Stellungnahme von Dr. Sven Herpig[1], Leiter für Internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung, für die öffentliche Anhörung des Verteidigungsausschusses am 14. Dezember 2020 zum Thema "Verfassungs- und völkerrechtliche Fragen im militärischen Cyber- und Informationsraum unter besonderer Berücksichtigung des Parlamentsvorbehaltes, der Zurechenbarkeit von Cyberangriffen sowie einer möglichen Anpassung nationaler und internationaler Normen".

Deutscher Bundestag
Verteidigungsausschuss

Ausschussdrucksache
19(12)939
04.12.2020 - 19/3486
5410

Die vorliegende Stellungnahme bezieht sich vor allem auf die Bereiche des Fragenkatalogs, die sich nicht mit völkerrechtlichen Aspekten oder Fragen des "Informationsraums" auseinandersetzen.

Der Sachverständige bedankt sich bei Dr. Matthias Schulze[2] für die wertvolle Grundlagenarbeit in diesem Bereich.

Kontakt

Dr. Sven Herpig
sherpig@stiftung-nv.de
@z_edian (Twitter)
Leiter für Internationale Cybersicherheitspolitik
Stiftung Neue Verantwortung

[1] Stiftung Neue Verantwortung (2020): Experten-Profil von Dr. Sven Herpig
[2] Stiftung Wissenschaft und Politik (2020): Experten-Profil von Dr. Matthias Schulze

1. Die Rolle der Bundeswehr in der deutschen Cybersicherheitsarchitektur

Der erste Grundstein für die deutsche Cybersicherheitsarchitektur wurde bereits 1986 gelegt. In diesem Jahr wurde in der Vorgängerorganisation des Bundesamts für Sicherheit in der Informationstechnik (BSI), der Zentralstelle für das Chiffrierwesen (ZfCh), „[...] eine Arbeitsgruppe aufgebaut, die sich vor dem Hintergrund der schnellen Entwicklung der IuK-Technik mit den Sicherheitsfragen beschäftigte“[3]. Am 1. Januar 1991 nahm das Bundesamt für Sicherheit in der Informationstechnik nach Ausgründung aus dem Bundesnachrichtendienst (BND) seine Arbeit auf. In den öffentlichen Fokus geriet die Cybersicherheitsarchitektur dann insbesondere im Jahr 2011 durch die Veröffentlichung der Cyber-Sicherheitsstrategie für Deutschland.[4] Seitdem hat sich einiges getan. Zum Einen wurde die Architektur um viele neue Akteure – wie zum Beispiel das Kommando Cyber- und Informationsraum der Bundeswehr – ergänzt.[5] Zum Anderen ist Cybersicherheitspolitik ein elementarer Bestandteil der deutschen Innen-, Außen- und Sicherheitspolitik geworden.

Cybersicherheit wird in Deutschland auf Bundes- und Länderebene seit je her von zivilen Behörden hergestellt.[6] Hierbei laufen alle Fäden beim Bundesamt für Sicherheit in der Informationstechnik zusammen. Diese Nationale Cybersicherheitsbehörde[7] ist unter anderem für den Schutz der Regierungsnetze, die Kooperation mit der Wirtschaft und die Bereitstellung von Informationen für die Gesellschaft verantwortlich. Hinzu kommen das Bundeskriminalamt zur Bekämpfung von Cyberkriminalität und des Bundesamt für Verfassungsschutz zur nachrichtendienstlichen Aufklärung. Auf Länderebene werden diese Funktionen analog übernommen, unter anderem vom Landesamt für Sicherheit in der Informationstechnik, dem Hessen3C, den Landesämtern für Verfassungsschutz und den Landeskriminalämtern. Nachrichtendienstliche Erkenntnisse aus dem Ausland zur Cybersicherheitslage fließen zusätzlich durch den Bundesnachrichtendienst in die Arbeit der Behörden ein.[8] Das Nationale Cyber-Abwehrzentrum – in dem auch das Bundesamt für den Militärischen Abschirmdienst und das Kommando Cyber- und Informationsraum der Bundeswehr vertreten sind – bietet für all diese Erkenntnisse eine Kooperationsplattform.[9]

Die Rolle des Bundeswehr bei der gesamtstaatlichen Sicherheitsvorsorge im Bereich Cybersicherheit im Frieden ist verfassungsrechtlich in der Praxis bisher hauptsächlich auf den Eigenschutz, also defensive Aktivitäten, begrenzt. Auf Basis der Anzahl und Heterogenität der eigenen IT-Systeme ist dies eine sinnvolle Nutzung der vorhandenen Ressourcen zur Steigerung der Resilienz der

[3] Bundesamt für Sicherheit in der Informationstechnik (2003): Jahresbericht 2003
[4] Bundesministerium des Innern (2011): Cyber-Sicherheitsstrategie für Deutschland 2011
[5] Sven Herpig und Rebecca Beigel (2020): Deutsche Cybersicherheits- und Cyberverteidigungspolitik: Staatliche Akteure und Zuständigkeiten
[6] Sven Herpig und Rebecca Beigel (2020): Deutsche Cybersicherheits- und Cyberverteidigungspolitik: Staatliche Akteure und Zuständigkeiten
[7] Offiziell “Cybersicherheitsbehörde des Bundes”, vgl.: Sven Herpig (2020): Die „Unabhängigkeit“ des Bundesamtes für Sicherheit in der Informationstechnik
[8] Bundesnachrichtendienst (2020): Cybersicherheit
[9] Bundeskriminalamt (2020): Nationales Cyber-Abwehrzentrum

Bundeswehr-IT, vor allem wenn zukünftig vermehrt auf den Einsatz von Maschinellem Lernen gesetzt werden soll.[10] Zukünftig könnte die Möglichkeit der Amtshilfe gem. § 35 GG durch die Bundeswehr bei schweren Cybervorfällen noch weiter beleuchtet werden, zum Beispiel durch konkrete Einsatzszenarios. In bisheriger Ermangelung eines zivilen Katastrophenschutzes für den Cyberraum[11], könnte die Bundeswehr möglicherweise öffentliche Einrichtungen wie Universitäten bei der Wiederherstellung ihrer Systeme nach einem "Großschadensfall" – z. B. einem Ransomware-Angriff – unterstützen.

2. Die Grenze von Defensiv und Offensiv im Cyberraum

Die Grenze zwischen defensiv und offensiv wird im Cyberraum in der Regel dann überschritten, wenn die getätigten Maßnahmen nicht mehr die eigenen Systeme, sondern Systeme von Dritten und / oder Systeme des intendierten Ziels betreffen (vgl. Abbildung 1).

Innerhalb offensiver Maßnahmen wäre eine trennscharfe Grenze zwischen Informationsgewinnung – im Sinne einer technischen Sondierung ohne intrusive Maßnahmen – und Aufklärung/ Wirkung dann erreicht, wenn die IT-Schutzziele[12] – Vertraulichkeit, Integrität und Verfügbarkeit – der Zielsysteme beeinträchtigt werden.[13] Solange sie nicht beeinträchtigt werden, zum Beispiel durch Aktivitäten wie Portscans, sind die Maßnahmen nicht intrusiv und es kann von Informationsgewinnung gesprochen werden.[14] Dies kann auch der Fall sein, wenn zwar das Schutzziel Vertraulichkeit verletzt wird, aber das Zielsystem über keinerlei Sicherheitsfunktionen verfügt, die umgangen werden müssen, z. B. bei falsch konfigurierten Cloudstorage-Systemen.[15] Es handelt sich hierbei aufgrund der bereits genannten Herausforderungen seitens des Ziels – Informationsgewinnung (nicht intrusiv) von Aufklärung und Wirkung (beides intrusiv) zu unterscheiden – um eine bewusst konservative Auslegung von Informationsgewinnung.

Informationsgewinnung dient zur Identifikation von möglichen Zielsystemen (Bürosysteme aber auch Wehrtechnik) und ihren Schwachstellen. Das daraus resultierende Wissen bildet die Grundlage, um eigene intrusive offensive Maßnahmen vorzubereiten. Hierfür müssen zum Beispiel Exploits

[10] Sven Herpig (2019): Securing Artificial Intelligence und Sven Herpig (2020): Understanding the Security Implications of the Machine-Learning Supply Chain
[11] Wie ein ziviler Katastrophenschutz für den Cyberraum aussehen kann, wie z. B. hier skizziert: AG KRITIS (2020): Das Cyber-Hilfswerk
[12] Bundesamt für Sicherheit in der Informationstechnik (2020): IT-Grundschutz Kompendium
[13] Oft wird in der Unterscheidung zwischen Maßnahmen der Informationsgewinnung und der Aufklärung angeführt, dass Informationsgewinnung passiv ist, während Aufklärung aktiv ist. Jedoch ist zum Beispiel ein Portscan, eine Maßnahme der Informationsgewinnung, durchaus eine vorsätzliche Aktivität. Eine wirklich passive Maßnahme zur Informationsgewinnung wäre im Gegensatz hierzu ein Honeypot, der vom Gegner ausgelöst wird und damit ausschließlich reagiert. Aus diesem Grund wird hier die Unterscheidung zwischen nicht-intrusiv/intrusive und defensiv/offensiv gewählt.
[14] Matthias Schulze (2020): Militärische Cyberoperationen. Nutzen, Limitierungen und Lehren für Deutschland
[15] Vgl. z. B. UpGuard Team (2017): Black Box, Red Disk: How Top Secret NSA and Army Data Leaked Online

entwickelt oder beschafft und in Offensivwerkzeuge und -plattformen integriert werden. Darüber hinaus gilt es auch, detaillierte Einsatzgrundsätze zu formulieren, die, wie die Wahl der Offensivwerkzeuge und -plattformen, von den Informationen aus der Informationsgewinnung profitieren[16]. Auf Basis dieser Definition sollte Informationsgewinnung nicht notwendigerweise dem Parlamentsvorbehalt unterliegen.

3. Cyberverteidigung durch die Bundeswehr

Über die Aufgaben beim Eigenschutz, der Amtshilfe und der Informationsgewinnung hinaus besitzt die Bundeswehr aber auch intrusive offensive Cyberfähigkeiten. Diese können im Spannungs-, und Verteidigungsfall, also im Rahmen der Landes- und Bündnisverteidigung, sowie bei (robusten) Auslandsmandaten zum Einsatz kommen.[17] Sie unterliegen dabei denselben Beschränkungen wie die Fähigkeiten in anderen Domänen. Der Rolle von IT-Systemen Dritter, vor allem von Drittstaaten und deren Interdependenzen, wird allerdings noch zu wenig Beachtung geschenkt. Weiterhin sollte auch beim Mandats-, Spannungs-, und Verteidigungsfall die Aufmerksamkeit der Bundeswehr im Cyberraum auf dem Eigenschutz und der Amtshilfe gerichtet sein. Behörden im Ressort des Bundesministeriums des Innern, für Bau und Heimat – wie das Bundesamt für Sicherheit in der Informationstechnik – sollten ihrer ursprünglichen Aufgabe zur Erhaltung der Cybersicherheit in Deutschland nachkommen.

Für die Ausweitung der Befugnisse zum Einsatz offensiver intrusiver Cyberfähigkeiten der Bundeswehr außerhalb von Mandats-, Spannungs-, und Verteidigungsfall werden vor allem zwei Aspekte ins Feld geführt: Aktive Cyberabwehr und Aufklärung.

Aktive Cyberabwehr, die im verteidigungspolitischen Bereich auch als “digitaler Verteidigungsfall” traurige Berühmtheit erlangte, wirft noch einige Fragen auf.[18] Wann genau dieser aktiviert werden soll, ist im Kontext hybrider Bedrohungen, sowie der geringen Trennschärfe von Cyberkriminalität, aktiven Maßnahmen (Desinformation) und Aufklärung/ Wirkung fremder Staaten bisher weitestgehend unklar.[19] Expert:innen sind sich darüber hinaus nahezu gänzlich einig, dass die Durchführung von offensiven Maßnahmen im Cyberraum nicht dazu geeignet ist, anhaltende und laufende Cyberoperationen abzuschrecken[20] oder gar abzuwehren[21]. Hinzu kommt, dass die aktuellen gesetzlichen Regelungen hier die Zuständigkeit für Gefahrenabwehr auf Länderebene sehen. Eine Änderung dieser Regelungen hat vor dem Hintergrund fehlender Effektivität und weiteren Herausforderungen wie fristgerechter Zurechnung (Attribution), vor allem in zeitkritischen Situationen, keinen Sinn. Die Zurechnung von gegnerischen offensiven intrusiven Maßnahmen ist in der Regel ein

[16] Jack Rhysider (2020): Darknet Diaries - Ep 50: Operation Glowing Symphony
[17] Matthias Schulze (2020): German military cyber operations are in a legal gray zone
[18] Sven Herpig (2018): Aktive Cyber-Abwehr / Hackback
[19] Matthias Schulze (2020): German military cyber operations are in a legal gray zone
[20] Matthias Schulze (2019): Überschätzte Cyber-Abschreckung
[21] Sven Herpig et al. (2020): Aktive Cyberabwehr/ Hackback in Deutschland – Leseliste 2017-2020 –

langwieriger, komplexer Prozess (lies: Wochen oder Monate statt Stunden oder Tage), der vor allem technische, aber auch nachrichtendienstliche und politische Erkenntnisse umfasst.

Die Aufklärung ähnelt in Ziel und Funktion der Informationsgewinnung, ist jedoch im Gegensatz zu ihr intrusiv. Das heißt es werden hierbei die IT-Schutzziele der Zielsysteme verletzt. Hierdurch können zusätzliche Informationen erworben werden, die für die Vorbereitung im Rahmen von Wirkungsmaßnahmen genutzt werden können. Weiterhin können Veränderungen in den Zielsystemen (z. B. unautorisierter Einbau von “Hintertüren”) vorgenommen werden, damit in einem späteren Bedarfsfall zeitnah gehandelt werden kann. Die Herausforderung hierbei ist, dass bei intrusiven offensiven Maßnahmen das Ziel kaum zwischen Aufklärung und Wirkung unterscheiden kann.[22] Offensive intrusive Maßnahmen der Bundeswehr im Cyberraum benötigen daher einen Mandats-, Spannungs-, Verteidigungs- und Bündnisfall als Rechtsgrundlage, auch wenn das einen gewissen Vorlauf zur Durchführung offensiver Maßnahmen benötigt. Nur so kann eine unabsichtliche Eskalation verhindert und internationales Recht (z. B. Artikel 2 Absatz 4 und Artikel 51, Charta der Vereinten Nationen)[23] geachtet werden.

<table>
<tr><th colspan="2">Defensiv</th><th colspan="3">Offensiv</th></tr>
<tr><th colspan="3">Nicht-Intrusiv</th><th colspan="2">Intrusiv</th></tr>
<tr><td>Eigenschutz</td><td>Amtshilfe</td><td>Informationsgewinnung</td><td>Aufklärung</td><td>Wirkung</td></tr>
</table>

Abbildung 1: Maßnahmen der Bundeswehr im Cyberraum (nicht abschließend)

4. Zurechnung (Attribution) von Aufklärungs- und Wirkungsmaßnahmen

Die Zurechnung von Aufklärungs- und Wirkungsmaßnahmen ist relevant für die Lagebilderstellung und mittel- bis langfristige strategisch-politische Beantwortung von Cyberaktivitäten. Diese können auch die öffentliche Zuschreibung (engl. ebenfalls Attribution) eines Vorfalls zu seinen Urheber:innen umfassen. Aktuell gibt es jedoch noch eine Vielzahl an ungelösten Herausforderungen bei der strategischen Beantwortung von Cyberaktivitäten in der deutschen Cybersicherheitspolitik., wie z. B. ein fragmentiertes Zurechnungsberichtswesen.[24]

[22] Bruce Schneier (2014): Computer Network Exploitation vs. Computer Network Attack
[23] United Nations Regional Information Centre for Western Europe (1973): Charta der Vereinten Nationen und Statut des Internationalen Gerichtshofs
[24] Seit November 2020 arbeitet die Stiftung Neue Verantwortung an einem Projekt, welches den strategischen Rahmen, aktuelle Herausforderungen und mögliche Lösungsvorschläge zur Beantwortung von maliziösen Cyberaktivitäten identifizieren wird. Die Studie wird voraussichtlich im 2. Quartal 2021 erscheinen.

5. Voraussetzung für den Einsatz offensiver intrusiver Cyberfähigkeiten durch die Bundeswehr

Grundlagen für Aufklärungs- und Wirkungsmaßnahmen sind die Kenntnis von Schwachstellen und Exploits, sowie Offensivwerkzeuge und -Plattformen. Die Beschaffung dieser Mittel muss genauer betrachtet werden. Beim Einsatz von Offensivwerkzeugen und -Plattformen sollten ethische Grundsätze berücksichtigt werden, da die entsprechenden Hersteller immer öfter mit suspekten Geschäftspraktiken[25] und daraus resultierenden Menschenrechtsverletztungen bis hin zur gezielten Tötung[26] in Verbindung gebracht werden. Aus Ermangelung eines nationalen staatlichen Schwachstellenmanagementmodells[27] sollte die Bundeswehr ausschließlich Exploits verwenden, die auf bereits bekannten Schwachstellen beruhen.[28] Es fehlt bisher an der behördenübergreifenden Analysefähigkeit, ob die Zurückhaltung einer spezifischen unbekannten Schwachstelle Deutschland mehr schadet (u.a. durch Kollateralschäden) als nutzt. Damit dies für die Bundeswehr und andere Akteure wie Nachrichtendienste ressortübergreifend sichergestellt werden kann, sollte von allen beteiligten Ressorts das Vorhaben des Bundesministeriums des Innern, für Bau und Heimat, ein staatliches Schwachstellenmanagement aufzubauen, aktiv unterstützt werden. Als Grundlage hierzu kann das SNV-Modell[29] dienen.

6. Schlussbemerkung

Während es im Rahmen von (robusten) Auslandsmandaten und – was hoffentlich nicht vorkommen wird – im Verteidigungs-, Spannungs- oder Bündnisfall durchaus Anwendungsfelder für den Einsatz offensiver intrusiver Cyberfähigkeiten geben kann, so müssen die rechtlichen, technischen und politischen Rahmenbedingungen von der Beschaffung bis zur Einbettung der Missionen in eine gesamtstaatliche Strategie detailliert und transparent ausgearbeitet werden.

Es ist jedoch wichtig anzuerkennen, dass die bisherige und aktuelle Cybergefährdungslage in Deutschland fast ausschließlich von organisierter Kriminalität und Nachrichtendiensten geprägt ist. Um diesen Aktivitäten entgegenzuwirken, muss die Bundesregierung gesamtstaatlich IT-Sicherheit und Resilienz fördern. Da der Bundeswehr als Teil dieses Ansatzes vor allem die Rolle des Eigenschutzes und ggf. der Amtshilfe zukommt sollte hier auch der politische und organisatorische Fokus liegen und nicht auf der Entwicklung offensiver intrusiver Cyberfähigkeiten. Der Satz: “Offensive ist die beste Defensive” gilt nicht im Cyberraum.

---

[25] Vgl. z.B. ZEIT ONLINE, dpa, msk (2020): Razzia bei Münchner BKA-Trojanerlieferant
[26] Vgl. z.B. David D. Kirkpatrick (2018): Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says
[27] Sven Herpig (2018): Schwachstellen-Management für mehr Sicherheit
[28] Als bekannt wird hier eine Schwachstelle angesehen, wenn sie entweder öffentlich ist, dem Hersteller gemeldet wurde oder dem Bundesamt für Sicherheit in der Informationstechnik mit der Zielsetzung gemeldet wurde, diese dem Hersteller zu melden oder öffentlich vor ihr zu warnen.
[29] Sven Herpig (2018): Schwachstellen-Management für mehr Sicherheit