Critical infrastructure and global networking

THE RISK OF DOMINO EFFECTS

Highly industrialised societies rely on complex networked infrastructures. Some of these infrastructures are deemed critical. Natural disasters can shock regions or entire countries but cyber attacks, too, can devastate the technical information networks underlying the infrastructure. Cyber security is evolving from a technical topic to a policy issue.

by Rudolf Meier, Publicist

If a natural disaster somewhere in the world destroys or damages part of the public infrastructures, the consequences for daily life are immediately apparent. Transport routes are interrupted, high-voltage masts crash to the ground, industrial facilities are flooded. The connection between cause and effect is readily visible. For this reason, the far-sighted protection of infrastructures generally begins at this point: with *physical* risks, also known as elementary risks. This approach is certainly not off base, also from the standpoint of interdependency. After all, if the energy supply fails, so too do parts of the production and transport services, for example.

Possible damage to infrastructure that networks, controls and coordinates other functions or sectors is less readily visible from the outside. For instance, if a railway data network connecting the signal towers to the control room is disrupted by a cable break during servicing, trains will no longer run within a wide circumference of that network. Electronic signals are not the only factors missing here but also the associated virtual processes with which other infrastructures are rendered functional.

Critical infrastructural sectors

Infrastructure consists of a mixture of sectors in the public and private sphere. They are heavily interdependent on each other and require complex interfaces to work together efficiently. The moment the word "critical" is added as a criterion for these sectors, it quickly becomes apparent that they vary in relevance to property and processes. Nodes that are *particularly* critical must be identified. There is no way around this task even though it can be highly controversial politically. The individual sub-sectors have different levels of resilience, i.e. ability to withstand interference and/or to resume a regular level of functioning after sustaining damage. Ultimately, however, *an end-to-end security approach must include all infrastructural sectors identified as critical.* The following infrastructural sectors identified as *critical* by the Swiss Federal Administration can serve as examples in this context: energy, waste disposal, finance, health care, industry, information and communication technologies, food, public security, transportation.

The ICT infrastructure as the central nervous system

There is a huge reciprocal need to control, regulate and coordinate activities across the entire ICT infrastructure. Most of the tasks are automated and thus carried out without direct human involvement. The bulk of the work is performed by infinite numbers of software elements of all sizes whose often vital control and regulation functions extend into the most remote areas. Wherever computers network, control and regulate matters, a special phenomenon inevitably occurs. Efficient programming is essentially an artificially created equilibrium that outside factors can disrupt relatively easily. If this equilibrium is *electronically* disrupted, the process can take on an insidious dynamism of its own (tendency towards entropy). Complex forms of networking therefore pose two major problems.

First, even minor errors (technical faults, accidents, data recording errors, etc.) can alter, disrupt or block the system processes *unintentionally*. No matter what their origin, these incidents can fall like dominoes and paralyse large parts of regulated or coordinated sectors.

Second, incorrect commands and chains of commands *intentionally* smuggled in can force systems to behave in ways not helpful for the task at hand. If these incidents are on a large scale they are referred to as cyber war. In future "www" might also stand for World Web War ...

Unfortunately, cyber war is more than just a catchword. The media reports almost daily on electronic attacks against industries, corporate headquarters, administrative and data centres, etc. The perpetrators generally remain unknown.

The IP problem: curse and blessing so close to each other

With digitalisation, it is much easier to conduct transactions in real time, produce efficient global data flows and use "inexpensive" standardised equipment. Why is there an almost fateful information risk associated with these advantages? The danger is to look at modern data technology merely as a network of lines. Nowadays, data is mostly transported using the Internet Protocol IP (a protocol that originated in the early 1980s). It is not important to know all the details but you should recognise the simple logical principle behind IP. The more efficient and useful a technology is, the easier and more efficiently it can be misused.

IP is involved in practically all situations, from transatlantic cables to local offices. And because not everyone in the world is good, the *passive* risk of data flows being tapped has been relevant from the very start of digitalisation. Today you have to take another aspect of the problem just as seriously, namely the possibility of outsiders *actively* misusing IP to intervene in infrastructure data processes with dishonest intentions. The potential for cyber war is enormous. The ruinous attack on the infrastructure of an entire country is a case in point (Estonia in 2007). The most recent examples are the Stuxnet viruses and their progeny. As a result, the IP network itself is becoming a critical infrastructure in the context of infrastructure facilities.

Trail-blazing security criteria

The protection of critical infrastructures is a task that cannot be described in just a few pages. And corresponding projects must be planned and implemented using specialists, the approach Crypto AG has been taking for user projects in these areas for years. That is why we will confine ourselves here to describing several key criteria of security planning for ICT networking (within and/or between sectors).

- **Risk potential:** The majority of the threats to critical infrastructures stems from information networking but this fact is not taken into account in security planning with sufficient consistency in all places. Priority is often given mainly to physical infrastructure components or these components are even treated in isolation (e.g. intact rail track system as an objective). By comparison, communication and data processing infrastructures are not included to a similar extent by either railway companies or public or private ICT providers, who also bear responsibility (electronic control system, VPN data networks, sensors, etc.).
- **Physical measures:** Of course, building and facility security is important, along with access controls and fire protection. However, the technical networking of information is often what makes it possible to implement these measures functionally in the first place in actual practice. Each individual physical measure must therefore be analysed with this fact and with the corresponding chain of effects in mind: Which dominoes will cause other dominoes to fall with them and what will the consequences be?

- **Logical measures:** Large flows of data occur between nodes and pass through unprotected public networks. And data transport and processing are also in an exposed position at many nodes (control and regulation units, power stations, etc.). This means data confidentiality, integrity, authenticity, availability and reliability are not guaranteed as they are required to be in the case of integrated security. Only comprehensive **security architecture** can remedy this situation. Its core elements include the following:
  - **Encryption** or broadband VPN technologies to protect transported backbone data plus end-to-end encryption to match the scenario between individual ultra-sensitive users or nodes.
  - **Security zones** with which to define and isolate areas requiring a high level of protection and distinguish them from the parts of the system which have to remain without sufficient protection for technical or operational reasons. This separation involves physical measures as well as electronic and operational measures.
  - **Zone transitions:** The security zones must be viewed as isolated areas. Zone transitions have to be defined wherever data has to be shared between two security zones. Steps must be taken to ensure that only data needed for operations is shared. The data expected at the zone transition is defined and all other data is blocked. This can be done with a logical separation or a physical separation of the networks, also known as an air gap. Special attention must be paid to access from the Internet or access for support purposes because both open up the possibility of cyber attacks.
  - **Security management:** This activity enables overall data traffic to be monitored centrally. The functional data occurring in regular operations serves as the reference point. All security elements can be accessed through specially protected management networks. This feature makes it much easier to diagnose incidents. For instance, a malware such as Stuxnet would have had barely any effect because the data flows of the associated industries would have been properly monitored.

The bottom line: **critical infrastructures constitute the nerve centre of every society.** You can hardly overdo efforts to ensure the security of these infrastructures.

Security Zones and Zone Transitions