10.05.2022
Meeting of the G7 Digital Ministers

Improving Resilience of Critical Activities in Cyberspace

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Cyberspace

Cyberspace includes all “**computers, systems and devices that are capable of**, with or without the use of intermediaries, **being connected to the Internet** – whether they are connected to the internet or not[.]”
– based on Sven Herpig, 2016, Anti-War and the Cyber Triangle

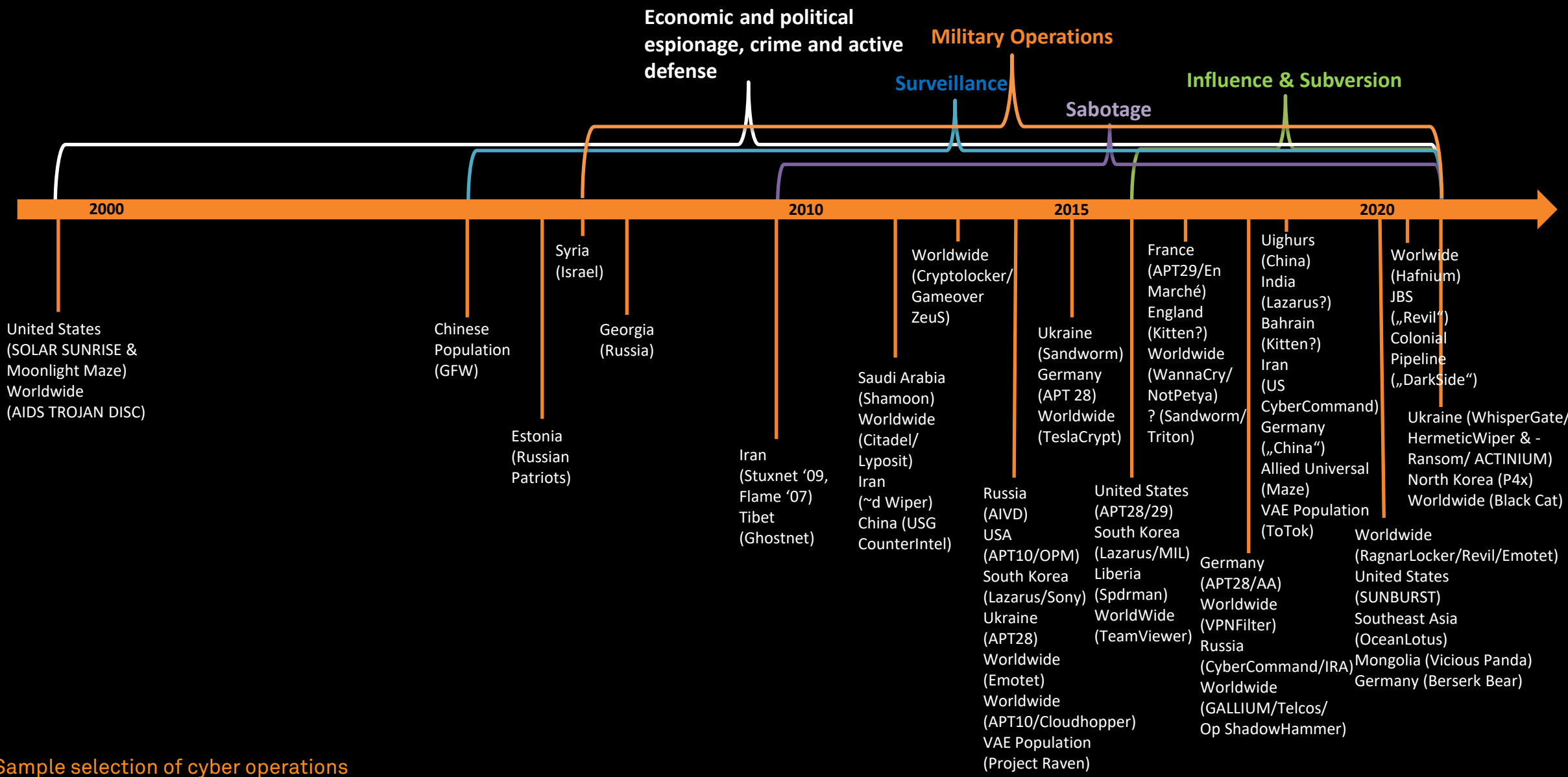
Critical Activities

"Critical activities refer to economic and social activities the interruption or disruption of which would have serious consequences on: –the health, safety, and security of citizens; –the effective functioning of services essential to the economy and society, and of the government; or –economic and social prosperity more broadly."
– OECD Legal Instruments, 2019, Recommendation of the Council on Digital Security of Critical Activities

Resilience

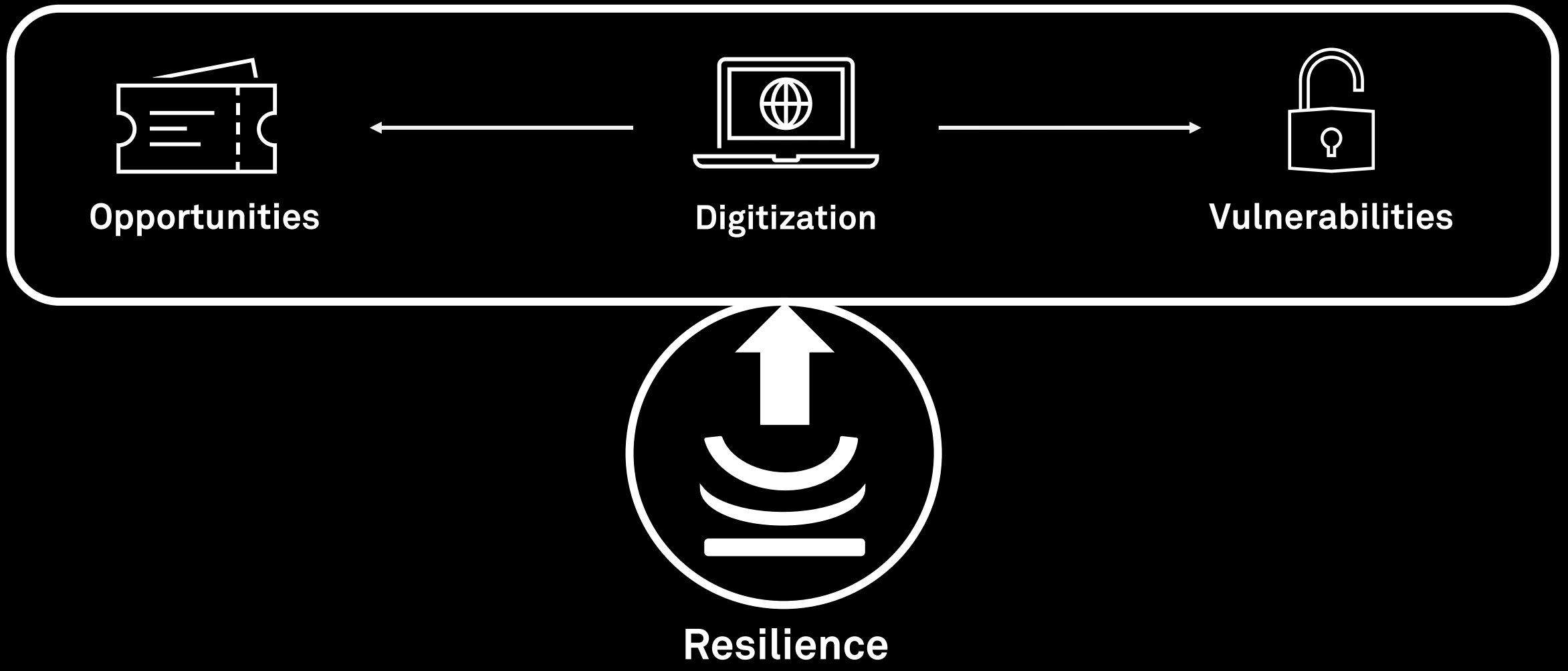
"Whereas cybersecurity is often considered as only protecting networks and IT systems against attacks (i.e. by implementing IT security tools or setting up security teams that deal with protecting a system) and preventing compromises, **cyber resilience enables quick recovery after successful attacks** (i.e. through secure regular backups) and, therefore, is an integral part of the IT system and organisational operation."
– Kate Saslow, 2019: Global Cyber Resilience

Threat Landscape*



*Sample selection of cyber operations

Digitization and Resilience



Shared Goal

As a result of an **assume-breach-mentality**, and as an extension to the **security-by-design** approach, we need to strive for **resilience-by-design** and vastly improved resilience of already digitized critical activities in cyberspace to reap the full reward of digitization for our economies and societies.

Challenges

- Shortage of skilled IT-security work force
- Lack of situational awareness for threat landscape
- Subsidiary responsibility for resilience facing well-resourced threat actors
- Absent int. coordination & collaboration to enhance resilience on the ground
- Lack of transition from knowledge, tools & awareness to actual implementation

Recommendations

Cyber norms	Document national implementation for allies and partners
Cyber CBMs	Support efforts to practically implement cyber CBMs regarding critical activities
Cybersecurity -policy- exercises	Conduct G7-wide-cybersecurity-policy-exercises to improve international coordination
Best practices	Implement and share best practices • strategic national priorization and risk assessment • cybersecurity education and (international) training programs • resilience-at-a-scale solutions through public-private-partnerships • mandatory breach notifications, IT security minimum standards and secure lifecycles for specialized hard- and software • proactive threat hunting teams and mobile incident response teams

Dr. Sven Herpig
Director for International Cybersecurity Policy
sherpig@stiftung-nv.de
@z_edian (Twitter)

Stiftung
Neue
Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel