Digitale Souveränität
Die Schweiz muss handeln

Die Lage ist verzwickt. Da will der chinesische Telekommunikationsriese Huawei in der Schweiz zwei Forschungs- und Entwicklungszentren aufbauen und rund 100 Millionen Franken investieren. Gleichzeitig droht genau dieses Forschungsprojekt die Beziehungen mit den USA zu belasten. Die USA befürchten, China könnte das von Huawei aufgebaute 5G-Netz zu Spionage- und Sabotagezwecken ausnutzen.

Die Furcht, dass über neue Technologien wichtige Informationen in unberechtigte Hände geraten könnten, ist real. Täglich müssen weltweit, aber auch in der Schweiz unzählige Cyberattacken auf Unternehmen, Forschungsprojekte und politische Institutionen abgewehrt werden. Angriffe auf das VBS oder auf die Ruag bleiben in schlechter Erinnerung.

Diese Entwicklung zeigt: Die digitale Souveränität der Schweiz steht auf dem Prüfstand. Sie zu erhalten, ist zu einer zentralen Aufgabe für den Staat geworden. Es geht um nichts weniger als darum, selber bestimmen zu können, wozu die eigenen Daten verwendet werden.

Es geht um die innere Sicherheit und die Verteidigung der eigenen Grenzen

Der Bund muss deshalb den Tatbeweis liefern, dass die digitale Vernetzung unsere Souveränität stärkt und nicht schrittweise aushebelt.

Dieser Beweis ist sowohl für die innere Sicherheit zentral als auch für die Verteidigung der eigenen Grenzen. Wichtig sind die Verstärkung und die effizientere Organisation der Cyberabwehr, wie sie der Bund in seiner nationalen Strategie formuliert hat. Ein neuer Cyber-Defence Campus soll dazu beitragen, laufende Entwicklungen früh zu erkennen und Handlungsstrategien zu entwickeln. Ein Kompetenzzentrum soll als nationale Anlaufstelle bei Fragen zu Cyberrisiken dienen.

Damian Müller
Ständerat FDP

«Der Bund muss den Tatbeweis liefern, dass die digitale Vernetzung unsere Souveränität stärkt und nicht schrittweise aushebelt.»

Angesichts der anstehenden Grossinvestitionen in die Telekommunikationssysteme der Armee muss der Bund schnell klare Leitplanken schaffen. Da unser Land die relevante Wertschöpfung auf dem eigenen Territorium nicht garantieren kann, ist es für den Aufbau digital souveräner Systeme auf verlässliche Industriepartner angewiesen.

Diese sollen die lokalen Kernfähigkeiten stärken, damit in Krisen schnell auf nahe gelegenes technologisches Know-how zurückgegriffen werden kann. Sie müssen auch bereit sein, ihre Hardware zu zertifizieren und die Quellcodes der Software offenzulegen. Die Schweiz darf im Verteidigungsbereich keine Hintertüren für das Absaugen von Daten akzeptieren. Bietet ein Lieferant nicht Hand dazu, kommt er als Partner für sensible Anwendungen nicht infrage.

Wichtige Industriepartner müssen unabhängig sein von Drittstaaten

Die Diskussion um den 5G-Mobilfunk zeigt, dass wichtige Industriepartner unabhängig von den Interessen von Drittstaaten sein müssen. Letztlich sind auch die Schweizer Vertretungen im Ausland gefordert: Besonders jene in strategisch wichtigen Botschaften sollen mit speziell ausgebildeten Cyber-Attachés verstärkt werden, um wichtige Informationen zur Bedrohung liefern zu können.

Eine verstärkte Abwehr von Cybergefahren, eine hohe Kompetenz von Wissenschaft und Forschung, klare Leitplanken für die Beschaffung von sensiblen Gütern und Dienstleistungen sowie vertrauenswürdige Industriepartner sind ein Muss für ein digital souveränes Land.

Die Verteidigungsbereitschaft der Schweiz befindet sich auf dem Prüfstand. Sie kann nur dann von der digitalen Revolution profitieren, wenn sie ihre digitale Souveränität wahrt.