4.5. EXCURSE: CRITICAL INFRASTRUCTURE PROTECTION

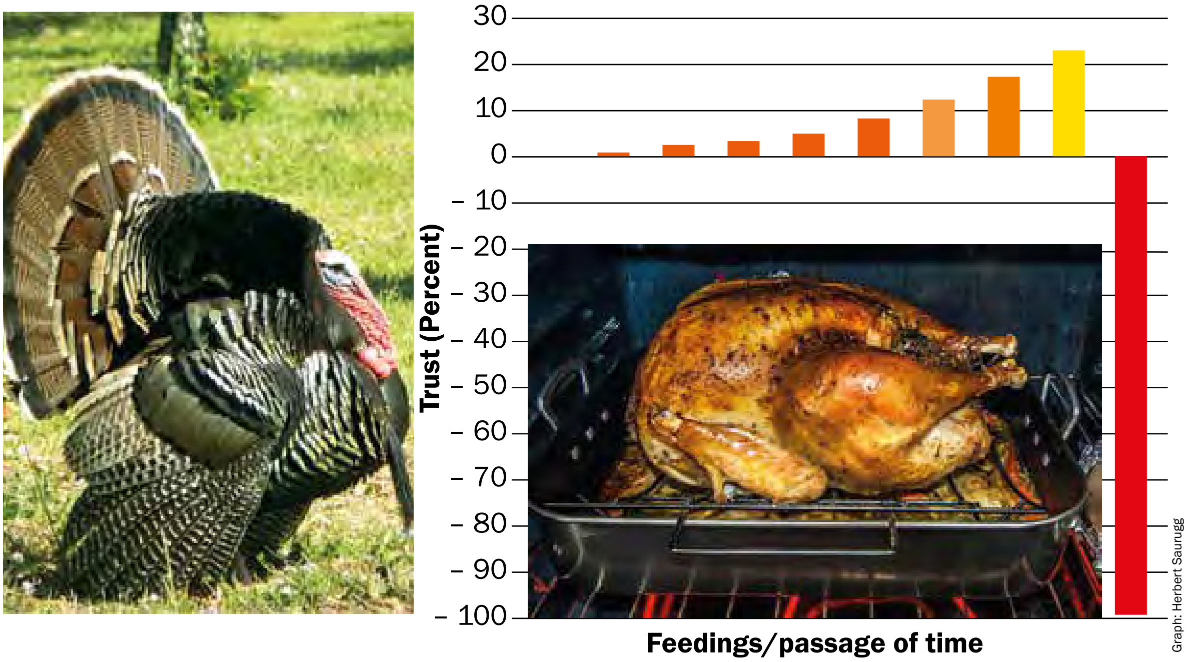
by Herbert Saurugg

Critical infrastructure protection (CIP) is a major topic because of an increasing number of incidents. The main focus of protection is prevention based on a sectoral approach. But how are we to cope with significant infrastructure interruptions if protection efforts fail and there are cascading effects? Public knowledge is limited and people do not have the necessary capabilities to deal with the incidents. Our belief that it will not happen does not actually prevent the event from happening. This can also be described as the 'Turkey Illusion'.

A turkey's trust in its owner, who feeds it daily, will increase based on its owner's good care. What the turkey doesn't know is that it is being fed for one purpose only. On the day before Thanksgiving, when turkeys are traditionally slaughtered, the turkey's trust will undergo a significant interruption.

Humans often act similarly. We look back at how successful we or our systems have been up until now and assume that past performance will continue in the future. Although we are unlike turkeys, who cannot foresee future or changing developments, we tend to ignore significant changes.

Similarly, there are significant indications that we are undergoing a major transformation process which will comprehensively change our societies and there are also sufficient signs that this process could be accompanied by 'creative destructions', as described by Joseph Schumpeter many decades ago. However, our essential infrastructure interdependencies mean that the outlook is not very pleasant.



Graph: Herbert Saurugg

Turkey Illusion

Herbert Saurugg

We are in a process of transformation to the Network Age or Society, which will change the way of life in our societies fundamentally.

TRANSFORMATION TO A NETWORK SOCIETY

During the Industrial Age, we had simple structures ('machinery') and clear hierarchies which worked very well most of the time. Now, however, we are in a process of transformation to the Network Age or Society, which began in the 1950s, and which will change the way of life in our societies fundamentally. In considering ongoing developments, it is dangerous to adhere currently to the knowledge and experience of former times, even if past solutions were successful in their day.

One major challenge will be that Industrial Age structures and thinking will not completely disappear, but they will increasingly lose influence and importance. This will increase complexity and requirements for those who must keep up with the developments and will have to cope with new challenges.

WHAT DOES COMPLEXITY MEAN?

Complexity is already a part of everyday language usage, even if there are often related different meanings like opacity, uncertainty, dynamism and so on. In short, complexity has the following typical characteristics:

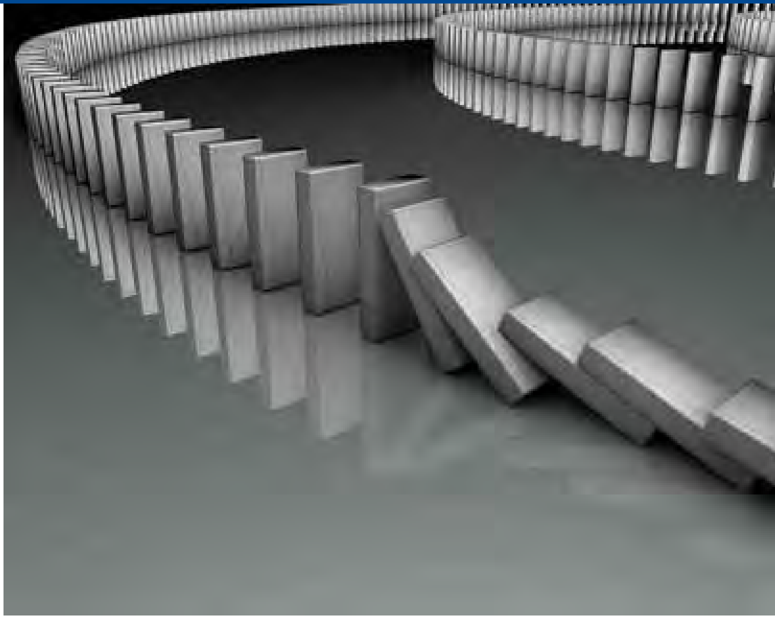
- Changing system properties because of feedback-loops and therefore the possibility of emergent new system properties.
  Take, for example, oxygen and hydrogen which, are flammable gases; these two elements combined produce a liquid, aqua, that puts our fire. Even if we knew the character of the gases, we would not be able to foresee the character of the new element.
- This also causes non-linearity where our approved risk management systems inevitably fail and predictions are difficult or impossible. They may work normally for

a certain amount of time but system behaviour could change completely in a single moment.

- Interconnectivity leads to an increasing dynamic (faster and faster) because the opportunities of system behaviour are increasing.
- This also leads to irreversibility (no way back) and the impossibility of reconstructing the causes or restarting at a well-known point.
  As an example of a complex system, take a creature: you cannot cut creatures into well-structured pieces, analyse them and put them back together again.
  It will not work. And this is valid for all complex (live) systems.
  Reconstruction only works with complicated ('dead') systems (i.e. machines).
- Another very well-known characteristic is that small causes could lead to large effects (known as the 'butterfly effect').
  A small problem in a supply chain link could bring down the whole system/production, as we have recently seen.
- Delayed and long-term effects are another, often underestimated, characteristic, especially in our very short-range focused economy. Figures are given for quarters.
  We know that apparent short-term solutions often have a negative impact on a long-term view and that, for long-term success, acceptance of short-term disadvantages is often needed.

VUCA-TIMES

Experts are therefore also speaking from new VUCA-times or a new VUCA-normal, the acronym for volatility, uncertainty, complexity and ambiguity, which is directly connected to the increasing complexity caused by the ongoing man-made interconnectivity between everything.
In particular, we are not used to dealing with ambiguity.



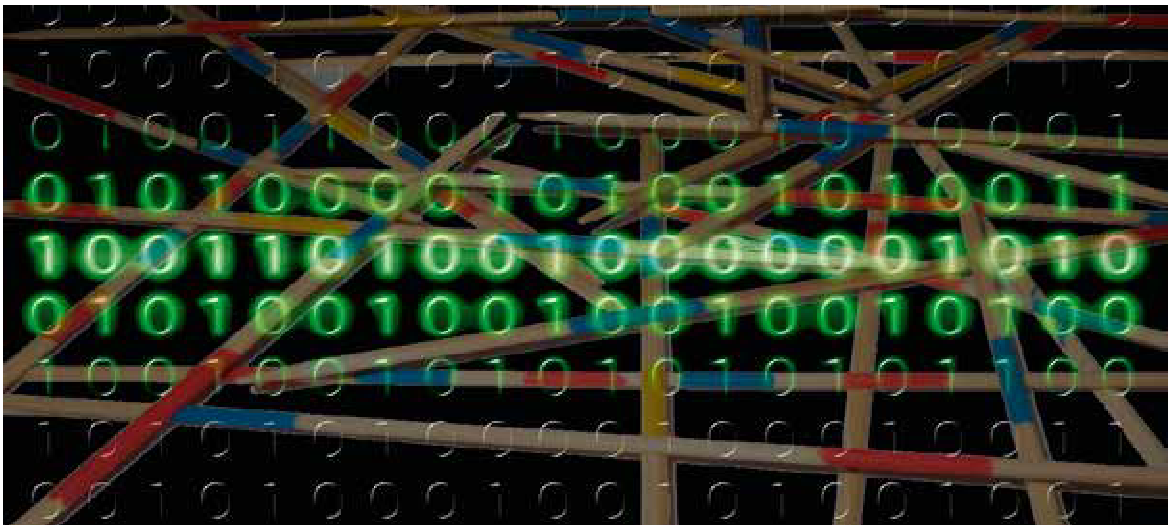
Systemic risks are characterised by a high degree of interconnectivity and interdependencies and missing outreach limitation.

RISK AND UNCERTAINTY

However, we still try to address new possible risks and developments with successful past methods which can hardly cope with increasing interconnectivity and complexity. In addition, risks are not the same as uncertainty. In a world with perfect hindsight, one knows what can/cannot happen and therefore assigns risk-weighted probabilities to such events, builds a model and takes calculated decisions. However, in a world where we cannot possibly know what can/cannot happen, assigning probabilities and building models might lead us to the same fate as that suffered by our turkey.

SYSTEMIC RISKS

Consequently, the rise of systemic risks is hardly observed. Systemic risks are characterised by a high degree of interconnectivity and interdependencies and missing outreach limitation. Cascading effects are possible. Because of complexity and feedback loops, there are no simple cause-and-effect chains and the triggers, as well as the impact, are systematically underestimated by organisations and the persons in charge.



Herbert Saurugg

We are always improving interconnections between technical systems, but the necessary interconnection between people and organisations to cope with non-intended side effects is lagging behind.

WHAT CHALLENGES ARE WE FACING?

First, we have to recognise that in nature there are only complex, open systems. These are new on a technical level, especially the increasing interdependencies (vulnerabilities). And we are still used to dealing with linear simple machines and not with complexity, which is caused mainly by a lack of education and training. Especially in the education system, we often still train and teach as was necessary for the Industrial Age, but that is hardly what is needed in the upcoming Network Age, where even a black and white description is too simple.

LACK OF KNOWLEDGE AND SYSTEMIC THINKING

There are of course improvements but, in general, they cannot keep up with the fast-moving technological developments and therefore we see more and more complexity gaps. Even though there are people who have the necessary knowledge to develop these emerging and converting technologies, most people, including people who should, do not have this knowledge, e.g. people working for public authorities or regulatory bodies to protect public interests. In particular, administrative bodies are often still organised under good old hierarchical structures which are hardly able to cope with fast changing VUCA-developments. Not to mention the fact that interconnected special knowledge and fast reactions are often needed. Today, nobody can know everything about everything and therefore we have to arrange more flexible ad-hoc networks and interaction among different experts to address complex dynamic challenges. This leads again to complexity gaps, which brings systemic risks and a danger of extreme events.

EXAMPLE ONE: CYBERSPACE AND CYBER SECURITY

Ten years ago, cyber security was hardly mentioned. We spoke about information and communication technology (ICT)security, but not about cyber security. With increasing networking of systems and infrastructures and with the spread of new technologies like smartphones, the focus grew broader. This was also necessary because of an increasing threat landscape, both qualitative and quantitative. Hardly any nation has a cyber security strategy to mitigate new challenges coming from the new virtual world. However, as we can see, everyday regulations and efforts do not seem to be able to follow up the developments on the dark side of interconnectivity.

One reason could be that we still focus on symptoms and not sources. We still try to fix vulnerabilities and wonder why it does not work. But more of the same will not work, to quote Albert Einstein: *'Problems cannot be solved with the same mindset that created them.'*

Of course, to conclude, some essential vulnerabilities will not be easy to fix because they are often based on significant design failures, which exist because the internet and also the connected hard- and software often were not designed for the purposes for which they are used nowadays. This problem is escalating, in particular, with legacy infrastructure systems like supervisory control and data acquisition (SCADA) or industrial control systems (ICS), which are used for automation and were designed for offline use. Nowadays, however, they are increasingly connected to office IT systems, so known office IT problems and threats could spread without the possibility of using known IT security solutions because of other system requirements or because of costs.

But developments do not stop: on the contrary, new technologies like the Internet of Things (IoT) emerge quickly and, with them, more future interconnectedness and threats. A few months ago, only a few experts warned that major risks could spread from these technologies. Since some major distributed denial-of-service (DDoS) attacks, we know that a large number of unsecured internet-connected digital devices, such as home routers and surveillance cameras and so on, could constitute a powerful weapon and could also bring down parts of our infrastructure. Until now, we have been lucky and only services have been interrupted. But what we have already seen would also be enough to trigger a major cascading infrastructure collapse, even if most people still believe that this is not possible. The threat increases with every new unsecure and connected device and with every new interconnection within infrastructure systems.

It is still early days but interconnectedness is likely to increase rapidly within the next few years because of smart grids, smart homes, smart cities and also with 'Industry 4.0'. Digitalisation is on everybody's lips, especially on politicians' lips. But do we really know what we are doing? Why should rapidly increasing threats from ICT be solved when they become more connected? Why are we again seeing serious security vulnerabilities in the IoT which we previously solved in other domains years or decades ago? Back then, they were in offline systems, but nowadays they are in highly interconnected systems where failure and disruptions could spread very fast and very far. It is as if we have not learned the right lessons, but the risks of today are growing exponentially and it seems that it will only be a matter of time before serious infrastructural disturbances arise because of an increasing complexity gap and underestimated systemic risks.

EXAMPLE TWO: EUROPEAN POWER SUPPLY SYSTEM

Another sector where a large complexity gap emerges is within the European power supply system. We just started the largest infrastructure transformation ever, with the transformation from fossil fuel driven power plants to renewable energy, which means a major shift from centralised to decentralised structures and power ratios. Yet every Member State is carrying out its transformation at its own speed and in its own way, with hardly any common aim or plan; this leads to an increasingly fragile system. However, insufficient new developments driven by the ICT-sector or new market players will also increase vulnerabilities in this highly sensitive system. It is our most important lifeline even if we do not notice it normally because it works seamlessly almost every day. This means that we do not have fall-back plans in the event of a considerable disturbance in the power supply system.

Herbert Saurugg

A European-wide power and infrastructure breakdown ('blackout') is unimaginable for many people, including most decision-makers.

Nevertheless, the warning signs have never been as tangible as in recent months. System instabilities have been increasing rapidly for years. And even the Association of European Transmission System Operators, ENTSO-E, stated in its investigation report on the 2015 Turkey blackout: ' Although the electric supply should never be interrupted, there is, unfortunately, no collapse-free power system!'

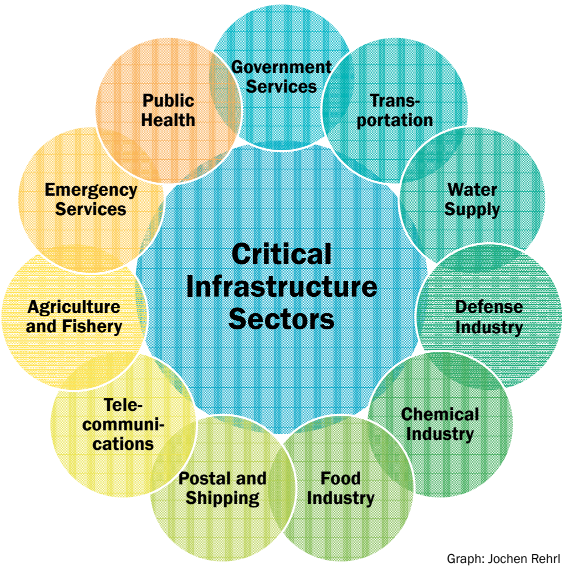
While most regions in the world have some experience of dealing with major disturbances like this, Europe does not, owing to its excellent security of supply. It is therefore also difficult to predict how long it would take for power to be restored. The estimate ranges from several hours to several days. The knock-on effect for our strong inverse infrastructure and society would be devastating, because we do not expect it and are not prepared for it.

For this crisis situation, there are rarely contingency plans for working 'offline', and, because of the power outage, nor would it be long before the telecommunication systems collapsed. So we could say that we have very good systems and operators because they have coped with all the problems to date. But we could also be suffering from a major Turkey Illusion.

LEARNING FROM NATURE – 'SMALL IS BEAUTIFUL'

We should learn more from nature, which has a very long history and development phase. Only survivable structures and organisms were successful and are still here. We often miss the so-called 'silent witnesses', those who did not survive and are not to be found in the history books. One major structure that did succeed is 'small is beautiful'.

- Small structures are more flexible and robust against strikes (asymmetry).
- People are more resilient in small structures.
- You cannot prevent the development, but early warning is an important part of navigation and we have to prepare to cope with uncertainty and with major incidents/disruptions.
- It is all about communication and knowledge. If people and decision makers know the challenges, they can react and prepare before a crisis or a disruption or change the path leading up to it.
- Security Communication will be a main driver to increase people's resilience and capacity to act in the event of uncertainty and after extreme events.
- 'Understanding the problem is half the solution', as Albert Einstein once said.



Graph: Jochen Rehrl

ARE WE PREPARING FOR THE RIGHT THING?

So we are moving along a very narrow path. Benefits and risks are very close together. One key question therefore is, are we mature enough? To prepare for an increasing number of possible and likely significant infrastructure interruptions, it is not enough to speak only at a high political or management level. We have to include people and mobilise them to prepare themselves, because such scenarios can be solved only by people themselves and not, as is usually the case, by emergency services.

- This calls for open security and risk communication, which addresses risks and uncertainties and assigns people their responsibilities in the event of significant infrastructure interruptions.
- We will also have to ask ourselves in politics and in the security sector if we have the right focus, or if we are preparing for 'the last war'. For example, on the one hand, we are devoting a large amount of money and effort to terrorism prevention, but on the other, we have a fundamental problem with our deadly vulnerable infrastructures.

The problem is that there is no easy, quick technical solution, but we have to start thinking about it and developing new design approaches, to mitigate already existing catastrophic potential. To start with all these steps in the aftermath of a first incident, as we have done in the past, will be too late in the future.