1 Introduction: Overview of NICT's Research and Development Projects on Network Security

Kazumasa TAIRA

ICT (Information and Communication Technology) supports our daily intellectual activities and economic activities. The Internet, in particular, takes the central role. Recently, people connect their personal computers to computer networks to use information and communication services, and furthermore, as smartphones have grown explosively, people have come to enjoy information and communication services through networks, at any time and from anywhere. So, how the information and communication infrastructures are used has been changed, quantitatively and qualitatively.

At the same time, many families that are using the Internet reportedly have concerns about the security of the Internet—they fear "computer virus infection," and they can't find out "to what extent they have to apply computer-security measures." Actually, we know of cases of business enterprises where their network systems were intruded into and their internal data were stolen and leaked, or criminal cases where computer viruses targeting smartphones were involved, and furthermore the number of such network incidents has increased day by day. We have come to be trapped in situations where, without countermeasures for securing the network environment, we can't use information and communication services safely and securely.

The National Institute of Information and Communication Technology (NICT), during its 3rd Medium- to Long-Term Target Period—five years from FY2011 to FY2015—has conducted research and development (R&D) projects on network security technologies. The competent minister (Minister of Internal Affairs and Communications) set "Medium- to Long-Term Target" for the conduction of the R&D projects. NICT built "Medium- to Long-Term Plan" according to the target, and obtained approval for the plan. The target and the plan are presented below.

(The Minister of Internal Affairs and Communications recommend NICT to conduct its R&D projects for the following objectives.)

[Medium- to Long-Term Target]

Conducting of the R&D of technologies in which the results of theoretical research and practical development are highly integrated, including the cutting-edge technologies that enable world-wide observation, analysis, countermeasures and prevention of cyber-attacks; technologies for the design, evaluation and optimization of secured networks; and next-generation cryptographic technologies.

(NICT built the following plans according to the above recommended objectives.)

[Medium- to Long-Term Plan]

For realizing a society where people can safely and securely use information networks without being aware of the supporting technologies existing behind them, NICT will promote its R&D projects by taking the two-directional approaches—"present-oriented," and "future-oriented"— as shown below.

Present-oriented approaches: aiming for creating ready-to-deploy research achievements, through conducting R&D with focus on technologies that enable to observe, analyze, take actions and take countermeasures on a nationwide basis against cyber-attacks which are advancing and becoming more devious day by day.

Future-oriented approaches: for the purpose of the realization of highly attack-resistant networks with high-level security, conducting the following R&D projects with mid- or long-range perspectives through reconfiguring the methods of security-design from scratch; new security architectures ensuring the automatic selection and deployment of the optimum device to different types of users or network devices; next-generation cryptography and authentication technologies freed from cryptographic algorithm compromises whose risks are growing as computer performance increases or advanced decryption technologies that ensure high-level safety for a long period: and security technologies to, even in a situation of social crisis

such as a great disaster, ensure prompt information gathering, secure information reliability and realize simple and robust authentication.

In addition, determining the subjects of R&D with care to pick as universal subjects as possible and, for the purpose of coping with situational changes that would newly rise during the mid/long-term period—for example, new types of cyber-attacks.

Preserving the flexibility of plans to ensure the modification or addition of R&D plans.

NICT has made the following project-promotion policy for implementing the plans described above:

In order to protect Japanese network infrastructure against cyber-attacks, we drive for a center of excellence in practical and theoretical network security by means of the high neutrality of NICT.

Following the policy, NICT had applied its R&D efforts for five years, focusing on and around the following three major projects:

(1) R&D of Cybersecurity Technologies

For the purpose of promptly and actively tackling cyber-attacks whose attack methods have become advanced in their technological level and deviousness, building observation networks that cover the world to promote R&D for cyber-attack observation, analysis, countermeasure and prevention. In addition, promoting studies on safe-and-secure distribution and utilization of various data and cases of cyber-attacks which would be accumulated in NICT—NICT stands in the best position for collecting such information because it is a public and neutral institution.

(2) R&D of Security Architecture Technologies

Promoting R&D of technologies that ensure the provision of network-based services through automatic configuration of security environments optimized for various network situations. In addition, promoting R&D of new types of technologies expected to be critical for services through mobile devices and the cloud that will grow in future.

(3) R&D of Security Fundamental Technologies

Promoting the R&D of technologies for the construction of information-theoretically safe networks where both post quantum cryptography and conventional cryptography are used. In addition, conducting security evaluation of cipher systems by using the most advanced decryption techniques.

NICT, in order to promote the above-described R&D projects, established the "Network Security Research Institute" for the 3rd Medium- to Long-Term Target Period, and further established in the institute the following three research laboratory: the "Cybersecurity Laboratory," "Security Architecture Laboratory," and the "Security Fundamentals Laboratory."

NICT conducted self-reviews of the research activities of the abovementioned R&D conducted in the five years, concluding that the achievements largely exceeded the Medium- to Long-Term Target. At the same time, the Competent Minister acknowledged that "NICT has attained achievements that largely exceed the original objectives set for the Medium- to Long-Term Plan." The Competent Minister stated that NICT was regarded with high valuation because it attained the achievements shown as follows:*

[Evaluation by the Competent Minister]

The Competent Minister gives NICT's research activity in its 3rd Medium- to Long-Term Target Period an "A." NICT conducted its research and development activities of network security, whose objectives set for the 3rd Medium- to Long-Term Plan were cyber security technology research and development including the establishment of technologies for cyber-attack analysis and prevention, having created remarkable achievements that are expected to lead to future developments under proper, effective, and efficient management for the purpose of obtaining "maximum achievements" from research activities .

Major achievements are shown below.

- Construction of the world largest cyber-attack observation network holding more than 300,000 IP addresses. Creation of remarkable achievements including the development of the cutting-edge observation, analysis and, visualization technologies for both of the absolutely different types of attacks—indiscriminate attacks and advanced persistent attacks.
- Great contribution to the improvement of Japan's cyber security threat through the technology transfer of DAEDALUS and NRVANA, including DAEDALUS operation on 558 local governments in Japan (as of

* Reference: www.nict.go.jp/disclosure/s3-hyouka.pdf (in Japanese)

March 2016).

- Establishment of the international consortium on cryptographic protocol evaluation technology "Cryptographic protocol Evaluation toward Long-Lived Outstanding Security (CELLOS) Consortium," taking the key role in its activity (including the administrative role) and taking a leading role in the international collaboration arrangement.
- The world's first implementation on a quantum network of secured external storage equipped with a password authentication function, which has secrecy and authentication functions that are information-theoretically safe. Also, active contribution for the international standardization of the abovementioned security scheme.

In this special edition, we present the R&D projects that were conducted during the 3rd Medium- to Long-Term Target Period, what NICT conducted and what achievements it attained, for each of the previously mentioned projects (1) to (3). Sections **3** to **5** cover project (1), Section **6** covers project (2) and Section **7** covers project (3). Details are shown in each of the sections. We have already reported in the special issue of "Journal of NICT" on our projects at the time when the 3rd Medium- to Long-Term Target Period was finished with a hope that the papers on our research will work as references for future-generation researchers. In a similar way, if this special issue could help researchers or engineers engaging in network security R&D, or others having interest in the field, we would feel very happy.

At present, we are in the middle of the R&D activities for the 4th Medium- to Long-Term Plan that started in April of this year, where the research field covered by the 3rd term plan was expansively renamed to "Cyber Security Technologies." We would appreciate if you could give further support and cooperation for the cyber security field.

Before closing this introductory section, we would like to express our appreciation to Dr. Yukio Takahashi who had been the Director of the Network Security Research Institute until September 2012 (at present, Associate Director General of Resilient ICT Research Center, Social Innovation Unit), each of the members of Planning Office of the Institute, each of the researchers from the academic or private organizations who gave cooperation, and others concerned.

Kazumasa TAIRA, Ph.D. (Eng.)

Director General, Applied Electromagnetic Research Institute/Former: Director General, Network Security Research Institute
Radio Wave Propagation, Electromagnetic Environment, Communication System