Grußwort von *Dr. Peter Tauber*,
Mitglied des Deutschen Bundestages und
Parlamentarischer Staatssekretär bei der Bundesministerin der Verteidigung

Sehr geehrte Damen und Herren,

wenn es darum geht, die politischen Herausforderungen für die kommenden Jahre zu benennen, darf in keiner Aufzählung der Begriff „Digitalisierung“ fehlen. Und ohne Zweifel fordert uns „die Digitalisierung“ in nahezu allen Bereichen, allem voran in unseren Schulen und Universitäten, in der Wirtschaft oder bei unserer verkehrlichen Infrastruktur. Und natürlich stellt sich dringender denn je die Frage, wie wir Digitalisierung mit Blick auf unsere Sicherheitsarchitektur verstehen.

Unsere Soldaten schwören im Rahmen ihres feierlichen Gelöbnisses, *„der Bundesrepublik Deutschland treu zu dienen und das Recht und die Freiheit des deutschen Volkes tapfer zu verteidigen.“* Wie aber verteidigen unsere Soldaten Recht und Freiheit in Konflikten, welche nicht mehr mit konventionellen Mitteln begonnen und geführt werden? Die Anonymität und Vernetzung der informationstechnischen Systeme werden genutzt werden, um nicht nur zu spionieren, sondern überlebenswichtige Systeme des Gegners zu zerstören, zu beschädigen oder zu infiltrieren. Eine als solche erkennbare feindliche Streitkraft muss nicht mehr in ein Land einmarschieren.

Machen wir uns nichts vor. Cyberangriffe sind keine Fiktion mehr, sondern tägliche Realität. Kriminelle, Terroristen, private sowie (halb-)staatliche Organisationen attackieren monatlich hundertausendfach Bundeswehr, Regierungsstellen sowie Unternehmen und versuchen unsere freiheitliche Gesellschaft systematisch zu destabilisieren. Natürlich sind die Motive bei den verschiedenen Bedrohungslagen stets unterschiedlich. Doch die Angreifer sehen in Cyberangriffen nicht nur schlicht ein lukratives Geschäft, die politische Ausrichtung und Bedrohung vieler Cyberattacken ist nicht zu unterschätzen.

Cyberkriminalität, Cyberspionage, Cyberterrorismus oder Cyberwar – die Grenzen verschwimmen zuweilen und fordern damit nicht nur eine einzelne Behörde heraus. Das Denken in starren Zuständigkeiten einzelner Behörden und Institutionen wird der Bedrohungslage nicht gerecht. Unser Land braucht eine Cyber-Sicherheitspolitik, die

es ermöglicht, dass Deutschland die großartigen Chancen und Potenziale einer digitalisierten Gesellschaft und Wirtschaft voll ausschöpfen kann, aber eben auch die Risiken und Bedrohungsszenarien beherrschbar sind. Dafür ist es erforderlich, ressort- und behördenübergreifend zusammenzuarbeiten. Das 2011 ins Leben gerufene „Nationale Cyber-Abwehrzentrum“ ist unter diesem Gesichtspunkt nur der Anfang gewesen. Mit der „Cyber-Sicherheitsstrategie für Deutschland 2016“ wurde der strategische Rahmen für weitere gemeinsame Aktivitäten geschaffen. Im Koalitionsvertrag findet das mit dem „Cyber-Abwehrzentrum Plus“ eine Fortsetzung.

Mit der Gründung des Kommando Cyber- und Informationsraum als eigenständiger militärischer Organisationsbereich leistet die Bundeswehr seit April 2017 einen unverzichtbaren Beitrag für die Wahrung der Cybersicherheit. Angesichts immer komplexerer Bedrohungslagen reicht dies aber nicht aus. Die sich ständig wandelnde Sicherheitslage erfordert den Ausbau der staatlichen Handlungsfähigkeit.

Mit der jüngst vorgenommenen Gründung einer „Agentur für Innovation in der Cybersicherheit“ leistet die Bundesregierung einen weiteren essentiellen Beitrag zur gesamtstaatlichen Sicherheitsvorsorge. So arbeiten das Bundesministerium der Verteidigung und das Bundesministerium des Innern für Bau und Heimat hierbei eng zusammen, um gemeinsam ambitionierte Forschungs- und Entwicklungsvorhaben mit hohem Innovationspotenzial auf dem Gebiet der Cybersicherheit zu finanzieren und Schlüsseltechnologien, welche für die innere und äußere Sicherheit unseres Landes von größter Bedeutung sind, in Deutschland zu halten. Denn seien wir ehrlich: es kann niemals im Interesse unseres Landes sein, wenn Informationstechnik mit hoher Sicherheitsrelevanz für unser Land von Drittstaaten entwickelt und kontrolliert wird.

Andere Nationen wie Israel oder USA gehen diesen Weg der Grundlagenforschung, eingebettet und eng abgestimmt mit den Sicherheitsbehörden, schon länger. Deutschland schlägt diesen Weg nun auch ein, um im digitalen Konfliktfeld bestehen zu können. Zur Wahrheit gehört aber ebenso, dass wir im kommenden Jahr auch darüber sprechen müssen, nicht nur die technischen, sondern auch die rechtlichen Handlungsmöglichkeiten unserer staatlichen Einrichtungen angesichts der Herausforderungen von Cyberkonflikten zu überprüfen und gegebenenfalls anzupassen, um eine umfassende aktive Cyberabwehr zu ermöglichen.

Maßgabe muss dabei sein, dass diejenigen, welche für die innere und äußere Sicherheit unseres Landes jeden Tag Verantwortung tragen, das notwendige technische und rechtliche Rüstzeug erhalten, um im Konflikt zu bestehen und das Recht und die Freiheit unseres Landes tapfer zu verteidigen.

Mit herzlichen Grüßen

Dr. Peter Tauber, MdB

Berlin, 21. Dezember 2018