Deutscher Bundestag
Verteidigungsausschuss

Ausschussdrucksache
18(12)640

22.02.2016 - 18/2702

5410

Stellungnahme zur Öffentlichen Anhörung des Verteidigungsausschusses des Deutschen Bundestages am 22. Februar 2016

„Die Rolle der Bundeswehr im Cyberraum - Verfassungs-, völker- und sonstige nationale und internationale rechtliche Fragen sowie ethische Aspekte im Zusammenhang mit Cyberwarfare und die hieraus erwachsenden Herausforderungen und Aufgaben für die Bundeswehr“

Schriftliche Stellungnahme von Dr. Marcel Dickow,
Leiter Forschungsgruppe Sicherheitspolitik, Stiftung Wissenschaft und Politik

Systematiken im Cyberraum

Im Datenraum (Cyberraum) sind klassische Paradigmen wie Angriff und Verteidigung, Unterscheidungen in rein defensive und offensive Fähigkeiten und das Prinzip der Territorialität wenigstens degeneriert, wenn nicht gänzlich aufgehoben. Das ist das Resultat besonderer technologischer Eigenschaften des Datenraums. Dazu zählen die logische Trennung von Daten und Infrastruktur, die Abstraktion von Software gegenüber der Hardware und die Möglichkeiten, die kryptologische, also mathematische Verfahren schaffen um Identifikation, Zurechenbarkeit und Aufklärung zu verhindern. Während Verteidigung in der realen, physischen Welt in einem kausalen, messbaren Verhältnis zum gerade ablaufenden Angriff oder gerade ablaufenden Angriffsvorbereitungen steht - sie ist die mittelbare oder unmittelbare Schutzreaktion auf (stattfindende oder unmittelbar bevorstehende) Gewaltausübung - fehlen solche Eindeutigkeiten im Cyberraum. Der Ursprung eines Angriffs kann hier selten direkt und unmittelbar beobachtet werden, eine Attribution ist wenn überhaupt nur mit erheblichem forensischen Aufwand im Nachhinein möglich. Oft scheitert sie gänzlich.

Konzepte von Verteidigung im Cyberraum können je nach Fähigkeiten, Strategie und politischer sowie rechtlicher Maßgabe unterschiedliche

Intensität, Reaktivität und Aggressivität aufweisen. Dieses Kontinuum beginnt beim rein passiven Eigenschutz von Infrastruktur, Diensten und Systemen. Schon das führt bereits zur Ausbildung offensiver Fähigkeiten. Nur wer in der Lage ist, den Schutz der eigenen, zu verteidigenden Systeme zu testen, kann sich einigermaßen wirksam und nachhaltig schützen. Das Testen ist allerdings ein Entwickeln und Üben von Angriffsfähigkeiten, wenngleich nur nach „innen“ und nicht nach „außen“ gerichtet. Damit verschwindet die technische Unterscheidung von defensiven und offensiven Maßnahmen, allein Intention und Ziel, also die Anwendung, bestimmen den Charakter des Mittels. Die komplexe Aufgabe des Infrastrukturschutzes beinhaltet folgerichtig ein kontinuierliches Angreifen eigener Systeme und die Implementierung daraus resultierender Erkenntnisse zur Verbesserung des Eigenschutzes. Zusätzlich müssen Fähigkeiten zur Detektion eines Eindringens (*intrusion detection*) eingesetzt und interne Dienste, Verkehre und Verhalten andauernd überwacht werden (*traffic and behavior monitoring*). Dieses Studium eigener Infrastruktur und Systemarchitektur generiert zusätzliches Wissen, das für offensive Mittel und Wirken genutzt werden kann. Um eine politische Schranke zwischen der Generierung von offensiven Wissen und der Entwicklung offensiver Fähigkeiten zu schaffen, hat die NSA bislang Eigenschutz und Operationen in fremden Netzen/Systemen institutionell getrennt gehalten[1].

Angriffe im Cyberraum

Angriffe auf IT-Systeme sind möglich, weil Hard- und Software systematische und/oder zufällige Schwachstellen (Verwundbarkeiten) aufweisen. Die Ursachen dafür sind vielfältig: *Security by design* ist noch immer keine Selbstverständlichkeit beim Entwickeln von Software, das Testen von Hard- und Software kann nicht beliebig intensiv durchgeführt werden, Systeme aus heterogenen Komponenten erzeugen unerwartete Fehlerquellen,

[1] Mit der aktuellen institutionellen Reform der NSA wurde diese Trennung aufgehoben. Siehe dazu z.B. „NSA merging anti-hacker team that fixes security holes with one that uses them | US news | The Guardian“, zugegriffen 21. Februar 2016, http://www.theguardian.com/technology/2016/feb/03/nsa-hacker-cybersecurity-intelligence. Schon im Jahre 2013 hatte eine von Präsident Obama berufene Regierungskommission in den USA das Gegenteil empfohlen (siehe „Liberty and security in a changing world - Report and Recommendations of The President’s Review Group on Intelligence and Communications Technologies“, 12. Dezember 2013, https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.).

benutzte Programmiersprachen und Compiler können selbst fehlerhaft und/oder veraltet sein, Überkomplexität, fehlerhafte Implementierungen, zu spätes Patchen (Fehlerbeseitigung) und menschliches Versagen stellen nur einige Ursachen dar. Nicht zuletzt ist Hardware und Software immer vom Menschen entwickelt und damit fehleranfällig, wenngleich inzwischen Teile von Softwareentwicklung und Programmierung automatisiert ablaufen können. Zum Schutz der eigenen Systeme müssen solche Schwachstellen möglichst schnell entdeckt und geschlossen werden. Angreifer jedoch sammeln und nutzen das Wissen um solche Verwundbarkeiten, um in gegnerische Systeme eindringen zu können[2]. Ungepachte Schwachstellen, sogenannte *0-day vulnerabilities*, stellen zusammen mit systematischen Verwundbarkeiten, z.B. unsicherer Hardware, das Haupteinfallstor dar. Staaten, staatliche Stellen und Streitkräfte geraten in einen nicht auflösbaren Interessenskonflikt, wenn sie gleichzeitig für den Schutz von IT-Infrastruktur und für offensive Cyber-Fähigkeiten zuständig sind. Das trifft um so mehr zu, wenn sie zum Schließen von Sicherheitslücken auf die Hilfe kommerzieller Unternehmen angewiesen sind. Dies ist die Regel in zivilen und staatlichen Netzen, die größtenteils proprietäre Software, wie z.B. Microsoft Windows, einsetzen. Dass solche Unternehmen zivile und militärische Netze ausrüsten, global Kunden akquirieren und diese mit Soft- und Hardware ausstatten, macht die beschriebenen Verwundbarkeiten zu einem Problem der internationalen (Cyber-)Sicherheit.

Schutz und Verteidigung im Cyberraum

Der Eigenschutz von Infrastruktur bietet nur relative Sicherheit. Wie in der zu schützenden Systemarchitektur können auch in der Sicherheitsarchitektur Schwachstellen und Lücken klaffen[3]. Dies ist statistisch gesehen bei komplexen Systemen sogar unvermeidbar. Entnetzung, Abschottung oder systematische, logische Begrenzungen innerhalb der Netze können das

[2] Dies geben inzwischen sogar staatliche Stellen, wie das FBI öffentlich zu: siehe „Meet the woman in charge of the FBI's most controversial high-tech tools - The Washington Post", zugegriffen 21. Februar 2016, https://www.washingtonpost.com/world/national-security/meet-the-woman-in-charge-of-the-fbis-most-contentious-high-tech-tools/2015/12/08/15adb35e-9860-11e5-8917-653b65c809eb_story.html.

[3] siehe z.B. das geringe Sicherheitsniveau von kommerzieller Anti-Virus-Produkten beschrieben bei „Mängel beim Selbstschutz von Antiviren-Software | heise Security", zugegriffen 21. Februar 2016, http://www.heise.de/security/meldung/Maengel-beim-Selbstschutz-von-Antiviren-Software-2465869.html.

Schutzniveau verbessern. Diese Maßnahmen können dauerhaft oder nur temporär, z.B. während eines Angriffs oder Eindringens, eingesetzt werden. Solange sie auf die eigene Infrastruktur begrenzt bleiben, entstehen keine völkerrechtlichen Grauzonen. Es gibt allerdings konzeptionelle Überlegungen, die Verteidigung gegen Angriffe bereits in die vorgelagerten Netzen Anderer zu tragen, wenn die eigenen Schutzsysteme nicht wirksam erscheinen oder technische Parameter dort höhere Erfolgsaussichten nahelegen. Konsequent zu Ende gedacht bedeutet eine solche Strategie, den Angreifer in seinem eigenen System anzugreifen während dieser von dort aus gerade operiert oder die Vorbereitungen dazu trifft. Die Identifikation des Angreifers ist aber nur dann eindeutig möglich, wenn der Angriff über alle benutzten eigenen und fremden Netze/Strukturen bis zu seinem Ursprung zurückverfolgt werden kann. Da bei komplexen Angriffsszenarien über das Internet nicht davon auszugehen ist, dass alle Betreiber der genutzten Kontenpunkte (augenblicklich, also während des Angriffs) kooperieren, ist der Angegriffene bei dieser Strategie gezwungen, selbst fremde Netze/Strukturen zu infiltrieren oder gar abzuschalten, um die Verteidigung wirksam werden zu lassen. Dieses Verfahren wird Counter-Hacking genannt und involviert zwangsläufig jene Dritte (bzw. ihre Netze/Strukturen), die der Angreifer zur Verschleierung seines Ursprungs genutzt hat. Nur bei Insider-Attacken in nach außen hin abgeschotteten Netzen ist eine solche, unmittelbare Verteidigungsstrategie erst einmal zwecklos.

Das Attributionsparadigma

Attribution von Cyber-Angriffen stellt also ein wesentliches, möglicherweise nie vollständig systematisch zu lösendes Problem des Cyberraums dar. Obwohl es forensische Instrumente gibt, die ein nachträgliches Bestimmen des Angreifers und seiner Herkunft gelegentlich ermöglichen, z.B. die Analyse des Angriffsquellcodes oder die Auswertung von Log- und Verkehrsdaten aller involvierten Netze, ist eine eindeutige Zuweisung von Angriffen zu (politischen oder institutionellen) Akteuren vermutlich nur dann realistisch, wenn der Angegriffene sich bereits im System des Angreifers befindet und somit den Beginn und Ablauf des Angriffs an seinem Ursprung mitverfolgen und nachweisen kann. Dieser Ansatz macht den Angegriffenen zum Angreifer und gefährdet die juristische Verwertbarkeit der so erlangten Beweismittel. In letzter Konsequenz führt dieser Ansatz die

danach handelnden Akteure dazu, zu jeder Zeit möglichst viele andere, gegnerische Systeme vorbeugend zu infiltrieren und somit ein Interesse an größtmöglicher Unsicherheit von IT-Systemen zu haben.

Charakteristika Digitaler Waffen

Digitale Waffen, also Schadcode (*malicious code*) zum Ausnutzen von Sicherheitslücken, beinhalten in der Regel weitere Funktionalitäten: (1) die Verhinderung bzw. Erschwerung der eigenen Entdeckung, (2) die Weiterverbreitung innerhalb bereits infiltrierter Systeme, (3) die Manipulation des Wirtsystems, (4) die Datenausleitung und (5) die Kommunikation zum *command and control server* zwecks Steuerung durch den Angreifer. Einmal entworfen müssen digitale Waffen ständig weiterentwickelt und an den Gegner und dessen IT-Systeme angepasst werden, und das in deutlich kürzeren zeitlichen Intervallen wie das bei herkömmlichen Waffensystemen notwendig ist. Neue Zugangsmöglichkeiten zum System des Angegriffenen (*0-day exploits*) müssen entdeckt, gesammelt und eingepflegt werden, das anzugreifende System muss unter ständiger Beobachtung - am besten von innen - stehen, um Abwehrmaßnahmen aufzuklären und um vor Entdeckung geschützt zu sein. Hard- und Software-Veränderungen beim Angriffsziel, die ein erfahrener Administrator neben systematischer Überwachung regelmäßig und quasi-willkürlich durchführt, müssen antizipiert und berücksichtigt werden. Deswegen werden digitale Waffen frühzeitig in gegnerischen Systemen platziert um im Angriffsfall bestmöglich auf das Angriffsziel vorbereitet zu sein[4]. Ist die digitale Waffe einmal eingesetzt, ist es nur noch eine Frage der Zeit, bis sie entdeckt und ihr Code analysiert bzw. *reverse-engineered* wurde. Deswegen sind digitale Waffen wartungsaufwändige Einmal-Wirkmittel, die zudem ein hohes Proliferationsrisiko aufweisen. Der Stuxnet-Angriff belegt dies eindrucksvoll. Trotz dieser Einschränkungen bleibt der Angreifer aber prinzipiell im Vorteil gegenüber dem Angegriffenen. Es ist leichter EINE neue Sicherheitslücke beim Gegner

[4] Wie weit solche Strategien gehen können, zeigen Gerüchte um das Programm „Nitro Zeus“, über die der Dokumentarfilm „Zero Days“ im Februar 2016 berichtet. Siehe dazu „U.S. Hacked Into Iran’s Critical Civilian Infrastructure For Massive Cyberattack, New Film Claims - BuzzFeed News“, zugegriffen 21. Februar 2016, http://www.buzzfeed.com/jamesball/us-hacked-into-irans-critical-civilian-infrastructure-for-ma#.qe7q1PkxX.

zu finden als ALLE vorhanden Sicherheitslücken (im eigenen System) zu schließen.

Digitale Waffen, also Angriffe im Cyberraum, können auf zivile wie militärische, auf geschlossene wie vernetzte Systeme geführt werden. Proprietäre, militärische Systeme können davon ebenso betroffen sein wie zivile, quelloffene Infrastruktur. Proliferation kann dazu führen, dass nach kurzer Zeit Trittbrettfahrer (wie die organisierte Kriminalität) militärischen Schadcode für Angriffe auf zivile Infrastruktur oder Computer nutzen, selbst wenn der ursprüngliche Angriff hochspezialisiert war (siehe Stuxnet). Der Trend in Streitkräften weltweit, zivile *commercial-off-the-shelf*-Technologie und IT einzusetzen, fördert das „Recyceln" militärischen Schadcodes zusätzlich.

Schlussfolgerungen für die Bundeswehr

Die Bundeswehr ist im Friedensfall, umso mehr im (Auslands-)Einsatz oder im Verteidigungsfall darauf angewiesen, ihre Netze und die dafür notwendige Infrastruktur gegen Angriffe von außen zu schützen. Im erklärten Verteidigungsfall kann sich diese Aufgabe zusätzlich auf die kritische, zivile Infrastruktur erstrecken, wie dies auch bei einem konventionellen Angriff gegeben wäre.

Neben der erforderlichen völkerrechtlichen Bewertung von Angriff und Verteidigung im Cyberraum bleiben politische Fragen bezüglich der Rolle und der Mittel der Bundeswehr. Erstens, soll und darf die Bundeswehr im Friedensfall Schutzfunktionen für kritische IT-Infrastruktur jenseits ihrer eigenen übernehmen? Zweitens, welche Mittel soll und darf sie zur Verteidigung (eigener und ziviler) Systeme einsetzen? Drittens, soll und darf die Bundeswehr offensive Fähigkeiten entwickeln und einsetzen?

1. *Soll und darf die Bundeswehr im Friedensfall Schutzfunktionen für kritische IT-Infrastruktur jenseits ihrer eigenen übernehmen?*

Mit Blick auf die Analyse von Systematiken und Charakteristika des Cyberraums plädiert der Autor für eine enge Beschränkung der Aufgaben der Bundeswehr im Friedensfall auf den Schutz eigener IT-Systeme. Das bedeutet nicht, dass Erkenntnisse über Verwundbarkeiten von IT-Systemen nicht mit anderen staatlichen Stellen zum Zwecke von deren Behebung geteilt werden sollen. Für den Schutz ziviler IT-Infrastruktur bedarf es ziviler,

unabhängiger Stellen, die in keinen Interessenskonflikt mit möglichen offensiven Fähigkeiten geraten können[5].

2. *Welche Mittel soll und darf die Bundeswehr zur Verteidigung (eigener und ziviler) Systeme einsetzen?*

Die Verteidigungsfähigkeit der Bundeswehr sollte im Friedensfall ausschließlich auf die eignen Netze und im Verteidigungsfall ausschließlich auf die eignen und die Netze der in den Konflikt involvierten Akteure (Gegner) beschränkt bleiben. Denkbare Angriffe im Zuge einer „aktiven" Verteidigung auf rein militärische Systeme[6] im Rahmen einer größeren, konventionellen Auseinandersetzung können wirksam und angemessen sein, bergen jedoch immer Eskalations- und Proliferationsrisiken. Eine solche Verteidigung wäre ohne intensive Vorbereitung nicht möglich und stellt de facto die Entwicklung von offensiven Cyber-Angriffsfähigkeiten dar. Der Autor rät in diesem Falle ebenfalls zu einem Verzicht bezüglich der Entwicklung dieser Einsatzmittel.

3. *Soll und darf die Bundeswehr offensive Fähigkeiten entwickeln und einsetzen?*

Vor dem Hintergrund der beschriebenen Eskalations-, Proliferations- und Sicherheitsrisiken rät der Autor generell davon ab, offensive Fähigkeiten im Cyberraum für die Bundeswehr zu entwickeln oder entwickeln zu lassen. Drei Gründe sind dafür besonders bedeutend: (1) Offensive Fähigkeiten im Cyberraum bedürfen offener Sicherheitslücken in Software, die im Allgemeinen auch eigene zivile und militärische System betreffen. Diese gezielt nicht zu schließen vergrößert die Risiken und unterminiert die internationale (Cyber-)Sicherheit. Zudem würde die Bundeswehr den globalen, kommerziellen Handel mit „0-days" weiter befeuern. (2) Vorbereitende Maßnahmen zum Entwickeln und für das Platzieren von Schadcode in gegnerischen Systemen führen auf einen Pfad, der beinhaltet, fremde Systeme generell als legitime Ziele aufzufassen und routinemäßig anzugreifen, um für den Ernstfall vorbereitet zu sein. Diese „Kolonialisierung des Netzes"[7] widerspricht der deutschen Kultur der militärischen Zurück-

[5] Der Autor plädiert an dieser Stelle für eine Unabhängigkeit des BSI vom Bundesministerium des Inneren und u.a. eine Beschränkung des BSI auf Daten- und Kommunikationssicherheit, den Schutz von kritischer IT-Infrastruktur sowie die (Entwicklung und) Zertifizierung von IT-Produkten.

[6] Z.B. die Sabotage von angreifenden Flugzeugen oder ihrer Command and Control (C2) Infrastruktur durch Schadcode.

[7] Vergl. Dokumente der NSA aus dem Fundus von Edward Snowden: „NSA/GCHQ: Das HACIENDA-Programm zur Kolonisierung des Internet | c't Magazin", zugegriffen 21. Februar

haltung und trägt große Eskalationsrisiken in sich, wenn sich dies als Staatenpraxis durchsetzt. (3) Die Entwicklung von offensiven Cyber-Angriffsfähigkeiten in und durch die Bundeswehr würde die Glaubwürdigkeit deutscher (Cyber-)Außenpolitik, vor allem in den Politikbereichen Internet Governance, Völkerrecht des Netzes und Menschenrechte online, massiv einschränken und damit gegen fundamentale ökonomische und menschenrechtspolitische Interessen der Bundesrepublik Deutschland verstoßen. Westliche Staaten wie die USA, Großbritannien und Frankreich haben diese Erfahrung in den vergangenen Jahren bereits gemacht. Diesem Beispiel sollte Deutschland nicht folgen.

2016, http://www.heise.de/ct/artikel/NSA-GCHQ-Das-HACIENDA-Programm-zur-Kolonisierung-des-Internet-2292574.html.

Ausgewählte, weiterführende SWP-Literatur:

Christian Schaller: *Internationale Sicherheit und Völkerrecht im Cyberspace*, SWP-Studie, Oktober 2014, http://www.swp-berlin.org/publikationen/swp-studien-de/swp-studien-detail/article/internationale_sicherheit_und_voelkerrecht_im_cyberspace.html.

Marcel Dickow: *Außenpolitik der Dienste - Die strategische Kommunikationsüberwachung und ihre Folgen*, SWP-Aktuell, Februar 2015, http://www.swp-berlin.org/fileadmin/contents/products/aktuell/2015A18_dkw.pdf.

Marcel Dickow und Oliver Meier: *Raus aus der Deckung! Rüstungskontrolle als Fundament einer modernen Ordnungspolitik*, Januar 2016, in Volker Perthes:
Ausblick 2016: Begriffe und Realitäten internationaler Politik, http://www.swp-berlin.org/fileadmin/contents/products/sonstiges/Ausblick2016.pdf#page=28.

Annegret Bendiek, Christoph Berlich und Tobias Metzger: *Drei Prioritäten für die Cyberdiplomatie unter dem deutschen OSZE-Vorsitz 2016*, SWP-Kurz-gesagt, November 2015, http://www.swp-berlin.org/publikationen/kurz-gesagt/drei-prioritaeten-fuer-die-cyberdiplomatie-unter-dem-deutschen-osze-vorsitz-2016.html.