SQUIRE PATTON BOGGS

Digital Networks Resilience and Security

EMEA – 30 January 2024

Escalating geopolitical tensions have placed unprecedented pressure on global networks, posing significant risks to digital infrastructure, cybersecurity, data privacy and the resilience of network systems.

The 2017 "NotPetya" ransomware attack – attributed to Russia – severely disrupted global business operations, although its primary target was Ukraine. The attacks on submarine cables between Sweden and Estonia in October 2023 is another example of the vulnerabilities that nations are facing currently. In this polycrisis environment, protecting global network integrity along with national networks is highly demanding and critical.

Sectors such as energy, industrial automation, and transportation – including navigation – are on the target list of state-backed actors and extremist groups, aiming to attack core functions and symbols of society. As far as state actors are concerned, such activities must also be seen as a key element of hybrid warfare.

> "The underlying message conveyed by attacks against infrastructure is the most important thing. Looking at an incident in isolation is not enough and can result in misleading conclusions."
> Interviewee

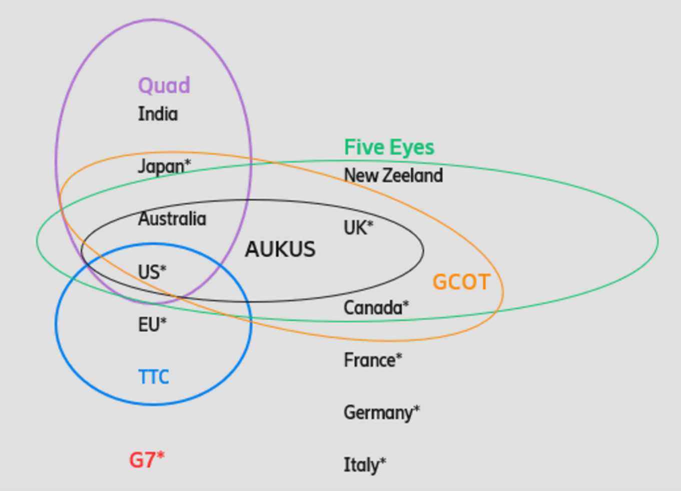
The Geopolitical Context Is Key

Western countries' security interests and the interdependencies across the alliances require the assessment and management of security threats in a geopolitical context. 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.

- Network security measures are about locking up, i.e., access systems, fences, locks.
- Network resilience is about standing up:
  - Resilience never makes the false assumption that security will stop all attacks and breaches. Resilience is about surviving inevitable attacks from inside and outside, and penetrations; continuing to do business even under attack; discovering breaches and containing them; and ultimately prevailing despite them. Network redundancy is one way of increasing resilience.
  - A holistic view comprises not only cables, switching and routing equipment, but also peering agreements, ownership relations, internet exchange point (IXP) presence, capacity issues and a look at the relation between physical and logical networks.

Emerging Global Governance Bodies

In increasingly complex and dynamic global governance bodies, new alliances are maturing where tech and 5G is high on the agenda. The focus includes trusted vendors, 5G architecture, open radio access networks (Open RAN), resilience, supply chain, cybersecurity, 6G research and development (R&D), semiconductors, artificial intelligence (AI) and quantum computing.



Emerging Global Governance Bodies (Source: Ericsson)

> "5G directly impacts global defense and security and is applying transformative 5G technologies through NATO core tasks of deterrence and defense, crisis prevention and management, and cooperative security."
> NATO

In 2021, the 5G Security Conference was held in Prague, where a strategic paper on vendor diversity was adopted. In September 2023, a group called Global Coalition on Telecommunications (GCOT) was founded. The US, the UK, Australia, Canada and Japan are members of this group. The Prague Declaration is one of the cornerstones of this initiative, which will focus on "shared priorities," including open networks and diversifying the telecom supply chain.

The Think-Tank of the European Parliament published, in June 2023, a wake-up call on the "Security implications of China-owned critical infrastructure in the European Union." This research demonstrates that traditional approaches to infrastructure protection based on direct ownership are insufficient, since China's party-state can obtain access to critical infrastructure through indirect, equally effective channels. As these cases show, infrastructure protection mechanisms, whose codification and implementation remains incomplete, must be extended to be able to scrutinize the risks that China's leverage over nonscience investors and Chinese state-linked contractors pose to the EU's critical infrastructure.

The emergence of global governance bodies is a welcome development – as regulatory authorities often have an overly narrow view focused on economic and legal issues, they tend to lack understanding in the geopolitical dimension as well as technical, strategic and cybersecurity know-how. Most importantly, regulatory authorities in most cases do not have a mandate to develop or apply a holistic view and break out of their vertical silos. In addition to network attacks by threat actors, events caused by climate change, such as increased wildfires, floods, landslides, etc., pose an additional threat to the functioning and integrity of the networks.

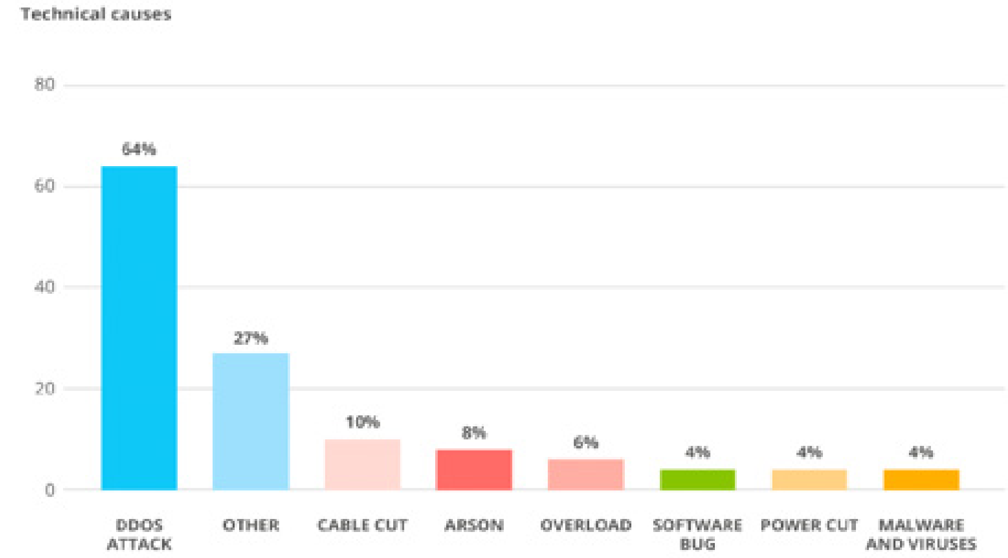
> "Building resilience in the 21st century is "one of our most urgent social and economic issues because we live in a world that is defined by disruption."

Judith Rodin, former president of the Rockefeller Foundation

Types of Attacks

The overall risk landscape is very complex. Governments often lack information; sometimes not even the operators have complete information.

Figure 23: Technical causes for incidents due to malicious actions – Telecom security incidents in the EU reported over 2012-2021



Telecom Security Incidents 2021, ENISA

Today's communication networks consist of various layers and highly complex structures, ranging from a single home or cell phone to very sophisticated internet of things (IoT)/cloud systems with billions of automated devices powered by complex AI systems. The number of devices also gives an unprecedented opportunity to weaponize distributed denial of service (DDoS) attacks and deploy them in geopolitical conflicts. Fighting against these threats is beyond the capability of a sole service or infrastructure provider and requires the cooperation of all global stakeholders, including operators, regulators, security agencies, states and international organizations.

There has been significant reporting of both alleged cyber- and physical-security attacks directly on critical national infrastructure, including telecommunications providers and cable and power infrastructure. Given the lengthy mean time to repair for infrastructure compromises, resilient network design, with adequate redundancy and effective preemptive physical protection controls, is key to building effective defenses.

Example Threats

GPS sabotage – The latest mystery failure in Western digital infrastructure came over Christmas 2023. On December 26, 2023, the Baltic Sea region was hit by an outage in the widely used GPS network..

Threats from IoT devices – Devices can be found literally "everywhere" – in transportation, smart city systems, home and industrial automation, etc. They are often only equipped with rudimentary or dubious security and communicate usually with cloud systems from the country of manufacture, in most cases China.

According to an article in *The Spectator* (May 2023), "…in January 2023, UK security services took apart a UK government car because data was being transferred via a 'Chinese e-sim' inside… we know from a separate Tesla scandal that it would be perfectly possible for a Chinese engineer to record a private conversation in a car like this with a cellular module."

Removal of Chinese equipment in electric power grids – The FT reported in December 2023, "…that UK National Grid has started removing components supplied by a Chinese state-backed company from Britain's electricity transmission network over cybersecurity fears, according to two people familiar with the matter. The move by National Grid, which runs the bulk of Britain's electricity grid, came after it sought advice from the National Cyber Security Centre. National Grid's decision to terminate its contracts with a UK subsidiary of China's Nari Technology in April 2023 and begin removing components has followed a broader rethink in the west in recent years about Chinese involvement in critical national infrastructure."

As the MERICS report (November 2023) shows, hacking has become a standard option with increasingly sophisticated methods and is part of a long-term Chinese strategy to achieve economic, military and political supremacy.

Subsea infrastructure – Sweden's government said in October 2023 that a subsea gas pipeline and telecommunications cable connecting Finland and Estonia were damaged, in what Finnish investigators believe may have been deliberate sabotage. Helsinki is investigating the pipeline incident, while Tallinn is looking into the cable incident.

Shallow waters like the Red Sea, Suez Channel and Baltic Sea are highly exposed to underwater sabotage.

Cable-cutting – October 2022, sabotage against Deutsche Bahn's fiber-optic lines in northern Germany caused a failure of the GSM-R network, a dedicated mobile network based on the GSM standard, maintained specifically for voice, signaling and security communication with freight trains. Perpetrators had cut fiber-optic cables at two separate locations in Germany. Investigators stated that these attacks were sufficient to take the GSM-R network infrastructure and backup system offline.

Stealing emergency power equipment – In Belgium and France, there have been thefts of batteries and solar cells from mobile phone base stations from containers that are not adequately protected. This has two consequences – firstly, the loss of expensive equipment, and secondly, the nonfunctioning of the emergency power supply in the event of a power outage. It is important to know that the mobile phone base stations in Belgium and France are usually not secured by an alarm system with a connection to a control center. Stolen batteries and solar cells are usually shipped to Africa.

Increasing the Cost for Attackers Is Crucial for Defense

A successful defense strategy requires, first and foremost, a reduction of threats; however, the question remains whether our tools are comprehensive enough to combat the threats effectively. Military doctrine on defense and offense needs to be adapted for the civilian domain to successfully disrupt threat actors and increase their costs. We should put more resources and thinking into strengthening civil society in the fight against criminal and politically driven actors.

The ICC cybersecurity working group advised policymakers to pursue a "third way" instead of a binary defense or offense strategy. This involves tackling the rising trend in cyberattacks head on and reversing this trend by changing the currently far-too-attractive payoff ratio that motivates attackers.

To change the expected cost-benefit calculation of the attackers, the attackers' costs must be increased as much as possible through multilayered defenses and a private sector regulation response. This can be achieved by increasing the likelihood that the attackers will be detected and caught, and must bear the consequences of their illegal actions.

Future Developments

As more global governance bodies and public/private working groups bring operators, regulators and policy makers together to tackle network resilience, we will see further key developments in:

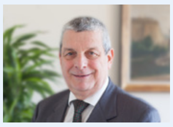
- **Architectural "resilience by design"** – The physical and logical layers of the network and their often-underestimated interdependence.
- **Regulatory** – How to impose obligations on operators to make their networks more resilient.
- **Cybersecurity** – Which attack techniques and surfaces are used by attackers.
- **Technological** – Understanding the new risks associated with technological changes, e.g., the widespread deployment of 5G introduced new vulnerabilities in areas like network slicing and IoT/cloud.

In this rapidly changing environment, we have expert communications and data privacy experts available to guide public and private bodies through this evolving landscape, from horizon scanning regulatory and legislative changes to understanding the direction of global cooperation of the governance bodies.

This summary is taken from a recent report by senior advisor Georg Serentschy, which provides a detailed and illustrative – but not exhaustive – overview of developments in the field of network security and resilience, from the outbreak of the COVID-19 pandemic to the present day. This report highlights the most important developments and trends in these areas.

The report is based on extensive desk research and numerous interviews with experts from the security apparatus, relevant people from industry and academic security experts.

Contact



Georg Serentschy
Senior Advisor, Brussels
T +322 627 11 11
E georg.serentschy@squirepb.com

The opinions expressed in this update are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.