Digital Infrastructure Security and Resilience Policy and Governance Implications

Ivey Business School
Western University, Ontario
May 14th, 2024

SERENTSCHY.COM
SERENTSCHY ADVISORY SERVICES GMBH

Resilience and Security of Digital Infrastructure
Intro and warm up

- In your opinion, is there a connection between China's increasing saber-rattling against Taiwan,
- the growing number of cyberattacks on the logistical infrastructure on the island of Guam in the middle of the Pacific (2.800km from Taiwan), and
- the increasing number of cyberattacks on civilian infrastructure (water supply, power grids, transportation systems) in the USA (12.000km from Taiwan)?
- Is there a causal correlation between these events and if so, why? Or is it pure coincidence?
- Please raise your hand, if you think its pure coincidence.
- And now, please raise your hand, if you think there is a causal correlation.
- Congratulations, everyone who voted for a causal correlation has intuitively understood the phenomenon of hybridization!

Resilience and Security of Digital Infrastructure
Main takeaways from our White Paper dealing with this topic

Relevant audience: policy makers and regulators, companies operating critical infrastructure, as well as wider audiences.

Goal: **Raise awareness** of the target audience of the necessity of urgent changes in the way the digital ecosystem is governed, against a backdrop of **seismic shifts in geopolitics** and an **ever-changing threat landscape to digital infrastructures and systems**. We aim to support this with the help of telling examples, covering the ramifications of the dynamic threat landscape. Building on this, recommendations for remedial action and structural improvements to digital governance are described.

Resilience and Security of Digital Infrastructure
Understanding the wider context (1)

- The **geopolitical context** is key: The issues addressed in this paper are vital to Western countries' security interests. Their interdependencies require the assessment and management of security threats in a geopolitical context. Without this context, security risks cannot be adequately addressed.
- **Hybridization:** Combination of different, temporally and geographically phased attacks that are guided by an overarching strategy in which a broad spectrum of hostile actions at different levels with a high combinatorial effect are deployed to reach the attacker's goal. The use of cyberattacks requires careful consideration of the immediate military benefit versus the strategic risk.
- **Complex threat landscape:** Disruptions to digital systems are caused by natural phenomena and man-made activities, such as cyber-physical attacks, sabotage, etc. However, there is a growing new phenomenon, a gray area between natural and man-made causes, triggered by climate change. This needs to be differentiated as the causes and prevention are different.

Resilience and Security of Digital Infrastructure
Understanding the wider context (2)

- **Telecom regulators** can play a crucial role in this context and their importance is sometimes underestimated. However, regulatory authorities in most cases do not have a mandate to develop or apply a holistic view and break out of their vertical silos. This is a wakeup call for policy makers to give regulators a new and expanded mandate which would enable them taking up a crucial role in this context.
- Enhancing the **resilience and security of digital systems** requires a **new form of public-private partnership between governments and the private sector**. Governments cannot tackle these challenges alone, nor can industry. This also has implications for the governance structure for digital affairs. The establishment of a central coordinating body is an important step towards overcoming the usual historically fragmented governance structures.

Resilience and Security of Digital Infrastructure
Important to know

For decades, network **security and resilience** have been seen as a purely technical matter. However, it should be kept in mind that security and resilience are not the same and not similar.

- **Security** measures are about **locking up** (firewalls, anti-malware software, access systems, fences, locks, etc.).
- **Resilience** is about **standing up**. Digital resilience never makes the false assumption that security will stop all attacks and breaches; therefore, resilience is about surviving inevitable attacks from inside and outside and about penetrations. **Resilience is about continuing to do business even under attack**, about discovering breaches and containing them, and about ultimately prevailing despite them. Network redundancy is one way of increasing resilience.

Resilience and Security of Digital Infrastructure Examples

EXAMPLES

Resilience and Security of Digital Infrastructure
We are faced with a complex threat landscape

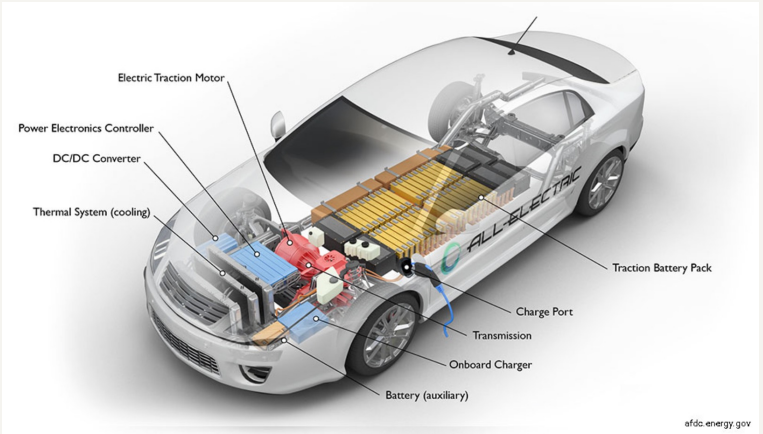
A security certification for IoT and control devices and EVs should be mandatory by law.

National Grid drops Beijing-backed supplier over UK power network fears

Move to end contract and start removing parts comes as west rethinks Chinese involvement in critical infrastructure

National Grid runs the bulk of Britain's electric power distribution system © Bloomberg

Electric vehicles (EVs) are a set of computers on four wheels. They communicate with clouds in their country of origin



Resilience and Security of Digital Infrastructure
Examples of attacks on digital infrastructures

Fiber cable sabotage in France

Resilience and Security of Digital Infrastructure
Examples of attacks on power infrastructures

Arson attack on the power supply of the TESLA factory in Brandenburg/Germany

Resilience and Security of Digital Infrastructure
Examples of attacks on power infrastructures

State actor involvement in Nord Stream pipeline attacks is 'main scenario', says Swedish investigator

By **Johan Ahlander**

April 6, 2023 12:39 PM GMT+2 · Updated a year ago

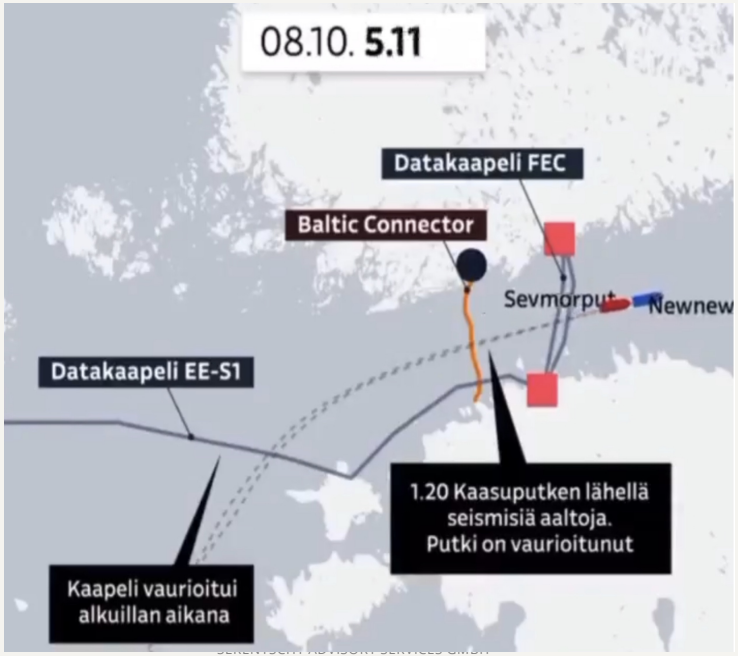
Gas bubbles from the Nord Stream 2 leak reaching surface of the Baltic Sea in the area shows a disturbance of well over one kilometre in diameter near Bornholm, Denmark, September 27, 2022. Danish Defence Command/Handout via REUTERS *Purchase Licensing Rights*

STOCKHOLM, April 6, 2023 (Reuters) A state actor's involvement in the blast of the Nord Stream pipelines last year is the "absolute main scenario“. In September 2022, several unexplained underwater explosions ruptured the Nord Stream 1 and newly-built Nord Stream 2 pipelines that link Russia and Germany across the Baltic Sea.

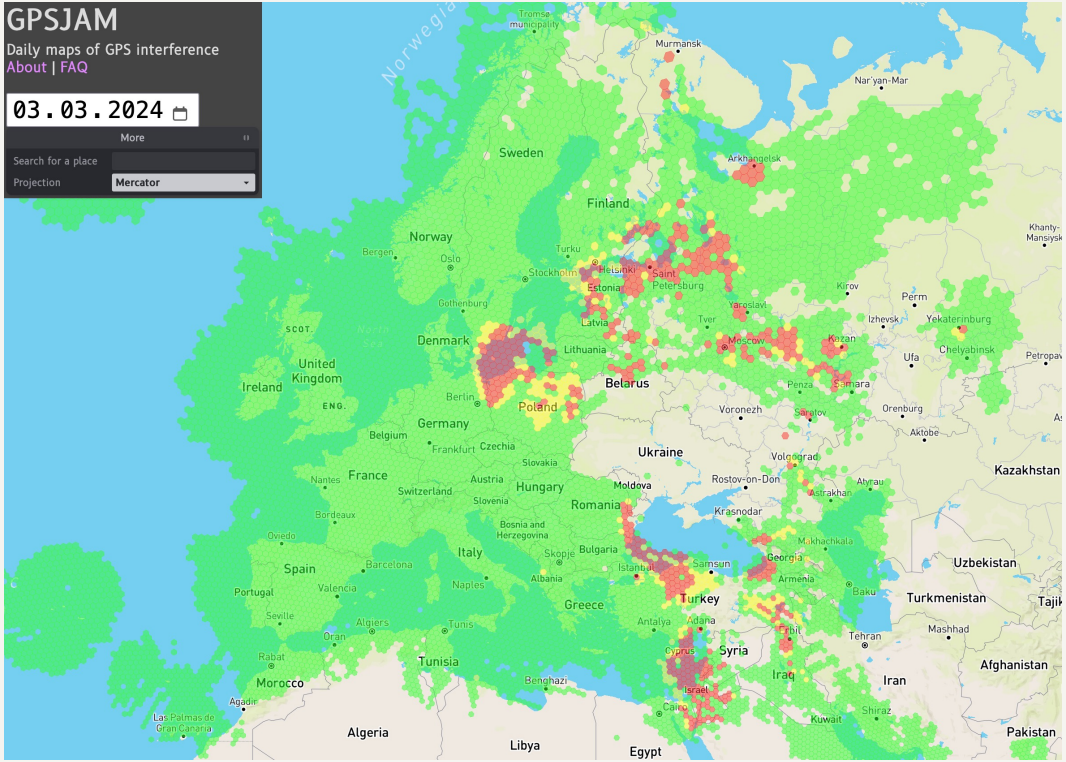
Resilience and Security of Digital Infrastructure

Damage on undersea infrastructure connecting Sweden, Finland, and Estonia

The Chinese cargo ship “NewNew Polarbear” dragged its anchor along the seabed for 185 kilometers over a crucial area of undersea infrastructure connecting. A pipeline and telecommunications cable connecting Finland and Estonia were damaged.



Resilience and Security of Digital Infrastructure
GNSS/GPS jamming and spoofing – PNT resilience



Governments globally should avoid an *over-reliance on GPS* and deal with emerging positioning-navigation-timing (PNT) technologies and methods for achieving a more resilient PNT (LEO satellites, eLORAN, Ring Laser Gyros, quantum-based clocks and combining quantum clocks with inertial sensors.

Resilience and Security of Digital Infrastructure
Hybridization

"**Hybridization**" describes a **combination of different, temporally and geographically phased attacks** that are **guided by an overarching strategy** in which a broad spectrum of hostile actions at different levels with a high combinatorial effect are deployed to reach the attacker's goal.

- For example, the dragging of an anchor by a ship over almost 200km in an area with sensitive underwater infrastructure,
- the weaponization of trade, supply chains, raw materials, energy supplies, the manipulation of financial markets and democratic elections through disinformation, the disabling or disruption of vital infrastructure such as navigation systems, satellite communications, etc., are just a few examples.

The term also illustrates that the conventional distinction between war and peace as different phases of a political process is outdated and requires new answers.

Resilience and Security of Digital Infrastructure
Taiwan Scenario – Don’t look at incidents in isolation!

HYBRIDIZATION: **Guam** is the central logistical hub in the Pacific for the USA for the delivery of military goods to Taiwan. A **disruption to Guam's logistical infrastructure** would adversely affect US military deliveries to Taiwan.

Cyberattacks on U.S. infrastructure (water supply, electricity, traffic systems, etc.) create confusion, civil unrest, and undermine political decision making.

Source: https://www.csis.org/analysis/cyberattack-civilian-critical-infrastructures-taiwan-scenario

Resilience and Security of Digital Infrastructure
Hybridization – a telling quote

Keir Giles

Senior Consulting Fellow, Russia and Eurasia Programme

CHATHAM HOUSE

…on **Hybridization:**

“As ever with a hostile state or state-backed actor, it’s wise not to look for a single explanation of why they are doing anything. There’s always a combination of things going on.”

Resilience and Security of Digital Infrastructure
”The subsea cold war" between the US and China

Growing geopolitical tensions between the US and China have begun to affect the flow of global data due to an expected sharp fall in new undersea cables linking China with the rest of the world.

On April 10, 2024, Google announced a $1 billion project to build two submarine cables to connect Japan, Guam and Hawaii. There are plans to lay four cables to Japan and seven to Singapore after 2024. In addition, nine cables will be laid to **Guam**, midway between the US mainland and Southeast Asia.

Guam is the central US logistical and military hub in the Pacific.

Source: https://asia.nikkei.com/Spotlight/Datawatch/More-subsea-cables-bypass-China-as-Sino-U.S.-tensions-grow

Resilience and Security of Digital Infrastructure
Ten key policy recommendations can be derived from our analysis

Recommendation 1: **Resilience and security do not come for free -** Telecom operators need incentives to invest in redundant infrastructures to increase resilience and consumers need to be aware that the use of security-certified products comes with higher prices for these products. For the credibility of a determined policy, the political level must offer concrete and binding incentives and/or relief for companies and consumers.

Recommendation 2: Setting up an **Expert Panel focused on network resilience** to advise the government based on their own and commissioned research. Major clients and supporters of such a body could include globally leading insurers like Munich Re, Lloyds and Swiss Re. However, we recommend not waiting for international initiatives, but acting at national level as quickly as possible.

Resilience and Security of Digital Infrastructure
Ten key policy recommendations can be derived from our analysis

Recommendation 3: A **security certification for all IoT devices and EVs** (electric vehicles), regardless of their origin, should be made mandatory by law. The absence of such a security certification - for whatever reason - can be seen as an attempt to undermine national security.

Recommendation 4: The **admission of students or scientists from non-like-minded countries without security clearance** in areas with dual-use potential **is strongly discouraged**. Furthermore, it is recommended to find a careful balance between the demands of national security, international obligations and the facilitation of legitimate trade and scientific cooperation.

Resilience and Security of Digital Infrastructure
Ten key policy recommendations can be derived from our analysis

Recommendation 5: Healthcare organizations are advised to **prioritize cybersecurity**, employ robust practices, conduct regular risk assessments, and stay updated on security threats and technologies to mitigate risks effectively.

Recommendation 6: Looking at an incident in isolation obscures the bigger picture and the effect of hybridization. It is recommended to **analyze incidents for possible further correlations through the lens of hybridization to take effective measures**.

Recommendation 7: More **transparency** seems to be **necessary** to show the public the extent of the vulnerability of modern society and to raise the willingness to take appropriate measures, i.e., reorganization of the responsibilities and/or authorities internally. **Transparency** resulting from a detailed analysis of the incident or reverse-engineering of the attack **exposes the attacker** and **leaves them no choice** but to **either admit to the attack** or use ridiculous excuses that any observer can easily see the truth.

Resilience and Security of Digital Infrastructure
Ten key policy recommendations can be derived from our analysis

Recommendation 8: Governments should avoid an over-reliance on GNSS/GPS and **deal with emerging PNT** (positioning-navigation-timing) **technologies and methods** for achieving a more resilient PNT.

Recommendation 9: Subsea Infrastructure: **(1) Promoting infrastructure diversity** (i.e. higher redundancy) as the most effective means of countering threats and making critical infrastructure less vulnerable, **(2) Complementary military protection** against targeted attacks when diversification and resilience alone are not sufficient, in particular through improved intelligence and deterrence. Focus on locations where several critical infrastructures (i.e. multiple cable landing station) come together, **(3) International cooperation to secure maritime critical infrastructures** for example through strategic dialogs, increased information exchange or joint military exercises.

Resilience and Security of Digital Infrastructure
Ten key policy recommendations can be derived from our analysis

Recommendation 10: **Institutional reform – Digital Authority**: **Improving the resilience and security of digital systems** requires a **new form of public-private partnership** between governments and the private sector.

- Governments cannot tackle these challenges alone, nor can industry.
- The establishment of a central coordinating body is an important step towards overcoming the usual historically fragmented governance structures.
- The **security and resilience of digital systems**, which are essentially the central nervous system of our society, is **too important to be left to the status quo**, which in most countries is a fragmented governance landscape, with critical gaps and often overlapping competencies.
- Isn't an **inadequate (i.e., silo-ed) structure of the authorities a security risk in itself?** Not only the lack of holistic thinking and action, but also regulatory gaps and overlaps, turf wars, “not-in-my-backyard, not-invented-here”, etc.

Resilience and Security of Digital Infrastructure
From plan to execution – what's next?

Key elements of an institutional reform:

- **Raising awareness**
- **Understanding that the status quo is inadequate**
- **Political ownership – who is the project owner?**
- **Implementation strategy and strategic controlling**

Resilience and Security of Digital Infrastructure
White Paper by Serentschy Advisory Services GmbH

Download link to the full White Paper:

https://www.serentschy.com/digital-infrastructure-resilience-and-securitypolicy-implications-and-mitigation-measures/

A final Memento: The biggest threat is ignorance combined with complacency.

Resilience and Security of Digital Infrastructure
Contact information

SERENTSCHY.COM

SERENTSCHY ADVISORY SERVICES GMBH

Riglergasse 6/6
1180 Vienna, Austria

Fon: +43-664-3000212
Fix: +43-1-4796297-12
Fax: +43-1-4796297-19

Web: https://www.serentschy.com/
Mail: your@advice-serentschy.com

UID: ATU68387168
FN: 409009i

Resilience and Security of Digital Infrastructure
Digital Authority - Austrian Example