FREMTIDENS SIKKERHETS-UTFORDRINGER

Ketil Stølen

SINTEF og Universitetet i Oslo

Fremtiden?

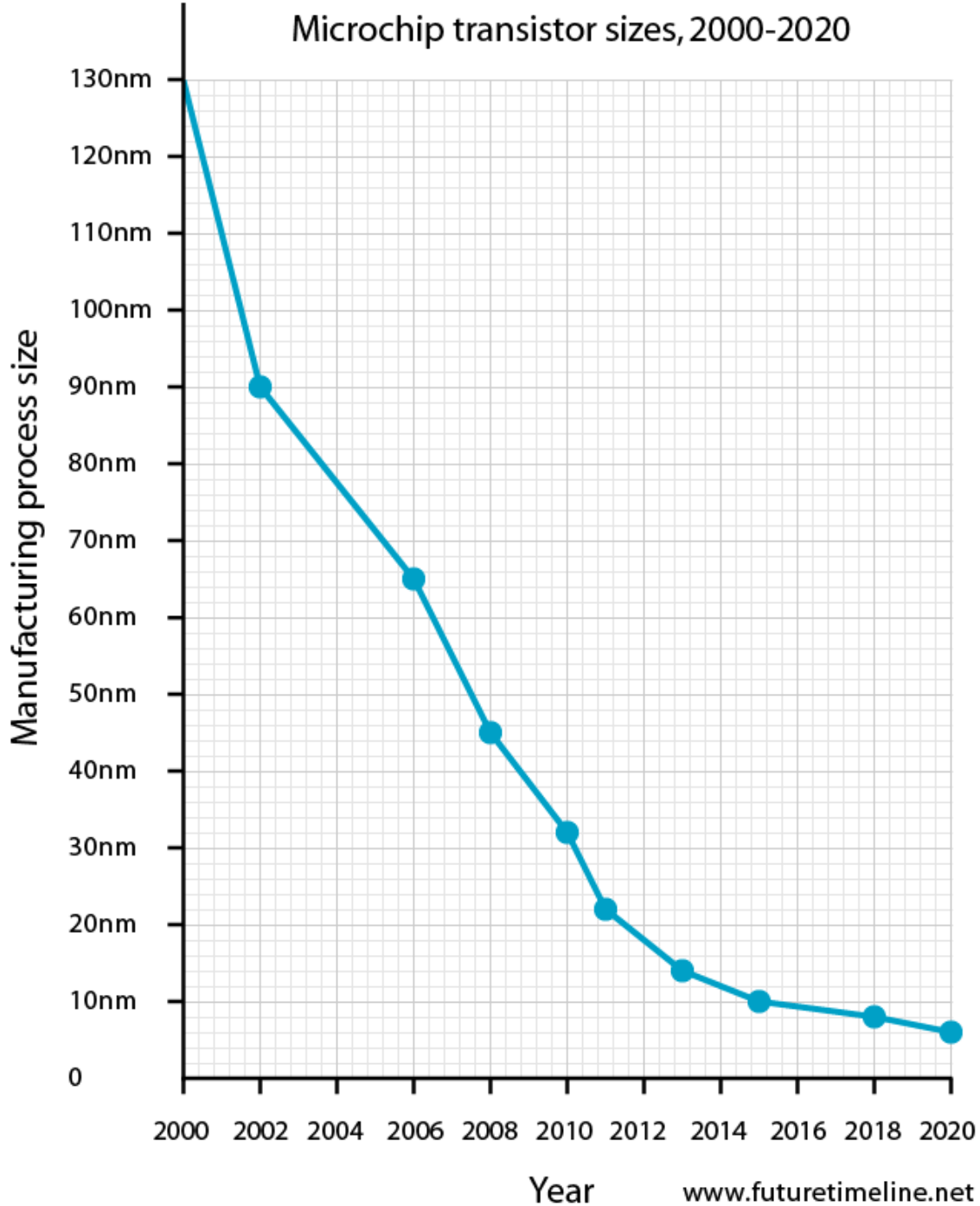
Fremtiden = om 10 år

Hva har endret seg siden jeg var student?

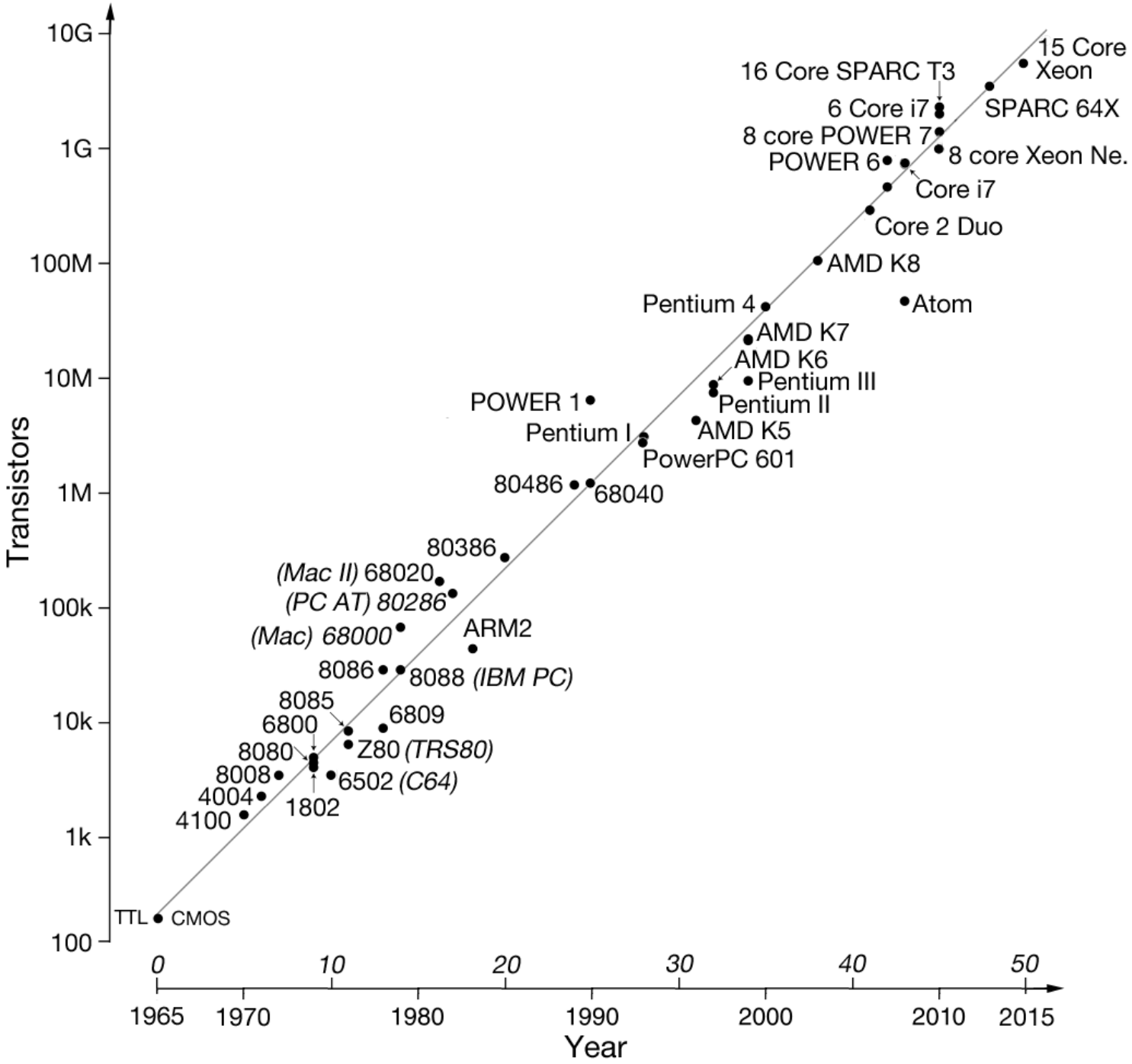
- Maskinvaren?
- Programvaren?
- Bruken?

Hva har endret seg siden jeg var student?

- Maskinvaren?


Microchip transistor sizes, 2000-2020
Manufacturing process size
130nm
120nm
110nm
100nm
90nm
80nm
70nm
60nm
50nm
40nm
30nm
20nm
10nm
0
2000
2002
2004
2006
2008
2010
2012
2014
2016
2018
2020
Year
www.futuretimeline.net

SINTEF



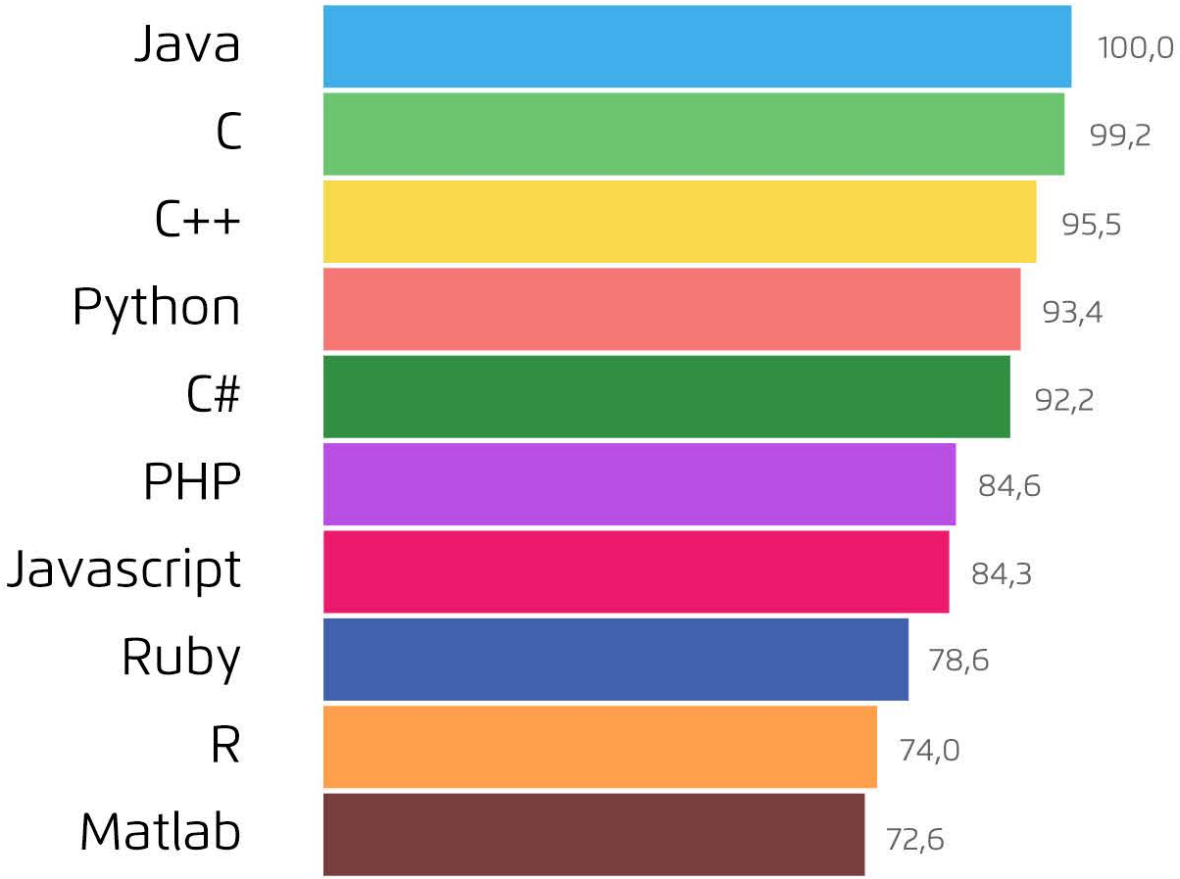
Gordon Moore

SINTEF

Hva har endret seg siden jeg var student?

- Programvaren?

The Top Programming Languages - IEEE Spectrum's 2014



Get more information at
http://spectrum.ieee.org/static/interactive-the-top-programming-languages

codeanywhere

SINTEF

Hva har endret seg siden jeg var student?

- Bruken?

Sikkerhetsutfordingene ligger i bruken

To fremtidsutsikter

- Disruptiv – f.eks. vi får kvantedatamaskiner, eller en 9/11 lignende IT-hendelse

- Kontinuerlig men eksponentiell utvikling som inntil nå

Hva hvis vi har kvantedatamaskiner?

Kvantedatamaskiner

- Utfører logiske operasjoner basert på kvantemekaniske prosesser
- Kalkulerer ved hjelp av qubits
- En qubit kan være i flere tilstander på en gang
- Veldig effektivt ved søking og faktorering

SINTEF

Konsekvens for asymmetrisk kryptering

- Dagens løsninger for asymmetrisk kryptering vil ikke skalere
- En kvantedatamaskin kan finne den private nøkkelen for en offentlig nøkkel på kort tid

Konsekvens for symmetrisk kryptering

- Styrke redusert med 50 %
- F.eks. 128 bits symmetrisk nøkkel vil ha styrken til en 64 bits symmetrisk nøkkel av i dag

Hva hvis utviklingen forsetter i samme takt?

STUDY

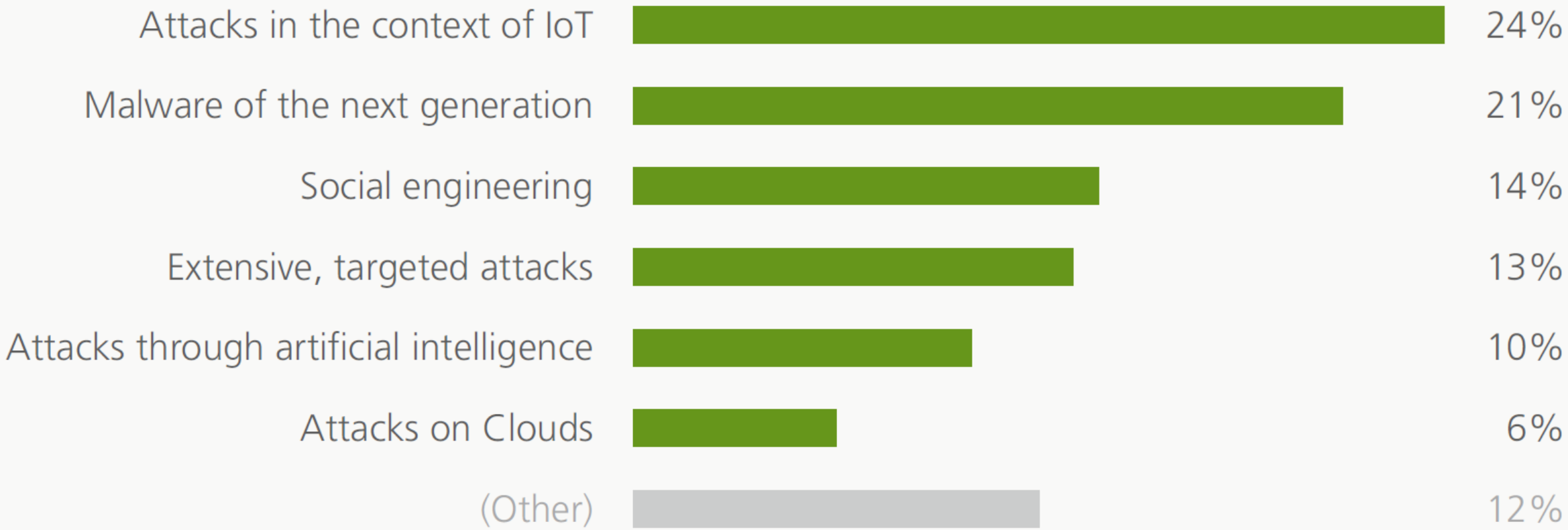
Cyber attacks and IT security management in 2025

Expert survey concerning future trends and challenges in IT security

https://www.radarservices.com/study2025/

SINTEF

With which type of cyber attacks will we be confronted with in 2025?



SINTEF

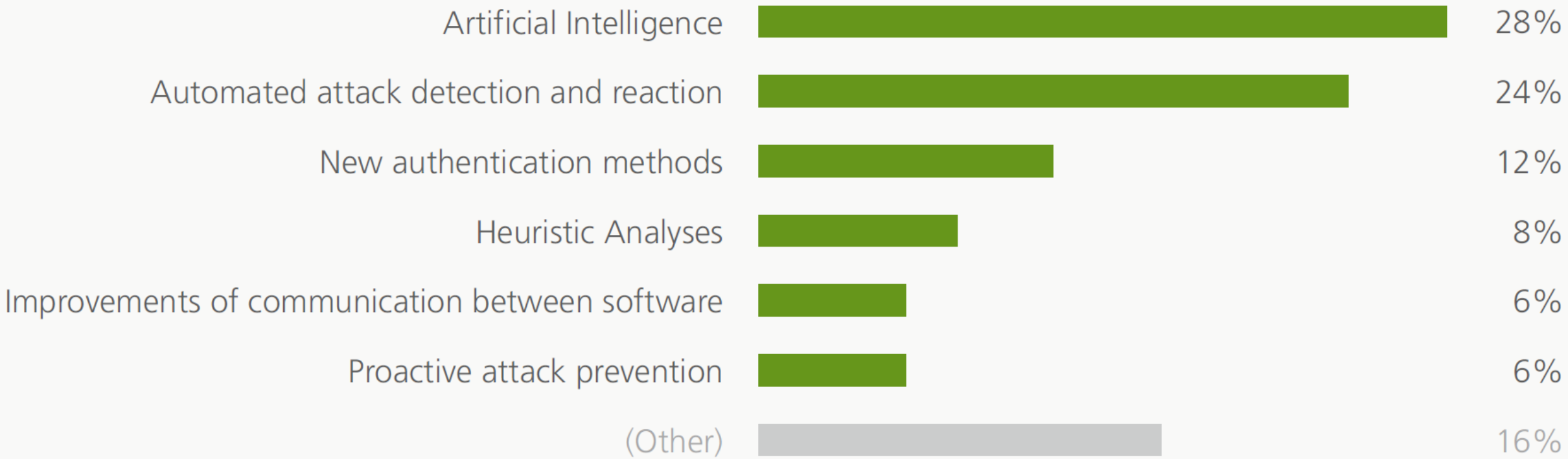
IoT problem I: Utilstrekkelig teknologi

- IT leverandørene tilbyr stadig nye IoT plattformer
  - alt mer enn 400 på verdensbasis
- På toppen av lite testa og ofte umodne produkter integreres tingene
- Tingene er bygget og designet for et helt annet sikkerhetsbehov
  - vanskelig å sikre pga liten batterikapasitet, beregningskraft og/eller hukommelse

IoT problem II: Kolossal angrepsflate

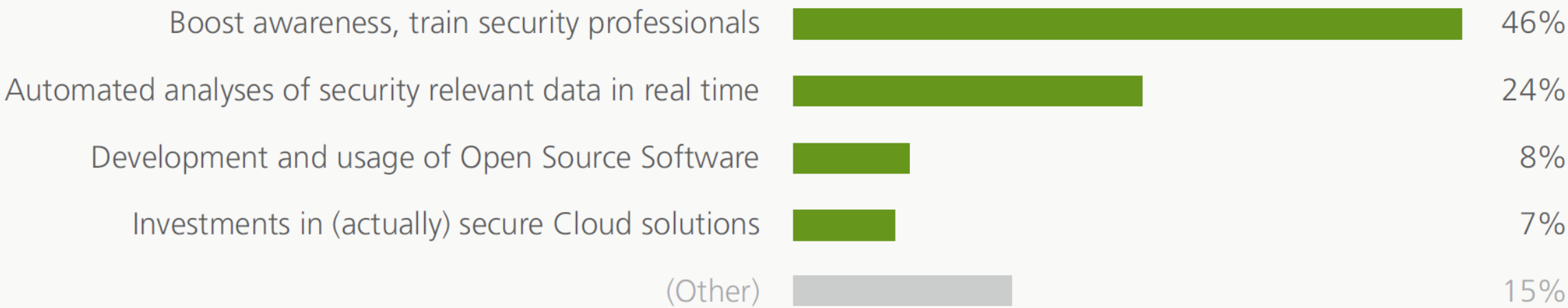
- Alt fornettes og kan potensielt nås fra overalt i verden
- Satt på spissen, en strømmast som tidligere kun kunne hugges ned eller sprenges, kan i fremtiden settes ut av drift elektronisk fra den andre siden av kloden

What do IT security technologies have to offer in 2025?



SINTEF

In which areas of IT security companies need to invest in order to be viable in 2025?



SINTEF

Digital Life in 2025

The Future of Privacy

Lee Rainie, Director, Internet, Science, and Technology Research, Pew Research

Janna Anderson, Director, Elon University's Imagining the Internet Center

202.419.4372

www.pewresearch.org

SINTEF

55% of the respondents said “no” they do not believe that an accepted privacy-rights regime and infrastructure would be created in the coming decade

45% said “yes” that such an infrastructure would be created by 2025

Flertallets synspunkter:

- Living a public life is the new default
- It is not possible to live modern life without revealing personal information to government and corporations
- Few individuals will have the energy or resources to protect themselves from dataveillance
- Privacy becomes a luxury

Flertallets synspunkter:

- There is no way the world's varied cultures, with their different views about privacy, will be able to come to an agreement on how to address civil liberties issues on the global Internet

Flertallets synspunkter:

- The situation will worsen as the Internet of Things arises and people's homes, workplaces, and the objects around them will "tattle" on them
- The incentives for businesses to monetize people's data and governments to monitor behavior are extremeley potent

Rosa, Hartmut (2013). *Social Acceleration: A New Theory of Modernity*. New York: Columbia University Press.

Akselerasjon på tre nivåer

- Teknologisk akselerasjon
- Akselerasjon av samfunnsmessig endring
- Akselerasjon av livstempo

akselerasjon
Teknologisk
Samfunnsmessig
Personlig

akselerasjon	karakterisert ved
Teknologisk	
Samfunnsmessig	
Personlig	

akselerasjon	karakterisert ved
Teknologisk	Tingenes Internett
Samfunnsmessig	
Personlig	

akselerasjon	karakterisert ved
Teknologisk	Tingenes Internett
Samfunnsmessig	Kontraksjon av nuet
Personlig	

akselerasjon	karakterisert ved
Teknologisk	Tingenes Internett
Samfunnsmessig	Kontraksjon av nuet
Personlig	Multitasking

akselerasjon	karakterisert ved	sikkerhet krever
Teknologisk	Tingenes Internett	
Samfunnsmessig	Kontraksjon av nuet	
Personlig	Multitasking	

akselerasjon	karakterisert ved	sikkerhet krever
Teknologisk	Tingenes Internett	Overvåkning
Samfunnsmessig	Kontraksjon av nuet	
Personlig	Multitasking	

akselerasjon	karakterisert ved	sikkerhet krever
Teknologisk	Tingenes Internett	Overvåkning
Samfunnsmessig	Kontraksjon av nuet	Sanntidsanalyse
Personlig	Multitasking	

akselerasjon	karakterisert ved	sikkerhet krever
Teknologisk	Tingenes Internett	Overvåkning
Samfunnsmessig	Kontraksjon av nuet	Sanntidsanalyse
Personlig	Multitasking	Intelligent beslutningsstøtte

akselerasjon	karakterisert ved	sikkerhet krever	implikasjon for personvern
Teknologisk	Tingenes Internett	Overvåkning	
Samfunnsmessig	Kontraksjon av nuet	Sanntidsanalyse	
Personlig	Multitasking	Intelligent beslutningsstøtte	

akselerasjon	karakterisert ved	sikkerhet krever	implikasjon for personvern
Teknologisk	Tingenes Internett	Overvåkning	"vi vet hvem du er"
Samfunnsmessig	Kontraksjon av nuet	Sanntidsanalyse	
Personlig	Multitasking	Intelligent beslutningsstøtte	

akselerasjon	karakterisert ved	sikkerhet krever	implikasjon for personvern
Teknologisk	Tingenes Internett	Overvåkning	"vi vet hvem du er"
Samfunnsmessig	Kontraksjon av nuet	Sanntidsanalyse	"vi vet hva du gjør"
Personlig	Multitasking	Intelligent beslutningsstøtte	

akselerasjon	karakterisert ved	sikkerhet krever	implikasjon for personvern
Teknologisk	Tingenes Internett	Overvåkning	"vi vet hvem du er"
Samfunnsmessig	Kontraksjon av nuet	Sanntidsanalyse	"vi vet hva du gjør"
Personlig	Multitasking	Intelligent beslutningsstøtte	"vi vet hva du vil gjøre"

Er dette bra?

Er dette svartmaling?

Hva mener dere?