Enhancement of Counter Cyber-attack Capabilities from Viewpoint of National Defense

Daiki Kasai
Moe Tajima
Yoshiyuki Saitou
Yoshinobu Tanigawa

OVERVIEW: Use of cyber-attacks for military purposes has grown in recent times, with an increasing number of these attacks being made on defense industries or other important infrastructure, and this has made the strengthening of capabilities for preventing these attacks an urgent requirement for national defense. Hitachi is utilizing the defense sector know-how of its Defense Systems Company in fields such as the implementation of command and control systems to investigate, from a defense perspective, the best ways of providing the capabilities needed to counter these cyber-attacks. Based on the results of this investigation, Hitachi intends to contribute to creating a safe and secure society that includes cyberspace by further enhancing its solutions that facilitate improvements in the capabilities for countering cyber-attacks.

INTRODUCTION

IN July 2011, the U.S. Department of Defense published the Department of Defense Strategy for Operating in Cyberspace[1] that specifies its initial cyberwar strategy. The background to this publication includes a series of cyber-attacks on government and other important infrastructure, and an increasing number of cases in which cyber-attacks have been used for political or military purposes.

The publication represents a strong stance by the USA on cyberwar, identifying five strategies that include the concept of cyberspace as the fifth operational domain (after land, sea, air, and space), and also the strengthening of organizations and equipment as well as relationships with relevant government agencies, corporations, and others.

One example of the actual use of a cyber-attack for military purposes occurred in a 2007 aerial campaign conducted by the State of Israel against the Syrian Arab Republic[2]. Israel launched a cyber-attack against Syria that disabled the detection capabilities of Syrian air defense systems while it carried out bombing attacks, making this an example both of the use of a cyber-attack for military purposes and a high level of coordination with physical operations.

Cyber-attacks targeting corporations have also been increasing in recent times, with such attacks taking place against defense industry and other targets in Japan, Israel, India, and the USA during 2011[3].

These examples clearly differ in character from conventional security risks involving information leaks achieved through infection with computer viruses and their indiscriminate spreading. Cyber-attacks are being perpetrated that use advanced strategies and accumulated technologies to achieve specific objectives.

Meanwhile, modern society has become highly dependent on information technology (IT). For example, IT underpins important infrastructure such as electric power, gas, water, transportation, and communications. The same applies to the defense equipment and other infrastructure of government agencies, where greater modernization brings an increasing reliance on IT. This means that the impacts

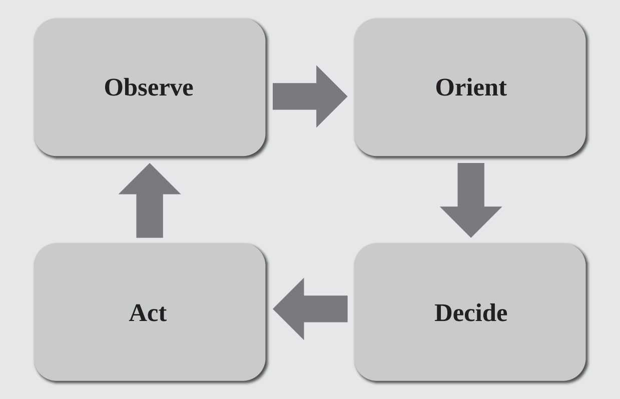

Fig. 1—OODA Loop.
A decision making methodology proposed by U.S. Air Force Colonel John Boyd involving the use of a repeated "observe, orient, decide, and act" cycle to achieve fast and accurate decisions.

of a cyber-attack are not limited to cyberspace and extend into the real world.

Given this potential for cyberwar, meaning the use of cyber-attacks to pose a risk to national security, there is a need to strengthen capabilities for countering cyber-attacks from the perspective of national defense.

This article describes how to go about strengthening capabilities for countering cyber-attacks, US policies and the response of corporations, and what Hitachi is doing in this field.

INVESTIGATION INTO STRENGTHENING CAPABILITIES FOR COUNTERING CYBER-ATTACKS

The OODA loop is a methodology, originally proposed by U.S. Air Force Colonel John Boyd, that has a long history of use in the military world. Based on insights gleaned from the experience of successful air campaigns in the Korean War, the OODA loop formalizes the process of decision making by the commanding officer. Over time, it has also come to be used in the business world and other civilian applications.

OODA stands for "observe, orient, decide, and act," and the concept behind the OODA loop is to achieve fast and accurate decision making by repeatedly working through this cycle (see Fig. 1).

The following section uses the OODA loop as a basis for considering, from a defense perspective, what needs to be done to strengthen capabilities for countering cyber-attacks (see Fig. 2).

Observation

The main objective of observation is to acquire information, such as identifying and tracking enemies. Tactics can be pursued more effectively by using analysis of collected information to infer information about the enemy, such as their capabilities and objectives, and also by protecting one's own side's information from the enemy.

Examples of observation in cyberspace might include functions for detecting the presence of attacks or other external threats to one's organization by using tools such as anti-virus software, intruder detection devices, and log collection utilities. Unfortunately, using these functions alone, it is very difficult to determine the objectives or intentions that have motivated a detected cyber-attack.

Additional functions for identifying objectives and intentions can be provided in the form of cyber-intelligence functions that include the collection and sharing of a wide variety of information. Specific examples of the type of information to collect include system, software, and other vulnerabilities (security weaknesses), infections by new viruses or other threats,

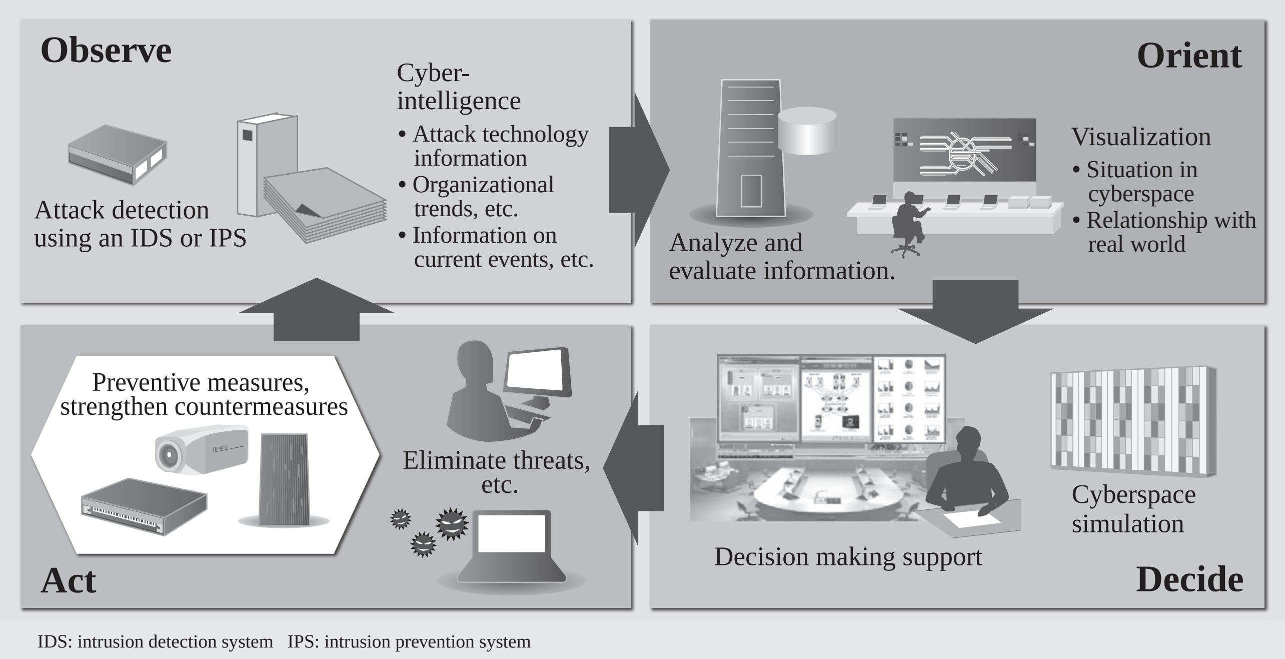
Observe
Attack detection using an IDS or IPS
Cyber-intelligence
• Attack technology information
• Organizational trends, etc.
• Information on current events, etc.
Orient
Analyze and evaluate information.
Visualization
• Situation in cyberspace
• Relationship with real world
Act
Preventive measures, strengthen countermeasures
Eliminate threats, etc.
Decision making support
Cyberspace simulation
Decide
IDS: intrusion detection system IPS: intrusion prevention system

Fig. 2—Use of OODA in Cyberspace.
The OODA loop is used as a basis for investigating, from a defense perspective, what needs to be done to strengthen capabilities for countering cyber-attacks.

and activities by malicious hacker groups. When current trends in cyber-attacks are considered, information sharing between relevant organizations is also very important. In particular, to prepare for attacks on government agencies or other important infrastructure, it is necessary to consider the relationships between different incidents, such as the increasing number of attacks on private companies that form part of the supply chain. To achieve this, in-house monitoring needs to perform the collection and sharing of information in a way that considers how incidents are interconnected.

However, careful attention needs to be paid to the requirements and scope of cyber-intelligence when designing the operation. It is also most important to protect information about the organization's own objectives, intentions, and capabilities (such as what information to collect and what it is possible to detect) to prevent this falling into the hands of potential attackers.

Orientation

Situation development (orientation) is performed to identify the objectives and intentions of an attack, and to use this as a basis for determining the impact on one's own organization.

This involves analyzing the observations to determine whether an incident is an inadvertent or other indiscriminate attack, or whether it is a cyber-attack with a deliberate military intent. It also includes analyzing the scope and severity of the impact that the attack will have on the organization's systems and tactics. In this way, the risk level can be determined in a way that includes the real world impact.

Performing a situation development in cyberspace requires the use of tools for analyzing the collected information, including log analysis, network monitoring, and incident management utilities.

One of the tools used for orientation in the military world is called "common operational picture" (COP). This supports situation development by displaying information, such as friends' and enemies' capabilities, status, objectives, and conditions (ground, weather, and sea conditions), based on the role, rank, and other attributes of the commanding officer or other personnel so that everyone has a consistent understanding of the situation.

Performing a situation development in cyberspace requires similar tools. Furthermore, by coordinating these tools with the real world COP, it is possible to perform situation developments in a way that includes correlations between the real world and cyberspace.

Decision Making

In the military world, decision making is one of the most important capabilities demanded of a commanding officer, and decision making is essentially something best done by people. However, it is also possible to help commanding officers make decisions by providing functions that improve decision making speed and accuracy.

Simulation functions are one example. In the case of cyberspace, this means setting up a test version of the organization's own system and network environment that can be used for activities such as assessing the impact of cyber-attacks and other threats, or for running training exercises to test responses.

Certain very special concepts are relevant to decision making in the context of national security. If a threat such as a device being infected by malware (malicious software) is detected within the organization, for example, common security practices include reinitializing the device or disconnecting it from the network to prevent secondary infection of other devices.

However, if this is something that could have an impact on military operations, there are cases, based on an appropriate risk assessment, in which priority is given to mission completion and the implementation of security measures is delayed. There may also be cases when, rather than responding immediately, a wait-and-see approach is taken to observe how the situation develops. For example, observing how the attacker goes about mounting a cyber-attack can help with situation development by providing information about their methods and other details.

Action

The action phase includes solving problems and eliminating risk factors. A key feature of the OODA loop approach is that the next observation phase makes active use of the results up to and including the action phase. That is, the cycle does not end with the action phase, and instead it places an emphasis on feedback to the observation phase.

Based on this approach, rather than treating countermeasures such as the removal of malware or the disconnection of unauthorized communications as being the end of the process, the OODA loop methodology uses the analysis and prediction of attack trends as the basis of feedback, such as setting up preemptive countermeasures or expanding the scope of data collection.

US POLICY MEASURES AND CORPORATE RESPONSE

U.S. Department of Defense is pursuing policies that recognize the importance of sharing information and the increasing number of cyber-attacks on companies in the supply chain. In addition to helping the U.S. Department of Defense strengthen its observational capabilities based on the OODA loop, this can also be seen as indicative of their desire for the defense industry to establish their own capabilities based on the OODA loop.

One specific policy being pursued in collaboration with the U.S. Department of Homeland Security involves taking steps to protect confidential defense information located on the networks or other systems of defense companies. This includes the Defense Industrial Base Cyber Security/Information Assurance (DIB CS/IA) Program[4].

In a pilot program that started in June 2011 and ran for approximately one year, the U.S. Department of Defense and a number of corporations (20 at the time the program started) shared information about cyber-threats, including confidential information. In May 2012, the program was upgraded from a pilot program to being open to all companies in the defense industry.

Under the DIB CS/IA Program, Department of Defense provides participating DIB Companies with unclassified indicators and related, classified contextual information. DIB Companies can choose whether to incorporate the indicators into their own traffic screening or other security tools, and they can review or act on the contextual information as they wish to better address the cyber security threats they face. Similarly, participating corporations are free to pass on any information they acquire about cyber-attacks to the U.S. Department of Defense or other program participants.

In this way, as a countermeasure against cyber-attacks that are becoming more sophisticated and serious, the USA is extending the sharing of information to include the supply chain and strengthening its ability to respond.

ACTIVITIES BY HITACHI

Hitachi, Ltd. adopted its company-based organizational structure in 2009. One of these companies is the Defense Systems Company that runs Hitachi's security business for social infrastructure, which includes the defense sector. The Defense Systems Company supplies a cyber-security solution that supports national security.

Based on the OODA loop, this solution provides functions for enhancing capabilities for countering cyber-attacks. Drawing on the investigation into strengthening capabilities for countering cyber-attacks described earlier in this article, Hitachi intends to enhance the following two aspects of the solution in particular.

Cyber-intelligence Solution

The types of information that should be collected to counter cyber-attacks cover a wide range. This extends beyond technical information, such as logs from in-house networked devices, asset management information, and e-mails. Instead, it is possible that a diverse range of information gathered from a variety of sources will be needed, such as background information on real world trends or examples of attacks that have taken place elsewhere.

In addition to systematizing this information so that it can be collected and used efficiently, its ease-of-use, meaning, and value as a basis for decision making can be established by classifying, assessing, and correlating the collected information, and subjecting it to forecasting and other analyses.

Solution for Cyberspace Situation Awareness

An awareness of the actual situation is important for achieving a fast and accurate response to a cyber-attack.

In addition to assessing risks associated with a cyber-attack and the scope of its impact on the organization, the solution makes the required information available in a visual format based on factors that include the user's role and rank, such as whether they are a commanding officer or part of the system management staff. In other words, it provides a COP for cyberspace. During a cyber-attack, this provides a consistent understanding of the situation across the organization, and allows a comprehensive response to be mounted.

CONCLUSIONS

This article has described how to go about strengthening capabilities for countering cyber-attacks, US policies and the response of corporations, and what Hitachi is doing in this field.

As noted in this article, the objectives and methods used in cyber-attacks have been changing recently, and the potential for cyberwar has arisen.

Hitachi is utilizing the defense sector know-how it has built up in fields such as the implementation of command and control systems to investigate, from a defense perspective, how to strengthen the capabilities needed to counter these cyber-attacks. In the future, Hitachi aims to make an even greater contribution to achieving a safe and secure society, including cyberspace, through initiatives that include enhancing its solutions based on the results of this investigation.

REFERENCES

(1) "DOD Announces First Strategy for Operating in Cyberspace," News Release, U.S. Department of Defense, http://www.defense.gov/releases/release.aspx?releaseid=14651 (Jul. 2011).

(2) R. Clarke et al., Cyber War: The Next Threat to National Security and What to Do About It," Ecco (Apr. 2010).

(3) "Japan, US Defense Industries Among Targeted Entities in Latest Attack," Trendlabs Security Intelligence Blog, Trend Micro Inc., http://blog.trendmicro.com/trendlabs-security-intelligence/japan-us-defense-industries-among-targeted-entities-in-latest-attack/ (Sep. 2011).

(4) "DOD Announces the Expansion of Defense Industrial Base (DIB) Voluntary Cybersecurity Information Sharing Activities," News Release, U.S. Department of Defense, http://www.defense.gov/releases/release.aspx?releaseid=15266 (May 2012).

ABOUT THE AUTHORS

Daiki Kasai

Joined Hitachi Advanced Systems Corporation in 2004, and now works at the Defense Information Systems Department. He is currently engaged in the marketing of cyber-security systems to the Japan Ministry of Defense.

Moe Tajima

Joined Hitachi, Ltd. in 2008, and now works at the Planning and Engineering Department, Defense Systems Company. She is currently engaged in the marketing of cyber-security systems to the Japan Ministry of Defense.

Yoshiyuki Saitou

Joined Hitachi, Ltd. in 1993, and now works at the Application Design Department, Defense Systems Company. He is currently engaged in the design of cyber-security systems to the Japan Ministry of Defense.

Yoshinobu Tanigawa

Joined Hitachi, Ltd. in 1993, and now works at the Enterprise Systems Research Department, Yokohama Research Laboratory. He is currently engaged in the research and development of security application technology for countering cyber-attacks. Mr. Tanigawa is a member of the Information Processing Society of Japan.