NATO : Cyber Defence als politisch-strategische Herausforderung

Autor(en): **Schlie, Ulrich**

Objekttyp: **Article**

Zeitschrift: **ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift**

Band (Jahr): **182 (2016)**

Heft 3

PDF erstellt am: **13.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-587009

NATO: Cyber Defence als politisch-strategische Herausforderung

«We are committed to developing further our national cyber defence capabilities, and we will enhance the cyber security of national networks upon which NATO depends for its core tasks, in order to help make the Alliance resilient and fully protected. Close bilateral and multi-national cooperation plays a key role in enhancing the cyber defence capabilities of the Alliance. We will continue to integrate cyber defence into NATO operations and operational and contingency planning, and enhance information sharing and situational awareness among allies.»

Ulrich Schlie

Die Ziffer 73 der Erklärung der Staats- und Regierungschefs auf dem NATO-Gipfel in Wales vom 5. September 2014 steckt voller guter Absichten und weist den Weg nach vorne. Die NATO wird ihre Cyber-Aktivitäten verstärken und nimmt dabei ihre Mitgliedsstaaten in die Pflicht. Cyber defence gilt heute übereinstimmend als eine wesentliche Herausforderung der Sicherheit. Als eine solche Gefährdung der Sicherheit werden die Bedrohungen aus dem Cyber-Raum wiederkehrend in politischen Grundsatzdokumenten und Reden führender Allianzpolitiker identifiziert. Rekapituliert man die Diskussionen über Cyber im Allianzrahmen, so zeigen sich die ganzen Schwierigkeiten, die ein unzweifelhaft aufwachsendes, aber gleichwohl schwer fassbares begriffliches Thema für die sicherheitspolitische Gemeinschaft darstellt. Denn zunächst hängen die richtigen Antworten auf die mit dem Politikfeld «Cyber security» verbundenen Herausforderungen vom Bewusstsein der tatsächlichen Dimension der Gefährdung ab.

Anspruchsvolle politische Definition

Dies betrifft zuerst und grundlegend die Frage der politischen Definition, dies schliesst sodann die richtige Form der Kommunikation der Bedrohung im politisch-strategischen Diskurs ein und stellt nationale Regierungen vor die organisatorisch-bürokratische Herausforderung, im Verständnis einer gesamtstaatlichen Sicherheitsvorsorge und ressortübergreifend die richtigen administrativen Organisationsentscheidungen zu treffen. Wesentlich mit dieser politisch-administrativen Dimension des Themas verbunden ist die Frage nach der angemessenen rechtlichen, insbesondere völkerrechtlichen Einstufung. Dies betrifft sowohl die Fortentwicklung des Völkerrechts als auch die im Allianzrahmen zu diskutierende Frage, ob Cyber-Attacken den Artikel 5 – Bündnisfall auslösen können. Die in Wales 2014 dazu gefundene Kompromisslösung, dass der NATO-Rat im Zweifelsfall darüber zu befinden habe, ist politisch konsequent und stellt gegenüber der bis dahin geltenden vollkommenen Grauzone zumindest einen Schritt nach vorne dar. Doch was genau stellt eine Cyber-Attacke dar? Die Aktivitäten im Cyber-Raum sind vieldimensional. Cyber-Spionage, Cyber-Verbrechen und Cyber-Krieg können dabei ineinander übergehen und folgen doch jeweils ganz unterschiedlichen Kalkülen. Kriminelle nutzen Sicherheitslücken in den gängigen Programmen und manipulieren die Software auf den als Ziel identifizierten Computern. Die auf diese Weise gekaperten Computer können systematisch ausgebeutet werden, und nicht selten handeln Cyber-Kriminelle für staatliche Auftraggeber.

Zu den Schwierigkeiten, die sich beim Politikfeld der Cyber security ergeben, gehört der Umstand, dass hierbei staatliches Handeln tief in Domänen eingreifen muss, die sich zu überwiegenden Teilen in privater Hand befinden. Denn die kritische Infrastruktur eines Landes – Strom, Wasser, Telekommunikation, Transport, Krankenhäuser, Banken – bildet naturgemäss bei Angriffen aus dem Cyber-Raum das bevorzugte Zielgebiet, und gemeinsam ist diesen Bereichen, dass sie sich in fast allen Ländern ausserhalb der unmittelbaren Kontrolle des Staates befinden. Wasser- und Stromversorgung, Abwasserentsorgung, U-Bahnnetze, Hochgeschwindigkeitsverkehrslinien und Eisenbahnknotenpunkte: immer erfolgt die Steuerung auf elektronischem Wege, der Ausfall eines Zentralcomputers kann ganze Systeme lahmlegen. Gerne von den Cyber-Kriminellen ins Visier genommen sind Bankbetriebssysteme, deren Kollaps in Zeiten des bargeldlosen Zahlungsverkehrs enorme volkswirtschaftliche Auswirkungen haben kann.

NATO Cyber Defence Centre in Tallinn (Estland). Bild: news.err.ee

Paradigmenwechsel Internet

Hinzu kommt ein Paradigmenwechsel, der mehr und mehr den Umgang mit dem Internet bestimmt. Einst, vor über zwei Jahrzehnten, ist das Netz auf der Grundlage von gegenseitigem Vertrauen aufgebaut worden. In der Zwischenzeit hat die kommerzielle Nutzungsorientierung, der Geheimnisverrat, die Verletzung der Privatsphäre und die fortlaufende Grenzübertretung beim Schutz intellektuellen Eigentums unser Verhältnis zum Netz grundlegend verändert. Der Ruf nach Schutzwällen und die Bemühungen um eine Ethik des Internets sind ein Gebot der politischen Klugheit. Das Internet ist zur Kampfzone mutiert. Als es im Sommer 2008 nach der Abspaltung Südossetiens und Abchasiens zum russisch-georgischen Krieg kam, war es nicht zufällig, dass zeitgleich die Homepage der georgischen Regierung und die des Staatspräsidenten Saakaschwili lahm gelegt waren. Der Urheber dieser Distributed Denial of Service-Attacke ist allerdings schwer zu lokalisieren. Viele Angriffe werden vor allem aus China verzeichnet, doch oft verläuft sich die Spur; die geographische Herkunft des Computers jedenfalls kann am wenigsten als zuverlässiges Indiz auf den Ausgangspunkt des Angriffs betrachtet werden. Ähnlich schwierig sind auch Rechtsfragen, die sich auf Aspekte der Cyber defence und der Cyber security beziehen. Gerade die schier unüberschaubaren Cyber-Daten verlangen danach, dass internationale Übereinkünfte die Sammlung und den Datenfluss kanalisieren. Regierungen müssen den Punkt definieren, ab dem ein Eingriff in die Regelungen des Cyber-Raums sinnvoll ist, bis wohin die Industrie in Eigenständigkeit, aber nach klar definierten Standards selbstregulierend tätig werden kann, und wie sich die Staaten am besten gegen die Sicherheitsgefährdungen aus dem Cyber-Raum schützen können. Dies beschreibt auch den politischen Rahmen, in dem die Nordatlantische Allianz das Thema Cyber-Sicherheit diskutiert.

Cyber-Attacke auf Estland 2007

Spätestens seitdem im Mai 2007 nach einem Streit über ein sowjetische Kriegsdenkmal eine allmählich aufwachsende massive Cyber-Attacke die estnischen Computer-Netze – allen voran die Website des Premierministers, der Regierung und einer führenden Supermarktkette – lahm legte, ist das Thema Cyber defence auf die Tagesordnung der Allianz aufgerückt. Beweise für eine russische Urheberschaft indes konnten nie gefunden werden. Es war deshalb folgerichtig, im Mai 2008 ausgerechnet in Tallinn ein Center of Excellence zu begründen. Dort geht heute entsandtes Personal aus derzeit acht Nationen Fragen der Forschung und Ausbildung im Zusammenhang mit Fragen der Cyber defence nach. Den offiziellen Eingang in die NATO-Doktrin fand Cyber durch das im Herbst 2010 auf dem Gipfel in Lissabon verabschiedete Strategische Konzept. Zu Recht wurden darin Cyber-Angriffe als Gefährdung für die transatlantische Sicherheit und Stabilität eingestuft. Seit Juni 2011 verfügt die Allianz mit der Cyber defence policy über ein neues Politikfeld, deren fortlaufende Umsetzung durch den Cyber Defence Action Plan sichergestellt ist. Im Falle einer Cyber-Krise obliegt dem Cyber Defence Management Board die Koordinierung der notwendigen Massnahmen sowie die Steuerung der NATO Computer Incident Response Capability (NCIRC). Mit dem NCIRC sind eine durchgehende zentrale Überwachung aller vorgesehenen Netze sowie die Erfassung auch anspruchsvoller Bedrohungen der NATO-Einrichtungen sichergestellt.

Der Cyber Defence Action Plan hat indes vor allem Auswirkungen auf die Streitkräftefähigkeiten im Allianzrahmen. In allen Ländern müssen zunächst die innerstaatlichen Voraussetzungen geschaffen und die entsprechenden Massnahmen getroffen werden, um auf dieser Grundlage die nationale Mitwirkung auf politisch-strategischer Ebene in den entsprechenden Foren von NATO und EU ermöglichen zu können. Dies betrifft insbesondere auch die Rolle von Streitkräften. Fragen der Cyber defence sind heute schon aufs engste mit Überlegungen der konventionellen Kriegführung verbunden. Mit nationalen Cyber-Führungselementen kann die Koordinierung des Einsatzes der CNO-Fähigkeiten in einem militärischen Einsatz gesteuert und im Bündnisrahmen als Teil einer defensiven oder auch offensiven Gesamt-Operationsführung koordiniert werden. Das Spektrum der Fähigkeiten für Computernetzwerk-Operationen ist heute vorrangig darauf gerichtet, im Rahmen der Bündnisverteidigung als Landesverteidigung einen bewaffneten Angriff abzuwehren. Dies erfordert die Befähigung zum Wirken im Cyber-Raum. Der Aufbau eines Cyber-Führungselementes als Kernelement mit Aufwuchsfähigkeit durch nationale und internationale Kräfte für Übungen und

den Einsatz ist deshalb folgerichtig. Schon die Verteidigungspolitischen Richtlinien vom Mai 2011 haben mit ihren Vorgaben, dass die deutschen Streitkräfte ein möglichst breites Fähigkeitsspektrum abdecken müssen, die Voraussetzungen für die Stärkung der CNO-Kräfte als unverzichtbares Wirkmittel moderner Streitkräfte sowohl mit Blick auf defensive als auch auf offensive Massnahmen geschaffen. Und die von Deutschland als «deliverable» für den NATO-Gipfel in Wales koordinierte Rahmennationen-Initiative (Framework Nations Concept) bildet für die Zusammenarbeit bei Cyber-Fähigkeiten einen wesentlichen Beitrag.

Konflikte werden heute, und erst recht morgen, auch im Cyber-Raum ausgetragen

Es zählt zu den unausweichlichen Konsequenzen, dass durch die Verschärfung der allgemeinen Bedrohungs- und Gefährdungslage die politische und wirtschaftliche Relevanz von Cyber-Sicherheit zunehmen wird. Bewaffnete Konflikte werden bereits heute, und erst recht morgen, auch im Cyber-Raum ausgetragen werden. Bei einer Cyber-Krise sind erhöhte Anforderungen an die gesamtstaatliche Koordination, aber insbesondere auch an das Wirken im Verbund mit Partnern gestellt. Es ist deshalb konsequent, dass Fragen der Cyber-Sicherheit in den supranationalen Foren an Bedeutung gewinnen werden. In der allgemeinen Wahrnehmung von Cyber-Sicherheit dominierten zunächst die technischen Aspekte. Die Auswirkungen auf Streitkräftefähigkeiten, die zunehmende operative Bedeutung des Cyber-Raums bei militärischen Auseinandersetzungen scheint erst allmählich ins Bewusstsein vorzudringen.

Die im Cyber Defence Action Plan festgehaltenen Aufgaben beschreiben den schleichenden Wandel, der insgesamt in den Partnerstaaten der Allianz mit Blick auf die Gefährdungen des Cyber-Raums stattgefunden hat. Denn in fast allen Partnerstaaten der Nordatlantischen Allianz wird das Thema Cyber-Verteidigung heute über die rein technische IT-Sicherheit und den Schutz der eigenen Systeme hinaus begriffen. Mit Blick auf das Bewusstsein und die Umsetzungsmassnahmen finden sich indes auch unter NATO-Mitgliedstaaten grosse Abweichungen. Es überrascht wenig, dass die Vereinigten Staaten auch beim Thema Cyber defence und Cyber security tonangebend sind. Die amerikanischen Streitkräfte verfügen im Cyber Command, das dem Strategic Command untersteht, über ein Instrument, das Aspekte der IT-Sicherheit mit operationellen Fähigkeiten zusammenbringt. Die Verantwortlichkeiten für Cyber Policy sind im Pentagon zwar noch immer an verschiedenen Stellen zusammengefasst, doch es gibt keinen anderen Ort auf der Welt, in dem Cyber so sehr als politisch-strategische Herausforderung erkannt ist wie in Washington. In Grossbritannien liegt seit November 2011 eine umfassende Cyber Security Strategy vor, die die Bekämpfung der Cyber-Kriminalität versieht, die Widerstandsfähigkeit gegen Cyber-Angriffe zum Schutz der britischen Interessen im Cyber-Raum stärken möchte und die Gewährleistung eines sicher nutzbaren Cyber-Raums als britisches nationales Interesse benennt. Auch in Frankreich ist in mehreren Grundsatzdokumenten der Anspruch auf eine globale Rolle des Landes beim Thema Cyber-Sicherheit erhoben. Mit diesen grundsätzlichen Betrachtungen geht immer auch eine politische Prioritätensetzung einher. So wurde in Deutschland als vorrangiges Thema der Cyber-Sicherheit die Gewährleistung sicherer Informationssysteme und eines sicheren Cyber-Raums sowie die Stärkung der Sicherheit kritischer IT-Netze identifiziert. Es war deshalb konsequent, dass in Deutschland im April 2011 ein Cyber-Abwehrzentrum eingerichtet wurde, bei dem die Bundesämter für Sicherheit und Information, Bevölkerungsschutz und Katastrophenhilfe und das Bundesamt für Verfassungsschutz vertrauensvoll zusammenwirken und Bundeskriminalamt, Bundespolizei, Bundesnachrichtendienst sowie Bundeswehr Verbindungselemente beisteuern. Ebenfalls seit Mai 2011 kommt ein Cyber-Sicherheitsrat mit Vertretern von mehreren Bundesministerien – Auswärtiges Amt, Bundesministerium der Finanzen, des Inneren, für Justiz, für Wirtschaft, für Bildung und Forschung, der Verteidigung, sowie Vertretern der Bundesländer – zu regelmässigen Arbeitstreffen zusammen. Für eine koordinierende Cyber-Aussenpolitik gibt es im Auswärtigen Amt seit August 2013 einen Sonderbeauftragten für Cyber-Aussenpolitik, und Bundesministerin von der Leyen hat 2015 in einer Strategischen Leitlinie zum Thema Cyber-Verteidigung die wesentlichen Vorgaben für den Geschäftsbereich des Bundesministeriums der Verteidigung zusammengefasst.

Fazit

Zu den politischen Zukunftsaufgaben, die sich aus einer aktiven Cyber security policy für die Mitgliedsstaaten der Nordatlantischen Allianz ergeben, zählt auch der Ausbau der Zusammenarbeit mit der Europäischen Union. Die Kooperation mit der Europäischen Union bleibt eine der Zukunftsaufgaben, bei der sich die europäischen Mitglieder der NATO um eine engere sicherheitspolitische Verklammerung, grössere Arbeitsteilung und die Identifizierung von verbindlichen gemeinsamen Standards verdient machen können und zu einem gemeinsamen Verständnis von Sicherheit gelangen können. Zwar hat sich die Europäische Union im zeitlichen Abstand zur NATO im Februar 2013 eine Cyber-Sicherheitsstrategie verpasst. Deren wesentliche Schwerpunkte sind das Verhältnis von Sicherheit und Freiheit in der Prävention, abgestufte Widerstandsfähigkeit, öffentlich-private Partnerschaften sowie die Zusammenarbeit mit Partnern weltweit. Cyber-Verteidigungspolitik und Cyber-Verteidigungsfähigkeiten im Rahmen der GSVP gelten als prioritär. Doch das im Vergleich mit der Allianz deutlich geringer ausgeprägte sicherheitspolitische Grundverständnis der Europäischen Union zeigt sich beim Thema Cyber security besonders deutlich. Von einem echten Brückenschlag zwischen zivilen und militärischen Ansätzen kann hier noch nicht die Rede sein, denn eine Betrachtung offensiver Cyber-Fähigkeiten ist bislang im Rahmen der Europäischen Union nicht vorgesehen. Die Europäische Union beansprucht in ihrer Cyber-Sicherheitsstrategie für sich allenfalls eine koordinierende, mitwirkende Rolle und überlässt den nationalen Regierungen den Vorrang. Bewusstseinsbildung, politische Kommunikation, Verbreiterung des gesamtstaatlichen Sicherheitsverständnisses und die entsprechenden Massnahmen zur Gewährleistung der Sicherheit im Cyber-Raum nehmen unsere Staaten in die Pflicht: Parlamente, Regierungen und deren Apparate, insbesondere Streitkräfte, Nachrichtendienste und Auswärtigen Dienste, sind daher auf besondere Weise gefordert. ■

Ulrich Schlie
Dr. phil. M.A.
ehemaliger Politischer Direktor im deutschen Verteidigungsministerium
Medford M.A., USA