OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

12.01.2022

Czech-German Cross-Border Situational Awareness for Critical Infrastructures

Summary of Interviews / Results

Background info

- In Germany, critical infrastructures (CI) are regulated by the IT-Security-Act 2.0 (from 2021) only when they are a certain size. The threshold is set at 500,000 citizens, which are directly depending on the service provided by a given CI.
- Regulations include, among others, mandatory security standards across different domains as well as the obligation to notify the Federal Cyber Security Authority (BSI) of any cyber incidents.
- CIs below the threshold are not obliged to obey these regulations.
- The city of Regensburg as well as the county surrounding Regensburg (Landkreis Regensburg) together account for approximately 350,000 citizens. Because this is below the threshold of 500,000, we found that many critical infrastructures in the region are most likely not regulated.
- A major disruption (e. g. due to a cyber-attack or a prolonged power outage, flooding etc.) however would most likely entail the same cascading effects among CIs in Regensburg and surroundings as it would it in other (more populated) areas.
- We therefore decided to start a series of interviews with regional providers of CIs in order to find out about the level of preparedness in (unregulated) CIs below the threshold.
- The population and industry in Regensburg are likely to grow in the future, which will likely bring a lot of the local CIs closer to the threshold and, thus, to being regulated. Our interviews and confrontation with the topic (IT-Security-Act 2.0; cascading effects) might therefore raise the necessary awareness in the corresponding CIs.

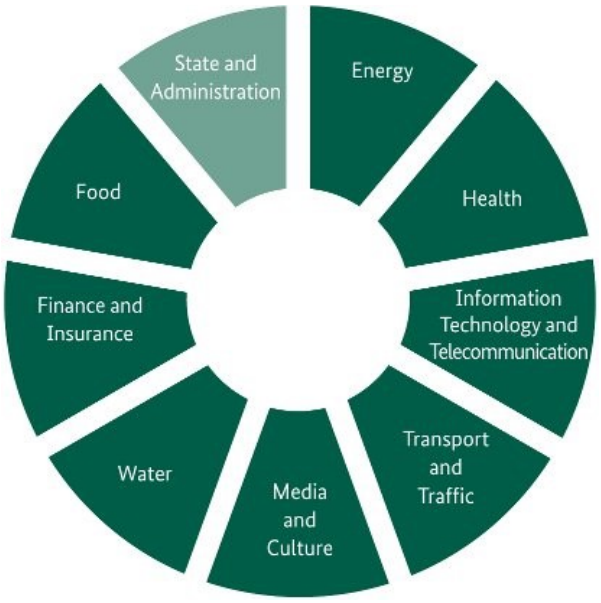

Figure 1. Sectors of CI in Germany. Source: https://www.kritis.bund.de/SubSites/Kritis/EN/introduction/introduction_node.html

Structured interview questions:

Critical infrastructures and the IT-Security-Act

1. What does the term "critical infrastructure" mean to you? Is your company/institution a critical infrastructure from your perspective?
2. If yes, then which measures are you implementing in this regard?
3. How familiar are you with the IT-Security-Act?

Possible disruptions

4. In which ways could there be a disruption to the service your company/institution provides? What could be the possible causes for this?
5. Which consequences might such a disruption bear?
6. Have there been any disruptions of this kind in the past?
7. If yes, then how have they been dealt with?

Preventive/preparatory measures

8. How (through which measures) does your company/institution prepare for possible disruptions?
9. To which extent are you protected against potential cyber-attacks?
10. How does your company/institution react to disruptions at or attacks against other critical infrastructures?
11. Is there a regular exchange of experiences between you and other critical infrastructure providers?

Next steps

12. What will change in the future if your company/institution continues to grow?
13. What are your thoughts on a potential "situational awareness workshop"? Would you at all be interested in joining such an event?
14. Which factors would be decisive for you to join such a workshop?

Summary of basic insights

From the preparatory phase:

- **It is extremely difficult to identify critical infrastructures from public sources**. The sectors in Figure 1 give a general overview of where to look for CIs, however there is much less guidance available beyond that. We wondered, for example, if a company/association providing and managing farming machinery is considered a CI under the sector food – we found that it is, but in many other cases the amount of (publicly) available guidance is insufficient.
- **It is also extremely difficult to identify whether a specific critical infrastructure falls below or above the threshold**. Power and water providers often have annual reports which outline specific figures measuring the output of their plants for example. Pharmaceutical companies, on the other hand, do not make their numbers public, meaning that the only way to identify them as regulated CI is through guessing or directly asking – the latter of which is unlikely to be answered given the sensitivity of the topic. **Identifying the level of a CI (above or below threshold) therefore varies among the individual sectors**.
- **The thresholds are defined using inappropriate units**. Whilst the 500.000 citizen threshold provides a general starting point, the workable thresholds outlined in the documents implementing the IT-Security-Act are transformed to sector-specific thresholds, e. g. measuring power in kWh. In some cases, however, this does not make sense. For example, the transport sector works with weight, e. g. tons. But ports do not weigh the containers they

dispatch; rather, they collect data on the number of containers moved per day. Discrepancies like this contribute to making the identification of CIs so difficult.

- **It is unclear how the threshold takes into consideration the industry** and how this is balanced across different CIs. There might be some critical infrastructures which provide a larger share of their services to the industry instead of the public than others. This inevitably impacts cascading effects and thus, preventative measures. To our knowledge there are no guidelines on how differences like this are best dealt with or at least taken into consideration.
- **Talking about CI safety and security is highly political and therefore many CI providers refuse to even participate in short, simple, and anonymous interviews for scientific research purposes**. It was extremely difficult to get CI providers – once successfully identified – to agree to participate in the interview, even after offering to share with them the interview questions in advance. In the case of the city of Regensburg administration, a very promising-sounding initial phone conversation with the person responsible for information security was followed two weeks later by an excuse that the interview cannot take place because the city administration will first need to discuss the matter internally. They signalled their gratitude for starting this process by sending out the interview questions in advance. We have not been able to get in touch with them again since.

From the interviews themselves:

- All of the interviewees see their service as essential to society and therefore define themselves as critical infrastructures.
- There is a general belief, that in case of a disruption (most commonly mentioned: prolonged power outage) the company/institution can handle many of their tasks “manually” or offline. Cascading effects further down the line (e. g. traffic collapses and some employees may not show up to work) are not always considered at first. There was consensus that a full-scale disruption of the entire information and communications technology infrastructure would entail disastrous consequences.
- Not all of the interviewees have heard of the IT-Security-Act. In some cases, it was mentioned that there is “certainly someone who knows” in the institution/company but it usually was not the person we interviewed. This leaves questions on who we should have contacted instead; on the other hand, the questions (including those on the IT-Security-Act) were provided upfront, so the interviewee could have prepared.
- None of the interviewees indicated that there is an exchange regarding disruptions (both past and potential) with critical infrastructures from other sectors.
- All of the interviewees have faced cases of short-term disruptions in the past and were able to handle them well. None of the examples, however, were linked to disruptions from prolonged power outages, or flooding; only one of them to a cyber-attack (ransomware).
- All of the interviewees consider themselves well prepared for most disruptions; they either referred to internal structures and redundancies or viable alternatives to deliver their services.
- There is a positive attitude towards CI situational awareness workshops, however since all of the interviewees indicated a good level of preparedness and shied away from outlining any difficulties, the workshop questions were not addressed with too much detail.

Next steps

- Interviews with more CI companies/institutions (also from different sectors) would be desirable. More interview protocols would make possible a qualitative analysis using codes to better compare the individual answers across the different questions.
- Where possible, it should be considered to invite multiple representatives to the interview (e. g. from the management as well as from the IT department).
- Perhaps the interview questions can be adjusted to foster the discussion regarding challenges and difficulties experienced with regard to the CI regulation/prevention topic (although it is likely that companies/institutions will try to avoid addressing these issues).
- If a sufficient number of CIs which are willing to share their thoughts and experiences are identified within the region then a platform for regular exchange can be set up.