BULLETIN Außen- & Sicherheitspolitik

Magazin des Außen- und Sicherheitspolitischen Arbeitskreises der CSU

Ausgabe 1 / 2016

DIE GRENZEN EUROPAS

Über europäische Lösungen und nationale Notwendigkeiten

BRAUCHT DIE BUNDESWEHR OFFENSIVE CYBERFÄHIGKEITEN?

Was spricht dafür, was spricht dagegen?

Current challenges for NATO in cyber domain

Piret Pernik,
Research Fellow at the International Centre for Defense and Security, Tallinn, Estonia

CYBER RISIKO

WIDERSTANDSFÄHIGKEIT, EINE DER WICHTIGSTEN GRUNDLAGEN ZUR UMFASSENDEN VERTEIDIGUNG

Florian Hahn, Vorsitzender ASP

**LIEBE LESERINNEN UND LESER,
LIEBE FREUNDE DES ASP,**

es ist das große Paradox des 21. Jahrhunderts, dass jene Technologien, die einen entscheidenden Nutzen versprechen, uns gleichzeitig verletzlich machen: Ein Großteil der kritischen Infrastruktur – unsere Finanzsysteme, unser Stromnetz oder Gesundheitssysteme – sind mit dem Internet verbunden. Die gleichen Informationstechnologien, die dazu beitragen, dass die Bundeswehr über modernste Fähigkeiten verfügen, werden zum Eintrittstor für mögliche Hackerattacken. Es ist evident, dass die Digitalisierung neue Schwachstellen geschaffen hat, die wir vorher nicht kannten. Wir müssen daher lernen, mit den wachsenden Bedrohungen Schritt zu halten. Denn Angriffe im Cyberraum sind unkonventionell, ohne physische Gewalt, verdeckt und voller Winkelzüge – und sie passieren tagtäglich.

Der Schutz im Cyberraum ist somit zu einer Frage der öffentlichen, wirtschaftlichen und nationalen Sicherheit geworden. Diese Ausgabe des „Bulletin Außen- und Sicherheitspolitik" widmet sich aus diesem Grund den Risiken im Cyberraum. Welche Grundlagen sind entscheidend, um die nationale Widerstandsfähigkeit zu erhöhen? Wie kann und sollte die NATO auf die neuartigen Herausforderungen reagieren? Und: Braucht die Bundeswehr offensive Cyberfähigkeiten? Diese und weitere Fragen werden von ausgewiesenen Experten im aktuellen Heft kritisch diskutiert.

Weitreichende Veränderungen in der Bundeswehr sollen die Verteidigungsfähigkeit im Cyberraum erhöhen: Mit der Aufstellung einer IT-/Cyberabteilung im Ministerium und eines kompletten Organisationsbereichs geht die Verteidigungsministerin neue Wege. Klar ist, dass die Angriffe immer komplexer und anspruchsvoller werden. Seit den ersten Computerviren auf PCs in den frühen 1980er Jahren befinden wir uns im Grunde in einem konstanten Cyberwettrüsten. Konsequenterweise entsteht aktuell das größte Forschungszentrum der Bundesrepublik für den Cyberraum an der Bundeswehruniversität in München. Daneben gilt, dass die Bekämpfung möglicher Angriffe eine gesamtstaatliche Aufgabe sein muss. Regierung, Industrie und Wissenschaft müssen eng kooperieren, um auf mögliche Cyberbedrohungen schnell zu reagieren. Es wäre deshalb nur folgerichtig, weitere politische und militärische Bereiche in München anzusiedeln und ein umfassendes Cyber-Cluster aufzubauen. Denn eins sollte uns bewusst sein: So wie wir im Cyberraum miteinander vernetzt sind wie nie zuvor, muss auch die Zusammenarbeit so weit reichen wie nie zuvor. Nur so können wir den Herausforderungen und Chancen des Informationszeitalters gleichermaßen gerecht werden. Ich freue mich darauf, gemeinsam mit Ihnen die nächsten Schritte zu diskutieren.

**Mit besten Grüßen
Ihr Florian Hahn MdB,
Landesvorsitzender des ASP**

Peter J. Wirnsperger – Partner Cyber Risk Services bei Deloitte

CYBER RISIKO

WIDERSTANDSFÄHIGKEIT, EINE DER WICHTIGSTEN GRUNDLAGEN ZUR UMFASSENDEN VERTEIDIGUNG

Der groß angelegte Angriff auf die Internet-Infrastruktur der USA am Freitag, den 21. Oktober 2016* hat sehr deutlich die Verletzlichkeit des Internets und der Services aufgezeigt, aber noch deutlicher gemacht, dass nicht immer nur die sogenannte kritische Infrastruktur besonders geschützt werden muss. Vielmehr müssen wir einen breiteren Blick auf die Absicherung unserer Kommunikations- und Service-Infrastruktur legen.
Mit der Verabschiedung des IT-Sicherheitsgesetzes und der Ausformulierung der industriespezifischen Anforderungen für die sieben betroffenen Sektoren hat Deutschland einen sehr großen Schritt in die richtige Richtung zu einem einheitlichen und fortlaufend sich verbesserndem Sicherheitsniveau in den Bereichen der kritischen Infrastruktur gemacht. Die meisten Industrieländer haben ähnliche Initiativen geplant oder bereits umgesetzt. Und auch die EU-Kommission arbeitet an der Festlegung und Vereinheitlichung der Standards, damit über den ganzen Kontinent ein einheitliches Schutzniveau umgesetzt werden wird.
Die breite Diskussion, die selbst in den ursprünglich nicht betroffenen Sektoren stattfindet, unterstreicht einmal mehr, welche Bedeutung das Sicherheitsthema für die gesamte zivile Volkswirtschaft gewonnen hat.
Durch den Aufbau des Cyber-Kommandos kommt die Bundewehr ebenfalls ihrer Aufgabe nach und baut die Abwehr- und Verteidigungsfähigkeit für die virtuelle Kriegsführung aus, auch wenn die Umsetzung noch ein steiniger Weg ist.
Die Problematik im Spannungsfeld der zivilen Infrastrukturabsicherung der militärischen Verteidigung liegt jedoch in der Tatsache, dass eine eindeutige Abgrenzung der Angreifer in Kleinkriminelle, Organisierte Kriminalität oder staatlich gestützte Angreifer in den seltensten Fällen möglich ist; es stellt sich vielmehr die Frage, ob eine solche Aufteilung und Systematisierung überhaupt sinnvoll und gewollt ist. Denn grade der eingangs erwähnte Angriff hätte alles sein können: die Vorbereitung auf einen ernst zu nehmenden Angriff einer fremden Macht auf die USA, aber genauso leidlich eine Spielerei einer Hacker-Gruppe. Bruce Schneier – einer der anerkanntesten Sicherheitsexperten auf der Welt – ging sogar soweit, dass er den Angriff als einen „einfachen Proof-of-Concept" einordnete. Zum Motiv der Hacker merkte er in seiner Rede am 24. April vor dem Information Security Forum in Berlin in dem Zusammenhang noch an, dass die Angreifer ihre Aktion wahrscheinlich nur durchführten, um zu zeigen, „dass sie es können".
Nicht auszudenken, wenn der Angriff auf kritische Infrastruktur abgezielt hätte. Es bedarf nicht viel Fantasie, was geschehen hätte können, wenn die Angreifer anstatt den Unterhaltungsdiensten den Straßenverkehr ins Chaos gestürzt oder die Wasserversorgung oder echte Kraftwerke angegriffen hätten, wie das die Terroristen im Film „Die Hard 4.0" mit Bruce Willis eindrucksvoll demonstrieren. In dem Film lassen die Angreifer ganze Kraftwerke in die Luft fliegen, in dem sie aus weiter Entfernung und aus sicherer Distanz auf die Systeme zugreifen und sie zur Explosion bringen.
Wenn der Angriff wirklich nur eine Kompetenzdemonstration war, dann müssen wir in naher Zukunft damit rechnen, dass wir solche Angriffe vermehrt erleben werden. Und tatsächlich haben ähnliche Attacken schon früher stattgefunden, nur sind sie selten so präsent. Eine der prominenten und bekannten Beispiele ist eine DDoS-Attacke** gegen Estland im Jahre 2007. Auch dort haben die Angreifer für einen längeren Zeitpunkt ganze Teile des Internets in Estland still gelegt.
Als Informationsgesellschaft müssen wir für unser Land und unsere Volkswirtschaft die Frage stellen, wie wir dieser realen und umfassenden Bedrohung entgegentreten wollen.
Alle Statistiken und die Erfahrung zeigen, dass Angriffe in ihrer Intensität und Komplexität zunehmen werden. Erstes Gebot ist daher der noch stärkere und gezieltere Ausbau der Abwehrmaßnahmen gegen gezielte Einzelangriffe als auch massive Attack-Kampagnen. Und dies muss sowohl im zivilen Sektor als auch im militärischen Bereich mit der gleichen Ernsthaftigkeit und Intensität geschehen. Gleichzeitig müssen wir dazu übergehen, unsere Kommunikations- und IT-Infrastruktur widerstandsfähig zu gestalten und auf das erforderliche „Resilience-Niveau" anzuheben.

Eines der größten Probleme in der Absicherung von kritischen Infrastrukturen insgesamt aber auch im privaten Umfeld ist, dass einzelne Komponenten noch so entwickelt und gebaut sind, dass sie keine eigenen Sicherheitsmechanismen eingebaut haben, einem einfachen Angriff oft nicht standhalten und damit ein einfaches Opfer für Angreifer werden. Der große Angriff am 21. Oktober baute genau auf der Schwachstelle in vielen Überwachungskameras und Festplattenrekorder auf, weil diese Systeme in fast allen Fällen bis heute keine Sicherheitsfunktionen eingebaut haben. Verschlimmert wird die Situation, weil kaum ein Anwender diese Systeme so installiert, dass sie gegen einen Angreifer bestehen können.
In der Produktions- und Steuerungs-IT ist die Situation besonders dramatisch, weil Angreifer für eine Systemmanipulation nicht einmal einen Umweg machen müssen.
Es ist also höchste Zeit, dass wir als Staat insgesamt die Absicherung und Verteidigung stärker in den Fokus rücken. Produkt- und Systemhersteller müssen zwingend Sicherheit in ihre Produkte mit einbauen – „Security by Design". Und die Betreiber von kritischen Infrastrukturen haben eine besondere Sorgfaltspflicht in der Umsetzung des adäquaten Sicherheitsniveaus. Die Grundkonzepte sind den Cyber Security Abteilungen und den IT-Bereichen bekannt. Lediglich war bisher die Priorisierung in der Umsetzung nicht entsprechend gewürdigt.
So dramatisch die Lage klingen mag, wichtig ist, dass alle Verantwortlichen mit der Umsetzung der Cyber Sicherheit zügig beginnen.

* *Unbekannte Angreifer haben über die Ausnutzung von Schwachstellen in Webcams, Festplattenrecordern und anderen Devices eine als DDoS-Attacke bezeichneten Angriff auf Services wie Twitter, Netflix und Paypal ausgeführt. Für mehrere Stunden waren die Dienste nicht mehr aufrufbar und über die Attacke war auch der gesamte Internet-Verkehr in großen Teilen der USA lahm gelegt.*

** *DDoS-Attacke steht für „Distributed Denial of Service Attack" und bedeutet, dass sein Angreifer einen Internet-Service mit Anfragen in kürzester Zeit überflutet und damit der Dienst nicht mehr verfügbar ist.*

CURRENT CHALLENGES FOR NATO IN CYBER DOMAIN

Piret Pernik, Research Fellow at the International Centre for Defense and Security, Tallinn, Estonia

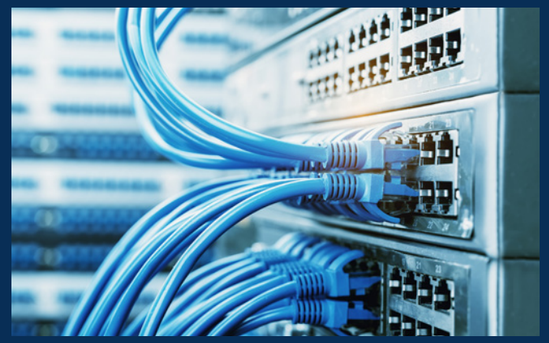
In response to the growing security challenges in cyberspace NATO has in the recent years intensified its cyber defence. NATO faces each weak around 250-300 serious cyber events against its sites, but even greater concerns are threats against integrity of information and information systems, especially manipulation of data, as well as cyber sabotage, such as degrading critical infrastructure, command and control or weapons systems of the member states. In the light of Russia's recent meddling in the US domestic politics and election process, electronic espionage can also have serious national security repercussions. It can be used by adversary states not only for getting access to sensitive or classified information, but also to influence decision making, impact public opinion and even undermine the political systems of the target countries.

In June this year at NATO's Warsaw Summit cyber defence received a renewed impetus. Two years ago at Wales Summit the Alliance had declared that cyberattacks against an Ally may lead to the invocation of any, including military, collective defence measures under article 5. This time NATO took a step even further recognizing that cyberspace constitutes a military domain that is characterised by the same warfighting principles as in traditional military theatres - land, sea and airspace.

Hence, since the collective defence principle encompasses countering threats emanating from cyberspace, NATO will be obliged to provide credible deterrence and collective defence for its member states in and through cyber domain. In practice it means that NATO must be prepared to use the full spectrum of cyber capabilities in its collective defence or crisis management operations. The Alliance must also plan for and train these capabilities to ensure its freedom of action in cyber domain. However, NATO does not own itself cyberspace capabilities just like it does not own troops, vessels or aircraft, but the Allied countries provide national capabilities to NATO's operations. Hence just like in traditional military domains in cyber domain the member states should develop capabilities for the operations. If there is a political willingness to do so, the questions is how and when to do it.

It implies that the Alliance should discuss the possible use of cyber capabilities both in supporting and standalone roles to its operations. In the expert parlance this is often referred to as moving from (more technical) information assurance to (tactical, operational and strategic) mission assurance. The discussion should address issues such as determining cyber defence tasks of NATO both in military and hybrid conflicts, and at peacetime; authority and decision-making procedures in regards to the execution of tasks; capacities and capabilities that must be developed and how to ensure interoperability of 28 different capabilities; institutions and structures that should be altered or put in place; as well as specific education, training, and exercises requirements.

This effort calls for change of the mindset and cannot be achieved without a broad political support from the member states. After all, the Alliance has now for decades focused on a more technical side of cyber defence – protecting its own systems and networks under the purview of NATO Communications and Information Agency. In contrast, mainstreaming cyber defence into military defence entails that tactical, operational and strategic levels commanders and decision makers understand the implications from the use of own and adversary's cyber capabilities. As a first step, a clear doctrinal framework and procedures to allow for the use of cyber capabilities in a standalone role in NATO operations must be developed.



Because the execution of NATO's core tasks depends on the networks and infrastructures of the Allied countries, its networks are only as strong as the weakest Ally. Likewise, NATO cannot execute its tasks without the course to the Allied capabilities and networks, so consequently the protection of national infrastructures and networks cannot be separated from the collective security.

The protection of critical infrastructure, information systems and networks of the member states is naturally their own responsibility. It is not a secret that there are significant gaps in regards to cyber capacities and maturity among the 28 member states. Acknowledging their mutual interdependence, the Allied countries endorsed in Warsaw the so-called cyber pledge, making the protection of their national networks NATO's top priority. The cyber pledge includes measures such as augmenting financial and other resources, speeding up the implementation of cyber defence capability targets in NATO's defence planning process (NDPP), improving national cyber defence skills and expertise, as well as sharing information and national threat assessments. Moreover, NATO will assess the progress made by the member states in developing the agreed capability targets and in implementing security requirements in national critical infrastructures.

As a defensive Alliance of liberal democratic countries, NATO is well positioned to facilitate the expansion of trust that constitutes a base for cooperation in sensitive national security matters. If NATO will be able to increase trust among Allies, they are likely to be more willing to declare national cyber capabilities in framework of the NDPP. Similarly, NATO's situational awareness is composed of information provided by the member states so greater trust would contribute to shared situational awareness.

In the context of a "new normal" use of electronic espionage by Russia in hybrid conflicts and in peacetime against political adversaries, NATO's renewed commitment in Warsaw to cooperate closer with the EU in countering hybrid and cyber threats was timely. The two organisations agreed to share information and intelligence concerning hybrid and cyber threats, as well as cooperate on the analysis, prevention, early detection and coordinating their exercises. The widespread use of information, psychological and cyber operations against liberal democracies with an aim to interfere in domestic politics, impact decision-making, and undermine citizen's trust into political systems and institutions must be addressed in cooperation with the EU who has a broad set of non-military instruments. Such subversive methods cannot be responded with counter operations, but diplomatic, economic and information measures can be more effective.

Two years ago NATO took a position that international law applies to cyberspace. Many member states have advocated in the UN Group of Governmental experts, OSCE, G7 and in other international forums the development of non-binding cyber norms for responsible behaviour of nation-states in cyberspace. To avoid a risk of escalation that increases with more nation states developing cyber capabilities, NATO should have a proactive role in promoting the applicability of international law in cyberspace, as well as cyber norms and related confidence-building measures.

To sum up, while NATO's mission in cyber defence is justifiedly defensive, it goes without saying that the Alliance needs to discuss among its member states under what circumstances offensive cyber capabilities can be used in accordance with the international law and agreed cyber norms. For example, if and under what circumstances could adversary's command and control structures or critical infrastructures be degraded by cyber means in peacetime or during NATO operations? It may be difficult if not impossible to find consensus, but nevertheless it is better to talk about it before a situation in hand has arrived.

Dr. Hans-Peter Friedrich, Stv. Vorsitzender der CDU/CSU Fraktion im Bundestag

DIE GRENZEN EUROPAS
ÜBER EUROPÄISCHE LÖSUNGEN UND NATIONALE NOTWENDIGKEITEN

Über europäische Lösungen und nationale Notwendigkeiten

Wir leben in unruhigen Zeiten: Der Fall des mutmaßlichen Terroristen in Chemnitz am 10. Oktober hat einmal mehr daran erinnert, welche Gefahren mit der Zuwanderung verbunden sind.

Unsere Sicherheit und unsere Freiheit ziehen Menschen aus aller Herren Länder an, die unter Gewalt und Unfreiheit leiden; aber auch Menschen, die keinen Schutz suchen, sondern unsere Sicherheit und Freiheit bedrohen. Dagegen müssen wir uns schützen.

Europäische Gemeinsamkeiten

Der Wegfall der Grenzkontrollen im sogenannten Schengenraum ist ein Pfeiler der europäischen Integration. Doch er hat zwei Voraussetzungen: Kontrolle der Außengrenzen und enge Zusammenarbeit und Vernetzung aller Sicherheitsbehörden in Europa. Kroatien, Rumänien und Bulgarien warten noch auf den Beitritt zum Schengenraum, ihre Grenzen bilden aber teilweise bereits heute die EU-Außengrenze. Deshalb achten die Europäer schon jetzt darauf, dass dort aufmerksam kontrolliert wird.

Die sogenannte Dublin-III-Verordnung der EU regelt den Umgang mit Menschen, die als Bürgerkriegsflüchtlinge oder politisch Verfolgte zu uns kommen wollen. Klar ist: Sowohl Schengen als auch Dublin funktionieren nur, wenn an den Außengrenzen konsequent kontrolliert und registriert wird. Erfüllen die Grenzländer diese Verpflichtung nicht, bedroht das alle Europäer.

Grenzen des europäischen Grenzmanagements

Manche Länder machen ihre Arbeit: Spanien hat seit 2006 die Zahl der illegalen Migranten um drei Viertel reduziert, auch durch den massiven Ausbau der Grenzzäune an seinen Exklaven Ceuta und Melilla. Den ersten Zaun zwischen Ceuta und Marokko finanzierte übrigens 1993 größtenteils die EU. Auch Rumänien und Bulgarien sicherten nach dem EU-Beitritt 2007 ihre EU-Außengrenzen mit Zäunen. Dafür erhielten sie zwischen 2007 und 2009 von der EU aus der sogenannten „Schengen-Faszilität" rund 800 Mio. Euro.

Angesichts der stark wachsenden illegalen Migration errichtete Ungarn im Sommer 2015 einen Grenzzaun an seinem Abschnitt der EU-Außengrenze. Die den Ungarn dafür entgegenschlagende Kritik, vor allem von Brüsseler und Berliner Sozialdemokraten, war umso peinlicher als sie sachfremde, allgemeinpolitische Gründe hatte.

Zumal der Grund für den Anstieg der illegalen Migration nach Mitteleuropa in Griechenland lag: Griechenland (aber auch Italien) hatte jahrelang illegale Einwanderer unregistriert nach Norden weiterreisen lassen, v. a. nach Deutschland. Ein Verstoß gegen das Dublin-Abkommen, den die EU-Kommission nicht ahndete. Mit dem anschwellenden Flüchtlingsstrom aus Syrien und Nordafrika registrierten die Griechen Anfang 2015 gar nicht mehr. Nicht zu vergessen: Der griechische Verteidigungsminister Kammenos drohte im März 2015 mit der massenhaften Durchreise unkontrollierter Migranten, um Deutschland zu Nachgiebigkeit bei den griechischen Staatsschulden zu erpressen.

Nationale Entscheidungen

Weil Schengen also nicht mehr funktionierte, mussten die Nationalstaaten handeln: Schweden und (Stunden später) Dänemark führten Anfang Januar 2016 wieder konsequente Grenzkontrollen ein. Schon seit September 2015 kontrollierte auch Deutschland an der Grenze nach Österreich, allerdings ohne die konsequente Zurückweisung von Menschen, die offensichtlich kein Asyl in Deutschland erhalten können. Erst die Schließung der Balkanroute im März 2016 ließ die Migration nach Deutschland spürbar abebben. Fast zeitgleich wurde das Rücknahmeabkommen mit der Türkei abgeschlossen. In diesen Monaten wird sich zeigen, ob es tatsächlich funktioniert, da Griechenland die Türkei noch immer nicht als sicheres Herkunftsland anerkennt und mit der Abwicklung der Asylanträge offensichtlich überfordert ist.

Die österreichische Regierung beschloss im Januar 2016 eine jährliche Obergrenze von 37.500 Zuwanderern. Das Signal war deutlich: wir entscheiden, wer zu uns kommt und wer nicht. Unterstrichen wurde dieses Signal, indem österreichische Soldaten medienwirksam die Sperrung der Grenze zu Slowenien übten.

Was Deutschland braucht

Eine bürgerlich geführte Regierung darf keinen Zweifel daran lassen, dass sie die Kontrolle darüber ausübt, wer in unser Land kommt. Um verloren gegangenes Vertrauen zurück zu gewinnen, braucht es anhaltende, auch hartnäckige Führung in dieser Frage. Wir müssen unser nationales Recht wieder konsequent anwenden, also auch diejenigen zurückweisen, die offensichtlich kein Asyl in Deutschland erhalten können. Wer keine Papiere (mehr) hat, muss zur Klärung der Personalien an der Grenze festgehalten werden. Die CSU hat immer wieder Transitzonen gefordert. Wenn diese an der SPD scheitern, muss man die Forderung solange wiederholen, bis auch in der SPD die Ideologie der Realität weicht.

Selbstverständlich muss eine Regelabfrage aller Migranten bei den Sicherheitsbehörden sein. Wir haben an verschiedenen Stellen unseres Sicherheitsapparats Informationen, die Leben retten können. Darauf müssen unsere Grenzbehörden auch zugreifen (können).

Was Europa braucht

Europa arbeitet seit Jahren an einem besseren Grenzmanagement. Wir müssen rasch ein europäisches Ein- und Ausreisesystem nach dem Vorbild des amerikanischen ESTA organisieren. Unter dem Akronym ETIAS („EU Travel Information and Authorisation System") erarbeitet die EU-Kommission dafür derzeit Pläne. Auch hierzu muss eine Regelabfrage bei den Datenbanken der Sicherheitsbehörden gehören.

Der Migrationsdruck nach Europa wird auf Jahrzehnte hoch bleiben. Unsere Freiheit und unsere Sicherheit werden weiterhin viele, viele Menschen von unseren Nachbarkontinenten Asien und Afrika anziehen. Wir müssen den Menschen dort helfen, vor allem in Afrika. Hier kann die EU wertvolle Koordinierung leisten.

Bei uns geht es derweil um die grundsätzliche Frage: Sollen wir alle Menschen, die zu uns wollen, auch zu uns lassen, wie die politische Linke es will? Oder wollen wir Europäer unsere Freiheit und unsere Sicherheit verteidigen, indem wir die Kontrolle über unsere Grenzen selbst ausüben?

Dr. Hans-Peter Friedrich, Stv. Vorsitzender der CDU/CSU Fraktion im Bundestag

DIE GRENZEN EUROPAS
ÜBER EUROPÄISCHE LÖSUNGEN UND NATIONALE NOTWENDIGKEITEN

Über europäische Lösungen und nationale Notwendigkeiten

Wir leben in unruhigen Zeiten: Der Fall des mutmaßlichen Terroristen in Chemnitz am 10. Oktober hat einmal mehr daran erinnert, welche Gefahren mit der Zuwanderung verbunden sind.

Unsere Sicherheit und unsere Freiheit ziehen Menschen aus aller Herren Länder an, die unter Gewalt und Unfreiheit leiden; aber auch Menschen, die keinen Schutz suchen, sondern unsere Sicherheit und Freiheit bedrohen. Dagegen müssen wir uns schützen.

Europäische Gemeinsamkeiten

Der Wegfall der Grenzkontrollen im sogenannten Schengenraum ist ein Pfeiler der europäischen Integration. Doch er hat zwei Voraussetzungen: Kontrolle der Außengrenzen und enge Zusammenarbeit und Vernetzung aller Sicherheitsbehörden in Europa. Kroatien, Rumänien und Bulgarien warten noch auf den Beitritt zum Schengenraum, ihre Grenzen bilden aber teilweise bereits heute die EU-Außengrenze. Deshalb achten die Europäer schon jetzt darauf, dass dort aufmerksam kontrolliert wird.

Die sogenannte Dublin-III-Verordnung der EU regelt den Umgang mit Menschen, die als Bürgerkriegsflüchtlinge oder politisch Verfolgte zu uns kommen wollen. Klar ist: Sowohl Schengen als auch Dublin funktionieren nur, wenn an den Außengrenzen konsequent kontrolliert und registriert wird. Erfüllen die Grenzländer diese Verpflichtung nicht, bedroht das alle Europäer.

Grenzen des europäischen Grenzmanagements

Manche Länder machen ihre Arbeit: Spanien hat seit 2006 die Zahl der illegalen Migranten um drei Viertel reduziert, auch durch den massiven Ausbau der Grenzzäune an seinen Exklaven Ceuta und Melilla. Den ersten Zaun zwischen Ceuta und Marokko finanzierte übrigens 1993 größtenteils die EU. Auch Rumänien und Bulgarien sicherten nach dem EU-Beitritt 2007 ihre EU-Außengrenzen mit Zäunen. Dafür erhielten sie zwischen 2007 und 2009 von der EU aus der sogenannten „Schengen-Faszilität" rund 800 Mio. Euro.

Angesichts der stark wachsenden illegalen Migration errichtete Ungarn im Sommer 2015 einen Grenzzaun an seinem Abschnitt der EU-Außengrenze. Die den Ungarn dafür entgegenschlagende Kritik, vor allem von Brüsseler und Berliner Sozialdemokraten, war umso peinlicher als sie sachfremde, allgemeinpolitische Gründe hatte.

Zumal der Grund für den Anstieg der illegalen Migration nach Mitteleuropa in Griechenland lag: Griechenland (aber auch Italien) hatte jahrelang illegale Einwanderer unregistriert nach Norden weiterreisen lassen, v. a. nach Deutschland. Ein Verstoß gegen das Dublin-Abkommen, den die EU-Kommission nicht ahndete. Mit dem anschwellenden Flüchtlingsstrom aus Syrien und Nordafrika registrierten die Griechen Anfang 2015 gar nicht mehr. Nicht zu vergessen: Der griechische Verteidigungsminister Kammenos drohte im März 2015 mit der massenhaften Durchreise unkontrollierter Migranten, um Deutschland zu Nachgiebigkeit bei den griechischen Staatsschulden zu erpressen.

Nationale Entscheidungen

Weil Schengen also nicht mehr funktionierte, mussten die Nationalstaaten handeln: Schweden und (Stunden später) Dänemark führten Anfang Januar 2016 wieder konsequente Grenzkontrollen ein. Schon seit September 2015 kontrollierte auch Deutschland an der Grenze nach Österreich, allerdings ohne die konsequente Zurückweisung von Menschen, die offensichtlich kein Asyl in Deutschland erhalten können. Erst die Schließung der Balkanroute im März 2016 ließ die Migration nach Deutschland spürbar abebben. Fast zeitgleich wurde das Rücknahmeabkommen mit der Türkei abgeschlossen. In diesen Monaten wird sich zeigen, ob es tatsächlich funktioniert, da Griechenland die Türkei noch immer nicht als sicheres Herkunftsland anerkennt und mit der Abwicklung der Asylanträge offensichtlich überfordert ist.

Die österreichische Regierung beschloss im Januar 2016 eine jährliche Obergrenze von 37.500 Zuwanderern. Das Signal war deutlich: wir entscheiden, wer zu uns kommt und wer nicht. Unterstrichen wurde dieses Signal, indem österreichische Soldaten medienwirksam die Sperrung der Grenze zu Slowenien übten.

Was Deutschland braucht

Eine bürgerlich geführte Regierung darf keinen Zweifel daran lassen, dass sie die Kontrolle darüber ausübt, wer in unser Land kommt. Um verloren gegangenes Vertrauen zurück zu gewinnen, braucht es anhaltende, auch hartnäckige Führung in dieser Frage. Wir müssen unser nationales Recht wieder konsequent anwenden, also auch diejenigen zurückweisen, die offensichtlich kein Asyl in Deutschland erhalten können. Wer keine Papiere (mehr) hat, muss zur Klärung der Personalien an der Grenze festgehalten werden. Die CSU hat immer wieder Transitzonen gefordert. Wenn diese an der SPD scheitern, muss man die Forderung solange wiederholen, bis auch in der SPD die Ideologie der Realität weicht.

Selbstverständlich muss eine Regelabfrage aller Migranten bei den Sicherheitsbehörden sein. Wir haben an verschiedenen Stellen unseres Sicherheitsapparats Informationen, die Leben retten können. Darauf müssen unsere Grenzbehörden auch zugreifen (können).

Was Europa braucht

Europa arbeitet seit Jahren an einem besseren Grenzmanagement. Wir müssen rasch ein europäisches Ein- und Ausreisesystem nach dem Vorbild des amerikanischen ESTA organisieren. Unter dem Akronym ETIAS („EU Travel Information and Authorisation System") erarbeitet die EU-Kommission dafür derzeit Pläne. Auch hierzu muss eine Regelabfrage bei den Datenbanken der Sicherheitsbehörden gehören.

Der Migrationsdruck nach Europa wird auf Jahrzehnte hoch bleiben. Unsere Freiheit und unsere Sicherheit werden weiterhin viele, viele Menschen von unseren Nachbarkontinenten Asien und Afrika anziehen. Wir müssen den Menschen dort helfen, vor allem in Afrika. Hier kann die EU wertvolle Koordinierung leisten.

Bei uns geht es derweil um die grundsätzliche Frage: Sollen wir alle Menschen, die zu uns wollen, auch zu uns lassen, wie die politische Linke es will? Oder wollen wir Europäer unsere Freiheit und unsere Sicherheit verteidigen, indem wir die Kontrolle über unsere Grenzen selbst ausüben?

STANDPUNKTE: BRAUCHT DIE BUNDESWEHR OFFENSIVE CYBERFÄHIGKEITEN?

PRO

VON DR. REINHARD BRANDL MdB,
MITGLIED DES VERTEIDIGUNGSAUSSCHUSSES


Dr. Reinhard Brandl MdB

Der Schutz der eigenen Kommunikation sowie das Aufklären und Stören von gegnerischer Kommunikation ist seit der Zeit ihrer Gründung fester Bestandteil des Fähigkeitsspektrums der Bundeswehr („Elektronische Kampfführung"). In den vergangenen 60 Jahren haben sich die technischen Rahmenbedingungen und die Bedeutung dieser Fähigkeiten grundlegend verändert. Elektronische Kommunikationsmittel werden nicht mehr nur zur Verständigung zwischen Truppenteilen und zur Steuerung von konventionellen Waffensystemen eingesetzt, sondern sind zum eigenständigen Instrument zwischenstaatlicher Konflikte geworden. Der Cyberraum hat sich zu einem militärischen Operationsraum analog zu Land, See, Luft und Weltraum entwickelt. Jeder bewaffnete Konflikt – heute und in Zukunft – wird zumindest in Teilen auch über das Internet geführt werden. Die Abwehr von Cyber-Angriffen ist eine gesamtstaatliche Aufgabe. Dafür und für mögliche Auslandseinsätze muss die Bundeswehr geeignete Kapazitäten vorhalten. Wie in jedem anderen Operationsraum gehören dazu sowohl defensive als auch offensive Mittel. Da auch mögliche Gegner von Fähigkeiten und Ressourcen im Cyberraum abhängig sind, kann die Bundeswehr in Auslandseinsätzen und im Verteidigungsfall offensive Mittel einsetzen, um sie an der Nutzung dieser Fähigkeiten und Ressourcen zu hindern. Ein solcher Einsatz der Bundeswehr unterliegt dabei denselben rechtlichen Voraussetzungen wie jeder andere Einsatz deutscher Streitkräfte.

In Friedenszeiten ist es die vorrangige Aufgabe der Bundeswehr, sich selbst vor Cyber-Angriffen zu schützen. Als mittlerweile voll digitalisierte Großorganisation bietet sie zahllose mögliche Angriffspunkte und ist täglich mehr oder weniger professionellen Attacken ausgesetzt. Bereits eine kleine unentdeckte Schwachstelle kann es einem Angreifer ermöglichen, maximalen Schaden anzurichten. Für eine wirkungsvolle Cyberabwehr benötigt die Bundeswehr deshalb auch Personal, das sich aus der Perspektive von Angreifern intensiv mit Schwachstellen, Angriffsmethoden und -instrumenten beschäftigt.

Unsere zunehmend vernetzte Gesellschaft ist in hohem Maße auf die Verfügbarkeit, Integrität und Vertraulichkeit ihrer Informations- und Kommunikationsinfrastruktur angewiesen. Es liegt nicht in unserem Interesse, dass der Cyberraum sich mehr und mehr zu einem Feld entwickelt, auf dem zwischenstaatliche Konflikte ausgetragen werden. Die deutsche Außen- und Sicherheitspolitik ist auf allen Feldern dem Frieden verpflichtet. Das entbindet uns aber nicht von der Verantwortung, die Bundeswehr für den Ernstfall auszurüsten und die politische sowie militärische Handlungsfähigkeit in jeder Situation sicherzustellen.

CONTRA

VON DR. MARCEL DICKOW,
LEITER FORSCHUNGSGRUPPE SICHERHEITSPOLITIK, SWP


Dr. Marcel Dickow

Ist der Cyberspace die neue, fünfte Dimension des Krieges? Nicht nur das neue deutsche Weißbuch zur Sicherheitspolitik formuliert das so. Tatsächlich zeigen die millionenfachen und geradezu sekündlichen Angriffe im Netz, dass viele Akteure diese Einschätzung teilen. Müssen Deutschland und die Bundeswehr deswegen auch im Cyberspace aufrüsten? Es bestehen in meinen Augen erhebliche Zweifel.

Unzweifelhaft ist, dass die zivilen und militärischen Netze der Bundesrepublik geschützt und im Ernstfall auch verteidigt werden müssen. Doch sind dafür auch offensive Fähigkeiten nötig? Und sollten Cyberangriffe zu einem Bestandteil der regulären Kriegsführung werden, nicht nur im Bereich der Landes- und Bündnisverteidigung, sondern auch bei Auslandseinsätzen? Drei Beobachtungen aus jüngster Vergangenheit legen nahe, Zurückhaltung zu üben. Erstens, die Angriffe im Cyberspace funktionieren weitestgehend über das Ausnutzen von offenen Sicherheitslücken in Hard- und Software, sogenannte 0-day-Exploits. Wer angreifen will, muss diese Schwachstellen suchen oder das Wissen bei dubiosen Firmen einkaufen. Um im Ernstfall einen gezielten digitalen Angriff durchzuführen, muss das Zielsystem schon im Vorfeld infiltriert und ausgespäht werden, wozu der Vorrat an Exploits teilweise eingesetzt wird. Da wir hier in der Regel über Schwachstellen in Betriebssystemen und gängigen kommerziellen Anwendungen sprechen, werden diese nicht geschlossen sondern bleiben ein gefährliches Einfallstor für Dritte, und zwar auf allen Rechnern. Das Pflegen von Cyberangriffswaffen vergrößert also das Sicherheitsrisiko aller Computerbenutzer, weil Sicherheitslücken nicht geschlossen werden. Zweitens zeigt der Einsatz staatlicher Schadsoftware, dass Kriminelle, wie beim Fall Stuxnet, diesen hochentwickelten Code im Nachgang recyceln und dann millionenfach an private Benutzer verteilen. Selbst Nachrichtendienste können ihren digitalen Instrumentenkasten nicht garantiert geheim halten, wie die letzten Enthüllungen über die Spionagetools der NSA nahelegen. Drittens, kann Deutschland wohl kaum international glaubwürdig für Regulierung und Rüstungskontrolle im Cyberspace eintreten, wenn es selbst offensive Cyberfähigkeiten entwickelt. Die Stärke der normenbasierten Außenpolitik besteht eben gerade darin, gutes Verhalten vorzuleben und keine Doppelstandards aufzubauen.

Dies alles schließt nicht aus, dass ein guter Verteidiger die Techniken der Angreifer im Cyberraum studieren sollte. Die dabei entdeckten Sicherheitslücken sollten aber geschlossen werden, sonst gefährden wir weltweit die Sicherheit unserer Computer.

Impressum
Herausgeber: Arbeitskreis Außen- und Sicherheitspolitik (ASP) der CSU • **Konzept & Gestaltung:** IT'S LIVE! Advertising GmbH
Redaktion: ASP-Landesgeschäftsführer Peter Rief, M. A. • **Kontakt Redaktion:** asp@csu-bayern.de • **Stand:** November 2016
Hinweis: Die Beiträge in dieser Zeitschrift geben die Meinung des Verfassers, nicht aber die der Redaktion oder des ASP wieder.