Overview of nicter

- R&D project against Cyber Attacks in Japan -

Daisuke INOUE
Cybersecurity Laboratory
Network Security Research Institute (NSRI)
National Institute of Information and Communications Technology (NICT)

nicter video → http://www.youtube.com/watch?v=asemvKgkib4
DAEDALUS video → http://www.youtube.com/watch?v=3u5u5A8_SE0

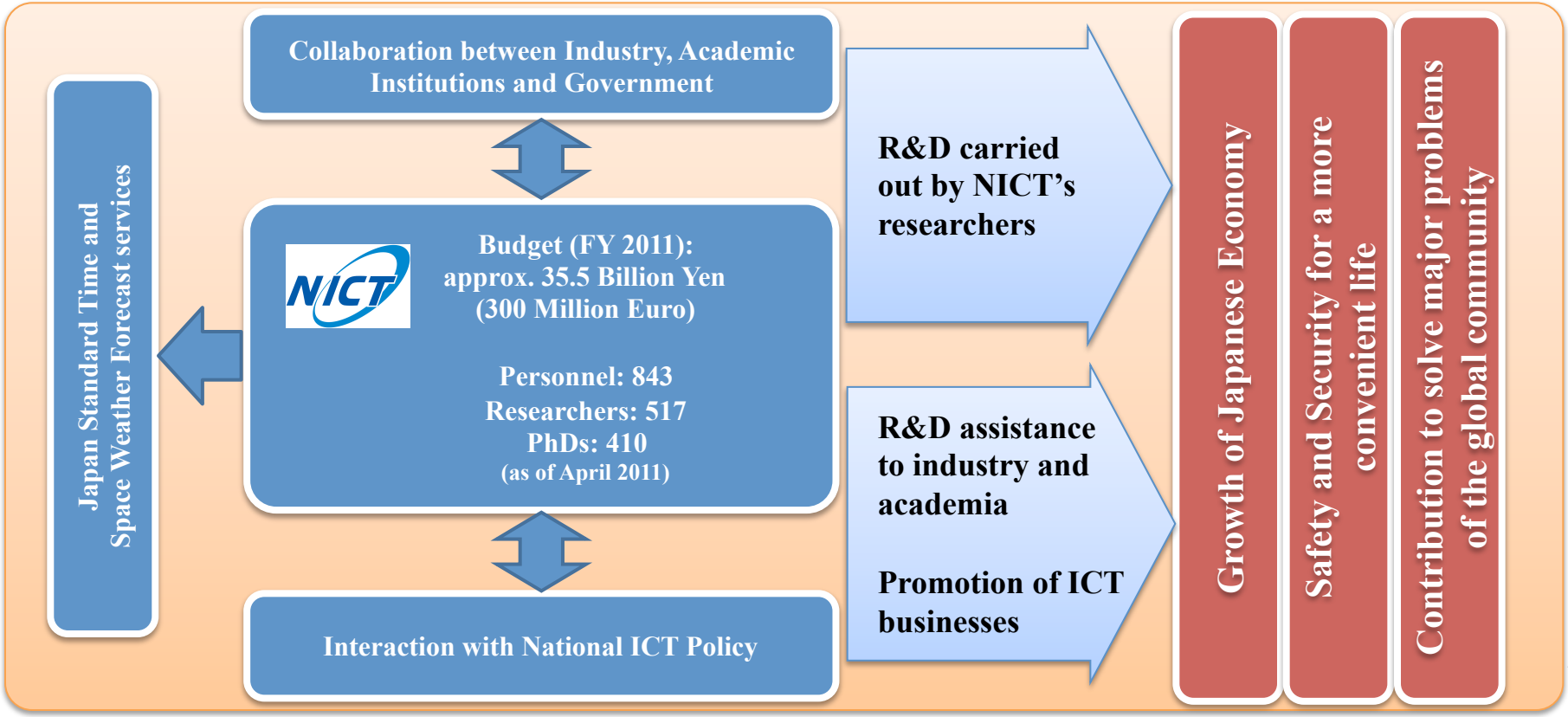
NICT National Institute of Information and Communications Technology

nicter Network Incident Analysis Center for Tactical Emergency Response

Outline of NICT

Mission

As the sole national research institute in the information and communications field, we as NICT will strive to advance national technologies and contribute to national policies in the field, by promoting our own research and development and by cooperating with and supporting outside parties.

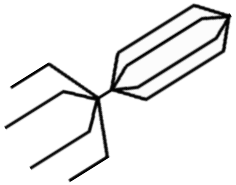


What we are fighting against?

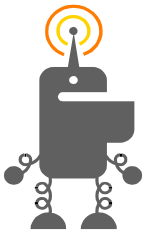
Malware

short for **malicious software** designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behavior.

(from Wikipedia)



Virus



Bot

Worm

Overview of the project nicter

nicter = **N**etwork **I**ncident analysis **C**enter for **T**actical **E**mergency **R**esponse

Target:

Integrated analysis of security threats in large scale networks

- What happens on the Internet?
- What is the root cause?

Strategy:

Network monitoring

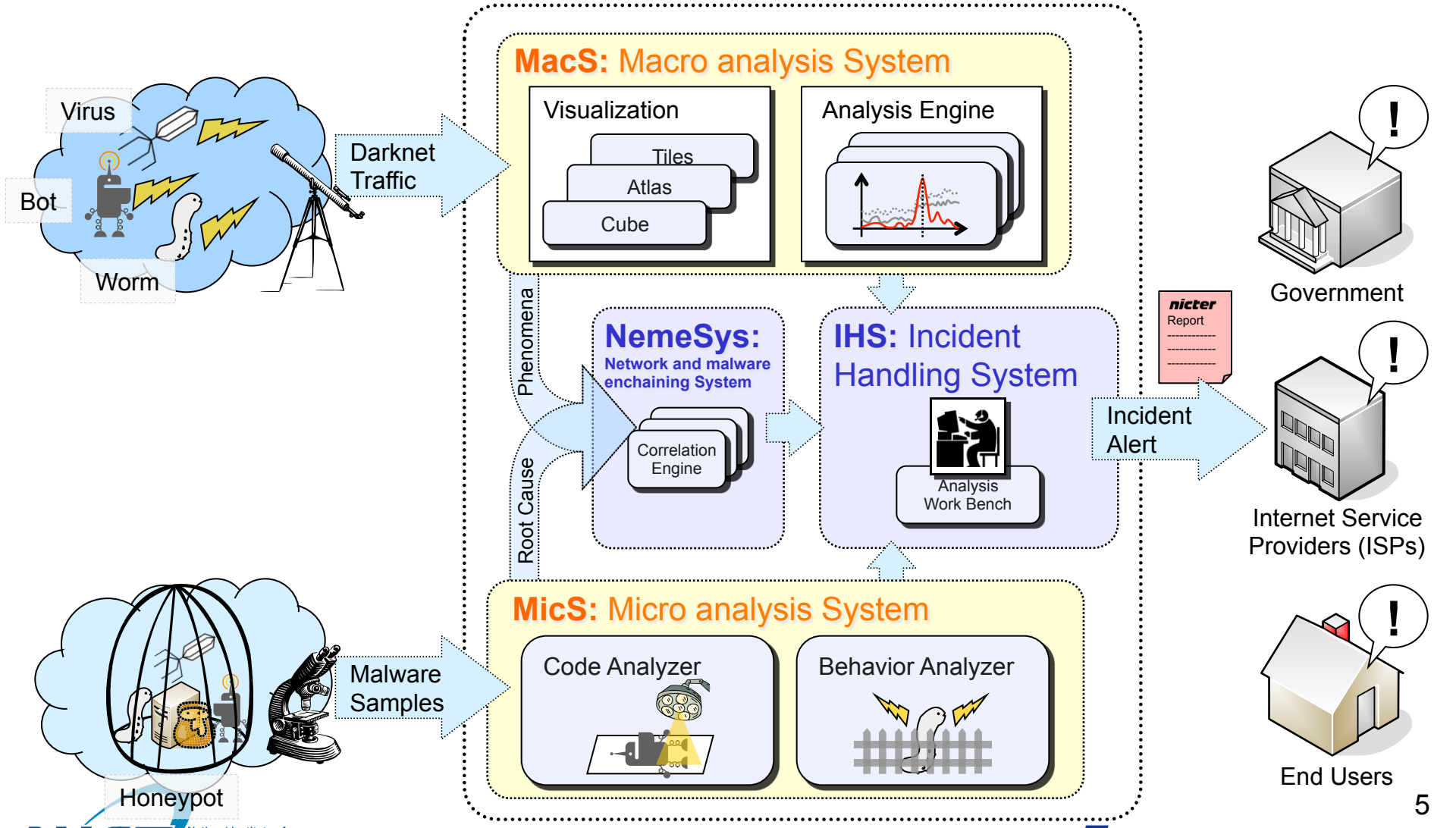
+

Malware analysis

nicter Operation Room

NICT National Institute of Information and Communications Technology

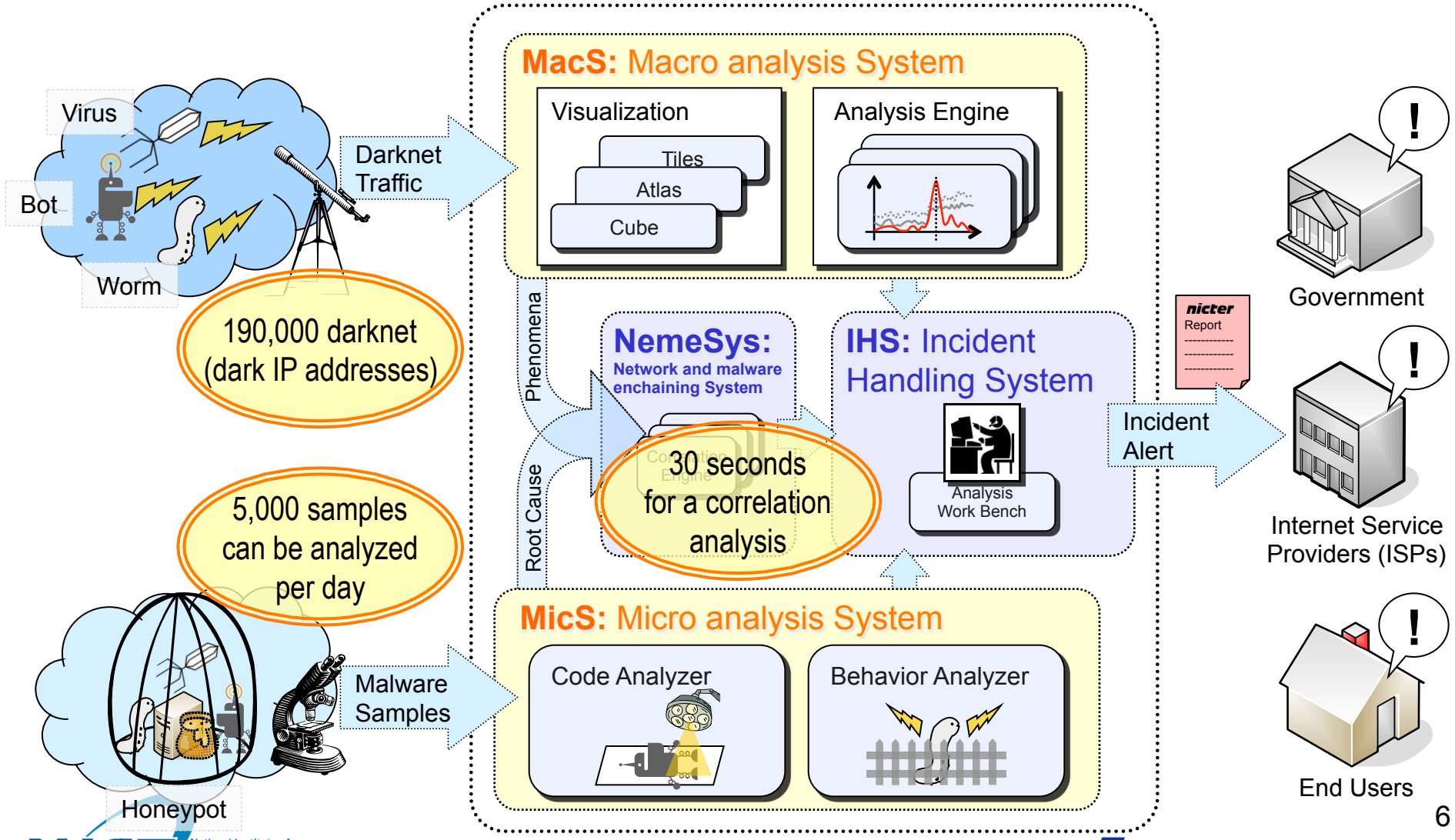
nicter System Overview



NICT National Institute of Information and Communications Technology

nicter Network Incident Analysis Center for Tactical Emergency Response

nicter System Overview



NICT National Institute of Information and Communications Technology

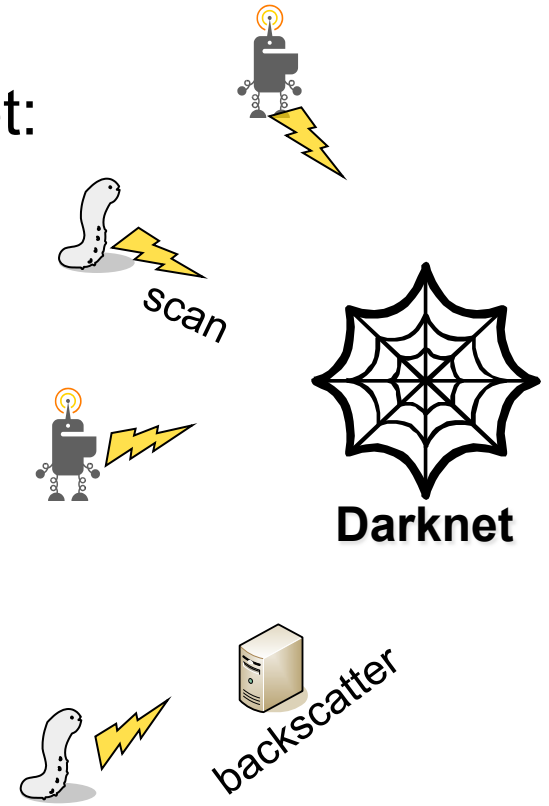
nicter Network Incident Analysis Center for Tactical Emergency Response

What is Darknet?

- **Darknet**: Unassigned IP addresses space and they are not connected to the real servers/PCs.

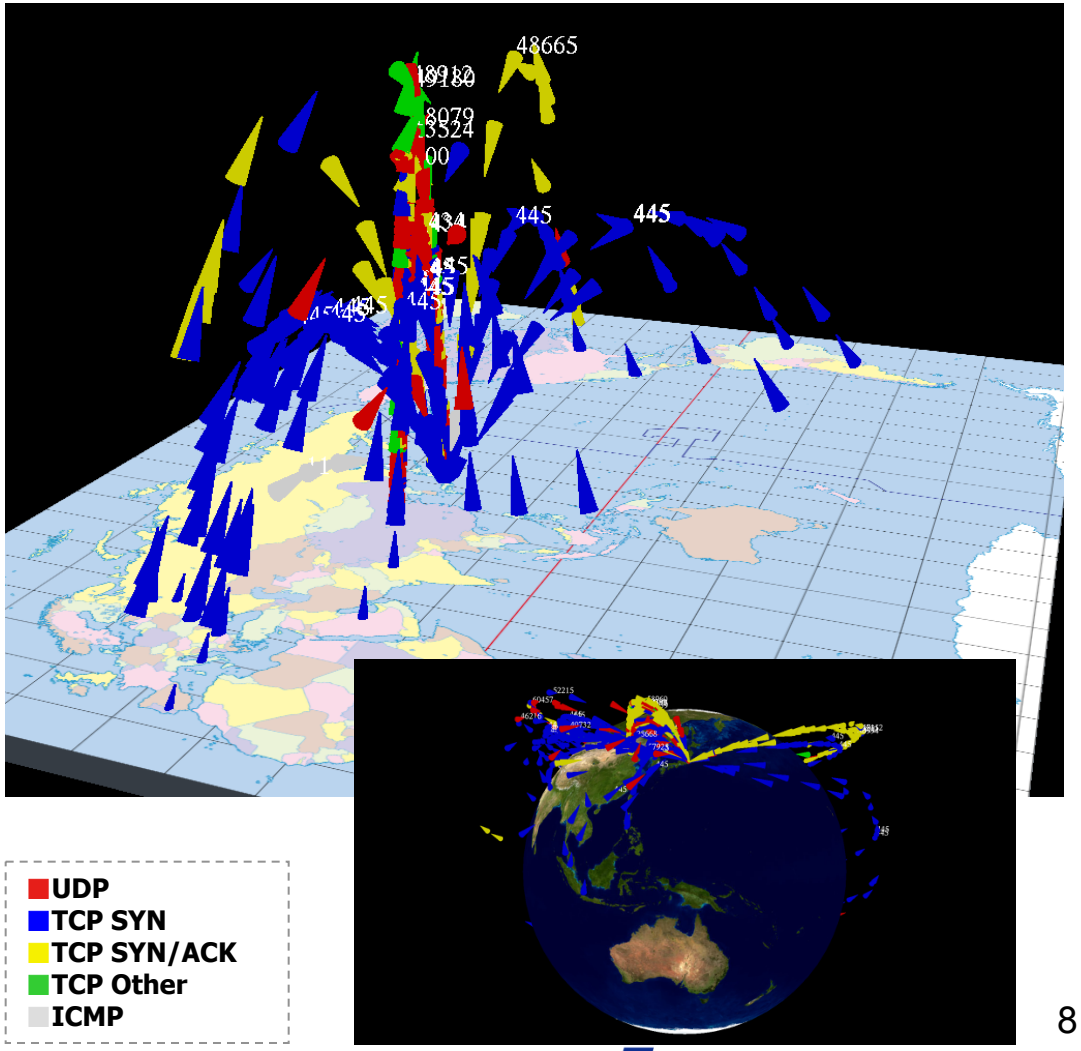
- Types of packets arrived to the darknet:
  - **Scans and attacks by malwares**
  - Backscatter (reflection of DDoS attack)
  - Miss configurations/mistakes

- It is very useful to observe the serious attacks behavior over the Internet.



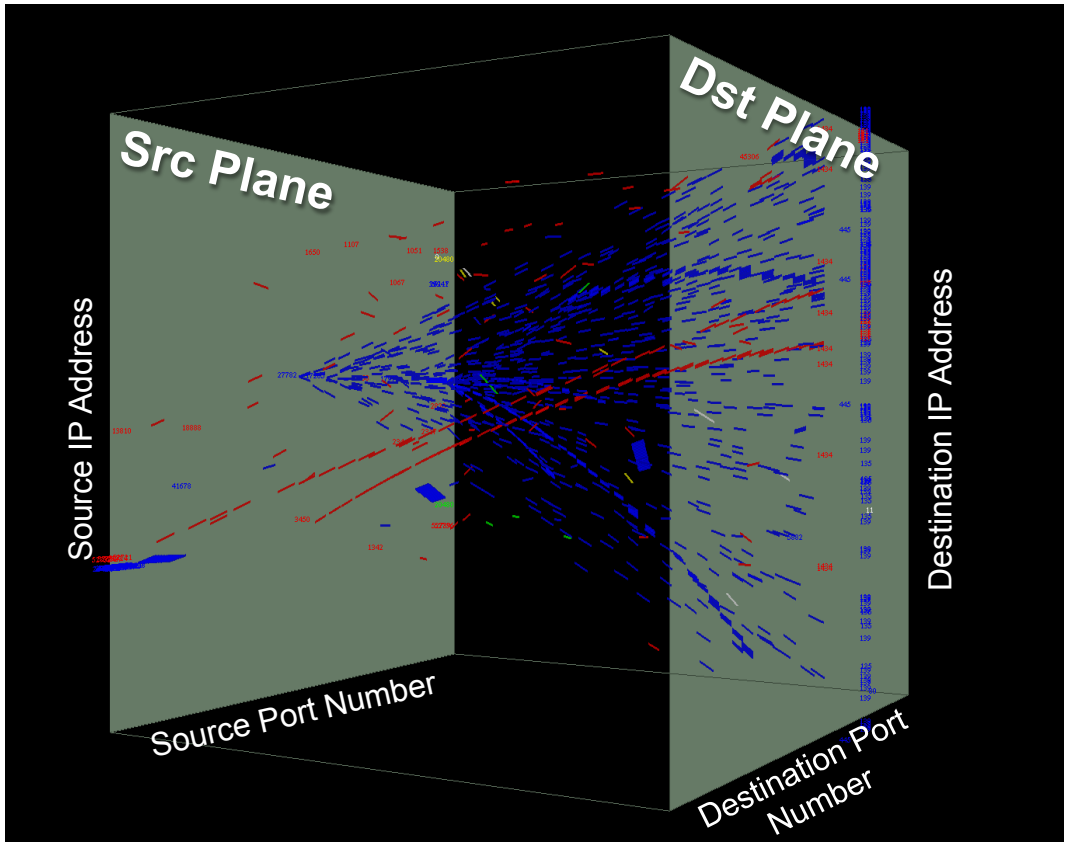
Atlas: Geographical Traffic Visualization

- Shows geographical positions of a packet's src and dst from the IP addresses **in real-time**
- **Each packet** is represented by **a rocket** traversing from source to destination
- The **color** of the rocket indicates the type of packet
- The **altitude** of the rocket is in proportion to its dst port number



Cube: 3D Traffic Visualization

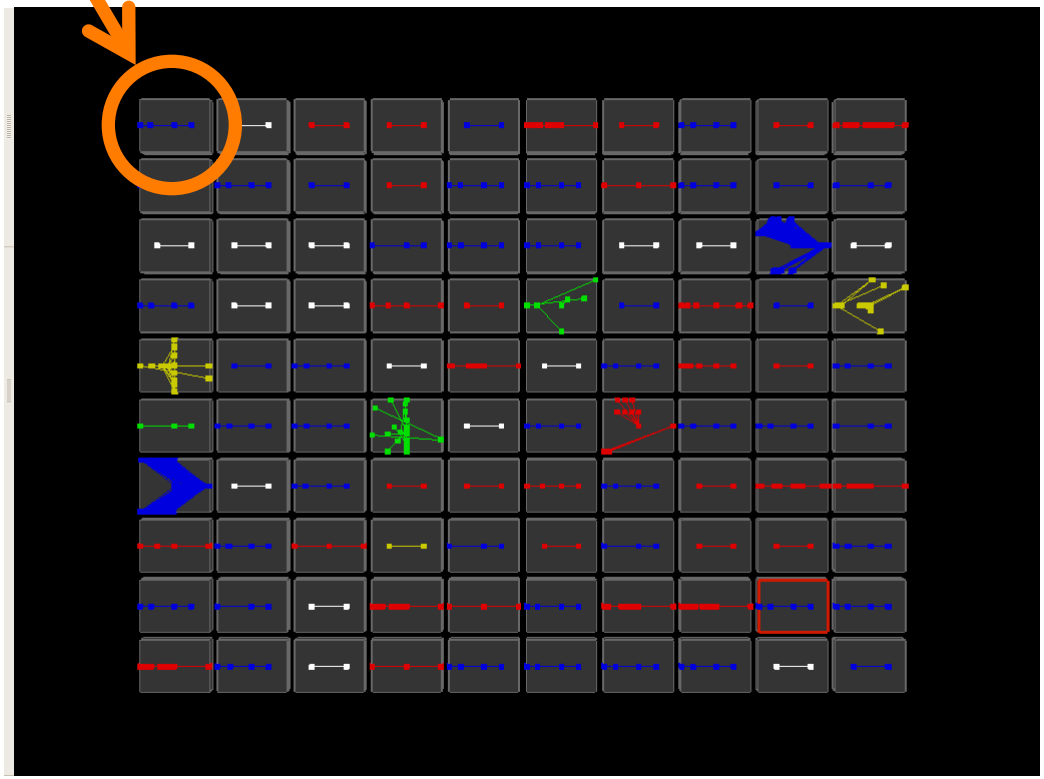
- Shows comprehensive traffic animation **in real-time**
- **Each packet** is represented by **a thin rectangle**
- The rectangle is placed on the source plane according to its **src IP addr and port number**
- It glides to the destination plane taking about six seconds
- The position it reaches is according to its **dst IP addr and port number**



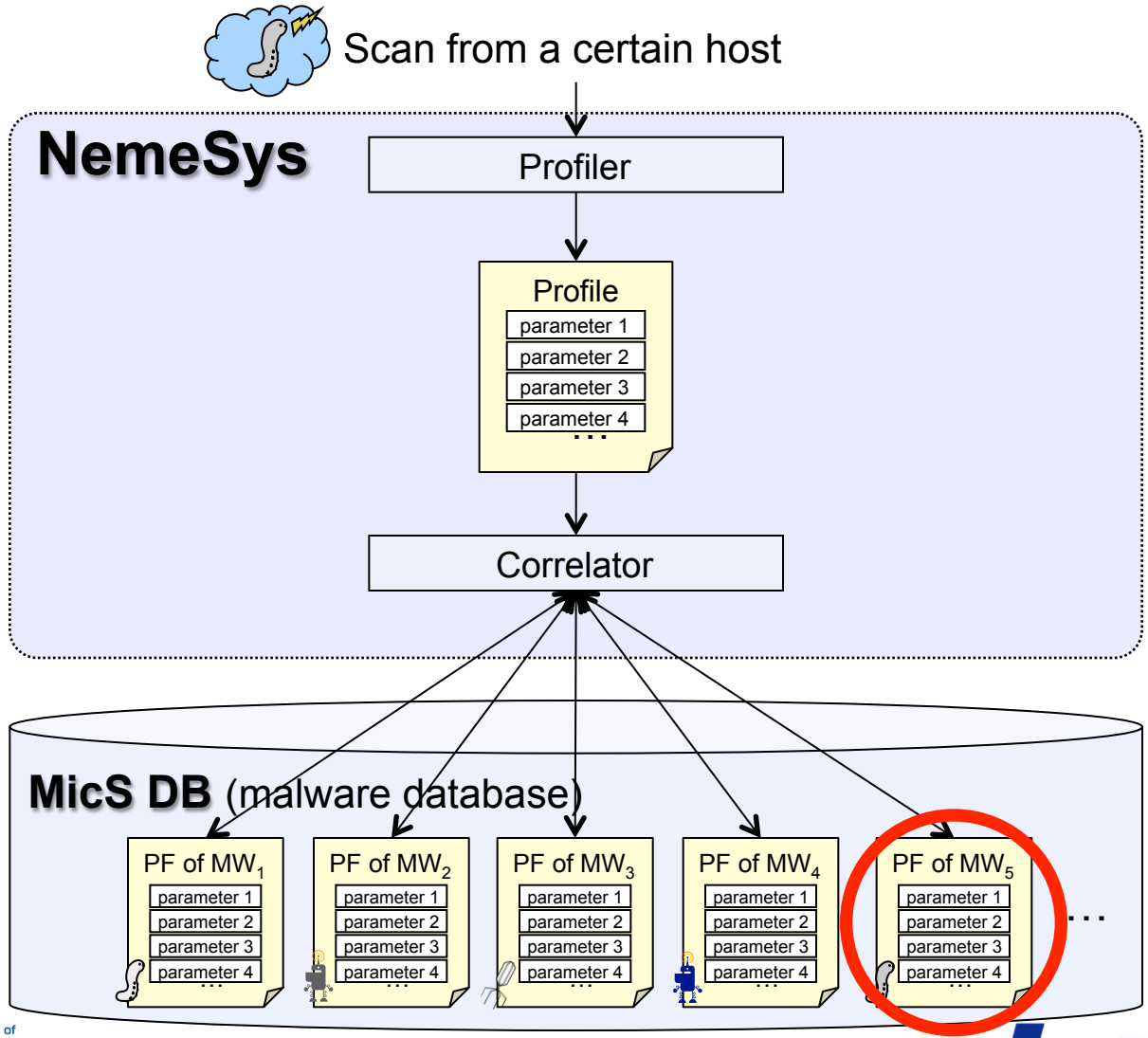
- UDP
- TCP SYN
- TCP SYN/ACK
- TCP Other
- ICMP

Tiles: Host-based Behavioral Analysis Engine

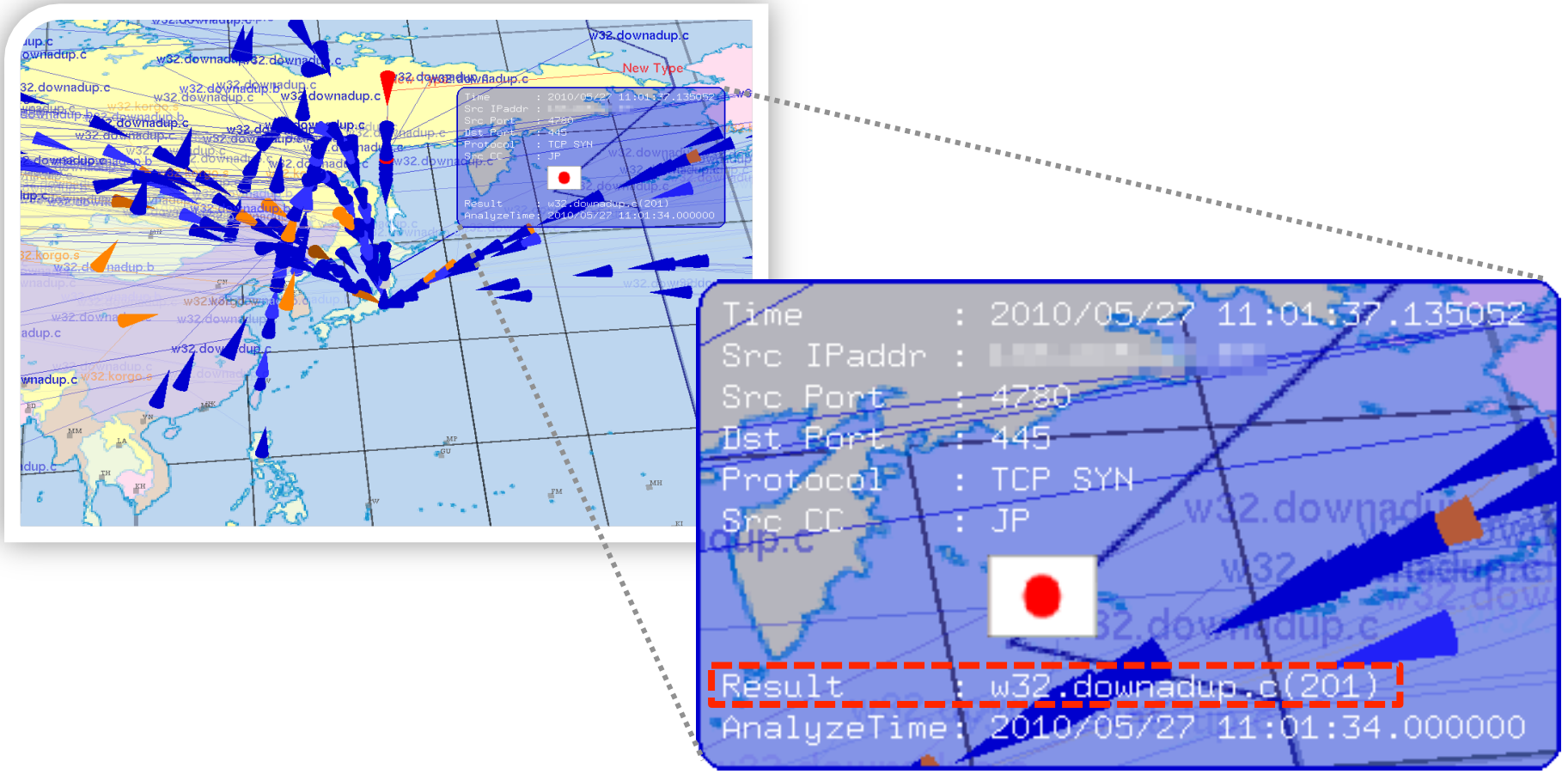
- One ***tile*** illustrates behavior of an attacking host in 30 sec.
- Each behavior is automatically categorized and stored in a DB.
- Unknown attack pattern can be detected.



NemeSys: Macro-Micro Correlation Analysis



Result of Real-time Correlation Analysis



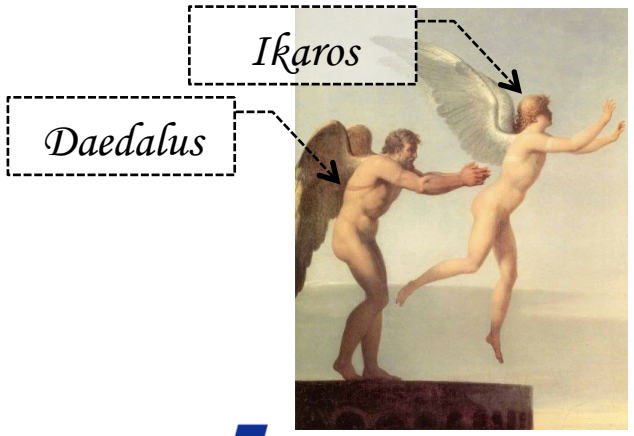
National Institute of Information and Communications Technology

nicter Network Incident Analysis Center for Tactical Emergency Response

- nicter real-time alert system -

DAEDALUS

(**D**irect **A**lert **E**nvironment for
Darknet **A**nd **L**ivenet **U**nified **S**ecurity)



National Institute of Information and Communications Technology

nicter Network Incident Analysis Center for Tactical Emergency Response

Goal and Mechanism of DAEDALUS

Goal:

Utilize the darknet monitoring results

for securing the livenet.

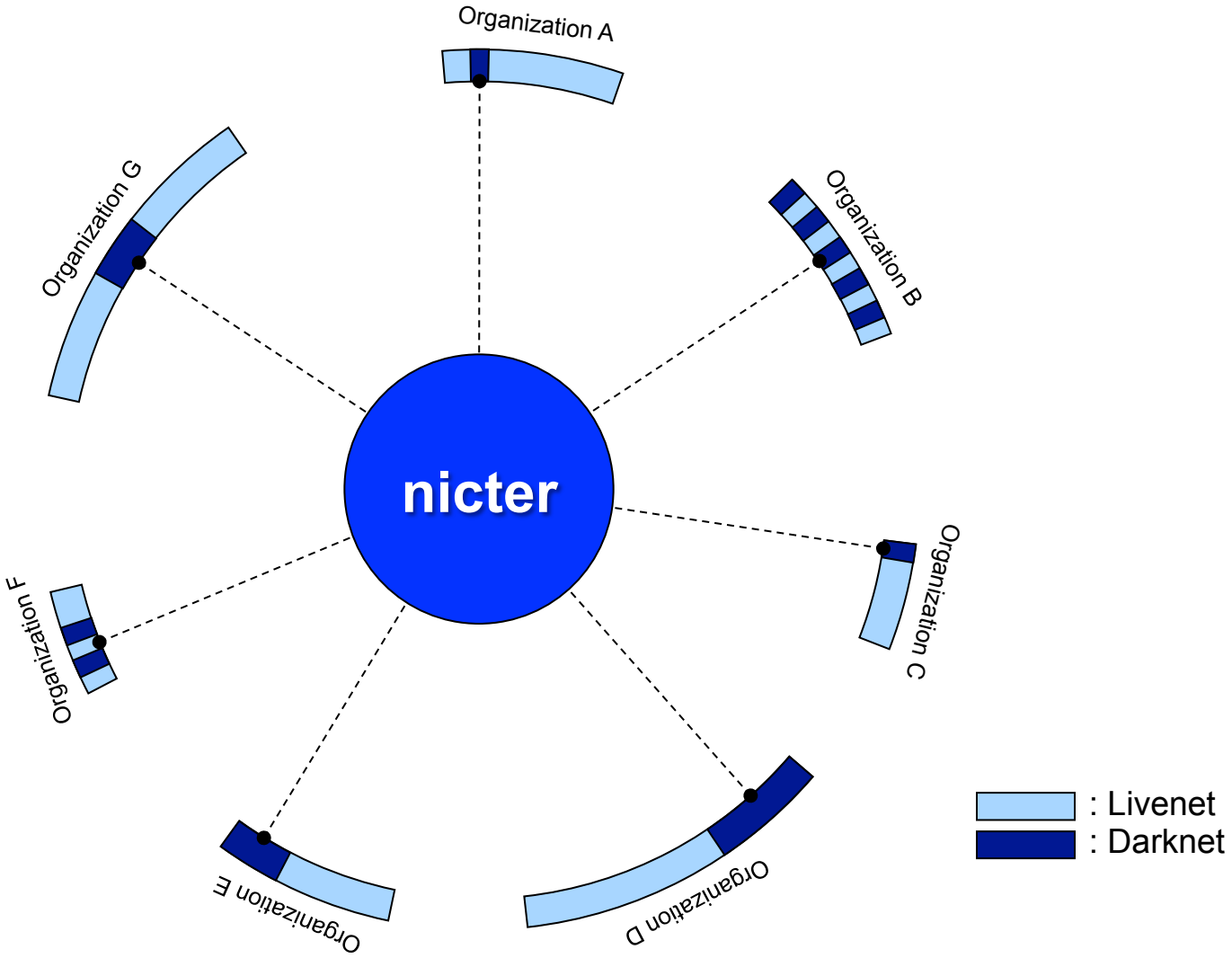
Mechanism:

if (nicter receives packets

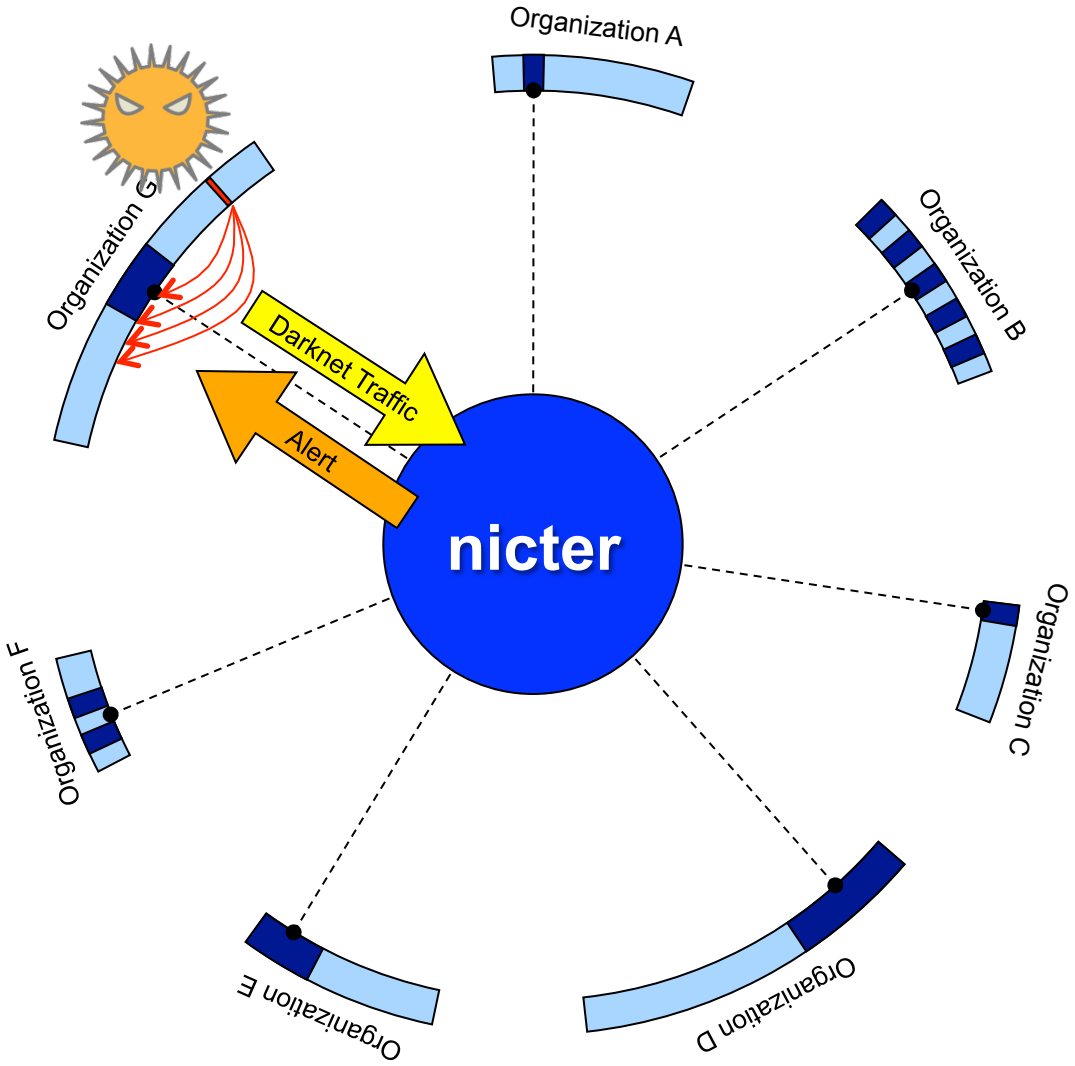
from a cooperative organization)

alert;

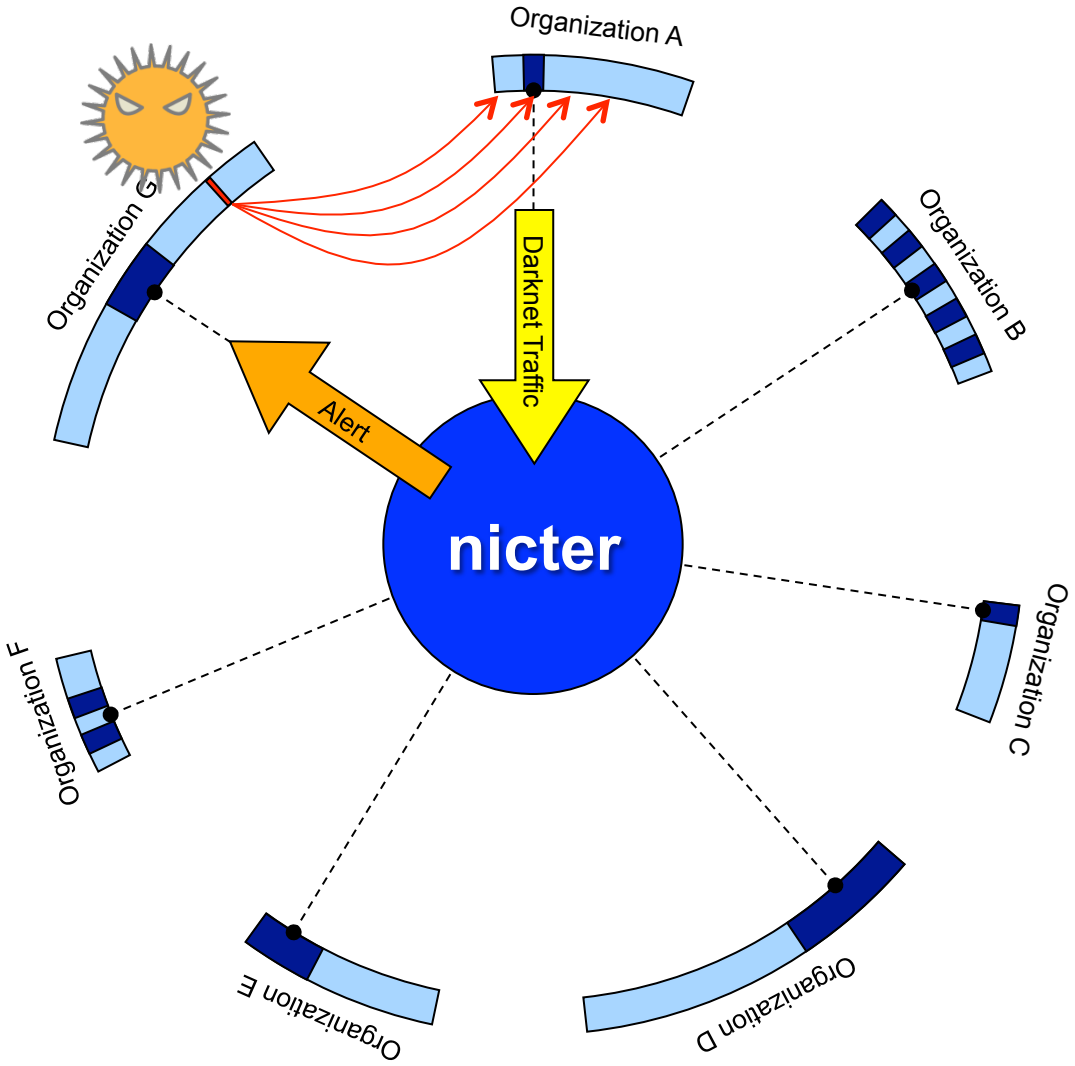
System Overview



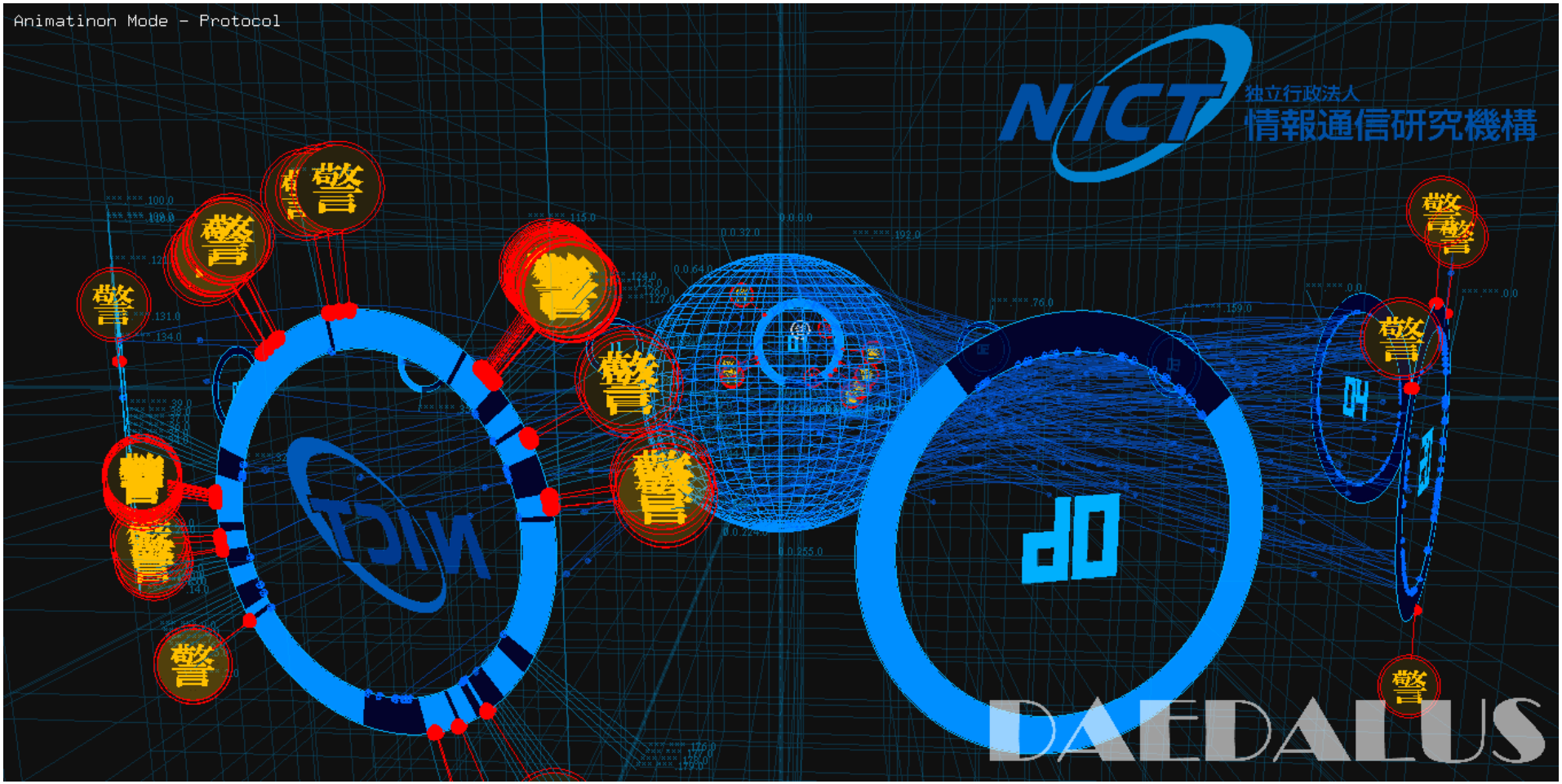
Internal Darknet Alert



External Darknet Alert



DAEDALUS viz



National Institute of Information and Communications Technology

nicter Network Incident Analysis Center for Tactical Emergency Response

Yet Other Emerging Threats…

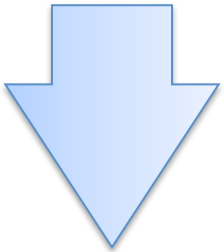
- Drive-by Download
- SNS Malware
- Targeted Attack
- Threats on IPv6 Network

etc…

Conclusions

- We are conducting R&D to investigate **practical** Cybersecurity technologies.

- We still need **new frameworks** to observe, analyze and respond to the emerging threats.



- **International collaboration** is crucial for developing state-of-the-art Cybersecurity technologies.