Stellungnahme von Thomas Reinhold[1], TU Darmstadt, zur öffentlichen Anhörung am 14.12.2020 im Verteidigungsausschuss des deutschen Bundestages zum Thema:

„Verfassungs- und völkerrechtliche Fragen im militärischen Cyber- und Informationsraum unter besonderer Berücksichtigung des Parlamentsvorbehalts, der Zurechenbarkeit von Cyberangriffen sowie einer möglichen Anpassung nationaler und internationaler Normen“

Deutscher Bundestag
Verteidigungsausschuss

Ausschussdrucksache
19(12)936
03.12.2020 - 19/3482
5410

Vorbemerkung zur Stellungnahme: Der Autor ist weder Völkerrechtler noch Jurist, sondern Informatiker sowie Friedens- und Sicherheitsforscher. Schlussfolgerungen zu rechtlichen Fragen werden vor allem auf Basis der technischen Grundlagen und Zusammenhänge in Bezug auf die Fragestellung sowie damit verbundener Belange gezogen.

[1] Webseite und Profil auf cyber-peace.org --- https://peasec.de/team/reinhold --- @CyberPeace1

Aus Sicht der Friedens- und Konfliktforschung ist die zunehmende Militarisierung des Cyberraums mit großer Sorge zu bewerten. Diese betrifft insbesondere folgende Problematiken, die nachfolgend näher erläutert werden:

1. Nachrichtendienstliche und militärische Aktivitäten in IT-Systemen gefährden die globale IT-Sicherheit.
2. Bereits Aufklärungsaktivitäten im Cyberraum können aufgrund der notwendigen Manipulationen an IT-Systemen dem Verbot friedensstörender Handlungen nach Art. 26 Abs. 1 GG entgegenstehen.
3. Entwicklung und Einsatz offensiv wirksamer Cyber-Hilfsmittel fördern den globalen Markt für Sicherheitslücken und unterbinden die Beseitigung von Verwundbarkeiten großflächig eingesetzter ziviler IT-Produkte.
4. Die Zunahme nachrichtendienstlicher und militärischer Aktivitäten unterhalb der Schwelle offener militärischer Konflikte erhöht das Eskalationspotential.
5. Fehlende internationale Vereinbarungen über Grenzen nachrichtendienstlicher und militärischer Aktivitäten in IT-Systemen steigern das Risiko von Fehlinterpretationen und Fehlreaktionen.
6. Die Priorisierung militärischer Offensiv-Maßnahmen im Cyberraum anstelle einer institutionellen Harmonisierung von IT-Sicherheit verschärft die Ressourcenknappheit bei IT-Fachkräften und technischem Knowhow.
7. Fehlende Maßnahmen der Rüstungskontrolle sowie technische Verfahren zur Stärkung der Vertrauensbildung im Cyberraum erschweren die Eingrenzung von Rüstungswettläufen im Cyberraum sowie die Reduktion von Konfliktpotentialen.

Zu 1: Nachrichtendienstliche und militärische Aktivitäten in IT-Systemen gefährden die globale IT-Sicherheit.

Nahezu[2] jegliche nachrichtendienstliche oder militärische Aktivität gegen oder in IT-Systemen erfordert Maßnahmen zur Umgehung von Schutzmaßnahmen, zur Erlangung spezifischer technischer Zugangs- und Ausführungsberechtigungen sowie zum Beseitigen digitaler „Fußspuren“ in den Systemen. Aus der Perspektive der IT-Sicherheit entspricht dies einer Manipulation des Regelverhaltens des betroffenen Systems, genauer einer Verletzung der IT-Schutzziele[3] „Vertraulichkeit” und „Integrität” sowie ggf. auch dessen „Verfügbarkeit”. Manipulierte Systeme können sich unerwartet verhalten, in der Ausführung ihrer Dienste gestört werden oder ausfallen. Dies gilt unabhängig vom eigentlichen Ziel der Cyberoperation bereits für Informationsgewinnungsaktivitäten ebenso wie für offensive Maßnahmen der „aktiven Verteidigung“, „Vorwärtsverteidigung”, „Hack-Backs“[4] oder einem „Persistent Engagement“[5]. Des Weiteren erfordern komplexe Cyberoperationen in aller Regel auch entsprechende manipulierende Aktivitäten gegen unbeteiligte, vorgeschaltete Systeme, um über Netzwerke hinweg Zugriff auf das Zielsystem zu erlangen. Einem IT-System ist weder von außen noch, mit ausreichender Sicherheit, von innen der Zweck und die Aufgaben des Systems sowie die Abhängigkeiten zu anderen IT-Systemen anzusehen. Direkte und indirekte Konsequenzen von Manipulationen sind dadurch kaum sicher abzuschätzen oder einzugrenzen. Damit werden zivile oder unbeteiligte IT-Systeme und die von ihnen ausgeführten Dienste durch Manipulationen in Gefahr gebracht und ggf. schwer kalkulierbare Kettenreaktionen ausgelöst.

Zu 2: Bereits Aufklärungsaktivitäten im Cyberraum können aufgrund der notwendigen Manipulationen an IT-Systemen dem Verbot friedensstörender Handlungen nach Art. 26 Abs. 1 GG entgegenstehen.

---

[2] Ausgenommen sind Zugriffe auf IT-Systeme mit Hilfe gültiger, gestohlener oder anderweitig erlangter Zugangsdaten. Selbst in diesem Fall kann es jedoch erforderlich sein, unerlaubte Zugriffe auf die Systeme durch das digitale „Verwischen von Spuren“ mit entsprechenden Manipulationen zu verbergen.

[3] Zu den drei Grundprinzipien der IT-Sicherheit siehe https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html

[4] Eine gesonderte Diskussion der sog. Hack-Backs findet sich unter https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/AP_Schulze_Hackback_08_2017.pdf

[5] Für eine ausführlichere Darstellung dieser, aktuell insbesondere von den USA verfolgten Maßnahme proaktiver Cyberoperationen in IT-Systemen mutmaßlicher Gegner siehe https://cyber-peace.org/2019/06/17/kurz-notiert-usa-weiten-offensive-cyber-operationen-aus-mehr-fruehere-schnellere-reaktion-auf-cyberbedrohungen/

In einem Gutachten des wissenschaftlichen Dienstes des Bundestages von 2018[6] stellt dieser fest, dass sich das Verbot friedensstörender Handlungen nach Art. 26 Abs 1 auch auf Cyber-Aktivitäten staatlicher Institutionen beziehen kann, unabhängig davon welche staatliche Institution diese ausführt. Das Gutachten betont dabei den Zusammenhang zwischen Art. 26 Abs. 1 GG und der Bewertung eines Cyberangriffs im Sinne von Art. 51 der UN-Charta, bei dem Menschen verletzt oder getötet oder erhebliche Sachgüter zerstört werden. Hinsichtlich der Wahrnehmung und Interpretation von Vorfällen im Cyberraum wird darüber hinaus betont, dass die Gefahr von Fehlinterpretationen und damit von ungewollten Eskalationen im Cyberraum erheblich ist.

Mit Blick auf die voran erläuterten technischen Aspekte von nachrichtendienstlichen und militärischen Aktivitäten im Cyberraum muss festgehalten werden, dass eine rein passive Aufklärung kaum möglich ist. Verfahren wie das sog. Port-Scanning[7] oder der Zugriff auf Systeme durch valide, auf anderem Wege erworbene Zugangsdaten[8] bieten zwar nicht-intrusive Möglichkeiten ein IT-System zu untersuchen, allerdings mit geringem nachrichtendienstlichen Erkenntnisgewinn. In aller Regel werden solche Maßnahmen nur als Vorbereitung für einen weitergehenden, manipulationsbehafteten Zugriff auf die Systeme verwendet. Darüber hinaus ermöglichen diese Verfahren jeweils nur den Zugriff auf die äußersten Schichten eines Zielnetzwerkes, während sich Hochwertziele in aller Regel tief in IT-Netzwerken eingebettet befinden, umgeben von anderen IT-Systemen und Schutzmaßnahmen. Ein Zugriff auf diese Hochwertziele ist nur durch ein sukzessives Ausspähen, Unterwandern und Manipulieren vorgeschalteter Systeme möglich. Dies gilt in jedem Fall auch dann, wenn diese Operation „nur" zum Zweck der Analyse und Aufklärung dieser Systeme durchgeführt werden. Es muss daher in aller Deutlichkeit festgestellt werden, dass jegliche Operationen in IT-Systemen, beginnend bei ausschließlichen Aufklärungsaktivitäten diese und angeschlossene IT-Systeme aufgrund der erläuterten technischen Sachverhalte hochgradig gefährden und unbeabsichtigte Schäden an Sachgütern und u.U. Menschenleben zur Konsequenz haben können.

Vor diesem Hintergrund ist auch die im Gutachten betonte Beschränkung der Nachrichtendienste auf Aufklärungsmaßnahmen relevant. Diesen Diensten stehen nach

---

6 https://www.bundestag.de/resource/blob/560900/baf0bfb8f00a6814e125c8fce5e89009/wd-3-159-18-pdf-data.pdf

7 Bei einem Port-Scan werden IT-Systeme von außen durch reguläre Anfragen auf Hinweise auf mögliche Sicherheitslücken analysiert, ohne in die Systeme direkt einzudringen. Selbst ein massenhafter Port-Scan kann jedoch ungenügend konfigurierte Schutzmaßnahmen zu einem Fehlverhalten bringen.

8 Vgl. Fußnote 2

Ansicht des wissenschaftlichen Dienstes auf Basis der derzeitigen Rechtslage keine klassischen Eingriffsbefugnisse zu. Wie erläutert, ist eine Aufklärung von IT-Systemen ohne Eingriff nicht sinnvoll umzusetzen. Es ist daher die Schlussfolgerung des Gutachtens, dringend zu betonen, dass „eine Durchführung von Cyberangriffen durch Nachrichtendienste (..) jedenfalls zu einer erheblichen Erweiterung der bisherigen nachrichtendienstlichen Befugnisse führen [würde]"[9].

Zu 3: Entwicklung und Einsatz offensiv wirksamer Cyber-Hilfsmittel[10] fördern den globalen Markt für Sicherheitslücken und unterbinden die Beseitigung von Verwundbarkeiten großflächig eingesetzter ziviler IT-Produkte.

Die Grundlage für Cyberoperationen und die dabei eingesetzten offensiv wirksamen Cyber-Hilfsmittel[11] bilden Zero-Day-Exploits[12] oder allgemein Sicherheitslücken in IT-Produkten, für die es bis dato noch keine Sicherheitsaktualisierung zur Behebung der Verwundbarkeiten gibt. Der steigende Bedarf durch staatliche Stellen für derartige Informationen fördert deren Marktwert und schafft Anreize für Unternehmen zum Aufkauf und Handel mit diesen Informationen. Je tiefgreifender oder weitreichender eine Sicherheitslücke ist, umso höher ist deren Wert und der Anreiz diese Information an Bedarfsträger zu verkaufen. Die Kenntnisse über entsprechende Verwundbarkeiten werden dadurch zurückgehalten, dem Hersteller des betroffenen IT-Produktes nicht gemeldet und folglich nicht geschlossen. Aufgrund des hohen Dual-Use-Charakters von IT-Produkten betreffen Verwundbarkeiten in Produkten, die für Nachrichtendienste und militärische Kräfte interessant sind, damit in aller Regel auch breit eingesetzte zivile IT-Produkte wie Betriebssysteme, Office-Anwendungen oder Smartphone-Programme.. Da ein Zugriff auf ein Zielsystem oft über diverse unterschiedlichste und zumeist

[9] Siehe Fußnote 6

[10] Als "offensiv wirksame Cyber-Hilfsmittel" werden jegliche Formen von fertiger oder spezifisch angefertigter Software sowie Verfahren verstanden, mit deren Hilfe IT-Systeme manipuliert, IT-Schutzmaßnahmen umgangen sowie anderweitig die reguläre Ausführung von Operationen in einem IT-System verändert werden können.

[11] Die Bezeichnung "Cyberwaffe" für derartige Hilfsmittel wird an dieser Stelle nicht verwendet, da es noch keine allgemein anerkannte Definition für den Waffen-Begriff im Kontext schadhafter Hilfsmittel im Cyberraum gibt. In der aktuellen Forschung sowie sicherheitspolitischen Debatten werden als "Cyberwaffen" üblicherweise all jene Hilfsmittel bezeichnet, die im Cyberraum wirken und im Sinne der völkerrechtlichen Perspektive auf bisherige Waffen-Technologien signifikante Schäden an Sachgütern oder der Gesundheit und dem Leben von Menschen verursachen können.

[12] Ein Zero-Day-Exploit (auch als 0-Day-Exploit bezeichnet) ist ein Angriff auf Grundlage einer Sicherheitslücke in einem IT-Produkt, die denjenigen unbekannt ist, die an der Verringerung der Sicherheitsanfälligkeit interessiert sein sollten, wie den Anwendern sowie dem Hersteller des Produktes. Da für eine Zero-Day-Sicherheitslücke noch keine Sicherheitsaktualisierung des Produktes verfügbar ist, kann diese Schwachstelle ungehindert durch jeden ausgenutzt werden, der über diese Information verfügt.

schlechter geschützte „Zwischenstationen" in den Zielnetzwerken realisiert wird, müssen in aller Regel mehrere Schwachstellen und Exploit-Ketten[13] verwendet werden. Derart nichtbehobene Schwachstellen können ebenfalls durch andere staatliche, nicht-staatliche oder kriminelle Akteure entweder entdeckt oder ihrerseits kommerziell erworben und für eigene Zwecke ausgenutzt werden. Dies kann unter Umständen extreme globale wirtschaftliche Schäden verursachen, wie im Falle von NotPetya[14]. Diese Schadsoftware basierte auf einer Sicherheitslücke in Microsoft Windows-Betriebssystemen, die mutmaßlich der US-amerikanischen NSA länger bekannt war und durch diese zurückgehalten wurde. Nach einem Diebstahl der Informationen wurden diese öffentlich bekannt und konnten von den Urhebern von NotPetya ausgenutzt werden[15].

Zu 4: Die Zunahme nachrichtendienstlicher und militärischer Aktivitäten unterhalb der Schwelle offener militärischer Konflikte erhöht das Eskalationspotential.

Die zunehmende Bewertung des Cyberraums als Domäne für nachrichtendienstliche und militärische Aktivitäten – von der Lagebilderstellung bis zur offensiven Cyberoperation – fördert eine Dynamik der globalen Bedrohungswahrnehmung in dieser Domäne, erkennbar an der zunehmenden Einrichtung staatlicher Institutionen zur Cyberverteidigung[16]. Gleichzeitig erfordert die Durchführung offensiver Maßnahmen in dieser Domäne Kenntnisse über Zielsysteme, deren Erreichbarkeit und Schwächen. Derartige Informationen müssen in aller Regel bereits im Vorfeld potentieller Operationen zusammengetragen werden, um im Bedarfsfall geeignete Angaben über mögliche Zugriffspunkte oder sogar bereits vorbereitete Zugangsmöglichkeiten zu relevanten Systemen zu verfügen. Dies gilt umso mehr, wenn die, auch im Rahmen der Bundeswehrfähigkeiten diskutierten offensiven Cyberoperationen schnell und flexibel gegen akute Cyberbedrohungen eingesetzt werden sollen. Offensive Cyberoperationen erhöhen demzufolge den Bedarf an Aufklärungsaktivitäten in Friedenszeiten um Zielinformationen zu sammeln und zeitnah bereitstellen zu können. Wie vorangehend

[13] Siehe Fußnote 12

[14] Details zu NotPetya sowie der zugrunde liegenden Sicherheitslücke „EternalBlue" unter https://cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfalle/petya_notpetya/

[15] Es ist anzumerken, dass nach dem Diebstahl der Informationen die NSA den Softwarehersteller Microsoft informierte und diese umgehend eine Sicherheitsaktualisierung bereitgestellt haben. Aufgrund des jedoch z.T. recht langsamen "Ausrollens" von Sicherheitsaktualisierungen in Unternehmen und Behörden konnte NotPetya dennoch erhebliche Schäden in ungesicherten und entsprechend verwundbaren Systemen verursachen.

[16] Siehe dazu exemplarisch die Liste der nationalen Cybersicherheits- und Verteidigungsstrategien wie sie durch das NATO Cooperative Cyber Defence Centre of Excellence bereit gestellt wird unter https://ccdcoe.org/library/strategy-and-governance/

erläutert, bergen derartige Aufklärungsaktivitäten dabei stets die Gefahr der unbeabsichtigten Störung von IT-Systemen mit unkalkulierbaren Konsequenzen. Je nach politischer Situation sowie den zwischenstaatlichen Beziehungen könnten solche Störungen durch einen Staat als Angriff auf die eigene staatliche Souveränität bis hin zu einem bewaffneten Angriff interpretiert werden.

Durch derartige Cyber-Aktivitäten verschwimmen zum einen zunehmend die Grenzen zwischenstaatlicher Konflikte. Andererseits verstärkt der Bedarf an Informationen die weitere Verzahnung geheimdienstlicher und militärischer Aktivitäten um bspw. dem für Deutschland geltenden Primat der defensiven Ausrichtung der Bundeswehr Rechnung tragen zu können. Eine solche Zunahme nachrichtendienstlicher Aufgaben muss jedoch durch eine adäquate parlamentarische Kontrolle überwacht und begrenzt werden können.

Zu 5: Fehlende internationale Vereinbarungen über Grenzen nachrichtendienstlicher und militärischer Aktivitäten in IT-Systemen erhöhen das Risiko von Fehlinterpretationen und Fehlreaktionen.

Den beschriebenen Aktivitäten in IT-Systemen durch Nachrichtendienste und militärische Kräfte steht das Fehlen spezifischer und verbindlicher internationaler Übereinkommen gegenüber, die derartige Maßnahmen regulieren oder begrenzen können. Gleichzeitig erhöht die Verfügbarkeit von Maßnahmen zur aktiven Gegenwehr bei Cyberattacken in Verbindung mit einer gebotenen Reaktionsgeschwindigkeit den Handlungsdruck, in Krisensituationen derartige Mittel einzusetzen. Vergangene Vorfälle verdeutlichen jedoch immer wieder das Problem der zuverlässigen Zuordnung des tatsächlichen Ursprungs einer Cyberattacke sowie des dahinterstehenden Angreifers. Neben der Problematik gezielter *False Flag*-Operationen[17] ist eine zuverlässige Attribution insbesondere bei komplexen IT-Angriffen oft nur zeitaufwendig und im mehrmonatigen Rahmen mit Hilfe von IT-Forensik, zum Teil auf Basis internationaler Kooperationen beim Zugriff auf die für den Angriff verwendeten IT-Systeme, umsetzbar. Vorschnelle Schlussfolgerungen bergen eine hohe Gefahr von Fehlinterpretationen und damit von Fehl- oder Überreaktionen, die sich unter Umständen gegen unbeteiligte Dritte richten. Gleichzeitig ist die Bewertung von offensiven Cyberhilfsmitteln als „chirurgische“ Einwirkung empirisch nicht belegbar da eine verlässliche

[17] Als *False Flag*-Operationen werden Cyberangriffe bezeichnet, bei denen der Angreifer durch die Wahl seiner eingesetzten Mittel wie dem Standort von Command & Control-Servern oder der im Code verwendeten Muttersprache gezielt die Aufmerksamkeit auf einen dritten, unbeteiligten Akteur zu lenken versucht.

Wirkungsentfaltung bei aktiven Reaktionen gegen IT-Systeme aufgrund der erläuterten komplexen Abhängigkeiten und Wechselwirkungen in IT-Netzwerken kaum möglich ist.

Zu 6: Die Priorisierung militärischer Offensivmaßnahmen im Cyberraum anstelle einer institutionellen Harmonisierung von IT-Sicherheit verschärft die Ressourcenknappheit bei IT-Fachkräften und technischem Knowhow.

Die Aufklärung und Vorbereitung offensiver Cybermaßnahmen erfordert eine umfangreiche Vorfeldaufklärung, den Zugriff auf vorgeschaltete Systeme sowie gegebenenfalls die Vorinstallation von Hintertüren für eine effektive Aktivierung des Wirkmittels im Bedarfsfall. Solche Vorbereitungen sind nur mit umfangreichem technischem Knowhow und entsprechend hohem Einsatz von IT-Fachkräften umsetzbar. Derartige Maßnahmen wären dementsprechend nur gegen ausgewählte, strategisch relevante potentielle Ziele umsetzbar, während ihr Nutzen und ihre Wirksamkeit – zusätzlich zu den voran erläuterten Problemen und Gefahren – in hohem Maße kritisch bewertet werden muss. Gleichzeitig ist auch die Wirksamkeit von Verteidigungsmaßnahmen auf Basis offensiver Gegenreaktionen im Cyberraum anzuzweifeln. Ein Angreifer, der mit derartigen Gegenmaßnahmen rechnen muss, wird geeignete Redundanzmaßnahmen, auf die gegebenenfalls ausgewichen werden kann, in die Angriffsinfrastruktur einbauen und in seinem taktischen Vorgehen wie beispielsweise durch die Nutzung von IT-Systemen dritter Parteien berücksichtigen. Vor diesem Hintergrund muss auch die Abschreckungswirkung militärischer Offensivfähigkeiten im Cyberraum dahingehend in Frage gestellt werden.

Gleichzeitig wäre angesichts der Breite potentieller staatlicher, nicht-staatlicher und krimineller Angreifer sowie der Heterogenität der deutschen IT-Landschaft der Aufbau umfangreicher Offensivmaßnahmen kein Ersatz für eine weitere Intensivierung defensiver Maßnahmen aus dem Bereich der IT-Sicherheit. Diese sollte primär gefördert und ausschließlich dort, wo sinnvoll durch nachrichtendienstliche und militärische Ressourcen, wie Knowhow oder Bedrohungsanalysen unterstützt werden. Die eigenen nationalen IT-Systeme sind der geeignete Raum zu Gestaltung von IT-Sicherheit. Auch angesichts gegenwärtiger und mittelfristig knapper Ressourcen bei IT-Fachkräften ist die Priorisierung einer defensiven Ausrichtung dringend angeraten, verbunden mit einer Stärkung ziviler IT-Sicherheit wie der Verbesserung der Qualität großflächig eingesetzter kommerzieller IT-Produkte. Die grenzüberschreitende Nachverfolgung und Abwehr von Cyberattacken sollte in internationaler Kooperation erfolgen und dafür die Zusammenarbeit im Rahmen bi- und multilateraler Übereinkommen verbessert und gestärkt werden. Gleichzeitig sollte international das *Due Dilligence*-Prinzip staatlicher

Verantwortungspflicht weiterhin mit Nachdruck betont und Staaten zur Zusammenarbeit motiviert werden.

Zu 7: Fehlende Maßnahmen der Rüstungskontrolle sowie technische Verfahren zur Stärkung der Vertrauensbildung im Cyberraum erschweren die Eingrenzung von Rüstungswettläufen im Cyberraum sowie die Reduktion von Konfliktpotentialen.

Ein wesentliches Hemmnis bei der Entwicklung internationaler Übereinkommen zur Regulierung und Reduzierung ungehemmter nachrichtendienstlicher und militärischer Aktivitäten im Cyberraum ist das fehlende gemeinsame Verständnis elementarer Begriffe wie „Cyberwaffe“[18] oder „Cyberangriff“. Bisherige Konzepte orientieren sich an etablierten Verfahren der Rüstungskontrolle aus anderen Technologiebereichen, tragen den technischen Besonderheiten der Domäne Cyberraum aber nur ungenügend Rechnung. So wird bspw. die Abschätzung des möglichen Schadens sowie die mutmaßlichen Intentionen eines Angreifers in aller Regel als Grundlage für die Bewertung einer potentiellen Cyberwaffe herangezogen. Eine solche Abschätzung ist jedoch im Gegensatz zu kinetischen Wirkmitteln aufgrund der abweichenden, zum Teil verzögerten und sukzessiven Wirkungsentfaltung von Cyberwaffen erheblich erschwerter und zuverlässig erst nach dem Einsatz der Cyberwaffe zu bewerten. Für Maßnahmen der Konfliktreduktion im Rahmen von Rüstungskontroll- und Abrüstungsübereinkommen, die auf einer Bewertung von potentiellen offensiv wirksamen Cyber-Hilfsmitteln vor deren Einsatz basieren, sind derartige Analyse-Verfahren nicht geeignet. Gleichzeitig fehlen im Bereich der naturwissenschaftlichen Friedens- und Konfliktforschung hinreichend entwickelte Konzepte und technische Verfahren, um diesen Herausforderungen der Rüstungskontrolle zu begegnen sowie andere geeignete Maßnahmen zur Unterstützung von Vertrauensbildung. Ein weitere gezielte Förderung und Anwendung derartiger Forschung im Rahmen deutscher außenpolitischer Initiativen als Gegengewicht zur allgemein zunehmenden Militarisierung des Cyberraum ist dringend geboten. Die friedliche Entwicklung des Cyberraum als globale, vernetzte und hochgradig voneinander abhängige Domäne ist für unsere Gesellschaft, Wirtschaft und Sicherheit von entscheidender Bedeutung.

[18] Vgl. dazu Fußnote Nr. 6