The Internet of Things

Digital meets the analog - the real -world

A risk to the real life ?

Hanns J. Proenen

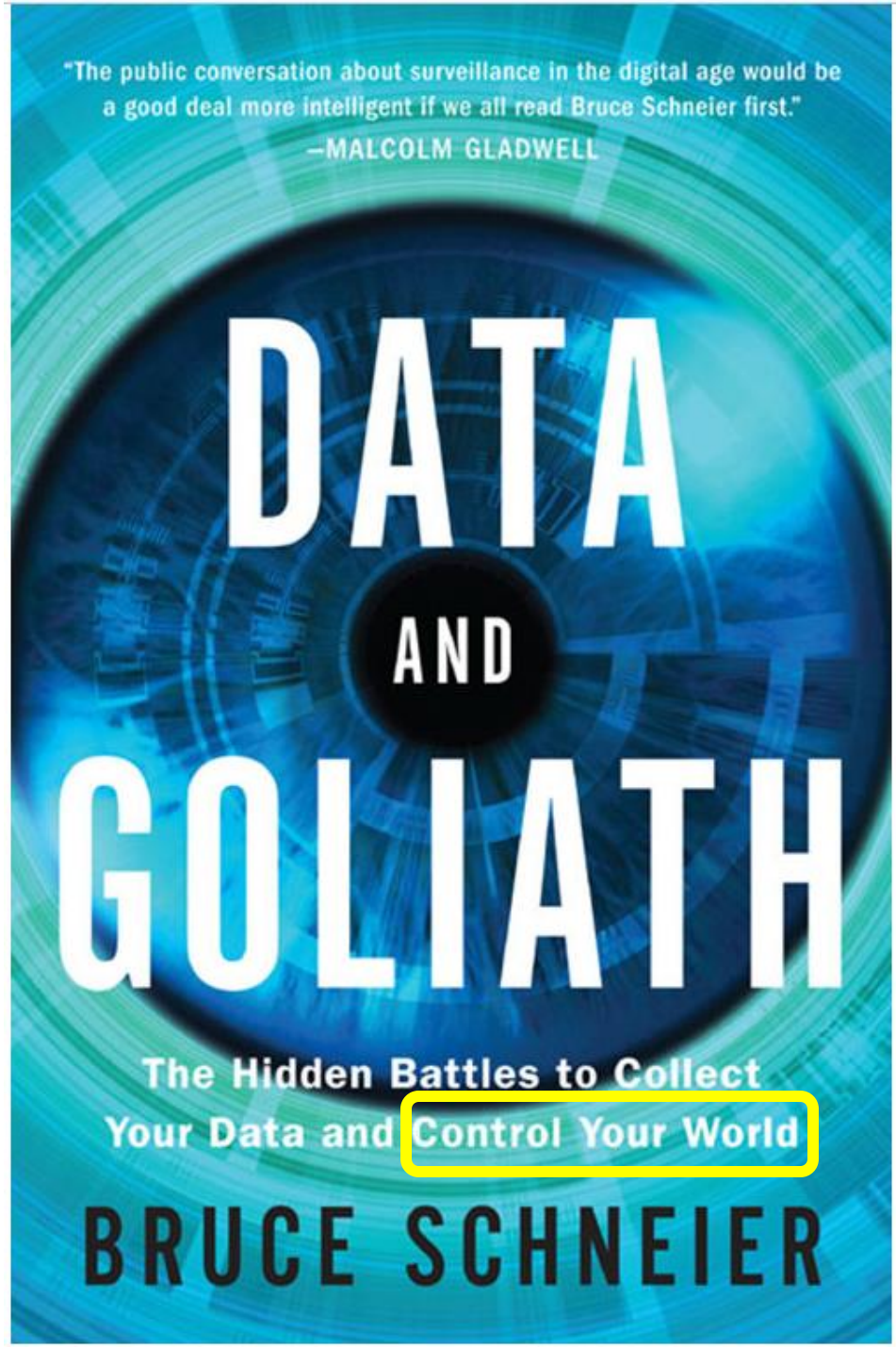
Disclaimer

Everything I say is purely private and not an official statement of GE

Any reference to a specific product, process, or service does not constitute or imply an endorsement by GE or myself.

A new device was found.
Device: Airbus A310
Shall Auto-Configuration be started ?

Source:
CT 1/2003
Ritsch-Renn.com


"The public conversation about surveillance in the digital age would be a good deal more intelligent if we all read Bruce Schneier first."
—MALCOLM GLADWELL
DATA AND GOLIATH
The Hidden Battles to Collect Your Data and Control Your World
BRUCE SCHNEIER

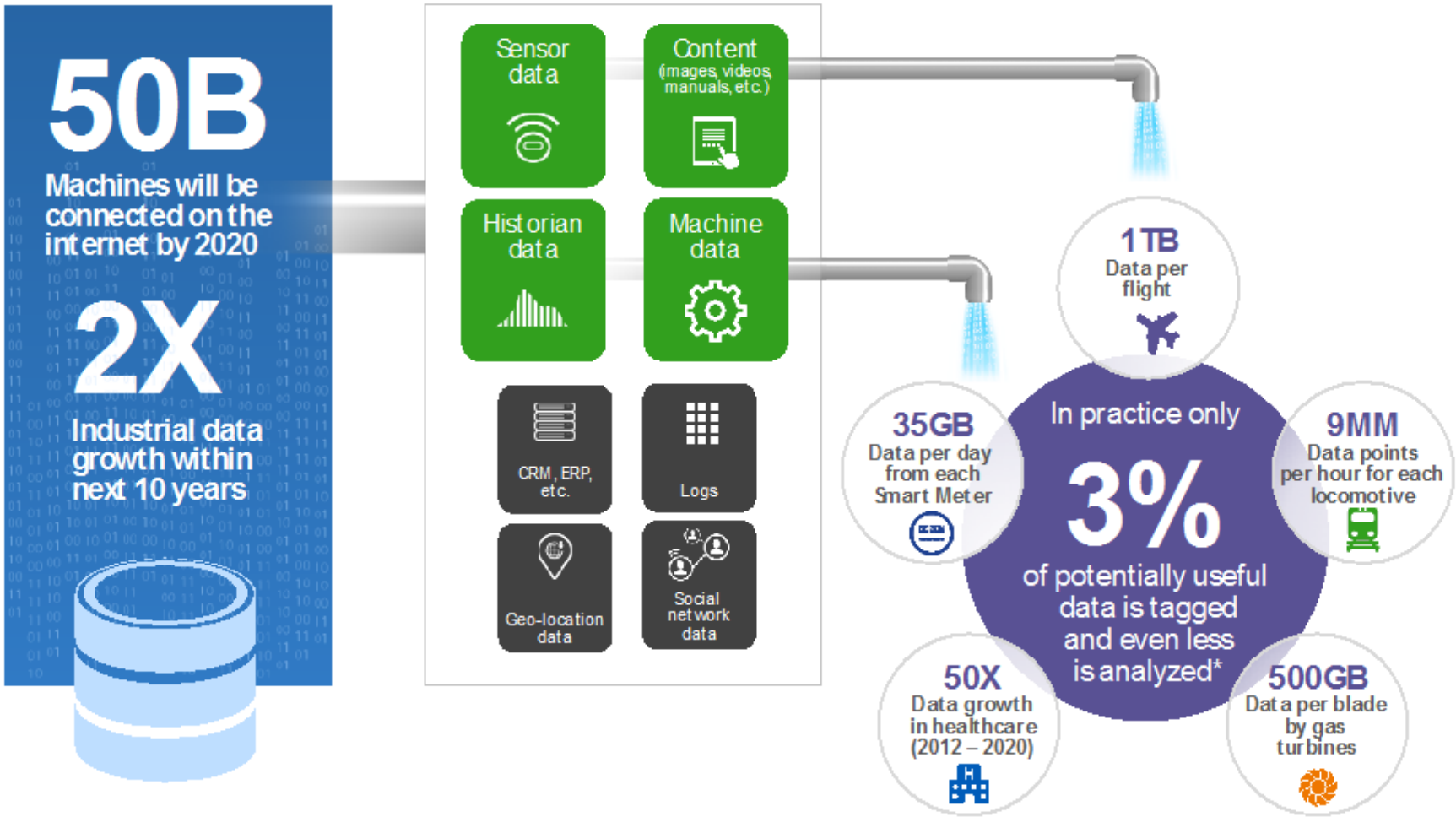
Public perception of threats

- The public takes threats serious when they become “physical” and align with personal experience
- In the 90ies – terrorism was “exotic” – not perceived as a major threat by the public. But the experts in the fileds saw it coming
- 9/11 was a turning point
  and terrorism was all of a sudden perceived as a big threat

---

- The threats resulting from the IoT has not yet reached wide public perception.
- We as security professional must look ahead and see the early indicators
- Stuxnet was such an indicator – resulted in physical damage
- TV5 Monde got lots of media coverage – Example of hybrid warfare
- More incidents will happen – more physical damage will happen
  That is when the public will perceive the IoT as a major threat
  ……. and over-react

Common perception of IoT:
„just collects“ data (confidentiality concerns)



*Source: IDC

Confidentiality - Integrity - Availability

The public perception is focused on „confidentiality“

For the Internet of Things
„Integrity“ and „availabilty“
will become the predominat factors

„Integrity“ and „availability“ of the real world !

Who can open your car ?

German automaker BMW says it has fixed a security flaw that made 2.2 million of its vehicles vulnerable to break-ins.

German automobile club ADAC, which discovered the flaw last summer, says hackers could have used a fake cellphone base station to intercept network traffic from the car and lower the windows or open the doors.

There are no reports such a break-in ever took place.

http://phys.org/news/2015-01-bmw-flaw-exposed-22m-cars.html

Great writeup in CT #9

Just a car

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Who controls the traffic lights ?

Cesar Cerrudo CTO, IOActive Labs
I found some interesting devices used by traffic control systems on important cities such as Washington DC, Seattle, New York, San Francisco, Los Angeles, etc. and I could hack them :)

I also found that these devices are also used in cities from UK, France, Australia, China, etc. making them even more interesting.

Oh, I almost forgot, after this presentation anyone will be able to hack these devices and mess traffic control systems since there is no patch available.

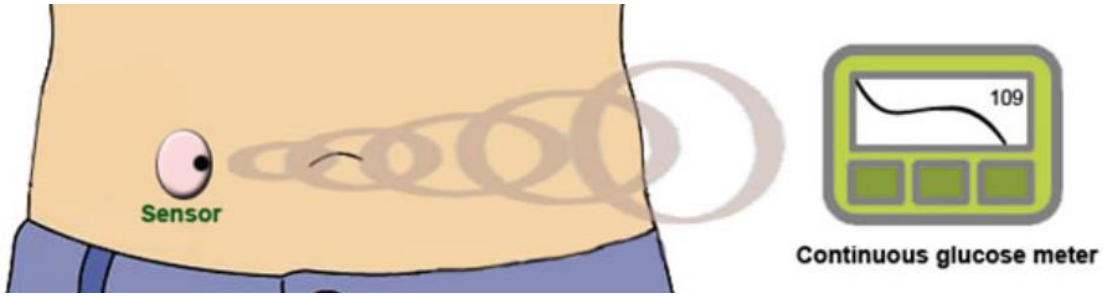
https://defcon.org/html/defcon-22/dc-22-speakers.html#Cerrudo

http://de.slideshare.net/cisoplatform7/defcon-22cesarcerrudohackingtrafficcontrolsystems

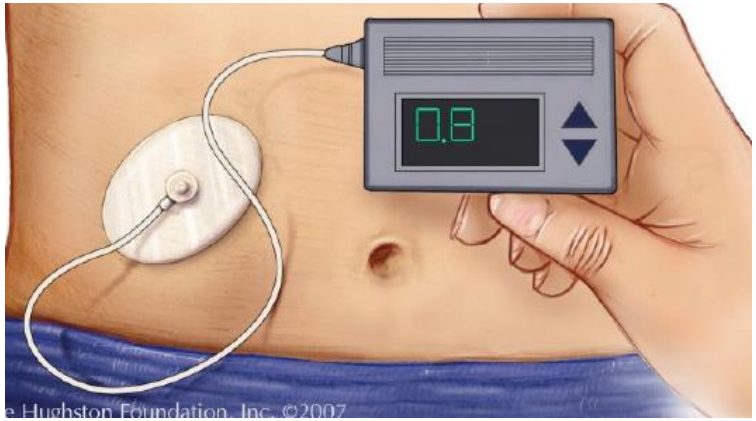
Just a traffic light

Breaking the Human SCADA System

presented at BlackHat 2011 by Jerome Radcliffe



Continuous glucose meter



https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_Slides.pdf

Just a life !!!

Turn off power & water ?

On 3 July 2014, DHS, responding to a Freedom of Information Act(FOIA) request on Operation Aurora, a malware attack on Google, instead released more than 800 pages of documents related to the Aurora Project, a 2007 research effort led by Idaho National Laboratory to show the cyber vulnerabilities of U.S. power and water systems, including electrical generators and water pumps.

The research project found that once these infrastructure systems are infiltrated, a cyberattack can remotely control key circuit breakers, thereby throwing a machine's rotating parts out of synchronization and causing parts of the system to break down.

http://www.homelandsecuritynewswire.com/dr20150107-dhs-releases-the-wrong-foiarequested-documents-exposing-infrastructure-vulnerabilities

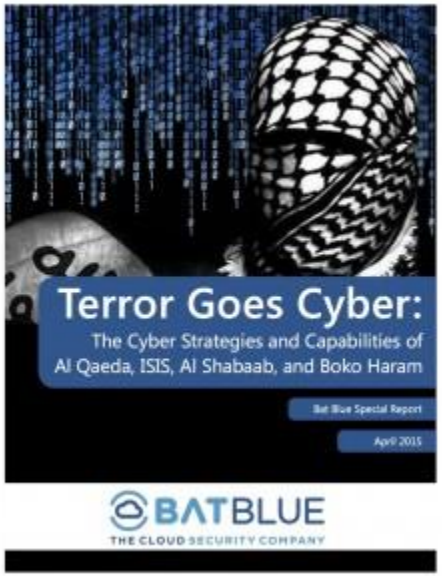
Stuxnet

- Designed to destroy nuklear centrifuges in Iran

- A weapon made entirely of code
- The source code is online
- It is an OpenSource Weapon

- The world was asking: „who did it“
- The more interesting question is: „who will do it again“

- **And what will they attack next ?**



Bruce Schneier on the Sony Hack:

- "Your reaction to the massive hacking of such a prominent company will depend on whether you're fluent in information-technology security.
- If you're not, you're probably wondering how in the world this could happen.
- **If you are, you're aware that this could happen to any company."**

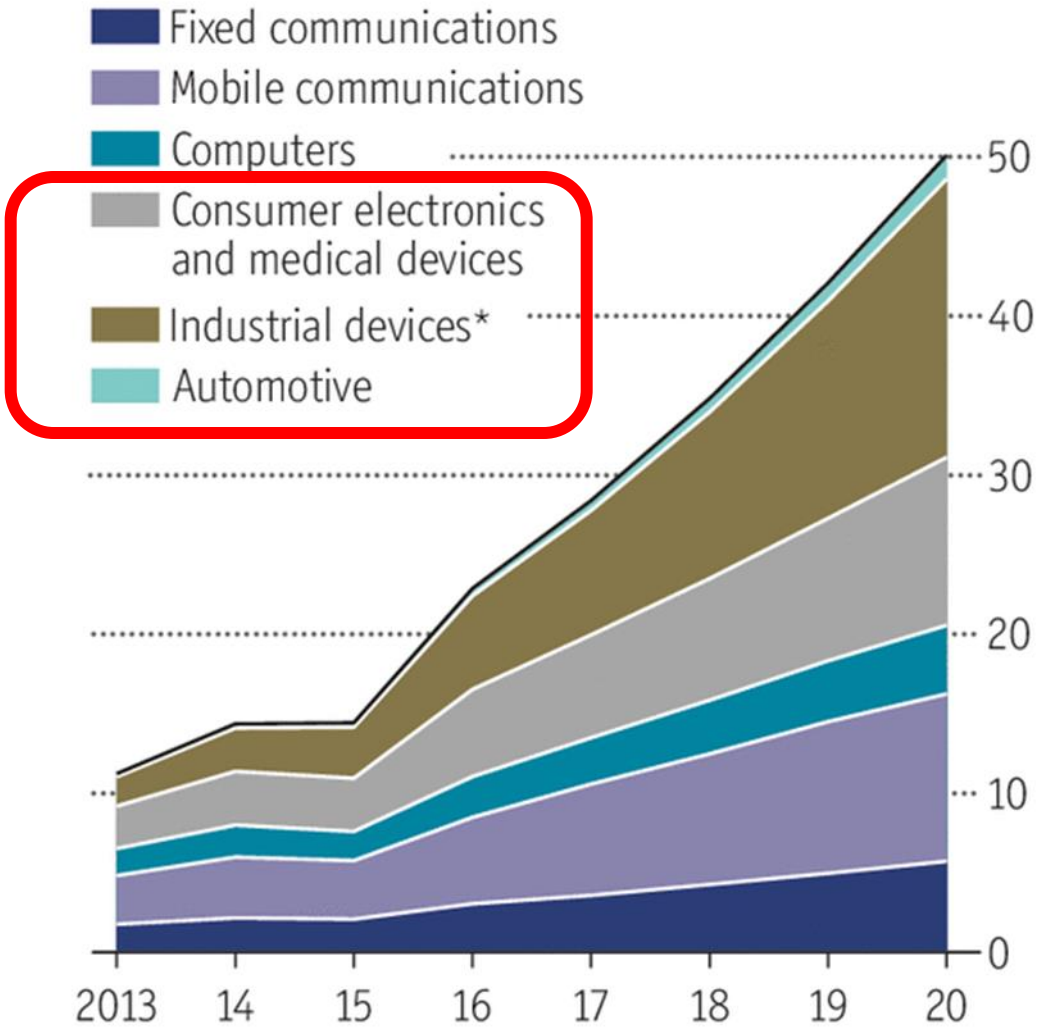
Hackers have accessed the personal records of some 80 million Anthem Health customers and others.

Last year, it was
- Home Depot
- JP Morgan
- Sony
- and many others

Do YOU think the security of YOUR IoT products is better than any of these companies?

The 50 billion question

Worldwide number of internet-connected devices, forecast, bn



Source: Cisco

*Includes military and aerospace

Security of mass produced “things”

We have developed mechanisms to patch security vulnerabilities on PC’s that work “ok”

Patching on Smartphones already a problem once vendor no longer supports the model – typically after 2 years
→ growing # of insecure devices

Cars can be recalled – Chrysler just did that for 1.2 million cars to fix the “hacked Jeep”.

What about mass produced items ?

- Stoves, Refrigerators, Laundry machines, Lightbulbs

Do we bring them back to the OBI store for patching ?
Or do we have to throw these “things” away once a security vulnerability was detected ?
Obsolesence due to a missing security patch ?

The computer industry learned its lessons over a decade ago.
Before then they ignored security vulnerabilities, threatened researchers, and generally behaved very badly.

I expect the same things to happen with Internet-of-Things companies.

Bruce Schneier
Schneier Cryptogram August 2015

Conclusion

- Attacks against ANY “thing on the internet” will happen
- Many will be successful – we must be prepared
- CISO‘s must understand the effects of successful attacks
  What damage will it do ?
- **„Prevent - Detect – React“ is still our job**
  But must take more efforts on „React“
- **Resilience is the key – containment & recovery**
  CISOs must understand the „things“ their IT controls
  CISOs must work closely with the engineers of the „things“

  CISOs must have a holistic view – not just IT

Thank You