Bearbeitungsstand: 26.01.2023

Prof. Dr. jur. Dennis-Kenji Kipker

Mündliche Stellungnahme

„Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“

Deutscher Bundestag, Ausschuss für Digitales

Öffentliche Anhörung am 25. Januar 2023

Sehr geehrte Ausschussvorsitzende, sehr geehrte Mitglieder des Digitalausschusses, sehr geehrte Damen und Herren,

ich bedanke mich für die Möglichkeit, hier heute Stellung zu Fragen der nationalen Cybersicherheitsarchitektur und ihrer künftigen Ausrichtung nehmen zu können. In dieser kurzen Zusammenfassung meiner ausführlichen schriftlichen Stellungnahme möchte ich vor allem die nachfolgenden Schwerpunkte im Besonderen in den Fokus der rechtspolitischen Betrachtung rücken:

1. **Begriff der „Cybersicherheit“:** Die derzeit in Deutschland kritisierte sog. „Verantwortungsdiffusion“ ist die Folge einer unzureichenden Definition und Eingrenzung des Begriffs der „Cybersicherheit“ – deutlich wird das vor allem an der im letzten Jahr durch das BMI vorgelegten „Cybersicherheitsagenda“. Wir brauchen ein ganz klares ontologisches Verständnis der Cybersicherheit als technisch-organisatorische Reaktion auf die gegenwärtigen Herausforderungen im digitalen Raum. Fragen wie zum Beispiel Regulierung von Online-Hasskriminalität, Plattformregulierung, die sog. „Chatkontrolle“ oder generell der schillernde Begriff der „digitalen Souveränität“ haben damit zunächst nur wenig zu tun. Es geht bei der Cybersicherheit primär um die Aufrechterhaltung der Funktionsfähigkeit der vernetzten IT-Systeme und daran sollten sich legislative und exekutive Maßnahmen künftig stärker orientieren, um keine systemimmanenten Widersprüche zu generieren. Operative Cybersicherheit in Deutschland ist primär eine technische und keine politische Aufgabe.
2. **„Digitaler Gegenschlag“ bzw. „aktive Cyberabwehr“:** Sämtliche im Konzeptpapier der Bundesregierung aus 2019 angegebenen Strukturen und behördlichen Akteure sind weder geeignet noch verfassungsrechtlich legitimiert, einen digitalen Gegenschlag durchzuführen bzw. darüber zu entscheiden. National allein zuständig ist für diesen Fall die Bundeswehr mit dem „Kommando Cyber- und Informationsraum“. Das setzt national verfassungsrechtlich einen Verteidigungsfall und international völkerrechtlich das Bestehen des Selbstverteidigungsrechts voraus. Auch hier fehlt es bislang an einem klaren begrifflichen Verständnis: Aktive Cyberabwehr betrifft nämlich nicht die bloße Blockade oder Umleitung schadhafter Datenverkehre, die bereits von gegenwärtig bestehenden gesetzlichen Vorschriften gedeckt sind. Daraus folgt, dass es aufgrund der verfassungsrechtlich eindeutigen Bestimmtheit der Zuständigkeit der Bundeswehr zurzeit keiner Gesetzesänderung bzw. Neuschaffung von Gesetzen im Bereich der aktiven Cyberabwehr bedarf.
3. **Umgang mit zero days:** Die Cybersicherheit und mit ihr verbundene öffentliche und Individualinteressen haben grds. Verfassungsrang, der aber nicht absolut gilt. Das bedeutet, dass der verhältnismäßige Ausgleich zu anderen ebenfalls verfassungsrechtlich geschützten Interessen herzustellen ist. Das BVerfG hat im Jahr 2021 klar entschieden, dass es deshalb als staatliche Maßnahme grds. verfassungsrechtlich zulässig sein kann, IT-Sicherheitslücken zB zur Durchführung von Quellen-TKÜ zu verwenden. Derlei Maßnahmen müssen jedoch auf Einzelfälle limitiert und auf das absolut notwendige Maß beschränkt sein. Umso wichtiger sind

an dieser Stelle klare funktionale Trennungen in der nationalstaatlichen Cybersicherheitsarchitektur, indem die Cybersicherheit kompromittierende Maßnahmen nicht Bestandteil einer nationalen Cybersicherheitsagenda sind.

4. **KRITIS-Dachgesetz:** Insbesondere unter dem Eindruck des verheerenden Russland-Ukraine-Kriegs wurde die Vulnerabilität der nationalen Kritischen Infrastruktur nochmals besonders deutlich. Das Problem ist aber keineswegs neu, sondern besteht schon seit Jahrzehnten. So stellt zum Beispiel das BMI in der nationalen KRITIS-Strategie aus 2009 bereits auf die hybride Bedrohungslage infolge terroristischer Anschläge seit dem 11. September 2001 in den USA ab. Dieser Fakt wird in der aktuellen politischen und medialen Debatte nur unzureichend wiedergegeben. Die Annahme, dass es sich bei dem KRITIS-Dachgesetz um eine spiegelbildliche Regelung zur KRITIS-Cybersicherheit im „Analogen“ handelt, geht deshalb fehl, denn das IT-SiG 2.0 regelt weitaus mehr als nur kritische Cybersicherheit und auch verfügen wir bereits seit Jahren über unzählige bereichsspezifische Fachgesetze für den nationalen KRITIS-Schutz. Deshalb kann ein KRITIS-Dachgesetz nur ein weiteres Artikel-Gesetz sein, das die Bestandsgesetze zum physischen KRITIS-Schutz bei nachgewiesenermaßen festgestellten Defiziten und Schwachstellen ergänzt, nicht aber komplett neue und weitere Verantwortlichkeiten schafft, die bestenfalls noch zusätzlich unter die „Cybersicherheit im weitesten Sinne“ gefasst werden. Eine solche begriffliche Überdehnung wäre fatal, da sie zwangsläufig eine nahezu vollständige Konturlosigkeit der nationalen Cybersicherheitsarchitektur zur Folge hätte.
5. **Ausbildung von „Cyberfachkräften“ in Deutschland:** Abschließend möchte ich noch ein Wort zur Ausbildung von IT-Fachkräften verlieren. Wenn wir über unternehmerische Cybersecurity-Compliance sprechen, dann geht es vor allem auch um rechtliche Fragestellungen. Wie bereits angesprochen, haben wir in Deutschland und der EU eine Vielzahl von Fachgesetzen, die Cybersicherheitsanforderungen festschreiben. Hier ist es dringend erforderlich, die juristische Ausbildung zu reformieren und weitaus interdisziplinärer als bislang zu gestalten, denn wir brauchen in Deutschland unbedingt mehr „IT-Juristen“, die sowohl die rechtlichen Fragestellungen beherrschen als auch das zur Anwendung notwendige technische Know-how besitzen. Gerichtet an die Hochschulen vorschlagen möchte ich deshalb das Ausbildungsmodell eines technischen Cybersecurity-Masters nach Abschluss des juristischen Studiums.

Vielen Dank.