



UNIVERSITÉ DU
LUXEMBOURG



UNIVERSITÉ DU
LUXEMBOURG

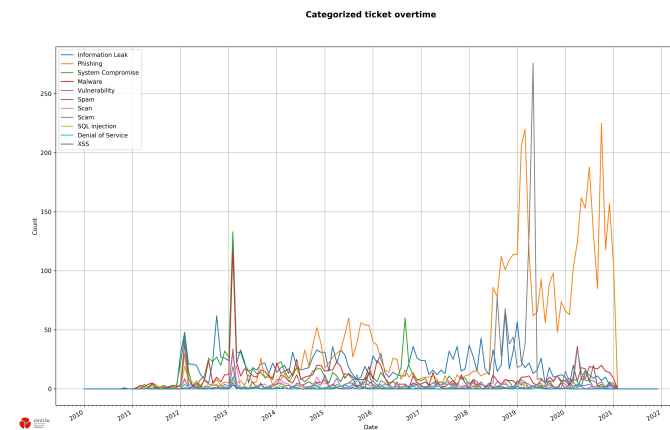
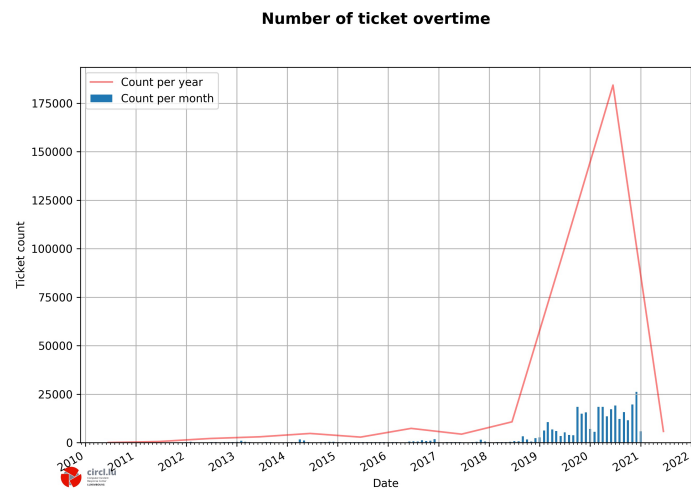
New Technology, old risks, IoT (in-)security

Master in Technopreneurship

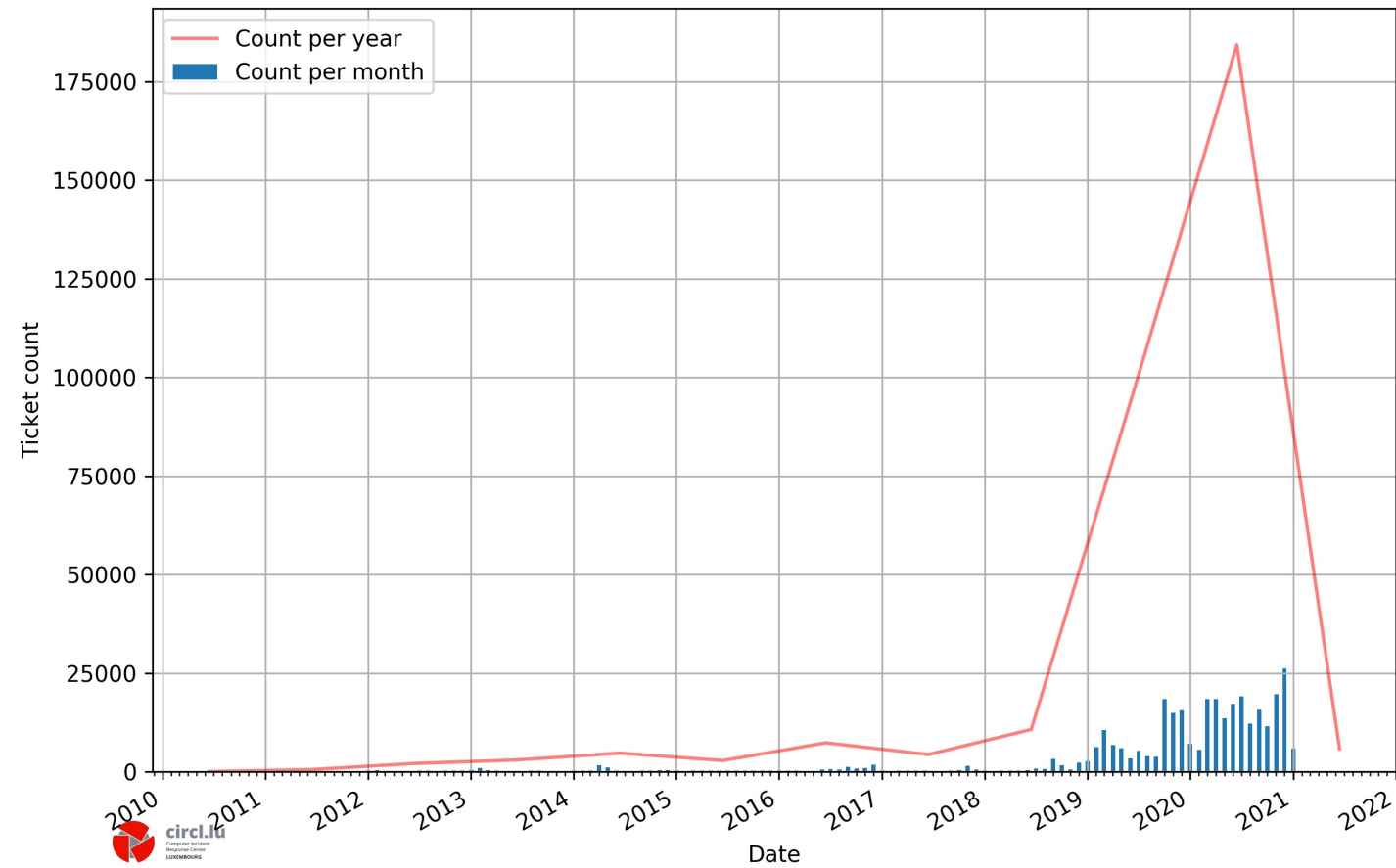
Threat landscape

2020/2021

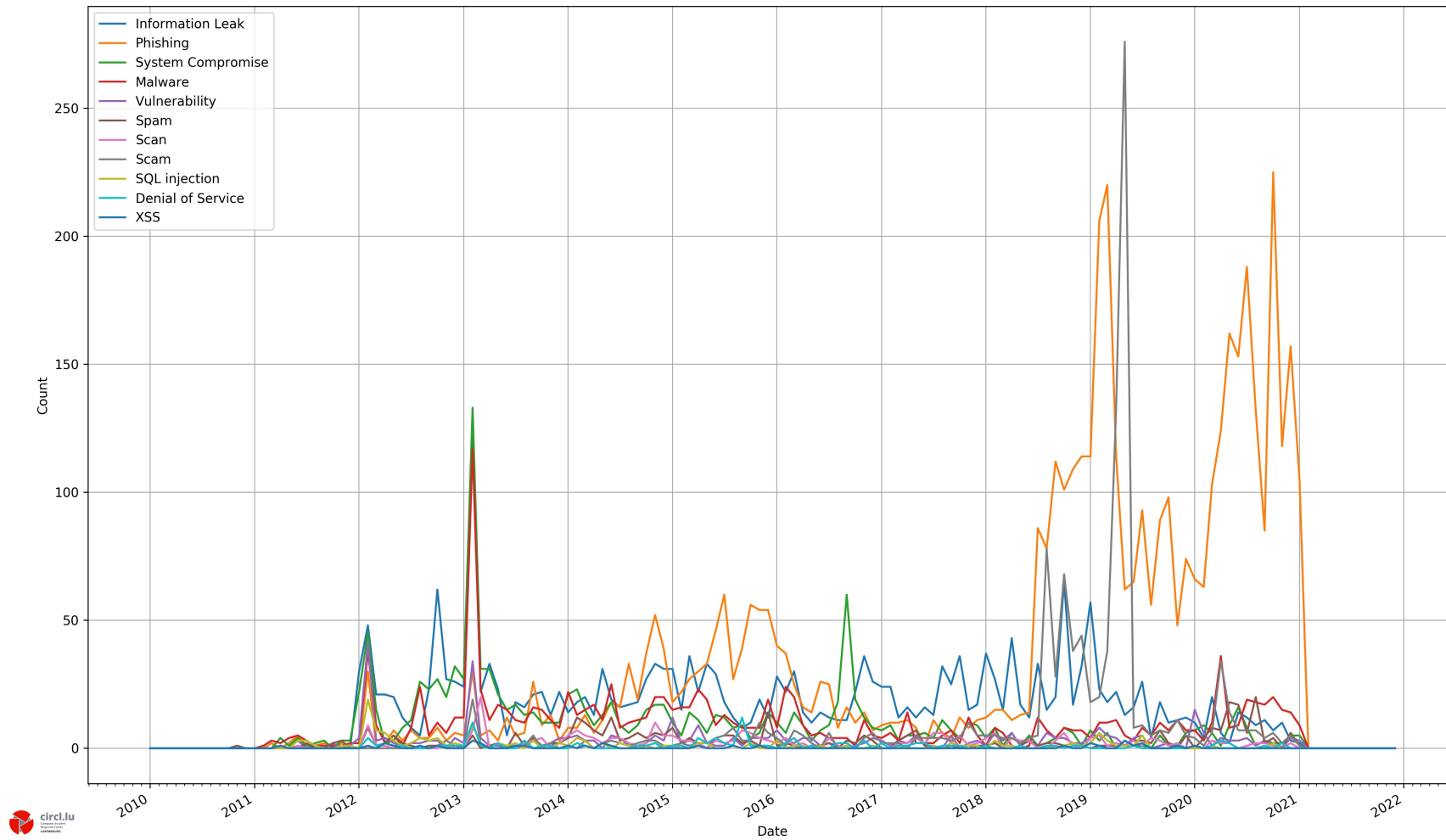
Luxembourg (numbers & type)



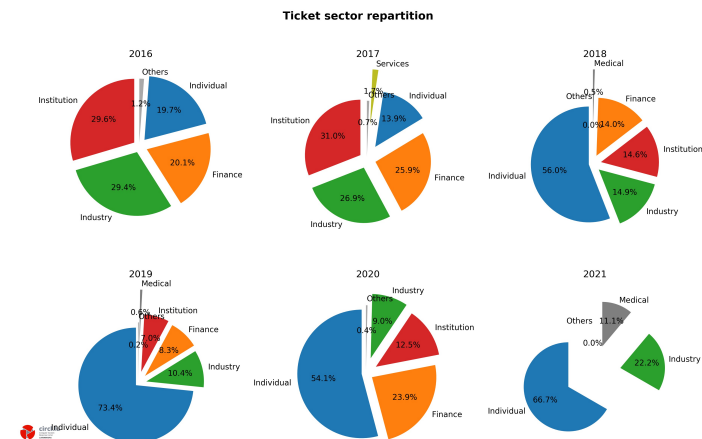
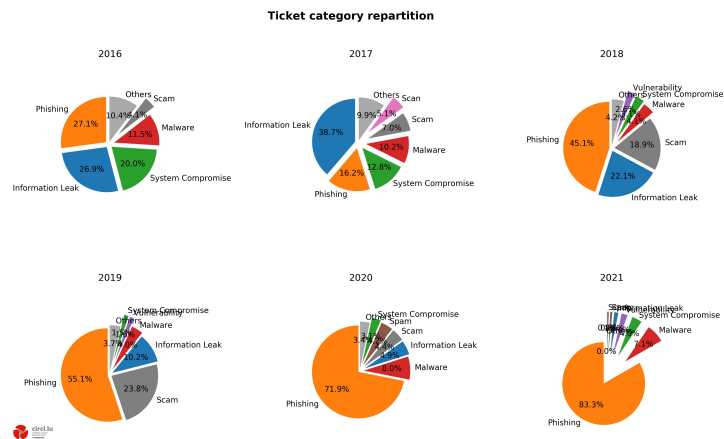
Number of ticket overtime



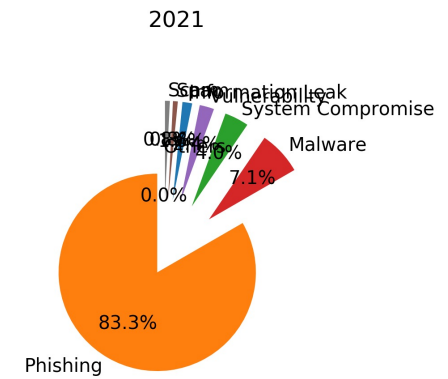
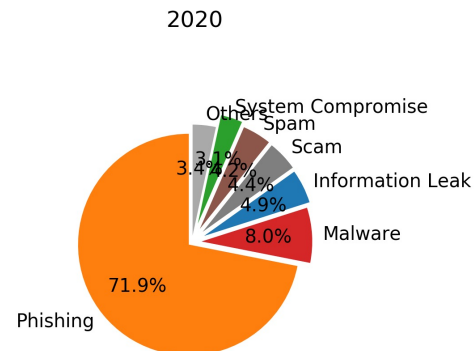
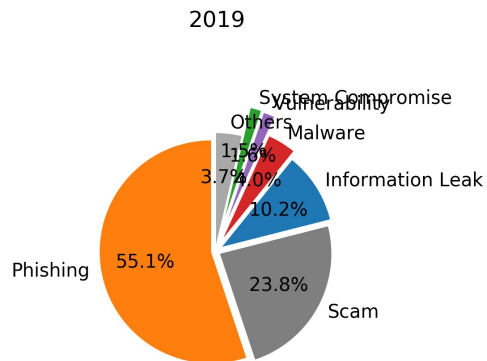
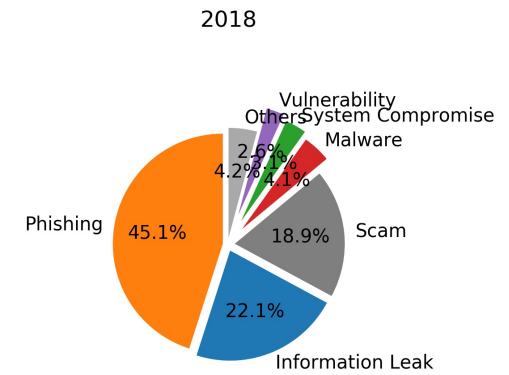
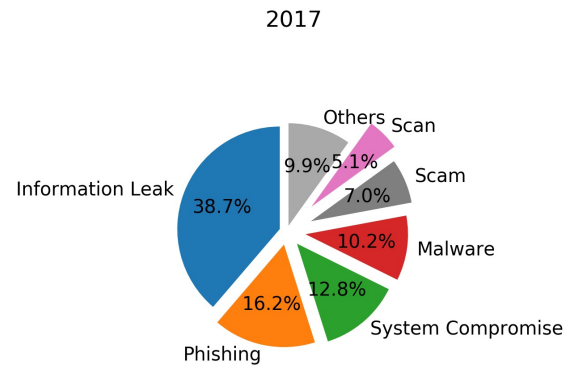
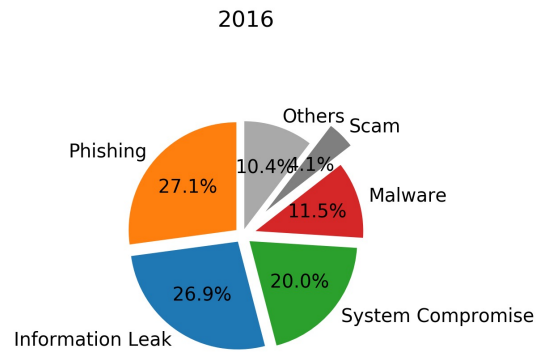
Categorized ticket overtime



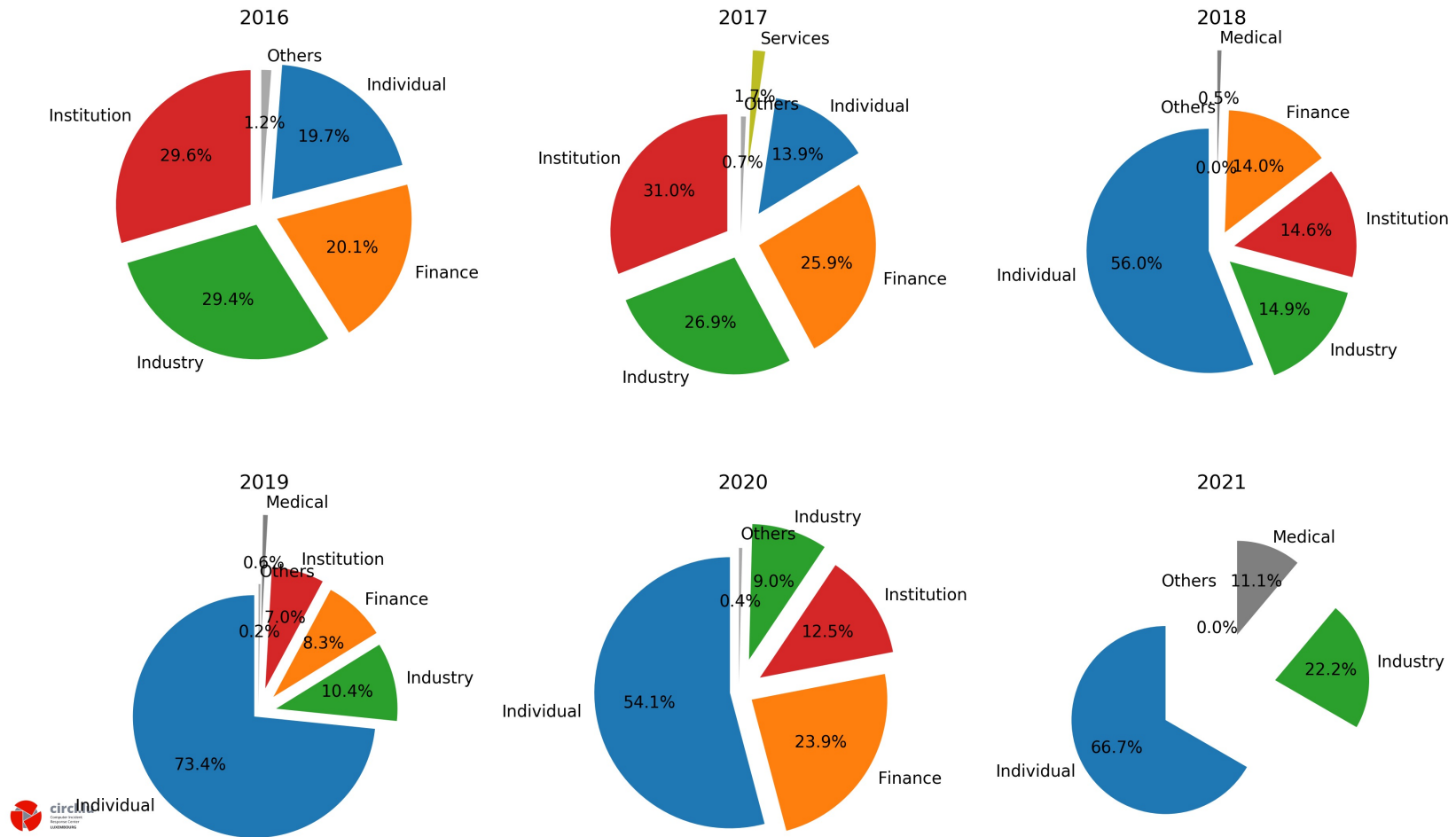
Luxembourg (category and sector)



Ticket category repartition



Ticket sector repartition



Europe (critical/vital systems)

Figure 1: ENISA Threat Landscape 2021 - Prime threats



Figure 4: Targeted sectors per number of incidents (April 2020-July 2021)

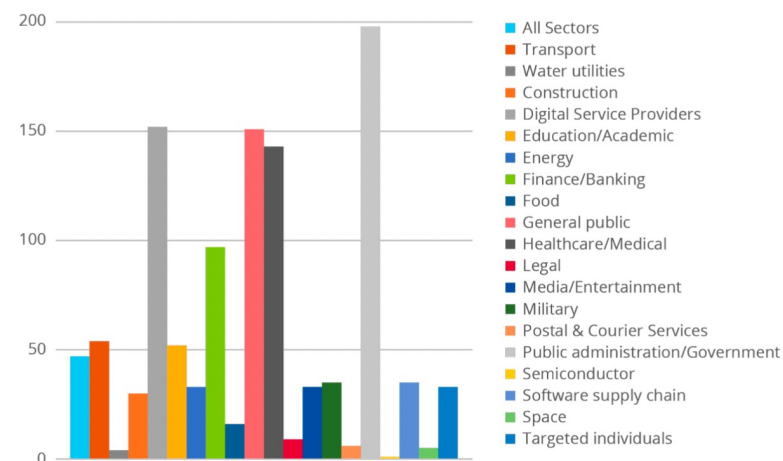


Figure 1: ENISA Threat Landscape 2021 - Prime threats

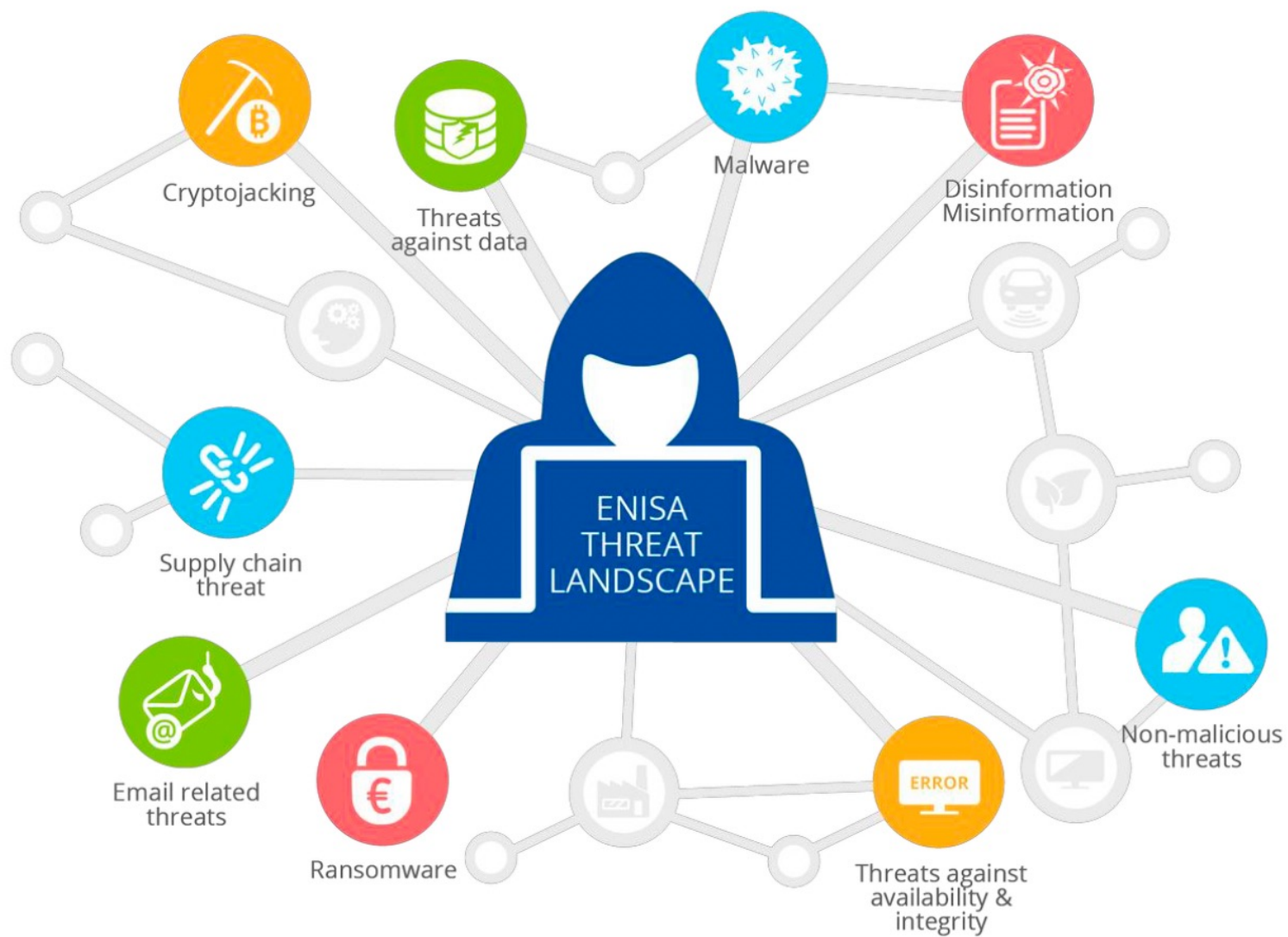
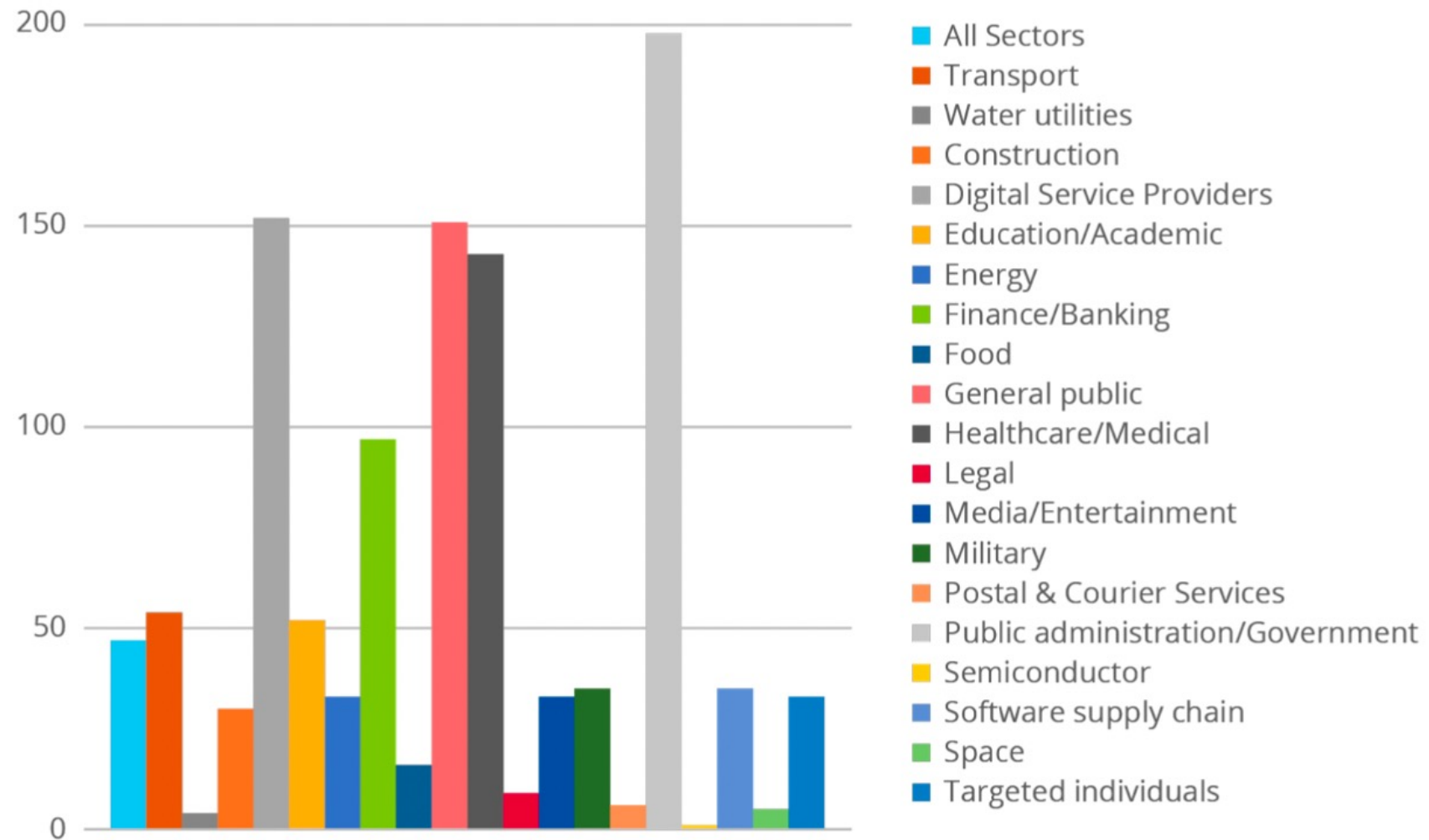


Figure 4: Targeted sectors per number of incidents (April 2020-July 2021)



Europe (main findings)

- **Ransomware** has been assessed as the **prime threat for 2020-2021**.
- **Cybercriminals are increasingly motivated by monetisation** of their activities, e.g. ransomware.
- **Cryptocurrency** remains the most common pay-out method for threat actors.
- **Malware decline** continues, however an increase in threat actors resorting to relatively new or uncommon programming languages to port their code.
- **Cryptojacking infections** attained a **record high**.
- **COVID-19 is still the dominant lure in campaigns** for e-mail attacks. There was a **surge in healthcare sector related data breaches**.
- **Traditional DDoS (Distributed Denial of Service) campaigns** are more targeted, more persistent and increasingly multi-vector. The **IoT (Internet of Things)** in conjunction with **mobile networks** is resulting in a new wave of DDoS attacks.
- **Spike in non-malicious incidents**, as the COVID-19 pandemic became a multiplier for **human errors** and **system misconfigurations**, up to the point that most of the breaches in 2020 were caused by errors.



Europe (threat actors)

- State-sponsored actors
- Cybercrime actors
- Hacker-for-hire actors
- Hacktivists

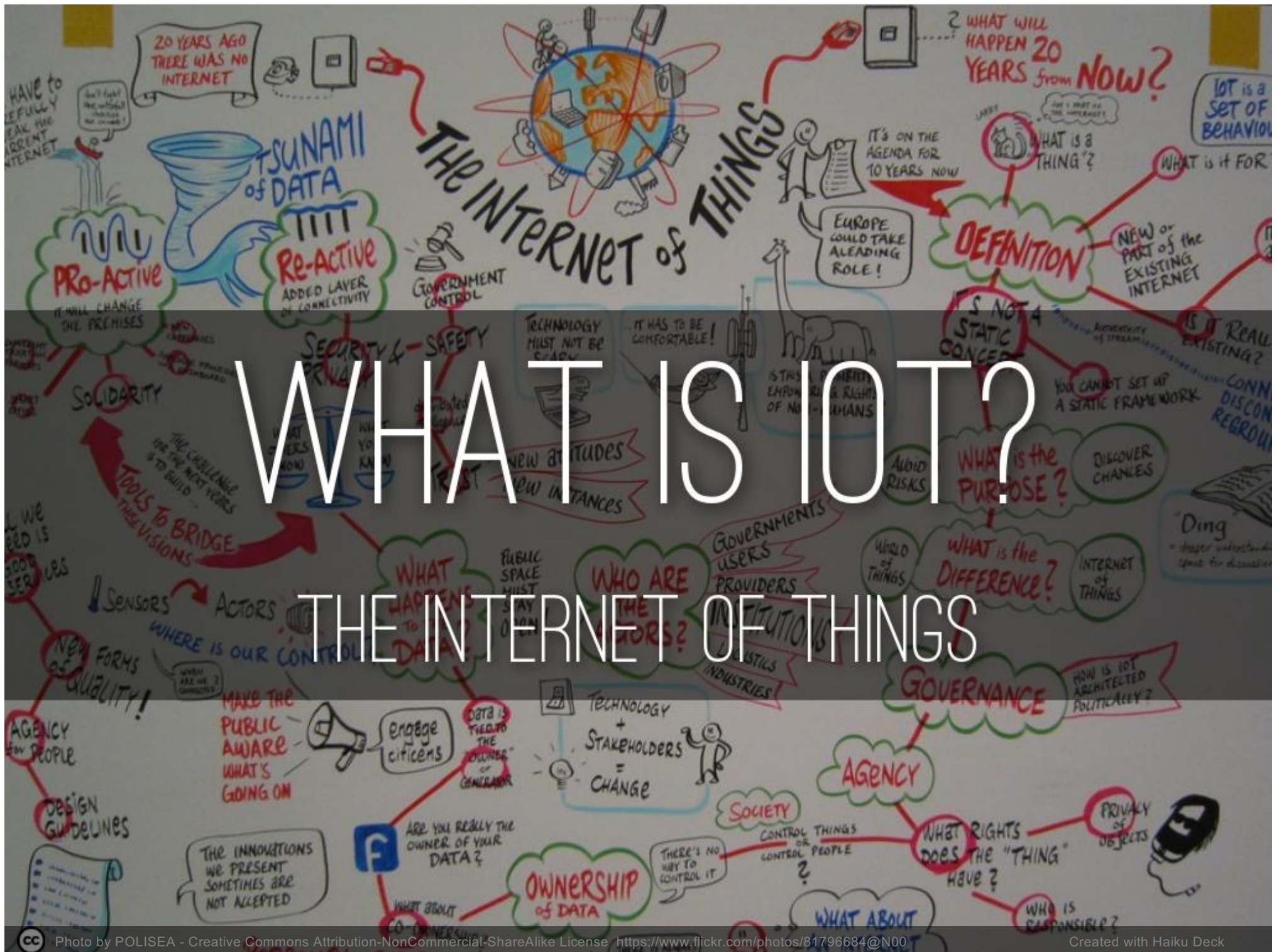


What is IoT?

The Internet of Things

WHAT IS IOT?

THE INTERNET OF THINGS



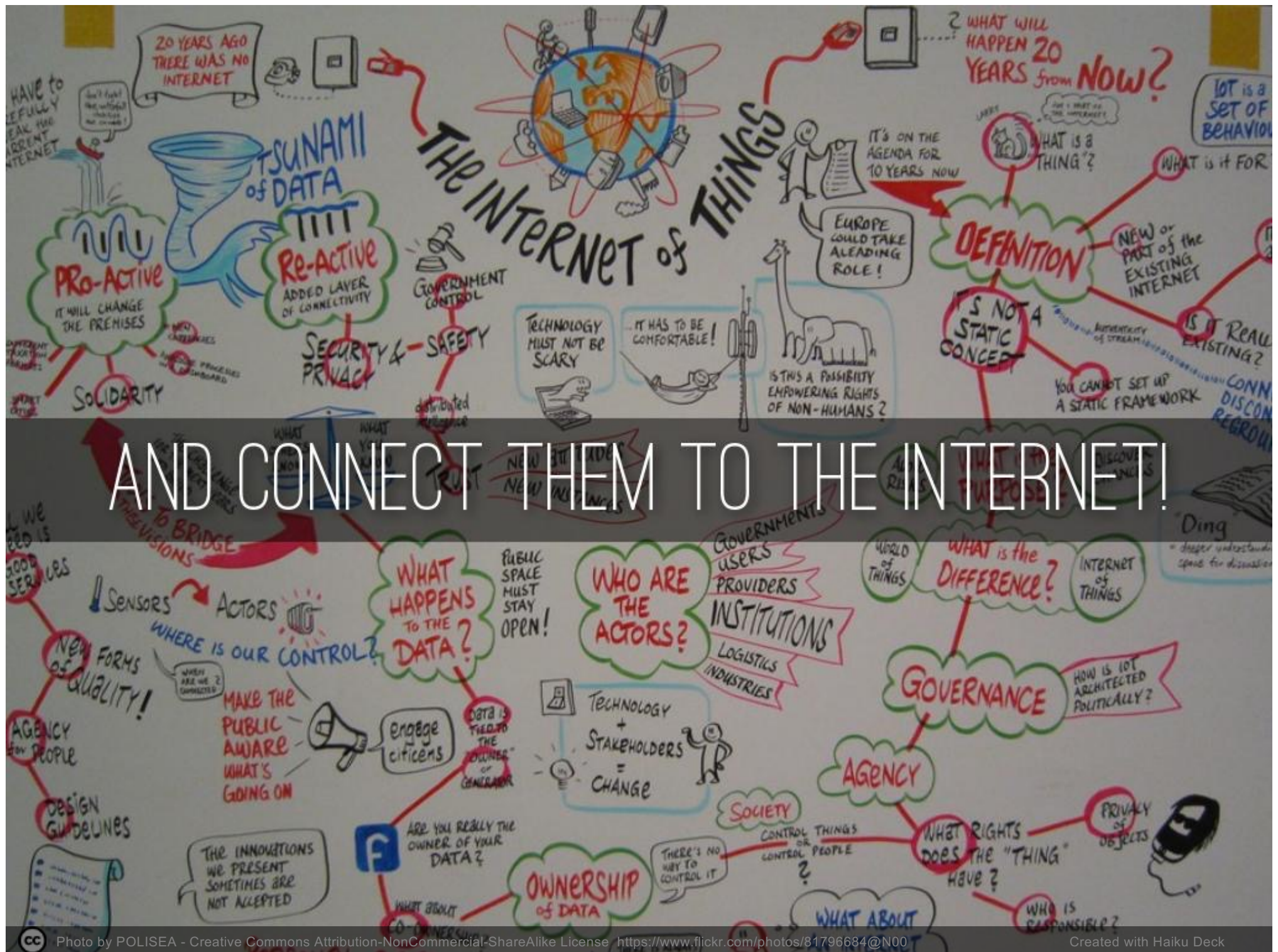
A top-down view of various electronic components laid out on a light-colored surface. In the center, there is a black battery pack with three AA batteries. To the right, an Arduino Uno micro-controller board is visible. Above it are two blue servo motors with orange and red wires. To the left of the servos are four small LEDs in blue, green, blue, and red. Below the servos are three potentiometers. In the bottom left, there are several small sensor modules, including a red one with a circular sensor and a black one with a blue potentiometer. In the bottom right, there is a black 4-digit LED display showing '0.0.0.0'. A semi-transparent dark grey banner with white text is overlaid in the center.

TAKE THESE SENSORS, MICRO-CONTROLLERS...



PUT THEM INTO "NORMAL" OBJECTS
(LIKE UMBRELLAS, DOLLS, FRIDGES, CARS...)





AND CONNECT THEM TO THE INTERNET!

A close-up photograph of a white humanoid robot, identified by its name tag as 'Pepper'. The robot has large, expressive blue eyes and a friendly, smiling mouth. It is holding a tablet computer in its right arm. The background is a blurred indoor setting with wooden paneling.

TO MAKE THEM SMART!
BUT WHAT ABOUT SECURITY?



MAJOR RISKS OF IOT

- account hijack
- data/privacy abuse
- interception/surveillance
- rogue/“zombie” devices
- supply chain/SDLC compromise
- massive botnets (e.g. DDoS)
- physical attacks
- human casualty

A photograph of a person standing on the edge of a dark, craggy rock formation. The person is silhouetted against a bright, hazy orange sky at sunset or sunrise. Below the cliff, a deep valley with forested hills is visible, shrouded in a light mist. The overall mood is contemplative and serene.

SOME EXAMPLES





MIRAI BOTNET

"SMART" CAMERAS





MIRAI SUENAGA

SMART DOLL

DESIGNED BY DANNY CHOO

CAYLA THE DOLL

SMART TOY





A photograph of a Medtronic Biotronik Cardiomesenger II Smart Pacemaker. The device is a small, rectangular, light-colored plastic unit with a clear, rounded top. It is resting on a light-colored wooden surface. The top of the device is transparent, revealing internal electronic components and a small, clear plastic cap. The Medtronic logo is visible on the front of the device. A semi-transparent dark grey banner is overlaid across the middle of the image, containing the text "BIOTRONIK CARDIOMESSENGER II" and "SMART PACEMAKER" in white, sans-serif, all-caps font. Below the main title, the serial number "SN NFD626591S" and the model number "7428" are visible on the device's surface.

BIOTRONIK CARDIOMESSENGER II

SMART PACEMAKER

A woman with long red hair, Marie Moe, is speaking on a stage. She is wearing a black jacket over a patterned top. The background is a blue screen with a circuit-like pattern. The text 'HACKING YOURSELF: MARIE MOE AND PACEMAKER SECURITY' is overlaid on the image.

HACKING YOURSELF: MARIE MOE AND PACEMAKER SECURITY

[HTTPS://YOUTUBE.BE/W1YWpVMpPi8](https://youtu.be/W1YWpVMpPi8)

Video: <https://youtu.be/W1YWpVMpPi8>



Photo by Ormintal - Creative Commons Attribution-NonCommercial License <https://www.flickr.com/photos/145819839@N03>

Created with Haiku Deck

RECOMMENDATIONS (USER)

- strong password security
- software/firmware updates
- network segmentation and filtering
- physical security
- check contracts, terms and conditions
- ! if you don't need it don't use it !



**ACCOUNT
HIJACKING**
The Digital First Aid Kit



**SECURE
COMMUNICATION**
The Digital First Aid Kit



**DDOS
MITIGATION**
The Digital First Aid Kit



MALWARE
The Digital First Aid Kit



**LOST & STOLEN
DEVICES**
The Digital First Aid Kit



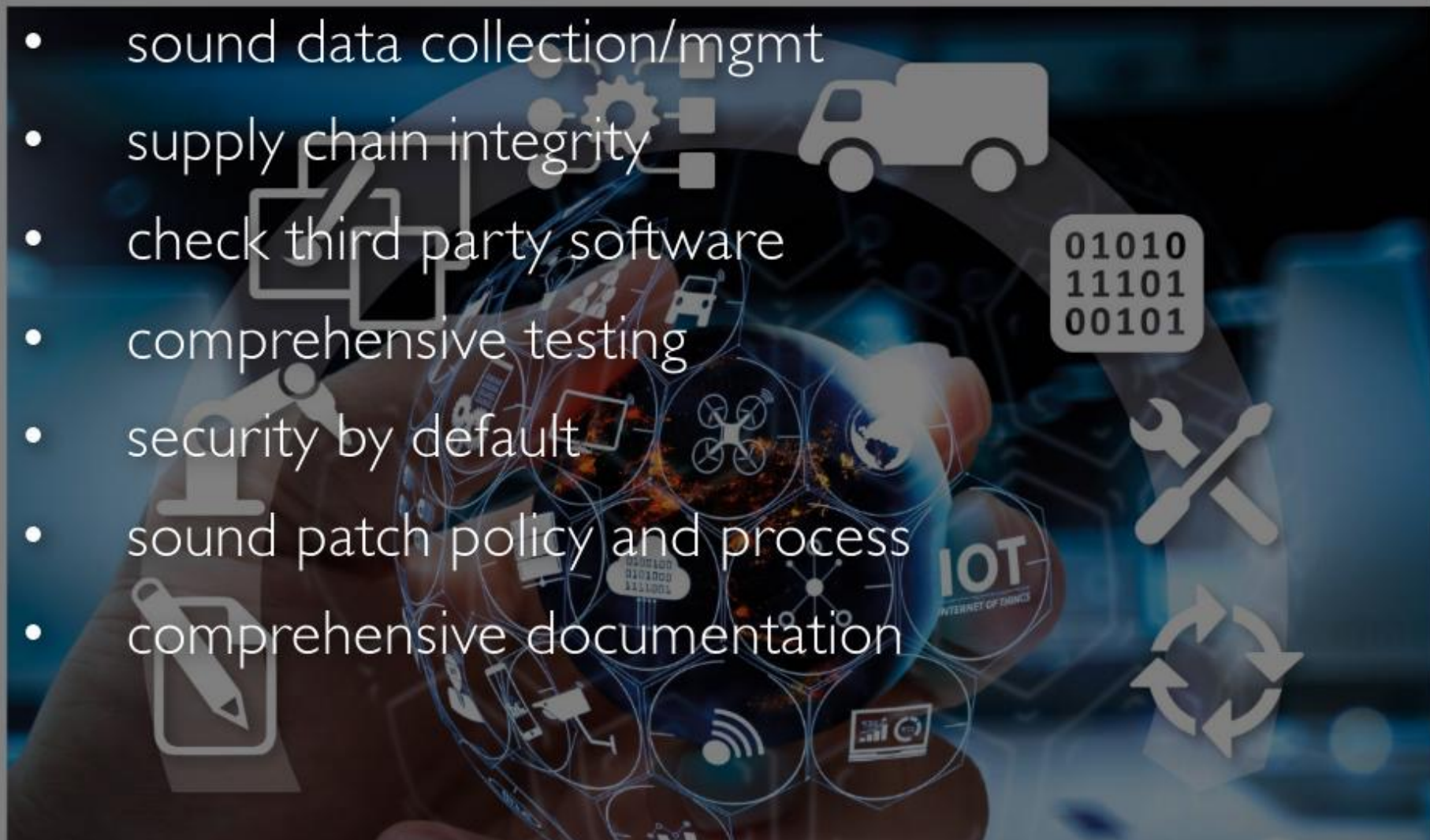
AND LAST BUT NOT LEAST
!! IF YOU DON'T NEED IT DON'T USE IT !!

RECOMMENDATIONS (PROVIDER)



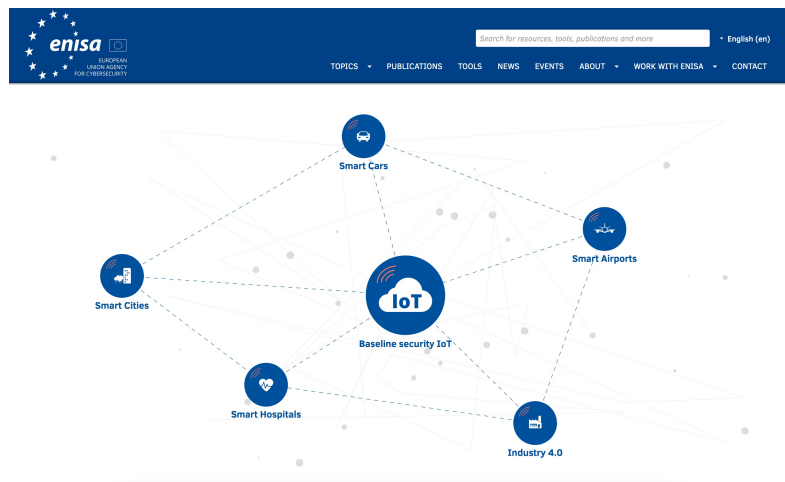
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

- security by design
- sound data collection/mgmt
- supply chain integrity
- check third party software
- comprehensive testing
- security by default
- sound patch policy and process
- comprehensive documentation



ENISA references

IoT and Smart Infrastructures Tool



Threat Landscape for Supply Chain Attacks

Threat Landscape for Supply Chain Attacks

This report aims at mapping and studying the supply chain attacks that were discovered from January 2020 to early July 2021. Based on the trends and patterns observed, supply chain attacks increased in number and sophistication in the year 2020 and this trend is continuing in 2021, posing an increasing risk for organizations. It is estimated that there will be four times more supply chain attacks in 2021 than in 2020. With half of the attacks being attributed to Advanced Persistence Threat (APT) actors, their complexity and resources greatly exceed the more common non-targeted attacks, and, therefore, there is an increasing need for new protective methods that incorporate suppliers in order to guarantee that organizations remain secure.

Published July 29, 2021
Language English

Download
 PDF document, 4.79 MB

<https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures>



SMART & SECURE

secure-iot.lu

SMART & SECURE

NATIONAL AWARENESS CAMPAIGN 2021



Smart Phone



Smart Office



Smart Home



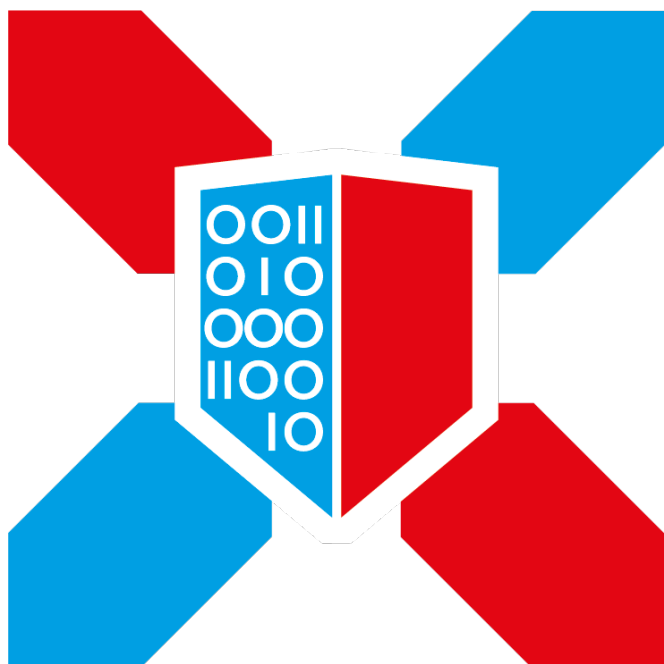
Smart Wearables



Smart Toys



WWW.SECURE-IOT.LU



CYBERSECURITY LUXEMBOURG

The Luxembourg Cybersecurity Ecosystem

*20 years of creating a culture of security
for economic and social prosperity*

— WHERE IT ALL STARTED

“I LOVE YOU” VIRUS (2000)

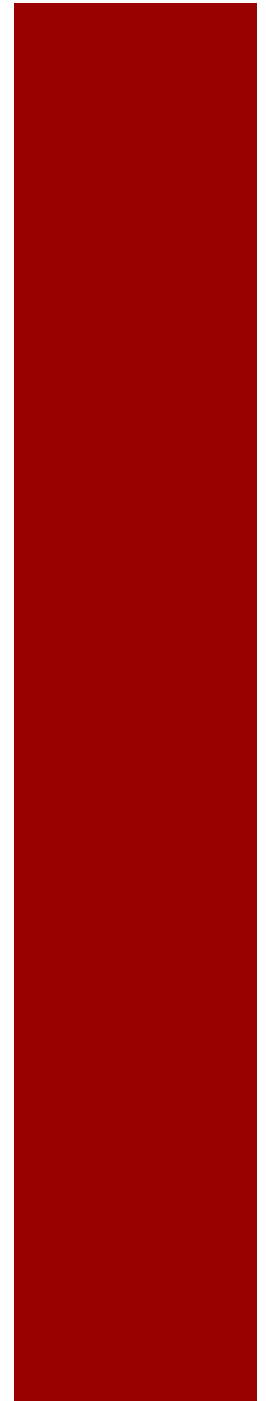


— TOWARDS A CULTURE OF SECURITY

OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS (2002)



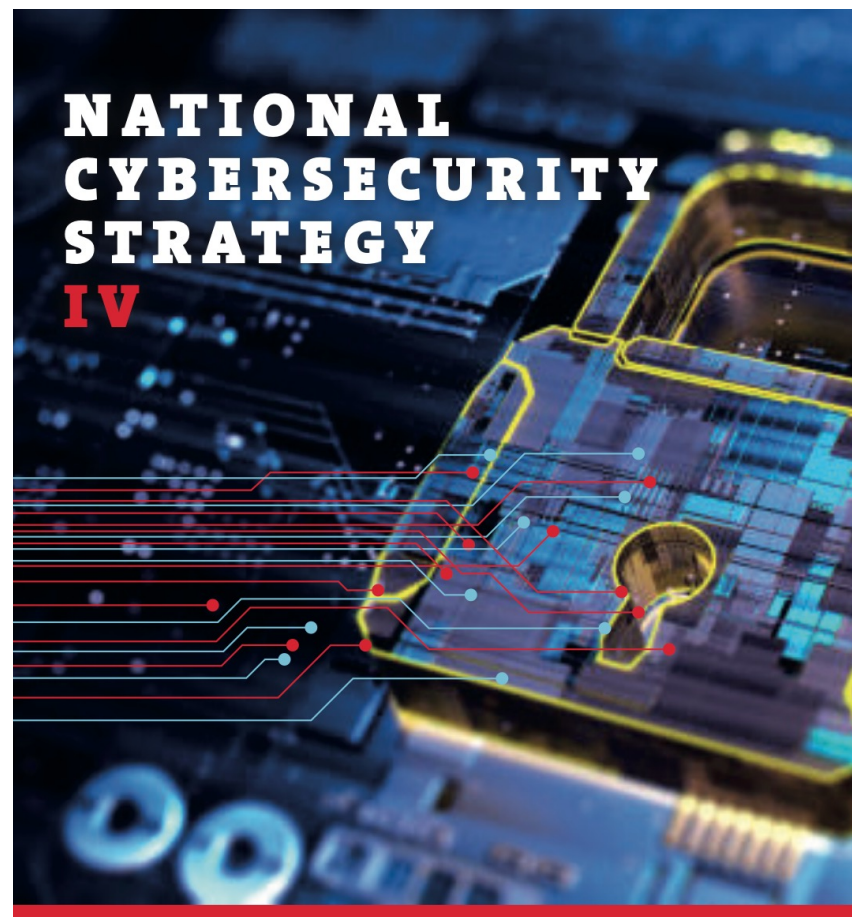
TODAY



— NATIONAL STRATEGY

2021-2025

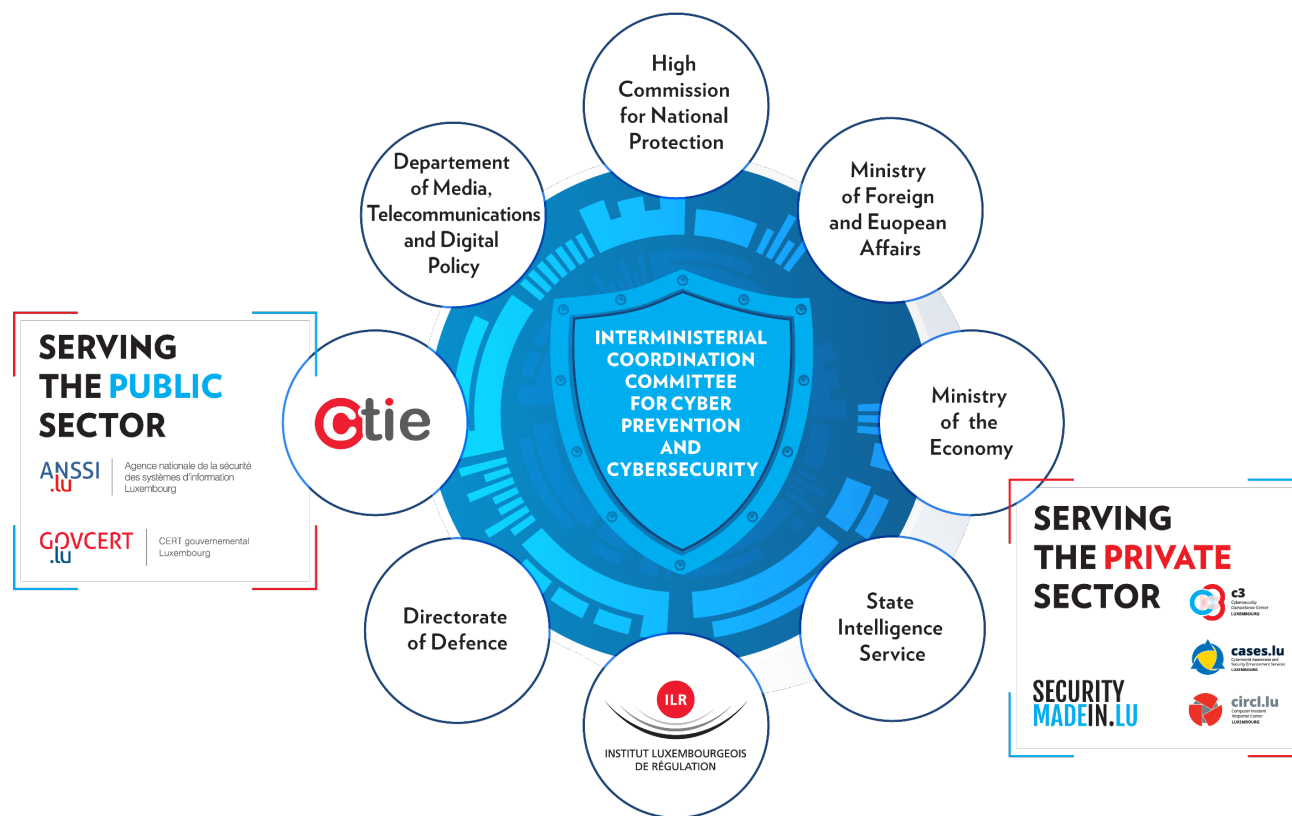
- Objectives
 1. Building trust in the digital world and protection of human rights online
 2. Strengthening the security and resilience of digital infrastructures in Luxembourg
 3. Development of a reliable, sustainable and secure digital economy
- Governance Framework
- Preparedness & Response
- Education and Awareness
- Research & Development



National Cybersecurity Strategy IV



NATIONAL GOVERNANCE



AUTHORITIES & REGULATORS

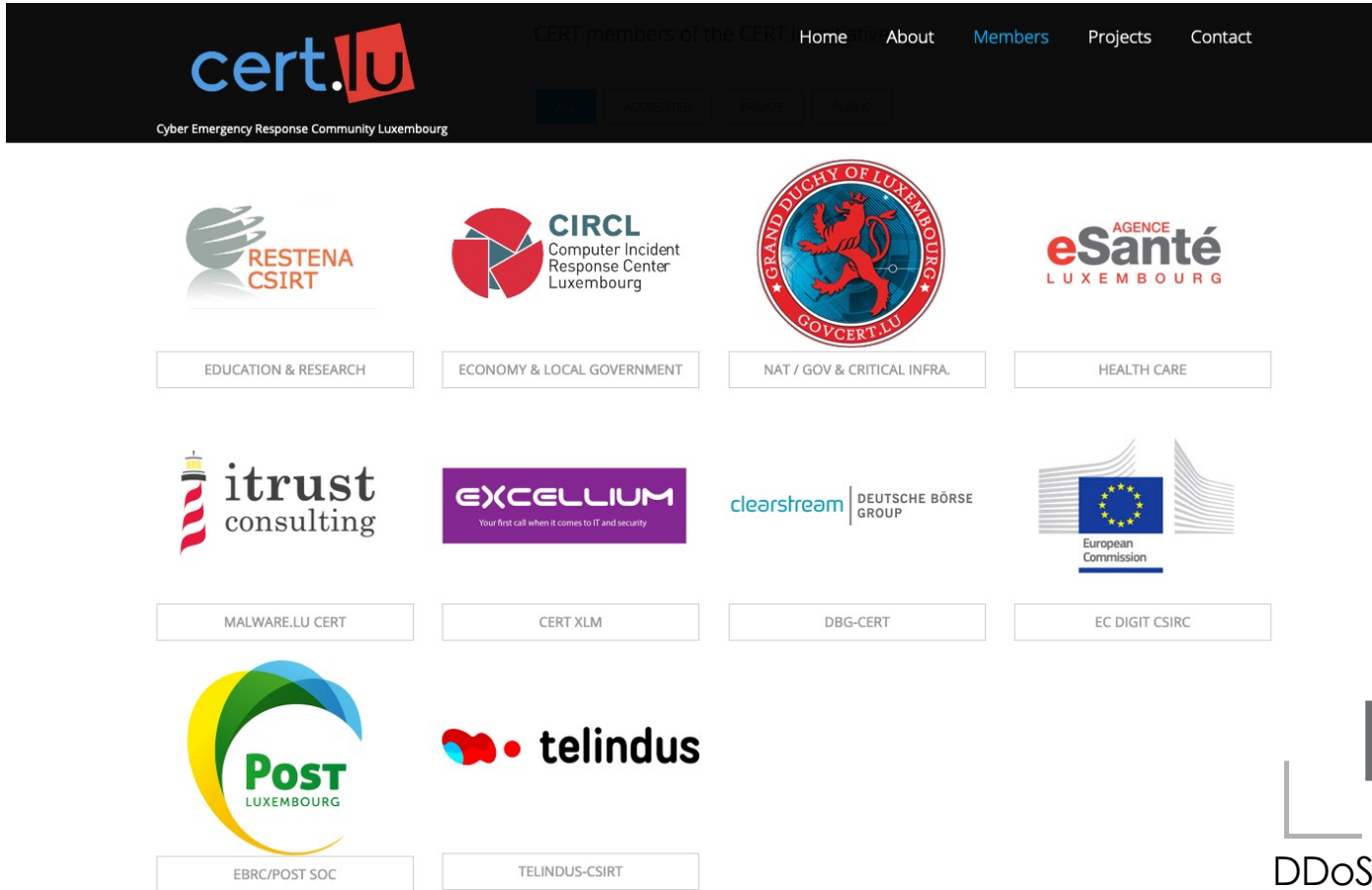


- **CIP** Critical Infrastructure Protection
(loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale)
- **GDPR** General Data Protection Regulation
(loi du 1er août 2018 portant mise en place du régime général sur la protection des données)
- **NIS** Network and Information Security
(loi du 28 mai 2019 portant transposition de la directive NIS)
- **PSDC** Prestataires de Services de Dématérialisation ou de Conservation
(loi du 25 juillet 2015 relative à l'archivage électronique)
- **PSF** Professionnels du Secteur Financier de Support
(loi modifiée du 5 avril 1993 relative au secteur financier)



— PREPAREDNESS & RESPONSE

PUBLIC-PRIVATE COOPERATION IN ACTION



The screenshot displays the cert.lu website, which lists various members of the Cyber Emergency Response Community Luxembourg. The members are organized into a grid, each with a logo and a label for their sector or role.

Member Logo	Sector / Role
RESTENA CSIRT	EDUCATION & RESEARCH
CIRCL Computer Incident Response Center Luxembourg	ECONOMY & LOCAL GOVERNMENT
GOVCERT.LU (Grand Duchy of Luxembourg)	NAT / GOV & CRITICAL INFRA.
eSanté LUXEMBOURG	HEALTH CARE
itrust consulting	MALWARE.LU CERT
EXCELLIUM	CERT XLM
clearstream DEUTSCHE BÖRSE GROUP	DBG-CERT
European Commission	EC DIGIT CSIRC
Post LUXEMBOURG	EBRC/POST SOC
telindus	TELINDUS-CSIRT

On the right side of the grid, there is a logo for **LU-CIX** with the text **DDoS Scrubbing Center** below it.



— EDUCATION & RESEARCH



ECOSYSTEM

-> WWW.CYBERSECURITY.LU

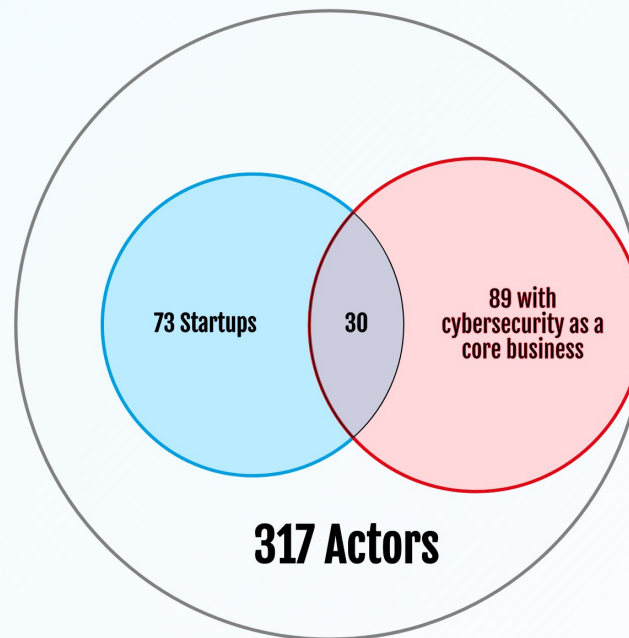
COMPANIES

89 Companies With
Cybersecurity As A Core
Business

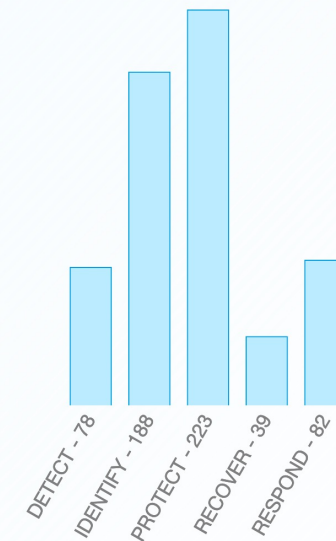
900
Total employees

32
Created during the last 5 years

30
Start-ups



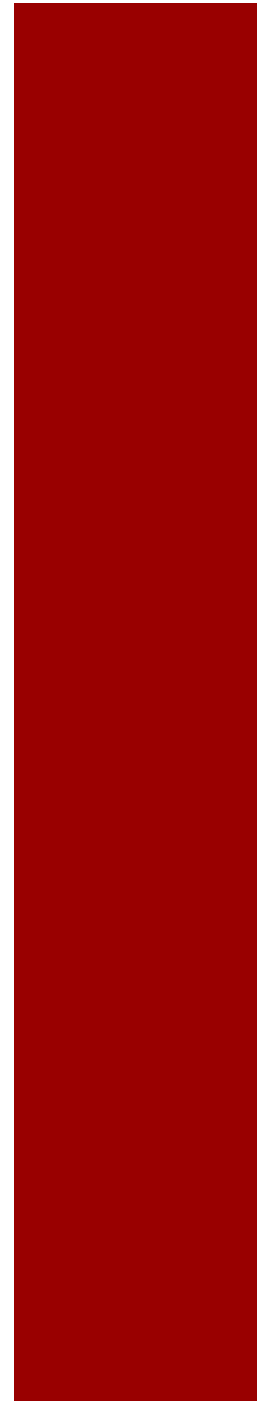
Diversified Solutions



Go back



Protecting the private sector



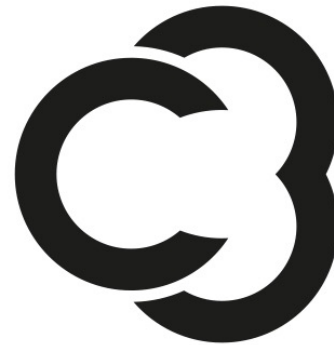
SECURITY MADEIN.LU



circl.lu



cases.lu



c-3.lu

— COMPUTER INCIDENT RESPONSE CENTER LUXEMBOURG

DFIR

- Incident Coordination and Incident Handling
- Incident Handling Support Tools and Services
 - **URL Abuse** - to check and review security of URLs
 - **cve-search** - Common Vulnerabilities and Exposures (CVE) web interface and API
 - **Passive SSL** - historical database of SSL certificate per IP address
- Projects and Software
 - Early Detection Network – **map.circl.lu**
 - **AIL** - Framework for Analysis of Information Leaks
 - **BGP Ranking**

BY SECURITYMADEIN.LU



circl.lu
Computer Incident
Response Center
LUXEMBOURG



Malware Information Sharing
Platform (MISP) and Threat
Sharing Platform



Dynamic Malware Analysis
Platform (DMA)



Clean documents from untrusted
USB keys / sticks



Database storing historical DNS
records



— CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT SERVICES

GRC

- Awareness Raising and promotion of best practices
- Democratisation of security for SMEs
- Supporting CISOs
- Organisational Security Tools
- Knowledge base of good practices

BY SECURITYMADEIN.LU



cases.lu

Cyberworld Awareness and
Security Enhancement Services
LUXEMBOURG



Startup Kit

The essential for a good start
in information security



MONARC

Governance of
information security



Diagnostic

Check-up on your
information security



Training

An introduction to
information security



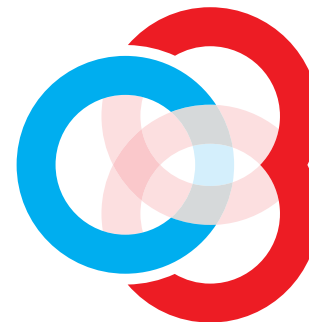
— CYBERSECURITY COMPETENCE CENTRE

HMI

- Threats and Vulnerabilities Observatory
- Testing facility
 - -> testing.c3.lu
- Training Centre



BY SECURITYMADEIN.LU



c3

Cybersecurity
Competence Center
LUXEMBOURG



Thank you
for your attention

Questions ?