9. Cybersicherheit für kritische Infrastrukturen

Die Funktionsfähigkeit moderner Gesellschaften ist heute hochgradig von verschiedenen Technologien und deren Zusammenspiel abhängig. Sie bilden dabei „kritische Infrastrukturen". Diese können als „Hauptschlagader" von Wirtschaft und Gesellschaft verstanden werden (Strauß/Krieger-Lamina 2017). Dementsprechend bedrohlich sind Ausfälle von Systemen, die zentral für die Funktionsfähigkeit der Daseinsvorsorge und Grundversorgung mit lebensnotwendigen Gütern sind. Neben elektromagnetischen Impulsen (EMP), wie etwa Sonnenstürmen, sind zunehmend Risiken durch gezielte Angriffe auf IT-Systeme (Cyber-Angriffe) von kritischen Infrastrukturen festzustellen (POST 2017; Panagiotis Trimintzios et al. 2017).

Im Hinblick auf die absehbar weiter zunehmende Vernetzung und Automatisierung (z. B. Industrie 4.0, Smart Grids, Smart Home, autonome Fahrzeuge, Internet der Dinge etc.) ist davon auszugehen, dass integrierte Systeme generell weiter an Bedeutung gewinnen werden. Es besteht daher insgesamt Bedarf nach verbesserten Schutzkonzepten von kritischen Infrastrukturen. Mittel- und längerfristig gibt es Bedarf nach Innovationen, die die Systemsicherheit in Design und Architektur insgesamt erhöhen (Security-by-design). Hierbei ist auch ein stärkerer Dialog zwischen Wissenschaft, Wirtschaft und Politik wichtig (vgl. Strauß/Krieger-Lamina 2017).

Das Österreichische Programm zum Schutz kritischer Infrastrukturen (APCIP[1]) beinhaltet strategische Maßnahmen, um die Resilienz Österreichs zu erhöhen. Hier wurde bereits einiges geleistet und Österreich zählt hier zu den Vorreitern in der EU. Eine Vielzahl an Strategien und Akteuren widmet sich der Thematik, dies verdeutlicht die Komplexität der Problematik, bringt aber auch Unklarheiten hinsichtlich Kompetenzen und Zuständigkeiten mit sich. Daneben besteht die Österreichische Strategie für Cyber-Sicherheit (ÖSCS) und das staatliche Krisen- und Katastrophenschutzmanagement (SKKM). Eine Analyse (und gegebenenfalls Adaptierung) dieser beiden Elemente in Hinblick auf Überschneidungen, Synergien und Ressourcen mit APCIP und vice versa wäre zweckmäßig (vgl. Strauß/Krieger-Lamina 2017).

Das Parlament als zentraler Ort der politischen Meinungsbildung und Kontrolle kann wesentlich zur Koordination österreichischer staatlicher und privater Aktivitäten sowie zur notwendigen Bewusstseinsbildung in der Öffentlichkeit beitragen. Darüber hinaus wäre durch die Förderung österreichischer Innovationen in technischen und organisatorischen Sicher-

[1] Austrian Programme for Critical Infrastructure Protection.

heitsmaßnahmen doppelter Nutzen zu erzielen.

Zitierte Literatur

Panagiotis Trimintzios, Chatzichristos, G., Portesi, S., Drogkaris, P., Palkmets, L., Liveri, D., and und Dufkova, A. (STOA), 2017, *Cybersecurity in the EU Common Security and Defence Policy (CSDP)*, Nr. EPRS/STOA/SER/16/214N: STOA < http://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf >.

POST (Parliamentary Office of Science and Technology), 2017, *Cyber Security of UK Infrastructure*, Nr. Number 554 May 2017, London < http://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-0554 >.

Strauß, S. und Krieger-Lamina, J., 2017, *Digitaler Stillstand: Die Verletzlichkeit der digital vernetzten Gesellschaft – Kritische Infrastrukturen und Systemperspektiven. Projekt-Endbericht*, 2017-03-31, Wien < http://epub.oeaw.ac.at/ita/ita-projektberichte/2017-01.pdf >.