IPG
Internationale Politik
und Gesellschaft

„Cyber-Gedöns“

Warum der neue Vorstoß zur Cyber-Sicherheit am Kern des Problems vorbei geht.

Von Frank Rieger | 02.05.2016

„Das Kernproblem ist und bleibt angreifbare Software.“

Jeden Tag soll es rund 6500 Cyber-Angriffe auf Bundeseinrichtungen geben. Bisher ist es glücklicherweise noch zu keinem massiven Ausfall eines Kraftwerks oder ähnlich sensibler Infrastruktur gekommen. Nun hat Verteigigungsministerin Ursula von der Leyen bekanntgegeben, bei der Bundeswehr eine eigene Truppenorganisation „Cyber- und Informationsraum“ (CIT) mit 13 500 Soldaten und zivilen Mitarbeitern aufzustellen. Warum?

Es handelt sich dabei um den Versuch des Verteidigungsministeriums, den Bereich Netzwerksicherheit als Handlungsfeld zu besetzen. Aus meiner Sicht ist das reines Machtkalkül und wenig zielführend. Der Versuch, das Feld zu militarisieren und zu „vergeheimdienstlichen“ geht am Kern des Problems vorbei: schlechte Software, mangelnde Ausbildung und fehlende Haftungsregeln für Unternehmen. Zu glauben, man könne hier mit militärischen Mitteln irgendetwas anderes als eine Eskalation bewirken, ist naiv.

Die Lage fasste ein Bundeswehr-General mir gegenüber auf einer Veranstaltung treffend zusammen: „Solange ich über das Bundeswehr-Logistiksystem nicht einmal zuverlässig Toilettenpapier bestellen kann, brauche ich auch kein Cyber-Gedöns.“ Die Bundeswehr könnte sicher mehr IT-Experten vertragen, um ihre internen Probleme besser und sicherer zu lösen. Sich einzubilden, man bekäme qualifizierte Mitarbeiter, in dem man „Cyber Cyber“ auf Plakate druckt, ist jedoch einfach nur lächerlich.

Welche technischen, rechtlichen und ethischen Fragen wirft diese neue Art der Kriegsführung auf?

Es gibt im digitalen Raum keine Attribution. Das heißt ein „Gegenschlag“ ist kaum treffsicher zu führen, jeder Akteur wird mehrschichtige Methoden der Tarnung anwenden. Daraus folgt auch,

dass es keine wirksame Abschreckung gibt. Wenn man abschrecken will, muss man in der Lage sein, glaubhaft zu machen, dass man Angriffe zuordnen, eben attribuieren kann. Das ist jedoch selbst in einem umfassenden Überwachungssystem nicht sicher möglich.

Aus meiner Sicht ist das reines Machtkalkül und wenig zielführend.

Wird die Bundeswehr allein für Deutschlands Cyber-Sicherheit sorgen oder wie müsste eine Arbeitsteilung mit Polizei, Bundesnachrichtendienst, Ministerien und anderen Behörden aussehen?

Zuallererst ist hier das Bundesamt für die Sicherheit in der Informationstechnik zuständig. Deswegen muss es aus der Verantwortung des Innenministeriums befreit und zu einem wirklich unabhängigen Dienstleister für digitale Sicherheit gemacht werden, bei dem nicht der Verdacht der Kungelei mit Sicherheitsbehörden mit angriffsorientierten Interessen besteht. Weder Militär noch Geheimdienste haben irgendeinen strukturellen Vorteil, der ihre Verantwortlichkeit für das Gebiet nahelegt, im Gegenteil. Das Kernproblem ist und bleibt angreifbare Software, und das lässt sich nur mit massiven Förderprogrammen für eine Verbesserung der technischen Lage beheben, nicht mit Cyber-Soldaten oder Cyber-Agenten.

Ist die deutsche Cyber-Strategie mit europäischen und internationalen Maßnahmen vereinbar?

Es gibt derzeit keine Strategie, weder national noch international. Es gibt Wunschträume und Machtgerangel. Insofern passt der Bundeswehr-Vorstoß ins Bild.

Die Fragen stellte Anja Papenfuß.