Bundesministerium
der Verteidigung

- 1780001-V633 -

Bundesministerium der Verteidigung, 11055 Berlin

Frau
Dr. h.c. Susanne Kastner, MdB
Vorsitzende
des Verteidigungsausschusses
des Deutschen Bundestages
Platz der Republik 1
11011 Berlin

Thomas Kossendey
Parlamentarischer Staatssekretär
Mitglied des Deutschen Bundestages

HAUSANSCHRIFT Stauffenbergstraße 18, 10785 Berlin
POSTANSCHRIFT 11055 Berlin

TEL +49 (0)30 18-24-8060
FAX +49 (0)30 18-24-8088
E-MAIL BMVgBueroParlStsKossendey@bmvg.bund.de

Deutscher Bundestag
Verteidigungsausschuss

Ausschussdrucksache
17(12)896
13.04.2012 - 17/2883
5420-4

Berlin, 13. April 2012

Sehr geehrte Frau Vorsitzende,

mit Schreiben Ihres Sekretariats vom 8. März 2012 bitten Sie um Vorlage eines schriftlichen Berichtes zum Themenkomplex „Cyber Warfare“.

Den erbetenen Bericht füge ich als Anlage bei.

Mit freundlichem Gruß

Thomas Kossendey

Anlage zu Parl Sts beim Bundesminister der Verteidigung Kossendey
1780001-V633 vom 13. April 2012

Bericht

zum

Themenkomplex „Cyber-Warfare“

Gefährdungslage

Fehlerbehaftete oder kompromittierte IT-Produkte und Komponenten, der Ausfall von Informationsinfrastrukturen oder schwerwiegende Angriffe im Cyber-Raum können zu erheblichen Beeinträchtigungen der technischen, wirtschaftlichen und administrativen Leistungsfähigkeit und damit der gesellschaftlichen Lebensgrundlagen Deutschlands führen.

Dabei werden die IT-Systeme und -Komponenten aufgrund hoher Komplexität immer verwundbarer. Insbesondere die Wandlungsfähigkeit von Schadsoftware und die Verfügbarkeit von immer ausgereifteren Werkzeugen für das Design und Redesign von Schadsoftware stellen eine zunehmende Bedrohung dar. Potenzielle Angreifer können somit im Internet preiswert angebotene Schadsoftware nebst Werkzeugen zu deren Konfiguration und Anpassung mieten und für missbräuchliche Zwecke nutzen.

Der Vorfall „Stuxnet" (Juli 2010) hat gezeigt, dass Cyber-Angriffe nicht ausschließlich online, sondern z.B. auch über bewegliche Datenträger erfolgen können. Damit sind selbst bislang vom offenen Internet als sicher abgetrennt vermutete IT-Systeme, wie Industrieproduktionsstätten oder Kritische Infrastrukturen, verwundbar. Hieraus muss auch die zunehmende Bedeutung von notwendigen Maßnahmen der IT-Abschirmung abgeleitet werden.

Im Rahmen des Risikomanagements analysiert und bewertet die Bundeswehr kontinuierlich die Bedrohungs- und Gefährdungslage des IT-Systems der Bundeswehr. Das Computer Emergency Response Team der Bundeswehr (CERTBw) führt dazu auf Basis einer Vereinbarung zum Informationsaustausch mit anderen nationalen und internationalen CERT-Organisationen und mit Hilfe seiner technischen Sensorik ein aktuelles Lagebild zur IT-Sicherheit. Das Betriebszentrum IT-System der Bundeswehr führt darüber hinaus ein aktuelles Gesamtlagebild des IT-Systems Bundeswehr, bei dem auch Gefährdungen betrachtet werden, die nicht informationstechnischer Natur sind (z.B. Naturkatastrophen, Feuer). Bei einer möglichen kritischen Lage wird ein Risiko Management Board einberufen, in dem die von der Gefährdung betroffenen Bereiche und die für den Schutz bzw. die Wiederherstellung der Sicherheit zuständigen Funktionsträger die weitere Koordinierung der Maßnahmen übernehmen.

Die extern zugänglichen Schnittstellen des IT-Systems der Bundeswehr werden kontinuierlich durch gerichtete und ungerichtete Angriffe von Hackern bzw. durch das Einbringen von Schadsoftware bedroht.

Zum Begriff des „Cyber-War"

„Cyber-War" beschreibt dem Wortsinn nach gezielte Angriffe staatlicher Institutionen auf Computersysteme und IT-Netzwerke eines oder mehrerer anderer Staaten, die substanzielle Auswirkungen auf die Handlungsfähigkeit dieser Staaten haben. Die nationale Sicherheitsstrategie „Cyber-Sicherheitsstrategie für Deutschland" definiert lediglich den Begriff „Cyber-Angriff" und verwendet den Begriff „Cyber-War" oder „Cyber-Krieg" nicht. Der Begriff „Cyber-Angriff" umfasst je nach Urheber zusätzlich die Aktionen „Cyber-Ausspähung" und „Cyber-Spionage".

Aus Sicht der Bundesregierung beschreibt der Begriff „Cyber-War" oder „Cyber-Krieg" die tatsächlichen sicherheitspolitischen Herausforderungen nur unzureichend und suggeriert ein falsches Bild sowohl betreffend der Bedrohungslage im Cyberspace als auch der möglichen Gegenmaßnahmen.

Das IT-System der Bundeswehr ist, genau wie alle IT des Bundes, zu jeder Zeit einer Vielzahl von unterschiedlich motivierten und technisch versierten Angriffen eines breiten Spektrums von Akteuren ausgesetzt, ohne dass hierfür der Begriff Krieg angemessen wäre.

In der Bewertung der Bedrohungslage durch die Bundesregierung werden Maßnahmen im und durch den Cyberspace zunehmend operative Bedeutung bei kriegerischen Auseinandersetzungen sowohl zwischen Staaten als auch bei Auseinandersetzungen nicht-staatlicher Akteure haben. Militärisch wird der Cyberspace daher, entsprechend der Bedeutung des Faktors Information für die Erfüllung der politisch vorgegebenen Aufgaben, als operative Domäne, vergleichbar dem Luft- oder Seeraum, behandelt.

Cyber-Sicherheit in der Bundeswehr

Die Bundeswehr hat sich sehr frühzeitig auf die Bedrohungen aus dem Cyberspace eingestellt und bereits 1992 begonnen, zur präventiven Cyberabwehr eine IT-Sicherheitsorganisation mit speziell ausgebildeten IT-Sicherheitsbeauftragten in allen Dienststellen der Bundeswehr, aufzubauen. Im Jahr 2002 wurde das CERTBw eingerichtet, das dem Bundesamt für Informationsmanagement und Informationstechnik der Bundeswehr (IT-AmtBw) unterstellt ist.

Da zielgerichtete Cyber-Angriffe hoher Qualität durch präventive Maßnahmen nicht vollständig verhindert werden können, kommt dem Krisenmanagement und der Fähigkeit zur Angriffserkennung, Schadensbegrenzung und Wiederherstellung der IT-Systeme eine wachsende Bedeutung zu. Hierzu haben das für die IT-Sicherheitsorganisation zuständige IT-AmtBw und die für den Betrieb des IT-Systems verantwortliche Führungsunterstützungsorganisation der Bundeswehr, geführt durch das Streitkräfteunterstützungskommando, das eingangs erwähnte gemeinsame Risiko Management-Board eingerichtet.

Ende 2010 erreichte die zentrale Betriebsführungseinrichtung für das gesamte IT-System der Bundeswehr seine Grundbefähigung. Dort können Betriebsanomalien, die u.a. durch Cyber-Angriffe hervorgerufen werden können, erkannt werden. Vor allem jedoch erfolgen dort verzugslos alle betrieblichen Steuerungsmaßnahmen für das IT-System der Bundeswehr auf Basis umfassender, aktueller Lageerkenntnisse zu allen wesentlichen IT-Systemen nach aktuellen operationellen Schwerpunkten.

Das IT-System der Bundeswehr nutzt die verfügbaren technischen Sicherheitsmaßnahmen (u.a Virenschutz, Firewalls, Intrusion Detection Sensoren, Verschlüsselung, Schnittstellenkontrollmaßnahmen) und orientiert sich dabei an den grundsätzlichen Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Insgesamt ist zu betonen, dass die Gewährleistung von Sicherheit im Cyber-Raum eine Aufgabe ist, die nicht ausschließlich durch die IT-Sicherheitsorganisation oder die IT-Abschirmung geleistet werden kann. Vielmehr müssen auch die Betreiber der Netze (militärische und nicht-militärische Betriebsführung und IT-Administratoren, aber auch Vertragspartner, sog. Provider) als auch die Nutzer selbst ihren Beitrag zur Sicherheit leisten. Die Bundeswehr trägt dieser Notwendigkeit durch entsprechende Ausbildung ihres IT-Betriebspersonals genauso Rechnung wie durch Sicherheitsauflagen für zivile Provider, ständige Unterrichtungen und Belehrungen der Nutzer.

Die Fähigkeiten der Bundeswehr zur Wirkung in gegnerischen Netzwerken (Computer Netzwerk Operationen (CNO)) ist grundsätzlich getrennt von Maßnahmen der Cyber Defence, also der Abwehr von Cyber-Angriffen, zu sehen. CNO sind ein weiteres Wirkmittel der Streitkräfte.

Die Bundeswehr stellt derzeit beim Kommando Strategische Aufklärung die Abteilung Computernetzwerkoperationen auf. Eine Anfangsbefähigung zum Wirken in gegnerischen Netzen wurde erreicht. Für die Ausbildung bzw. zur Erprobung von Verfahren besteht die Möglichkeit zur Durchführung von Simulationen in einer abgeschlossenen Laborumgebung.

Zusammenarbeit in der Cyber-Sicherheit

Nationale Ebene

IT-AmtBw und CERTBw arbeiten auf Grundlage des BSI-Gesetzes eng mit dem BSI und dem dort angesiedelten IT-Lage- und Analysezentrum zusammen. Ziel der Zusammenarbeit ist es, Gefahrenquellen so früh wie möglich zu erkennen, zu beurteilen und so schnell wie möglich konzertierte Gegenmaßnahmen zu ergreifen. Dabei ist immer auch eine enge Zusammenarbeit mit nationalen und internationalen Herstellern von IT-Sicherheitsprodukten von Bedeutung. Gemäß der „Allgemeinen Verwaltungsverordnung zu § 4 des BSI-Gesetzes" meldet die Bundeswehr kritische IT-Sicherheitsvorkommnisse an das IT-Lage- und Analysezentrum beim BSI. Die Bewertung nimmt der IT-Sicherheitsbeauftragte der Bundeswehr vor. Bei einer vom BSI festgestellten übergreifenden oder nationalen IT-Krise wächst das IT-Lage- und Analysezentrum beim BSI zu einem IT-Krisenreaktionszentrum auf.

Grundsätzliche Fragen der IT-Steuerung und IT-Sicherheit der IT des Bundes werden zudem im ressortübergreifenden Rat der IT-Beauftragten (auch IT-Rat genannt) behandelt. Hier wird die Bundeswehr durch den IT-Direktor vertreten.

Mit der Cyber-Sicherheitsstrategie für Deutschland wurden die bestehenden Maßnahmen der Bundesregierung zur Gewährleistung der Cyber-Sicherheit in Deutschland weiterentwickelt.

Das Bundesministerium der Verteidigung (BMVg) ist ständiges Mitglied des Cyber-Sicherheitsrats, vertreten durch einen beamteten Staatssekretär. Darüber hinaus beteiligt sich die Bundeswehr am Nationalen Cyber-Abwehrzentrum unter Wahrung ihrer verfassungsrechtlichen sowie gesetzlichen Aufgaben und Befugnisse. Im Cyber-Abwehrzentrum tauschen die beteiligten Behörden Erkenntnisse zu neuen Bedrohungen, Sicherheitslücken oder Schadprogrammen aus. Hierzu wurden

Verbindungspersonen der IT-Sicherheitsorganisation der Bundeswehr, der zentralen Betriebsführung und des Militärischen Abschirmdienstes in das Nationale Cyber-Abwehrzentrum entsandt.

Internationale Ebene

Aufgrund des globalen Charakters des Cyberspace kann den sicherheitspolitischen Herausforderungen nur in einem kooperativen und internationalen Ansatz begegnet werden.

Von besonderer Bedeutung ist dabei der zügige Informationsaustausch der Experten auf europäischer und internationaler Ebene zu neuen Sicherheitslücken, Schadprogrammen oder anderen Cyber-Bedrohungen. Das BSI betreibt hierzu für die Bundesverwaltung das CERT-Bund, das mit ähnlichen Einrichtungen innerhalb der EU sowie weltweit in regelmäßigem Kontakt steht, um frühzeitig neue Gefahren zu erkennen und Handlungsempfehlungen zu geben.

Großes Potential zur Verbesserung der Cyber-Sicherheit misst die Bundesregierung Maßnahmen kooperativer Sicherheit im Cyberspace zu. In enger Abstimmung insbesondere mit USA, GBR und FRA setzt sich die Bundesregierung für die Entwicklung von Normen für staatliches Verhalten im Cyberspace und Vertrauens- und Sicherheitsbildende Maßnahmen ein. Anlässlich der Cyber-Sicherheits-Konferenz der OSZE im Mai 2011 hat DEU erste Vorschläge für mögliche Elemente eines solchen, von möglichst vielen Staaten zu zeichnenden Verhaltenskodex vorgestellt, u.a.:

- Die Bestätigung der grundsätzlichen Prinzipien von Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität von Daten und Netzwerken sowie des Schutzes geistigen Eigentums;

- die Verantwortung zum Schutz kritischer Infrastrukturen;

- die Intensivierung internationaler Kooperation mit dem Ziel, Vertrauen, Transparenz und Stabilität zu fördern und Risiken zu reduzieren;

- die Etablierung oder Aufwertung von Krisenkommunikationsverbindungen und Frühwarnmechanismen unter Einbeziehung von Cyber-Angriffen.

NATO

Das 2010 beschlossene Strategische Konzept der NATO identifiziert Cyber-Sicherheit als prominente sicherheitspolitische Herausforderung. Die Staats- und Regierungschefs der Allianz haben anlässlich des Gipfeltreffens in Lissabon die Erarbeitung einer neuen NATO Cyber Defence Policy beauftragt.

Der Kern dieser beim Treffen der NATO-Verteidigungsminister am 8. Juni 2011 beschlossenen Cyber Defence Policy ist die Schaffung klarer Zuständigkeiten für Cyber Defence innerhalb der Organisation, damit diese besser in der Lage ist, einheitliche Grundsätze und Standards für die Netzwerklandschaft der NATO durchzusetzen und auf diese Weise einen wirksamen Schutz der NATO vor Angriffen aus dem Cyber-Raum zu gewährleisten.

Ebenso wichtig ist die Berücksichtigung von Fragen der Cyber-Sicherheit im gesamten Aufgabenspektrum der NATO, d.h. sowohl in der Bewusstseinsförderung von Risiken und Bedrohungen im Umgang mit IT bis hin zur Einbeziehung in den militärischen Planungsprozess, um eine Auftragserfüllung auch bei einer Beeinträchtigung der IT-Netze sicherstellen zu können. Alle Schritte zur Umsetzung der NATO Cyber Defence Policy sind in einem detaillierten Arbeitsplan festgehalten, der durch die jeweiligen Gremien und Agenturen innerhalb der NATO abgearbeitet wird. Die Erfüllung der Maßnahmen wird engmaschig durch das Defence Policy and Planning Committee (DPPC) und das Consultation, Command and Control Board (C3B), in dem auch die Bundesregierung vertreten ist, überwacht.

Wichtigstes Gremium im Falle einer Cyberkrise ist das Cyber Defence Management Board (CDMB), das die notwendigen Maßnahmen zur Krisenbewältigung ergreift und über ein Cyber Defence Coordination and Support Center (CD CSC) u.a. auch das NATO Computer Incident Response Capability (NCIRC) steuert. Auf Arbeitsebene kooperiert das CERTBw eng mit dem CERT der NATO (NCIRC).

Die Bundeswehr beteiligt sich darüber hinaus seit dessen Aufstellung am „Cooperative Cyber Defence Centre of Excellence" (CCD CoE) in Tallinn, das durch die NATO Ende 2008 als Kompetenzzentrum akkreditiert worden ist. Derzeit stellt die Bundeswehr dort den Chef des Stabes, eine Rechtsberaterin und einen Offizier in der Forschungs- und Entwicklungsabteilung. Das BMVg ist stimmberechtigtes Mitglied in der Steuerungsgruppe des CCD CoE.

Bilaterale Beziehungen

Fragen der Cyber-Sicherheit sind grundsätzlich Gegenstand der militärpolitischen Abstimmungen mit DEU Verbündeten und Partnern.

Eine besondere Bedeutung kommt dabei insbesondere den USA, FRA und GBR sowie CHE zu. Mit dem USA Verteidigungsministerium wurde im Mai 2008 ein entsprechendes Kooperationsabkommen der IT-Sicherheitsorganisationen geschlossen, auf militärpolitischer Ebene wurde der Dialog mit den USA im November 2010 aufgenommen. Analog wurde auch mit CHE sowohl auf Arbeitsebene als auch zwischen den beteiligten Regierungsressorts ein Erfahrungsaustausch begonnen.