NTNU CCIS
Center for Cyber and Information Security

Cyber and Information security - a future with possibilities

Sokratis K. Katsikas
Center for Cyber & Information Security
Norwegian University of Science & Technology
sokratis.katsikas@ntnu.no

Attempting to predict the future is risky

"I think there is a world market for maybe five computers."

Thomas Watson, president of IBM, 1943

Who are we?

Institutt for informasjonssikkerhet og kommunikasjonsteknologi (IIK)

- 80 ansatte i Gjøvik og Trondheim
- Forskningsgrupper og -laboratorier innen avhengighet og ytelse, biometri, cyberforsvar, forensics, intelligente transportsystemer, internet of things, informasjonssikkerhetsledelse, kritisk infrastruktur, kryptografi, skadevare, e-helse og velferd
- 1 bachelor- (70), 2 master- (74 + 25), 1 siv.ing- (45) og 2 PhD-utdanninger
- Forskningsprosjekter: EU H2020 (5), EU FP7 (4), EU Cost (1), EDA (1), IARPA Odin Thor (1), NFR FME (1), NFR IKT+ (4), NFR ENERGIX (1), NFR BIA (2), NFR Forskerskole (1), NFR NæringsPhD (1), RFF (4)
  Omfang ca 40 MNOK i 2017 (45% av budsjettet)
- Vertsinstitutt for NTNUs Center for Cyber and Information Security
- Akademiske konferanser, Cyber symposiet, SikkertNOK, Sikkerhetstoppmøtet

NTNU CCIS
Center for Cyber and Information Security

Information Security and Privacy Management

Cyber Defence

Critical Infrastructure Security and Resilience

e-Health and, Welfare Security

NTNU Digital Forensics Group

Norwegian Biometrics Laboratory

NTNU

Norges teknisk-naturvitenskapelige universitet

NTNU CCIS

Center for Cyber and Information Security

Contact: Sokratis Katsikas
sokratis.katsikas@ntnu.no

Statkraft
IBM
KRIPOS
FORSVARET
Datatilsynet
telenor
NorSIS
NISlab™
mnemonic
FFI
POLITIET OSLO POLITIDISTRIKT
ØKOKRIM
Statnett
NC-Spectrum
Nasjonalt ID-senter
KPMG
NSM
POLITIET
pwc
Eidsiva
OPPLAND fylkeskommune
WATCHCOM
HØGSKOLEN I INNLANDET
POLITIHØGSKOLEN
PST

CISR Group Mission and vision

- To support the private and public sector in their preparedness for and response to security incidents that involve the critical infrastructures of Norway, at the regional and national level, by means of knowledge and capacity building through research, education, and training.
- To become one of the leading academic & research groups for critical infrastructure security and resilience in Europe and beyond.

NTNU CCIS
Center for Cyber and Information Security

People

- **Academic staff**
  - Prof. Sokratis K. Katsikas
  - Prof. Stephen Wolthusen
  - Prof. Bernhard Hämmerli
- **Postdocs**
  - Dr Alessio Baiocco
  - Dr Pankaj Pandey
  - Dr Goitom Weldehawaryat
  - Dr Georgios Spathoulas
  - Dr Gyuri Kalman
- **PhD candidates**
  - Mr Vasileios Gkioulos

Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control

NTNU CCIS
Center for Cyber and Information Security

Future tamper-proof Demand rEsponse framework through seLf-configured, self-opTimized and collAborative virtual distributed energy nodes

D E L T A

NTNU CCIS
Center for Cyber and Information Security

What is happening now?

Are there threats?

Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware		→
2. Web based attacks		→
3. Web application attacks		→
4. Phishing		↑
5. Spam		↑
6. Denial of service		↓
7. Ransomware		↑
8. Botnets		↓
9. Insider threat		→
10. Physical manipulation/damage/ theft/loss		→
11. Data breaches		↑
12. Identity theft		↑
13. Information leakage		↑
14. Exploit kits		↓
15. Cyber espionage		→

Trends

- **Complexity of attacks** and sophistication of malicious actions in cyberspace continue to increase.
- Threat agents of all types have advanced in **obfuscation**, that is, hiding their trails.
- **Malicious infrastructures** continue their transformation towards multipurpose configurable functions including anonymization, encryption and detection evasion.
- **Monetization of cybercrime** is becoming the main motive of threat agents, in particular cyber-criminals. They take advantage of anonymity offered by the use of digital currencies.
- **State-sponsored actors** are one of the most omnipresent malicious agents in cyberspace. They are a top concern of commercial and governmental defenders.
- **Cyber-war** is entering dynamically into the cyberspace creating increased concerns to critical infrastructure operators, especially in areas that suffer some sort of cyber crises.
- **Skills and capabilities are the main concerns for organisations**. The need for related training programmes and educational curricula remains almost unanswered.

It will not happen to me

Norway healthcare cyber-attack ‘could be biggest of its kind’

Belgacom Attack

Britain's GCHQ Hacked Belgian Telecoms Firm

A cyber attack on Belgacom raised considerable attention last week. Documents leaked by Edward Snowden and seen by SPIEGEL indicate that Britain's GCHQ intelligence agency was responsible for the attack.

Ukraine power cut 'was cyber-attack'

11 January 2017

Moller-Maersk puts cost of cyber attack at up to $300m

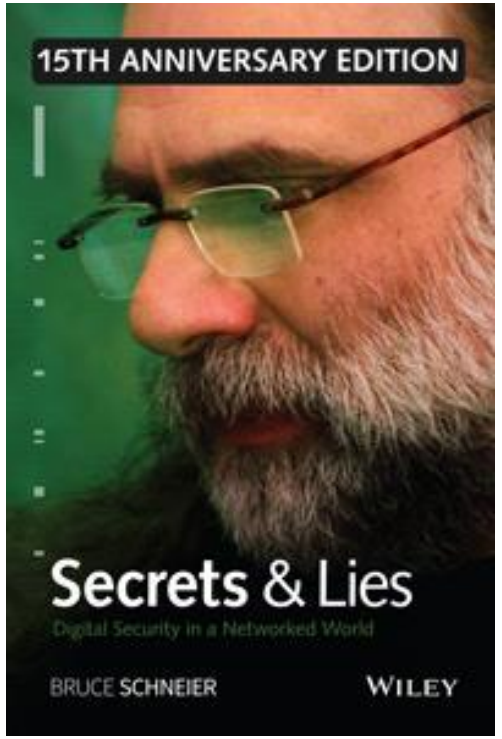
Container shipping conditions best since financial crisis, says Danish conglomerate

http://map.norsecorp.com/#/

How to approach the problem?

Who is the weakest security link?

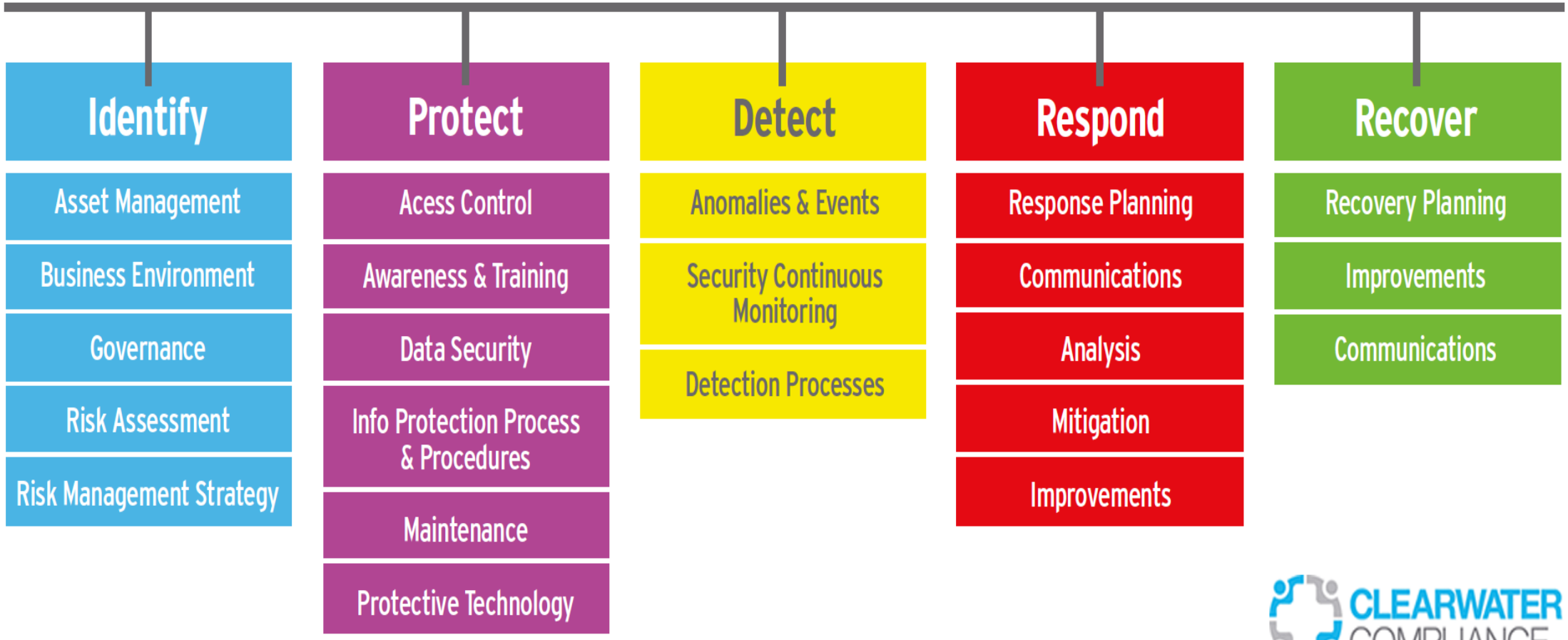
If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.



https://www.schneier.com/books/secrets_and_lies/pref.html

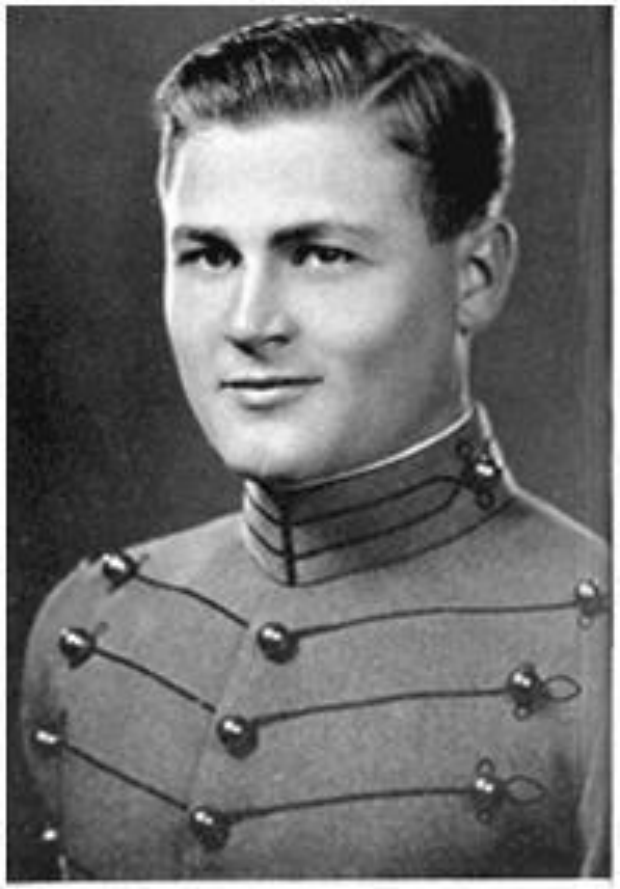
A structured, holistic approach is needed

NIST Cyber Security Framework



CLEARWATER COMPLIANCE

Is complete protection possible?



- “If there are two or more ways to do something, and one of those ways can result in a catastrophe, then someone will do it”; or
- Anything that can go wrong will go wrong.

Edward Aloysius **Murphy Jr**. (January 11, 1918 – July 17, 1990)

From Protection to Resilience (1)

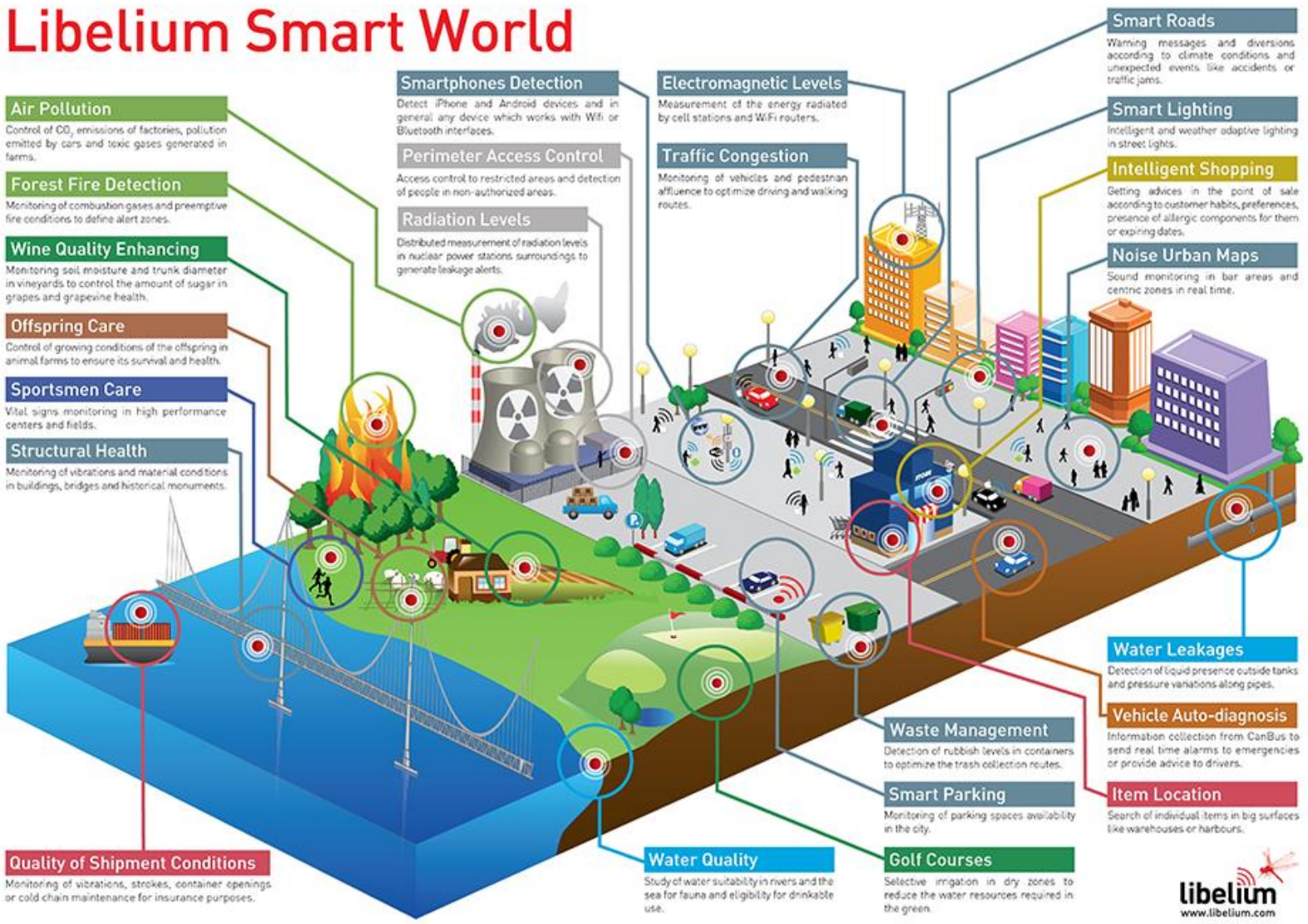
- “A resilient infrastructure is a component, system or facility that is able to withstand damage or disruption, but if affected, can be readily and cost-effectively restored.” (CIIP Resilience Series Monograph, George Mason University 2007).
- Very often, achieving the desired level of protection is simply not cost-effective in relation to the actual threats. A small amount of extra protection might introduce a large amount of additional costs.
- As full protection can never be achieved, we should ask whether the money could be better spent on making the proper preparations in order to ensure a graceful degrading of the infrastructure when disaster eventually knocks at the door.

From Protection to Resilience (2)

- A fringe benefit from a more resilience-based preparation approach is that these “measures are substantially less expensive than investments in specific infrastructure upgrades to avoid certain risk scenarios which may or may not occur.”
- In short, these resilience measures encompass such activities or elements as protection, prevention, training, education, research, deterrence, risk-based mitigation, response, recovery and longer-term restoration.

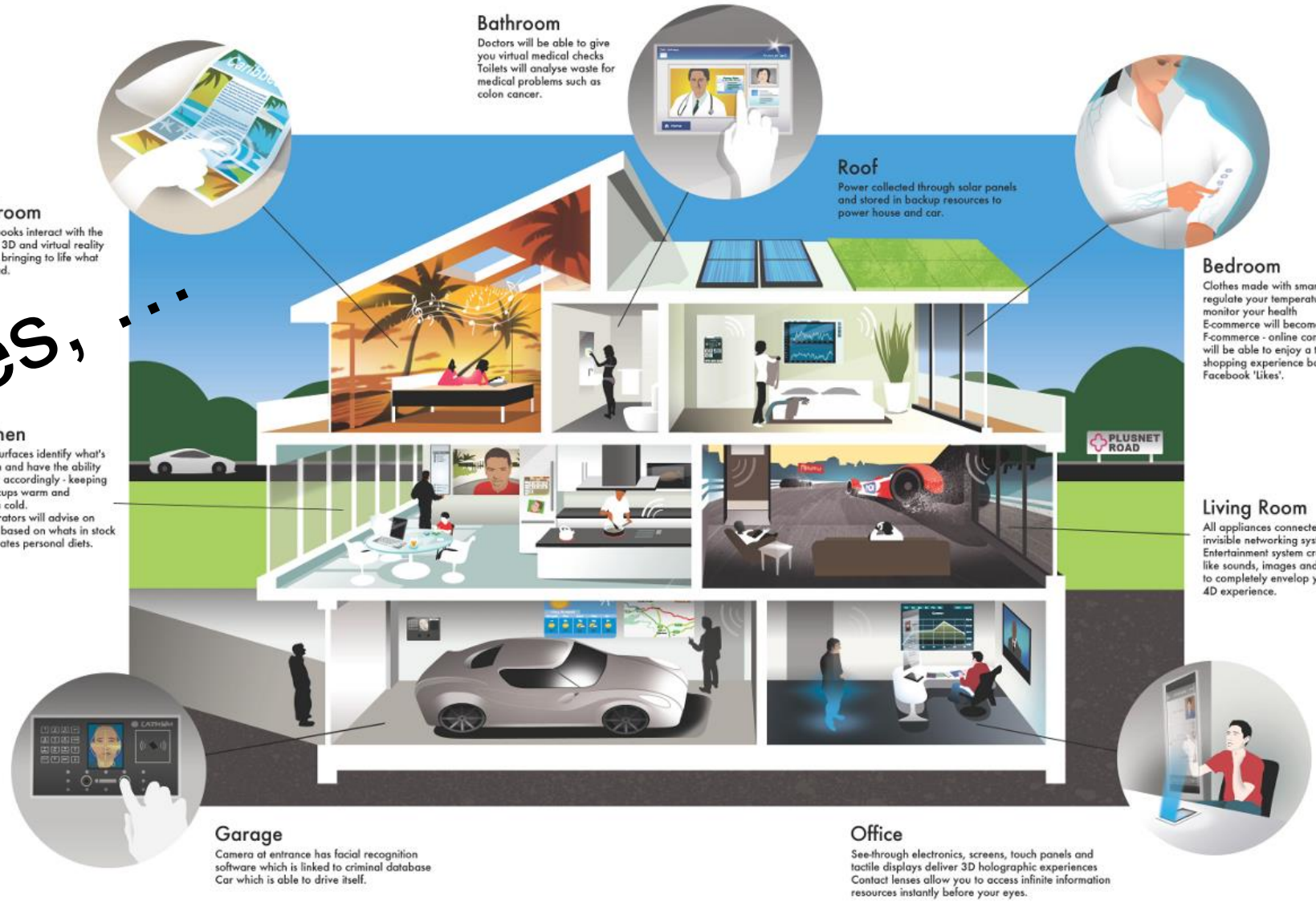
Back to the future

A smart world

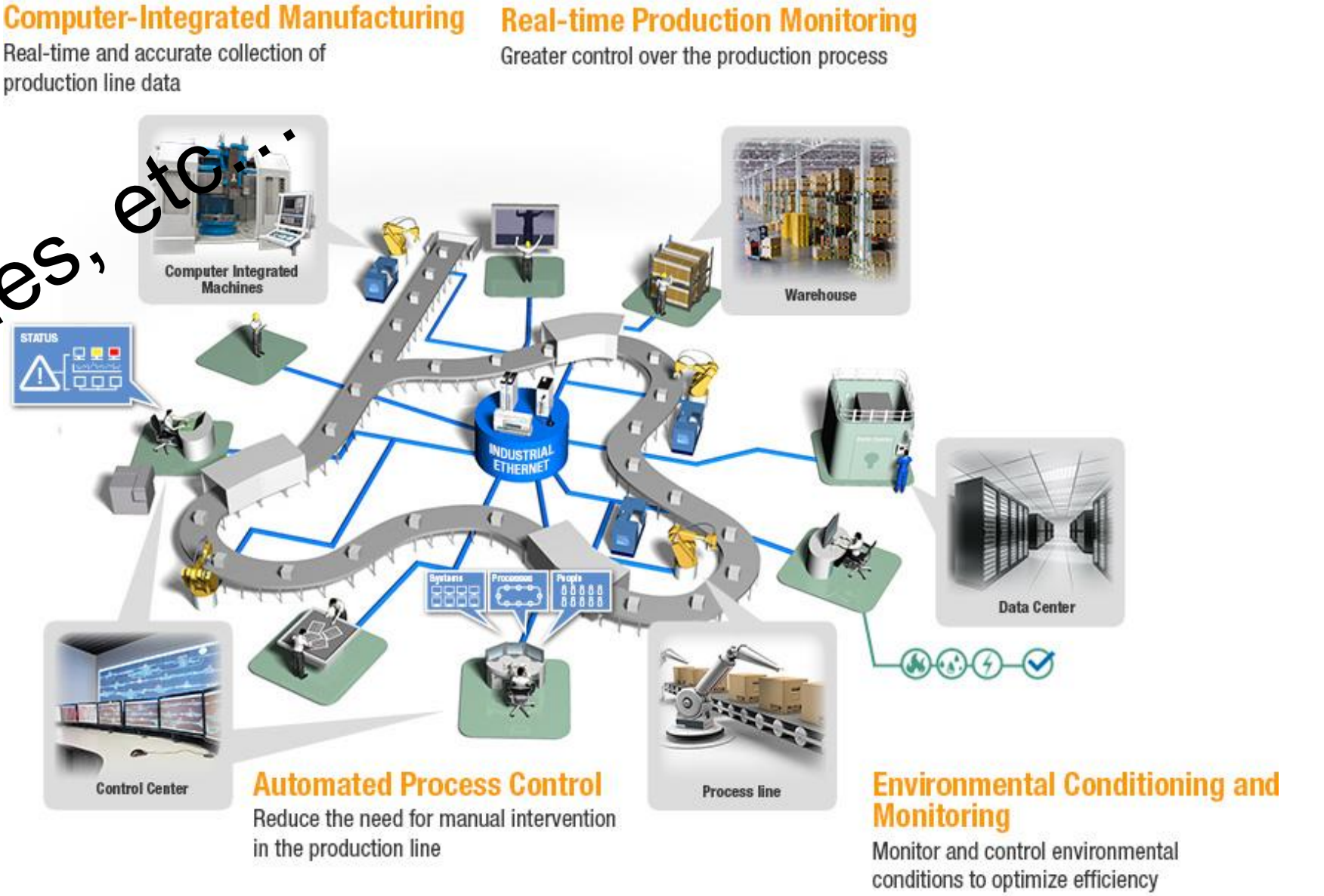


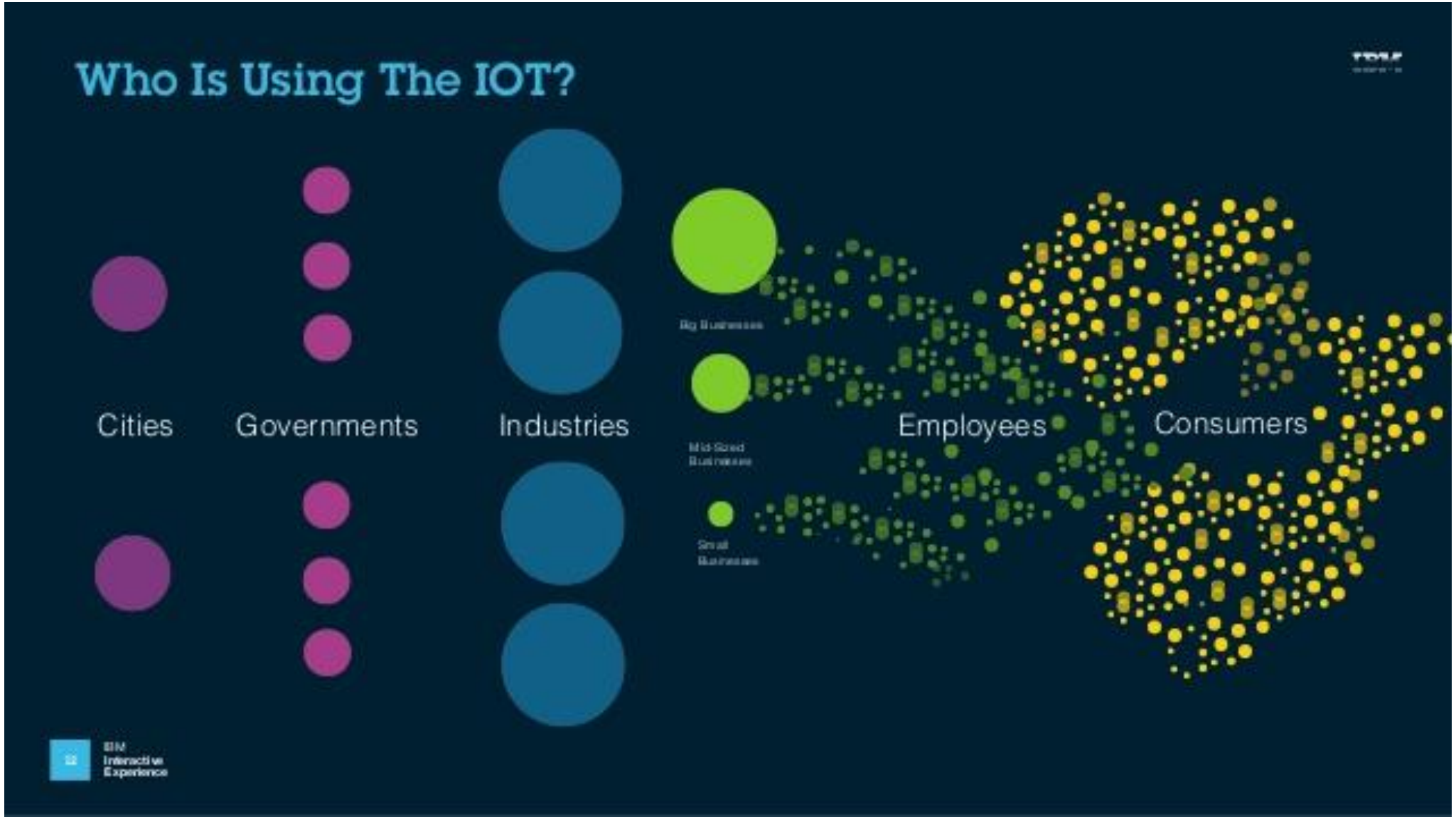
With smart cities, …

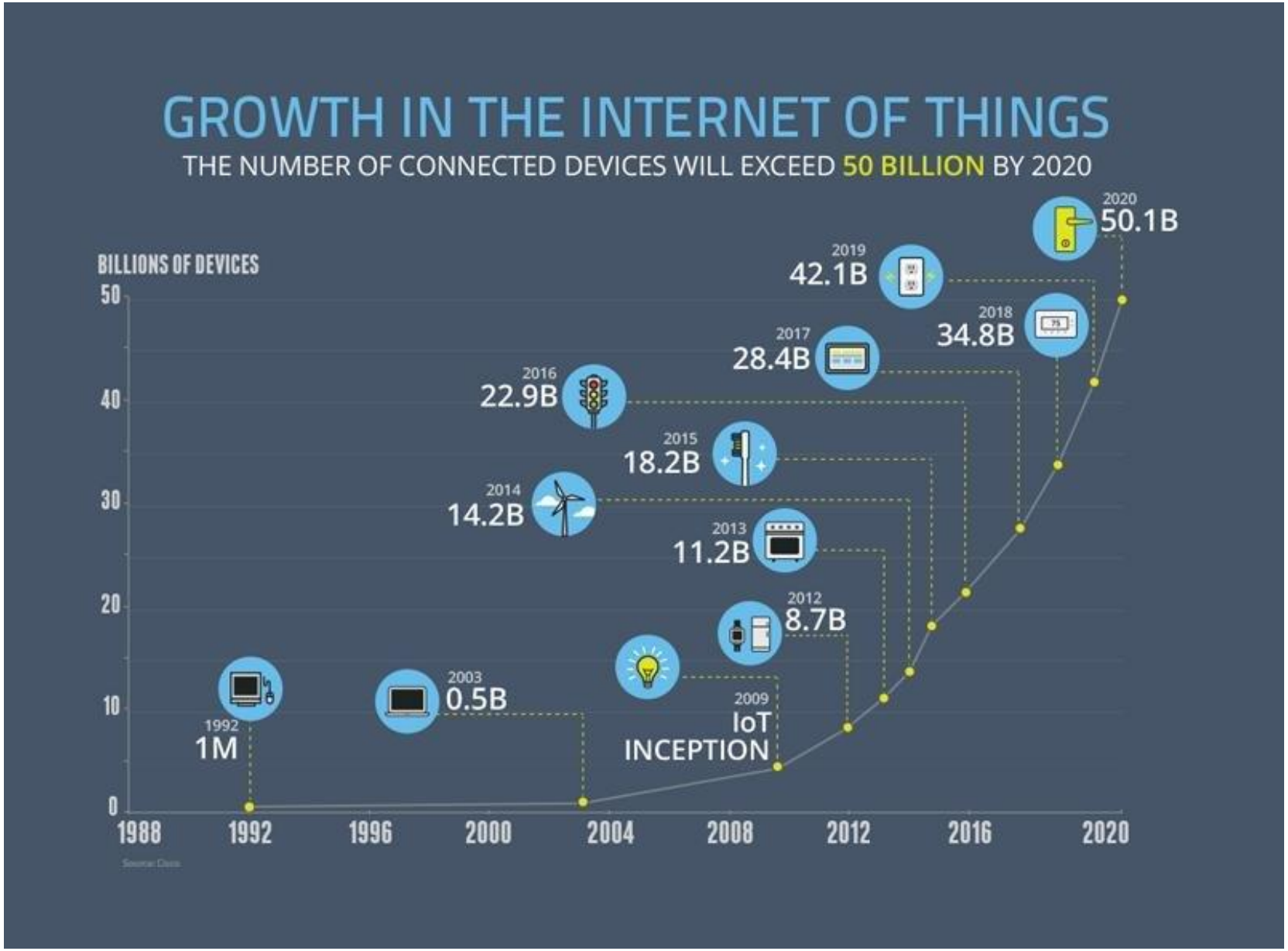
…Smart homes, …

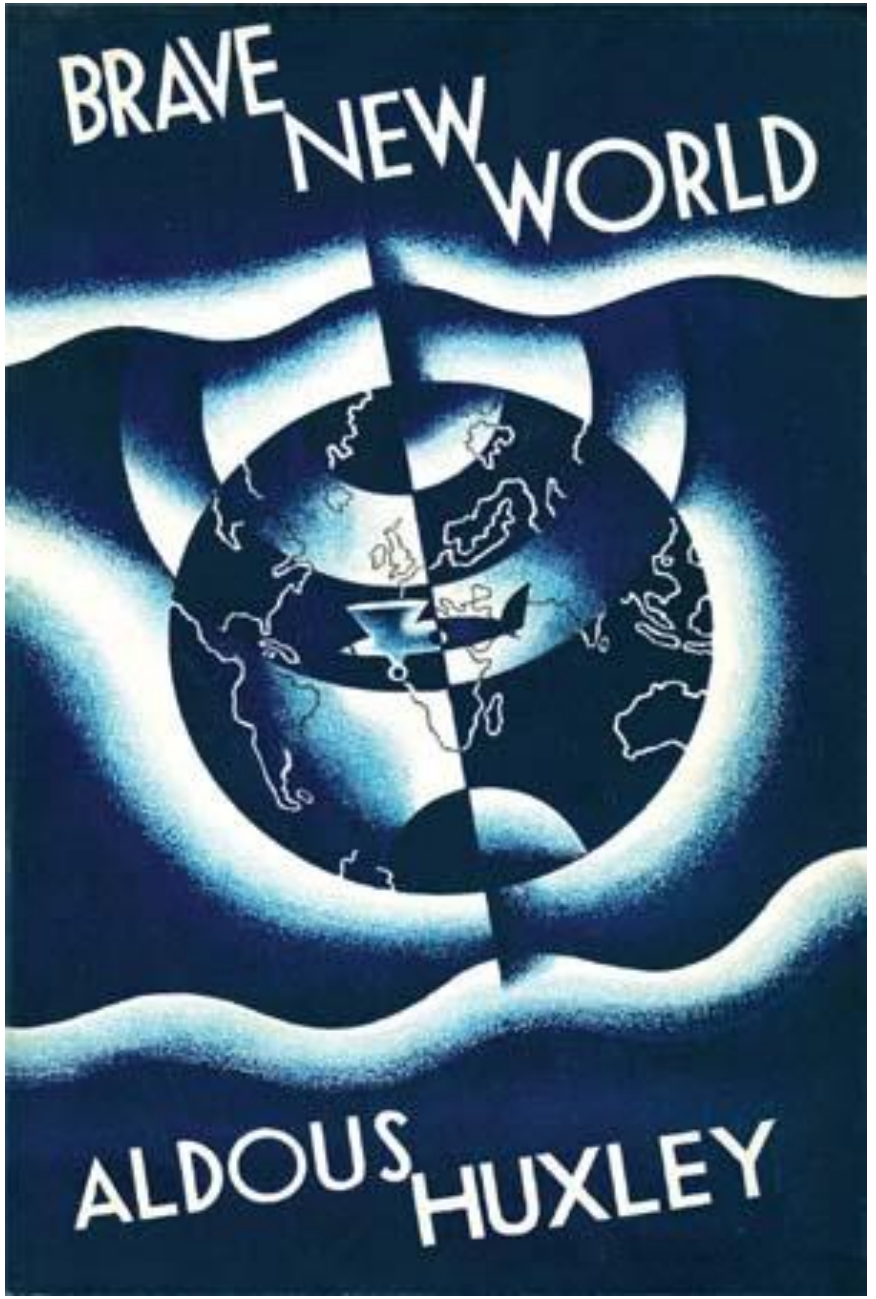

Bathroom
Doctors will be able to give you virtual medical checks
Toilets will analyse waste for medical problems such as colon cancer.
Roof
Power collected through solar panels and stored in backup resources to power house and car.
Bedroom
Smart books interact with the house's 3D and virtual reality system, bringing to life what you read.
Bedroom
Clothes made with smart fabrics regulate your temperature and monitor your health
E-commerce will become F-commerce - online consumers will be able to enjoy a tailored shopping experience based on Facebook 'Likes'.
Kitchen
Smart surfaces identify what's on them and have the ability to react accordingly - keeping coffee cups warm and iced-tea cold.
Refrigerators will advise on recipes based on whats in stock and creates personal diets.
PLUSNET ROAD
Living Room
All appliances connected through invisible networking system
Entertainment system creates life like sounds, images and experiences to completely envelop you in near 4D experience.
Garage
Camera at entrance has facial recognition software which is linked to criminal database
Car which is able to drive itself.
Office
See-through electronics, screens, touch panels and tactile displays deliver 3D holographic experiences
Contact lenses allow you to access infinite information resources instantly before your eyes.

…Smart factories, etc…



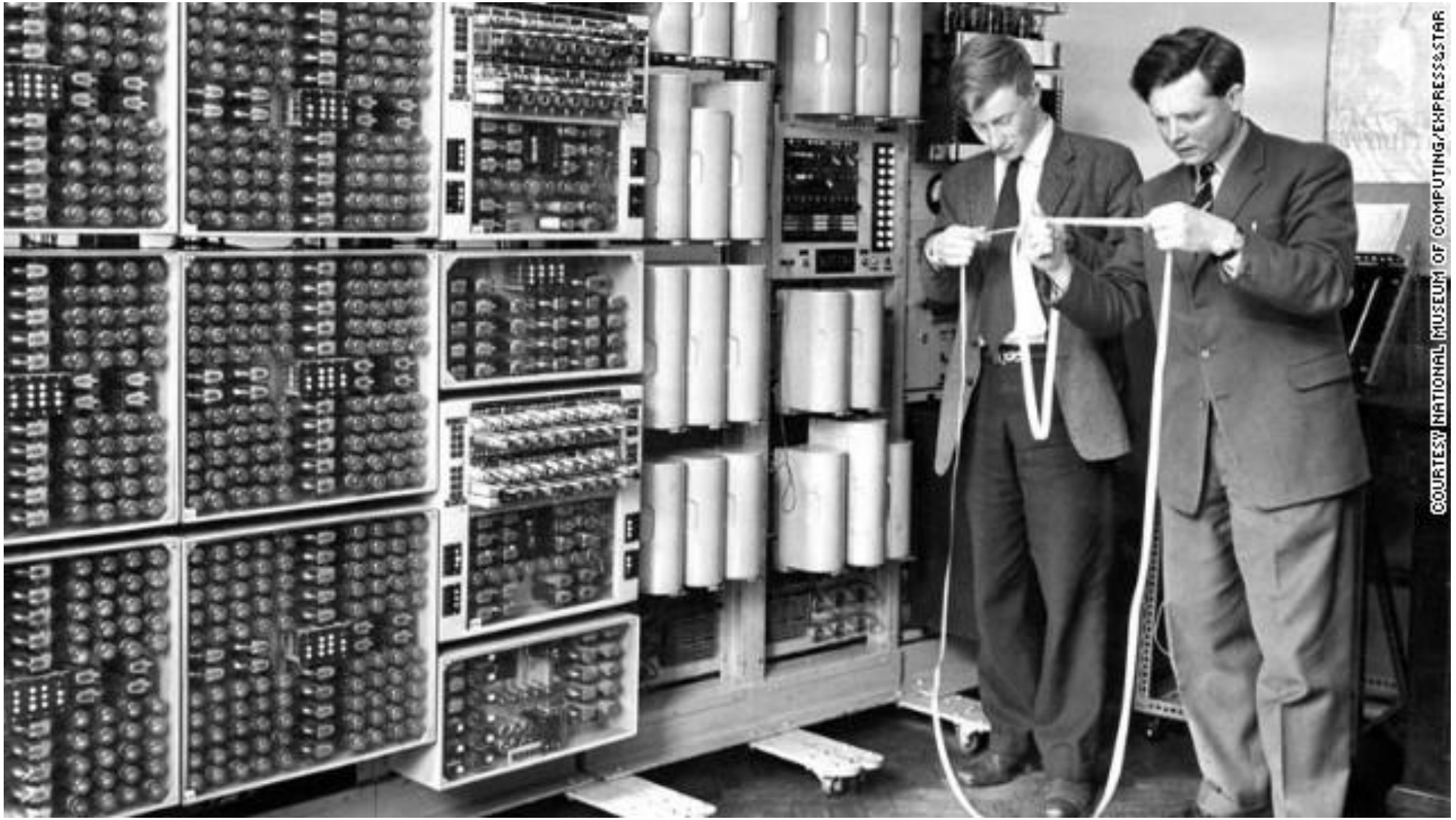

Who Is Using The IOT?
Cities
Governments
Industries
Employees
Consumers
IBM
Interactive
Experience


GROWTH IN THE INTERNET OF THINGS
THE NUMBER OF CONNECTED DEVICES WILL EXCEED 50 BILLION BY 2020
BILLIONS OF DEVICES
50
40
30
20
10
0
1988
1992
1996
2000
2004
2008
2012
2016
2020
1992
1M
2003
0.5B
2009
IoT
INCEPTION
2012
8.7B
2013
11.2B
2014
14.2B
2015
18.2B
2016
22.9B
2017
28.4B
2018
34.8B
2019
42.1B
2020
50.1B



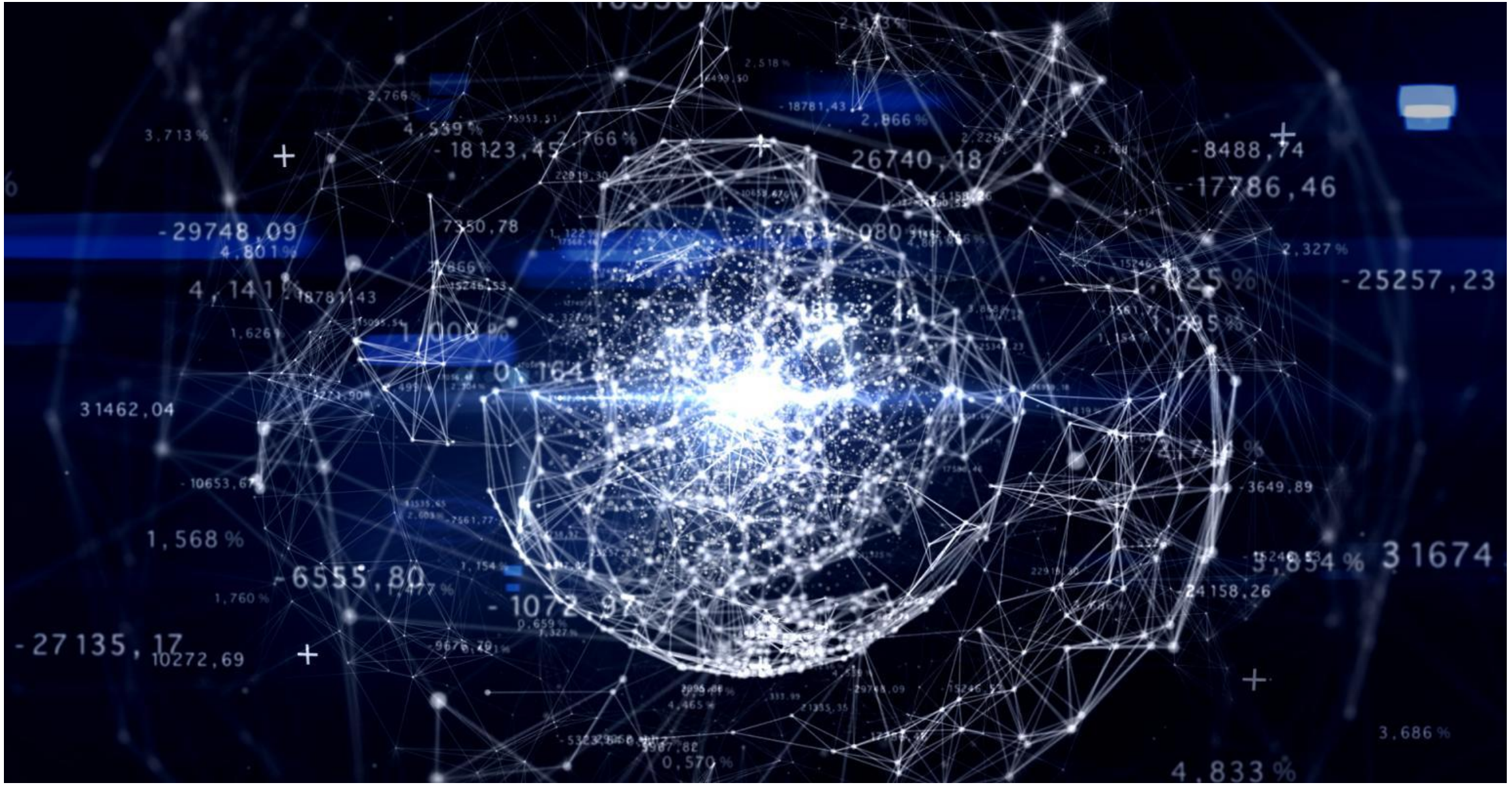
https://en.wikipedia.org/w/index.php?curid=8103565

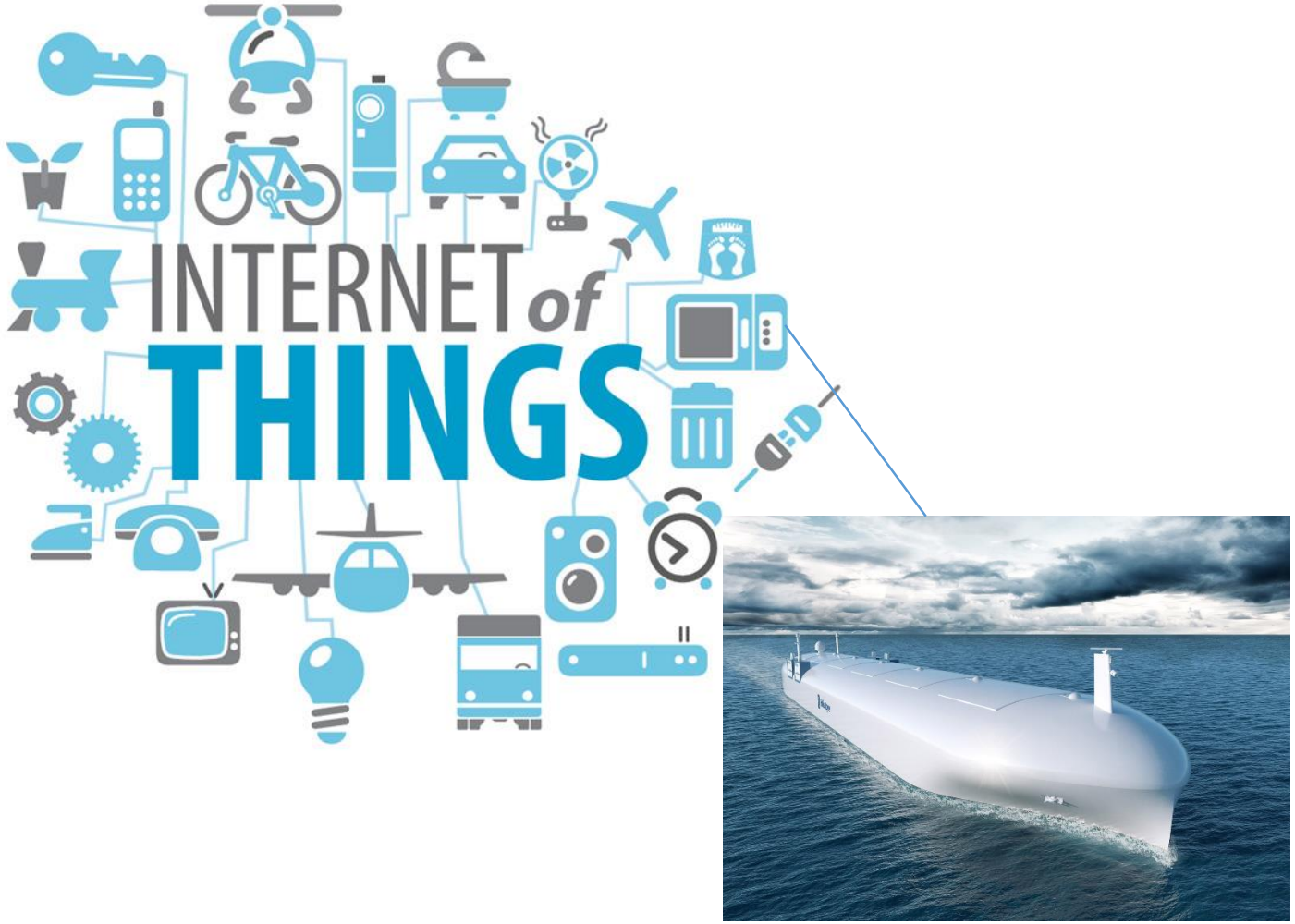
Look at the past to glimpse the future

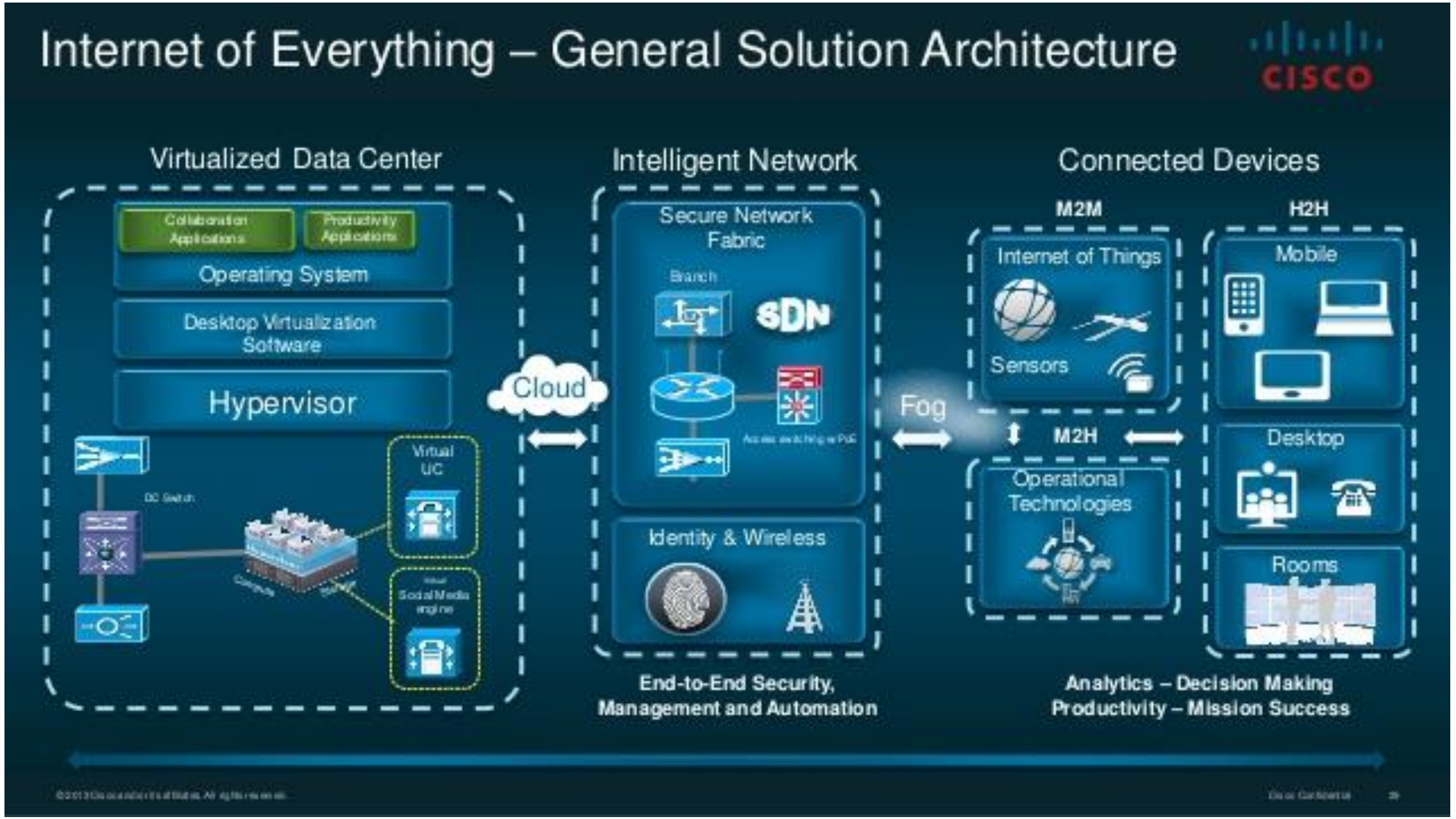

COURTESY NATIONAL MUSEUM OF COMPUTING/EXPRESS&STAR

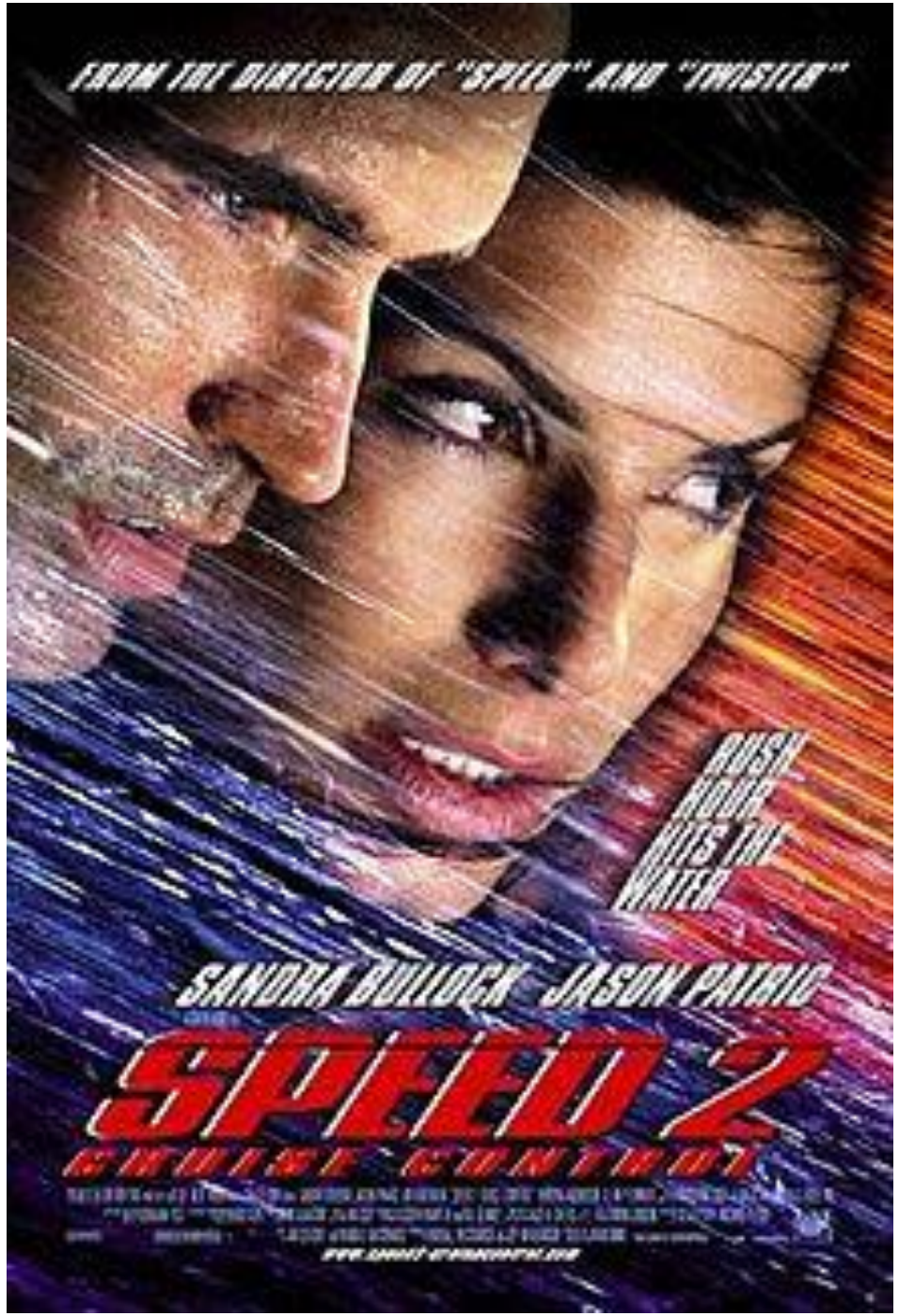

sinclair
ZX Spectrum
ENTER
SPACE
CAPS SHIFT
alamy stock photo
A6M1HJ
www.alamy.com

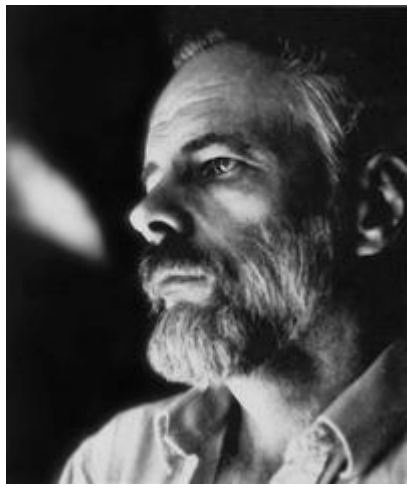

DELL
studio
DELL


-29748,09
4,801 %
7350,78
4,141
18781,43
1,626
31462,04
-10653,67
1,568 %
-6555,80
1,760 %
-27135,17
10272,69
26740,18
-18123,45
2,766 %
3,713 %
4,539 %
2,866 %
-8488,74
-17786,46
2,327 %
-25257,23
-3649,89
3,854 %
31674
24158,26
-1072,97
0,659 %
0,164
3,686 %
4,833 %
0,570 %


INTERNET of
THINGS


Internet of Everything – General Solution Architecture
CISCO
Virtualized Data Center
Collaboration Applications
Productivity Applications
Operating System
Desktop Virtualization Software
Hypervisor
DC Switch
Virtual UC
Virtual Social Media engine
Cloud
Intelligent Network
Secure Network Fabric
Branch
SDN
Identity & Wireless
End-to-End Security, Management and Automation
Fog
Connected Devices
M2M
Internet of Things
Sensors
M2H
Operational Technologies
H2H
Mobile
Desktop
Rooms
Analytics – Decision Making
Productivity – Mission Success


FROM THE DIRECTOR OF "SPEED" AND "TWISTER"
RUSH HOUR
SPEED 2
CRUISE CONTROL



There will come a time when it isn't “They're spying on me through my phone” anymore. Eventually it will be “My phone is spying on me”.

Philip K. Dick

A call to engage

NTNU CCIS

Center for Cyber and Information Security

Norwegian Center of Excellence for Critical Infrastructure Cyber Security (NORCICS)

Vision and Strategic Objective

- Norway is the most digitalized country in the world. NORCICS's **vision** is to contribute to making Norway the most securely digitalized country in the world, by improving the cyber security and resilience of her critical infrastructures.
- NORCICS's overarching **strategic objective** is
  - to develop and operationalize innovative solutions within a cyber-physical security ecosystem,
  - so as to enhance the capability of the business sector to innovate in the field of critical infrastructures
  - in order to respond efficiently to the current and future cyber-physical security risks,
  - by focusing on long-term research and fostering close alliances between research-intensive enterprises and prominent research groups in academia.
- In the long run, NORCICS aspires to achieve the efficient and effective transition of new and innovative capabilities and technologies for the security and resilience of critical infrastructures into practice.

NTNU CCIS

Center for Cyber and Information Security

Thank you!