korea). In fact, these sorts of information-sharing and cooperation protocols not only make initiatives like the joint submarine project possible, but they are the rationale for such projects in the first place. This is an example of the spiraling virtuous cycle of information integrity and sustainable command and control networks.

10. Alliance managers need to help crisis managers dealing with homeland security to consider how humanitarian and military contingencies could pose serious challenges to homeland peace and security, and vice versa. These are not separate portfolios; however, governments organize around particular responsibilities. A deteriorating security environment in Northeast Asia and around Japan includes a range of risks arising from the Korean Peninsula. Potential maritime tensions with China might affect civilian populations in Japan's home islands and, through them, Japan's ally the United States. Such contingencies are important to consider in part because they reveal the obstacles to bureaucratic politics that otherwise prevent integrated whole-of-government and whole-of-society solutions.

Appendix A

Everymay Dialogue Participants List

Brooke Adams
Shimpei Ara
Dr. David Asher
Suzanne Basalla*
LT Jake Bebber, USN
Richard Bejtlich*
Phoebe Benich
Nils Bildt
Daniel Bob
Leo Bosner
Jason Bruzdzinski
Robert Butler
The Honorable Dr. Kurt M. Campbell*
Dr. Victor Cha*
Amy Chang
Dr. Daniel Chiu
Frank J. Cilluffo*
Michael Clauser
Roberta Cohen*
Dr. Audrey Kurth Cronin
Dr. Patrick Cronin*
The Honorable Richard Danzig*
Robert Fedrick
Mr. Robert J. Fenton, Jr.*
Dr. Steve Fetter*
Nathaniel B. Fick*
The Honorable Michèle Flournoy*
Mr. Richard Fontaine
Dr. Maki Fukami*
Dr. Akiko Fukushima
Mayumi Fukushima*
Tetsuro Fukuyama*
Markus Garlauskas
Ambassador William Garvelink*
Paul Giarra
Kate Goodall
John Gudgel
Ozge Guzelsu
Dr. T.X. Hammes
General Michael V. Hayden, USAF (Ret.)*
Ryuichi Hirano*
Lt. Gen. Masayuki Hironaka, JASDF (Ret.)
Professor Bruce Hoffman*
Mr. Zachary Hosford
Goshi Hosono*
Aaron Hughes*
Katsuhiko Ichikawa
Brian Jenkins*
Dr. James Kendra*
Mike King
VADM Yoji Koda, JMSDF (Ret.)*
Harry Krejsa
Takashi Kume
Dr. Sachiko Kuno*
Dr. Irv Lachow
RDML William “Bill” Leigher, USN (Ret.)*
Dr. James Lewis*
Keith Luse
The Honorable Jane Holl Lute*
Lt Col Robert Lyons, USAF
Mr. Ado Machida
Shuji Maeda

Dr. Mark Manyin
Kyosuke Matsumoto
David Maxwell*
Patrick McCabe
RADM Michael McDevitt, USN (Ret.)*
Ellen McHugh
Dr. Narushige Michishita*
Dr. James N. Miller, Jr.*
Dr. James Mulvenon*
Yuko Nakano
Hiroyuki Namazu
The Honorable Andrew Natsios*
Dr. Norman Neureiter*
Grant Newsham
Kirstjen Nielsen, J.D.*
Ippeita Nishida
Itsunori Onodera*
Jun Osawa
VADM Umio Otsuka, JMSDF*
Christine Parthemore
Dr. Gill Pratt
Jonathan Reiber
Harvey Rishikof*
Dr. David Roberts
Andrew Saidel
Keisuke Saito
LCDR Yusuke Saito, JMSDF
Nobuko Sasae
His Excellency Kenichiro Sasae
Masanori Sasaki
Eric Sayers
Greg Scarlatoiu*
Michael Schiffer
Sydney Seiler
RADM Yuki Sekiguchi, JMSDF
Mark Shaheen*
Dr. Gary Shiffman
Ushio Shiota*
LCDR Toshihiko Shiraishi, JMSDF
Dr. Sheila Smith*
Dr. Anne Speckhard *
Dr. Paul Stockton
Hannah Suh
Alexander Sullivan
Sugio Takahashi
Yuki Tatsumi*
Lt. Colonel Bert B. Tussing, USMC (Ret.)
Frances Veasey
ADM Nirmal Verma, Indian Navy (Ret.)*
Tetsuji Watanabe
LTG Yoshikazu Watanabe, JGSDF (Ret.)
VADM James P. Wisecup, USN (Ret.)*
Shotaro Yachi*
Shigeo Yamada
Kanji Yamanouchi
Takeshi Yamawaki

*Speaker at Evermay Dialogue

Endnotes

1. One of the five Evermay Dialogue events was moderated by CNAS' chairman of the board, Dr. Kurt Campbell.

2. "The Fukushima Nuclear Accident and Crisis Management: Lessons for Japan-U.S. Alliance Cooperation" (The Sasakawa Peace Foundation, September 2012), 1, https://www.spf.org/jpus/img/investigation/book_fukushima.pdf.

3. *A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*, Report 109-377 (February 15, 2006), ix, https://www.gpo.gov/fdsys/pkg/CRPT-109hrpt377/pdf/CRPT-109hrpt377.pdf.

4. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States, Executive Summary* (July 2004), 1, http://govinfo.library.unt.edu/911/report/911Report_Exec.pdf.

5. Richard Danzig, Andrew M. Saidel, and Zachary Hosford, "Beyond Fukushima: A Joint Agenda for U.S.-Japanese Disaster Management" (Center for a New American Security, November 16, 2012), http://www.cnas.org/publications/policy-briefs/beyond-fukushima-a-joint-agenda-for-u-s-japanese-disaster-management#.Vrj_HRHA3dk.

6. Nassim Nicholas Taleb, *Antifragile: Things That Gain From Disorder* (New York: Random House, 2012).

7. Patrick Tucker, "The Next Wave of Cyberattacks Won't Steal Data — They'll Change It," DefenseOne.com, September 10, 2015, http://www.defenseone.com/threats/2015/09/next-wave-cyberattacks-wont-steal-data-theyll-change-it/120701/print/.

8. The Government of Japan, *Cybersecurity Strategy*, provisional translation (September 4, 2015), http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf.

9. Jen Weedon, "Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China," testimony before the U.S.-China Economic and Security Review Commission, June 15, 2015, http://www.uscc.gov/sites/default/files/Weedon%20Testimony.pdf.

10. That said, the U.S. government is facing an increasing threat to securing essential data from exfiltration and tampering. For instance, see Government Accountability Office, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, GAO-16-294 (January 2016), http://gao.gov/assets/680/674829.pdf.

11. Anonymous is a prime example of this activity. For one interesting implication of this private hacking activity on national security, see Larry Greenemeier, "Anonymous's Cyber War with ISIS Could Compromise Terrorism Intelligence," *Scientific American* (November 19, 2015), http://www.scientificamerican.com/article/anonymous-s-cyber-war-with-isis-could-compromise-terrorism-intelligence/.

12. Richard Danzig, "Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies" (Center for a New American Security, July 2014), 6–7.

13. U.S. Department of Defense, *The DoD Cyber Strategy* (April 2015), http://www.dtic.mil/doctrine/doctrine/other/dod_cyber_2015.pdf.

14. *Best Practices for Incident Response and Cyber Coverage* (Chicago: American Bar Association Center for Professional Development, 2015), http://www.americanbar.org/content/dam/aba/multimedia/cle/materials/2015/04/ce1504prc.authcheckdam.pdf.

15. Roberta Cohen, "Human Rights and Humanitarian Planning for Crisis in North Korea," *International Journal of Korean Studies,* Fall/Winter 2015, http://www.brookings.edu/research/articles/2016/02/human-rights-north-korea-cohen.

16. An example of this is the appointment of an Australian general officer as deputy commander of U.S. Army Pacific, a practice that started in 2013. See "Australian General Gets Key US Army Post," The Associated Press for Washington.CBSlocal.com, February 1, 2013, http://washington.cbslocal.com/2013/02/01/australian-general-gets-key-us-army-post/.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy.

CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan. CNAS does not take institutional positions on policy issues. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

1152 15th Street, NW Suite 950 Washington, DC 20005

t. **202.457.9400** | f. **202.457.9401** | **info@cnas.org** | **cnas.org** | **@cnasdc**

Bold. Innovative. Bipartisan.