Overview of Cybersecurity Research in NICT

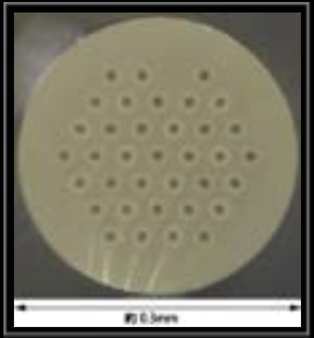
Daisuke Inoue
Cybersecurity Research Institute
National Institute of Information and Communications Technology (NICT)

NICT - the sole national research institute in the field of ICT in Japan -

- ICT for sustainable world and human happiness
- Promoting its own research and development
- Cooperating with and supporting industry and academia

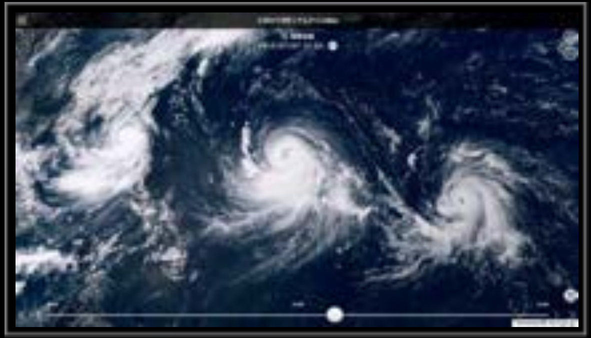
Research Topics in NICT

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



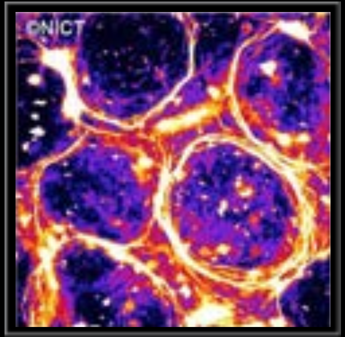
Optical Communication
(Peta bps class multi-core fiber)

Satellite Communication
（Internet Satellite WINDS）



Science Cloud
（Reai-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)

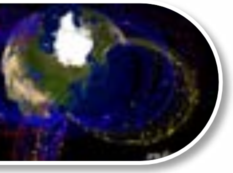
Ultra Realistic Communication
(Electronic Holography)

Cybersecurity
(DAEDALUS)

Cybersecurity Laboratory

CYBERSECURITY
Laboratory

Research Map of Cybersecurity Laboratory (since 2005)



Network Incident analysis Center for Tactical Emergency Response

NICTER

Direct Alert Environment for Darknet And Livenet Unified Security

DAEDALUS

Passive

NICTER Real-network Visual ANAlyzer KAI

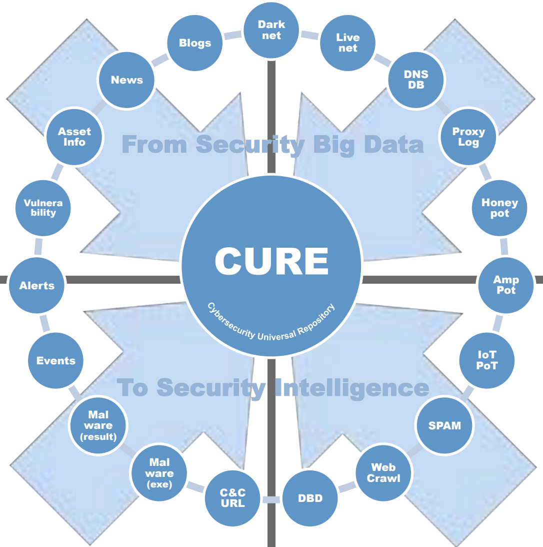
NIRVANA改

NICTER Real-network Visual ANAlyzer KAI-II

NIRVANA改弐

Global (indiscriminate attack)

(targeted attack) Local

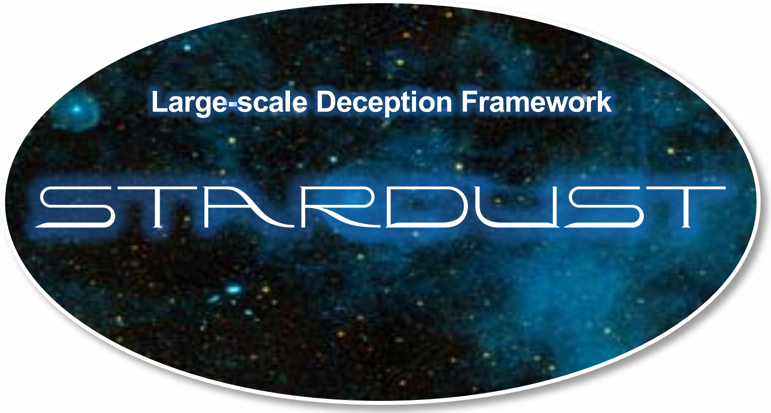


Cybersecurity Universal REpository

Web-based Attack Response with Practical and Deployable Research InitiatiVE

WARPDRIVE

(Commission Research)



Large-scale Deception Framework

STARDUST

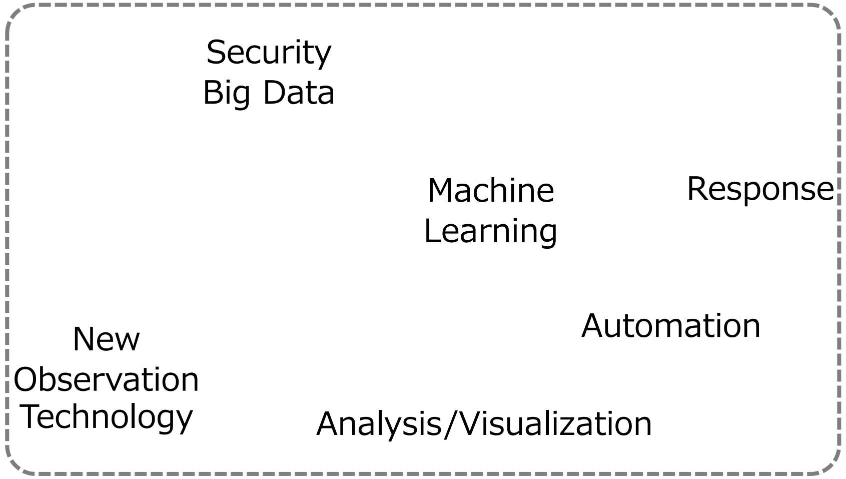
Active

# Collaborative research with Yokohama National Univ. and Saarland Univ.

Research Topics (2021-2026)

(1) Data-driven Cybersecurity Research

- ✓ Next-gen STARDUST
- ✓ Sustainable evolution of CURE
- ✓ AI x Cybersecurity, etc.



Security Big Data

Machine Learning

Response

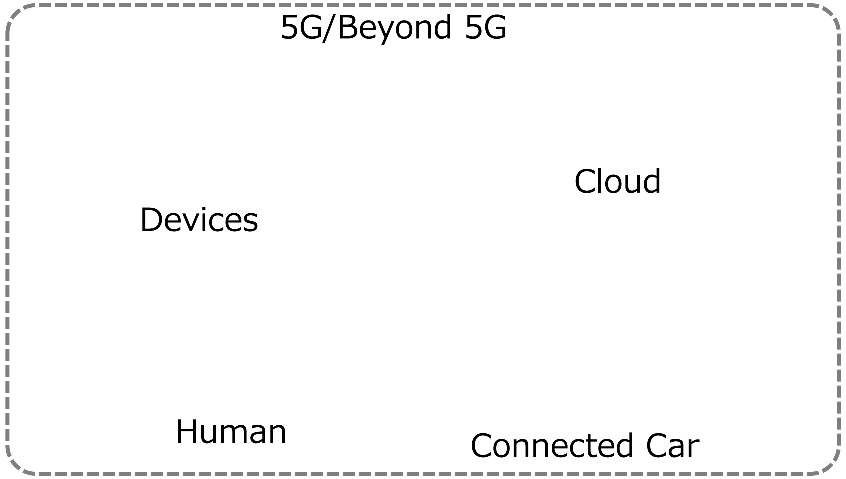
New Observation Technology

Automation

Analysis/Visualization

(2) Emerging Security Research

- ✓ 5G/B5G security
- ✓ Low-layer security
- ✓ Usable security



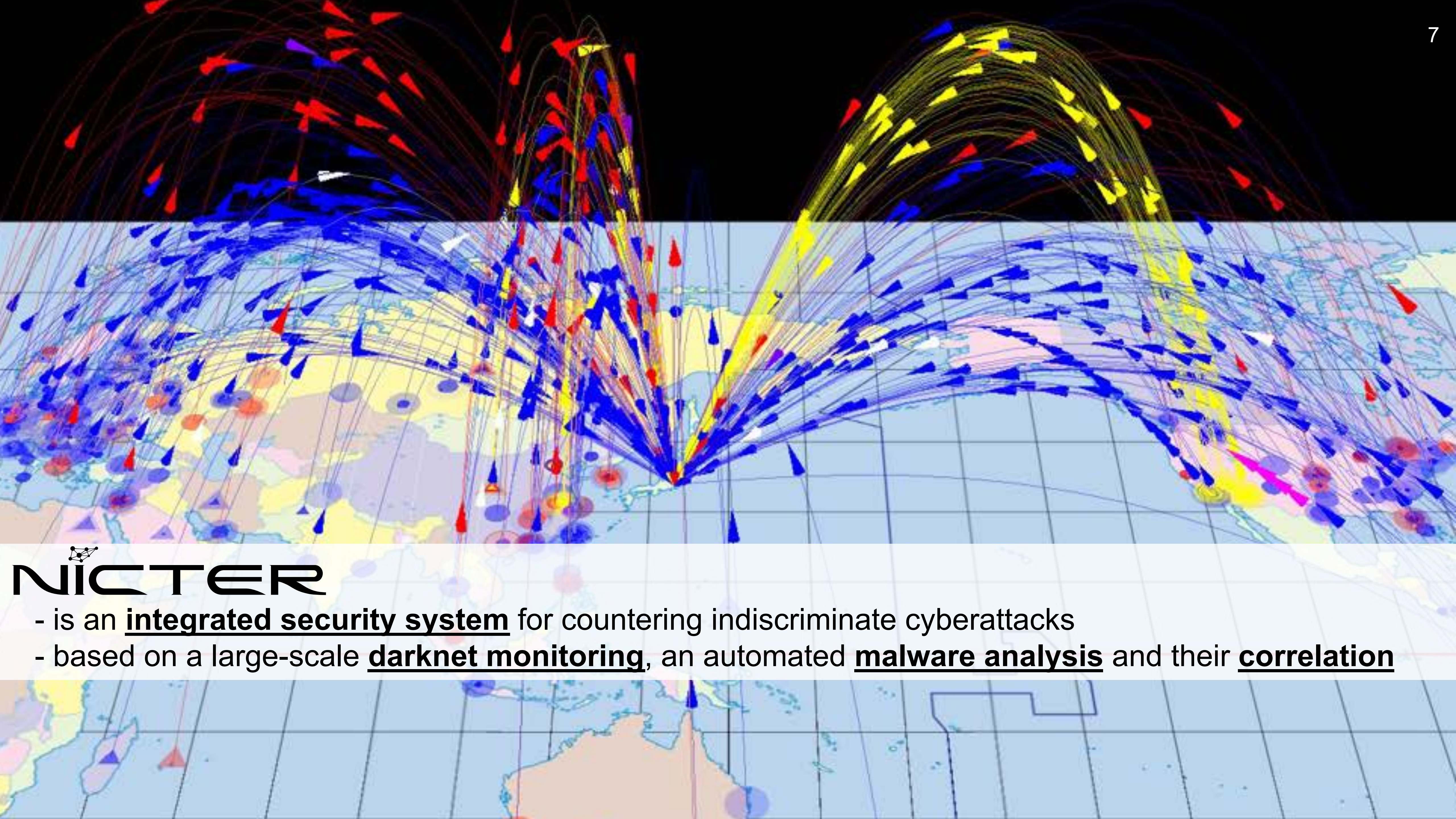
5G/Beyond 5G

Cloud

Devices

Human

Connected Car

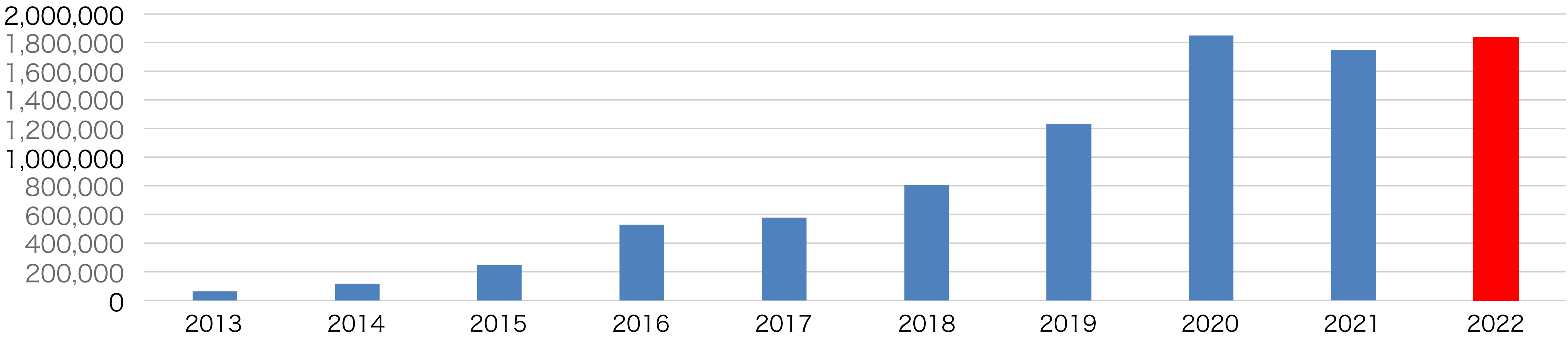


NICTER

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

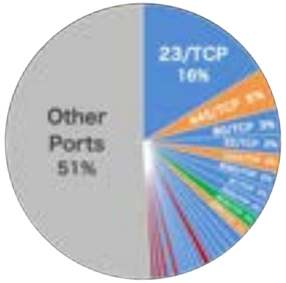
Yearly Stats of Darknet Traffic (Last 10 Years)

Year	Number of packets par year	Number of IP address for darknet	Number of packets par 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**

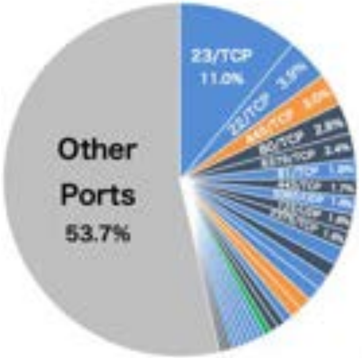


Number of packets per IP address per year

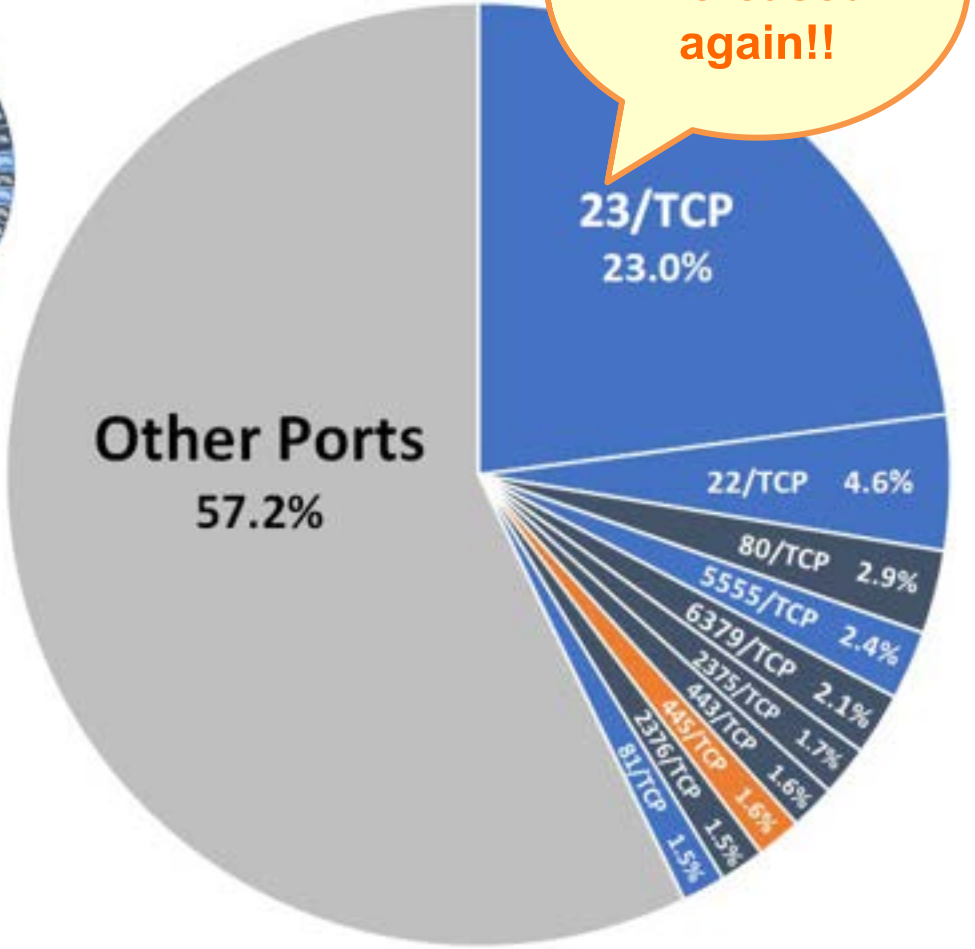
Top 10 Dst Ports observed by NICTER (2022)



2020



2021



2022

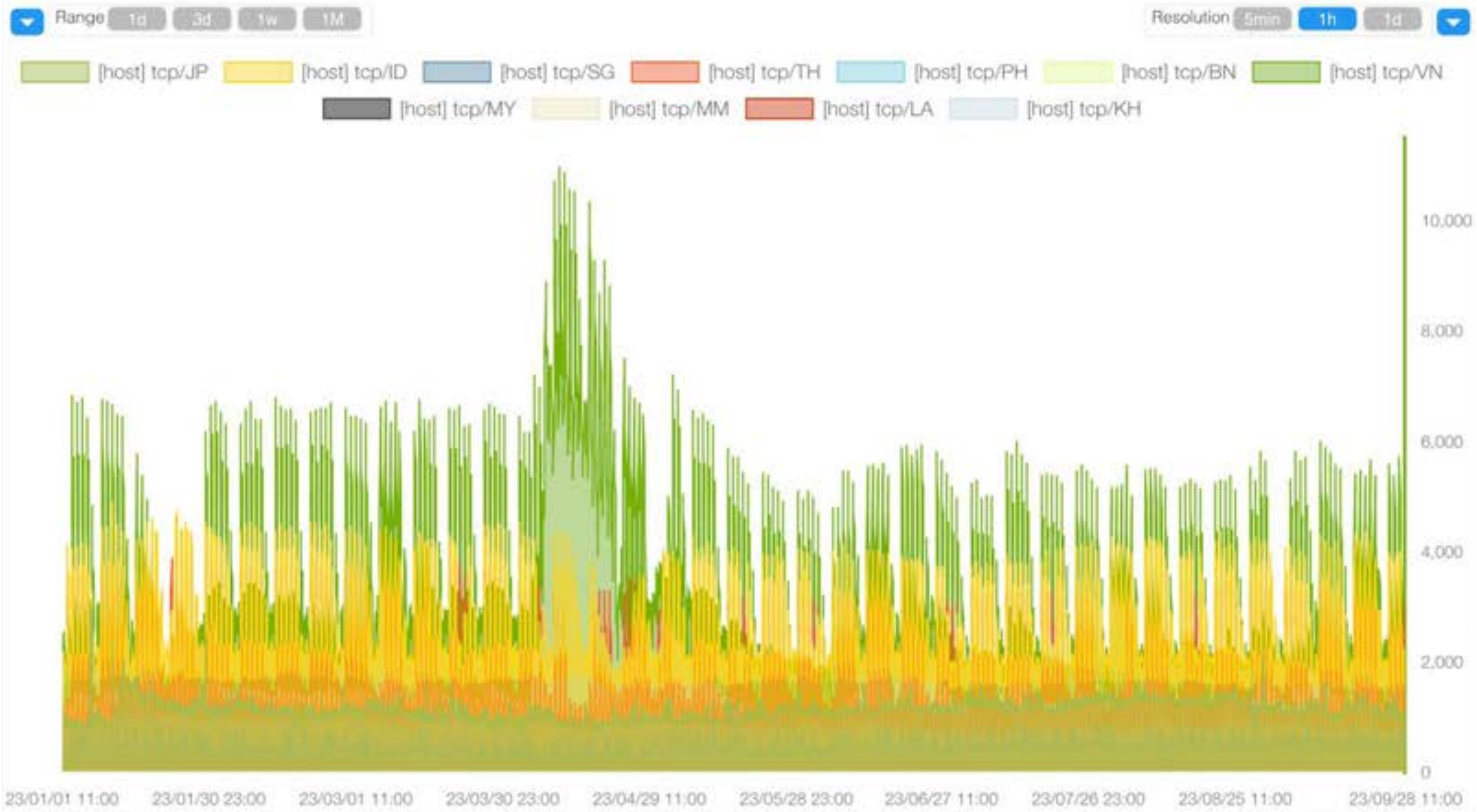
23/TCP increased again!!

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)

Number of Attacking Hosts from ASEAN and JP

Results of NICTER Darknet Monitoring from Jan to Sep 2023



Challenges for Cybersecurity Research

- **Data collection**
  - ✓continuous and large-scale data collection is crucial
- **Talent acquisition**
  - ✓how to deal with talent competition against private sector?
- **Implementation to society**
  - ✓only a few domestic companies make their own products

Challenges for AI x Cybersecurity

●Ground Truth

✓ how do we collect enough volume of labeled data?

●False Positive Reduction

✓ true positive 99.9% → 100 thousand false positives in 100 million security alerts

●Explainable AI (XAI)

✓ explainability is the most important for real incident handling

●Real-time ML Engines

✓ security operation needs real-time and 24/7 ML engines