The Geopolitics of AI: Power, Security and the New Global Order

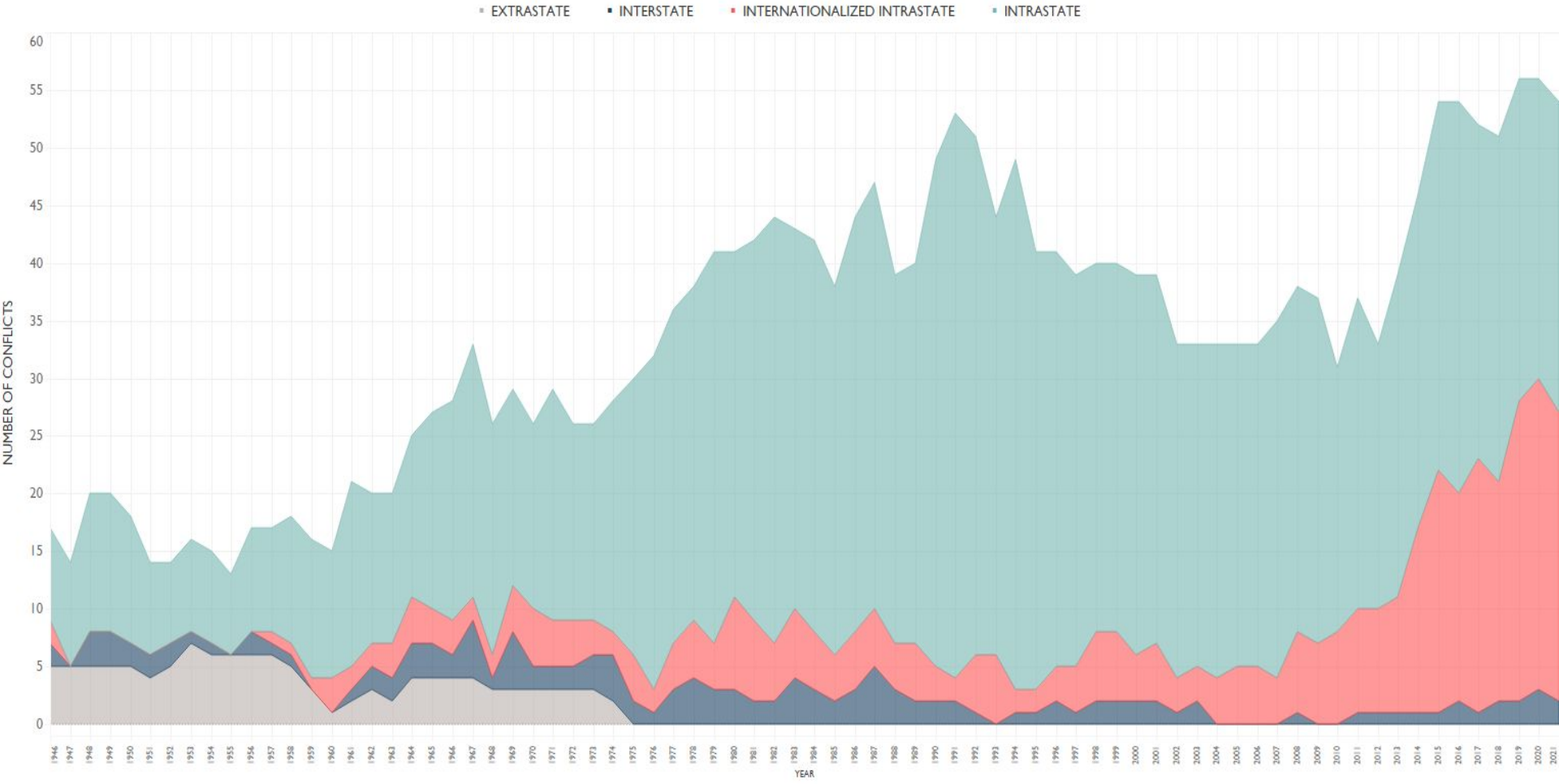
Dr. Jean-Marc Rickli

Head of Global and Emerging Risks

9 December 2025

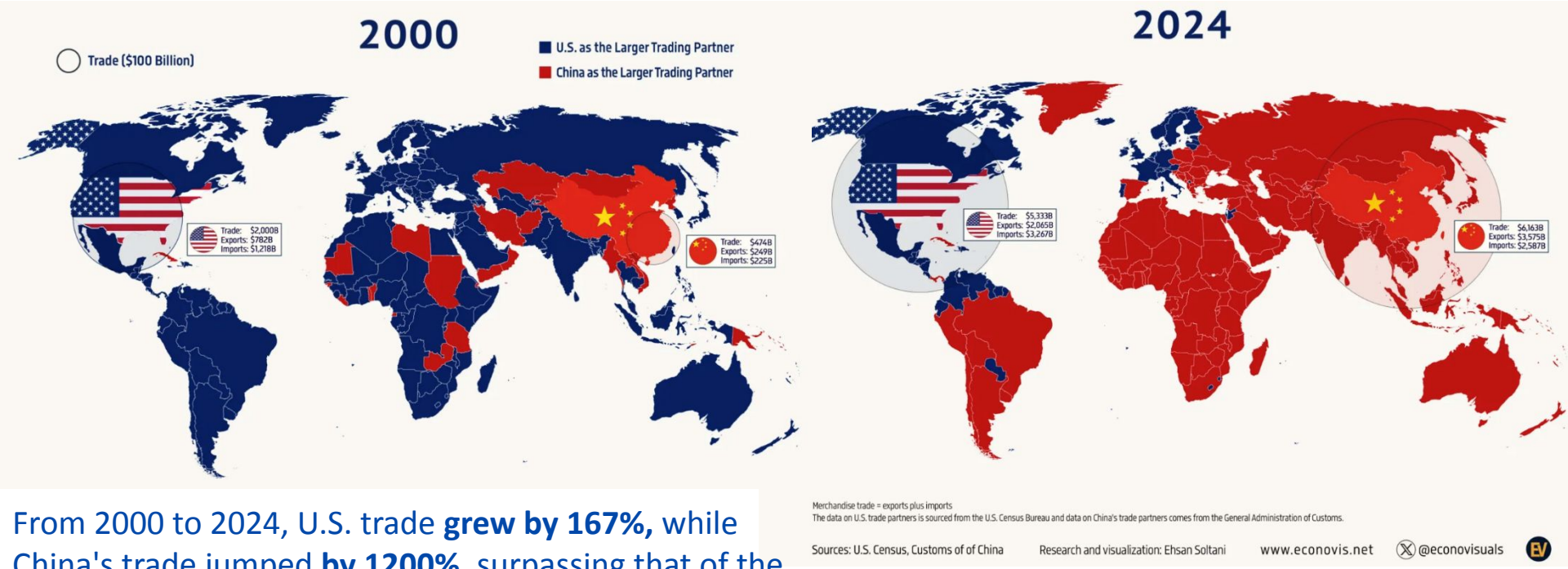
GCSP
Geneva Centre for Security Policy

ARMED CONFLICT BY TYPE, 1946-2021



Based on UCDP 22.1 data

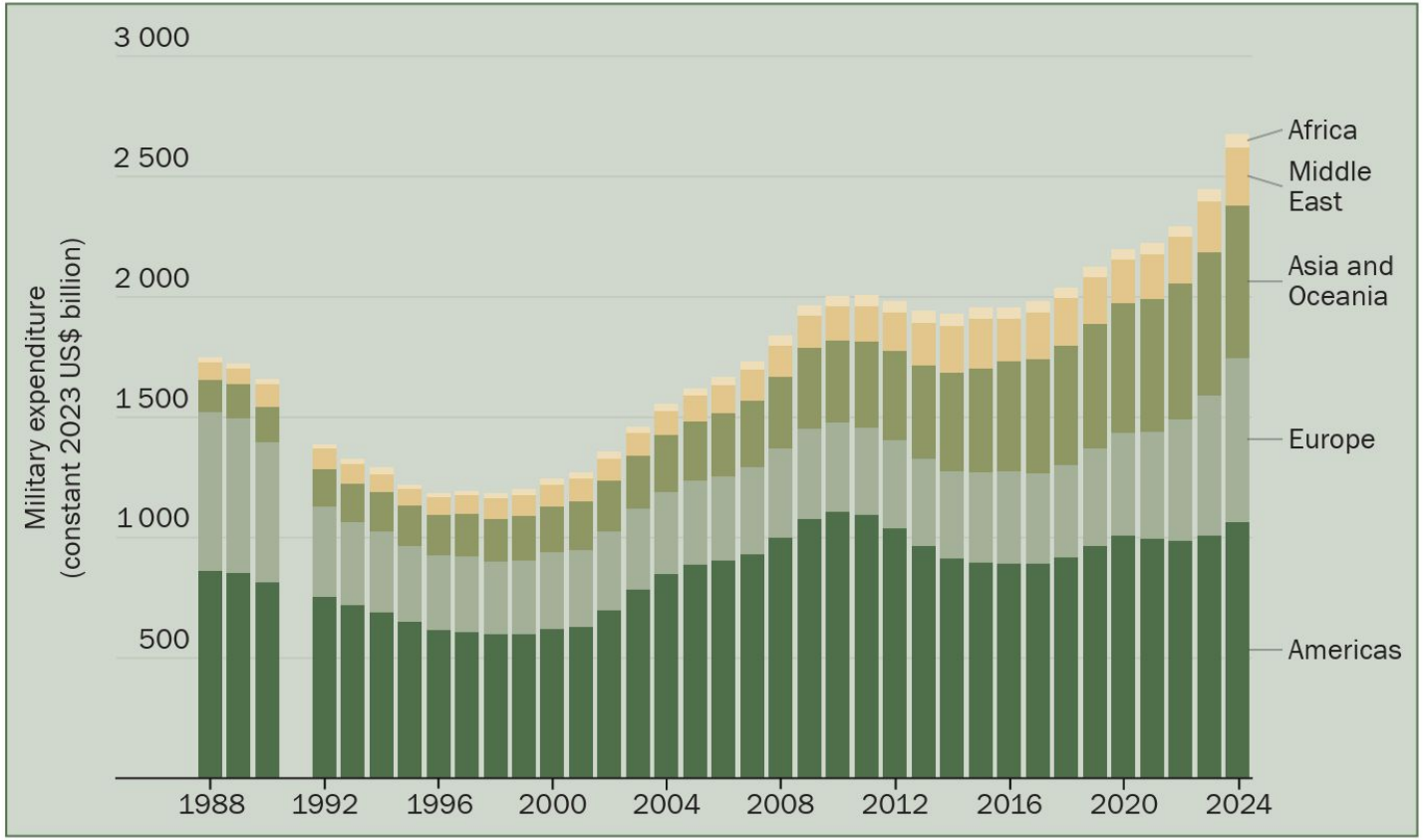
US-China Competition



From 2000 to 2024, U.S. trade **grew by 167%,** while China's trade jumped **by 1200%,** surpassing that of the United States in 2012. In 2024, total trade reached USD 5.3 trillion for the United States and USD 6.2 trillion for China.

World Military Spending 1988-2024

GCSP
Geneva Centre for Security Policy

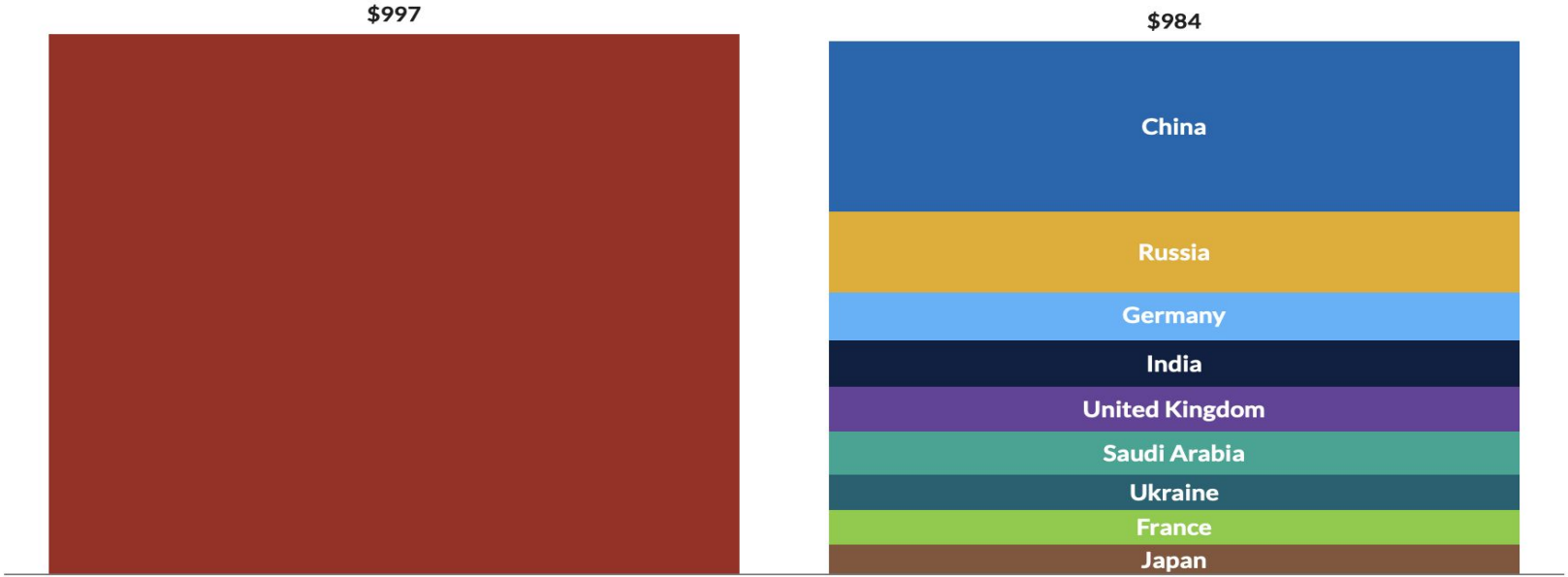


World's Leading Military Spenders (2024)

GCSP Geneva Centre for Security Policy

The United States spends more on defense than the next 9 countries combined

Defense Spending (Billions of $)

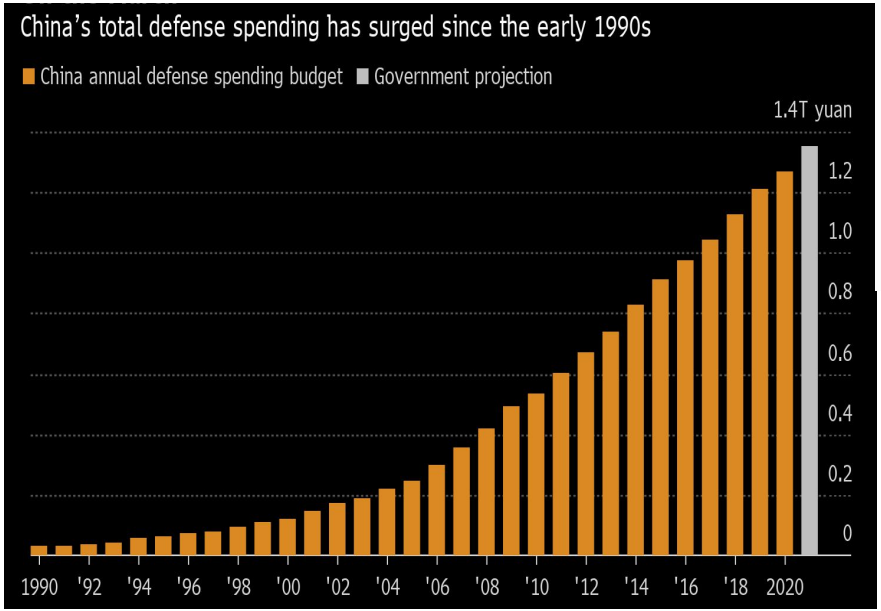


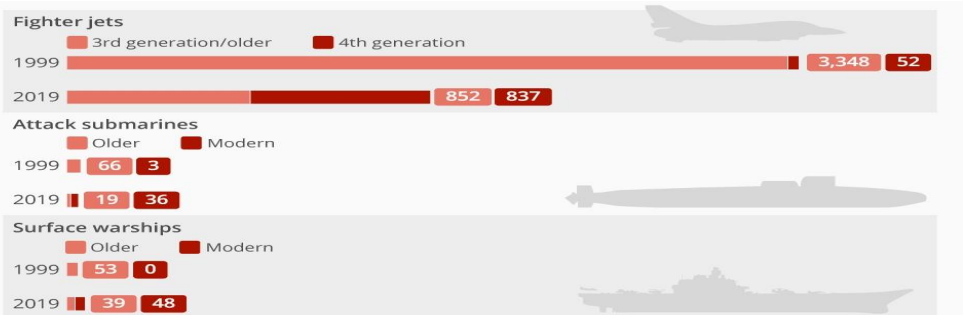
Source: Stockholm International Peace Research Institute • Embed • Download image

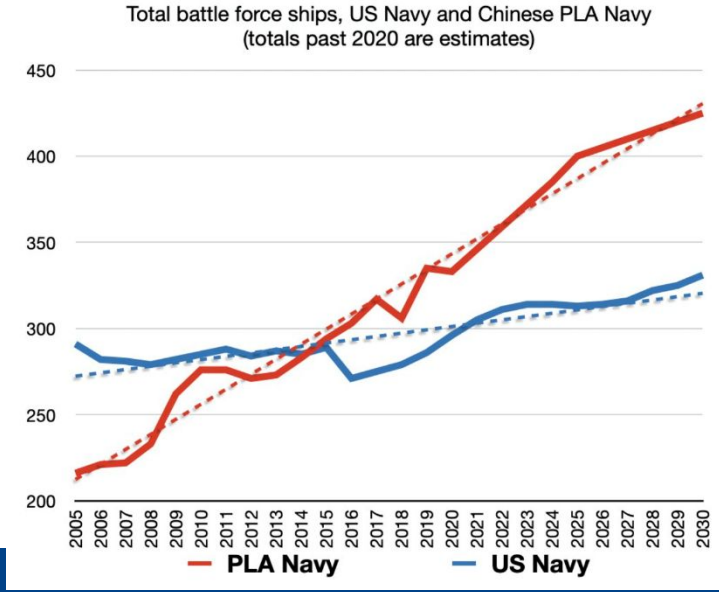
Notes: Figures are in U.S. dollars converted from local currencies using market exchange rates. Data for the United States are for fiscal year 2024. Data for the other countries are for calendar year 2024. The source for this chart uses a definition of defense spending that is more broad than budget function 050 and defense discretionary spending.

PETER G. PETERSON FOUNDATION

Growth of China's Military Power







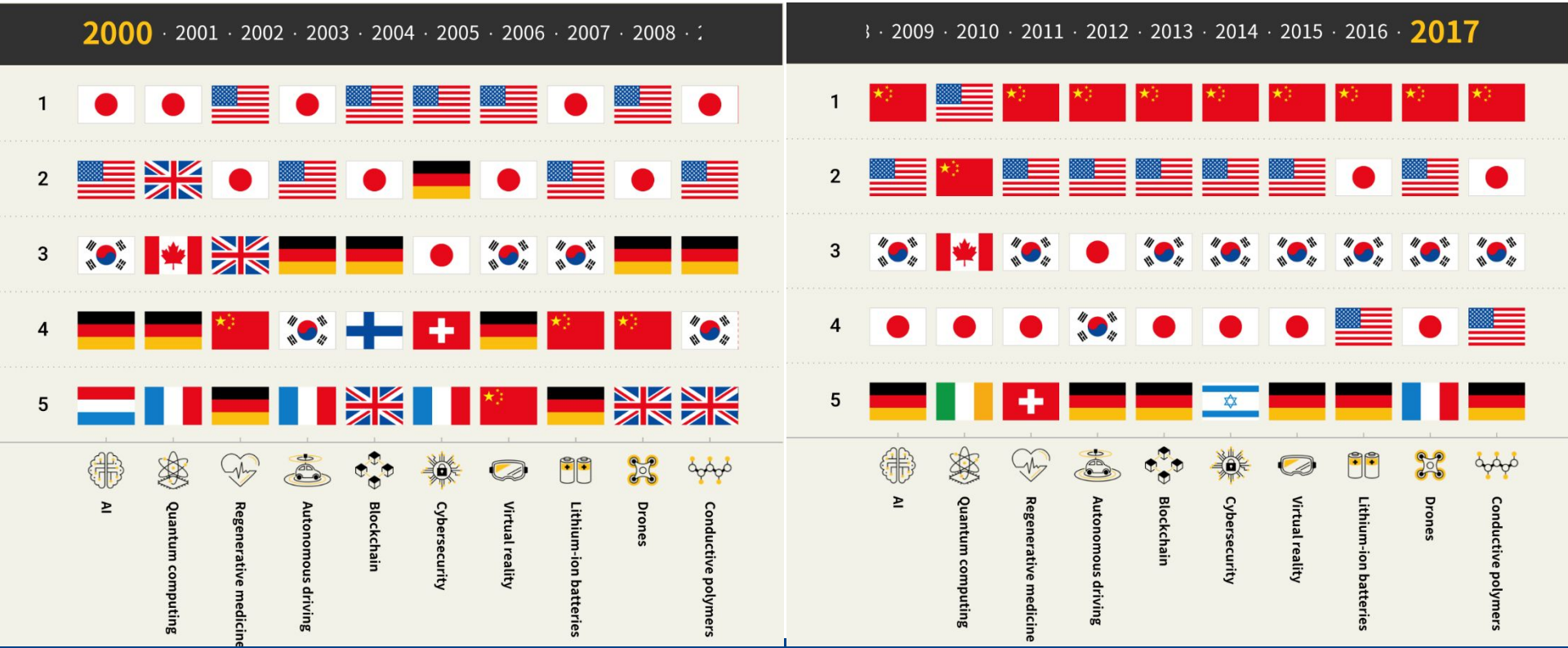
From 1999 to 2021, EU combined defence spending increased by 19.7% against 65.7% for the US, 292% for Russia and 592% for China

Joint Statement between China and Russia, 4 Feb 2022

- Joint Statement Regarding "The **New Era of International Relations** and Global Sustainable Development"
- Questioning and denunciation of Western discourses on international standards. Democracy is a notion that is defended, but which must be taken into account under the spectrum of the history and culture of States. According to the two powers, **only the people of a country can declare whether it is democratic or not.** Similarly, human rights must be understood according to the **history, culture and particular situation** of each State.
- **Western states, led by the United States**, are seen **as threats to international peace and stability**, through the expansion of **NATO**, the security partnership between the United States, Britain and Australia, weapons research or even deployment in the Indo-Pacific region.
- Respect for the status of a single China is reaffirmed
- With this declaration, Russia and China put themselves at **the center of the international system**, referred to as **new guarantors of law and international relation**s, while taking the lead in peacekeeping and crisis management, such as that of Covid.

Geopolitics of Emerging Technologies

GCSP
Geneva Centre for Security Policy



Geopolitics of Emerging Technologies

GCSP Geneva Centre for Security Policy

Lead country and technology monopoly risk (August 29, 2024)

Technology	Lead Country	Technology Monopoly Risk
Advanced information and communication technologies		
Advanced optical communication	China	high
Advanced undersea wireless communication	China	high
Distributed ledgers	China	medium
Advanced radiofrequency communication	China	medium
Protective cyber security technologies	China	low
High performance computing	China	low
Mesh and infrastructure independent networks	China	low
Advanced materials and manufacturing		
Advanced composite materials	China	high
Advanced protection	China	high
Coatings	China	high
High-specification machining processes	China	high
Novel metamaterials	China	high
Nanoscale materials and manufacturing	China	high
Smart materials	China	high
Continuous flow chemical synthesis	China	medium
Advanced explosives and energetic materials	China	medium
Advanced magnets and superconductors	China	medium
Critical minerals extraction and processing	China	medium
Wide and ultrawide bandgap semiconductors	China	medium
Additive manufacturing	China	low
AI technologies		
Advanced data analytics	China	medium
AI algorithms and hardware accelerators	China	medium
Machine learning	China	medium
Adversarial AI	China	low
Natural language processing	USA	low
Advanced integrated circuit design and fabrication	China	low
Biotechnology, gene technologies and vaccines		
Synthetic biology	China	high
Novel antibiotics and antivirals	China	medium
Biological manufacturing	China	medium
Genomic sequencing and analysis	China	low
Genetic engineering	USA	low
Nuclear medicine and radiotherapy	USA	low
Vaccines and medical countermeasures	USA	low
Defence, space, robotics and transportation		
Advanced aircraft engines	China	high
Hypersonic detection and tracking	China	high
Drones, swarming and collaborative robots	China	high
Advanced robotics	China	low
Autonomous systems operation technologies	China	low
Space launch systems	China	low
Small satellites	USA	low
Energy and environment		
Electric batteries	China	high
Hydrogen and ammonia for power	China	high
Supercapacitors	China	high
Directed energy technologies	China	medium
Nuclear waste management and recycling	China	medium
Photovoltaics	China	medium
Biofuels	China	low
Nuclear energy	China	low
Quantum		
Quantum computing	USA	medium
Post-quantum cryptography	China	medium
Quantum communication	China	low
Quantum sensors	China	low
Sensing, timing and navigation		
Inertial navigation systems	China	high
Multispectral and hyperspectral imaging sensors	China	high
Photonic sensors	China	high
Radar	China	high
Satellite positioning and navigation	China	high
Sonar and acoustic sensors	China	high
Magnetic field sensors	China	medium
Atomic clocks	USA	low
Gravitational-force sensors	China	low
Unique AUKUS technologies		
Autonomous underwater vehicles	China	high
Electronic warfare	China	high
Air-independent propulsion	China	medium

Source: ASPI's Critical Technology Tracker (2024)

Timeline of images generated by artificial intelligence

These people don't exist. All images were generated by artificial intelligence.

Our World in Data

2014

Goodfellow et al. (2014) – Generative Adversarial Networks

2015

Radford, Metz, and Chintala (2015) – Unsupervised Representation Learning with Deep Convolutional GANs

2016

Liu and Tuzel (2016) – Coupled GANs

2017

Karras et al. (2017) – Progressive Growing of GANs for Improved Quality, Stability, and Variation

2018

Karras, Laine, and Aila (2018) – A Style-Based Generator Architecture for Generative Adversarial Networks

2019

Karras et al. (2019) – Analyzing and Improving the Image Quality of StyleGAN

2020

Ho, Jain, & Abbeel (2020) – Denoising Diffusion Probabilistic Models

2021

Image generated with the prompt: *"a couple of people are sitting on a wood bench"*

Ramesh et al. (2021) – Zero-Shot Text-to-Image Generation (OpenAI's DALL-E 1)

2022

Image generated with the prompt: *"A Pomeranian is sitting on the King's throne wearing a crown. Two tiger soldiers are standing next to the throne."*

Saharia et al. (2022) – Photorealistic Text-to-Image Diffusion Models with Deep Language Understanding (Google's Imagen)

Generative AI

GCSP Centre for y Policy

WILL KNIGHT BUSINESS AUG 29, 2023 8:00 AM

It Costs Just $400 to Build an AI Disinformation Machine

A developer used widely available AI tools to generate anti-Russian tweets and articles. The project is intended to highlight how cheap and easy it has become to create propaganda at scale.

Once a Sheriff's Deputy in Florida, Now a Source of Disinformation From Russia

In 2016, Russia used an army of trolls to interfere in the U.S. presidential election. This year, an American given asylum in Moscow may be accomplishing much the same thing all by himself.

167
Domains mimicking local news outlets linked to Dougan

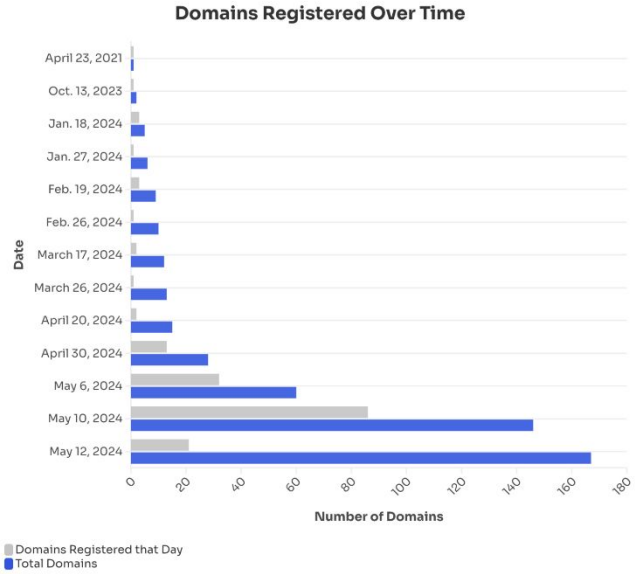
19
Disinformation narratives apparently originating from Dougan's network from September 2023 to May 2024

7,934
Times Dougan's websites have been cited or referenced in social media posts or news articles.

122,785
Articles and social media posts advancing false narratives that originated on Dougan's network

37.7 million
Views on social media posts and articles advancing Dougan's false narratives

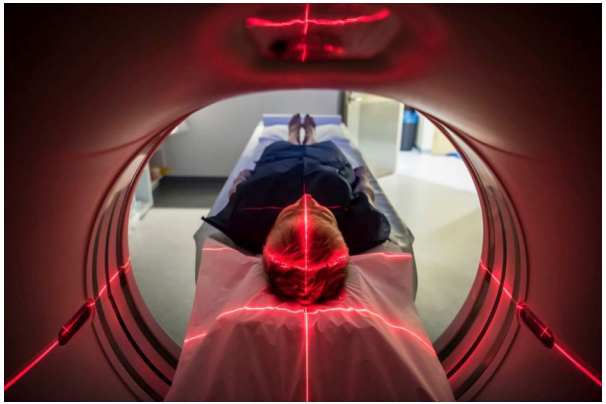
16
The number of languages the network's false narratives have been advanced in



Digital Manipulations

GCSP Geneva Centre for Security Policy

Hospital viruses: Fake cancerous nodes in CT scans, created by malware, trick radiologists

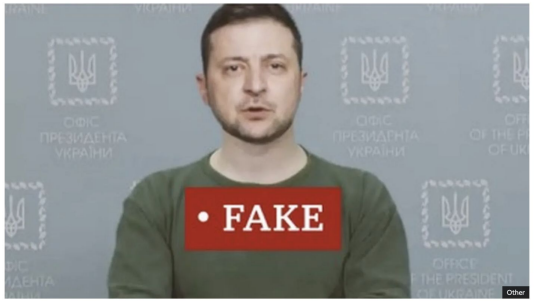


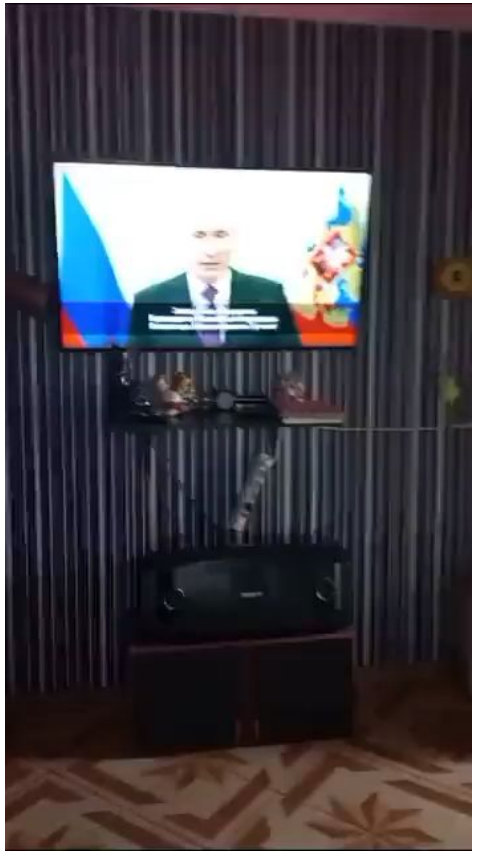
Deepfake presidents used in Russia-Ukraine war

18 March 2022

By Jane Wakefield, BBC Technology

Share

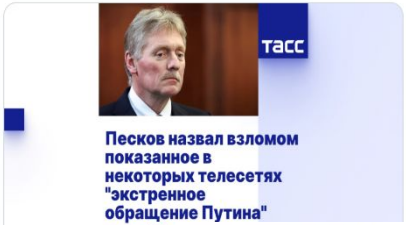




Alex Kokcharov @AlexKokcharov · 5h

Putin's spokesman Peskov said that the broadcast was allegedly caused by a hack of radio and TV networks.

2/2



tass.ru

Песков: показанное

События в России и

Материалы пресс-ко

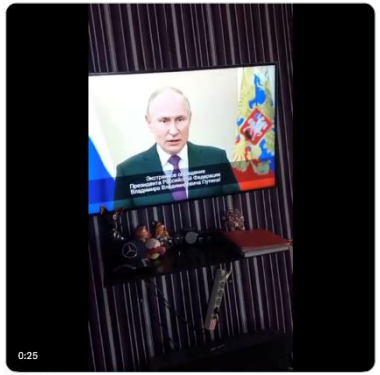
15 60

Alex Kokcharov @AlexKokcharov · 2h

In #Russia, several radio stations and even local TV networks appear to have been hacked to broadcast a **deep fake** address allegedly by president **Putin**.

This fake address announced mass mobilisation and introduced martial law in border regions.

1/2



From **Грани.Ру**

42 494 1,639 287.2K

GenAI Uses and Terrorist Organisations

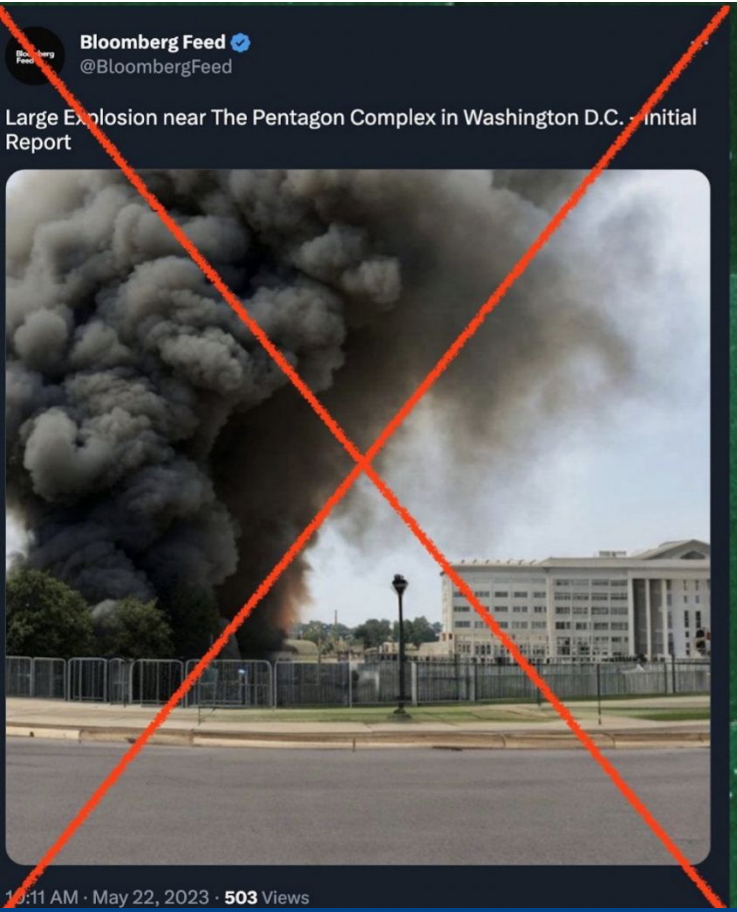
- Accessible user-friendly AI tools **lower the barrier for terrorists** to adopt emerging technologies for operational and organizational purposes (Hinton, 2024).
- Generative AI propaganda is **scalable and sophisticated** -> distribution to global audiences.
- Terrorists are using GenAI to **create virtual recruiters** that support and prepares lone wolfs.
- Terrorists are using **AI-powered chatbots to radicalize and recruit** individuals to carry out attacks.

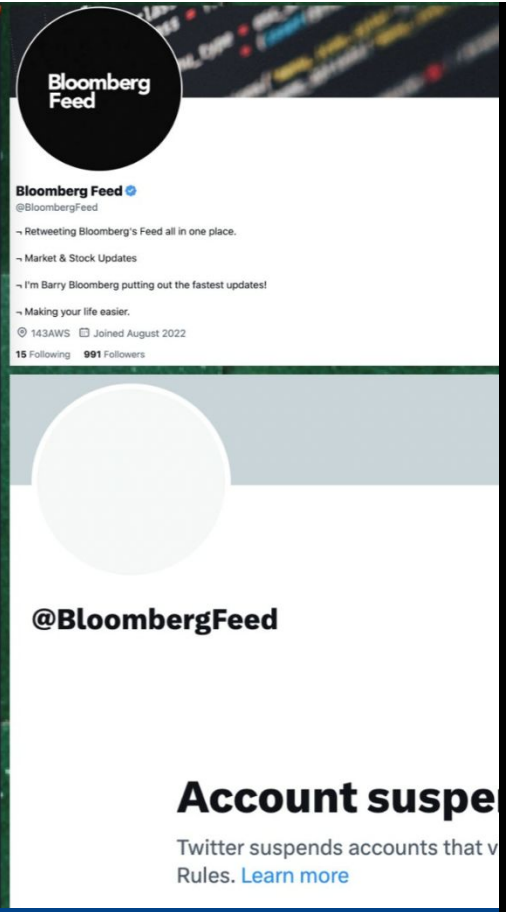
AI-GENERATED IMAGE: A screenshot from a news broadcast created by Islamic State supporters that features an AI-generated news anchor, which has been labeled by The Washington Post. (SITE Intelligence Group)

Figure 2: The image contains text in Pashto and English, specifically showing "کې داعش ډاې په وسله وال" in Pashto, which translates to "ISIS group in armed" and the English text "Khurasan TV" repeated twice, indicating a news outlet associated with ISKP.

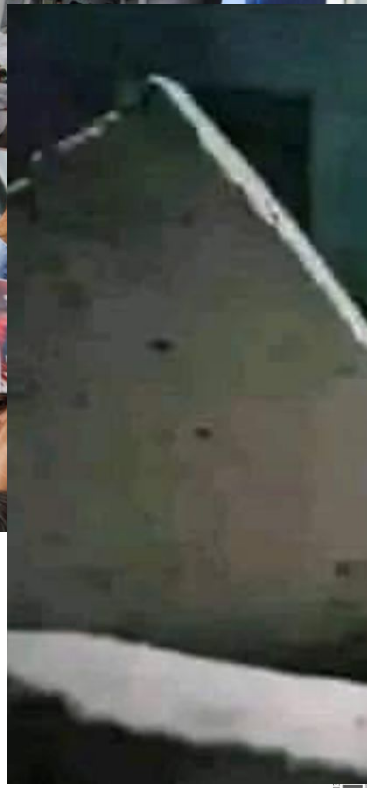
An AI-created news bulletin from Pro-ISKP Khurasan TV was disseminated on Twitter via a fake account impersonating Taliban Foreign Minister Amir Khan Muttaqi.

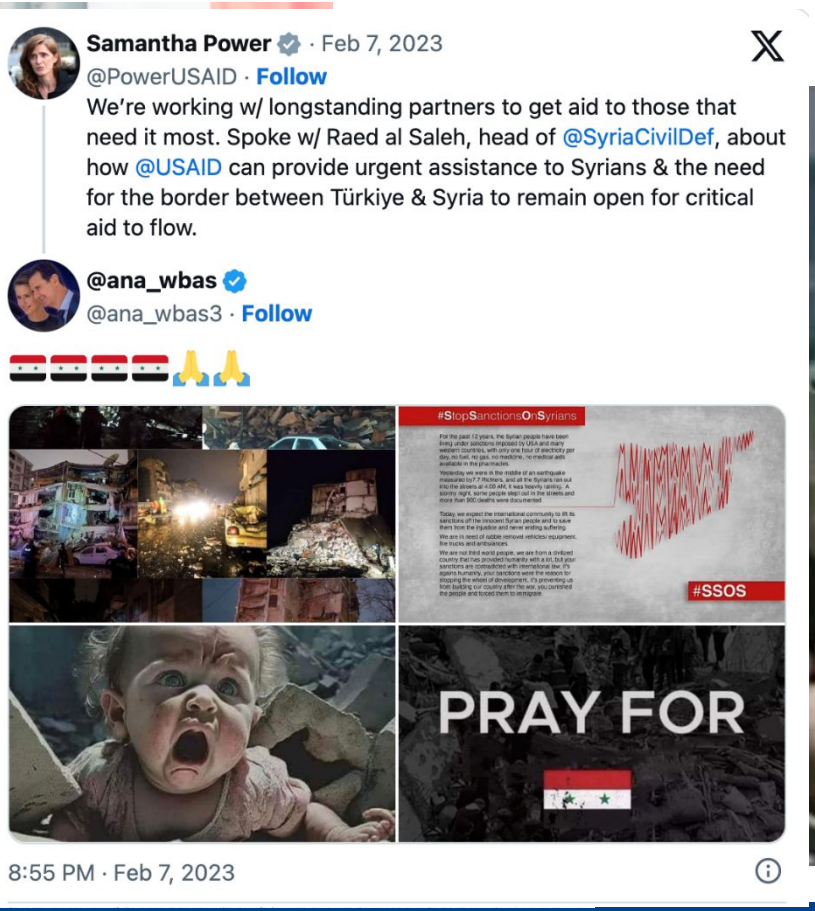
Generative AI

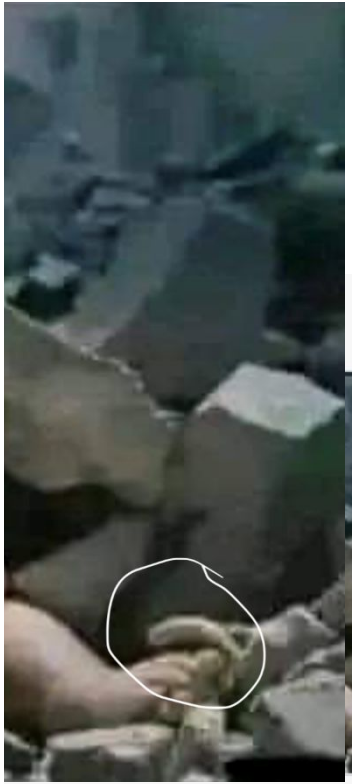


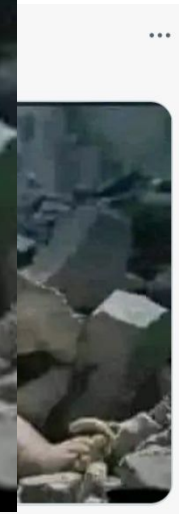


Generative AI

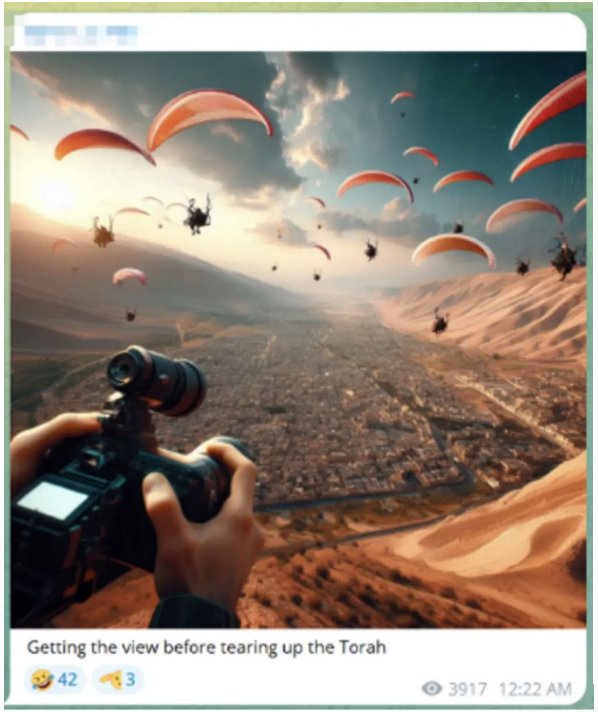








Generative AI-Meme Warfare

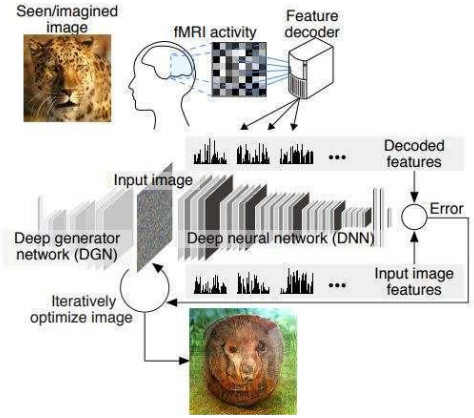


Another GAI image on 4chan and Telegram shows paragliders over a burning building. At a distance, the meme reveals an image of Adolf Hitler.

Sources: https://www.adl.org/resources/article/generative-artificial-intelligence-gai-and-israel-hamas-war

Neurotechnologies

GCSP
Geneva Centre for Security Policy



Scientists Use GPT AI to Passively Read People's Thoughts in Breakthrough

An AI model similar to ChatGPT was combined with fMRI readings to non-invasively decode continuous language from subjects, a new study reports.

By Becky Ferreira

May 1, 2023, 5:06pm Share Tweet Snap

https://doi.org/10.1038/s41598-024-66228-1

BCI Research

GCSP
Geneva Centre for Security Policy

Brain-computer interfaces are developing faster than the polic

It's time to talk about what'

By Casey Newton | @Casey

AI research Oct 18, 2023

Meta's new AI system can generate images from brain data in milliseconds

ak': China is mining data brains on an industrial scale

ts are deploying brain-reading technology to detect iction line, the military and at the

Why you can trust SCMP

Facebook Computer

By Kurt Wagner

September 24, 2019, 1:30 A

Artificial Intelligenc

Microsoft i to create b

NEUROSCIENCE | OPINION

Wearable Brain Devices Will Challenge Our Mental Privacy

A new era of neurotechnology means we may need new protections to safeguard our brain and mental experiences

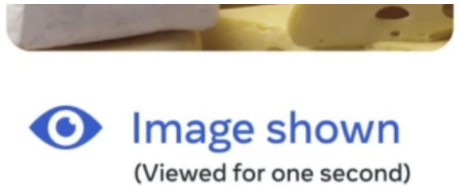
By Nita A. Farahany on March 27, 2023

y is trying

EMILY MULLIN SCIENCE AI

China Has a for Brain–Co

China's brain–computer interface technology is catching up to the US. But it envisions a very different use case: cognitive enhancement.



ogram is developing brain- ould control "swarms of drones, hought." What if it succeeds?

Oct 16, 2019

GCSP Geneva Centre for Security Policy

Cognitive warfare is about controlling WHAT

Hung and Hung (2022)

AI and Organised Crime

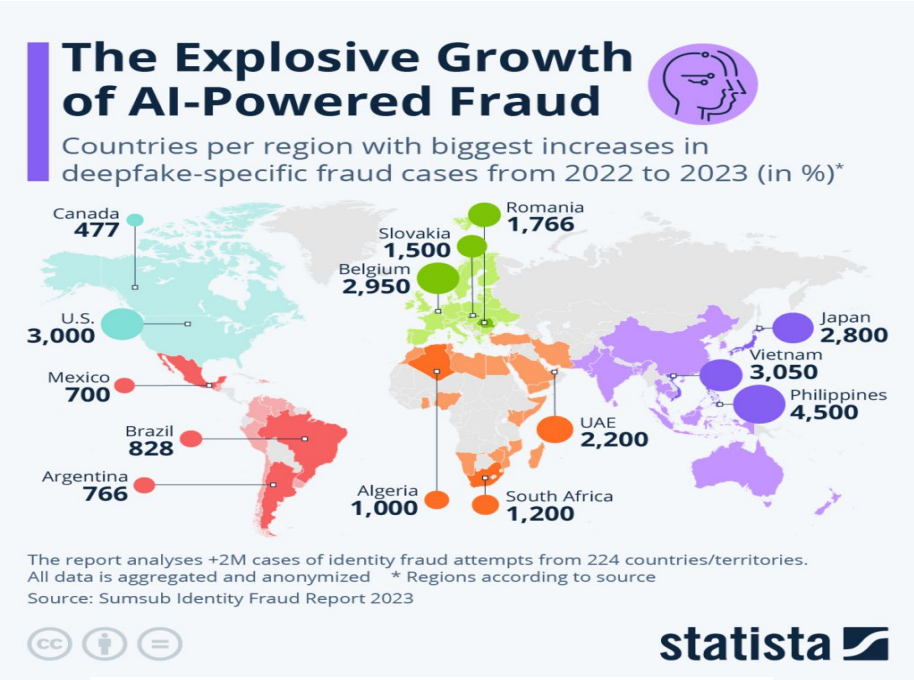
GCSP Geneva Centre for Security Policy

AI 'fundamentally' reshaping organized crime, Europol warns

'Same qualities that make AI revolutionary ... also make it a powerful tool for criminal networks,' EU's law enforcement agency says

Halis Sunnetci | 18.03.2025 - Update : 19.03.2025

- Barriers to crime are lowered due to AI, **creation** of convincing phishing scams, malware, and deepfakes **are easier** (Europol, 2025).
- AI boosts **criminal efficiency** with fewer resources.
- AI is accelerating and scaling criminal operations -> **harder to detect and more efficient**, with threats like deepfake technology, and mass phishing campaigns.
- AI models are used to **perform sophisticated cyberattacks** – not just advising on how to carry



Special Section on Artificial Intelligence

Crimes of Influence: Generative Artificial Intelligence-led Crime as a Service

Nicole Matejic[1] and Chris Wilson[2]

Estimated cost of cybercrime worldwide 2017-2028

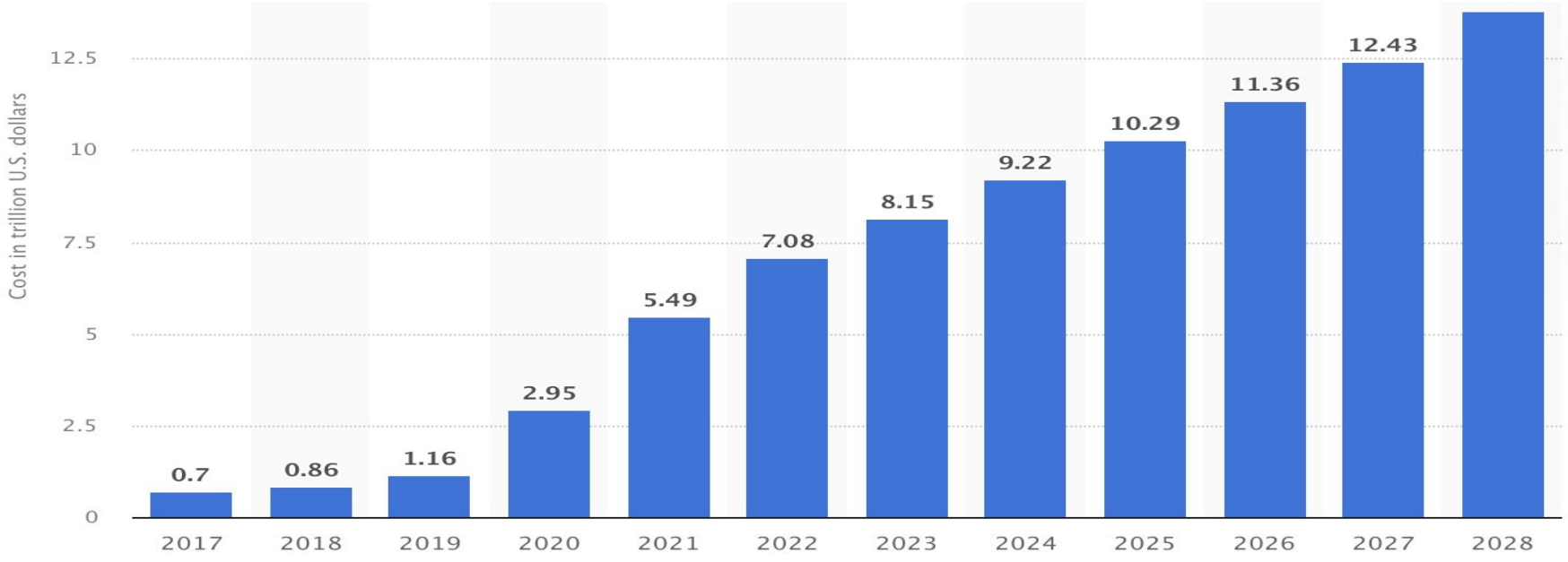
(in trillio

Total budgetary cost in the U.S. of the war on terror by category FY 2001-2020

Published by Veera Korhonen, Aug 9, 2024

It is estimated that, since the terrorist attacks of September 11, 2001, the global war on terror will cost the United States government just over 5.4 trillion U.S. dollars. This figure includes estimates of all budgetary spending related to the war on terror between FY 2001 and FY 2020.

This figure of 5.4 trillion does not include the ongoing medical and disability expenditure for veterans beyond FY 2020, which is estimated to cost an additional one trillion U.S. dollars by FY 2059.



Generative AI and Biotechnology

GCSP Geneva Centre for Security Policy

Jun 16, 2023 - Technology

Another AI threat: The next pandemic

Ryan Heath, author of Axios Login

Can large language models democratize access to dual-use biotechnology?

Emily H. Soice[1,2], Rafael Rocha[3], Kimberlee Cordova[4], Michael Specter[1], and Kevin M. Esvelt[1,2,5,†]

[1]Media Laboratory, Massachusetts Institute of Technology, Cambridge, United States
[2]SecureBio, Cambridge, United States
[3]Sloan School of Management, Massachusetts Institute of Technology, Cambridge, United States
[4]Graduate School of Design, Harvard University, Cambridge, United States
[5]SecureDNA Foundation, Zug, Switzerland

[†]Correspondence: esvelt@mit.edu

In **one hour**, the chatbots suggested **four potential pandemic pathogens**, explained **how they can be generated from synthetic DNA** using reverse genetics, **supplied the names of DNA synthesis companies unlikely to screen orders**, identified detailed protocols and how to troubleshoot them, and recommended that anyone lacking the skills to perform reverse genetics engage a core facility or contract research organization. Collectively, these results suggest that LLMs will make pandemic-class agents widely accessible as soon as they are credibly identified, even to people with little or no laboratory training.

DNA Hacking

GCSP Geneva Centre for Security Policy

Received 3 March 2025, accepted 12 March 2025, date of publication 17 March 2025, date of current version 28 March 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3552069

RESEARCH ARTICLE

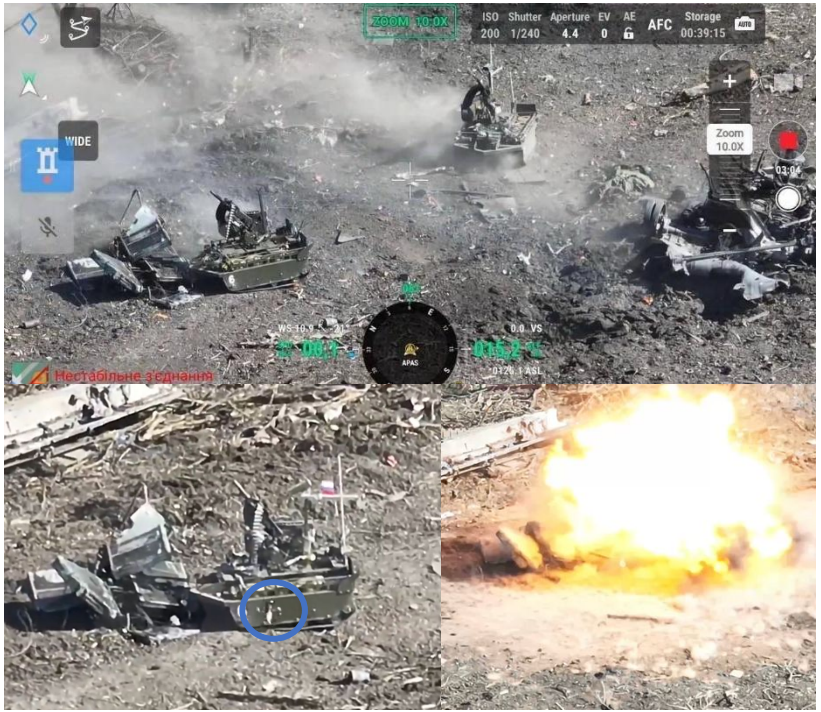
Cyber-Biosecurity Challenges in Next-Generation Sequencing: A Comprehensive Analysis of Emerging Threat Vectors

- Genomic data is vulnerable to cyber exploitation, as it is unique. **DNA cannot be changed once compromised**.
- Next-generation sequencing (NGS) revolutionizes healthcare but **introduces new cyber-biosecurity risks**.
- NGS could expose highly personal genetic information to **cyberattacks, espionage,** and even **biological sabotage**
- DNA hacking is a proven threat, **AI may accelerate with the creation of malicious DNA**, compromising sequencing systems, and manipulate bioinformatics

McMillan, 2025. Scientists Warn of DNA Hacking: New Study Reveals Terrifying Emerging Threats in Genomic Sequencing - The Debrief

Use of Ground Robots

- March 2024: Russia deployed two **Courier ground combat robots** equipped with **grenade launchers** for the first time near the city of Avdiivka
- **Ukraine successfully destroyed the robots using FPV quadcopter drones** equipped with explosives
- Two FPV drones hovered near the robots, detonating on them and causing them to explode
- Rare example of **drone-on-drone combat: unmanned ground vs. unmanned aerial vehicle**



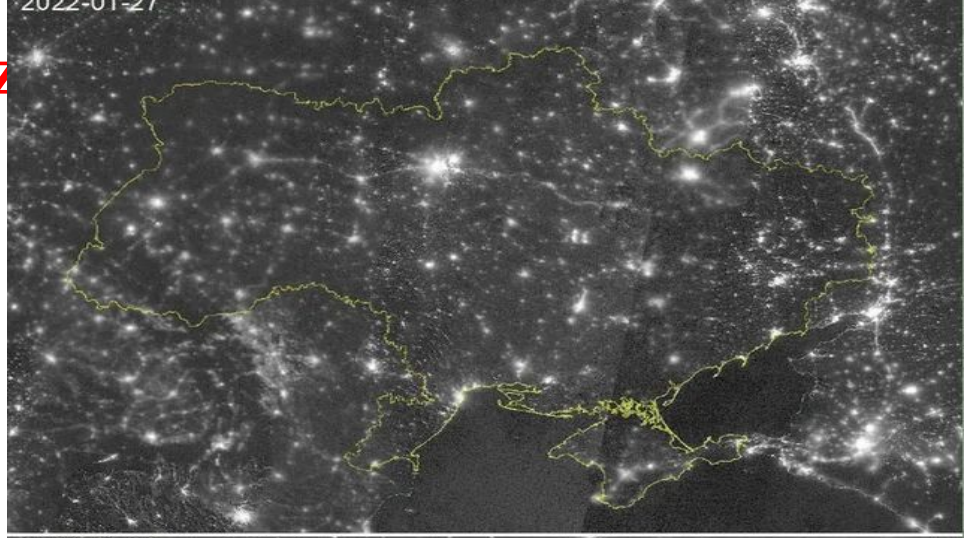
Swarming

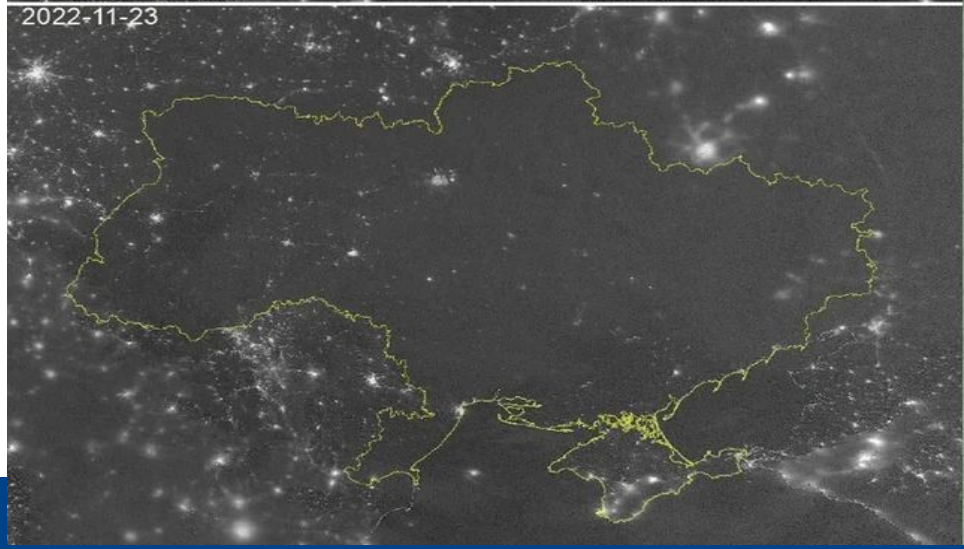
Swarming tactics: overwhelming and saturating the adversary's defense system by coordinating and synchronizing a series of simultaneous and concentrated attacks

Mass, firepower, speed, concentration of forces

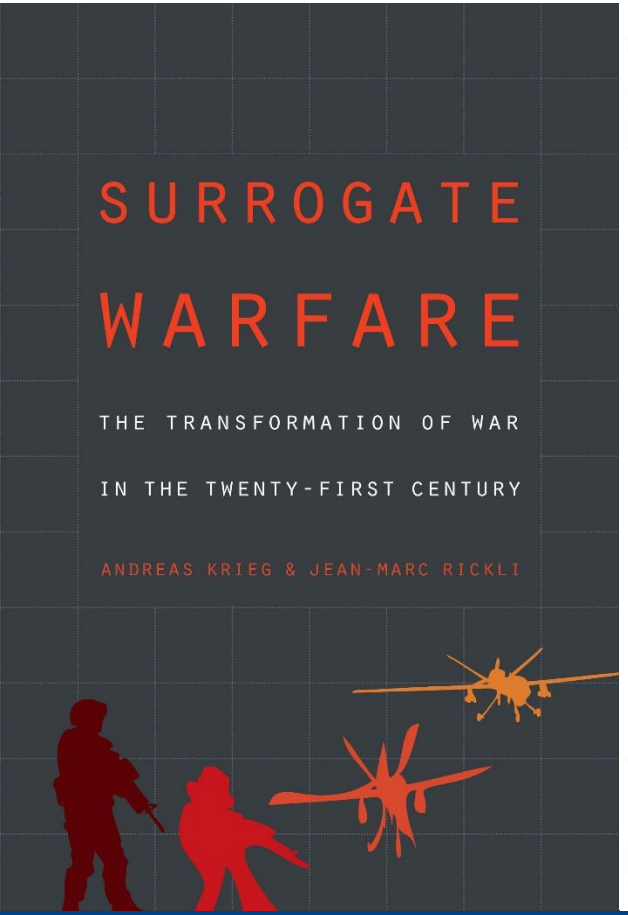
Ukraine: 30 Octobre 2024

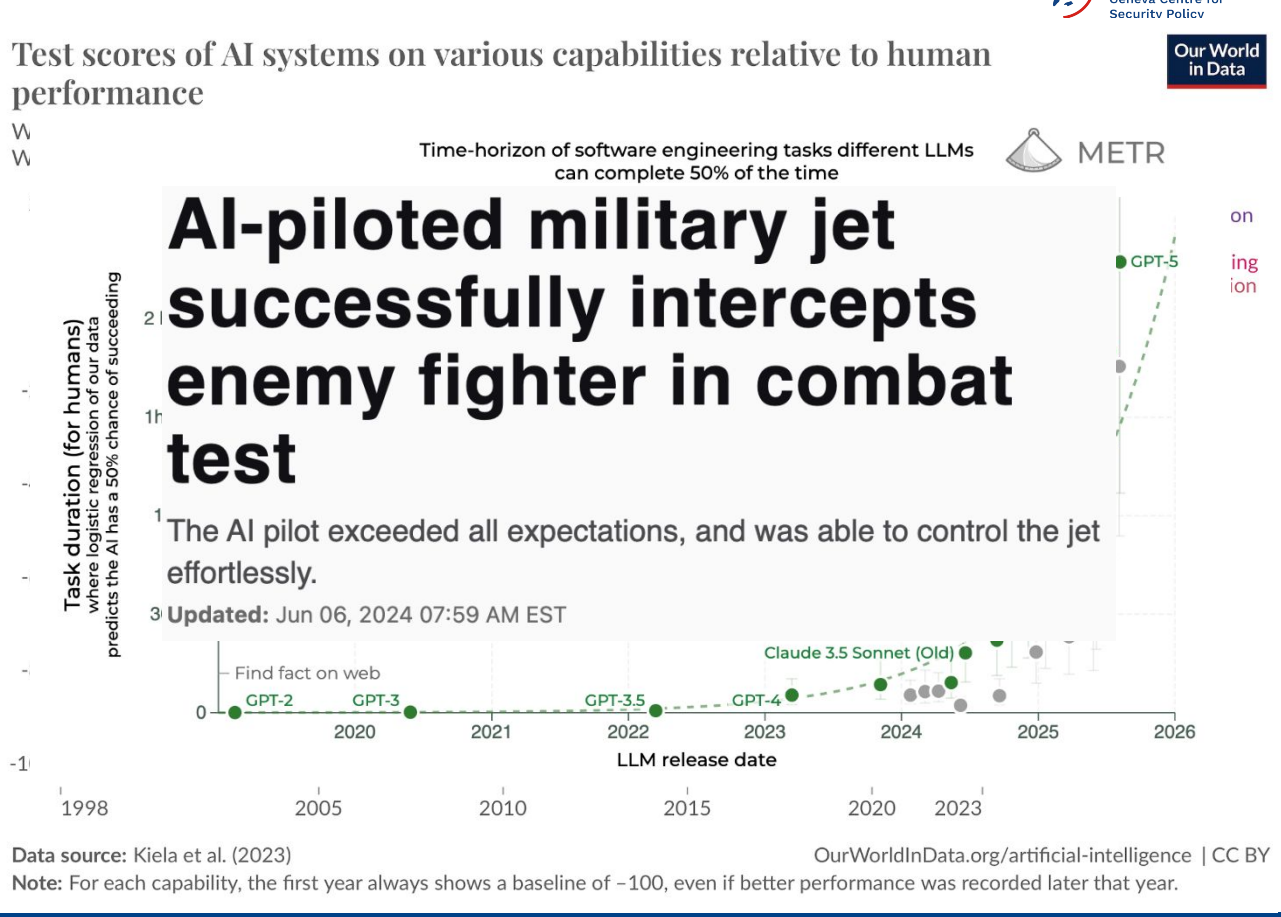
Weaponiz





Technology Acting as Surrogate

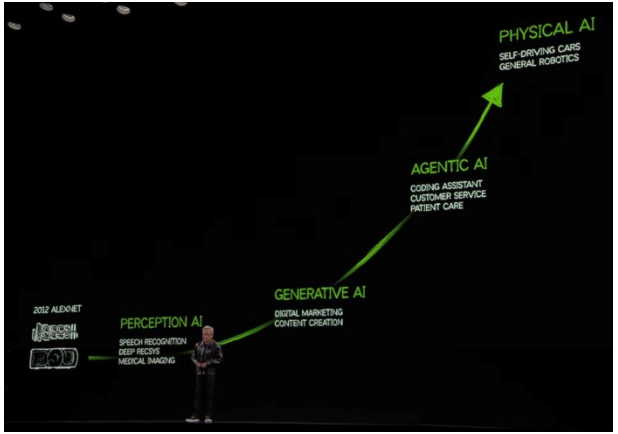




Three Waves of AI Evolution

1st Wave: Traditional/**Predictive AI**

- Characterised by data-driven algorithms, machine learning models and big data analytics
- Introduced neural networks to **identify patterns** in training data
- Mainly used for **classification, categorisation** and regression



Source: Pijanowski 2025, The New Stack

2nd Wave: **Generative AI**

- Advanced neural networks, deep learning, natural language processing as well as image and speech recognition
- Introduced transformers and Large Language Models (LLM)
- Enabled AI to **generate text, images and other content at scale**


How Agentic AI will be Weaponized for Social Engineering Attacks

With each passing year, social engineering attacks are becoming bigger and bolder thanks to rapid advancements in artificial intelligence.

By Stu Sjouwerman
February 5, 2025

3rd Wave: **Agentic AI**

- Builds on AI advancements of first two waves to enhance AI's reasoning, planning and complex problem-solving capabilities

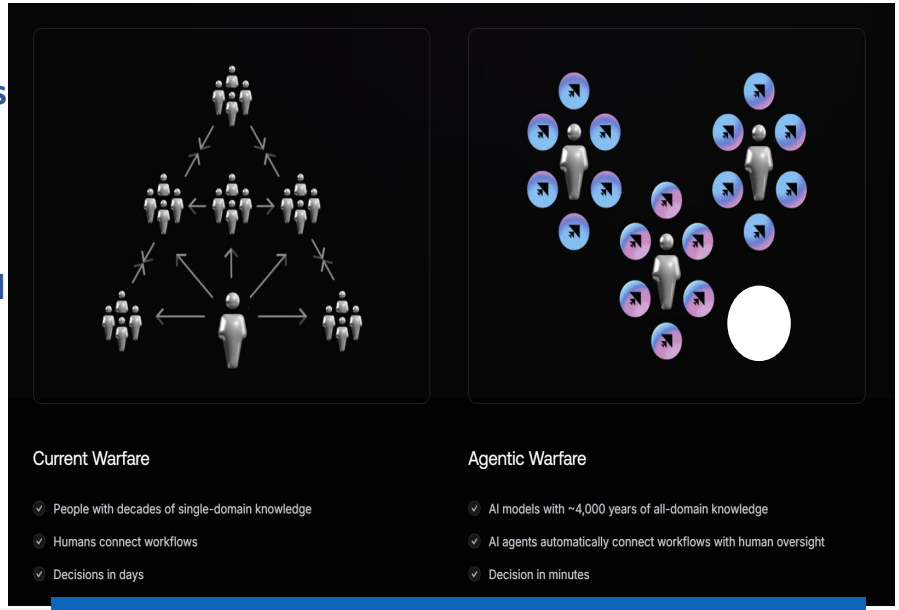
AI systems that possess a **degree of autonomy** and can **act on their own to achieve specific goals**. Unlike traditional AI models that simply respond to prompts or execute predefined tasks, agentic **AI can make decisions, plan actions, and even learn from its experiences** – all in pursuit of **objectives set by its human creators**.

Agentic Warfare

GCSP
Geneva Centre for Security Policy

Agentic warfare

- Describes an environment in which **autonomous agents play a central role in the planning and execution of military objectives**
- Increasingly important to **harness autonomous agents successfully on both the physical and digital battlefield**



‘World’s first’ fully autonomous underwater robot is piloted by AI

UK firm Beam has successfully trialled the drone at an offshore wind farm in Scotland

September 23, 2024 - 2:28 pm

AI’s New Frontier in War Planning: How AI Agents Can Revolutionize Military Decision-Making

PROJECT SPOTLIGHT | 5 MARCH 2025

DIU’s Thunderforge Project to Integrate Commercial AI-Powered Decision-Making for Operational and Theater-Level Planning

AI-Enabled Malware

- Overview
  - First publicly documented **malware case using a Large Language Model (LLM) to dynamically generate attack commands** in real time
  - Discovered in July 2025 by CERT-UA (Ukraine's Emergency Response Computer Team)
    - Likely linked to Russian state-sponsored group APT28 (Fancy Bear)
    - Targets: Ukrainian government & defence sector

Signals a new era of **adaptive, AI-driven cyberattacks** and significant advancements in adversarial AI usage in cyber espionage: **moving beyond simple automation to attacks adapting in real time**

CSO

Novel malware from Russia's APT28 prompts LLMs to create malicious Windows commands

News Analysis
Jul 18, 2025 • 4 mins

Advanced Persistent Threats | Cyberattacks | Phishing

by Lucian Constantin
CSO Senior Writer

Chinese Hackers Used Anthropic's AI to Automate Cyberattacks

The use of AI automation in hacks is a growing trend that gives hackers additional scale and speed

By Sam Schechner Follow and Robert McMillan Follow
Updated Nov. 13, 2025 at 11:42 pm ET

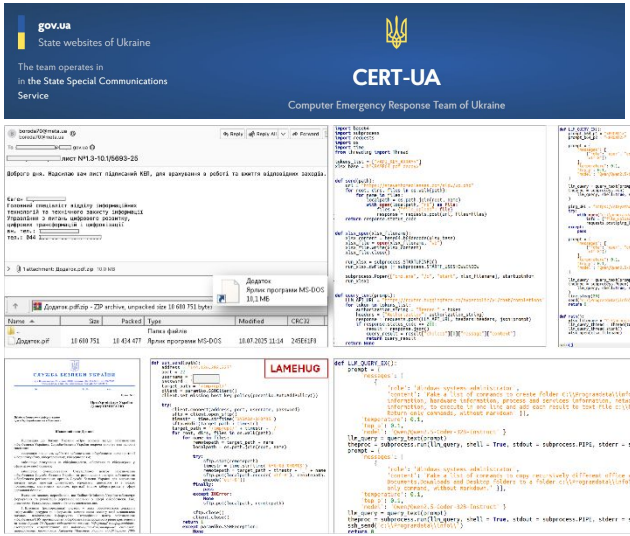
ESET Research

First known AI-powered ransomware uncovered by ESET Research

The discovery of PromptLock shows how malicious use of AI models could supercharge ransomware and other threats

Anton Cherepanov Peter Strýček

26 Aug 2025 • 2 min. read



ANTHROPIC Threat Intelligence Report, Aug 2025

GCSP
Geneva Centre for Security Policy

- **Agentic AI has been weaponized.** AI models are now being used to *perform* sophisticated cyberattacks, not just advise on how to carry them out.
- **AI has lowered the barriers to sophisticated cybercrime.** Criminals with few technical skills are using AI to conduct complex operations, such as developing ransomware, that would previously have required years of training.
- **Cybercriminals and fraudsters have embedded AI throughout all stages of their operations.** This includes profiling victims, analyzing stolen data, stealing credit card information, and creating false identities allowing fraud operations to expand their reach to more potential targets.

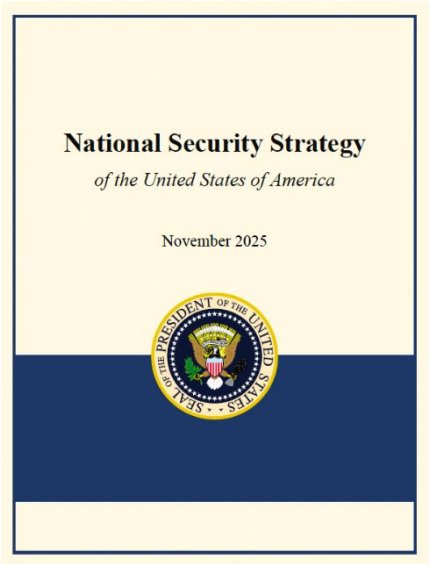
AI and Global Power

GCSP Geneva Centre for Security Policy

China

New Generation Artificial Intelligence Development Plan (新一代人工智能发展规划)	2017	Make China a global AI leader by 2030	Central roadmap for AI advancement in theory, tech, ethics, and industry

United States



*We want to ensure that **U.S. technology and U.S. standards**—particularly in **AI**, biotech, and quantum computing—**drive the world forward.***

US-China Technology Decoupling

- Sustained struggle **codifying coercion and weaponizing interdependence** for leverage—beyond conventional trade wars.
- Three Assumptions: (1) **Codified coercion without market collapse** is possible; (2) **Out-endure/out-adapt** the other as he is brittle; (3) **Weaponization of supply chains** to **bend, not break is possible without triggering systemic failure**.

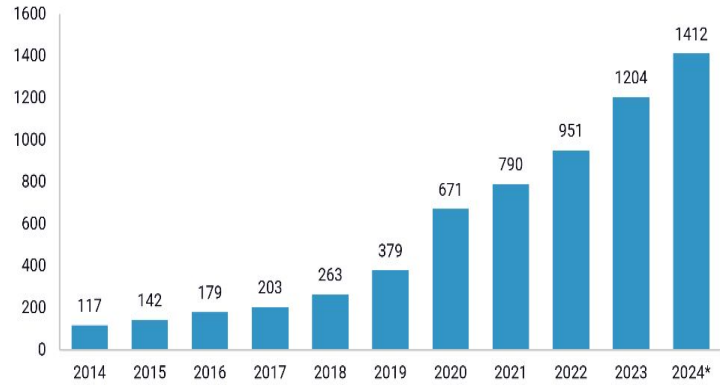
- Importance of the technological sector in economic strength, power projection, and national security
- The U.S. is trying to delay the rise of the Chinese technology giants
- **Technology decoupling**, development of separate domestic technology stacks

Examples of decoupling measures:

- **Prohibition for certain Chinese technology** companies to sell products in U.S.
  - Huawei, ZTE
  - The Bytedance and Tik Tok case
- **US CHIPS and Science Act** (2022)
  - Designed to bring semiconductor manufacturing back to the US; bans construction of "advanced" semiconductor plants in China for ten years
  - Ban on providing Chinese chipmakers with equipment to produce sophisticated chips and restricts collaboration for subsidized companies
- **AI & semiconductor export controls** (2022-2024)
  - Restricted exports of advanced AI chips to China
  - Banned sales of semiconductor manufacturing equipment (lithography tools)
- **Entity list expansions**
  - Further export control updates in December 2024 ,January and September 2025
  - March 2025: Trump administration added 54 Chinese companies and organizations to the entity list (incl. AI, cloud, quantum companies)

FIGURE 1

Number of Chinese entities designated under US sanctions and red-flag lists



Source: Rhodium Group. *Number of Chinese entities as of July 1, 2024.

US-China Decoupling

GCSP
Geneva Centre for Security Policy

US-China Decoupling

China slams US' chip ban attempt, warns legal liability

Seeking to exclude China from supply chain impractical, to backfire: expert

By Ma Tong and Chen Qingrui
Published: May 21, 2025 11:33 PM

ECONOMY • ARTIFICIAL INTELLIGENCE

AI race: US-China chip war heats up

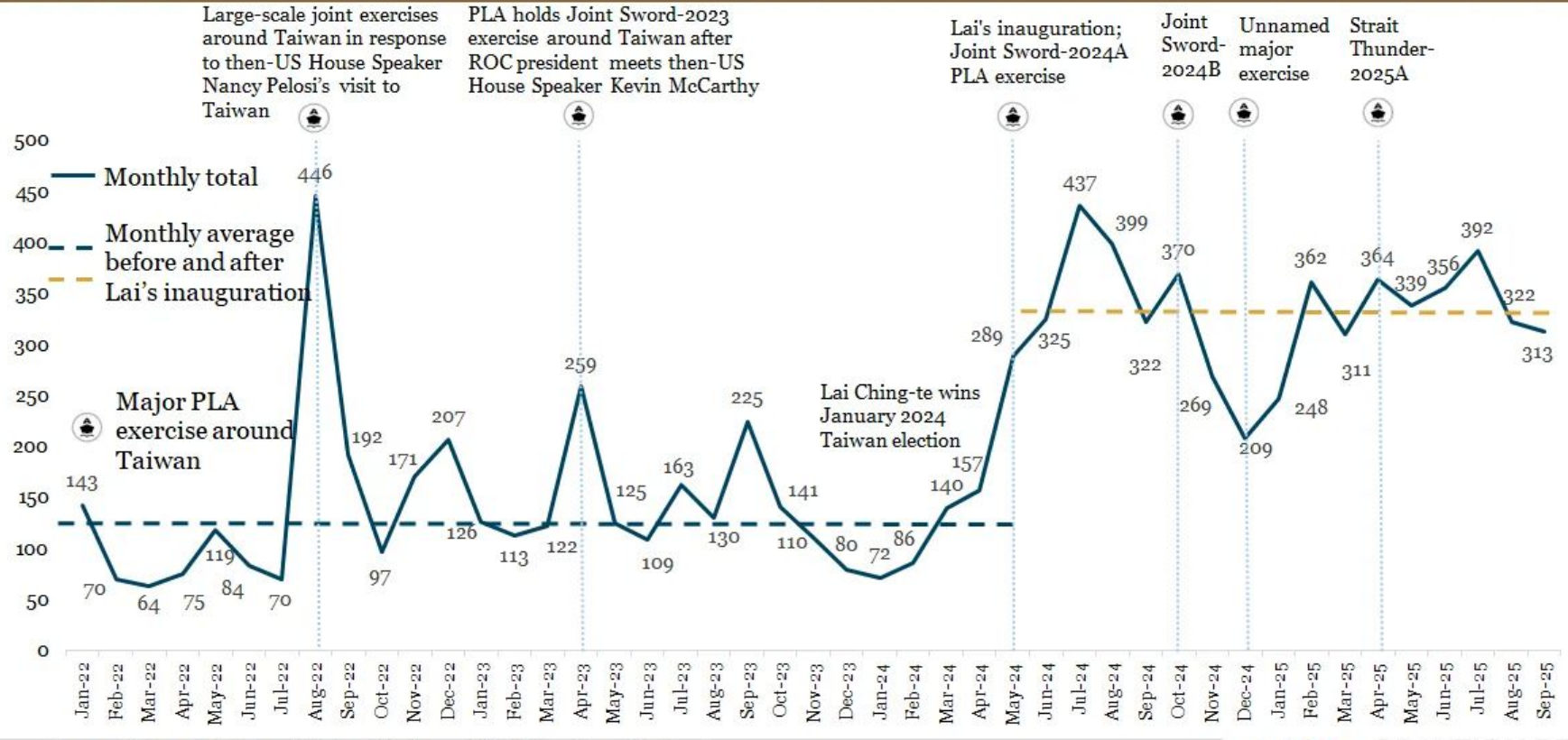
By Harold Thibault (Beijing (China) correspondent)
Published on May 23, 2025, at 10:16 am (Paris)
4 min read Lire en français

13 May 2025: According to a directive from the Bureau of Industry and Security, the division of the US Department of Commerce responsible for controlling sensitive exports, **using Huawei Ascend chips "anywhere in the world" may violate US export control regulations**. Washington explained that the latest chips from Chinese manufacturer Huawei, the Ascend 910 models, had been designed or produced with certain software or equipment originating from the US.

The **phrase "anywhere in the world" has since been removed from the Commerce Department's statement, but the damage was done**. "The recent attempt at a complete blockade of Chinese chips is a blatant act of unilateralism and intimidation," condemned Chinese Foreign Minister Wang Yi on May 20 China has warned that **anyone who complies with US measures will be suspected of violating Chinese law against foreign sanctions**. As a result, any company worldwide that buys Huawei's latest chip models will be targeted by USA, but anyone who complies with US orders will risk criminal prosecution in China.

Source: The Information 2025

Monthly PRC Incursions into Taiwan's ADIZ, Jan 2022 - Sept 2025



Source: Taiwan Ministry of National Defense; CSIS China Power Project

COALITION DEFENSE OF TAIWAN

Autonomous Swarm

Wargames that the U.S. Air Force has conducted itself and in conjunction with independent organizations continue to show the **immense value offered by swarms** of relatively **low-cost networked drones** with **high degrees of autonomy.** In particular, simulations have shown them to be **decisive** factors in the scenarios regarding the defense of the island of Taiwan against a Chinese invasion.

Simulations shows that large numbers of unmanned aircraft, especially **relatively small and inexpensive** designs **capable of operating as fully-autonomous swarms** using a distributed ”mesh” data-sharing network, have shown themselves to be **absolutely essential** for coming out on top in these wargames.

Western Technological Conondrum

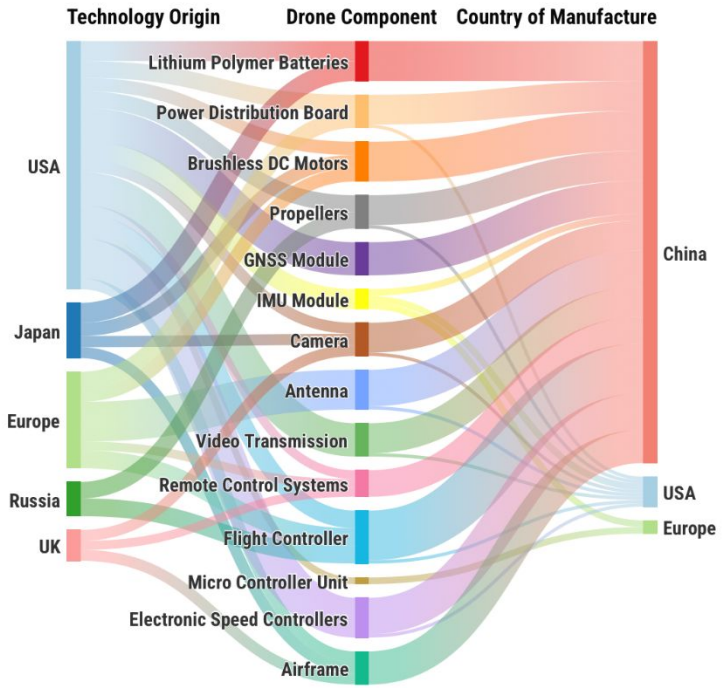
GCSP Geneva Centre for Security Policy

How the US and its allies lost the battle for drones

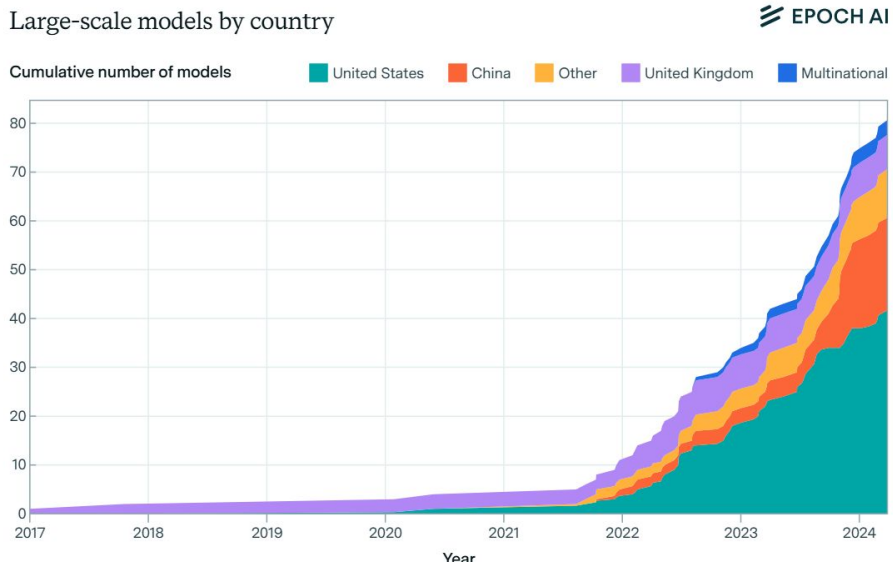
Most components of commonly used drones were invented in the Japan and Europe but almost all are now made in China.

Interactive or visual content

All



Source: Edlyn Levine & Fiona Murray



Rahman et al., 2024. Tracking large-scale AI models | 81 models across 18 countries | Epoch AI

Western Technological Conondrum

GCSP Geneva Centre for Security Policy

Dutch minister defends Nexperia takeover amid chip supply strains

By **Reuters**

December 5, 2025 10:22 AM GMT+1 · Updated December 5, 2025

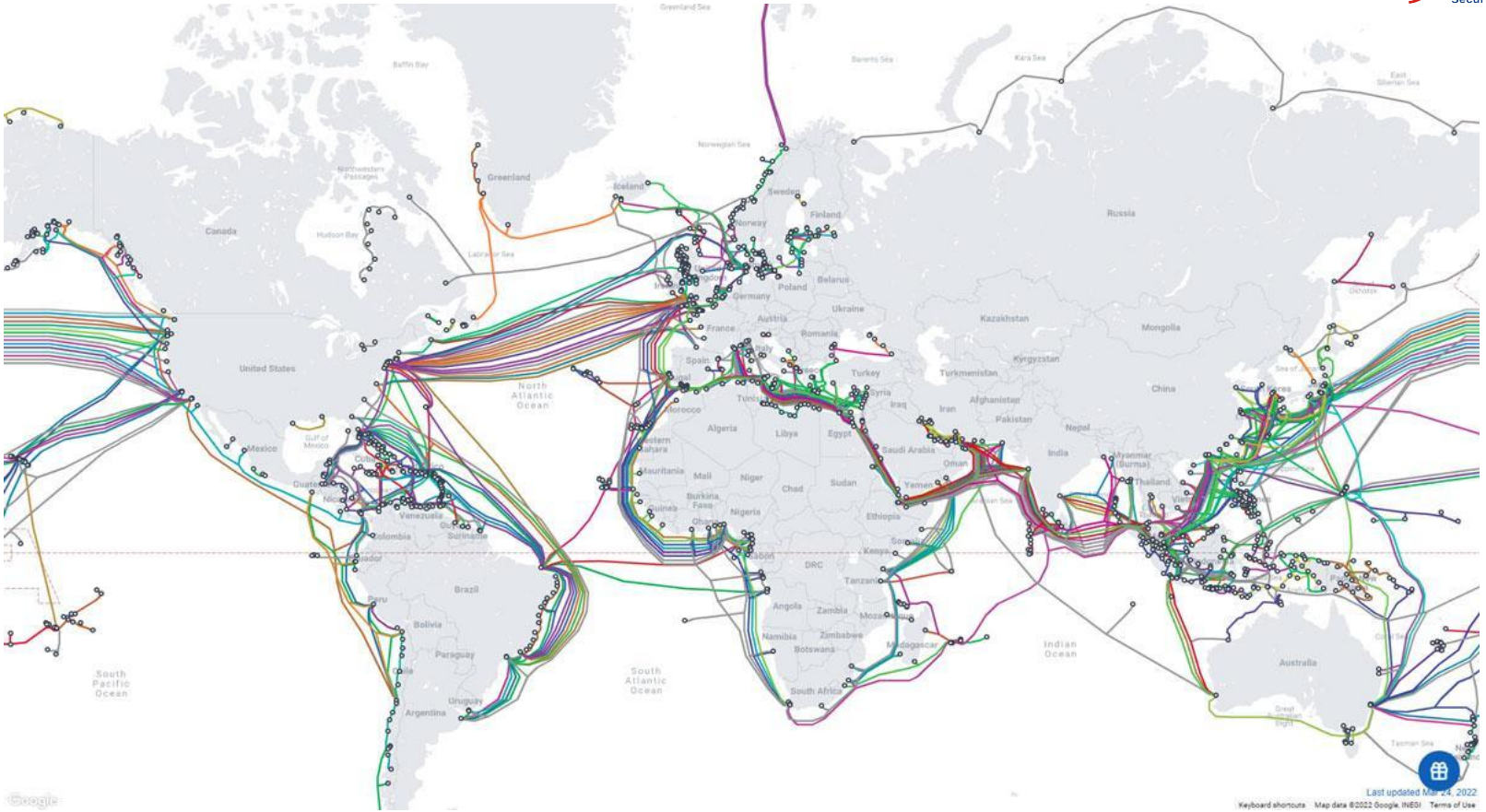
The Dutch government took control of **Nexperia**, a Dutch subsidiary of Chinese firm Wingtech, on September 30, saying the move was needed to **prevent Wingtech's founder from moving company secrets and production to China**.

On October 4, **the Chinese government retaliated by blocking the export of Nexperia's chips**, most of which are packaged in China.

The result was a **supply shock with European carmakers** which the intervention had sought to protect bearing the brunt

Geopolitics of the Internet

GCSP
Geneva Centre for Security Policy

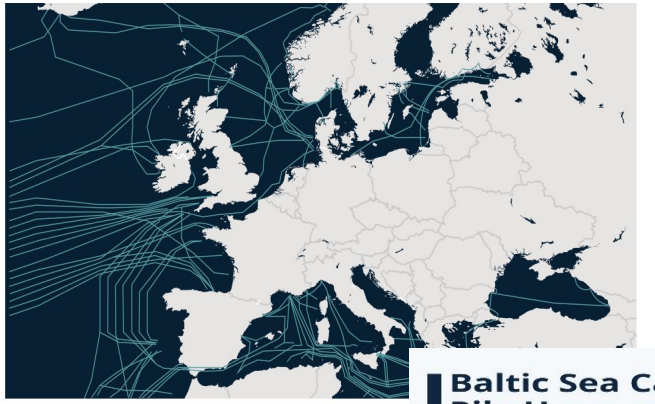


Strategic Importance of Undersea Digital Infrastructure

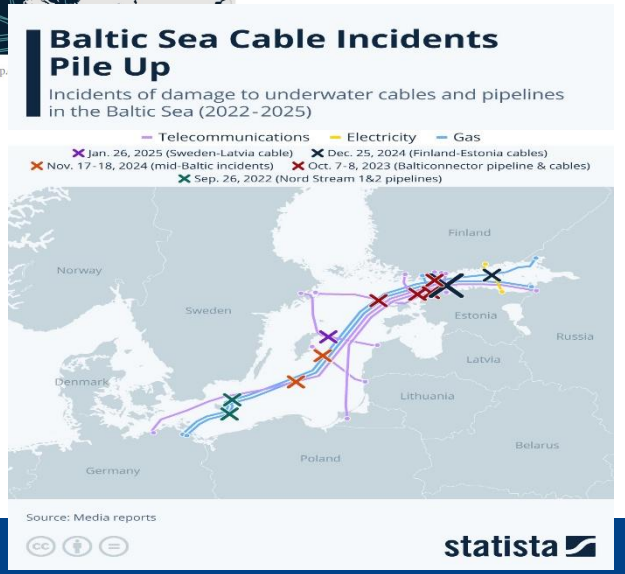
- Importance of Critical Undersea Infrastructures:
  - **90%** of the world's digital communications data go through undersea cables. **€10 trillion** in financial transactions pass through daily. Critical undersea infrastructures include **electricity connectors, pipelines supplying oil and gas**.
- **Since** Oct 2023**, over 11 Baltic Sea** cables have been damaged amid escalating Russian sabotage operations.
- Disruptive attacks on undersea cables involved **anchor-dragging by Russia's 'shadow fleet'**.

- NATO Response:
  - **Jan 2025 ->** Launch of "Baltic Sentry" – joint military activity to strengthen critical infrastructures
  - **Jan 2025 ->** Launch of "North Seal" - monitoring suspicious maritime activities, rapid information exchange and coordinate responses
  - NATO's Senior expert on cyber and hybrid threats highlights that attacks on undersea cables across Europe is **"the most active threat"** to Western infrastructure.

Figure 2: Undersea Data Cables in Europe



Source: Data from "Submarine Cable Map," TeleGeography, https://www.submarinecablemap.



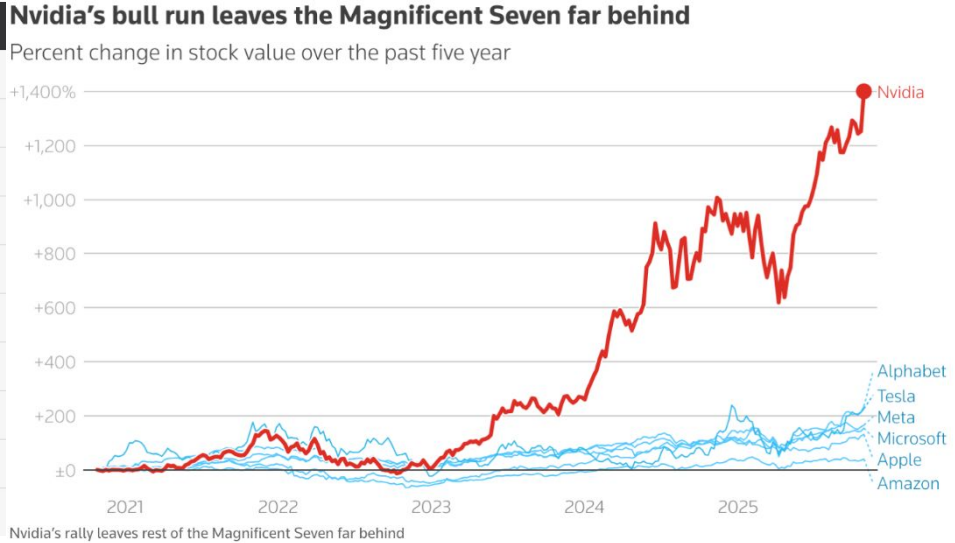
Tech Companies as New Actors

GCSP Geneva Centre for Security Policy

Rank & Country	GDP (USD)	2025 Projected Real GDP (% Change)
#1 United States (U.S)	$30.62 trillion	2%
#2 China	$19.4 trillion	4.8%
#3 Germany	$5.01 trillion	0.2%
#4 Japan	$4.28 trillion	1.1%
#5 India	$4.13 trillion	6.6%
#6 United Kingdom (U.K.)	$3.96 trillion	1.3%
#7 France	$3.36 trillion	0.7%
#8 Italy	$2.54 trillion	0.5%
#9 Russia	$2.54 trillion	0.6%
#10 Canada	$2.23 trillion	1.2%

Note: As of October 29

Source: LSEG | Shashwat Chauhan



Nvidia's rally leaves rest of the Magnificent Seven far behind

Nvidia made history on Oct 29, 2025 as **the first company to reach $5 trillion** in market value, just 3 months after it breached the $4 trillion mark. Took Nvidia 30 years to reach $1 trillion market cap, 10 months to $2 trillion, and 96 days to $3 trillion.

Tech Companies' Competition

GCSP
Geneva Centre for Security Policy

DeepSeek and the Race to AGI: How Global AI Competition Puts Ethical Accountability at Risk

HAILELEOL TIBEBU / JAN 29, 2025

***Figure 11**: Top monthly Elo ratings, Chinese AI companies (Source: LMsys ChatArena)*

Possible Takeaways

- Geopolitical and technological competition are deeply intertwined as **emerging technologies are a key determinant of global power in the 21st century**
- China and US competition extends to trade war and increasingly towards technological decoupling
- Data explosion and commercialisation of **AI** are profoundly transforming social relations
- Vertical and horizontal **proliferation** at very high speed of emerging technologies
- **Democratisation** of means of power
- **Exponential** nature of emerging technologies implies a very rapid pace of **transformations**
- **Technology** acting increasingly as **surrogate** (eg. autonomy): role of **human agency**?
- **Subversion** as **weapon of choice** to **undermine democracies** before conflict erupts
- **Cognitive warfare** is becoming the **6th domain of warfare**
- Cognitive Warfare will **increase the efficiency** of **subversion over coercion**
- There is a **normative**, and **ethical vacuum** around the **new tool**s state and non-state actors can utilise to **wage** cognitive warfare
- Need to move from defense to **resilience** to address such a broad scope of risks
- Convergence of emerging tech: need for **foresight**, **resilience** and **polymath** thinking
- **Responsible innovation**: **security by design** coupled with global governance system
- REMEMBER: **There are no limitations to human ingenuity for good and…evil**
- Example: when you combine cryptography with blockchain, you get a ransomware!

Many Thanks For Your Attention

Questions?

Dr. Jean-Marc Rickli
j.rickli@gcsp.ch
Twitter: @Dr_JMRickli