Volume 16 | Issue 13 | Number 4 | Article ID 5170 | Jul 01, 2018

The Untold Story of Japan's Secret Spy Agency

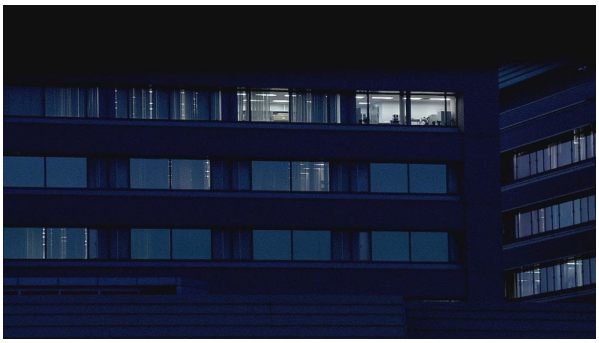
Ryan Gallagher

This story is the product of a two-year collaboration between U.S. news website The Intercept and the Japanese broadcaster NHK. The project began in mid-2016, and was initially focused on investigating three U.S. military bases in Misawa, Okinawa, and Yokota. In April 2017, we revealed that the bases were an integral part of the global surveillance network controlled by the U.S. National Security Agency. With the help of a batch of leaked U.S. documents, we showed that the Japanese government had spent more than half a billion dollars to fund the facilities, and received in return powerful surveillance equipment for its own spies to use to eavesdrop on emails and phone calls.

After we published that information, sources in Japan came forward and provided us with new details about the inner workings of Japan's little-known spy agencies. That was an extraordinary development for us, because prying classified information out of the Japanese government is not an easy thing to do. I have reported on the activities of spies in countries across the world, and never before have I encountered a group that is more institutionally secretive than the Japanese. For decades, basic details about the structure, size, operations, and funding of Japan's intelligence community have been withheld from the public. Even within the Japanese government, only a select few officials at the highest echelons of power are provided with any information about the shadowy people in control of the country's surveillance systems.

With this story, in an effort to serve the public interest, we chipped away some of the secrecy, and in the process documented that Japan's spies may be carrying out covert actions that violate the country's constitution. I hope our disclosures will not be the last, and that they will help to contribute to greater transparency – and more informed debate – about the Japanese government's surveillance powers in the future.

Every week in Tokyo's Ichigaya district, about three miles northeast of the bright neon lights and swarming crowds in the heart of Shibuya, a driver quietly parks a black sedan-style car outside a gray office building. Before setting off on a short, 10-minute drive south, he picks up a passenger who is carrying an important package: top-secret intelligence reports, destined for the desks of the prime minister's closest advisers.



Night view of the C1 building, inside Japan's Ministry of Defense compound in Ichigaya. Photo: NHK

Known only as "C1," the office building is located inside a high-security compound that

https://doi.org/10.1017/S1557466018014493 Published online by Cambridge University Press

houses Japan's Ministry of Defense. But it is not an ordinary military facility – it is a secret spy agency headquarters for the Directorate for Signals Intelligence, Japan's version of the National Security Agency.

The directorate has a history that dates back to the 1950s; its role is to eavesdrop on communications. But its operations remain so highly classified that the Japanese government has disclosed little about its work – even the location of its headquarters. Most Japanese officials, except for a select few of the prime minister's inner circle, are kept in the dark about the directorate's activities, which are regulated by a limited legal framework and not subject to any independent oversight.

Now, a new investigation by the Japanese broadcaster NHK — produced in collaboration with The Intercept — reveals, for the first time, details about the inner workings of Japan's opaque spy community. Based on classified documents and interviews with current and former officials familiar with the agency's intelligence work, the investigation shines light on a previously undisclosed internet surveillance program and a spy hub in the south of Japan that is used to monitor phone calls and emails passing across communications satellites.

According to the current and former officials, the Directorate for Signals Intelligence, or DFS, employs about 1,700 people and has at least six surveillance facilities that eavesdrop around the clock on phone calls, emails, and other communications. (The NSA, in comparison, has said it has a workforce of more than 30,000 and Britain's signals intelligence agency claims more than 6,000 staff.) The communications collected at the spy facilities are sent back to analysts who work inside the C1 building, which has four underground floors and eight above ground.

"Very few people know what the DFS is doing and can enter the building," according to an active-duty official with knowledge of the directorate's operations, who spoke on condition of anonymity because they were not authorized to talk to the media. The official agreed to share details about the directorate after The Intercept and NHK last year revealed that the spy agency had obtained a mass surveillance system called XKEYSCORE, which is used to sift through copies of people's emails, online chats, internet browsing histories, and information about social media activity. The official said that they believed the directorate's use of XKEYSCORE was "not permissible" under the Japanese Constitution, which protects people's right to privacy.

The directorate – known in Japanese as the "Denpa-Bu," meaning "electromagnetic wave section" – currently has 11 different departments, each focused on a different subject, such as information analysis, public safety and security, and cryptography. However, the departments are kept separate from each other and there is limited communication between them, the active-duty official said. Each department in the C1 building has a different lock installed on the rooms it uses, and these can only be accessed by a select group of people who have the appropriate security clearance, access codes, and identification. The directorate operates as the largest arm of Japan's Defense Intelligence Agency, which has other divisions focused on, for example, analyzing satellite imagery, sources said.

Miyata Atsushi, who between 1987 and 2005 worked with the directorate and the Ministry of Defense, said that his work for the spy agency had involved monitoring neighboring countries, such as North Korea, and their military activities. But the agency's culture of intense secrecy meant that it was reluctant to share information it collected with other elements of the Japanese government. "They did not share the data inside of [the] Defense Ministry properly," said Miyata. "Even inside the

https://doi.org/10.1017/S1557466018014493 Published online by Cambridge University Press

Defense Ministry, the report was not put on the table. So the people did not understand what we were doing."

The directorate is accomplished at conducting surveillance, but has a tendency to be excessively secretive about its work, according to classified documents The Intercept disclosed last year. A 2008 NSA memo described its Japanese counterparts as being "still caught in a Cold War way of doing business" and "rather stove-piped." The U.S. continues to work closely with Japan's intelligence community, however, and collaborates with the country to monitor the communications of countries across Asia.

DFS surveillance facilities in Higashi Chitose (top left/top), Tachiarai (top right/second), Kofunato (bottom left/third), and Miho (bottom right/fourth).Screenshots: Google map.

About 700 miles southwest of Tokyo, there are two small towns called Tachiarai and Chikuzen, which have a combined population of about 44,000 people. Japan's military, known as the Self-Defense Forces, has a base situated on a patch of grassy farmland in between the towns. But the base is not used to train soldiers. It is one of the country's most important spy hubs.
For years, the large antennae inside the secure compound, which are concealed underneath what look like giant golf balls, attracted concerns from local residents who were worried that the powerful radio waves they emitted might damage their health or interfere with their televisions. The Japanese government sent senior officials to reassure the locals that there would be no problems, and the

https://doi.org/10.1017/S1557466018014493 Published online by Cambridge University Press

government began paying the Chikuzen council an annual fee of about $100,000 as compensation for the disturbance caused by the base. But the function of the antennae was never revealed.

The large antennae inside the secure compound at the Tachiarai surveillance facility.

A top-secret document from the directorate offers unprecedented insight into some of the Tachiarai base's activities. The document – an English-language PowerPoint presentation – appears to have been shared with the NSA during a meeting in February 2013, at which the Japanese spy agency's then-deputy director was scheduled to discuss intelligence-gathering issues with his American counterparts. The presentation was contained in the archive of classified files provided to The Intercept by Edward Snowden. No internal documents from Japan's surveillance agency have ever been publicly disclosed before.

According to the presentation, Japan has used Tachiarai for a covert internet surveillance program code-named MALLARD. As of mid-2012, the base was using its antennae to monitor communications passing across satellites. Each week, it collected records about some 200,000 internet sessions, which were then being stored and analyzed for a period of two months. Between December 2012 and January 2013, Tachiarai began using the surveillance technology to collect information about potential cyberattacks. As a result, its data collection rapidly increased, and it began sweeping up information about 500,000 internet sessions every hour – 12 million every day. Despite this, the directorate indicated that it was only able to detect a single email that was linked to an apparent cyberattack. It struggled to cope with the amount of data it was harvesting and asked the NSA for help. "We would like to see processing procedure which the U.S. side employs in order not to affect traditional SIGINT collection," the directorate told the NSA, "and would appreciate your technical assistance."

Chris Augustine, a spokesperson for the NSA, declined to answer questions about the agency's cooperation with Japan, saying in a statement that he would "neither confirm nor deny information concerning potential relationships with foreign intelligence services." He added: "Any cooperation among intelligence services is conducted lawfully, in a manner that mutually strengthens national security."

The directorate's work at Tachiarai appears to focus on monitoring the activities of foreign countries in the region. It is unclear whether it collects Japanese citizens' communications, either deliberately or incidentally, through dragnet programs like MALLARD. The law in Japan prohibits wiretapping landlines without a court order, but monitoring communications as they are being transmitted wirelessly across satellites is a gray area, Japanese legal experts say, because there are no legal precedents in the country that place limitations upon that kind of surveillance, though there is a general right to privacy outlined in the constitution.

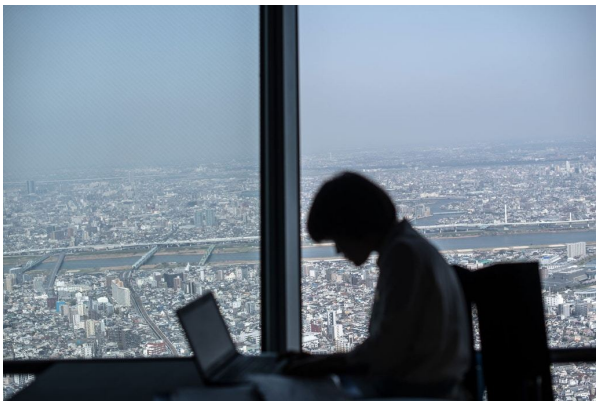
According to Richard Tanter, a professor at the University of Melbourne who specializes in researching government surveillance

https://doi.org/10.1017/S1557466018014493 Published online by Cambridge University Press

capabilities, more than 200 satellites are "visible" from Tachiarai, meaning the base can intercept communications and data passing between them using its surveillance systems. Of the 200-plus satellites, said Tanter, at least 30 are Chinese and potential targets for ongoing surveillance. Moreover, he added, "satellites owned or operated by Russia, South Korea, Taiwan, and even the United States or European states may be targeted" by the Tachiarai facility.

Snowden, who worked at a U.S. military base in Japan as an NSA contractor between 2009 and 2012, told The Intercept that Japanese spies appeared to have targeted "entire internet service providers, not just any one customer." Referencing the MALLARD program, he said that there were not "500,000 terrorist communications happening in one year, much less one hour. … Is this authorized in law in a way that's well-understood, that's well-regulated, to make sure they are only targeting bad guys and not simply everything that they see?"

A spokesperson for Japan's Ministry of Defense refused to discuss MALLARD, but said that the country's "information-gathering activities" are necessary for national security and "done in compliance with laws and regulations." The spokesperson acknowledged that Japan has "offices throughout the country" that are intercepting communications; however, he insisted that the surveillance is focused on military activities and "cyberthreats" and is "not collecting the general public's information." When pressed to explain how the country's spy systems distinguish ordinary people's communications from those related to threats, the spokesperson would not provide details on the grounds that doing so "may be a hindrance to effective future information activities.



A woman works on her laptop on the viewing platform of the Tokyo Skytree on March 29, 2018, in Tokyo, Japan. Photo: Carl Court/Getty Images

In October 2013, the Directorate for Signals Intelligence was planning to launch an operation aimed at what it described as the "Anonymous internet," according to the 2013 presentation. This suggests that the directorate wanted to collect data about people's usage of privacy tools such as Tor, which allows people to mask their computer's IP address while they browse the internet. Tor is often used by journalists and dissidents to evade government surveillance; however, it is also used by child abusers and other criminals to plan or carry out illegal acts. In April 2013, it was reported that Japanese police were urging internet service providers to find ways to block people who were using Tor to commit crimes. In 2012, the country's police investigators were repeatedly thwarted by a hacker known as the "Demon Killer," who posted a series of death threats online. The hacker used Tor to successfully evade detection for seven months, which was a major source of embarrassment for Japanese police — and likely fueled demand for new surveillance capabilities.

The directorate's activities at Tachiarai and elsewhere are aided by an organization called J6, which is a specialist technical unit connected to Japan's Ministry of Defense,

https://doi.org/10.1017/S1557466018014493 Published online by Cambridge University Press

according to sources familiar with its operations. However, the cooperation between the directorate and J6 has been inhibited by the extreme secrecy that is pervasive within the Japanese government, with each agency apparently reluctant to open up to the other about its respective capabilities. In the 2013 presentation, Japanese officials from the directorate described J6's role to the NSA, but admitted that they had relied on "assumptions" to do so, because "J6 function is not disclosed to us."

According to the presentation, the directorate's role is to carry out surveillance and analyze intelligence. The role of J6 includes analyzing malware and developing countermeasures – such as firewalls – to prevent hacks of Japanese computer systems. A third organization, called the Cabinet Intelligence and Research Organization, or CIRO, is the ultimate beneficiary of intelligence that is collected. Headed by a powerful figure named Kitamura Shigeru, it oversees the work of both the directorate and J6 and is connected to the prime minister's office, based out of a building known as "H20," a short walk from the prime minister's official residence in Tokyo's Chiyoda district.

Between 2000 and 2005, prior to development of the MALLARD internet surveillance program, expansion work took place at the Tachiarai facility. At that time, the then-town council chair, Miyahara, was shown a map of the construction plans, which revealed that a tunnel was being built below the base. Miyahara Hitoshi was allowed to visit the construction site, he said, but was prevented from entering the underground area. The current town council chair, Yano Tsutomu, had a similar experience. He visited the facility about four years ago and was shown around a gymnasium, a cafeteria, and a conference room. He was prevented from accessing the underground tunnel and a space he was told was used for "communications." Yano said he repeatedly questioned the Self-Defense Forces about the Tachiarai facility's function. But he never received any answers.

Ryan Gallagher is an investigative journalist and editor with the U.S. news website The Intercept. His work focuses on national security, human rights, counterterrorism, and technology. He can be contacted at: ryan.gallagher@theintercept.com

Ed Noguchi contributed reporting and translation.

https://doi.org/10.1017/S1557466018014493 Published online by Cambridge University Press