Introduction of the NICTER project

Cybersecurity Laboratory
Cybersecurity Research Institute (CRI)
National Institute of Information and Communications Technology (NICT)

NICT

NICTER Network Incident Analysis Center for Tactical Emergency Response

Overview of the project NICTER

NICTER = Network Incident analysis Center for Tactical Emergency Response

Objective

Comprehensive analysis of security threats on the Internet
- What happens on the Internet?
- What is the root cause?

Approach

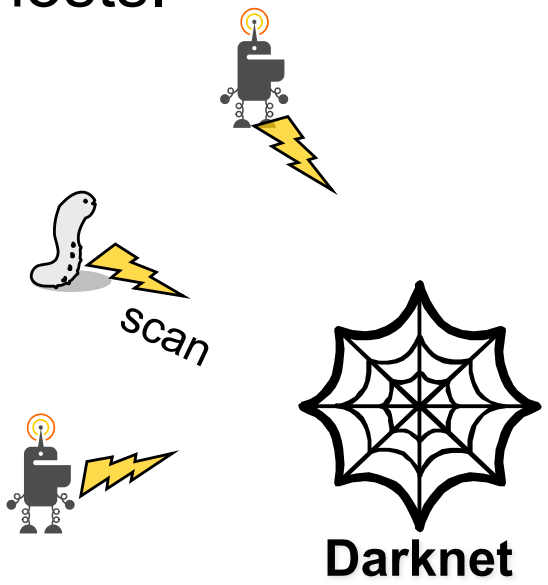
Network monitoring
+
Malware analysis

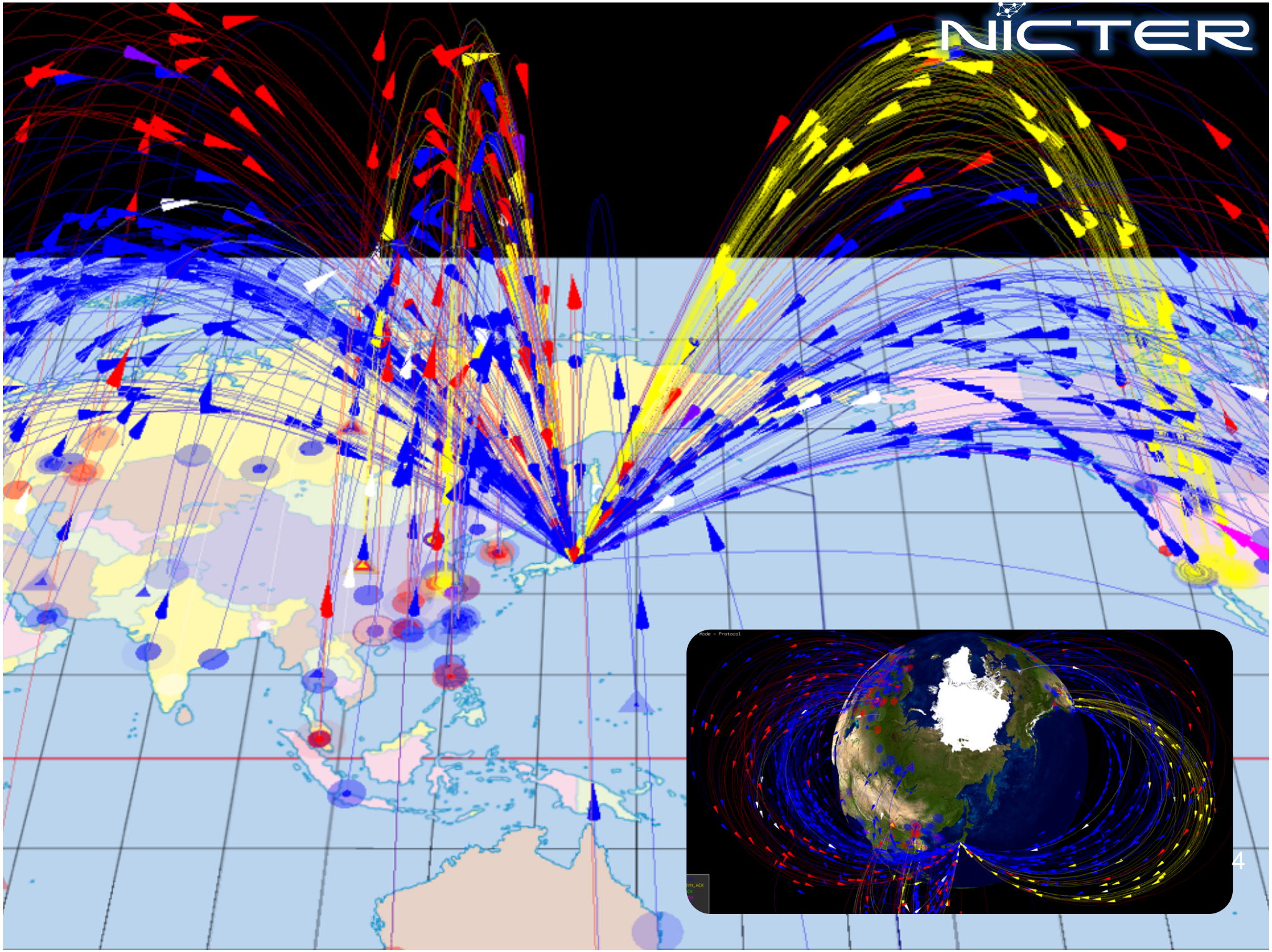
NICT

NICTER Network Incident Analysis Center for Tactical Emergency Response

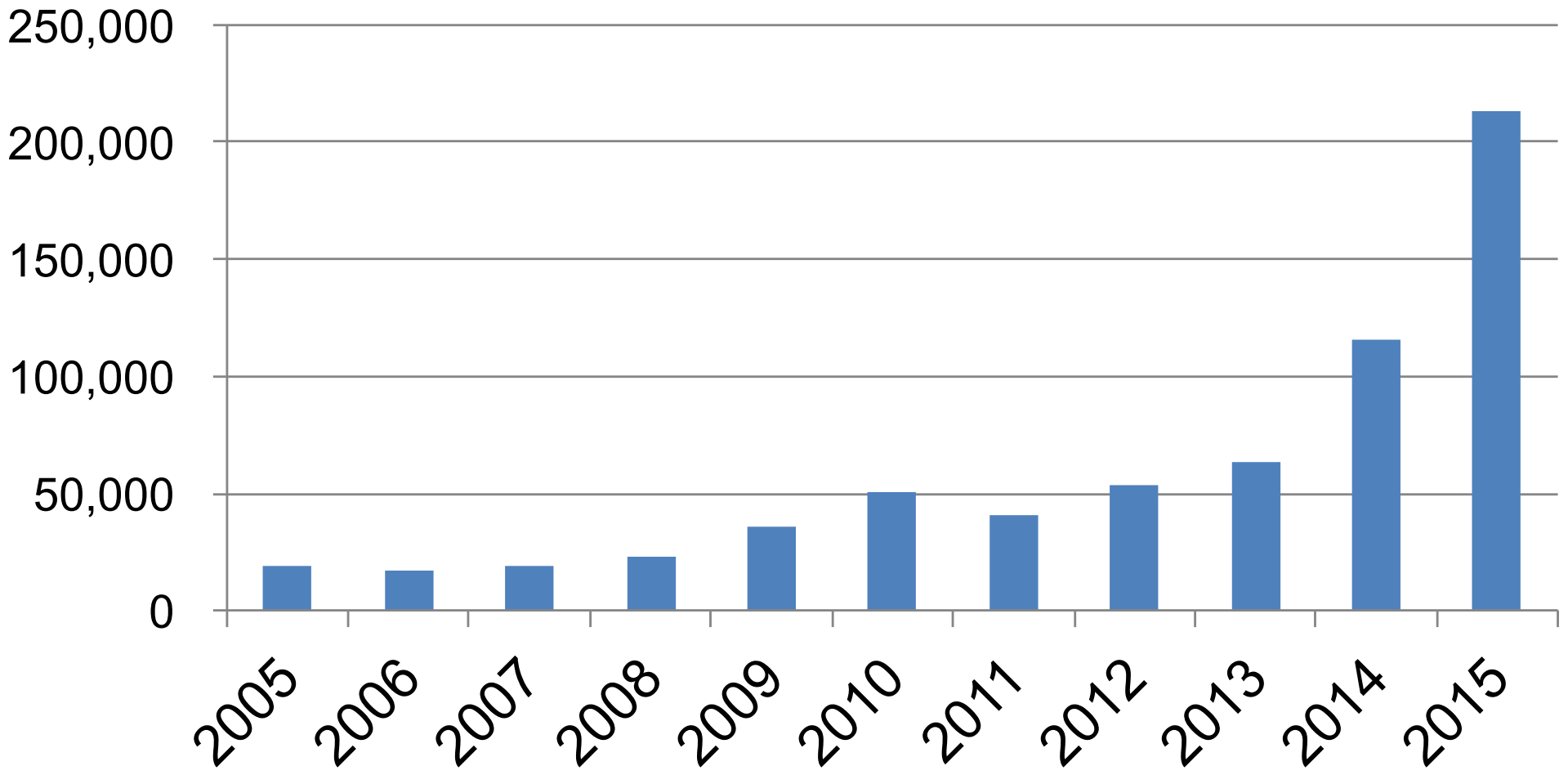
What is Darknet?

- Darknet: Unused IP addresses space
- In theory: any packets should NOT arrive at the darknet because they are not connected to any hosts.
- In fact: quite a few packets DO arrive!
- Packets arriving at the darknet are…
  - Scans by malwares
  - Backscatter (reflection of DDoS attack)
  - Mis configurations etc.
- Darknet traffic reflects global trend in malicious activities on the Internet.




NICTER

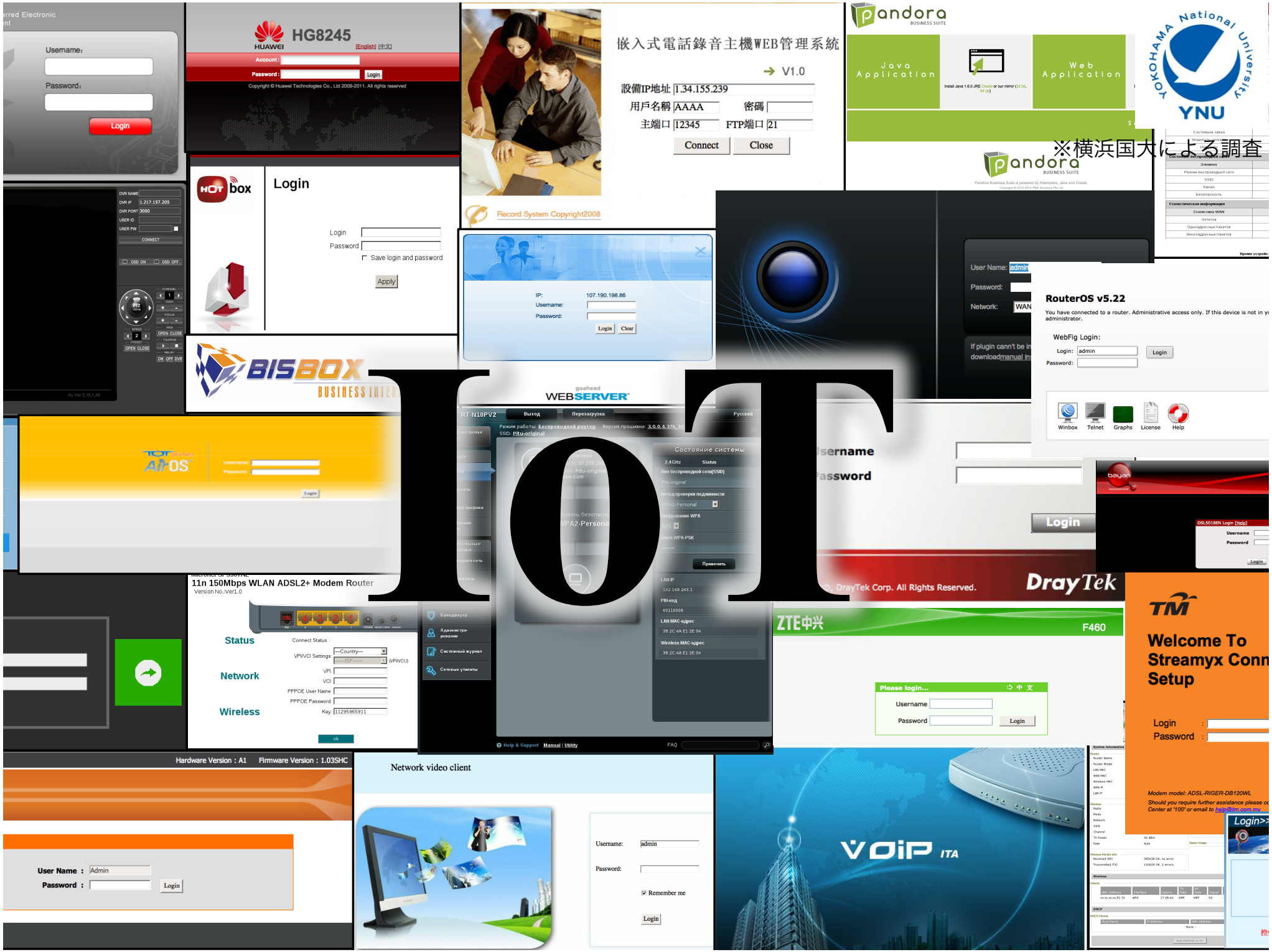
Yearly Stats of Darknet Traffic



Number of packets par 1 IP address per year

NICT National Institute of Information and Communications Technology

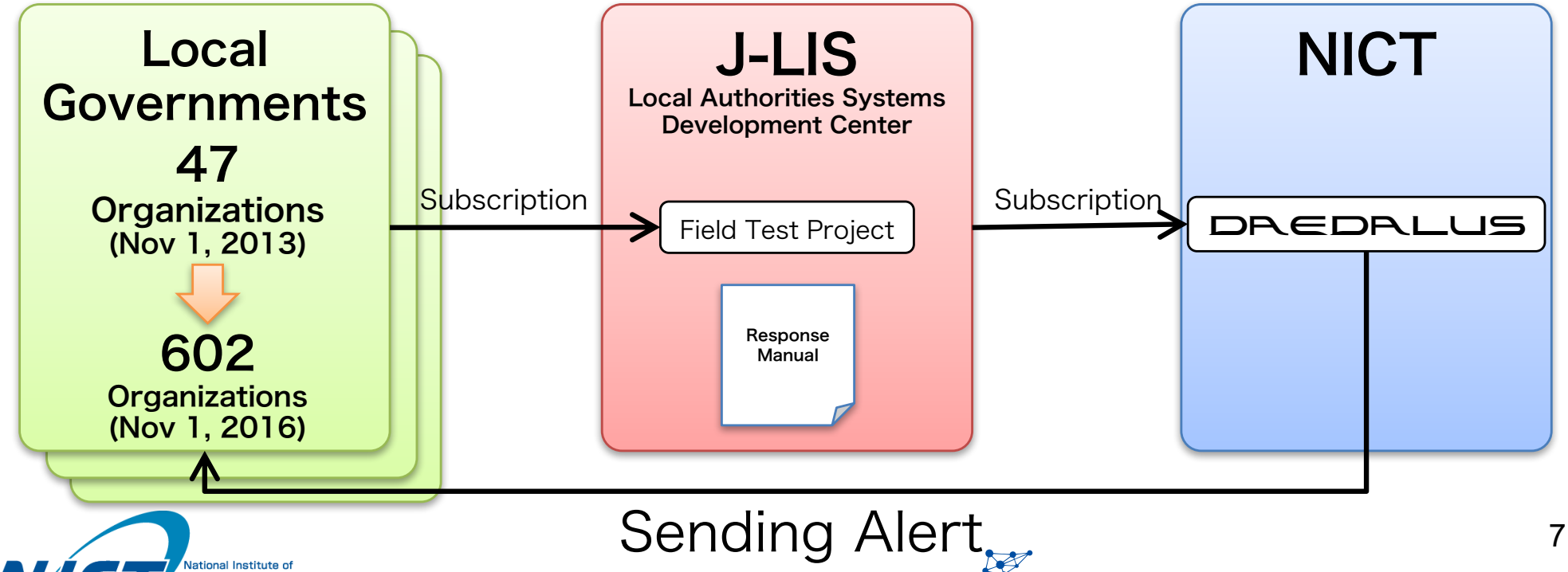
NICTER Network Incident Analysis Center for Tactical Emergency Response


HG8245
HUAWEI
Login
Password
嵌入式電話錄音主機WEB管理系統
V1.0
設備IP地址 1.34.155.239
用戶名稱 AAAA
密碼
主端口 12345
FTP端口 21
Connect
Close
pandora
BUSINESS SUITE
Java Application
Web Application
YOKOHAMA National University
YNU
※横浜国大による調査
Record System Copyright2008
hot box
Login
Apply
BISBOX
BUSINESS INTER
goahead
WEBSERVER
RouterOS v5.22
WebFig Login:
Winbox
Telnet
Graphs
License
Help
AirOS
11n 150Mbps WLAN ADSL2+ Modem Router
Status
Network
Wireless
DrayTek
ZTE中兴
F460
Please login...
Welcome To
Streamyx Conn
Setup
Hardware Version : A1
Firmware Version : 1.03SHC
User Name :
Admin
Network video client
VoIP ITA

DAEDALUS for Local Gov.

DAEDALUS has started to provide alerts to local governments in Japan (free of charge).

- ✓ From Nov. 1, 2013.
- ✓ Started with 47 local governments.

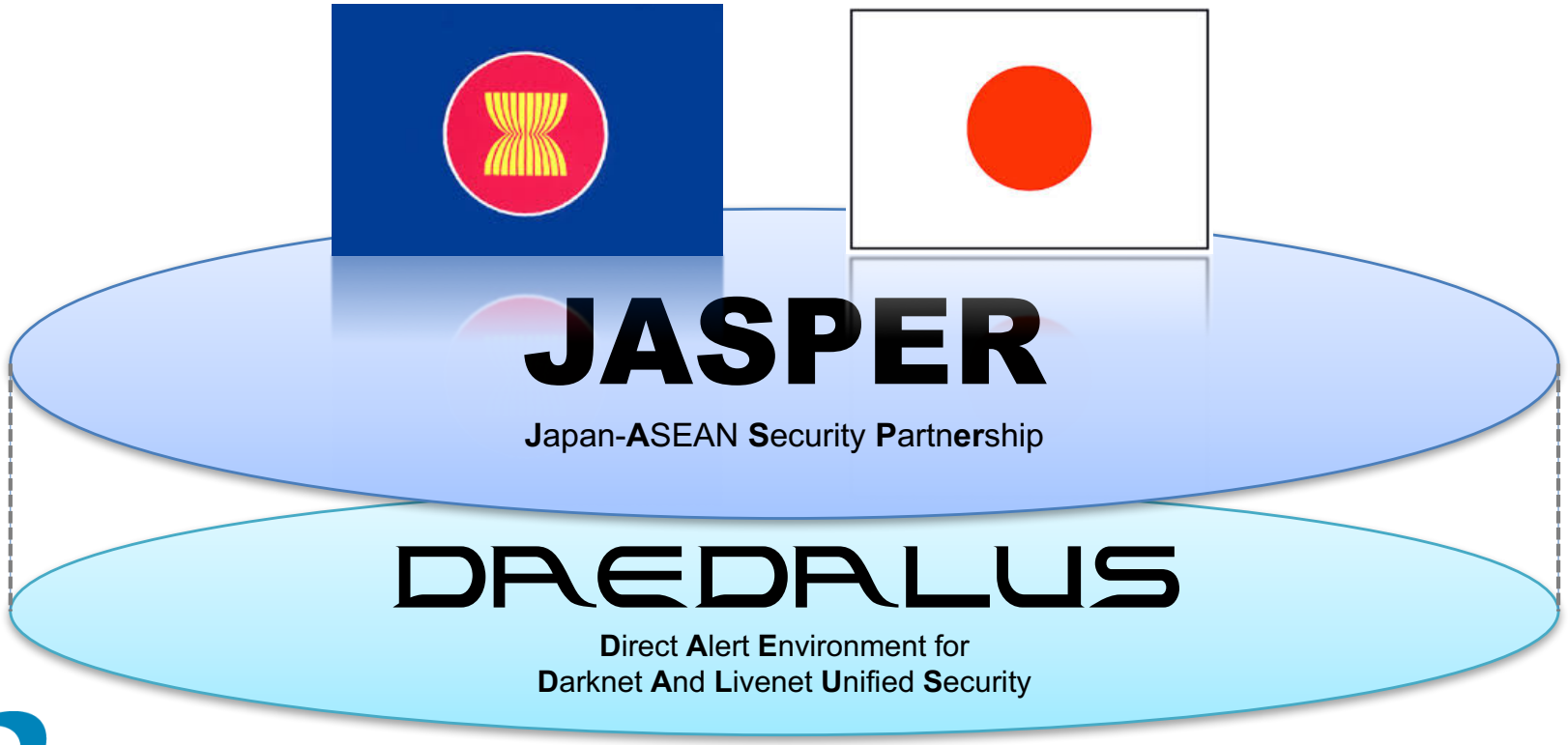


National Institute of Information and Communications Technology

NICTER Network Incident Analysis Center for Tactical Emergency Response

DAEDALUS for ASEAN

JASPER: security partnership between Japan and ASEAN initiated by the Ministry of Internal Affairs and Communications (MIC) since 2013.



National Institute of Information and Communications Technology

NICTER Network Incident Analysis Center for Tactical Emergency Response