Essential Infrastructure Interdependencies

Would We Be Prepared For Significant Interruptions?

DeepSec 2017, Vienna

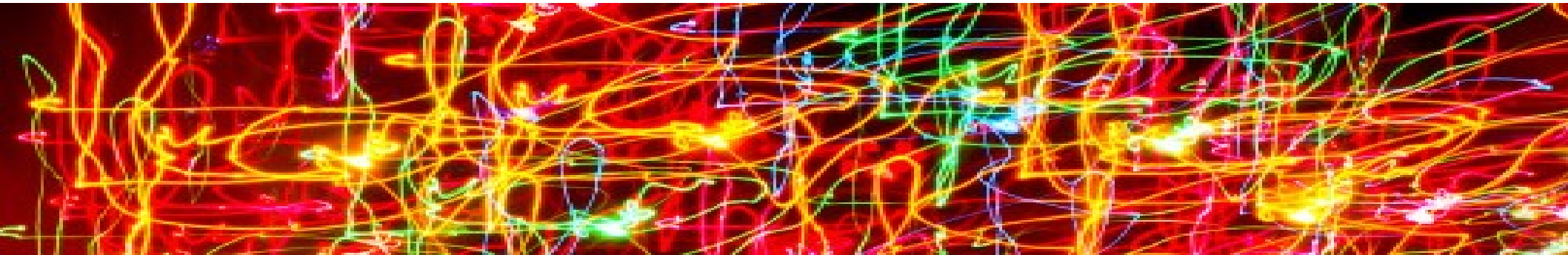
Interconnectivity & digitalisation …

Connectivity leads to Complexity!

- Complexity leads to Systemic Risks!
- Systemic Risks could lead to X-Events!

What does Complexity mean?

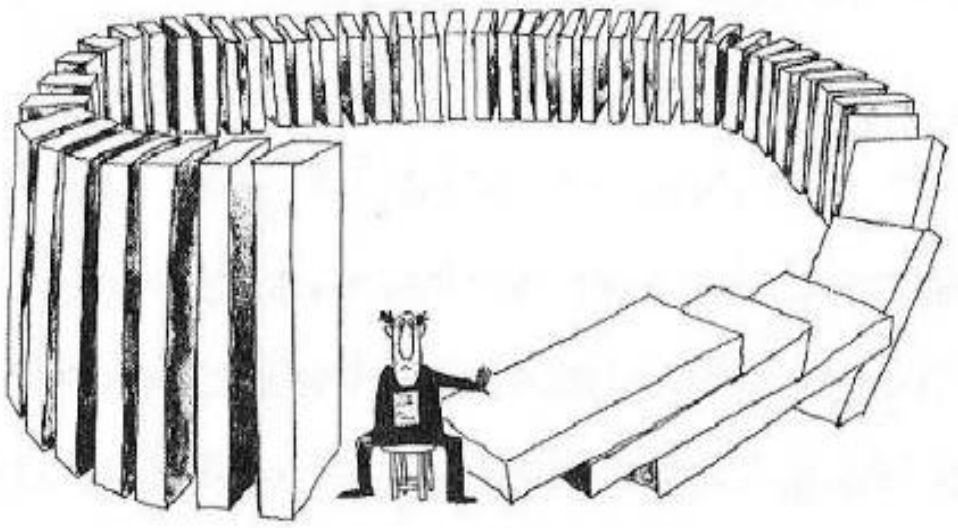
- Changing system properties (feedback-loops)
- Non-linearity (predictions, risk management fail)
- Increasing dynamic (faster and faster ...)
- Irreversibility (no way back!)
- Emergence (1+1=3; cause ⊣ effect)
- Small causes, large effects ("butterfly effect")
- Delayed / long term effects
- ...



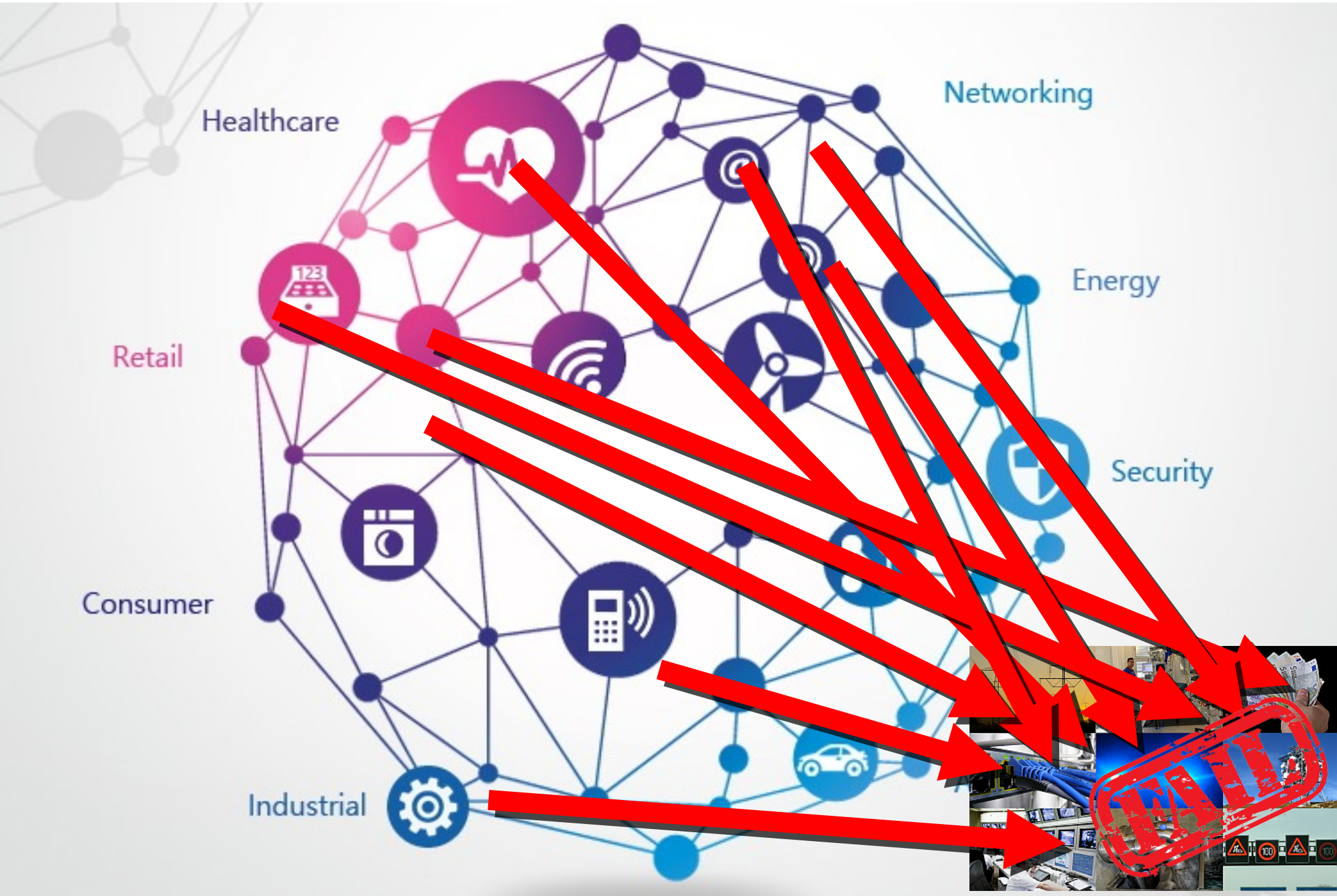
Systemic Risks

- **High degree of cross-linking / interdependencies**
  - missing outreach limitation
- **Feedback loops ⊐ non linearity!**
- **Cascading effects are possible**
- **Triggers and effects are systematically underestimated**

Current risk management methods fail!



Internet of things, Small causes ...



DDoS Attacks Cause Train Delays Across Sweden

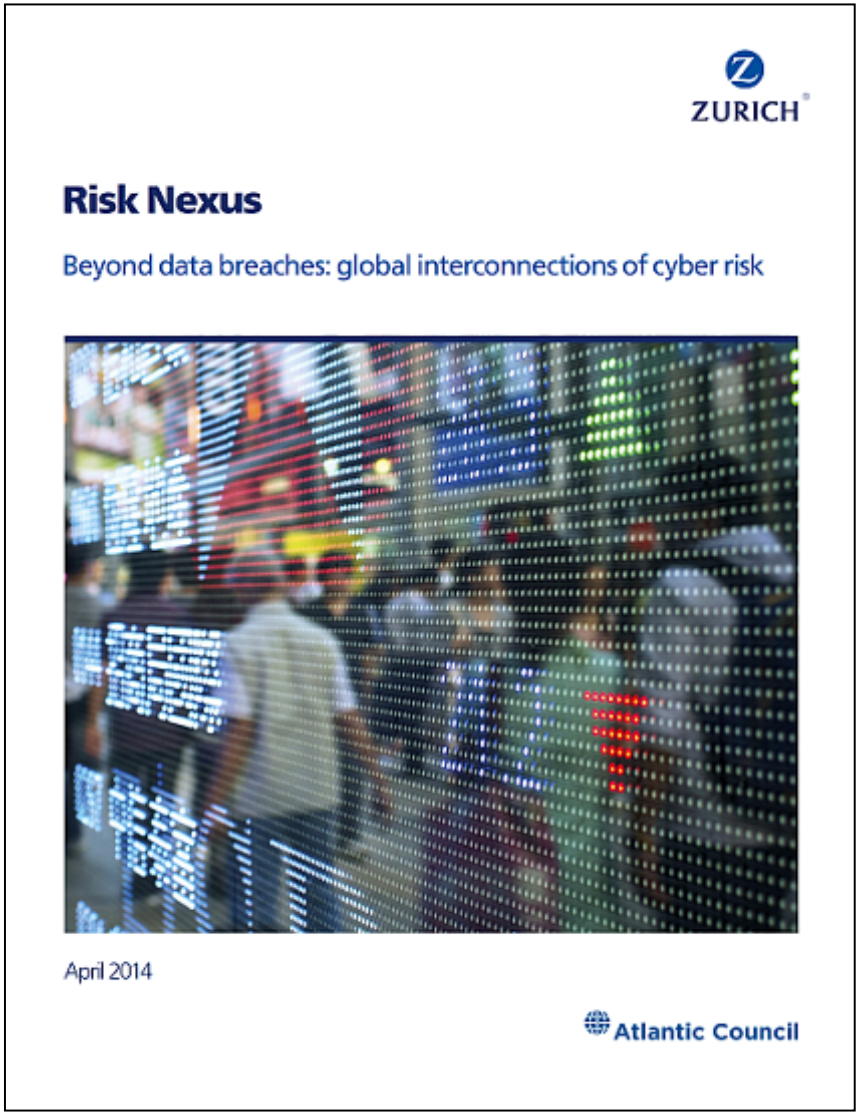
By Catalin Cimpanu

October 13, 2017 05:40 AM 1

DDoS attacks on two separate days have brought down several IT systems employed by Sweden's transport agencies, causing train delays in some cases.

Study 2014

The way in which the complexity of interconnected risks is assessed is painfully similar to how financial risks were assessed prior to the 2008 crash … in the end, it was this very complexity which helped bring the system down.



http://www.saurugg.net/2014/blog/cyber/beyond-data-breaches-global-interconnections-of-cyber-risk

How we have reacted until now

There will be no second line of defence!

X-Event

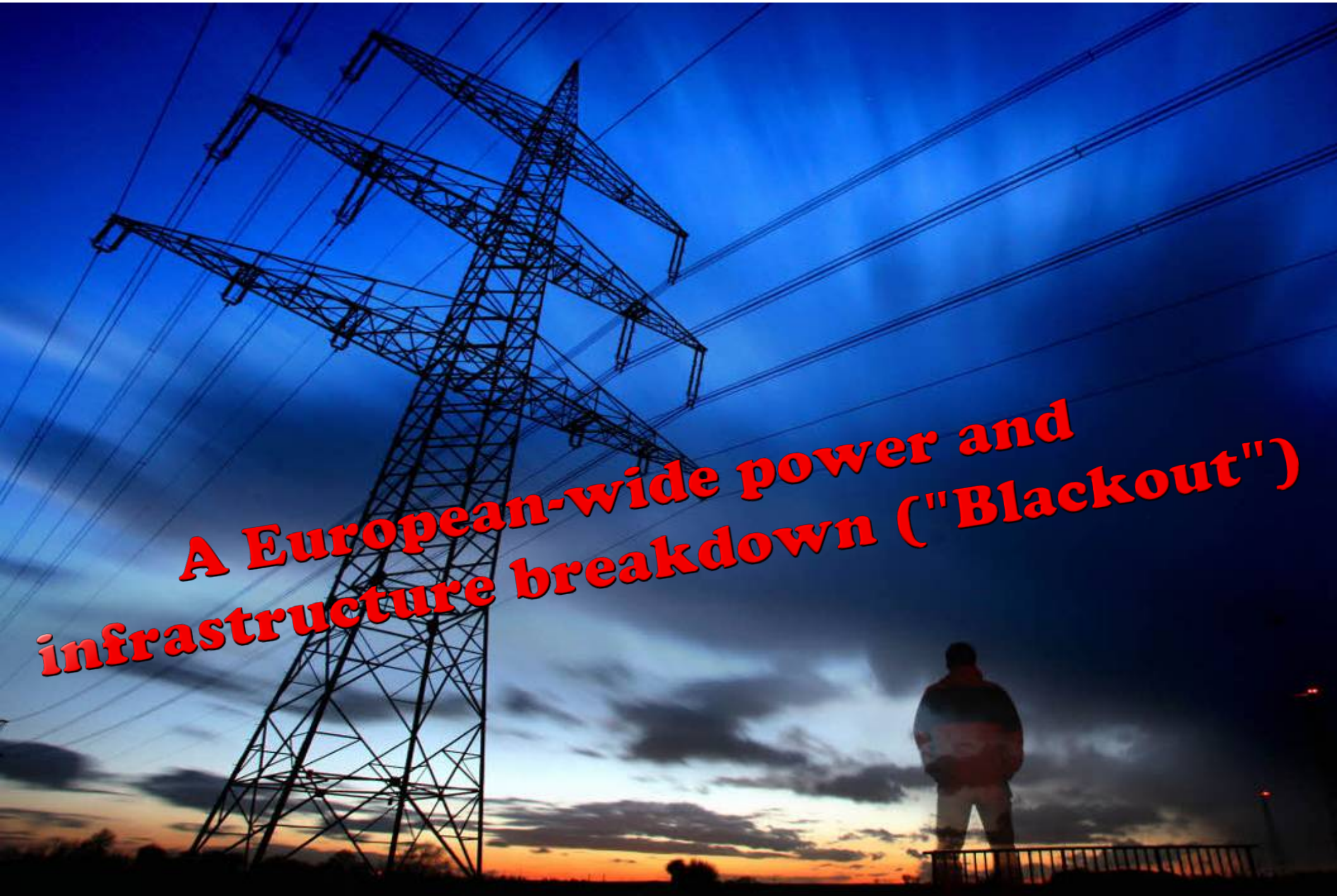
~~Cyber-Security~~

~~Cyber-Defence~~

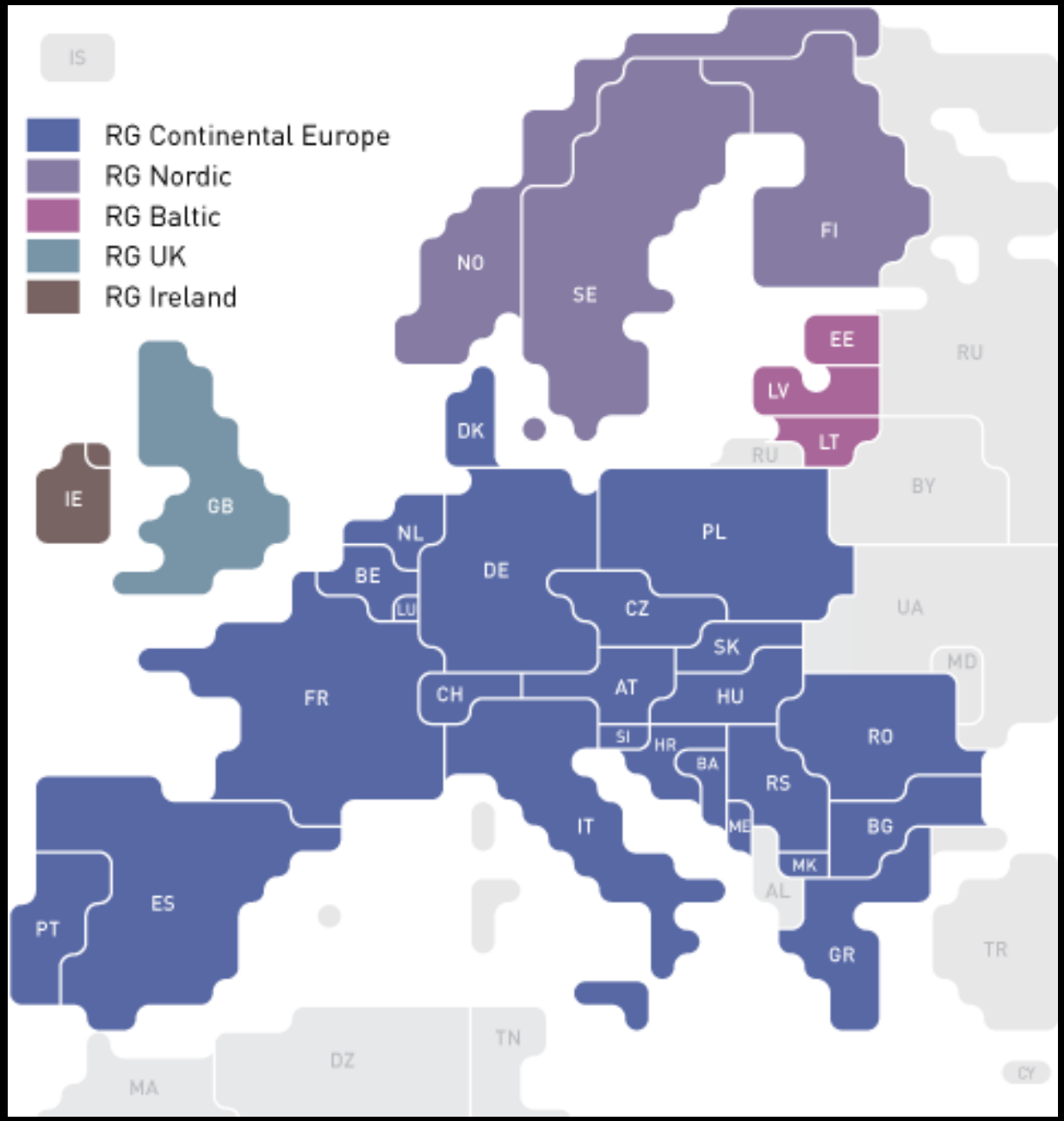
~~Critical Infrastructure~~


Protection is not enough!
We also have to
prepare for the worst!
And we have to rethink
our system design!

A second example with complexity gaps ...



The European Power Supply System



"Too Big to Fail"

Unilateral system interventions

Market and politics are ignoring physics

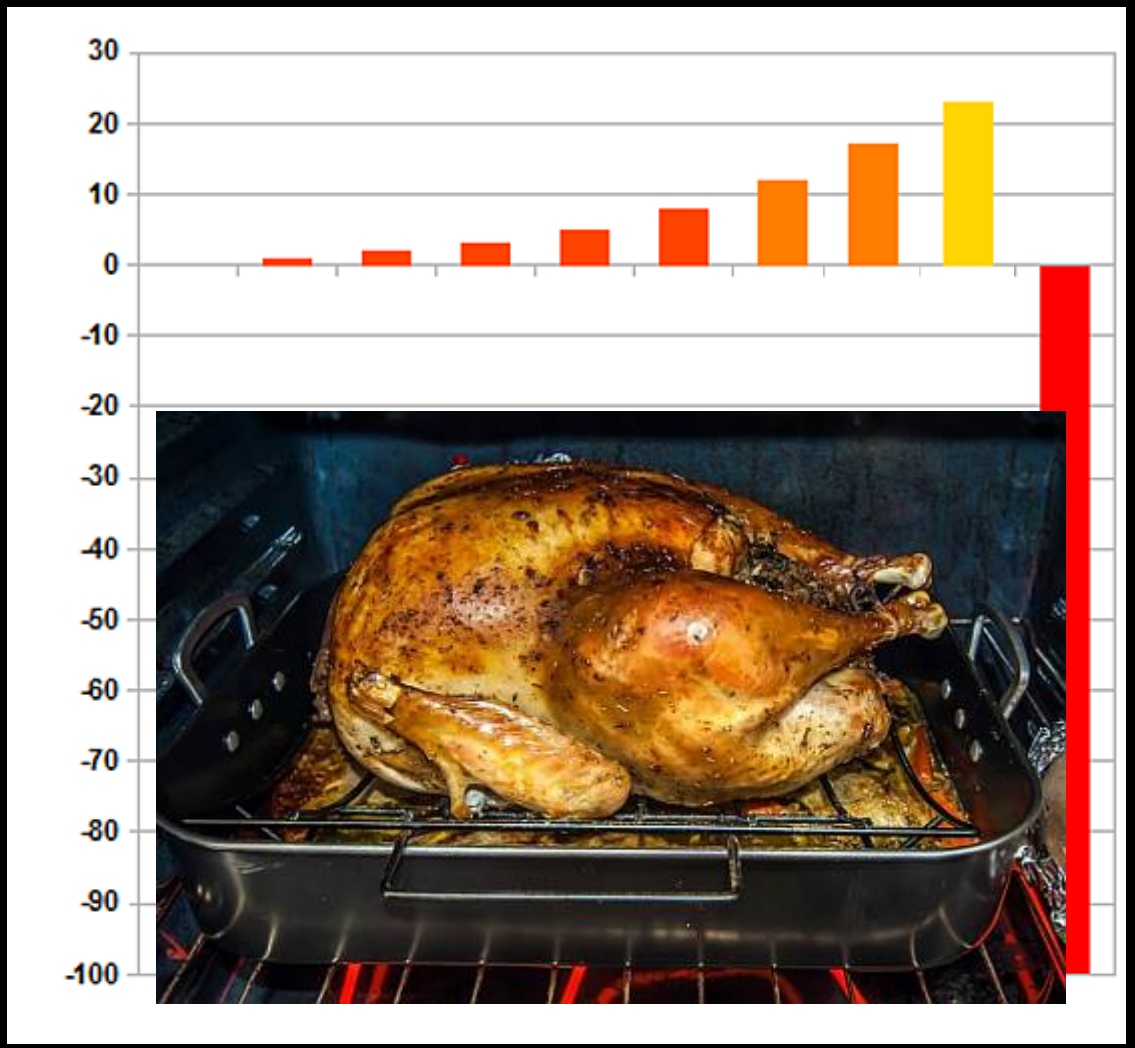
Operation increasingly at the stress limit

Digitalisation/Smart

(without systemic thinking)

How likely is a blackout?

+ There is no evidence!
– Turkey-Illusion
→ Important is: **Would we be prepared?**



How can a blackout be triggered?

Extreme weather events

Energy transition

Technical failure, „Aging Infrastructures“

Terrorist attacks

Earthquake

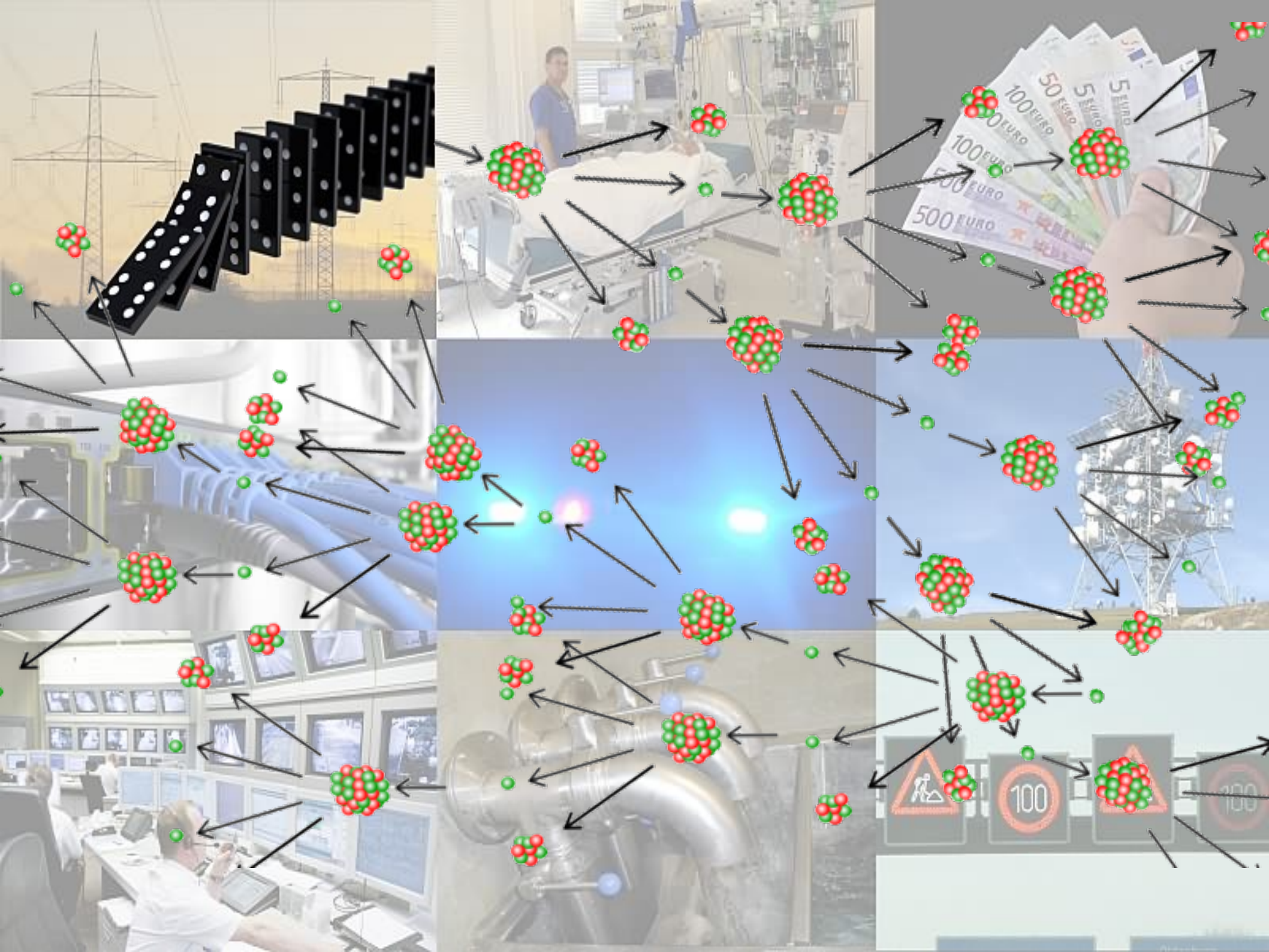
Cyber attacks

Solar storms

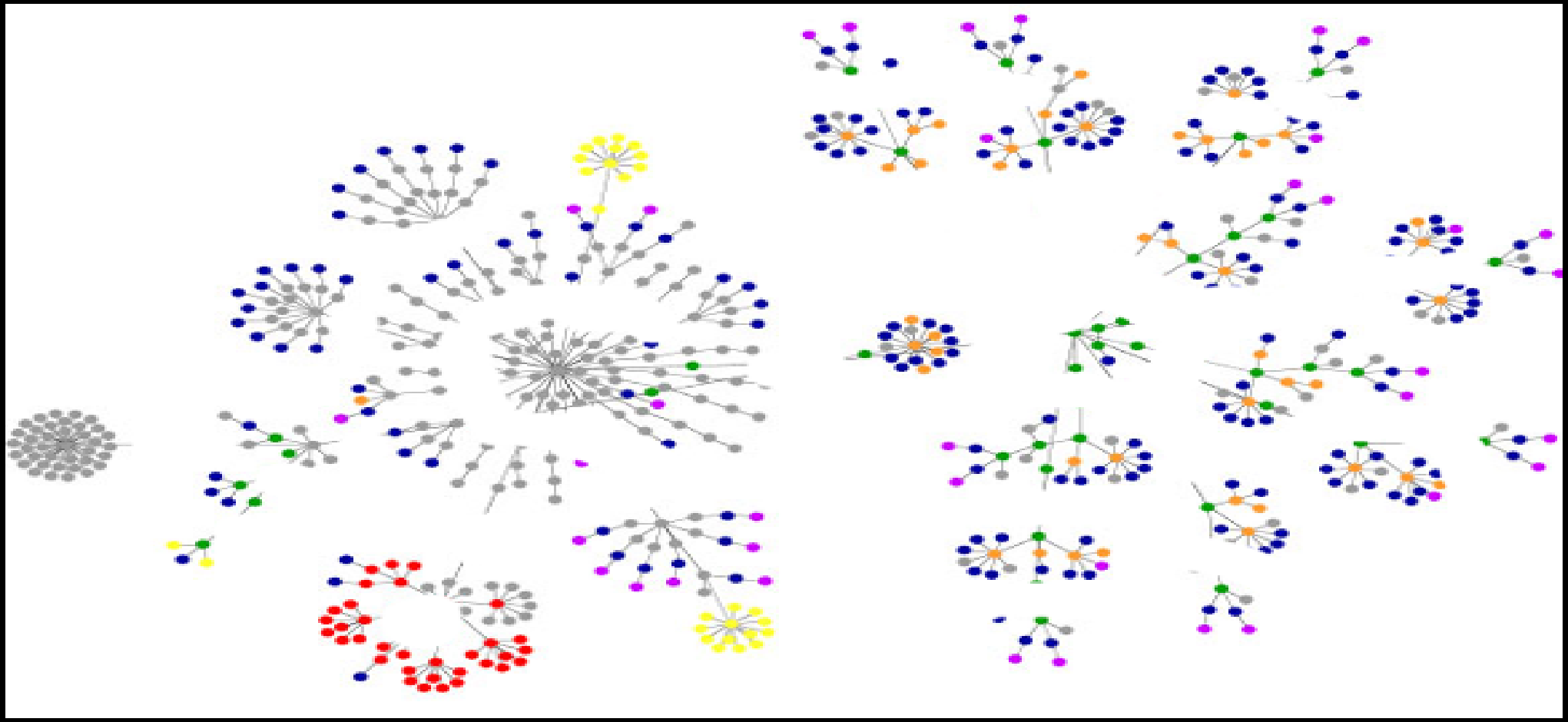
...

Market manipulation

System failure

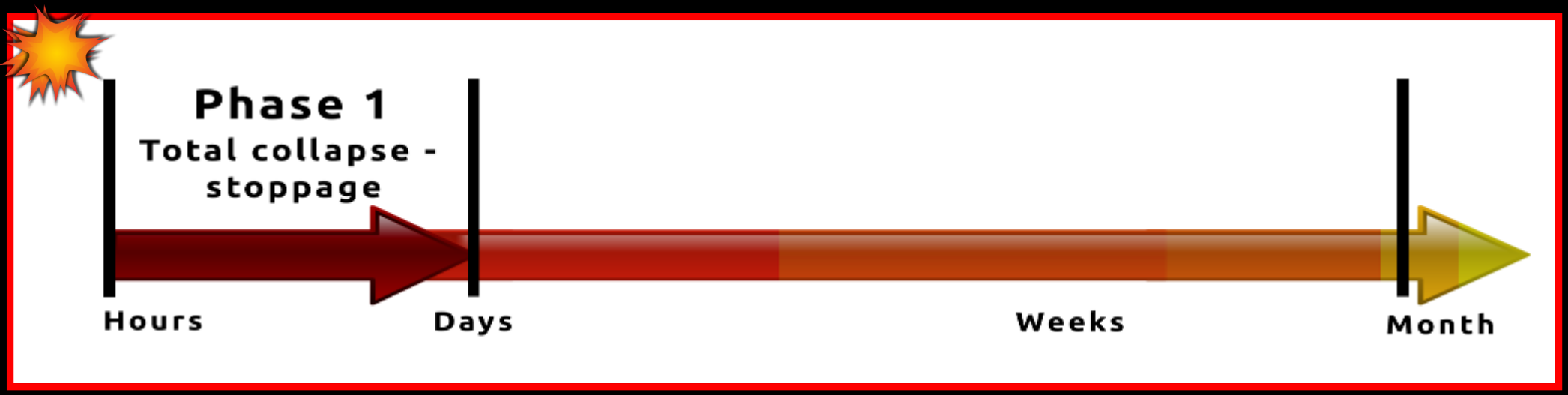

100 EURO
500 EURO
5 EURO
50 EURO
100
100

Without telecommunication systems society will fall apart into small structures!



"Management" as applied in other crises will not be possible! Self organisation on a local level!

If it happened ...



AUT: ½ - days (without infrastructure damages)

Europe: several days

Rebounds are possible

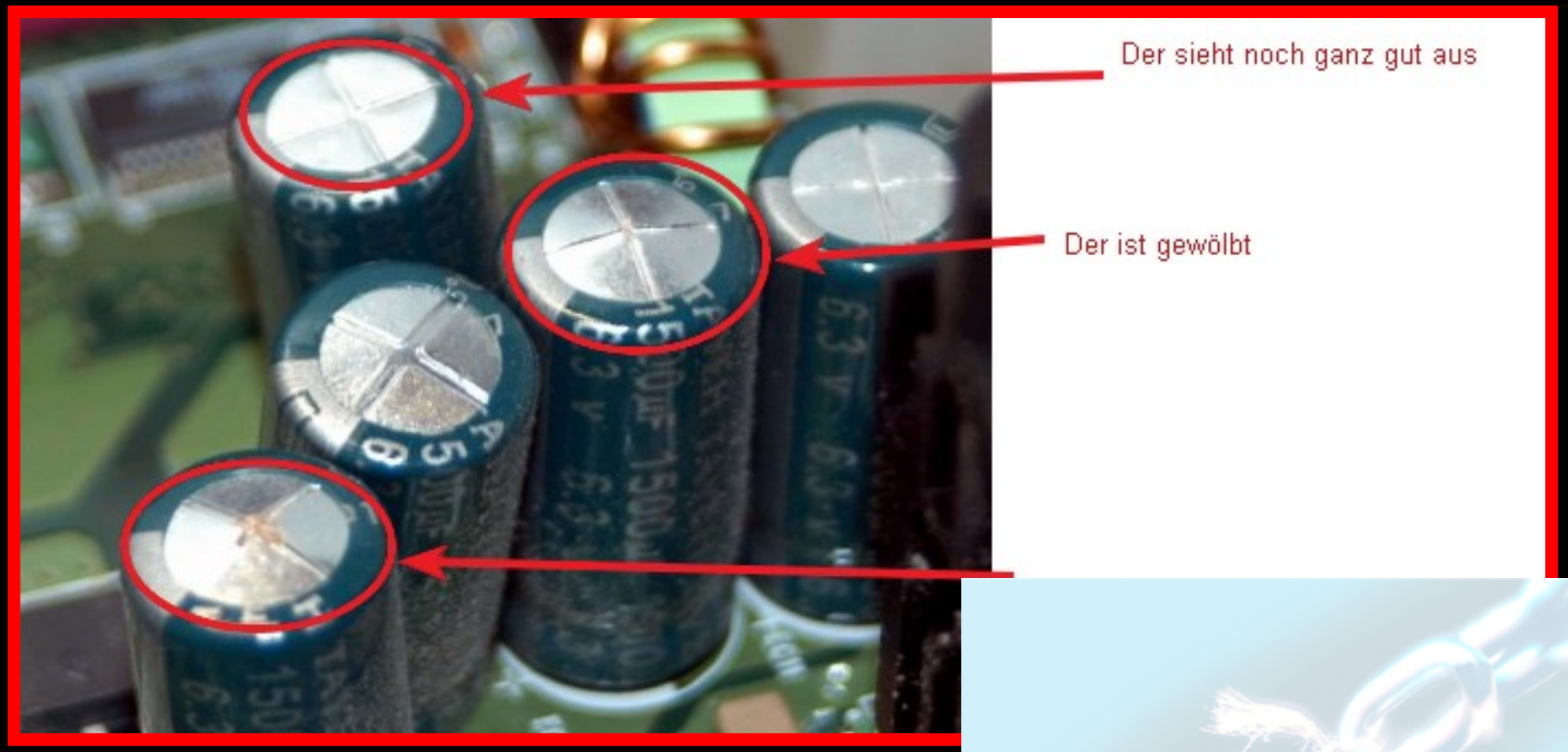
Telecommunication: several days (after power is back!)

Logistics? Goods? (weeks to month)

Damages?

!!! Transnational dependencies !!!

Experience in infrastructure operation (24/7)



... caused by electricity and hardware problems

Lower Bavaria phone service restored following outages in Vodafone's network

Tuesday 7 November 2017 | 11:03 CET | News

Mobile and fixed-line telephone services in the eastern part of the German state of Bavaria are functional again following outages that began in the early morning hours on 05 November due to a technical malfunction in Vodafone's network.

The outages were cau ion station in Vodafone's network. N re phone services at police stations and alc

Logistical dependencies

… even if power is back

Supply bottlenecks for weeks,
or even longer!

Experienced organisations will fail too

What can we do?


START
Action!

How are you personally prepared for it?

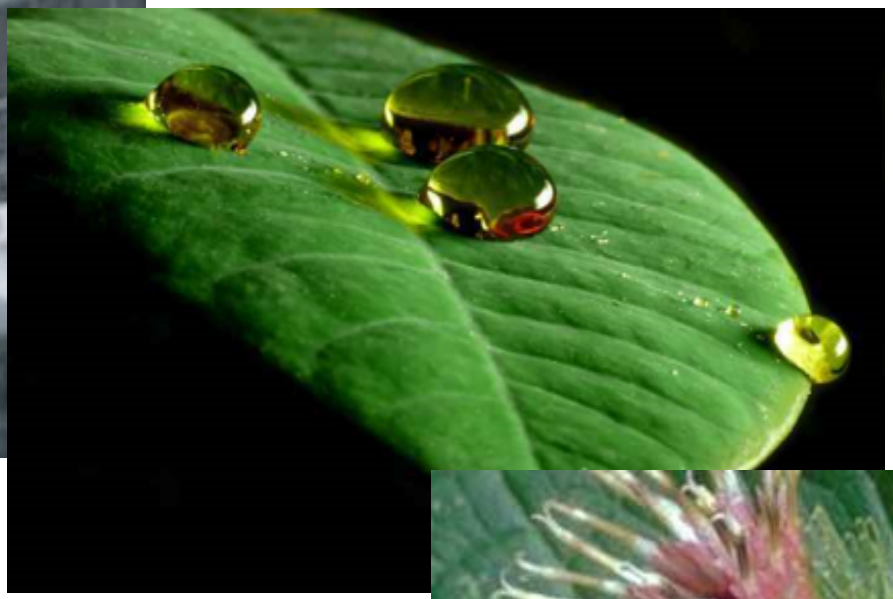
Knowledge in your family?

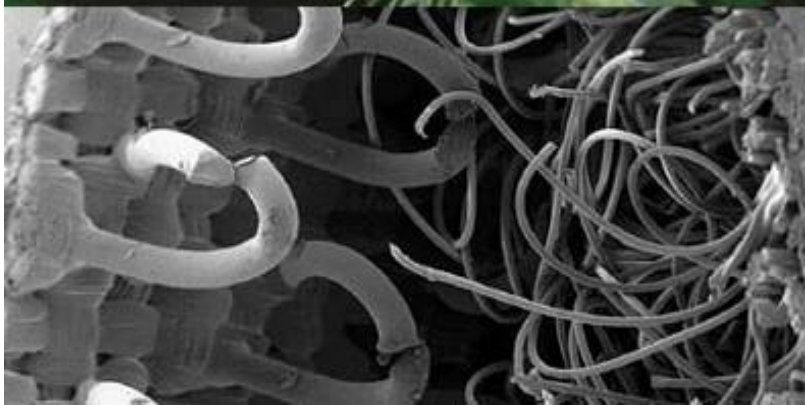
Ability to help yourself? Self storage?

Your employees and their families?

… reduce illusions of safety and security

Learning from nature …



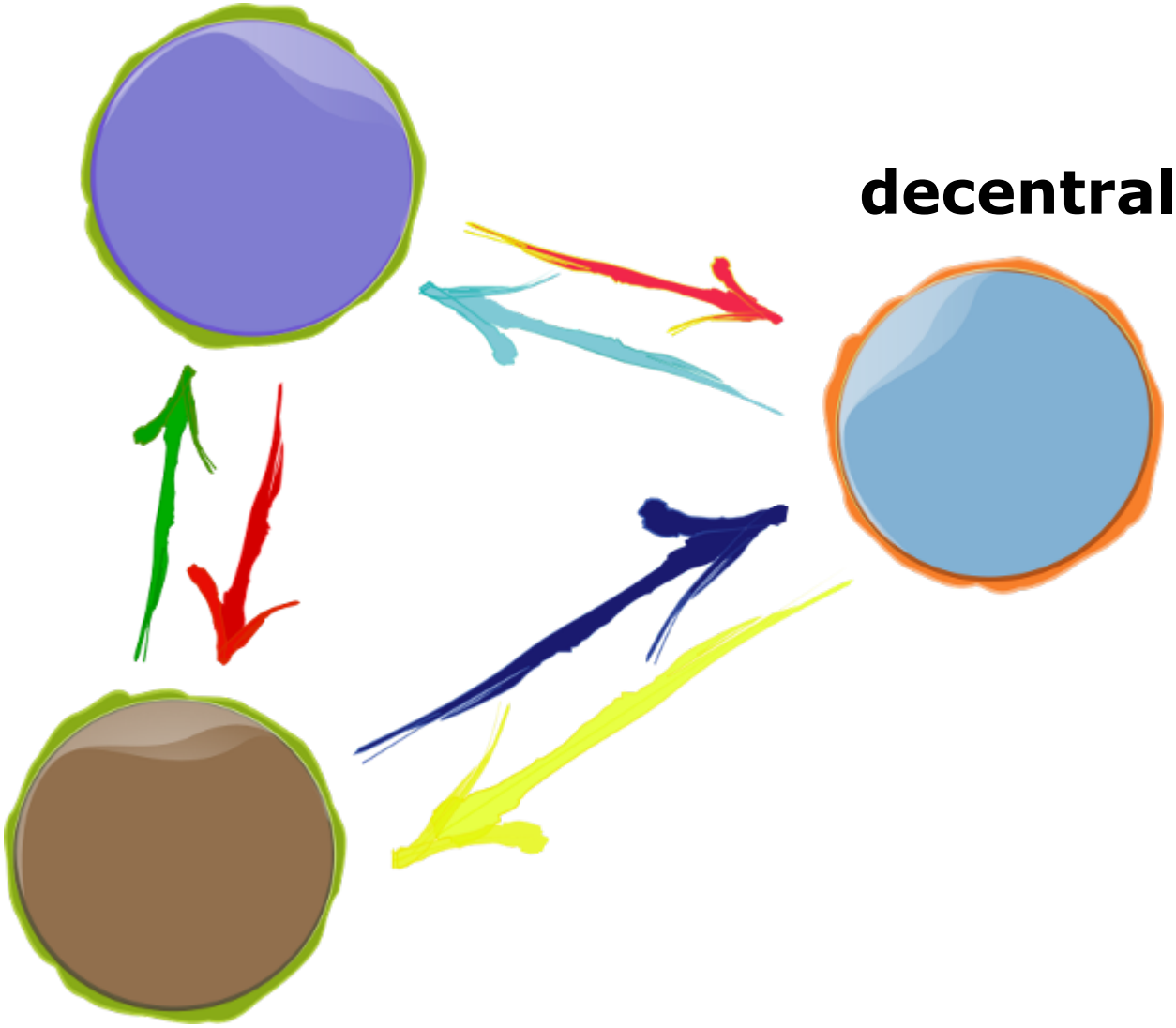


Small is beautiful

Small structures are more flexible and robust against strokes

Viable systems design

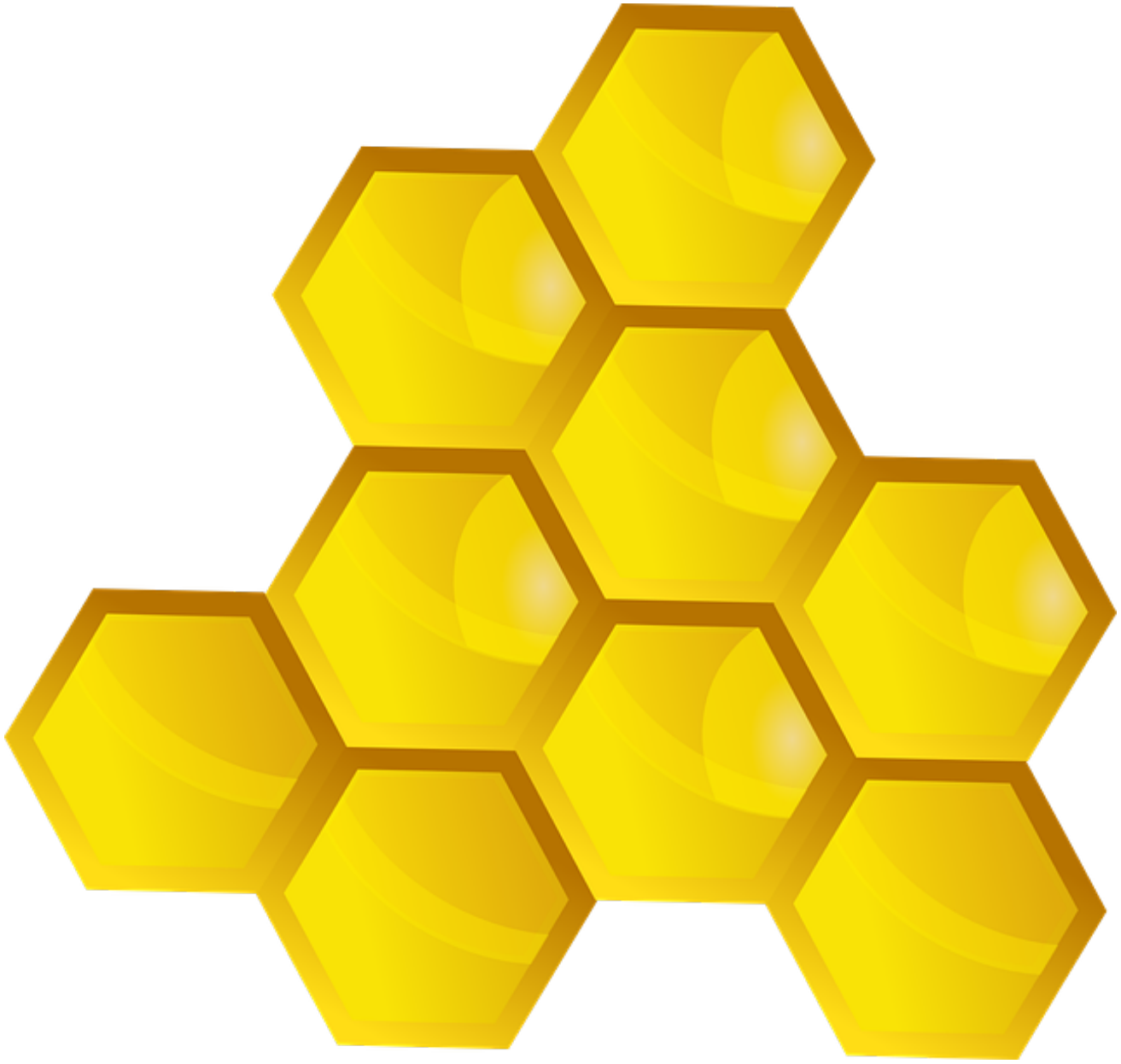
reduce energy- and resources consumption, simplicity



decentralisation

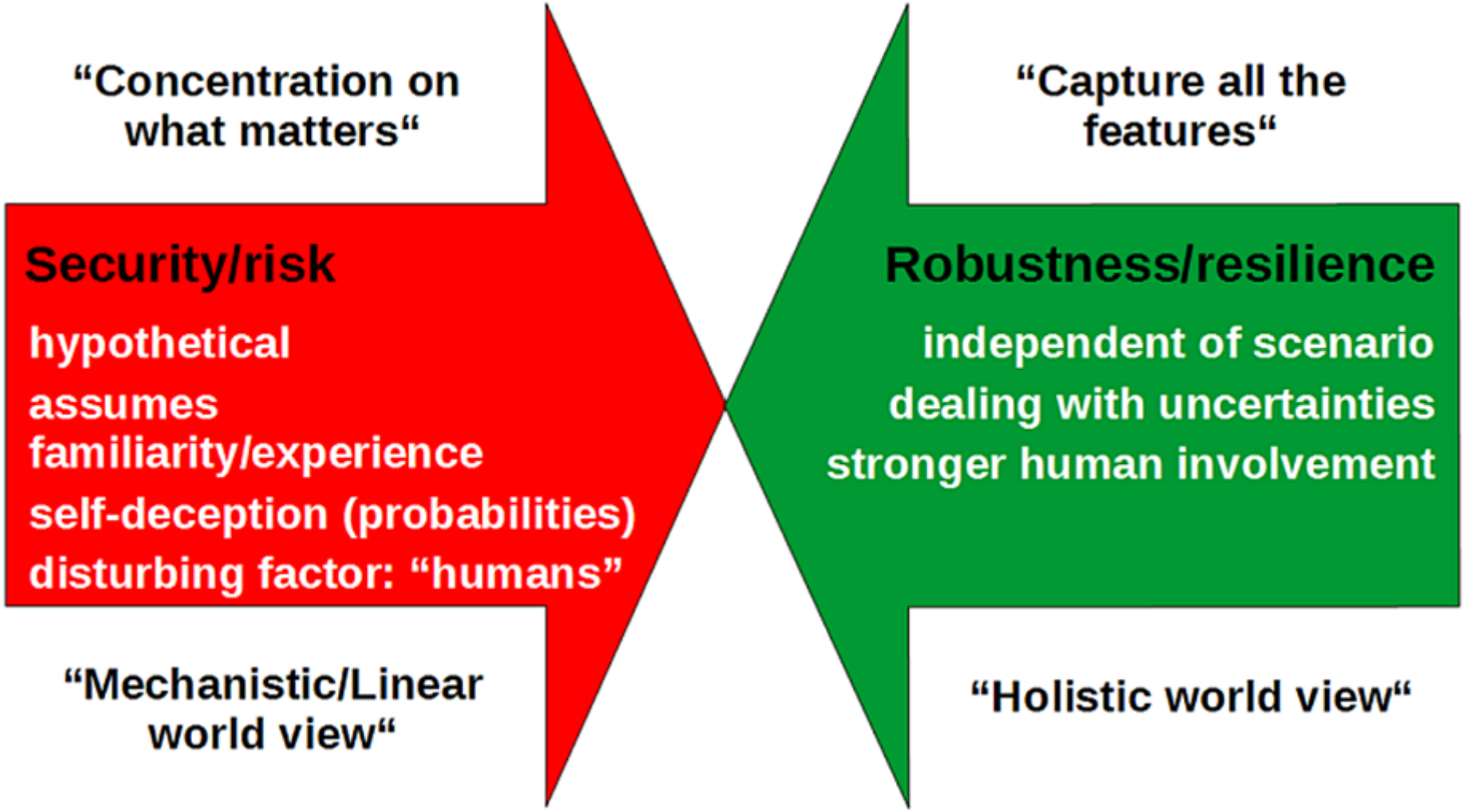
Error-friendly/Error tolerance

(Energy) cell system



Systems thinking and action

A holistic world view is needed



The consequences are relevant!

What are our goals?

Efficiency

"Doing things right"

Robustness

Resilience

Effectiveness

"Doing the right things"

Conclusions

Benefits ⊣ Risks - are we mature enough?

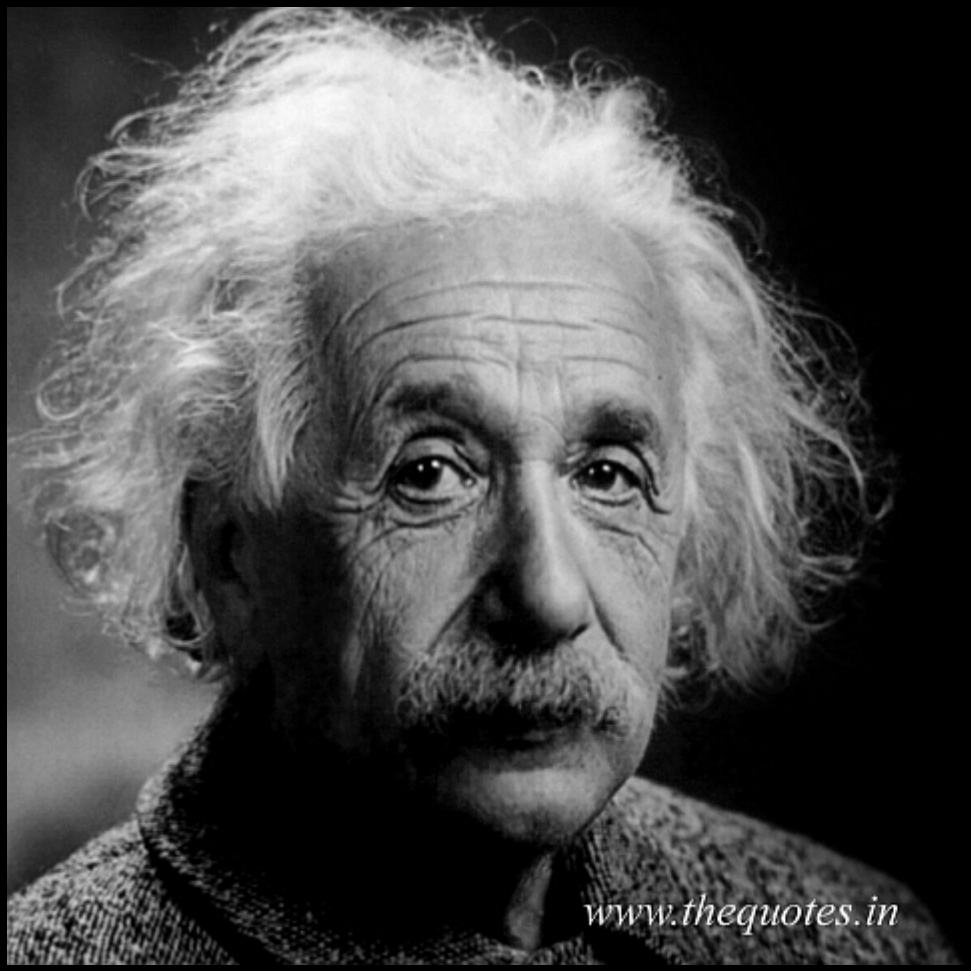
Critical Infrastructure Protection and Cyber Security …

… AND protection FROM Critical Infrastructures!

We also need …

… robust infrastructures and resilient people!

Then it is not all about technique …



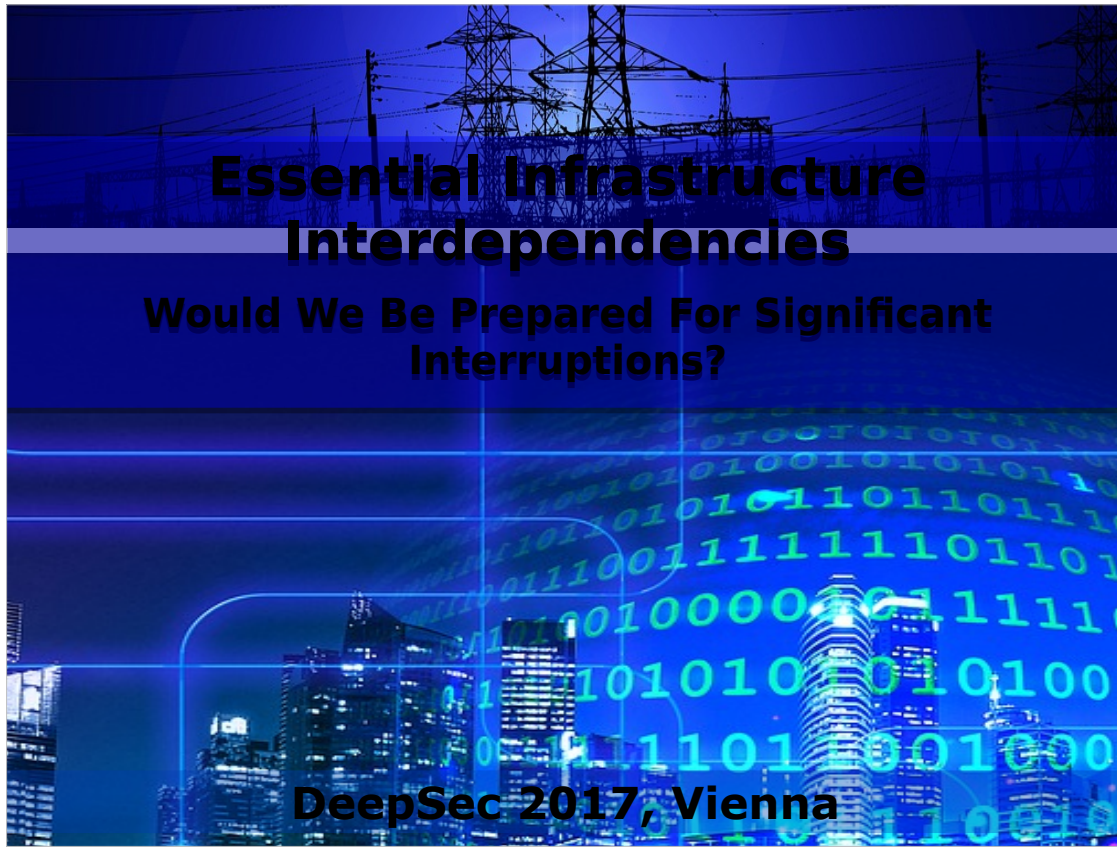
We cannot solve our problems with the same thinking we used when we created them.

Albert Einstein

Herbert Saurugg

1120 Wien
office@saurugg.net
www.saurugg.net

Herbert Saurugg has been a career officer in the ICT-Security Section of the Austrian Armed Forces until 2012. Since then he has been on leave and is engaged in raising awareness about the increasing systemic risks due to the rising interconnections and dependencies between many Critical Infrastructures, which is contributing to extreme events. He is known as an expert on the topic of blackout: a Europe-wide power-cut and infrastructure collapse. He is also a founding member of the association Cyber Security Austria which is the mastermind behind the European Cyber Security Challenge. As a result of his systemic reflections he is calling for more efforts to raise awareness and resilience throughout our societies to face major extreme events in the foreseeable future.


Essential Infrastructure Interdependencies
Would We Be Prepared For Significant Interruptions?
DeepSec 2017, Vienna

The title of my talk is, of course, too broad.

Therefore I would like to bring your attention to two special topics, even though that will be possible only on a very small meta level: Interconnectivity & digitalisation … and to our personal reliance on infrastructures.

Connectivity leads to Complexity!

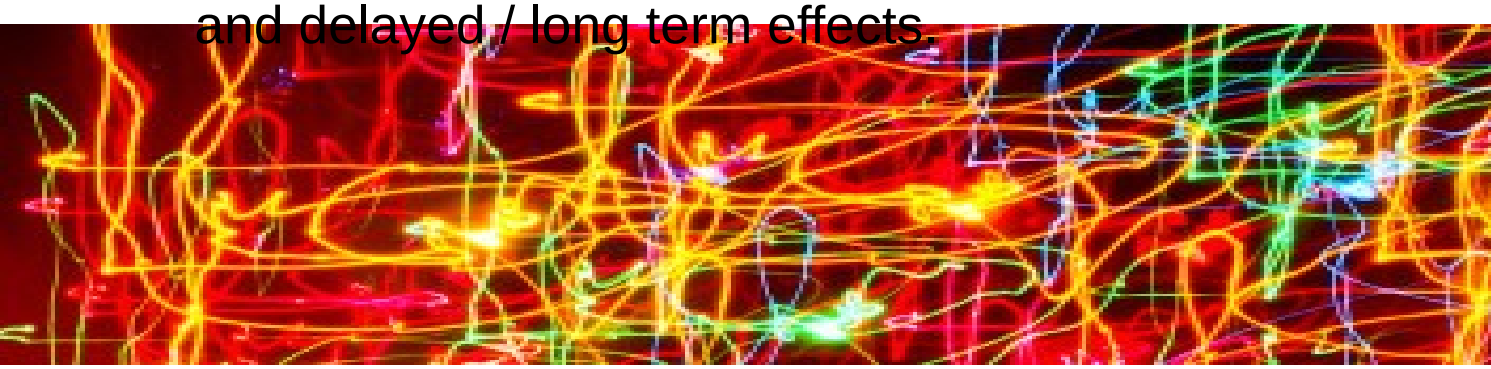
- **Complexity leads to Systemic Risks!**
- **Systemic Risks could lead to X-Events!**

The first point I would like to highlight is that connectivity leads to complexity. But most people, and even decision makers on all levels of society outside this room, are often not aware. And even fewer people know that complexity leads to systemic risks; nor do they have an idea what it could mean if, as a result, X-Events were to happen. Even though we know that X-Events would change our way of life dramatically. One problem is that humans orientate their view based on events which they have already experienced. But with our technical interconnectivity and interdependencies we are entering relatively new territory.

What does Complexity mean?

- Changing system properties (feedback-loops)
- Non-linearity (predictions, risk management fail)
- Increasing dynamic (faster and faster …)
- Irreversibility (no way back!)
- Emergence (1+1=3; cause ⊣ effect)
- Small causes, large effects ("butterfly effect")
- Delayed / long term effects
- …

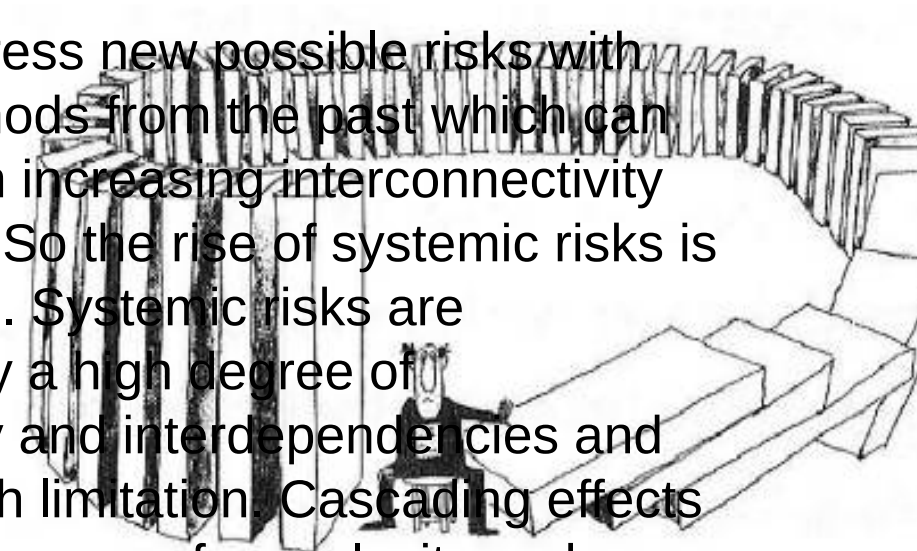
I am sorry that I cannot go into detail about what complexity means. Therefore I would like to highlight to aspects - small causes, large effects and delayed / long term effects.



Systemic Risks

- **High degree of cross-linking / interdependencies**
  - missing outreach limitation
- **Feedback loops ⊟ non linearity!**
- **Cascading effects are possible**
- **Triggers and effects are systematically underestimated**

Current risk management methods fail!



We still try to address new possible risks with successful methods from the past which can hardly cope with increasing interconnectivity and complexity. So 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 responsible persons and organisations.

Therefore I briefly want to address small causes, large effects, as we have seen more often in recent months, when unsecure Internet of Things was misused to attack critical infrastructures on a level which we have not seen until now. From one point of view, these devices, such as IP-cameras, toasters, fridges, routers and so on, are no danger if they are unsecure, which is the view of manufacturers. But criminals are now able to bring millions of those devices together to make a very powerful weapon. And what I fear is that we will see some major interruptions of infrastructures in the near future. One major problem is that we have not learned much from the past 20 years of IT-security problems which are still unsolved. 20 years ago devices were still often offline and threats could not spread as they do today

DDoS Attacks Cause Train Delays Across Sweden

By Catalin Cimpanu

October 13, 2017 05:40 AM 1

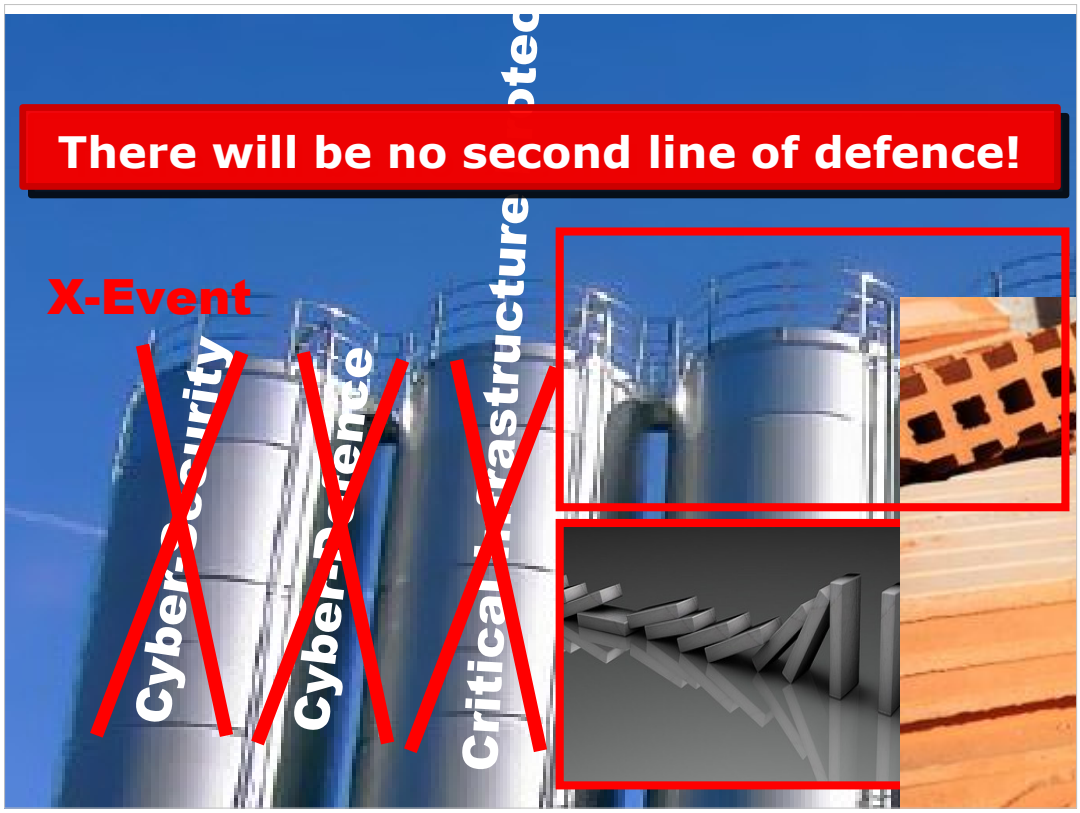
DDoS attacks on two separate days have brought down several IT systems employed by Sweden's transport agencies, causing train delays in some cases.

Study 2014

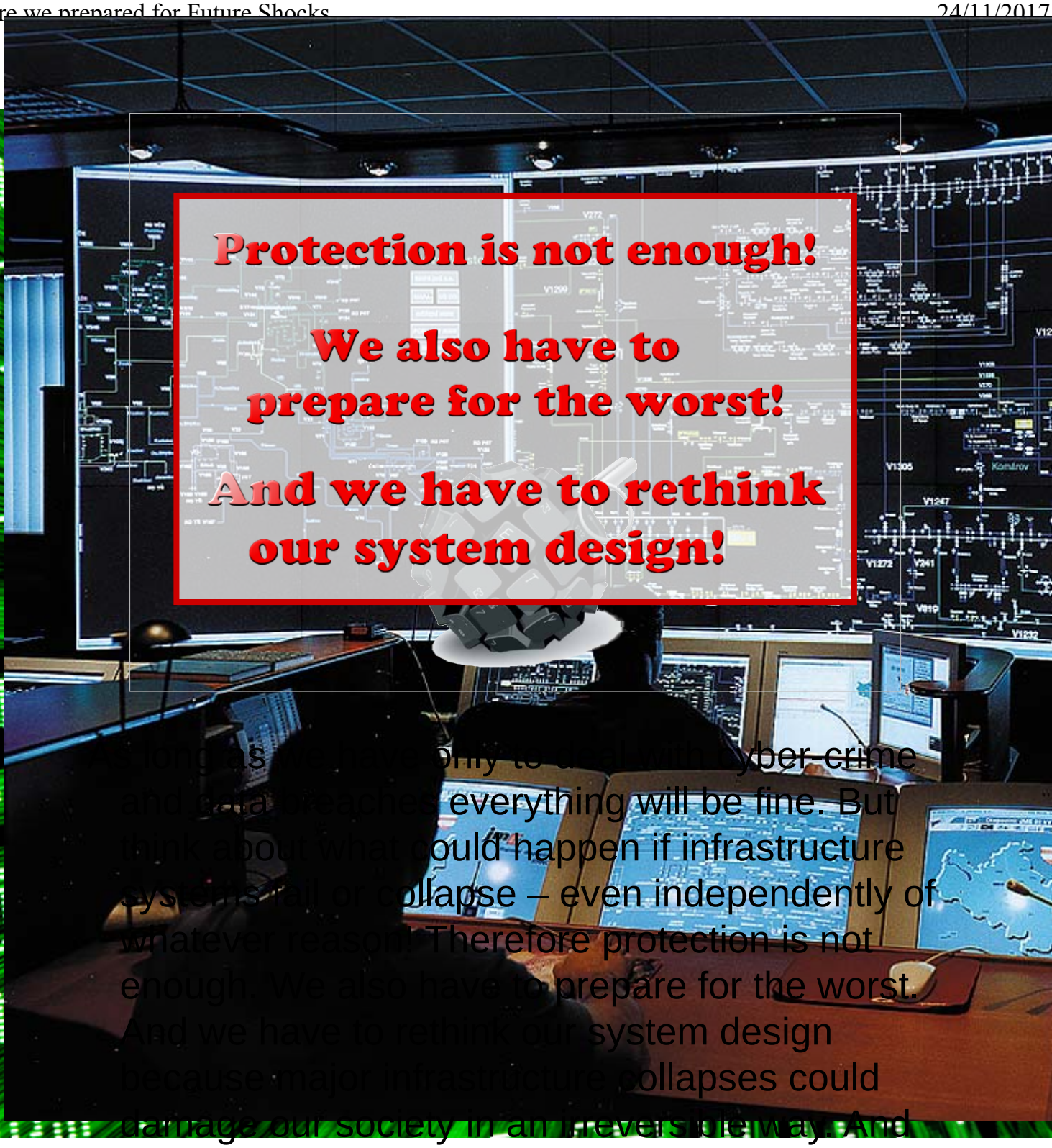
The way in which the complexity of interconnected risks is assessed is painfully similar to how financial risks were assessed prior to the 2008 crash … in the end, it was this very complexity which helped bring the system down.

http://www.saurugg.net/2014/blog/cyber/beyond-data-breaches-global-interconnections-of-cyber-risk

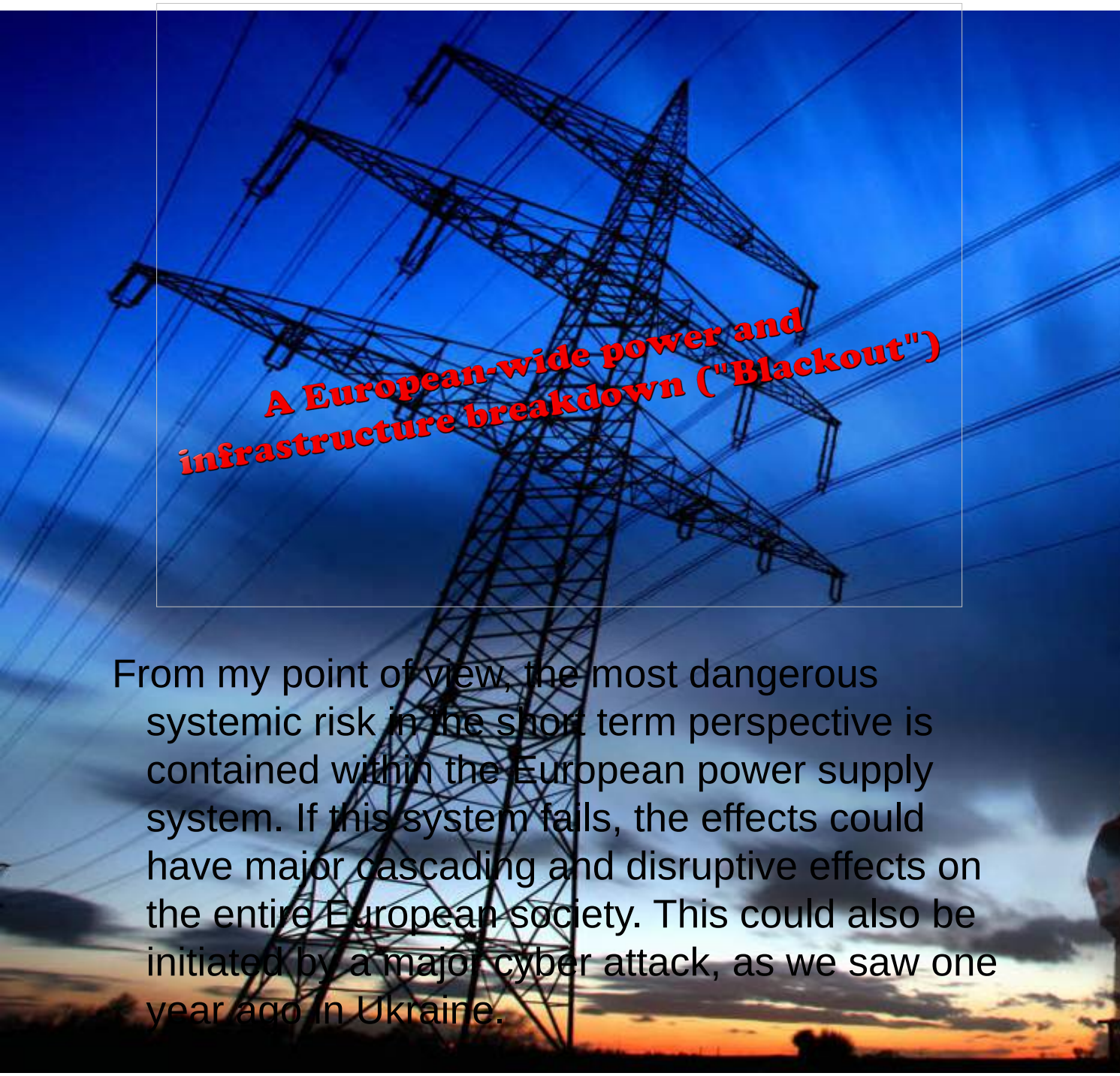
As early as in 2014 the study “beyond data breaches” stated: “The way in which the complexity of interconnected risks is assessed is painfully similar to how financial risks were assessed prior to the 2008 crash … in the end, it was this very complexity which helped bring the system down.”



But we still react as in past times with “silo”-organisations and structures, like police are responsible for cyber-security, military forces for cyber-defence. Then there is also critical infrastructure protection which is focusing more on physical protection. But if cybersecurity fails on a high level, there will be no second chance or line of defence, which is how responsible leaders are often thinking and communicating.

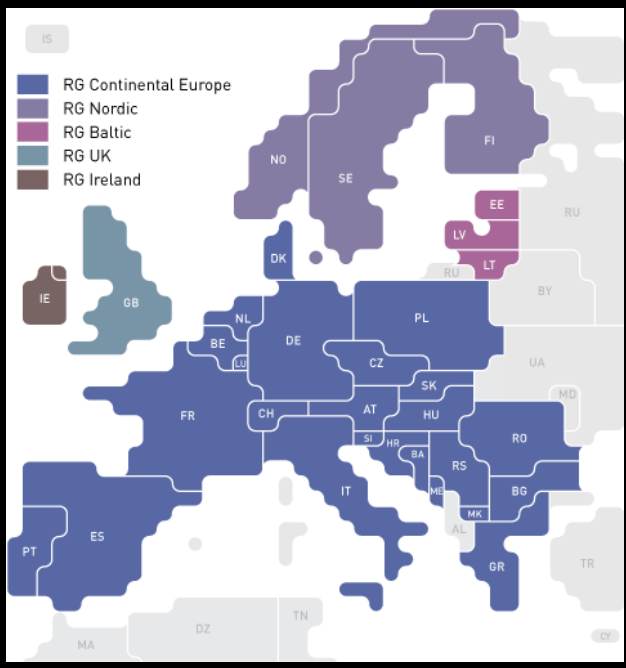


[illegible] only to deal with cyber-crime and data breaches, everything will be fine. But think about what could happen if infrastructure systems fail or collapse – even independently of whatever reason! Therefore protection is not enough. We also have to prepare for the worst. And we have to rethink our system design because major infrastructure collapses could damage our society in an irreversible way. And we are not prepared to handle such X-Events, especially in Europe where we are used to having the best supply system in the whole world.



From my point of view, the most dangerous systemic risk in the short term perspective is contained within the European power supply system. If this system fails, the effects could have major cascading and disruptive effects on the entire European society. This could also be initiated by a major cyber attack, as we saw one year ago in Ukraine.

The European Power Supply System



"Too Big to Fail"

Unilateral system interventions

Market and politics are ignoring physics

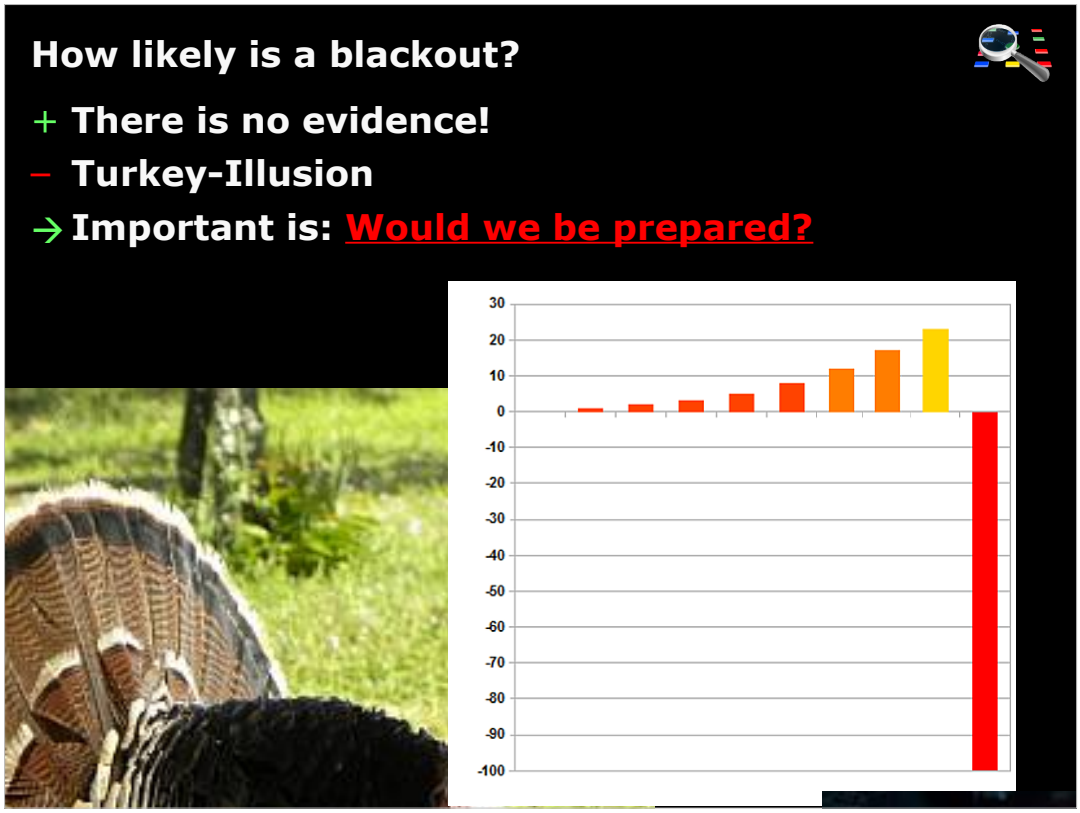
Operation increasingly at the stress limit

Digitalisation/Smart

(without systemic thinking)

You will know that power is not coming only on a very high level of reliability from the socket. Behind it, there is a huge supply system, which includes many countries. But if you read the news or follow statements about power supply, you will get the impression that there are only national power supply systems. And actions are very similar. So every country in Europe does its own energy transformation in a different direction but within a very sensitive European-wide system. You are dealing with complexity and will know that this could not work in the long term.

Some major topics we can see at the moment: We have a system that is "Too Big to Fail", a term which you will have known at least since the financial crisis in 2007/2008. We also know



Of course there will now be the question as to how likely a collapse is. The positive news is there is no evidence! The last one where several countries were involved was in 1976. But there is also the phenomenon called the Turkey Illusion. A turkey's trust in its owner, who feeds it daily, will increase in view of the owner's good care. The turkey doesn't know that this is only for one purpose. When turkeys are traditionally slaughtered on the day before Thanksgiving, the turkey will undergo a significant interruption of its trust.

Humans often act similarly. We are looking back at how successful we or a system have been until now and estimate that this will also continue in future. At the same time we tend to overlook significant changes, unlike turkeys

How can a blackout be triggered?

Extreme weather events

Energy transition

Technical failure, „Aging Infrastructures“

Terrorist attacks

Earthquake

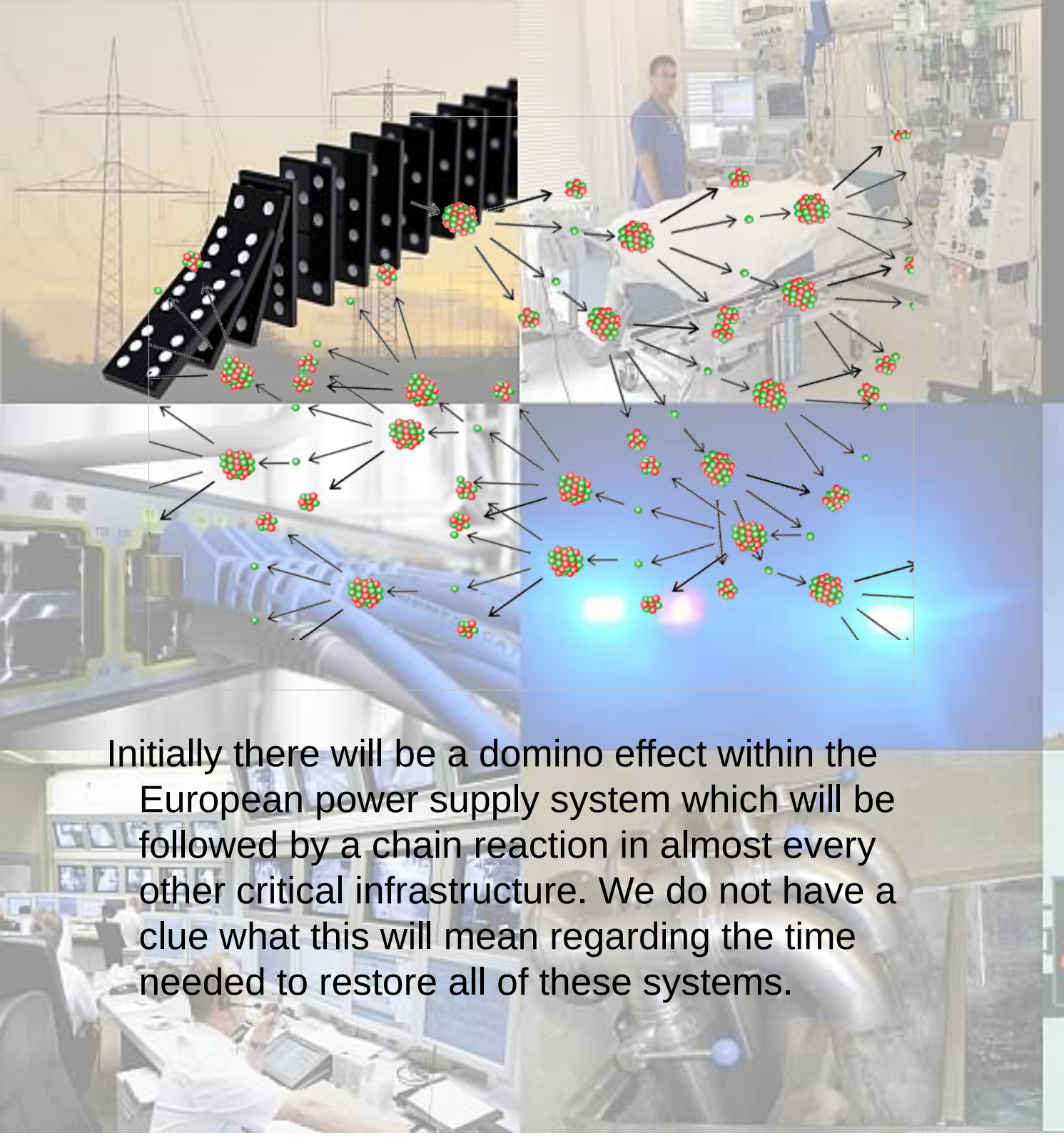
Cyber attacks

Solar storms

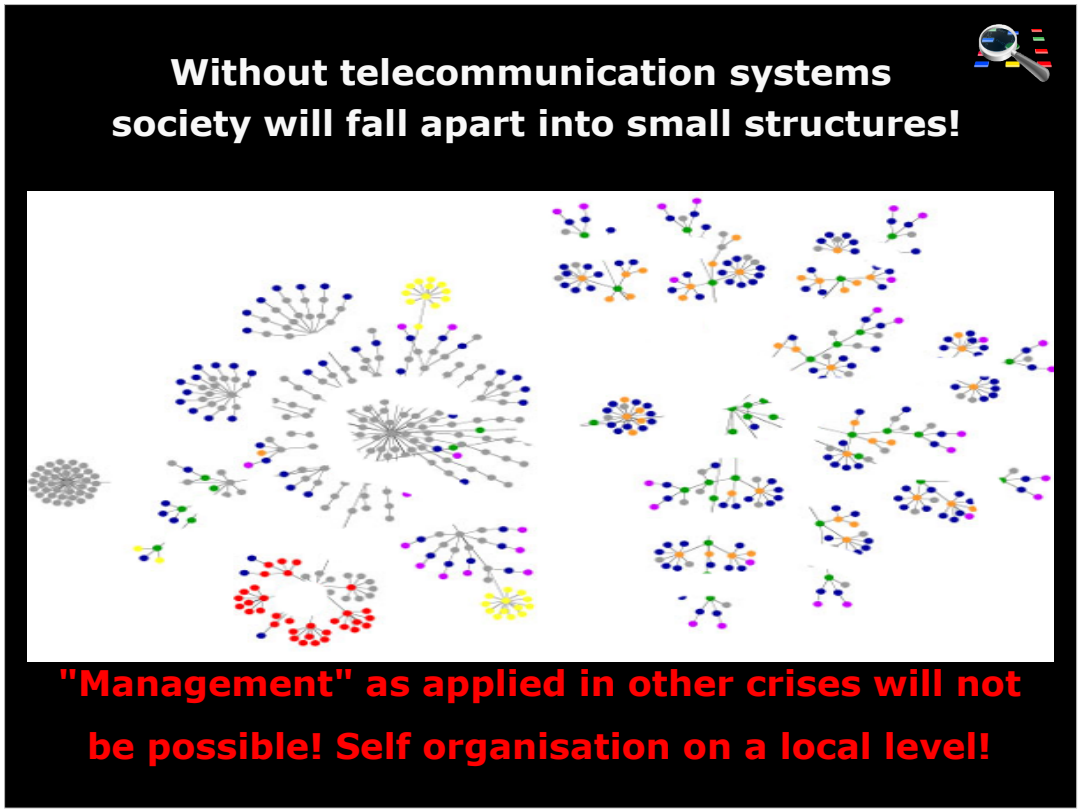
...

Market manipulation

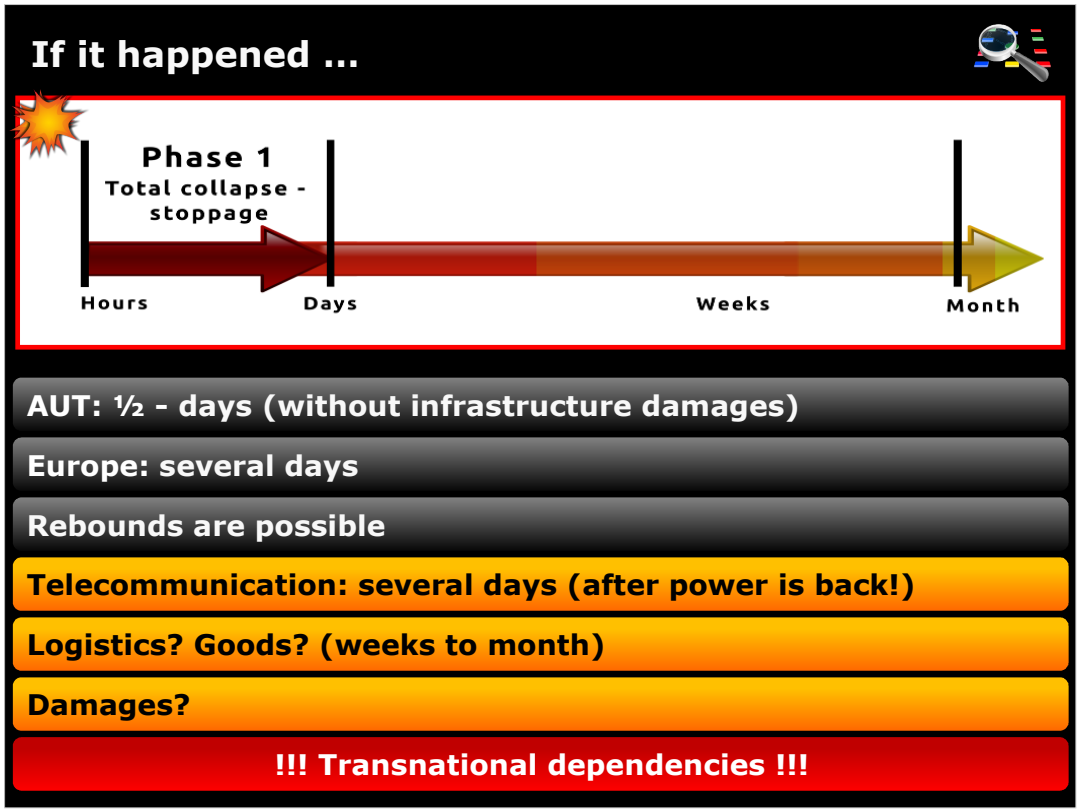
System failure



Initially there will be a domino effect within the European power supply system which will be followed by a chain reaction in almost every other critical infrastructure. We do not have a clue what this will mean regarding the time needed to restore all of these systems.



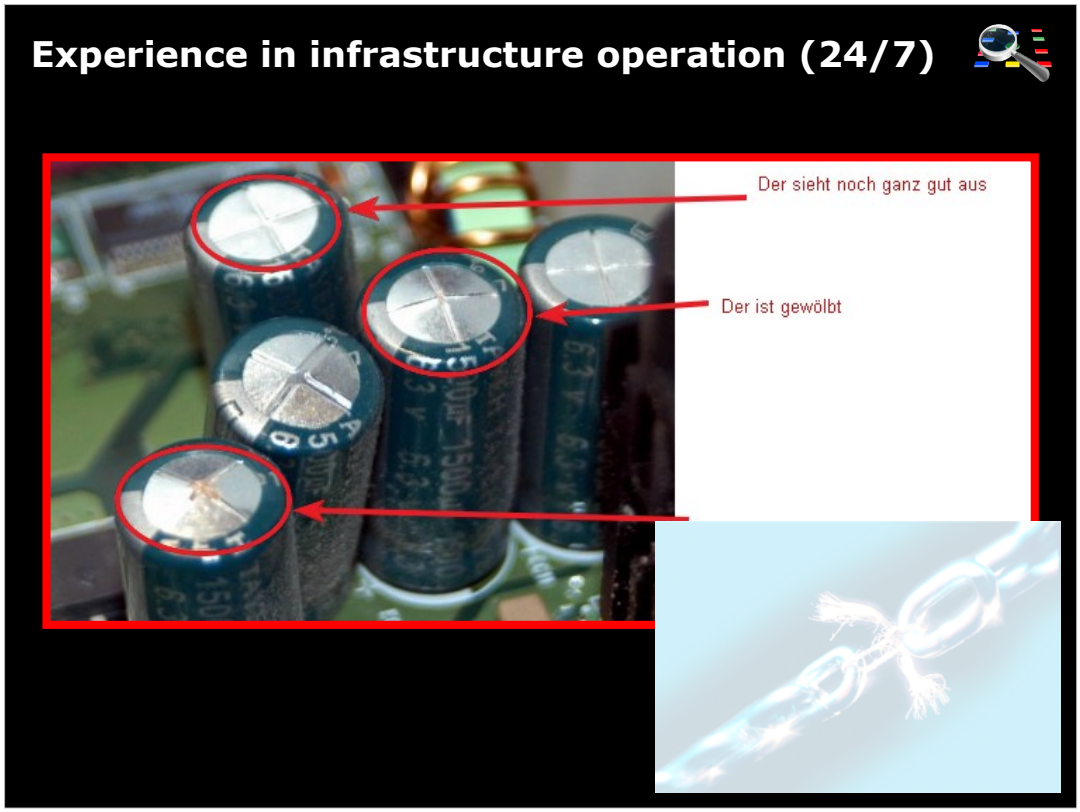
One major effect will be that within a very short time the whole civil telecommunication infrastructures will collapse. If not by the power-cut then by an overload, because many people will try to contact other people. Without communication, our society will fall apart into small structures. Our normally successful crisis management will not be possible any more. We will have to self organise on a local level, which we are not often used to doing any more.



One thing that is heavily underestimated is that in the event of a blackout there will be two major phases.

Phase 1: Total collapse – stoppage. For Austria I am estimating a half to some days until the power supply system will be restored again, if there are no major infrastructure damages, because of our structures and many hydro plants. On the European level, we will have to expect a few days. And it is very likely that rebounds during restoration could bring down the whole system again.

Phase 2: Time will be needed to restore other infrastructures and supply chains after power supply has been restored. And it will last for days, weeks and in some cases also months



I have learned from different sources that organisations which are running infrastructures made the experience that up to 30 percent of the power adapters failed after a larger power cut because of destroyed capacitors. Normally this is not noticed, because it will be possible to get enough spear parts. But think about what this could mean in case of a blackout, especially in the telecom sector!

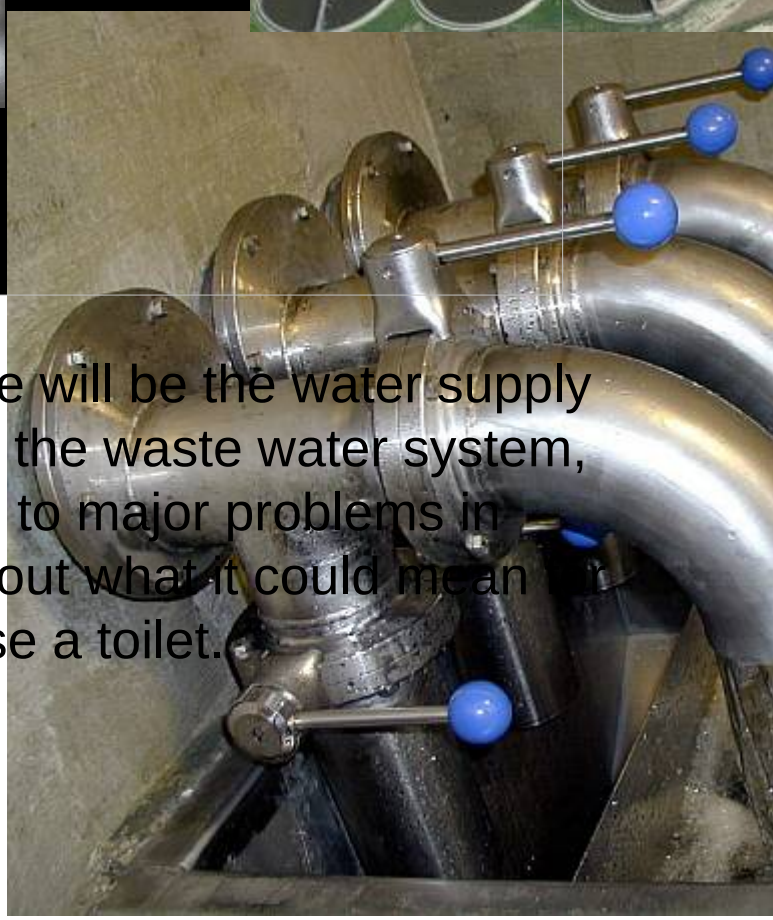
… caused by electricity and hardware problems

Lower Bavaria phone service restored following outages in Vodafone's network

Tuesday 7 November 2017 | 11:03 CET | News

Mobile and fixed-line telephone services in the eastern part of the German state of Bavaria are functional again following outages that began in the early morning hours on 05 November due to a technical malfunction in Vodafone's network.

The outages were cau ion station in Vodafone's network. N e phone services at police stations and alo



An other major challenge will be the water supply system and especially the waste water system, which could soon lead to major problems in urban areas. Think about what it could mean for you if you could not use a toilet.

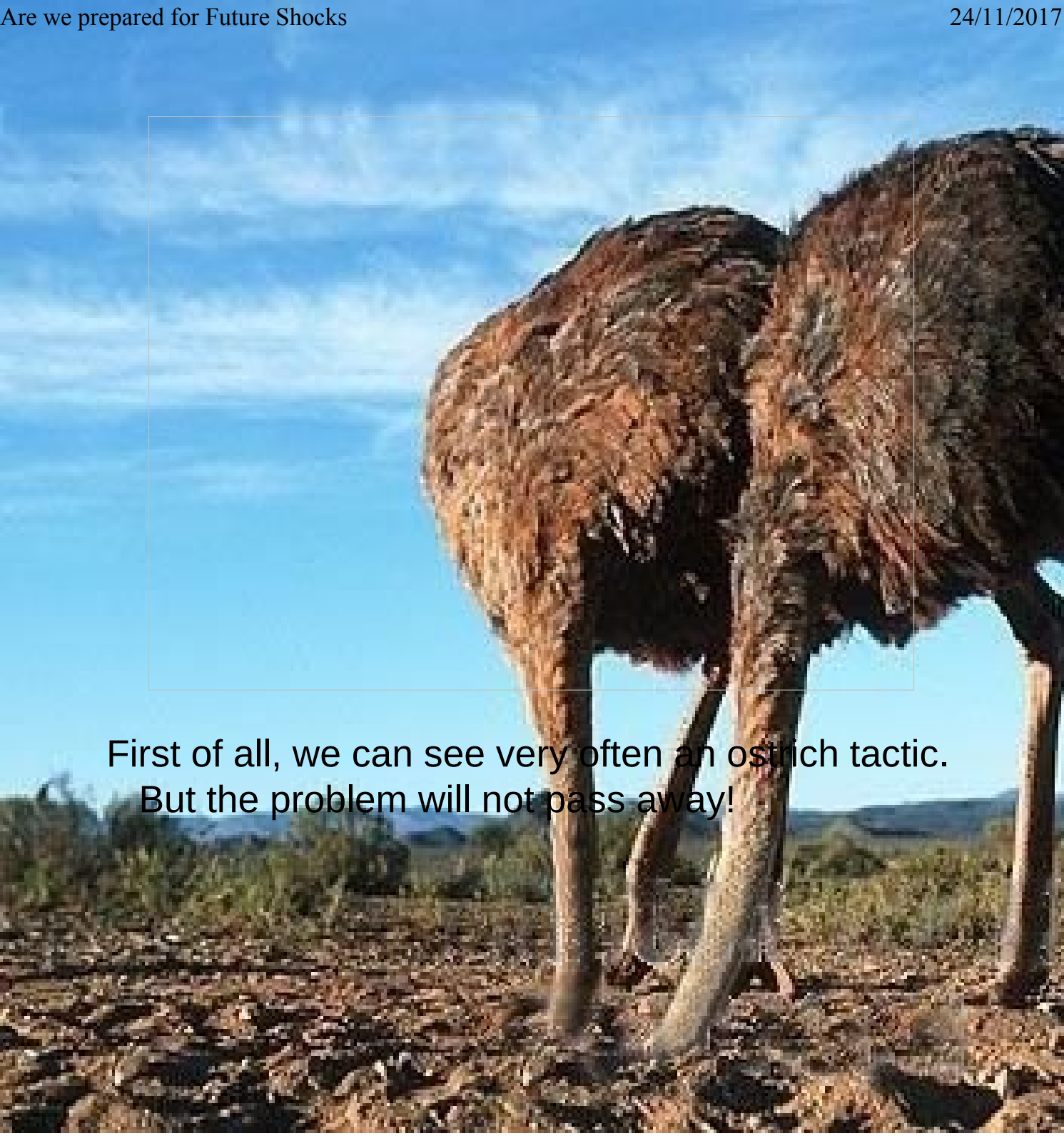
But also the whole supply chains will fail!

Think also about the food supply which will also stop instantaneously. And it will also be a major challenge in phase 2, because it will be not restored very soon. There is an Austrian study which stated that about 3 million people will have a major problem no later than on the 4th day without an external food supply. There is no organisation, no process, no storage to fix this problem. So this is one of the most important points to raise resilience and the capability to cope with such possible events.

Emergency services, security forces and even military forces will not be able to face a major infrastructure collapse. Our whole societies will fail within days.

What can we do?

Enough bad news! Now I would like to address what could we do.


First of all, we can see very often an ostrich tactic.
But the problem will not pass away!


S
T
A
Action!

How are you personally prepared for it?

Knowledge in your family?

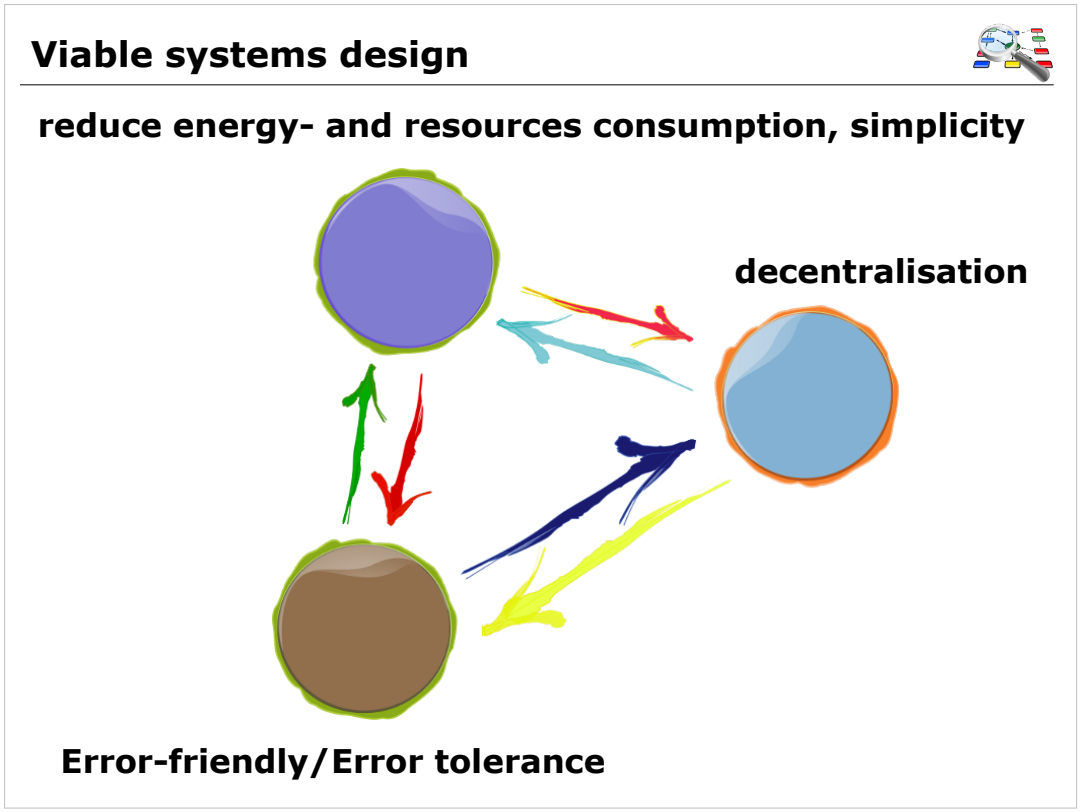
Ability to help yourself? Self storage?

And this starts with a simple personal preparedness of people to bypass major food supply chain interruptions. But this is the most important base for handling X-Events, also for emergency services and security forces which often forget to stress this point to their personal contacts and their families.

I think one of the most important short term points will be to reduce illusions of safety and security of our supply systems. They have more and more vulnerabilities where protection becomes harder and harder and, at the same time, systemic risks and danger of X-Events grow. Therefore we should also prepare for possible interruptions and collapses, even though we should still try anything to prevent it. But it will be irresponsible if we try only to prevent events, because that is too little. And remember the Turkey Illusion.

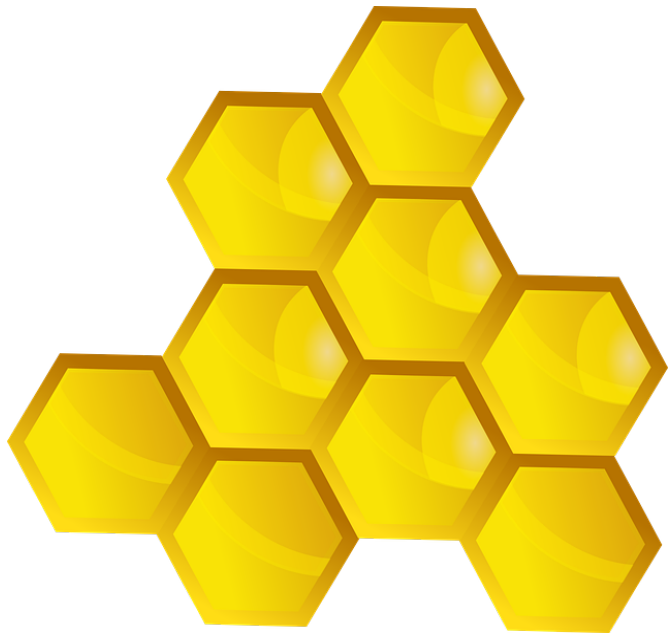
Small structures are more flexible and robust against strokes

From a longer-term point of view, we should learn more from nature to design viable technical systems. As “small is beautiful” because those structures are more flexible and robust against strokes.



Other points are the reduction of the consumption of energy and resources to decrease dependencies. Also simplicity will be needed. You can not manage complex systems with centralised structures: you will need a decentralised self organisation (autonomous systems). Systems must be also error friendly. And we should stop to try patching humans: this will not be successful!

(Energy) cell system



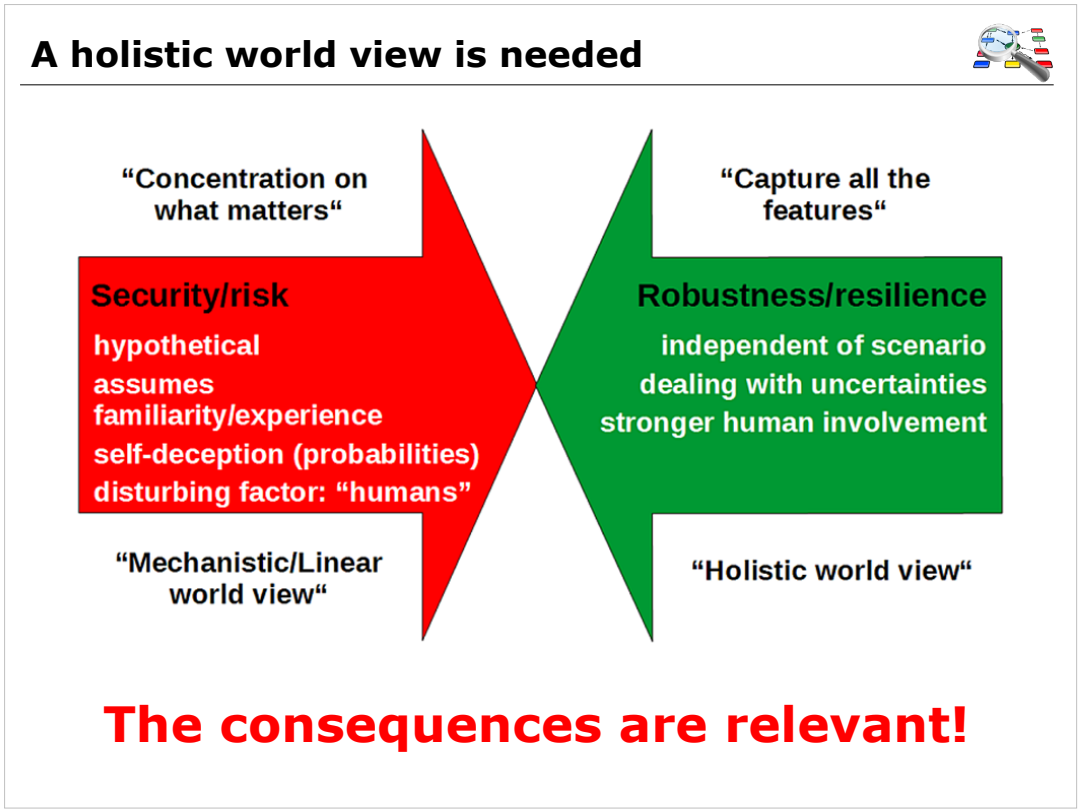
From nature we know that cellular structures were successful and have survived. Which should not be seen only on a technical level, but also including people – which is often forgotten in our current energy transformation process. Decentralised generation is insufficient.

Systems thinking and action

Therefore it will need systems thinking and action to bring down old old-fashioned silo boundaries.

Security is always relative and subjective. But the choice of how we implement the process of examination and our resources is up to us. Security does not mean the elimination of risk, but rather dealing with it sensibly. Because security and continued development are not possible without insecurity. The polar opposites are mutually dependent.

As has also emerged from the investigation, we should step back from those “silo” viewpoints so common to date, because they do not correspond with networked reality and, in the best case, only create apparent security.



With concentration on what matters and with a focus on security and risks we are still trapped in an Industrial Age view, but we have to adapt to a holistic world view and seek more for robustness and resilience. From my point of view, only people can be resilient which means to be capable of learning and adapting. Technique can be only robust and support resilience of people, which is very often overlooked in technical considerations.

What are our goals?

Efficiency

"Doing things right"

Effectiveness

"Doing the right things"

Robustness

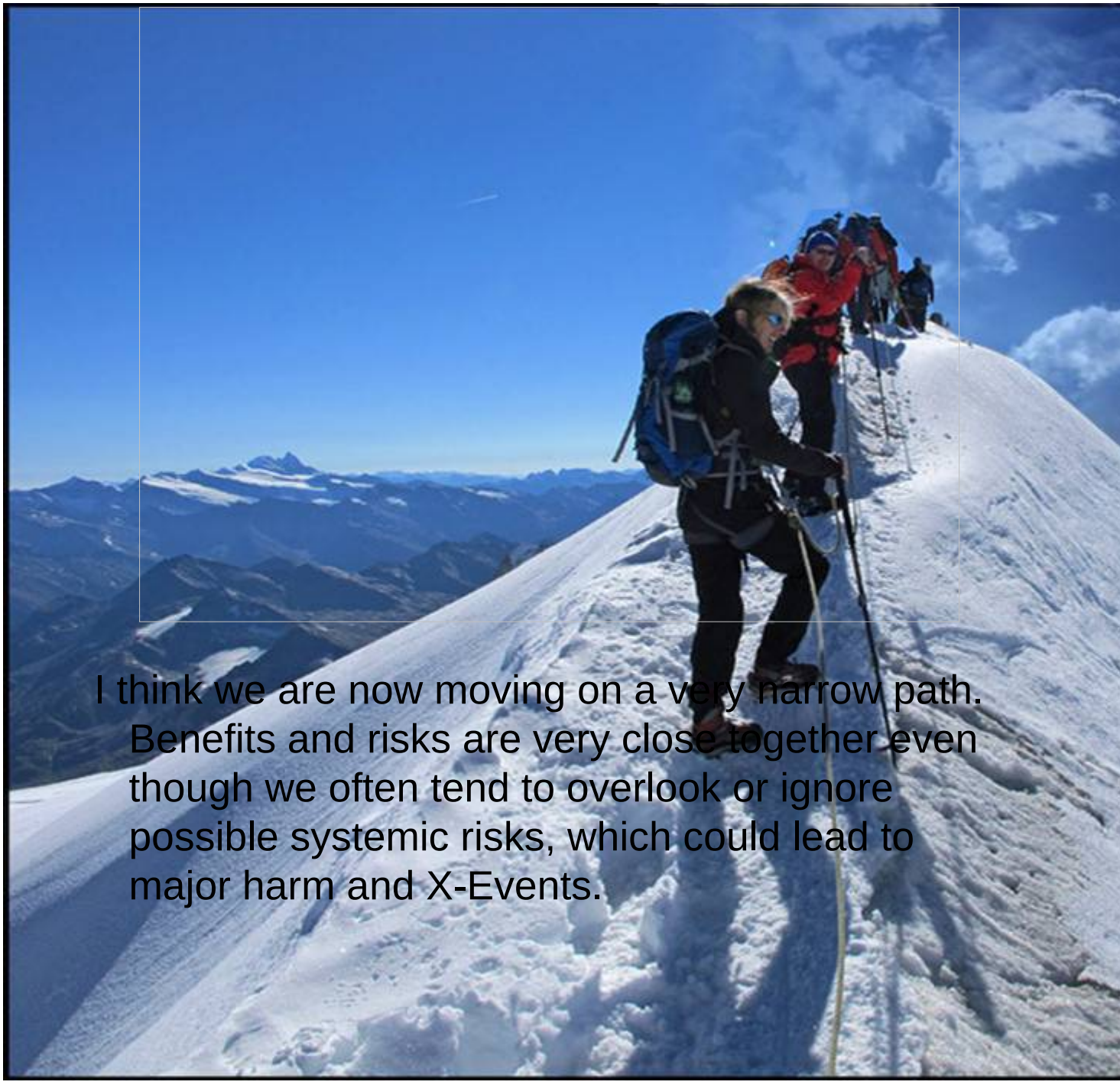
Resilience

34

Conclusions

35

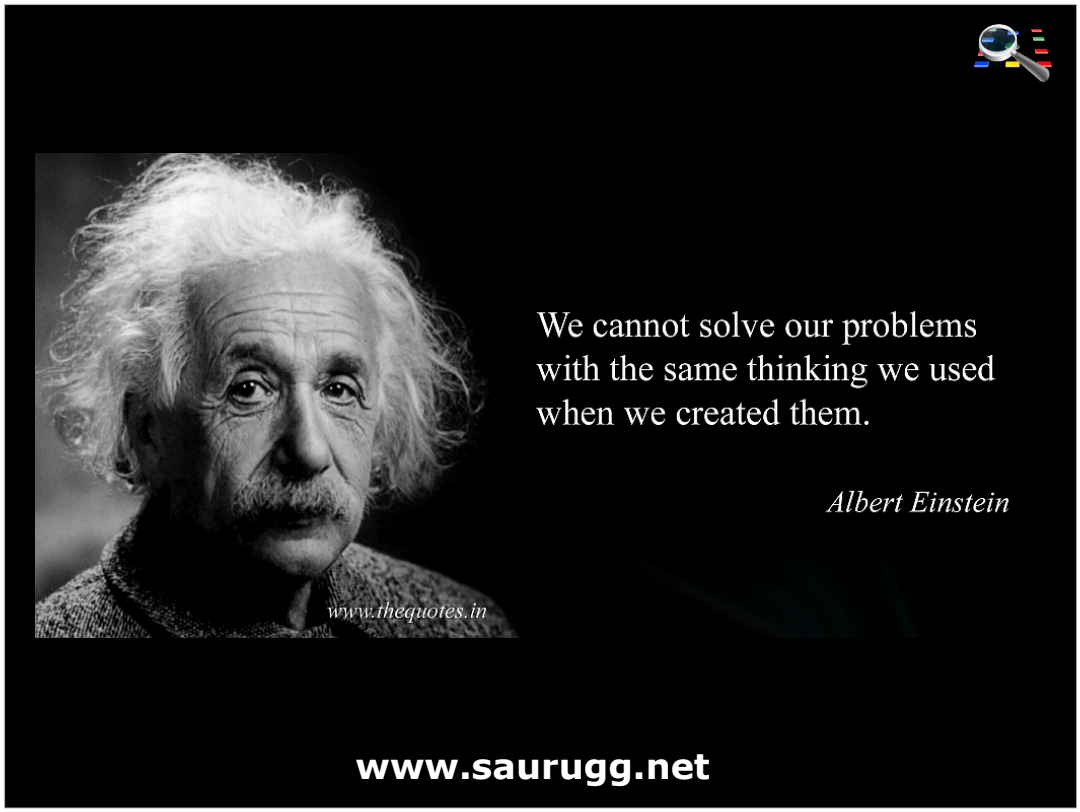
So I would like to come now to my conclusions.


I think we are now moving on a very narrow path.
Benefits and risks are very close together even though we often tend to overlook or ignore possible systemic risks, which could lead to major harm and X-Events.


Also critical infrastructure protection and cyber
security is important, it is insufficient.

We also need a protection FROM critical infrastructures, which will mean self-help capacity and resilient people.


... robust infrastructures and resilient people!



Therefore I would like to finish my talk with a quote by Albert Einstein and I hope I have been able to give you an additional point of view.

...ug

1120 Wien
office@saurugg.net
www.saurugg.net

...career officer in the ICT-Security Section of the Austrian Armed ...n he has been on leave and is engaged in raising awareness ...ic risks due to the rising interconnections and dependencies ...structures, which is contributing to extreme events. He is known as an expert on the topic of blackout: a Europe-wide power-cut and infrastructure collapse. He is also a founding member of the association Cyber Security Austria which is the mastermind behind the European Cyber Security Challenge. As a result of his systemic reflections he is calling for more efforts to raise awareness and resilience throughout our societies to face major extreme events in the foreseeable future.