clusil/

INFORMATION / SECURITY / LUXEMBOURG

IOT & Regulation

Jean Goetzinger
Président du CLUSIL
jean.goetzinger@clusil.lu
www.clusil.lu

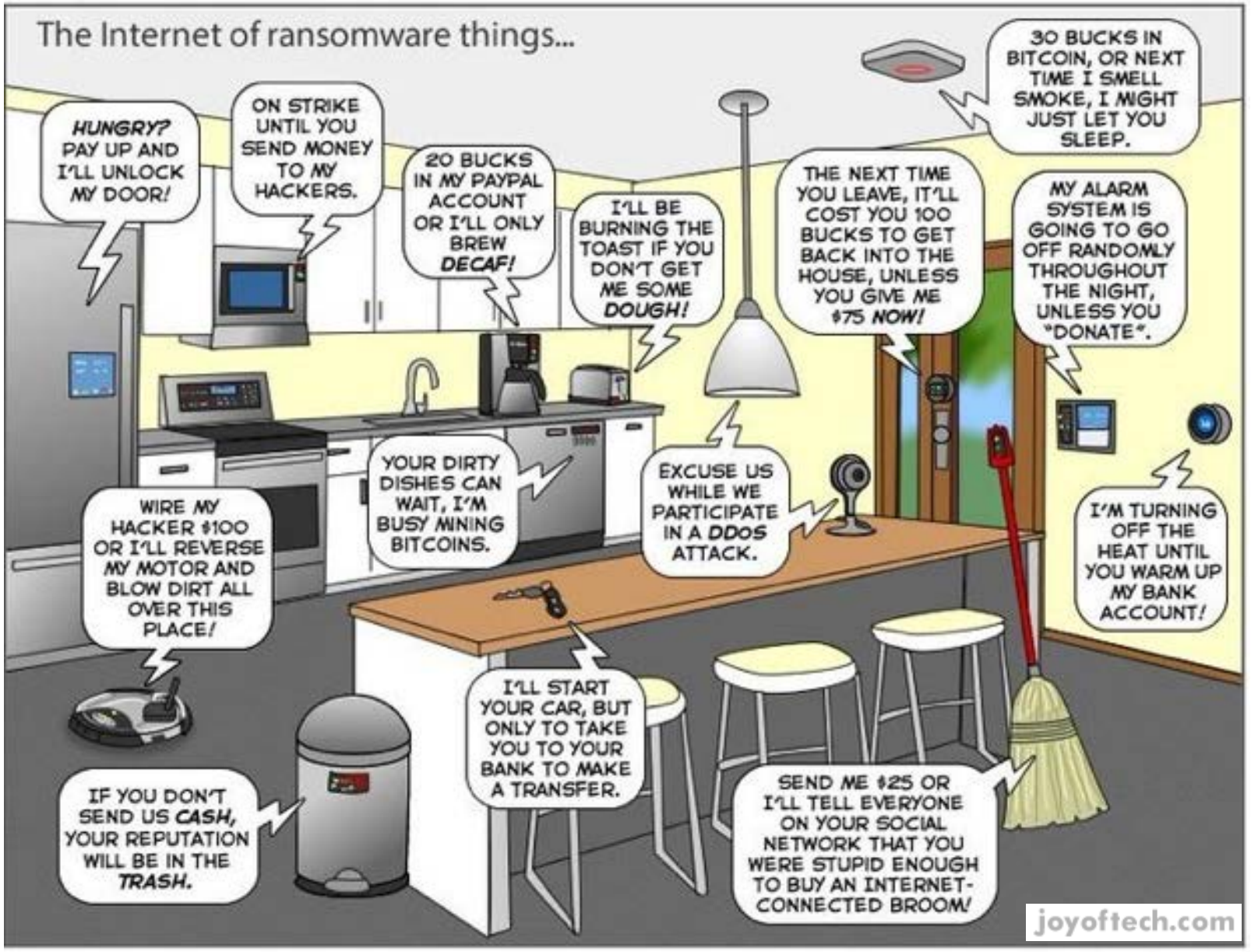
Agenda

- What is Internet of Things ?
- Some Security Aspects
- IOT and Regulatory Issues
- Recommendations
- Questions & Answers

Introduction

The **Internet of Things** (**IoT**) refers to the ever-growing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems.

Introduction



I Am The Cavalry

We believe that our dependence on computer technology is increasing faster than our ability to safeguard ourselves.

New: How IoT is "different"

Aspect	Descriptions
Adversaries	Different adversaries with different motivations and capabilities
Consequences of Failures	Life & Limb, Physical Damage, Market Stability/Confidence, National Security
Context & Environment	Operational contexts can be quite different. Migratory, Perimeter-less, Inaccessible, Difficult to patch/replace
Composition of Goods	Differences in Hardware, Firmware, Software stacks
Economics	Margins, Buyers, Investors, Costs of Goods, etc
Time Scales	Time-to-Live (TTLs), R&D Cycles, Response Times

https://www.iamthecavalry.org/

Introduction

clusil
INFORMATION / SECURITY / LUXEMBOURG

'There will be as many as

40 TO 80 BILLION

connected objects by 2020.

There will be **10** connected objects for every man, woman, and child on the **PLANET.**

Through the power of smart devices, people will not only consume data, but contribute observed data to the IoT through their phones and tablets as

human sensors

Examples of IOT

- Smart Home
- Smart Cities
- Smart Devices
- Wearables

- Automobiles
- Transport Systems
- Manufacturing
- Smart Metering
- eHealth

Security Considerations

Dyn estimated that the attack had involved '100,000 malicious endpoints', and the company said there had been reports of an extraordinary attack strength of 1.2 terabits (1,200 gigabytes) per second. Photograph: Alamy

The market can't fix this because **neither the buyer nor the seller cares**.

IOT Expands Security Needs

Converged Managed Network

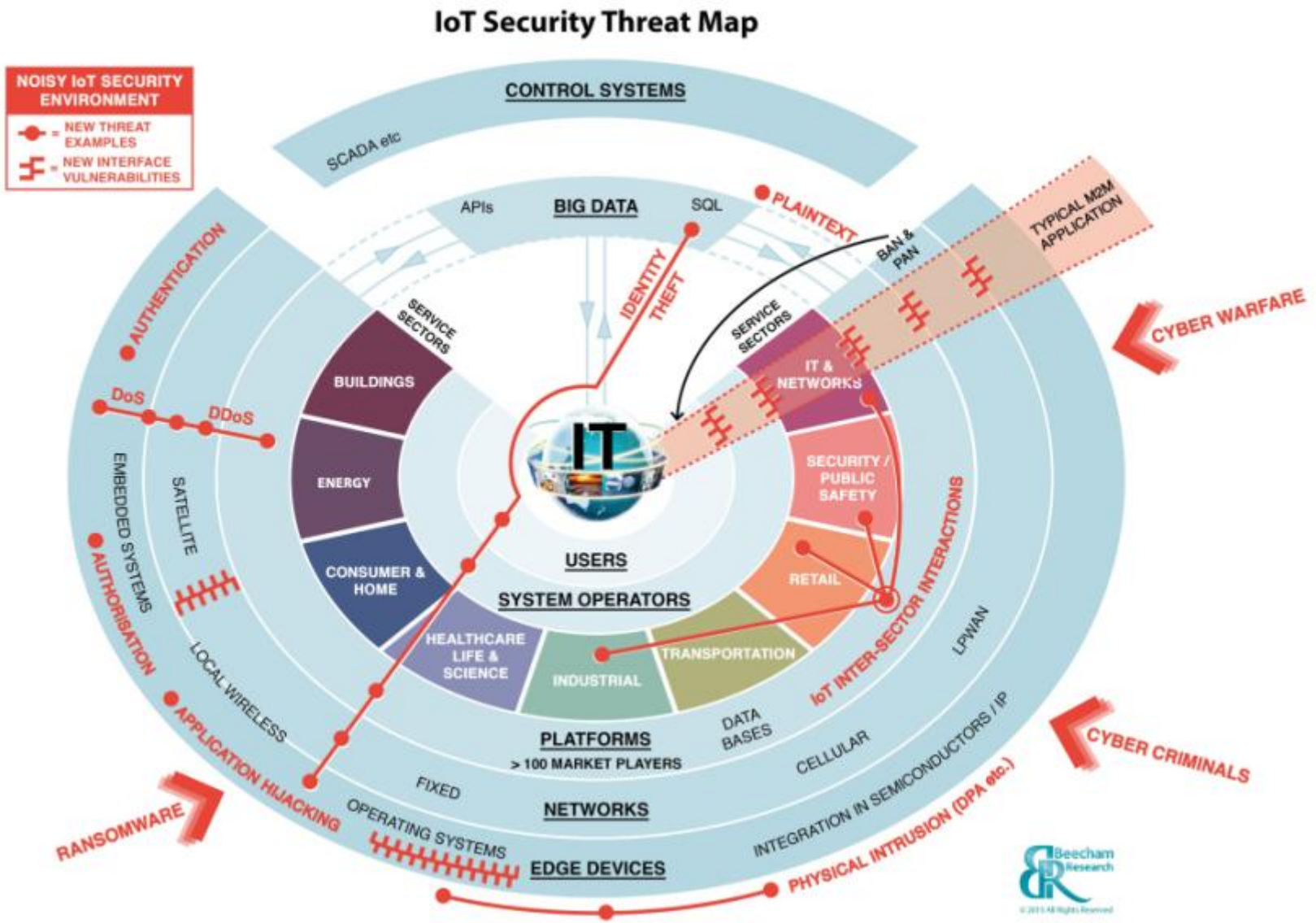
Resilience at scale

Security

Distributed Intelligence

Application Enablement

Security Considerations



Regulatory Issues

✓ Licensing and spectrum management

Ensure spectrum is available for a wide range of IoT applications, at short and long range, in licensed and unlicensed bands.

✓ Switching and roaming

Encourage development of SIMs and mobile network accounts suitable for large M2M users, roaming mobile devices, and fixed devices in areas of poor reception

✓ Addressing and numbering

Large address space needed for globally addressable things

✓ Competition

Ensure competition regulators have capability to monitor IoT markets for abuses of dominant positions. Provide institutional mechanism for ongoing review of laws and regulations for impact on IoT competitiveness.

✓ Security and privacy

Security and Privacy

Goal

- ✓ Significantly reduce security vulnerabilities in IoT systems,
- ✓ Encourage security and vulnerability patching of devices.
- ✓ Smart city vulnerabilities can be hard to fix due to legacy systems, but present significant safety issues (e.g. in traffic lights).
- ✓ Ensure individual control of profiles, which can be used to infer sensitive personal information, such as medical disorders.
- ✓ Reduce potential for discrimination in employment, financial and healthcare services.

Best practice

- ✓ Ensuring security and privacy from outset of IoT system design process.
- ✓ Development of co-regulation by all stakeholders to protect security and privacy.
- ✓ Further development of privacy and consumer protection rules to ensure security testing of IoT systems that process sensitive personal data.

Security and Privacy Measures

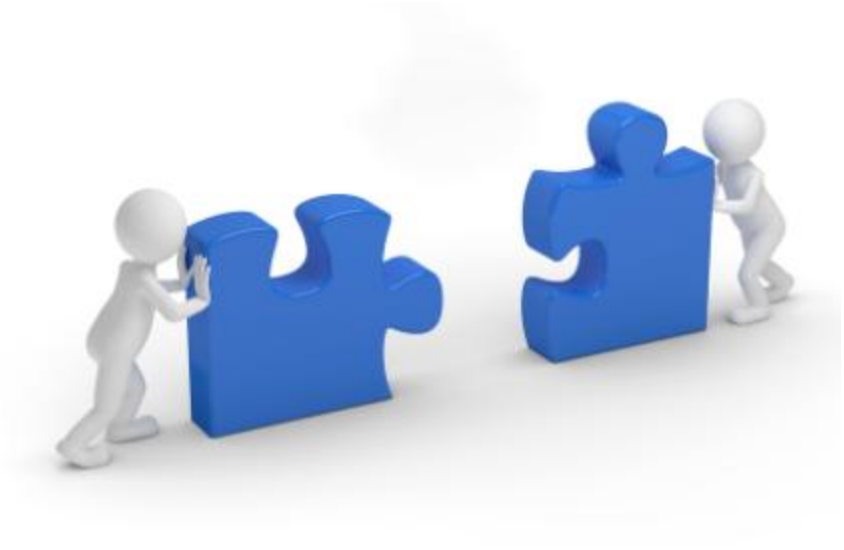
- ✓ Incorporate Security at the Design Phase
- ✓ Promote Security Updates and Vulnerability Management
- ✓ Build on Recognized Security Practices
- ✓ Prioritize Security Measures According to Potential Impact
- ✓ Promote Transparency across IoT
- ✓ Connect Carefully and Deliberately
- ✓ Development of further guidance for privacy requirements
  - ✓ PIA, data minimisation,
  - ✓ Collaboration telecoms and DP agencies

OWASP Top 10

- ✓ Insecure Web Interface
- ✓ Insufficient Authentication/Authorization
- ✓ Insecure Network Services
- ✓ Lack of Transport Encryption
- ✓ Privacy Concerns
- ✓ Insecure Cloud Interface
- ✓ Insecure Mobile Interface
- ✓ Insufficient Security Configurability
- ✓ Insecure Software/Firmware
- ✓ Poor Physical Security

All elements need to be considered

- ✓ The Internet of Things Device
- ✓ The Cloud
- ✓ The Mobile Application
- ✓ The Network Interfaces
- ✓ The Software
- ✓ Use of Encryption
- ✓ Use of Authentication
- ✓ Physical Security
- ✓ USB ports



Regulations

- Data Protection and Privacy
- Communications Law
- Cyber Security
- Cybercrime
- Intellectuel Property Law
- Consumer and product liability law

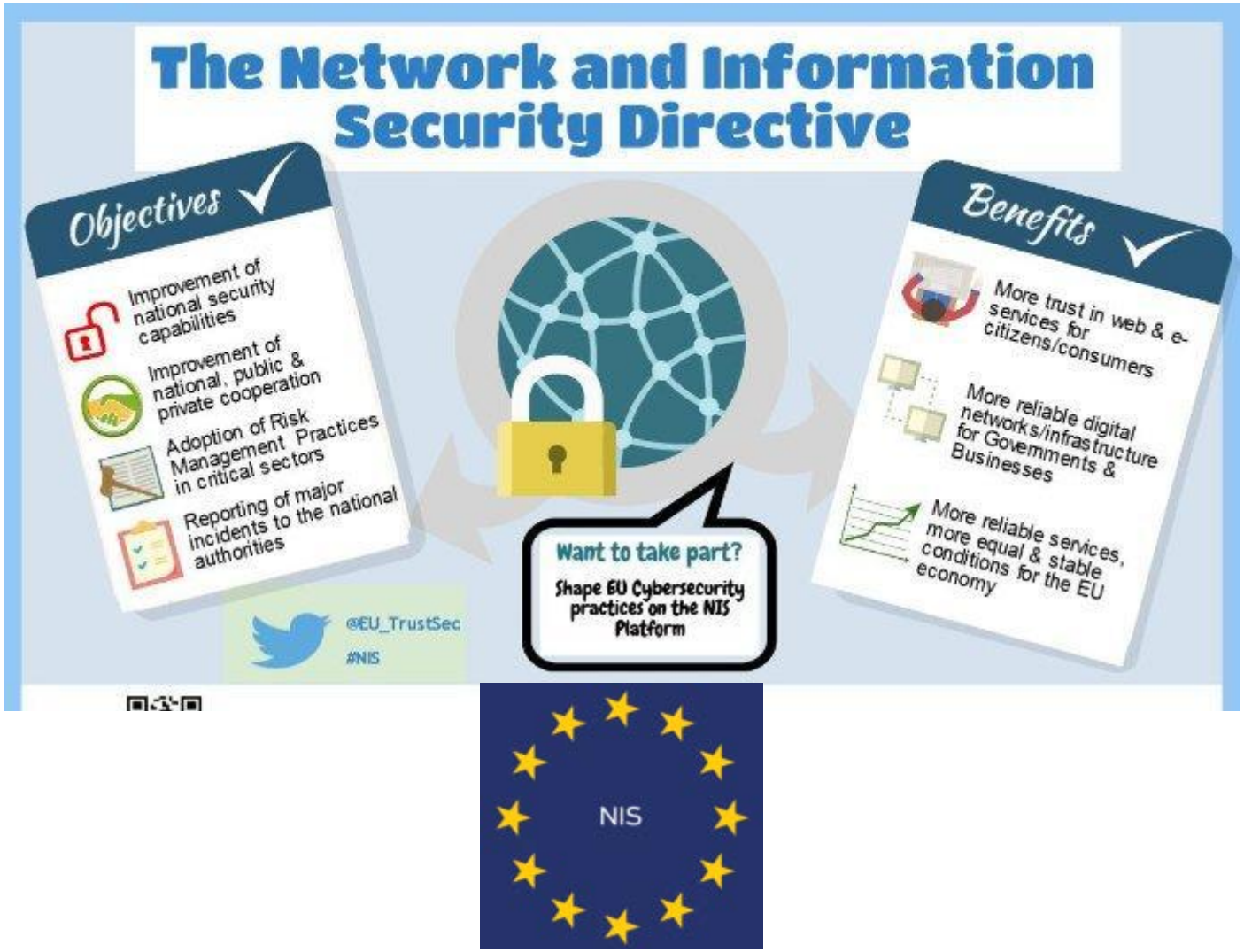
Regulations

clusil
INFORMATION / SECURITY / LUXEMBOURG

General Data Protection Regulation

Stricter Consent Req.
Privacy by Design
Privacy by default
Data Portability
Encryption, anonymisation

Regulations



Regulations

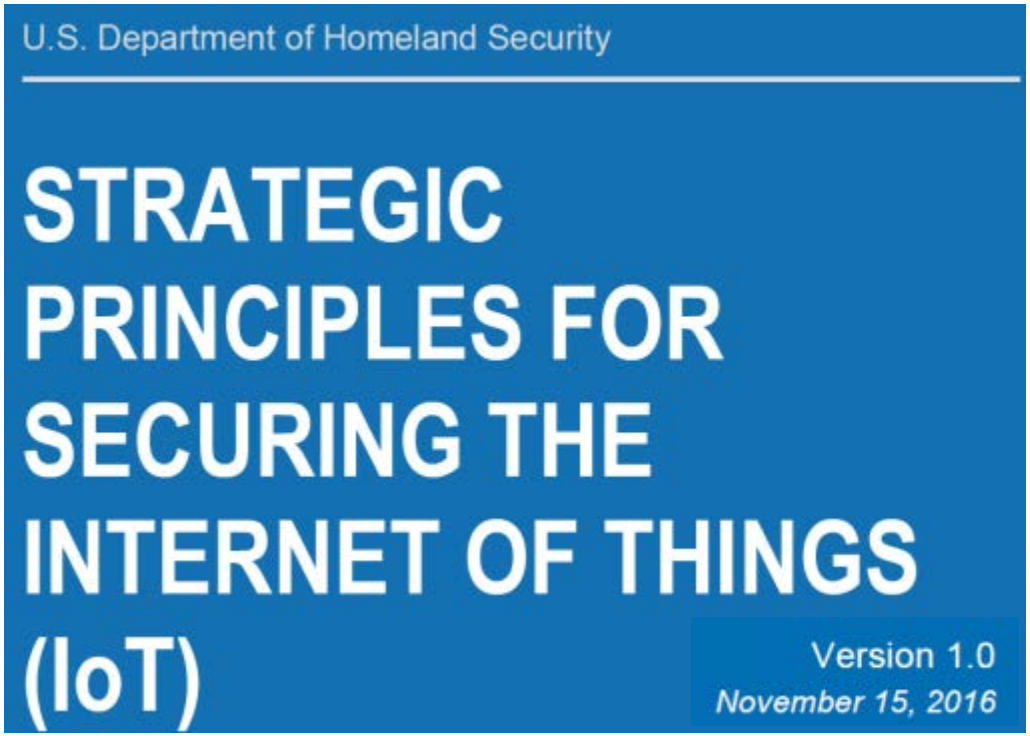
AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

The overall goal of the establishment of the AIOTI is the creation of a dynamic European IoT ecosystem to unleash the potentials of the IoT. This also offers an opportunity to discuss policy obstacles to further IoT take up, and to forge consensus.

WG4 makes Policy recommandations on:

- *Privacy*
- *Security*
- *Liability*
- *Net Neutrality*

Regulations



Homeland Security

Prioritizing IOT Security

Regulations

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

establishing the European Electronic Communications Code

- **Increased competition**
- **Stronger Consumer Protection**
- **Better use of radio frequencies**
- **A safer online environment**

Body of European Regulators for Electronic Communications

BEREC

Modernisation of current telecoms rules to drive investment !

Regulations

Thank You