

# Cyber Green

# Improving Cyber Health through Measurement and Mitigation

Yurie Ito

Director

JPCERT Coordination Center

# CYBER GREEN



Question: Would you build your national critical systems and cybersecurity measures on;

A: global internet ecosystems being Infected, vulnerable, and with high ratio of malicious traffic

B: global internet ecosystems being cleaned, patched, and with less malicious traffic

# Background / Motivation

---

- Increasing dominance of cyber in communications, business, utilities
- Cyber risks continue to increase
- Fundamental to success will be the ability to measure risks to motivate action and to get actionable information to those who can act
  - This will require increased efficiency of data sharing
- Transparency into the sources and presence of cyber risk necessary to improve the ecosystem

# Applying Public Healthcare model to Cyber space

Presence of  
Malware /  
Botnets  
Infection

**Incidents;**

Patients disease  
counts  
e.g. Malaria Patients  
counts

Number of  
Incidents

OS Update, server  
misconfigurations,  
Education...

**risks**

**Threat vector;**

Amount of swamp  
water / mosquitos  
counts

**Conditions;**

Number of Obesity,  
smokers, famine  
level



# Applying Root-Cause Analysis to Internet Health

Symptom	Cause	Root Cause
Malaria	Mosquito (transmission vector)	Swamps (mosquito breeding grounds)
DDoS	Amplifiers	Misconfigured servers
		Lack of access control lists at the application layer
		Source IP spoofing is possible
	Bots	Lack of patches hosts
		Misconfigured servers
		No AV on endpoints

# Introduction: The Cyber Green & Its Mission

---

- **What is the Cyber Green?**
  - **Cyber Green core focus** is on tapping the collaborative potential of stakeholders in cyberspace through promoting the concept of “**cyber health.**”
- **How will Cyber Green Accomplish its Mission**
  - Cyber Green will establishing a reliable platform for generating cross-comparable statistics and information sharing mechanisms to enabling operational cyber remediation efforts, and providing insight into systemic risk conditions in the cyber ecosystem.

# Defining Cyber Health

---

- **“Cyber Health” is defined as, “a condition of cyber systems and networks that are not only free from infection from malware and botnets but also contributes more broadly to the overall trust and usability of the cyberspace for the well-being of all.”**
- This definition helps to clarify what a healthy cyber ecosystem is, and will provide future Cyber Green stakeholders a consistent definition that will enable effective participation.

Yurie Ito, “Managing Global Cyber Health and Security through Risk Reduction.” July 18, 2011.

# Key Internet Health Risk Indicators

---

- Percent infected population
  - Bots membership via sinkholes
  - Bin by specific botnet... etc
- Percent vulnerability
  - Specific vulnerabilities client side / Server side
  - Detected misconfigurations .... etc
- Percent malicious traffic
  - Spam, DDoS, attack, ....etc
  - Realized events, wasted capacity

Goal is to drive these values to 0

# Data Sources

---

- Third party risk condition data
- Reliable, global data sources
- Look for high confidence data
- Accept redistribution restrictions
- Free of any fees
- Import regularly (daily, etc) measurement into the system

# Cross-Comparable Statistics

Cyber Green will make available high-confidence, cross-comparable, and actionable information to stakeholders.

Cybergreen Metrics Risks Login

## Statistics

No single value can adequately capture the health levels of the Internet, it is a concept with a number of different dimensions. However, a combination of values can reveal the status of the Internet per quarter. Looking at the WHO website, their "Data and Statistics" page reveals three key indicators about global health and the effect of actions and policy on public health and safety. Cyber Green's goals are similar, and we should be able to distill cyber health into a handful of key metrics that reveal the impact of investment efforts and the potential for major incidents.

### 3%

of internet traffic is attack traffic.

In 2008, Arbor Networks suggested that approximately 2-3% of Internet traffic was attack traffic; in August, 2014, Senderbase shows that approximately 14% of mail is legitimate compared to 85% that is spam. This metric over time should reveal the balance between wanted and unwanted (spam, attack, etc) traffic.

### 10%

of the internet population is infected with malware

This can include the fraction of websites that are being abused for attack traffic and botnet infection rate estimates. This metric over time should reveal the effect of efforts to combat infections.

### 40%

of the internet population is highly vulnerable and considered a risk to others

This can include the fraction of websites that are being abused for attack traffic and botnet infection rate estimates. This metric over time should reveal the effect of efforts to combat infections.

Last 7 Days



# Counting Strategy

---

- By unique IP seen in a 24 hour window
  - Commonly done
  - Admit problem can't be solved (yet)
- Look for trend lines
- Normalize using regular means

# Data Normalization

---

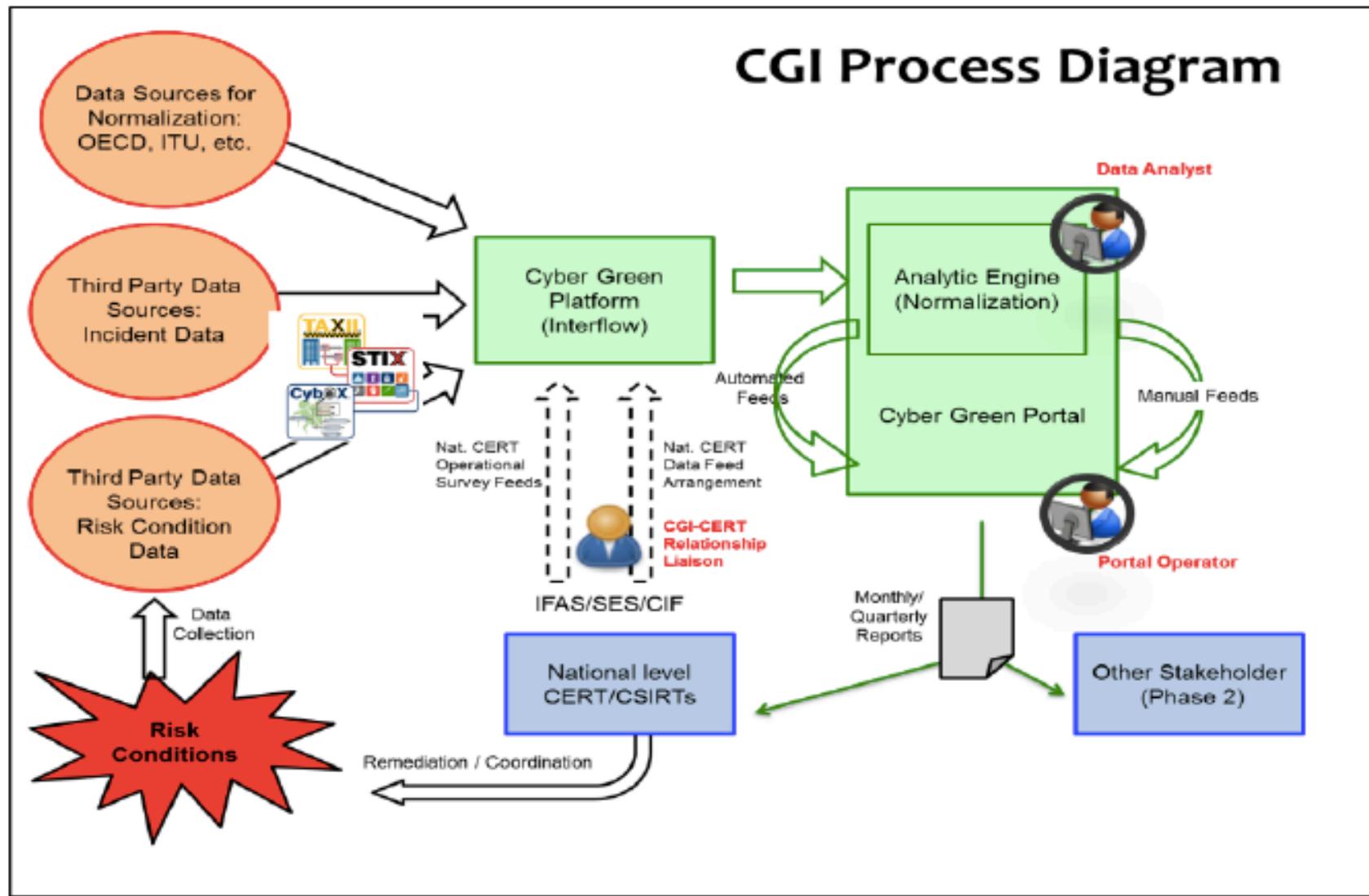
- Permits comparison across time
- Permits comparison across space
- By IP address (IPv4, IPv6) – ARIN, etc
- By population – global sources
- By Internet-connected population – OECD
- By Internet subscriptions – ITU
- By website count – internal data
- By Internet connected device – *unknown*

# Correlations to Look For

---

- By ICT budget – in progress from OECD
- By pirated software rates – from BSA
- By CERT bulletins released – internal data

# Planned activities and Goals for 2014



# Key stakeholders

---

- The CERT community of organizations
- Organizations, both commercial and non-profit, that are sources of data relate to cyber risk
- Research organizations and individuals specifically focusing on measurement of cyber health and risk factors
- Advisors knowledgeable in organizational models, data gathering, analysis and measurement related to public health

# Expected impact

---

- Cyber Health and Environmental Norm
- Global approach and coordination
- Long term impact to improving the cyber space resiliency and health
- Capacity building
- Metrics - Common language to policy

# Join the Cyber Green Initiative!

## - Global internet healthiness initiative

---

- Cyber Green Training / Capacity Building
- Access;
  - Tools
  - Access to the Cyber Green platform
  - Get risk condition data
  - Remediation best practices to risk factors
  - Statistics report

---

# Towards the Safe, Clean and Reliable Internet Ecosystem



Yurie Ito

[global-cc@jpcert.or.jp](mailto:global-cc@jpcert.or.jp)