SASAKAWA USA
Sasakawa Peace Foundation USA

Improving Cybersecurity Cooperation between the Governments of the United States and Japan

Linton Wells II, Motohiro Tsuchiya, and Riley Repko

1. Executive Summary

Cybersecurity is becoming more important to the economic, security, and social well-being of both the United States and Japan. Sasakawa Peace Foundation USA therefore commissioned this paper to examine ways to improve cybersecurity cooperation between the two nations. Its main parts include (a) how the U.S. and Japanese governments are organized to deal with cybersecurity issues; (b) how the two governments currently coordinate in cybersecurity; (c) how the differences in organization and other matters affect coordination; (d) "whole-of-society" approaches to overcoming impediments, and (e) recommendations.

Several recent studies of Japan's cybersecurity and Japan-U.S. cooperation have produced useful recommendations.[1] This paper tries not to duplicate them. Rather, based on recent discussions in Japan and the United States, it focuses on ways to change behaviors to improve both long-term coordination and crisis response. Both nations have policies, procedures, plans and organizations in place to promote cybersecurity-related information sharing, law enforcement and incident response.[2] But there are critical gaps in how well these work in practice. However good high-level pronouncements may be, they have to be implemented effectively.

The authors would like to express their appreciation to Sasakawa Peace Foundation USA; Mr. Erick Kish of the American Embassy in Tokyo; Mr. Tom Puppi of the Office of the Secretary of Defense; Mr. Mark Weatherford, former Deputy Under Secretary for Cybersecurity at DHS; and RADM Katsuhiko Saito, JMSDF (ret), cybersecurity authority. Any errors, of course, are our own.

Improving information sharing across stovepipes needs particular attention in both countries. This requires agreed-upon frameworks for understanding risk and liability. Legal structures and other procedures and regulations should incentivize sharing and collaboration.

No one government or private sector organization has all the answers, and each nation can learn from the other. Since most economic assets and critical national infrastructures (CNI) are privately owned and operated, cybersecurity-related solutions will need significant amounts of public-private cooperation.[3] This includes education for citizens, the workforce, and management. Despite pronouncements by senior officials, many still do not see cybersecurity as a priority. However, people in both countries understand the need for counterterrorism and disaster preparedness, and cybersecurity can be related to these.

For example, a challenging, yet plausible, threat involves the concurrent disruption of several infrastructures by physical and virtual means, causing casualties that could cascade from one sector to another. This would require "whole of society" responses, across sectoral, organizational, and political boundaries, probably with international collaboration. Both countries already have effective mechanisms in place for counterterrorism and "all hazards" emergency preparedness—these could be brought to bear. Improvements certainly will be needed to fold cybersecurity into these frameworks, but whole new concepts need not be invented.

Japan can use the 2020 Tokyo Olympics as a "forcing function" to focus attention, identify gaps, shape training and exercises, and accelerate responses, but deadlines already are tight. The accelerating pace of technological change increases the penalties for inaction. This paper offers actionable recommendations in four areas to improve cybersecurity cooperation:

- **Between the U.S. and Japanese governments in civil sectors:** Establish exchange positions at Japan's Government Security Operations Coordination (GSOC) team and the U.S. National Cybersecurity and Communications Integration Center (NCCIC). Hold secure videoconferences among leaders and stakeholders, augmented by in-person meetings, plus real-time coordination when incidents do occur. Other organizations lend themselves to similar relationships.
- **Between the U.S. Armed Forces and Japan Self-Defense Forces on military networks**: Work to include Japan in the U.S. Mission Partner Environment (MPE) and related communications systems to improve security and interoperability. Begin with bilateral government-to-government talks to understand Japan's present reluctance to join. Emphasize that the effective defense of Japan's networks is essential not just to Japan, but also to the Alliance itself. The reverse also is true.
- **Between public and private sectors**: Take advantage of the fact that both countries already have integrated, well-understood response frameworks for counterterrorism and natural disasters and fold cybersecurity incident responses into them, vice inventing new approaches. Improve public-private collaboration by focusing on the U.S. and Japanese Information Sharing and Analysis Centers (ISACs) that serve common customers, e.g. information and communications technology and financial services. Promote (a) government actions to improve information flow to the ISACs and to address legal, policy, and regulatory issues; (b) private sector actions to let companies share more of the information on their networks with organizations such as law enforcement; and (c) direct binational coordination to facilitate more effective international exchanges. Ensure these mechanisms produce value to make businesses want to participate.
- **Among private sector entities:** Survey private sector organizations in both countries to identify the collaborative organizations with which members are particularly satisfied. Share best practices and examine ways to institutionalize these approaches. Incentivize action and train.

The authors, and Sasakawa Peace Foundation USA, are prepared to support interested parties in developing cybersecurity initiatives that can benefit the people of both our nations.

2. The Cybersecurity Landscape

Cybersecurity is complex and multi-faceted, but the basic components can be grouped by (a) attacker objectives, (b) sources of threat, (c) types of defense, and (d) management of risk. Effective cybersecurity programs must consider them all.

Computer espionage and cybercrime (including data exfiltration, blackmail, and identity theft) have been with us for years, now augmented by rapidly growing ransomware attacks. They typically involve some form of theft. Other forms of malicious cyberspace activity aim to deny, disrupt, degrade, destroy, or deceive adversary capabilities. Recent Distributed Denial of Service (DDoS) attacks fall into this category, while tools such as Stuxnet show that cyberattacks can physically destroy equipment.

There are four main threat sources:[4]

- Insiders, who may be good employees who cause unwitting damage with tainted technology, but who also could be rogues.
- Attacks over and through the internet. Despite "in depth" defenses, some degree of penetration is likely, leaving vulnerability to malware that is installed for later activation.
- Third party access to a system, which could be through a house, a business, or a vendor with an upgrade. Increasing connectivity and market liberalization bring more vulnerability daily, and the exploding Internet of Things (IoT) offers new paths into heretofore-isolated infrastructures (like to the power grid through smart meters) as well as a platform to mount massive denial of service attacks.
- Supply chain. It is very hard to check the pedigree of production supply chains.[5] Moreover, for key components, such as industrial control systems, the small number of worldwide suppliers limits defense options.

Security technology can help, but people are both the first line of defense and the greatest source of risk. Leaders and managers often look for technological "silver bullets," which do not exist. Solutions need to be integrated across people, organizations, processes and technologies.[6] Demand for security professionals greatly exceeds supply and those in place must train to stay current. Each person who handles a computer needs to practice good cybersecurity hygiene, engineers need to learn how to design cybersecurity into new systems, and executives need to understand the technology they are overseeing. It's often said that the most important cybersecurity decisions are made in the boardroom, not the server room.

Speed is critical to cybersecurity in many ways. Changing network configurations faster than the adversary can plan attacks can be an effective defense. The pace of technological change means that the capabilities of key components are doubling as fast as every eighteen months, so plans based on linear projections from present conditions cannot work, however comfortable they may be. Rapid innovation frequently comes from small and medium-sized businesses (SMBs), which need paths to get their ideas in play and not be blocked by larger and more established players. It also takes too long to detect and patch vulnerabilities.[7]

Good policies and regular discussions without action are not enough, for adversaries are not waiting. All parties need to focus on "mission assurance"—gracefully degrading under pressure to accomplish the mission under any level of attack.

No entity, public or private, has all the information it needs to protect itself, so this can only be addressed through aggressive information sharing and training at all levels, plus a commitment to security from the top to the bottom of an enterprise. Sharing always involves some degree of risk—of compromise, of loss of control, of liability, of exposure. Cybersecurity thus needs to be treated as a "risk management" issue, since there is no completely safe

approach (other than disconnecting, which has its own disadvantages). Information sharing may be risky, but holding on to outdated practices and not sharing adds even more dangers.

Finding the right balance between privacy, security and convenience is an ongoing challenge. The United States and Japan have very different historical perspectives with regard to these challenges, but the global nature of the networked economy and society make it essential for both nations to find common ground to address them.

3. How the U.S. and Japanese Governments Are Organized to Deal with Cybersecurity Issues

3.1 U.S. Government

U.S. Government (USG) activities and its organization for cyberspace operations are based on a strong set of recent foundational cybersecurity documents, which cover both steady state and crisis response approaches. These include:

- The *Cybersecurity National Action Plan* (CNAP),[8] issued in February 2016
- Presidential Policy Directive-41 (PPD-41) *United States Cyber Incident Coordination*, of July 26, 2016[9]
- A draft *National Cyber Incident Response Plan* (NCIRP), mandated by PPD-41[10]

3.1.1 U.S. Steady State Approaches to Cybersecurity Issues

Since 2009 the USG has pursued several initiatives that could relate to U.S. Government (USG)–Government of Japan (GOJ) cybersecurity collaboration:[11]

- Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections
- Coordinate and redirect research and development (R&D) efforts
- Connect current cybersecurity ops centers to enhance situational awareness
- Develop and implement a government-wide cybersecurity counterintelligence (CI) plan
- Expand cybersecurity education
- Develop a multi-pronged approach for global supply chain risk management
- Define the Federal role for extending cybersecurity into critical infrastructure domains

Current USG Divisions of Responsibility: There is a National Cybersecurity Coordinator who has regular access to the President. National policy coordination on specific issues is done through the Principals and Deputies Committees of the National Security Council (NSC). The Department of Homeland Security (DHS) is responsible for cybersecurity on most USG networks (the Intelligence Community protects its most sensitive networks and Department of Defense (DoD) protects some of its own). The Federal Bureau of Investigation (FBI), part of the Department of Justice (DOJ), has the responsibility for prosecuting cybercrimes. The National Security Agency (NSA), reporting both to the Secretary of Defense and the Director of National Intelligence (DNI), has the greatest technical capability of any organization in the USG on cybersecurity. It provides intelligence concerning potential and actual cyberattacks that it gathers outside the United States, as well as providing technical support to other government departments and agencies when requested. DoD developments have included the establishment of the National Cyber Mission Force, whose responsibilities include "defending the U.S. and its interests against cyberattacks of significant consequence and defense of the nation's critical infrastructure when significant consequences may include loss of life,

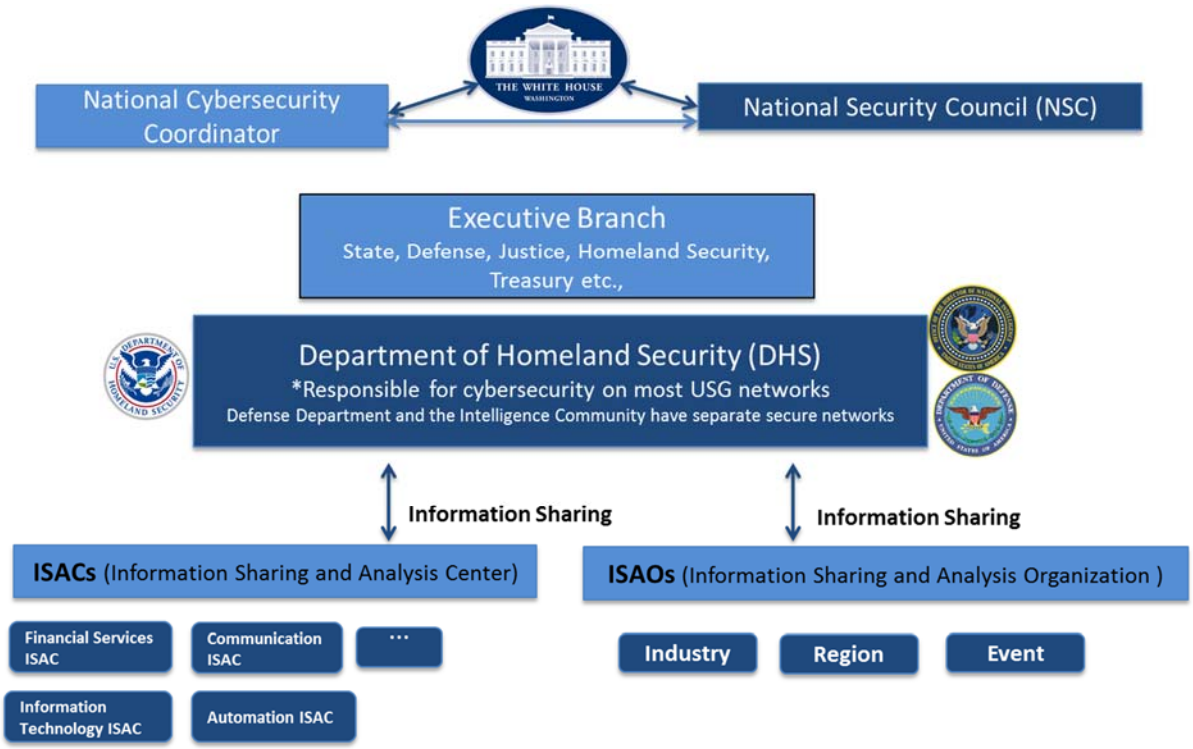

Figure 1. U.S. steady state cybersecurity stakeholders.

significant damage to property, serious adverse U.S. foreign policy consequences or serious economic impact on the United States."[12] These organizations cooperate with international partners through a variety of mechanisms. Those with Japan are described later in the paper. However, this international cooperation is not necessarily coordinated among the various U.S. agencies. See figure 1.

Each of the major Executive Branch departments (DHS, Department of State (State), DoD, DOJ, Department of the Treasury (Treasury), etc.) has internal coordination mechanisms and strategies.[13] There is a multi-agency and industry-led U.S.-Japan Cyber Working Group at the U.S. Embassy in Tokyo.

Whole-of Society Approaches and Public-Private Partnerships: Since the late 1990s, ISACs have been available to link government agencies and the private sector. There now are twenty-one U.S. ISACs which help critical infrastructure owners and operators collect, analyze and disseminate actionable virtual and physical threat information to their members and provide members with tools to mitigate risks and enhance resiliency. A National Council of ISACs (NCI) has been formed to maximize information flow across critical infrastructures and with the government. Japan's ISACs include the Financial ISAC Japan, and the recently formed ICT-ISAC Japan, which was established in July 2016 incorporating members from the previous Telecom-ISAC, the System Integrators and Vendor community, Broadcasters, and also Security Vendors. There is talk that an Electric Power ISAC may be formed in the future.

In the United States a new collaborative structure recently has been established called Information Sharing and Analysis Organizations (ISAOs), supported by an Executive Order.[14] ISAOs are more flexible than the sector-specific ISACs, with a make-up of vendors with similar business objectives and security vulnerabilities. A U.S. ISAO Standards Organization was set up in late 2015 to identify standards and guidelines "for robust and effective

information sharing and analysis related to cybersecurity risks, incidents, and best practices." Japan has been reorganizing its ISACs, and private sector organizations have been examining collaborative approaches, but the ISAO approach has not been formally adopted.

The recent CNAP[15] established a "Commission on Enhancing National Cybersecurity" comprised of top strategic, business, and technical thinkers from outside of government—some designated by Congress on a bi-partisan basis. The Commission recommended additional actions that can be taken over the next decade to strengthen cybersecurity in both the public and private sectors.[16] These include the need for public-private partnerships, international engagement and roles for consumers. The sixteen recommendations were categorized into six overarching imperatives, focused on infrastructure, investment, consumer education, workforce capabilities, government operations, and requirements for a fair and open global digital economy. Each has one or more action items. The section on securing the IoT is particularly valuable. The report calls for the current Administration to develop implementing actions.

It is clear that collaboration with the private sector and information sharing are dominant issues, repeated constantly within the cybersecurity domain. But the value of any private-sector participation must be made clear, especially to the SMBs, with a primary focus on revenue generation. Government and commission recommendations will fall on deaf-ears if the incentives are not clear and immediate. Also, after the information-sharing framework is in place, recommendations must be made on how to make the government acquisition process for the security goods and services meet the immediate needs of all parties involved.

The CNAP also proposes to empower Americans to secure their online accounts and transactions through multi-factor authentication. This will be central to a new National Cybersecurity Awareness Campaign launched by a National Cybersecurity Alliance designed to arm consumers with simple and actionable information to protect themselves in an increasingly digital world. The Alliance will partner with leading technology firms. The federal government will also work to safeguard personal data in online transactions with citizens.

Investments in cybersecurity: The CNAP includes a $3.1 billion fund to modernize government IT and transform how the government manages cybersecurity. It also forms a new position—the Federal Chief Information Security Officer—to drive these changes across the government. Overall, the CNAP proposes to invest over $19 billion for cybersecurity as part of the U.S. FY 2017 Budget (Oct 1, 2016 to Sep 30, 2017). This represents a more than 35 percent increase from FY 2016 in overall Federal resources for cybersecurity.

3.1.2 U.S. Cybersecurity Incident Response

PPD-41, "United States Cyber Incident Coordination"[17] specifies USG responses to a Significant Cyber Incident.[18] A key point is that it integrates cybersecurity and traditional preparedness efforts to "manage incidents that include both cyber and physical effects."[19] The federal government is to be guided by the following five principles in responding to cybersecurity incidents: "Shared responsibility, risk-based response, respecting affected entities, unity of governmental effort, and enabling restoration and recovery."[20] In doing this, federal agencies pursue three concurrent lines of effort:

- **threat response** (conducting law enforcement and national security investigations, etc.)
- **asset response** (furnishing technical assistance, facilitating information sharing, etc.)
- **intelligence support and related activities** (building situational awareness, mitigating threats, etc.)

If a private entity is affected, the federal government typically does not play a direct role, but stays aware of the affected entity's response.

Federal responses to significant cybersecurity incidents involve (a) National Policy Coordination, (b) National Operational Coordination, and (c) Field-Level Coordination.[21] The Cyber Response Group (CRG) coordinates policy development and implementation concerning "*significant cyber incidents* affecting the U.S. or its interests abroad." The CRG supports the NSC Deputies and Principals Committees.

National Operational Coordination procedures are described in PPD-41 and its annex. A Cyber Unified Coordination Group (UCG) shall be formed for significant cybersecurity incidents to be the primary coordination method "between and among Federal agencies…as well as for integrating private sector partners into incident response efforts, as appropriate."

Field-Level Coordination maximizes cooperation among federal representatives, the affected entity state, local, tribal and territorial (SLTT) governments, and international partners. The roles of USG organizations in cybersecurity incident response are shown in table 1.[22] Their relationships are shown in figure 2.

In September-October 2016, a draft National Cyber Incident Response Plan (NCIRP) was issued for public comment, as called for in PPD-41.[23] The NCIRP is "the strategic framework for operational coordination among

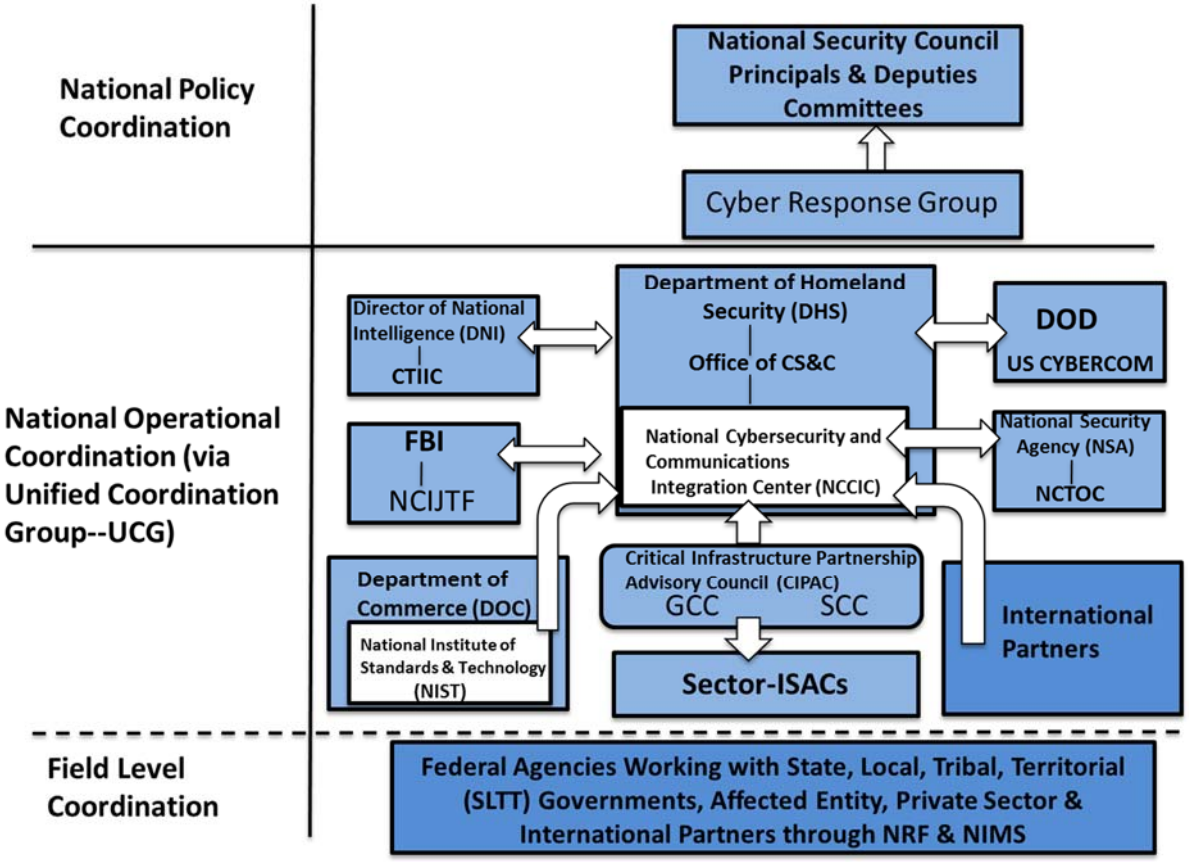

Figure 2. U.S. Crisis Response Stakeholders.

Table 1. Roles of USG Organizations in Cybersecurity Incident Response.

Organization	Function	Notes
National Cybersecurity and Communications Integration Center (NCCIC), DHS	Lead for asset response during a significant cyber incident	Threat indicators are shared through Automated Indicator Sharing (AIS)
FBI and National Cyber Investigative Joint Task Force (NCIJTF), DOJ	Lead Federal Agency for threat response	NCIJTF has an multi-faceted "Operation Clean Slate" initiative to address the "botnet" threat
U.S. Secret Service, DHS U.S. Secret Service and cyber crime:	Investigates financial crimes	
Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), DHS	Threat response for cyber-related crimes	HSI is part of ICE. It is a critical investigative arm of DHS (www.ice.gov/hsi). Cybercrimes fall within its charter.
Cyber Threat Intelligence Integration Center (CTIIC), ODNI	Lead Federal Agency for intelligence support during significant cyber incidents	
National Institute of Standards & Technology (NIST), DOC	Cybersecurity Security Framework development	
U.S. Cyber Command (USCYBERCOM), DOD	Directs U.S. military's cyberspace operations and defense	
National Cybersecurity Threat Operations Center (NCTOC), NSA	Informs partners of current and potential malicious cyber activity through its analysis of foreign intelligence	Focus on adversary computer network attacks, capabilities and exploitations.
Critical Infrastructure Partnership Advisory Council (CIPAC), Sector & Govt Coordinating Councils (SCC/GCC), Sector ISACs	Information sharing for shared situational awareness; intra-government and public-private cooperation	National operational coordination between the public and private sectors
SLTT Coordinating Councils with both International Partners & Private Sector	Field-level forum for coordination of activities and best practices	Organizational structure for coordinating strategies & programs among jurisdictions

Federal and SLTT governments, the private sector, and international partners." It is designed to "enable a coordinated whole-of-nation approach to response activities and coordination with stakeholders during a significant cybersecurity incident impacting critical infrastructure." It relies heavily on public and private partnerships to mitigate, respond to, and recover from a cybersecurity incident. The NCIRP reinforces the linkages between cybersecurity and other kinds of incidents by tying cybersecurity incident response to the U.S. National Response Framework (NRF).[24] The NRF is one of five frameworks in the National Preparedness System and is part of achieving the "Response" goal.[25] Cybersecurity incident response also will use the National Incident Management System (NIMS),[26] to stay aligned with well-established procedures. The links between physical and cybersecurity are reinforced by the fact that the NCIRP is "designed to integrate and interface with industry standards and best practices for cybersecurity risk management, as developed by the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity."[27] The NCCIC is composed of four branches, of which the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is most involved with international and private sector CERTs. NIST is connected to DHS and NCCIC through their mutual contributions to the Cybersecurity Framework.

To improve U.S.-Japanese collaboration, the NCCIC should invite key Japanese agency involvement through dedicated seats on the NCCIC floor. These are described in more detail in the Recommendations section.

Despite these steps, much work remains to be done. All ISACs have not performed equally well, as the establishment of the more flexible ISAOs indicates. Moreover, hacks at the Office of Personnel Management (OPM),

FBI, Internal Revenue Service (IRS), National Aeronautics and Space Administration (NASA) and elsewhere, as well as the Chelsea Manning and Edward Snowden leaks, show serious weaknesses in USG cybersecurity. In February 2016, a commercial "Cybersecurity Scorecard"[28] review "analyzed and graded the current security postures of 600 local, state, and federal government organizations, each with more than 1,000 public-facing IP addresses, to determine the strongest and weakest security standards based on security hygiene and security reaction time compared to their peers." The results were sobering. Government organizations received the lowest security scores of the seventeen major entities surveyed. Three categories of security measurements were particularly challenging to low-performing government organizations: Malware Infections, Network Security and Software Patching Cadence.

The United States thus has much to share with Japan regarding cybersecurity approaches and "whole of society" approaches, but also much yet to learn.

3.2 Government of Japan

3.2.1 Information Security Strategy for Protecting the Nation 2011 and Cybersecurity Strategy 2013

In response to massive scale DDoS attacks against the United States and the Republic of Korea in July 2009, the GOJ began paying more attention to cybersecurity. After the defeat of the Liberal Democratic Party (LDP)–Komeito coalition by the Democratic Party of Japan (DPJ), Chief Cabinet Secretary Hirofumi Hirano of the Hatoyama Administration said in a press briefing that cyberattacks could be a national security and crisis management issue. In May 2011, the GOJ published the *Information Security Strategy for Protecting the Nation*, which was the country's first national strategy regarding cybersecurity.

In December 2012, the LDP and Komeito came back into power and Shinzo Abe formed his second cabinet. The Abe administration started reforming national security policies in various ways and the Prime Minister ordered the Chief Cabinet Secretary, Yoshihiro Suga, to revise the *Information Security Strategy for Protecting the Nation*, which was developed under the DPJ government. It resulted in the *Cybersecurity Strategy*, authorized by the Information Policy Security Council (IPSC) in June 2013.

However, this Cybersecurity Strategy did not have any legal status. The IPSC itself was a sub-unit under the IT Strategic Headquarters and its strategy did not legally bind any ministry or agency in the government. As most of these ministries and agencies were involved in drafting the strategy, they were eager to follow it and fulfill commitments written in the strategy. But its legal status remained unclear.

In response to a series of high profile attacks against business and government targets, e.g. Mitsubishi Heavy Industries (MHI) in 2011, SONY Pictures Entertainment (SPE)[29] in 2014, and the Japan Pension Service (JPS) in 2015, the GOJ has taken significant additional steps to improve cybersecurity.[30] Even before the SPE incident became public, the Japanese Diet was acting to reinforce cybersecurity. In November 2014, the Diet passed the Cybersecurity Basic Act, which became effective in January 2015; in the Japanese system, a basic act sets the country's long-term strategic goals in a certain policy area.

After passing the act, the National Information Security Center was transformed into the National Center for Incident Readiness and Strategy for Cybersecurity (NISC).[31] It acquired more authorities and strengthened its legal basis to oversee cybersecurity issues in Japan. Since the passing of the act, NISC now has the ability to "request"

information from each of the ministries. However, since these same ministries aren't required to comply with these requests, it seems to undercut NISC's abilities to execute its mission.

The IPSC, which sets cybersecurity policies across the government and reported to the Chief Cabinet Secretary, was promoted and renamed the Cybersecurity Strategic Headquarters (CSH). Today this body cooperates closely with the new Japanese National Security Council (NSC), chaired by the Prime Minister. The CSH's mandate is broad, overseeing Japan's strategic goals for cyberspace, the protection of critical infrastructures, the raising of public awareness, research and development, and finally, information-sharing.

There is an international component of the Cybersecurity Basic Act. Article 23 requires Japan to contribute to international arrangements that improve its cybersecurity. Although the SPE incident largely took place overseas, its timing in late 2014 reinforced the importance of Japan's evolving cybersecurity policies.

3.2.2 Cybersecurity Strategy 2015

Based on the Cybersecurity Basic Act, the CSH laid out its draft of a new Cybersecurity Strategy on May 25, 2015. Chief Cabinet Secretary Suga, who heads the CSH, immediately ordered a second version of the draft when the JPS was found to have been hacked. The new strategy was finalized on August 20, 2015, and was approved by the Cabinet on September 4. While the Cabinet's approval did not make the strategy law, it did confer on it quasi-legal status. The strategy demonstrated Japan's high-level commitment to cybersecurity and formed the basis of measures to be implemented henceforth at ministries, agencies, and other government organizations. The current organizational structure is represented in figure 3. The acronyms refer to the following agencies: CIRO, Cabinet Intelligence and Research Office; GSOC Government Security Operations Coordination; ICTICU, International Counter-Terrorism Intelligence Collection Unit; METI, Ministry of Economy, Trade and Industry; MIC, Ministry of Internal Affairs and Communications; MOD, Ministry of Defense; MOFA, Ministry of Foreign Affairs; NISC, National Center of Incident Readiness and Strategy for Cybersecurity; NPA, National Police Agency; NSC, National Security Council; and PSIA, Public Security Intelligence Agency.

Looking at the new strategy, the first thing to note is the increased capabilities of the Government Security Operations Coordination team (GSOC). As a part of the NISC, the GSOC has mainly been responsible for watching over the computer systems and networks of central government ministries. It was the GSOC that first discovered the hacking of the JPS and informed them of the intrusion, though (owing to the nature of the hack) the breach could not be addressed quickly. In response to this, the government extended GSOC's monitoring abilities to cover government-affiliated organizations as well, including incorporated administrative agencies and special public corporations (the JPS falls under the latter). It also is expected to bolster the budgets and staff of the NISC and GSOC to enable them to fulfill their roles as cybersecurity control centers.

A second point of the strategy is the government's efforts not only toward post-incident response but also toward proactive prevention. The strategy promotes an understanding among relevant parties of the need to report even small-scale damage and signs of suspicious activity to safeguard against large-scale cyberattacks. It also puts an emphasis on bolstering both internal and external systems for cooperation and information sharing. It goes without saying that a speedy response and recovery is essential following a cyberattack, but it also should be possible to prevent incidents by monitoring networks and systems and sharing information about them among different agencies and with global partners.

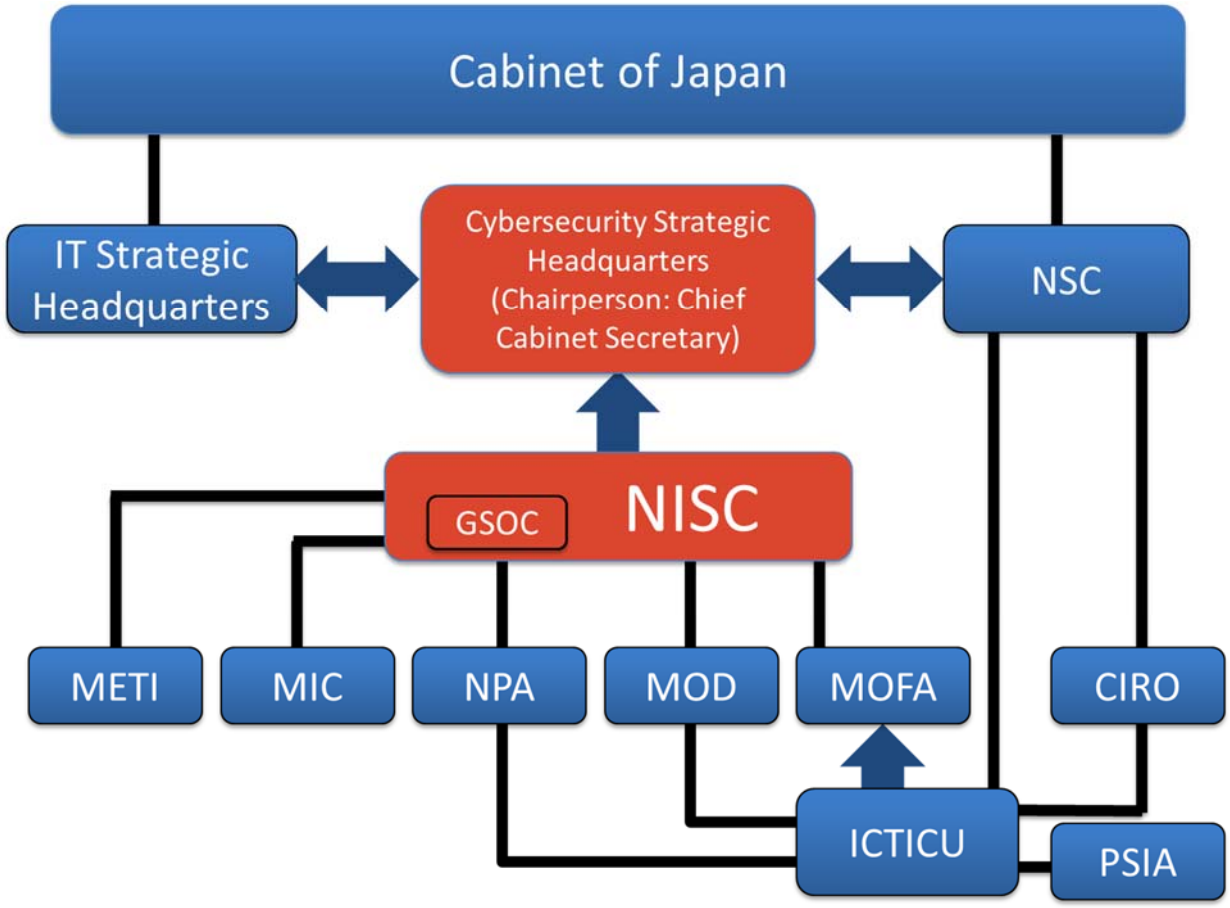

Figure 3. Japanese Government Structure for Cybersecurity.

A third point is the strategy's effort to strike a balance between security and free access. It underscores the impossibility and impracticality of tasking the government alone with maintaining order in cyberspace. In global cybersecurity talks, China and Russia have called on states and governments to take greater roles in policing unlawful activities by boosting surveillance and control measures. In response, Japan, the United States, and European countries have argued for the need to guarantee freedom of speech and the free flow of information while still protecting networks against criminal attacks. Entrusting cybersecurity solely to the state without rules and regulations and procedures and institutions that protect privacy may result in the kind of surveillance society that exists in China and Russia. Japan has openly expressed its opposition to such an approach. Japan's strategy articulates the government's firm stance against state use of cyberspace to control, censor, steal, or destroy information, as well as its "illicit use" by terrorists and other non-state actors. It goes on to establish the government's commitment to contribute proactively to conserving cyberspace for "peaceful purposes" while also ensuring the safety of the country.

Looking at the language of the 2015 strategy, the forty-page document contains fifty-one variants of the word "sharing" and eighty usages of the word "cooperation." By comparison, "sharing" appeared forty-eight times and "cooperation" just sixty-two times in the earlier, forty-three-page Cybersecurity Strategy approved in June 2013. Information sharing in the wake of hacking incidents and cooperation among organizations can be seen as pillars of Japan's Cybersecurity Strategy. Those activities are actually becoming more common domestically and internationally.

Japan plans to establish a new government agency to protect the country's critical infrastructure from cyberattacks. The Industrial Cybersecurity Promotion Agency (ICPA) is planned to become operational in 2017; the

government wants this agency to be capable of defending critical systems by the time Tokyo hosts the Olympic Games in 2020. ICPA will include two divisions: one focused on research and the other focused on active response.[32] A difference between U.S. and Japanese strategies to date has been that the U.S. approach seems to include more cooperation between the government and the private sector, including information sharing, and combined action against criminals (such as botnet takedowns), whereas Japan's policies and actions so far have been primarily directed at government networks.

3.2.3 SIGINT Capability in the Internet Age

Japan lacks a Signals Intelligence (SIGINT) capability over digital wired networks. Article 21 of the Japanese Constitution protects the secrecy of communications. So does Article 4 of the Telecommunications Business Act.[33] These were designed in the 1940s for a pre-cellphone and Internet world. Under the Constitution and the Telecommunications Business Act, the Ministry of Internal Affairs and Communications (MIC) and telecommunication providers have been strictly regulating themselves in order not to violate the secrecy of communications. Capturing metadata has also been restricted except for commercial purposes such as billing. However, the rise of recent cyberattacks such as DDoS is contributing to a slight policy change. In order to protect facilities and service qualities, communication providers are now allowed to monitor their own communications based on MIC guidelines. The third version of the guidelines, which was published July 22, 2014, reads as follows:

> *Where the confidentiality of communications between parties is compromised without their consent, this compromise is permitted and lawful if it meets the elements for one of the following statutory justifications: (1) justified self-defense (Article 36 of the Penal Code), emergency evacuation (Article 37 of the Penal Code), or other justified grounds (Article 35 of the Penal Code).*[34]

Still, intelligence and law enforcement agencies in the government are not allowed to monitor communications without court orders. The number of cases of judicial wiretapping is usually less than fifty per year and those cases are for mobile communications only. No Internet traffic is monitored by government agencies.

Another related problem is that there is no intelligence oversight committee in the Diet. However, since Edward Snowden's revelation of highly classified NSA information, oversight of intelligence activities must also be established in Japan.

4. How the two Governments Currently Coordinate in Cybersecurity

Japan and the United States have an extensive web of coordination on cybersecurity issues. These include bilateral governmental meetings, collective meetings in international bodies such as the cybersecurity group under the G7, private-sector engagements, and academic collaboration.

4.1 Bilateral Governmental Meetings

4.1.1 Diplomatic Partnership[35]

As stated many times in the 2015 Cybersecurity Strategy, the GOJ is stressing "information sharing" and "cooperation" in developing its bilateral cybersecurity relationships with the United States, the United Kingdom, Estonia, India and

others; its trilateral cybersecurity relationship with the Republic of Korea and China; and its multilateral relationships with ASEAN and NATO.

There are formal frameworks between Japan and the United States, including the Japan-U.S. Cyber Dialogue led by the Ministry of Foreign Affairs and the Department of State, and the Japan-U.S. Policy Cooperation Dialogue on the Internet Economy, led by MIC on the Japanese side and the U.S. Economic Bureau of State.

When Prime Minister Abe and President Obama met in April 2015, they issued a joint statement agreeing to "ensure the safe and stable use of cyber space based on the free flow of information and an open Internet."[36] A year later the leaders of the G7 at Ise-Shima reiterated the importance of an open, interoperable, reliable, and secure internet, and agreed to promote security and stability in cyberspace, along with the digital economy.[37]

The United States and Japan actively participate in the UN's Group of Governmental Experts (GGE), which has shown that international law can be applied in cyberspace and emphasized the importance of norms. The 2016–17 GGE discussions have started, and probably will focus on the need for capacity building and a better understanding of terms such as prevention, cooperation, and stability.

Japan hosted the Cyber3 Conference in Okinawa in November 2015 to examine issues associated with connectivity, cybercrime, and cybersecurity. Preparations for the 2020 Olympics were a major discussion topic.

Based on the authors' research and experience, these meetings between U.S. and Japanese government representatives often involve exchanges of information about current or planned activities. While these exchanges have some value, they add little to the cybersecurity of either government. They fall short, for example, of the best information exchanges within ISACs, and rarely include ways to coordinate action in the event of attacks affecting the network of both countries, to form combined plans to improve the security of common systems such as critical infrastructure systems, or to address new technologies such as the IoT.

4.1.2 Defense Cooperation[38]

In contrast to the relatively pro forma state of the U.S.-Japan Cyber Dialogue, a quite close cooperation has developed between the American DoD and the Japanese MoD. The Japanese and American governments agreed on and published versions of *The Guidelines for Japan–U.S. Defense Cooperation* in 1978, 1997, and 2015. Needless to say, no mention of cybersecurity was included in the 1978 and 1997 guidelines. The 2015 guidelines have eight chapters, and the sixth chapter outlines cooperation in outer space and cyberspace. The full text of the "Cooperation on Cyberspace" portion reads as follows:[39]

> *To help ensure the safe and stable use of cyberspace, the two governments will share information on threats and vulnerabilities in cyberspace in a timely and routine manner, as appropriate. The two governments also will share, as appropriate, information on the development of various capabilities in cyberspace, including the exchange of best practices on training and education. The two governments will cooperate to protect critical infrastructure and the services upon which the Self-Defense Forces and the United States Armed Forces depend to accomplish their missions, including through information sharing with the private sector, as appropriate.*
>
> *The Self-Defense Forces and the United States Armed Forces will:*
>
> - *maintain a posture to monitor their respective networks and systems;*
> - *share expertise and conduct educational exchanges in cybersecurity;*
> - *ensure resiliency of their respective networks and systems to achieve mission assurance;*

- *contribute to whole-of-government efforts to improve cybersecurity; and*
- *conduct bilateral exercises to ensure effective cooperation for cybersecurity in all situations from peacetime to contingencies.*

In the event of cyber incidents against Japan, including those against critical infrastructure and services utilized by the Self-Defense Forces and the United States Armed Forces in Japan, Japan will have primary responsibility to respond, and based on close bilateral coordination, the United States will provide appropriate support to Japan. The two governments also will share relevant information expeditiously and appropriately. In the event of serious cyber incidents that affect the security of Japan, including those that take place when Japan is under an armed attack, the two governments will consult closely and take appropriate cooperative actions to respond.

Since this section is part of the overall *Guidelines for Defense Cooperation,* it is essential to recognize that security-related cybersecurity incidents will be addressed within the overall coordination mechanisms of the U.S.-Japan Alliance. The security of Japan's networks is essential to the Alliance since, in a networked environment, "a risk accepted by one is a risk imposed on all." The effectiveness of Japan's cybersecurity defenses is thus critical to both nations, just as the security of U.S. networks also is.

The last sentence in the quoted section is important. The interpretation of "in the event of serious cyber incidents that affect the security of Japan" is critical. Neither the Ministry of Defense of Japan nor the U.S. DoD have clarified in what kind of situations they can deploy Japan's Self-Defense Forces and U.S. Armed Forces. In the case of a cyberattack defined narrowly within the Tallinn Manual, there would need to be human loss or physical damage for a cybersecurity intrusion to qualify as an "attack" under this definition.[40] Such an attack would clearly fall within the scope of engaging the right of self-defense. Cyberattacks that did not result in the loss of life or physical damage to property could more accurately be characterized as cybercrimes, cyberespionage, or cybersabotage in most cases, and it would be difficult to deploy the Self-Defense Forces or the U.S. military to respond to such events. Instead, law enforcement organizations or intelligence agencies would be expected to take the lead in responding through criminal indictments; economic sanctions might also be a useful tool to employ.

One possible scenario is a cyberattack against command and control systems that support the Japan Self-Defense Forces. If those systems were lost and a possible enemy were moving military forces, cybersecurity counterstrikes (also known as "hack back") by Japan might be considered. But how to respond proportionally in such a crisis requires careful consideration. Without enough understanding on both sides, a virtual conflict might escalate to a physical one, or even a war.

The Ministry of Defense of Japan and the Self-Defense Forces are not considering the use of active "offensive" measures in cyberspace due to Article 9 of the Japanese Constitution. Even in cyberspace, the use of weapons to undertake a first strike would be hard under current Japanese legal frameworks. However, if Japan could clearly identify the sources of cyberattacks in foreign countries, it would be able to stop them using cybersecurity measures (not deploying troops). MOD's "Toward Stable and Effective Use of Cyberspace," which was published in September 2012, states, "The possibility of the need to deny an opponent the use of cyberspace in order for JSDF to effectively dispel an armed attack against Japan should also be noted."[41] From this perspective, "active defense measures" in cyberspace would be an option Japan could consider. As noted above, however, the overall structure of the U.S.-Japan Alliance provides a wide range of options for addressing many contingencies.

In 2008 a classified U.S. defense network was hacked after a USB thumb-drive was inserted in a military laptop computer in the Middle East.[42] In September 2016, Japan Self-Defense Forces and the MOD's Defense Information Infrastructure (DII), a classified and closed network, was also hacked.[43] The attacker first compromised

the National Defense Medical College to penetrate the DII since academic gateways have relatively lower security. This incident is quite serious, not only for Japan's defense but also for the Japan-U.S. Alliance. It is common knowledge that an alliance needs operational interoperability, which means that a breach of one network might open vulnerabilities on the other side.

The Cyber Defense Policy Working Group (CDPWG) was set up following the 2013 meeting of the Security Consultative Committee (SCC) to increase cooperation in cybersecurity between the U.S. DoD and Japan's MOD. Discussions focused on (a) the threat environment, (b) close MoD-DoD cooperation if an attack occurs, (c) roles and missions, (d) information sharing, and (e) critical infrastructure protection. It is chaired by the Deputy Director General (DDG) of the MoD in Japan and the Deputy Assistant Security of Defense (DASD) for Cyber Policy in the United States.

The MOD is organizing a working group on cybersecurity defense policy to share information on incidents and other critical issues between the government and military contractors. As shown by the MHI penetration in 2011, military contractors remain a high-value target for cybercriminals, rival companies, and opponents' intelligence services.

4.1.3 Other Collaborative Venues[44]

In addition to diplomatic and defense dialogues there are many other bilateral channels. For example, the Cyber Working Group at the American Embassy, Tokyo includes representatives from DHS, Justice, Treasury, Commerce, and other organizations, who also engage with their Japanese counterparts. The U.S. officials in this working group are not cybersecurity specialists themselves, however they can call on cybersecurity experts within their departments and agencies, and act as channels of information between U.S. and Japanese government departments on cybersecurity issues. The Assistant Secretary of Commerce was in Tokyo in May 2016 for a Cybersecurity Trade Mission, which also resulted in a digital attaché being assigned to the Embassy.

There has been a series of dialogues over the preparations for the 2020 Olympic and Paralympic Games. Japanese cybersecurity leaders have met with INTERPOL and counterparts from the 2012 London and 2016 Rio Olympics. Japan hosted a global ISAC meeting in November 2016, and there was an APEC telecommunications meeting the same month. According to Japanese press reporting, MIC has "started the IoT Cybersecurity Action Program 2017 to hold Cybersecurity Task Force meetings with experts, enhance the security level of IoT devices, develop cybersecurity professionals, launch Internal Affairs and Communications Minister Award for cybersecurity professionals and organizations, and expand global cooperation. MIC also plans to hold Cyber Colosseo exercises to prepare for Tokyo 2020 by the end of JFY 2016 [Mar 31, 2017]."[45] There are several other cybersecurity exercises and training programs, some of which involve DHS.[46]

On the non-profit side, the Japan Cybercrime Control Center (JC3) meets with the U.S. National Cyber-Forensics & Training Alliance (NCFTA). On the private sector side, the American Chamber of Commerce in Japan (ACCJ) has an economic task force and is standing up a cybersecurity task force. Google chairs the Internet Economy Task Force. An academic Center of Excellence (CoE) has been established at Keio University. A U.S. technology firm has held a number of well received "trust symposia" for Diet members.

4.2 Government-Private Partnership

Despite the potential value of any campaign to harmonize the cybersecurity efforts of both nations' governments and private sectors, there are legal, pragmatic, cultural, and competitive hurdles to effective cooperation, which impede progress. There is more cooperation and information sharing between the USG and American companies than there is between the GOJ and Japanese companies, but in neither country is there full trust and sharing. Despite the pervasive and persistent threat, a number of companies in each country will not consider working with the government until they are in a crisis and responding to a cybersecurity incident, rather than on an ongoing and proactive basis.

Obstacles to effective public-private cybersecurity cooperation in both the United States and Japan include: (a) issues surrounding trust and control of incident response in a siloed organizational environment; (b) questions about obligations regarding disclosure and exposure; (c) the evolving liability, risk management, and regulatory landscape; (d) attribution challenges faced in cross-border investigations of cybercrime; and finally, (e) domestic and international data transfer restrictions that impede the ability of private industry to respond nimbly to cybersecurity threats and incidents.

Given the diverse range of resources, priorities, and perspectives that government and industry bring to all these issues it is not surprising they sometimes compete. But, at a strategic level, they often are fundamentally aligned in a shared desire to develop effective strategic solutions to the many cybersecurity challenges. The key is to maximize the collective resources of business and government in both countries where they do align.

Ultimately no single actor (or group of actors) can figure it out alone. A strategic cybersecurity solution must combine the resources and skill sets of government and industry, informed by academia, within a practical framework that balances effectiveness with efficiency and security with privacy and innovation. Achieving this requires an understanding of the benefits, barriers, and alternatives to effective coordination, and why the nature of the problem demands new and innovative forms of collaboration. In fact, the governments and private sectors in both countries have good ideas. The challenge is to move beyond broad policies to institutionalize and expand ways of working together, and to implement these steps effectively.

5. How the Differences in Organization and Other Matters Affect Coordination

Senior levels of government in both nations have committed to improving cybersecurity, and both countries have taken significant new initiatives in the past several years. The kinds of cybersecurity incidents described above should have increased pressures on politicians, regulators, and corporate executives to act, but they still have not done so sufficiently. The higher overall interest in national security in the United States; the larger size of the defense, homeland security, and intelligence budgets; the acknowledged government role in protecting critical national infrastructures (while leaving the lead to the private sector infrastructure owners); and the willingness to use more active cybersecurity defense measures make the USG more likely than Japan to be proactive in various cybersecurity areas. These take certain matters off the table for coordination in bilateral channels, as well as in international fora. But there still are many opportunities for collaboration.

In any bureaucracy there is a natural tendency to try to control information for a variety of reasons, but the more networked nature of the USG—and the general difficulty of keeping things secret today—probably makes USG personnel more inclined to share than their counterparts in the GoJ. It also may be that Japan suffers more from siloing of information than does the United States. However, the establishment of the Japanese NSC and its secretarial arm, the National Security Secretariat (NSS), is changing the landscape. The Prime Minister's Office (Kantei) of the Abe

administration is much more aggressive than any previous administration's in making the "intelligence cycle" work. The Japanese intelligence community is receiving a large number of requests and orders from the Kantei.

Japan's establishment of the International Counter-Terrorism Intelligence Collection Unit (ICTICU) under the Ministry of Foreign Affairs (MOFA) in December 2015 is also changing the situation.[47] The NSC and the NSS "demand" information from the intelligence community, while the ICTICU primarily is on the "production" side. Though the ICTICU's overall mission is less clear and currently not strong legally, it was established based on collaboration among MOFA, the NPA, the MOD, the PSIA, and the CIRO. These ministries and agencies are providing talented officials to the ICTICU, enabling it to grow both in capability and capacity. Cybersecurity is one of the highest priority agendas for the ICTICU.

Securing and utilizing sensitive data is another task, which both governments should tackle. Both nations place a high value on citizen privacy, and particularly on protecting patient medical records. However, the United States is farther along than Japan in digitizing medical records and in "anonymizing" such data, so that aggregate statistics can be collected and analyzed quickly about disasters, disease outbreaks, etc. Because the U.S. private sector seems to have more experience in applying "big data analytics" to anonymized individual information for profit, (e.g. bundling general information on people's locations derived from their cell phone "externals" and selling it to "proximity marketers"[48]), the United States probably could make better use of such private sector information as part of a disaster response, as well as in responding to complex scenarios involving both virtual and physical attacks.

A particular concern in Japan is how to cover liabilities, how to allocate risk, and who ultimately takes responsibility for actions. This can be paralyzing and the issues need to be understood better. A robust cybersecurity insurance industry could address some of these questions by monetizing risk. A related problem is that it generally is acceptable in Japan to talk about vulnerabilities writ large, but discussions of specifics often raise sensitive matters of both face and trust, which curtail dialogues. In some cases, the USG, or outside observers, may be able to facilitate such exchanges.

Neither nation has enough technically skilled people in government. Moreover, people in key policy positions typically are not comfortable with ICT or networked technologies. This lack of technical proficiency and diversity of opinion runs the risk of groupthink.[49] Education and training programs can improve the technical proficiency of the staff that support senior leaders to help them provide better advice.

One of Japan's strengths is that it can move quickly once a decision or consensus is reached. So the approaching 2020 deadline (like Y2K in 2000) may provide a means to mobilize support.

6. "Whole-of-society" Approaches to Overcoming Impediments

Section 4 outlines many of the collaborative measures that are underway between the United States and Japan. The question is how to make them more effective.

Cybersecurity impacts are so pervasive, and the required actions so distributed, that preparations and responses must be "whole of society" efforts. Moreover, since cyberspace issues transcend sovereignty domestic solutions alone are no longer adequate. Neither nation has a monopoly on best practices and both need to show they can move beyond present management practices to do better. Fixes cannot be mandated by "top-down" decrees. Citizens will have to "buy in" all the way down to the daily use of their computers and mobile devices for approaches to be really effective. Success will require exceptional communications skills (or a massively impactful external event) and an understanding of the several target audiences to raise the importance of cybersecurity in the public's eyes. This

can then be leveraged to influence attitudes, laws, policies and resources to produce a more effective national posture. Nuanced understanding about differences among cybercrimes, cyberwarfare, cyberespionage, cybersecurity incidents, cyberattacks, etc., will need to be internalized and articulated, at least by those who speak to policymakers or to the public.

Both nations will have to overcome profound citizen distrust of both experts and government pronouncements and recognize that there will be no technological "silver bullet." Effective solutions will have to integrate "people, organizations, processes, and technology" (sociology always trumps technology).

Japan has done this before. People at all levels embraced the importance of quality control in the 1950s and adapted it as a pillar of the nation's economic prowess. In the '60s and '70s, Japan recognized the need for dramatic improvements in the environment. In these cases, there were visible individuals (e.g., W. Edwards Deming, in the case of the children of Minamata disease) or conditions (e.g., pollution in Tokyo) to catalyze action.

It is not clear what symbol would be catalytic today, but concerns about information sharing, anonymized records, and liability in a cybersecurity context are similar to those raised in situations in which the Japanese people have shown significant interest, such as counterterrorism[50] and natural disasters, especially in light of lingering concerns in the aftermath of 3-11.[51] Thus, converging issues like the approaching Olympics, with its 2020 "date certain;" concerns about much-discussed pending natural disasters, like an earthquake in Tokyo; and fears that ISIS or others may target Japan[52] could be woven together to promote meaningful changes in information sharing policy, anonymization of records, and allocation of liability that could be useful in several contingencies. The fact that the United States uses the same National Response Framework and National Incident Management System for responses to cybersecurity incidents as for terrorist attacks and natural disasters could serve as a model.

"Serious games" could be used to supplement information sharing and education and highlight issues for a variety of audiences.[53] "Tabletop exercises" (TTXs) are ideal venues to inform senior officials, and can be complemented by technical approaches like hacking ranges for cybersecurity defense practitioners. If done cleverly, videogames and other types of entertainment could engage the general public. The results should be publicized in ways that highlight best practices rather than "shaming" mistakes. These could be integrated with emergency planning and disaster response games to show the linkages between cybersecurity and other whole-of-society problems and potential solutions. The RAND Corporation's "Day After" methodology has been useful in many scenarios, and the repeated emergency response exercises New York City had held before 9-11 bore fruit when needed. Japan already is conducting a variety of cybersecurity-related exercises.[54] Perhaps elements of the U.S. National Cyber Incident Response Plan (NCIRP) could be of value to Japan.

Since employees pose probably the greatest security risk, cooperating on new ways to help them understand data security needs would be an excellent starting place.

7. Recommendations

The study makes recommendations to improve cybersecurity collaboration in four areas:

- Between the U.S. and Japanese governments in civil sectors—both infrastructure and business-related
- Between U.S. Armed Forces and the Japan Self-Defense Forces on military networks
- Between the public and private sectors
- Among private sector entities

Implementing the steps below could help overcome impediments to U.S.-Japan cybersecurity collaboration while building on strengths.[55]

7.1 Improving technical coordination between the governments in civil sectors

There are excellent opportunities to strengthen the ties between NISC on the Japanese side, and the NCCIC (within DHS) on the U.S. side. These two organizations are connected with the rest of the stakeholders in their respective governments, and with several private sector organizations. These collaborative operations could take place at three levels: (a) the ongoing protection of government networks, (b) post-incident response, and (c) protection of critical infrastructure(s). One recurring problem has been personnel turnover on both sides, so there will need to be a more structured engagement, which can include the exchange of liaison officers and having scheduled conference calls. This is discussed below.

Within Japan's NISC, the GSOC mainly watches over the computer systems and networks of GOJ ministries. As a result of the GSOC's discovery of the hack of the Japan Pension System (JPS), the government extended GSOC's monitoring abilities to cover government-affiliated organizations, which today includes administrative agencies and special public corporations. In 2017, the expected budget and staff increase of both the NISC and GSOC will enable these organizations to better fulfill their roles as cybersecurity control centers.

On the U.S. side, NCCIC acts as a "24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the federal government, intelligence community, and law enforcement."[56] It is a logical counterpart to the GSOC for monitoring, situational awareness, and response oversight.

In the general cybersecurity incident response area, US-CERT[57] and JPCERT/CC[58] perform comparable functions and both are members of the global Forum of Incident Response and Security Teams (FIRST).[59] They too would be logical partners.

The U.S. Industrial Control Systems CERT (ICS-CERT) is more focused on incidents involving critical infrastructures.[60] As noted earlier, Japan plans to establish the ICPA in 2017, which will be capable of defending critical systems by the time of the 2020 Olympics. The ICPA's active response division[61] would be a logical partner for ICS-CERT.

Information to be shared within the channels above:

- Pre-incident: Japan's strategy encourages relevant parties to report even small-scale damage and signs of suspicious activity to safeguard against large-scale cyberattacks. It also seeks to bolster both internal and external systems for cooperation and information sharing. Japan seeks to prevent incidents by monitoring networks and systems and sharing information about cybersecurity incidents among different agencies and with global partners. A problem in both countries is that many private companies do not report routinely to the government, much less to each other. Nonetheless, while it may not be practical to share all "small-scale damage and signs of suspicious activity,"[62] efforts still should be made, such as accumulations of indicators pointing to mutual threats. Other pre-attack exchanges could include statistics on attacks over, for instance, the previous quarter; forensic data from serious individual attacks; specific malware signatures; and suspicious IP addresses.
- Trans-incident and post-incident: Information sharing and cooperation among organizations during and after cybersecurity events should conform to established CERT processes.

Over time the quality of sharing is likely to improve as experience is accumulated and trust built.

Recommendation: Establish exchange positions at both the GSOC and NCCIC. Past concerns about personnel turnover could be improved if the points of contact on both sides were tied to billets, such as office directors or equivalents, vice individuals who might not be replaced. This could improve continuity amidst the inevitable rotations. In addition, hosting periodic (e.g., quarterly) secure videoconferences among leaders and stakeholders could be augmented by in-person meetings (e.g., annually), as well as real-time coordination when incidents do occur.

Similar relationships should be explored between US-CERT and JPCERT/CC and between ICS-CERT and ICPA. Although relationships between US-CERT and JP-CERT are already strong, the ICS-CERT addresses a problem that is growing globally. This area requires further evaluation to establish improved and more consistent communications.

7.2 Improving U.S. and Japanese government collaboration on military networks

Several innovative initiatives are underway to improve U.S. and Japanese collaboration on military networks. Today there is connectivity on several channels, such as NIPRNET (Non-Classified Internet Protocol Router Network), SIPRNET (Secret Internet Protocol Router Network), CENTRIXS-J (Combined Enterprise Regional Information Exchange System-Japan) and others. The United States is establishing a Mission Partner Environment (MPE) to promote multinational information sharing (MNIS) globally with allies and coalition partners within communities of interest (COI). An emerging component is the Common Mission Network Transport (CMNT), which will let multiple networks share a common transport layer instead of having to rely on separate, duplicative infrastructures. The extensive use of virtualization allows for COIs to be established within days within the MPE, instead of months. Moreover, since the overall CMNT is protected with commercial communications security, it will make it much easier for Japan to join via Mission Partner Gateways (MPGs) using its own communications and cryptographic equipment. In addition to bilateral U.S.-Japan COIs, this also will facilitate partnerships like the Japan Area Defense Coalition (JADC) and multilateral engagements like the Northeast Asia Coalition.

Current MOD policy prohibits direct connection of JSDF networks with foreign country networks, but the MPE is designed to provide a shared, international, collaborative network environment. Since much of it is virtual and makes use of commercial security equipment, it should be easier to get approvals from both sides to at least begin serious exploration.

Recommendation: Make it a priority to include Japan in MPE and CMNT. Begin with government-to-government talks to make sure that Japan's reluctance to join is not based on outdated understandings. Japan could apply its own security policy for a Japan CMNT-like network. In any case, improving understanding of the value added by the CMNT concept is an important first step in this process.

Continue to collaborate on ways to improve existing bilateral military communications, including the CENTRIXS-J network. The MPE and MPE transport issue should be a formal agenda topic at upcoming U.S.-Japan senior military conferences, including consideration for developing an implementation plan.

Encourage Japanese firms to develop equipment that can be certified for use in the MPGs (Japan's entry into the MPE). Establish a combined U.S.-Japanese network operations center for this environment, with exercises, red teaming and training as appropriate. Provide mutual assistance in case of cybersecurity incidents. Both JSDF and U.S.

Pacific Command (PACOM) should include the evaluation of MPE in their exercises or with demonstrations within the Pacific Warfighting Center (PWC).

This cooperation will enable both the MOD and PACOM to investigate more closely the technology gaps currently impacting Japan-U.S. interoperability, both in operational systems and those under consideration. Underpinning all efforts should be a recognition that the effective defense of Japan's networks is essential not just to Japan, but also to the Alliance itself. The reverse also is true.

7.3. Strengthen public-private cybersecurity cooperation

As noted earlier, ISACs are designed to improve communications and coordination between the private and the public sectors, focused on sector-based critical infrastructures. Their goals are to share information and analysis and provide incident response recommendations to their members, but their record has been mixed, both for public-private and for private-private coordination. Arguably ISACs work best when specific cybersecurity vulnerability gaps can be identified and dealt with promptly. However, given the rate of change in today's threat environment and uncertainty about areas such as the relationship between the IoT and infrastructure vulnerability, the value is less clear.

Recommendation: Improve public-private collaboration by focusing on the common ISACs—the U.S. Communications, Financial Services, and Information Technology ISACs and their Japanese counterparts—the ICT and Financial Services Japan ISACs. Promote (a) government actions to improve information flow to the ISACs and to address legal, policy, and regulatory issues of concern; (b) private sector actions to let companies share more of the large amounts of information they have on their networks with organizations that can do something about it, such as law enforcement; and (c) direct bilateral coordination to facilitate more effective international exchanges.

This approach would allow Japanese leaders to manage their respective ministry or agency issues better and to work on salient sector questions with their USG partners and private-sector stakeholders. The process should emphasize capabilities development, rather than only information exchanges—fixing security gaps while increasing understanding of how to balance privacy and security issues. Particular focus needs to be placed on rationalizing the very complicated rules for international data exchange in different countries, as well as clarifying liability issues around information sharing.

Collaborative mechanisms must produce value to give business a reason to participate, so activities should be well attuned to stakeholder needs and not just collaboration for collaboration's sake. The particular needs of SMBs need to be addressed. They are generally straightforward. For the most part, these small companies do not want to sit in on weekly staff calls but rather to know what actions they need to take to prevent or to stop attacks.

7.4 Strengthen private-private cooperation

Private-private cooperation can be improved in several ways. The Industry 4.0 discussions at the November 2016 Cyber3 conference emphasized expanding cybersecurity information sharing within corporate groups, but didn't pay much attention to sharing with other companies. ISACs may not be the best organizations for this. Just as ISAOs are being organized in the United States around COIs, other new, self-organizing, collaborative relationships are popping up today, focused on what's happening within their communities to clarify the indicators and/or types of reconnaissance an adversary may be applying. These human driven activities enable proactive collaboration, not just

amongst themselves but also with partners in law enforcement, diplomatic, or financial groups all contributing to the successful hunt of the adversary.

Questions for this coordination process include:

- What are the stakeholders looking for to improve their information sharing?
- What will happen to the information once it is gathered?
- What do the stakeholders get in return?

The answers could help build an information-sharing framework, which could lead to an automated exchange. This process can be accomplished in an anonymous fashion to achieve actionable intelligence that can be used to identify and/or disrupt the adversary.

One important function that the private sector can lead is training, at several levels. At the most senior levels, ISACs, ISAOs, and COIs are well suited to sensitize corporate leaders to macroscopic cybersecurity risks. At the next level, organizations themselves need to be training continuously. This includes organizing and participating in periodic large exercises with on-going smaller scale penetration testing and red-teaming to ensure best practices are being adhered to. These training events should include diverse participation with SMEs from relevant agencies, the private sector and academia. Finally, ISACs, ISAOs, and COIs can be used to train the workforce.

Recommendation: Survey private sector organizations in both countries to identify the ISACs, ISAOs, and COIs with which members are particularly satisfied. Share best practices and examine ways to institutionalize these approaches. Focus particularly on training (at all levels), incentives for sharing, exercises, and red-teaming.

Although not an explicit recommendation of this section, increased resources for cybersecurity are a recurring theme. Virtually all studies recommend that both governments allocate more funds, support measures, and trained people to cybersecurity and promote capacity building in cybersecurity and related intelligence areas. One aspect that may be overlooked, but which is potentially very important is the kind of defense-related research projects in academia that Japan's MOD started funding in 2015. Recognizing the sensitivities of JSDF cybersecurity activities, it should be recognized that the Japanese public probably would expect the JSDF to contribute to the nation's defense in case of a serious cybersecurity incident affecting CNI. This kind of research deserves continued attention.

8. Conclusion

Approaches that break down information-sharing stovepipes and cut across multiple infrastructures are particularly important. The fact that both Japan and the United States already have processes in place to respond to terrorism or mass casualty situations should be leveraged so that major cybersecurity incidents can be addressed within the same frameworks.

Education at all levels will be essential, especially in Japan, to raise public awareness and cause them to put pressure on public officials. This is necessary since people will be reluctant to act decisively until legal questions relating to risk, liability, and problem ownership are clarified. The Japanese people have wholeheartedly embraced society-wide solutions to new technical problems before, with the mandates they gave to quality control in the '50s and environmental quality in the '70s. They can do so again.

The impending deadline of the 2020 Olympic and Paralympic games often is cited as a "forcing function." But all parties need to make sure that it doesn't become an excuse for expecting that someone else "must" do something.

By most accounts Tokyo already is behind where London was in getting ready for the Olympics. The time is short, and new threats such as ransomware and denial of service attacks from the IoT will further complicate preparations.

The current structure of general discussions between the governments of the United States and Japan can be strengthened with focused meetings between organizations with comparable cybersecurity responsibilities, with agendas that discuss the details of recent incidents, and by comparing recovery measures and plans to deal with other potential cyberattacks.

In sum, the next few years offer great opportunities to improve cybersecurity in both Japan and the United States, but also add significant risks if the chances to fix weaknesses are ignored.

Notes

1. These studies include: (a) Center for Strategic & International Studies (CSIS), U.S.- Japan Cooperation in Cybersecurity. A Report of the CSIS Strategic Technologies Program. Author: James Andrew Lewis. November 2015. (https://www.csis.org/analysis/us-japan-cooperation-cybersecurity) (b) Cybersecurity Strategy, September 4, 2015, Cabinet Decision, The Government of Japan. (http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf), (c) CISCO 2016 Midyear Cybersecurity Report, July 2016 (http://www.cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html?POSITION=SEM&COUNTRY_SITE=us&CAMPAIGN=SC-04+threat-centric+security&CREATIVE=SEM_SC_Security_(BMM)_(B)-Report_MSR&REFERRING_SITE=Bing&COUNTRY=United%20States&KEYWORD=%2Bcisco%20%2Bmidyear%20%2Bsecurity%20%2Breport&KWID=p12066135149&KEYCODE=001344793&utm_source=bing&utm_medium=cpc&utm_campaign=US_SEM_SC_Security%20(BMM)%20(B)&utm_term=%2Bcisco%20%2Bmidyear%20%2Bsecurity%20%2Breport&utm_content=Report_MSR&dclid=CPLQvJXgwtECFZQGDAod_mQNXA), (d) "Japan's Approach Towards International Strategy on Cyber Security Cooperation" by Yoko Nitta, Japan Science and Technology Agency (JST) / Research Institute of Science and Technology for Society (RISTEX). (http://lsgs.georgetown.edu/sites/lsgs/files/Japan_edited%20v2.pdf_for_printout.pdf), (e) Center for International Public Policy Studies (CIPPS); Cyber Security in Japan (V.2), R. Masuoka & T. Ishino, Cyber Security Policy Research Team, Dec. 2012. (http://www.cipps.org/group/cyber_memo/003_121204.pdf), (f) The Diplomat. "Japan's Achilles Heel: Cybersecurity" by Mina Pollman, April 13, 2016. (http://thediplomat.com/2016/04/japans-achilles-heel-cybersecurity/), (g) Deloitte Press Release. Asia-Pacific Outlook 2016. Report finds accelerating naval buildup, growing vulnerability of Asia-Pacific's "Cyber Five" nations, Feb. 24, 2016. (https://www2.deloitte.com/sg/en/pages/public-sector/articles/deloitte-2016-asia-pacific-defense-outlook.html), (h) Japan's Changing Cybersecurity Landscape By: Nir Kshetri (2014). Japan's changing cyber security landscape, Computer, 47(1), 83–86. doi: 10.1109/MC.2014.17 Made available courtesy of Institute of Electrical and Electronics Engineers(IEEE); (http://libres.uncg.edu/ir/uncg/f/N_Kshetri_Japans_2014.pdf), (i) The Software Alliance. Asia-Pacific Cybersecurity Dashboard. Country: Japan. (http://cybersecurity.bsa.org/2015/apac/assets/PDFs/country_reports/cs_japan.pdf), (j) Georgetown Journal of International Affairs, Cyber Intelligence: The Challenge for Japan, March 17, 2015. (http://journal.georgetown.edu/cyber-intelligence-the-challenge-for-japan/), (k) Business Insider. Associated Press. "Japan its Own Enemy in Push to Improve Cybersecurity", Gerry Shih, Nov. 8, 2015. (http://www.businessinsider.com/ap-japan-its-own-enemy-in-push-to-improve-cybersecurity-2015-11)

2. Melissa Hathaway's Cyber Readiness Index 2.0 (CRI 2.0) measures cyber readiness across seven dimensions: (a) National Strategy, (b) Incident Response, (c) E-Crime and law enforcement, (d) Information sharing, (e) Cyber R&D, (f) Diplomacy and trade, and (g) Defense and crisis response.

3. Derived from draft U.S. National Cyber Incident Response Plan (NCIRP) https://www.dhs.gov/blog/2016/09/30/national-cyber-incident-response-plan-now-available-public-comment

4. Taxonomy from Melissa Hathaway's presentation to the Sasakawa USA-Auer Center conference on critical infrastructure protection, December 2, 2016, Washington, DC.

5. See, for example, outputs from the Sasakawa USA Conference *Supply Chains, Security, and Cyber Threats: Promoting U.S.-Japan Cooperation to Mitigate Risks and Improve Practices,* March 9, 2016. http://spfusa.org/event/supply-chains-security-and-cyber-threats-promoting-u-s-japan-cooperation-to-mitigate-risks-and-improve-practices/

6. Some approaches are described in CRI 2.0.

7. Cisco Mid-Year Security Report 2016: The Rise of Ransomware https://mkto.cisco.com/Mid-Year-Security-Report.html

8. CNAP https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan The CNAP builds on a 2015 effort called the Cybersecurity Sprint.

9. PPD-41 http://fas.org/irp/offdocs/ppd/ppd-41.html

10. NCIRP https://www.dhs.gov/blog/2016/09/30/national-cyber-incident-response-plan-now-available-public-comment The NCIRP was open for comments in Sept-Oct 2016. The comments now are being incorporated.

11. In May 2009 President Obama accepted the recommendations of a Cyberspace Policy Review that built on the Bush Administration's Comprehensive National Cybersecurity Initiative (CNCI). https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative The list above is a subset of accepted CNCI initiatives that could apply to U.S.-Japanese collaboration.

12. National Cyber Mission Force http://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability

13. For example, DoD's include: The DoD Cyber Strategy, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, and the DoD Cybersecurity Discipline Implementation Plan of Oct 2015, updated to Feb 2016, http://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf

14. ISAOs were encouraged in 2015 through Executive Order 13691 https://www.dhs.gov/isao

15. Drawn from CNAP press release, *op. cit.*

16. https://www.nist.gov/cybercommission

17. PPD-41 is at http://fas.org/irp/offdocs/ppd/ppd-41.html

18. PPD-41 defines a cyber Incident and a significant cyber incident as follows:

Cyber incident: An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For purposes of this directive, a cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Significant cyber incident: A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

19. PPD-41, Section VII

20. PPD-41 Section III

21. Federal response coordination for significant cyber incidents is described in PPD-41, Section V.

22. Organization and functions drawn from: https://www.dhs.gov/blog/2016/09/30/national-cyber-incident-response-plan-now-available-public-comment

23. NCIRP draft of Sept 30, 2016 https://www.us-cert.gov/sites/default/files/ncirp/NE%20DRAFT%20NATIONAL%20CYBER%20INCIDENT%20RESPONSE%20PLAN%2020160930.pdf Comments received on the NCIRP during National Cybersecurity Awareness Month are being adjudicated. https://www.dhs.gov/national-cyber-security-awareness-month

24. NRF http://www.fema.gov/national-response-framework

25. National Preparedness Goal http://www.fema.gov/national-preparedness-goal

26. NIMS http://www.fema.gov/national-incident-management-system

27. Framework for Improving Critical Infrastructure Cybersecurity, version 1.0. NIST, February 12, 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/roadmap-021214.pdf

28. Cybersecurity Scorecard. https://cdn2.hubspot.net/hubfs/533449/SecurityScorecard_2016_Govt_Cybersecurity_Report.pdf?t=1467846772274

29. Sony Pictures Entertainment itself is an American company, but SONY brand originates in Japan.

30. Scott W. Harold, Martin C. Libicki, Motohiro Tsuchiya, Yurie Ito, Roger Cliff, Ken Jimbo, Yuki Tatsumi, *U.S.-Japan Alliance Conference: Strengthening Strategic Cooperation*, Santa Monica: RAND Corporation, 2016. See especially Chapter 3: "Japan-U.S. Cooperation on Cybersecurity," by Motohiro Tsuchiya.

31. The NISC tried to keep its acronym as NISC and ended up with a strange name with "cybersecurity" and without "Information security."

32. http://news.softpedia.com/news/japan-to-create-cyber-defense-government-agency-to-protect-scada-infrastructures-504293.shtml

33. Japanese text of the Telecommunications Business Act is available at http://law.e-gov.go.jp/htmldata/S59/S59HO086.html

34. Japanese text is found here, https://www.jaipa.or.jp/other/mtcs/guideline_v3.pdf

35. From Tsuchiya, RAND Chapter 3.

36. Ministry of Foreign Affairs of Japan, "U.S.-Japan Joint Vision Statement," April 28, 2015.

37. G7 Principles and Actions on Cyber, May 27, 2016, http://www.japan.go.jp/g7/summit/documents/

38. From Tsuchiya, RAND Chapter 3.

39. Ministry of Defense of Japan, *Guidelines for Japan-U.S. Defense Cooperation*, April 27, 2015.

40. Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York: Cambridge University Press, 2013 Rule 30.

41. http://www.mod.go.jp/e/d_act/others/pdf/stable_and_effective_use_cyberspace.pdf

42. See, for example, William J. Lynn III, "Defending a New Domain: The Pentagon's Cybersecurity Strategy," *Foreign Affairs,* September/October 2010. https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

43. "Cyberattacks against Japan Ground Self-Defense Force (Rikuji System Ni Cyber Kogeki)," http://www.sankei.com/affairs/news/161128/afr1611280003-n1.html (in Japanese)

44. Based on conversations with personnel in Washington and Tokyo.

45. MIC started the IoT Cybersecurity Action Program 2017, which includes global collaboration

http://www.soumu.go.jp/main_content/000458523.pdf

46. Japanese and US governments will work together on cyber exercises and training in FY 2017. http://www.yomiuri.co.jp/politics/20170104-OYT1T50001.html

47. The Ministry of Foreign Affairs, "Press Conference by Foreign Minister Fumio Kishida," Ministry of Foreign Affairs http://www.mofa.go.jp/press/kaiken/kaiken3e_000011.html, November 24, 2015.

48. Douglas Karr, "What is Proximity Marketing?" https://marketingtechblog.com/proximity-marketing/

49. https://www.weforum.org/agenda/2016/08/why-governments-and-all-of-us-need-to-do-more-to-prevent-cyber-threats/

50. For example, in January 2013, a Japanese company, Nikki, in Algeria was hit by Islamic terrorists and seven Japanese were found dead. In 2015 seven employees of JICA (Japan International Cooperation Agency) in Bangladesh were killed by an armed group.

51. 3-11 represents March 11, 2011, the date of the Great East Japan Earthquakes and Tsunamis that hit Tohoku (North East) part of Japan covering Iwate, Miyagi, Fukushima and Ibaraki prefectures. The tsunamis caused a serious nuclear incident at Fukushima Daiichi Nuclear Plant.

52. Two Japanese were captured in Syria and killed by ISIS in January and February 2015. See, for example, Tomoko Otake and Shunsuke Murai, "'Proactive pacifism' makes Japan a target for Islamic terrorists: experts," *Japan Times*, November 16, 2015. http://www.japantimes.co.jp/news/2015/11/16/national/proactive-pacifism-makes-japan-target-islamic-terrorists-experts/#.WBTMMuArLDc

53. https://www.dhs.gov/cyber-storm

54. Japan CRI 2.0, p. 4

55. This list was expanded from Nikkei-CSIS Virtual Think Tank's policy recommendation, which was published on October 21, 2016. In addition, the recommendations were compared with the studies cited in note 2 to eliminate duplicates and sharpen others. http://www.csis-nikkei.com/doc/%E7%AC%AC2%E5%9B%9E%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E6%8F%90%E8%A8%80.pdf

56. https://www.dhs.gov/national-cybersecurity-and-communications-integration-center

57. https://ics-cert.us-cert.gov/

58. http://www.jpcert.or.jp/english/

59. https://www.first.org/

60. https://ics-cert.us-cert.gov/

61. http://news.softpedia.com/news/japan-to-create-cyber-defense-government-agency-to-protect-scada-infrastructures-504293.shtml

62. Quote from Japan's *Cybersecurity Strategy 2015*