Toward Stable and Effective Use of Cyberspace

Ministry of Defense Japan

September 2012

Toward Stable and Effective Use of Cyberspace

Table of Contents

B. Cooperation with Friendly Nations and International Organizations

I. Background

Cyberspace is a "virtual space including internet where information is exchanged by information and communication technology (ICT)."[1] The use of this space is rapidly expanding and the development of ICT and cyberspace has recently become recognized as one of the "global commons," similar to the domains of sea and space.

On the other hand, as a result of the expansion of cyberspace and increasing dependence of various activities in our society on it, a possibility has emerged that our use of cyberspace can be disturbed by cyber attacks.[2] These types of disruptions have the potential to extend quickly and broadly to affect not only individual companies and government agencies but also our entire society.

The 2010 Japan National Defense Program Guidelines (NDPG) noted that the "risks to the stable use of cyberspace" are one of new challenges to our national security. It maintained that the Japanese Government will comprehensively strengthen capabilities and posture to respond to cyber attacks and that the Self Defense Forces (SDF) will develop advanced knowledge and expertise thereby contributing to the Government's efforts.

In addition, in the event of a cyber attack as part of an armed attack, the Ministry of Defense (MOD) and SDF are tasked with responding to it. To this end, the MOD and SDF must be prepared to securely and effectively use cyberspace, first by responding properly to cyber attacks against their own systems.

In consideration of these points, previously, MOD had adopted a guideline for promoting comprehensive policies to adapt to IT revolution in December 2000. Under its policy of "building joint and secure advanced networks to construct a foundation to enable defense forces to operate in a joint and coordinated manner," the MOD and SDF have implemented various measures to actively leverage ICT.

In addition to such efforts, the MOD and SDF adopt this document as a guideline to promote various programs in a united and coordinated manner by defining meanings and risks of cyberspace and by setting the context for and identifying key features of cyber-related policy to enable a more secure and effective use of the cyber domain[3].

---

[1] See 'Information Security Strategy for Protecting the Nation' (May 2010)

[2] In this document, 'cyber attack' means various malicious activities through cyberspace such as an act to intend to prevent legitimate use of systems, to cause physical damage, or to acquire information illegally.

[3] As the "Information Security Strategy for Protecting the Nation" states, preparing for a potential large-scale cyber attack and strengthening information security policy are measures to be undertaken by the whole government; this document puts forward measures to be promoted by MOD and SDF for the fulfillment of their duties.

II. Basic Understanding

A. Defining Cyberspace for the MOD and SDF

As a result of the recent world-wide growth and expansion of ICT devices such as computers and mobile phones, cyberspace has become an integral part of human life. ICT growth has continued to expand globally to reach almost every region.

Naturally, the MOD and SDF use cyberspace in all aspects of its activities such as policymaking, operations, personnel affairs, public relations, and research and development. Cyberspace is an essential infrastructure that supports various operations across the actual domains of land, sea, air, and space. Therefore, the secure use of cyberspace is a critically important element to achieve MOD/SDF's missions.

Additionally, for the MOD and SDF, cyberspace is a 'domain' in which various activities such as intelligence, offense, and defense are conducted just as in land, sea, air, or space domains. Effective operations in this 'domain' are as important as those in land, sea, air, and space.[4]

B. Risks in Cyberspace

1. Cyber Attacks

Cyber attacks are conducted for the purposes such as theft and/or manipulation of information or to halt and/or cause the malfunction of systems. Methods for cyber attack are diverse. Examples include inserting malware,[5] sending massive amounts of data to overload a system, or illegal access of systems. In addition, attribution for the source of the attack is difficult and deterrence of attacks remains challenging (see Appendix-1).

Every day, MOD and SDF systems and networks are defended from cyber attacks, which pose the risk of national defense information exfiltration or the disruption of effective command and control and information sharing. Moreover, there are 'supply chain risks', for example malware being inserted during the design, manufacturing, procuring, or installing of equipment.

During an armed attack against Japan, it can be assumed that the opponent will mount a variety of cyber attacks against MOD/SDF's systems and networks. Furthermore, it can be assumed that those attacks will be directed against other government agencies as well as the private sector.

[4] The possibility exists that conflicts between states could be conducted exclusively in cyberspace without the use of conventional force in other domains.
[5] Malicious software including computer viruses.

2. Other Risks

Damage of ICT devices by natural disasters or accidents and misuse of systems by a legitimate user are also risks that can cause information leaks and system malfunction. Furthermore, an employee's failure to maintain safe security practices, such as not changing passwords periodically or inappropriately dealing with suspicious e-mails, increases the risk that the entire systems and networks used by the MOD and SDF become vulnerable to cyber attacks.

III. Policy Directions

To achieve its missions and meet the expectations of the Japanese people, the MOD and SDF must maximize its opportunities for the use of cyberspace while limiting any risks. For that purpose, it is necessary to secure not only the stable use of cyberspace for systems networks as infrastructure for the MOD and SDF, but also to strengthen the capabilities of the MOD and SDF, as organizations responsible for the defense of our nation, to better operate in the 'domain' of cyberspace. Therefore, the MOD and SDF will promote the policy directions set out below to accomplish the programs listed in Appendix-2.

1. Strengthening MOD/SDF's Capabilities

The MOD and SDF must aim to acquire cutting-edge capabilities in cyberspace just as they do for other domains in order to fulfill its missions such as national defense. Given the nature of cyberspace, namely the difficulties of attribution and deterrence, as well as the importance of cyberspace to achieving information superiority[6], strengthening MOD/SDF capability for protection of its own systems and network protection must be a priority.

Therefore, the MOD and SDF will strengthen the capability to collect and analyze threat information and to monitor and counter cyber attacks against MOD and SDF systems and networks, by means including necessary organizational restructuring. Parallel to such efforts, given that absolute cyberspace safety cannot be realistically secured, the MOD and SDF will acquire the capability to quickly recover from any damage caused by cyber attacks to continue to achieve the missions of the SDF.

In terms of operational planning, the MOD and SDF will use cyberspace and other domains as an organic whole. More practical exercises and operation manuals will be introduced that take into account cyber attacks. The possibility of the need to deny an opponent the use of cyberspace in order for SDF to effectively dispel an armed attack against Japan should also be noted.

[6] Superiority over an opponent in terms of swift and accurate recognition, collection, process and distribution of information

To ensure that the MOD and SDF have the knowledge base to accomplish these tasks, we will systematically train and retain personnel to deal with cyber attacks. This will be planned with a long-term point of view, paying due regard to the respective attributes of military officers, technical experts, and administrative officials.

Based on the assumption that all information in cyberspace can be stolen and manipulated, the MOD and SDF will make efforts to ensure that our employees act as the first line of defense by increasing awareness of information assurance and information security best practices.

2. Contribution to National Efforts, including Partnership with the Private Sector

MOD and SDF activities rely on social infrastructure such as electricity, transportation, and communication networks. Development and maintenance of equipment is also dependent on the private sector. Therefore, securing the stable use of cyberspace in society at large is critical for MOD and SDF. MOD and SDF have cooperated with other government agencies and private companies according to the "Information Security Strategy to Protect the Nation" and other directives. By providing their expertise, the MOD and SDF will continue to actively contribute to ongoing national efforts, led by the Cabinet Secretariat, toward improving the nation's overall security level. In addition, the MOD and SDF will promote cooperation with the private sector, including defense industry partners, by sharing information on the latest attack methods and technological trends.

3. Cooperation with Allies and the International Community

Cooperation with our ally, the United States, with regard to cyberspace is critically important for the MOD and SDF to achieve its missions. A wide range of cooperation such as policy consultations, information sharing, and practical joint exercises will be promoted between Japan and the United States in the field of cyber.

Because cyberspace has expanded globally, cooperation with like-minded countries and international organizations will be promoted with the intent of securing the stable use of cyberspace.

IV. Regarding Legal Issues and the Implications from Cyber Attacks

Considering the trend of society at large to increasingly depend on cyberspace and the increasingly sophisticated and skilled forms of recent cyber attacks, the possibility that serious damages will result in the future from cyber attacks alone cannot be ruled out.

Although it is difficult to generalize the relation between such cyber attacks and an armed attack, and whether a certain situation can be regarded as an armed attack should be determined based on individual and concrete circumstances, it can be assumed that the first

requirement of exercising the right of self-defense will be met in the event of a cyber attack as part of an armed attack[7].

The international community is at present actively debating the legal status of cyber attacks, including those which are especially destructive. Taking into account these discussions and efforts in SDF operations, MOD and SDF will continue to examine both international and domestic legal issues regarding the ramifications of cyber attacks and responses to them. Additionally, the MOD and SDF will actively participate in efforts to shape international norms regarding cyberspace.

V. Process Management and Review

The “Committee on Responses to Cyber Attacks” will act as the key vehicle to follow-up on and manage the various MOD and SDF cyberspace efforts by setting a concrete schedule for the process.

MOD and SDF efforts will be constantly reviewed and updated to deal with various risks in cyberspace. The goal will be to appropriately take into account GOJ cyber efforts and to adapt to rapidly advancing technological ICT trends, for example the spread of cloud computing and the increasing capability of mobile devices.

[7] Armed force can be used to exercise the right of self-defense only when the following three conditions are met: (1) When there is an imminent and illegitimate act of aggression against Japan; (2) When there is no appropriate means to deal with such aggression other than by resorting to the right of self-defense; and (3) When the use of armed force is confined to be the minimum necessary level.

Appendix A

Characteristics of Cyber Attacks

I. Diversity

A. Actors

Cyber attack tools are much easier to acquire and use than conventional military equipment such as vessels and aircraft. Therefore, not only states but various actors such as individuals and organizations are able to conduct cyber attacks from almost any point on the globe via the internet.[8]

B. Methods

There are a wide range of methods to conduct cyber attacks such as:

- injecting malware which can conduct harmful activities such as the theft of information
- sending a massive amount of data to servers (Distributed Denial of Service (DDoS) attack)
- unauthorized access to systems[9]

Some of these methods are thought to be mainly conducted by state actors because of the high degree of skills and planning required to accomplish these types of attacks.

C. Objectives

Those perpetuating cyber attacks have various aims for their acts. For example, cyber attacks can be conducted for the theft or manipulation of information in systems, causing the malfunction or failure of systems, or interrupting internet service.

D. Context

Cyber attacks can be conducted under any situation from peacetime to wartime.

II. Anonymity

A cyber attack is easy to conceal; actors can easily disguise their identity. There is a possibility that, without even leaving a trace, a state could attack another state. Complicating matters more, a state could order/encourage/tolerate a group of individuals or an independent organization to attack another state in a similar manner.

[8] MOD/SDF's systems that deal with classified information are closed networks that do not connect with the outside. However, even closed networks can be infected with malware via removal media such as USB memory devices

[9] As for methods to obstruct the stable use of cyberspace, it is also possible to cause the physical destruction of ICT infrastructure, such as servers.

III. Stealth

While some types of cyber attacks such as DDoS attacks are easy to recognize, other varieties of attacks, such as malware, are difficult to identify until damage actually occurs. Cyber attacks can also take place without causing any realization of damage, such as in the case of information theft. It is thought that this stealthy nature of cyber attacks will increase along with the technological trends of ICT.

IV. Offensive Dominance

In cyberspace, offensive attacks are overwhelmingly superior over defensive actions due to attack tools being easy to acquire, the lack of attribution, the difficulty in eliminating software vulnerabilities, and because an attacker can choose the most vulnerable point of interconnecting networks.

V. The Difficulties of Deterrence

It is difficult to deter cyber attacks by either deterrence by punishment[10] or deterrence by denial[11].

For deterrence by punishment, even if an intention is expressed to a potential attacker that, should a cyber attack be attempted, retaliation in a manner that will cause damage on an equal or greater scale can be expected, deterrence is not likely to work when the attacker is not a state actor and does not possess assets which he/she fears to lose. Furthermore, since it is difficult to attribute the target to retaliate due to the anonymity of cyber attacks, a warning of retaliation does not have enough power to deter a potential attacker.

As for deterrence by denial, it is necessary to make an attacker think that he/she cannot obtain the expected effect by his/her cyber attack. However, because of offensive superiority over defense in cyberspace, it is hard to improve the security level to such a high degree that an attacker will be persuaded to refrain from attacking.

[10] To influence the opponent's cost calculus to give up any attack based on threats to cause unbearable damage (see 2010 Defense White Paper).
[11] To influence the opponent's estimate of goal attainment possibility based on the capability to physically deny a specific attack (see same).

Appendix B

Programs

I. Strengthening MOD and SDF capabilities

A. High Priority Programs

1. Improve Situational Awareness and Recovery Capabilities

- Increase the surveillance devices placed within the Defense Information Infrastructure (DII) in order to improve surveillance abilities.

2. Improve Skills and Expertise

- Conduct realistic exercises in an environment that simulates conditions of the MOD systems. For this purpose, conduct a research and development project to construct a large-scale simulated environment necessary for this end.

3. Enhance Early Warming Capability

- Improve functions of the security and analysis devices for cyber defense for early detection of indications of cyber attacks against the MOD/SDF and to strengthen MOD and SDF alert capability.
- Strengthen methods for information collection and analysis of cyber threats, such as the latest malware and attack methods, through cooperation among MOD agencies and the active use of information from other government agencies and private companies.

4. Organization

- Establish a cyberspace defense unit in FY2013 as the core organization to deal with cyber attacks against systems and networks of MOD and SDF, thereby strengthening their joint counter-capabilities.
- Improve the overall capability of the C4SC (Command Control Communication Computer Systems Command) and the system-protection units of each service.
- Improve the capability of information collection and analysis on cyber attacks outside Japan by the Defense Intelligence Headquarters and other units.
- Consider improving the cyber-related organizational structure in the fields of policy planning, research and development, and interagency coordination including the establishment of a permanent CISO[12].

B. Priority Programs

1. Upgrade Protection in Individual Systems

- Upgrade protection of individual systems for each service.

2. Integrate Surveillance Information Derived from Individual Systems

[12] Chief Information Security Officer

- Implement security information management (SIM) systems to integrate the surveillance information of each service and to deal with incidents more effectively.

3. Decreasing Vulnerability

- Enhance regular vulnerability checks and introduce host-based intrusion prevention systems (IPS).
- Promote outsourcing to effectively conduct inspection of system vulnerabilities and decrease vulnerability.

4. Education and Training

- Consider the projects listed below to steadily retain talented MOD personnel who have the advanced expertise, skills, and experience to deal with cyber attacks:
  - Education within each service for personnel who deal with cyber attacks for their respective units.
  - Promotion of education and research at the National Institute for Defense Studies, the National Defense Academy, as well as in universities in Japan and abroad.
  - Exchanges of personnel with private companies.
  - Hire personnel who already possess advanced cyber security capabilities, such as those with security certification or private sector experience.

5. Research and development

- Based on recent technological trends, promote the following research and development projects:
  - Construction of a large-scale simulated environment.
  - Research and development of automated technology to search for malware within networks, specify workstations infected, and remove the malware.
  - Research and development of technology to prevent the unauthorized access of important information from equipment lost during SDF operations.

C. Foundational Programs

- Conduct more practical unit training, by assuming a cyber environment degraded by cyber attacks in various exercises, including joint Japan-U.S. exercises.
- Revise manuals based on lessons learned from exercises.
- Research and study the latest attack methods and technological trends.
- Provide continued education about the latest trends in attack methods and technology, recent incidents, and relevant regulations through training

opportunities such as workshops for employees. Provide focused training and constant awareness about the proper use and storage of removal media and electronic devices.

II. Contribution to National Efforts including Partnership with the Private Sector

A. Contribution to GOJ-level Efforts

- Actively contribute to Cabinet Secretariat's coordinated national efforts to raise government-wide security level through the efforts below
  - Actively participate and support cyber exercises chaired by Cabinet Secretariat, for example by providing know-how to create scenarios.
  - Provide information on the latest attack methods and technological trends as discovered by the MOD and SDF.
  - Dispatch highly talented staff to the GSOC[13].
  - Promote cooperation with other agencies in case of a large-scale cyber attack, such as providing support personnel through the Cabinet Secretariat's emergency support team on information security (CYMAT[14]).

B. Partnership with the Private Sector

- Raise the security level of defense industry companies by requiring rigid controls for important information as well as requiring them to provide their employees with intensive education. The MOD will also implement effective inspections on a regular basis.
- Using a governmental framework for information sharing with the private sector, provide information on the latest attack methods and technological trends to defense industries and other private sector companies.
- Exchange opinions with defense industry partners about how to decrease supply chain risks.

III. Cooperation with Allies and the International Community

A. Cooperation with the United States

- As mentioned in the June 2011 2+2 joint statement, promote a bilateral strategic policy dialogue on cyber security and strengthen bilateral cooperation such as information sharing.
- Improve joint response capability through bilateral exercises that assume a cyber environment degraded by cyber attacks.

B. Cooperation with Friendly Nations and International Organizations

- Promote cooperation, such as information sharing, with partners such as

[13] Government Security Operation Coordination Team which is an interagency information collection and analysis team in the Cabinet Secretariat's office
[14] Cyber incident Mobile Assistance Team

Australia, the United Kingdom, Singapore, and NATO through dialogues at various levels.