»Cybersicherheit« Perspektiven für einen sicheren digitalen Raum

Öffentliches Fachgespräch der Bundestagsfraktion DIE LINKE

Eingangsstatement

Vielen Dank für ihre Einladung und die Möglichkeit, hier Erkenntnisse aus meinem Forschungsgebiet der Friedens- und Sicherheitsforschung beitragen zu können. Ich glaube es ist wichtig einleitend nochmals darauf hinzuweisen, welch elementarer Bestandteil der Cyberspace als weltweite Vernetzung von IT-Systemen und deren Dienstleistungen für die Wirtschaft, die staatlichen Institutionen und das Leben jedes einzelnen darstellt. Dementsprechend entscheidend ist es, dass sich der Staat dem Schutz und der Sicherheit dieses Raumes widmet. Selbstverständlich bleibt auch die Bundeswehr von dieser Entwicklung nicht unberührt. Die Anstrengungen des Verteidigungsministeriums in der Bundeswehr für eine sichere IT-Landschaft zu sorgen sind ungemein wichtig, da mittlerweile jede Fregatte, jeder Panzer und Helikopter von Computern durchdrungen ist, die angegriffen werden können. Gleichzeitig ist es jedoch besorgniserregend, dass der Cyberspace dort zunehmend auch als Domäne für das militärisch offensive Wirken aufgefasst wird. Aus sicherheits- und friedenspolitischer Perspektive ergeben sich aus diesem nationalen wie weltweiten Trend zur Militarisierung des Cyberspace mehrere Probleme, auf die ich hinweisen möchte:

- Zum einen folgt man damit der Entwicklung eines weltweiten Rüstungswettlauf um Cyberwaffen, also jegliche Art von Software oder Know-How mit dem fremde IT-Systeme gestört oder beschädigt werden können. Andererseits ist jedoch noch unklar, ob und wie etablierte Regeln des Völkerrechts auf den Cyberspace und dessen spezielle Eigenschaften anwendbar sind. International verbindliche Regeln die sich gezielt mit dieser Domäne befassen und festlegen was Staaten hier machen dürfen und was nicht gibt es bislang nicht.
- Ein weiterer Punkt ist, dass nach wie vor Hack-Backs als sinnvolle Strategie der militärischen Verteidigung diskutiert werden, also Maßnahmen die darauf ausgerichtet sind IT-Systeme von denen Cyberattacken ausgehen durch Gegenmaßnahmen zu stören. Der tatsächliche Nutzen solcher Operationen ist zweifelhaft während die Gefahren von Fehlinterpretationen und damit möglicherweise auch Fehl-Reaktionen sehr viel höher sind als bei herkömmlichen Waffensystemen wie Raketen oder Landstreitkräften.

Exemplarisch möchte ich dabei auf das sogenannte Attributionsproblem verweisen, also auf die immensen Schwierigkeiten bei der möglichst zweifelsfreien Identifikation des Angreifers im Cyberspace. Dazu kommt, dass die Frage wie bei militärischen Cyberoperationen Kollateralschäden an zivilen IT-Systemen vermieden werden können noch völlig offen ist. Der Nimbus sauberer und zielgerichteter Gegenschläge im Cyberspace ist bei eingehender Analyse der technischen Details solcher Operationen nicht haltbar.

- Unklar ist auch, wie die offensiven Cyber-Fähigkeiten der Bundeswehr mit der Tatsache in Einklang gebracht werden soll, dass die Bundeswehr eine Parlamentsarmee ist, der Bundestag also über jeden bewaffneten Einsatz einzeln entscheiden und zustimmen muss. Eigentlich müssten die Cyberkräfte bereits lange vor der Beteiligung an Konflikten den zeitaufwendigen Prozeß der Identifikation relevanter Ziele im Cyberspace und das Ausspähen der fremden Systeme durchführen. Solche Informationen sind notwendig um den Zugriff auf diese Ziele zu üben oder sich sogar bereits digitale Hintertüren zu erschließen. Ein solches Vorgehen ist jedoch weder vom Grundgesetz gedeckt noch wünschenswert. Bundesverteidigungsministerin Frau von der Leyen betont regelmäßig, dass der Parlamentsvorbehalt selbstverständlich auch für Cybereinsätze der Truppe gilt. Allerdings werfen gerade die technischen Details solcher Einsätze wie eben kurz angedeutet viele Fragen und Unsicherheiten auf. Hier sind spezifische Antworten und Regeln notwendig - letztlich auch im Interesse der Soldatinnen und Soldaten, damit diese rechtlich abgesichert handeln.

- Gerade mit Blick auf die eben angesprochenen notwendigen Cyber-Aufklärungsinformationen, die mutmaßlich auch in Friedenszeiten gesammelt werden müssten, stellt sich die Frage der Neu-Bewertung nachrichtendienstlicher Aktivitäten. Insbesondere dem Bundesnachrichtendienst dürfte hier als Auslandsgeheimdienst eine zentrale Rolle als “Zuträger” für solche Informationen zufallen. Dieser Aspekt wurde unlängst auch in einem Gutachten des wissenschaftlichen Dienstes des Bundestages betont. Ob solche verstärkte Aktivitäten des BND wünschenswert sind und welche politischen Konsequenzen sich daraus ergeben sollte als gesellschaftliche Debatte öffentlich geführt werden.

- Um in fremde IT-Systeme eindringen zu können benötigen Nachrichtendienste oder das Militär Informationen darüber, wo das fremde System Sicherheitslücken hat. Solche Sicherheitslücken sind der digitale Türöffner um Schutzmaßnahmen zu umgehen.

Darunter fallen auch die besonders potenten und gefährlichen Schwachstellen, die so genannten "Zero-Days". Solche Sicherheitslücken können am effektivsten dann ausgenutzt werden, wenn sie öffentlich nicht bekannt sind. Auf der anderen Seite bedeutet das Verschweigen aber auch, dass man damit Gefährdungen unterschlägt, die eine Bedrohung der eigenen zivilen IT-Infrastruktur darstellen können. Es stellt sich die Frage, wie und nach welchen Regeln staatliche Institutionen mit Sicherheitslücken umgehen sollen und welche Gremien dies kontrollieren könnten. Dies betrifft insbesondere die notwendige Abwägung zwischen Aufgabenerfüllung und dem gesellschaftlichen Anspruch auf Schutz durch staatliche Institutionen.

- Die angesprochene Konzentration auf Möglichkeiten des offensiven Wirkens im Cyberspace ist in den vergangenen Monaten auch deutlich geworden an der Gründung verschiedener staatlicher Einrichtungen. Zu nennen sind dabei die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS), der Cyber-Innovation-Hub der Bundeswehr oder die kürzlich gegründete Agentur für Innovation in der Cybersicherheit. Diese Einrichtungen dienen alle mutmaßlich der Beschaffung oder Entwicklung von offensiven Hilfsmitteln für den Cyberspace. Eine vergleichbar ausgeprägte institutionelle Stärkung ziviler IT-Sicherheit, die zum Beispiel sichere Endverbraucher-Geräte fördert, findet kaum statt.

Aus Sicht der Friedens- und Konfliktforschung muss man feststellen, dass die Militarisierung des Cyberspace in Deutschland bislang unzureichend kritisch wissenschaftlich begleitet wird. Dies betrifft insbesondere die notwendige naturwissenschaftliche Friedens- und Konfliktforschung zu dieser Domäne, die hier Hand in Hand mit der Informatik arbeiten müsste. Konkret geht es um Verfahren der Rüstungskontrolle und Abrüstung für den Cyberspace. Solche Maßnahmen sind eine entscheidende Voraussetzung für zukünftige zwischenstaatliche Verträge bzw. internationale Abkommen um die destabilisierenden Entwicklungen der Cyberaufrüstung einzugrenzen. Dafür ist es jedoch notwendig zu klären, wie bei Cyberwaffen Maßnahmen der Nichtverbreitung gefährlicher Technologien aussehen könnten oder welche Formen von Kontroll- und Verifikationsverfahren im Cyberspace anwendbar sind. In gleicher Weise ist es dringend notwendig Gegenentwürfe zum übermachtigen Attributionsproblem zu entwerfen, wie zum Beispiel mit einer gesicherten, nachweisbaren Nicht-Einmischung bei Cyberkonflikten. Die Friedens- und Konfliktforschung kann hier Möglichkeiten und Wege aufzeigen, wie diese neuen Waffen kontrolliert werden können.

Leider muss man festhalten, dass für solche Forschungsfragen bislang der politische Wille zu fehlen scheint. Gleichermaßen beklagenswert ist die oft fehlende Bereitschaft zum Diskurs in den betroffenen Ministerien sowie der Bundeswehr und die fehlende Aufgeschlossenheit, sich über diese sicherheitspolitischen Aspekte der Cyber-Aufrüstung und deren Konsequenzen auszutauschen.

Abschließend ist es mir wichtig zu betonen, dass bei all den skizzierten Schwierigkeiten der Cyberspace gegenüber früheren Technologien einen entscheidenden Vorteil bietet. Der Cyberspace ist eine vollkommen vom Menschen erschaffene und kontrollierte Domäne. Die Regeln, Grenzen und Funktionsprinzipien dieses Raumes werden durch Techniker und Ingenieure weiterentwickelt und von internationalen Gremien bestimmt. Die sich damit bietenden Gestaltungsmöglichkeiten für die friedliche Entwicklung des Cyberspace sollten unbedingt aufgegriffen werden. Dafür ist es notwendig, sich als Regierung weiter in internationale Gremien einzubringen, wie dies bspw. im Rahmen der diplomatischen Bemühungen um Vertrauensbildung unter der deutschen Leitung der OECD initiiert worden ist.

Um es zusammen zu fassen: Aus friedens- und sicherheitspolitischer Perspektive gilt es, IT-Sicherheit als Bestandteil zum Schutz des weltweit friedlichen gesellschaftlichen und wirtschaftlichen Wachstums aufzufassen. Dementsprechend müssen den militärischen und nachrichtendienstlichen Aktivitäten im Cyberspace die Risiken offensiver Maßnahmen entgegen gestellt und die destabilisierende Entwicklung mit sicherheitspolitischen Werkzeuge eingegrenzt werden.

Vielen Dank.