**Deutscher Bundestag**
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)255 A

Stiftung Neue Verantwortung

# Sachverständigenstellungnahme von Dr. Sven Herpig[1], Leiter für Internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung, für die Sitzung des Bundestagsausschusses für Inneres und Heimat am 08.04.2019 zum Thema "IT-Sicherheit"

Die folgende Stellungnahme bezieht sich vor allem auf die Drucksachen 19/1328 (IT-Sicherheit stärken, Freiheit erhalten, Frieden sichern" vom 21.03.2018), 19/7698 (Antrag "Digitalisierung ernst nehmen - IT-Sicherheit stärken" vom 12.02.2019) und 19/7705 (Antrag "Umsetzung effektiver Maßnahmen für digitale Sicherheit statt Backdoors" vom 13.02.2019) aber auch auf die aktuellen Gesetzes- und Policy-Entwicklungen der Bundesregierung, wie dem IT-Sicherheitsgesetz 2.0, dem Gesetz zur Harmonisierung des Verfassungsschutzrechts, dem nationalen Schwachstellenmanagement, der Aktiven Cyberabwehr, einer Umorganisation des Cyber-Abwehrzentrums und der Unabhängigkeit des Bundesamts für Sicherheit in der Informationstechnik.

[1] SNV-Profil: Dr. Sven Herpig
Sachverständigenstellungnahme für den Bundestagsausschuss für Inneres und Heimat am 08.04.2019 von Dr. Sven Herpig, SNV.

Die zukünftige Cybersicherheitspolitik in Deutschland sollte auf folgenden Kernaspekten basieren, um ein gleichermaßen hohes Maß an Freiheit wie auch an IT-Sicherheit gewährleisten zu können:

1. Strategische Planung und Umbau der nationalen Cybersicherheitsarchitektur[2] um Redundanzen und Friktionen zu vermeiden sowie um ein hohes Maß an Sicherheit durch Prävention, Detektion, Reaktion und Repression herzustellen. Hierbei sollte unbedingt die strikte Trennung zwischen zivilem und militärischem Bereich sowie von Nachrichtendiensten und Strafverfolgern beachtet und eine stärkere Unabhängigkeit des Bundesamts für Sicherheit in der Informationstechnik von Bundesministerium des Innern, für Bau und Heimat geprüft werden.

2. Erhöhen der Resilienz des nationalen IT-Ökosystems mit Fokus auf den Umgang mit Schwachstellen in Hardware, Software und Online-Dienstleistungen (u.a. IT-Sicherheitskennzeichen, Patch-Bereitstellung, Zwei-Faktor-Authentisierung[3] und Einführen eines nationalen Schwachstellenmanagements[4]).

3. Erhöhung der Schutzmaßnahmen[5] von Individuen und Institutionen gegenüber invasiver staatlicher Überwachungsmaßnahmen (u.a. Online-Durchsuchung und Quellen-TKÜ), Überarbeitung entsprechender Kontrollmechanismen[6] und Stärkung der Transparenz über den staatlichen Einsatz solcher Maßnahmen.

4. Erarbeitung einer umfassenden "whole-of-government"-Strategie zum repressiven Umgang mit Cyberoperationen; von der Entwicklung eines gemeinsamen (internationalen) Attributionsverständnisses bis zur Verknüpfung mit entsprechenden (u.a. nachrichtendienstlichen, politischen und wirtschaftlichen) Gegenmaßnahmen im Rahmen internationaler Normen. Hierbei ist ein differenzierter Diskurs zur "Aktiven Cyberabwehr"[7] unerlässlich.

5. Verbesserung der Fachkräfteausbildung und -weiterbildung im Bereich der IT-Sicherheit und innovative Maßnahmen zum (Ein-)Binden entsprechender Fachkräfte im öffentlichen Dienst[8]; auch mit Hinblick auf die Strategieentwicklung Deutschlands.

[2] Sven Herpig und Clara Bredenbrock: Cybersicherheitspolitik in Deutschland. Akteure, Aufgaben und Zuständigkeiten. Im Fokus: Das Cyber-Abwehrzentrum
[3] Jan-Peter Kleinhans: Mehr IoT-Sicherheit in der EU
[4] Sven Herpig: Schwachstellen-Management für mehr Sicherheit
[5] Sven Herpig: A Framework for Government Hacking in Criminal Investigations
[6] Thorsten Wetzling: Stellungnahme zum Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (BND) sowie weiterer Vorlagen
Thorsten Wetzling: Nachrichtendienstkontrolle in Deutschland und Europa jetzt vorantreiben!
[7] Sven Herpig: Hackback ist nicht gleich Hackback
[8] Julia Schuetze: Warum dem Staat IT-Sicherheitsexpert:innen fehlen

Im Einzelnen

Ad 1. Eine Übersicht zur deutschen Cybersicherheitsarchitektur mit Kurzanalyse des Cyber-Abwehrzentrums wurde am 1. April 2019 von der Stiftung Neue Verantwortung veröffentlicht.[9]

Ad 1. Die Digitalisierung als Querschnittsaufgabe erfordert die direkte Zusammenarbeit der für IT-Sicherheit zuständigen Stelle, hier das Bundesamt für Sicherheit in der Informationstechnik (BSI), mit den Bedarfsträger:innen, u.a. Ministerien, Institutionen innerhalb der Bundesländer, der Industrie aber auch Institutionen mit verfassungsrechtlicher Unabhängigkeit. Gleichzeitig wird spätestens seit Verabschiedung der Cybersicherheitsstrategie für Deutschland 2016 eine starke Konvergenz öffentlicher Sicherheit (u.a. auch durch den Einsatz von Hacking-Werkzeugen) und IT-Sicherheit vorangetrieben. Um einen singulären Fokus des BSI auf IT-Sicherheit zu wahren und eine entsprechende vertrauenswürdige und effektive Zusammenarbeit mit anderen staatlichen und nicht-staatlichen Stellen zu gewährleisten, sollten verschiedene Modelle der Unabhängigkeit des BSI vom Bundesministerium des Innern, für Bau und Heimat (BMI) geprüft werden. Hierbei steht vor allem die Frage der Fachaufsicht im Vordergrund. Modelle die als Vorbild dienen könnten wären u.a. der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) oder das statistische Bundesamt. Grundkonsens muss hierbei sein, dass die Behörde nicht aufgeteilt wird, da die bestehenden Synergien elementar zu ihrer Funktionsfähigkeit beitragen.

Ad 1. Die seit Jahren diskutierte Umorganisation der Cyber-Abwehrzentrums (Cyber-AZ) sollte umgehend umgesetzt werden. Hierbei ist es wichtig, dass zusätzlich zu den bestehenden Verwaltungsvereinbarungen der im Cyber-AZ vertretenen Behörden eine Rechtsgrundlage über die Zusammenarbeit geschaffen wird. Dort muss u.a. geregelt sein, welche Kommunikationspflichten den einzelnen Behörden gegenüber dem Cyber-AZ zukommen sollen. Weiterhin ist eine Einbindung der Länder erforderlich. Eine institutionelle Anbindung des Cyber-AZ beim BSI ist u.a. aufgrund der dort existierenden technischen Fachkenntnisse und artverwandten Strukturen (CERT-Bund, Nationalem IT-Lagezentrum, Lagezentrum und IT-Krisenreaktionszentrum) unerlässlich. Eine Angliederung an den militärischen Bereich (z. B. an die Bundeswehr) wäre kontraproduktiv, genauso wie eine Aufweichung des Trennungsgebots zwischen Nachrichtendiensten und Strafverfolgern.

Ad 1. Die immer komplexer werdende Cybersicherheitsarchitektur in Deutschland braucht einen "Masterplan". Während ein gewisses natürliches Wachstum der Behörden und Strukturen in den ersten Jahren der deutschen Cybersicherheitspolitik verständlich ist, ist es – auch aufgrund der begrenzten Ressourcen wie IT-Fachkräften – notwendig, einen kohärenten Plan vorzulegen, wie z.B. der Nationale Pakt für Cybersicherheit (s. Koalitionsvertrag[10]) oder das Deutsche Institut für Internationale Cyber-Sicherheit (s. Cyber-Sicherheitsstrategie

[9] Sven Herpig und Clara Bredenbrock: Cybersicherheitspolitik in Deutschland. Akteure, Aufgaben und Zuständigkeiten. Im Fokus: Das Cyber-Abwehrzentrum

[10] Bundesregierung: Koalitionsvertrag zwischen CDU, CSU und SPD

für Deutschland 2016[11]) eingebunden werden sollen. Nur so kann dem Aufbau von Parallelstrukturen entgegengewirkt und die vorhandenen Ressourcen effizient genutzt werden. Dies beinhaltet auch klare Zuständigkeiten, Kooperation und Kommunikation von Bundes- und Landesebene (s. Gründung des Landesamts für Sicherheit in der Informationstechnik in Bayern). Eine Militarisierung des Bereichs Cybersicherheit in Deutschland – u.a. durch geographische Angliederung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) an das Forschungsinstitut Cyber Defense (CODE) oder das gemeinsame Betreiben der Agentur für Innovation in der Cybersicherheit – sollte strikt vermieden werden. Seit 1991 ist Cybersicherheit in Deutschland eine zivile Domäne, die militärische Aufgabe im Cyberraum muss daher auf den Schutz der eigenen Systeme und mandatierte Einsätze von Cyber-Wirkmitteln begrenzt bleiben. Für Cybersicherheit in Deutschland hat weiterhin das Primat des Zivilen in den zivil-militärischen Beziehungen zu gelten.

Ad 2. Ein:e hochranginge:r Vertreter:in des zuständigen BMI bezeichnete Schwachstellen 2018 als "die Seuche der modernen IT". Nur wenn diesem Zustand entschieden entgegengewirkt werden kann, kann die IT-Sicherheit in Deutschland signifikant erhöht werden. Dem Bereich der "bekannten" Schwachstellen, die in weit mehr als 90% der Exploits zum Einsatz kommen[12], gilt es daher, besondere Aufmerksamkeit zu widmen. Dies geht über Schwachstellen in Computern und Smartphones hinaus und betrifft den gesamten Sektor des Internets-der-Dinge (u.a. Smart Home und Connected Cars). Die Marktüberwachung und Verbraucherschutzbehörden müssen ertüchtigt werden, um überhaupt IT-Sicherheit einfordern und Produkte/Unternehmen überprüfen zu können. Eine Kennzeichnungspflicht allein schafft nicht unmittelbar mehr IT-Sicherheit. Standardisierung, Zertifizierung und Marktüberwachung müssen immer gemeinsam betrachtet werden[13], da sie voneinander abhängen.

Im Bereich der "unbekannten" Schwachstellen sollte die Bundesregierung „Bug Bounty“-Projekte für Programme (z.B. EU-Fossa[14]) unterstützen[15] und ein rechtlich verankertes, behördenübergreifendes und transparentes Schwachstellenmanagementmodell einführen. Ein Referenzmodell wurde durch die Zusammenarbeit von internationalen Expert:innen erstellt, im August 2018 von der Stiftung Neue Verantwortung veröffentlicht und dem Bundesministerium des Innern, für Bau und Heimat vorgestellt.[16] Um diese Puzzleteile zusammenzuführen, wäre es ggf. hilfreich, ein umfassendes nationales Konzept zur Verringerung von Schwachstellen mit konkreten Maßnahmen zu erarbeiten und dann zu implementieren.

[11] Bundesministerium des Innern: Cyber-Sicherheitsstrategie für Deutschland 2016
[12] Sven Herpig: Schwachstellen-Management für mehr Sicherheit
[13] Jan-Peter Kleinhans: Standardisierung und Zertifizierung zur Stärkung der internationalen IT-Sicherheit
[14] Sebastian Grüner: EU erweitert Bug-Bounty-Programm für Open-Source-Software
[15] Fraktion der FDP im Bundestag: Digitalisierung ernst nehmen - IT-Sicherheit stärken
[16] Sven Herpig: Schwachstellen-Management für mehr Sicherheit

Ad 2. Zwei weitere Grundvoraussetzungen um die IT-Sicherheit in Deutschland nachhaltig zu erhöhen, sind die Bekräftigung und Förderung der Maßnahmen aus den Eckpunkten der Kryptopolitik 1999 und das Vorantreiben und die Förderung von Multifaktorauthentifizierung bei Dienstleistungen wie E-Mails und sozialen Medien.

Ad 3. Im aktuellen Referentenentwurf zum "Gesetz zur Harmonisierung des Verfassungsschutzrechts" werden die Befugnisse zum Eingriff in informationstechnische Systeme durch das Bundesamt für Verfassungsschutz und den Bundesnachrichtendienst ausgeweitet, ohne ihnen entsprechende Schutz- und Kontrollmaßnahmen für Individuen und Institutionen entgegenzustellen. Dies folgt der Ausweitung entsprechender Befugnisse und Aufgaben des BKA aus 2017. Die vom Bundesverfassungsgericht angemahnte Gesamtschau der Überwachung[17] ist hier dringend geboten. Die Gesamtschau müsste Kontrolleur:innen zum Zeitpunkt der Erfordernis- und Zulässigkeitsprüfung auch in praktischer Weise zur Verfügung stehen. Auch wenn einer bedarfs- und lagenangepassten Ausweitung der Aufgaben und Befugnisse im Allgemeinen (!) nichts entgegensteht, so ist ein weiterer staatlicher Ausbau von invasiven Eingriffen in informationstechnische Systeme ohne empirische Evidenz des Bedarfs und Identifikation weißer Flecken bei der Arbeit von Nachrichtendiensten und Strafverfolgern höchst problematisch. Hierbei gilt es, auch vergangene Operationen von Strafverfolgern und Nachrichtendiensten (z.B. NSU, Anis Amri) von unabhängiger Stelle daraufhin zu analysieren, ob das Fehlen aktuell geforderter Befugnisse ausschlaggebend für den Verlauf der Ermittlungen war. Die Bundesregierung versprach im Koalitionsvertrag bereits die "gleichzeitige und entsprechende Ausweitung der parlamentarischen Kontrolle" bei Ausweitung der Befugnisse der Sicherheitsbehörden[18]. Mögliche technische und rechtliche Schutzmaßnahmen gegen Quellen-TKÜ und Online-Durchsuchung (Oktober 2018)[19] sowie Beispiele für gute Rechtsnormen und innovative Kontrollpraxis/-instrumente gegen nachrichtendienstliche Überwachung (März 2019)[20] wurden von der Stiftung Neue Verantwortung erarbeitet.

Ad 4. Der Bundesregierung fehlt aktuell eine kohärente und umfassende Strategie, wie politisch auf Cyberoperationen zu reagieren ist. Eine solche Strategie muss u. a. gemeinsame, international harmonisierte Attributionsstandards, eine kohärente Kommunikationsstrategie und ein allgemeingültiges Verständnis von "Aktiver Cyberabwehr" (bekannt auch als "Hackbacks") enthalten. Schwerwiegender ist jedoch das Fehlen eines "whole-of-government"-Ansatzes von der IT-Sicherheitstrinität (Prävention, Detektion, Reaktion) über Attribution und ggf. aktive Cyber-Abwehr bis hin zur Verknüpfung mit unterschiedlichen politischen Reaktionen inkl. nachrichtendienstlicher Gegenmaßnahmen, wirtschaftlichen oder finanziellen Sanktionen, politischen Sanktionen uvm. Das eine solche Strategie fehlt, ist auch in der Zusammenarbeit mit Partnern (gemeinsame

[17] Fraktion der SPD im Bundestag: Positionspapier der AG Inneres und der AG Digitale Agenda
[18] Bundesregierung: Koalitionsvertrag zwischen CDU, CSU und SPD
[19] Sven Herpig: A Framework for Government Hacking in Criminal Investigations
[20] Thorsten Wetzling und Kilian Vieth: Massenüberwachung bändigen. Gute Rechtsnormen und innovative Kontrollpraxis im internationalen Vergleich

Attribution oder Implementierung von gemeinsamen Maßnahmen im Rahmen der Cyber Diplomacy Toolbox/ eines Sanktionsregimes) hinderlich.

Ad 4. Aktive Cyber-Abwehr ist ein Überbegriff verschiedener Maßnahmen, die politisch, rechtlich und technisch äußerst unterschiedlich zu bewerten sind. Äußerst problematisch sind hierbei unter anderem Eingriffe in informationstechnische Systeme in Deutschland. Einen Überblick über entsprechende Maßnahmen hat die Stiftung Neue Verantwortung im Juli 2018 vorgelegt.[21] Einige Maßnahmen nach dieser Definition sind bereits legitimiert (z.B. "Walled Garden"-Maßnahmen für Internet Service Provider durch das IT-Sicherheitsgesetz 2015), andere sollen gerade durch die Harmonisierung des Verfassungsschutzgesetzes (Einsatz von Hacking-Werkzeugen zur Attribution) und durch das IT-Sicherheitsgesetz 2.0 (u.a. Anweisungsbefugnis gegenüber Providern zur Datenlöschung oder Datenumleitung) eingeführt werden. Das Fehlen einer nuancierten (öffentlichen) Debatte zu den verschiedenen Maßnahmen inklusive Bestandsaufnahme sowie das Fehlen einer Einbettung in die nicht-vorhandene deutsche Strategie zum politischen Umgang mit Cyberoperationen (s. vorheriger Absatz) kann und wird zu Problemen in unbekanntem Ausmaß führen. Welche Rolle der Bundeswehr im Rahmen der Cyberabwehr zukommt, ist nicht abschließend geklärt. Auch ist es beim aktuellen Vorgehen unmöglich hervorzusehen, ob die wenigen Ressourcen, die in Deutschland vorhanden sind (IT-Fachkräftemangel) aktuell effizient investiert werden.

Ad 5. IT-Fachkräfte sind die wichtigsten Ressourcen, um IT in Deutschland abzusichern. Ihre Ausbildung, Weiterbildung und effizienter Einsatz sind neben den genannten technischen und politischen Rahmenbedingungen die Grundvoraussetzung für mehr IT-Sicherheit. Gleichzeitig übernimmt der Staat vermehrt Aufgaben im Bereich staatliche IT-Sicherheitsvorsorge. Ideen diesbezüglich hat die Stiftung Neue Verantwortung im Februar 2018 vorgelegt[22].

Ad 5. Im Hinblick auf den effizienten Einsatz der vorhandenen Fachkräfte wäre es daher notwendig, die Cyber-Sicherheitsstrategien aus den Jahren 2011 und 2016 zu evaluieren. Es gibt keine Erkenntnisse, ob diese Strategien erfolgreich waren oder nicht. Dies ist aber auch eine Grundvoraussetzung für die Verabschiedung weiterer politischer und legislativer Maßnahmen im Bereich der IT-Sicherheit in Deutschland.

[21] Sven Herpig: Hackback ist nicht gleich Hackback
[22] Julia Schuetze: Warum dem Staat IT-Sicherheitsexpert:innen fehlen

Fazit

Zusammenfassend muss gesagt werden, dass in der deutschen Cybersicherheitspolitik gleichzeitig eine gewisse Strategieunfähigkeit (u. a. politischer Umgang mit Cyberoperationen, Entwicklung der Cybersicherheitsarchitektur), ein Fehlen empirischer Evidenz (u. a. Evaluation der Cybersicherheitsstrategien, Gesamtschau der Überwachung), eine Vernachlässigung der notwendigen Anpassung von Schutz- und Kontrollmaßnahmen (u. a. gegenüber Quellen-TKÜ und Online-Durchsuchung) und ein Mangel an Ressourcen (Fachkräfte) vorliegen.

Staatliche Aufgaben und Befugnissen getreu dem Motto "besser haben als brauchen" zu erweitern, ist höchst problematisch und führt zusammen mit den vorher genannten Herausforderungen zu falschen Prioritäten und ggf. zu weniger, anstatt mehr IT-Sicherheit; definitiv aber zu einem ineffizientem Einsatz der vorhandenen Ressourcen und einem grundlosen Ausbau repressiver Maßnahmen. Umso schlimmer ist es dann, wenn Befugnisse erweitert werden, ohne die Ressourcen und Instrumente der Kontrolle entsprechend anzupassen.

An dieser Stelle sollte jedoch nicht außer Acht gelassen werden, dass verschiedene politische und rechtliche Maßnahmen, auch im internationalen Vergleich, als positiv zu bewerten sind. Hier zählen u. a. das bisherige Primat des Zivilen bei Cybersicherheit, Aufbau und Rolle des Bundesamts für Sicherheit in der Informationstechnik (inkl. CERT-Bund, Nationalen IT-Lagezentrum und Cyber-Abwehrzentrum), IT-Sicherheitsstandards und Meldepflichten für kritische Infrastrukturen, sehr gut ausgebildete IT-Spezialist:innen sowie eine (begrenzte) öffentliche Debattenkultur und Gesprächsbereitschaft der Verantwortlichen.