MEINE MEINUNG

Die Bundeswehr im Cyber-Raum

Dr. Reinhard Brandl MdB (CSU)
Mitglied im Verteidigungsausschuss und im Haushaltsausschuss des Deutschen Bundestages

Die Bundesverteidigungsministerin hat angekündigt, einen neuen Organisationsbereich für den Cyber- und Informationsraum in der Bundeswehr einzurichten. Dort sollen die vorhandenen Kompetenzen gebündelt und verstärkt werden. Dieser Schritt ist richtig. Fast in jedem größeren Unternehmen berichtet ein Chief Information Officer (CIO) direkt an die Leitung. Das hat seinen Grund. Der Fortschritt und die Verbreitung von Informationstechnologien verlaufen in vielen Bereichen exponentiell. Innovationszyklen werden immer kürzer. Unternehmen passen sich dem entweder rechtzeitig an oder sie verschwinden vom Markt. Die Bundeswehr wird zwar nicht verschwinden, aber ihr Auftrag im Rahmen einer gesamtstaatlichen Sicherheitsvorsorge wird sich verändern. Sie muss rechtzeitig ihre Strukturen anpassen, um in einer zunehmend digitalisierten Welt handlungsfähig zu bleiben.

Politisch werden unter dem Stichwort „Handlungsfähigkeit" oft die offensiven und defensiven Optionen im Falle von Cyber-Angriffen diskutiert. Der Schutz der eigenen Infrastruktur vor Sabotage und Spionage ist natürlich die Grundvoraussetzung, um in jeder Situation handlungsfähig zu bleiben. Da die Qualität der Angriffe steigt und auch eine indirekte Beteiligung von ausländischen Hard- und Software-Herstellern nicht ausgeschlossen werden kann, wurde der Bereich „Cyber" von der Bundesregierung zurecht als nationale Schlüsseltechnologie eingestuft. Offensive Handlungsoptionen gehören in allen Bereichen zum Portfolio der Bundeswehr. Das gilt auch für den Cyber- und Informationsraum. Meiner Meinung nach wird in der politischen Diskussion die Bedeutung dieses Bereiches für die Handlungsfähigkeit der Bundeswehr aber überschätzt. Unterschätzt werden dagegen die Herausforderungen, die erforderlichen IT-Fachkräfte am Markt zu gewinnen und die wachsende Komplexität der eigenen Infrastruktur zu beherrschen.

Ohne IT-Unterstützung wären bereits heute Einsatz und Grundbetrieb nicht im Entferntesten denkbar. Jedes moderne Waffensystem wird von einem oder mehreren Prozessoren gesteuert und ist direkt und/oder indirekt über Logistiksysteme mit dem Netz der Bundeswehr verbunden. Wenn diese nicht rechtzeitig Ersatzteile bestellen oder Wartungen vorsehen, ist das Waffensystem nicht einsatzfähig – ganz ohne Cyber-Angriff. Führung und Parlament erwarten zudem, dass die Bundeswehr „auf Knopfdruck" zu allen möglichen Fragen auskunftsfähig ist. Informationen sollen von oben nach unten, von unten nach oben sowie zwischen Organisationsbereichen und Partnernationen möglichst schnell und ohne Verluste an Schnittstellen fließen. Jede Schnittstelle ist aber gleichzeitig ein möglicher Angriffspunkt und mit jeder neuen Software/Hardware kommen neue Schnittstellen hinzu. Die eine große Herausforderung für den neuen Organisationsbereich ist daher, dies alles über zentrale Architekturvorgaben zu steuern und beherrschbar zu halten.

Die zweite große Herausforderung wird sein, die Rolle der Bundeswehr in einer nationalen IT-Sicherheitsarchitektur neu zu verankern. Es ist eine Binsenweisheit, dass der Cyber-Raum kein In- und Ausland kennt und dass sich Angreifer nicht an Ressortzuständigkeiten orientieren. Die Bundesregierung verfolgt deshalb mit ihrer Cyber-Sicherheitsstrategie zu Recht einen gesamtstaatlichen Ansatz. Das für Verteidigung zuständige Ressort, das mit weitem Abstand auch über die meisten IT-Ressourcen verfügt, müsste in einem solchen Ansatz eigentlich eine Schlüsselrolle spielen. Das ist heute nicht der Fall. Die Bundeswehr schützt sich selbst und ist darüber hinaus weitgehend auf Unabhängigkeit vom federführenden BMI bedacht. Das führt z. B. dazu, dass das WANBw, als das größte Netz innerhalb der Bundesregierung, aufgrund der Verwendung amerikanischer Verschlüsselungstechnologien über keine Zertifizierung des BSI verfügt. Wenn „Cyber" eine nationale Schlüsseltechnologie werden soll, können wir uns ein solches „Nebeneinander" von BMI und BMVg schlicht nicht leisten.

In 2016 gibt es gleich mehrere Chancen, um mehr „Miteinander" zu etablieren. Die IT im BMVg wird neu organisiert, das neue Weißbuch wird sich aus gesamtstaatlicher Sicht mit den Herausforderungen des Cyber-Raums beschäftigen. Das im Rahmen des ÖPP-Projekts HERKULES gegründete IT-Dienstleistungsunternehmen BWI geht als GmbH mit seinen ca. 2.800 Mitarbeitern in das vollständige Eigentum des Bundes über und kann damit ressortübergreifend Aufgaben übernehmen. Als Parlament sollten wir darauf achten, dass diese Chancen auch genutzt werden.