ADVICE FROM THE CYBER SECURITY COUNCIL

Connection under pressure

The resilience of the (digital) communication infrastructure in insecure times

I. Summary of advice

The digital telecommunications and internet infrastructure (hereinafter: the communication infrastructure) is the backbone of the Netherlands: Citizens, the government, and small and large businesses depend on this. Failure of parts of this infrastructure could disrupt our society. The Dutch communication infrastructure is of high quality and the sector functions well, but it is under pressure from the geopolitical relations that have changed in recent years. Malicious state actors have intensified cyber operations against Western countries, in which the communication infrastructure is also a target. The resilience of the Dutch communication infrastructure must therefore be strengthened.

The Cyber Security Council (hereinafter: the Council) conducted research into this and found five systemic risks:

1. the geographical concentration of internet exchange and data center infrastructure around Amsterdam;
2. mutual chain interdependence between energy and communication infrastructure;
3. automatic fallback in the event of (prolonged) outage;
4. the limited capacity to cope with prolonged power outages;
5. dependence on parts of the communication infrastructure from a limited number of suppliers.

In this advice, the council makes several urgent recommendations to the Cabinet to address these risks. The advice was developed in close collaboration with experts from the sectors concerned.

Recommendations

1. Increase the geographical distribution, decentralization, and redundancy of infrastructure.
2. Connect the communications and energy sectors and jointly set priorities.
3. Ensure automatic failover for critical communication in the event of prolonged outage.
4. Research into where emergency power capacity during power outages can be improved and recovery capability increased.
5. Focus on the strategic autonomy of vital processes.

II. Advice

Cause

The world has become more unsafe and unpredictable at a rapid pace. This has prompted the council to investigate where the resilience of the Dutch communication infrastructure needs improvement.
The council drafted the advice in close collaboration with experts from the communications and internet sector. The underlying research was conducted by TNO on behalf of the council.

The research consists of two parts, with the central question:

Is the Dutch digital communication infrastructure sufficiently resilient [1] against deliberate, geopolitically driven disruption by a state actor [2]?

The present recommendation stems from the first part of the study and focuses on the systemic resilience of the sector [3]. The focus here lies on the availability and continuity of the communication infrastructure during times of major threat. A follow-up recommendation regarding the security of the underlying technical protocols that enable data and voice traffic – based on the second part of the study – will follow in the second half of 2026.

This advice follows the logical connection between interests, threats, and the risks arising therefrom. The recommendations have been formulated based on these risks.

The importance of communication infrastructure for the Netherlands

The digital communication infrastructure is indispensable for the daily functioning of Dutch society. Citizens depend on this infrastructure for, for example, communication, access to information, and financial and emergency services. A large-scale outage or disruption directly affects the daily lives of millions of people. Digital communication is particularly crucial for the functioning of society during times of heightened tension or crises.

The Netherlands holds a prominent position as Europe's digital hub. For instance, the Amsterdam Internet Exchange (AMS-IX) is one of the largest in the world. Consequently, the communication infrastructure is a significant economic factor and makes the Netherlands attractive to international companies, AI factories, data storage, and scientific research.

The Dutch business community is highly digitized and heavily dependent on data and connectivity to deliver products and services. Disruption of the infrastructure results in immediate and significant economic damage. Furthermore, the communication infrastructure is closely intertwined with other vital sectors. For instance, communication networks are logically dependent on energy networks, but with the rise of *smart grids,* the reverse is increasingly true. Failure in the communication infrastructure has direct and far-reaching consequences for virtually all vital sectors.

Threat assessment

In its 2025 annual report, the AIVD notes that the Netherlands is experiencing the greatest security threat in decades. Malicious state actors have intensified their cyber operations against Western countries [4], with communication infrastructure also being a target.
The intelligence and security services warned Parliament in September 2025 that hybrid operations pose a continuing threat to Dutch society. These operations include covert influence, espionage, cyber operations, and pre-positioning for sabotage. Both services advise a more active Dutch stance in this hybrid confrontation.

---

[1] Resilience is defined as measures regarding risks arising from the impact of threats on interests to be protected.
[2] And criminal organizations, which are often hardly inferior to state actors in terms of knowledge, skills, and tenacity.
[3] TNO 2025 R12358 - Resilience of the Dutch digital communication infrastructure, Part I: Global exploration (final), January 9, 2026.
[4] Some criminal networks now possess extensive capabilities to conduct intelligence research themselves. This means that major criminal organizations are employing methods previously attributed primarily to states or intelligence services. Consequently, it is also becoming increasingly difficult to distinguish between criminal and state actors.

Threat particularly from Russia and China

Intelligence agencies have been warning for some time that state actors—particularly from Russia and China—are operating on a large scale in Western digital infrastructures. The attacks target not only geopolitical adversaries but also allies and neutral parties when strategically opportune.

The AIVD warns[5] that Russia is preparing for a prolonged confrontation with Western countries and classifies certain activities as sabotage bordering on state terrorism, intended to sow fear and cause societal disruption. The MIVD has also observed concrete cyber operations by Russian state actors against Dutch vital infrastructure[6], possibly in preparation for sabotage. China poses the greatest threat to Dutch economic security: a threat manifesting itself in espionage activities, cyberattacks, and the covert acquisition of technology and knowledge.[7]

The number of countries developing offensive cyber capabilities has grown significantly in recent years, the so-called proliferation of advanced cyber capabilities.[8] It is to be expected that the offensive use of AI will further drive the growth in the number of states (and other actors) with advanced cyber capabilities.

Sabotage: the attack on Kyivstar (2023)

In 2023, Kyivstar, Ukraine's largest mobile network operator, was hit by a large-scale cyberattack that led to a nationwide disruption of mobile voice and data services lasting for days. The attack was reportedly carried out by a Russian-affiliated hacker group that had infiltrated Kyivstar 's network months earlier. The effects were destructive: thousands of virtual servers were reportedly wiped, and more than half of the Ukrainian population was without access to mobile communication services for a considerable period. The attack also had broader societal impacts, including disruptions to air raid warning systems, financial services, and public transport. The attack on Kyivstar is a clear manifestation of hybrid warfare and underscores the extent to which vital infrastructure can be targeted in geopolitical disputes.

Pre-positioning: the Volt Typhoon campaign (2021)

The Chinese state actor Volt Typhoon has been compromising IT systems in US critical infrastructure since 2021. The most plausible goal of this group is to pre-position itself. for disruptive or destructive cyberattacks in the event of a conflict with the United States. The activity was discovered in 2023, but the group had been present in a dormant state within various vital infrastructures (digital communications, but also, for example, energy, transport, and water) for a long time prior to that. Notably, Volt Typhoon often managed to gain access through vulnerabilities in outdated or poorly maintained equipment and was highly effective at evading detection solutions. As far as is known, the Volt Typhoon campaign has not yet led to actual disruption of digital communications infrastructure (or other vital services), but the extent to which this actor has invested in preparatory actions for a potential disruptive attack is quite unique.

Findings and risks

Solid foundation, new risks

The Netherlands has a well-developed digital communications landscape. Dutch internet exchange points are among the largest in the world, Dutch mobile networks perform very well in international benchmarks, and there is a competitive market with sufficient providers across all service domains. The latter offers consumers the option to purchase services from various providers, thereby making them less susceptible to individual outages or disruptions.

At the same time, the world has become more unpredictable and dangerous at a rapid pace. Many parties are aware of this evolving threat and have established a solid foundation of resilience measures in response. Simultaneously, the inherent complexity of large-scale and mixed technology environments makes reducing vulnerabilities a permanent focus, certainly in light of the heightened threat level.

[5] AIVD Annual Report 2025
[6] MIVD Annual Report 2024
[7] AIVD Annual Report 2025
[8] AIVD Annual Report 2024

The council identifies five systemic risks in the communication infrastructure where the government and the sector can take action to bring robustness to the level necessary for the present time.

1. **Geographic concentration**
   Internet exchanges and data centers are concentrated in the Amsterdam region. This stems from the strong concentration of physical cabling for *long- haul* routes[9] in this region and the *low latency* requirements of Companies in the Randstad that house critical business functions in external data centers. This concentration can be historically explained by efficiency, but it is at odds with the prevailing design principle of ensuring sufficient geographical distance between redundant data centers of a single party. These principles have, for example, been applied by providers of fixed and mobile data services, who have geographically distributed their main data centers across the Netherlands. Due to this lack of geographical distribution of major internet exchanges and data centers, regional incidents, such as those caused by willful sabotage, can have a nationally disruptive effect.

2. **Chain interdependence between energy and communication infrastructure**
   The communication infrastructure is directly dependent on the energy sector. Disruptions in the power supply have immediate consequences for communication services. Conversely, the energy infrastructure is highly dependent on the communication infrastructure, for example in controlling inverters, charging stations, home batteries, climate systems, and grid energy management. Both vital sectors are the central nervous system of the Dutch economy and society; therefore, greater mutual cooperation is desirable.

3. **No automatic failover**
   The Netherlands has no formal regulation for the mutual transfer of users. from service or infrastructure domains to another provider, in the event of a prolonged outage. For mobile communication, national or *disaster roaming can* improve the resilience of data and telephony services for critical users. However, 112 is always reachable via the network of another provider.

4. **Limited capacity to handle power outages**
   Base stations – such as those for mobile communication – have battery capacity available in the event of a power outage. Thanks to this emergency power, communication can usually continue for a period of several hours. During a longer power outage, mobile and other communication services are lost, even though communication is crucial precisely at these times.

5. **Dependence on critical parties**
   Dutch connectivity, particularly for internet exchanges, resolving and registration parties, and satellite service providers, is often dependent on data center services from third parties with foreign ownership. In the current turbulent world, the Netherlands can be vulnerable due to these dependencies, for example through collateral damage from sabotage targeting another country, trade blockades, or the sudden cessation of services otherwise. Some providers mitigate this dependency by purchasing infrastructure from multiple providers or by utilizing both cloud and on- premises solutions.

Lessons from Ukraine
Ukrainian society and vital infrastructure, including communication infrastructure, have proven surprisingly resilient against the relentless kinetic and digital attacks from Russia. There are many lessons to be learned for the Dutch communication infrastructure from four years of war. Efficiency and centralization, both geographically and in terms of network architecture, have proven to be vulnerabilities. In response, the Ukrainians rapidly decentralized and made their network redundant. Furthermore, communication infrastructure providers realized at an early stage that they should not compete on availability and security. Together, they feel the responsibility to keep the country connected. There is also a strong focus on rapid recovery in the event of power outages and sufficient emergency power capacity to cope with power failures for extended periods. The key lessons from Ukraine have found their way into this advice from the council.

[9] This concerns (trans-Atlantic) submarine cables.

Recommendations

1. **Increase the geographical distribution, decentralization, and redundancy of infrastructure**
   The council advises the Cabinet to actively encourage the geographical distribution of peering[10] and transit capacity. By geographically distributing exchanges and data centers and constructing additional network routes, the robustness of the Dutch communication infrastructure is increased. In the event of a failure or attack, traffic can thus be automatically rerouted via other nodes. The council also advises strengthening decentralization and redundancy throughout the entire communication infrastructure, both physically and logically[11]. Networks with a dense, interconnected structure and diverse routing paths are significantly more resilient to sabotage. Connection recovery times after an incident are considerably shorter in decentralized and distributed networks, such as the internet, than in centralized architectures.

2. **Connect the telecom and energy sectors and jointly set priorities**
   The council advises the Cabinet to develop an approach specifically aimed at the interaction between both sectors in order to reduce the likelihood and impact of cascading disruptions. This should lead to aligned investment plans in resilience, connections, and chain dependencies, agreements on priority restoration, periodic crisis exercises, and better integration of crisis structures.

3. **Ensure automatic failover for critical communication in the event of prolonged outages.**
   The Council advises the Cabinet to ensure that agreements are made between providers, based on an exploration of roaming possibilities, particularly aimed at critical users. Additionally, the Council advises the Cabinet to encourage providers within vital infrastructure to use satellite communication as a backup. In this way, the availability of a critical fallback option is better guaranteed.

4. **Improve recovery capacity and emergency power capacity in the event of power outages.**
   The faster damage to energy infrastructure is repaired, the smaller the consequential damage. The council therefore advises the Cabinet to increase this recovery capacity of the energy infrastructure. In addition, the council advises the Cabinet to develop a plan together with the sector to increase emergency power capacity at critical points.

5. **Focus on the strategic autonomy of vital processes**
   The Council advises the Cabinet to encourage diversification in the market as well as the supply chain, in line with European initiatives[12] such as the Strategic Autonomy Directives and the Cybersecurity Act. This reduces the security risks arising from dependence on a single party. In addition, the Council advises safeguarding vital data and core network functions within Dutch or European jurisdiction as much as possible.

The Hague, July 1, 2026

[10] Peering is the exchange of (free) traffic between providers; transit is other traffic that goes to networks with which there is no direct connection.
[11] Logical means how data, functions, or connections are organized and interpreted by software.
[12] Including the EU Tech Sovereignty Package, a set of measures to strengthen Europe's capacities for semiconductors, AI cloud, and open source.