IIPS
Institute for International Policy Studies

IIPS Quarterly, Volume 6 Number 3
Policy Research

The Cybersecurity Challenges for the Ministry of Defense and the Self-Defense Forces

Miyuki Matsuzaki
Senior Research Fellow

In January of this year (2015), the government of Japan established the Cybersecurity Strategic Headquarters and released a new Cybersecurity Strategy in May. Through these and other developments, the government is promoting cybersecurity initiatives. At the same time, a plethora of cybersecurity issues have been accumulating, as should be evident just from the single example of the cyberattack on the Japan Pension Service.

As part of Japan's cybersecurity policy, the Ministry of Defense is engaged in bolstering, from a national security perspective, the capabilities and organization of the Self-Defense Forces (JSDF) to deal with cyberattacks. This paper considers the cybersecurity issues for the Ministry of Defense and the JSDF, considering the cybersecurity initiatives of the US—which have preceded any similar efforts in other countries.

Responses to cyberattacks

International norms pertaining to actions taken in cyberspace are currently under development; creating legal basis for responses to cyberattacks is a common problem for the international community. There exists a shared understanding internationally that the right of self-defense, which the United Nations Charter permits the exercise of in response to "armed attacks," can also be applied to attacks that occur in cyberspace. However, cyberattacks take a multitude of forms, cause varying degrees of damage, and possess different characteristics. In this situation, there are no established definitions that speak to what sorts of cyberattacks are equivalent to "armed attacks" and would thus make tenable a country's claim that it was exercising its right of self-defense in response.

In 2011, the US government released "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World." With a statement that the US would "reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law," the document clearly established that the US cybersecurity strategy includes military means.

That same year, the U.S. Department of Defense stated in its "Department of Defense Cyberspace Policy Report" that the military options "may include using cyber and/or kinetic options." It implies that the US would not exclude responses using its kinetic capabilities if attacked in cyberspace.

Generally, attack and defense in cyberspace are two sides of the same coin. Primarily, the U.S. Cyber Command (USCYBERCOM) focuses on defensive capabilities. According to the testimony before Congress by the Commander of USCYBERCOM, the committee on armed service, however, argued that they increase offensive capabilities in order to provide a broader range of options. Thus they differentiate between offensive and defensive capabilities. The fiscal year 2016 Department of Defense budget requested increases in both defensive and offensive capabilities in cyberspace. However, President Obama has yet to decide whether to delegate authority to the USCYBERCOM commander for "the offensive application of cyber," demonstrating that the US is cautious about carrying out offensive measures.

Attacks conducted via servers in third countries are a problem particular to cyberattacks, as opposed to other forms of aggression. The US Department of Defense lists the following as some of the criteria for determining how to respond to cyberattacks conducted via third countries: "whether a third country is aware of malicious cyber activity originating from within its borders"; "the role, if any, of the third country"; and "the ability and willingness of the third country to respond effectively to the malicious cyber activity." Thus, the US does not deny that it might engage in responses directed at third countries. If the US will not exclude the option of conducting kinetic military attacks on third countries, then this matter will become a significant point of debate internationally.

The Ministry of Defense states that "whether a certain situation can be regarded as an armed attack should be determined based on individual and concrete circumstances" and then presents the basic view that "it can be assumed that the first requirement of exercising the right of self-defense will be met in the event of a cyberattack as part of an armed attack." If Japan has suffered a cyberattack "as part of an armed attack," then it will presumably be forced to decide—among other matters—whether to respond using what it would term "military means." If Japan is to respond, it must decide whether to do so in cyberspace or by using conventional weapons. Furthermore, there are many issues concerning responses to attack in cyberspaces such as responses directed at third countries when an attack has been conducted via servers located within those countries.

The technology used in cyberattacks is advancing rapidly. Because technological development results in new issues to address, it would be difficult—and thus inappropriate—to strictly define matters such as the requirements that a cyberattack would need to fulfill to justify the exercise of the right of self-defense and the way in which to respond to an attack. However, because the situation seems to advance rapidly, it is necessary to consider response plans and related matters, hypothesizing about all currently conceivable situations. Furthermore, to improve the effectiveness of responses, it will be essential to improve the JSDF's *offensive* capabilities in cyberspace.

Cybersecurity and intelligence

In both preventing and responding to cyberattacks, it is essential to collect and analyze intelligence concerning the cyber-capabilities and intentions of nations, organizations, and individuals that could be the sources of attacks. Therefore, cybersecurity and intelligence are closely related. In the US, the National Security Agency (NSA) and USCYBERCOM are located at the same base, and one person holds the director of the NSA and the Commander of USCYBERCOM concurrently. The NSA and USCYBERCOM are partners with a shared mission, as the NSA collects and analyzes data relating to threats in cyberspace that originate from abroad. Amid the debate concerning NSA reform, the merits of having an NSA-director-concurrently serve as USCYBERCOM commander have been argued, and the debate continues: Admiral Michael S. Rogers, the Director of NSA and the Commander of USCYBERCOM, has testified before Congress that he strongly supports the dual role because it helps to strengthen both organizations.

In February 2015, President Obama initiated a new effort to strengthen the relationship between cybersecurity and intelligence when he instructed the director of national intelligence to establish the Cyber Threat Intelligence Integration Center (CTIIC). The new organ will not collect intelligence itself; rather, it will aggregate the intelligence collected individually by agencies such as the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), the Department of Defense, the NSA, and the Central Intelligence Agency (CIA). CTIIC's goal will be to then swiftly formulate response measures by identifying attackers and performing analyses.

Given the information that has been released publicly, it is difficult to speculate about the current state of cooperation between the Cyber Defense Unit—the JSDF unit in charge of cyber-defense—and various intelligence entities. In any event, it is necessary to engage in initiatives in which different organizations aggregate and share the intelligence-gathering and analysis that they are assumed to be engaged in individually. These initiatives should not be limited internally to the Ministry of Defense and the JSDF but, instead, should encompass the entire government, as well as, to the extent possible, companies in the private sector.

Cybersecurity for critical infrastructure and the defense industry, and the roles of the Ministry of Defense and the JSDF

In the US, the DHS is in charge of cybersecurity for critical infrastructure. However, it is assumed that, when such infrastructure has been subject to a cyberattack that has resulted in significant damage, it will be a unit from USCYBERCOM that will respond.

Similarly in Japan, the cabinet’s National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and the relevant ministries and agencies are in charge of the cybersecurity of critical infrastructure, while the Cyber Defense Unit—whose mission is to monitor the networks of the Ministry of Defense and the JSDF, and to respond to incidents occurring in them—does not defend the systems and networks used in critical infrastructure or in the defense industry. Unlike in the US, there are currently no provisions for the Cyber Defense Unit to respond in the event that a cyberattack on critical infrastructure results in significant damage.

Cooperation between the Ministry of Defense and private sector companies is growing. In 2013, the Cyber Defense Council was established with the aim of promoting intelligence-sharing among participating companies and with the Ministry of Defense serving as the council’s hub. Thus, cooperation between the Ministry of Defense and companies involved with critical infrastructure or in the defense industry continues to strengthen. Perhaps the participation of the Cyber Defense Unit in responses to future cyberattacks on critical infrastructure and the defense industry should be up for discussion.

(The views expressed in this paper are those of the author as an individual and do not necessarily represent the views of any organizations to which the author belongs.)