Developing Fundamental Solutions to Combat the Rise in Cybercrime:

What role can a third-party all-Japan industry-academia-government organization play in containing the threat posed by cybercrime?

Random, elusive, and ever more widespread, cybercrime today has become a menace to ordinary citizens, governments, and businesses alike. Already hackers have stolen private financial and medical data from credit bureaus and health insurance companies, exposing millions of people to fraud, identity theft and worse. From targeted attacks to ransomware, cybercrime is everywhere and no one is safe. Growing concern about the danger these threats pose to society has led to increasing cooperation worldwide between industry academia and government to develop anti-cybercrime solutions at the most fundamental level. Established in November 2014 with the participation of private companies, universities, and the National Police Agency (NPA), the Japan Cybercrime Control Center (JC3) has already succeeded in exposing the activities of many criminal groups. We asked Mr. Akira Saka, the JC3's executive director, about trends in cybercrime and how the organization is preparing to cope with them.

Akira Saka

Executive Director,
Japan Cybercrime Control Center (JC3)

Joined the NPA in 1981. After serving as Chief of the Meguro Police Station, Head of the Central and South America Office of Trade Policy Bureau of the Ministry of International Trade and Industry (MITI) — now the Ministry of Economy, Trade and Industry (METI), Chief of Hyogo Prefecture Police Office, Deputy Director General (Road Transport Bureau) of the Ministry of Land, Infrastructure, Transport and Tourism (MLIT), he became a leading advocate of the importance of taking on the challenge of cybercrime as Head of the Security System office in the Community Safety Bureau, and later took on the role of Director of the Cybercrime Division at the NPA. In 2002, he taught as an associate at the Weatherhead Center for International Affairs at Harvard University and, from 2008 to 2010, served as a Professor at the Graduate School of Media and Governance at Keio University. Since November 2014, he has been serving as Executive Director of the JC3. He is now also a member of Nuclear Security Regulatory Commission and CISO of the Tokyo Organizing Committee of the Olympic and Paralympic Games.

What are some of the recent trends in cybercrime?

—— Cyberattacks are creating havoc around the world, while cybercrime is becoming ever more prevalent. Is the threat environment changing? What trends are you seeing?

First of all, I have to point out that targeted attacks still account for the majority of attacks. According to the data of the first half of FY 2016 released by the NPA, actual targeted attacks — that is, attacks that target a specific victim — are increasing at a much faster rate than indiscriminate attacks that strike randomly at many different people. You can see a typical example of this trend in Daserf — which is a type of malware that specifically targets critical infrastructure companies. The modi operandi are becoming more sophisticated and more subtle — instead of brute force attacks, data is quietly collected from infected PCs over long periods of time. The same thing applies to ransomware, in addition to extorting users by taking files hostage, many types of new threats are appearing — for example, destruction of systems by self-propagation via networks.

Also on the rise recently is business email compromise — or BEC — in which perpetrators impersonate managers and clients to give fraudulent remittance orders to

financial and accounting staff members of targeted companies. There's also a new type of malware called Mirai, which mainly targets IoT devices such as network cameras and digital video recorders, as well as a new type of modus operandi called USB data theft — in which confidential information stored on USB drives used to transfer data from a closed network environment is stolen.

—— So now we've entered an era in which every business or individual is exposed to threats, haven't we?

Assailants always aim at targets they deem the weakest. In the financial industry, for example, major banks and regional banks had traditionally been the targets. But as banks have strengthened their security measures, the focus has switched to small-and-medium scale financial institutions such as credit unions/cooperatives, agricultural cooperative banks, and workers' credit unions. In particular, servers belonging to mid-rank small-and-medium-scale businesses can potentially be used as springboard to penetrate major corporations in supply chains. In other words, no matter what the size of the entity or the type of business, robust security is a must.

—— It seems that the number of targeted email attacks is also on the rise.

According to the NPA's Cyber Intelligence Information Sharing Network, the number of targeted email attacks increased in 2016 by 218 to 4,046. The number of inquiries from companies and the general public that year exceeded 130,000 — the highest ever. As for illegal remittances via Internet banking, while total financial damage has decreased, hackers continue to seek out new targets, searching for more vulnerable entities in various fields using new methods to exploit those targets. **Fig. 1** shows the financial losses incurred as a result of these attacks in the first half of 2015. As is clear from this figure, a wide range of financial institutions are being targeted, and the weakest ones are increasingly being preyed upon. Recently, even bitcoin accounts have become targets.

—— With threats increasing, what measures should governments and corporations take and what can they do to protect themselves?

In a sense, cybercrime is already established as a global business. Division of labor, so to speak, is also underway — in which many criminals such as malware developers, malware attack commanders, those who actually distribute malware, those who provide the servers used

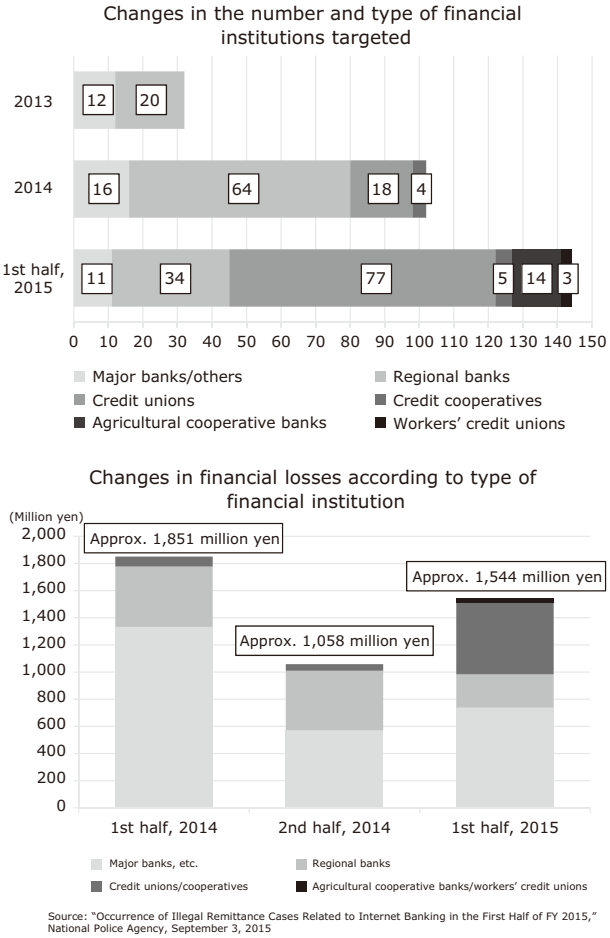

Fig. 1 Changing targets.

in these crimes, those who demand illegal remittance, those who provide illegal accounts, and cash "withdrawers" are all organically connected, even though they may be scattered around the world. To prevent such crimes, it is essential to cut off at some point the cyber kill chain — which is the attackers' action process.

At this point, the perpetrators most frequently arrested in Japan are the so-called "withdrawers." Though more exposed than those who plan and execute these crimes, "withdrawers" are nonetheless part of the cybercriminal infrastructure and may provide a means to trace back the instructions for illegal remittances. However, what's more important is to perform preemptive and comprehensive measures to fundamentally invalidate criminal groups while getting an overview of entire cyber kill chains. For this reason, an organization called the National Cyber-Forensics & Training Alliance (NCFTA) — which incorporates the FBI and other law enforcement agencies, private companies, and academic institutions — was established in 1997. Now underway at the NCFTA are efforts to cope with cybercrimes through collection/

analysis of cybercrime-related information and investigative cooperation on a global scale.

A mediator that makes the most of industry, government, and academia

—— So the JC3, of which you are executive director, was modeled on the NCFTA, right?

That's right. The JC3 was established in November 2014 — after studies at the government's Information Security Policy Council and the Abe administration's cabinet decision — with a view to dealing with threats in cyberspace by setting up a collaborative structure that transcends the barrier between industry, government, and academia. The JC3's participants include private businesses, the NPA, and academic/research institutions. They are sharing their respective information, experience, and know-how based on trust and non-disclosure agreements, while deploying activities to eliminate threats by elucidating the actual conditions of threats and specifying and pursuing the perpetrators. Other pillars of the JC3's operation include training of human resources and international cooperation with relevant overseas organizations.

—— What is the JC3's role in this consortium of industry, government, and academia?

I would say we play the role of mediator, leveraging the strengths of industry, law-enforcement, and academic/research institutions. In other words, we act like a hub that facilitates collaboration between these entities, distilling the insights that the participating enterprises have gained in their own experiences with cyberattacks and reinforcing that with the analysis and research conducted by academic/research institutions, while taking advantage of the investigative jurisdiction of law-enforcement agencies to develop powerful solutions that can stop cybercriminals in their tracks (**Fig. 2**).

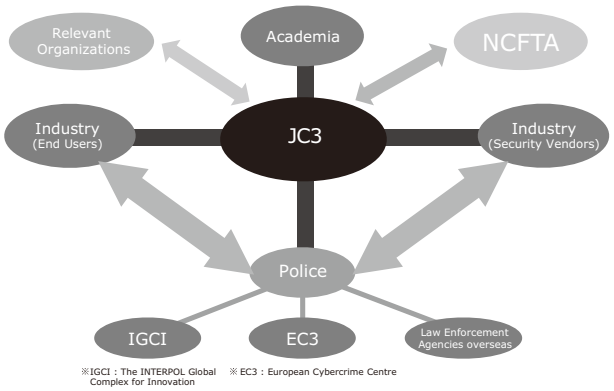

Fig. 2 Conceptual diagram of information/knowledge sharing at the JC3.

—— It seems that the NCFTA, after which the JC3 was modelled, has already had significant success in the United States.

Yes, it has. The NCFTA has been around for almost two decades, so they've chalked up quite a few successes. I heard that the number of arrests in cybersecurity cases last year alone added up to more than three hundred. The JC3 is also in a collaborative relationship with the NCFTA. And we are learning their methods such as the concept and organizational administration. For example, the NCFTA has four basic policies. They are: "One Team, One Goal," "Face to Face," "Industry First," and "Focus on What You Can Share and Are Comfortable Sharing."

The JC3 is operating with basically the same policies. The participants are building strong relationships of trust with each other, sharing information to fight against cybercrime as one team.

However, we do differ from the NCFTA in some ways. For example, more than fifteen national law-enforcement agencies, such as the FBI, as well as agencies outside the United States, are participating in the NCFTA. With the JC3, members of the NPA, which integrates police organizations throughout Japan, are permanently seconded to the organization. This makes it very easy for the JC3 to undertake simultaneous, coordinated investigations and police actions on a nationwide scale. Also because being a participant of the NCFTA puts an organization at greater risk of becoming the target of cyberattacks, many companies do not publicize their membership. On the other hand, the JC3 makes public the names of participating companies and supporting organizations — as you can see on our website. I think it's a reflection of our commitment to fight against cybercrime as a united front with each company implementing robust security measures and operating in harmony with partner companies.

Cooperating to take down cybercrime

—— As reported in the media, the JC3 — like the NCFTA — has had a lot of success in its efforts to crack down on cybercrime.

It's just over three years since the JC3 was established, so the number of cases we've worked on is by no means high. Nevertheless, in that limited time we have achieved some impressive success, arresting per-

petrators and taking down infrastructure of organized cybercrime. In November 2015, for instance, we helped arrest thirteen perpetrators, including administrators of illegal adult sites, in cooperation with municipal police in ten prefectures. In this case, the JC3 developed software in cooperation with the Ibaraki Prefectural Police to detect adult sites that were conducting illegal operations on the Internet. We identified about two thousand sites, including ones outside Japan, thereby helping them locate the administrators of those sites. We cannot ignore the operations of illegal sites and overseas servers, as the former can infect PCs that visit them and the latter can serve as a front for cybercrime if left unchecked.

Additionally we have been conducting cyberpatrols in conjunction with the Saitama Prefectural Police in an effort to combat the use of fraudulent bank accounts for illegal remittances via the Internet or for phone fraud. We detected about five hundred postings offering to buy or sell accounts, and exposed twelve perpetrators in October 2016. Seven of them were subsequently arrested and charged with enticement to buy and sell accounts, as well as with the purchase and sale of bank deposit passbooks.

—— So you have indeed had some tangible success in cutting off cyber kill chains.

In parallel to the crackdowns on these crimes, we are also working on the neutralization of fake websites. We started this effort because joint research conducted by the JC3 and participating companies found that the damage resulting from ransomware and illegal remittance viruses was expanding due to an attacking tool called Rig RIG-EK*. Users who browse fake sites are led to sites with RIG-EK installed where they are at risk of becoming victims of cybercrimes such as illegal remittance (**Fig. 3**). This is what's called a "watering hole attack." We are now working to get an overall picture of attacks carried out with RIG-EK, while working together with various prefectural police forces to help the administrators of victimized sites restore those sites and to help them develop the appropriate security measures to prevent further attacks.

As for awareness-raising activities, we post information about cybercrime cases on our website and warn of emergency situations based on analyses conducted by the JC3 and threat information obtained from the participating companies. Recent examples demonstrate how we have helped minimize the damage resulting from

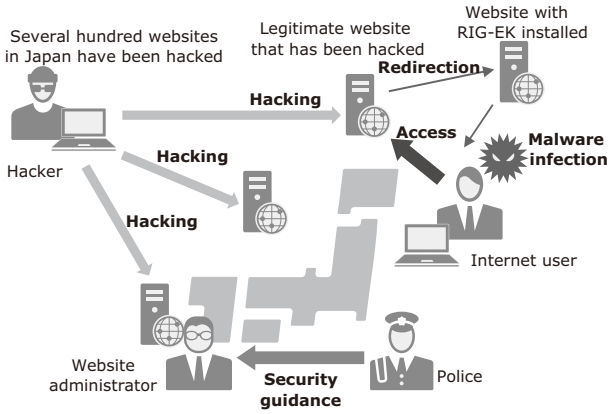

Fig. 3 Commitment to neutralizing fake sites.

these types of attack. In one case, we immediately posted a warning that virtual currency exchange sites were in danger of becoming targets of malware called DreamBot and we also publicized without delay the news that a new modus operandi to steal USB information had been confirmed.

The commitment of the JC3 is contributing to the suppression of cybercrimes

—— Could you tell us what are some of the difficulties you face in taking on the challenge of cybercrime?

Preventing or solving a cybercrime takes much more time and trouble than you might imagine. These crimes are exceedingly complex and contain numerous intertwined elements. Let's assume that we find a site that has been hacked as part of a watering hole attack for the purpose of infecting the user's computer with ransomware or illegal remittance viruses. In a case like this, it is very difficult to convince the administrators of the hacked site that there is a problem even though we notify them that their site is under attack and advise them that the site be repaired immediately. The way they respond to us is often like, they see no change taking place in their site because there is no obvious sign that the site has been tampered with or if they do accept that what we say is true they don't know how to cope with it.

Also when cracking down on the buying and selling of illegitimate accounts, we have to conduct simultaneous nationwide operation to prevent the perpetrators from noticing our activities. To achieve this, we also need to

* An exploit kit (EK) designed for attacking. It comes with various programs to infect PCs with malware according to the vulnerability of the accessed PCs.

conduct an investigation to identify perpetrators, collect and secure evidence such as logs, request collaboration from Internet providers and telecom carriers who are private companies, coordinate the operations of various prefectural police forces who actually carry out the crackdown operation, and arrange advance cooperation with international law-enforcement agencies if servers are located overseas. Without close and careful coordination between all the entities involved, an effective crackdown is not possible. In other words, a lot of time and effort is required before we can close the net on any particular cybercrime.

—— Yet when we look at the damage from cybercrimes in the past few years, we get the impression that the steady efforts you just mentioned have come to fruition since the launching of the JC3. For example, according to a report put out by the NPA in March 2017, illegal Internet banking remittances were down in terms of both the number of cases and the actual amount of money swindled. Similarly, the number of unauthorized accesses detected continued to decrease, down again from the previous year. The number of arrests, on the other hand, was the highest ever with 502, while the number of investigations conducted was also the highest ever with 200. Now isn't it fair to say that the JC3's commitment has significantly impacted these trends?

Thank you very much. We certainly played a part, but, of course, those results could not have been achieved by the JC3 alone. My understanding is that they are the results of the synergy between the leading-edge security measures implemented by private companies, the resolute attitude of the police forces who refuse to tolerate cybercrimes, and their collaboration with overseas law-enforcement agencies. For example, there was a famous international case recently. It was a take-down operation of a cybercrime infrastructure called Avalanche. This operation succeeded in taking apart the networks used for command and control at the end of 2016, thanks to the cooperation of law-enforcement agencies and security vendors over the world. As part of this take-down operation, many entities in Japan including the NPA actively endeavored to eradicate malware by notifying users based on information shared with overseas organizations. A big issue now is how to cope with botnets that are used for various crimes. I'd be delighted to see efforts like this being originated in Japan and more than happy if the JC3 can contribute to it.

—— The war against cybercrime will continue for sure. What role do you see the JC3 playing in the future?

If we are to defeat cyberattackers — whose modi operandi become daily more sophisticated — it is critical that we work together with all affected parties to build relationships of trust so that we can create the universal solutions required to neutralize the very source of threats. At the JC3, cooperation between companies, government and academia is growing and is being accompanied by tangible results. We have received cooperation from security-related companies, financial institutions, and e-commerce-related companies. We believe that it is important that we share actual threat conditions by soliciting reliable partners that transcend the frameworks of types of business and industry — including manufacturing, logistics, and trading companies — according to the actual threat conditions. From a global perspective, we will fight against global cybercrimes by strengthening collaboration with investigative organizations such as Britain's Cyber Defense Alliance (CDA) as well as the Interpol and Europol, in addition to the NCFTA.

—— We look forward to seeing your impact on cybercrime in the future. Thank you very much for speaking with us today.

* This article is based on an interview conducted in July 2017.

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.12 No.2 Cybersecurity

- Building Futureproof Security to Support Business Safety and Reliability -

Vol.12 No.2
January 2018

Special Issue TOP