An Analysis of the Actual Status of Recent Cyberattacks on Critical Infrastructures

NOGUCHI Mutsuo, UEDA Hirofumi

Abstract

An increase in cyberattacks on critical infrastructures, especially on electric power systems, has been reported recently. It was previously thought that the risk of cyberattacks on critical infrastructures was low because of the need for specialist knowledge on the control system configuration and administrative operations as well as on the absence of suitable Internet connections. However, now that cyberattacks on critical infrastructures are exerting a significant impact on society, it has become necessary to reconfirm the risks by analysing the techniques used in such attacks. This paper references some cases of cyberattacks on electric power systems and discusses the issue of system administrations avoiding protective measures and thereby permitting attacks.

Keywords

critical infrastructures, control systems, Power & Utilities, cyber security, incident cases

1. Introduction

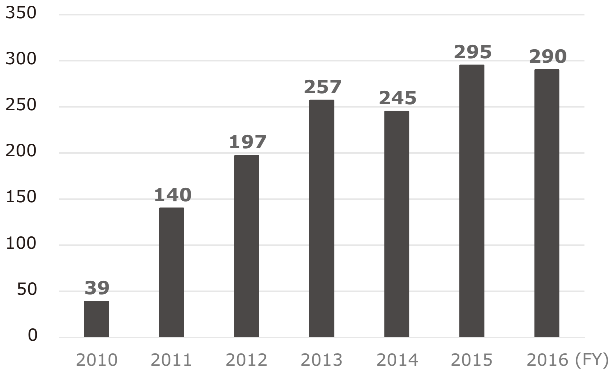
Among the critical infrastructures including electricity, gas and water supply systems, cyberattacks on electric power systems have recently been reported at an increasing rate. Many of the causes permitting these attacks lie in the ICT components that were introduced in the past with the aim of improving system maintenance efficiency and reducing the costs of critical infrastructures. These components act as a gateway for attacks that permit intrusion of the control systems using malware infections. Since the ICT employs many open technologies such as standardized specifications and universal OSs, critical infrastructures introducing ICT inevitably include security risks similar to those of information systems. As a countermeasure to such risks, critical infrastructures have been operated without connecting their control systems to external networks, including the Internet. A deep knowledge of the configuration and administrative operations of control systems is necessary for a cyberattack to cause physical damage to a critical infrastructure. Therefore it has been widely assumed that attacking an infrastructure would be difficult compared to attacking an information system[1]. Nevertheless, the creation of malware targeting control systems, such as Stuxnet and Black Energy, has made it a reality to cause malware infection and control system manipulation without passing through an external network. The shutdown of a critical infrastructure due to a cyberattack may lead to failures of the associated social settings and of business activities and can exert a significant social impact. Therefore, it is important to analyse the attacks that target control systems and reflect on the results in planning the security measures of the future.

In this paper, the authors analyse the techniques used in some of the actual cases of cyberattacks on critical infrastructures of the past. Based on the analysis, we discuss the issues of the attacks being successfully accomplished due to administrative neglect in applying protective measures.

2. An Examination of Cyberattacks on Critical Infrastructures and Its Analysis

2.1 Increase in the Number of Incidents

Fig. 1 shows the recent change in the number of incidents on critical infrastructures. Stuxnet is a malware that destroyed the centrifuges in the uranium enrichment plant in Iran in 2010. Since this attack, cyberattacks in the fields of energy, critical equipment manufacturing and communications have been increasing in overseas countries. For example, as in the successive large-scale power outages caused by cyberattacks on the Ukrainian power supply systems in 2015 and 2016[2]. These events suggest that the energy field, including that of power supply has a high risk of exposure to high-impact cyberattacks because they can have a particularly high effect on a nation's economy.



FY : Fiscal Year (Oct./1 – Sep./1)
Graph created based on ICS-CERT Year in Reviews 2012-2016

Fig. 1 Number of incidents handled by U.S. ICS-CERT[3].

2.2 Cases of Incidents Caused by Cyberattacks, Their Causes

The present section focuses on the energy field, including the power supply systems that have experienced serious incidents by cyberattacks. **Table 1** shows some of the actual cases of incidents that have occurred in the past. The 2000's were the period in which the use of ICT advanced globally. Due to the spread of broadband networks, VPN connection devices were introduced for the maintenance of the control systems of critical infrastructures from the viewpoints of convenience and cost reduction. The use of control equipment based on universal OSs such as Windows was also expanded. As a result of these trends, the control systems that had used independent specifications have come to be configured using open standardized specifications and universal products. On the other hand, the introduction of ICT has created a security risk and illegal connections to VPNs and malware infections via USB memory devices began to occur as is shown in Table 1. The above trend was not caused exclusively by the introduction of ICT but also because the vulnerability of software was left untouched. There was a condition that was specific to control systems – they were designed based on the idea of "eliminating any factor that would jeopardize the system availability," which tended to hinder the application of the measures as listed below:

- Introduction of antivirus software
- Application of a security patch to an OS

Table1 Some of the actual cases of incidents involving critical infrastructures.

Country	Publication	Case Summary	Cause
USA	2001	SCADA system 2-week shutdown for repair.	Insufficient access protection of VPN connection system for contracted vendors
USA	2003	SCADA system approx. 5-hour shutdown & process computer approx. 6-hour shutdown at Davis-Besse Nuclear Power Station.	Intrusion and infection by slammer warm through VPN connection used by a contracted vendor
EU	2003	3-day loss of management functions of several power distribution/transformation stations.	Malware infection of distributed SCADA system
Japan	2005	Leak of atomic power plant's confidential information via file sharing software.	Malware infection of an employee's home PC storing confidential info
Japan	2006	Leak of thermal power plant's confidential information via file sharing software.	Malware infection of an employee's home PC storing confidential info
USA	2006	Loss of control of recirculated water pump at Browns Ferry Nuclear Power Plant.	Malfunction of Siemens Perfect Harmony VFD controller due to excessive traffic on power plant's integrated ICS network
USA	2010	Gas leak from pipeline due to computer malfunction.	Computer malfunction (cause unknown)
Iran	2010	Destruction of centrifuges at Natanz uranium enrichment facility by malware Stuxnet.	Malware infection
USA	2012	Malware infection of computers in control system environments of two power plants, causing 3-week restart delay for one and operation limiting for the other.	Malware infections of work USB drives
USA	2014	Information leak due to attacks targeting at US/Canadian aero-defence firms/air carriers and energy businesses including EU ones.	Malware (Havex) infection of SCADA systems due to attacks by Dragonfly hacker group
USA	2015	Large-scale DoS attack of FirstEnergy Corp. (No damage)	Unknown
Ukraine	2015	A few hours of power outage in western Ukraine (Ivano-Frankivsk Oblast).	Cyberattack using malware Black Energy 3
Israel	2016	2-day shutdown of part of computer system for dealing with a cyberattack.	Malware infection by phishing attack
Germany	2016	Publication of confusion produced by a cyberattack in around 2013 or 2014.	Unknown
Ukraine	2016	Approx. 1-hour power outage of 1/5th of power supply destinations in Kiev.	Cyberattack using malware Industroyer/Crash Override
Ukraine	2017	Infection of malware NotPetya of radiation monitoring system at Chernobyl nuclear power plant forcing manual control.	Malware infection (ransomware)

- Updating of installed software

What we noticed about the damage caused by malware infections was that the operational errors due to information leaks and overloads was predominant in the earlier years but that the physical damage has been increasing more recently. Based on this background, the section that follows will focus the techniques used in the cyberattacks that have led to physical damage.

2.3 Analysis of Techniques of Cyberattacks Causing Physical Damage

The present section explains the techniques that have caused physical damage by controlling systems in actual cyberattack cases including; 1) An attack using the Stuxnet malware that occurred in Iran in 2010; 2) An attack using Black Energy 3 that occurred in Ukraine in 2015.

(1) Analysis of a case of cyberattack in Iran

Fig. 2 shows the stages of this cyberattack as analysed using the cyber kill chain[4] framework that models the series of actions that the attacker takes by likening them to military actions. Although the methods of “reconnaissance” and “weaponization” are not clear, it is reported that it was the United States that collected information in advance and created Stuxnet using the nuclear facility equipment that was confiscated from Libya[5]. The characteristics of this attack include “utilization of the vulnerability of universalized control equipment” and “cover-up of communication for hiding the attack and invalidation of warning devices.” Although the operating status of equipment in a control system is surveyed by warning devices and workers, sophisticated invalidation can be regarded as the cause allowing this cyberattack to result in physical destruction.

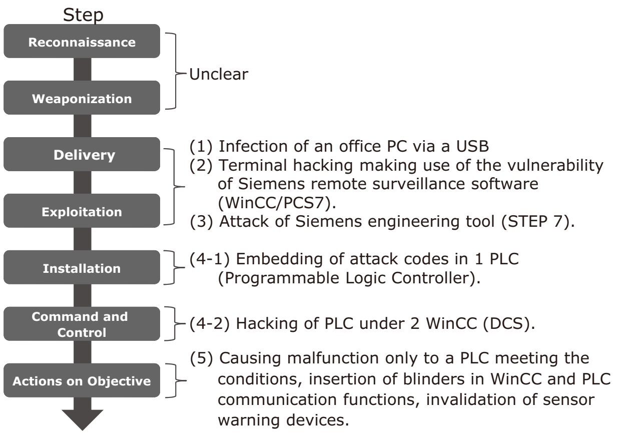

Step
Reconnaissance
Weaponization
Unclear
Delivery
Exploitation
(1) Infection of an office PC via a USB
(2) Terminal hacking making use of the vulnerability of Siemens remote surveillance software (WinCC/PCS7).
(3) Attack of Siemens engineering tool (STEP 7).
Installation
(4-1) Embedding of attack codes in 1 PLC (Programmable Logic Controller).
Command and Control
(4-2) Hacking of PLC under 2 WinCC (DCS).
Actions on Objective
(5) Causing malfunction only to a PLC meeting the conditions, insertion of blinders in WinCC and PLC communication functions, invalidation of sensor warning devices.

Fig. 2 Flow of cyberattack using Stuxnet.

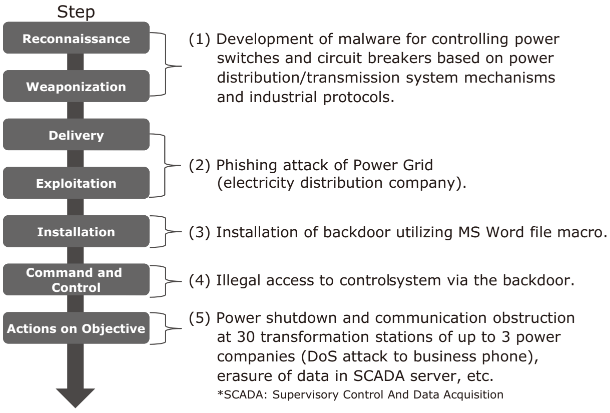

Step
Reconnaissance
Weaponization
(1) Development of malware for controlling power switches and circuit breakers based on power distribution/transmission system mechanisms and industrial protocols.
Delivery
Exploitation
(2) Phishing attack of Power Grid (electricity distribution company).
Installation
(3) Installation of backdoor utilizing MS Word file macro.
Command and Control
(4) Illegal access to controlsystem via the backdoor.
Actions on Objective
(5) Power shutdown and communication obstruction at 30 transformation stations of up to 3 power companies (DoS attack to business phone), erasure of data in SCADA server, etc.
*SCADA: Supervisory Control And Data Acquisition

Fig. 3 Flow of cyberattack using Black Energy 3.

(2) Analysis of a cyberattack case in Ukraine

Fig. 3 shows the steps of a cyberattack in Ukraine using malware Black Energy 3 in the same way as for case (1). This attack had three characteristics including: “involvement of persons with knowledge of industrial protocols in malware development,” “large-scale simultaneous attacks of 30 power transformation stations” and “obstruction of incident response after attack occurrences (paralysation of business communication processes, deletion of data). There had previously been direct attacks aimed at controlling system equipment but there had been no cases in which multiple control systems were attacked simultaneously by utilizing the industrial protocol used in communications between control systems. In addition, it is regarded that the change in the attack hiding method from hiding the communication to obstructing the recovery operations led to the additional damage. The consequent simultaneous attacks on the control system and on the administrative operations is regarded as being the factor that made the attack successful. This case also shows that the attackers now have detailed knowledge on the mechanisms of control systems and on their administrative operations at a level capable of causing large-scale power outages via cyberattacks.

2.4 Conditions Enabling Cyberattacks on Critical Infrastructures

The conditions enabling the cyberattacks that succeeded in producing physical damage to critical infrastructures, described in sections 2.2 and 2.3 above, are as follows.

(1) Utilization of open control system equipment.
(2) Attacker's understanding of specifications and ad-

ministrative operations.

(3) Multiplexed faults (including obstruction of recovery operations)

As some pieces of control equipment use a universal OS, the attacker can make use of the difficulty of software patch application as described in section 2.2. The attacker understands the specifications and administration operations of the control system well, so that the attack is organized accurately.

The control system usually retains availability based on the functional safety as defined in IEC61508[6] and it is very resistant to accidental (single point of) failures. However, as described above, the cyber-attacker can intentionally produce multiplexed faults. Since the viewpoint of functional safety tends to consider that the probability of such simultaneous occurrences of multiple faults would be very low, many organizations may not apply countermeasures when assuming such a case. Consequently, the means of succeeding in a cyberattack becomes how to produce multiplexed faults and how to avoid the mechanisms of functional safety.

3. The Importance of Current Electric Power System Protection Measures

3.1 Security Measures Taken in the USA

This section explains the protection measures taken currently for electric power systems. After the threat of cyberattacks of control systems increased as described in section 2 above, the United States prepared the regulations and organizations as shown in **Table 2**. After the North American Electric Reliability Corporation (NERC) defined the minimum security for electric power systems ((1) in Table 2), power companies are obliged to enforce countermeasures and to report them. The E-ISAC (Electricity Information Sharing and Analysis Center) was established as an organization for information sharing among power companies. Furthermore, the NERC also defined enforcement of training, so that optimum response could be made in the case of a cyberattack ((5) in Table 2). It seems that the definition of such regulations under governmental leadership is backed by the committed recognition by the government that damage to the security of critical infrastructures could seriously shake national security.

Table 2 Electric Power System security regulations in the U.S.

Item	USA
(1) Standard	NERC CIP Standards version 6 (Standard guidelines) ＊Established by NERC and approved by FERC (FederalEnergy Regulatory Commission). Obligatory standards for the electricity field composed of a total of 383 pages in 11 documents. Other representative guidelines • NIST IR 7628(Guidelines for Smart Grids) • ES-C2M2（Management maturity model） • NIST Framework（Guidelines for critical infrastructures） • NIST SP 800-82（Guidelines for control systems）
(2) Audit	North American Electric Reliability Corporation (NERC) ＊Also enforced by a state government if the state has its own regulations.
(3) Penetration Test	Enforced at the discretion of each business. ＊Vulnerability assessment (paper or active) is defined as obligatory by the NERC CIP.
(4) Information Sharing	Electricity ISAC(E-ISAC)
(5) Exercises	Including development of control system security technologies such as Grid EX (Security exercise for Power & Utilities's systemoperators) and Cyber Storm (Security exercise in the USA)

3.2 Security Measures in Japan

In Japan, the Basic Act for Cybersecurity was enacted in 2014 in order to enhance the security of critical infrastructures such as those for electricity and gas supply. In 2017, the JE-ISAC (Japan Electricity Information Sharing and Analysis Center) was launched. JE-ISAC is expected to take a similar role with the one in the U.S. as an organization for cybersecurity information analyzing and sharing among electricity business entities. However, preparation of the regulations and countermeasures at JE-ISAC are still insufficient (see **Table 3** and compare it to Table 2). The reason for this is that no significant incident at critical infrastructures has yet happened in Japan. Frequent natural disaster occurrence in Japan can be another reason. In comparison with other countries situation, advanced and stable maintenance and operation of good power distribution and transmission systems such as recovery from large-size power outage, etc. are already provided in Japan. Such situations may result in less progress of the regulation preparation.

Table 3 Electric Power System security regulations in Japan.

Item	Japan
(1) Standard	Guidelines for Power Control System Security ＊JESC standard No. JESCZ0004 (2016) Established on May 30, 2016 for giving conceptual guidance in 12 pages.
(2) Audit	None
(3)Penetration Test	Arbitary
(4) Information Sharing	JE-ISAC (established on March 2017)
(5) Exercises	Arbitary

3.3 The Importance of Electric Power System Protection Measures

As described in the previous section, the situations of the applied measures are quite different between the United States and Japan, although both belong to advanced countries. Based on this anomaly, this section discusses the importance of power system protection measures by taking economic damage as an index. There is a report estimating a cyberattack to an UK critical infrastructures, published by Lockheed Martin, which is a major U.S. arms company, and Cambridge University.[7] This estimate calculates that, if a power outage due to cyberattack should last for several weeks, the economic effects would continue for five years from the incident occurrence and the losses would be equivalent to 2.3% of the GDP. This means, considering that the economic growth of an advanced country is a few percent[8], that a cyberattack to a power supply can become a cause of significant stagnation affecting economic growth. Meanwhile, particularly recently, the attack groups performing cyberattacks to specific businesses and critical infrastructures are often backed by certain countries and some cyberattacks stem from their intensions[9] [10] [11], in which case cyberattacks serve as a means of political exchange between nations. When interstate conflicts deepen and interventions in other nations' affairs by means of cyberattacks increase, it seems that electric power systems become one of the clear targets because of the potentially critical social impact. Therefore, studies and the establishment of sufficiently robust protection measures will also be required, as in Japan.

4. Conclusion

Cyberattacks on critical infrastructures such as power systems have important economic implications and risk becoming targets in conflicts between nations. On the other hand, the current situation does not encourage the conventional ideas on critical infrastructures such as that "control systems without the Internet connections are safe" or "attacks are difficult without knowledge of operations." In the future, the security of power systems should be considered in presupposing that the attackers have an understanding of the system configurations and administrative operations. Moreover, considering the potentiality of becoming a source of conflict between nations, it is regarded that the collaboration between the efforts made by industry such as via E-ISAC or JE-ISAC and the national government is no longer sufficient. A deeper collaboration between the private and governmental sectors, including those with the ISACs of other countries, will therefore tend to increase in importance in the future.

* Windows is a registered trademark of Microsoft Corporation in the U.S. and other countries.
* All other company names and product names that appear in this paper are trademarks or registered trademarks of their respective companies.

Reference

1) Ministry of Economy: Trade and Industry, Cybersecurity measures for electricity (in Japanese), July 2016
http://www.meti.go.jp/committee/sougouenergy/denryoku_gas/kihonseisaku/pdf/007_06_00.pdf
2) ArsTechnica: Hackers trigger yet another power outage in Ukraine, 2017.1
https://arstechnica.com/information-technology/2017/01/the-new-normal-yet-another-hacker-caused-power-outage-hits-ukraine/
3) ICS-CERT
https://ics-cert.us-cert.gov/
4) Cyber kill chain
http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html
5) ArsTechnica: Confirmed: US and Israel created Stuxnet, lost control of it
https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/
6) International Electrotechnical Commission: Functional Safety and IEC 61508
http://www.iec.ch/functionalsafety/
7) Kelly, S. et al.: Integrated Infrastructure: Cyber Resiliency in Society, University of Cambridge, 2016.01
8) United Nations: National Accounts Main Aggregates Database
https://unstats.un.org/home/
9) FBI Press Releases: Update on Sony Investigation, 2014.12
https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation
10) FBI Implicates North Korea in Destructive Attacks, 2014.12
https://www.crowdstrike.com/blog/unprecedented-announcement-fbi-implicates-north-korea-destructive-attacks/
11) WIRED: Your Guide to Russia's Infrastructure Hacking Teams, 2007.12
https://www.wired.com/story/russian-hacking-teams-infrastructure/

Authors' Profiles

NOGUCHI Mutsuo
Senior Researcher
Security Research Laboratories

UEDA Hirofumi
Senior Researcher
Security Research Laboratories

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 -

\Orchestrating a brighter world NEC
NEC Technical Journal
Cybersecurity
- Building Futureproof Security to Support Business Safety and Reliability -
Vol.12 No.2

Vol.12 No.2
January 2018

Special Issue TOP