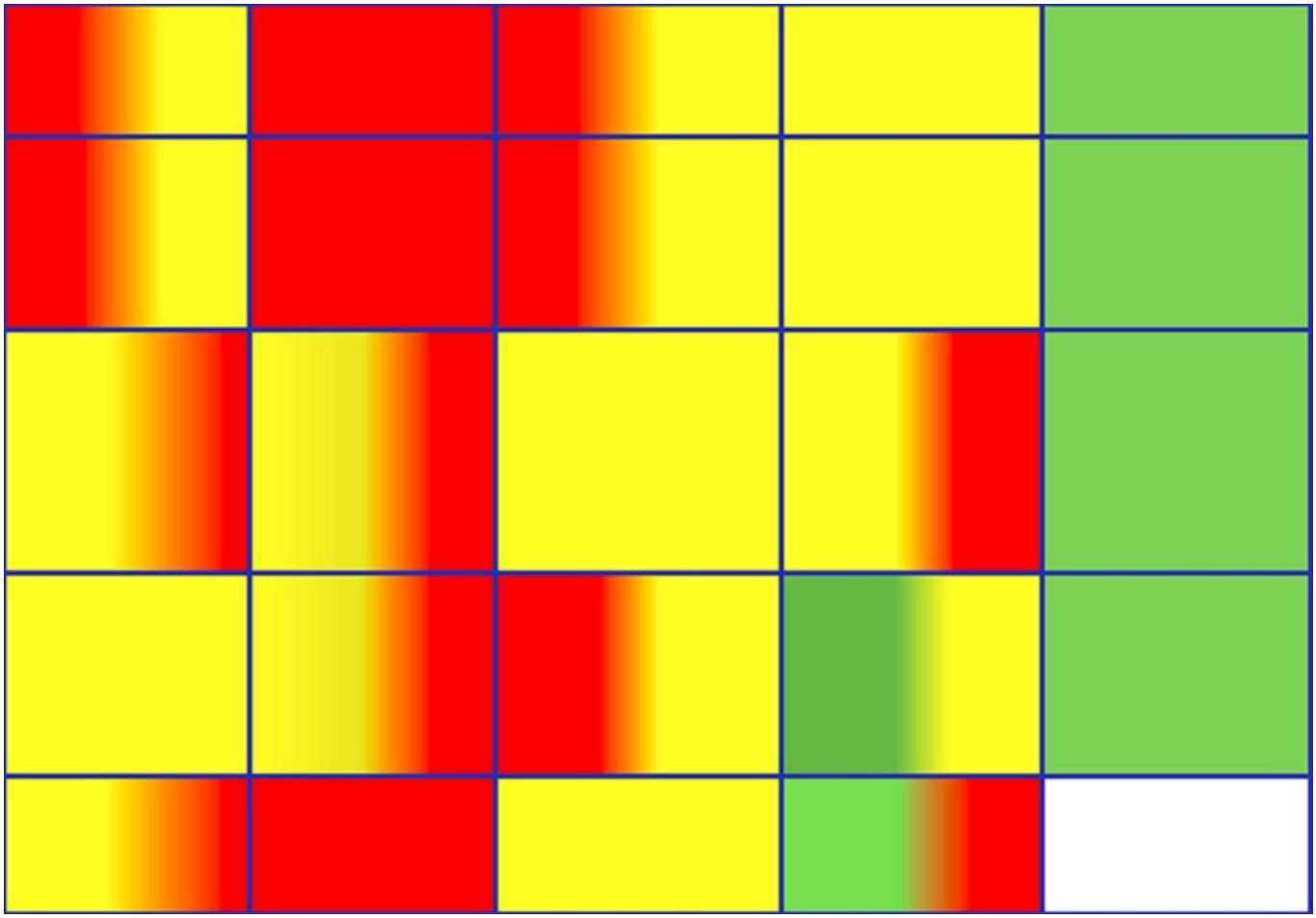
CHALLENGES IN RISK GOVERNANCE FOR SAFETY AND SECURITY IN JAPANESE NUCLEAR POWER SECTOR



Recommended Citation

Taketoshi Taniguchi, "CHALLENGES IN RISK GOVERNANCE FOR SAFETY AND SECURITY IN JAPANESE NUCLEAR POWER SECTOR", NAPSNet Special Reports, May 18, 2017, https://nautilus.org/napsnet/napsnet-special-reports/challenges-in-risk-governan-e-for-safety-and-security-in-japanese-nuclear-power-sector/

Taketoshi Taniguchi

May 18, 2017

I. INTRODUCTION

This essay by Taketoshi Taniguchi gives an overview of the risk environment surrounding critical infrastructures including nuclear power, and discusses challenges in nuclear power sector in order to avoid slow-developing catastrophic risk and to mitigate malicious threats. “Ultimately, a well-informed public, on top of adequate emergency preparedness and response plan, and growing capabilities, will be crucial for mitigating malicious threats and risks.”

Taketoshi Taniguchi is Professor at the Policy Alternatives Research Institute (PARI), the University of Tokyo.

Credit: Banner image is by Taketoshi Taniguchi and shows deficits revealed after Fukushima in various social capacities to respond.

II. SPECIAL REPORT BY TAKETOSHI TANIGUCHI

CHALLENGES IN RISK GOVERNANCE FOR SAFETY AND SECURITY IN JAPANESE NUCLEAR POWER SECTOR

May 18, 2017

1. Introduction

The East Japan Mega-quake and tsunami, and subsequent Fukushima nuclear disasters have really put risk landscape of Japanese society into relief. Faced the unprecedented disasters and subsequent confusion in the society, the author realized again that we are in an interconnected complex world with rapid technological progress. Increases of interdependency and complexity of socio-economic activities mean the strong links between physical, social and economic risks. And perception and awareness of risks are diversifying due to fragmentation and atomization of society. In addition, communication tools and devices with different characteristics such coverage, speed and capacity, can induce unstable dynamics of risk information delivery. These phenomena amplify systemic nature. The Fukushima nuclear disaster clearly illustrated these social phenomena.

Nuclear power in Japan has been tightly and complexly interlinked with and interdependent on socio-economic-political activities and has also produced nested or collective interests everywhere. Nuclear accident risk, therefore, may be relatively low in frequency, but it has broad ramifications for human health, safety and security, the environment, economic wellbeing and the fabric of societies.

This article provides my observation on critical deficits in nuclear safety risk governance before and after the Fukushima nuclear disaster and a brief overview of risk environment surrounding critical infrastructures including nuclear power, and discusses challenges in nuclear power sector in order to avoid slow-developing catastrophic risk and mitigate malicious threats.

2. Risk governance deficits observed from the Fukushima

Based on risk governance framework proposed by the International Risk Governance Council, the author conducted the deficit analysis of emergency preparedness and response and severe accident management of nuclear power plants in Japan before, during and after the Fukushima nuclear accident. In the case study, whether common governance deficits identified by IRGC could be observed or not, and to what extent are seriousness of the deficits have been examined subjectively and relatively by each major actor (electric utilities, regulatory authorities, academic and research institutions, administrative ministries and agencies, local government). As a result, many serious deficits were observed before the Fukushima. In summary, the followings are underlined as critical deficits.

First, risk-related knowledge base was deficient or inadequate. For emergency preparedness and response and severe accident management policy-making, a wide range of knowledge and information are inevitably needed and should be understood by decision-makers and responders in emergency situation. From these viewpoints, lacks of gathering knowledge about hazards and risks, their early signals, stakeholders' risk perception, interests and concerns were definitely fatal.

Second, interface problem among stakeholders was a serious underlying problem. For instance, a failure of interdisciplinary communication can be observed in the phase of risk knowledge generation. Advances in tsunami research have made the uncertainty of tsunami predictions more obvious in the tsunami experts' community. Nevertheless, their recognition of uncertainty was not transmitted to the nuclear safety experts. This example emphasizes a deficit, in which relevant stakeholders are not involved in the assessment process. Consequently, they missed or ignored early risk signals.

A lack and/or dysfunction of consultation not only between safety regulation personnel and security personnel in Nuclear and Industrial Safety Agency but also among the relevant ministries and agencies were also an example. Each requirement for ensuring nuclear safety and security would be contradictory or complementary according to the case. Authorities in charge, therefore, must continually consult with each other. But this awareness was absent in all the stakeholders. This is a likely underlying cause of inaction of terror countermeasures, so-called B.5.b, which was raised as a crucial issue from the U.S. experts in the Fukushima nuclear accident. This example demonstrated a failure to balance transparency and confidentiality needed for decision-making.

Third, appreciation or understanding fundamental changes and interdependencies of agents in complex societal system was lacking. During the period that nuclear power generation has planted its roots deeply in Japanese society, socio-economic-political fabric of the society including local communities where nuclear power plants are located has been significantly changing, and therefore, various interests and stakeholders have emerged, and their interdependent relationships became more complicated. Despite these situations, nuclear fraternity, being basically introverted, held only a narrow perspective (myopia). Inward-looking and non-holistic management might hinder awareness of the systemic and multi-faceted natures of many risks of critical infrastructure and economic system advancement.

Fourth, deficits in legal system and departmentalized emergency response scheme could exacerbate risks and make organizations insensitive to risk. These are obstacles of the all-hazards and the whole-of-government approaches to emergency preparedness and response.

Fifth, organizational capacity building for managing risks (in particular, specialized competence and knowledge, organizational integration, flexibility and its network) was inadequate. The backdrop of the deficit is an absence of safety culture. Both the regulatory authorities and power companies

structurally failed to assimilate “safety culture”, which is to reject satisfaction with status quo regarding safety, and diligently pursue autonomous reforms aimed at higher objectives. Instead, “safety culture” remained simply a pleasant sounding slogan without any behaviors for detection, recognition, sharing, assessment, or response to risks.

Lastly, scientific advices were not coordinated in crisis situation at all. In risk governance, scientific advice can play a critical role in not only the routine but also emergency situation. During the Fukushima nuclear accident, the Japanese government experienced difficulties in taking wholly consistent action. For instance, a restricted area was set up immediately, but its range was subsequently enlarged several times and evacuation or precautionary safety measures were modified over time without due provision of detailed information to the local residents. In the case of catastrophic event with systemic nature, it is really difficult but important to coordinate and synthesize scientific inputs from many different fields and institutions and to translate them into useful policy advice at very short notice.

Needless to say, lessons from the Fukushima and our challenges ahead are to urgently and seriously correct the deficits noted above. After the Fukushima, however, a few deficits are slightly corrected, but critical deficits still remain. Rather it seems that some deficits are getting worse.

3. Critical infrastructures and nuclear power facilities

3-1. Risk environment

Critical infrastructure represents “systems and assets, whether physical or virtual, so vital to the nation that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” Many assets are dependent upon multiple elements and systems to maintain functionality. In some cases, a failure in one sector will have a significant impact on the ability of another sector to perform necessary functions. Systemic risks are exacerbated by interdependencies among the units often because of weak links in the system. As services provided by critical infrastructure become ever more embedded in wider systems, it becomes increasingly important to maintain their integrity and resilience.

Nuclear power in Japan is a major part of electric power supply system that forms the fundamentals of critical infrastructures in the society. Nuclear power sector, therefore, has multiple dependencies and interdependencies with other critical infrastructure sectors and key resources owners and operators including energy supply, transportation and physical distribution, information and communication, medical services and public health, emergency services etc. These interconnectivities and interdependencies are brought into relief particularly in emergency response and recovery processes as demonstrated in the Fukushima. Thus, safety and security of nuclear power should be holistically appreciated in terms of system of systems rather than a single technological system.

The risk environment affecting interdependent coupled critical infrastructures is becoming an increasingly complex and uncertain in terms of threats, vulnerabilities and consequences. Recently critical infrastructure that has long been subject to risks associated with physical threats and natural disasters is now increasingly exposed to cyber risks. Critical assets, systems, and networks face many of the threats, including intentional threats such criminal (terrorist act, extremist act, individual criminal act, organized crime, corporate/insider sabotage, corporate espionage), unintentional threats/hazards (social, technical/accidental), heath threats/hazards (pandemics/epidemics, large-scale contamination), emerging technologies, and natural threats/hazards (meteorological, geological, ecological/global phenomena). In addition, serious

vulnerabilities may exist as a result of a retiring work force or lack of skilled labor in Japan. Skilled operators are necessary for infrastructure maintenance and, therefore, security and resilience.

These various factors influence the risk environment, along with the policy and operating environments, and create the backdrop against which decisions are made for critical infrastructure security and resilience. The complex environment with a dynamic nature underlines the challenge in securing and enhancing the resilience of the nation's critical infrastructure.

3-2. Policy environment

The government as risk bearer of last resort and critical infrastructure community should implement an effective balanced risk management under budget constraints to achieve security and resilience of civil society.

The Minister in charge of building national resilience was appointed in January 2013 and subsequently the Advisory Committee on National Resilience (Disaster Prevention and Mitigation: Bosai & Gensai) was set up in the Cabinet Secretariat. The Basic Act for National Resilience Contributing to Preventing and Mitigating Disasters for Developing Resilience in the Lives of the Citizenry (hereafter referred to as "Basic Act") was enacted in December 2013. Under the Basic Act, the Policy Outline, the Fundamental Plan and the Action Plan 2014 were developed.

Looking at national resilience initiatives, there are some shortcomings. Japan's national resilience policy and action plan are substantially partial to large-scale natural disasters and technical fixes from short-term perspective without using knowledge and findings derived from comprehensive risk assessments. Vulnerability analysis for making the action plan 2014 is methodologically immature comparing with ones used in the US Department of Homeland Security (DHS). In the vulnerability analysis done by each ministry and agency, the current status of achievement level of policies regarding responses to 45 worst events that should never happen in specific sectors and cross-cutting sectors is to be first qualitatively and quantitatively assessed, and countermeasures in each sector were decided based on administrative judgments. Interdependencies among sectors or critical infrastructures are not taken into account at all in risk scenarios development and risk identification. Quantitative assessment based on systems approach has not been conducted. Furthermore, what-if analysis is not carried out at all. It seems to be still zero-risk obsessions behind the Action Plan.

In order to help top-level policy-makers and critical infrastructure owners to make informed decisions on priority setting of resource allocation and burden sharing for reinforcing the national resilience, and to provide policy options for effective risk management and communication at national level, all-hazards risk assessment of critical infrastructures, taking their inter-dependencies into account, is needed. All-hazards approach means to focus on minimizing damages to citizens' lives, health and assets, vital societal functions and the environment regardless of the type or magnitude of hazard and threat, and enable to respond effectively and efficiently as the whole-o--government, as opposed to the dispersed authorities and responsibilities for disasters and emergencies.

3-3. Institutional challenges

The Japanese government still faces many challenges in managing risks. In particular, Nation's institutional set-up is important. First, it needs to establish a governmental office responsible for national risk assessment, which needs collaboration with agencies supervising vital societal functions/critical infrastructures and private sectors. Second, it is desirable to consider institutional arrangement for integrating and coordinating the dispersed authorities and responsibilities as national incident management system operating in the United States.

In order to maintain a secure and resilient society, the government must have horizon-scanning capacity to strategically forecast the possible socio-economic-political environments surrounding critical infrastructures. For building policy-relevant strategic foresight capacity, at first it is important to foster anticipatory thinking, which is an awareness of cognitive biases and mental

preparedness for wild card scenarios. Second is to develop an adaptive capacity that consists of learning with critical thinking and its feedback mechanism. Third is to promote more collaboration to collectively draw insights about our future and to create an interoperable environment under the responsibility of more than one department to pursue holistic and broad policy perspectives.

4. Nuclear Power with Slow Developing Catastrophic Risk (SDCR)

4.1 Slow-developing Catastrophic Risk

As the name implies, key characteristics of the risk are; slowly evolving changes that take place over a long period of time, imperceptible until reaching to a tipping point, difficult to anticipate, and dramatic, sudden, sometimes disastrous and irreversible, imminent and avoidable. Risks are endogenous, that is, arises from interactions and consequent changes with the system itself, rather than as a result of external factors.

Risks that built up over time in Japanese nuclear fraternity have been actualized. The Fukushima nuclear disaster was a typical SDCR event, although sudden natural events triggered. As noted above, serious deficits still exist in nuclear risk governance. Behind these deficits, there may be still affirmative awareness and attitude of justifying and maintaining the status quo. As a consequence, even if certain warning signs are found, any contradiction with an existing plan or purpose led to reluctance toward recognizing them as such. Furthermore, since safety and security culture have not been rooted genuinely in the organization, countermeasures or corrective actions are postponed. Even after the Fukushima, it seems that a moral hazard of the thought pervades all hierarchy, such as following the precedent, willful blindness, only formality (i.e. plowing the field, don't forget the seed), and autonomously deciding that the status quo is, for the most part, not negative. Moreover, within the governmental agency in particular it can be noted that practice of the bad-mark system affects in every aspect. Vested interests may wish to keep the status quo.

Nuclear fuel cycle issues are likely more complicated and uncertain, given public concerns after the Fukushima disaster. When bringing nuclear power plants back online as possible without corrective actions of risk governance deficits, nuclear power sector would undoubtedly have the potential of SDCRs. What signals foreshadow the imminence of endogenous tipping point in time for nuclear power sector to take appropriate action to avoid them or better cope with their consequences? To put our heads together for the question, the first hurdle we must overcome may be a head-in-t-e-sand mentality or a lack of imagination, where people refuse to believe that endogenous transition can truly occur.

4-2. Coping with malicious threats against nuclear facilities and critical infrastructures

Nuclear power assets, systems and networks including nuclear fuel fabrication, spent fuel storage, reprocessing and radioactive wastes management are increasingly exposed to many different kinds of threats and hazards. Under recent technological advancement, notable threats are cyber attacks and malicious usages of the emerging technologies such as drone, 3D-printing and forgery of ID card. In this circumstance, the Sep. 11 attack and the Fukushima, two key events have amplified the nuclear terror threat. In particular, the Fukushima demonstrated the devastating effects of radioactive materials release into the environment, even when it resulted from a non-malicious event. What if the two combine? The situation that spent fuel (currently, around 17,000 tons)

in temporary storage pools at the reactors undoubtedly generates even more under unforeseeable back-end businesses could bring about concerns against nuclear terror nightmare. As for nuclear terrorism, attacks by the improvised nuclear device and the intact nuclear weapon are a less or the least probable, given the extensive security measures employed. On the other hand, with aim of exploiting psychological impact, a radiological attack such dirty bomb is likely to occur. In the worst case scenario of nuclear attack on Japan, it will not only cripple the critical infrastructure supporting our economy and society but also will seriously harm our country's reputation affecting political standing in global arena.

In order to cope with malicious threats against nuclear facilities and critical infrastructures, the facility owners and operators have to reinforce not only preventive and protective measures but also intelligence gathering and analytical capability in cooperation with public safety authorities. For example, current spent fuel pools at reactors are not required to have safety features based on defense-in-depth concept, because the major premise is that they would be used only for short-term storage before spent fuels are removed for reprocessing. So that, taking uncertain back-end circumstance into account, the utilities have to consider without delay the physical protection system based on protection-in-depth, minimum consequence of component failure and balanced protection. And with regard to the threats, it should be considered the class of adversary (outsider, insider, outsider in collusion with insiders), the range of their tactics (i.e. deceit, force, stealth, or any combination of these) and their capabilities (i.e. knowledge of the PPS, level of motivation, skills). In particular, nuclear power sector should identify and prevent the potential insider threat resulting from infiltration or individual employees determined to do harm, and conduct exercises and blind drills to physically and mentally prepare employees for potential terrorist activity. Furthermore, it is important to identify and protect employees and other people with critical knowledge or functions.

Many governance deficits originate from the lack of an appropriate legal or regulatory framework. The imperfections to the legal system could not only hinder an anticipatory approach for regulated entities, but also prevent assurance of proper procedures, and induce distrust in the regulatory process. In regard to dealing with malicious threats noted above, two legal considerations are needed in the existing regulatory framework.

The first issue is to urgently introduce the personnel reliability certification system into nuclear regulation. Unlike the United States and other nuclear industrialized countries, the personnel reliability certification in the existing regulatory framework is still the electric utilities' voluntary action consisting of self-declaration by the employee and its verification by the electric utilities. The major premises for voluntary action are both assimilation of security culture and adequate organizational risk management capability. Nevertheless, it cannot expect in the present situation that both premises would reach to enough level. Ideally, it is desired to introduce the personnel reliability certification system into crosscutting legal system and regulations for protecting critical infrastructures.

The second issue is nuclear material-based regulation. The Nuclear Regulation Act in Japan, unlike other major nuclear developed countries, regulates all nuclear activities through institutions that handle nuclear materials and techniques, so-called institution-based (or operation/action-based) regulatory scheme. A shortcoming of the Nuclear Regulation Act is to not exactly cope with terrorists and unauthorized removal of nuclear materials. This regulatory scheme becomes less effective in the changing environment surrounding nuclear fuel cycle business. Furthermore, concerns about failure of nuclear utility business in full-scale competitive electricity market are growing recently. In this context, taking "Away From Reactors" spent fuel storage, high-level radioactive wastes management and disposal, and international scheme for safeguard and non-

proliferation into account, it is necessary to examine amendment of the Nuclear Regulation Act or new legislation in terms of nuclear materials-focused regulation.

Finally, the author notes some general challenges for enhancing capabilities of crisis managementandresilience.

First is red teaming, which is the independent application of a range of structured, creative and critical thinking techniques to assist the end user make a better informed decision or produce a more robust product. The United States intelligence community (military and civilian) has red teams that explore alternative futures. Red teaming is important to improve quality of strategic planning or decision-making for emergency preparedness and responses.

Second, it is really important to shift the focus from whether an event could occur to how it may happen. Policy-maker should suspend judgment about the likelihood of the event and focuses more on what developments (even unlikely ones) may enable such an outcome, a so-called “What-if?” approach.

Third, it is necessary to promote complex-adaptive-system studies in interdisciplinary manner for better understanding state and behavior of our complex socio-political-economic-ecological system. The interaction of multiple feedback loops in the complex system produces changes that are often counterintuitive and which cannot be unforeseen except by very careful and detailed modeling of the system as a whole. A feature of these changes is that they are usually non-linear, that is, a small change in one part of the system can produce a disproportionately large response in another.

5. Concluding remarks

Nuclear safety and security that have been commonly recognized as technical and/or political issues in nuclear policy context become increasingly complex issues with multi-faceted and systemic natures in complexly interconnected and interdependent world. In order to realize the effective governance for nuclear safety and security, therefore, it needs to expand the horizon and take the different contexts into consideration.

Under the evolving risk environment, along with unforeseeable nuclear policy and business environments, how nuclear power sector addresses the problem of balancing transparency and confidentiality would be crucial issue in risk governance for safety and security relevant to the downstream management of the spent fuel as well as nuclear power plant. An excessive focus on confidentiality may reduce trust in risk management and in decision-makers by raising suspicion that the shield of confidentiality is being used as a power lever by the government and/or industry to advance or protect particular interests without adequate justification.

On the other hand, an excessive transparency may not respect the need to protect legitimate interests such national security threat intelligence and the privacy interests of individual citizens. It is difficult but seriously important to balance transparency and confidentiality. The general trend in public governance is towards more disclosure of data, more transparent reporting and fuller accountability, while maintaining some confidentiality under compelling circumstances. Ultimately, a well-informed public, on top of adequate emergency preparedness and response plan, and growing capabilities, will be crucial for mitigating malicious threats and risks. We should change the prevalent culture of avoiding open discussion of risks in Japan. If not, history proves risks will become reality in the not-so-distant future.

III. REFERENCES

Department of Homeland Security (2013), *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*.

Hebling (2013), *Globally networked risks and how to respond*, Nature Vol. 497 pp51-59, 2 May 2013.

International Risk Governance Council (2005), *Risk Governance towards Integrative Approach*, IRGC White paper, Geneva.

International Risk Governance Council (2010), *Risk Governance Deficits: Analysis, illustration and recommendations*, IRGC Policy Brief, Geneva.

International Risk Governance Council (2012), *Using National Risk Assessment to Develop Risk Management Capabilities at the Country Level*, ÎRGC Workshop, Paris, 12 December, 2012.

International Risk Governance Council (2015), *Preparing for Future Catastrophes: Governance principles for slow-developing risks that may have potentially catastrophic consequences*, IRGC Concept Note, Lausanne.

M Matsuo, H. Shiroyama and T. Taniguchi (2015), *Nuclear-related Risk Governance Deficit after Fukushima*, presented at World Congress on Risk 2015, Singapore, 20th-22nd July, 2015.

Ministry of Defense (2012), *Red Teaming Guide 2nd Edition*, The Development, Concepts and

Doctrine Centre, United Kingdom.

Tanabe (1998), *Characteristics and Problems on Legal Framework for Japanese Nuclear Activities: A Proposal for Introducing Material-based Regulations to Japanese Nuclear Regulations*, Research Report Y97011, Central Research Institute of Electric Power Industry, (in Japanese).

Tanabe (2009), *Potential Problems in Introduction of Personnel Reliability Certification Systems in Japan's Nuclear Industry: Implications from the German and the U.S. Laws*, Research Report Y08021, Central Research Institute of Electric Power Industry, (in Japanese).

Taniguchi (2014), *Institutional Challenges for Building and Maintaining A Secure and Resilient Japan*, presented at Workshop on Risk and Security: Redefining the Concept and the Structure of Governance, University of Tokyo, 16th July, 2014.

Taniguchi (2014), *Lessons Learned from Deficit Analysis of Nuclear Risk Governance*, presented at International Symposium on Earthquake, Tsunami and Nuclear Risks after the Accident of TEPCO's Fukushima Daiichi Nuclear Power Station, Kyoto University, 30th October, 2014.

W. Whitehead et al (2007), *Nuclear Power Plant Security Assessment Technical Manual*, SAND2007-5591, Sandia National Laboratory.

IV. NAUTILUS INVITES YOUR RESPONSE: The Nautilus Asia Peace and Security Network invites your responses to this report. Please send responses to: nautilus@nautilus.org. Responses will be considered for redistribution to the network only if they include the author's name, affiliation, and explicit consent.

Nautilus Institute
608 San Miguel Ave., Berkeley, CA 94707-1535 | Phone: (510) 423-0372 | Email: nautilus@nautilus.org