Antrag W-06
Jusos Bezirk Hannover

ZITiS in die Schranken weisen

Die „Zentrale Stelle für Informationstechnik im Sicherheitsbereich“ (ZITiS) wurde mit der Maßgabe ins Leben gerufen, Überwachungstechniken für digitale Dienste und Messenger-Programme zu entwickeln. Als dienstleistende Schnittstelle zwischen Sicherheitsbehörden, Verfassungsschutz und der Bundeswehr soll sie dabei den neuen Anforderungen der inneren Sicherheit im Zeitalter der Digitalisierung gewachsen sein. Die Bundesregierung rechtfertigt die Gründung dieser neuen Bundesbehörde damit, dass durch die serienmäßigen Verschlüsselungssysteme, z.B. bei WhatsApp oder Apple-Produkten, staatliche Abhör- und Überwachungsmaßnahmen ins Leere laufen. Diese Zentrale Stelle soll folglich also nicht selbst abhören, sondern lediglich die erforderliche Technik dafür entwickeln und den staatlichen Sicherheitsbehörden zur Verfügung stellen. Dadurch müssen besagte staatliche Stellen nicht „jede für sich“ an geeigneten Techniken forschen und können auf die Entwicklungen und Ergebnisse der ZITiS zurückgreifen.
Wie jedoch bereits viele Quellen übereinstimmend wiedergeben, ist die geplante Strategie der ZITiS, bestehende Sicherheitslücken aufzukaufen und sie bestehen zu lassen, damit sie entsprechend ausgenutzt werden können durch staatliche Stellen. In der Vergangenheit war es übliche Praxis, dass User*innen entdeckte Sicherheitslücken den zuständigen Unternehmen gemeldet haben, um sie schließen zu lassen und den Datenschutz im Allgemeinen zu verbessern. Dadurch wurden gemeldete Sicherheitslücken durch Sachleistungen von Seiten der Unternehmen entlohnt. Der*die User*in wird sich nun natürlich – einer kapitalistischen Logik entsprechend – eher dazu entschließen, die gefundenen Sicherheitslücken für hohe Geldsummen an die ZITiS zu verkaufen, die die nötigen finanziellen Mittel vom Bundesministerium des Innern zur Verfügung gestellt bekommt.
Mit dieser Vorgehensweise eröffnen sich mehrere Probleme. Zum einen lässt sich keine rechtliche Grundlage für das Verwenden von sogenannten Staatstrojanern entdecken und, damit einhergehend, fehlt es dann auch an der gesetzlichen Le-

Empfehlung der Antragskommission
Überweisen an: Bezirksvorstand

gitimation und Möglichkeit der Überprüfung durch das Bundesverfassungsgericht. Zum anderen besteht dadurch auch immer das Risiko, dass offen gelassene Sicherheitslücken von Dritten entdeckt werden und etwa ausländische Geheimdienste oder die Organisierte Kriminalität sich diese zu eigen machen. In diesem Sinne ist die neuerdings eingeführte Behörde verfassungsrechtlich sehr bedenklich, da sie die Integrität und das Vertrauen in digitale Kommunikation und Dienste untergräbt, indem sie Datenhehlerei betreibt. Wir sollten vielmehr eine öffentliche Debatte darüber führen, dass Steuergelder aufgewendet werden, um Sicherheitslücken zu kaufen, Computer zu hacken, Verschlüsselungen unsicherer zu machen. Elementare Grundsätze des Datenschutzes werden damit billigend vom Staat missachtet. und damit elementare Grundsätze des Datenschutzes billigend missachtet werden.

Mit Erschrecken müssen wir also dabei zusehen, wie Massenüberwachung und digitale Überwachungsinfrastruktur massiv ausgebaut wird und Grundrechte zunehmend beschnitten werden. Aus diesem Grund fordern wir, den Aufgabenbereich der ZITiS umzustrukturieren:

- Sie soll eine finanziell solide ausgestattete Kryptopolitik vorantreiben, die die gesamte Thematik der Verschlüsselungstechnik öffentlich aufbereitet und für jede*n einfach verständlich zugänglich macht.
- Sie soll maßgeblich an einer Digital Agenda 2030 mitwirken, um die Bundesrepublik auf die Herausforderungen der Digitalisierung vorzubereiten.
- Sie soll zu einer dienstleistenden Schnittstelle werden, die IT-Sicherheitsprodukte erforscht und entwickelt, sowie eine finanzielle und personelle Unterstützung bestehender Datenschutzbehörden gewährleistet.
- Sie soll eine öffentliche Kampagne starten, die in ihrer Botschaft die Notwendigkeit einer Charta der Digitalen Grundrechte verkörpert und Deutschland dazu antreibt, sich dafür auf europäischer Ebene verpflichtend einzubringen.
- Ihr wird untersagt, Geld zu investieren, um Sicherheitslücken zu kaufen, Computer zu hacken sowie Verschlüsselungen unsicherer zu machen.