

## Antrag

der Abgeordneten Eugen Schmidt, Barbara Lenk, Beatrix von Storch, Edgar Naujok und der Fraktion der AfD

### Umsetzung der Digitalstrategie des Bundesministeriums für Digitales und Verkehr – Sicherheit kritischer Infrastruktur gewährleisten, Cyberabwehr priorisieren

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Am 31. August 2022 verabschiedete das Bundeskabinett die Digitalstrategie des neu benannten Bundesministeriums für Digitales und Verkehr ([bmdv.bund.de/SharedDocs/DE/Pressemitteilungen/2022/063-digitalstrategie.html](https://bmdv.bund.de/SharedDocs/DE/Pressemitteilungen/2022/063-digitalstrategie.html)). Darin sollen die politischen Schwerpunkte der Bundesregierung beim Querschnittsthema Digitalisierung unter einem Dach zusammengeführt werden und einen übergeordneten Rahmen für die Digitalpolitik der Bundesregierung bis möglicherweise zum Jahr 2025 bilden ([bmdv.bund.de/SharedDocs/DE/Anlage/K/presse/063-digitalstrategie.pdf?\\_\\_blob=publicationFile](https://bmdv.bund.de/SharedDocs/DE/Anlage/K/presse/063-digitalstrategie.pdf?__blob=publicationFile), S.2).

Als die drei Handlungsfelder der Strategie werden die digital souveräne Gesellschaft, innovative Arbeit und Wirtschaft sowie der digitale Staat benannt, mit Einzelthemen wie beispielsweise Smart Cities, Datenökonomie oder Cybersicherheit (ebenda).

In Bezug auf die Cybersicherheit wird eine gesetzliche Grundlage für das Nationale Cyber-Abwehrzentrum, der Ausbau des BSI zur unabhängigen Zentralstelle im Bereich der IT-Sicherheit und ein wirksames Schwachstellenmanagement angekündigt (ebenda, S. 48)

Zum Zeitpunkt der Verabschiedung der Digitalstrategie war bereits der Krieg in der Ukraine seit dem 24. Februar 2022 im Gange, welcher Bundeskanzler Scholz zur Definition einer „Zeitenwende“ sowie zu der Ankündigung eines Sondervermögens Bundeswehr im Bundeshaushalt 2022 mit einer Ausstattung von 100 Milliarden Euro veranlasste ([www.bundesregierung.de/resource/blob/992814/2131062/78d39dda6647d7f835bbe76713d30c31/bundeskanzler-olaf-scholz-reden-zur-zeitenwende-download-bpa-data.pdf?download=1](https://www.bundesregierung.de/resource/blob/992814/2131062/78d39dda6647d7f835bbe76713d30c31/bundeskanzler-olaf-scholz-reden-zur-zeitenwende-download-bpa-data.pdf?download=1)).

Ferner sollten „Jahr für Jahr mehr als zwei Prozent des Bruttoinlandsprodukts in unsere Verteidigung investiert“ werden, „wohl wissend, dass sich nicht alle Bedrohungen der Zukunft mit den Mitteln der Bundeswehr einhegen lassen (ebenda, S. 15). Es folgte die Ankündigung: „Deshalb werden wir unsere Resilienz stärken, technisch und gesellschaftlich, zum Beispiel gegen Cyberangriffe und Desinformationskampagnen, gegen Angriffe auf unsere kritische Infrastruktur und Kommunikationswege.“

Mit großer Besorgnis stellt der Deutsche Bundestag fest, dass es in der Folge des Kriegsbeginns in der Tat zu einem massiven, Satelliten-induzierten Ausfall von Windindustrieanlagen zum exakten Zeitpunkt des Überfalls kam ([www.golem.de/news/ukraine-krieg-tausende-deutsche-windraeder-ohne-satelliten-kommunikation-2202-163499.html](http://www.golem.de/news/ukraine-krieg-tausende-deutsche-windraeder-ohne-satelliten-kommunikation-2202-163499.html)), dass ein Sabotageakt auf die digitale Infrastruktur der Deutschen Bahn erfolgte ([www.merkur.de/welt/zugausfall-polizei-news-deutsche-bahn-sabotage-stoerung-bahnverkehr-norddeutschland-technik-zr-91837627.html](http://www.merkur.de/welt/zugausfall-polizei-news-deutsche-bahn-sabotage-stoerung-bahnverkehr-norddeutschland-technik-zr-91837627.html)) oder dass Truppenübungsplätze, auf denen ukrainische Soldaten ausgebildet werden, mit unbekanntem Drohnenobjekten (sog. UDOs) zu Aufklärungszwecken überflogen wurden ([www.n-tv.de/politik/Bundeswehr-meldet-Drohnen-Überfluege-in-Bayern-article23625519.html](http://www.n-tv.de/politik/Bundeswehr-meldet-Drohnen-Überfluege-in-Bayern-article23625519.html)).

Mit großer Besorgnis stellt der Deutsche Bundestag ebenso fest, dass in dieser akuten Cyber-Bedrohungslage, der Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI) unter mysteriösen Umständen von der Bundesministerin des Inneren vom Dienst freigestellt wird. Dieser hatte sich stets vehement für ein Schließen aller Software-Sicherheitslücken ausgesprochen, was letztlich ein „wirksames Schwachstellenmanagement“ obsolet machen würde.

Der nur wenige Tage nach der Freistellung des BSI-Präsidenten veröffentlichte Lagebericht 2022 seiner Behörde weist für das laufende Jahr über 20.000 Software-Schwachstellen, über 116 Millionen neue Schadprogramm-Varianten, über 15 Millionen Cyber-Angriffe auf deutsche Netzbetreiber sowie den ersten digitalen Katastrophenfall Deutschlands aus ([www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht\\_node.html](http://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html)).

- II. Der Deutsche Bundestag fordert von der Bundesregierung,
1. die Cybersicherheitsstrategie zu aktualisieren und die IT-Sicherheitsgesetzgebung zu konsolidieren,
  2. die Cybersicherheitsarchitektur so aufzustellen, dass hybride Bedrohungen schneller erkannt und besser abgewehrt werden können,
  3. ein KRITIS-Dachgesetz zu verabschieden, das alle kritischen Infrastrukturen (KRITIS) abbildet und eine Antwort auch auf komplexe, hybride Bedrohungen bietet, indem es Verfahrensstandards und Zuständigkeiten definiert,
  4. eine klare Verantwortlichkeit für den Schutz der digitalen Hochseeinfrastruktur zu schaffen,
  5. eine eindeutige Rechtsgrundlage für die Zusammenarbeit im Nationalen Cyber-Abwehrzentrum zu schaffen und so eine effektive Kontrolle durch Parlament und Aufsichtsbehörden zu ermöglichen,
  6. zunächst die eigenen digitalen Infrastrukturen zu härten und die Vulnerabilität für Angriffe zu verringern,

7. Angriffen zukünftig stärker präventiv entgegenzuwirken und dabei auch auf eine engere Kooperation von Staat und Wirtschaft zu setzen,
8. bedrohte Unternehmen und Einrichtungen vor allem aus dem KRITIS-Bereich hinsichtlich der Abwehr von Angriffen mit Hilfe von Software-Schwachstellen durch ein optimal ausgestattetes Bundesamt für Sicherheit in der Informationstechnik (BSI) als Zentralstelle für Cybersicherheit in weitaus größerem Umfang als bisher zu beraten und sehr viel stärker zu unterstützen,
9. neue völkerrechtliche Übereinkünfte zur Ächtung von militärischen und hybriden Angriffen auf digitale Infrastrukturen und zur Ächtung des Verteilens von Schad- und Spionagesoftware umgehend zu etablieren,
10. nicht-vertrauenswürdige Unternehmen beim Ausbau kritischer Infrastrukturen, wie z. B. auch Container-Terminals an Seehäfen, nicht zu beteiligen.

Berlin, den 13. Dezember 2022

**Dr. Alice Weidel, Tino Chrupalla und Fraktion**

*Vorabfassung - wird durch die lektorierte Fassung ersetzt*