CYBER FUSION
Twining Physical and Virtual Security
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Introduction</td>
</tr>
<tr>
<td>02</td>
<td>Beginning of a Threat</td>
</tr>
<tr>
<td>03</td>
<td>How It Can Affect Cities</td>
</tr>
<tr>
<td>04</td>
<td>Need for Actionable Intelligence</td>
</tr>
<tr>
<td>06</td>
<td>A Possible Scenario</td>
</tr>
<tr>
<td></td>
<td>A  Verifying an Attack</td>
</tr>
<tr>
<td></td>
<td>B  Tracing the Attack</td>
</tr>
<tr>
<td></td>
<td>C  Finding the Suspects</td>
</tr>
<tr>
<td>08</td>
<td>NEC Solutions Can Help</td>
</tr>
</tbody>
</table>
Safer cities through a fusion of cyber and physical security

A smart fusion of cyber security and physical surveillance will help keep cities safe and secure from increasingly sophisticated threats in the years ahead.

From acts of teenage mischief in the 1980s, cyber attacks have today become immeasurably more potent and dangerous. Often large scale, organized and sophisticated, they are capable of targeting the critical infrastructure of cities and countries worldwide.

These threats have the potential to paralyze governments and threaten public safety if they affect critical resources such as power, water or connectivity that citizens rely on for daily living.

A coordinated attack today is not unlike spy movies in the past. From stealing information that compromises the privacy of millions of citizens to causing physical damage to public facilities, attackers are finding ways around many traditional cyber defenses.

The amount of damage such a future attack can bring can be substantially worse than any seen before. In March 2014, a United States federal study on the vulnerability of the country's electricity grid found that it could trigger a national blackout by taking out just nine of the country’s 55,000 electric-transmission substations.

In November 2014, US Homeland Security sources told ABC News that a destructive malware had penetrated the software running much of the nation's critical infrastructure, including oil and gas pipelines, power transmission grids, water distribution and filtration systems, wind turbines and even some nuclear plants.

In late December 2014, South Korean authorities said they found evidence of a “low risk” malware in devices connected to some nuclear plant control systems, but fortunately no harmful attack was mounted against the reactor controls by a hacker.

Through a myriad of technical and non-technical attack techniques, from physical trespasses to exploiting zero-day vulnerabilities, sophisticated adversaries are turning into real and persistent threats to public safety that cities and public organizations have to face up to in the years ahead.

The emergencies of cyber-physical security threats call for a change in defense strategy. Besides shoring up sophisticated cyber defenses and real-world video surveillance, government agencies can be better prepared by using the information generated from both realms to better derive actionable, timely information.

This would enable them to more quickly piece together the shape of an attack, identify potential suspects and apprehend them before they could launch further attacks on other critical infrastructure.
In 2010, when Iran was hit by an unprecedented cyber attack on its nuclear plants, the world was suddenly awoken to a new type of threat to a city’s critical infrastructure that was more potent than anything before.

The malware known as Stuxnet had managed to enter the Iranian industrial control computers, likely through a contaminated USB drive, stayed dormant for years, before slowly taking over the control systems at the facility.

Fooling human operators by sending out fake signals, it shut down the centrifuges little by little, eventually damaging the equipment and setting back Iran’s nuclear plans by several years. That was the start.

Just four years later, the same code used in Stuxnet has been modified, spread openly and made even more dangerous. It has been used to attack another nuclear facility, it is believed, and may have even spread to the International Space Station, according to one security firm.

For city authorities, warding off a sophisticated cyber attack is something that has become an increasingly difficult and costly task.

While the defenders are in the open, they face threats quietly lurking in the dark confines of cyber space. Without a name or face to place a suspect to, law enforcement agencies are also often at a loss to find and remove threats proactively.

The solution could lie in a smart fusion of both cyber security tools and physical surveillance. In other words, deriving actionable intelligence from clues in cyberspace as well as those from physical locations.

Digital log files from servers could be pieced together for deriving clues of where an attack originated, for example. From here, physical surveillance and facial recognition could help pinpoint suspected perpetrators of an attack.

Despite advances made of late, this innovative cyber fusion of technologies is still new to many cities. As they increasingly depend on smart systems to wire up critical infrastructure, the daily risk they face is increasing.

A coordinated cyber attack has a larger “surface area” to aim at, because of the deployment of SCADA or supervisory control and data acquisition systems to handle industry equipment in recent years.

Where it once took human operators to make a lot of decisions, say, at a power plant, today a computer has that role. If successful, a cyber attack that successfully takes over a SCADA system will cause significant damage to a city.

Many experts believe the presence of such an attack that manages to paralyze big parts of a city’s critical infrastructure is not only possible, but undeniable, in the years ahead.

In 2013, a former director of the United States’ National Security Agency claimed that up to 90 per cent of the world’s computers holding strategic, monetary or intellectual value may have already been infected by undetected malware.

And at the start of 2014, the unrest in Ukraine was marked by the use of sophisticated cyber weapons. One known as Snake is said to have infected dozens of government systems, and could potentially prevent many public services from being provided.

In the years ahead, it’s clear that city planners and leaders have to make cyber fusion a key defense strategy in their public infrastructure.
The threat of a city being deprived of its vital resources — power, water or connectivity — is real today. A city can come under such a coordinated attack from well-organized groups that would have penetrated vulnerable computer systems for years and waited for the right moment to strike.

These advanced persistent threats (APTs) are the biggest worry for many system administrators today. And city authorities are rightly seeking solutions to tackle them as well.

Perpetrators of such attacks often attempt to enter an organization through the most vulnerable points. Part of the playbook includes some forms of social engineering and/or physical trespass. Certain executives in an organization, for example, could be targeted through infected USB drives, e-mails and attachments that appear innocuous and genuine.

If their systems are not updated and protected, all it takes for an intruder to get into a PC and a network is for the user to click on a malicious attachment or link to a website loaded with malware.

Once a hacker takes control of one computer — sometimes, this can be even a network printer or other such device — he can take his time to learn what is happening in the network which the infected computer is connected to, and slowly find ways to penetrate other computers connected to the organization.

Sometimes, hackers get into well-protected organizations through third-party contractors who have dealings with them. Once inside, they usually keep a backdoor open to quietly install more harmful malware in more highly-guarded systems.

To damage a water control system, for example, a hacker could slowly take control of computer servers in the facility over several months. In the same way, a group targeting a power station could keep harvesting information on the facility over months before suddenly turning the power off when it comes the time to strike.
Key to any defense effort is actionable intelligence. Many cities already have cyber defenses set up to counter threats from external sources. At the same time, they have surveillance cameras ready to capture suspicious activity around key locations in a city.

The missing link is usually a glue, or fusion, to strengthen these two sources of intelligence. This means that a lead found from a server log, through digital forensics, can be followed up by physical surveillance such as city video feeds.

A lot of effort has been spent by organizations on checking networks for tell-tale signs of a cyber intrusion. These include looking for zombie computers “phoning home” to command and control servers operated by hackers, or suspicious information flow that is unusual between usually disconnected computers on a network.

At the same time, physical video surveillance lets the authorities see suspicious persons loitering near a sensitive location, such as a location housing critical infrastructure. These videos are invaluable in checking out potential threats that may appear right at the doorstep of a targeted facility.

Yet, these two types of intelligence have to be better combined to combat threats facing cities in the years ahead. They have to provide the authorities with timely and immediately actionable information that leads to the apprehending of suspects, whether they are based locally or abroad.

Clearly, it is crucial for various security agencies to work together in a time of crisis, especially in the face of an impending threat or right after a devastating attack.

From the time one agency finds out that a power generation facility is under attack to when the location of the suspected hackers is found, time is of the essence. Often, missing out on critical intelligence during the first hours after an attack enables the attackers to cover their tracks and melt into the background in cyberspace once again.
What makes the task of investigators more difficult is the usually cross-border nature of such threats. With perpetrators often launching such attacks from overseas, usually through zombie computers they have commandeered, they leave very little evidence for investigators to get hold of.

In these cases, the fusion of actionable intelligence is critical in preventing or reacting effectively to such attacks. As threats are becoming increasingly sophisticated with years of planning, espionage and social engineering before a final “payload” is released to great effect, defenses have to be no less coordinated.

Currently, the lack of such coordination is hampering responses to large-scale, sophisticated attacks. Cities will have to improve on such agency-to-agency coordination, especially through regular exercises and drills, to counter possible attacks in future. Cyber fusion is the solution.

The fusion of cyber and physical intelligence will provide a quantum leap to law enforcement and homeland security agencies seeking to quickly apprehend a suspect for an attack on a city’s critical infrastructure.

In the past, when they often had no clue where to look at and no identifiable suspect to search for, an investigation could take too painstakingly long for it to be effective.

However, with cyber fusion, investigators get the information they need — fast. The key is not just putting together a battery of technologies. It is making them work together seamlessly to provide human operators and decision makers a timely sense of what is happening in both cyber and physical realms.
City authorities have to expect attacks on critical infrastructure in future that could severely disrupt citizens’ lives or even threaten their safety.

If a power station is targeted, it could fail to deliver electricity to sectors in a city. Systems at the station could be paralyzed after being controlled and damaged by hackers who may have left few signs after launching their strike.

Once an attack is suspected, staff at the station would contact security agencies in charge of cyber defense. Key to confirming an attack is detecting any suspicious activities on cyber space.

Experienced investigators would usually not take long to find that several external computers have been communicating in an unusual manner to the victim systems. From here, they could find various IP addresses worth a closer look.

Smart hackers, of course, won’t leave such an easy trail for investigators to follow. This is where a cyber fusion center comes into play.

**Verifying an Attack**

Alerted of a possible attack, investigators would seek out the attack pattern of the advanced persistent threat, studying the tell-tale signs of an attack planned and executed remotely through other online computers, likely from a foreign country.

Once it is established that an attack is being mounted, the next thing would be to seek out the source of the attack, while preventing the attack from being carried out.

Here, a number of technologies assist investigators immensely.

Firstly, NEC’s expertise in Security Information and Event Management helps find the necessary data to understand a sequence of events that may have led to a cyber attack. By looking at the pattern of an attack, this better helps prevent as well as recover from it.

Secondly, NEC’s Malware Analysis provides clues to the malicious software that hackers may have used to create a backdoor entry to a network. It is important as well in detecting threats proactively, even if they originate from overseas.
Tracing The Attack

With this information sent to the police department, the city authorities can work with counterparts in the foreign country to track down the IP addresses of these computers. Not all countries are expected to be as fast or efficient in sharing such information, so it is crucial that an international police agency, such as INTERPOL, is involved to bridge and facilitate cross-border investigations.

Joining hands, investigators can look up log files to trace the suspected login accounts to servers used to control and coordinate the attack in the foreign country. From the malware binary, they can seek out any signatures or handles that may provide clues to the attack and its perpetrators.

Piecing together these clues enables investigators to identify the pattern of the attack, how the malware penetrated cyber defenses and the type of command and control as well as the IP address from which the attack was launched.

What is critical in this part of the scenario is Digital Forensics expertise to help investigators find out where hackers entered the system, how they executed the attack and where they may have originated from. Through examining the log files, this enables investigators to narrow down possible suspects and where to locate them.

At the same time, another technology in the form of Complex Event Processing assists in the investigation as well. With it, investigators can turn to data analytics to determine the relationships between events and patterns that should alert human operators and decision makers. This helps to find the “needle in the haystack” when searching for useful intelligence, such as how a hacker may have attacked a system.

At this critical time, NEC’s technologies in Inter-agency M2M interfacing systems help multiple agencies to tap on the same sources of information, say, a video feed, but with each agency given the different levels of access. This multiplies the resources available to track down an attacker.

Finding The Suspects

With the amount of information shared online today, pictures of a suspect may even be found on public networks. He may also be boasting about his latest exploits online.

NEC’s Cyber Information Surveillance uses the vast database of information online to locate useful intelligence on cyber space that may provide clues to a group of attackers. Tapping on available information on the Internet, this is useful in tracking down groups that have executed an attack, or are about to strike.

Using Facial Recognition technology, it may even be possible that suspects can be identified through a known database of videos and pictures from a police database.

What’s key here is to have clearly usable videos for analysis. NEC’s Video Enhancement technology helps improve the quality of video surveillance footage for investigators to seek out suspects if they are captured by cameras in a city.

With the help of a smart video search of videos from a city’s surveillance cameras, a person of interest could be traced physically. Where he was last spotted could be a tell-tale sign of where he might be picked up for questioning as well.

This is where NEC’s particular expertise in Geo-Spatial Analytics comes into play. It provides real-time visuals that aid decision making. They include relevant areas of operation and critical information, including maps of ongoing operations or surveillance, to assist the authorities in nabbing the suspects.

In a nutshell, what a cyber fusion system would allow investigators to do includes:

- Inspection of logs of heterogeneous sources to determine the location of hackers
- View surveillance camera recordings to find possible suspects
- Search through known databases for possible sightings — virtual and physical — for suspects’ last known location
NEC has the key technologies to blend the physical and cyber data for government agencies to combat the new threats facing cities in the future.

Whether this is our world-leading facial recognition technology or advanced digital forensics expertise, we are able to bring together a cyber fusion strategy that provides better defense against tomorrow’s threats.

By combining the signals from computer networks and feeds from physical sensors such as cameras, our cyber fusion platform works like a sensory brain that offers greater insight into a fast developing situation.

Our complex event processing can detect an upcoming attack by identifying the patterns for one through data analytics. At the same time, using NEC’s security and information management technologies enable city authorities to proactively prevent an attack, or recover faster from a successful attack.

In the event that a hacker has successfully penetrated a system, NEC’s digital forensics provide investigators the capability to piece together a picture of what happened and to find traces left behind that may point to possible suspects or their locations.

Through our malware analysis, cities can better understand the nature of a threat and prevent similar occurrences in future. At the same time, NEC’s cyber surveillance helps find possible suspects through their actions online.

Through video enhancement and NEC’s renowned facial recognition technology, suspects can be more easily found through camera feeds in a city that a suspect may be located.

Finally, in an operation to apprehend a suspect, the geo-spatial analysis and inter-agency collaboration provided by NEC will prove invaluable in sharing information that makes decision making easier for city leaders.

NEC’s work has been recognized by global partners. In December 2012, NEC signed a three-year-agreement with INTERPOL to develop core elements of the Digital Crime Centre established at the Interpol Global Complex in Singapore. NEC will provide technical and human resources worth some EUR 76million to establish a Digital Forensic and Cyber-Fusion Centre at Interpol’s complex.
This lab will focus on identifying and test-bedding digital forensic technology and methodologies to help investigators better coordinate and conduct digital crime investigations.

While other security vendors specialize in one area of security, our solutions address the multi-faceted threats.

At NEC, we also have a wide range of solutions to help create a better, safer city. We have decades of experience working with governments, city planners and other public agencies in projects as varied as identification to public transport.

Besides the protection of critical installations and safeguarding of cyber infrastructure, our solutions include national identification, law enforcement, immigration, and emergency and disaster response.

While bringing together the latest cutting-edge technology, NEC's team also possesses the experience and expertise to deal with projects — both private and government — on municipal and international levels.

Find out more about cyber fusion from NEC today and how we can enable a safer city for citizens. E-mail us at safety@gsd.jp.nec.com

REFERENCES


2. Crashing The System

3. Hacking Gets Physical: Utilities At Risk For Cyber Attacks

4. Three Bills To Protect Critical Infrastructure From Cyber Attack Passed By House

5. Stuxnet, Gone Rogue, Hit Russian Nuke Plant, Space Station

6. Cyberattack On U.S. Infrastructure

7. ‘Trojan Horse’ Bug Lurking in Vital US Computers Since 2011

8. Low-risk ‘Worm’ Removed At Hacked South Korea Nuclear Operator
   http://www.reuters.com/article/2014/12/30/us-nuclear-southkorea-cybersecurity-idUSKBN0K80J620141230
Contributors:
Douglas Tang, Senior Director & Global Lead of Cyber Security, Global Safety Division, NEC Corporation
Woo Kang Wei (PhD), Technical Director of Inter-Agency Collaboration, Global Safety Division, NEC Corporation
Kwok-Yan Lam (PhD), Adjunct Professor, National University of Singapore

About NEC Global Safety Division
NEC Global Safety Division, a business division within NEC Corporation, spearheads the company’s public safety business globally. The Division is headquartered in Singapore and offers solutions in the following domains: Citizen Services & Immigration Control, Law Enforcement, Critical Infrastructure Management, Public Administration Services, Information Management, Emergency & Disaster Management and Inter-Agency Collaboration. Leveraging on its innovative solutions, the Division aims to help government and business make cities safer.

NEC Global Safety Division
Global headquarters: 2 Fusionopolis Way #07-01/02/03, Innovis, Singapore 138634
For enquiries, please contact safety@gsd.jp.nec.com

nec.com/safety

Orchestrating a brighter world

NEC brings together and integrates technology and expertise to create the ICT-enabled society of tomorrow. We collaborate closely with partners and customers around the world, orchestrating each project to ensure all its parts are fine-tuned to local needs.

Every day, our innovative solutions for society contribute to greater safety, security, efficiency and equality, and enable people to live brighter lives.

The information contained in this white paper is the proprietary and exclusive asset of NEC unless otherwise indicated. No part of this white paper, in whole or in part, may be reproduced, stored or transmitted without the prior written permission of NEC. Unauthorized use or disclosure may be considered unlawful. It is intended for information purposes only, and may not be incorporated into any binding contract. This white paper is current at the date of writing only and NEC will not be responsible for updating the reader of any future changes in circumstance which may affect the accuracy of the information contained in this white paper. Some of the ideas in the paper are aspirational, and NEC is working towards realizing these ideas in our vision of making cities safer.

Copyright © NEC Corporation 2015. All rights reserved. NEC and the NEC logo are registered trademarks of NEC Corporation.