



Smart Energy 2017, Halden, Feb 2017

Industrial view - Smart Grid Security Centre

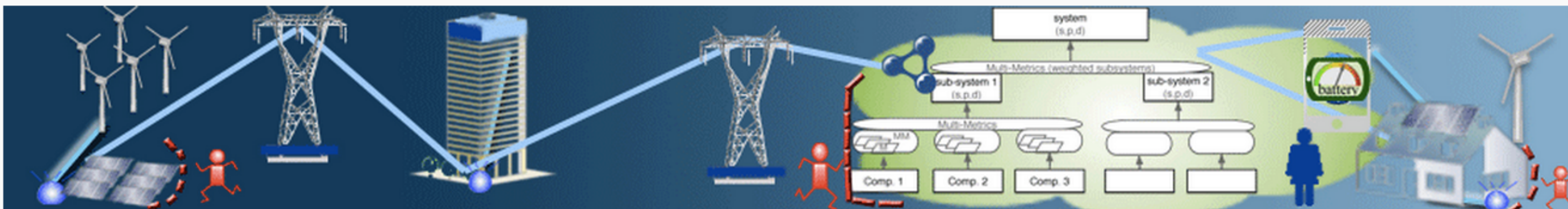
Otto Rustand
Glitre Energi Nett
IoTSec Security Officer
otto.rustand@glitreenerginett.no

National initiative for a more secure future in IoT

IoTSec.no - Security for IoT for Smart Grids

[Home](#) [Research Areas](#) [Security Centre](#) [Publications](#) [About us](#)





The **IoTSec - Security in IoT for Smart Grids** initiative was established in 2015 to promote the development of a safe and secure Internet-of-Things (IoT)-enabled smart power grid infrastructure. The [Research Project](#) received funding from the [Research Council of Norway](#) (RCN) to contribute to a safe information society.

IoTSec addresses the basic needs for a reliable and efficient, uninterrupted power network with dynamic configuration and security properties. It addresses in addition the needs of businesses and end users of additional IoT services by exploring use cases for value-added services with the intent to design the building blocks for future services that consider the necessary security and privacy preconditions of successfully deployed large-scale services. IoTSec will apply the research in the envisaged Security Centre for Smart Grids, co-located with the Norwegian Centre of Excellence (NCE Smart).

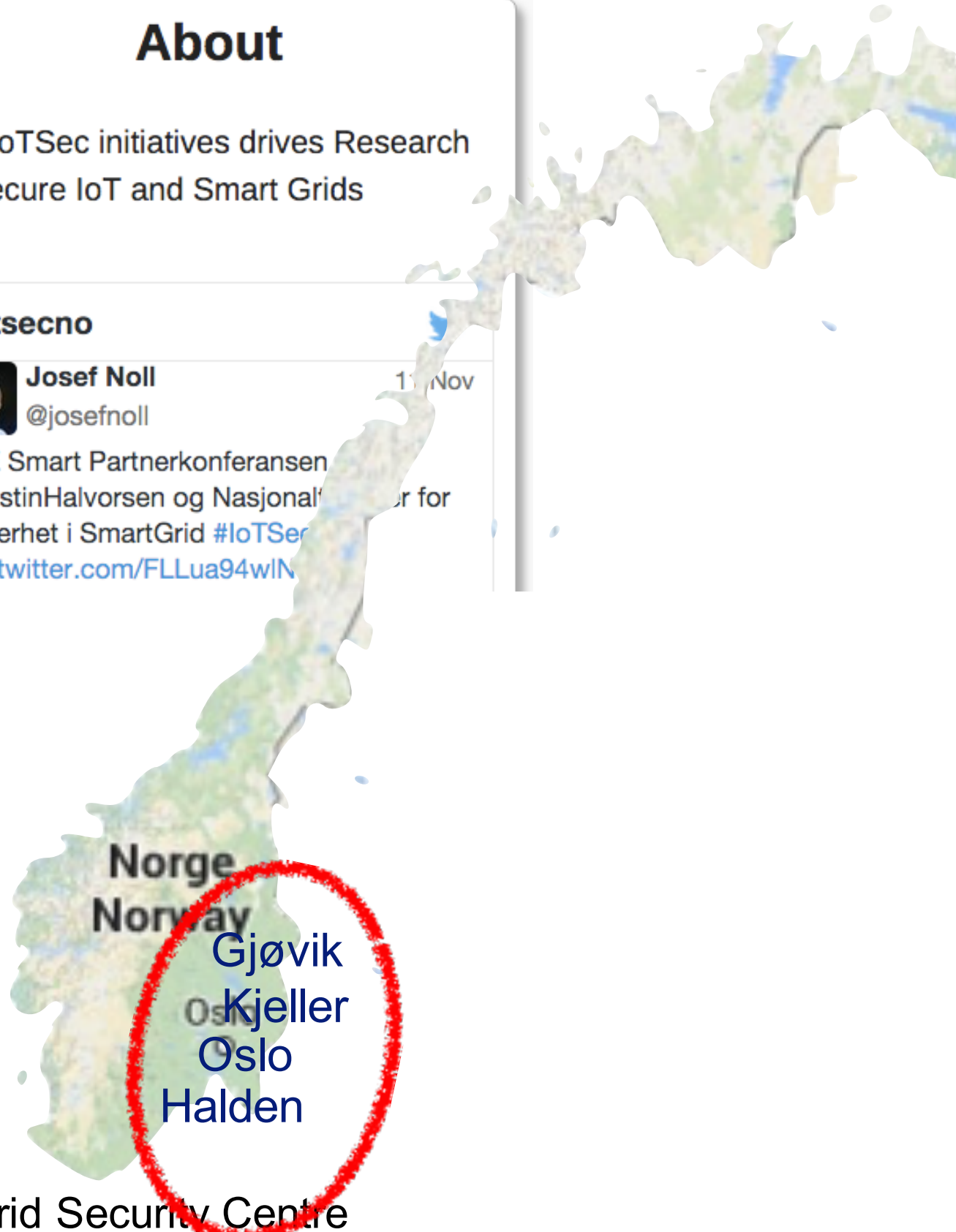
About

The IoTSec initiatives drives Research for secure IoT and Smart Grids

#iotsecno

**Josef Noll**
@josefnoll
11 Nov
NCE Smart Partnerkonferansen
@KristinHalvorsen og Nasjonal
Sikkerhet i SmartGrid #IoTSec
pic.twitter.com/FLLua94wIN

«Open World Approach»
everything that is not declared closed is open



Partners and Collaborations

- UiO
- UNIK
- NR
- Simula
- NTNU

Academia

- Smart Innovation Østfold
- eSmart Systems
- Fredrikstad Energi
- EB Nett
- Movation

Industry

- Smartgrid Centre
- Norw. Data Protection Auth.
- Forbrukerrådet

Interest Org.

- EyeSaaS
- mnemonic

Industry

- Mondragon Unibersitatea
- University of Victoria
- Universidad Carlos III
- La Sapienza
- COINS Research School
- Nimbeo
- H2020 and ECSEL projects

International

Handling of Confidential and security-critical material

Retningslinjer på

http://cwi.unik.no/wiki/loTSec-Secure_and_Confidential_information

Confidential information [edit]

- Documents which are given to the project being confidential to the project shall be watermarked by *IoTSec confidential, shall not be distributed outside of the project without consent*
- Deliverables being confidential shall be stored on the project server, e.g. owncloud.unik.no

Security-critical information [edit]

Each project participant is asked to not publish security-critical information. If a participant regards information as potentially security-critical, he shall ask IoTSec's security officer for advice.

We have to follow the rules from NVE, outlining the rules and regulations, see [Action Item to address NVE rules and regulations](#). The rules include a.o. a non-disclosure agreement for certain information.

Security critical information shall be watermarked "security-critical - do not distribute", and shall only be given to project partners on request. The distribution shall be noted to our COO ([Christian Johansen](#)), who keeps a list of the documents and whom they have been distributed to.

The IoTSec security officer is [Otto Andreas Rustand](#), ask him for advice.

grid

1. Next-generation energy storage: the project at glance

World's population is increasing and with it the amount of energy needed. Today's confluence of challenges – rapidly escalating global energy demands and wide access to energy sources – demand innovative way of thinking to forge a pathway to a sustainable energy future. According to recent projections, in order to achieve climate change targets of 80-90 percent reduction of the greenhouse gas carbon dioxide from the power sector, Europe is aiming to increase to 90 % or more the penetration of renewable energy in 2050. With the current state of electricity distribution grid, the new scenario would require a significant transmission lines addition (so called grid extension) in order to spread resources over large areas. This will have a strong impact on our landscape and will not solve the problem of energy loss during transmission from alternating to direct current (AC/DC). Beyond penetrating 90%, the variable renewable supply and demand will impose increasing scientific challenges and will require additional enabling technologies such as energy storage.

The last decades the scientific community focused on developing Li-ion batteries for portable and vehicular applications, due to their high energy and power capabilities. However, concerns are getting over Li availability facing a future demand for batteries with requirements different than the portable electronics, for example for large scale applications such as the electricity grid. Finding the energy grid will require innovative ideas for energy storage systems and huge breakthroughs in materials discovery.

In the present proposal, I suggest an innovative concept of how the future grid could be. My vision is decentralizing the energy generation and distribution, where the electricity produced through renewable sources by a single house, or neighborhood consortium, could be stored in a novel couple of stationary batteries able to exchange electricity and information with the grid in an "intelligent" manner. Thus, the main aim of the current proposal is to develop Na-ion based batteries for stationary storage device for integration of renewable energy in smart-grid applications. The new battery will use inorganic nanotubes and porous nano-composites to house the electrodes better in terms of energy capacity than other existing batteries. The choice of sodium, instead of lithium addresses the availability and toxicity issues of the materials. Additionally, the new proposed storage device will require modeling the security and the exchange of information with the grid along the type of renewable energy used, the energy capability of the network, and the profile usage of the clients.

To achieve this, three main hypotheses are put forth:

1) Sodium can replace lithium in next-generation energy storage materials for large scale applications
2) Nanocomposites architectures in the electrodes in the form of nanoconfined materials and inorganic nanotubes will enhance the mass diffusion and electron transfer increasing the accessibility of the active material

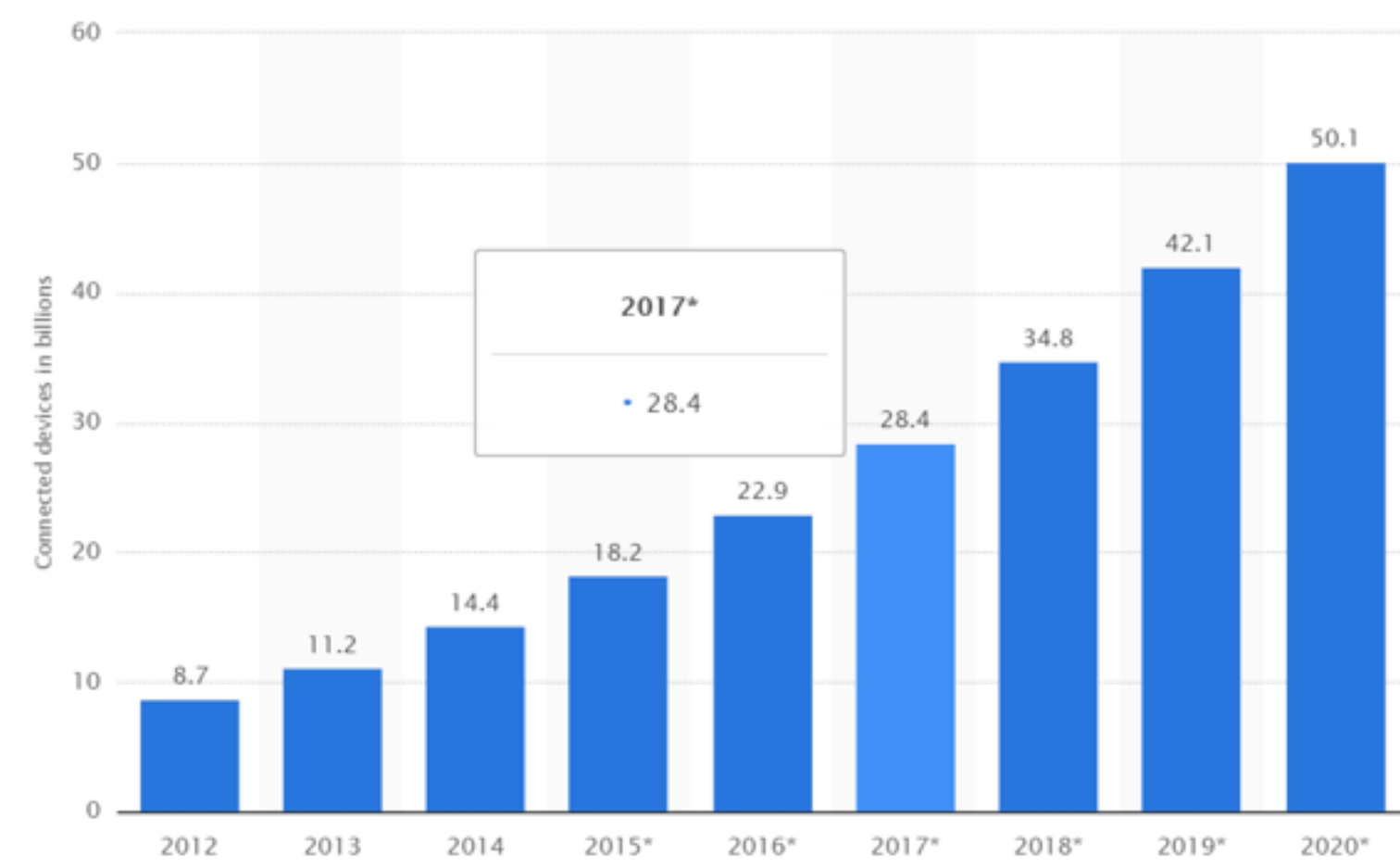
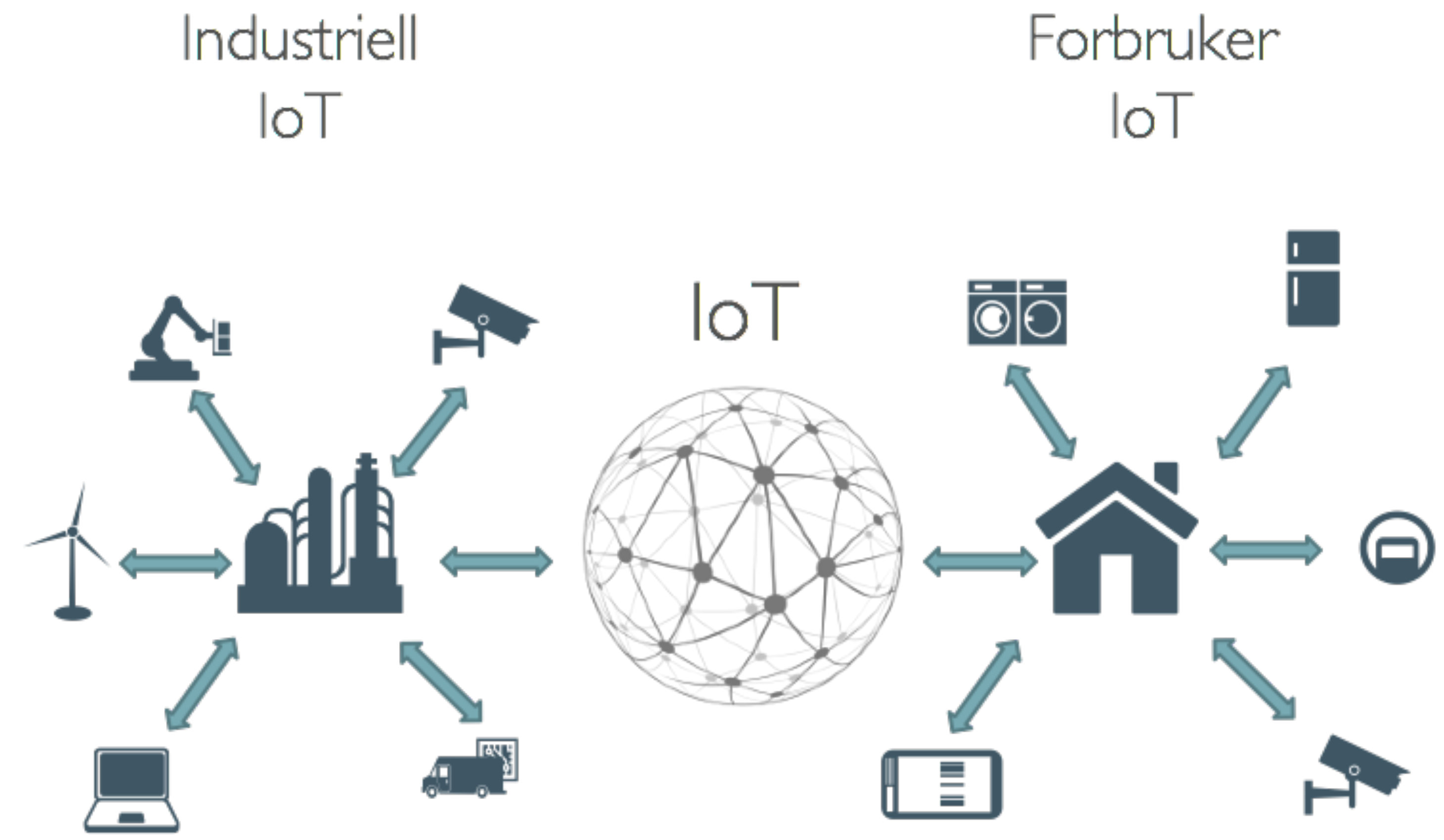
3) Future grid will allow a higher penetration of renewables and empowering consumers through energy storage units. A new communication system between the storage units/customers and the grid will allow an increase flexibility of the grid and protection of private information.

In the next pages I will explain how these hypothesis will be tested. But first I will describe shortly how SmartStorage fits into the bigger picture of global energy demands.

2. Future growth in demand of wind and solar photovoltaic energy means growing need of storage capacity

A fundamental challenge to significantly integrating renewable-generated power sources – such as wind and sun – into the electric grid is their inherent variability. This challenge makes electricity storage critical and, I believe, the next frontier in energy infrastructure.

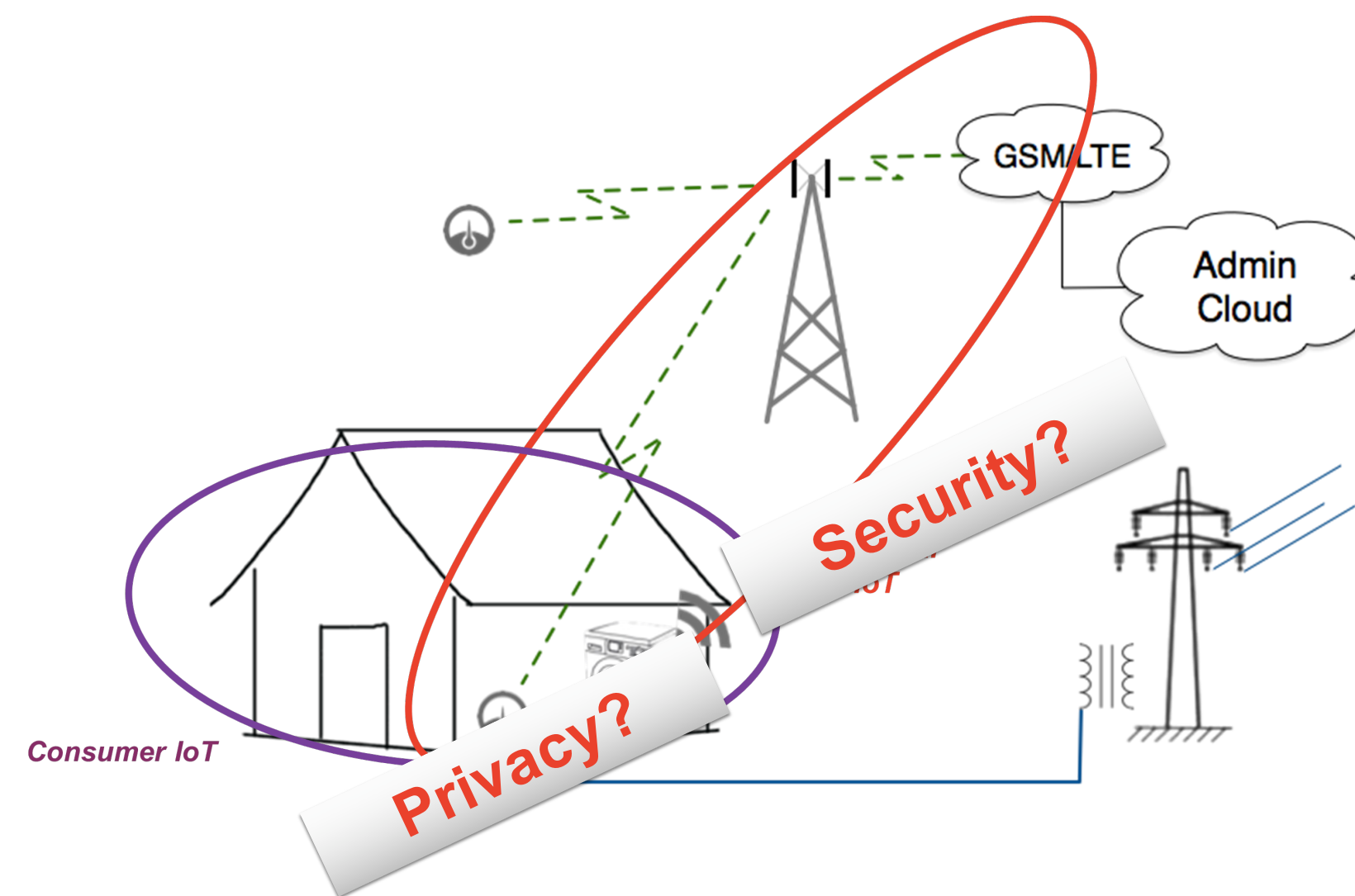
Industrial view versus Consumer view



The challenges - Smart Grid vs Smart Home

Smart Home

- «Wild West» of devices
- «Plug and play»
- Limited user knowledge
- Limited security awareness



Smart Grid

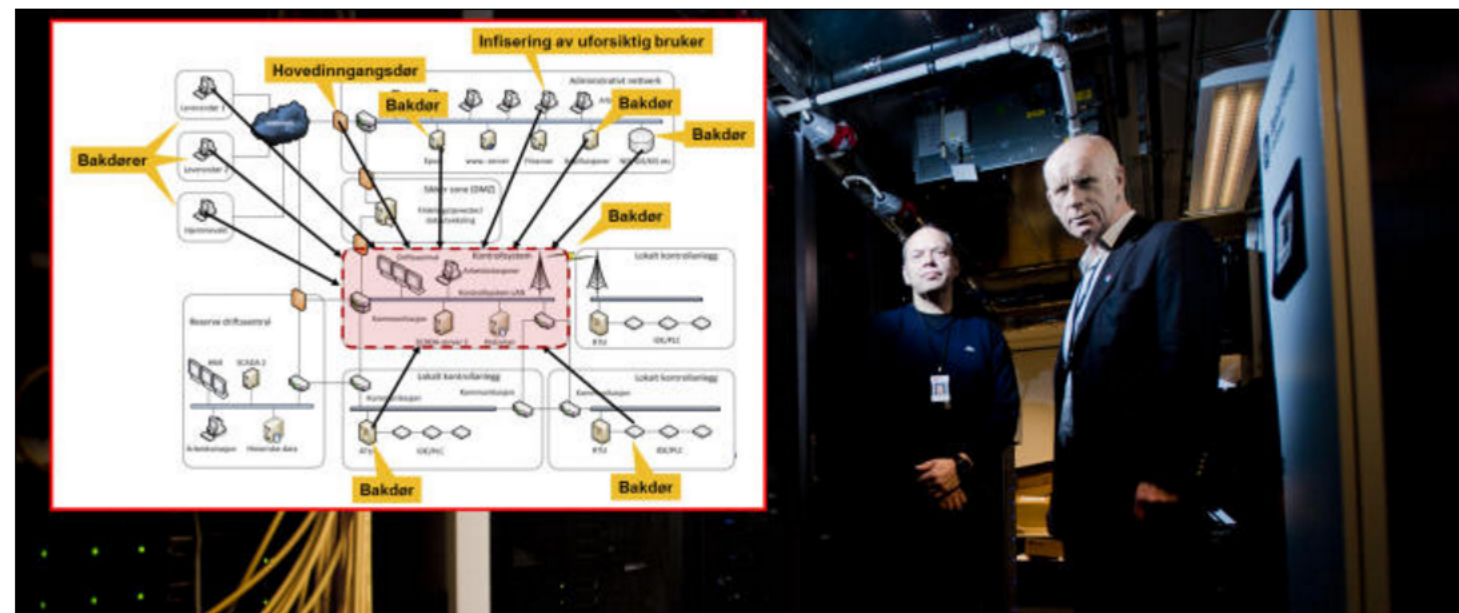
- Limited public knowledge
- Security by design
- Security is the responsibility of supplier

Smart home services



[Source: https://www.samsungsds-nss.com/?p=en_smarthome_private]

Treaths

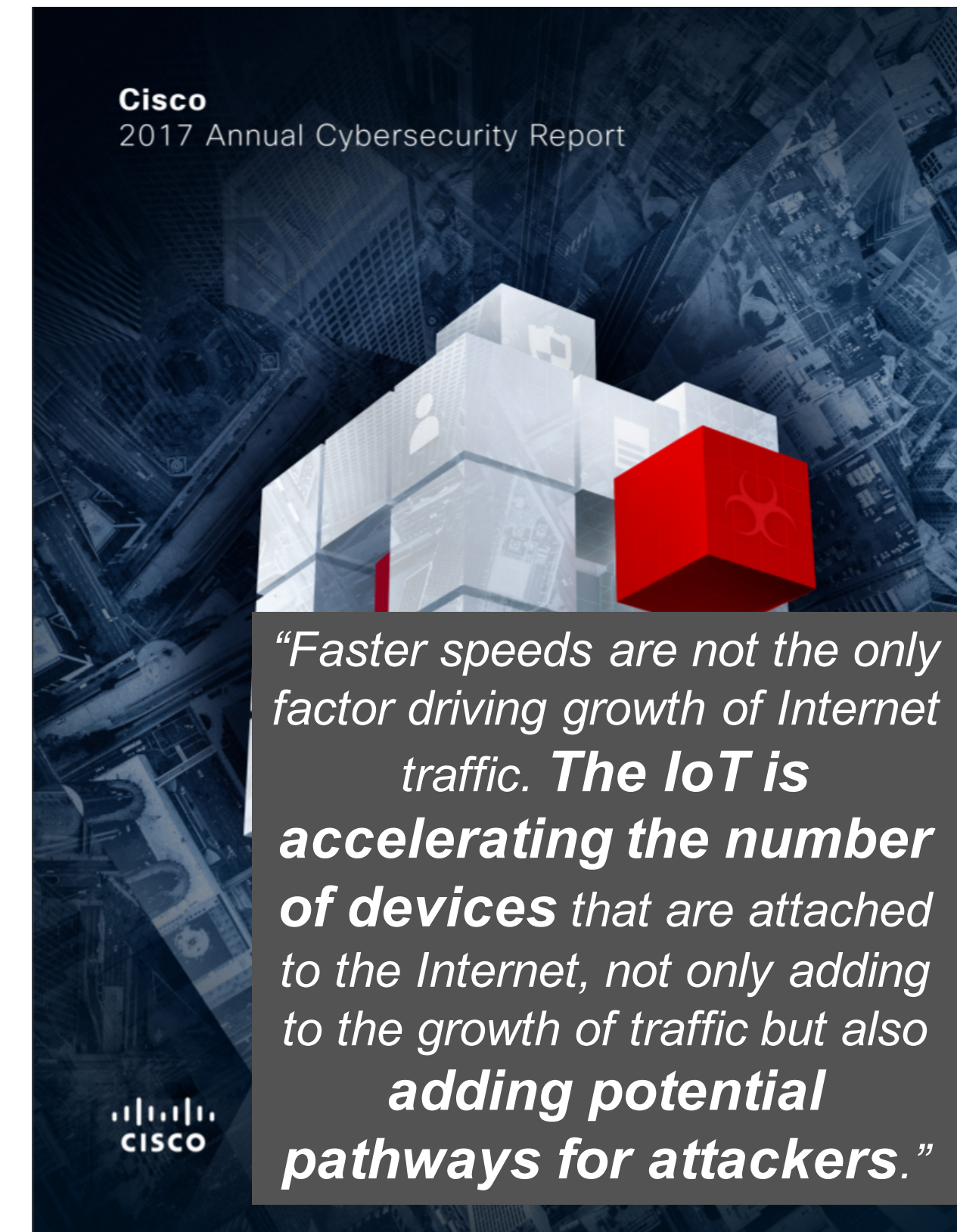


**- Denne typen tiltak
gjør oss mer sårbare
for ondsinnede angrep**

db tv NVE advarer om nye trusler mot strømmettet. [Les mer](#)



Trends in security

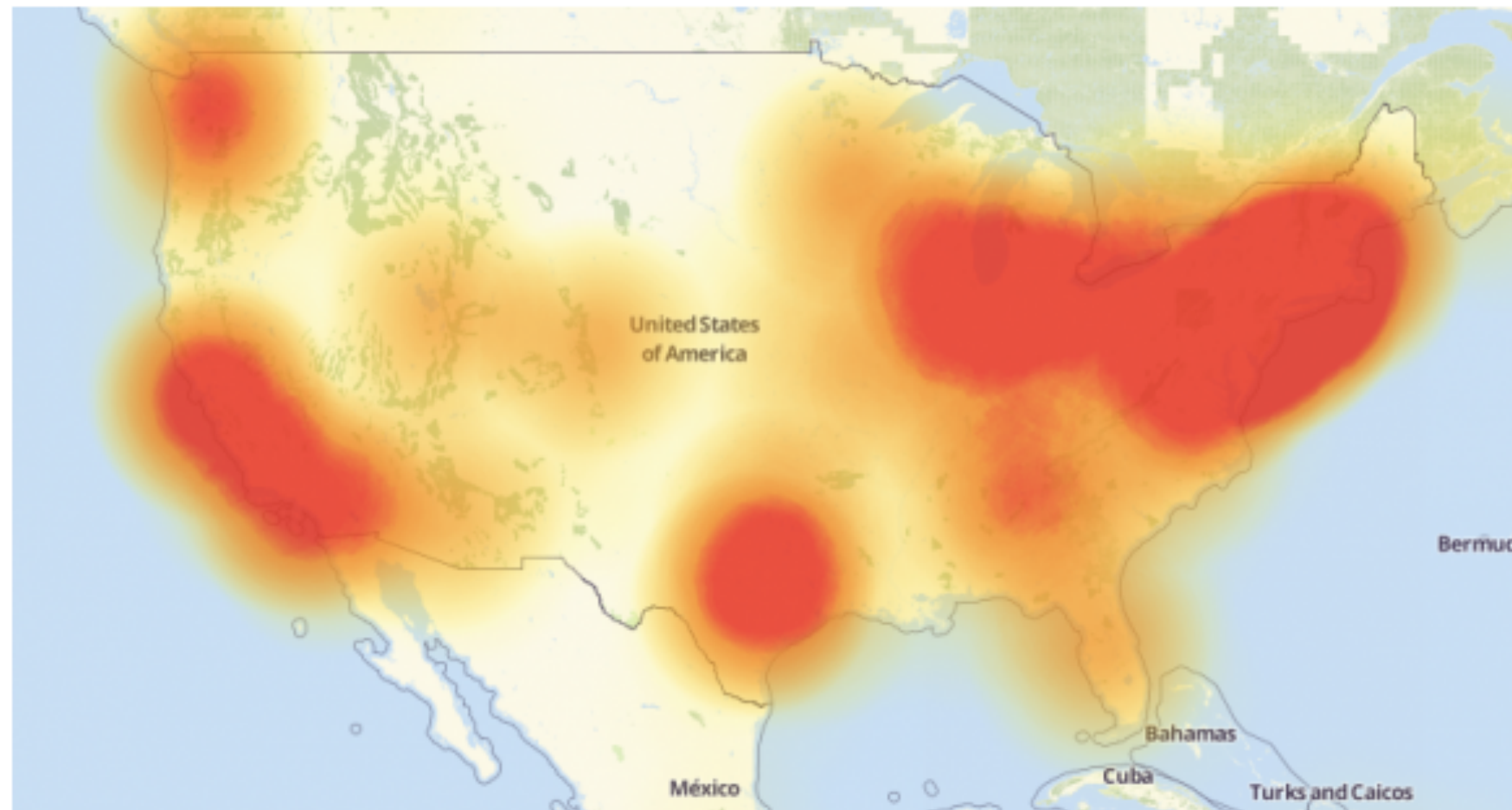


Treath examples

21 Hacked Cameras, DVRs Powered Today's OCT 16 Massive Internet Outage

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked “Internet of Things” (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

Earlier today cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet’s top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.



[Source: <https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/>]

Computing

Ukraine’s Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks

Russian hackers may be behind attacks leveled at the nation’s power grid and artillery. The West should take note.

by Jamie Condliffe December 22, 2016

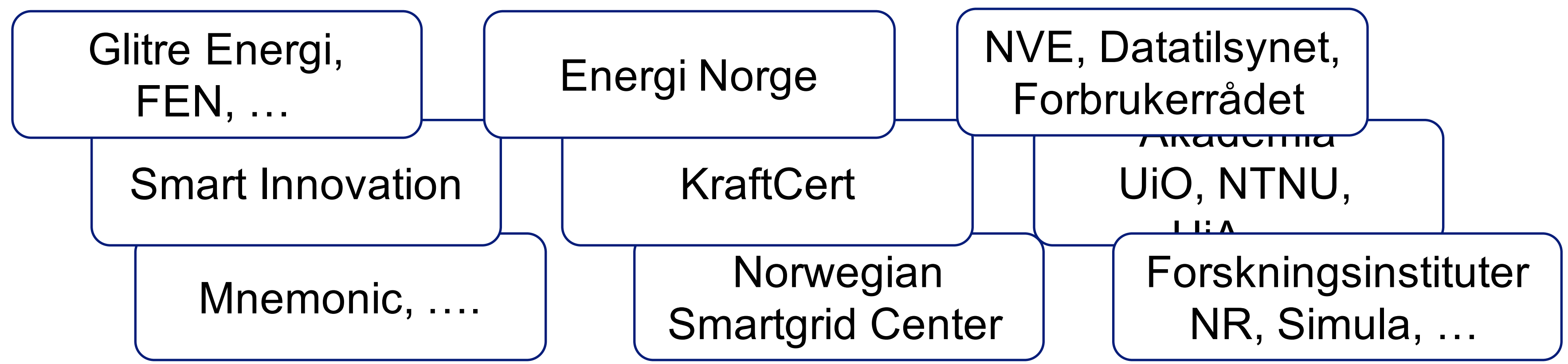
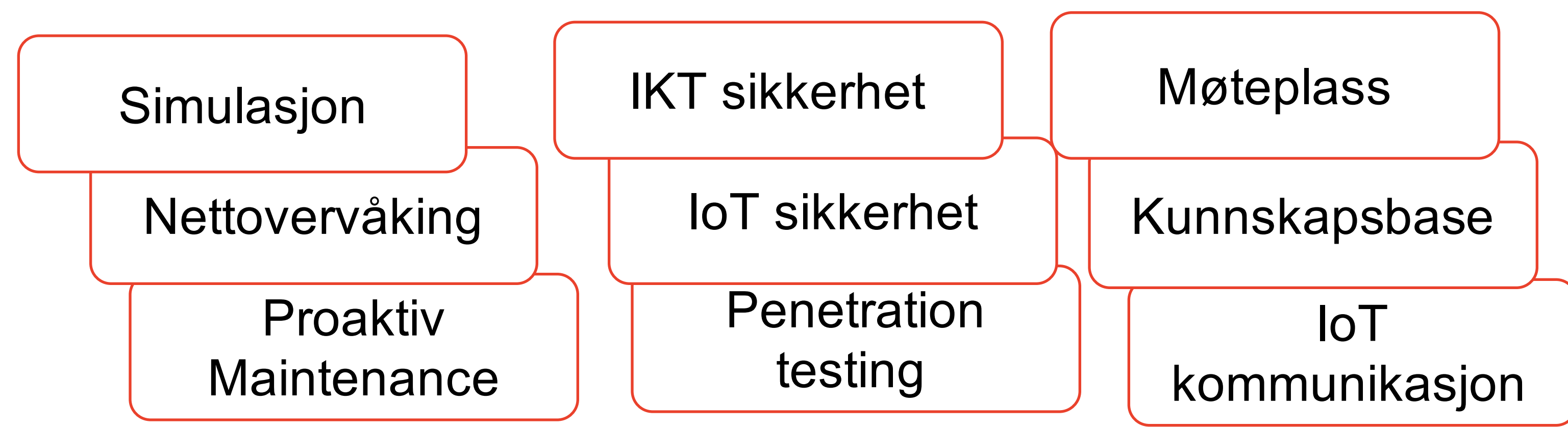
[Source: <https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/>]

IoTSec Movie
<http://www.iotsec.no>



Samarbeid basert på tillit

- Industriell perspektivet
- Samarbeid for å øke tillit
 - ➔ blant aktører
 - ➔ til forbrukeren
- Samarbeid for å øke sikkerhet
 - ➔ samfunnssikkerhet
 - ➔ forsyningssikkerhet
- Utdannelse fra Akademia



Mission Statement

We help the Utility Companies achieve their smart grid goals with higher resiliency and quicker response times against security threats.

