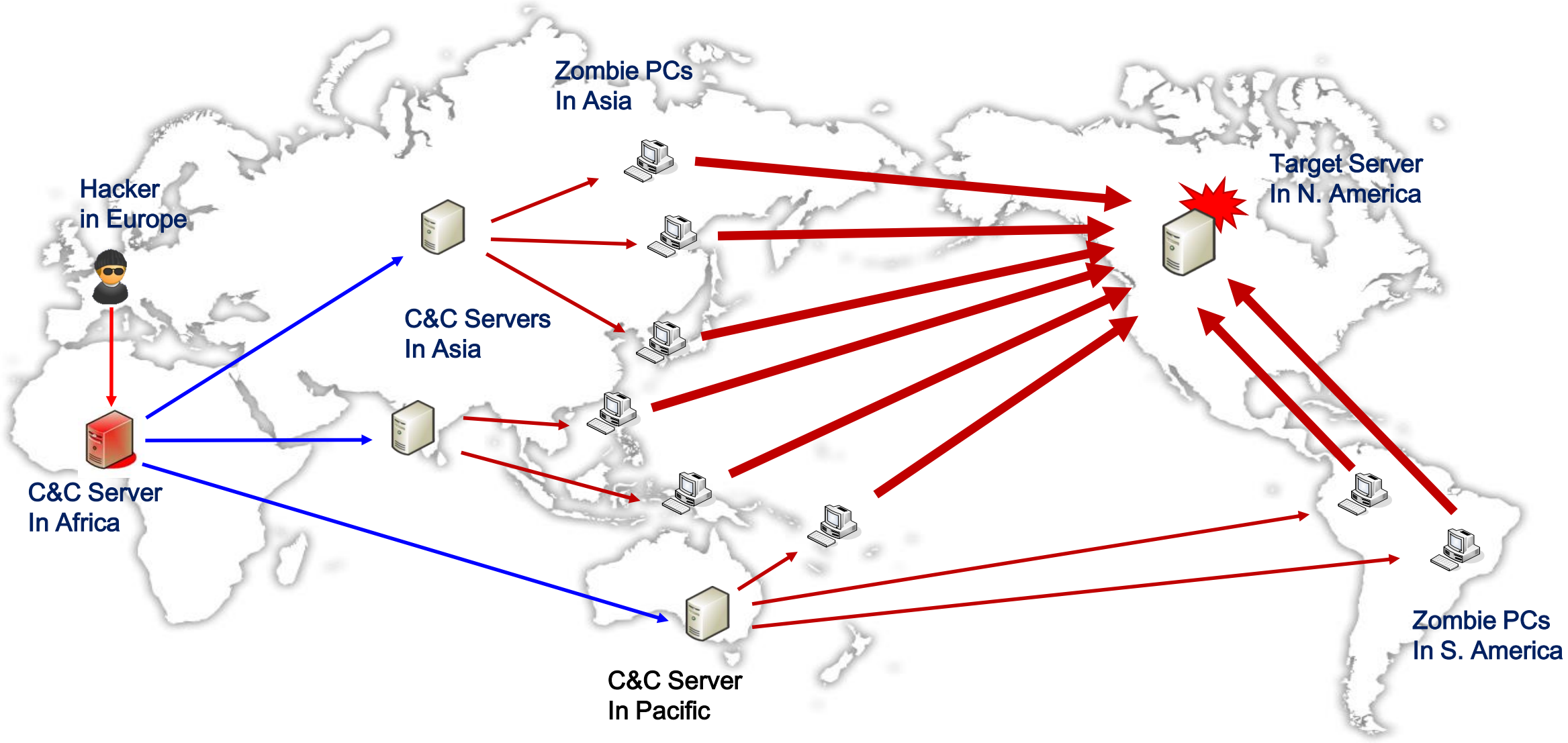
# CERT and International Cooperation

Hongsoon Jung

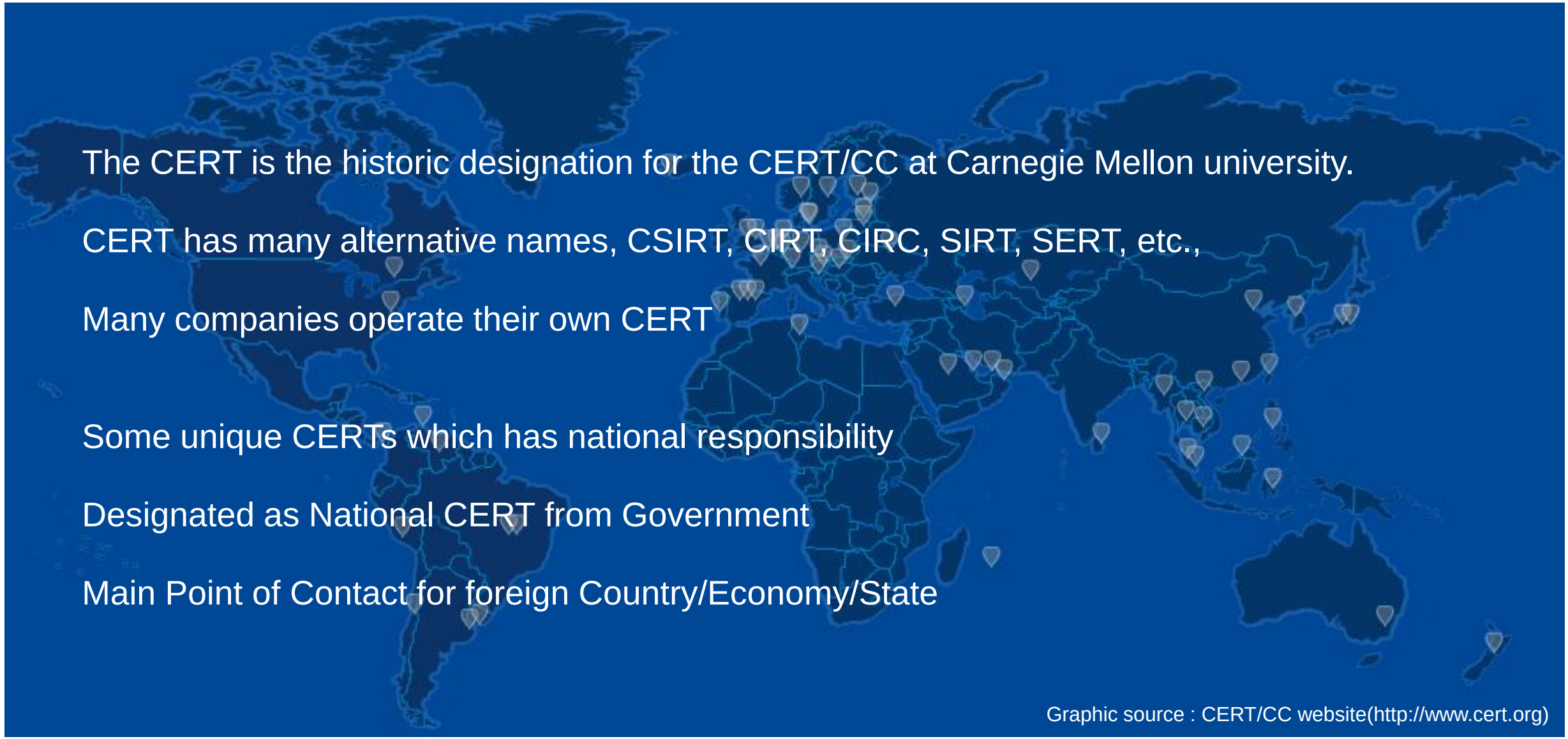
KISA 한국인터넷진흥원
Korea Internet & Security Agency

Collaboration is very important

# Simulated Cyber Attack Scenario



# CERTs and National CERTs



The CERT is the historic designation for the CERT/CC at Carnegie Mellon university.

CERT has many alternative names, CSIRT, CIRT, CIRC, SIRT, SERT, etc.,

Many companies operate their own CERT

Some unique CERTs which has national responsibility

Designated as National CERT from Government

Main Point of Contact for foreign Country/Economy/State

Graphic source : CERT/CC website(http://www.cert.org)

# CERT functions

CERT has functions that reactive and proactive service


Alert and warning

Incident handling

Vulnerability handling

Artifact Handling

Technology watch & Security related information dissemination

Security audits & Assessment

# National CERT functions

National CERT has broad functions

Serve as a trusted point of contact

Develop an infrastructure for coordinating response to computer security incidents within a country or economy

Develop a capability to support incident reporting across a broad spectrum of sectors within a nation’s borders

Conduct incident, vulnerability, and artifact analysis

Identify and maintain a list of CSIRT capabilities and points of contact within country or economy

Help organizations within the nation develop their own incident management capabilities

Source : Steps for Creating National CSIRTs(CERT/CC)

# Domestic CERT Collaboration in Korea case

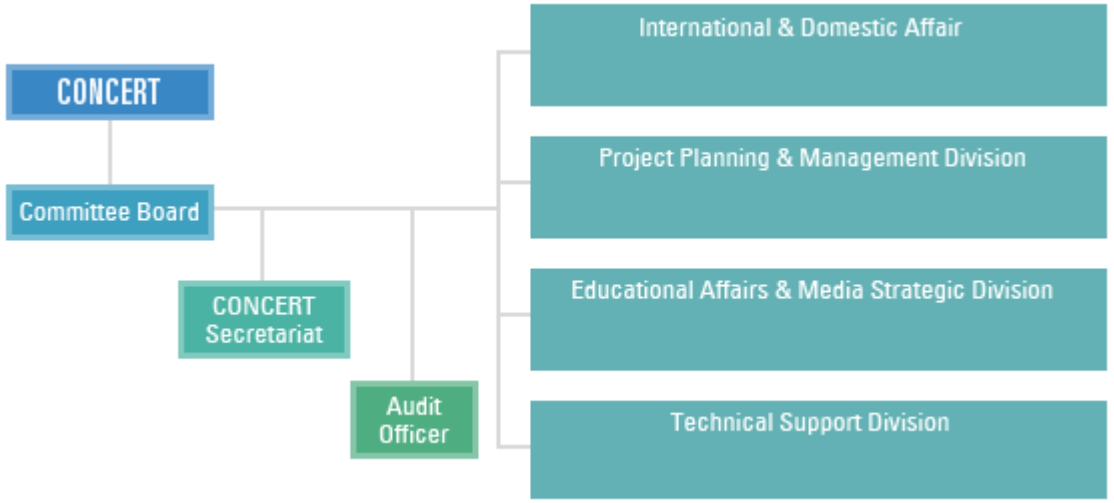
Concert – CONsortium of CERTs

Exchange and share information and

Cooperate with its partners on the issues

Of common interests such as cyber attacks

And security related incidents.




Started since 2005 as a non-profit organization

Host Annual Anti-Hacking workshop

Has 431 members

# CERT Collaboration

Bilateral Cooperation - Based on trust and official relationship(ex. MoU)

KrCERT/CC
Korea Internet Security Center

JPCERT CC®
Japan Computer Emergency Response Team Coordination Center

CNCERT/CC

Multilateral Cooperation - Through global/regional association or expert group or meeting

FIRST
Improving Security Together

APCERT
Asia Pacific Computer Emergency Response Team

National CSIRT Annual Meeting

# CERT Collaboration in AP region

Asia Pacific Computer Emergency Response Team(APCERT)

APCERT Annual General Meeting & Conference(2014 in Taiwan)

APCERT Drill(Every year)

Real time communication by Mailing List, WIKI, Online meeting


# Collaboration cases

March 20, 2013 - KrCERT/CC with CNCERT/CC and JPCERT/CC

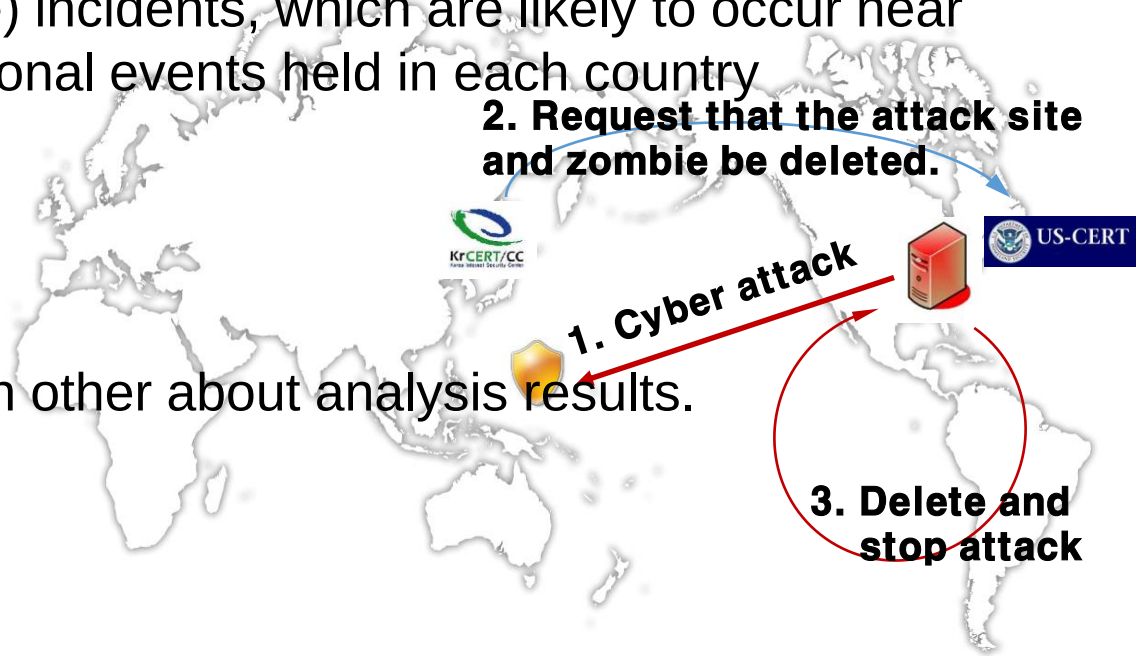
KrCERT/CC sent a request to CNCERT/CC and JPCERT/CC to check on the suspicious access to certain IP addresses hosted in both countries

March 1, August 15, every year – KrCERT/CC with JPCERT/CC

Joint threat monitoring has been conducted for (possible) incidents, which are likely to occur near the specific days of the year and/or big bilateral/international events held in each country

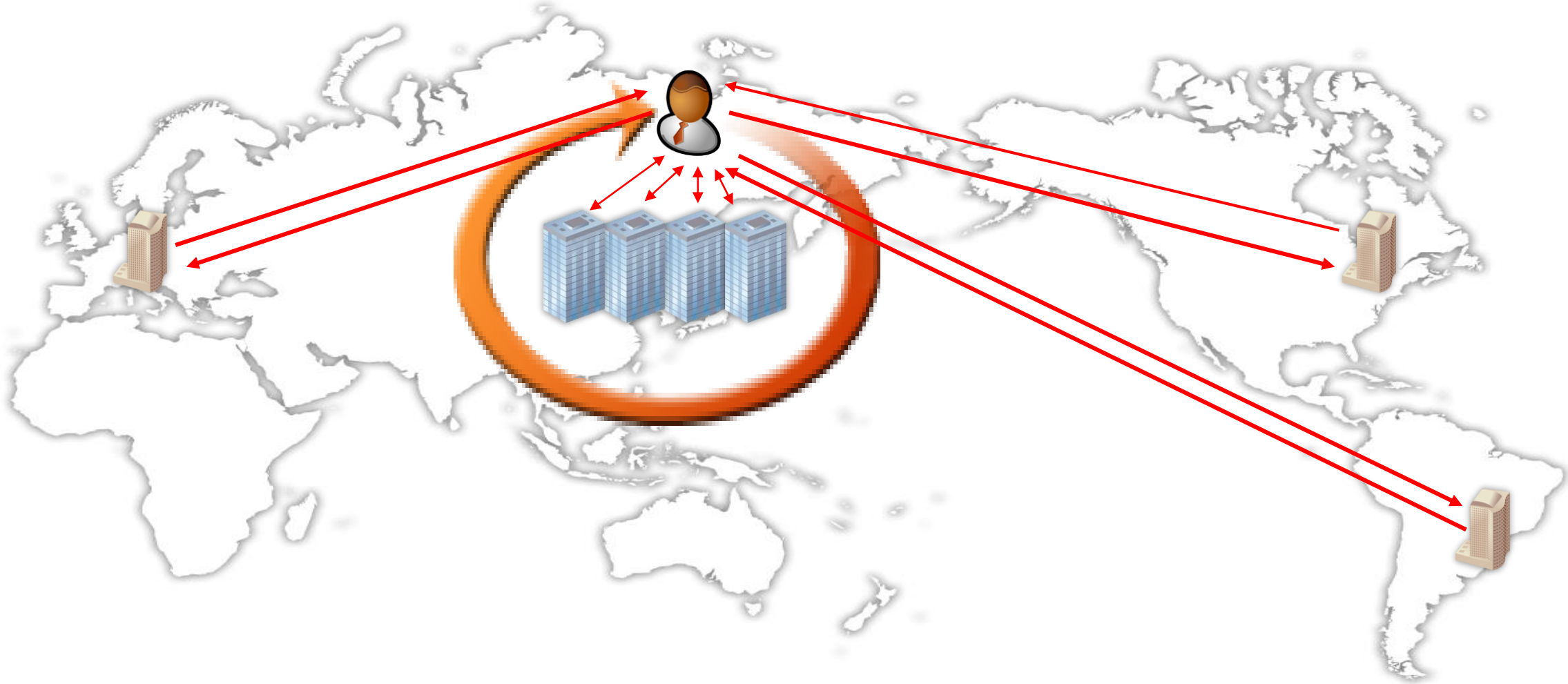
March 4, 2011 - KrCERT/CC with US-CERT

Shared sample malicious codes and consulted with each other about analysis results.
Then quickly deleted 51 sites and zombies in US



# Coordination

Coordination is the major role for National CERTs



# Cooperation and Trust building

Participation to the cybersecurity international conferences

Participation to the international associations

Host security training courses for giving a chance to meet each other

Signing MoU with other cybersecurity organizations



Thank you