



27th ANNUAL
FIRST BERLIN
CONFERENCE

14 - 19 JUNE 2015

**UNIFIED SECURITY:
IMPROVING THE FUTURE**



Working Towards the 2020 Tokyo Olympics *- The Current Situation in 2015*



Mariko Miya

Cyber Defense Institute, Inc.

miya@cyberdefense.jp

Agenda

1. Introduction
2. The current situation in Japan 2015
 - Analytics and general framework
 - New framework & new cybersecurity strategy
 - Government initiatives for Tokyo 2020
 - TOCOG
3. Next steps in preparing for 2020
 - Comparing London 2012 and Tokyo 2020
 - Other aspects that may affect the Games in 2020 and evidence
 - The changing threat landscape
4. Lessons learned
 - Lessons learned from research
 - A recent incident tells us we have to make change
5. Conclusion



1. Introduction

About Cyber Defense Institute

- Cyber Defense Institute, *Inc.*
- Based in Tokyo, Japan
- 30+ people
- What we do: incident response, penetration testing, digital forensics, malware analysis, training, cyber exercises, security research, cyber intelligence etc.
- Main clients: government and private sector (energy, nuclear, gas, financial institutions, telecom, web service providers (from e-commerce to games) etc.)



About me (Mariko Miya)

What do I do?

- Chief Security Analyst
- I travel, say hello to people, research, report

How are we involved in the Tokyo 2020 Games?

- I've been doing research on the past Olympics/ Paralympics and other major sports events since 2013
- Clients: government agencies and organizations directly involved with Tokyo Games



2. The current situation in Japan 2015

Cyber attacks in Japan

- According to NICT (National Institute of Information and Communications Technology):



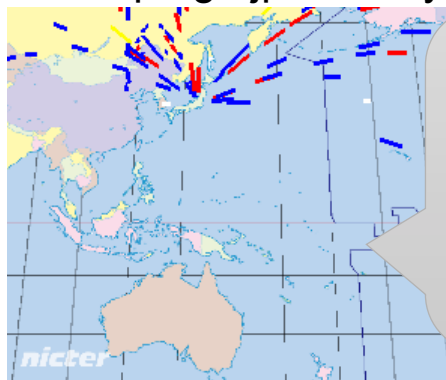
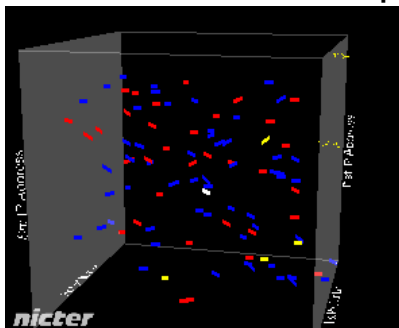
- In 2013, there were about 12.88 billion alerts
- In 2014, there were about 25.66 billion alerts related to cyber attacks targeting Japanese government agencies and private companies

✓ NICT analyzed data collected from 240,000 sensors

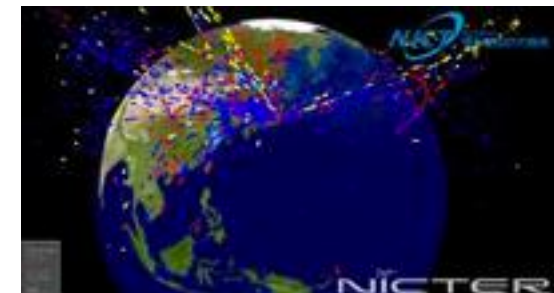


- IPA's report – 10 Major Security Threats in 2014

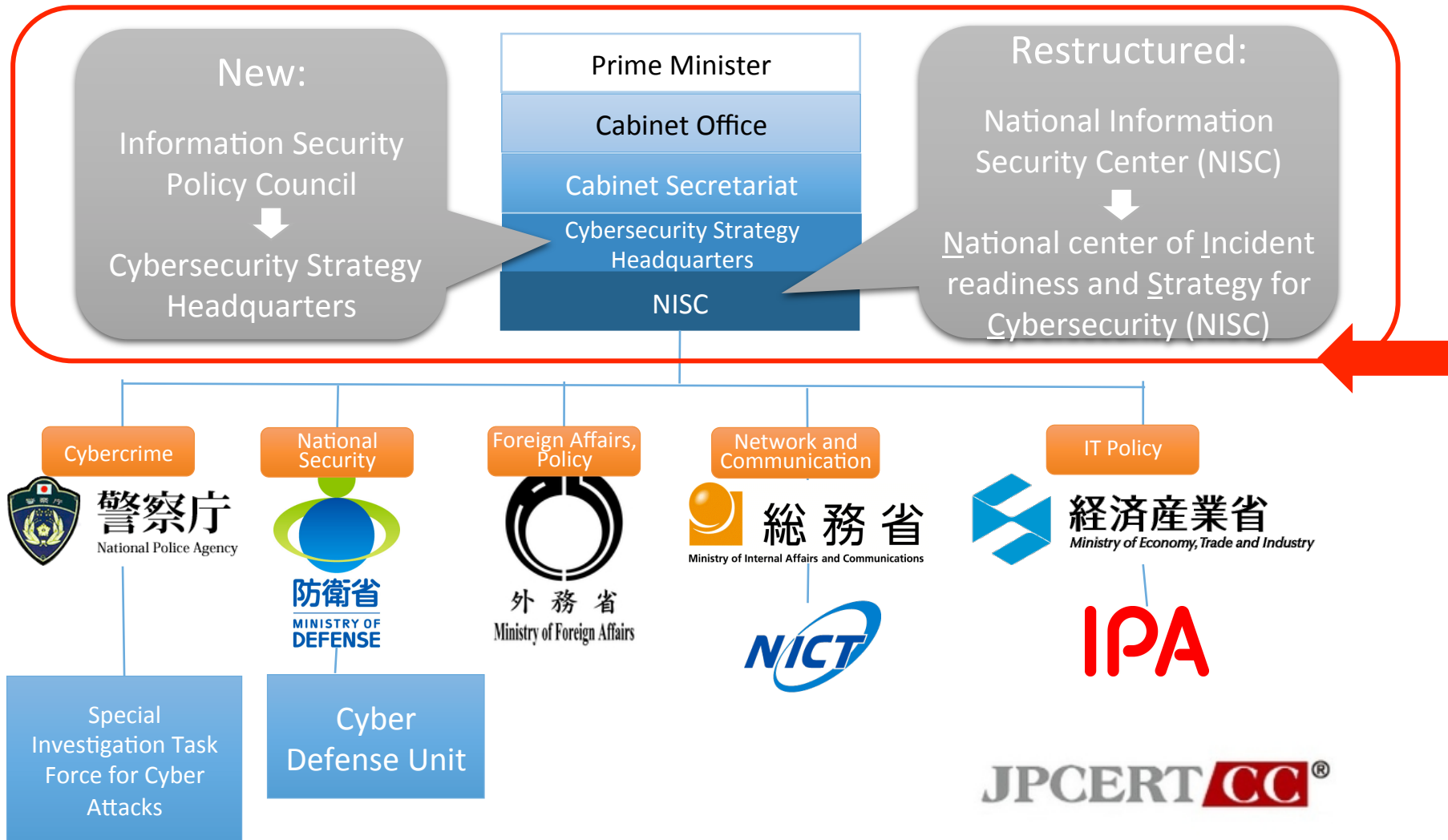
✓ http://www.ipa.go.jp/security/english/vuln/10threats2014_en.html



Part of the real-time live traffic collected from the NICTER (Network Incident analysis Center for Tactical Emergency Response) project can be seen on the website:
<http://www.nictcr.jp/>



Cyber Security Basic Law and “Government” in terms of cyber



A new Cyber Strategy (draft)*

- Will be finalized at the end of June
- This strategy looks beyond the 2020 Tokyo Games and lays out the direction of basic cyber policy for the next 3 years
- 5 basic principles:
 - Freedom of information
 - Rules and norms
 - Openness
 - Autonomy
 - Cooperation



http://www.kantei.go.jp/jp/97_abe/actions/201505/25cyber_security.html



Government Initiatives for 2020

- National Police Agency (NPA)
 - 2020 Olympic and Paralympic Tokyo Games Preparation Office
- Tokyo Metropolitan Police Department
 - “TMPD’s Visions to achieve the ‘World’s Safest City Tokyo’” and Action Plan
- Ministry of Internal Affairs and Communications
 - 2020 Olympic and Paralympic Tokyo Games etc. Ministry of Internal Affairs and Communications Preparation Headquarters
 - [Proposal for Cyber Security Policy Promotion](#)
- Ministry of Defense
 - Ministry of Defense and Self Defense Force 2020 Tokyo Olympic and Paralympic Games Special Action Committee
- Ministry of Land, Infrastructure, Transport and Tourism
 - Ministry of Land, Infrastructure, Transport and Tourism 2020 Olympic/Paralympic Tokyo Tokyo Games Preparation Committee



Japan's unique system

- Japan has a unique system of outsourcing
 - Government(s) and private sector are distantly related
 - <http://eaces.liuc.it/18242979200401/182429792004010105.pdf>



The European Journal of Comparative Economics
Vol. 1, n. 1, pp. 107-125
ISSN 1824-2979



**Outsourcing and Information Management.
A Comparative Analysis of France, Italy and Japan in
both Small and Large firms**

Alessandro Innocenti
University of Siena

Sandrine Labory
University of Ferrara



About TOCOG

- Tokyo Organizing Committee of the Olympic and Paralympic Games (TOCOG)
 - Launched Jan 24, 2014
 - Mission: Act as the center bringing together the JOC (Japan Olympic Committee), JPC (Japan Paralympic Committee), the Tokyo Metropolitan Government, other government and business community to ensure the successful delivery of the Tokyo 2020 Games
 - ✓ Technology Services Department – System development and operations
 - ✓ Security Department, Cyber Attack Response Section – in charge of running “[TOCOG-CSIRT](#)”
 - ✓ General Affairs Department – overall risk management



Next steps for TOCOG

- Coordinating with the **Olympic CERT** (To be established by Japanese governments)
 - **TOCOG CSIRT** – protecting Games infrastructure
 - **Olympic CERT** – intelligence gathering, analysis, incident response, coordination
- Enhancing cyber intelligence capabilities
 - Creating an intelligence database & system
- Cyber exercises and simulation
 - Idea : creating a simulated Olympic network for a hacking contest



TOCOG's Goals

- Protect not only the Games systems but secure all systems (government, critical infrastructure, companies, etc.)
= protecting Japan's reputation
- Training and securing cybersecurity experts
 - Key is sustainability – not only for Tokyo 2020 but to continue training and developing experts, and make needs more wide spread
= nurturing cybersecurity experts for the future

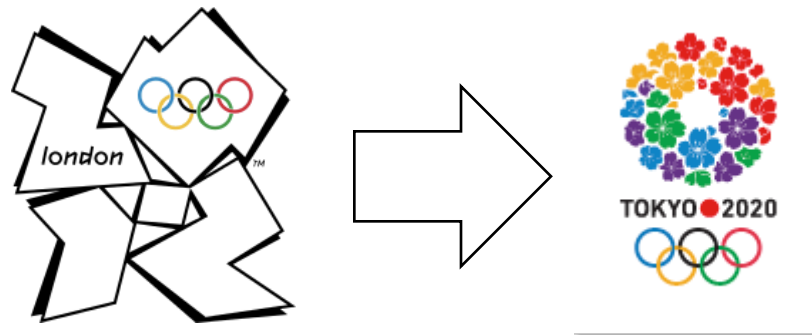


3. Next step in preparing for 2020

Comparing and analyzing from past experiences

Example: Major differences between London 2012 and Tokyo 2020

1. Communication (network) interception
2. Mobile devices and Wi-Fi traffic
3. Terrorist organizations and cyberspace
4. Impact of cyber attacks on businesses



Major differences between London 2012 and Tokyo 2020 - 1

1. Communication (network) interception



Intelligence agencies and law enforcement implemented communication (network) interception according to anti-terrorism laws (intelligence agencies and law enforcement have response capabilities against potential threats)



Law enforcement can only implement interception methods according to court order (response capabilities of law enforcement depend on detection, judgment and response capabilities of targeted organizations)



Major differences between London 2012 and Tokyo 2020 - 2

2. Mobile devices and Wi-Fi traffic



It was the transition phase of dramatic increase smartphone and tablet use, so the amount in increase of Wi-Fi traffic was within expectations



In addition to smartphones and tablet devices, rapid increase in the usage of cloud applications and wearable devices is expected, and it is extremely difficult to estimate the amount of traffic in 2020



Major differences between London 2012 and Tokyo 2020 - 3

3. Terrorist organizations and cyberspace



Illegal / criminal activities using cyberspace was somewhat limited



rapid increase in illegal / criminal activities using cyberspace is expected (an easily accessible environment is being continually being built at an accelerating pace)



Major differences between London 2012 and Tokyo 2020 - 4

4. Impact of cyber attacks on businesses



Legacy systems were intermixed, so business impact was limited



Fewer legacy systems, and it is likely that there will be dependency on extremely efficient or highly productive systems, so business impact will be extremely high



Case examples - 1

- Terrorism – ISIL supporters defaced several Japanese websites in March 2015
- Cyber incidents that may be triggered by geographical / historical / political issues



Case example – 2

Olympic sponsors as target

Example 1 – London 2012

- Atos was targeted as part of physical protest

Example 2 – Sochi 2014

- Anonymous Caucasus targeted Sochi Games related websites
- sochi-airport.com, Sberbank also targeted, websites service failure occurred several times



Example 3 – FIFA World Cup Brazil

- Anonymous - list of attack targets in #OpHackingCup
 - FIFA Partner (Adidas, CocaCola, Hyundai, KIA, Emirates Airlines)
 - FIFA Sponsors (Budweiser, Castrol, Johnson&Johnson, McDonalds etc.)
 - National supporters (FIFA.com, Apex-Brasil, Centauro, Garoto) etc.



Case examples – 3

Natural Disaster

- Example: targeted email attack taking advantage of people's interests right after the 3.11 East Japan Earthquake and Fukushima No.1 Nuclear Power Plant accident

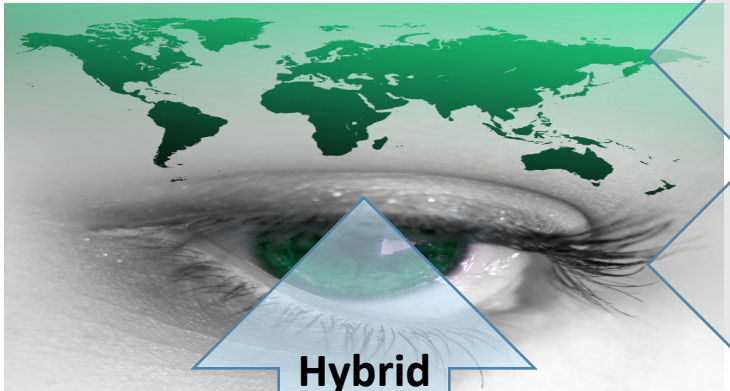
- Subject:
March 30th Condition
of Radiation
- Body: <blank>
- Attached file:
March 30th Condition
of Radiation.doc



Changing threat actors

Nation States

Individuals or Groups



"Patriot"
Hackers

Hybrid
Conflict

Failing/Failed
States
Radicalisation?

Proliferation/
Money Laundry



ANONYMOUS



Hybrid
Conflict

(Trans)national Terrorism

Slide by Mr. Wolfgang Roehrig, European Defense Agency



4. Lessons learned

Past – Present – Future

Collaboration and Information Sharing

- 2008 Beijing (Summer) Games
- 2010 Vancouver (Winter) Games
- 2012 London (Summer) Games
- 2014 FIFA World Cup Brazil
- 2014 Sochi (Winter) Games
- 2015 Summer - the First European Games in Baku, Azerbaijan (June 12-28 !)
- 2015 Summer - Pan Am & Parapan Am Games in Toronto, Canada (Pan Am: July 10-26, Parapan Am: August 7-15 !)
- 2016 Rio (Summer) Games
- 2018 FIFA World Cup Russia
- 2018 Pyeongchang (Winter) Games



Lessons learned and some ideas we got from our research

- Clearance and stress test for Gmes staff (i.e. BT during London Olympics)
- New methods for Accreditation
- Collaboration for cyber preparedness and response (i.e. cyber exercises with other well experienced organizations like experts from Cyber-EXE Poland exercises)
- Enhance collaboration for information sharing and strengthen analysis capabilities for every day intelligence collection



An example of a learned lesson: Don't use barcodes for Accreditation!



<http://mariskarichters.com/the-olympic-spirit-project/>
<http://www.bradleyherald.org/2014/02/21/icheers-from-olympic-sochi/>
<http://www.gettyimages.co.jp/detail/%E3%83%8B%E3%83%A5%E3%83%BC%E3%82%B9%E5%86%99%E7%9C%9F/mens-figure-skater-yuzuru-hanyu-of-japan-shows-his-%E3%83%8B%E3%83%A5%E3%83%BC%E3%82%B9%E5%86%99%E7%9C%9F/466739191>

Better options:

- Use smart chips instead
- Link with passport



A recent incident...



日本年金機構
Japan Pension Service

Japan Pension Service (JPS) data breach

- 1.25 million files containing personal information was leaked
 - 1.17 million items included 10 digit ID numbers in National Pension Plan and Employee's Pension Plan, names, birthdate
 - 52,000 items included 10 digit ID numbers, names, birthdate, address
 - 31,000 included ID numbers, names
- Method : targeted email attack

There's wonderful services, technology, products in the world, and no matter how much technology advances, there's no point if it's not operational for the users

= “user level” cybersecurity

= raising the level for *EVERYONE*



5. Conclusion

Conclusion




- More deep Cooperation and Collaboration
- Cyber security for ***EVERYONE*** (*we're all connected!*)
- We can work together to secure not only Tokyo 2020 but make a step towards



“Improving the Future”



A photograph of a sunset over a body of water. The sky is a gradient of yellow and orange, transitioning into a deep blue over the water. Concentric ripples are visible on the water's surface, reflecting the light from the sky. The overall mood is serene and peaceful.

Thank you!

Mariko Miya
miya@cyberdefense.jp

