Preventing & Mitigating Potential Threats at Large-Scale Events:

A look at past & future plans involving the Olympics & Super Bowl

13:30-14:30, Wednesday, 16 September 2015
The World Bank D.C. Headquarters, Washington DC
Introduction

• **Session Facilitator:** *Kazuo Noguchi*
  Senior Manager, Hitachi America, Ltd.

• **Andy Williams**
  *Cyber Envoy, UKTI Defence and Security Organisation, British Embassy (London Olympic 2012)*

• **Ko Ikai**
  *Counsellor, The National Center of Incident Readiness and Strategy for Cybersecurity (NISC), Cabinet Secretariat, Government of Japan (Tokyo Olympics)*

• **Michael Meglino**
  *Cybersecurity Portfolio Manager, Program Manager – Information Sharing Environment, Office of the Director of National Intelligence*
Session Overview

• Learn from past experiences and advance planning to for large-scale event such as Olympics and Super Bowl
• Success measure would be no security event - Smooth and joyful Olympic games or Super Bowl games
• 2012 London Olympics was successful - Under budget, no major cyber issues in public hard work as discipline
• NJ/NY Super Bowl at MetLife Stadium was large and continuously successful - originally panned for Olympics
Opening Questions

1. What have been the most important cybersecurity risks in past Olympics and Super Bowl?

2. What kinds of resources are available to address cybersecurity in large events like the Olympics?

3. How can cyber-threats be addressed in facilities automation systems?

4. What kinds of reputation risk and trust issues arise in global-scale events like the Olympics?
Discussion Points

- KSF and Prevention
- Large event planning and legacy
- Newly identified risks in cyber for large events
- Preparation for unknown
- Risk vs. Cost
- Human aspect vs. M2M in large event
- International collaboration
- Field service, public areas
- STIX/TAXII/CYBOX coverage, position, recommendation
- Other standards - NIEM, ISO, ITU, etc.
- Re-usability for other purposes
- Key takeaways for advanced and/or developing countries
Preventing & Mitigating Potential Threats at Large-Scale Events:

2012 Olympics
London

Andy Williams
UK Cyber Envoy
British Embassy Washington
London 2012 - The First Digital Games

+ BBC Sport broke all previous records with **55m** global browsers (35m in the UK)
+ London 2012 website **4.73 billion** web page views (109m unique users in Games time)
+ BT and Cisco provided the largest high-density Wi-Fi network in the World (around the Olympic Park)
+ Online video **106m** requests across all platforms (more than double of any previous event)
Threat and Risk

Reputational risk
- Scale / pressure to deliver
- Errors / things going wrong

Hostile threats
- Cyber crime
- Cyber espionage
- Cyber terrorism
- Cyber activism / ‘hacktivism’

Strategic risk assessment
- 23 strategic cyber risks identified
- Senior Risk Owners
Governance and Stakeholders

- Ministers (Olympic Ministers, Home Secretary, Prime Minister, Mayor)
- Government Olympic Executive – overall lead, assurance & finance
- Home Office – security lead
- Senior ICT leaders group (Director & Chief Information Officer level)
- Information assurance and cyber security co-ordination group

- Other key cyber stakeholders
- Technology suppliers/ utilities/ transport
- Managed service provider forum (CPNI)
- TISAC – Telecommunication industry security advisory forum
- Broadcasters (national, international and Olympic) – international broadcast centre/main broadcast centre
- Olympic sponsors
- Public / spectators / overseas visitors
London 2012 Information Assurance Strategy/Program

Command, Control and Comms (C3) architecture / testing & exercising

London 2012 Information Assurance

- Organisations
- Operations Centres
- Venues
- Critical Supporting systems

Information assurance criteria

- Accreditation standards (ISO 27001 etc)
- Information security awareness
- Protective and defensive monitoring
- Personnel security (security clearance/ID checks)
- Technical maintenance (patching/penetration testing etc)
- Fall back/resilience/business continuity management
Command, Control and Communications (c3)
Olympic Cyber Co-ordination Team

UK Joint team brought together establishing the first dedicated ‘Olympic CERT’
Critical systems

- Surveyed 450 Olympic specific and supporting systems
- Identified 40 critical systems
- Criteria:
  - risk to public safety
  - impact on sporting event
  - quality and ability to broadcast
  - impact on spectator experience
  - damage to reputation of UK
- Multi layered assurance (questionnaires, visits, inspections, games readiness statements)
- Non-critical systems
Testing and Exercising

+ ‘FLAMING TORCH’
  - programme of table top exercises
+ ‘BENDING METAL’
  - specific cyber / CERT testing
+ Command post exercises
  - fully integrated testing
+ LIVE EX (exercise)
+ Torch relay
+ Technical rehearsals – test events
What we saw

+ London 2.35 billion security system messages logged (Beijing reportedly 12 billion security events)
+ Blocked 200 million malicious connection requests, 11,000 per second in one distributed denial-of-service attack.
+ Olympic website – 493,000 peak concurrent users
+ Olympic cyber coordination team and technology operations centre – 50 incidents which required action each
+ Virus during construction (Conflicker)
+ DOS & DDOS (Olympic Website, government sites, other sites)
+ Theft of cable and high value components
+ Spoof websites/e-mail scams (tickets, accommodation and merchandise)
+ 200 arrests under “PODIUM” (approx 100 related to online crime)
+ Laptop thefts
+ Evacuation of technology operations centre
+ Flooding - evacuation of police control centre
+ Two national level cyber response incidents - Opening ceremony – national level response (COBR)
Lessons Learned

What we got right

+ Testing & exercising
+ C3 / Olympic CERT
+ Blend between government and industry
+ Spectrum allocation
+ Right technology partners (BT, Atos, Cisco etc.)
+ Broadcasting (digital) is a critical
+ Utilities – generally a low level threat, but potentially very high impact – manual resilience / C3

What we learned

+ ICT is very expensive, particularly to retrofit (get it right first time)
+ Build cyber-security from very beginning, preferably into contracts
+ Build relationships with commercial providers and government early
+ Co-ordination across many different systems and sectors is hard but crucial (information assurance and cyber security coordination group / senior ICT group / Olympic cyber coordination team)
Could We Have Done it Better?

+ Started earlier
+ Built information assurance into contracts at an earlier stage
+ Establish senior governance and leadership in place earlier
+ Better/earlier engagement with Ministers on cyber issues
+ Appointed an independent overarching partner to assure cyber security
+ Heavily reliant on technology sponsors (inevitable)
+ If a national CERT in place, would not have needed to create one
+ Considered cyber issues in terms of insurance (e.g. loss of broadcast, or other major services)
+ Online ticketing – some issues with website (almost inevitable)
+ **Delivered the most connected Games ever**
Evolving Global Cyber Landscape & Future Challenges

- Increase in Digital Connectivity
- Global Cyber Threat Landscape
  - Rising geopolitical instability
  - Increased national attacks
  - Exponential growth in malware tools
  - Rising threat of physical CNI attacks

- Source: Strategy Analytics, October 2014
Preparation for Cybersecurity in Tokyo 2020 Olympic/Paralympic Games

September 16, 2015

Ko IKAI
National center of Incident readiness and Strategy for Cybersecurity(NISC)
Cabinet Secretariat, Government of Japan
I am the only panelist to talk about the upcoming event in this panel.

- I have less lessons learned from event’s result.

What I can share here is the current situation and my personal worries.

- Everything can change during 5 years later.
  ex. IT utilization, platform, vulnerability, attack methodology and so on.
- A lot of things planned for the Olympic/Paralympic Games is still on blueprint.
- Many organizations have been already involved, and cooperation and coordination among them is crucial.
  ...

NOTICE: All comments and opinions in this presentation are my personal ones, NOT official ones of Government of Japan.
Outline of Cybersecurity Policy in Japan

**Cabinet**
- Submission of "Cybersecurity Strategy" to a Cabinet meeting for approval

**The Prime Minister**
- Offers opinions on direction and supervision of ministries

**IT Strategic HQs**
- views on CSS
- Close cooperation on important issues
- Formulates the priority plan for establishing an Advanced Information and Telecommunications Network Society (AITNS) and its implementation.
- In addition, deliberates to plan important policies for establishing AITNS and its implementation.
- Some of these responsibilities will be entrusted to the Government CIO.

**Cybersecurity Strategic Headquarters**
- Formulates the "Cybersecurity Strategy" (CSS) and its implementation
- Formulates common standards for information security measures for national administrative organs and incorporated administrative agencies. Evaluate (including audit) and promote the implementation of such measures
- Evaluate the measures taken by national administrative organs in the event of significant cybersecurity incidents (including examinations for cause).
- In addition, perform the following functions:
  a. Research and deliberate on the planning of major cybersecurity policies;
  b. Formulate: inter-governmental implementation plan for such major policies; the national administrative organs’ expense budgeting plan for cybersecurity; guidelines on the implementation of such policies. Promote and evaluate these policies.
  c. Lead comprehensive coordination of cybersecurity policies.

**National Security Council**
- Close cooperation on important issues related to national security
- Flexible and substantial discussions on foreign and defense policies related to national security.
- Discussion on important issues regarding national defense: e.g., measures against an armed attack situation.
- Responsive discussions on important issues regarding measures against critical incidents; provide advice about what measures the Gov. should take.

**Local governments, Independent Administrative Agencies, National Universities, Corporations with special semi-governmental status, Relevant organizations, etc.**
- May request HQs cooperation (e.g. provision of information, etc.)
- Legislation required to enable the Cabinet Secretariat to appropriately address these functions.

**National Administrative Organizations, etc.**
- Makes an effort to satisfy the request
- Report collection about measures based on the recommendation
- Obligated to submit materials, etc.
- Recommendations

**Views on CSS**
- Obligated to submit materials, etc.
- Makes an effort to satisfy the request
- Report collection about measures based on the recommendation
- Recommendations

**Asks cooperation (e.g. necessary materials)**
- Local governments, Independent Administrative Agencies, National Universities, Corporations with special semi-governmental status, Relevant organizations, etc.
1. Understanding of Cyberspace
   - Blessings of Cyberspace: Generating infinite values, essential foundation for our socio-economic activity
   - “Hyper-connected and converged society” is coming
   - Cyber threats are becoming more serious and being perceived as national security matters

2. Objective
   - Develop and advance free, fair, and secure cyberspace subsequently contribute to:
     1) Socio-economic vitalization  2) Safe and secure society  3) International Peace and stability, National security

3. Principle
   - 1. Free Flow of Information
   - 2. Rule of Law
   - 3. Openness
   - 4. Self-governance
   - 5. Cooperation among Multi Stakeholders

4. Policy Measure
   - 1) Socio-Economic Vitalize and Sustainable Development
     - From Cost to Investment
       - Creating Secure IoT System
         New industry creation by safe IoT
       - Promoting Management with cybersecurity mindset
         Awareness raising of senior executives
       - Improving Business Environment
         Promoting cybersecurity business
   - 2) Realizing a Safe and Secure Society for the People
     - Foundation for 2020, further
       - Protecting People and Society
         Enhancing capability and countermeasure
       - Protecting CII
         Enhancing information sharing public with private
       - Protecting Governmental Agencies
         Strengthening defense and management audit
   - 3) Peace and Stability of International Community and Japan’s National Security
     - Proactive contribution to peace in cyberspace
       - Ensure Japan’s National Security
         Improving Cyber capabilities
       - International Peace and Stability
         Rule of law in cyberspace, confidence building
       - International Partnership
         Cooperation in a wide range of area

5. Organization
   - Enhancement cooperation with public and private sector, Institution building toward the Tokyo Olympic and Paralympic Games in 2020
6. **Promotion and Implementation of Cybersecurity Strategy**

Moreover, it is an upmost necessity for Japan to work towards ensuring cybersecurity for the major international events, including the Tokyo 2020 Olympic and Paralympic Games, to the maximum extent feasible. Especially with regard to the Tokyo Olympic and Paralympic Games, based on a clear understanding of cybersecurity risks and challenges related to the Tokyo 2020 Olympic and Paralympic Games, the Government will accelerate the formulation process of the Tokyo 2020 Olympic and Paralympic CSIRT as a core organ responsible for: the accurate prevention and detection of cyber attacks against relevant entities involving the management and operation of the Olympic and Paralympic Games and other associated businesses as well as those against the services provided by relevant CII; and the sharing of information absolutely necessary for these stakeholders to take appropriate measures. The Government will take steady actions step by step to: build and maintain necessary organizations, facilities, and cooperative relationships; assure a pool of cybersecurity experts; and conduct comprehensive preparatory training based on the process taken for and during the 42nd G7 Summit in the Ise-Shima region in 2016 as well as the Rugby World Cup held in Japan in 2019. Capabilities developed through these measures will be utilized later for the sustainable enhancement of Japan’s cybersecurity.

…
Structure for Governmental Decision Making

The HQ for the Tokyo 2020 Olympic/Paralympic Games
Chair - Prime Minister
Member - all ministers

Liaison Conference of Ministries/Agencies
Chair - Deputy Chief Cabinet Secretary
Member - all vice-ministers

Security Committee
Chair – Deputy Chief Cabinet Secretary for Crisis
Co-chair – Secretary General of HQ for TOKYO2020, Assistant Chief Cabinet Secretary(interior),
Assistant Chief Cabinet Secretary(Crisis), Deputy Commissioner General of National Police Agency
Member – Director Generals of relevant ministries/agencies
Observer – Tokyo Metropolitan Government, Tokyo Metropolitan Police Department,
Tokyo Metropolitan Fire Department,
Tokyo Organising Committee of the Olympic and Paralympic Games
Secretariat – Cabinet Secretariat(including NISC)

Anti-Terrorism WT
Chair – Councillor, Cabinet Secretariat(Crisis, Interior)
Co-chair – Councillor, Cabinet Secretariat(Tokyo2020),
Councillor, NPA(Security)
Member – Directors of relevant ministries/Agencies
Secretariat – Cabinet Secretariat(Crisis, Interior)

Cybersecurity WT
Chair – Councillor, Cabinet Secretariat(NISC)
Co-Chair – Councillor, Cabinet Secretariat(Tokyo2020)
Councillor, NPA(Security)
Member – Directors of relevant ministries/agencies
Secretariat - NISC
## Timeline for Tokyo2020 (draft)

<table>
<thead>
<tr>
<th>Risk Assessment</th>
<th>Government Tokyo 2020 CSIRT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>▲ Identify critical services involved in the management of the Game.</td>
<td>▲ Determine the role of Government CSIRT</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>▲ Create a procedure for CII owners to conduct self-assessments of cybersecurity risks properly.</td>
<td>▲ Implementation of measures based on the result</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Fiscal Year in Japan starts on April 1st.
○ **Risk Assessment**
  - Identify critical services involved in the management of the Game.
  - Create a procedure for CII owners to conduct self-assessments of cybersecurity risks properly.

○ **Preparation for Government Tokyo2020 CSIRT**
  - Determine the role of the Government Tokyo2020 CSIRT
  - Determine staff, equipment, physical location for the CSIRT
    - Staffing during the Games
    - Supporting system for collecting and sharing information
    - Location --- Relations with NISC, OPIC, etc.
  - Allocate roles among entities concerned
  - Conduct comprehensive preparatory training

○ **Others**
  - Secure proper experts
  - Build relationships of trust with entities concerned.
    (Build face-to-face relationships)
  - Increased cybersecurity risks as byproducts of development of utilization of IT in various areas.
Thank you for your attention!

... and any your helps and advices are absolutely welcome.

Ko IKAI
(ko.ikai@cas.go.jp)
National center of Incident readiness and Strategy for Cybersecurity(NISC)
Cabinet Secretariat, Government of Japan
Michael Meglino

Cybersecurity Portfolio Manager
Program Manager – Information Sharing Environment
Office of the Director of National Intelligence
Questions?