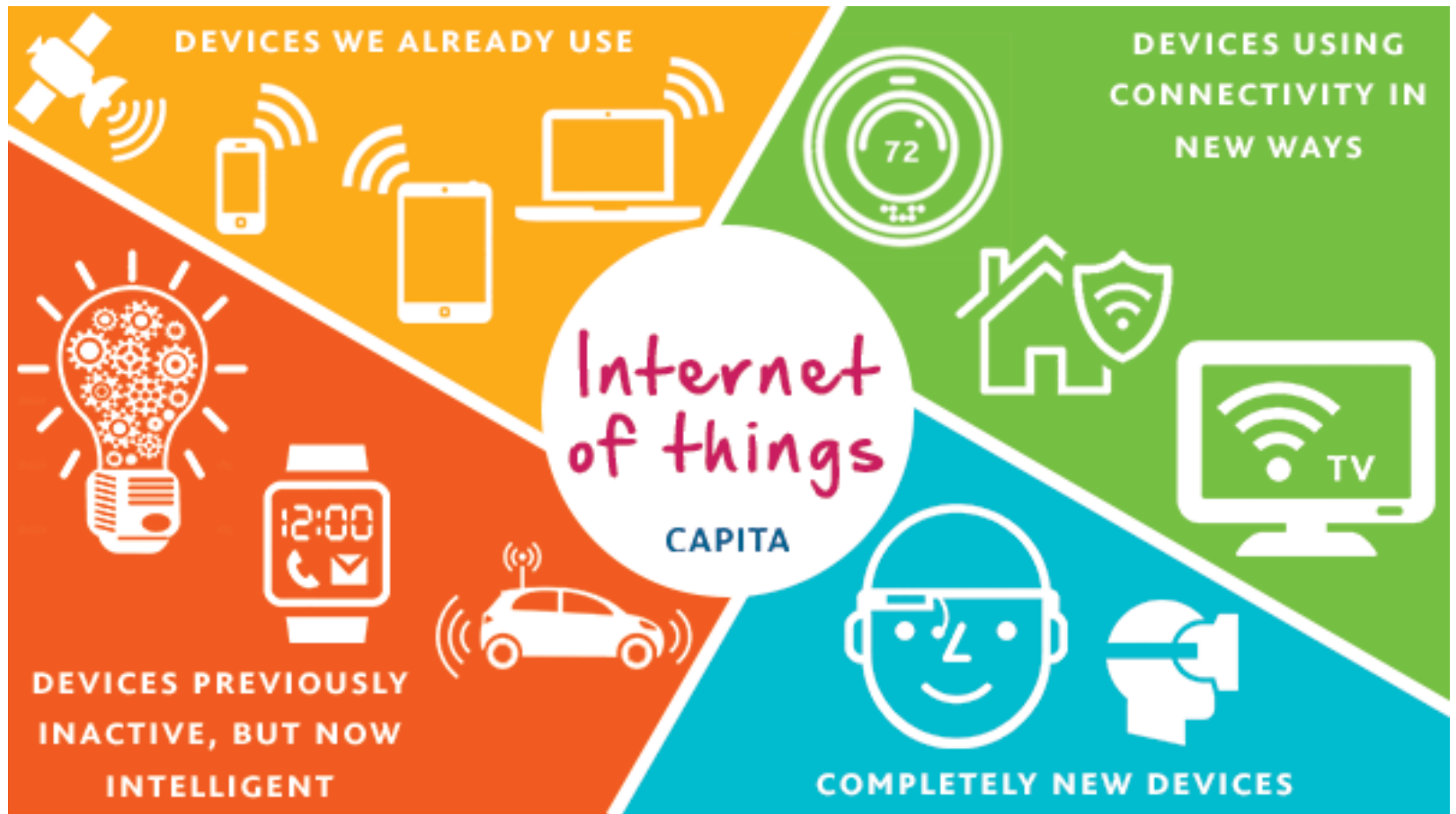


the Internet of Things

via SKYPE

5 IV , 9.00



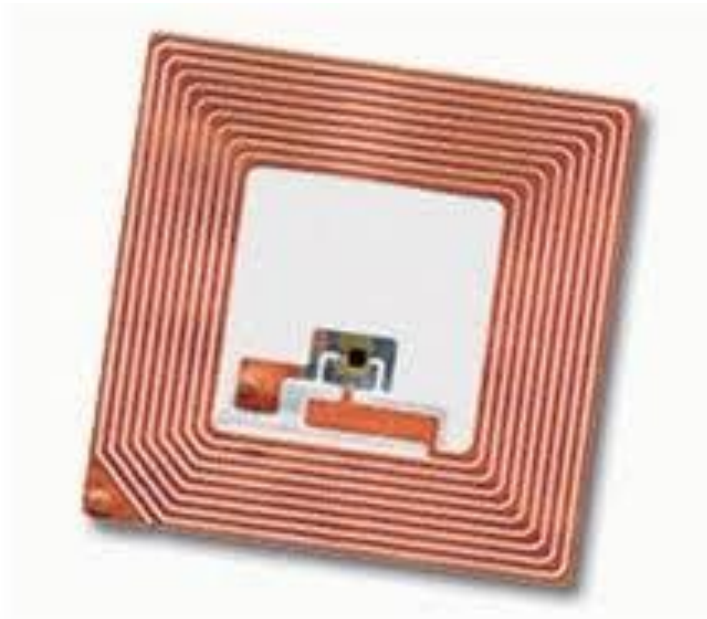


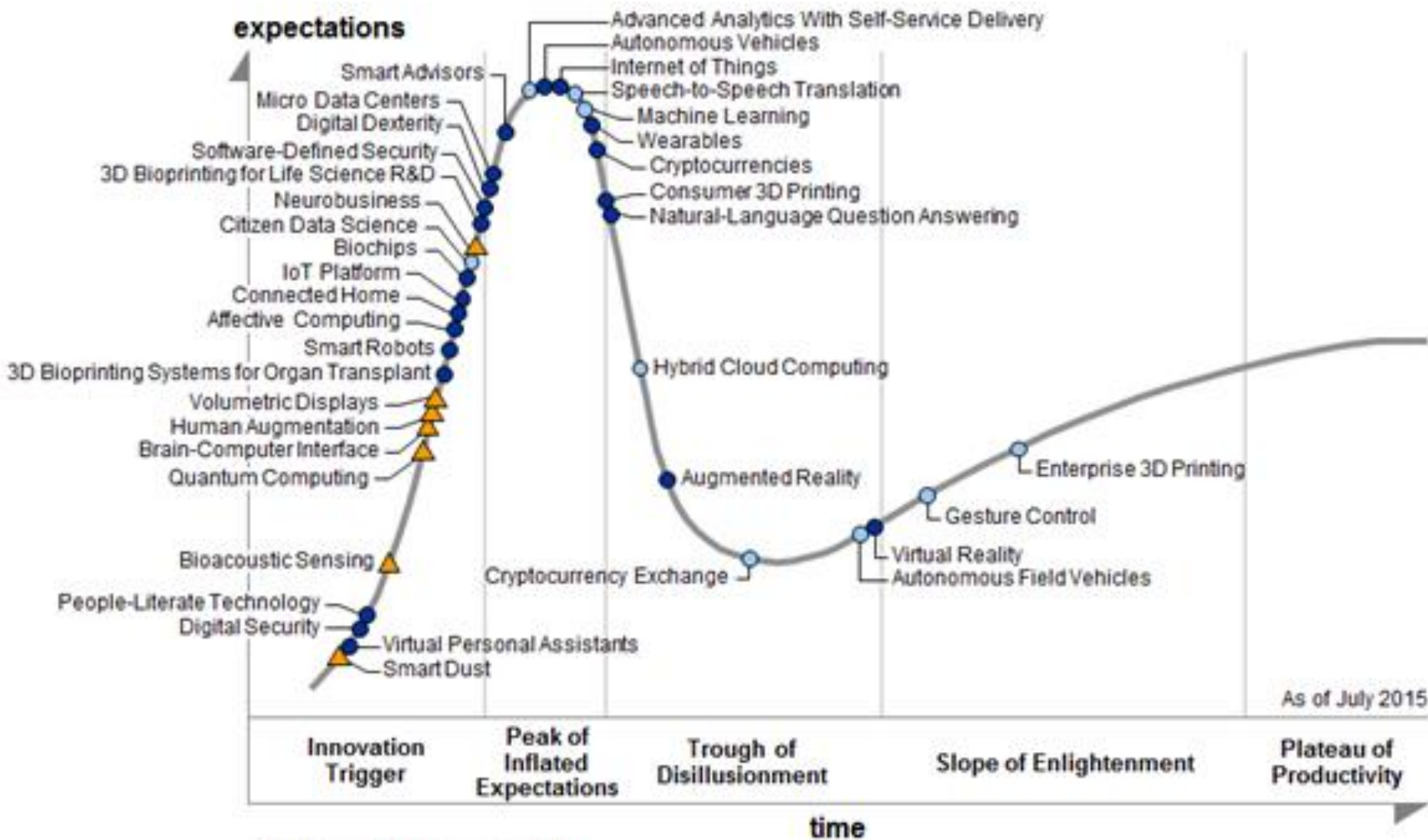
Kevin Ashton (born 1968) is a British technology pioneer who cofounded the Auto-ID Center at the MIT, which created a global standard system for Radio-frequency identification - RFID and other sensors. He is an innovator and consumer sensor expert who coined the phrase “the Internet of Things” (1999/2009) to describe the network connecting objects in the physical world to the Internet.

Internet Rzeczy należy rozumieć jako ekosystem, w którym przedmioty mogą komunikować się między sobą, za pośrednictwem człowieka lub bez jego udziału.

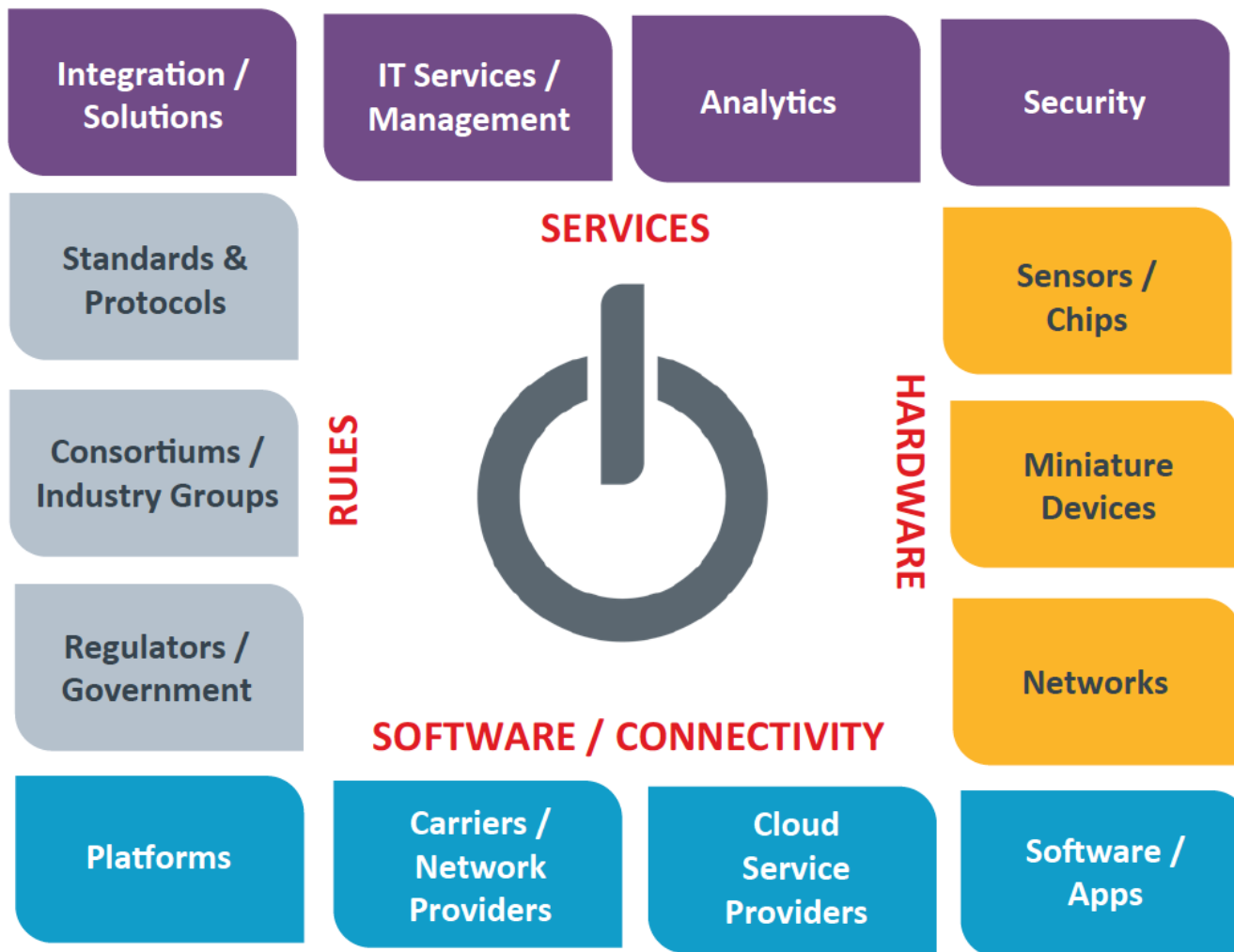
Technologia RFID

- *Radio-frequency identification* - Technika umożliwia odczyt, a czasami także zapis układu RFID. W zależności od konstrukcji umożliwia odczyt etykiet z odległości do **kilkudziesięciu centymetrów lub kilku metrów** od anteny czytnika. System odczytu umożliwia identyfikację wielu etykiet znajdujących się jednocześnie w polu odczytu. RFID przytwierdzony do przedmiotu może być jedną z form zabezpieczenia przedmiotów przed ich fałszowaniem.





The Evolving Internet of Things Ecosystem



Intel's Vision Internet of Things

INTELLIGENT DEVICES



Deliver Intelligence where needed to acquire and filter data securely

INTELLIGENT SYSTEM OF SYSTEMS

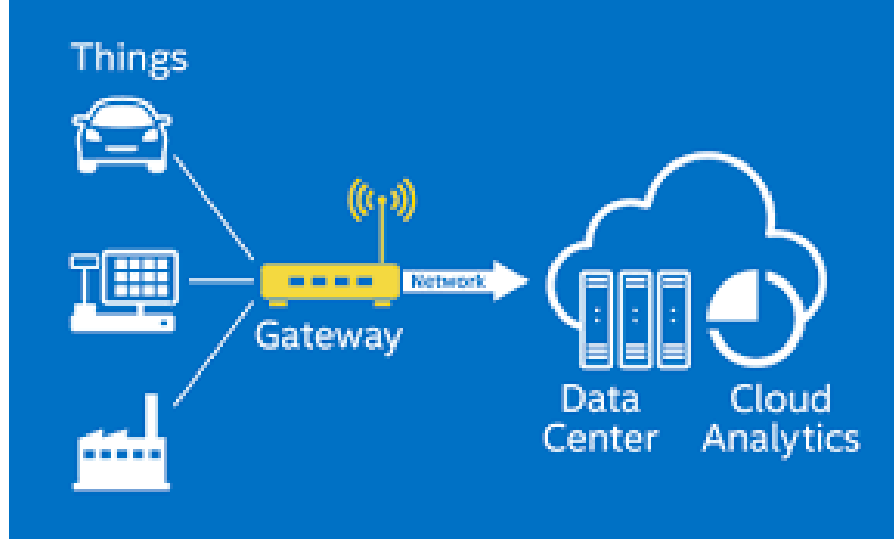


Billions of intelligent devices sharing data and securely, supporting legacy and new environments

END TO END ANALYTICS



Solutions from device to cloud to deliver end-to-end customer value

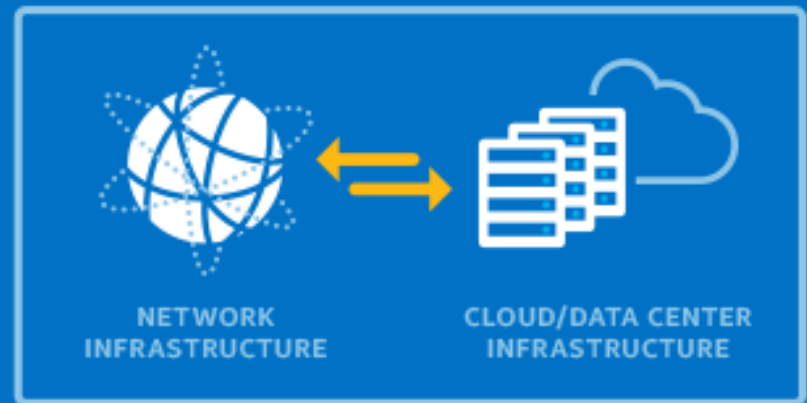


SERVICES CREATION AND SOLUTIONS LAYER



THINGS

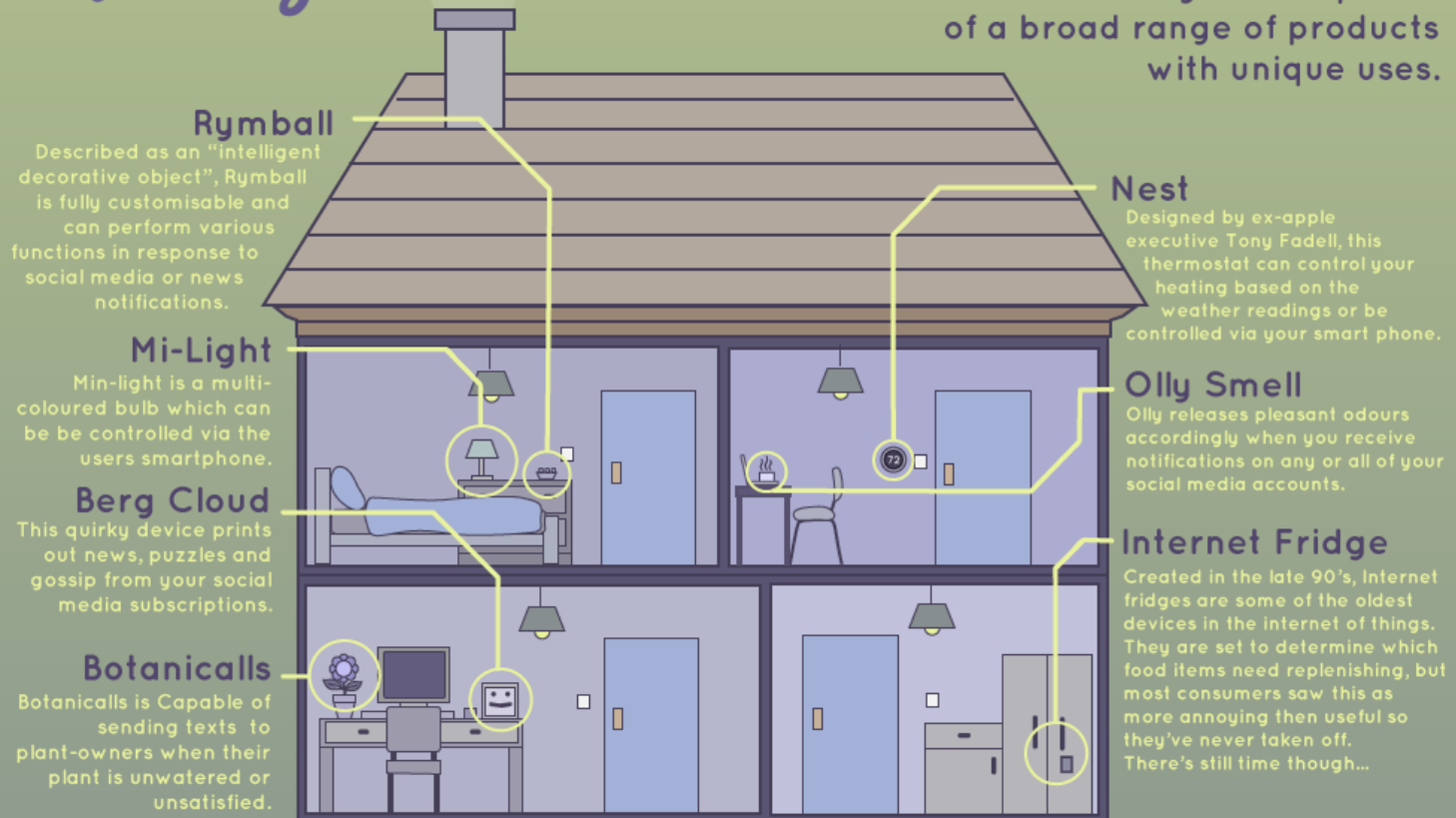
GATEWAY



NETWORK AND CLOUD

INTERNET Of things

The internet is no longer predominantly accessed by PC's. More and more non-PC internet connected devices are being created, and their not just smartphones and tablets. The internet of things is composed of a broad range of products with unique uses.



Population of things

Over the past decade, the amount of things connected to the internet has exceeded the amount of people living on earth.



2003



2010



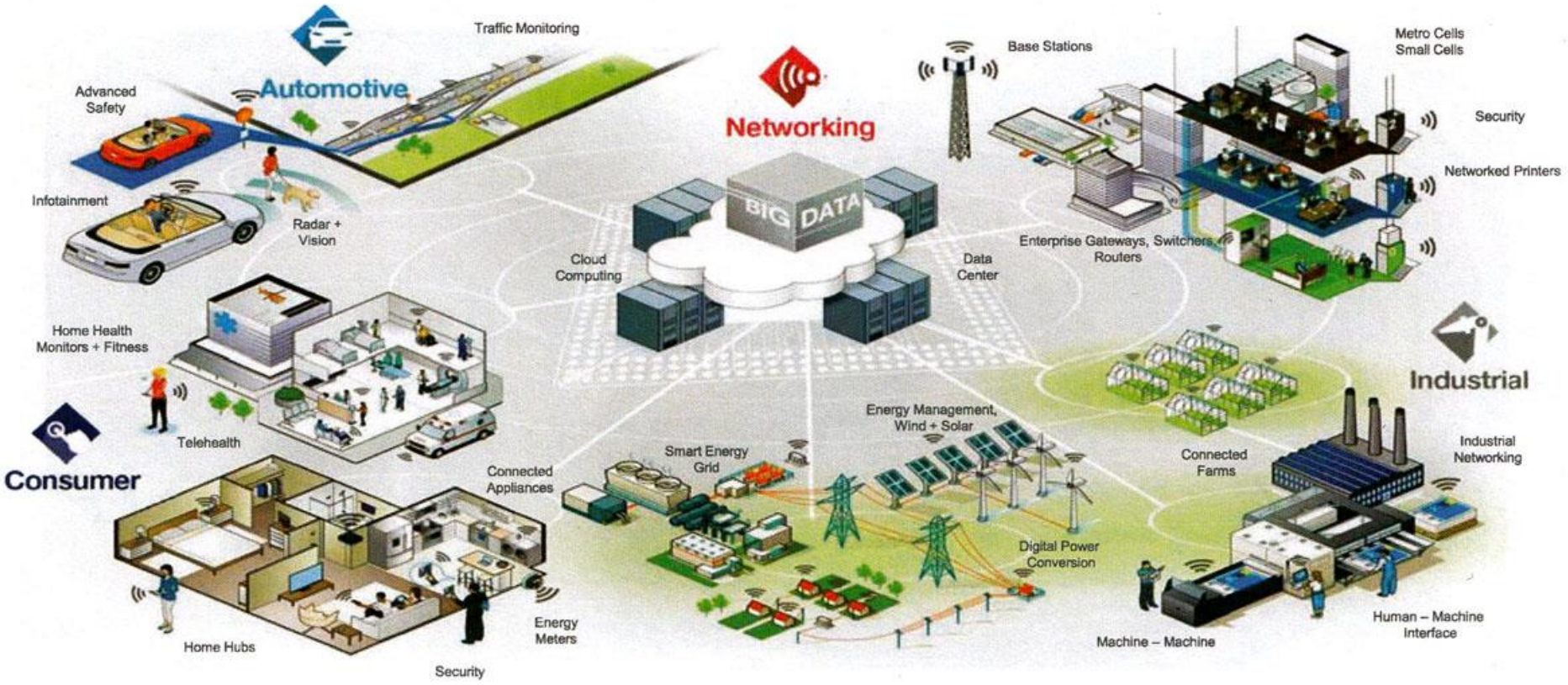
2015



2020

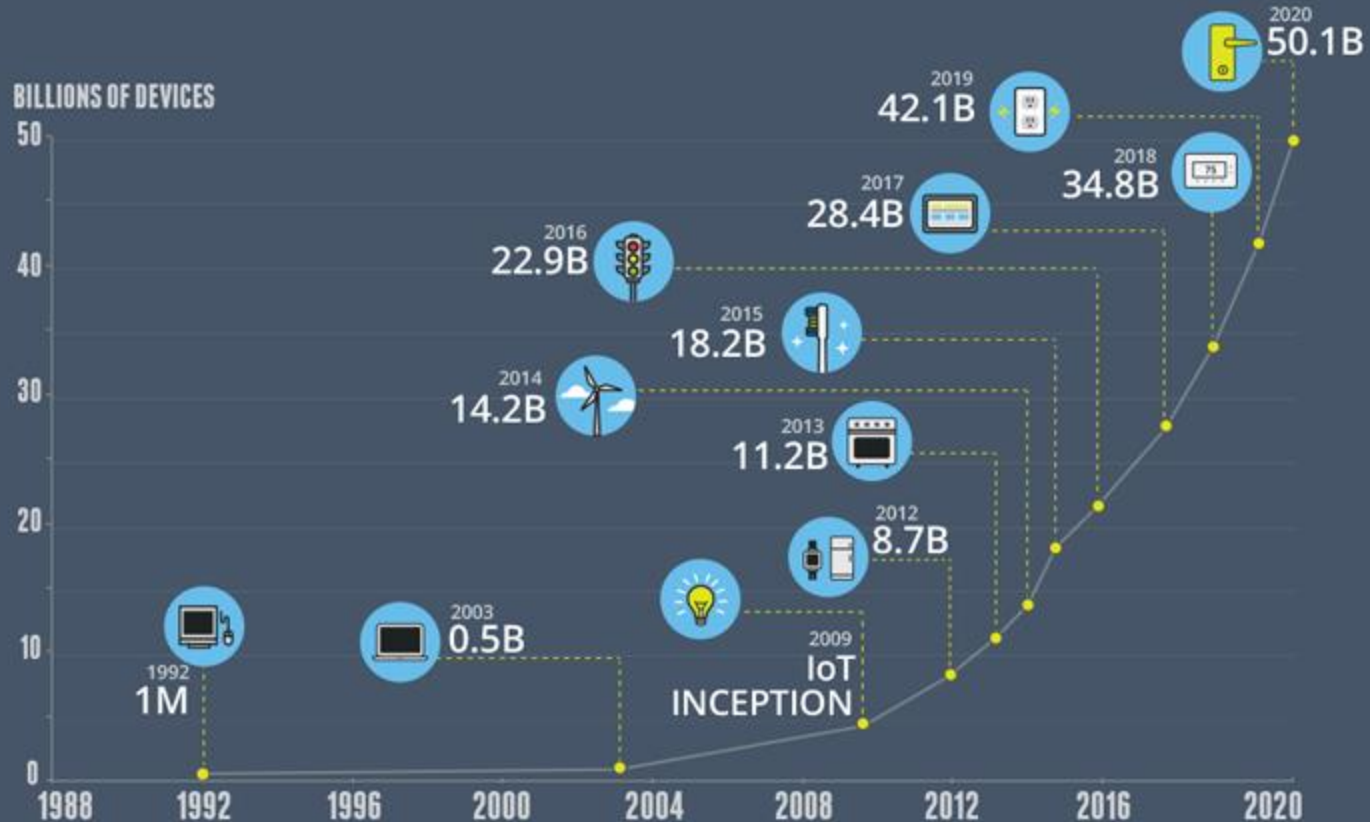
It is estimated that by 2020, the internet of things will be populated by over 50 billion internet devices. Approximately seven for everyone on the planet.

The Internet of Things

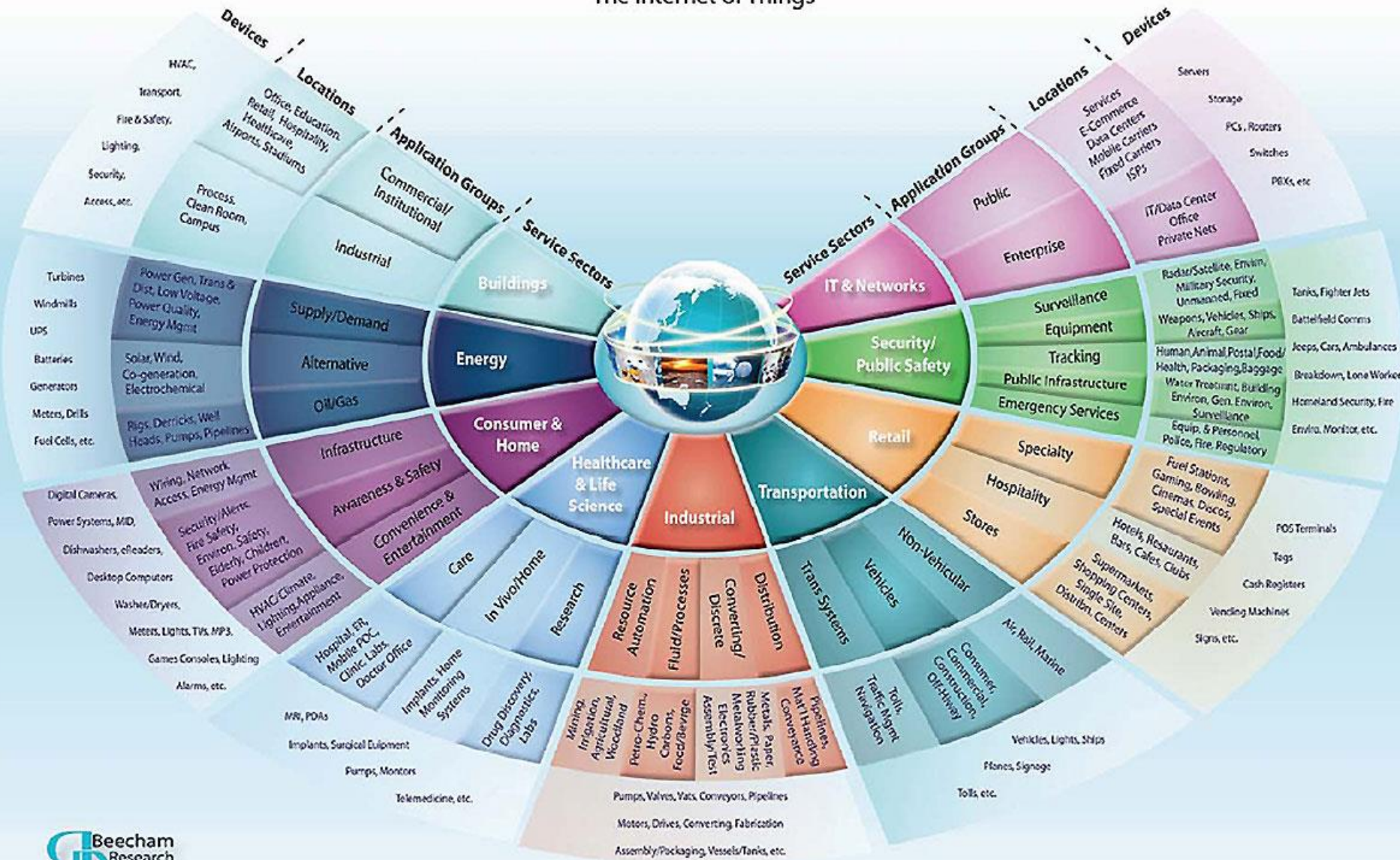


GROWTH IN THE INTERNET OF THINGS

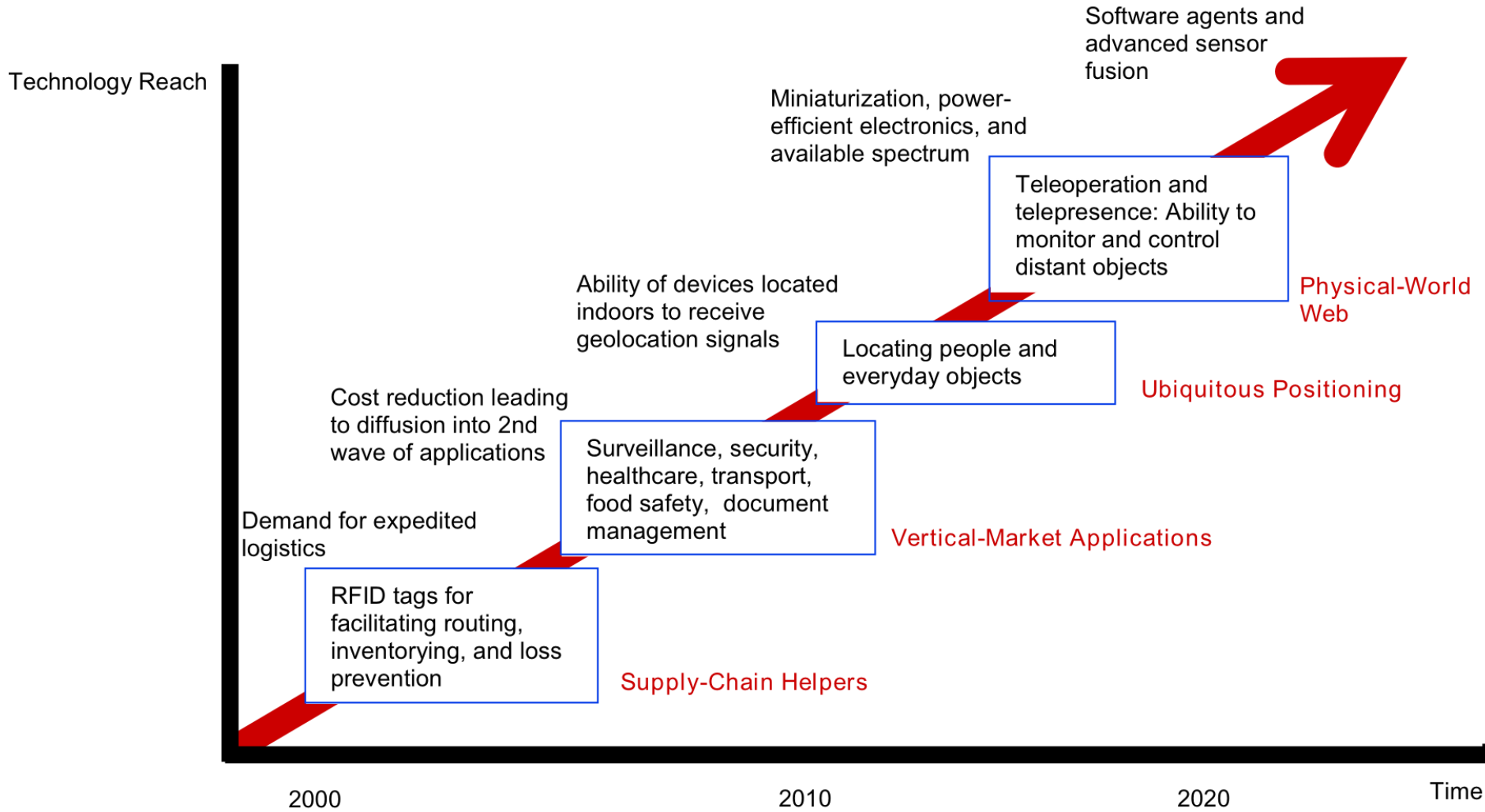
THE NUMBER OF CONNECTED DEVICES WILL EXCEED **50 BILLION** BY 2020



The Internet of Things



TECHNOLOGY ROADMAP: THE INTERNET OF THINGS



Source: SRI Consulting Business Intelligence

The INTERNET *of* THINGS



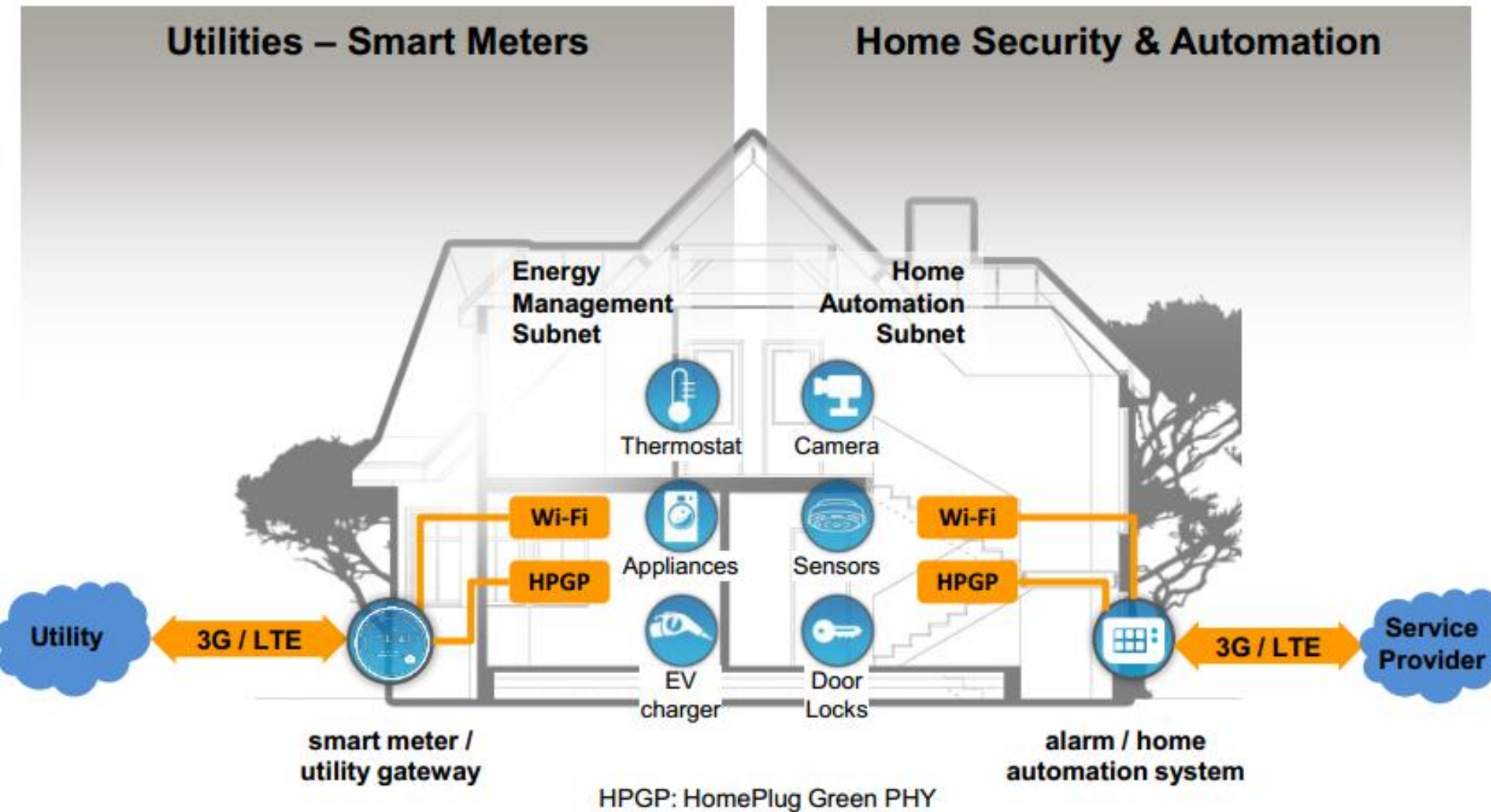
During 2008, the number of **things** connected to the internet exceeded the number of **people** on earth.



By 2020 there will be **50 billion**.



Intelligent Home





Every move you make

23 listopada 2017 r. (czwartek), godz. 17.00-
18.30

Uniwersytet SWPS w Warszawie, ul.
Chodakowska 19/31, sala S303 (III piętro)

- „Every move you make... every step you take, I'll be watching you” [Każdy Twój ruch...każdy Twój krok będę obserwował] – śpiewał zespół The Police w 1983 r. W 2017 r. te słowa są bardziej aktualne niż kiedykolwiek wcześniej. Dziś permanentna obserwacja nie odbywa się jednak w rzeczywistości realnej, lecz wirtualnej. Każde wyszukiwanie w internecie, każde polubienie na Facebooku, wszystkie zachowanie konsumenckie w sieci pozostawiają cyfrowy odcisk palca w cyberprzestrzeni. Cyfrowe ślady pomnożone przez miliony ludzi składają się na Big Data, zbiór informacji, z którego można uzyskać szczegółowe dane o każdym z nas. Dr Michał Kosiński, wykładowca w Stanford Graduate School of Business oraz absolwent Uniwersytetu SWPS, podczas wykładu „The End of Privacy” 23 listopada 2017 r. w Strefie Psyche opowie o tym, jak nowoczesne technologie ingerują w prywatność.

Koniec prywatności

- W sieci toczy się nasze życie towarzyskie, tutaj uczestniczymy w wydarzeniach kulturalnych, robimy zakupy, wyszukujemy tysiące informacji, itp. Te aktywności generują niezliczoną ilość cyfrowych śladów. Powstają one także w wyniku przetwarzania informacji o nas przez narzędzia i systemy informatyczne. Cyfrowe ślady trafiają do internetu, chmur obliczeniowych, baz danych. I zaczynają żyć własnym życiem, o którego istnieniu cybermieszkaniec często nie ma pojęcia.
- Podobnie jak i o tym, że na podstawie cyfrowych śladów można stworzyć precyzyjny profil użytkownika. Słowem, zrekonstruować jego styl życia, codzienne rutynowe aktywności, cechy charakteru. Poznać osobowość, inteligencję, zainteresowania. Algorytm może połączyć setki tych mikrozależności i z dużym prawdopodobieństwem przewidzieć przyszłe zachowania, np. wybory polityczne czy konsumenckie.
- Biorąc pod uwagę rozwój sztucznej inteligencji i zastosowanie psychologii do metod obliczeniowych, powinniśmy się przygotować na przyszłość, w której prywatność będzie przywilejem tylko dla wybranych.

Algorytm prawdę Ci powie?

- Dziś wróżbici mogą oddać swoje szklane kule do recydingu. Lepiej by zainwestowali w dobry algorytm, który z dużym prawdopodobieństwem przewidzi nie tylko przyszłe zachowania ludzi (np. jak ktoś będzie głosował w nadchodzących wyborach – 85 proc. prawdopodobieństwa), lecz także ich cechy indywidualne, jak kolor skóry (95 proc.) czy orientację seksualną (88 proc.). W wielomilionowym zbiorze Big Data kryją się nawet najbardziej osobiste informacje: wyznanie, poziom inteligencji czy pochodzenie (np. z pełnej bądź niepełnej rodziny). Jeśli naukowiec zajmujący się wykorzystaniem psychologii do analizy informacji ze zbioru Big Data powie: „Spotkasz wysokiego bruneta wieczorową porą”, to z 90-proc. prawdopodobieństwem tak się stanie.

Dr Michał Kosiński

- Profesor w Stanford Graduate School of Business. Doktoryzował się w dziedzinie psychologii na Uniwersytecie Cambridge, gdzie był również wicedyrektorem Centrum Psychometrycznego. Absolwent Uniwersytetu SWPS.
- Ekspert w dziedzinie psychometrii. Bada zachowania ludzkie przez pryzmat cyfrowych odcisków palców powstających w wyniku przetwarzania informacji przez narzędzia i systemy informatyczne. Koordynuje projekt myPersonality, w ramach którego ponad 200 badaczy z całego świata analizuje profile 8 milionów użytkowników Facebooka. W trakcie studiów na Uniwersytecie Cambridge zainicjował w sieci opensourcową, adaptacyjną platformę testową Concerto oraz aplikację ApplyMagicSauce.com, przeznaczoną do tworzenia psycho-demograficznych profili użytkowników Facebooka i Twittera. W 2013 r. IBM i DataIQ zaliczyły go do 50 najbardziej wpływowych osób w świecie Big Data. W 2016 r. został uznany za Wschodzącą Gwiazdę przez Association for Psychological Science.

COVID - 19





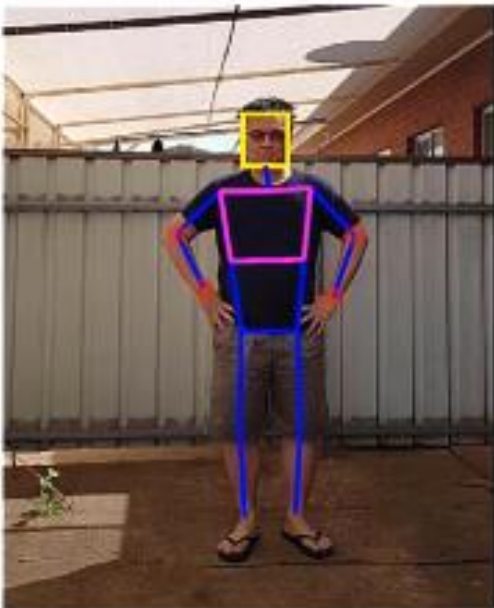
An employee of the Hankou Railway Station in Wuhan, China, monitoring thermal scanners on January 21, 2020.
Reuters



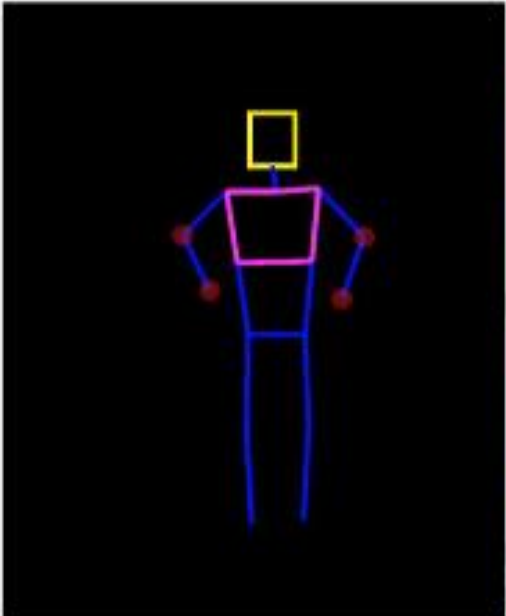
'Pandemic Drone' Could Detect Virus Symptoms Like COVID-19 in Crowds



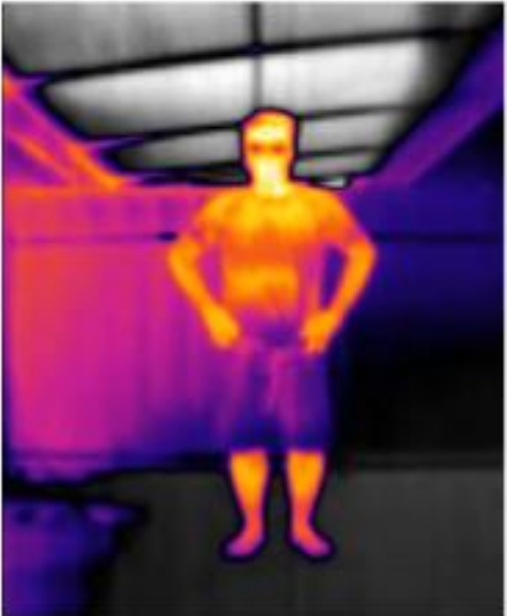
ROBOTS DRONES CCTV SMARTPHONE



Breathing Rate: 15



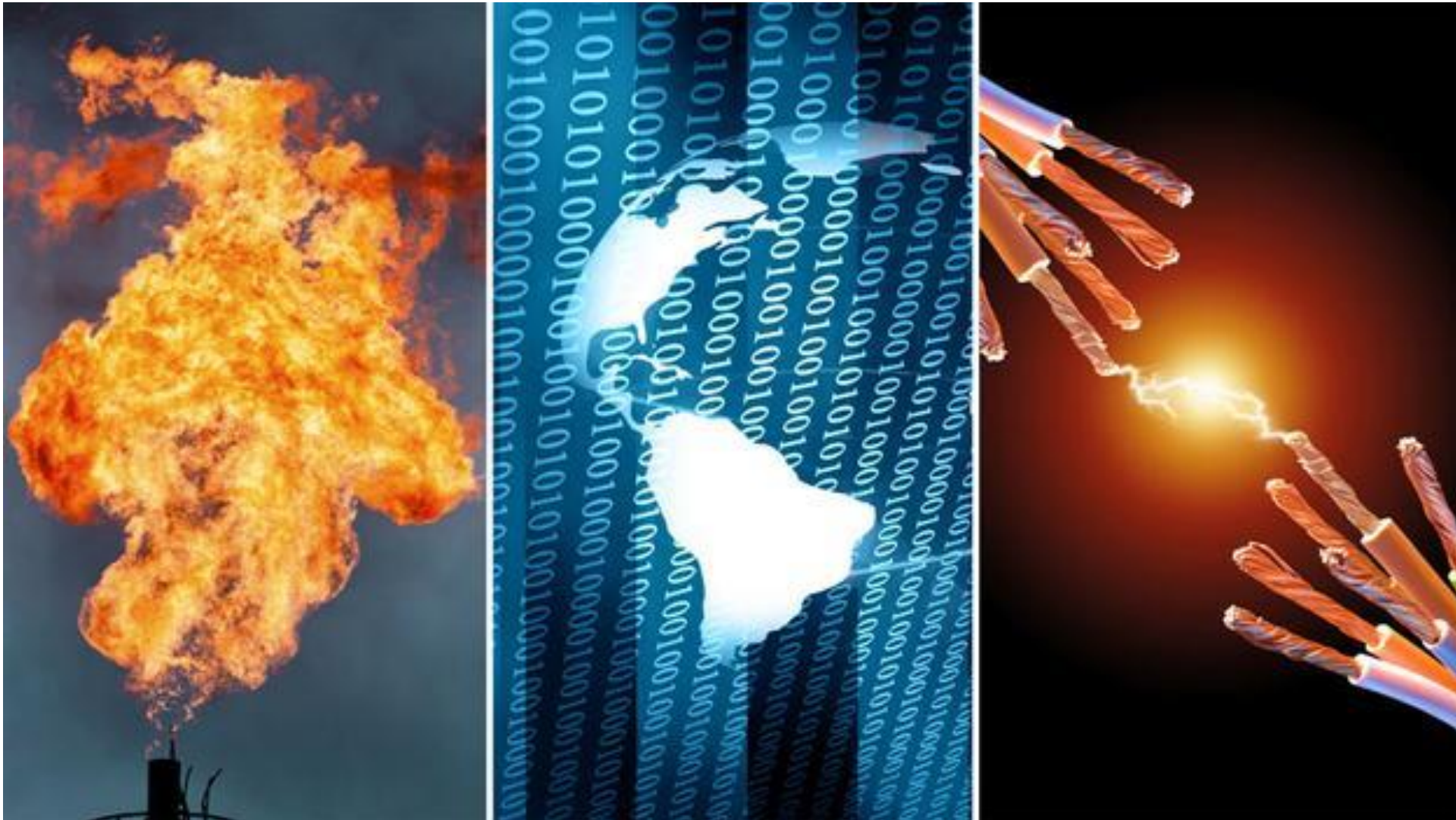
Heart Rate: 80



Temperature

Action

Oil, electricity and the internet have vastly altered the planet



IOT



T

is a cohesive body. A single point of weakness can have major ramifications on all other parts connected to the body – just as malware aimed to disrupt a national infrastructure has consequently leaked into other systems through indirect infections. As a result, even smaller nations are being forced to tighten their responsibilities.

Austria's energy concerns

As we mentioned in our recent look into the [regulation changes on the horizon](#), the European NIS-Directive's aim is to improve the EU Member States national cybersecurity capabilities, enhance cross-border cooperation and information sharing both between Member States and the public and the private →

he discussion surrounding information security in Europe continues to intensify this year as the pending introduction of new regulations collides with a time of heightened security. For businesses involved in critical national infrastructure (CNI), demand for the discussion has never been more urgent. Not only is the number of attacks increasing on CNI systems, but the sophistication of these attacks continues – in many cases – to outpace the provisions for countermeasures. In a world where disruption of IT systems can have huge impact on the economy, these systems have become seen as a prime target for those trying to create political havoc.

For Germany, research into the vulnerabilities and the best way to close them has been the subject of huge investment as well as discussion. An leading voice in the EU, Germany has been pressed to take on a leadership role in securing its CNI as it calls for Member States to follow suit. The idea is that the continent – and to some degree, the wider world –

'Should plans for a European 'super grid' take effect, the risks could become greater.'

DACH ICS
CYBER SECURITY

ENERGISING SECURITY

GERMANY AND AUSTRIA BUILDING CRITICAL CYBER DEFENCES



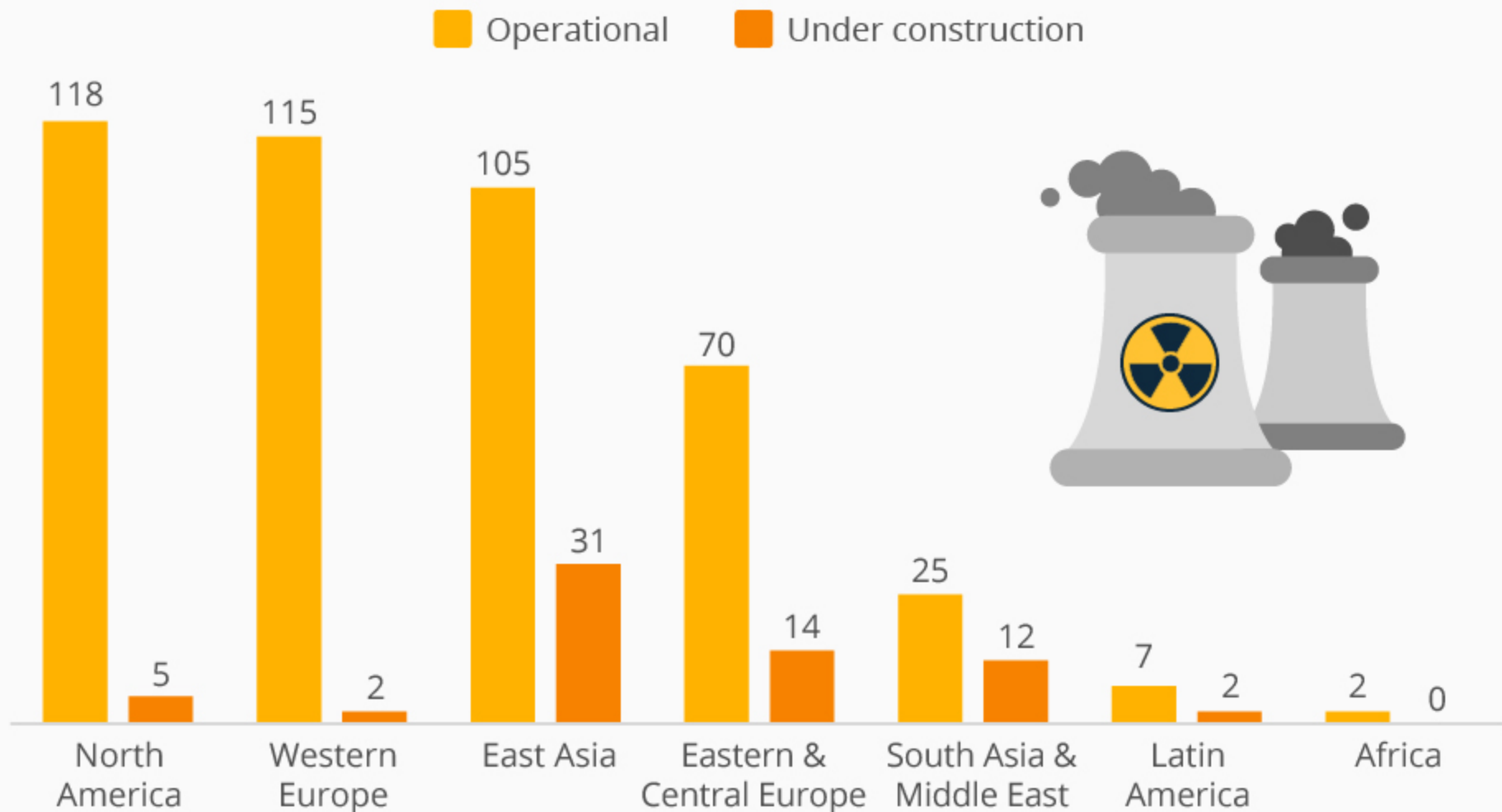
Nuclear Power Plants Are The Next Easy Target Of Hackers All Over The World

January 15, 2016

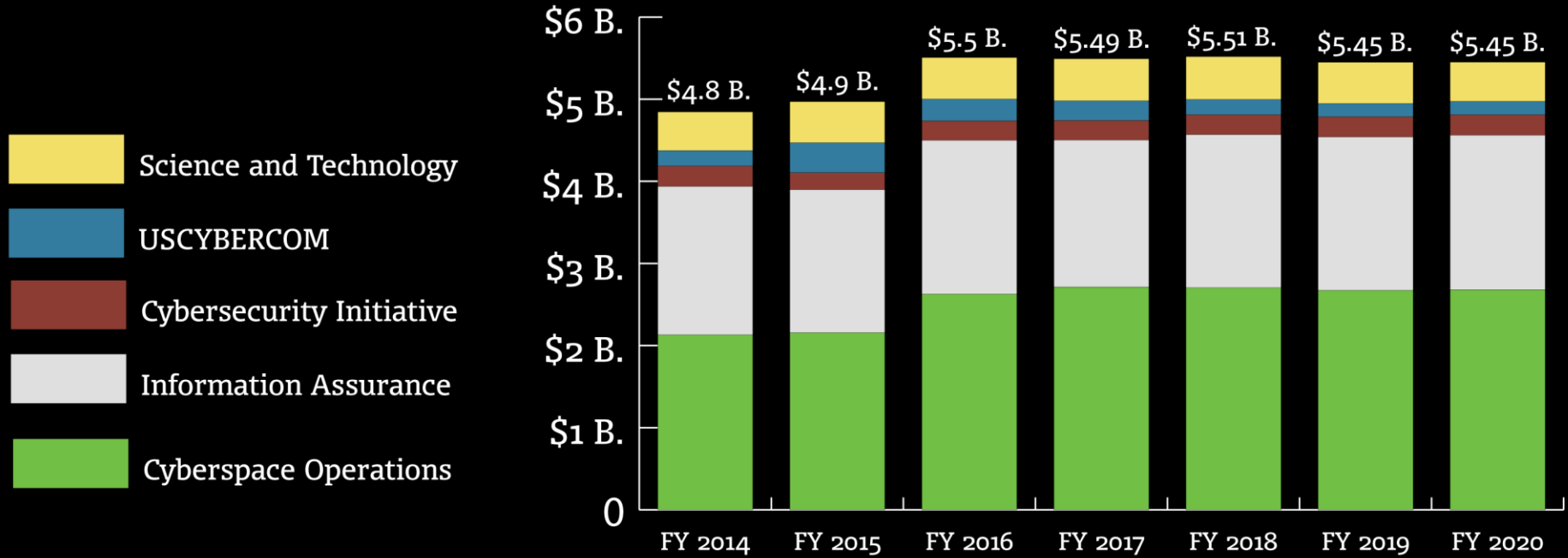


Nuclear Energy Worldwide

Operational reactors and reactors under construction*



Total Defense Department Cyber Spending



23 June
2009



NHS is hit by large-scale cyber attack with patients turned away and operations cancelled in hospitals across Britain as hackers take over computers and demand cash not to wipe out records



HACKERS RANSOM NHS

The NHS has been hit by an 'unprecedented' hack that has shut down computers and cut off phone lines in a cyber attack that could 'endanger lives', doctors said today. Hackers have taken control of computers in at least 40 NHS Trusts across the country including Lister Hospital in Stevenage (bottom right). It means doctors cannot access patients' files which are stored online. Messages popped up on computers this afternoon which said 'oops, your files have been encrypted' and demanded a ransom of £230 to regain access to the PC otherwise the files would be wiped forever. Some NHS Trusts can't carry out emergency MRI and CT scans and have turned off all their IT systems, reverting to using pen and paper as hundreds of non-urgent operations have been delayed. One doctor at Colchester General Hospital said screens were 'wiped out one by one' while another described a matron running around frantically yelling: 'Turn off your computers'.

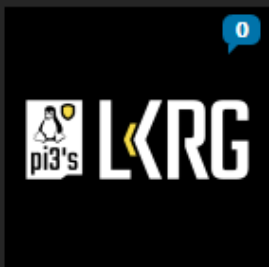
Czy jesteśmy bezpieczni, jak
zobaczyć nasze cyberbezpieczeństwo?

<https://zaufanatrzeciastrona.pl/>

<https://niebezpiecznik.pl/>



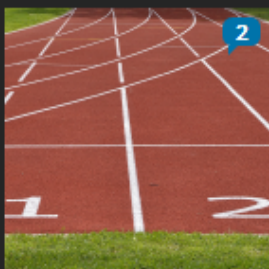
Zaufana Trzecia Strona



0

Linux Kernel Runtime Guard – ochrona przed (jeszcze) nieznanymi exploitami

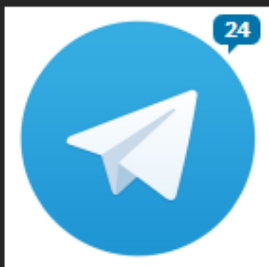
W dobie wszechobecnych exploitów warto zastanowić się nad zabezpieczeniami. Solar Designer, założyciel inicjatywy OpenWall niedawno poinformował o pojawieniu się nowego projektu do proaktywnej ochrony systemów opartych na Linuxie. [Czytaj dalej »](#)



2

Poniedziałek z trenerem – CSS Injection i kradzież sekretów

Trochę czasu minęło od ostatniego wydawania „Poniedziałku z trenerem”, ale spieszymy poinformować, że nie zrezygnowaliśmy z prowadzenia cyklu. Dzisiaj poniedziałek wypada we wtorek, zatem zapraszamy do lektury. [Czytaj dalej »](#)



24

Poważny błąd w Telegramie pomagał w instalacji kryptominerów

Od kilku lat nastąpił wysyp komunikatorów internetowych. Spora część z nich twierdzi, że ich używanie gwarantuje wyższy poziom bezpieczeństwa. Nie zawsze jednak okazuje się to prawdą, co pokazuje przykład Telegramu. [Czytaj dalej »](#)

do 40% taniej na wszystkie VPS

aruba CLOUD

SPRAWDŹ TERAZ >>>

oferta ważna do 02.01.2018

Powered by vmware

Data Center w Warszawie

Najlepsze w tym miesiącu

Jak aplikacje fitnessowe ujawniają lokalizacje tajnych obiektów wojskowych

Kupiłem trzy iPhone'y, ale nikt mi o tym nie powiedział – przewodnik ofiary

Mistrz świata social engineeringu zhakował dyrektorów CIA, FBI i wywiadu

Jak Chińczycy sprezentowali Afryce nie konia

Najbliższe Szkolenia:

Atak/Ochrona Webaplikacji

8-9 marca
KRAKÓW

19-20 marca
GDAŃSK

26-27 marca
WROCŁAW

Bezpieczeństwo Sieci/Testy Penetracyjne

14-15 marca
WARSZAWA

20:26
13.2.2018

Serwis PZPN ujawnił skany dowodów osobistych kibiców

Autor: Marcin Maj | Tagi: dane osobowe, dowody osobiste, kibice, piłka nożna, PZPN, sport, wyciek |



Uczestniczenie w imprezach sportowych coraz częściej wiąże się z rejestracją online. Czasem aby kupić bilet przez internet trzeba nawet podesłać skan dowodu. Takie właśnie skany podsyłali użytkownicy serwisu internetowego PZPN dla kibiców -- laczynaspilka.pl. Niestety, przesyłane obrazy dowodów nie były odpowiednio zabezpieczone i podejrzeć je mógł każdy. [Czytaj dalej »](#)

18 komentarzy

TOP 5 miesiąca

1. Rosyjscy rządowi hackerzy byli podglądani przez kamerę przez ...holenderskich rządowych hackerów kiedy hackowali amerykański rząd
2. Tajne obiekty wojskowe z całego świata zaświeciły się na żółto na tej mapie
3. CBA zatrzymało twórców polskiego antywirusa ...który w ogóle nie działał
4. Wyciek haseł 144 000 użytkowników Autocentrum.pl
5. Ten biletomat cię podgląda, a o tym wjeżdźcie na parking ktoś może od razu się dowiedzieć

8:00
13.2.2018

Jak w niecodzienny sposób mBank wziął "pożyczkę" od klienta na 20%

Zaproś nas do Twojej firmy!

Przyjedziemy do Twojej firmy i wygłosimy jeden z 6 **cyberwykładów**. Wiedzę przekażemy z humorem i w przystępny dla każdego pracownika sposób. Kliknij tu i zobacz opisy wykładów!

Newsletter

Aby otrzymywać powiadomienia o nowych postach, wpisz swój e-mail:

lub dodaj nas do czytnika RSS:



*ptr //czyli nasz linkblog

* Niezbyt popularny, ale ciekawy atak "na negatywa z Allegro"

* Naprawdę uważajcie na

Bitcointomaty

* Korzystałeś z poczty Plusnet? Pozwól, że Cię uspokoimy...

* Uwaga na skan potwierdzenia wpłaty od "kancelarii"

* Lotnisko w Modlinie i hasła na

10 rad podnoszących bezpieczeństwo komputera od [Niebezpiecznik.pl](http://niebezpiecznik.pl)

(ver 0.9 z 10 sierpnia 2014)

>> Krótki link do tego dokumentu to <http://nbzp.cz/10-porad-bezpieczenstwa>

Oto zestaw czynności, których wykonanie powinno podnieść ogólne bezpieczeństwo Twojego prywatnego komputera, telefonu lub tabletu. Wykonaj je, a utrudnisz hakerom/cyberprzestępcom kradzież twoich prywatnych danych zarówno z dysków twoich urządzeń jak i z serwisów internetowych, na których masz konta.

Porady kierowane są do “przeciętnego Kowalskiego”, ale część z nich może wymagać pewnego obycia z komputerem. W razie niejasności pytaj w komentarzach lub poproś znajomego informatyka o pomoc w konfiguracji. Obiecujemy maksymalnie uprościć język tego poradnika w jego przyszłych edycjach.

UWAGA! Dokument jest w trakcie tworzenia. Każdy może zostawić komentarz, do czego zachęcamy.

Wystarczy skorzystać z menu na górze strony. Prosimy jednak o dodawanie **maksymalnie praktycznych komentarzy**, zawierających przydatne narzędzia oraz porady podnoszące bezpieczeństwo. Wasze komentarze zostaną rozpatrzone i przeniesione do tekstu. Chętnych do aktywnego rozbudowania tego poradnika zapraszamy do [kontaktu](#) - otrzymacie uprawnienia edytora tego dokumentu. A jeśli bardzo lubicie pisać o (nie)bezpieczeństwie, to zachęcamy do stałej współpracy w ramach serwisu [Niebezpiecznik.pl](http://niebezpiecznik.pl) – [szukamy redaktorów](#) (i **płatimy** za artykuły :-)

Akcja	Opis neutralizowanego ataku	UWAGI i przydatne programy
1. Zaszzyfruj *cały* dysk twardy (tzw. <i>full disk encryption</i>)	Chroni przed nieuprawnionym dostępem do danych, np. na skutek kradzieży lub w sytuacji w której zostawiłeś sprzęt bez opieki w hotelowym pokoju, schodząc na śniadanie (tzw. atak Evil Maid).	Programy: - TrueCrypt dla Windows (http://www.truecrypt.org/ projekt przechodzi pewne niezrozumiałe zmiany , został nagle zamknięty przez developerów, zaleca się korzystanie z innego oprogramowania lub pozostanie przy wersji 7.1.a) - FileVault2 dla Mac OS X (wbudowany w system, w zakładce “Security & Privacy” w systemowych preferencjach). Po skonfigurowaniu FileVaulta uruchom terminal i wydaj polecenie: <code>sudo pmset -a hibernatemode 25</code>



XI Forum Bezpieczeństwa i Audytu IT

SEMAFOR

15-16 MARCA 2018
PGE NARODOWY
WARSZAWA

POWRÓT DO PODSTAW: NOWE ZAGROŻENIA, STARE PROBLEMY

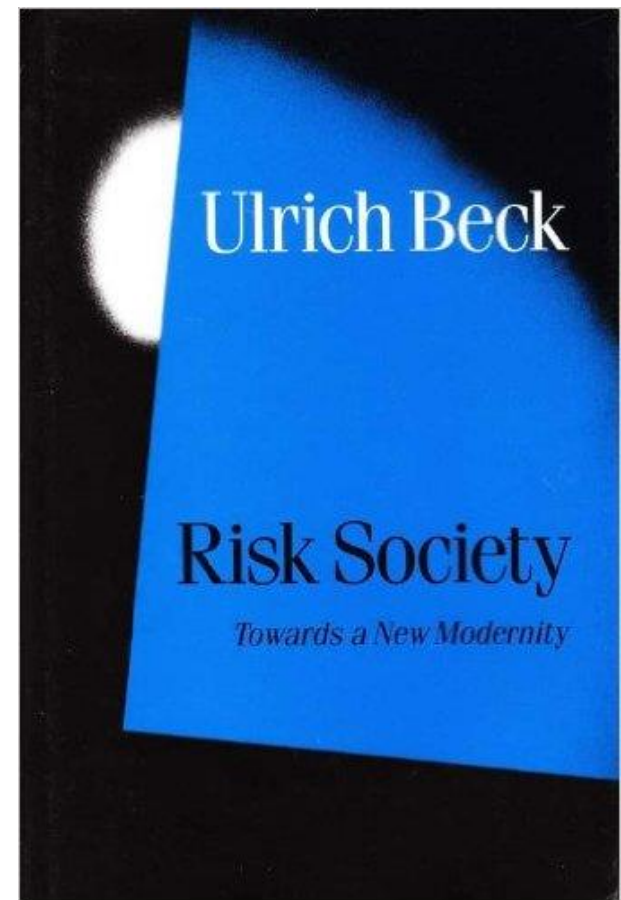
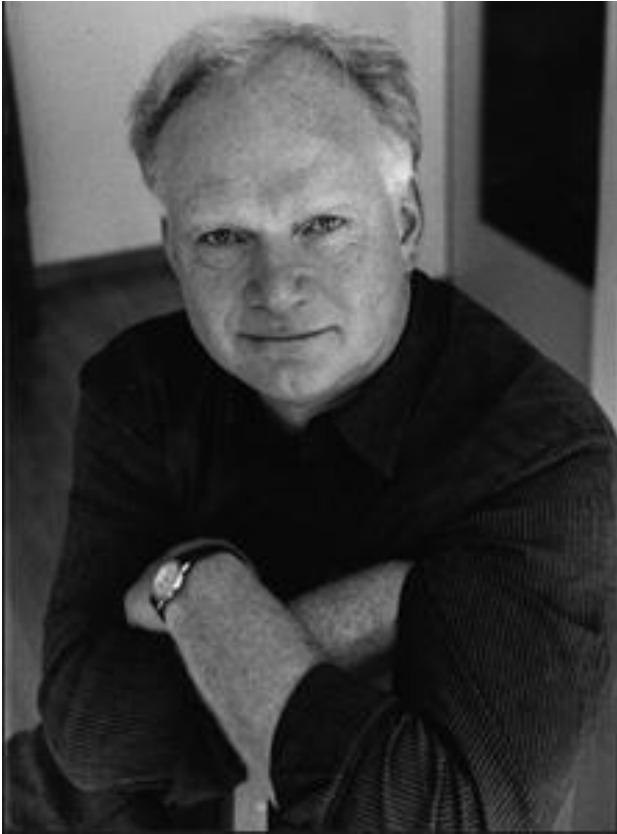
ZAREJESTRUJ SIĘ

RODO

- Od maja 2018 roku przepisy dotyczące ochrony danych osobowych dla wszystkich 28 państw członkowskich zostały ujednolicone.
- Intencją unijnych urzędników było unowocześnienie regulacji o ochronie danych osobowych, które obowiązuje od 1995 r. i w dobie postępującej cyfryzacji mają coraz mniejsze zastosowanie praktyczne. Jednocześnie nowe prawo zostało stworzone tak, aby było „technologicznie neutralne”, czyli aktualne niezależnie od rozwoju technologii.



Ulrich Beck (1944 – 2015)



Niebezpieczeństwo jest do przewidzenia. Ryzyko jest nie do przewidzenia, póki się nie objawi.

„Próbujemy zgadnąć, co się może wydarzyć, ale wszystkich ewentualności nie sposób przewidzieć. To jest istota ryzyka.”

Powodzenie w stworzeniu sztucznej
inteligencji byłoby największym
osiągnięciem w historii ludzkości.
Mogłoby też być ostatnim.

Stephen Hawking