



UpGreat
we know-how to do IT

Wsparcie dla biznesu





KONFERENCJA

„NOWOCZESNA INFRASTRUKTURA IT W CZASACH NIEPEWNOŚCI – INNOWACYJNOŚĆ,
BEZPIECZEŃSTWO, WYDAJNOŚĆ – SPOJRZENIE W PRZYSZŁOŚĆ Z HUAWEI”

Concordia Design
Poznań, 22 maja 2025

Piotr Flis
UpGreat Systemy Komputerowe Sp. z o.o.

AGENDA

PROWADZENIE

- Arkadiusz Giedrojć – Chief Technology Officer Norddics & CEE, Huawei Enterprise
- Konrad Tutak – Data Center Solution Sales Leader, Huawei Enterprise
- Piotr Flis – Prezes Zarządu, UpGreat Systemy Komputerowe

AGENDA

- 10:00 - 10:15 – Rejestracja uczestników i swobodny networking przy kawie i przekąskach
- 10:15 - 10:30 – Otwarcie spotkania i przywitanie gości
- 10:30 - 11:00 – Wyzwania dla infrastruktury IT w obliczu globalnej niepewności – Piotr Flis, Prezes Zarządu, UpGreat Systemy Komputerowe
 - Wpływ geopolityki na wybory technologiczne
 - Znaczenie niezależności dostawców i odporności łańcucha dostaw
 - Dlaczego warto inwestować w sprawdzone rozwiązania z silnym wsparciem lokalnym,
 - Referencje w Polsce i w Europie oraz certyfikaty CC i EUCC
- 11:00 - 11:15 – Przerwa na kawę i rozprostowanie kolan
- 11:15 - 12:00 – Nowoczesne systemy storage Huawei – bezpieczeństwo, elastyczność i niezawodność – Konrad Tutak, Sales Leader, Huawei Enterprise Data Center Solution
 - Macierze All-flash SAN i NAS – szerokie portfolio dostosowane do małych oraz dużych przedsiębiorstw
 - W jaki sposób odtworzyć backup w kilka minut? Użyj najlepszych na rynku deduplikatorów OceanProtect
 - Cyfrowy bunkier nie tylko dla zamożnych – architektura rozwiązania
- 12:00 - 12:45 – Rozwiązania sieciowe Huawei – stabilność, wydajność, bezpieczeństwo - Arkadiusz Giedrojc, Chief Technology Officer, Norddics & CEE, Huawei Enterprise
 - Portfolio Huawei w zakresie przełączników, routerów i Wi-Fi 6/7
 - Centralne zarządzanie z iMaster NCE
 - Case studies i wdrożenia w Polsce
 - Live-demo interfejsu iMaster NCE i/lub NetMaster (DeepSeek R1)
- 12:45 - 13:00 – Podsumowanie spotkania i wręczenie upominków – Piotr Flis, Prezes Zarządu, UpGreat Systemy Komputerowe
- 13:00 - 14:00 – Lunch



O UPGREAT



SPOKÓJ W BIZNESIE

O UPGREAT

- **BEZPIECZEŃSTWO SYSTEMÓW IT**

Bezpieczeństwo w IT jest zagadnieniem złożonym i obejmującym wiele obszarów kompetencyjnych. Składa się na nie m.in. bezpieczeństwo procesów biznesowych, bezpieczeństwo danych, bezpieczeństwo infrastruktury, bezpieczeństwo użytkowników, bezpieczeństwo komunikacji, zgodność z wymogami prawa.



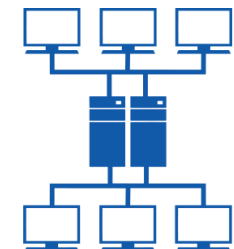
- **OUTSOURCING IT**

Sprawne zarządzanie nowoczesnym i złożonym środowiskiem IT wymaga zaawansowanej wiedzy nie tylko w zakresie technologii, ale również procesów biznesowych, czy dobrych praktyk zdefiniowanych np. w bibliotece ITIL. Nasz zespół techniczny jest przygotowany do przejęcia opieki nad całością lub wybranymi fragmentami systemu IT.



- **ARCHITEKTURA SYSTEMÓW IT**

Od warstwy fizycznej po warstwę aplikacyjną infrastruktura IT wymaga przemyślanych i dostosowanych do wymogów Klienta rozwiązań. Wieloletnie doświadczenie w tym zakresie pozwoliło nam na przygotowanie kompleksowej oferty z zakresu systemów IT.



BEZPIECZEŃSTWO IT

INSTALACJE NISKOPRĄDOWE

SIECI / CCTV / KD / SSP / ZASILANIE

LAN – 100+

WLAN – 100+ | POMIARY i SYMULACJE

WAN – 1000+

STYK Z SIECIĄ INTERNET

PROJEKT

WYKONAWSTWO

ZARZĄDZANIE

PARTNERZY



ZAUFALI NAM



Szkoła Główna
Służby Pożarniczej





Wyzwania dla infrastruktury IT w obliczu globalnej niepewności

ZŁY CHIŃCZYK – DOBRY AMERYKANIN



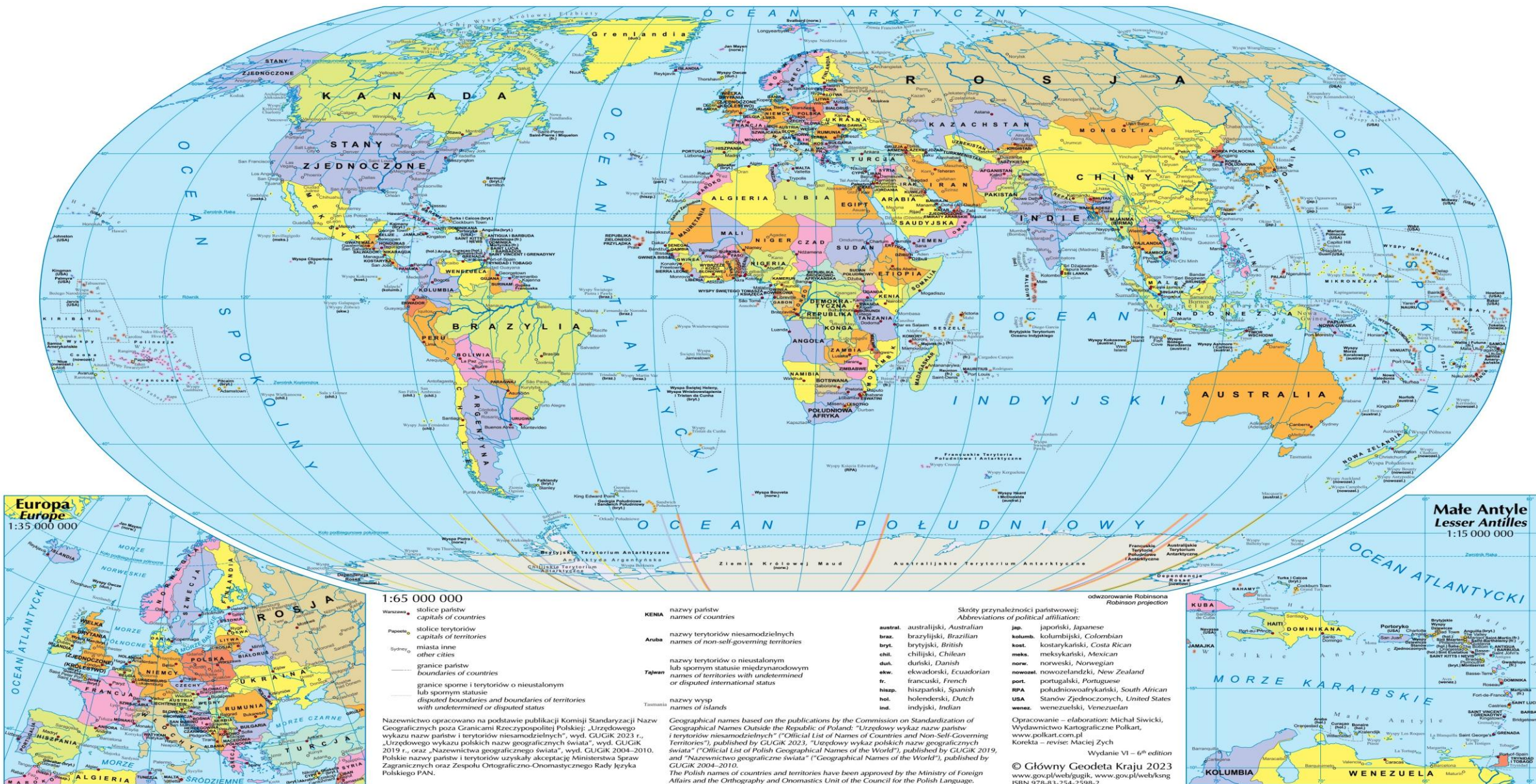
PIVOT TO ASIA

- Barack Obama ogłosił „pivot to Asia” (zwrot ku Azji) w listopadzie 2011 roku. Kluczowym momentem była jego przemowa przed parlamentem Australii, w której wyraźnie zaznaczył zmianę priorytetów amerykańskiej polityki zagranicznej z Europy i Bliskiego Wschodu na region Azji Wschodniej i Pacyfiku.
- Strategia ta miała być odpowiedzią na rosnącą potęgę Chin i miała na celu wzmocnienie amerykańskiej obecności militarnej, gospodarczej i dyplomatycznej w regionie.
- Kolejni prezydenci konsekwentnie realizują tę politykę.
- Deng Xiaoping ogłosił otwarcie Chin na świat w ramach reform zapoczątkowanych podczas III Plenum Komitetu Centralnego Komunistycznej Partii Chin XI kadencji, które odbyło się w grudniu 1978 roku
 - Od tego czasu PKB Chin wzrósł z 149,5 mld. do przewidywanego w 2025 roku 18,6 bln. USD
 - Oznacza to ponad 120 krotny wzrost PKB
- Obecnie dług USA w Japonii do 1 bln USD a Chinach to 970 mld. USD



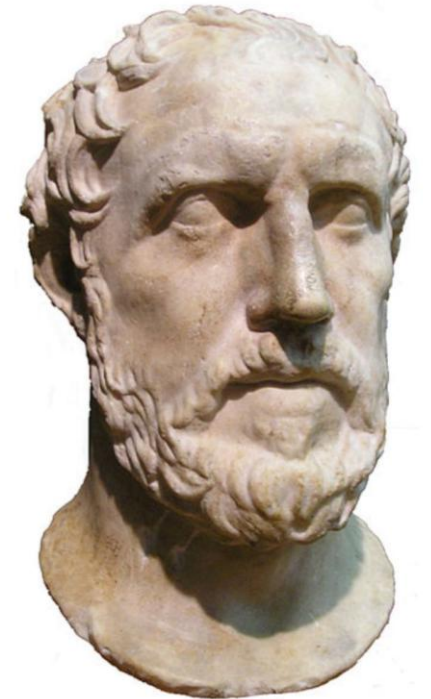
ŚWIAT – państwa i terytoria niesamodzielne 2023

THE WORLD – countries and non-self-governing territories 2023



CO TO JEST PUŁAPKA TUKIDYDESA?

- Pułapka Tukidydesa to pojęcie współczesnej teorii stosunków międzynarodowych, zaczerpnięte od starożytnego greckiego historyka Tukidydesa, który w dziele „Wojna peloponeska” opisał mechanizm prowadzący do konfliktu między rosnącą potęgą a dotychczasowym hegemonem.
- Według Tukidydesa prawdziwą przyczyną wojny peloponeskiej był szybki wzrost potęgi Aten i strach, jaki to wzbudziło w dominującej dotąd Sparcie. Sparta, obawiając się utraty swojej pozycji, zdecydowała się na wojnę, mimo że ani ona, ani Ateny nie chciały jej w rzeczywistości. Konflikt okazał się nieunikniony, ponieważ obie strony postrzegały działania drugiej strony jako zagrożenie dla własnego bezpieczeństwa i statusu.
- Współcześnie termin „pułapka Tukidydesa” został spopularyzowany przez amerykańskiego politologa Grahama Allisona i odnosi się do sytuacji, gdy wschodząca potęga (np. Chiny) zagraża dotychczasowemu hegemonowi (np. USA), co może prowadzić do eskalacji napięć, a nawet konfliktu zbrojnego, nawet jeśli żadna ze stron nie dąży do wojny.
- Mechanizm ten polega na tym, że wzrost siły jednej strony wywołuje obawy i reakcje drugiej strony, co może prowadzić do błędnej oceny intencji i eskalacji działań, często pod wpływem sojuszników lub okoliczności.

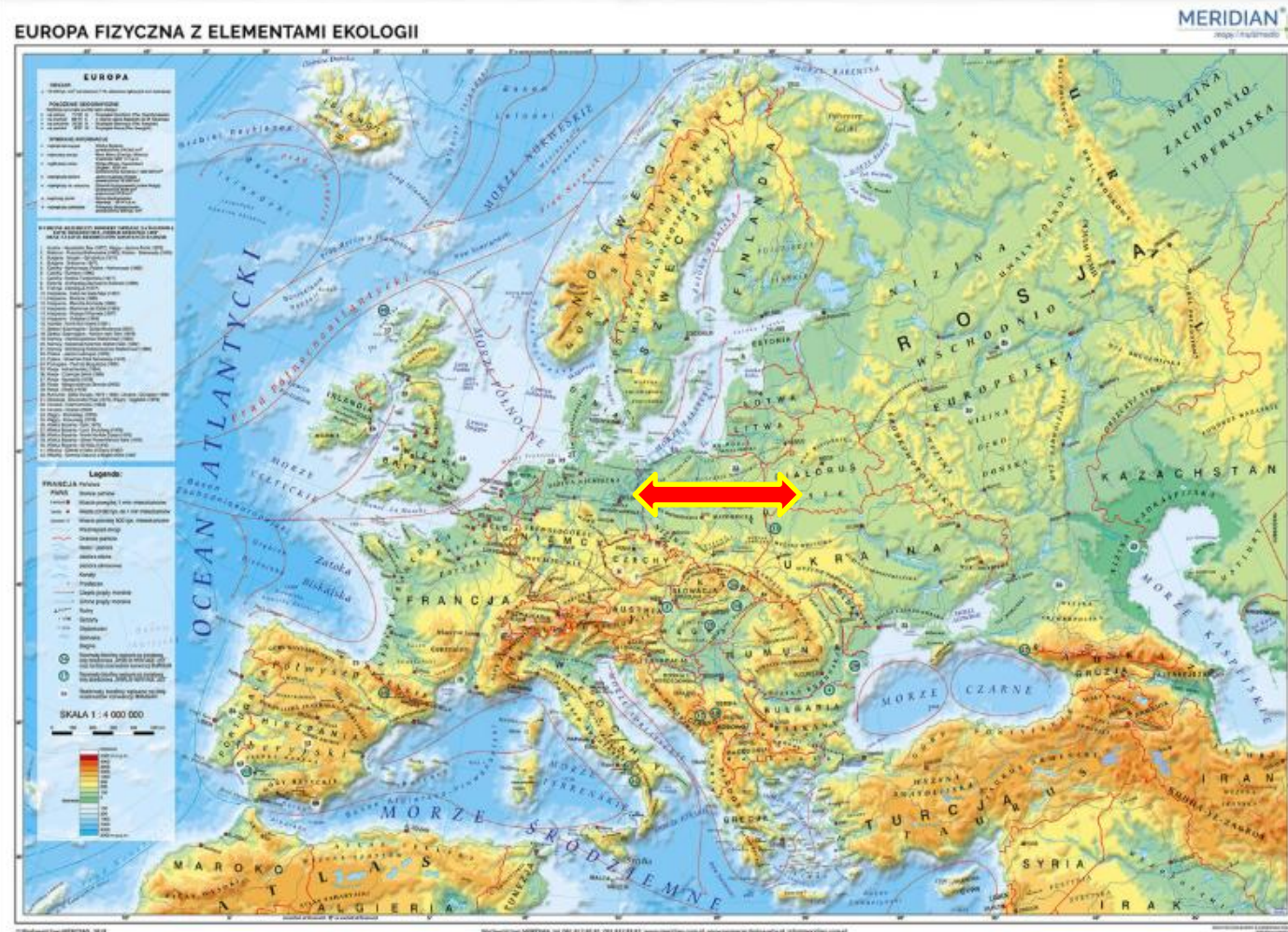


POLSKIE INTERESY NARODOWE I CELE STRATEGICZNE – 1

- Interesy narodowe:
 - strzeżenie niepodległości, nienaruszalności terytorialnej, suwerenności oraz zapewnienie bezpieczeństwa państwa i obywateli;
 - kształtowanie porządku międzynarodowego, opartego na solidarnej współpracy i poszanowaniu prawa międzynarodowego, dającego gwarancje bezpiecznego rozwoju Polski;
 - umacnianie tożsamości narodowej i strzeżenie dziedzictwa narodowego;
 - zapewnienie warunków do trwałego i zrównoważonego rozwoju społecznego i gospodarczego oraz ochronę środowiska naturalnego.
- Cele strategiczne
 - Zintegrowanie elementów systemu kierowania bezpieczeństwem narodowym;
 - Zwiększenie poziomu odporności państwa, ze szczególnym uwzględnieniem ochrony ludności i obrony cywilnej;
 - Stworzenie systemu obrony powszechnej, opartego na wysiłku całego narodu we wszystkich formach jego organizacji; 4)
 - Wzmacnianie zdolności Sił Zbrojnych RP do odstraszenia i obrony przed zagrożeniami dla bezpieczeństwa państwa oraz w ramach kolektywnej obrony NATO, ze szczególnym uwzględnieniem podniesienia poziomu modernizacji technicznej i reformy organizacyjnej, umożliwiającej prowadzenie długotrwałego konfliktu zbrojnego o dużej intensywności;
 - Zapewnienie proaktywnej obrony i ochrony przed zagrożeniami w nowych domenach, w tym m.in. w cyberprzestrzeni, w przestrzeni informacyjnej i kognitywnej;

https://t.prezydent.pl/storage/file/core_files/2024/7/4/7fa9f08052b51758d6ed4e9a11a9d32d/REKOMENDACJE%20SBNRP%204%20lipca%202024.pdf

BRAMA DO EUROPY – MIĘDZY BAŁTYKIEM I KARPATAMI



POLSKIE INTERESY NARODOWE I CELE STRATEGICZNE – 2

- Cele strategiczne cd.
 - Aktywne promowanie wizerunku Polski, a także jej polityki i celów strategicznych na arenie międzynarodowej;
 - Kształtowanie polityki NATO i UE w sposób zgodny z interesami bezpieczeństwa Polski, utrzymywanie strategicznego partnerstwa z USA oraz intensyfikację współpracy w formatach regionalnych i bilateralnych;
 - Wzmacnianie tożsamości narodowej i spójności społecznej;
 - Tworzenie warunków umożliwiających poprawę sytuacji demograficznej, w tym warunków do ochrony i rozwoju rodziny (szczególnie zwiększenie dzietności);
 - Tworzenie warunków do rozwoju gospodarczego i społecznego w powiązaniu z interesami bezpieczeństwa państwa;
 - Wzmocnienie konkurencyjności polskiej gospodarki poprzez promowanie polskiej nauki oraz zwiększenie nakładów na badania i rozwój ze szczególnym uwzględnieniem technologii podwójnego zastosowania;
 - Zbudowanie potencjału polskiego przemysłu obronnego zdolnego do zabezpieczenia potrzeb Sił Zbrojnych RP (w tym w zakresie systemów bezzałogowych i amunicji), rozbudowa jego zdolności eksportowych oraz zredukowanie uzależnienia od zewnętrznych łańcuchów dostaw w tym zakresie;
 - Wzmocnienie bezpieczeństwa energetycznego państwa;
 - Zapewnienie bezpieczeństwa ekologicznego państwa;
 - Podniesienie i zapewnienie bezpieczeństwa żywnościowego, również na wypadek zaistnienia konfliktu zbrojnego;
 - Zapewnienie bezpieczeństwa zdrowotnego.

https://t.prezydent.pl/storage/file/core_files/2024/7/4/7fa9f08052b51758d6ed4e9a11a9d32d/REKOMENDACJE%20SBNRP%204%20lipca%202024.pdf

CO JEST WAŻNE DLA NAS (POLAKÓW) W KONTEKŚCIE IT?

- Cyfrowa suwerenność
 - W ujęciu najprostszym - cyfrowa suwerenność to zdolność do kontrolowania przez dany kraj własnej sytuacji w aspektach technologiczno-cyfrowych. Czy suwerenne może być państwo, które wszystkie technologie (również te, które służą administracji publicznej) bierze od wielkich, zagranicznych firm internetowych?
 - Suwerenność danych to kontrola nad danymi, miejscem ich przechowywania, wykorzystaniem
- Co jest potrzebne aby uzyskać cyfrową suwerenność?
 - Własne zdolności
 - Dywersyfikacja
 - Bezpieczeństwo
 - Fizyczne
 - Cyber
 - Odporność Państwa

<https://cyberdefence24.pl/social-media/cybermagazyn-czym-jest-cyfrowa-suwerennosc-i-dlaczego-warto-w-nia-inwestowac>

ANALIZA RYZYKA – OBOWIĄZEK RZĄDZĄCYCH TO OCENA KAŻDEJ Z EWENTUALNOŚCI

- Identyfikacja zagrożeń – rozpoznawanie potencjalnych niebezpieczeństw i źródeł ryzyka.
- Ocena prawdopodobieństwa i wpływu – określenie, jak często dane ryzyko może wystąpić i jakie mogą być jego konsekwencje.
- Priorytetyzacja ryzyk – ustalenie, które zagrożenia są najistotniejsze dla realizacji celów.
- Planowanie działań zaradczych – opracowanie strategii przeciwdziałania lub minimalizacji skutków ryzyka.

NA MARGINESIE – IMPREZA 11 CZERWCA – Ransomware - wielkie zagrożenie dla firm i organizacji w Polsce. Jak się zabezpieczyć? → TUTAJ MOŻNA SIĘ ZAREJESTROWAĆ

Miejsce Concordia Design Poznań
Data 11 czerwca 2025 godzina 09:00

09:00 09:15 Rejestracja uczestników i swobodny networking przy kawie i przekąskach.

O zagrożeniach

09:15 10:00 "Krajobraz zagrożeń 2025" - o czym musimy wiedzieć planując bezpieczeństwo
Złośliwe oprogramowanie historycznie i dzisiaj
Jak wygląda cyber kill chain?
Macierz Mitre ATT&CK - ile realnych zagrożeń musimy zwalczyć?
Lolbin/Lolbas - techniki wykorzystywane przez malware
Znane grupy APT
Wnioski

Kuba Staśkiewicz

10:00 10:25 Dobre praktyki w obszarze cyber-bezpieczeństwa systemów IT/OT

Kuba Staśkiewicz, Piotr Flis

10:25 10:35 Przerwa na kawę i rozprostowanie kolan

-

Narzędzia

10:35 11:10 Netapp – backup, snapshoty, aktywna ochrona przed Ransomware, wczesne wykrywanie anomalii
11:10 11:40 **A Teraz Polska!** – Rublon MFA – must have dla każdego
11:40 12:10 **A Teraz Polska!** – FuseAI – ofensywne usługi cyberbezpieczeństwa realizowane w sposób ciągły

Łukasz Bajer

Przemek Kucharzewski

Przemek Kucharzewski

12:10 12:20 Przerwa na kawę i rozprostowanie kolan

-

12:20 12:50 **A Teraz Polska!** – LOG Plus – więcej niż ITAM

Dominika Maciaszek

12:50 13:15 ExaGrid – skuteczna deduplikacja i odporność na ransomware

Łukasz Bajer

13:15 13:25 Podsumowanie spotkania i wręczenie upominków

Piotr Flis

13:25 14:15 Lunch

CZY EUROPA UZALEŻNIŁA SIĘ OD TECHNOLOGII Z USA?

Infrastruktura teleinformatyczna w typowej europejskiej firmie:

- Rozwiązania sieciowe – Cisco, Fortinet, Juniper, Dell, HP, Aruba, Ubiquity, PaloAlto,
- Serwery, desktopy, laptopy: HP, Dell, Apple
- Pamięci masowe: EMC, Dell, HP
- Wirtualizacja: VMware, HyperV (Microsoft), Oracle
- Cloud computing: AWS, Google, Microsoft
- Oprogramowanie i platformy SaaS: Microsoft, Google, Salesforce, Oracle, Slack, Asana, Jira
- Platformy społecznościowe i video: FB, Instagram, X, YouTube, Vimeo
- Inne: CloudFlare



<https://opensecurity.pl/czy-europa-uzaleznila-sie-od-technologii-z-usa/>

ALTERNATYWA

Na liście nie widać firmy z Polski ☹️ I z Chin również ...

- Sami (lub nie sami) zdeindustrializowaliśmy się w IT
- Co to jest myślenie słonia?
- Ile kosztuje fabryka chipów?



GRUPA PRODUKTÓW	PRODUCENT	KRAJ
Sieci LAN/WAN/WiFi/GSM  	Nokia	 Finlandia
	Ericsson	 Szwecja
	Alcatel-Lucent	 Francja
	Siemens	 Niemcy
	Allied Telesis	 Japonia
	LANCOM	 Niemcy
Serwery rack, desktopy, laptopy  	Atos	 Francja
	Fujitsu	 Japonia
	OVH	 Francja
	ASUS	 Tajwan
	ASRock	 Tajwan
	Gigabyte	 Tajwan
	Samsung	 Korea Płd.
	Dynabook(Toshiba)	 Japonia
Pamięci masowe 	Hitachi	 Japonia
	Fujitsu	 Japonia
	OVH	 Francja
	Atos	 Francja
Cloud computing, wirtualizacja 	ProxMox	 Niemcy
	OVH	 Francja
	T-Systems	 Niemcy
	Atos	 Francja
SaaS, praca grupowa, poczta 	Nextcloud	 Niemcy
	Proton	 Szwajcaria

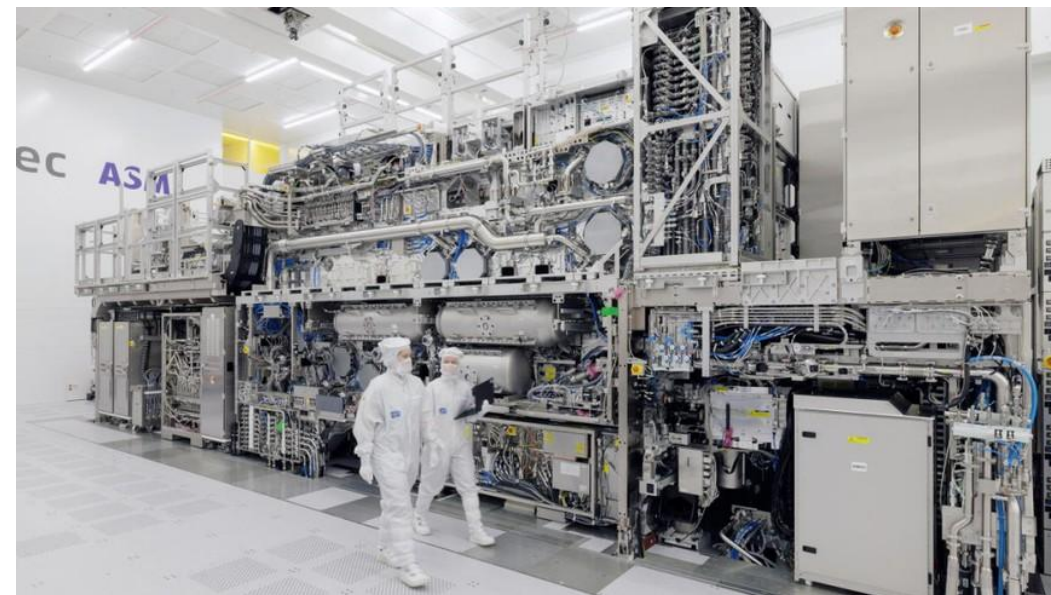
ILE KOSZTUJE FABRYKA CHIPÓW?

YOUR EASY KEY TO IOT

GET YOUR IOT SOLUTION



We Włoszech powstanie fabryka chipów - koszt wyniesie 3,5 mld dolarów Jak poinformowało włoskie ministerstwo przemysłu, produkująca półprzewodniki singapurska firma Silicon Box zainwestuje 3,2 mld euro (3,50 mld dolarów) w nową fabrykę w północnych Włoszech.



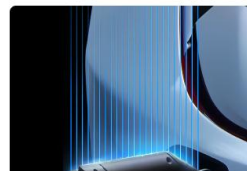
ASML EXE:5000, czyli kosztujący ponad 350 mln dol. skaner EUV High-NA

Ruszyła budowa fabryki chipów w Saksonii. Miliardy dotacji Kanclerz Niemiec Olaf Scholz broni rządowych dotacji dla fabryki półprzewodników tajwańskiego giganta TSMC w Dreźnie. Eksperci są sceptyczni

ILE KOSZTUJE FABRYKA CHIPÓW?

YOUR EASY KEY TO IOT

GET YOUR IOT SOLUTION



We Włoszech wyniesie 3,5 m

włoskie ministe
półprzewodnik
zainwestuje 3,2
nową fabrykę w

HEADQUARTERS

TELTONIKA IOT GROUP

 Saltoniškų st. 14, LT-08105, Vilnius, Lithuania

 +37052409650

CONTACT US



nad 350 mln dol.

Miliardy dotacji

n dotacji dla
a TSMC w

ALTERNATYWA Z EUROPY



Google Analytics

Google Analytics is a free and wid...

30 alternatives



Amazon Web Services (AWS)

Amazon Web Services is one of th...

12 alternatives



Gmail

Gmail is a free email provider by ...

21 alternatives



NordVPN

NordVPN is one of the most popu...

7 alternatives



Google Maps

Google Maps is one of the most p...

8 alternatives



Slack

Slack is one of the most widely us...

12 alternatives



Google Tag Manager

Google Tag Manager (GTM) is a ta...

7 alternatives



Microsoft Teams

Microsoft Teams is a business co...

12 alternatives



Sentry

Sentry is an error tracking service....

4 alternatives



Cloudflare

Cloudflare provides CDN and DD...

6 alternatives



Microsoft Bing

Microsoft Bing is after Google Sea...

6 alternatives



Google Public DNS

The Google Public DNS is a free D...

10 alternatives

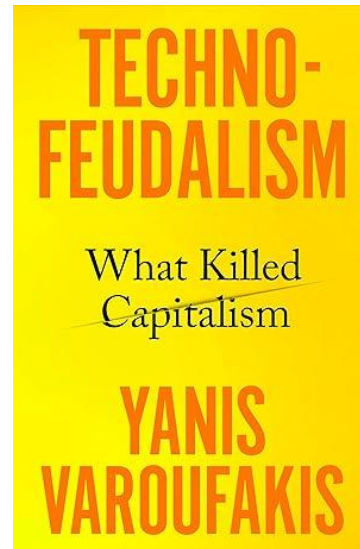
<https://european-alternatives.eu/alternatives-to>

DO CZEGO UŻYWANE SĄ NASZE DANE?

Ludzka wolna wola nie istnieje – człowiek może być uważany za „operatora”, realizującego program przekazany mu w procesie warunkowania - B.F. Skinner, twórca behawioryzmu radykalnego.

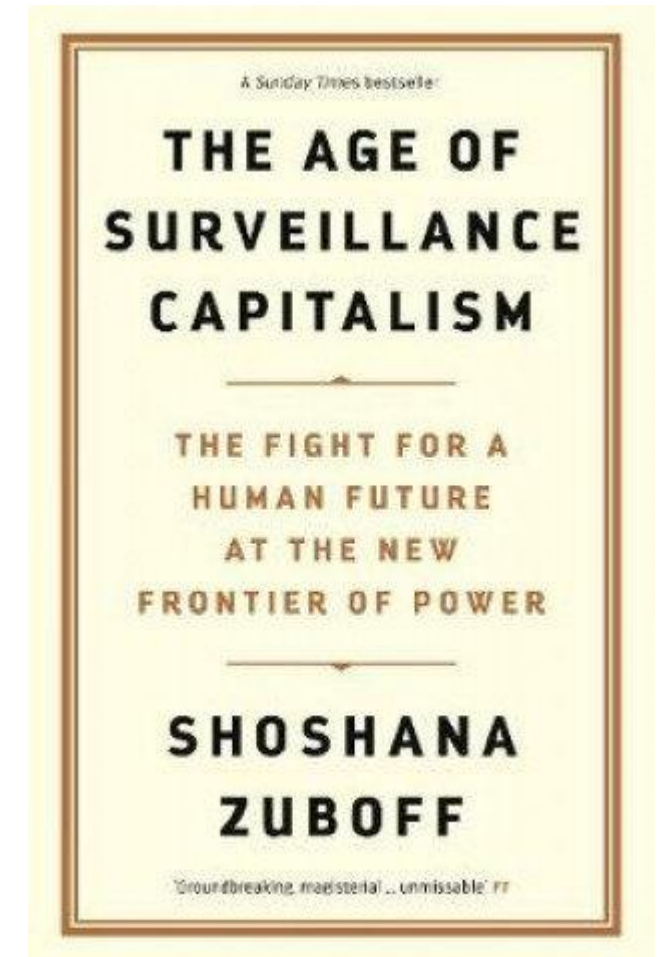
Dane to najważniejszy zasób

- Big Data
- AI
- Manipulacja
- Handel danymi
- E-Commerce
- Reklama
- Cyberprzestępczość
- ...



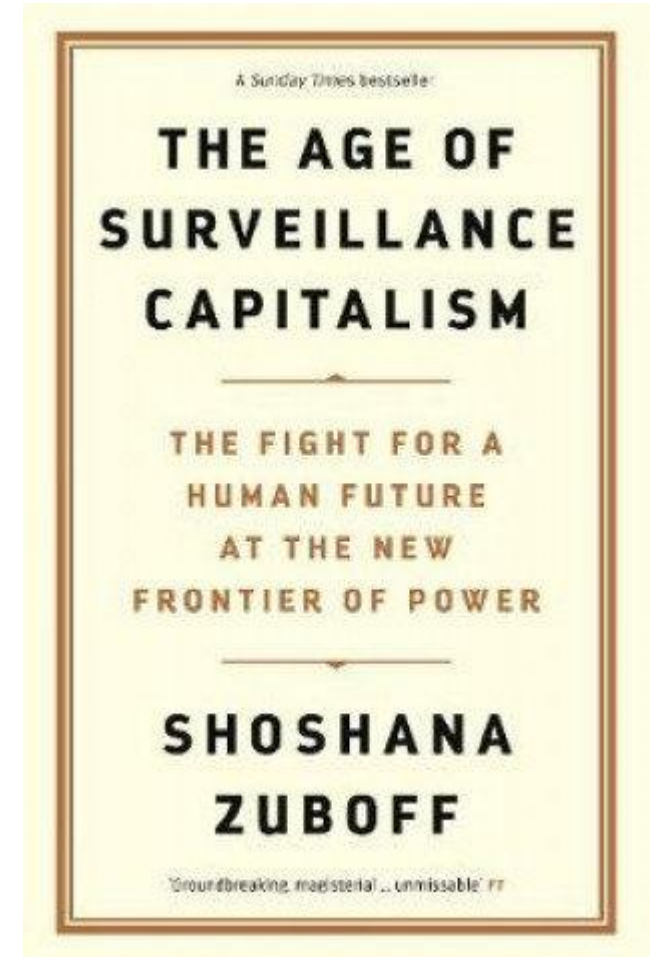
KTO KRADNIE NASZE DANE?

- **WSZYSCY** – inwigilacja to **model biznesowy największych firm technologicznych**
- Samochody Google Street View, oprócz wykonywania zdjęć ulic, zbierały dane o sieciach Wi-Fi – początkowo miały to być wyłącznie publicznie dostępne nazwy sieci (SSID) i adresy MAC routerów, co miało służyć poprawie geolokalizacji w usługach Google Maps. W wyniku audytu okazało się jednak, że oprogramowanie używane w samochodach Street View „przez pomyłkę” zbierało także fragmenty tzw. payload data, czyli rzeczywiste dane przesyłane przez otwarte, niezabezpieczone sieci Wi-Fi. Mogły to być m.in. fragmenty e-maili, hasła czy adresy odwiedzanych stron. -> <https://epic.org/documents/investigations-of-google-street-view/>
- [The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power - Book - Faculty & Research - Harvard Business School](#)
 - Google i Facebook gromadzą ogromne ilości danych o użytkownikach – nie tylko te, które są niezbędne do działania usług, ale także tzw. „behawioralny nadmiar” (behavioural surplus). Dane te są przetwarzane przez algorytmy, by przewidywać i wpływać na przyszłe zachowania użytkowników, a następnie sprzedawane na „rynkach przyszłości behawioralnych” (behavioural futures markets).
 - Ukryte mikrofony i sensory w urządzeniach domowych – Zuboff opisuje przypadki, gdy użytkownicy nie byli świadomi obecności mikrofonów w urządzeniach takich jak Google Nest, co rodzi pytania o zakres i cel zbieranych danych.



KTO KRADNIE NASZE DANE?

- Zuboff przytacza sytuacje, w których urządzenia do leczenia bezdechu sennego przesyłają dane o użytkowaniu do ubezpieczycieli zdrowotnych, którzy na tej podstawie mogą ograniczać świadczenia lub podnosić składki.
- Według Shoshany Zuboff, inwigilacja danych jest fundamentem modelu biznesowego cyfrowych gigantów (**Google, Facebook, Microsoft, Apple, Amazon**), ale rozprzestrzeniła się także na inne sektory, np. ubezpieczenia zdrowotne czy edukację. Dane o klientach i użytkownikach są wykorzystywane do profilowania, manipulacji oraz podejmowania decyzji biznesowych.
- Każde urządzenie **Google Nest** jest objęte wieloma umowami i politykami prywatności, które są trudne do przeanalizowania przez przeciętnego użytkownika. Według analiz naukowców z **University of London**, korzystanie z jednego termostatu Nest w ekosystemie połączonych urządzeń i aplikacji może wymagać zgody na nawet **1000 różnych umów i polityk**.



KTO KRADNIE NASZE DANE?

- W 2013 roku **Edward Snowden** ujawnił, że:
 - NSA śledziło rozmowy telefoniczne milionów amerykańców,
 - GCHQ wpięło się do 200 telekomunikacyjnych kabli światłowodowych by śledzić do 600 milionów rozmów telefonicznych dziennie,
 - NSA przeprowadziło ponad 61 000 operacji hackerskich, w tym dotyczących Singapuru i Chin kontynentalnych.
- W lipcu 2013 **Der Spiegel** oskarżył **NSA** o podsłuchiwanie urzędników Unii Europejskiej.
- W październiku 2013 **The Guardian** ujawnił, że **NSA** podsłuchiwało 35 światowych liderów, w tym **Kancelarz Angelę Merkel**.
- Począwszy od 2017 roku **USA** twierdziły, że **Huawei** i **ZTE** stanowią zagrożenie dla bezpieczeństwa narodowego. Śledztwa prowadzone przez **FBI** nie dostarczyły dowodów udziału **Huawei** w działaniach szpiegowskich.
- Jednocześnie restrykcje miały jednoznaczny wymiar gospodarczy:
 - **Huawei** oferował sprzęt telekomunikacyjny po bardzo atrakcyjnych, często dumpingowych cenach, co zagrażało pozycji amerykańskich i zachodnich firm na rynku globalnym.
 - Sankcje i ograniczenia miały na celu ograniczenie rozwoju **Huawei** i utrzymanie przewagi technologicznej **USA**, zwłaszcza w obszarze 5G, półprzewodników i sztucznej inteligencji.
 - Ograniczenia były też elementem szerszej wojny handlowej i technologicznej między **USA** a **Chinami**, mającej na celu spowolnienie wzrostu chińskiej potęgi technologicznej.

Attacks from America – NSA Spied on European Union Offices
<https://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html>

Edward Snowden: Leaks that exposed US spy programme - BBC News ->
<https://www.bbc.com/news/world-us-canada-23123964>

KTO KRADNIE NASZE DANE?

W ramach systemu PRISM, National Security Agency (NSA) miała dostęp do danych użytkowników gromadzonych przez największe amerykańskie firmy internetowe. Według ujawnionych przez Edwarda Snowdena dokumentów, do programu PRISM przystąpiły następujące przedsiębiorstwa:

- Microsoft (11 września 2007)
- Yahoo! Inc (12 marca 2008)
- Google (14 stycznia 2009)
- Facebook (3 czerwca 2009)
- AVM Software (administrator Paltalk; 7 grudnia 2009)
- YouTube (24 września 2010; YouTube jest własnością Google)
- Skype (6 lutego 2011; Skype był wówczas własnością Microsoftu)
- AOL (31 marca 2011)
- Apple Inc. (październik 2012)

Afera podsłuchowa: NSA ma “bezpośredni dostęp” do serwerów Google, Facebooka, Skype, Microsoftu i Yahoo oraz podsłuchuje rozmowy telefoniczne wszystkich Amerykanów -- Niebezpiecznik.pl -> <https://niebezpiecznik.pl/post/afera-podsluchowa-nsa-ma-bezposredni-dostep-do-serwerow-google-facebook-a-skype-microsoftu-i-yahoo-oraz-podsluchuje-wszystkich-amerykanow/>

CO OZNACZA SŁOWO FABLESS?

FABLESS – model biznesowy polegający na projektowaniu oraz sprzedaży sprzętu elektronicznego i układów półprzewodnikowych przy jednoczesnym outsourcingu ich produkcji do wyspecjalizowanych producentów działających w modelu biznesowym nazywanym foundry („model odlewni”), którzy zlokalizowani są zazwyczaj, choć nie wyłącznie, w Stanach Zjednoczonych, Chinach i na Tajwanie ->

<https://pl.wikipedia.org/wiki/Fabless>

Udział państw w produkcji zaawansowanych chipów (procesy 5 nm i poniżej):

- Tajwan: 68% udziału w 2023 roku, ale prognozowany spadek do 60% do 2027 roku.
- Korea Południowa: 12% w 2023, wzrost do 13% do 2027.
- USA: 12% w 2023, wzrost do 17% do 2027 (część tej produkcji będzie prowadzona przez zagraniczne firmy, takie jak TSMC i Samsung, na terytorium USA).
- Japonia: 0% w 2023, wzrost do 4% do 2027.
- Chiny: 8% w 2023, spadek do 6% do 2027.

<https://www.visualcapitalist.com/advanced-semiconductor-market-share-2023-2027/>

<https://www.congress.gov/bill/117th-congress/house-bill/4346> -

52.7 mld. USD

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en - **43 mld. EUR**

Ranga	Firma	Siedziba	Przychody (w miliardach US\$)
1	Nvidia	Stany Zjednoczone	49
2	Qualcomm	Stany Zjednoczone	31
3	Broadcom	Stany Zjednoczone	28
4	AMD	Stany Zjednoczone	22
5	Apple	Stany Zjednoczone	19

JAK UFAĆ? CERTYFIKACJE POZWALAJĄ STWIERDZIĆ CZY PRODUKT JEST „BEZPIECZNY”

- Common Criteria (CC) to międzynarodowy standard oceny bezpieczeństwa produktów i systemów IT, określony w normie PN-EN ISO/IEC 15408. Certyfikaty CC potwierdzają, że dany produkt spełnia określone wymagania bezpieczeństwa zgodne z tą normą.
 - Zakres i cel: CC umożliwia formalną weryfikację zabezpieczeń systemów teleinformatycznych, definiuje zagrożenia, zabezpieczenia oraz metody oceny ich skuteczności.
 - Poziomy oceny (EAL): Certyfikacja może być prowadzona na różnych poziomach szczegółowości, od EAL1 (podstawowe testy funkcjonalne) do EAL7 (pełna formalna weryfikacja projektu i testy).
 - Profil ochrony (PP): Określa specyficzne wymagania bezpieczeństwa dla typu produktu lub konkretnego produktu, na podstawie których przeprowadza się ocenę i wydaje certyfikat.
 - Uznawalność międzynarodowa: Certyfikaty CC wydawane przez akredytowane jednostki są uznawane w większości krajów europejskich na mocy porozumienia SOG-IS MRA oraz w wielu krajach świata dzięki porozumieniu CCRA (Common Criteria Recognition Arrangement).
 - Jednostki certyfikujące: W Polsce certyfikaty CC wydaje NASK, jako jedyna jednostka w regionie -> [Common Criteria – NASK OSiC](#)
- EU CC (European Common Criteria Certification) to europejski schemat certyfikacji oparty na standardzie Common Criteria, realizowany w ramach porozumienia SOG-IS MRA. Certyfikaty EU CC są wzajemnie uznawane przez kraje członkowskie, co ułatwia handel i wdrażanie bezpiecznych produktów IT na rynku europejskim
 - [Ramy prawne dla certyfikacji cyberbezpieczeństwa - projekt ustawy Ministerstwa Cyfryzacji - Ministerstwo Cyfryzacji - Portal Gov.pl](#)
 - [European Union Security Certification](#)

JAK UFAĆ? CO ZAPEWNIAM NAM BEZPIECZEŃSTWO?

- Odpowiednio zaprojektowane systemy IT
- Przeszkolony personel
- Bieżąca obsługa systemów
 - Dobre praktyki
 - Aktywne skanowanie podatności
- Certyfikaty bezpieczeństwa
 - CC – Common Criteria
 - EU CC – European Union Cybersecurity Certification
- Referencje Huawei
 - Poznańskie Centrum Superkomputerowo-Sieciowe
 - Ministerstwo Finansów RP
 - NASK – Naukowa i Akademicka Sieć Komputerowa
 - Poczta Polska
 - Volkswagen Poznań
 - Zakład Ubezpieczeń Społecznych
 - Media Expert
 - Urząd Miasta Warszawa
 - Uniwersytet Jagielloński w Krakowie



AC 223



HUAWEI – PRZYKŁADY CERTYFIKACJI

- Wiele produktów z certyfikatami Common Criteria (CC), w tym na różnych poziomach oceny (EAL)
 - Huawei OceanStor Dorado All-Flash Storage – uzyskał certyfikat CC, potwierdzający bezpieczeństwo i niezawodność systemów pamięci masowej.
 - HongMeng Kernel (system operacyjny) – otrzymał najwyższy poziom certyfikacji CC EAL6+, co jest unikalnym osiągnięciem dla jądra systemu operacyjnego w urządzeniach smart.
 - Rozwiązania firewall Huawei (Unified Security Gateway i seria Eudemon) – certyfikowane na poziomie CC EAL4+, co potwierdza ich bezpieczeństwo i niezawodność w zastosowaniach sieciowych.
 - Huawei iTrustee (TEE OS) – uzyskał certyfikat CC EAL4+, będąc pierwszym systemem TEE w branży z takim poziomem certyfikacji.
 - Huawei BSBC 2.0 – produkt oceniony na poziomie EAL5+ z rozszerzeniami, potwierdzający wysoki poziom zabezpieczeń.
- Łącznie Huawei posiada ponad 40 certyfikatów CC oraz liczne certyfikaty [FIPS](#), [PCI](#) i [ISO](#), które potwierdzają zgodność z międzynarodowymi standardami bezpieczeństwa.
- W Chinach działa ponad **50 milionów** prywatnych przedsiębiorstw, w tym około **400 000** przedsiębiorstw wysokich technologii
 - [Obserwator Finansowy: ekonomia, debata, Polska, świat](#)
 - [W Chinach działa ponad 50 milionów prywatnych przedsiębiorstw - Silk Road Poland](#)

- Wartość rynku:
 - Globalna sprzedaż półprzewodników w styczniu 2025 roku osiągnęła 565 miliardów dolarów, co oznacza wzrost o 17,9% w porównaniu do stycznia 2024 roku.
 - W lutym 2025 r. sprzedaż wyniosła 54,9 miliarda dolarów tylko w tym miesiącu, co jest rekordowym wynikiem w historii dla lutego.
 - Przewiduje się, że rynek półprzewodników w 2025 roku wzrośnie o około 15%, głównie dzięki popytowi na układy do sztucznej inteligencji i wysokowydajnych obliczeń (HPC).
- Najwięksi producenci:
 - Tajwan: TSMC odpowiada za około 50% światowego rynku półprzewodników w segmencie foundry (produkcja kontraktowa). Inne ważne firmy to UMC, PSMC i VIS.
 - Korea Południowa: Samsung Electronics jest liderem w produkcji pamięci DRAM i NAND, z udziałem w rynku na poziomie 10,6% i przychodami 66,5 miliarda USD w 2024 roku.
 - USA: Intel oraz firmy projektujące chipy (np. Nvidia, AMD, Qualcomm) są liderami w innowacjach i projektowaniu, choć większość produkcji wciąż odbywa się w Azji.
 - Chiny: SMIC i inne firmy dynamicznie rozwijają produkcję, ale nadal pozostają w tyle za liderami w zakresie najnowocześniejszych technologii. Chiny odpowiadają obecnie za około 9% światowej produkcji, ale szacuje się, że w 2030 roku będą produkować blisko 25% półprzewodników na świecie.
 - Europa: Infineon Technologies jest liderem w produkcji półprzewodników dla motoryzacji, z globalnym udziałem 13,5% w tym segmencie.

PRODUKCJA CHIPÓW NA ŚWIECIE

- Wartość rynku:
 - Globalna sprzedaż półprzewodników wzrosła o 17,9% w porównaniu do stycznia 2024 r.
 - W lutym 2025 r. sprzedaż wyrównała rekord lutego.
 - Przewiduje się, że rynek półprzewodników będzie napędzany sztuczną inteligencją i wysoką wydajnością.
- Najwięksi producenci:
 - Tajwan: TSMC odpowiada za 60% produkcji. Inne ważne firmy to UMC, PSMC.
 - Korea Południowa: Samsung Electronics (10,6% i przychodami 66,5 mld USD).
 - USA: Intel oraz firmy projektujące, większość produkcji wciąż od Korea Południowej.
 - Chiny: SMIC i inne firmy dynamicznie rozwijające najnowocześniejsze technologie. W 2024 roku będą produkować blisko 10% globalnej produkcji.
 - Europa: Infineon Technologies, STMicroelectronics w tym segmencie.



w, co oznacza wzrost o 17,9% w
ordowym wynikiem w historii dla
ęki popytowi na układy do
foundry (produkcja kontraktowa).
udziałem w rynku na poziomie
acjach i projektowaniu, choć
erami w zakresie
dukcji, ale szacuje się, że w 2030
z globalnym udziałem 13,5% w

PATENTY

- Global patent filings reached approximately 3.6 million in 2023, with a growth of 2.7% compared to the previous year.
- Semiconductor patents specifically saw a 59% increase over five years, reaching a record 69,190 global filings in the most recent year.

Country/Company	Patent Focus/Area	Notable Data/Statistic
China	Semiconductors, AI	46,591 semiconductor patents (2023/24); 70% of global AI patent applications
Taiwan	Semiconductors	22% of global semiconductor patent filings
South Korea	Semiconductors, AI	12,000+ semiconductor patents (2023)
Japan	Semiconductors, AI	10% annual growth in semiconductor patents
USA	5G, Semiconductors, AI	Qualcomm: 140,000+ patents; high-impact AI patents
Huawei	5G, Wireless, AI	Top global 5G patent holder, tens of thousands of patents

[World Intellectual Property Organization](https://www.wipo.int/en/ipfactsandfigures/patents) (WIPO) is the United Nations agency->
<https://www.wipo.int/en/ipfactsandfigures/patents>

MODEL ROZWOJU – Z WYJĄTKAMI PODOBNE

Aspekt	USA	Chiny
R&D	Bardzo wysokie wydatki na badania i rozwój (ok. 750 mld USD rocznie), silne inwestycje w nowe technologie, AI, chmurę, biotechnologię.	Szybko rosnące inwestycje w R&D (ok. 700 mld USD rocznie), nacisk na samowystarczalność technologiczną, rozwój własnych standardów (np. RISC-V).
Akwizycje	Duża liczba przejęć, zwłaszcza startupów i firm technologicznych, szybki dostęp do nowych technologii i talentów. Częste blokowanie chińskich akwizycji w USA.	Próby przejmowania firm zagranicznych, często blokowane przez rządy innych krajów. Inwestycje w startupy w USA, Kanadzie, Izraelu; silna presja na rozwój własnych technologii.
Strategia	Model hybrydowy: własny R&D + akwizycje. Dominacja w innowacjach, wysokiej jakości patentach i globalnych rynkach.	Model hybrydowy, ale z silnym naciskiem państwa na samodzielność technologiczną. Wysoka liczba patentów, niższa jakość, nacisk na szybki wzrost i skalę.
Wsparcie rządowe	Wsparcie poprzez granty i regulacje, mniej bezpośrednie niż w Chinach.	Bardzo silne wsparcie rządowe, subsydia, plany strategiczne (np. „Made in China 2025”).
Przykłady firm	Google, Apple, Microsoft, Nvidia, Qualcomm.	Huawei, Tencent, Alibaba, Baidu.
Wyzwania	Utrzymanie przewagi technologicznej, konkurencja z Chinami, blokowanie transferu technologii do Chin.	Ograniczony dostęp do najnowszych technologii z USA, konieczność rozwijania własnych rozwiązań, presja na innowacje i skalę

Jak działa NDAA w kwestii sankcji?

- Podstawa prawna:
 - NDAA to ustawa budżetowa dotycząca obronności, ale zawiera także zapisy dotyczące ochrony infrastruktury krytycznej, w tym telekomunikacyjnej.
 - Art. 889 NDAA 2019 zakazuje agencjom federalnym USA korzystania z urządzeń lub usług firm takich jak Huawei i ZTE, a także ich podwykonawców.
- Mechanizm:
 - Kongres USA może wprowadzić ograniczenia lub zakazy dotyczące konkretnych firm, jeśli uzna, że ich działalność stanowi zagrożenie dla bezpieczeństwa narodowego.
 - Takie decyzje mogą być podejmowane bez przedstawiania szczegółowych dowodów publicznie, co spotkało się z krytyką i pozwami ze strony firm objętych sankcjami.
- Skutki:
 - Agencje rządowe muszą usunąć sprzęt objęty zakazem ze swoich sieci.
 - Amerykańskie firmy nie mogą korzystać z rządowych funduszy na zakup sprzętu od firm uznanych za zagrożenie.
 - Departament Handlu USA może unieważniać licencje na eksport technologii do tych firm, co dodatkowo ogranicza ich dostęp do amerykańskich komponentów i technologii.
- Rozszerzenie:
 - Administracja prezydencka może rozszerzać sankcje na podstawie innych przepisów, np. ustawy o nadzwyczajnych uprawnieniach gospodarczych (IEEPA) lub rozporządzeń wykonawczych.

ASCEND – SERIA ZAAWANSOWANYCH CHIPÓW DLA AI OD HUAWEI

- Konkurencja dla NVIDIA H100
 - Przyspieszenie postępu technologicznego w Chinach
 - Zakaz zakupu ASCEND od Bureau of Industry & Security (BIS)
-
- <https://chiny24.com/news/amerykanskie-restrykcje-wobec-huawei-dlaczego-trudno-budowac-zaufanie-pomiedzy-usa-a-chinami>
 - <https://www.bis.gov/press-release/departement-commerce-rescinds-biden-era-artificial-intelligence-diffusion-rule-strengthens-chip-related>

System	Performance (TFLOPS)	Memory Bandwidth	Process Node	Status/Notes
Ascend 910C	800 (FP16)	3.2 TB/s	7nm (DUV)	Mass production, low yield
Ascend 910D	Not disclosed	Not disclosed	Not disclosed	Testing, late May 2025
Ascend 920	900+ (BF16)	4 TB/s	6nm (!)	Mass production H2 2025
CloudMatrix 384	300 petaflops (BF16)	Aggregate high	—	Integrated system

CENTRUM R&D HUAWEI

- Zakończono budowę flagowego projektu firmy HuaWei. To zlokalizowane w Szanghaju, w dzielnicy QingPu HuaWei LianQiu R&D Center .
- Na terenie tego ośrodka badawczo-rozwojowego może zostać zlokalizowanych ponad 40 tysięcy biur i laboratoriów dla 35 tysięcy techników i inżynierów.
- Powierzchnia 10,522 mln m² i jest większe od Apple Park i Microsoft Redmond Campus razem wziętych (odpowiednio zajmują 708 200 m² i 2,032 mln m²)
- STEM (nauki ścisłe, technologia, inżynieria, matematyka)
 - Chiny ponad 4,7 miliona absolwentów rocznie
 - USA 800 000 absolwentów rocznie
 - Na poziomie doktoratu 77 000 vs 40 000
- R&D w Huawei
 - 20,8% przychodów w 2024 czyli 25 mld USD
 - 50% pracowników
 - 240 000 patentów (łącznie) – Apple 116 000 (łącznie)

<https://chiny24.com/wiadomosci/nowe-centrum-rd-huawei-w-szanghaju>



CHINY VS. USA

Indicator	United States	China
GDP (Nominal, 2025)	\$30.51 trillion	\$19.23 trillion
GDP (PPP, 2025)	\$28.78 trillion	\$35.29 trillion (estimates vary, up to \$43.2T)
Per Capita GDP (2024)	~\$86,600 ₂	~\$13,445
GDP Growth Rate (2025)	~2.15%	~4.48%
Key Economic Drivers	Consumer spending, technology, services	Manufacturing, exports, infrastructure, tech
Consumption	Consumer-driven (PCE ~70% of GDP)	Transitioning to more consumption-led, but lower
Unemployment (2024)	~4%	~5% (urban, youth higher)
Inflation (2024)	2.3%	0.2%
International Trade	Leading in services, financials	Leading in goods, Belt&Road Initiative investments
Challenges	Income inequality, commercial real estate risks	Real estate instability, weak domestic demand

<https://www.cia.gov/the-world-factbook/countries/china/>

<https://www.cia.gov/the-world-factbook/countries/united-states/>

Dziękuję za uwagę

Piotr Flis

tel.: 0-605 586 588

mail: piotr.flis@upgreat.com.pl

UpGreat Systemy Komputerowe Sp. z o.o.

60-122 Poznań, ul. Ostrobramska 22

<http://www.upgreat.com.pl>