Technology – its challenges and opportunities

15.6.2026

Jarno Limnell
Member of Parliament, Finland
Member of NATO-Parliament
Adjunct professor, National Defence University, University of Jyväskylä, University of Tampere
Member of Expert network in World Economic Forum
Doctor of Military Science

Happiest Country in the World!







COFFEE



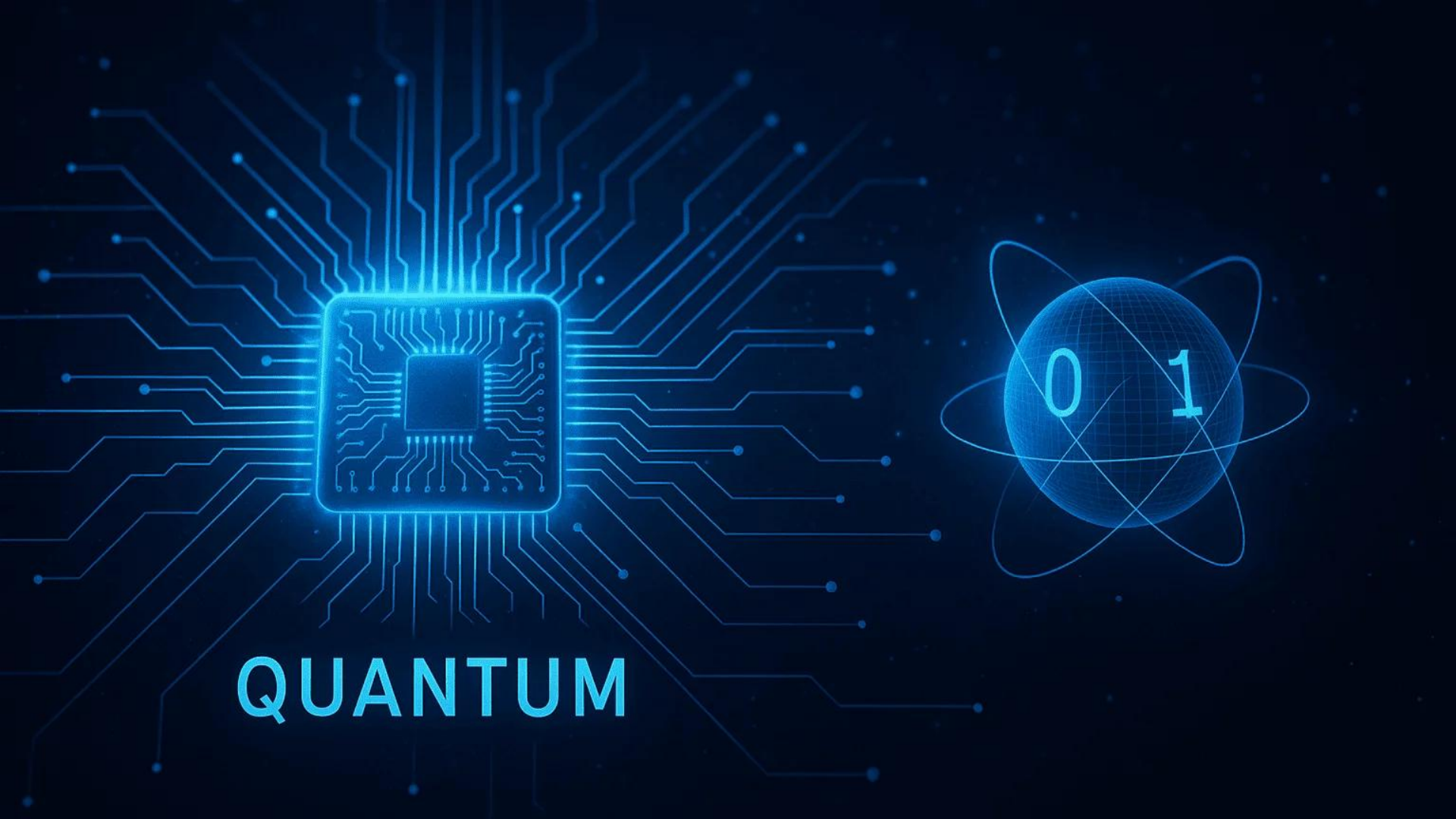

Physical and Digital –
One Security
Technology is integral part of
security policy

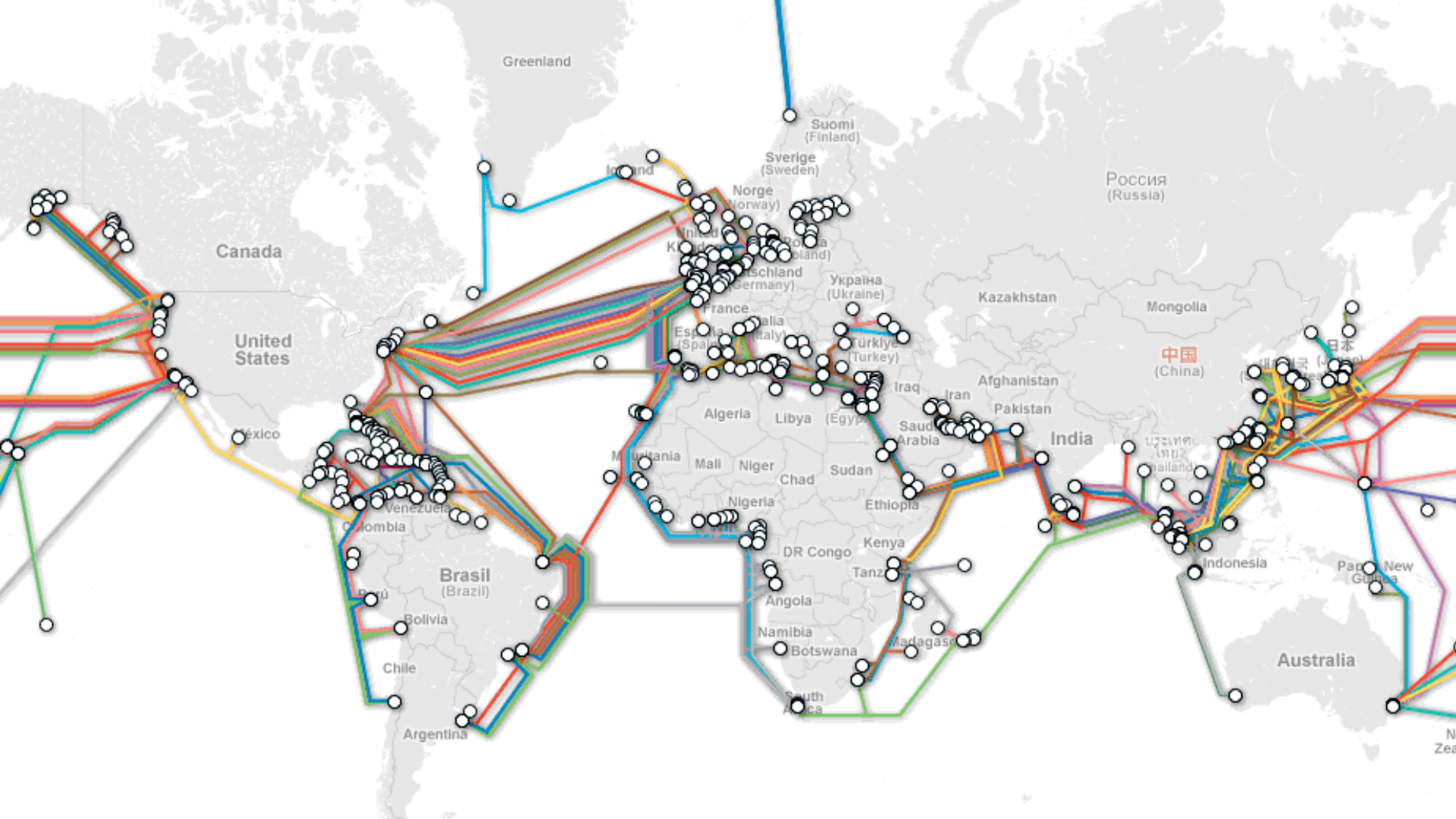
Technology is now developing faster than ever before



What should not be digitalized?



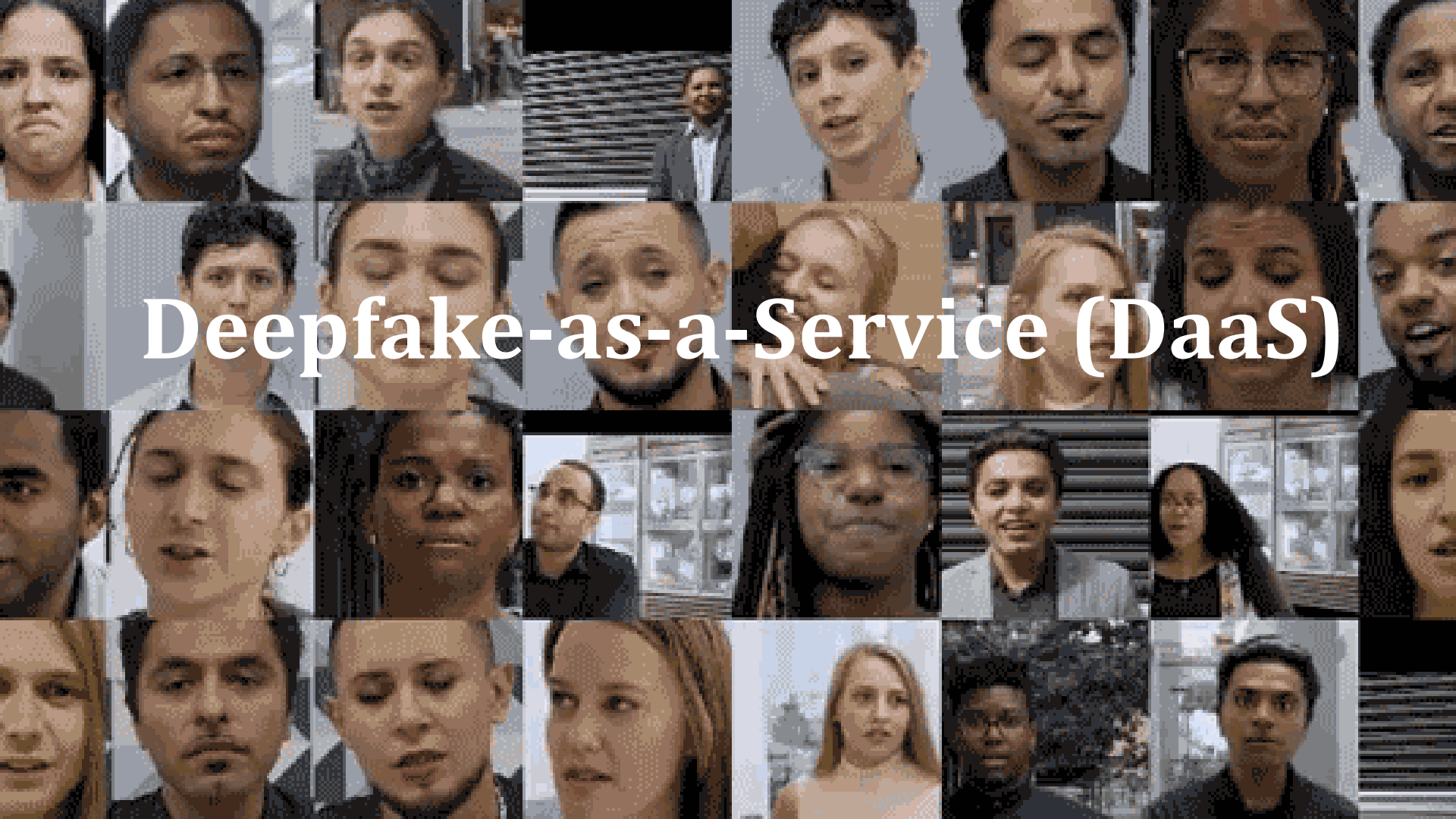

0 1
QUANTUM


Greenland
Canada
United States
México
Venezuela
Colombia
Brasil (Brazil)
Perú
Bolivia
Chile
Argentina
Suomi (Finland)
Sverige (Sweden)
Norge (Norway)
Ísland
Россия (Russia)
Україна (Ukraine)
France
España (Spain)
Italia (Italy)
Türkiye (Turkey)
Kazakhstan
Mongolia
中国 (China)
Iraq
Iran
Afghanistan
Pakistan
India
Saudi Arabia
Algeria
Libya
Mauritania
Mali
Niger
Chad
Sudan
Nigeria
Ethiopia
Kenya
DR Congo
Tanzania
Angola
Namibia
Botswana
Madagascar
Indonesia
Australia


LAND
SEA
AIR
SPACE
CYBER
330
501

The human mind as a battleground – emotions and images

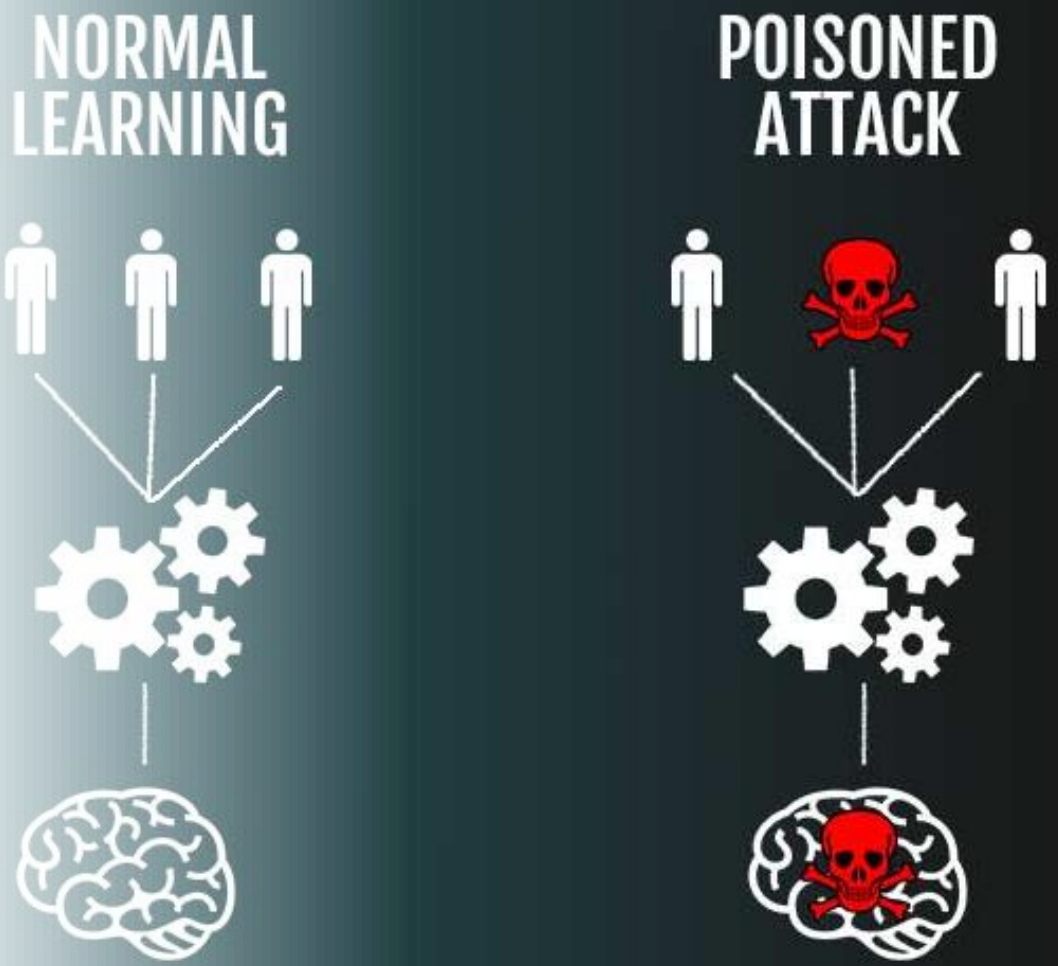



Deepfake-as-a-Service (DaaS)

Datapoisoning

Misleading content is being systematically and abundantly fed into the internet so that algorithms start to process it as normal information.

Trying to modify the system that produces the answers.



1. Technology is now a core element of national power

Control over AI, data, communications, satellites, energy systems and semiconductors increasingly determines a country’s economic strength, military capability and political independence.



2. Every country must identify its critical dependencies

Governments should know which foreign technologies, cloud services, components and supply chains could become pressure points during a crisis. Critical dependencies must be reduced before they are exploited.



3. Artificial intelligence will strengthen both societies and adversaries

AI can raise productivity, improve healthcare and modernise public services. It also enables more effective cyberattacks, deepfakes, surveillance, autonomous weapons and influence operations.



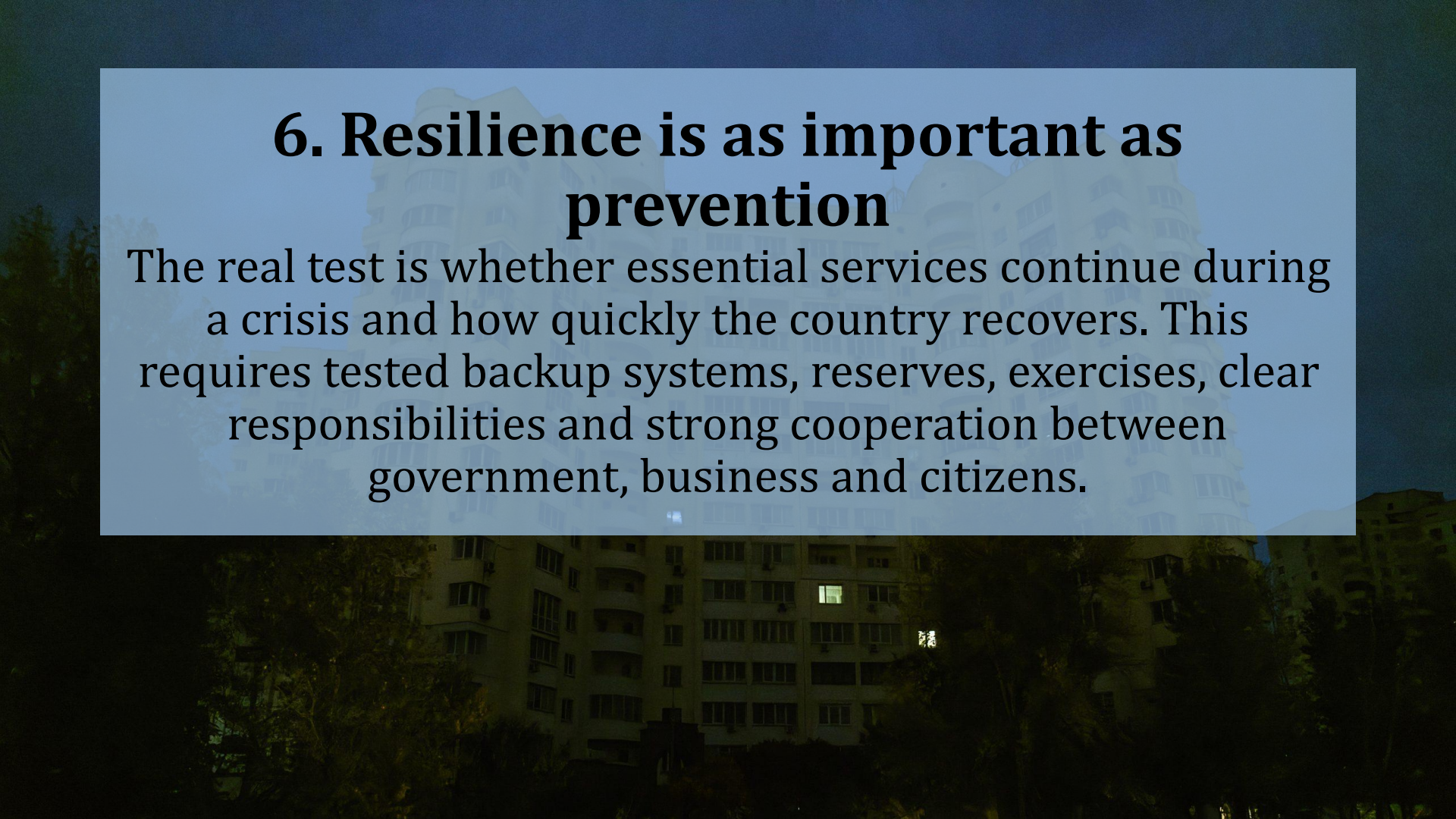
4. Cybersecurity must move from IT departments to national leadership

Cyber risks affect electricity, ports, hospitals, banks, water systems and elections. Boards, ministers and public authorities must treat cyber resilience as a strategic responsibility with regular exercises.



5. Critical infrastructure must be protected against both cyber and physical attacks

The same systems can be targeted through malware, drones, sabotage, insider activity or supply-chain manipulation. Ports, energy networks, telecommunications and data centres require layered protection and close public-private cooperation.



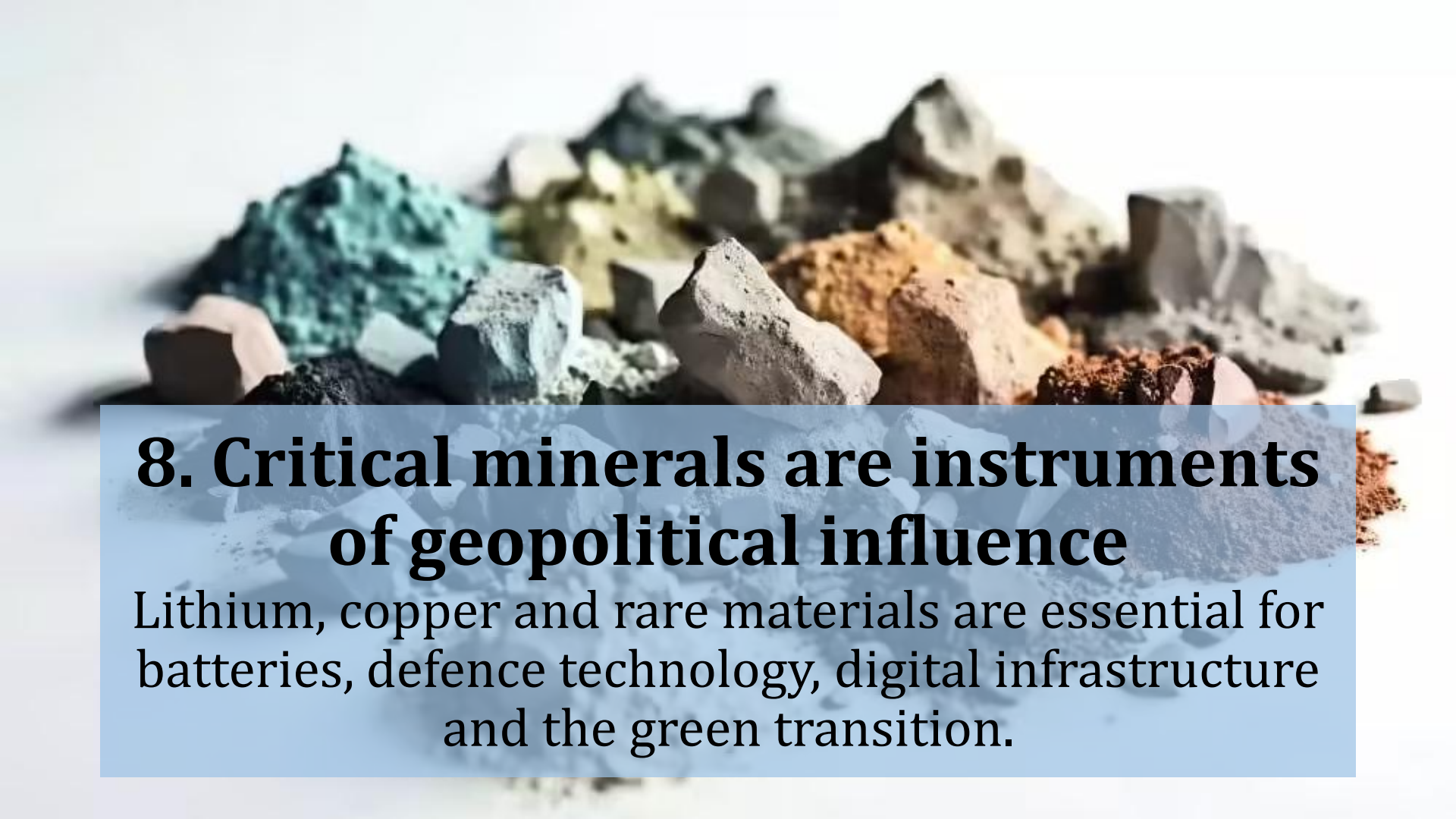
6. Resilience is as important as prevention

The real test is whether essential services continue during a crisis and how quickly the country recovers. This requires tested backup systems, reserves, exercises, clear responsibilities and strong cooperation between government, business and citizens.



7. Technology must be developed around people

Human-centric technology means that systems are safe, understandable, accessible and accountable. People must know when AI is used, who is responsible for decisions and how those decisions can be challenged.



8. Critical minerals are instruments of geopolitical influence

Lithium, copper and rare materials are essential for batteries, defence technology, digital infrastructure and the green transition.

9. Democracies must act faster than technological disruption

Legislation cannot always move at the speed of innovation, but democratic decision-making cannot remain permanently behind.

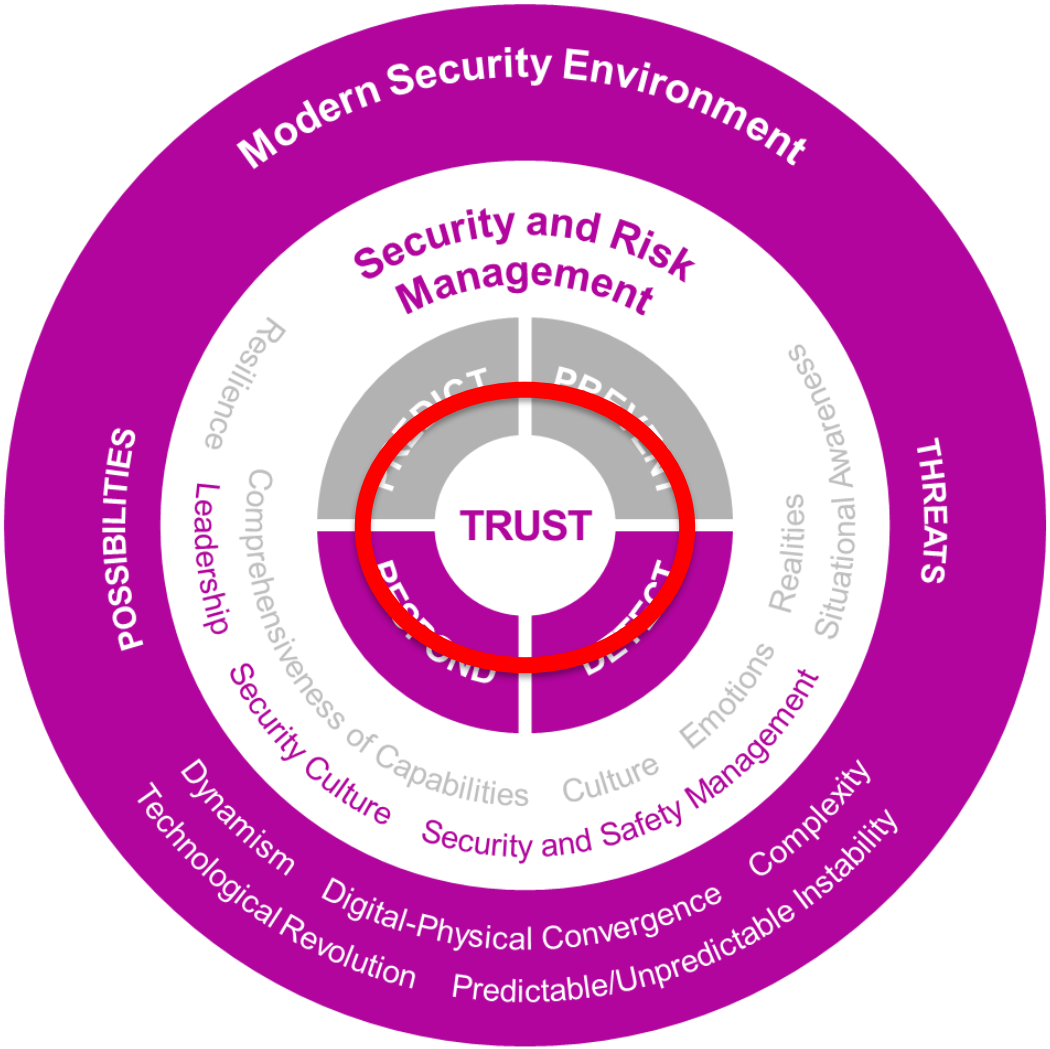


(State Dept./D. Thompson)



10. Technological development requires clear ethical principles

Not everything that is technically possible should automatically be implemented. Ethical assessment must be part of technology development from the beginning, especially in AI, biotechnology, surveillance and autonomous systems.

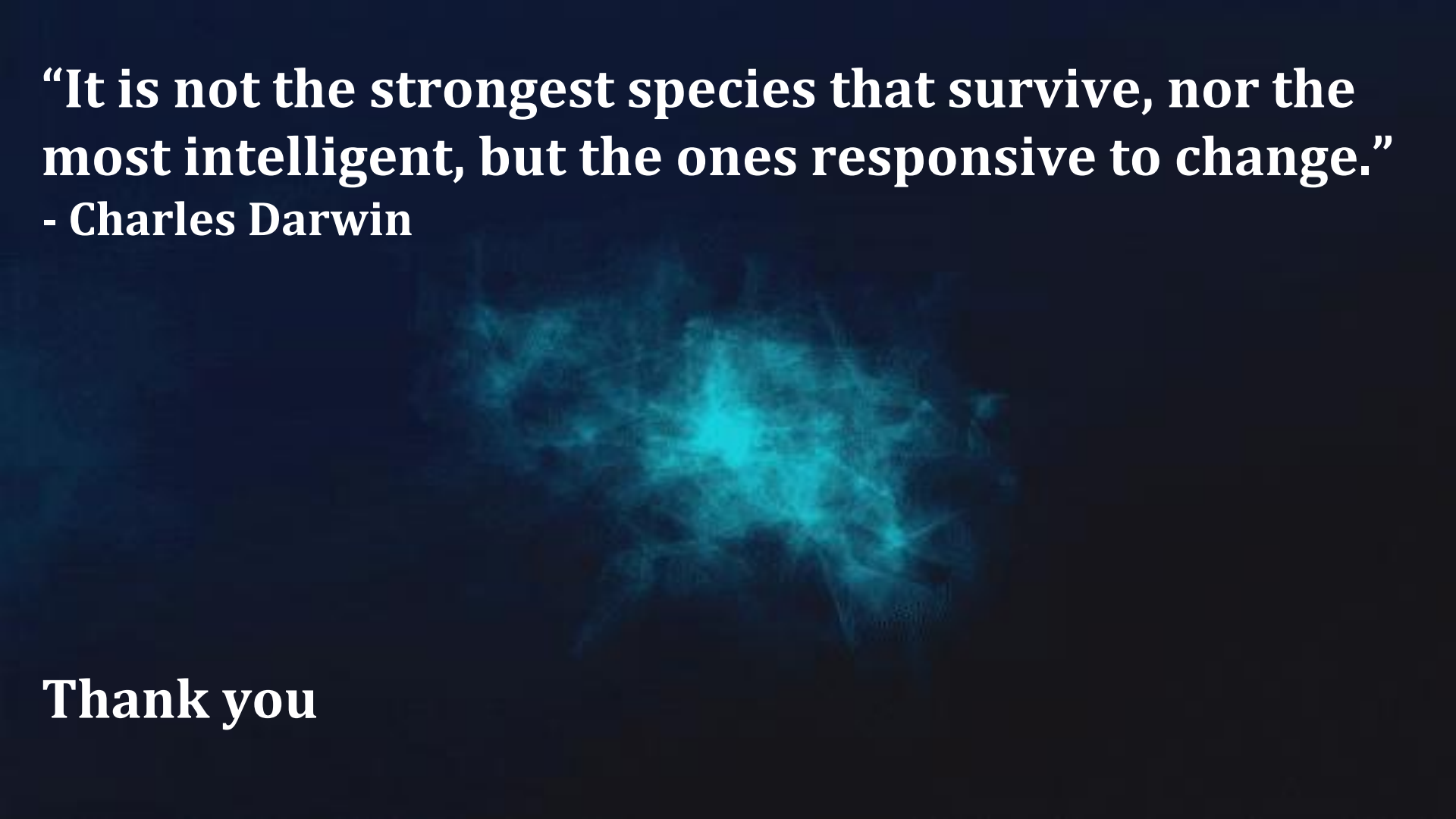

Modern Security Environment
POSSIBILITIES
THREATS
Security and Risk Management
TRUST
Resilience
Leadership
Comprehensiveness of Capabilities
Security Culture
Culture
Emotions
Realities
Situational Awareness
Dynamism
Technological Revolution
Digital-Physical Convergence
Security and Safety Management
Complexity
Predictable/Unpredictable Instability


The importance of trusted partners is a very important issue in security / states and companies

Finland and Chile are geographically distant, but strategically complementary. Finland brings expertise in digitalisation, cybersecurity, clean technology, education and resilient institutions.



“It is not the strongest species that survive, nor the most intelligent, but the ones responsive to change.”
- Charles Darwin



Thank you