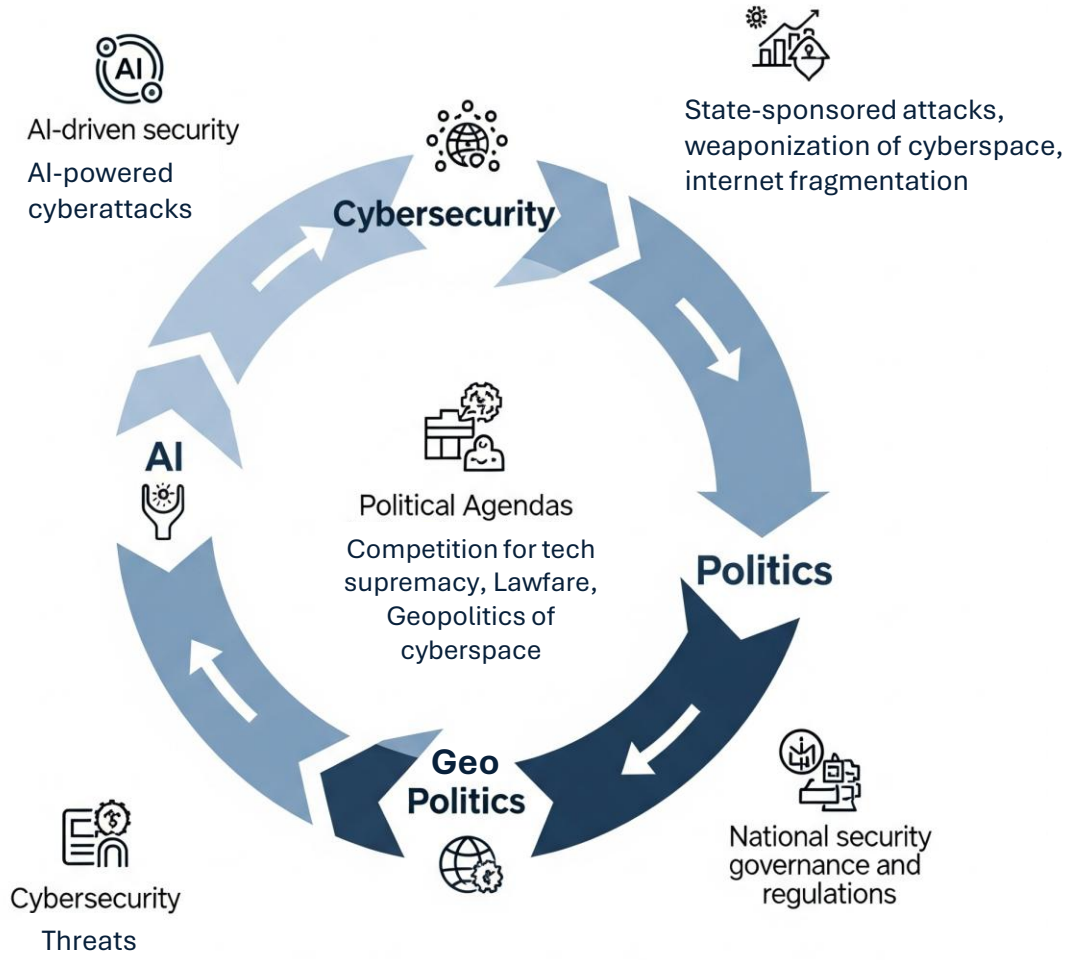
AI & Politics...
& Cyber...
& Technopolarity

Filipe Domingues
Co-founder & Director
June 6th 2025

Interconnected Realms

Cycle of impact



center for cooperation in cyberspace

Interconnected Realms

Cycle of impact

Not FIMI
Not Deep Fakes
Not Job Replacement
Not the AI-Armaggedon

Cybersecurity

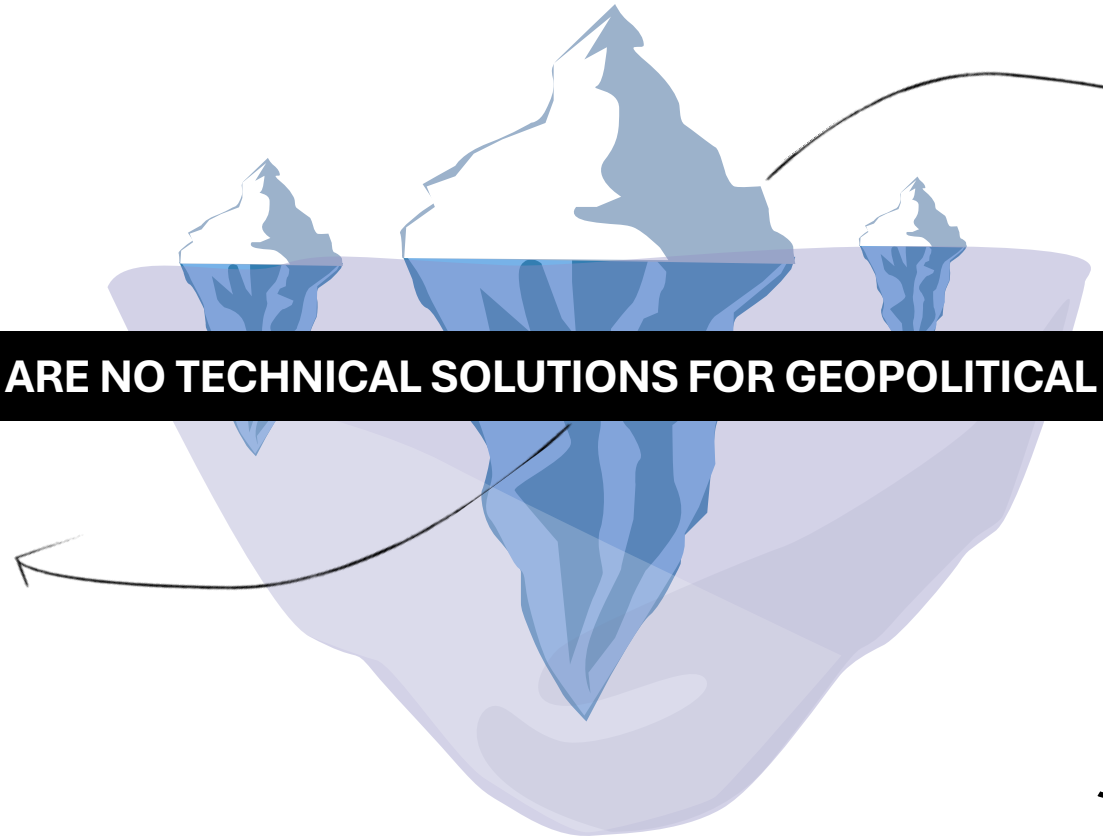
The #1 AI-related concern among experts today

AI-powered Social Engineering

center for cooperation in cyberspace

The convergence between geopolitics and cyberspace

The same power struggle, fought differently



This is what we see:
Unstoppable growth of cybercrime, as well as of the digital divide. Regulatory enthusiasm.

THERE ARE NO TECHNICAL SOLUTIONS FOR GEOPOLITICAL PROBLEMS

This is the Real Problem:
Lack of trust resulting from competition between great powers and the absence of international governance.

The problem area:
Serious risks to international security and global connectivity.

center for cooperation in cyberspace

The convergence between geopolitics and cyberspace

Power, not profit, is emerging as the real driver

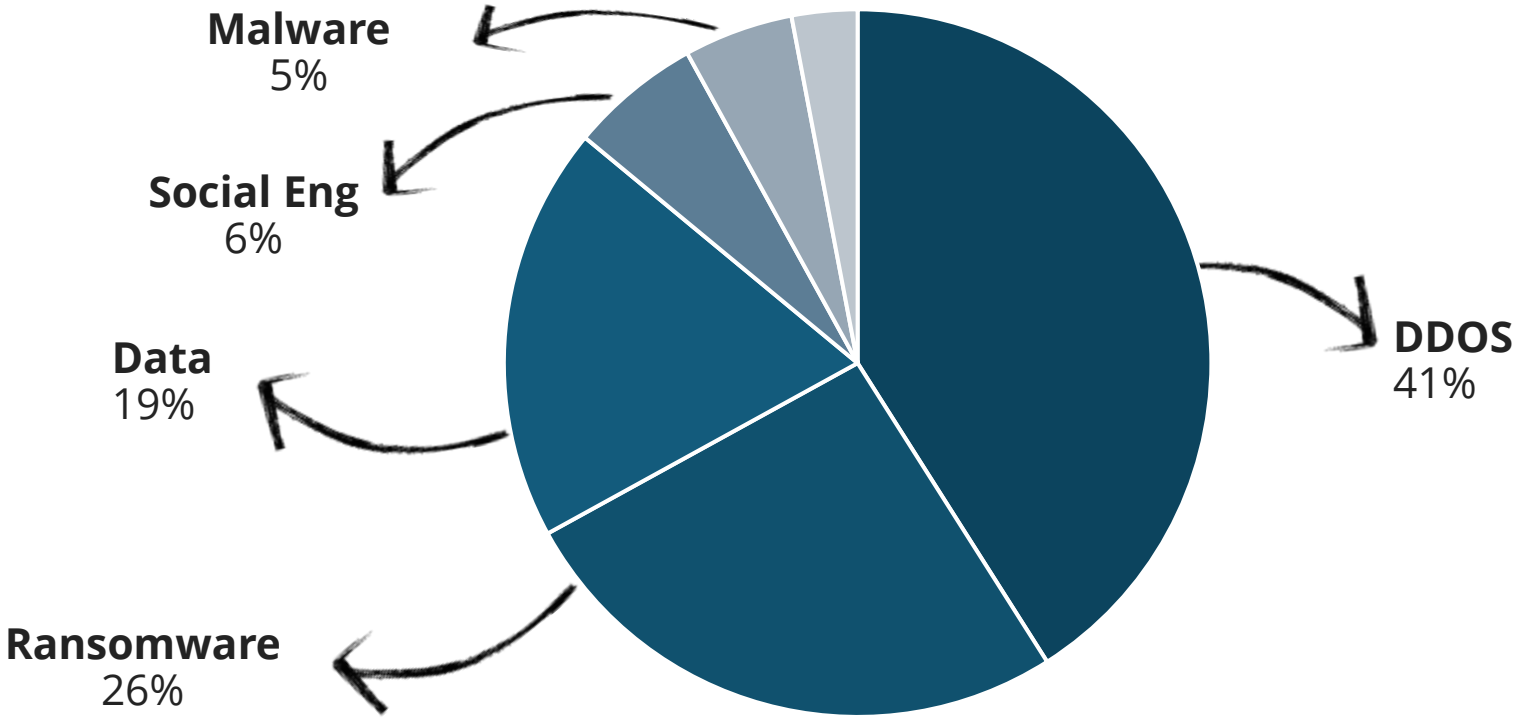
MOTIVATIONAL GRID

Financially Motivated	Geopolitically Motivated	Ideologically Motivated
Ransomware groups	State-sponsored groups	Hacktivists
Fraudsters & Botnet operators	Cyber mercenaries	Terrorist organizations
MONEY-DRIVEN	POWER-DRIVEN	VALUES-DRIVEN

center for cooperation in cyberspace

The convergence between geopolitics and cyberspace

EU: Incidents by threat type



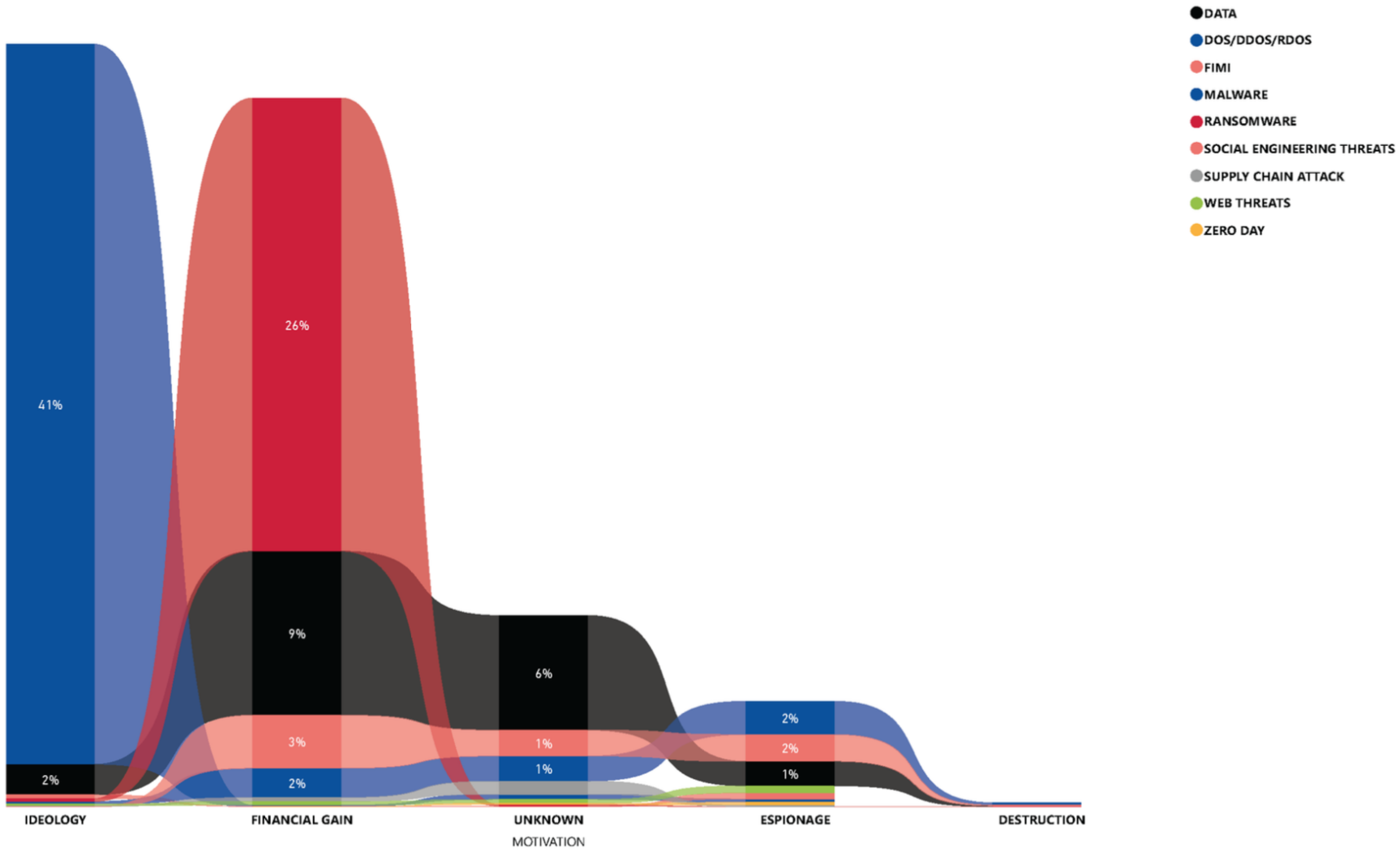
Source: ENISA Threat Landscape 2024

center for cooperation in cyberspace

The convergence between geopolitics and cyberspace

Power, not profit, is emerging as the real driver

MOTIVATION PER THREAT CATEGORY

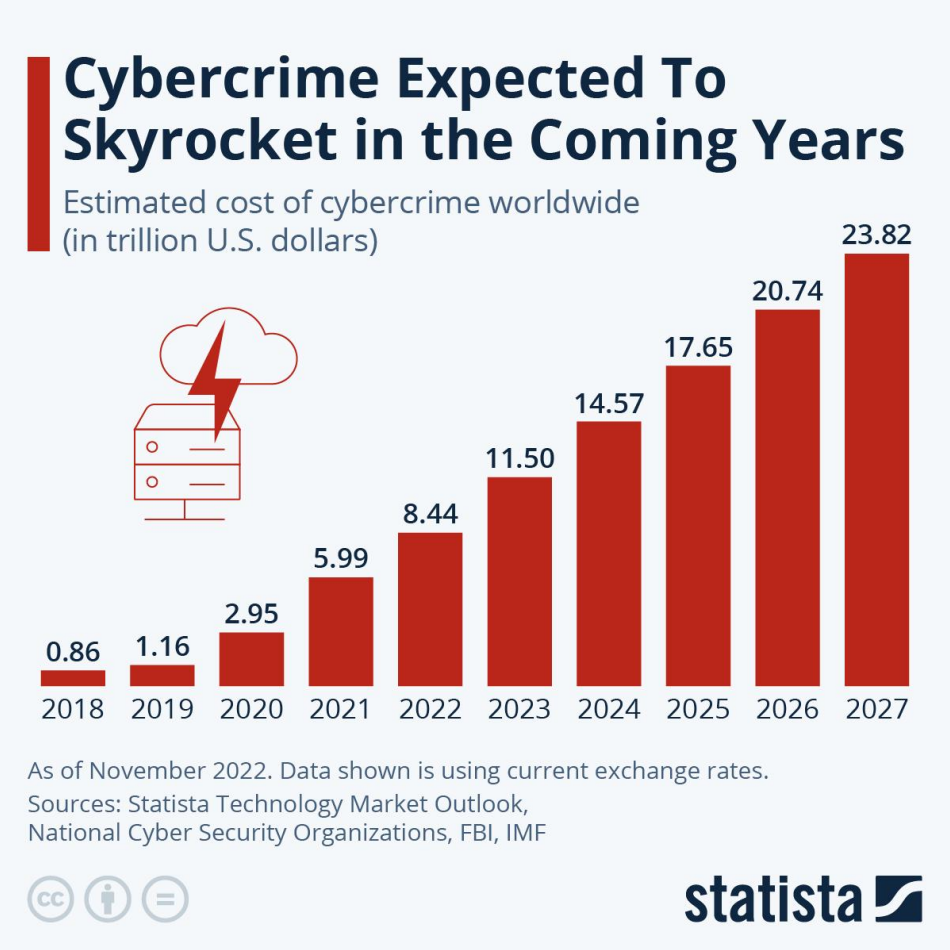


Source: ENISA Threat Landscape 2024

center for cooperation in cyberspace

The cybercrime ecosystem

Authorities are on a treadmill: pouring in more resources, yet falling further behind



- ❑ The third-largest “economy” in the world
- ❑ Cybercrime now costs more than natural disasters
- ❑ More profitable than the global drug trade

center for cooperation in cyberspace

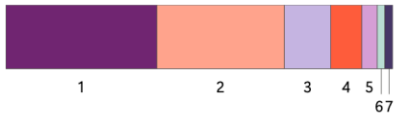
Atlas of cyberattacks

Aggressions in cyberspace have a clear geopolitical context

China

Nation state threat actor activity

Targeting by region

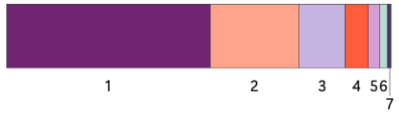


	Sector	Percentage
1	East Asia & Pacific	39%
2	North America	33%
3	Europe & Central Asia	12%
4	Latin America & Caribbean	8%
5	South Asia	4%
6	Middle East & North Africa	2%
7	Sub-Saharan Africa	2%

Iran

Nation-state threat actor activity

Targeting by region

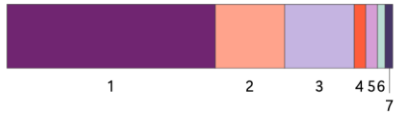


	Sector	Percentage
1	Middle East & North Africa	53%
2	North America	23%
3	Europe & Central Asia	12%
4	South Asia	6%
5	East Asia & Pacific	3%
6	Latin America & Caribbean	2%
7	Sub-Saharan Africa	1%

North Korea

Non-state threat actor activity

Targeting by region



	Sector	Percentage
1	North America	54%
2	East Asia & Pacific	18%
3	Europe & Central Asia	18%
4	Latin America & Caribbean	3%
5	Middle East & North Africa	3%
6	South Asia	2%
7	Sub-Saharan Africa	2%

Russia

Nation state threat actor activity

Targeting by region

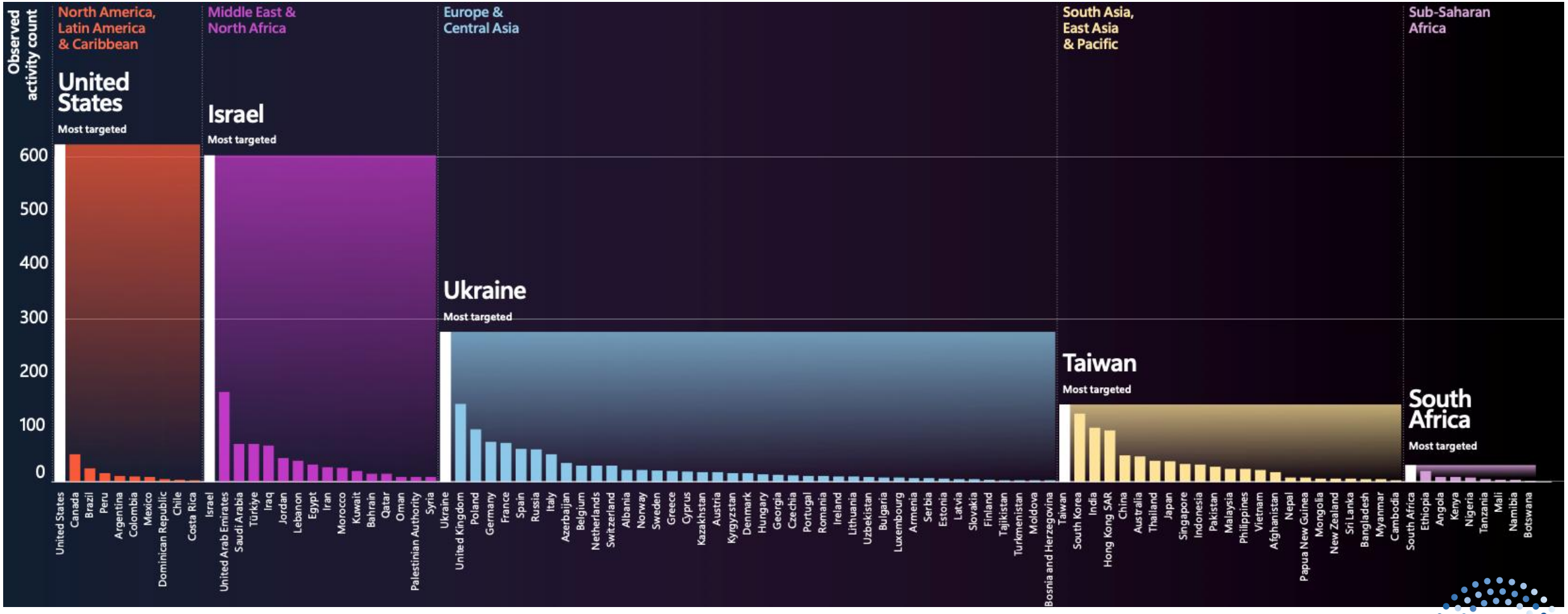
	Sector	Percentage
1	Europe & Central Asia	68%
2	North America	20%
3	Middle East & North Africa	5%
4	East Asia & Pacific	3%
5	Latin America & Caribbean	3%
6	South Asia	1%
7	Sub-Saharan Africa	1%

Source: Microsoft Digital Defense Report 2024

center for cooperation in cyberspace

Atlas of cyberattacks

Aggressions in cyberspace have a clear geopolitical context



Source: Microsoft Digital Defense Report 2024

center for cooperation in cyberspace

April 2022

Entire governments held hostage - assault on the nation's digital infrastructure: 30 government institutions, causing daily losses of approximately $30 million.

Ransomware = National Emergency

Conti

US State Dept

"FOR COSTA RICA"

https://www.hacienda.go.cr/
https://www.mtss.go.cr
https://fodesaf.go.cr
https://siua.ac.cr

Conti is primarily a community of people who understand information security. and we believe that we understand it very well, I want to say: we stop any actions against Costa Rica (any attacks on this country are not considered our actions) w e believe that the country is so aware of the views of the United States that the Americans simply sacrifice it in this regar d. why not just buy a key? I do not know if there have been cases of entering an emergency situation in the country due t o a cyber attack? In a week we will delete the decryption keys for Costa Rica

I appeal to every resident of Costa Rica, go to your government and organize rallies so that they would pay us as soon as possible if your current government cannot stabilize the situation? maybe it's worth changing it?

center for cooperation in cyberspace

The convenience of cyber warfare

Low-cost, hard to trace, and in a legal vacuum

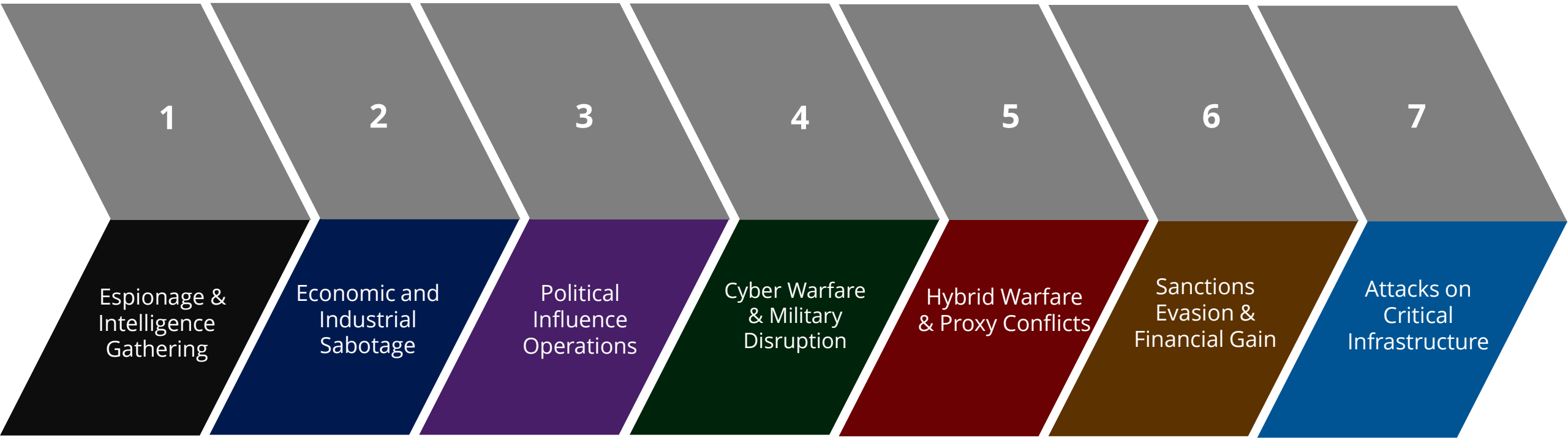
Cheap weapon	When compared to conventional weapons, cyber tools are incredibly more cost-effective for causing damage or disruption.	*Edge 1*
Remote and **Anonymous**	Cyberspace enables powerful actors to strike from anywhere on the planet without a clear signature, making attribution extremely challenging.	*Edge 2*
Lawlessness field	**The lack and the overlap of international regulation** makes it difficult for law enforcement agencies to track and apprehend cybercriminals.	*Edge 3*
A **versatile** tool	Cyberwarfare enables a wide range of operations, **blurring the lines between war, sabotage and influence.**	*Edge 4*

center for cooperation in cyberspace

The convenience of cyber warfare

Broad spectrum of operations available

"[by targeting critical infrastructures] State-sponsored cyber attacks **undermine the very foundations of our societies** and economies" - Gen Nakatani, Japanese Defense Minister | May 30th 2025



center for cooperation in cyberspace

The convenience of cyber warfare

A growing **attack surface**

Chemical sector

Commercial facilities

Communications

Critical manufacturing

Financial services

What about Election Integrity?

Food and agriculture

Government facilities

Health care and public health

Dams

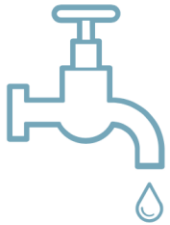
Defense industrial bases

Emergency services

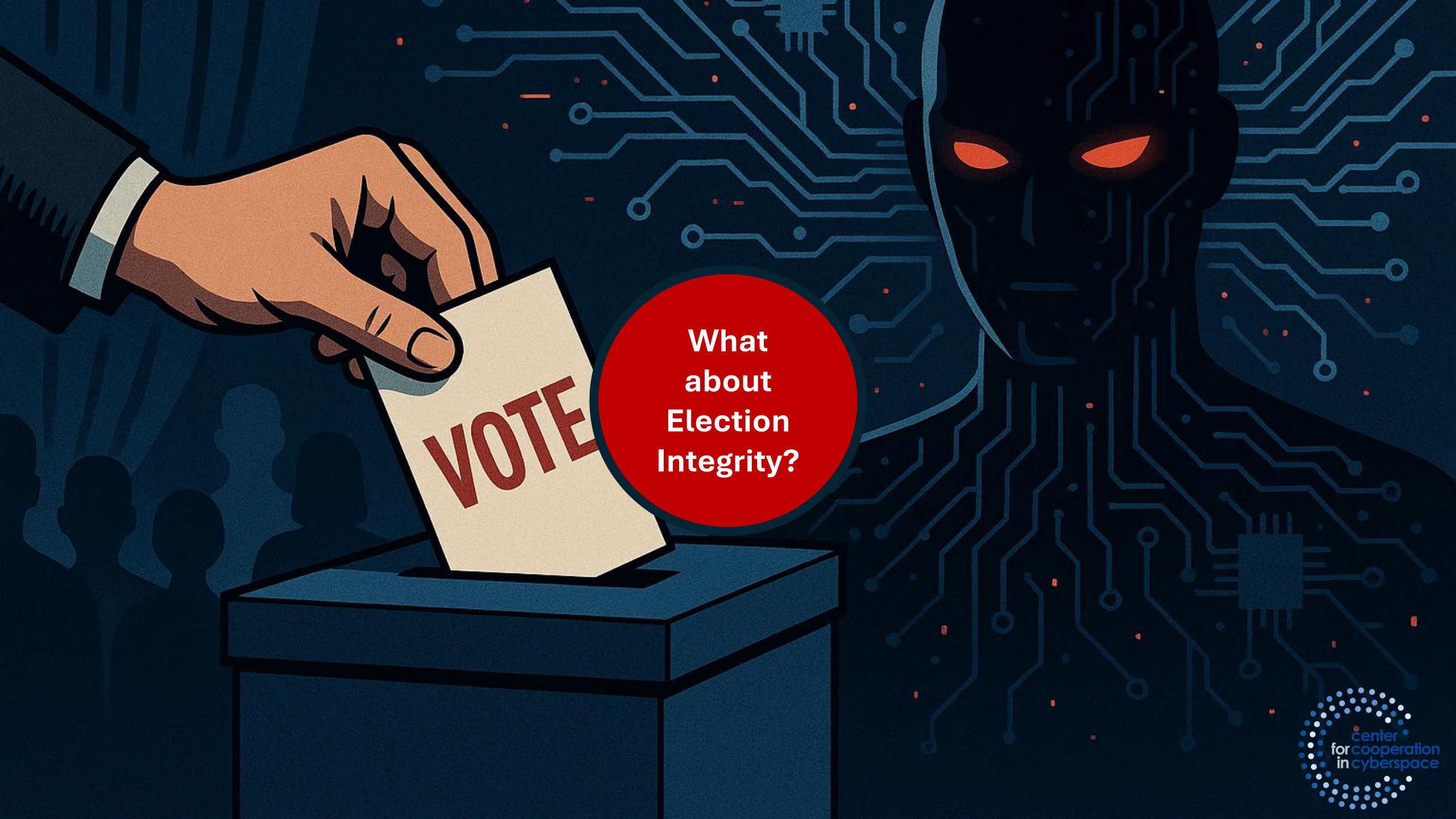
Nuclear reactors, materials and waste

Transportation systems

Water and wastewater systems



center for cooperation in cyberspace

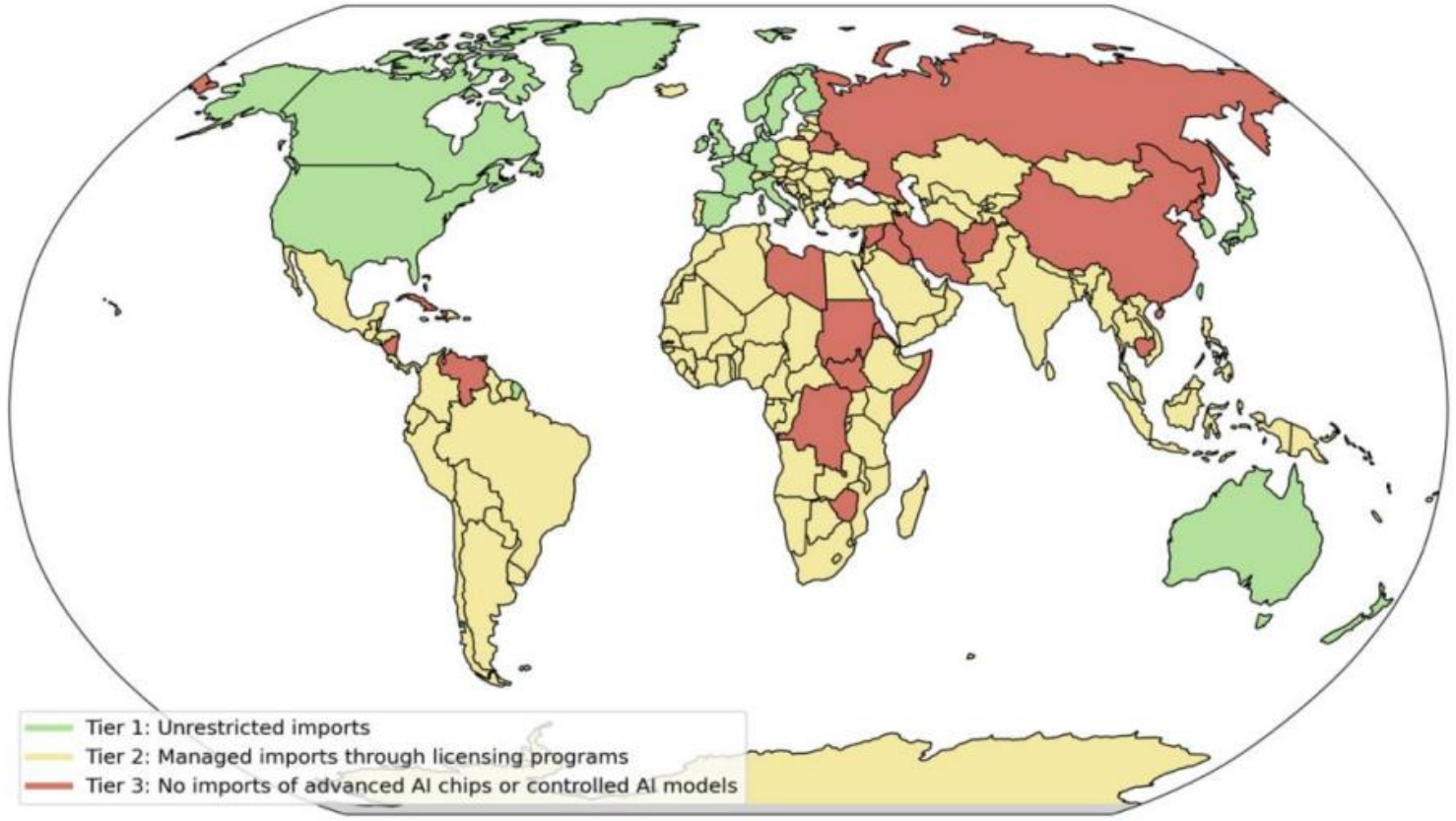

VOTE
What about Election Integrity?
center for cooperation in cyberspace

The EU AI Act - Risk-Based Approach:

Minimal	Limited	High	Unacceptable
			Manipulative AI: use of subliminal, manipulative, or deceptive techniques to distort the behavior of individuals or groups or influence their capacity to make informed decisions.
			Predictive Policing: anticipate criminal behavior by profiling individuals based on personal data, such as previous actions and inferred or predicted personality traits
			Social Scoring: use of systems that evaluate or classify individuals based on their civic behavior or inferred personal characteristics. These systems are sometimes used to facilitate or block access to jobs, financial credit, or public services.
			Biometric Identification: AI systems that use biometric data (e.g., facial recognition) for real-time identification, particularly in public spaces or for law enforcement purposes.
			Emotion Recognition: AI systems that infer emotions in contexts like the workplace or educational settings, often without explicit consent from those being monitored.

center for cooperation in cyberspace

The AI Diffusion Framework



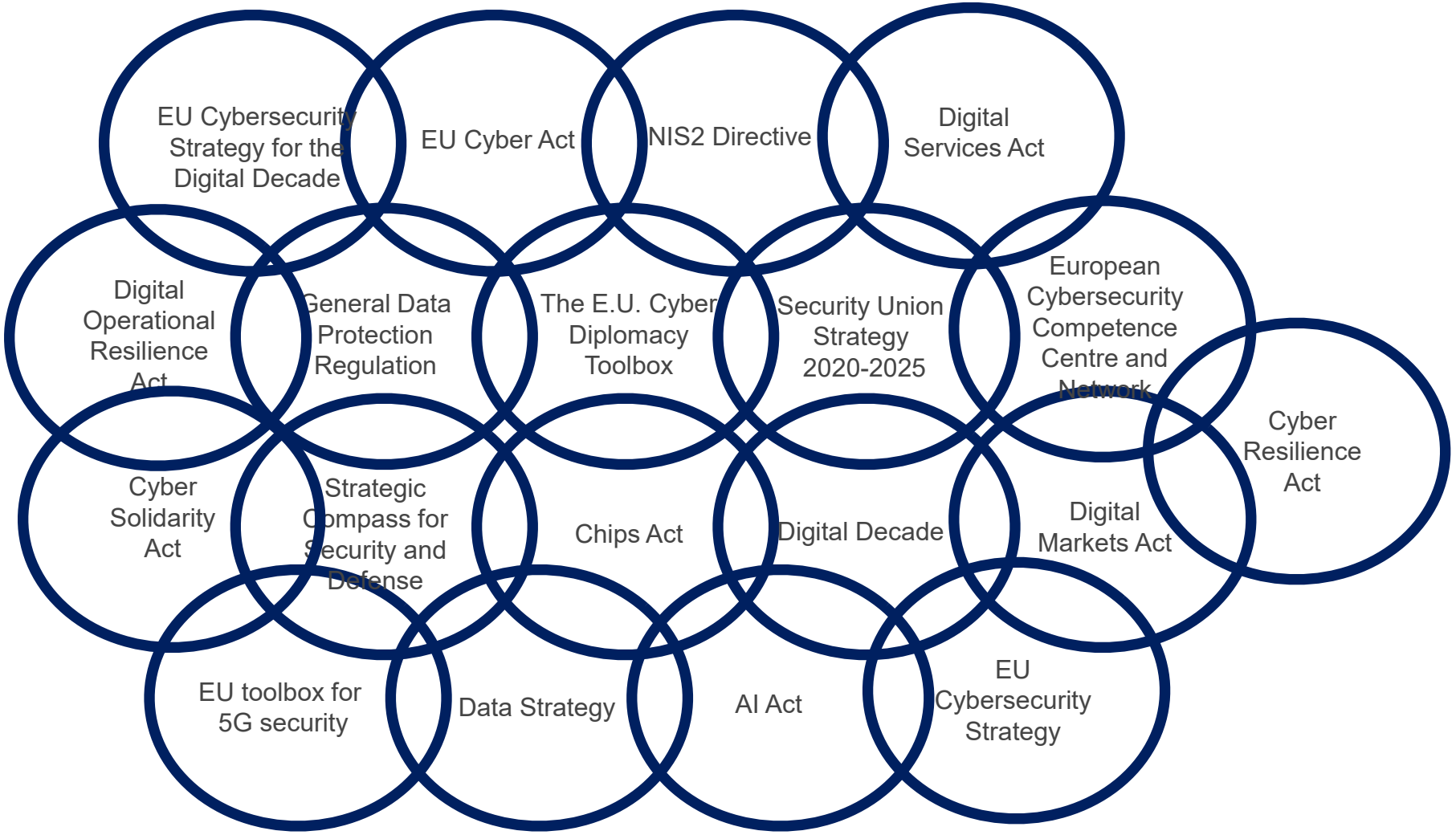
SOURCE: Country list from the framework.
NOTE: The framework divides the world into three tiers, reflecting varying levels of access: Tier 1 (the United States and 18 key partners, shown in green) receives unrestricted access, Tier 2 (most other nations, shown in yellow) receives controlled access through licensing programs, and Tier 3 (strategic competitors, shown in red) faces continued restrictions from previous export controls implemented in October 2022.

https://www.rand.org/content/dam/rand/pubs/perspectives/PEA3700/PEA3776-1/RAND_PEA3776-1.pdf

center for cooperation in cyberspace

The EU maze of cyber-everything

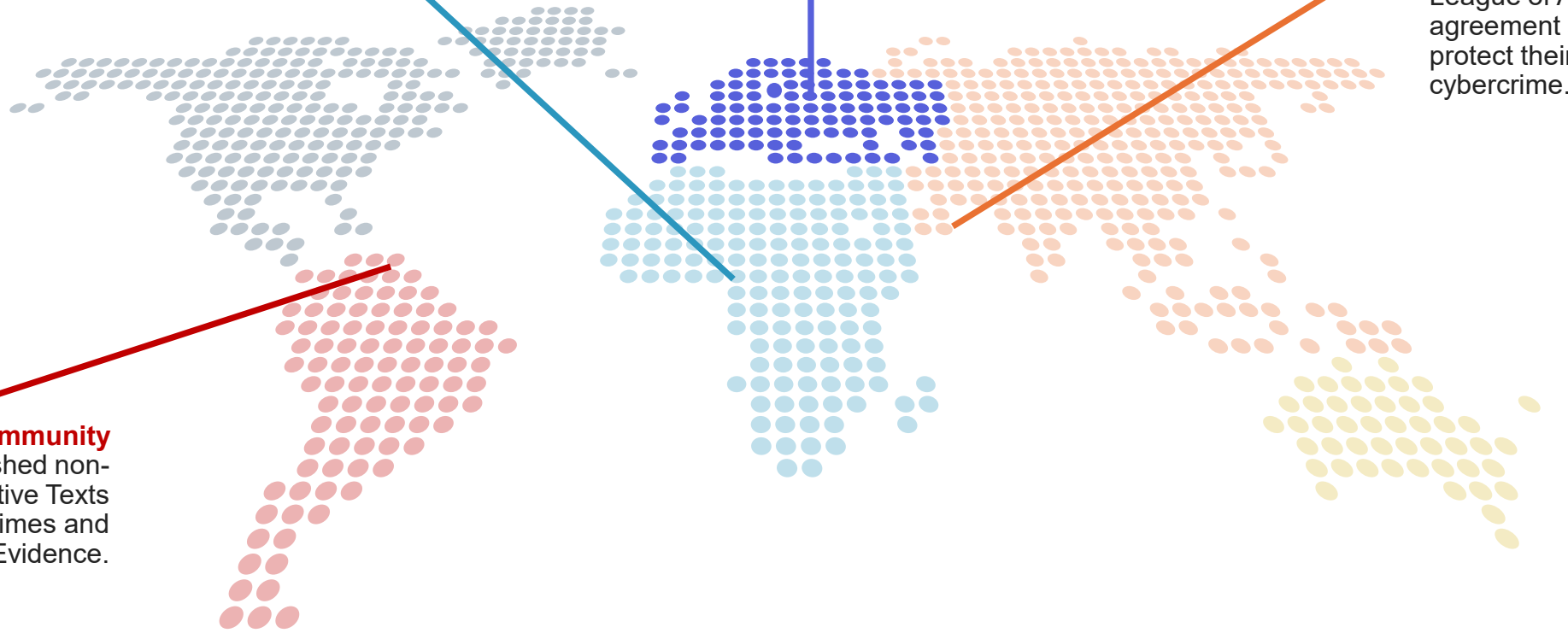
The world's most advanced region in digital regulation…



center for cooperation in cyberspace

A threat to international security

Yet there are no global binding rules



Malabo Convention
Adopted in 2014 and officially known as the African Union Convention on Cyber Security and Personal Data Protection.

Budapest Convention
Council of Europe treaty that seeks to create a framework for the harmonization of laws and cooperation in combating cybercrime.

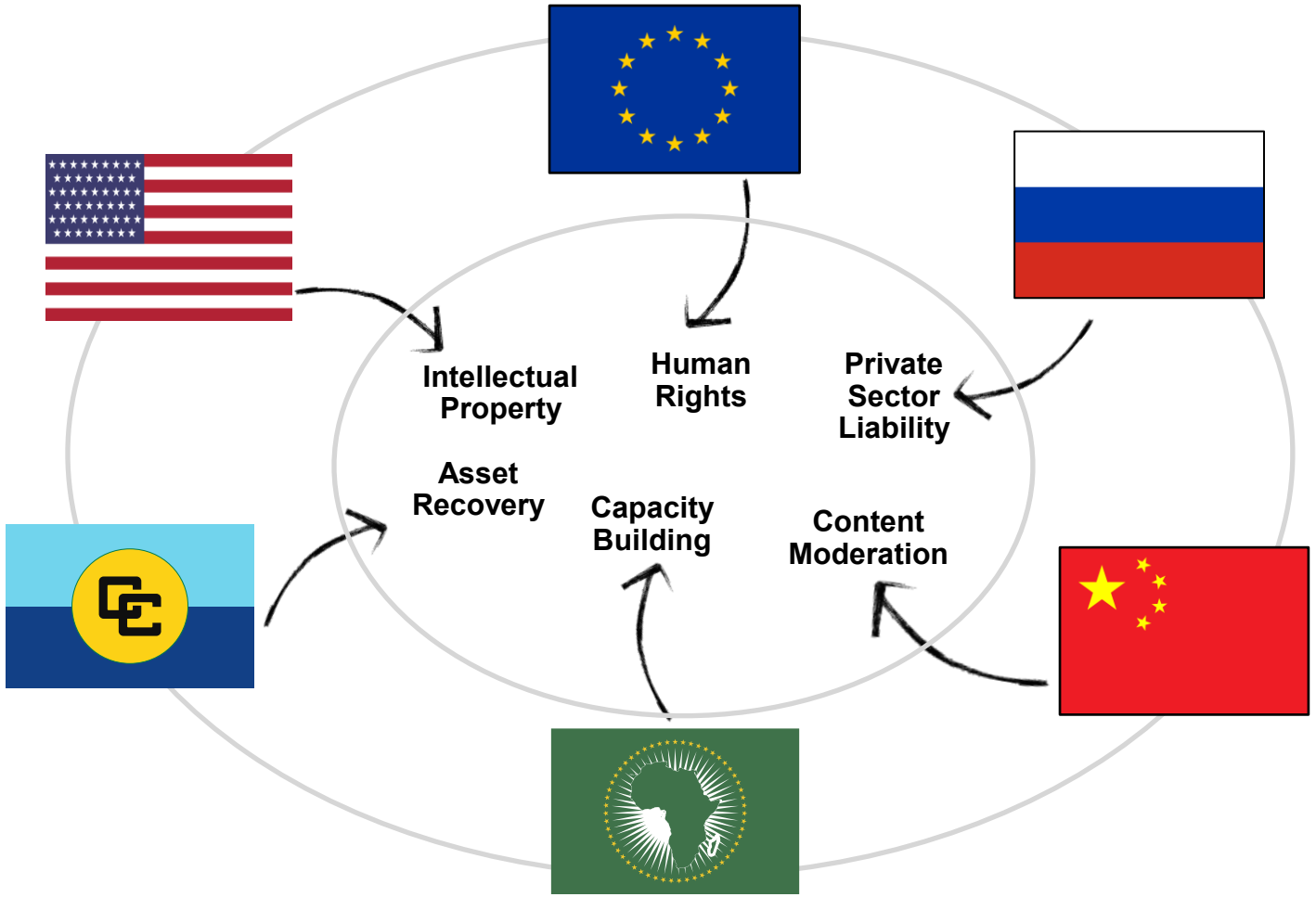
Arab Convention on Combating Tech Offences
Exclusive to members of the League of Arab States, the agreement aims to enable them to protect their interests from cybercrime.

Caribbean Community
CARICOM has established non-binding Model Legislative Texts of Cybercrime, e- Crimes and Electronic Evidence.

center for cooperation in cyberspace

Clash of Civilizations

Regional Divides: Where To Find Minimum Common Ground?



center for cooperation in cyberspace

Technological Neutrality Vs. Clash of Civilizations

Regionalism Replacing Globalism

Fonte: South China Morning Post

PROTECT

The People

The Economy

The State

center for cooperation in cyberspace

Technopolarity

"A technopolar world: one where technology companies wield unprecedented influence on the global stage, where ***sovereignty and influence is determined not by physical territory or military might, but control over data, servers, and, crucially, algorithms****"*

Ian Bremmer, Founder & CEO of the Eurasia Group

center for cooperation in cyberspace

REUTERS/Ann Wang | https://www.reuters.com/technology/like-pop-star-nvidias-ceo-huang-stirs-up-jensanity-taiwan-2024-06-05/

Final Remarks

We are still living the early stages of AI – if we can call it that

Main threat: Cyberattacks

We are already living in a permanent, universal threat ecosystem

These trends reflect a fundamental shift in how conventional and digital aggressors attempt to influence democratic life and election outcomes.

The widespread availability of generative AI tools has turbocharged the creation of sophisticated disinformation, enabling both foreign adversaries and domestic extremists to produce convincing fake content at unprecedented speed, scope and scale.

center for cooperation in cyberspace