Cybersicherheitspolitik entwickeln

Die derzeitige Neuausrichtung der Bundeswehr ist angesichts der Verwundbarkeit der digitalen und weltweit vernetzten Gesellschaft dringend notwendig. Das Netz und der Cyberraum wird – neben den klassischen Bereichen Land, Luft, See und Weltraum – als neuer „Operationsraum“ der Bundeswehr definiert. Für eine auf ihre Vertraulichkeit, Verlässlichkeit und Authentizität der IT-Systeme angewiesene digitale Gesellschaft wird die Cybersicherheitspolitik zu einer essenziellen Fragestellung – und von daher ist zu begrüßen, dass die Bundesregierung diese Gefährdungen erkannt hat und diesen begegnen will. Mit dem Einsatz von Cyberfähigkeiten stellen sich zahlreiche technische, rechtliche – insbesondere völkerrechtliche – aber auch ethische Fragen, auf die es derzeit noch keine Antworten gibt. Die Entwicklung der Cyberverteidigungspolitik durch das Verteidigungsministerium muss auf diese Fragestellungen Antworten geben:

1. Die Frage, ob wir einen neuen Operationsraum definieren, stellt sich nicht mehr. Er ist da. Auch wenn die ganz überwiegende Mehrheit der Cyberangriffe derzeit auf private Akteure zurückzuführen ist, entwickeln immer mehr Staaten militärische Cyberfähigkeiten.

2. Im Zeitalter von Industrie 4.0, dem Internet der Dinge und Big Data erlangt der Cyberraum eine strategische Dimension und es besteht Handlungsnotwendigkeit. Die Verletzlichkeit von Staat, Wirtschaft und Gesellschaft wächst. Wir brauchen schnelles und konsequentes politisches Handeln, um den Herausforderungen der heutigen Zeit gerecht zu werden.

3. Cyberangriffe bedrohen die moderne Industriegesellschaft. Cybersicherheit wird zur Grundlage einer digitalisierten und weltweit vernetzten Gesellschaft. Wir brauchen hierfür Prävention und Reaktion. Nicht alles ist jedoch Aufgabe der Bundeswehr. Mehr als bisher kommt es auf eine Kooperation der unterschiedlichen Akteure und eine feste Ressortzusammenarbeit an. Hierfür brauchen wir klare Regeln, Absprachen und definierte Prozesse.

4. Überprüft werden muss, in wie weit rechtliche Rahmen für die Bundeswehr ausreichend ist, damit sie auf die neuen Gefährdungslagen reagieren und eine Cyberstrategie implementieren kann.

5. Wir brauchen einen breiten gesellschaftlichen Diskurs über die notwendigen Fähigkeiten der Bundeswehr im Cyberraum. Angriffe sind häufig nicht als militärischer Akt zu erkennen. Grenzen verschwimmen, etwa zwischen Militär und Geheimdiensten, nicht-staatlichen oder Third-Party-Attacken. Gerade im Hinblick auf hybride Kriegsformen sind einzelne Aktionen schwer zu definieren und zu kategorisieren. Unklar ist auch die genaue Abgrenzung zwischen defensiven und offensiven Fähigkeiten und Instrumenten.

6. Wir brauchen eine umfassende Bestandsaufnahme. Dazu gehört auch Gefährdungs- und Angriffsszenarien für die Systeme der Bundeswehr zu definieren. Auch die Frage welche Kompromittierungen von Hard- und Software bekannt sind und welche Investitionen notwendig sind um diese abzustellen, ist bis heute nicht geklärt. Bei künftigen Ausschreibungen muss die IT-Sicherheit zwingend berücksichtigt werden,

7. Die Bundeswehr muss zum Treiber der Entwicklung deutscher IT-Kompetenz und somit digitaler Souveränität werden. Hierzu muss der Stellenwert der IT-Sicherheit in der Bundeswehr massiv gestärkt und die IT-Kompetenz ausgebaut werden, bestehende Abhängigkeiten müssen abgebaut werden. Es kommt auf eine kluge Strategie und eine strategische Beschaffungsausrichtung gerade im sicherheitsrelevanten Bereich an. Hier können erhebliche Investitionen freigesetzt werden.

8. Das Ministerium muss um die Bundeswehr ein Umfeld für innovative Sicherheitstechnologie entwickeln. Hierzu zählt auch eine Förderstrategie für Start-ups. Dies muss auch die Bereitstellung von Risikokapitel beinhalten. Andere Länder können Vorbild sein.

9. Die Forschung und Entwicklung von sicherer und vertrauenswürdiger IT – von Hard- und Software sowie Netzwerktechnik – muss massiv ausgebaut werden. Dies ist die Grundvoraussetzung, um die digitale Souveränität zurückzugewinnen bzw. zu erhalten. Um die bestehenden Abhängigkeiten abzubauen, bedarf es hier einer enormen Anstrengung auf europäischer Ebene. Entscheidende Bedeutung kommt hierbei dem Einsatz von sicherer und vertrauenswürdiger Verschlüsselungstechnologie zu. Kryptotechnologie muss daher massiv gestärkt werden.

10. Vertrauenswürdige und sichere IT setzt voraus, die Sicherheit der Komponenten und Systeme bewerten und die Funktionalitäten erkennen zu können, etwa durch die Offenlegung des Quellcodes.

11. Die Bundeswehr braucht einen durchsetzungsfähigen IT-Direktor (CIO) mit eigener Budgetverantwortung.

12. Wir brauchen eine Bestandsanalyse unserer Waffensysteme. Fast alle basieren heute auf internetbasierter Technologie. Wie technisch verwundbar sind diese und besteht Nachsteuerungsbedarf, um die Sicherheit zu erhöhen? Welche Maßnahmen müssen ergriffen werden, um die IT-Sicherheit der im Einsatz befindlichen Waffen- aber auch der Informations- und Kommunikationsinfrastruktur sicherzustellen? Das Ministerium muss hier schnell einen Investitionsplan vorlegen und die bestehenden Lücken aufzeigen. Für künftige Ausschreibungen muss die IT-Sicherheit umfassend berücksichtigt werden.

13. Neben der materiellen Ausrüstung und der Forschung und Entwicklung wird die künftige Personalentwicklung einer der Schwerpunkte der Cyberpolitik im Verteidigungsministerium sein müssen. Hier brauchen wir einen Dreiklang aus eigener Ausbildung und Anreizsystem (Laufbahn und Besoldung), einem stärkeren Einbinden der Reserve und einer Kooperation mit der Privatwirtschaft.

14. Die Stärkung der Bundeswehruniversitäten sowie die Kooperation mit weiteren Hochschulen muss ausgebaut werden. Es müssen vergleichbare Karriereperspektiven für hochausgebildete IT-Experten in der Bundeswehr eröffnet werden. Nur so kann es gelingen, die besten digitalen Köpfe für die Bundeswehr zu binden. Auch muss es durch entsprechende Datenbanken gelingen, IT-Experten der Bundeswehr und deren Kompetenz nach ihrem aktiven Dienst zu behalten und an die Bundeswehr zu binden.

15. Unter Federführung des Auswärtigen Amtes müssen völkerrechtliche Fragestellungen vorangetrieben werden. Wie muss sich das Völkerrecht in

Zeiten der Digitalisierung weiterentwickeln? Wie kann das bindende Völkerrecht mit einem gemeinsamen Verständnis über Rechte und Normen im Netz sowie über verantwortungsvolles Staatenverhalten im Cyberraum weiterentwickelt werden und ineinandergreifen? Wie können digitale Abrüstungsinitiativen und Kooperationen für mehr Sicherheit im weltweiten Netz aussehen? Deutschland muss hier wie bisher Treiber der Diskussion in den Vereinten Nationen sein, Deutschland und Europa müssen sich aktiv in allen internationalen Gremien und auf allen Ebenen, die derzeit Handlungsempfehlungen für den Cyberraum sowie dessen juristische Erfassung erarbeiten, einbringen.

16. Auf internationaler Ebene muss das Kriegsvölkerrecht, einschließlich des humanitären Völkerrechts, weiterentwickelt werden und Antworten auf die Herausforderungen der digitalen Kriegsführung geben. Dies betrifft ein besseres Verständnis, welche Art des Einsatzes von Cybermitteln völkerrechtlich zulässig ist, wo die Schwelle zum bewaffneten Angriff überschritten sein kann. Aber auch die Frage der Kennzeichnung (false flag), die Frage der Zurechenbarkeit, des Einsatzes von nicht-staatlichen Akteuren im staatlichen Auftrag (proxies) sowie der zulässigen bzw. unzulässigen strategischen und taktischen Angriffsziele und Kriegslist. Geklärt werden muss auf internationale Ebene auch die Rolle von Nachrichtendiensten. Auch hier bedarf es auf internationaler Ebene Vereinbarungen zu den notwendigen Kompetenzen und Möglichkeit von Nachrichtendiensten, aber auch zu deren Begrenzung.

17. Die Bundeswehr und die Nachrichtendienste kooperieren insbesondere bei Auslandseinsätzen. Im Bereich der Cyber-Sicherheit ist enge Zusammenarbeit notwendig. Wir müssen an dieser Schnittstelle jedoch parlamentarische Kontrolle sicherstellen.

18. Die Vereinigten Staaten von Amerika haben mit Russland und China sowie Russland und China haben untereinander Verabredungen zum Umgang mit internationalen Bedrohungen aus dem Cyberraum getroffen. Deutschland sollte mit Schlüsselpartnern ähnliche Absprachen anstreben und sich auch auf europäischer Ebene dafür einsetzen.

19. Im Rahmen der UN sollten auf internationaler Ebene Abrüstungs- und Rüstungskontrollvereinbarungen getroffen werden, um die Verwundbarkeit der digitalen und weltweit vernetzten Gesellschaft abzubauen. Deutschland sollte Arbeiten in den Vereinten Nationen zur internationalen Cybersicherheit aktiv unterstützen und vorantreiben. Dies könnte neben der Ächtung bestimmter Cybereinsätze das Einrichten von Mechanismen zur Bewältigung von Cyberzwischenfällen und Maßnahmen zur Unterstützung aller Staaten beim Erreichen eines Mindestmaßes an IT-Sicherheit umfassen.

20. Das im März 2013 von einer internationalen Expertengruppe am NATO-Exzellenzzentrum für kooperative Cyberverteidigung in Tallinn vorgestellte „Tallinn-Handbuch über das auf Cyberkriegführung anwendbare Völkerrecht“ („Tallinn Manual“) bildet eine wichtige Basis für den transatlantischen Umgang mit militärisch relevanten Cyberbedrohungen und trägt wesentlich zur Klärung bei, wie das Kriegsvölkerrecht unter den Bedingungen des Cyberzeitalters anzuwenden ist. Es sollte durch kommentierte

Rechtssätze für Cyberoperationen in Friedenszeiten ergänzt werden („Tallinn Manual 2.0“).

21. Notwendig und für die Lagekontrolle unerlässlich ist ein internationales Beobachtungs-, Analyse und Kontrollsystem zum frühzeitigen Erkennen von Cyberwaffen und Angriffen. Dies ist Aufgabe der CERTs und der CERT-Verbünde. Weiterentwickelt und in ihrem Anwendungsbereich ausgeweitet werden müssen auch die internationalen Vereinbarungen, etwa das Europaratsübereinkommen über Computerkriminalität, das derzeit eine internationale Zusammenarbeit bei geheimdienstlichen Aktionen ausschließt. Es sollte geprüft werden, ob ein solches internationales Beobachtungs-, Analyse- und Kontrollsysteme der CERT-Verbünde bei der OSZE angesiedelt werden kann.

22. Das CERTBw muss massiv gestärkt und die Zusammenarbeit mit den anderen CERTS intensiviert werden. Dabei ist zu berücksichtigen, dass die Zusammenarbeit zwischen den CERTs in den Verbünden auf die zivile IT-Sicherheit ausgerichtet ist. Das CERTBw ist darauf angewiesen, am Verbund der CERTs zu partizipieren. Diese Zusammenarbeit der CERTs darf nicht gefährdet werden.

23. Dem Bundesamt für Sicherheit in der Informationstechnik kommt in der nationalen und auch internationalen Kooperation eine Schlüsselrolle zu. Grundvoraussetzung dafür ist die Neutralität und Unabhängigkeit des BSI. Damit das BSI dieser Rolle auch in Zukunft gerecht werden kann, muss das BSI eine unabhängige oberste Bundesbehörde werden. Nur dann ist

eine offene und vertrauenswürdige Kooperation mit den unterschiedlichsten Partnern aus Wirtschaft und Gesellschaft und den verschiedenen CERTs sichergestellt.

24. Die Cybersicherheitsstrategien auf nationaler und europäischer Ebene und ihr Ineinandergreifen sollten zeitnah evaluiert und kontinuierlich weiterentwickelt werden.

25. Die Bundeswehr braucht eine Big Data Strategie um die eigene Effizienz weiter zu erhöhen. Gerade im Rüstungsbereich kann dies eine wichtige Rolle spielen.

26. Die Sensibilität innerhalb der Bundeswehr für die Gefahren im Cyberraum muss durch Intensivere Beratung und verstärktes Cybersicherheitstraining erhöht werden.

27. Der Deutsche Bundestag muss bei der zukünftigen Mandatierung der Bundeswehr für Auslandseinsätze denkbare Cyberangriffe berücksichtigen. Dies muss auch die Möglichkeit von verdeckten Einsätzen aus anderen Staaten als dem Einsatzgebiet („false flag“) und den Einsatz von nichtstaatlichen Akteuren („proxies“) umfassen.

28. Ausgebaut werden muss auch die Friedens- und Konfliktforschung: Angesichts der Verwundbarkeit der digitalen Gesellschaft und der Vielzahl und der gesamtgesellschaftlichen Bedeutung dieser vielen offenen ethischen und rechtlichen (auch völkerrechtlichen) Fragen sollten Cyberbedrohungen sowie der Einsatz von Cyberfähigkeiten in Konfliktsituationen einen

solchen Forschungsschwerpunkt für Friedens- und Konfliktforscher mit IT-Sicherheits- und Rechtswissenschaftlern bilden. Ziel muss sein, eine Gefährdung von Frieden und Sicherheit durch Cybermittel zu vermeiden.