FRAKTIONSBESCHLUSS VOM 25.4.2017

» SICHERHEIT IM DIGITALEN

FREIHEIT ERHALTEN, FRIEDEN SICHERN, SCHUTZ WIRKSAM STÄRKEN

Hacking-Angriffe auf den Bundestag, auf Parteien und das Bundeskanzleramt, Attacken auf Unternehmen, auf Kundendatenbanken oder selbst auf vernetzte Geräte in Küche, Kinderzimmer und Krankenhaus: All das macht deutlich, dass die Sicherheit im Digitalen zu einer zentralen Herausforderung unserer Infrastrukturen und Kommunikationssysteme geworden ist. Angesichts dieser vielfachen systemischen Risiken in einer immer vernetzteren Welt besteht ein enormer Handlungsdruck. Scheinbar simple Programmier- und Konfigurationsfehler in Produkten, bei Diensten und Dienstleistungen können weitreichende Folgen für die gesamte Bevölkerung haben. Potenziell jedes System kann von staatlichen wie nichtstaatlichen Akteuren gehackt und zum Ziel von Überwachung, Kriminalität oder militärischen Strategien werden. Die Sicherheit im Digitalen ist somit heute eine wesentliche Bedingung unserer grundrechtlichen Freiheiten, unserer verfassungsrechtlichen Ordnung sowie der völkerrechtlichen Friedensordnung.

Zu oft wird die Debatte um "Cyberwar" und -Sicherheit auf militärische Eskalationsszenarien oder den Schutz kritischer Infrastrukturen verengt, weswegen wir bewusst von der Sicherheit im Digitalen bzw. der IT sprechen. Ein ganzheitlicher Ansatz ist dringend notwendig. Als Grüne im Bundestag setzen wir uns für IT-Sicherheit für alle ein. Dabei orientierten wir uns an der Schutzpflicht des Grundrechts, allen Menschen Vertraulichkeit und die Integrität ihrer informationstechnischen Systeme zu gewährleisten. Es kann nicht nur darum gehen, Wirtschaftsunternehmen zu schützen, die bisher zu den "Kritischen Infrastrukturen" (KRITIS) gezählt werden. Die Verantwortung darf nicht allein auf Nutzerinnen, Nutzer und Unternehmen abgewälzt werden. Dem Staat kommt eine direkt aus unserer Verfassung abzuleitende Schutzverantwortung zu, die weitreichende und effektive Maßnahmen für mehr IT-Sicherheit erfordert.

Die Aktivitäten der Nachrichtendienste und der Bundeswehr im digitalen Raum müssen effektiv und wirksam vom Parlament kontrolliert werden können. Zersplitterte Aufsichtsstrukturen und eine teils willkürliche Unterrichtungspraxis stehen dem heute entgegen. Wir wollen über ein integriertes parlamentarisches Kontrollregime sicherstellen, dass das Parlament umfassend, konsistent und zeitnah unterrichtet wird.

Besonders den Snowden-Enthüllungen ist es zu verdanken, dass endlich eine breitere öffentliche Debatte um die Sicherheit von Informationstechnik und Internet geführt wird. IT-Sicherheit und Datenschutz sind für die Bundesfraktion Bündnis 90/ Die Grünen jedoch seit langem konstitutives Element einer freiheitlichen digitalen Gesellschaft. Gerade der von uns seit Ende der 1990er Jahre geführte Modernisierungsdiskurs zum Datenschutz hat zahlreiche, auch heute noch elementare Lösungsansätze erbracht. Für uns standen und stehen bei der IT-Sicherheit besonders der Erhalt von Freiheit durch Rechtsstaat, Frieden, Demokratie und Bürgerrechte im Vordergrund.

1. IT-SICHERHEIT: DIE BUNDESREGIERUNG KANN UND WILL NICHT

Die Merkel-Regierungen der vergangenen zwölf Jahre haben bei der IT-Sicherheit kläglich versagt. Die Bundesregierung verliert sich nicht nur in einem digitalpolitischen Wetteifern ohne Plan und Koordination, sie tut vor allem so, als habe es die zahlreichen Erkenntnisse aus dem parlamentarischen Untersuchungsausschuss zum geheimdienstlichen Abhör- und Ausspähskandal nie gegeben. Bis heute zieht sie hier nicht die richtigen Konsequenzen, obwohl sie rechtstaatlich dringend

geboten wären. Im Gegenteil: Überwachungsbefugnisse wurden massiv ausgebaut und die parlamentarische Kontrolle erschwert. Die Grundrechte auf Vertraulichkeit und Integrität informationstechnischer Systeme und auf informationelle Selbstbestimmung lässt die Bundesregierung ins Leere laufen und schwächt sie mit fragwürdiger Massenüberwachung sogar noch.

Maßnahmen des Bundesinnenministeriums beschränkten sich allenfalls auf die Sicherheit der Bundesverwaltung. Den Koordinierungsbedarf mit Ländern und Kommunen ließ man lange schleifen. Den Bürgerinnen und Bürger erklärt man, sie seien bei Fragen der IT-Sicherheit im Wesentlichen für sich selbst verantwortlich. Es existiert keine übergreifende Strategie, etwa für staatlich unterstützte Beratungsangebote oder zur Stärkung der Medienkompetenz.

Die Datenschutzgesetze schaffen zwar ein solides Mindestniveau auch an Daten- und IT-Sicherheit, doch sie wurden über Jahre ignoriert, als Bürokratie diffamiert und mit Blick auf die EU-Datenschutzreform zunächst sogar massiv behindert. Stattdessen verfiel der Bundesinnenminister in eine Art aktionistischen Schweinsgalopp bei der IT-Sicherheit: "Strategien" mit kurzer Lebensdauer wie ein Cyberabwehrzentrum, eine neue umstrittene Bundesbehörde ZITIS ("Zentralstelle für Informationstechnik im Sicherheitsbereich") auf unklaren Rechtsgrundlagen und zuletzt gar eine private "Cyberwehr" wirken planlos und wenig koordiniert. Das IT-Sicherheitsgesetz hingegen kam nur auf Druck der europäischen Ebene zustande und greift viel zu kurz. Kaum in Kraft muss es bereits wieder reformiert werden, weil die aktuelle EU-Richtlinie zur IT-Sicherheit (NIS-RiL) viel weiter geht. Auch handwerklich klappt es nicht: An der immens teuren IT-Konsolidierung des Bundes hat der Bundesrechnungshof massiv Kritik geübt

Symptomatisch für Wirrwarr und Widersprüche ist auch die Frage der Verschlüsselung. Die Bundesregierung gab die Parole aus, Deutschland soll "Verschlüsselungsland Nummer 1" werden. Doch die staatliche De-Mail scheiterte. Statt einer Ende-Zu-Ende-Verschlüsselung wurde der Einblick in die Datenverkehre bei den Providern ermöglicht. Zudem kauft und nutzt die Bundesregierung für Überwachungsmaßnahmen weiterhin das Wissen über IT-Sicherheitslücken ("Zero-Day-Exploits") – anstatt diese zu schließen. Vertrauen schafft man so wahrlich nicht. Es bedarf einer echten Kehrtwende in der IT-Sicherheits- und Datenschutzpolitik.

2. GRUNDSÄTZE EINER BÜRGERRECHTSORIENTIERTEN UND VERBRAUCHERFREUNDLICHEN POLITIK DER IT-SICHERHEIT

Wir wollen die Chancen der Digitalisierung nutzen und in Abwägung mit den zugleich entstehenden Risiken sicher gestalten. Es ist eine zentrale Frage der Glaubwürdigkeit, ob es der Bundesrepublik gelingt, den Herausforderungen bürgerrechtsorientiert und rechtsstaatlich zu begegnen. Dem schlechten Vorbild der geheimdienstlichen Massenüberwachung und Militarisierung des Internets nachzueifern, halten wir Grüne im Bundestag für den falschen Weg.

- **IT-Sicherheit differenziert vorantreiben:** Nur vielschichtige Lösungsansätze werden effektiv zu mehr Sicherheit führen. Denn Schutzvorkehrungen für die Informationstechnik und die Infrastruktur, staatliche Maßnahmen gegen IT-Kriminalität, Unterstützung der Bürgerinnen und Bürger beim IT-Selbstschutz, Fragen der staatlichen Überwachung und Strafverfolgung im Internet sowie das militärische Handeln in öffentlichen, zivilen wie nicht-zivilen Netzinfrastrukturen sind ganz unterschiedliche, doch zugleich oftmals zusammenhängende Probleme.
- **Kohärentes und koordiniertes Vorgehen:** Differenziert heißt nicht isoliert. Eine so globale und vielschichtige Problematik erfordert interdisziplinär wie international ein kohärentes, koordiniertes Handeln. Jedoch besteht kein Anlass, darüber die rechtsstaatlich begründete Kompetenzordnung des Grundgesetzes auszuhöhlen. Ebenso wenig dafür, das Trennungsgebot

zwischen Polizei und Geheimdiensten und die gebotene Trennung zwischen Verteidigungs- und Innenpolitik infrage zu stellen.

- **Zeitgemäße Instrumente einsetzen:** Über das Ordnungsrecht allein bewirken staatliche Aufsichtsstrukturen- und Sicherheitsbehörden kaum Wesentliches für die IT-Sicherheit. Denn erstens können bereits einzelne Programmierfehler schwerwiegende Risiken nach sich ziehen, zweitens ist durch die tragende Infrastruktur des Internets ein internationaler Handlungsrahmen vorgegeben und drittens sind die Träger der Infrastruktur private, häufig multinational agierende Unternehmen. Über das Ordnungsrecht hinaus müssen die Instrumente aufgefächert und die beteiligten Akteure einbezogen werden. Überfällig sind freiwillige, aber unabhängige Produkt- und Verfahrens-Zertifizierungen, gezielte Anreize und Vorgaben für ein Privacy by Design und Security by Design über den gesamten Fertigungs- und Lebenszyklus von IT-Produkten und Anwendungen hinweg. Das gilt ebenso für wirksame Sanktionen und grundlegende Verbesserungen des Haftungsregimes.

  Als Grüne im Bundestag wollen wir, dass Bürgerinnen und Bürger die Freiheiten im und mit dem Netz wahrnehmen können – privat wie gegenüber dem Staat. Mehr Transparenz dank digitaler Datenbestände, gestärkte Beteiligung durch Online-Verfahren und nutzerfreundlichere Digitalangebote der öffentlichen Verwaltung: Diese Errungenschaften für die Bürgerinnen und Bürger wollen wir sichern und ausbauen. Hierfür ist Vertrauen in digitale Infrastrukturen und IT-Produkte essenzielle Voraussetzung. Geheimdienstliche Massenüberwachung und staatliche Hacking-Projekte sind hingegen hierfür Gift.

3. BESSERE IT-SICHERHEIT: HANDLUNGSFELDER UND MAßNAHMEN

- **Datenschutz und IT-Sicherheit zusammen denken:** IT-Sicherheit darf aber nicht auf Kosten der Privatheitsrechte gehen. Deshalb bedürfen zahlreiche Zielkonflikte zwischen einer verbesserten IT-Sicherheit einerseits, und der Wahrung der Grundrechte und Freiheit der davon Betroffenen andererseits, einer normenklaren Regelung. So rücken etwa bei einem IT-Zwischenfall sogenannte CERT-Teams von IT-Sicherheitsexperten an und erheben im Einsatz entsprechend Daten. Dies muss auf das erforderliche Mindestmaß beschränkt bleiben. Im Rahmen des IT-Sicherheitsgesetzes konnte immerhin verhindert werden, dass weitere Vorratsdatenspeicherungen bei Unternehmen zum vermeintlich notwendigen Zweck der IT-Sicherheit legalisiert werden. Doch auch die Sicherheitsbehörden und selbst das BSI erlangen im Rahmen von IT-Sicherheitsmaßnahmen gewaltige und zum Teil sehr sensible Informationssammlungen. Als Grüne im Bundestag fordern wir, die Datenschutzbehörden in Fragen der IT-Sicherheit von Beginn an zu beteiligen und dafür mit ausreichenden Mitteln auszustatten.

- **Verschlüsselung von Daten stärken:** Die Snowden-Enthüllungen haben gezeigt, dass so gut wie jede elektronische Kommunikation Angriffsziel für geheimdienstliche Überwachung werden kann. Die Integrität weiter Teile der digitalen Infrastruktur steht heute in Frage. So genannte Ende-zu-Ende-Verschlüsselungen bieten bislang aber ein weitgehend wirksames Mittel gegen unbefugtes Abhören zumindest der Inhalte, auch wenn die so genannten Verkehrsdaten hierbei ungeschützt bleiben. Die Bundesregierung muss endlich erkennen, dass eine gute Kryptografie wesentlich zum Grundrechtsschutz im Digitalen beiträgt. Es braucht eine echte Verschlüsselungsoffensive. Dazu gehört die Förderung von Aufbau, Betrieb und Angebot von echter Ende-zu-Ende-Verschlüsselungen bei allen IT-Großprojekten und mehr Engagement für die Forschung und Entwicklung von Verschlüsselung. Zudem fordern wir neben anderen bereits bestehenden gesetzlichen Vorgaben eine Verpflichtung etwa der Internetzugangsprovider zur sicheren und verbraucherfreundlichen Verschlüsselung der Kommunikation ihrer Kundinnen und Kunden.

- **Keine Hintertüren für Geheimdienste zulasten der Allgemeinheit:** Geheimdienste und Polizei wehren sich gegen wirksame Verschlüsselung und fordern staatliche Hintertüren zu den verschlüsselten Datenverkehren. Der Bundesinnenminister behauptet einerseits, "Sicherheit durch Verschlüsselung" zu verfolgen. Gleichzeitig plant er mit seinem französischen Amtskollegen europaweite Regeln, die die gesicherte Ende-zu-Ende-Verschlüsselung etwa von Messenger-Diensten unterminieren soll. Damit würde die freiheitliche Kommunikation aufgegeben. Als Grüne im Bundestag lehnen wir diese Vorstöße entschieden ab. Auch das staatliche Offenhalten und gezielte Nutzen von so genannten Zero Day-Sicherheitslücken ist rechtsstaatlich nicht vertretbar. Im Gegenteil führt dies zu insgesamt weniger IT-Sicherheit, da bekannte, aber nicht geschlossene Sicherheitslücken immer auch Dritten gegenüber offen stehen und der Schwarzmarkt für solche Angebote nicht auch noch indirekt gefördert werden darf. Der Staat ist hier in einer Schutzpflicht, daher fordern wir weiterhin ein Verbot des staatlichen Offenhaltens und Aufkaufs von Sicherheitslücken. Stattdessen brauchen wir eine Verpflichtung für staatliche Stellen, Lücken nach Bekanntwerden umgehend zu melden und/oder ggf. selbst zu schließen. Zudem reicht bei betroffenen Unternehmen eine passive Meldepflicht von Sicherheitslücken nicht aus. Vielmehr müssen positive und wettbewerbsrelevante Anreize wie Auditierungen für die Wirtschaft mindestens flankierend eingeführt werden.

- **Straftaten konsequent rechtsstaatlich verfolgen:** Auch im Digitalen muss eine konsequente Strafverfolgung stattfinden. Straftaten sind zielgerichtet durch eine materiell und technisch entsprechend ausgestattete Polizei und Justiz zu verfolgen und zu ahnden. Die heutigen Aufklärungsquoten zeigen, dass dies durchaus möglich ist. Die im Digitalen hinterlassenen Spuren bieten Ermittlerinnen und Ermittlern eine Unmenge an Anhaltspunkten für ihre tägliche Arbeit. Jedoch wissen wir um teils erhebliche Defizite bei der Verfolgung einzelner Delikte. Hier stehen alle Verantwortlichen in der Pflicht, diese schnellstmöglich abzustellen. Für den Einsatz von Online-Durchsuchungen und Quellen-Telekommunikationsüberwachung hingegen hat das Bundesverfassungsgericht engste Grenzen gezogen. Tragfähige Rechtsgrundlagen fehlen, weil der Nachweis eines rechtsstaatlich vertretbaren Einsatzes dieser, stets auch die Allgemeinheit gefährdenden Instrumente, weiterhin aussteht. Als Grüne im Bundestag stehen wir einem weiteren Ausbau auch anderweitiger staatlicher Hacking-Befugnisse bzw. der gezielten Ausnutzung von Schwachstellen in IT-Systemen kritisch gegenüber. Hier gelten die hohen Hürden des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme. Und es stellt sich immer die Frage der Verhältnismäßigkeit. Angesichts des potenziellen Schadens für die IT-Sicherheit und den Datenschutz anderer Nutzerinnen und Nutzer verlangen wir die transparente und öffentliche Debatte sowie rechtliche Klarstellungen aller unterschiedlichen Formen des staatlichen Hackings, der gezielten staatlichen Ausnutzung von Schwachstellen in IT-Systemen und deren geplanten und tatsächlichen Einsatz.

- **Massenüberwachung stoppen:** Insbesondere die Geheimdienste haben dem Vertrauen in die Digitalisierung und die freiheitliche Nutzung des Internets massiv geschadet. Ihre Aktivitäten gefährden die IT-Sicherheit durch die Nutzung von Instrumenten, die mit freiheitlichen Gesellschaften unvereinbar sind und grundlegende Standards für die Wahrung der Internetsicherheit und der digitalen Telekommunikation aushöhlen. Was vormals allein chinesischen und russischen Geheimdienste zugeschrieben wurde – gezielte Angriffe auf IT-Infrastrukturen der westlichen Industriestaaten und sogar manipulative Eingriffe in die Meinungsbildung über Plattformen des Internets – muss von nun an auch als Geschäft westlicher Geheimdienste angesehen werden. Leider haben die Snowden-Enthüllungen bis heute zu keiner Abkehr von dieser Praxis der Massenerfassung, Spionage und Sabotage in Informations- und Kommunikationsinfrastrukturen geführt.

Angesichts neuer Bedrohungslagen durch den Terrorismus ist es umso dringender, die bestehenden Möglichkeiten zur zielgerichteten Abwehr zu nutzen, um konkrete Gefährdungen abzuwenden. Stattdessen mussten wir in den vergangenen Jahren eine beispiellose und unfokussierte Aufrüstung staatlicher Überwachungs- und Hackingkapazitäten hinnehmen. Auch bei deutschen Diensten als einem Teil des weltweiten geheimdienstlichen Überwachungssystems. Unter dem Vorwand der Terrorbekämpfung wurde das allgemeine Geschäft der Geheimdienste im Internet sowie anderer IT-Strukturen massiv ausgebaut. Die parlamentarische Kontrolle wurde sabotiert und am Ende aufgeflogene rechtswidrige Praktiken auch noch einfach nachträglich legalisiert.

Wir fordern deshalb die Abkehr vom System der Massenüberwachung. Die Legalisierung der Ausland-Ausland-Überwachung des BND ist verfassungswidrig und muss gestoppt werden, vor allem da weiterhin für Nichtdeutsche kein Grundrechtsschutz des Fernmeldegeheimnisses gelten soll und dem BND die massenhafte Sammlung von Verkehrsdaten erlaubt wird. Auch die Praxis der strategischen Fernmeldeüberwachung im Rahmen des Artikel-10-Gesetzes kann in der gegenwärtigen Form nicht fortgesetzt werden. Unbescholtene Nutzerinnen und Nutzer werden vor allem bei massenhaft überwachten Internet-Verkehren allzu oft "Beifang". Jeder und jede kann heute in die dauerhafte Rasterfahndung der Geheimdienste geraten.

- **Zurechenbarkeit von Angriffen unabhängig bewerten:** Bei der Verfolgung von Straftaten als auch im Rahmen des Umganges mit Überwachung, Spionage und militärischen Aktivitäten ist die Frage der Zurechnung von Angriffen (Attribution) zentral. Viele staatliche wie nichtstaatliche Angreifer betreiben einen hohen Aufwand, um ihre Spuren zu verwischen. Gleichzeitig kann die Zuordnung eines Angriffs zu einem Urheber mit entsprechendem Aufwand auch gefälscht werden. Dementsprechend schwierig gestaltet sich oft die Identifikation und Verfolgung der Taten.

  Die Frage der Attribution lädt dazu ein, Feindbilder zu produzieren und aufrecht zu erhalten, ohne die notwendige Sorgfalt bei der Ermittlung der Täterschaft zu beachten. Auch gezielte Falschmeldungen sind möglich, um öffentliche Meinungen zu steuern und eigene politische Ziele zu verfolgen. Wir schlagen deshalb vor, sowohl national als auch europäisch und international auf die Schaffung von vertrauenswürdigen und unabhängigen Stellen hinzuwirken, die für die Erforschung, Bewertung und den Umgang von und mit IT-Angriffen herangezogen werden können.

4. MILITÄR UND INTERNET/CYBERWAR

Der Einsatz des Internets zu militärischen Zwecken stellt inzwischen eine eigenständige Herausforderung dar. Die in den 1980er Jahren auf UN-Ebene erhobene Forderung, militärische Aktionen in der zivilgesellschaftlichen Infrastruktur des Internets vollständig zu ächten, läuft derzeit ins Leere. Öffentliche Netzwerkinfrastruktur mitsamt der vernetzten Geräte und geschützte staatliche Netze sind längst zum Schauplatz gegenseitiger Angriffe geworden. Insbesondere Russland, China und die USA ringen um die Vorherrschaft. Zu den Zielen und Instrumenten zählen die Beeinflussung politischer Prozesse und die Manipulation von Meinungsdebatten. Ebenso die Spionage und Sabotage gegen zentrale Einrichtungen und die Unterwanderung nationaler kritischer Infrastrukturen samt Installation von Schadsoftware mit potentiell schwersten Folgen für den Fall einer militärischen Konfrontation.

Eine Politik der Abschreckung erscheint in diesem Umfeld angesichts der Zuordnungs- und Abgrenzungsprobleme mehr denn je aussichtslos. Die Bundesregierung muss sich daher auf internationaler Ebene für einen Verhaltenskodex einsetzen, der u.a. eine Selbstverpflichtung enthält, zivile (Netz-)Infrastruktur nicht für militärische Angriffe durch digitale Angriffskapazitäten zu nutzen

oder selbst zum Angriffsziel zu machen. Internationale Regelungen, die es Staaten erlauben unter dem Deckmantel der Cybersicherheit Zensur zu betreiben, lehnen wir als Grüne im Bundestag ab. Entsprechende Vorstöße, "Cyber-" durch "Informationssicherheit" zu ersetzen, wie sie Russland und China ins Spiel bringen, müssen von der Bundesregierung entschieden zurückgewiesen werden.

Zwingend notwendig sind ein verbesserter Eigenschutz und die Härtung der IT-Infrastruktur der Bundeswehr, zum Schutz der eigenen Systeme. Einen Ausbau der Rolle der Bundeswehr beim Schutz der nationalen kritischen Infrastruktur über den bislang bestehenden Rahmen hinaus lehnen wir hingegen ab. Die Federführung für die Sicherheitsvorsorge im IT-Bereich liegt derzeit beim Bundesministerium des Inneren. Ein Erodieren des Verbots eines Einsatzes der Bundeswehr im Inneren über den Umweg der IT-Sicherheit können wir nicht akzeptieren.

Grundlegende Fragen im Zusammenhang mit dem Aufbauen, dem Vorhalten und der potenziellen Anwendung von digitalen Einsatzfähigkeiten im Bereich der Bundeswehr sind bisher unbeantwortet und müssen dringend geklärt werden. Eine klare Definition darüber, was unter einem "Cyber-Angriff" zu verstehen ist, fehlt ebenso wie klare Standards für mögliche Reaktionen. Hier muss die Bundesregierung tätig werden. Zu den offenen Fragen gehört u.a., wann ein solcher Angriff vorliegt, wie auf einen solchen geantwortet werden soll und wovon Umfang und Reichweite der Reaktion abhängig gemacht werden soll. Auch ist unklar, inwiefern mit digitalen Einsatzfähigkeiten auf einen etwaigen bevorstehenden Angriff proaktiv agiert werden könnte. Wie soll bei einer äußerst schwierigen Trennung von privaten und öffentlichen bzw. zivilen und militärischen Netzwerkstrukturen verhindert werden, dass im Rahmen eines bewaffneten Konfliktes zivile Netzwerkinfrastruktur und mithin Bürgerinnen und Bürger Teil eines solchen Konfliktes werden? Die jüngsten, noch sehr unbestimmten Regierungsäußerungen zu digitalen Rückschlagsszenarien haben hier eher zu mehr Fragen und Sorgen denn Klarheit geführt.

Selbstverständlich muss sich auch die Bundeswehr auf neue Bedrohungslagen einstellen und ihre eigene IT-Infrastruktur schützen können. Die Durchführung offensiver Operationen in anderen Netzen lehnen wir jedoch klar ab. Zum einen, weil dabei zentrale zivile Versorgungsinfrastrukturen mit völlig unkontrollierten Konsequenzen für die Bevölkerung des angegriffenen Staates in Mitleidenschaft gezogen werden können. Zum anderen lehnen wir es ab, das Internet und digitale Infrastrukturen als weitere Domäne der Kriegsführung zu etablieren und so auch zivile Netzwerkinfrastruktur weiter zu militarisieren. Diese Risiken gelten auch für vermeintlich niederschwellige, gezieltere Angriffe, etwa im Rahmen des Schutzes von mandatierten Einsätzen der Bundeswehr.

Jeglicher Einsatz von digitalen Einsatzkapazitäten der Bundeswehr muss ebenso wie der Einsatz sonstiger militärischer Kräfte der parlamentarischen Kontrolle des Deutschen Bundestages unterliegen. Grundlage dafür ist das Gesetz über die parlamentarische Beteiligung bei der Entscheidung über den Einsatz bewaffneter Streitkräfte im Ausland (sogenanntes Parlamentsbeteiligungsgesetz). Die parlamentarische Kontrolle des Deutschen Bundestags von Auslandseinsätzen der Bundeswehr halten wir seit Jahren für verbesserungswürdig. So unterliegen die Aktivitäten des Kommandos Spezialkräfte der Geheimhaltung, über die die Bundesregierung nur einzelne Abgeordnete des Verteidigungsausschusses und des Auswärtigen Ausschusses informiert.

Mit dem Aufbau von Kapazitäten zum Vorgehen der Bundeswehr im digitalen Raum droht eine immer weiter zersplitterte Informationspolitik in einem weiteren äußerst sensiblen Bereich. Gerade über Aktivitäten und Operationen im digitalen Raum darf es nicht nur eine punktuelle und selektive Unterrichtung geben. Es braucht eine wirksame parlamentarische Kontrolle aus einer Hand, die ein Gesamtbild über entsprechende Operationen ermöglicht. Die derzeitigen Regelungen und die Akteursvielfalt auf Seiten der Nachrichtendienste und der Behörden sorgen für gravierende Probleme und Lücken bei der Kontrolle.

Viel spricht dafür, dass auch die Bundeswehr mit anderen Partnern massenhaft in ihren Einsatzgebieten überwacht – weitgehend ohne klare Vorgaben und Kontrolle. Als Grüne im Bundestag fordern wir daher eine breite gesellschaftliche Debatte darüber, ob und unter welchen Bedingungen dieses Vorgehen und die damit verbundenen Nachteile für die Zivilbevölkerung der betroffenen Staaten vertretbar sind. Auch bei militärischen Einsätzen im Ausland gelten die einschlägigen grund- und menschenrechtlichen Vorgaben für das Erheben, Verarbeiten und Austauschen dieser sensiblen Daten.

Die Geltung des Völkerrechts im Kontext von IT-Netzen und des Internets wird inzwischen auf allen internationalen Regelungsebenen anerkannt. Wir unterstützen die Bemühungen um vertrauensbildende Maßnahmen im Umfeld von IT-Sicherheit. Das gilt ebenso für weitere konkretisierende Regelungen und Vereinbarungen, die militärische Aktivitäten in Informations- und Kommunikationsinfrastrukturen von Zivilgesellschaften begrenzen.

5. WAS ZU TUN IST – MAßNAHMEN ZUR STÄRKUNG DER IT-SICHERHEIT

- **IT-Sicherheit als grundrechtliche Gewährleistungspflicht wahrnehmen:** Neue Risiken und Bedrohungen für die IT-Sicherheit verpflichten zum Handeln – nicht nur in Hinblick auf die Bundesverwaltung. Gerade die Bürgerinnen und Bürger, aber auch Unternehmen, sind bislang am häufigsten tatsächliche Opfer von schlecht geschützten IT-Systemen, aber auch von gezielten Angriffen. IT-Sicherheit muss sich an der Gewährleistungspflicht des Staates und seiner Verantwortung ausrichten, IT-Systeme in allen zentralen Lebensbereichen verfügbar und zugänglich zu machen. Daneben sind zwingend zentrale Vorgaben des Grundgesetzes, darunter auch das Recht auf die Vertraulichkeit und Integrität informationstechnischer Systeme und der Datenschutz zu gewährleisten. Hierbei handelt es sich keineswegs um Mindestvorgaben oder Untergrenzen.

- **Übergreifende Ressortverantwortlichkeit schaffen:** IT-Sicherheit muss als echte Querschnittsverantwortung aller Arbeitsbereiche der Bundesregierung etabliert werden. IT-Sicherheit und Datenschutz müssen endlich an allerhöchster Stelle mit klaren Verantwortlichkeiten bearbeitet werden. Es muss ein ganzheitlicher Ansatz bei der Umsetzung zentraler Sicherheitsziele in allen Arbeitsbereichen verfolgt und ggf. eingefordert werden können. Insbesondere müssen die notwendigen Veränderungen zur Stärkung der Sicherheit der IT-Infrastrukturen vorangetrieben werden. Anstrengungen in Bereichen, in denen der Bund nicht ohne weiteres Zuständigkeit beanspruchen kann, müssen über die dafür bestehenden Gremien wie den IT-Planungsrat mit Ländern, Kommunen und Wirtschaft koordiniert werden.

- **Die IT-Sicherheit aus dem Innenministerium lösen:** IT-Sicherheit und Datenschutz sind im Innenministerium schlecht aufgehoben. Der Bundesinnenminister agiert für Bürgerinnen und Bürger alles andere als vertrauensbildend. Denn er hält unbeirrt an anlasslosen Massenspeicherungen wie auch am staatlichen Ankauf und Einsatz von Sicherheitslücken und so genannten "Zero Day Exploits" fest, die gefährliche Lücken in Infrastrukturen reproduzieren und mitfinanzieren. Das zeigt die strukturell angelegten Zielkonflikte zwischen der gebotenen IT-Infrastruktursicherheit der Bürgerinnen und Bürger einerseits, und den Eingriffsinteressen der Sicherheitsbehörden andererseits.

- **Unabhängigkeit des BSI sicherstellen:** Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) kommt eine tragende Rolle bei der Gewährleistung der IT-Sicherheit zu. Das mit dem IT-Sicherheitsgesetz geschaffene System von Mindestschutzstandards und Meldepflichten für Unternehmen der kritischen Infrastrukturen kann nur greifen, wenn das BSI als unabhängig und vertrauenswürdig wahrgenommen wird. Nur so kann es seiner Rolle als Berater und Ansprechpartner der Bürgerinnen und Bürger gerecht werden. Deshalb fordern wir, das BSI

zumindest bei der Erfüllung dieser Aufgaben aus dem Weisungsstrang des Bundesinnenministeriums herauszulösen, das oftmals einseitig zugunsten von Eingriffen staatlicher Behörden agiert. Die Unabhängigkeit des BSI muss zumindest im Umfang dieser Aufgaben sichergestellt werden.

- **Das IT-Sicherheitsgesetz ausbauen:** Zwar ist das IT-Sicherheitsgesetz ein längst überfälliger Schritt in die richtige Richtung, umfassendere Lösungsansätze bietet es aber nicht. Es bezieht sich ausschließlich anhand quantitativer Größen- und Versorgungszahlen auf die Betreiber ausgewählter Kritischer Infrastrukturen. Kritische Versorgungsleistungen wie im Gesundheitsbereich oder nicht weniger sensible Gesellschaftsbereiche wie z.B. das politische System werden so nicht erfasst. Deshalb führt bereits der Titel in die Irre. Die Chance, das Gesetz aufgrund der europäischen NIS-Richtlinie für IT-Sicherheit weiterzuentwickeln, wurde verpasst. Der Kreis der erfassten Infrastrukturen, die Mindestsicherheitsstandards unterliegen, müsste bedeutend erweitert und auf spezifische Kontexte angepasst werden. Nachweise der Einhaltung sollten primär über konkrete Prüfverfahren (sog. Penetrationstests) anstelle bürokratischer Pflichtenhefte erfolgen. Es müssen Pflichten zur Information auch der Öffentlichkeit verankert und ein strengeres, an Umfang und Qualität der Datenschutzgrundverordnung angelehntes Sanktionsregime eingeführt werden. Auch die Orientierung der Länder und Kommunen sowie kritischer Bereiche wie Medien und Kultur an den Sicherheitsstandards dieser Regelung muss sichergestellt und überprüft werden.

- **Die Haftungsregelungen erweitern:** Mehr Schutz für die Nutzerinnen und Nutzer und ein insgesamt besseres Schutzniveau setzt ein wirksames Haftungsregime voraus. Es ist eines der effektivsten Steuerungsinstrumente. Positive Anreize zur Qualitätssicherung werden in der IT bislang nur sehr lückenhaft eingesetzt. Teilweise wird von der Bundesregierung gar mit pauschalen Haftungsfreistellungen gearbeitet. Entscheidend ist deshalb, sowohl die zivilrechtlichen, als auch die öffentlich-rechtlichen Regelungen mit Blick auf die bekannten Risiken, als auch die rechtlichen Haftungshindernisse differenziert zu erweitern. Anreize für alle in der IT-Kette verantwortlichen Stellen bis hin zum Endnutzer sollen dabei erhalten bleiben, damit diese ihren Beitrag leisten.

  Bei der Haftung für Sicherheitsverletzungen wie fahrlässig implementierte oder nicht beseitigte Sicherheitslücken von Herstellern (Produktsicherheitsgesetze; Produkthaftung, Produzentenhaftung, Schutzgesetze), der Verkäufer-Haftung bei Hard- und Software (Gewährleistung, Fehlerbegriff, zugesicherte Eigenschaft, berechtigte Erwartung des Käufers) sowie von Dienstleistern (Sicherheitspflichten und berechtigte Sicherheitserwartungen der Nutzer) müssen mit Blick auf die Besonderheiten und Risiken vernetzter IT-Systeme Regelungslücken angegangen werden. Die häufig komplexer gelagerten Streitfälle von geteilter und oft nicht mehr konkret feststellbarer Verantwortung von Herstellern, Diensteanbietern und Nutzern dürfen nicht einseitig zu Lasten der Endnutzerinnen und -nutzer ausgehen.

  Auch die rasante Zunahme von vernetzten Geräten (Internet of Things) muss für die IT-Sicherheit berücksichtigt werden, bilden sie doch vielfach kritische Angriffspunkte. Daher sollte analog zur bisher im IT-Sicherheitsgesetz vorgesehenen Verpflichtung von Diensteanbietern durch technische und organisatorische Vorkehrungen Verbraucherinnen und Verbraucher besser zu schützen, auf vernetzte Geräte und Software erweitert werden. Hersteller und Entwickler von bspw. Smartphones, Apps, vernetzten Geräten sind verpflichtet, ab Verkauf für einen angemessenen Zeitraum regelmäßig Sicherheits-updates vorzuhalten.

- **Transparenz gegenüber der Öffentlichkeit schaffen:** Transparenz ist ein wesentliches Element einer demokratischen und glaubwürdigen Politik der IT-Sicherheit: Transparenz gegenüber der

Öffentlichkeit bei Maßnahmen, Vorgängen und Angriffen sowie den betroffenen Infrastrukturen und Unternehmen. Selbstverständlich sind schutzwürdige Interessen von Unternehmen hinsichtlich einer möglichen Sicherheitsgefährdung oder geschäftlicher Nachteile bei einer Veröffentlichung zu achten. Die Spielräume für eine verbesserte Information der Öffentlichkeit sind jedoch bislang nicht ausgeschöpft. In gravierenden Fällen muss das BSI zur Veröffentlichung unter konkreten Angaben verpflichtet werden. Unternehmen muss wiederum das weitgehende Recht eingeräumt werden, über die Praxis von Anfragen der Sicherheitsbehörden möglichst differenziert berichten zu können. Für beides braucht es klare rechtliche Regelungen.

- **Den Aufbau sicherer IT-Infrastruktur fördern:** Im Vordergrund müssen der schrittweise Aufbau sicherer IT-Infrastrukturen und sichere Produkte stehen. Das hat der Heartbleed-Bug-Fall gezeigt: Die Sicherheitslücke in der Open-SSL-Verschlüsselung stand zwei Jahre lang unerkannt dem Missbrauch offen. Bei derartigen, weit verbreiteten Open Source Produkten fehlen Anreize für die Wirtschaft, systematische Auditierungen bzw. Prüfungen auf Softwarefehler durchzuführen. Abhilfe könnten mit öffentlichen Mitteln ausgestattete Belohnungssysteme (Bug Bounties) zur Identifizierung von Softwarefehlern bzw. Sicherheitslücken für konkret benannte Softwarebereiche schaffen. Mit gutem Beispiel vorangehen sollte das öffentliche Auftragswesen und im Vergaberecht nicht-proprietäre, auditierbare Produkte grundsätzlich bevorzugen. Transparente Hard- und Software sowie Nachweise von Höchststandards bei der Sicherheit auch von Dienstleistern sowie Lieferketten produzierter Hardware sollten neue Maßstäbe setzen.

  Hohe Dynamik ist beim Roll-Out neuer Technologien zu erleben, etwa im Bereich des "Internets der Dinge". Hier bedarf es zügiger Sicherheitsstandards. Denn bereits heute zeichnen sich weitere schleichende Sicherheitsgefahren ab, beispielsweise durch Bot-Netz-Angriffe über schlecht abgesicherte Geräte. Soweit die einschlägigen Gremien, auch auf europäischer Ebene, die erforderliche rasche Umsetzung nicht gewährleisten, sollte zumindest über die Organisation und Vorgabe von Best Practices gesteuert werden.

- **Der Zusammenarbeit im CAZ eine rechtliche Grundlage geben:** Das so genannte "Cyberabwehrzentrum" (CAZ) der Bundesbehörden ist sowohl funktional als auch aus datenschutzrechtlicher Sicht mehr als eine bloße Zentralstelle des Bundes. Die Entscheidungen der teilnehmenden Behörden sind nur scheinbar eigenständig. Sie dürften in der Praxis von den beratenden Prozessen, Gutachten und Vorläufen gerade im CAZ kaum zu trennen sein. Wenn die kompetenziellen Vorschriften des Grundgesetzes nicht leerlaufen sollen, braucht es deshalb hinreichend bestimmte Regelungen zu den zulässigen Aufgaben des CAZ. Es geht nicht an, dass unter dem Vorwand gemeinsamer Verantwortung der Sicherheitsbehörden unterschiedliche rechtsstaatlich-kompetenzielle Grundlagen schleichend ausgehöhlt werden.

  Die Zusammenarbeit im CAZ muss auf eine gesetzliche Grundlage gestellt werden, die sowohl die Rechte und Pflichten der beteiligten Behörden als auch Maßgaben für unterschiedliche Handlungsformate und den Umgang mit Informationen und Daten klar regelt.

- **ZITIS auf den Prüfstand stellen:** Ähnlich gelagert sind Fragen der Zulässigkeit bei der bereits im Aufbau befindlichen Zentralstelle für Informationstechnik im Sicherheitsbereich (ZITIS). Die Bundesregierung hat bislang widersprüchliche Angaben zu den voraussichtlichen Aufgaben der Einheit gemacht. Es bestehen erhebliche Zweifel an der Rechtsstaatlichkeit des Grundkonzeptes. Auch hier wäre eine enge, rechtsstaatlich wie grundrechtlich orientierte gesetzliche Regelung erforderlich.

  Mit ZITIS soll offenbar ein zentraler Dienstleister geschaffen werden, der Aufgaben und Befugnisse ganz unterschiedlicher Sicherheitsbehörden im Internet erfüllt. Das unterstellt, dass die

vielfältigen denkbaren staatlichen Hackingansätze und Instrumente austauschbar bzw. universell einsetzbar sind. Die oftmals höchstsensiblen Grundrechtseingriffe unterliegen aber ganz unterschiedlichen grundrechtlichen Bindungen der jeweiligen Behörde. Das ist maßgebend für die Frage, ob überhaupt und wenn ja, in welcher Weise und in welchem Umfang, Eingriffe in unterschiedliche informationstechnische Systeme erfolgen dürfen. An den notwendigen spezialgesetzlichen Regelungen fehlt es aber bislang. Vor diesem Hintergrund ist es rechtsstaatlich wie auch haushälterisch nicht vertretbar, eine derartige Einheit zum Aufbau von Hackingkapazitäten ins Blaue hinein auf den Weg zu bringen.