LANDTAG
NORDRHEIN-WESTFALEN
18. WAHLPERIODE

STELLUNGNAHME
18/508

A09, A20

Prof. Dr. Michael Meier
Universität Bonn · Informatik 4 · Friedrich-Hirzebruch-Allee 5 · D-53115 Bonn

UNIVERSITÄT BONN

Rheinische
Friedrich-Wilhelms-
Universität Bonn

Institut für Informatik
Abteilung 4

Prof. Dr. Michael Meier
Arbeitsgruppe IT-Sicherheit

Postanschrift:
Friedrich-Hirzebruch-Allee 5
D-53115 Bonn

https://net.cs.uni-bonn.de

Tel.: +49 228 - 73-54249
Fax: +49 228 - 73-54254

mm@cs.uni-bonn.de

Landtag Nordrhein-Westfalen
Innenausschuss
Postfach 10 11 43
40002 Düsseldorf

Per E-Mail: anhoerung@landtag.nrw.de

Bonn, 1. Mai 2023

Drucksachen 18/2564
Stellungnahme zum Antrag der Fraktion der FDP „Kommunikation und IT-Sicherheit im Falle eines Katastrophenfalles durch einheitliche Planbarkeit sicherstellen“

Sehr geehrte Frau Vorsitzende,
sehr geehrte Ausschussmitglieder,

vielen Dank für die Gelegenheit zur Stellungnahme zum Antrag der Fraktion der FDP „**Kommunikation und IT-Sicherheit im Falle eines Katastrophenfalles durch einheitliche Planbarkeit sicherstellen**“.

Stellungnahme zum Antrag der Fraktion der FDP:

Zur Ausgangslage:

Der Antrag stellt dar, dass „alles zu tun“ ist um kritische Infrastrukturen zu schützen und diese bei einem Ausfall „unverzüglich wiederherzustellen“ sind. Die Bedeutung funktionierender kritischer Infrastrukturen für unsere Gesellschaft ist ohne Zweifel groß. Der Absolutheit der Darstellungen („alles zu tun“, „unverzüglich wiederherzustellen“) möchte ich mich jedoch nicht anschließen, sondern eine differenziertere Betrachtung anregen, die der im Zusammenhang stehenden Komplexität gerecht wird. Es sind Güter vorstellbar, die höher zu bewerten sind, als das ununterbrochene Funktionieren Kritischer Infrastrukturen. Ebenso kann es in konkreten Fällen sinnvoll sein, zusammengebrochene IT-Infrastrukturen bewusst verzögert wiederherzustellen.

Die Vor- und Nachteile einheitlicher bzw. uneinheitlicher Konzepte der Gefahrenabwehr werden im Antrag richtig dargestellt, die damit verbundene Forderung nach (absoluter) Einheitlichkeit geht jedoch zu weit. So kann es z.B. regionale Besonderheiten geben, die in angepassten Gefahrenabwehrkonzepten berücksichtigt werden müssen.
Die Forderung nach einheitlichen Mindeststandards bei der Gefahrenabwehr unterstütze ich.

Der Antrag führt aus, dass das Fehlen von Kommunikationsmöglichkeiten für die Bevölkerung in Krisensituationen die Entstehung von Panik fördern kann. Ohne dem widersprechen zu wollen, halte ich diese Betrachtung für zu einseitig. Vielmehr halte ich Szenarien für vorstellbar, in denen gerade das von der Bevölkerung gezeigte (Individual-)Kommunikationsverhalten die Entstehung oder Verbreitung von Panik fördert. Hier liegen auch Ansatzpunkte für bewusste Manipulation der Einstellungen der Bevölkerung mittels Fehlinformation. Die Frage mit welcher Priorität, welche Mittel der Individualkommunikation der Bevölkerung im Krisenfall zusätzlich zu behördlichen Kommunikationswegen und Rundfunk etc. zu ermöglichen sind, bedarf detaillierter Untersuchung.

In einer digitalisierten Gesellschaft bedarf es zur Bewältigung von Krisen im Zusammenhang mit digitalen Infrastrukturen Digitalisierungskompetenz. Der Antrag fordert in diesem Zusammenhang die Einrichtung eines Cyber-Hilfswerks um diese Kompetenzen vorzuhalten. Dabei wird die Analogie zum Technischen Hilfswerk aufgegriffen. Hier stellt sich mir die Frage, ob es der Einrichtung einer neuen Struktur Cyber-Hilfswerk bedarf oder ob existierende Strukturen, z.B. das Technische Hilfswerk, um entsprechende Kompetenzen ausgebaut werden sollten. Aufgrund der Vermeidung von Zuständigkeitsfragen sowie der Nutzung von Synergien und Erfahrungen sollte die Erweiterung des Technischen Hilfswerks geprüft werden.

Der Antrag fordert den Aufbau einer zentralen Informations- und Kommunikationsstelle „Bevölkerungsschutz“. Die Erfassung und Verbreitung einer übergreifenden Informationslage ist zu unterstützen. Um Ausfallrisiken zu begegnen sollte hier eine de-zentrale redundante Infrastruktur zur übergreifenden Kommunikationen genutzt werden.

Der Antrag fordert die Schaffung redundanter Kommunikationssysteme, insbesondere den Einsatz von Satelliteninternet bei KRITIS-relevanten Stellen sowie für die Bevölkerung zugänglichen Hotspots, um bei Ausfall oder Beeinträchtigung anderer Kommunikationstechniken (etwa bei Stromausfall) hierüber Kommunikation zu ermöglichen. Die Forderung nach einem adäquaten Maß an redundanter Auslegung der KRITIS-Kommunikation unterstütze ich. Ob allerdings die Nutzung von Satelliteninternet in Verbindung mit Notstromaggregaten in jedem Fall die geeignetste Lösung darstellt muss genauer untersucht werden: Könnten die hierfür geplanten Notstromaggregate nicht alternativ genutzt werden, um die „klassische“ Internetanbindung im Fall eines Stromausfalls aufrecht zu erhalten?

Zur Beschlussfassung

Die dargestellten Forderungen können einem erforderlichen verbesserten Katastrophenschutz zuträglich sein, jedoch müssen die vorgeschlagenen konkreten Instrumente hinsichtlich ihrer Eignung überprüft werden, so etwa hinsichtlich der Fragen ob

- Notfall-Digitalisierungskompetenz in einem neu aufzubauenden Cyber-Hilfswerk oder in einem erweiterten Technischen Hilfswerk aufgebaut werden soll;
- redundante KRTITS-Kommunikation durch Ausrüstung mit Satelliteninternet oder alternative Ansätze am besten erreicht werden kann.

gez. Prof. Dr. Michael Meier