Munich IT Security Research Group

Crisis 4.0: Lack of Security and Privacy Could Kill Digitalization

Hans-Joachim Hof

hof@insi.science

Munich IT Security Research Group

Munich University of Applied Sciences

INSicherheit – Ingolstädter Forschungsgruppe angewandte IT-Sicherheit, Technische Universität Ingolstadt

Digitalization

Digitalization
=
Increasing interconnection between humans and/or machines

Digitalization
=
Increasing number of automated data acquisition and data analysis

Digitalization
=
Exploitation and access to big data

Digitalization

Digitalization

=

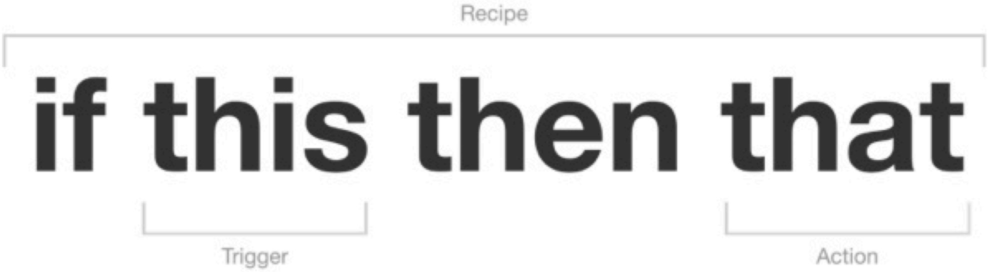
IT Everywhere

My personal digitalization

IFTTT

My personal digitalization

IFTTT



Recipe

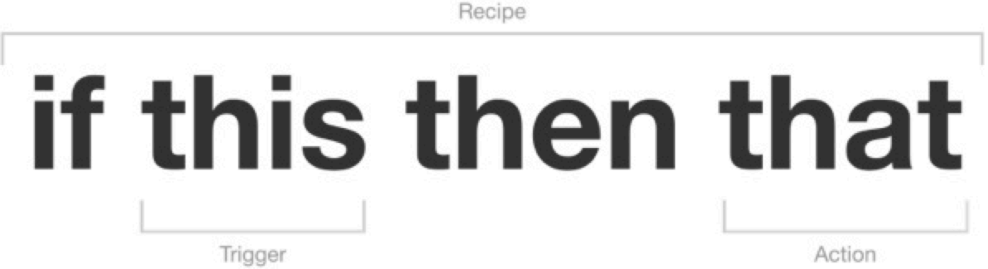
if this then that

Trigger

Action

My personal digitalization

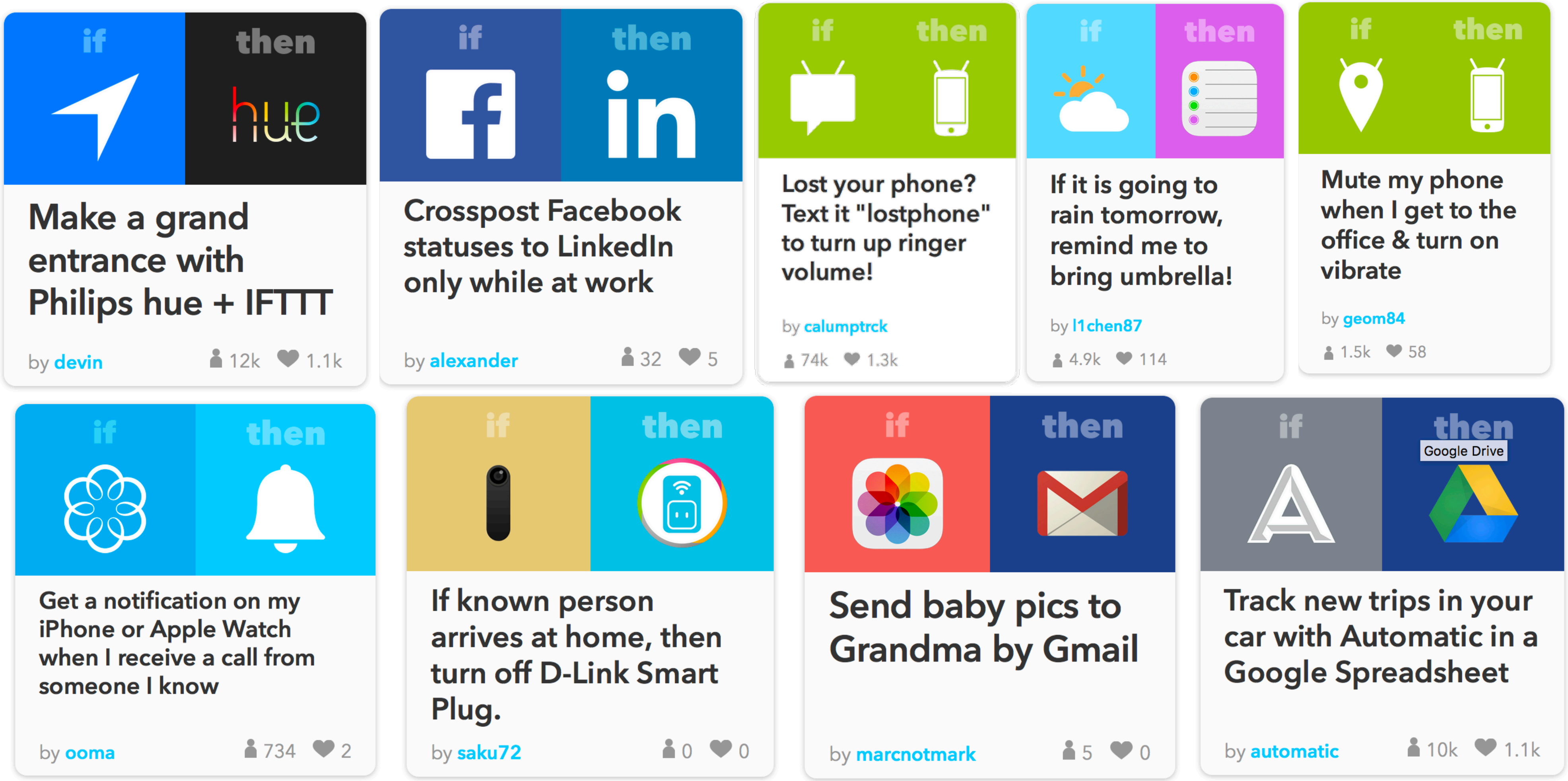
IFTTT


Recipe

if this then that

Trigger

Action



Make a grand entrance with Philips hue + IFTTT
by devin 12k 1.1k

Crosspost Facebook statuses to LinkedIn only while at work
by alexander 32 5

Lost your phone? Text it "lostphone" to turn up ringer volume!
by calumptrck 74k 1.3k

If it is going to rain tomorrow, remind me to bring umbrella!
by l1chen87 4.9k 114

Mute my phone when I get to the office & turn on vibrate
by geom84 1.5k 58

Get a notification on my iPhone or Apple Watch when I receive a call from someone I know
by ooma 734 2

If known person arrives at home, then turn off D-Link Smart Plug.
by saku72 0 0

Send baby pics to Grandma by Gmail
by marcnotmark 5 0

Track new trips in your car with Automatic in a Google Spreadsheet
by automatic 10k 1.1k

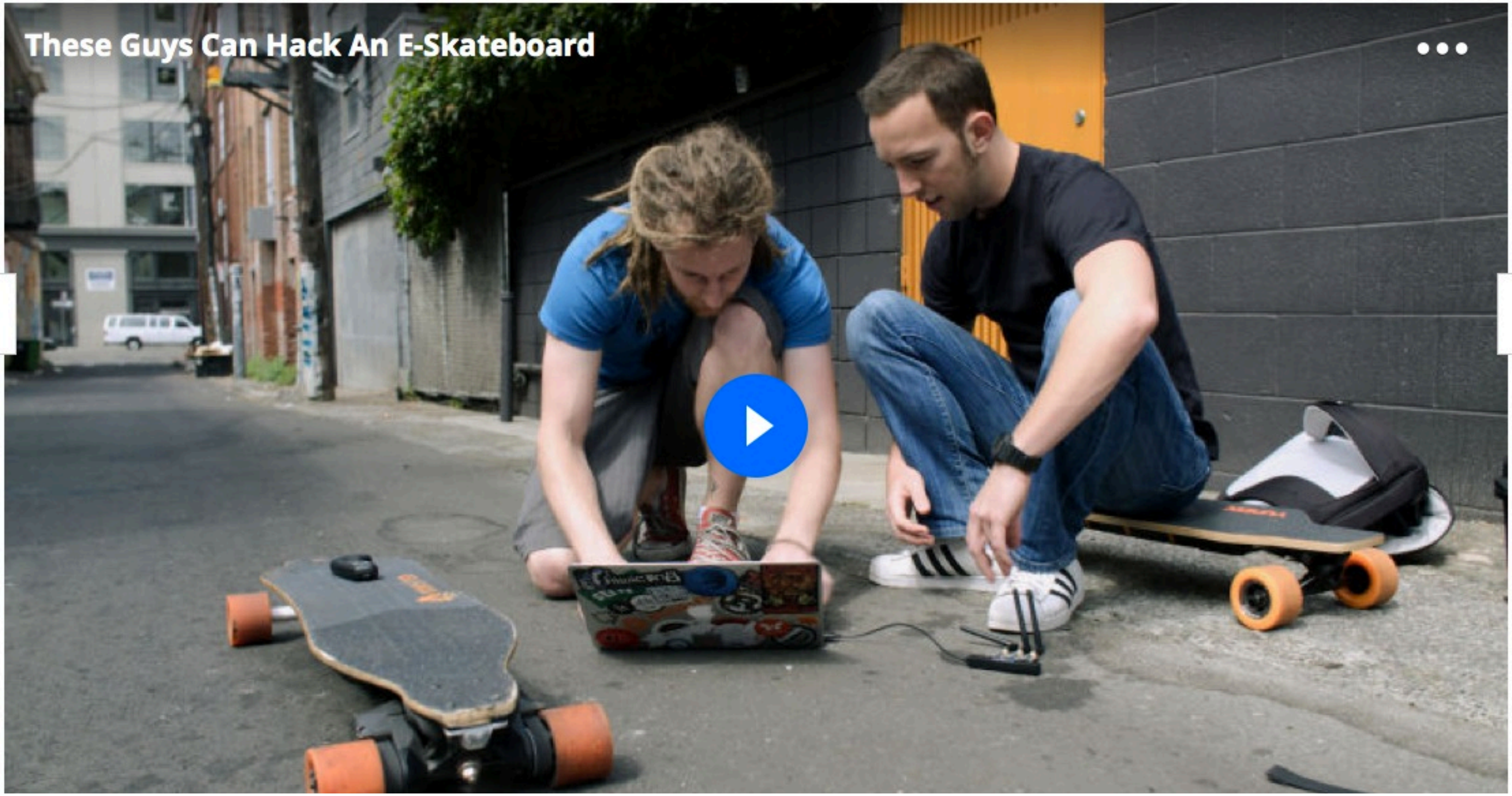
Collection of intelligent things

Benefits and drivers of digitalization

- Cost reduction (e.g., increased efficiency, less resource consumption)
- New business models (e.g., digital products + print shop)
- Advanced analysis, better forecasts
- Lifestyle (e.g., fitness, smart home)
- Me too („more than half of surveyed companies (59%) noticed that the disruptive effects of their digital business activities was higher than expected”)
- ...because we can ☺☺☺

Risks of digitalization

HACKERS CAN SEIZE CONTROL OF ELECTRIC SKATEBOARDS AND TOSS RIDERS



These Guys Can Hack An E-Skateboard

Quelle: WIred.com

Risks of digitalization

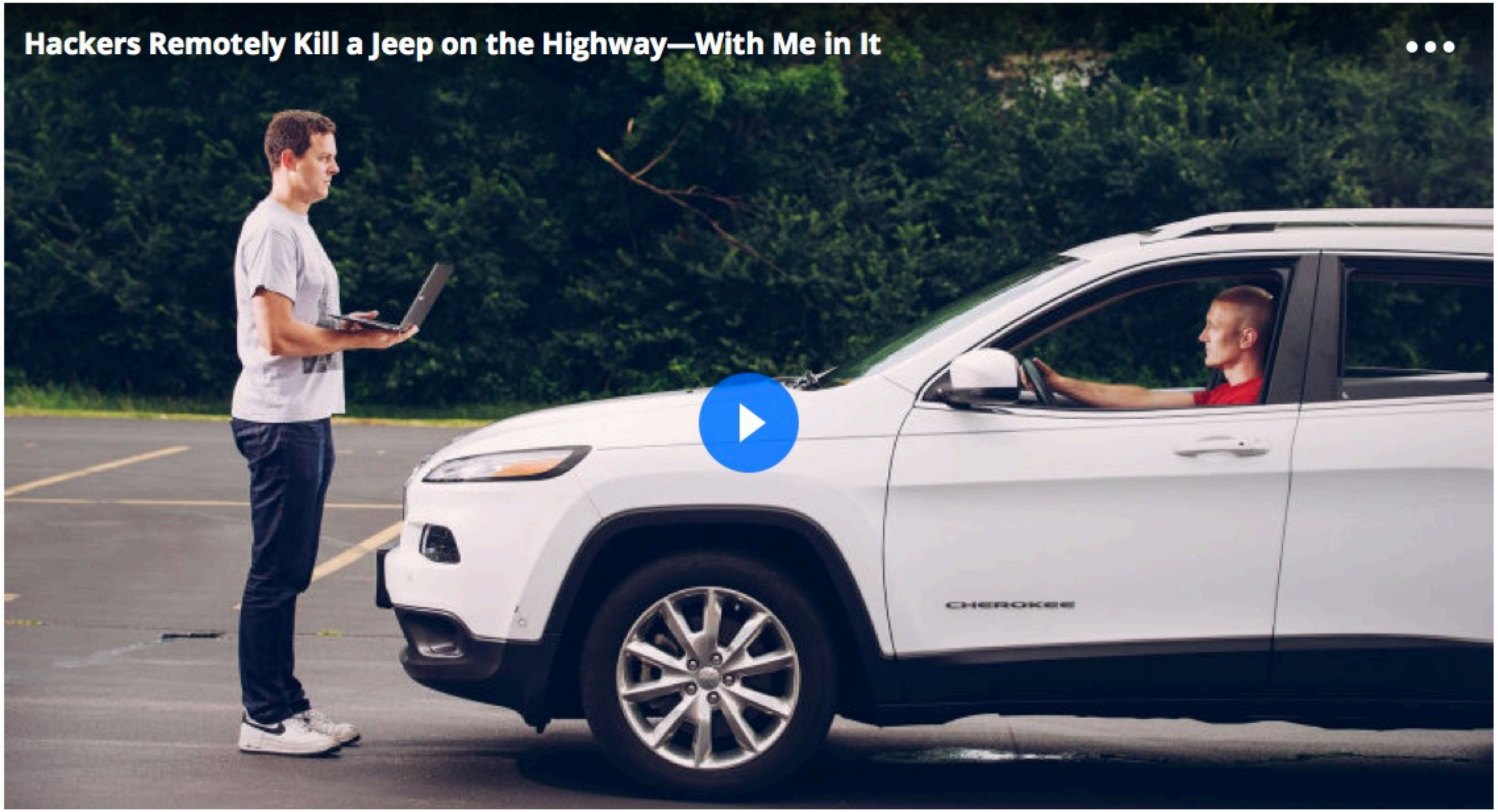
HACKERS CAN DISABLE A SNIPER RIFLE—OR CHANGE ITS TARGET

Hacking a "Smart" Sniper Rifle

Quelle: WIred.com

Risks of digitalization

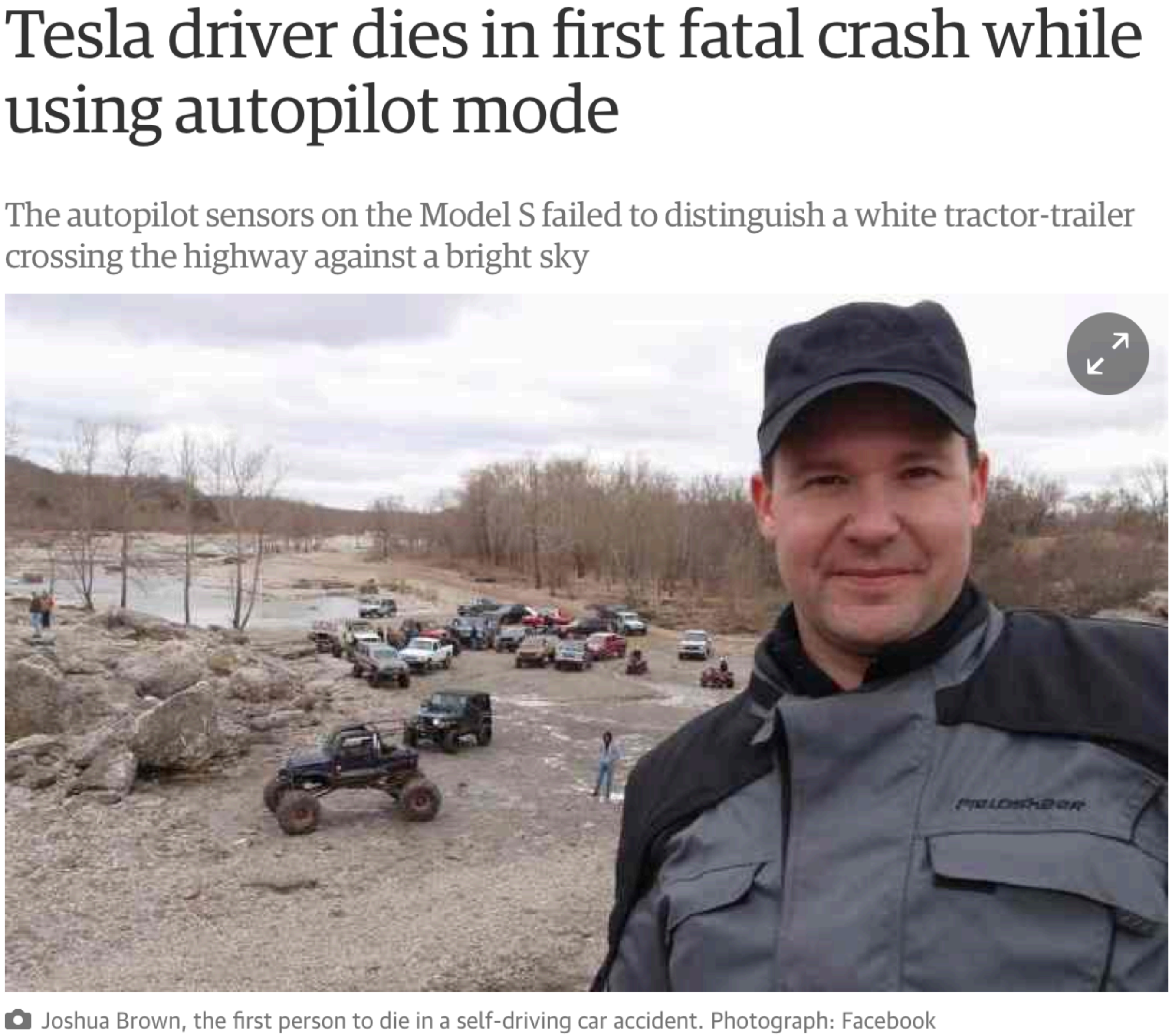
HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



Hackers Remotely Kill a Jeep on the Highway—With Me in It

Quelle: WIred.com

Risks of digitalization



Tesla driver dies in first fatal crash while using autopilot mode

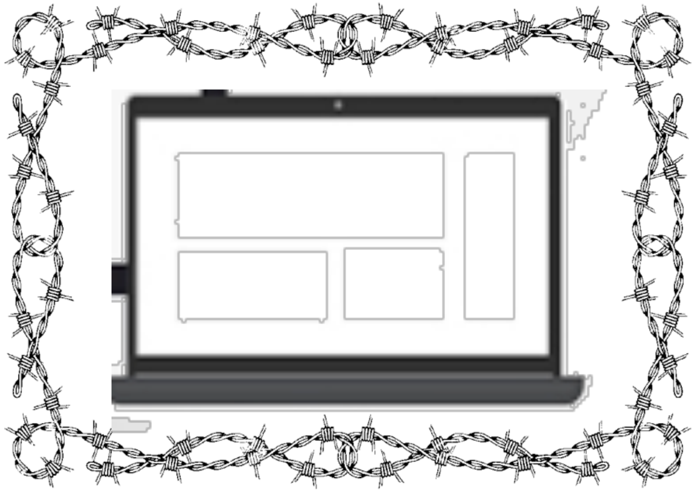
The autopilot sensors on the Model S failed to distinguish a white tractor-trailer crossing the highway against a bright sky

Joshua Brown, the first person to die in a self-driving car accident. Photograph: Facebook

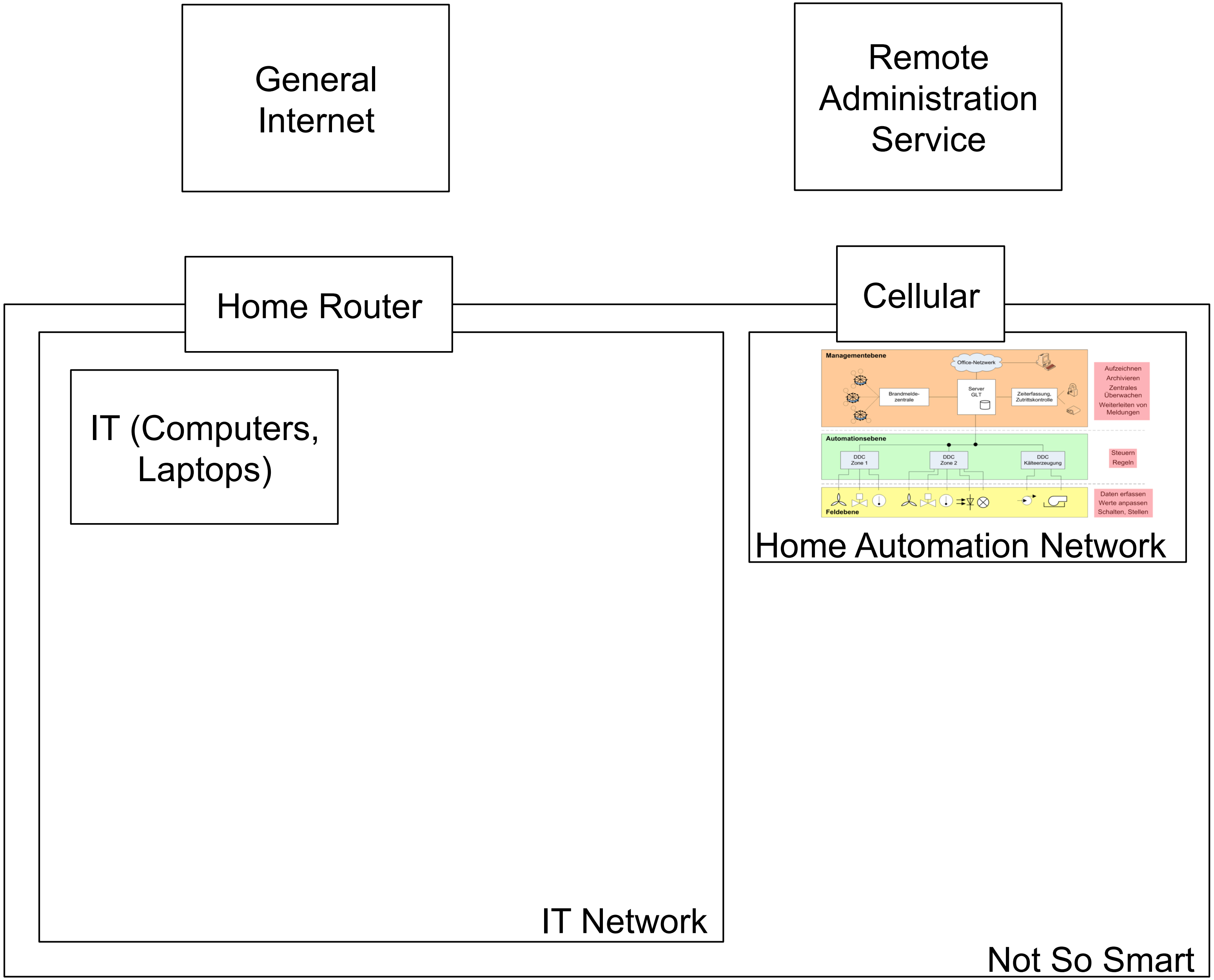
What does digitalization mean for security and privacy?

past

present



Example: Not so smart home



General Internet

Remote Administration Service

Home Router

Cellular

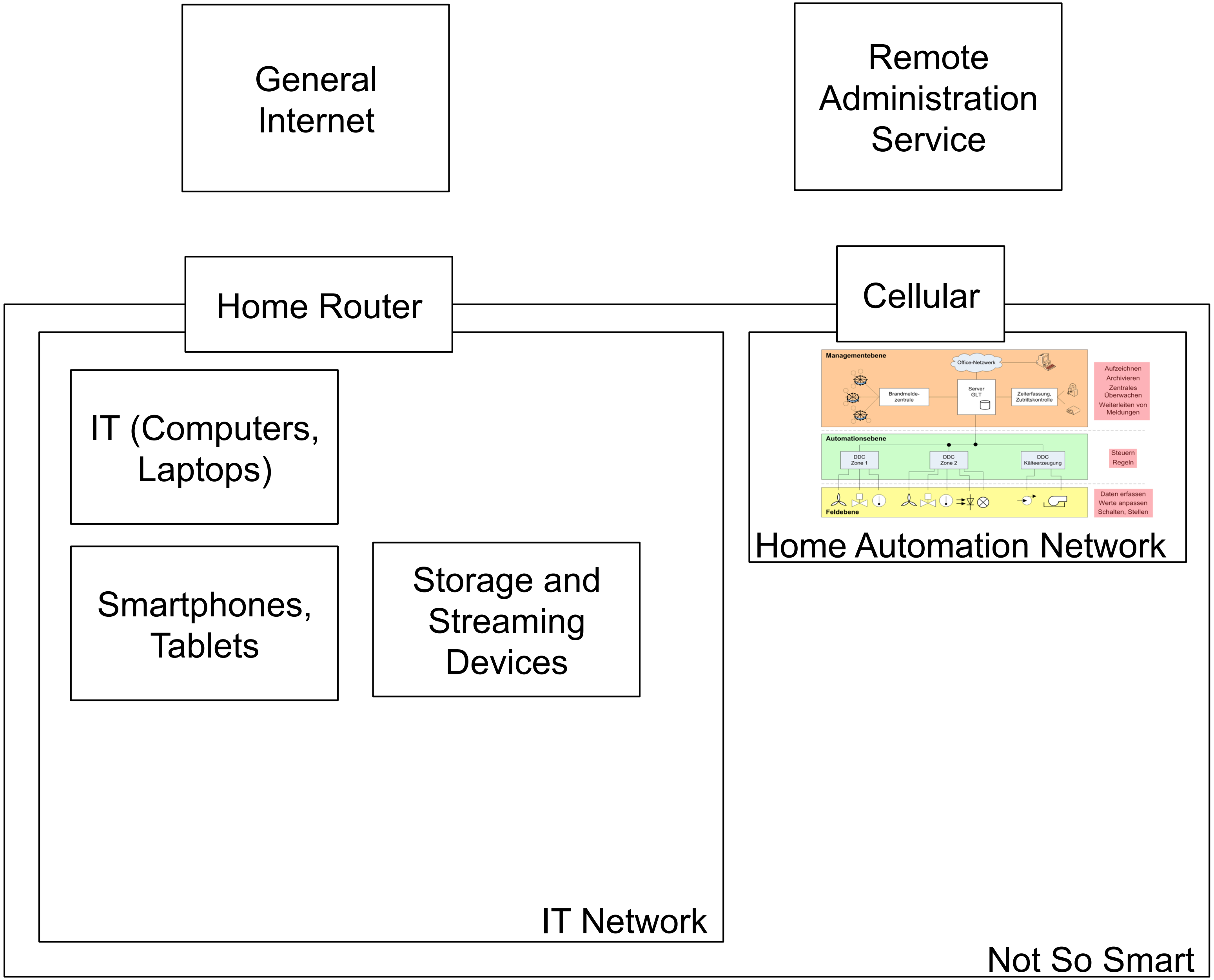
IT (Computers, Laptops)

IT Network

Home Automation Network

Not So Smart

Example: Not so smart home



General Internet

Remote Administration Service

Home Router

Cellular

IT (Computers, Laptops)

Smartphones, Tablets

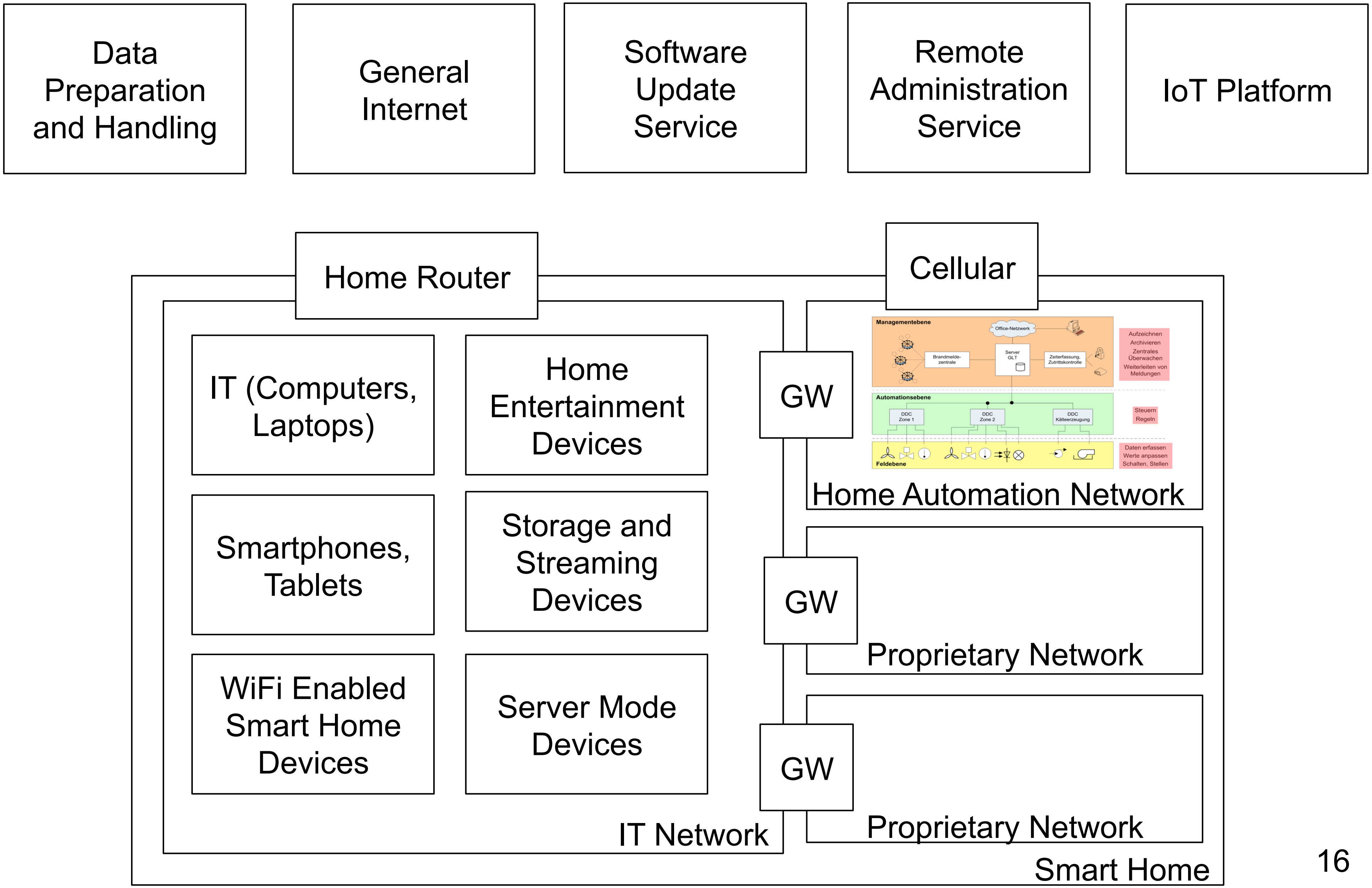
Storage and Streaming Devices

IT Network

Home Automation Network

Not So Smart

Example: Not so smart home



Data Preparation and Handling

General Internet

Software Update Service

Remote Administration Service

IoT Platform

Home Router

Cellular

IT (Computers, Laptops)

Home Entertainment Devices

Smartphones, Tablets

Storage and Streaming Devices

WiFi Enabled Smart Home Devices

Server Mode Devices

IT Network

GW

GW

GW

Home Automation Network

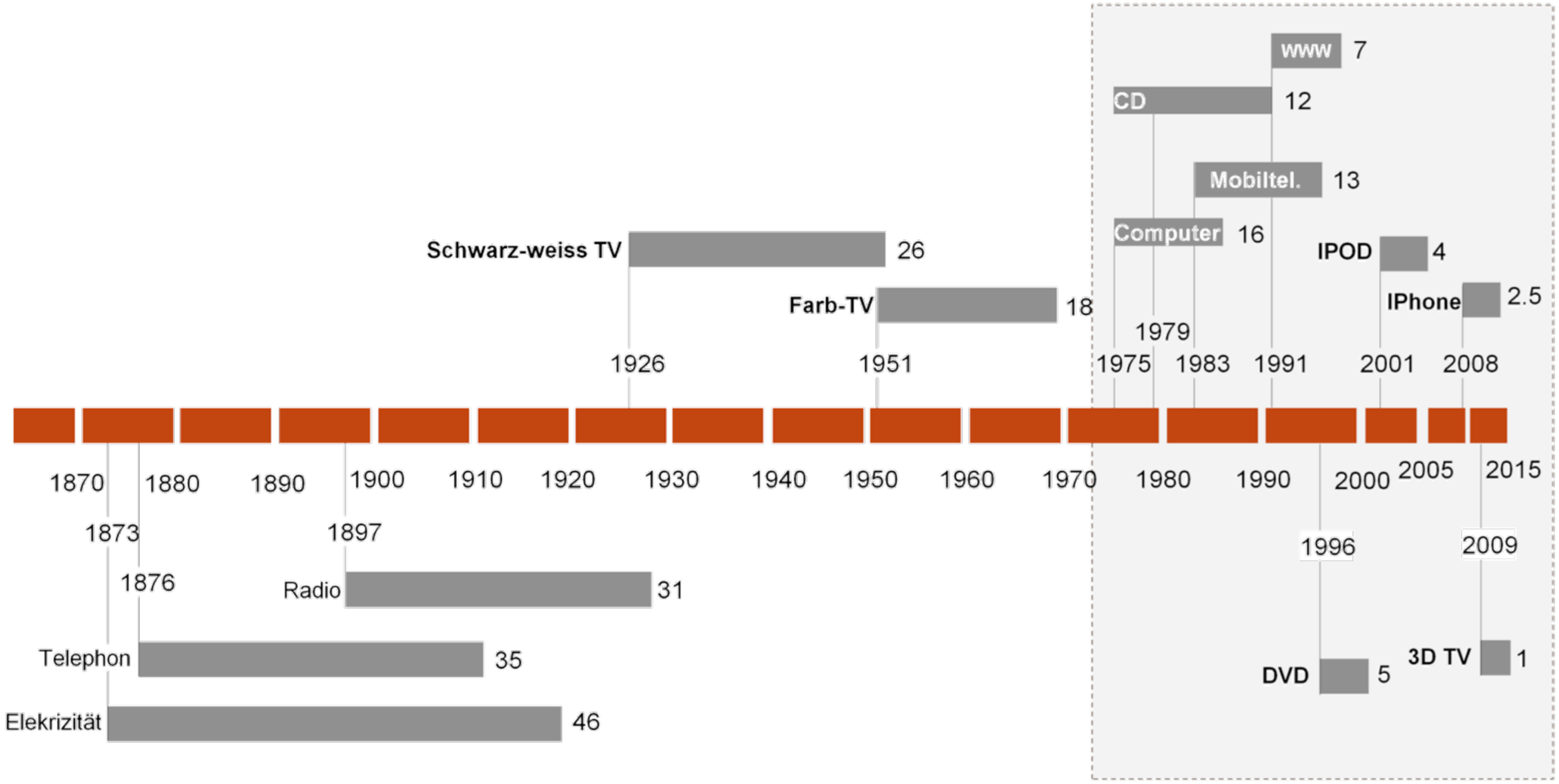
Proprietary Network

Proprietary Network

Smart Home

What does digitalization mean for security and privacy?

Years an innovation needed until ¼ of the population uses it



What does digitalization mean for security and privacy?

- Embedded devices have different constraints
  - Resource efficiency necessary
  - Physical access to devices may be difficult, „installed and forgotten“
  - Other protocols, other development processes
  - Electrical engineers at work ...

- High damage potential (business damage, loss of lifes)

- Diversity of system lifetime (months to decades)

- IT Everywhere => acquisation of privacy relevant data everywhere

Recent security fails

- Configuration error: alarm system with standard password (l:admin p:admin1234, l:1234, p:1234)
- Design errors: Vulnerable key management of ZigBee Home Automation 1.2 used in intelligent door locks
- Programming errors: Buffer overflow in drive used in home routers

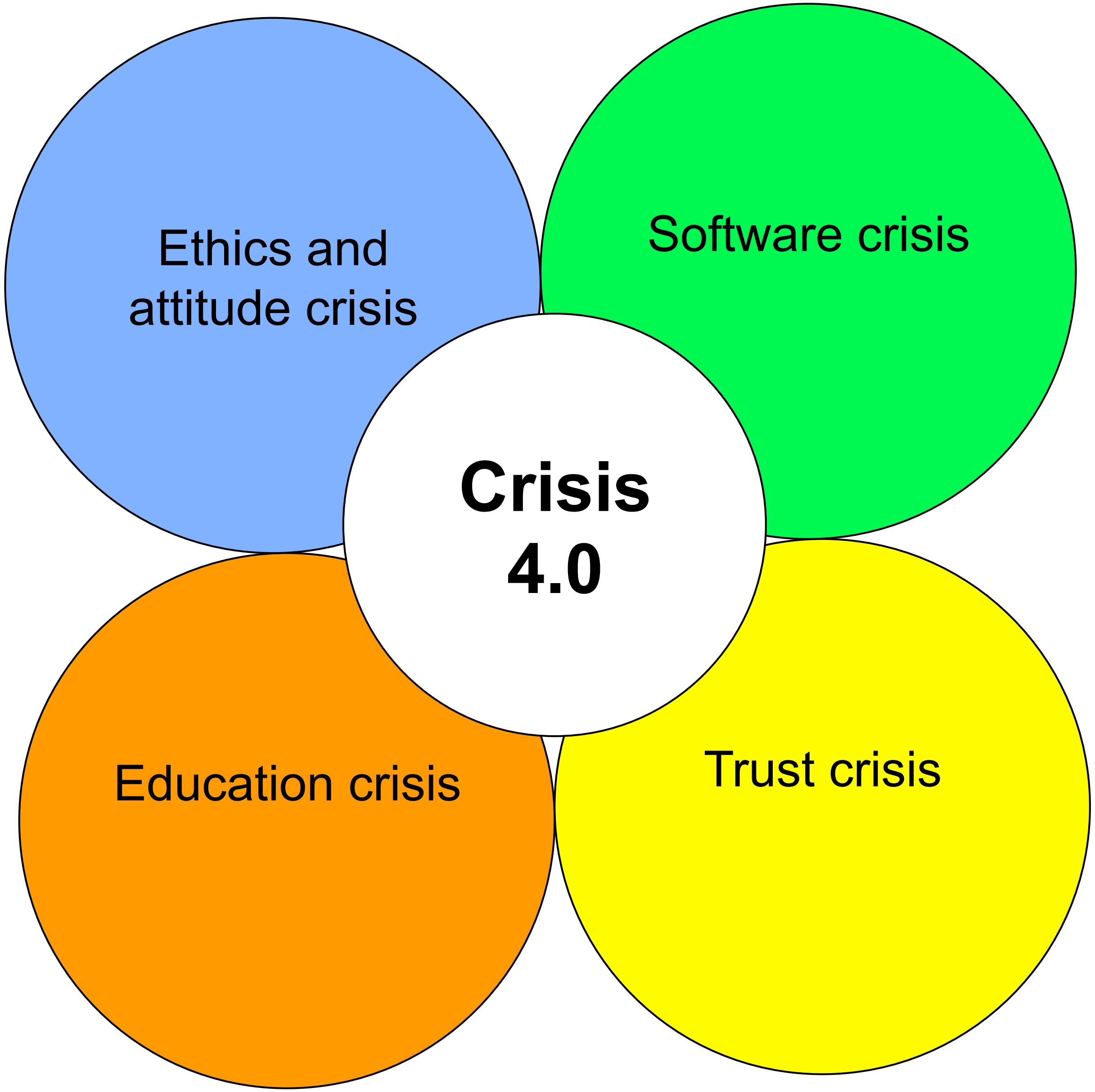
Problems from the 90s ...

- For a lot of fun go to Shodan (www.shodan.io):

The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

Crisis 4.0



Ethics and attitude crisis

Software crisis

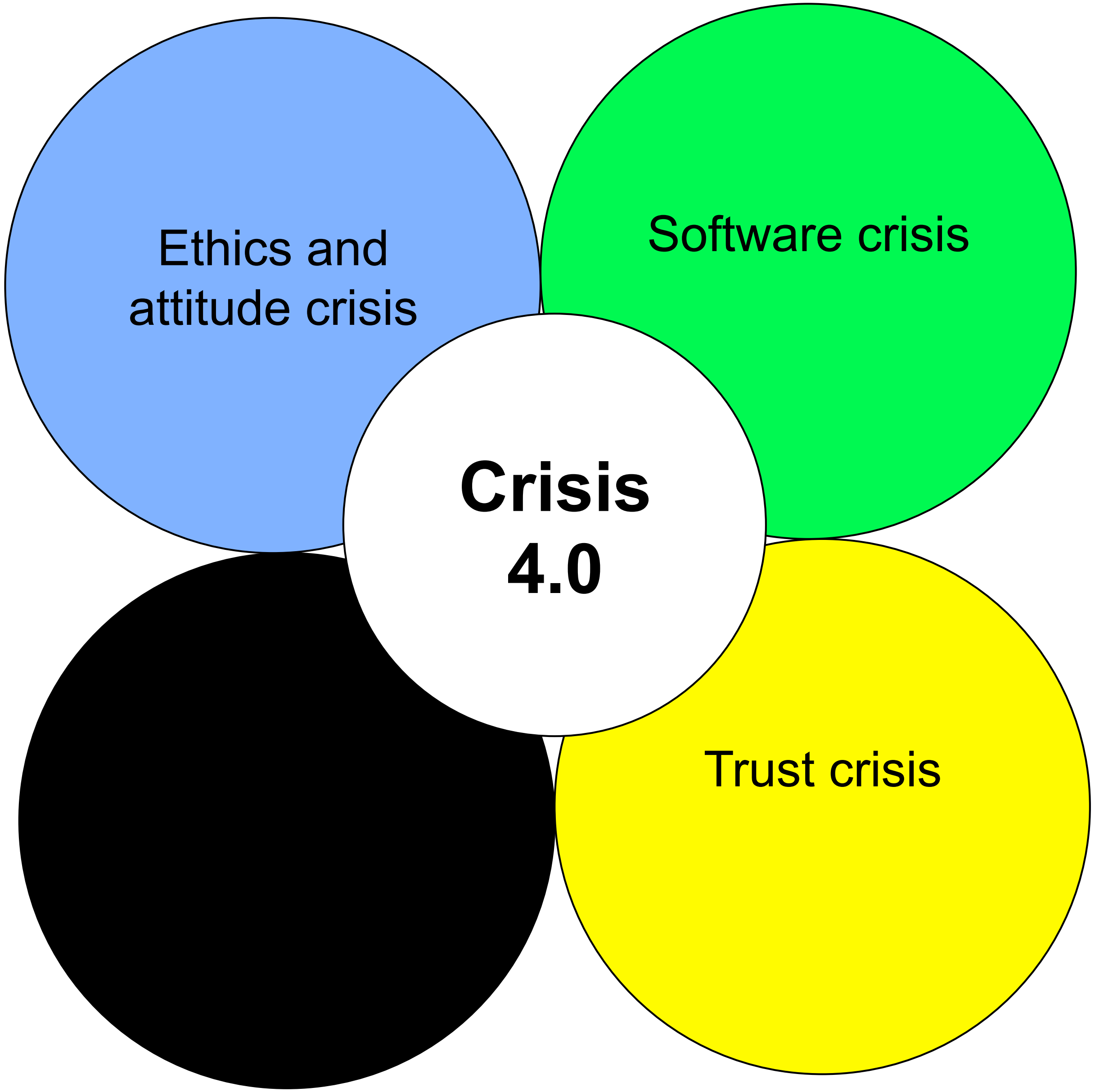
Crisis 4.0

Education crisis

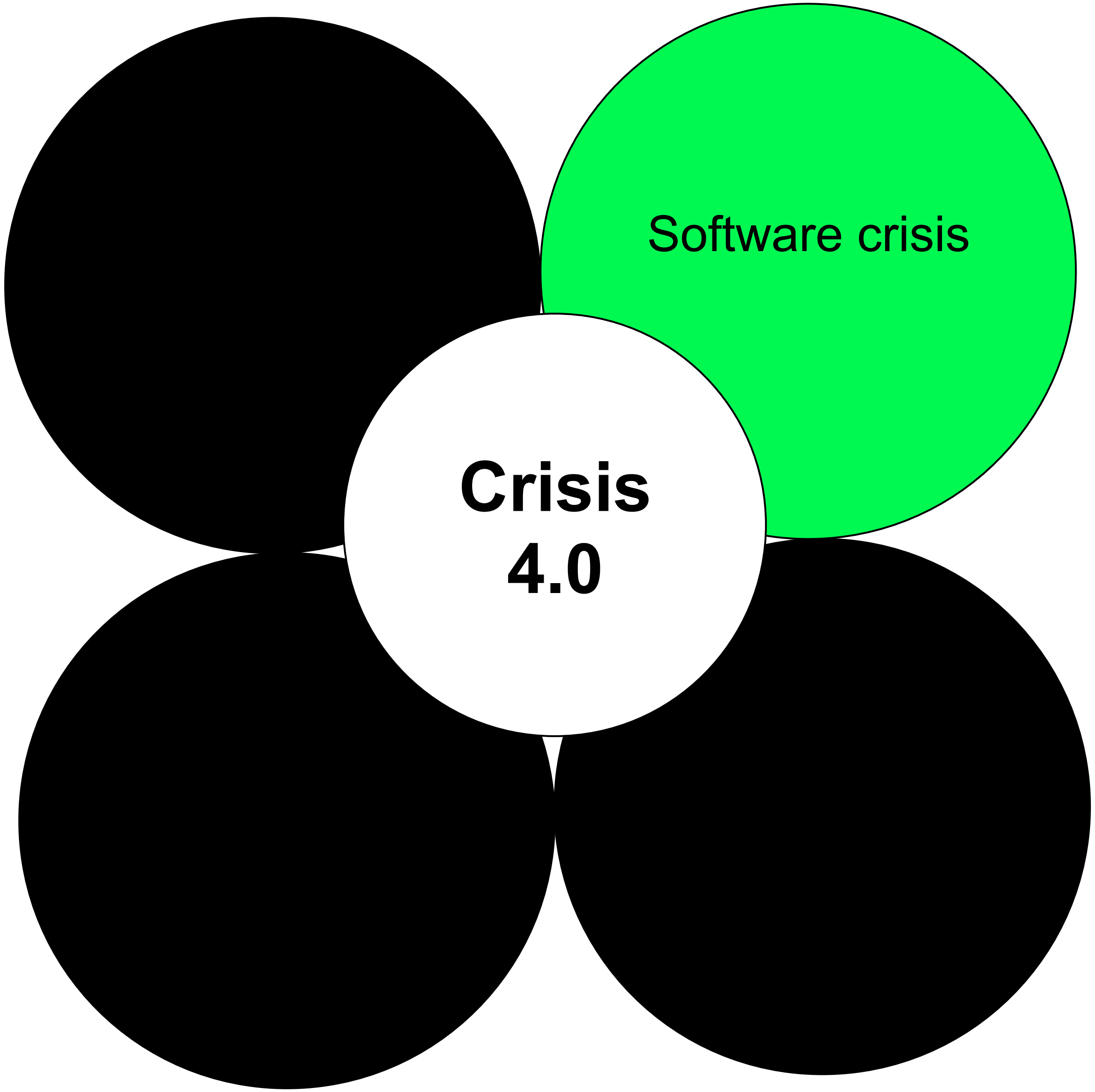
Trust crisis

Crisis 4.0 – this talk

Munich IT Security Research Group

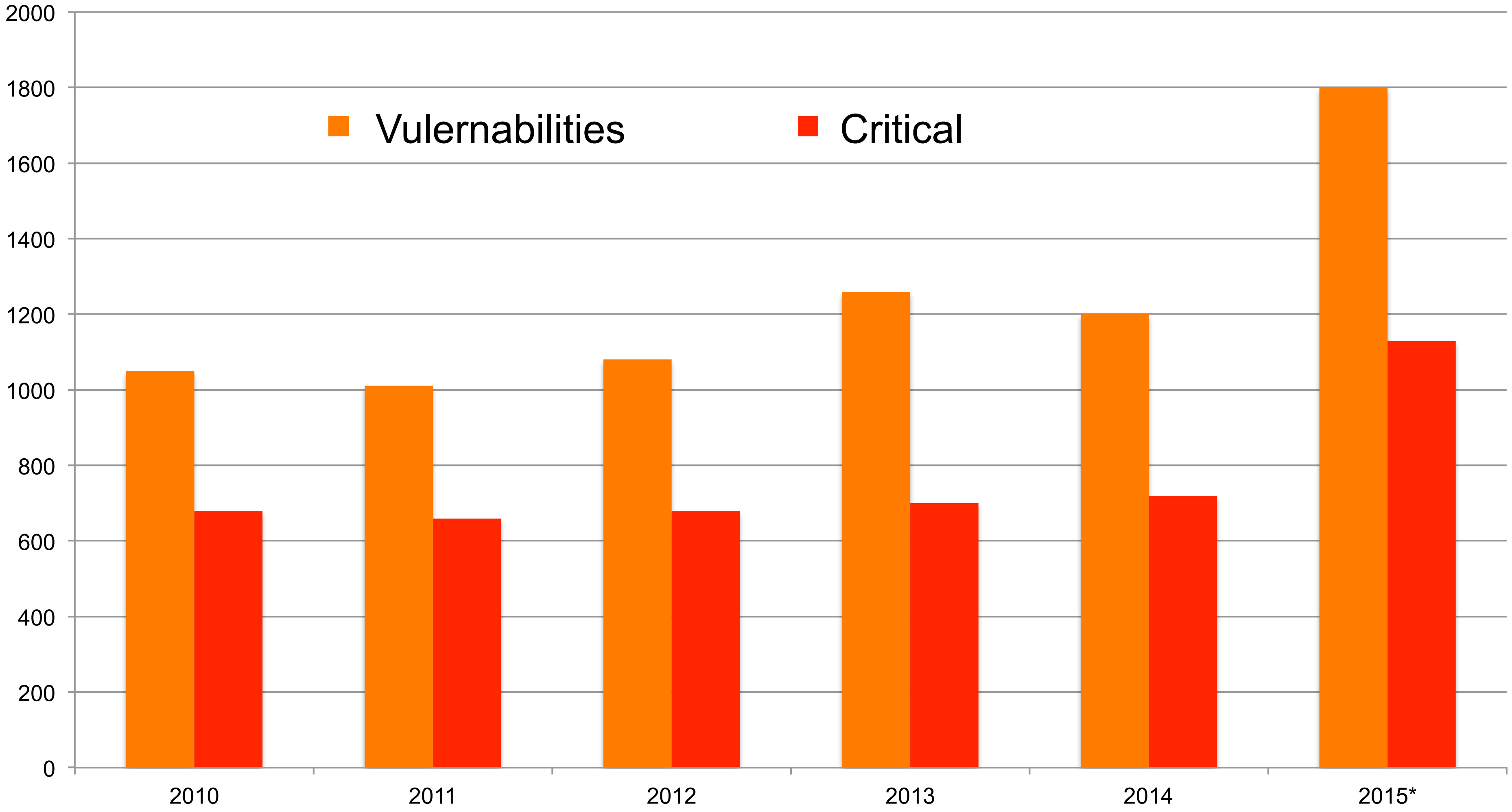


Crisis 4.0 – the software crisis

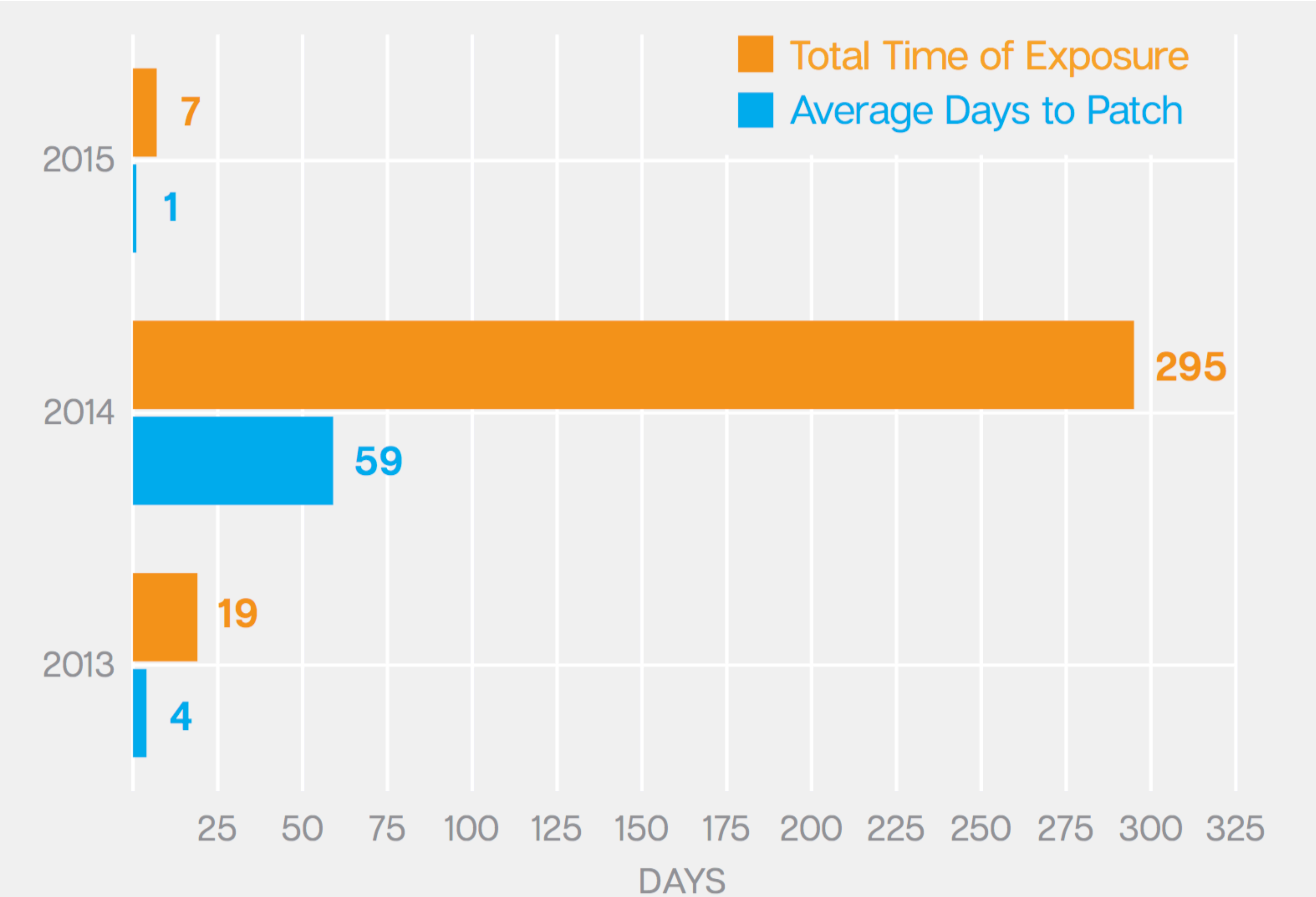


Vulnerabilities

- Vulnerabilities for 13 popular standard software products (BSI):



Software Crisis: Handling of vulnerabilities



Source: Symantec Internet Security Threats Report

Software Crisis: Handling of vulnerabilities

- Study of Heartbleed attack: Number of vulnerable hosts
  - Day 0 : 600.000
  - Day 0 + 30 : 300.000
  - Day 0 + 60 : 300.000 (!!!)
  - 43 % of admins tried to close vulnerability, only 14% succeeded

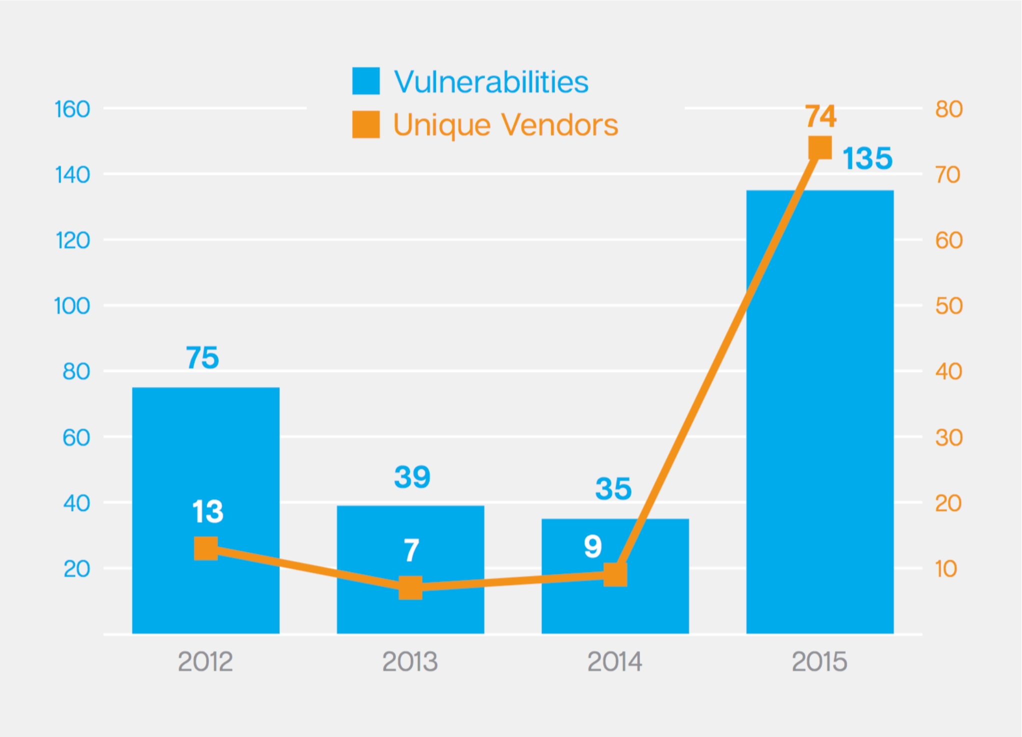
- Evaluation of web application vulnerabilities
  - 75% of websites had unpatched vulnerabilities
  - 15% of websites had critical unpatched vulnerabilities
  - Numbers do not change over years!!!

Software Crisis: Can figures be transfered to new domains?

Munich IT Security Research Group

- McAffee: IoT devices often stay unpatched („installed and forgotten“)

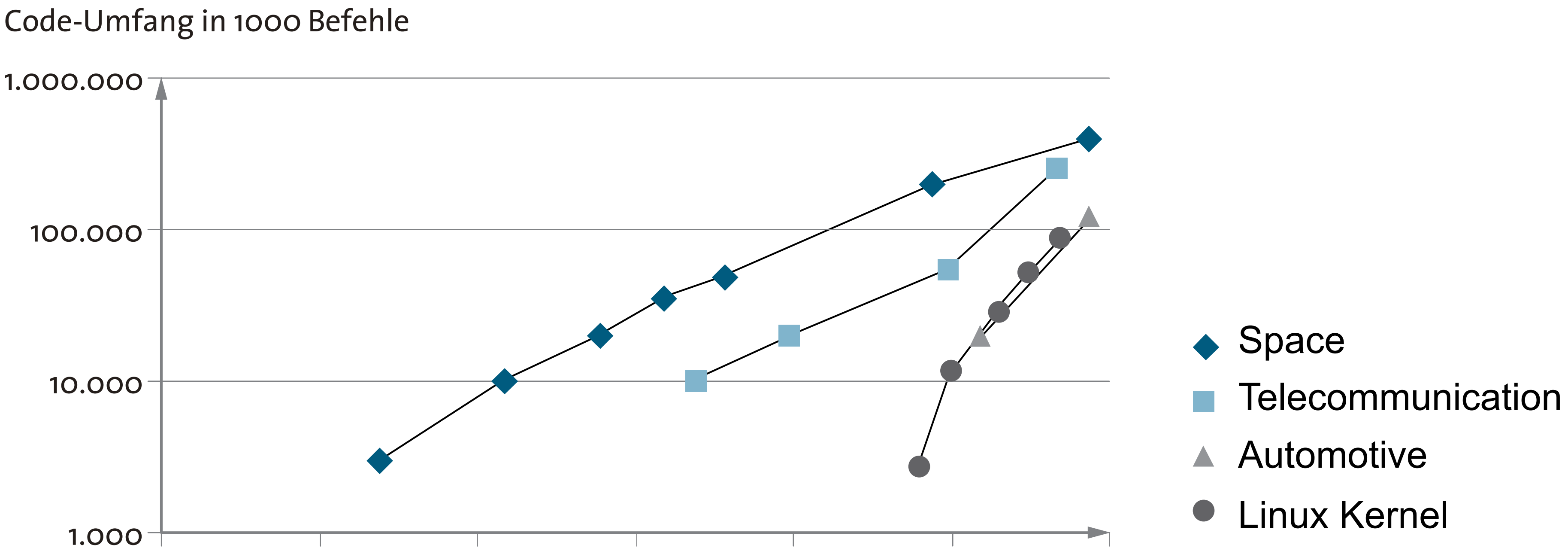
- Vulnerablities of Industrial Control Systems (Symantec):



Software Crisis: Can figures be transfered to new domains?

Munich IT Security Research Group

- Many domains with complexity higher than standard IT



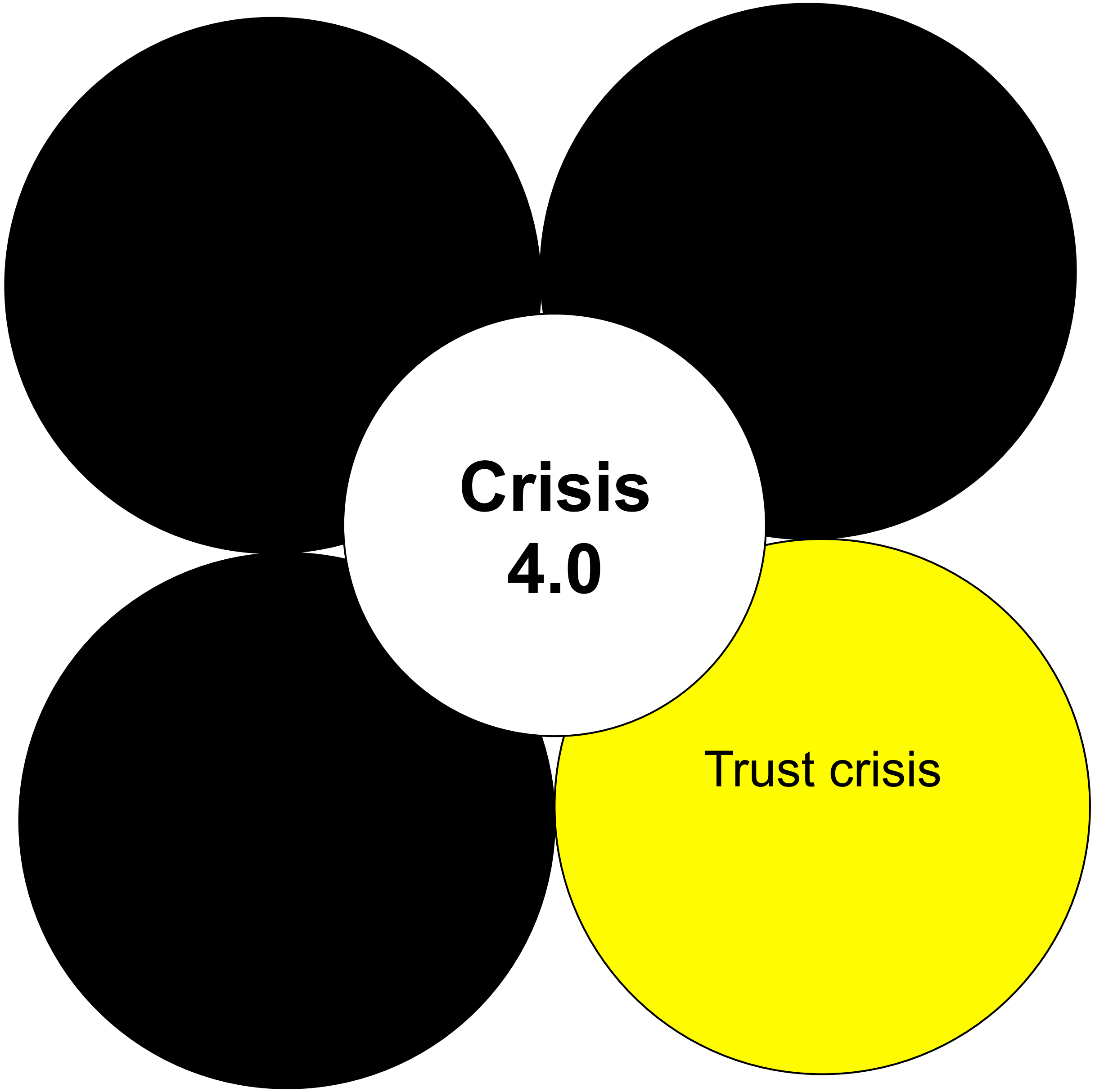
Quelle: Bitkom „Eingebettete Systeme – ein strategisches Wachstumsfeld für Deutschland“

- There is hope: Other domains (e.g., automotive) achieve high quality of non-functional requirements (e.g., safety)

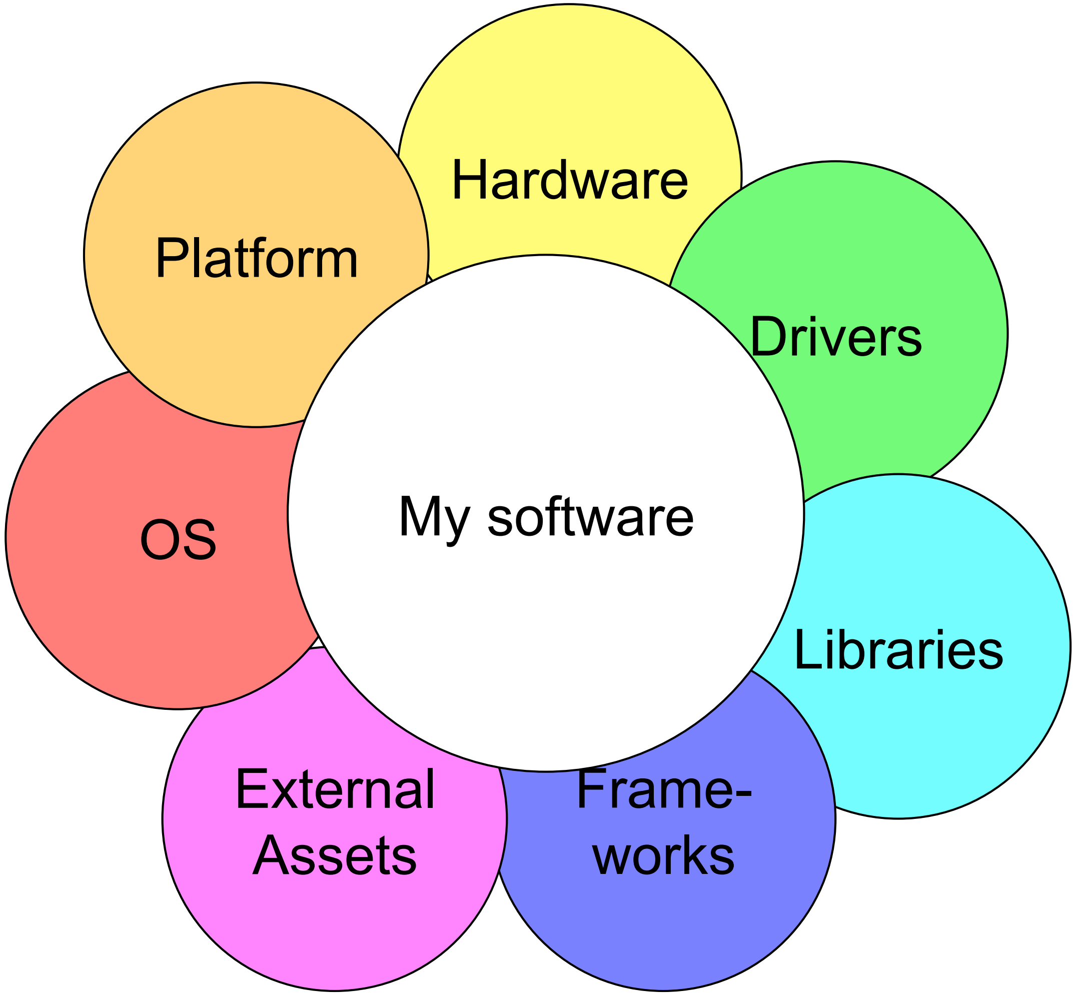
Necessary actions

- Increase activities to ensure software quality
- Design:
  - Goal: Resilient systems
  - Don‘t forget a software update mechanism, system may live for a long time
  - Learn from safety
- Legislation:
  - Enforce „Security by Design“ similar to safety and privacy
  - We need a law stating a strong liability for software
- Risk-based approach
  - Goal should be: „zero vulnerabilities“
  - Offer transparent risk rating
- Increase security education for computer scientists and electrical engineers

Crisis 4.0



External data and code in own software



Examples

- CVE-2015-3036 (04/2015): KCodes NetUSB Linux Kernel driver with buffer overflow vulnerability
  - Used in routers of TP-Link, D-Link, Trendnet, Netgear, Zyxel
- Foscom surveillance camera uses IOTC Platform
  - P2P network for NAT-NAT-Traversal
  - Controlled by a chinese company (ThoroughTek)
- ZigBee Home Automation 1.2
- Buffer Overflow in OpenSSL library (Heartbleed attack)
- ...

Trustworthiness of foreign software

Image removed for web version

Trustworthiness of Open Source Software

- Often heard: „An error in open source software does not go unnoticed for a long time“

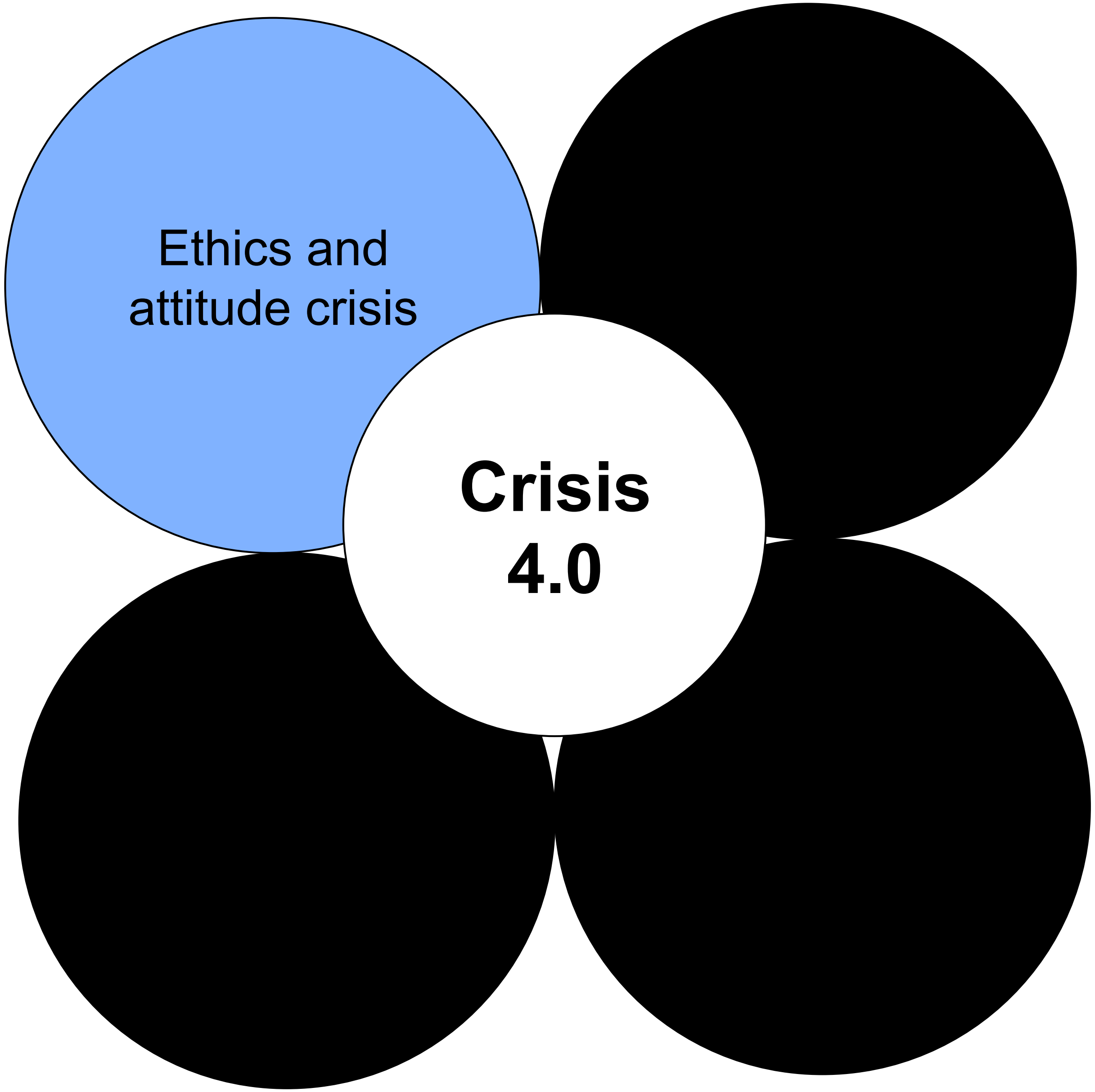
- Recent counterexamples:
  - Heartbleed bug
  - Shell Shock

- It is evident to rethink the use of open source software

Necessary actions

- It is necessary to have a European security-certified platform (hardware, OS)
- We need diversity of ciritical resources (e.g., crypto library)
- Developers should not be feature creepers

Crisis 4.0 - Ethics and attitude crisis



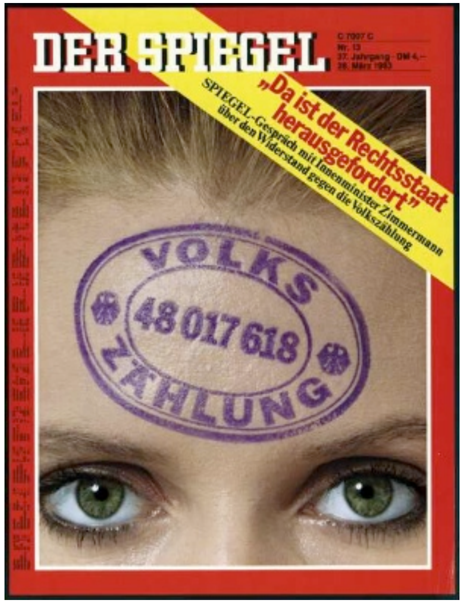
Ethics and attitude crisis

DER SPIEGEL
„Da ist der Rechtsstaat herausgefordert"
SPIEGEL-Gespräch mit Innenminister Zimmermann über den Widerstand gegen die Volkszählung
VOLKS
48 017 618
ZÄHLUNG

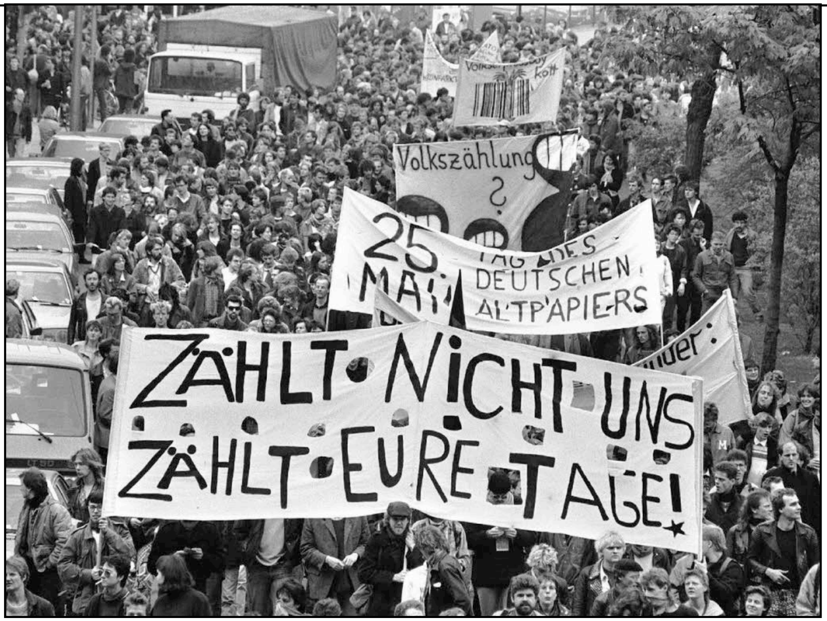
1983

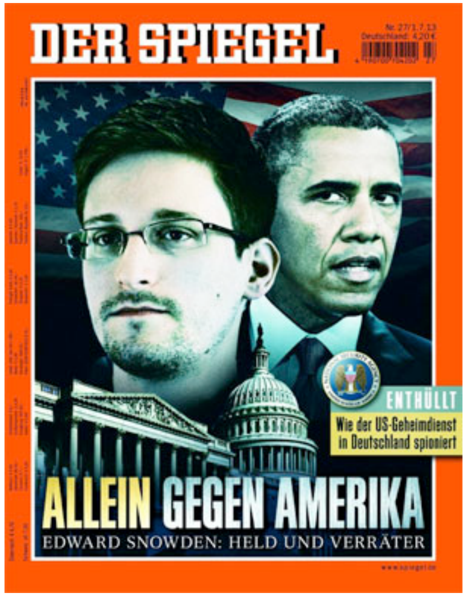
Volkszählung ?
25. MAI
TAG DES DEUTSCHEN ALTPAPIERS
ZÄHLT NICHT UNS ZÄHLT EURE TAGE!

Ethics and attitude crisis


DER SPIEGEL
C 7007 C
Nr. 13
37. Jahrgang · DM 4,–
28. März 1983
„Da ist der Rechtsstaat herausgefordert"
SPIEGEL-Gespräch mit Innenminister Zimmermann über den Widerstand gegen die Volkszählung
VOLKS
48017618
ZÄHLUNG

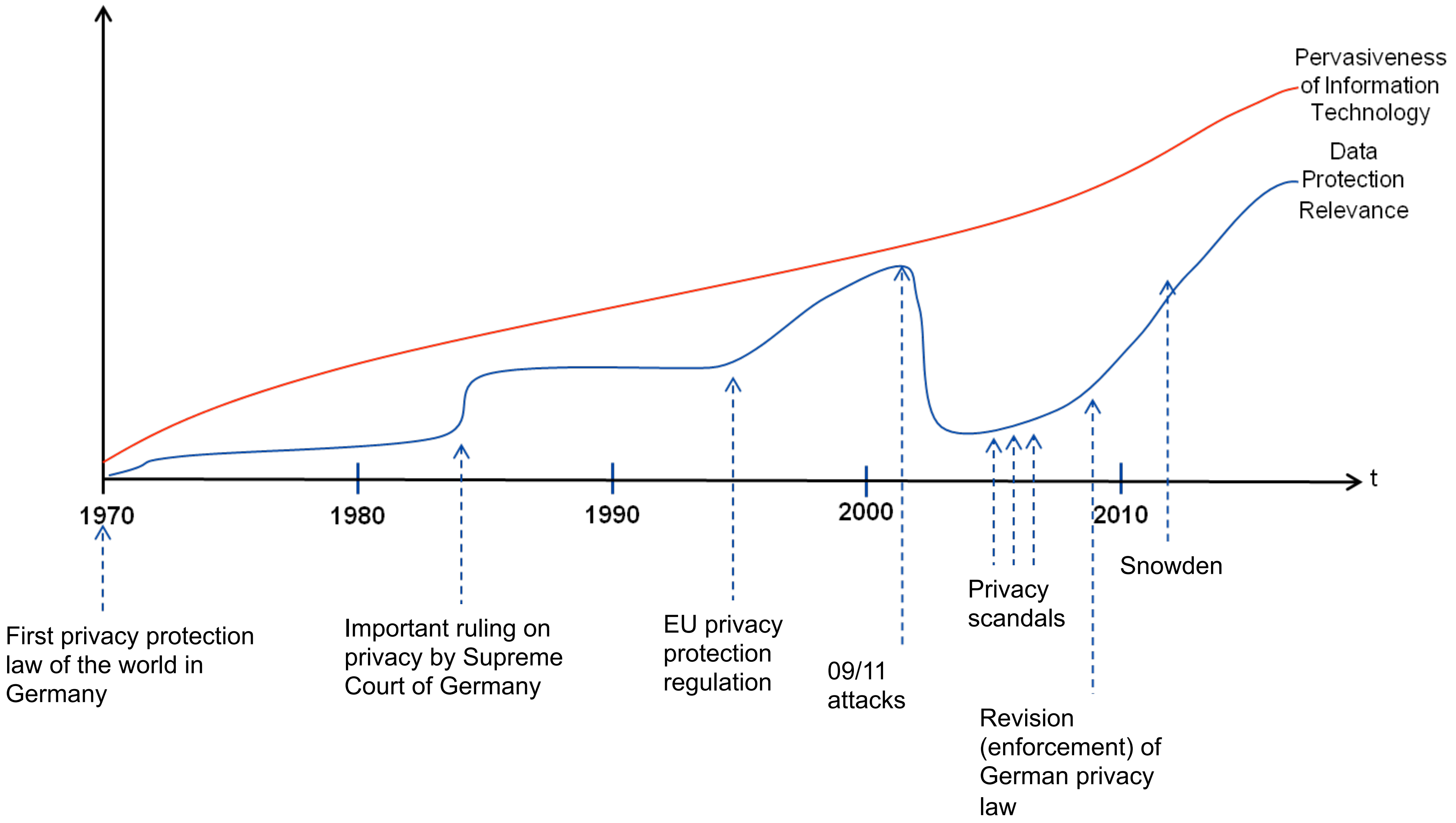
1983


Volkszählung ?
25. MAI
TAG DES DEUTSCHEN ALTPAPIERS
ZÄHLT NICHT UNS ZÄHLT EURE TAGE!


DER SPIEGEL
ENTHÜLLT
Wie der US-Geheimdienst in Deutschland spioniert
ALLEIN GEGEN AMERIKA
EDWARD SNOWDEN: HELD UND VERRÄTER

2013

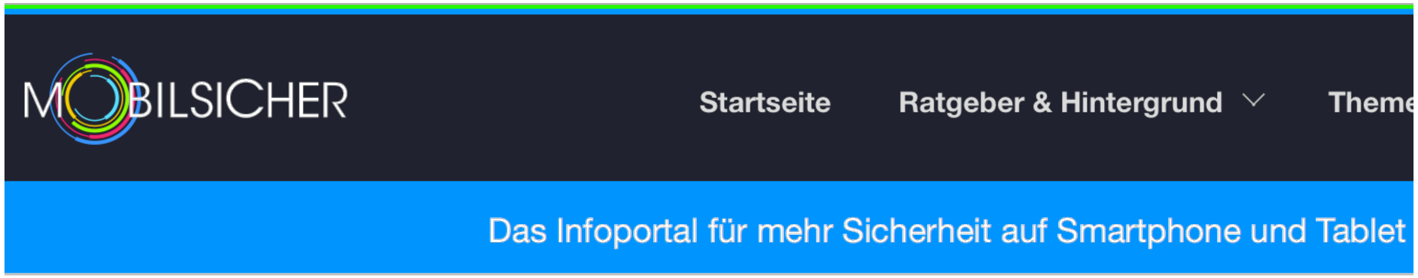
Attitude of society



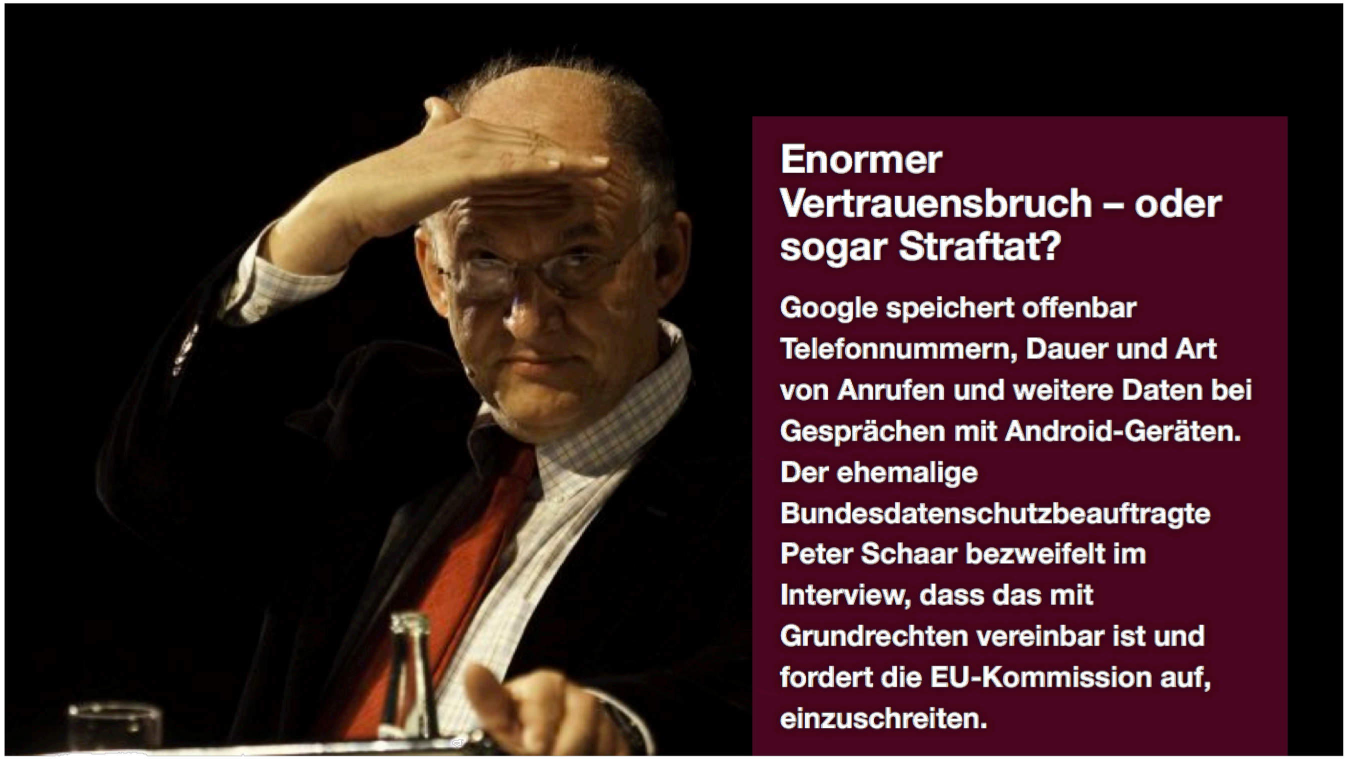
Source: Miguel Reiser, „Was verbirgt sich hinter dem Begriff Managing Trust?“

Attitude of companies

Culture of free stuff:
„If an online service is free, you are not the customer. You are the product“



Das Infoportal für mehr Sicherheit auf Smartphone und Tablet



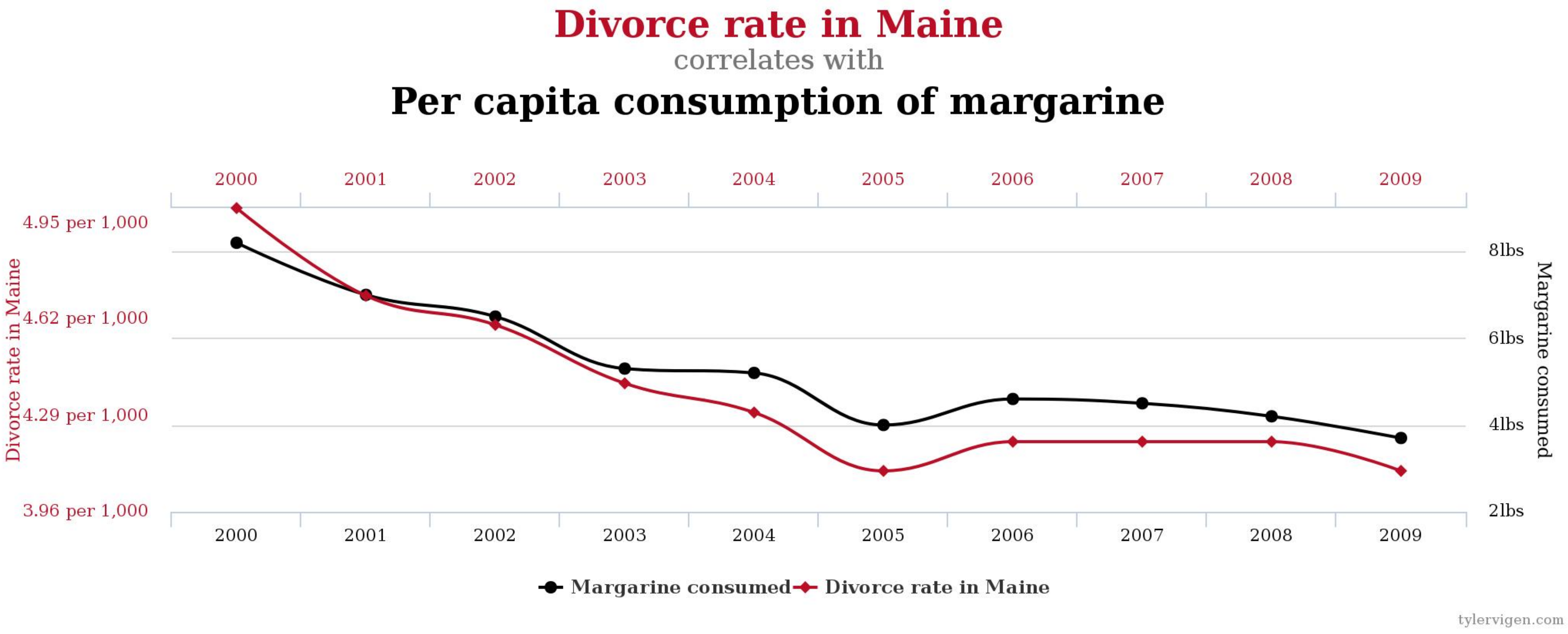
Enormer Vertrauensbruch – oder sogar Straftat?

Google speichert offenbar Telefonnummern, Dauer und Art von Anrufen und weitere Daten bei Gesprächen mit Android-Geräten. Der ehemalige Bundesdatenschutzbeauftragte Peter Schaar bezweifelt im Interview, dass das mit Grundrechten vereinbar ist und fordert die EU-Kommission auf, einzuschreiten.

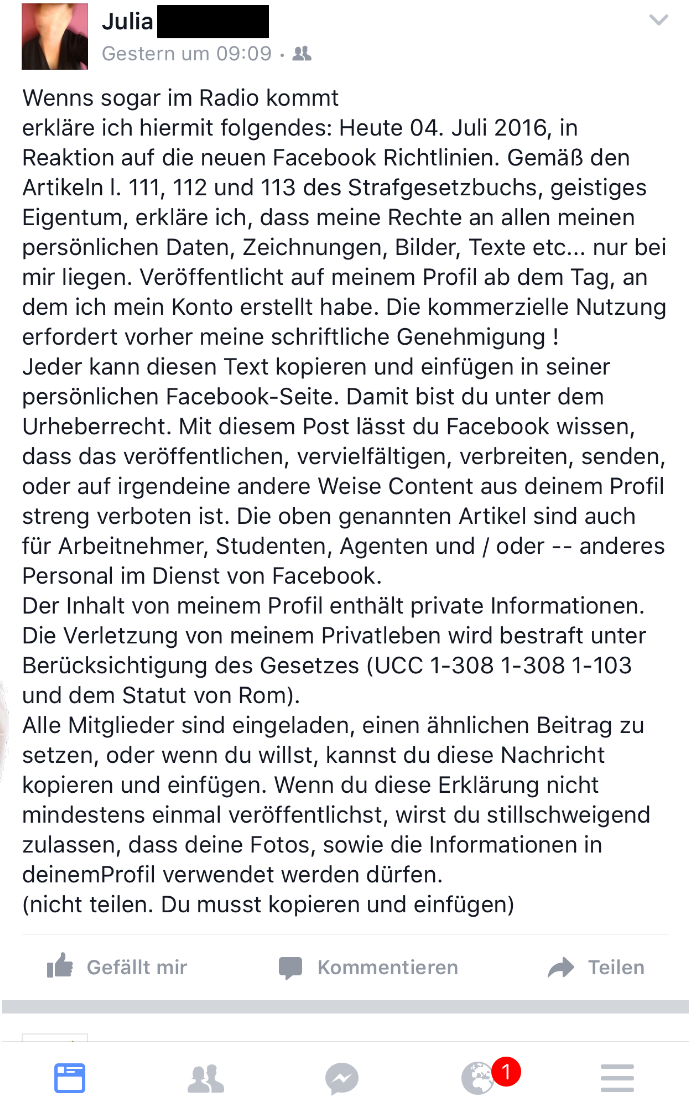
Attitude of companies

Image removed for web version

Attitude of companies: insufficient tools for easy answers



Attitude of users

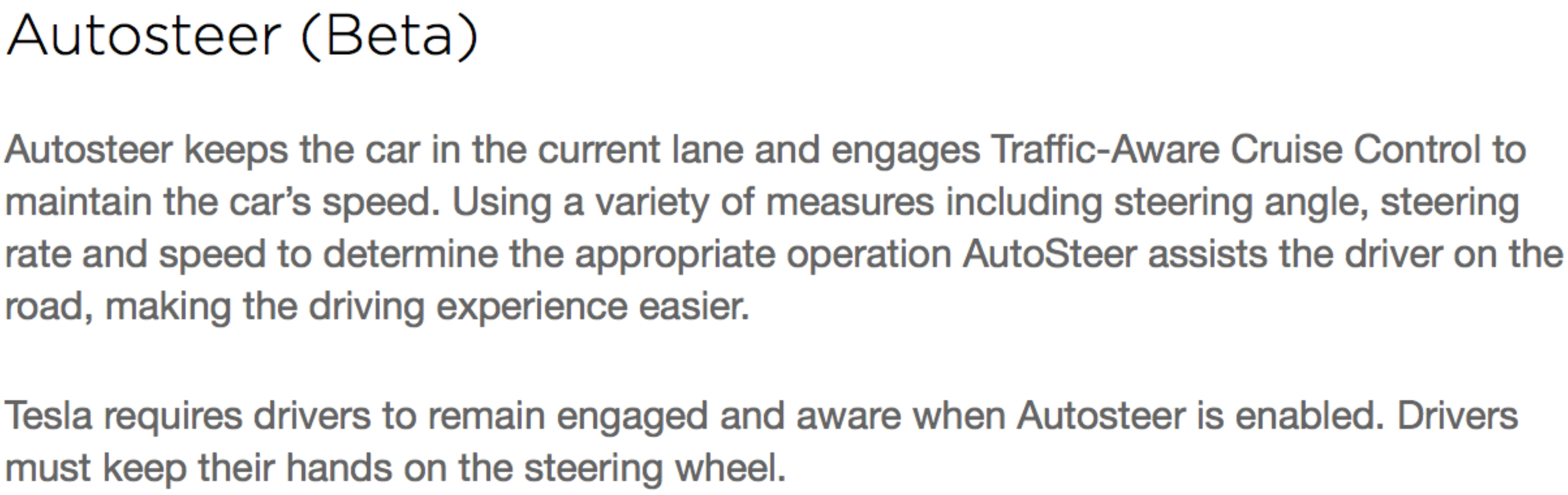


Julia [redacted]

Gestern um 09:09 ·

Wenns sogar im Radio kommt
erkläre ich hiermit folgendes: Heute 04. Juli 2016, in Reaktion auf die neuen Facebook Richtlinien. Gemäß den Artikeln l. 111, 112 und 113 des Strafgesetzbuchs, geistiges Eigentum, erkläre ich, dass meine Rechte an allen meinen persönlichen Daten, Zeichnungen, Bilder, Texte etc... nur bei mir liegen. Veröffentlicht auf meinem Profil ab dem Tag, an dem ich mein Konto erstellt habe. Die kommerzielle Nutzung erfordert vorher meine schriftliche Genehmigung !
Jeder kann diesen Text kopieren und einfügen in seiner persönlichen Facebook-Seite. Damit bist du unter dem Urheberrecht. Mit diesem Post lässt du Facebook wissen, dass das veröffentlichen, vervielfältigen, verbreiten, senden, oder auf irgendeine andere Weise Content aus deinem Profil streng verboten ist. Die oben genannten Artikel sind auch für Arbeitnehmer, Studenten, Agenten und / oder -- anderes Personal im Dienst von Facebook.
Der Inhalt von meinem Profil enthält private Informationen. Die Verletzung von meinem Privatleben wird bestraft unter Berücksichtigung des Gesetzes (UCC 1-308 1-308 1-103 und dem Statut von Rom).
Alle Mitglieder sind eingeladen, einen ähnlichen Beitrag zu setzen, oder wenn du willst, kannst du diese Nachricht kopieren und einfügen. Wenn du diese Erklärung nicht mindestens einmal veröffentlichst, wirst du stillschweigend zulassen, dass deine Fotos, sowie die Informationen in deinemProfil verwendet werden dürfen.
(nicht teilen. Du musst kopieren und einfügen)

Attitude of users/government: Tesla autopilot

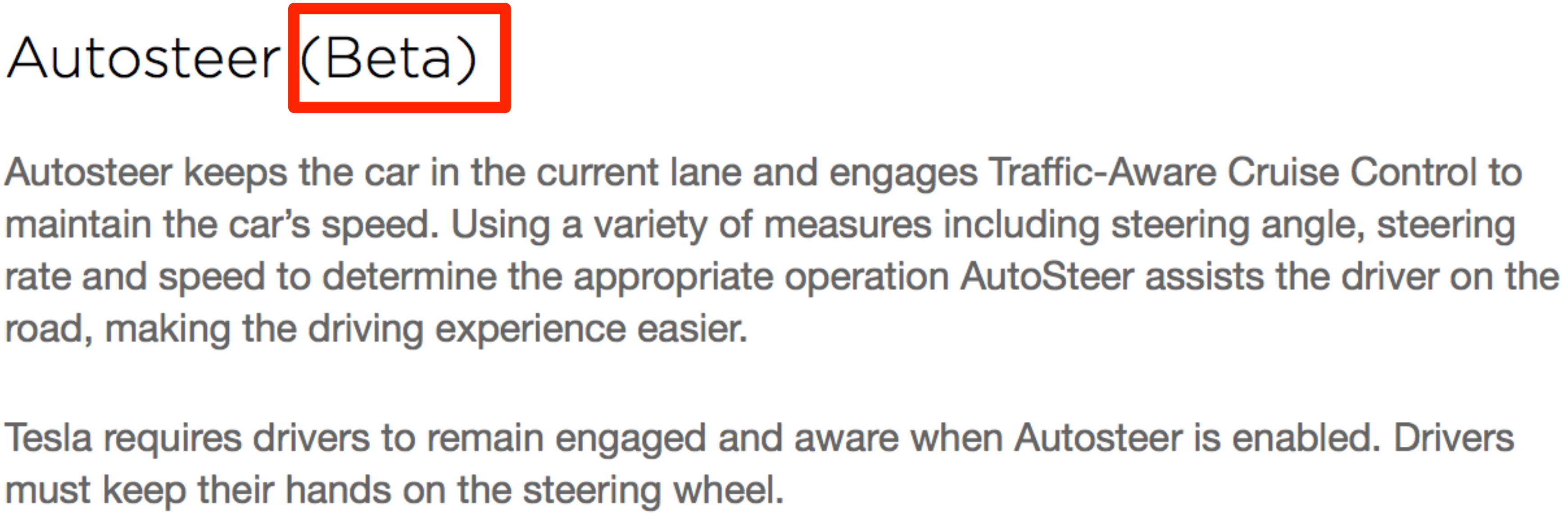


Autosteer (Beta)

Autosteer keeps the car in the current lane and engages Traffic-Aware Cruise Control to maintain the car’s speed. Using a variety of measures including steering angle, steering rate and speed to determine the appropriate operation AutoSteer assists the driver on the road, making the driving experience easier.

Tesla requires drivers to remain engaged and aware when Autosteer is enabled. Drivers must keep their hands on the steering wheel.

Attitude of users/government: Tesla autopilot



Autosteer (Beta)

Autosteer keeps the car in the current lane and engages Traffic-Aware Cruise Control to maintain the car's speed. Using a variety of measures including steering angle, steering rate and speed to determine the appropriate operation AutoSteer assists the driver on the road, making the driving experience easier.

Tesla requires drivers to remain engaged and aware when Autosteer is enabled. Drivers must keep their hands on the steering wheel.

Privacy in the IoT

- It gets more and more impossible to protect one‘s privacy by own action
  - IoT devices use sensors to collect data about people in sensor range
  - Many IoT devices used in public space

- Privacy 2020:

?

?

There is hope: EU data protection act

- Immediately effective for whole EU, no national loopholes
- Broad scope
- Enforces "Privacy by Design"
- Violations can be punished (max. 3% of total revenue)

Necessary actions

- Defeat loopholes in EU Data Privacy Act

- Discuss codes of conduct

Association for Computing Machinery
Advancing Computing as a Science & Profession

The Code

ACM Code of Ethics and Professional Conduct

ACM promotes the highest professional and ethical standards through The Code created to uphold the belief that the power of computing technology should be harnessed for the benefit of society.

The Code guides ACM Members in their professional conduct to:

- Contribute to society and human well-being
- Avoid harm to others
- Be honest and trustworthy
- Be fair; take action not to discriminate
- Honor property rights, i.e. copyrights & patents
- Give proper credit for intellectual property
- Respect the privacy of others
- Honor confidentiality

ACM Members will fulfill their commitment to The Code through:

- The highest quality and effectiveness in professional work
- Professional competence
- Respect for existing laws pertaining to professional work
- Appropriate professional review
- Comprehensive evaluations of computer systems and impacts
- Honored contracts, agreements and assigned responsibilities
- Public understanding of computing and its consequences
- Authorized access to computing and communication resources

Access to the complete ACM Code of Ethics & Professional Conduct is at www.acm.org/about/code-of-ethics

- Sensibilize for security, safety, and privacy, review own behavior

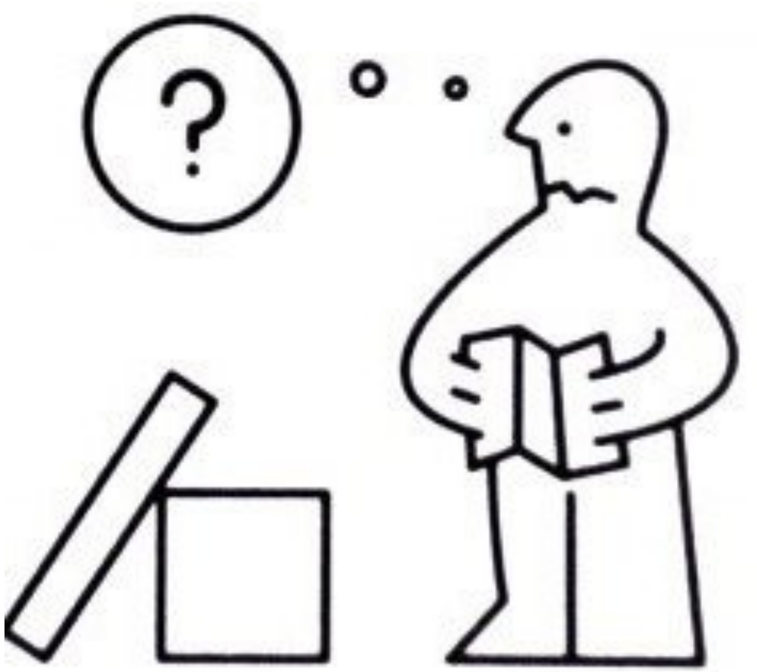
- Avoid the next data privacy scandal when developing the Internet of Things

Conclusion

Fighting crisis 4.0 means...

- ... focusing on software quality
- ... reducing dependencies on other software as well as on foreign products
- ...reawaken interest for non-functional requirements like privacy, security, and safety
- ...educate for ethical behavior

Discussion



For offline questions please contact hof@insi.science