

# BESCHLUSS

---

**des Präsidiums der FDP, Berlin, 7. November 2022**

---

## KRITIS stärken – Kritische Infrastruktur umfassend definieren und sichern

Ein funktionierendes Land braucht Verkehrs- und Versorgungswege sowie Kommunikationslinien, auf die sich Bürgerinnen, Bürger und der Staat zu jeder Zeit verlassen können. Die vergangenen Wochen haben uns vor Augen geführt, wie zentral kritische Infrastruktur (KRITIS) für das Funktionieren unseres Landes ist und wie verletzlich wir hier sind. Durch Explosionen beschädigte Pipelines in der Ostsee und durchtrennte Telekommunikationskabel, die den Bahnverkehr in Norddeutschland lahmgelegt haben, zeigen dies exemplarisch.

Schon der große Hackerangriff auf den Deutschen Bundestag im Jahr 2015 hat die Vulnerabilität unserer demokratischen Institutionen aufgezeigt. Auch die Demokratie ist Teil der KRITIS. Sie zu schützen verlangt, wie der Bundespräsident treffend formulierte, Widerstandsgeist und Widerstandskraft der Bürgerinnen und Bürger.

Die aktuelle Debatte um den Teilverkauf eines Containerterminals im Hamburger Hafen an ein chinesisches Staatsunternehmen zeigt, dass es nicht nur um den technischen Schutz unserer Infrastruktur geht, sondern auch um den Schutz vor externer wirtschaftlicher und geostrategischer Einflussnahme auf unsere Infrastruktur. Häfen sind das Rückgrat des internationalen Handels. Sie spielen zugleich eine besondere wirtschaftspolitische Rolle bei der zukünftigen Ausrichtung der heimischen Wirtschaft in einem fortlaufenden Strukturwandel.

In der Ukraine können wir täglich verfolgen, welche dramatischen Folgen Angriffe auf KRITIS für die Zivilbevölkerung haben, besonders für die Elektrizitäts- und Wasserversorgung. KRITIS ist sowohl in Friedens-, aber erst recht in Zeiten von Kriegen und Konflikten Ziel feindlicher Operationen. Die Täter agieren professionell und häufig aus dem Cyberspace heraus. Wiederholt wurden solche Operationen von autoritär regierten Staaten wie Russland durchgeführt – Regime, die unsere Art zu leben nicht akzeptieren. Wir dürfen deshalb das knallharte Machtinteresse, das diese Staaten verfolgen, nicht unterschätzen.

Angriffe auf die KRITIS haben enorme wirtschaftliche, gesellschaftliche und sicherheitspolitische Folgen. Sie sind deshalb so gefährlich, weil mit relativ geringem Aufwand und einer relativ geringen Wahrscheinlichkeit, entdeckt zu werden, erhebliche Schäden angerichtet werden können.

Eine Stärke unserer liberalen Demokratie ist ihre Lern- und Selbstkorrekturfähigkeit. Wir benötigen daher eine Zeitenwende beim Schutz der KRITIS unseres Landes. Dazu gehört auch eine neue Strategie im Umgang mit Investitionen autoritärer Staaten in deutsche KRITIS. Denn: Es darf keine Einfallstore autoritärer Staaten in KRITIS der Bundesrepublik Deutschland geben.

Unsere Infrastruktur ist zu komplex, um sie universell und dauerhaft vor der möglichen Vielzahl von Angriffen schützen zu können. Wenn wir diese Prämisse akzeptieren, muss es stattdessen darum gehen, einem Angreifer mehr Aufwand und Ressourcen zur Erreichung seiner Ziele abzuverlangen und gleichzeitig, die Folgen eines erfolgreichen Angriffs geographisch und funktionstechnisch so klein zu halten, dass die Schwachstelle nicht mehr für einen strategischen Angriff ausnutzbar ist. So können wir auch staatlichen Akteuren begegnen, die physische Angriffe mit Cyber-Angriffen kombinieren.

Wir Freie Demokraten wollen unsere KRITIS besser schützen und sprechen uns für folgende Maßnahmen aus:

- Die Schaffung einer modernen Infrastruktur soll als Ziel im Grundgesetz festgeschrieben werden. Eine zuverlässige Infrastruktur ist entscheidend für unsere Sicherheit. Die Verankerung im Grundgesetz würde zudem helfen, die Sanierung des Bahnnetzes, welches relevant zum Transport strategischer Güter ist, zu beschleunigen. Bei Abwägungsfragen könnte es Investitionsentscheidungen erleichtern und damit zugleich als Hebel auch für private Investitionen wirken.
- Wir erwarten, dass das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) umgehend eine Verschärfung des Außenwirtschaftsrechts vorschlägt. Wir müssen in Zukunft besser auf Deals ähnlich zu dem in Hamburg vorbereitet sein. Bei Entscheidungen wie dem Teilverkauf eines Terminals des Hamburger Hafens an ein chinesisches Staatsunternehmen sollte künftig das ganze Kabinett aktiv zustimmen müssen und nicht nur einstimmig widersprechen können. Für alle Häfen in Deutschland muss gelten, dass bei Investitionen in die Hafeninfrastruktur, aber auch bei Beteiligung an der Suprastruktur, eine besondere Prüfung zu erfolgen hat. Das gilt insbesondere auch für Deutschlands zweitwichtigsten Hafen in Bremerhaven. Um perspektivisch abwägen und definieren zu können, was KRITIS oder Suprastrukturen sind, ist es wichtig, dies für die heimischen Häfen zu identifizieren und zu sichern. Wir fordern deshalb einen Stresstest für alle relevanten Häfen in Deutschland. Nur so ist es möglich, bei Beteiligungsvorhaben von ausländischen Staatsunternehmen klare Grenzen zu ziehen.
- Wir erwarten vom Bundesministerium des Innern und Heimat (BMI) den schnellen Entwurf eines KRITIS-Dachgesetzes, das den Erfordernissen der Zeitenwende entspricht. So wie wir es im Koalitionsvertrag bereits formuliert haben. Auch sind zum Beispiel Häfen Bestandteil der kritischen Infrastruktur und sollten deshalb in das Gesetz aufgenommen werden.
- Die Anzahl der „single points of failure“ muss bei KRITIS reduziert werden, indem mehr in physische Redundanz und eine stärkere Dezentralisierung der Infrastruktur investiert wird, zum Beispiel durch eine Mehrfachverlegung von Kabeln. Wichtig sind aber auch Software- und Datenredundanzen. Zusätzlich müssen die Reparatur- und Wiederanlauffähigkeiten drastisch verbessert und Prozesse beschleunigt werden. Wir wollen KRITIS außerdem besser schützen, indem Standards und Beschaffungspläne an den Schutzanforderungen ausgerichtet

werden. Dabei sprechen wir uns auch für den Einsatz von Open-Source-Software aus. Wir fordern zudem die Einführung eines Patchmanagements für KRITIS im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI). Wir wollen potenzielle Sicherheitslücken auch von Externen prüfen lassen und einen Notfallplan entwickeln. Unsere gewachsenen, auf zahlreichen älteren Standards basierenden Telekommunikationsnetze können ohne nachgelagerte Schutzmaßnahmen aktuellen Bedrohungen nicht adäquat standhalten. Die Umsetzung solcher Schutzmaßnahmen muss folglich weiter forciert werden. Auch sollte die Möglichkeit eines lokalen und regionalen Notbetriebs bei einem zu erwartenden Ausfall oder bei Kompromittierung sichergestellt sein.

- Den besseren Schutz unserer Cybersicherheit. IT- und Datensicherheit müssen der Grundpfeiler des Schutzes kritischer Infrastruktur sein. Dazu wollen wir ein Cyber-Hilfswerk gründen und eine Internet-Notversorgung durch Satelliten erreichen. Es muss regelmäßige externe Prüfungen auf Sicherheitslücken und wiederkehrende Schulungen für Mitarbeiterinnen und Mitarbeiter in KRITIS geben. Die Sicherheitsbehörden des Bundes und der Länder müssen ein funktionierendes und auf die Schließung von IT-Sicherheitslücken ausgerichtetes Schwachstellenmanagement einführen.
- Innovationen zum Schutz der digitalen Gesellschaft und ihrer Infrastruktur kommen eine zentrale Bedeutung zu. Wir wollen deshalb die Forschung und Entwicklung im Bereich der IT- und Cyber-Sicherheit fördern, die Kooperation von universitärer und außeruniversitärer Forschung stärken und vermehrt Anreize für den erfolgreichen Transfer in die Praxis schaffen. Neue Erkenntnisse und Innovationen aus der Wissenschaft können im Bereich der zivilen Sicherheit und insbesondere bei der Energiesicherheit helfen, unsere Souveränität zu stärken und im Falle von Angriffen bei der Aufklärung zu unterstützen. Ein relevantes Beispiel dafür ist die zuletzt genutzte Infrastruktur aus der deutschen Forschung bei den Tauchvorgängen zur Analyse der Schäden an Nord Stream II oder zur Untersuchung der Sensorik bei der Aufzeichnung der Explosionen. Die Wissenschaft muss daher integraler Bestandteil der Nationalen Sicherheitsstrategie der Bundesregierung sein. Zentrale Schlüsseltechnologien wollen wir von Anfang an sicher ausgestalten („security by design“) und dafür auch die Chancen von Quantencomputing nutzen.
- Für einen besseren Schutz unserer technischen Infrastruktur und kritischer Technologie. Dazu zählen unter anderem die Infrastruktur der Bahn, die Stromversorgung und die Telekommunikation. Wir dürfen deshalb keine Unternehmen, die den umfangreichen Einflussmöglichkeiten autoritärer Regime unterliegen, beim Ausbau kritischer Infrastruktur wie dem 5G-Netz berücksichtigen. Bei autoritären Regimen dürfen nicht nur rein wirtschaftliche Kriterien berücksichtigt werden. Auch sicherheitspolitische Aspekte müssen bedacht werden. Die Standards und die Beschaffung wollen wir deshalb an Schutzanforderungen ausrichten.
- Für eine umfassende Sicherheitsüberprüfung und die Ertüchtigung des digitalen Zugfunks. Der digitale Zugfunk als Voraussetzung eines störungsfreien Bahnverkehrs ist nicht nur hinsichtlich seiner stark zentralisierten Netzarchitektur, sondern auch seitens der Funktechnik hochgradig verwundbar. Sicherheitsüberprüfungen sowohl auf der Netz- wie auch auf der Triebfahrzeugseite müssen von einer schnellen Umsetzung von Maßnahmen zur Eingrenzung möglicher Sabotage begleitet werden.

- Wir sollten unsere KRITIS gesamteuropäisch betrachten. Wir Freie Demokraten sehen einen Abstimmungs- und Kooperationsbedarf auf europäischer Ebene bei ausländischen Investitionen in KRITIS. Insbesondere sollten wir den strategischen Einfluss autoritärer Staaten auf die KRITIS prüfen. Auch die Wahlinfrastruktur aller EU-Mitglieder ist wichtig – denn auch unsere Demokratie ist KRITIS.
- Wir fordern ein handlungsfähiges Bundesamt für Sicherheit in der Informationstechnik (BSI) und eine schnelle Klärung der Besetzung des Behördenleiters durch das Bundesministerium des Innern und Heimat. Das BSI muss unabhängig werden und zur zentralen Stelle für die Cybersicherheit ausgebaut werden. Zu einer handlungsfähigen Behörde gehört auch die richtige Prioritätensetzung beim Personaleinsatz. Bei einer Aufstockung des Personals muss zugleich eine angemessene Ausstattung sowie eine fortlaufende Aus- und Weiterbildung in Bezug auf KRITIS gewährleistet werden. Dies gilt neben dem BSI auch für das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und für die Bundesanstalt Technisches Hilfswerk (THW).
- Das BBK muss, wie im Koalitionsvertrag vorgesehen, nach dem Vorbild des Bundeskriminalamtes mit einer Zentralstellenfunktion ausgestattet werden. Im Katastrophenfall braucht es eine bessere Koordinierung der Anstrengungen von Bund, Ländern und Kommunen. Die dafür erforderliche Grundgesetz-Änderung wollen wir zügig auf den Weg bringen.