

Hardware Security and the Rise of the ***Bloc***-Cipher

Dr. Axel Y. Poschmann

What is a **Bloc**-Cipher?

- Not a Typo!



- A **cipher** primarily used *within* a **bloc**



Dictionary

Definitions from [Oxford Languages](#) · [Learn more](#)



cipher¹

/ˈsaɪfə/

noun

1. a secret or disguised way of writing; a code.
"he wrote cryptic notes in a cipher"

Similar:

code

secret writing

coded message

cryptograph

cryptogram



bloc

/blɒk/

noun

- a group of countries or political parties with common interests who have formed an alliance.
"the Soviet bloc"

Similar:

alliance

association

coalition

federation

confederation

league

THE *Real* TRUTH

OF COOKING ON SALT BLOCK

Disclaimer

My own
personal
views and
observations

Wherever
possible backed
up by data and
references

This discipline
can have
different
interpretations

Radically
simplified to
drive a point

To be taken with a
pinch *block* of salt!



Why are Geopolitics Important?

 **CNN BUSINESS** [Markets](#) [Tech](#) [Media](#) [Calculators](#) [Videos](#)

Jamie Dimon warns: 'Now may be the most dangerous time the world has seen in decades'

 By [Nicole Goodkind](#), CNN
Updated 10:12 AM EDT, Fri October 13, 2023



“What’s happening on the geopolitical front right now is the most important thing for the future of the world - freedom, democracy, food, energy, immigration.”

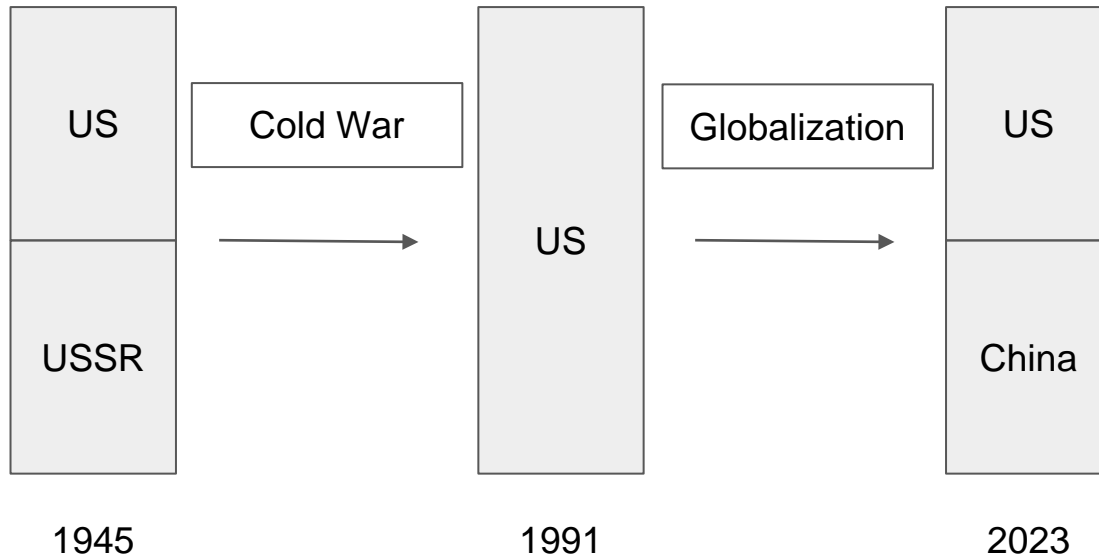
- *Jamie Dimon November 2023*

- Highly Topical
- Affect everyone
- Impact our work

Geopolitics = Power Play













- Power = ability to achieve your goals
- Guns = ability to protect yourself
- Butter = GDP = ability to
 - Buy influence
 - Buy guns (*Zeitenwende*)
 - Create new technology

Outrageously Simplified Geopolitics



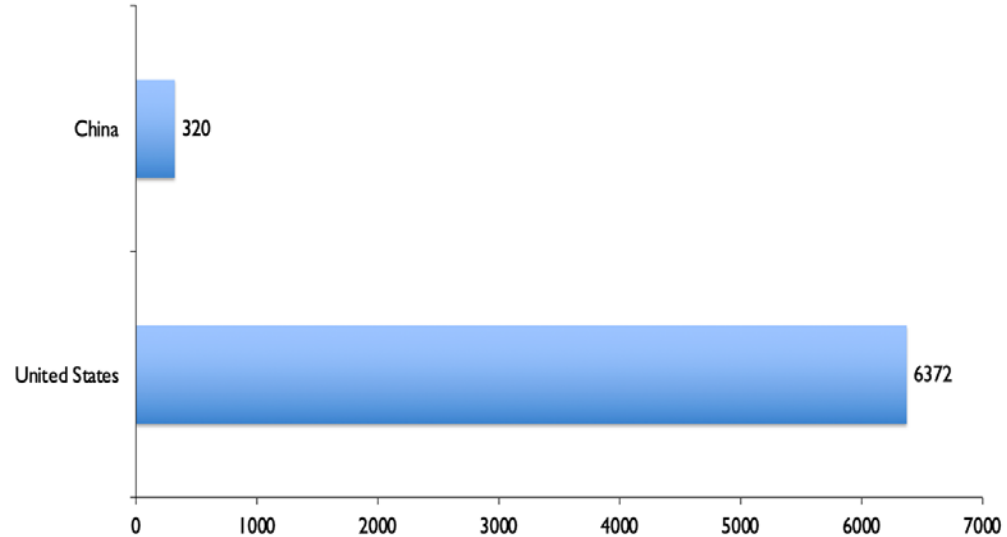
Guns comparison: US vs China

COMPARISON BRIEF

✗		Manpower		✓
✓		Airpower		✗
✗		Land Power		✓
✗		Naval Power		✓
✓		Nat.Resources		✗
✗		Financials		✓
✓		Logistics		✗
✓		Geography		✗

“The great equalizer”

TOTAL NUCLEAR MILITARY STOCKPILES, 2020

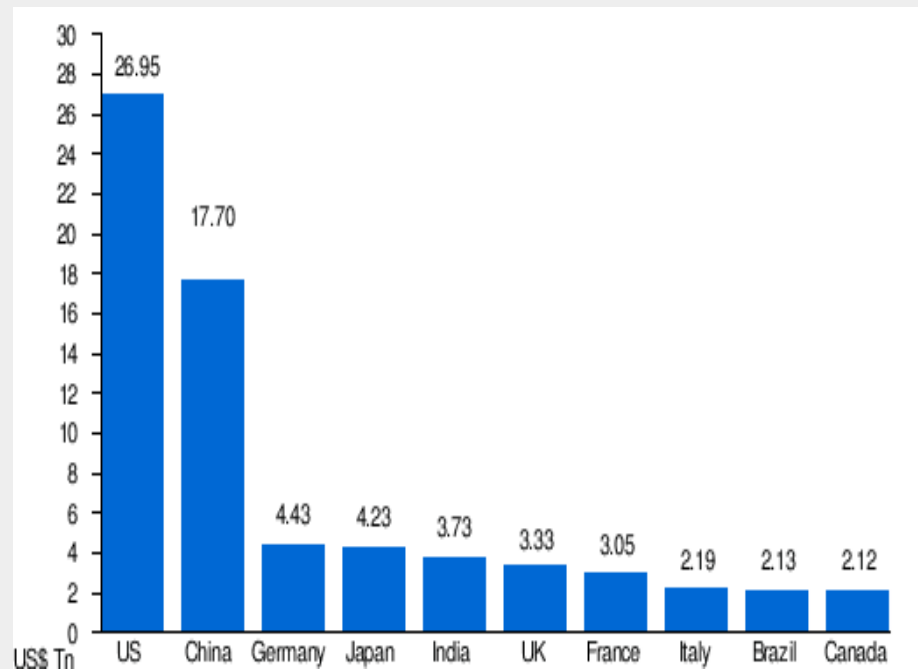


Source:

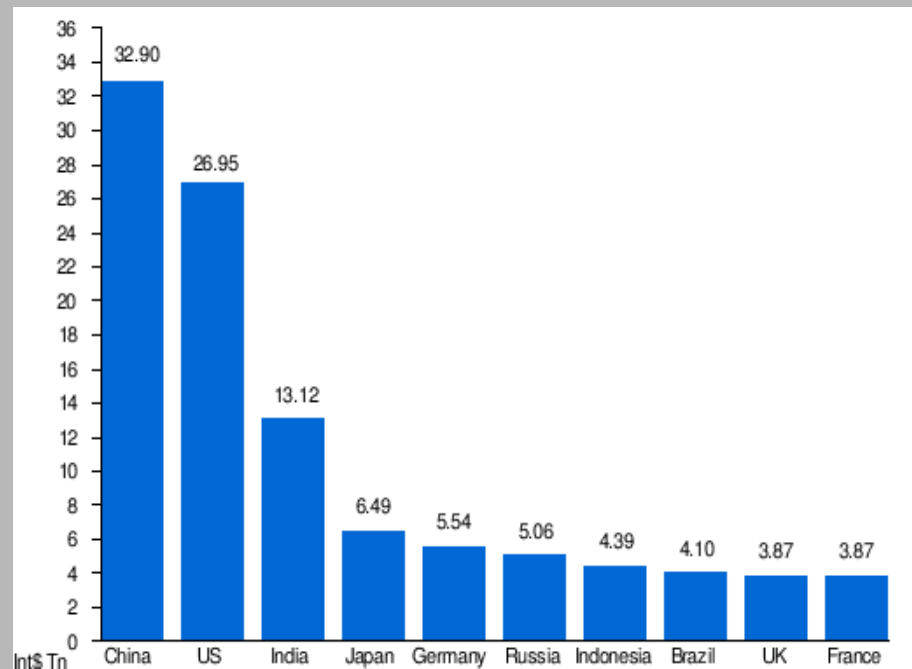
<https://www.globalfirepower.com/countries-comparison-detail.php?country1=united-states-of-america&country2=china>

Butter comparison: US vs China October 2023

Nominal



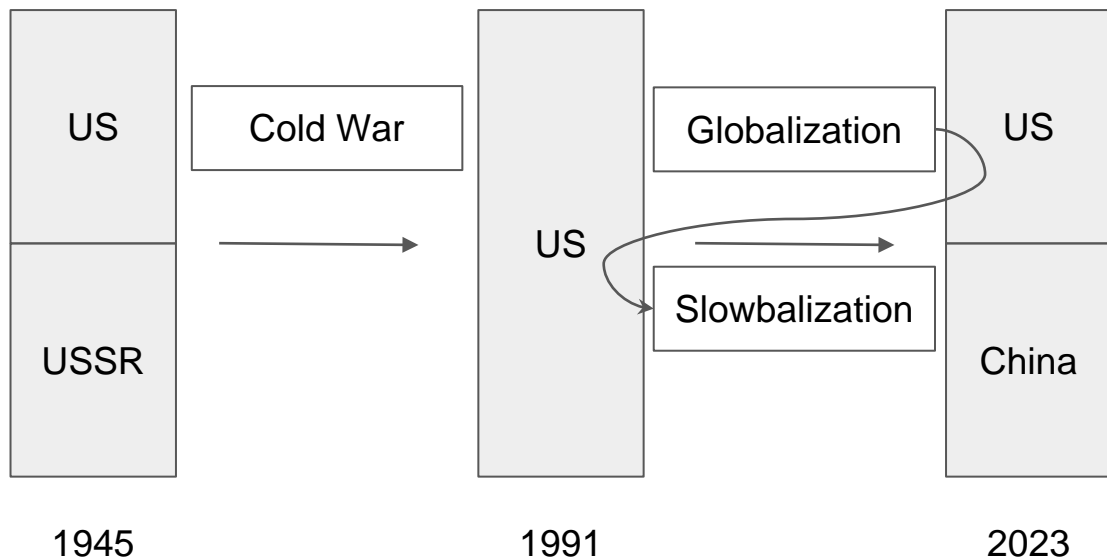
PPP = Purchasing Power Parity



Source:

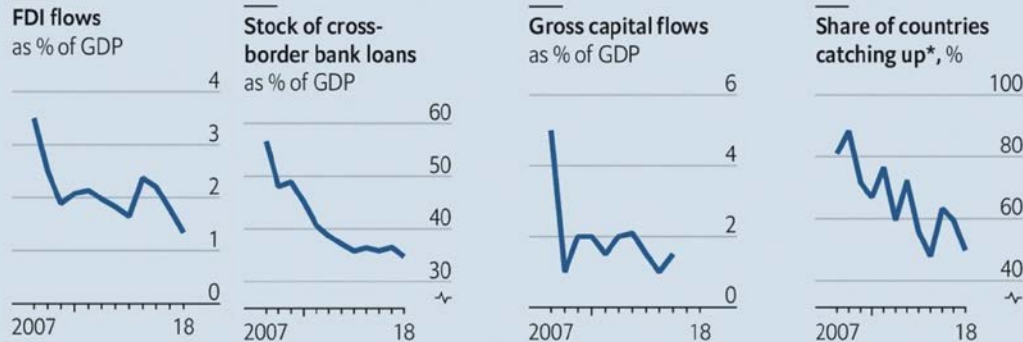
"World Economic Outlook Database, October 2023 Edition". IMF.org. International Monetary Fund. Retrieved 5 November 2023.

Outrageously Simplified Geopolitics



Slowbalization

- Foreign Direct Investments peaked in 2008
- So do other key indicators



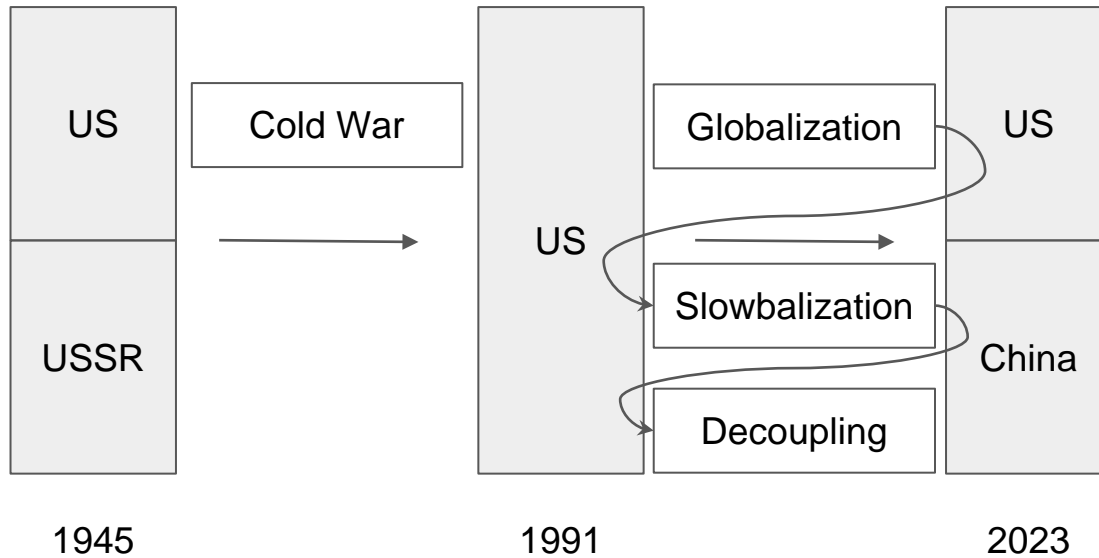
Source:

The Economist, 2020, <https://www.economist.com/weeklysedition/2020-05-16>

The Economist, 2019, <https://www.economist.com/briefing/2019/01/24/globalisation-has-faltered>



Outrageously Simplified Geopolitics



Friendshoring/Nearshoring/Derisking/Decoupling

“Western countries are increasingly adopting industrial policies that promote **“friendshoring” of strategic industries.**”



The Economist explains

What is “friendshoring”?

Western policymakers want to move supply chains to friendly countries



...a government pushes businesses to restructure supply chains, shifting production away from **geopolitical rivals** to friendly powers.

Source:

Bloomberg, 24/07/2023, <https://www.bloomberg.com/news/articles/2023-07-24/germany-readies-20-billion-in-aid-to-bolster-chip-production#xj4y7vzkg>

Bloomberg, 25/07/2023, <https://www.bloomberg.com/news/articles/2023-07-25/eu-enacts-43-billion-chips-act-in-bid-to-boost-production>

White House 09/08/2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/>

Chip Manufacturing = Strategic Capability

Semiconductor scramble

New investments in domestic fabrication plants and facilities by country, in USD billions

Country	Investment ▼
United States	\$165.5bn
Germany	\$26.1bn
China	\$22.8bn
India	\$22.5bn
Ireland	\$11.8bn
South Korea	\$10.6bn
Japan	\$10.0bn
Malaysia	\$9.3bn
Singapore	\$9.0bn
France	\$5.7bn
Italy	\$5.1bn
Taiwan	\$3.5bn
United Kingdom	\$1.3bn
Vietnam	\$1.1bn
Total	\$303.12bn

Source: Semiconductor Engineering | A.F. Alias | Breakingviews | June 1, 2023

Source:

Bloomberg, 24/07/2023, <https://www.bloomberg.com/news/articles/2023-07-24/germany-readies-20-billion-in-aid-to-bolster-chip-production#xj4y7vzkg>

Bloomberg, 25/07/2023, <https://www.bloomberg.com/news/articles/2023-07-25/eu-enacts-43-billion-chips-act-in-bid-to-boost-production>

White House 09/08/2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/>

Reuters 02/06/2023, <https://www.reuters.com/breakingviews/securonomics-is-fuzzy-new-lodestar-investors-2023-06-02/>

Bloomberg

Subscribe

Economics

Germany Readies €20 Billion in Aid to Bolster Chip Output

- About 75% of the money is going to US's Intel, Taiwan's TSMC
- Funds are set to come from off-budget pot despite fiscal cuts



THE WHITE HOUSE



AUGUST 09, 2022

FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China

\$280B

Bloomberg

Subscribe

Technology

EU Enacts €43 Billion Chips Act in Bid to Boost Production



Decoupling

China

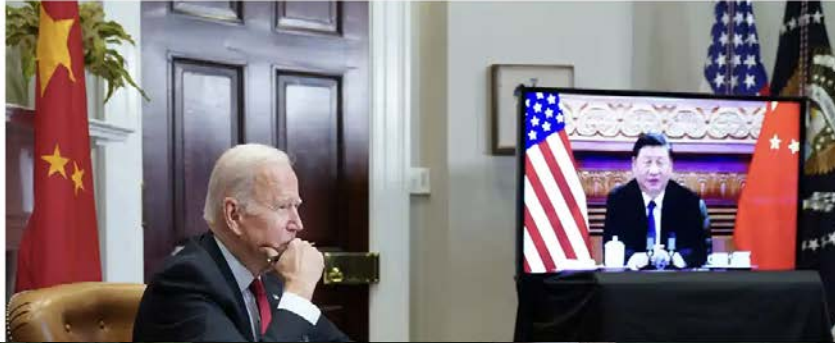
Competitor or adversary? West struggles to define relationship with Beijing

US's most vital trade partner and main long-term competitor presents a sticky 'pacing challenge'



Julian Borger world affairs editor

Thu 16 Feb 2023 04:00 GMT



Strategy on China

of the Government of the
Federal Republic of Germany

Against this backdrop, China is simultaneously a **partner, competitor and systemic rival** for the Federal Government. Our Strategy on China is firmly rooted in the common policy on China of the EU.



China, Once Germany's Partner in Growth, Turns Into a Rival

'China is not a developing country, not at all. It's an established, top-notch manufacturing country'

Source:

The Guardian 2023, <https://www.theguardian.com/world/2023/feb/16/competitor-or-adversary-the-west-struggles-to-define-its-relationship-with-beijing>

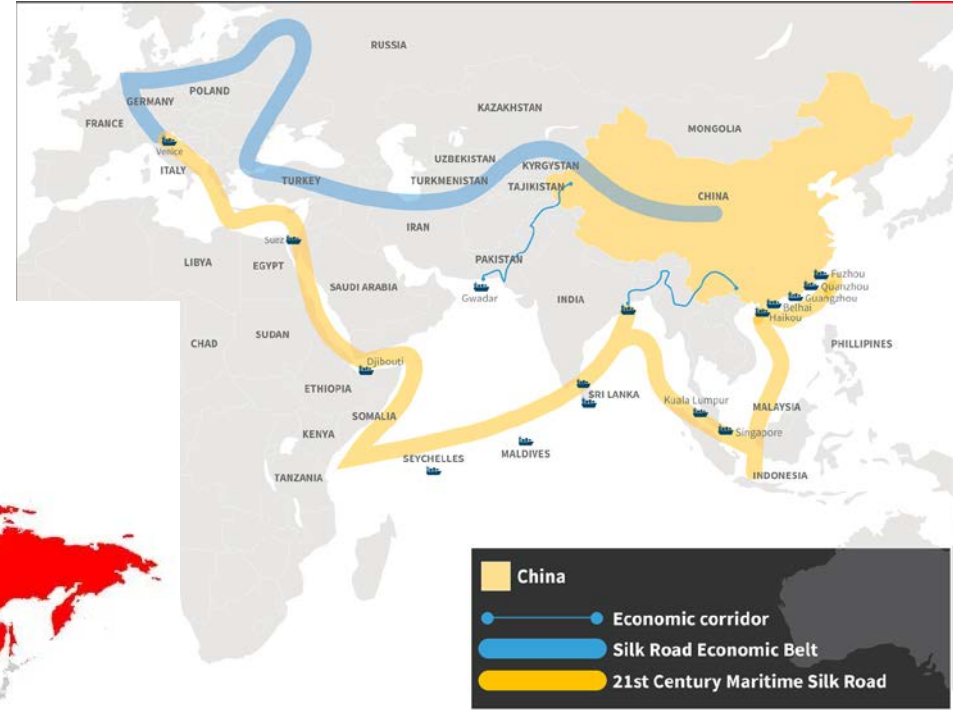
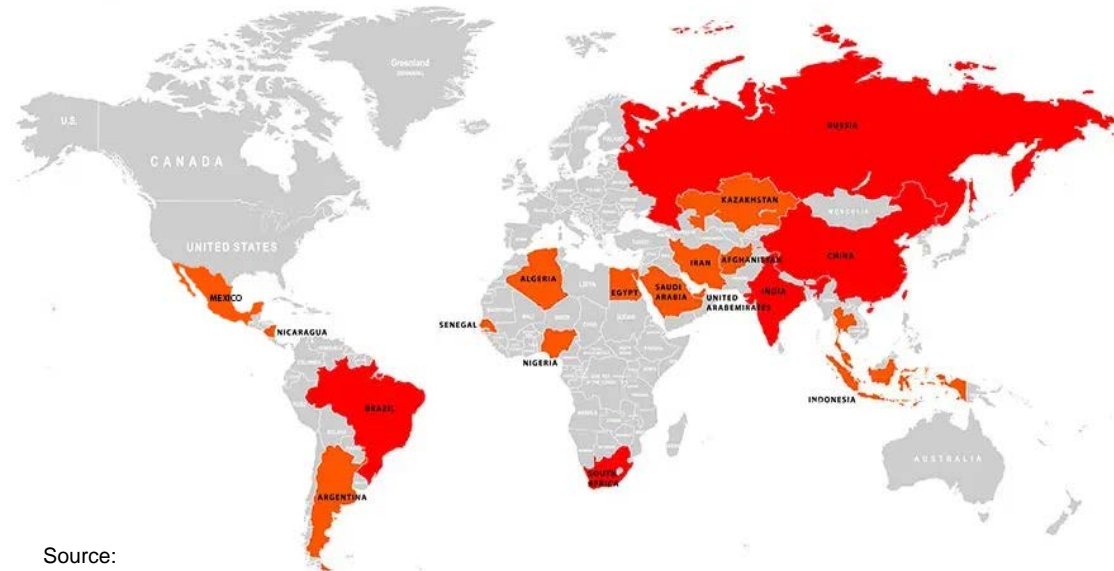
CNN, 2023, <https://edition.cnn.com/2023/03/14/australia/aukus-deal-china-tensions-analysis-intl-hnk/index.html> AA, 2023, <https://www.auswaertiges-amt.de/blob/2608580/49d50fecc479304c3da2e2079c55e106/china-strategie-en-data.pdf>

WSJ. 2020. <https://www.wsj.com/articles/china-once-germanys-partner-in-growth-turns-into-a-rival-11600338663>

Decoupling

Proposed BRICS Expansion

- Current BRICS members
- Proposed BRICS members



- One Belt, One Road Initiative
- Asian Infrastructure Investment Bank
- Ren Min Bi as trade currency
- BRICS+

Source:

<https://www.weforum.org/agenda/2017/06/china-new-silk-road-explainer/>

<https://www.silkroadbriefing.com/news/2023/03/27/the-brics-has-overtaken-the-g7-in-global-gdp/>

Decoupling

G20 summit: New 'spice route' deal to counter China's OBOR

Dipak K Dash / TNN / Updated: Sep 10, 2023, 11:24 IST



India, along with the US, EU, Saudi Arabia and UAE, clinched a deal Saturday to set up the India-Middle East-Europe Economic Corridor that will provide faster and cheaper sea and rail transit option to west Asia and Europe and is seen as a counter to One Belt One Road initiative. Praising PM Modi for helping clinch a deal to set up a trade corridor linking India with west Asia and Europe, Biden said the proposed partnership was in sync with the current G20's theme of One Earth, One Future.

- New Spice Road
- I2U2
- AUKUS
- QUAD

Source:

<https://www.defense.gov/Spotlights/AUKUS/>
<https://www.theguardian.com/world/2023/may/20/australia-india-japan-and-us-take-thinly-veiled-swipe-at-china>
<https://www.orfonline.org/expert-speak/an-india-europe-trade-corridor/>

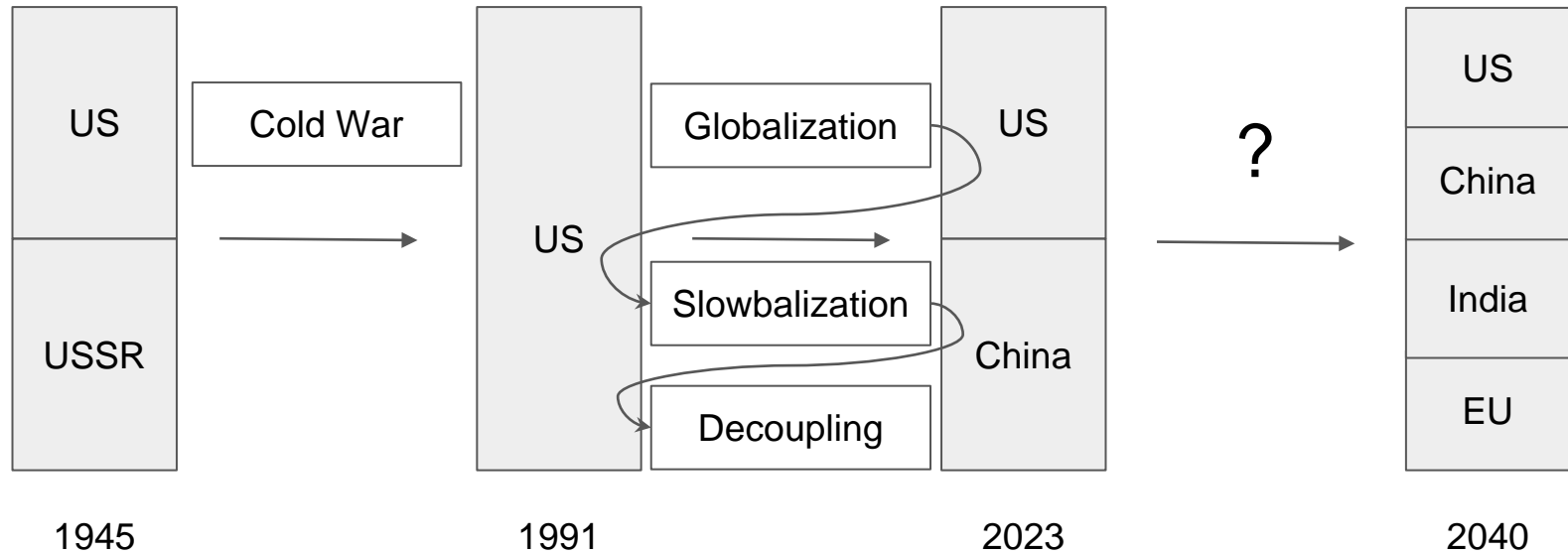


Australia, India, Japan and US take thinly veiled swipe at China

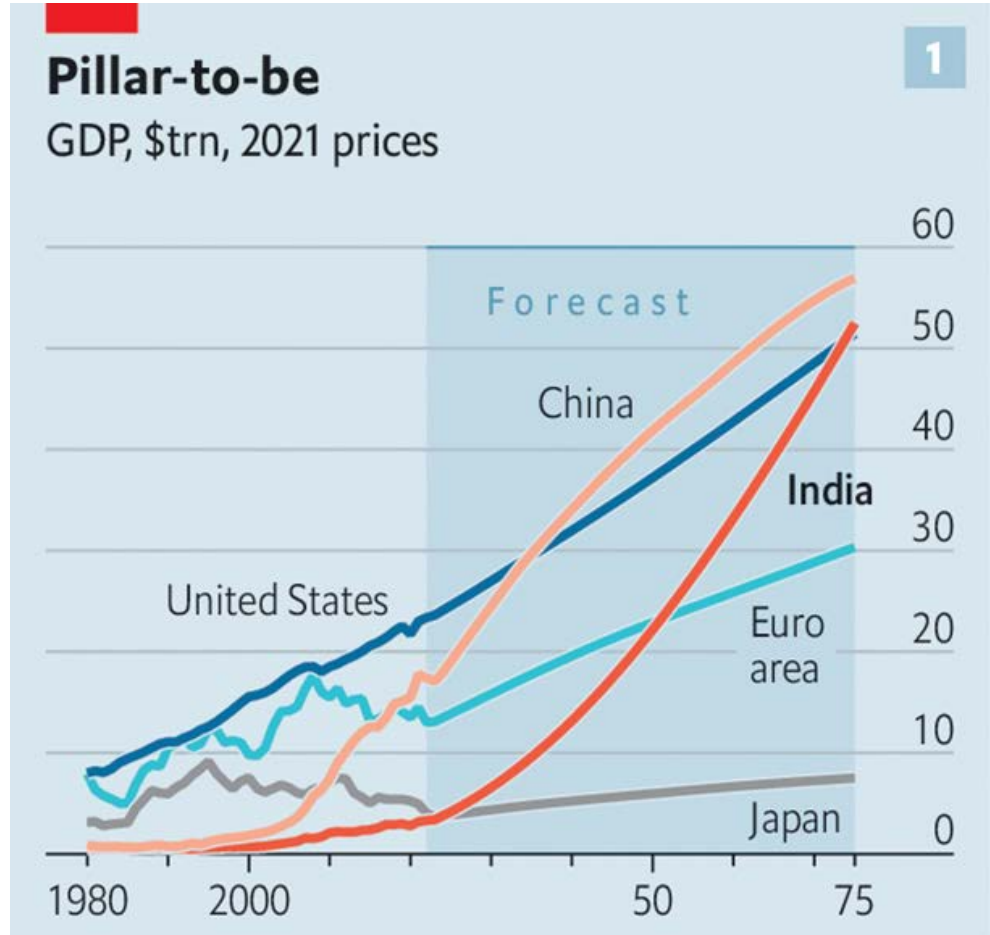
Beijing clearly target of joint statement by Quad group calling for 'stability in Indo-Pacific maritime domain'



Outrageously Simplified Geopolitics

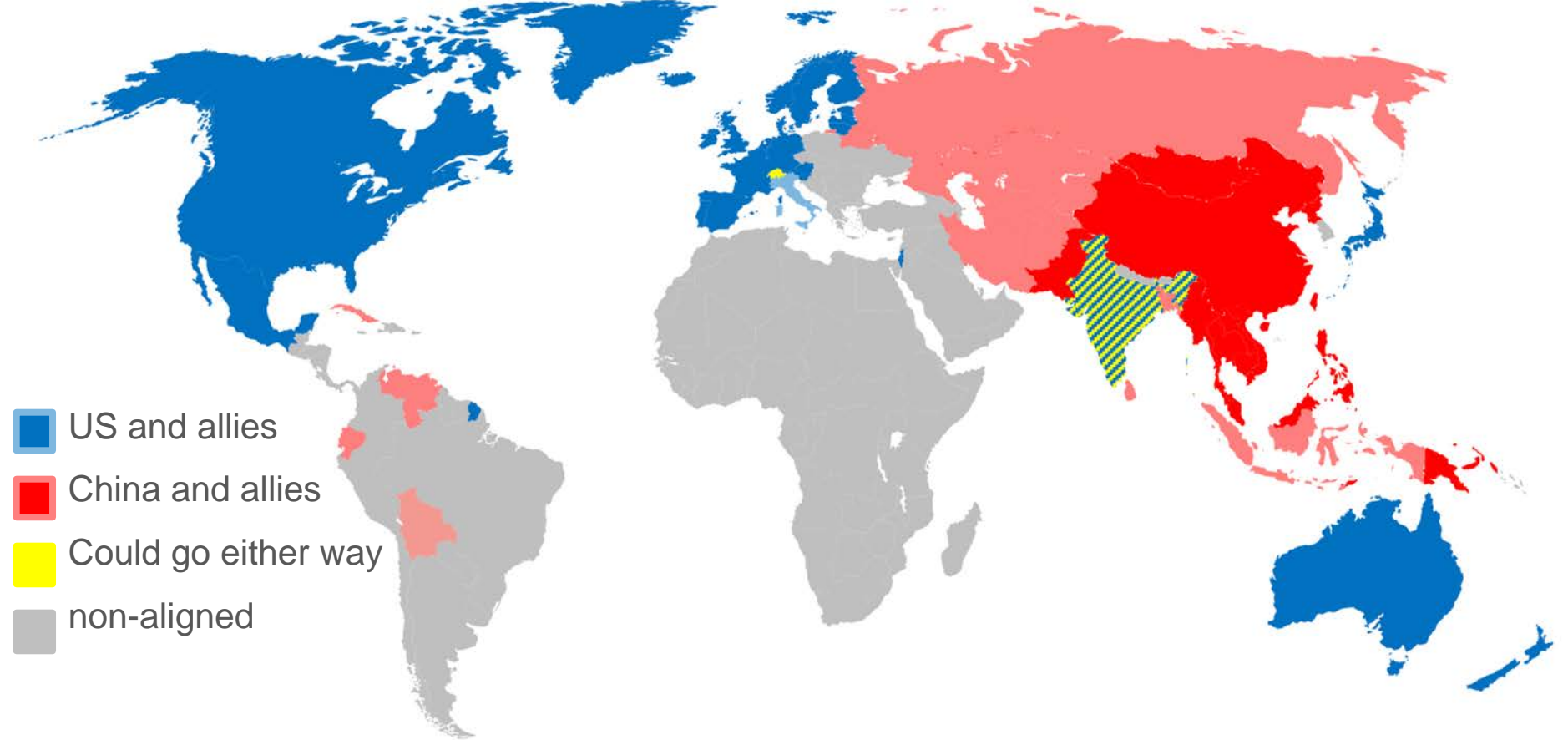


Butter Forecast



Source:
The Economist, <https://www.economist.com/asia/2023/06/13/america-is-courting-india-in-part-for-its-growing-economic-clout>

Decoupling Forecast



What is a **Bloc**-Cipher?

- Not a Typo!

- A **cipher** primarily used *within* a **bloc**

Dictionary

Definitions from [Oxford Languages](#) · [Learn more](#)



cipher¹

/ˈsaɪfə/

noun

1. a secret or disguised way of writing; a code.
"he wrote cryptic notes in a cipher"

Similar:

code

secret writing

coded message

cryptograph

cryptogram



bloc

/blok/

noun

a group of countries or political parties with common interests who have formed an alliance.
"the Soviet bloc"

Similar:

alliance

association

coalition

federation

confederation

league

**"If everything is connected,
everything can be hacked."**







**“If everything is connected,
everything can be hacked.”**

**“We cannot talk about defence,
without talking about cyber.”**

Cryptography = Dual-use Technology

EU General Export Authorisations (EUGEAs):

EU General Export Authorisations (EUGEAs) allow exports of dual-use items to certain destinations under certain conditions (see Annex II of the Regulation). Regulation (EU) 2021/821 provides for the following EUGEAs:

- exports to Australia, Canada, Iceland, Japan, New Zealand, Norway, Switzerland, Liechtenstein, the United Kingdom and the United States of America;
- export of certain dual-use items to certain destinations;
- export after repair/replacement;
- temporary export for exhibitions or fairs;
- telecommunications;
- chemicals;
- intra-group technology transfers, and;
- encryption.



Source:
European Commission, https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en
BIS, <https://www.bis.doc.gov/index.php/policy-guidance/encryption>

Cryptography = Strategic Capability

- 1,000 researchers
- 500M\$ annual budget?
- 10 research centres



develop the most advanced,
disruptive technological
innovations

- Advanced materials
- Directed energy
- AI and Digital Science
- Propulsion and space
- Autonomous robotics

- Quantum
- Biotechnology
- Renewable and sustainable energy
- Cryptography
- Secure systems

Problem: CRQC



FJJ B 1 0023 XNJ
9EJNU 1 0023 XNJ
9JWMJJXJ 1 0023 XNJ
UUY2GVAREQCA 1 0023 XNJ
E88WHJEI88RIKFJ 1 0023 XNJ
PPRORUTNNTMCNBDGTE 1 0023 XNJ
662HEJJD 1 0023 XNJ
JYAEWMXPOLNAOD 1 0023 XNJ
KWKHYCEN10 1 0023 XNJ
XUQVO 1 0023 XNJ
E0 1 0023 XNJ

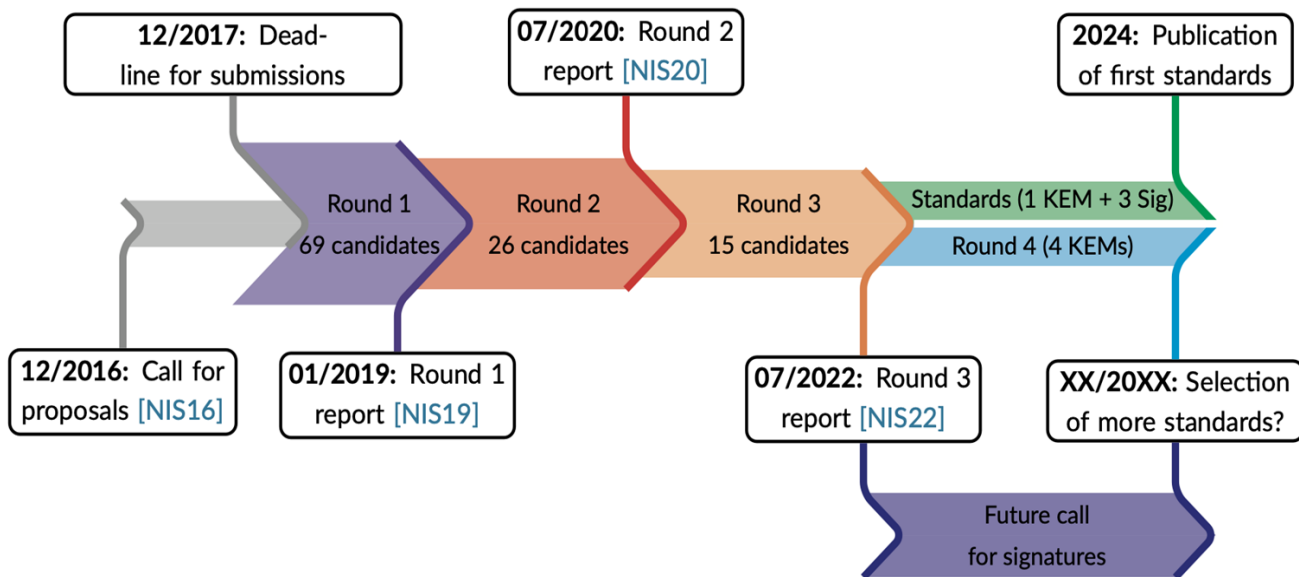


Polynomial-Time Algorithms for Prime Factorization
and Discrete Logarithms on a Quantum Computer*

Peter W. Shor[†]



Solution 1: NIST PQC Competition

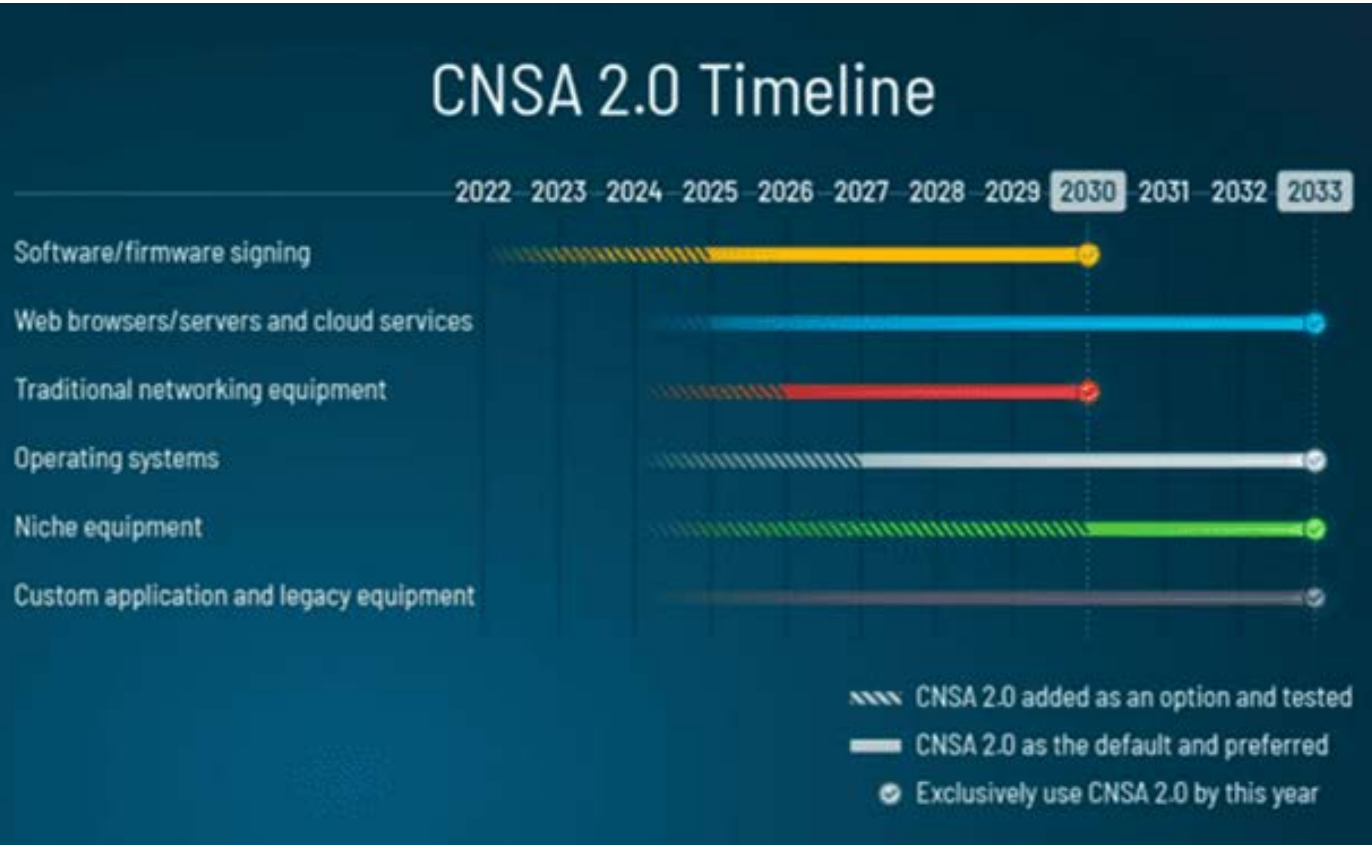


- FIPS 203 ML-KEM (*Kyber*)
- FIPS 204 ML-DSA (*Dilithium*)
- FIPS 205 SLH-DSA (*Sphincs+*)
- FIPS 206? FN-DSA (*Falcon*)

Previous crypto competitions

- AES
- SHA3
- ASCON

Solution 2 : CNSA2.0



- ML-KEM
(*Kyber*)
- ML-DSA
(*Dilithium*)
- LMS/HSS
- XMSS/XMSS^{MT}

More algorithms, more complexity

China, Russia to Adopt 'Slightly Different' PQC Standards From US



Nancy Liu | Editor

October 19, 2022 6:00 PM

Share this article:



Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie



- Aigis-Sig
- Lac.PKE
- Aigis-Enc

- FrodoKEM
- McEliece
- ...

Source:

<https://www.sdxcentral.com/articles/analysis/china-russia-to-adopt-slightly-different-pqc-standards-from-us/2022/10/>

Birth of the BLOC-Cipher

- New algorithms are already more complex and resource-hungry than RSA/ECC
- Supporting geography-dependent algorithms increases pains
 - More complex
 - More (prohibitively?) expensive
 - Less efficient
- It is desirable to support less algorithms
 - Being compatible across *blocs* is penalized
 - Staying inside blocs is incentivized

Cryptography is another differentiator between *blocs*

Geopolitics

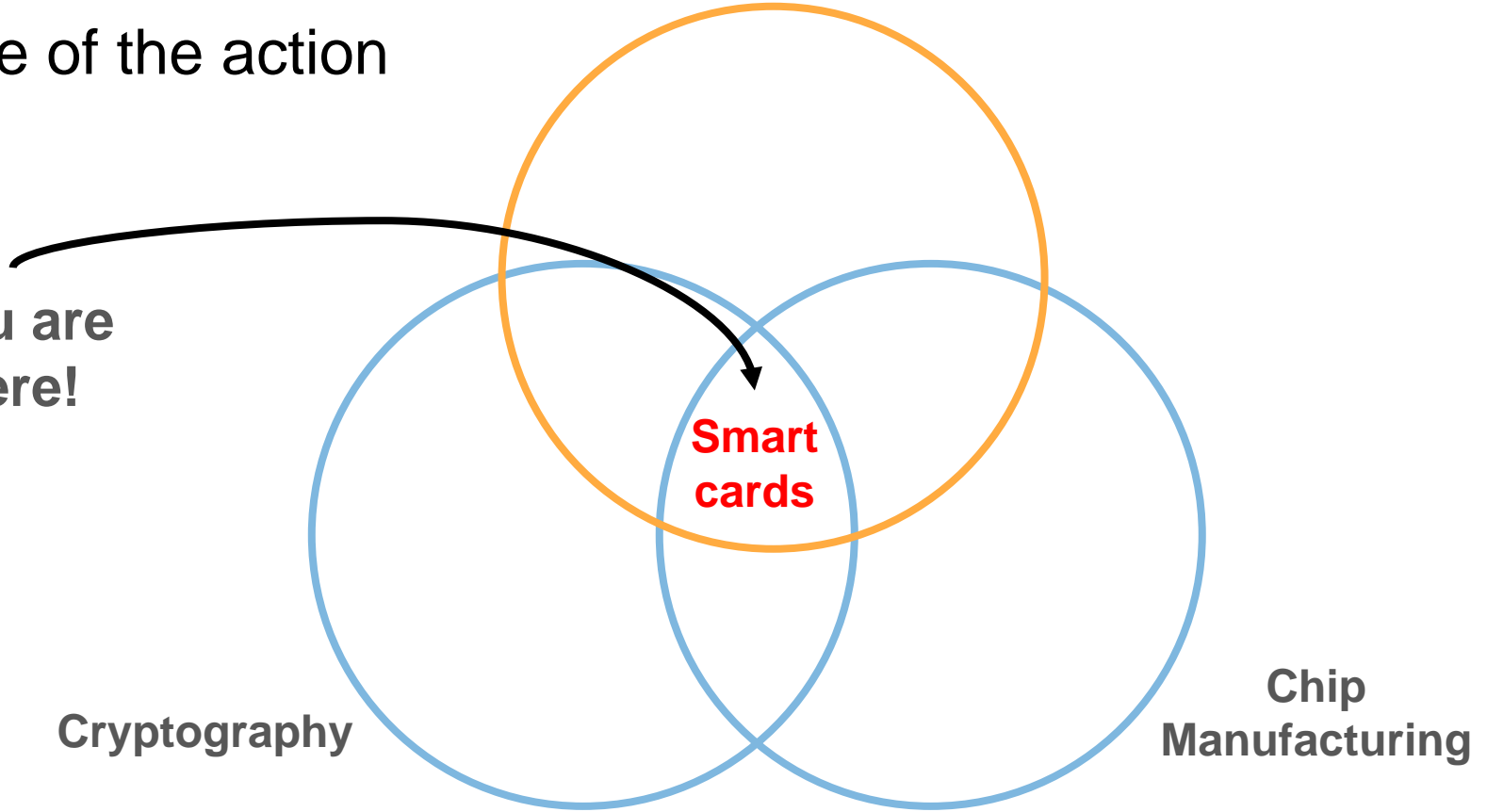
Centre of the action

You are
here!

Smart
cards

Cryptography

Chip
Manufacturing



Key take aways

Research policy NWO › Themes › International Collaboration › Knowledge security

Knowledge security

Knowledge security is primarily about preventing the undesired transfer of sensitive knowledge and technology. An undesired transfer of knowledge occurs when our national security is at risk. In addition, knowledge security focuses on the covert influence of state actors on education and research. Such interference threatens academic freedom and social safety. Knowledge security also involves ethical issues that may arise in cooperation with countries that do not respect fundamental rights.

Much of our prosperity is due to (international) scientific cooperation. At the same time, geopolitical power shifts are taking place, with economics and security intertwined. In this context, knowledge

Major geopolitical changes are currently happening with increasing separation into spheres of influence (*friendshoring, decoupling*)

Guns and Butter

Cryptography and chip manufacturing are

- Dual-use technologies
- Strategic capabilities
- Increasingly used in a geopolitical context

Cryptography standard selection

- Is influenced by geopolitics
- Adds to decoupling

Thank you for your attention!

Dr. Axel Y. Poschmann

<https://www.linkedin.com/in/dr-axel-york-poschmann>

X @stylenerd