What If the EU Did Not Share Data to Protect Its Critical Infrastructure?

Mattila, Päivi; Mattila, Isto

Veröffentlichungsversion / Published Version
Stellungnahme / comment

#WHATIF

DGAP MEMO

German Council on Foreign Relations

No. 4 | September 2022

What If the EU Did Not Share Data to Protect Its Critical Infrastructure?

By Dr. Päivi Mattila and Isto Mattila

This scenario shows what could happen if the EU fails to establish an information exchange environment among its critical infrastructure (CI) entities. In 2030, only a few services related to the EU's CI remain local and confined to a single domain. Most are heavily interconnected – and thus increasingly subject to hybrid attacks. Because the EU still provides no common guidelines to record and share information about such attacks, CI operators cannot analyze threats, recognize EU-wide patterns, or identify adversaries. Two EU directives from the early 2020s recognized this gap but did not provide the tools to address it.

INTERDEPENDENCIES LEAD TO CASCADING EFFECTS

On May 9, 2030, Greece suffers a major cyberattack on its electrical grid. Within hours, the delivery of energy to customers is disrupted. The flow of electricity to gas suppliers is reduced, debilitating a major industry that is itself energy dependent. Cascading effects not only impact the energy balance in the region, but also connected infrastructures in Italy.

As governments in the north of the EU reel from the shock and belatedly face up to the cost of such shared vulnerabilities, a second massive cyberattack hits Germany and the financial messaging services of SWIFT. Carefully designed malware inserted into SWIFT's main communications system disturbs time-sensitive payments, cutting all bank transfers and making shopping and business transactions impossible. This attack appears to trigger a concerted disinformation campaign directed to German *Querdenker* (contrarians) and other fringe groups. Targeted social media messaging highlights the euro's vulnerability to cyberattacks and urges German citizens to hold their savings in cash. Germans respond to these scare stories in sufficient numbers that banks' cash holdings are exhausted.

It takes days for governments in the EU to correctly assess the situation and ascertain whether the attacks on Greece and Germany are linked and who is behind them. An IP address leads online investigators to St. Petersburg, where the perpetrators had evidently used quantum technologies against which EU member states had no ready countermeasures. Furthermore, the Russian hackers targeted communally owned CI services such as water delivery and payment systems that were made vulnerable by a lack of investment in the security of their IT networks. The real problem, however, is not the sophistication of the attack so much as the fact that European governments had, for a decade, disregarded warning signs.

EU MEMBER STATES SEE THE NEED TO SHARE CI DATA

In 2022, member states had agreed that it was their priority to protect the EU from hybrid threats when they signed off on the Strategic Compass for Security and Defense. This comprehensive strategy document was completed in the immediate aftermath of Russia's aggression against Ukraine, which all agreed was a wake-up call to the corrosive effect of disinformation and hybrid warfare. But governments subsequently failed to establish a common protection mechanism for non-physical critical infrastructure based on data sharing. As a result, several warning signs – including small signals and adversary signatures – went undetected for years. Each incident that governments failed to recognize as part of an EU-wide pattern of hybrid action increased the risk of the kind of largescale coordinated attack on the EU described above.

In 2024 and 2027, major cyber incidents – most likely carried out by the same adversary state – probed the security of the EU's critical infrastructure. While authorities from the affected member states did share reports on the outages per the "CER Directive" on the resilience of critical entities, they could neither ascertain the hybrid nature of the attacks nor the signature of the attacker. Even though some of the targeted countries solved their own cases

independently, joint resilience-building measures among member states did not exist. The lack of such measures – for example, agreement on how to approach quantum threats – caused them to fail to connect the dots.

These developments reflect two perpetual challenges related to the sharing of CI data. The first is that the private sector is hesitant to share data because it fears this would draw attention to business vulnerabilities within its services that would be prohibitively expensive to address. The second is the cost of data sharing itself. Data sharing can result in huge financial burdens for small and medium-sized industries, which subsequently weaken their competitiveness on the global market. These relative costs are one reason why spoiler powers like Russia find hybrid attacks so attractive. While attacks are relatively cheap for the perpetrators, the lack of certainty about the modus operandi of those perpetrators creates huge speculative costs for their possible targets.

MEETING THE CHALLENGE OF PROTECTING CRITICAL INFRASTRUCTURE

In the early 2020s, the EU's CI sectors increasingly monitored threats by digital means, but they were unable to adequately share data on incidents (through so-called incident data analyses) across sectors and borders. EU authorities recognized that they needed to address this problem by shaping a common data-sharing environment, but they were locked in a vicious cycle that was hard to break. Providers lacked awareness of the pan-European nature of the threat environment and so had little reason to collect or share data. But raising awareness of these threats was only possible if the authorities had the requisite data from business to create a solution based on a data warehouse approach through which every CI entity could share findings with similar CI entities across the EU for an agreed fee. Ideally, data attributes related to critical external risks would not only be shared but also followed by anomaly detection mechanisms (AI/machine learning).

The key to breaking this cycle would have been to create a strong commercial incentive. Making data sharing profitable to industry would have stimulated businesses to exchange information even before they were aware of the security reasons. Yet such commercial incentivization required a shift in focus from both the EU and its member states – away from the protection of individual critical assets to the sharing of data among CI entities as a solution for improving CI hybrid threat management.

This new thinking would have allowed CI actors in EU member states to build an understanding of their shared risk environment and implement mechanisms to manage hybrid threats in a systematic way. If the EU recognized existing threats such as cyberattacks and disinformation as a threat to interconnected critical infrastructure, it could not only detect hybrid incidents in a coherent way but also support its aim to strengthen its strategic autonomy when meeting related tech challenges such as supply chain dependencies.

DR. PÄIVI MATTILA
Director of the Coherent Security Research Program, Laurea University of Applied Sciences

ISTO MATTILA
Director of Research and Development, Laurea University of Applied Sciences

BOTH AUTHORS COORDINATE EU-HYBNET, A PAN-EUROPEAN NETWORK TO COUNTER HYBRID THREATS FUNDED BY THE EU.

In its "What If" series, the German Council on Foreign Relations (DGAP) envisions the state-of-play in different policy fields in around 2030 and highlights the drivers behind them. The series aims to create awareness of opportunities and risks on issues that may not be top of mind for today's decision-makers but could turn out to be highly impactful. The stories are meant to trigger reflection about Germany's and the EU's strengths and weaknesses and to draw attention toward possibilities for desirable change in a forward-looking manner. For more information, please visit: ***www.dgap.org/whatif***

DGAP
Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
info@dgap.org
www.dgap.org
@dgapev

The German Council on Foreign Relations (DGAP) conducts research and advises on current topics of German and European foreign policy. This text reflects the opinions of the author(s), not those of DGAP.

DGAP receives funding from the German Federal Foreign Office based on a resolution of the German Bundestag.

Publisher
Deutsche Gesellschaft für Auswärtige Politik e.V.

ISSN 749-5542

Editing Helga Beck

Layout Lara Bührer

Design Concept Luise Rombach

Author photo(s) courtesy of authors