Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Verwaltungspraxis der Bundesbehörden VPB
Jurisprudence des autorités administratives de la Confédération JAAC
Giurisprudenza delle autorità amministrative della Confederazione GAAC

VPB 3/2009 vom 2. September 2009

2009.10a (S. 141-177)

Gutachten über Rechtsgrundlagen für Computernetzwerkoperationen durch Dienststellen des VBS

EJPD, Bundesamt für Justiz und EDA, Direktion für Völkerrecht

Gutachten vom 10. März 2009

Stichwörter: Computernetzwerkoperationen, Nachrichtendienst, CND, CNE, CNA, Privatsphäre, ius ad bellum, ius contra bellum, Cyber-Kriminalität.

Mots clés: Opérations dans les réseaux informatiques, service de renseignements, CND, CNE, CNA, sphère privée, ius ad bellum, ius contra bellum, cybercriminalié**.**

Termini chiave: Operazioni nelle reti informatiche, servizio informazioni, CND, CNE, CNA, sfera privata, ius ad bellum, ius contra bellum, cibercriminalità.

Regeste:
Die heutigen Rechtsgrundlagen genügen für nicht-aggressive Computer Network Defense (CND). Computer Network Exploitation (CNE) und Computer Network Attack (CNA) sind heute nur im Aktivdienst möglich. Für die anderen Einsatzarten bestehen keine gesetzlichen Grundlagen. Da CNA nur im Aktivdienst durchgeführt werden soll, ist keine formell-gesetzliche Grundlage notwendig. Will man CNE betreiben, bedingt dies eine formell-gesetzliche Grundlage. Die bestehende Rechtsgrundlage für den Nachrichtendienst (Art. 99 MG) erlaubt keine Informationsbeschaffung mittels CNE.

Regeste:
Les bases légales actuelles sont suffisantes pour justifier les mesures non-agressives de défense de réseaux informatiques (Computer Network Defense, CND). Les mesures d'exploitation de réseaux informatiques (Computer Network Exploitation, CNE) et les attaques de réseaux informatiques (Computer Network Attack, CNA) sont aujourd'hui possibles dans le cadre du service actif. Comme une CNA ne peut être effectuée que dans le cadre du service actif,une base légale expresse n'est nécessaire. Pour procéder à des CNE, une base légale formelle est toutefois requise. La base légale sur laquelle se fonde actuellement le service de renseignements (art. 99 LAAM) ne permet pas la recherche des informations par le biais de CNE.

Regesto:
Le basi legali attuali sono sufficienti per giustificare le misure non aggressive di difesa delle reti informatiche (Computer Network Defense, CND). Oggi le misure di gestione delle reti informatiche (Computer Network Exploitation, CNE) e gli attacchi alle reti informatiche (Computer Network Attack, CNA) sono possibili solo nell'ambito di un servizio attivo. Siccome gli CNA possono essere effettuati solo nell'ambito del servizio attivo, non è necessaria una base legale formale. Per gestire una CNE, è indispensabile una base legale formale. La base legale attuale per il servizio informazioni (art. 99 LM) non permette la ricerca di informazioni mediante la CNE.

Rechtliche Grundlagen:
Art. 5, Art. 13, Art. 16, Art. 36, Art. 58 Abs. 2; Art. 173 Abs. 1, Art. 185 Abs. 4 BV (SR 101);
Art. 8, Art. 10, Art. 13 Konvention vom 4. November 1950 zum Schutze der Menschenrechte und Grundfreiheiten (EMRK; SR 0.101);

Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997 (RVOG; SR 172.010);
Verordnung vom 26. September 2003 über die Informatik und Telekommunikation in der Bundesverwaltung (Bundesinformatikverordnung, BinfV; SR 172.010.58);
Organisationsverordnung vom 7. März 2003 für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (OV-VBS; SR 172.214.1);
Art. 1, Art. 65, Art. 66, Art. 66b, Art. 70, Art. 99, Art. 100 Abs. 1 lit. b Bundesgesetz vom 3. Februar 1995 über die Armee und die Militärverwaltung (Militärgesetz, MG; SR 510.10);
Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit (BWIS ; SR 120);
Verordnung vom 10. Juni 1996 über die Mobilmachung (VMobSR; 519.1);
Verordnung vom 2. Dezember 2005 über das Personal für die Friedensförderung, die Stärkung der Menschenrechte und die humanitäre Hilfe (PVFMH; SR 172.220.111.9);
Departementsverordnung vom 26. Februar 1997 über den Friedensförderungsdienst (SR 172.220.111.91);
Verordnung vom 3. September 1997 über den Truppeneinsatz zum Schutz von Personen und Sachen (VSPS; SR 513.73);
Verordnung vom 3. Mai 2006 über den Truppeneinsatz zum Schutz von Personen und Sachen im Ausland (VSPA; SR 519.4);
Verordnung vom 8. Dezember 1997 über den Einsatz militärischer Mittel für zivile und ausserdienstliche Tätigkeiten (VEMZ; SR 510.212);
Verordnung vom 29. Oktober 2003 über die militärische Katastrophenhilfe im Inland (VmKI; SR 510.213);
Verordnung vom 15. Oktober 2003 über die elektronische Kriegführung (VEKF; SR 510.292);
Verordnung vom 15. September 1997 über die Informatik im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (Informatikverordnung VBS; SR 510.211.2).

Base juridique:
Art. 5, art. 13, art. 16, art. 36, art. 58 al. 2; art. 173 al. 1, art. 185 al. 4 Cst. (RS 101);
Art. 8, art. 10, art. 13 de la Convention du 4 novembre 1950 de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH; RS 0.101);
Loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA; RS 172.010);
Ordonnance du 26 septembre 2003 sur l'informatique et la télécommunication dans l'administration fédérale (Ordonnance sur l'informatique dans l'administration fédérale, OIAF; RS 172.010.58);
Ordonnance du 7 mars 2003 sur l'organisation du Département fédéral de la défense, de la protection de la population et des sports (Org-DDPS; RS 172.214.1);
Art. 1, art. 65, art. 66, art. 66b, art. 70, art. 99, art. 100 al. 1 let. b de la loi fédérale du 3 février 1995 sur l'armée et l'administration militaire (LAAM; RS 510.10);
Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI; RS 120);
Ordonnance du 10 juin 1996 concernant la mobilisation (OMob; RS 519.1);
Ordonnance du 2 décembre 2005 sur le personnel affecté à la promotion de la paix, au renforcement des droits de l'homme et à l'aide humanitaire (OPers-PDHH; RS 172.220.111.9);
Ordonnance du 26 février 1997 sur le service de promotion de la paix (RS 172.220.111.91);
Ordonnance du 3 septembre 1997 sur le recours à la troupe pour assurer la protection de personnes et de biens (OPPB; RS 513.73);
Ordonnance du 3 mai 2006 concernant l'engagement de la troupe pour la protection de personnes et de biens à l'étranger (OPPBE; RS 519.4);
Ordonnance du 8 décembre 1997 réglant l'engagement de moyens militaires dans le cadre d'activités civiles et d'activités hors du service (OEMC; RS 510.212);
Ordonnance du 29 octobre 2003 sur l'aide militaire en cas de catastrophe dans le pays (OAMC; RS 510.213);
Ordonnance du 15 octobre 2003 sur la guerre électronique (OGE; RS 510.292);
Ordonnance du 15 septembre 1997 concernant l'informatique au Département fédéral de la défense, de la protection de la population et des sports (Ordonnance INF DDPS; RS 510.211.2).

Basi legali:
Art. 5, art. 13, art. 16, art. 36, art. 58 cpv. 2; art. 173 cpv. 1, art. 185 cpv. 4 Cost. (RS 101);
Art. 8, art. 10, art. 13 Convenzione del 4 novembre 1950 de per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU; RS 0.101);
Legge del 21 marzo 1997 sull'organisazione del Governo e dell'Amministrazione (LOGA; RS 172.010);
Ordinanza del 26 settembre 2003 concernente l'informatica e la telecomunicazione nell'Amministrazione federale (Ordinazia sull'informatica nell'Amministrazione federale, OIAF; RS 172.010.58);

Ordinanza del 7 marzo 2003 sull'organisazione del Dipartimento federale della difesa, della protezione della popolazione e dello sport (OOrg-DDPS; RS 172.214.1);
Art. 1, art. 65, art. 66, art. 66b, art. 70, art. 99, art. 100 al. 1 let. b Legge frderale del 3 febbraio 1995 sull'esercito e sull'amministrazione militare (Legge militare, LM; RS 510.10);
Legge federale del 21 marzo 1997 sulle misure per la salvaguardia della sicurezza interna (LMSI; RS 120);
Ordinanza del 10 giugno 1996 concernente la mobilitazione (OMob; RS 519.1);
Ordinanza del 2 dicembre 2005 sul personale impiegato per la promozione della pace, il rafforzamento dei diritti dell'uomo e l'aiuto umanitario (OPers-PRA; RS 172.220.111.9);
Ordinanza del 26 febbraio 1997 sul servizio di promovimento della pace (RS 172.220.111.91);
Ordinanza del 3 settembre 1997 sull'impiego della truppa per la protezione di persone e di beni (OPPB; RS 513.73);
Ordinanza del 3 maggio 2006 concernente l'impiego di truppe per la protezione die persone e beni all'estero (OPBE; RS 519.4);
Ordinanza del 8 dicembre 1997 cencernente l'impiego di mezzi militari a favore di attività civili e attività fuori del servizio (OIMC; RS 510.212);
Ordinanza del 29 ottobre 2003 sull'aiuto militare in cado di catastrofe in Svizzera (OAMC; RS 510.213);
Ordinanza del 15 ottobre 2003 concernente la guerra elettronica (OGEL; RS 510.292);
Ordinanza del 15 settembre 1997 concernente l'informatica nel Dipartimento della difesa, della protezione della popolazione e dello sport (Ordinanza INF DDPS; RS 510.211.2).

Inhaltsverzeichnis

Verzeichnis der wichtigsten Abkürzungen

CNA	computer network attack
CND	computer network defense
CNE	computer network exploitation
CNO	computer network operations
DAP	Dienst für Analyse und Prävention (VBS)
EW	Electronic Warfare
FUB	Führungsunterstützungsbasis, Bundesamt
InfoOps	Informationsoperationen
MILDEC	Military Deception
Op Info Fhr	operationelle Informationsführung
OPSEC	Operations Security
PSYOPS	Psychological Operations

Die Geschäftsprüfungsdelegation (GPDel) stellte dem Bundesamt für Justiz sowie der Direktion für Völkerrecht die folgenden Fragen, welche im vorliegenden gemeinsamen Gutachten beantwortet werden:

1. *Genügen die heutigen Rechtsgrundlagen für Computer Network Defense (CND)?*
2. *Welche Rechtsgrundlagen erlauben Computer Network Exploitation (CNE) und Computer Network Attack (CNA) durch Dienststellen des VBS? Im Rahmen welcher Einsatzarten der Armee sind heute CNE und CNA möglich?*
3. *Wie verhalten sich die bestehenden Rechtsgrundlagen für den Nachrichtendienst (Art. 99 MG) zu allfälligen Rechtsgrundlagen für InfoOps der Armee, insbesondere die Informationsbeschaffung mittels CNE?*
4. *Welche Konsequenzen hätte die Annahme des neuen Art. 18m BWIS (Geheimes Durchsuchen eines Datenverarbeitungssystems) auf die Arbeiten im Bereich CNE und CNA im VBS?*

Das Gutachten ist wie folgt gegliedert: Nach einer gründlichen Skizzierung der Ausgangslage wird analysiert, inwieweit für die CNO gesetzliche Grundlagen bestehen müssen. Dabei stellen sich in erster Linie für CNE Rechtsfragen (siehe Teil 2.2). Daran anschliessend werden die völkerrechtlichen Vorgaben für CNO eingehend dargestellt. Dieser Teil ist v.a. für CNA relevant (siehe Teil 3.).

1. Ausgangslage

1.1. Begriffe

InfoOps, Information Operations, sind sämtliche Aktionen von Op Info Fhr, EW, CNO, MILDEC und OPSEC, mit dem Ziel die Entscheidfindungsprozesse eines Gegners zu beeinflussen, zu stören, zu verschlechtern oder zu missbrauchen und die eigenen Prozesse zu schützen[1].

Gemäss der vom VBS vorgelegten schweizerischen Definition umfassen CNO folgende militärische Aktionen in oder mittels Computer-Netzwerken: CND: Massnahmen zur Überwachung und zum Schutz von eigenen Datenverarbeitungsanlagen; CNE: Massnahmen, mit denen sich in fremden Datenverarbeitungsanlagen befindende Daten ermittelt werden; CNA: Massnahmen, mit welchen die Integrität und Verfügbarkeit von Datenverarbeitungsanlagen und der darin befindlichen Daten beeinträchtigt werden.

Die drei Hauptgruppen von CNO werden nachfolgend erläutert. Die im Anhang abgedruckte Grafik 1 (CNO) soll die Schwierigkeiten der exakten Abgrenzung der drei Arten und der dazwischen existierenden Graubereiche verdeutlichen. Zumindest in Bezug auf CNE und CNA kann dies die Verwischung der Grenze zwischen Krieg und Frieden bedeuten[2].

Die Graubereiche werden in diesem Gutachten für die nationalen Rechtsgrundlagen zur jeweils stärkeren Stufe CNE bzw. CNA gerechnet. Beispielsweise fallen defensive Gegenattacken im Rahmen von CND bereits unter CNA.

CND ist die Sicherung von in erster Linie militärischen Netzwerken (z.B. Waffensystemen) und deren Inhalte durch präventive Massnahmen, frühe Feststellung von allfälligen Angriffen und Bereitstellung von Gegenmassnahmen im Falle von Angriffen. CND überschreitet die Grenze von reiner Abwehr im Falle des tatsächlichen Ergreifens von Gegenmassnahmen bzw. Gegenattacken (CNA); ebenso wird die Grenze von reiner Abwehr im Falle des aktiven Sammelns von Informationen über die Angreifer überschritten (CNE)[3]. CND als reine Abwehr von Gefahren unterscheidet sich nach diesem Verständnis nicht wesentlich von einer im privaten und öffentlichen Bereich praktizierten üblichen Informatiksicherheit. CND wird bereits heute durch die Führungsunterstützungsbasis FUB praktiziert[4].

CNE sind Massnahmen die unter Ausnutzung von Computernetzwerken das Sammeln von Informationen von bzw. in gegnerischen Computern und Computernetzwerken ermöglichen, ohne Inhalte und Zustand des Systems zu ändern. Zu CNE wird in diesem Gutachten auch CND-basiertes, aktives Sammeln von Informationen über gegnerische Fähigkeiten gezählt[5]. CNE wird nach Auskunft des VBS heute von Schweizer Stellen nicht betrieben. Dem Charakter nach handelt es sich um eine nachrichtendienstliche Tätigkeit gegen in erster Linie andere Armeen bzw. Staaten.

[1] Op Info Fhr: operationelle Informationsführung (international spricht man von PSYOPS, Psychological Operations); EW: Electronic Warfare; CNO: Computer Network Operations; MILDEC: Military Deception; OPSEC: Operations Security.

[2] Mehr dazu unter 3.2.1.

[3] In der Grafik 1 (CNO) im Anhang sind dies die grau dargestellten Bereiche – diese sind jeweils zur nächststärkeren Stufe CNE bzw. CNA zuzurechnen.

[4] Vgl. die Präsentation vom 8. März 2008 anlässlich der Jahresversammlung der Schweizerischen Offiziersgesellschaft Führungsunterstützung von Div. K. Nydegger, Chef Führungsunterstützungsbasis FUB, Folien 18 ff.

[5] Siehe Grafik 1 (CNO) im Anhang und den Grundsatz in Fn.3.

Um ein konkretes Beispiel für den Bedarf an CNE zu geben, sei auf das Programm Skype verwiesen. Skype ermöglicht das Führen kostenloser Gespräche mit anderen Skype-Teilnehmerinnen und -teilnehmern über das Internet. Aufgrund der Verschlüsselung wäre ein Abhören nach derzeitigem Wissensstand nur mittels Trojanern in den betroffenen Computern möglich.

CNA sind Massnahmen, die unter Anwendung von Computernetzwerken dazu dienen, den Zugriff auf Informationen in Computern oder Computernetzwerken zu stören, zu verhindern, zu verlangsamen oder die Information, die dazugehörigen Computernetzwerke oder die dazugehörigen Computer zu zerstören. Zu CNA werden in diesem Gutachten auch agressives CNE sowie defensive Gegenattacken gezählt[6]. CNA wird nach Auskunft des VBS heute von Schweizer Stellen nicht betrieben.

1.2. Einsatzarten der Armee

Die Armee wird gemäss Art. 65 MG für Friedensförderungsdienst, Assistenzdienst und Aktivdienst eingesetzt[7]. Nachfolgend seien die drei Einsatzarten der Armee kurz erläutert.

Einsätze zur Friedensförderung können auf der Grundlage eines UNO- oder OSZE-Mandates angeordnet werden (Art. 66 Abs. 1 MG)[8]. Friedensförderungsdienst wird von schweizerischen Personen oder Truppen geleistet, die eigens dafür ausgebildet sind (Art. 66 Abs. 2 MG). Zuständig für die Anordnung eines Friedensförderungseinsatzes ist der Bundesrat. Allerdings ist ein Friedensförderungseinsatz von der Bundesversammlung zu genehmigen, wenn er bewaffnet und mit mehr als 100 Armeeangehörigen erfolgen oder der Einsatz länger als drei Wochen dauern soll (Art. 66*b* MG).

Die Armee unterstützt gemäss Art. 1 Abs. 3 MG die zivilen Behörden, wenn deren Mittel nicht mehr ausreichen bei der Abwehr von schwer wiegenden Bedrohungen der inneren Sicherheit und bei der Bewältigung von anderen ausserordentlichen Lagen, insbesondere im Falle von Katastrophen im In- und Ausland (Assistenzdienst)[9]. Art. 58 Abs. 2 BV beschränkt die mögliche Hilfestellung der Armee jedoch auf zivile Behörden, die im Bereich der Abwehr schwerwiegender Bedrohungen der inneren Sicherheit und bei der Bewältigung anderer ausserordentlicher Lagen tätig sind. Art. 1 Abs. 3 MG ist an der Verfassungsvorgabe zu messen, wenn er der Armee die Aufgabe zuweist, die zivilen Behörden zu unterstützen, wenn deren Mittel nicht mehr ausreichen, bei der Abwehr von schwer wiegenden Bedrohungen der inneren Sicherheit und/oder bei der Bewältigung von anderen ausserordentlichen Lagen, insbesondere im Falle von Katastrophen im In- und Ausland. Es fallen damit nur solche Bundesbehörden unter den Begriff der zivilen Behörden nach Art. 58 Abs. 2 BV, die im Bereich der Abwehr schwerwiegender Bedrohungen der inneren Sicherheit und bei der Bewältigung anderer ausserordentlicher Lagen tätig sind.

[6] Siehe Grafik 1 (CNO) im Anhang und den Grundsatz in Fn.3.

[7] Vgl. hierzu PATRICK SUTTER, Recht der militärischen Operationen, in: Sicherheit & Recht 1 (2008) 19.

[8] Siehe auch die Bundesratsverordnung vom 2. Dezember 2005 über das Personal für die Friedensförderung, die Stärkung der Menschenrechte und die humanitäre Hilfe (PVFMH), SR 172.220.111.9, sowie die Departementsverordnung vom 26. Februar 1997 über den Friedensförderungsdienst, SR 172.221.104.41.

[9] Vgl. hierzu Verordnung vom 3. September 1997 über den Truppeneinsatz zum Schutz von Personen und Sachen (VSPS), SR 513.73; Verordnung vom 3. Mai 2006 über den Truppeneinsatz zum Schutz von Personen und Sachen im Ausland (VSPA), SR 519.4; Verordnung vom 8. Dezember 1997 über den Einsatz militärischer Mittel für zivile und ausserdienstliche Tätigkeiten (VEMZ), SR 510.212; Verordnung vom 29. Oktober 2003 über die militärische Katastrophenhilfe im Inland (VmKI), SR 510.213.

Zusätzlich ist gemäss Art. 58 BV für einen Einsatz der Armee immer dessen Subsidiarität zu beachten[10]. Daueraufgaben sind von den Polizeikräften ohne Beizug der Armee zu erfüllen[11].

Zuständig für das Aufgebot zum Assistenzdienst ist der Bundesrat bzw. das VBS bei Katastrophen im Inland. Allerdings ist ein Assistenzdienst von der Bundesversammlung zu genehmigen, wenn er länger als drei Wochen dauern soll (Art. 70 MG).

Aktivdienst wird geleistet, um die Schweiz und ihre Bevölkerung zu verteidigen (Landesverteidigungsdienst), die zivilen Behörden bei der Abwehr von schwerwiegenden Bedrohungen der inneren Sicherheit zu unterstützen (Ordnungsdienst) sowie bei steigender Bedrohung den Ausbildungsstand der Armee zu erhöhen[12].

Zuständig für die Anordnung von Aktivdienst ist gemäss Art. 173 Abs. 1 BV die Bundesversammlung; nur in dringenden Fällen liegt diese Zuständigkeit beim Bundesrat, der aber die Bundesversammlung einzuberufen hat, wenn für den Einsatz mehr als 4'000 Armeeangehörige aufgeboten werden oder ein Einsatz voraussichtlich länger als drei Wochen dauern wird (Art. 185 Abs. 4 BV).

1.3. Organisatorisches

Für die einzelnen Arten von CNO kommen nicht alle der dargestellten Einsatzarten in Frage. Gleichzeitig gehen wir davon aus, dass Ausbildungsdienst (Art. 41 ff. MG) für CNO nur dann zulässig ist, wenn eine entsprechende gesetzliche Grundlage vorliegt.

Für CND ist keine der Einsatzarten nach Art. 65 MG notwendig in dem Sinne, dass CND sonst nicht ausgeführt werden könnte. Vielmehr handelt es sich darum, dass CND das Funktionieren von Waffensystemen und Netzwerken der Armee fortlaufend sicherstellt; es ist damit systemimmanent notwendig.

Für CNE sind – eine gesetzliche Grundlage vorbehalten – zum heutigen Stand ebenfalls keine der drei Einsatzarten konstitutiv; hingegen kann nicht ausgeschlossen werden, dass bei Friedensförderungsdienst und Assistenzdienst Massnahmen im Rahmen von CND und CNE ergriffen werden.

Für CNA und die damit verbundenen Graubereiche kommt – jedenfalls sobald die Schwelle zu einem bewaffneten Angriff überschritten wird[13] – nur Aktivdienst in Frage; unter dieser Einsatzart erscheinen alle der drei Arten von CNO grundsätzlich zulässig[14]; siehe dazu Grafik 2 (Einsatz der Armee für CNA) im Anhang.

Im Fall eines bewaffneten Konflikts gelten für alle Arten von CNO die Regeln des Völkerrechts (*ius ad bellum*, Neutralitätsrecht, *ius in bello*)[15].

Es besteht ausserhalb des Aktivdienstes keine gesetzliche Grundlage für CNA.

Wir gehen davon aus, dass CNA nur im Falle eines Krieges – und zwar durch die Armee – zur Anwendung gelangen soll. Damit erübrigt sich die Schaffung einer gesetzlichen Grundlage für Friedenszeiten. Dies beinhaltet die Entwicklung von entsprechenden Kapazitäten durch die FUB.

---

[10] HANSJÖRG MEYER in: Die Schweizerische Bundesverfassung. Kommentar, 2. Auflage, Zürich/St. Gallen 2008 (St. Galler Kommentar), ART. 58, RZ. 16 *in fine*.

[11] SUTTER (Fn. 7), 28.

[12] Art. 76 MG. Siehe auch Verordnung vom 10. Juni 1996 über die Mobilmachung (VMob), SR 519.1.

[13] Dazu mehr unter 3.2.2.1. ff.

[14] Vgl. Art. 36 Abs. 1 BV, wonach in Fällen ernster, unmittelbarer und nicht anders abwendbarer Gefahr, Einschränkungen von Grundrechten ohne gesetzliche Grundlage möglich sind. Siehe RAINER J. SCHWEIZER, in: St. Galler Kommentar (Rz. 10), Art. 36, Rz. 17 mit Hinweisen.

[15] Dazu mehr unter 3.

Neu soll die FUB die drei Arten der CNO, nämlich CND, CNE und CNA, durchführen (können).

Die FUB[16] hat die Aufgabe, im Rahmen des allgemeinen Auftrags der Armee deren computergestützten bzw. elektronischen Führungssysteme sicherzustellen[17]. Die Armee kann aufgrund eines entsprechenden (zeitlich begrenzten) Auftrags in ihren verschiedenen Einsatzarten Aufklärungs- und Störsysteme im In- und Ausland einsetzen. Die FUB ist für die Beschaffung (zusammen mit armasuisse) und Einführung der entsprechenden (taktisch/operativen) Systeme bei der Truppe zuständig.

Bereits heute wird von Bediensteten der FUB die ständige Funkaufklärung permanent betrieben[18]. Sie erfasst militärische und zivile Ausstrahlungen von Antennen, Satelliten und dergleichen aus dem Ausland. Sie kann diese Ausstrahlungen wenn dies gewünscht wird als Einzelinformationen identifizierbar und lesbar machen. Das wichtigste Instrument dafür ist derzeit das System ONYX, das sich hauptsächlich auf zivile Satellitenverbindungen richtet und das im Rahmen der ständigen Funkaufklärung betrieben wird[19]. Die so gewonnenen Informationen werden nach heutiger Praxis den Auftraggebern im Sicherheitsbereich des Bundes zur Auswertung weitergegeben. Die Erfassung und Weitergabe erfolgt im Rahmen entsprechender Leistungsvereinbarungen mit diesen Dienststellen[20]. Die FUB nimmt die dem Auftrag entsprechende Triage und Klassifizierung der einzelnen Informationen vor; es identifiziert ferner in eigener Kompetenz sogenannte Zufallsfunde und leitet diese an die zuständigen Dienststellen weiter[21]. Unmittelbare Auftraggeber sind derzeit der Strategische Nachrichtendienst (SND) des VBS, der Militärische Nachrichtendienst (MND) im Führungsstab der Armee sowie der Dienst für Analyse und Prävention (DAP) des Bundesamtes für Polizei (FEDPOL)[22]. Informationen aus der ständigen Funkaufklärung können zudem über die unmittelbaren Auftraggeber im Rahmen von beschränkten Leistungsaufträgen anderen Dienststellen (z.B. der Nationalen Alarmzentrale) zur Verfügung gestellt werden. Die Auswertung und allfällige Weiterverbreitung der Informationen erfolgt ausschliesslich durch die Auftraggeber und im Rahmen der für ihre Tätigkeit massgebenden Rechtsgrundlagen.

Im Auftrag der GPDel reichte ihr Präsident, Ständerat Hans Hofmann, am 13. März 2007 die Parlamentarische Initiative mit dem Titel «Übertragung der Aufgaben der zivilen Nachrichtendienste an ein Departement» (Pa. Iv. 07.404) ein. Die GPDel wurde mit der Ausarbeitung eines Gesetzesentwurfs beauftragt, welchen diese im Feb-

[16] Die FUB ist das Ergebnis einer Fusion der Untergruppe Führungsunterstützung (UGFU) und der Direktion Informatik VBS (DIK VBS). Im Dezember 2004 als Bundesamt formiert, ist die FUB auch für das nationale Krisenmanagement verantwortlich, zudem ist sie Informatik-Leistungserbringer des VBS. In der FUB sind zur Zeit ca. 660 Mitarbeitende an 15 Standorten in der Schweiz beschäftigt.

[17] Art. 11 lit. h OV-VBS vom 7. März 2003, SR 172.214.1.

[18] Rechtliche Grundlage hierzu bildet die Verordnung über die elektronische Kriegführung (VEKF) vom 15. Oktober 2003, SR 510.292.

[19] Siehe hierzu den Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte vom 10. November 2003 zum Satellitenaufklärungssystem des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (Projekt «Onyx»), BBl 2004, 1499; Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte vom 9. November 2007 über die Rechtmässigkeit und Wirksamkeit des Funkaufklärungssystems «Onyx», BBl 2008, 2545.

[20] Art. 3 Abs. 3 VEKF.

[21] Art. 5 Abs. 3 VEKF.

[22] Der Bundesrat hat am 21. Mai 2008 in Wahrnehmung seiner Organisationsautonomie betreffend die Bundesverwaltung (Art. 8 Abs. 1 RVOG; SR 172.010) beschlossen, dass der DAP auf den 1. Januar 2009 zum VBS transferiert werden soll. Das Bundesgesetz über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (ZNDG) vom 3. Oktober 2008 sieht seinerseits die Unterstellung des DAP und des SND unter dasselbe Departement vor; Ablauf der Referendumsfrist für dieses Gesetz: 22. Januar 2009; BBl 2008, 8249. Siehe auch Parlamentarische Initiative Übertragung der Aufgaben der zivilen Nachrichtendienste an ein Departement Bericht der Geschäftsprüfungskommission des Ständerats vom 29. Februar 2008, BBl 2008, 4015; Stellungnahme des Bundesrates vom 23. April 2008, BBl 2008, 4035. Zum Zeitpunkt der Fertigstellung dieses Gutachtens wurde an einer Zusatzbotschaft (BWIS II) gearbeitet, um materielle und gesetzestechnische Abstimmungsprobleme mit der Botschaft vom 15. Juni 2007 betreffend die Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit aus dem Weg zu räumen; siehe dazu mehr unter 2.2.5.

ruar 2008 vorlegte[23]. Die Inkraftsetzung ist für 2009 geplant. Die vorgeschlagenen Gesetzesänderungen haben im Wesentlichen organisatorischen Charakter und sollen die angestrebte Unterstellung der zivilen Nachrichtendienste unter ein Departement ermöglichen. Dies bedingt einerseits eine Herauslösung des SND als zivilen Dienst aus dem Bereich des Militärgesetzes und die Schaffung einer entsprechenden spezialgesetzlichen Grundlage für die zivile Auslandaufklärung. Andererseits muss durch eine Anpassung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit dafür gesorgt werden, dass der DAP für die Wahrnehmung der nachrichtendienstlichen Aufgaben nach diesem Gesetz nicht von Gesetzes wegen Teil des Justiz- und Polizeidepartements sein muss.

Daneben besteht im Führungsstab der Armee ein Bereich Informationsoperationen. Dieser Bereich stellt die Abwehrmassnahmen in der Informationsdimension militärischer Operationen sicher. Er ist für die gesamte Operationslinie zuständig (Operationen, Ausbildung und Weiterentwicklung) und somit Vorgabestelle der Armee in diesem Bereich.

2. Gesetzliche Grundlagen für CNO

2.1. Gesetzliche Grundlage für CND

In der Notiz Recht Verteidigung / Recht VBS vom 19. Februar 2008 wird als rechtliche Abstützung für CND das Militärgesetz „im weitesten Sinne“ sowie die Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (Bundesinformatikverordnung, BinfV) vom 26. September 2003[24] genannt.

Die angeführte BinfV hält in Art. 2 Abs. 3 fest, dass die Informatikvorgaben nach dieser Verordnung nicht für die Informatik der Waffensysteme und nicht für die Führungs- und Einsatzsysteme der Armee Geltung besitzen.

Die Verordnung über die Informatik im Eidgenössischen Departement für Verteidigung[25] (Informatikverordnung VBS) vom 15. September 1997[26], verweist in Art. 9 (Sicherheit) auf die BinfV, ist also (auch) nicht einschlägig.

Die Verordnung über die elektronische Kriegführung (VEKF) vom 15. Oktober 2003[27] umfasst zwar nach Art. 1 Abs. 1 auch die „elektronische Kriegsführung“, worunter CNO fallen könnte, doch ist der eigentliche Hauptgegenstand der VEKF die „ständige Funkaufklärung“. Mithin finden sich in der VEKF keine expliziten Bestimmungen zu CND bzw. CNE oder CNA.

Die Armee hat mit Art. 1 Abs. 2 MG den Auftrag, die Schweiz und ihre Bevölkerung zu verteidigen. Gemäss Art. 92 stehen der Truppe im Einsatz die Polizeibefugnisse zu, die zur Erfüllung ihrer Aufgaben erforderlich sind. Eine dieser Aufgaben wird in Art. 100 Abs. 1 lit. b MG näher beschrieben: Der Dienst der militärischen Sicherheit (Mil Sich) soll für die Informatiksicherheit sorgen. Nach unserem Verständnis von CND besteht damit eine genügende gesetzliche Grundlage für CND durch die Mil Sich. Kraft seiner Organisationsautonomie[28] steht es dem Bundesrat bzw. dem zuständigen Departementschef frei, eine andere Einheit innerhalb des Departements zusätzlich mit der Informatiksicherheit zu betreuen. Ausgeschlossen wäre dies nur

[23] Bundesgesetz über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (ZNDG) vom 3. Oktober 2008.

[24] SR 172.010.58.

[25] Der nicht fertiggeschriebene Titel in der Systematischen Sammlung (SR) sollte bei Gelegenheit vervollständigt werden.

[26] SR 510.211.2.

[27] SR 510.292.

[28] Art. 8 RVOG.

dann, wenn die Bundesversammlung die Organisationskompetenz des Bundesrates ausdrücklich eingeschränkt hätte, wofür es vorliegend keine Anzeichen gibt.

2.2. Rahmenbedingungen für CNE im innerstaatlichen Recht

2.2.1. Grundsätze rechtsstaatlichen Handelns und Bundeszuständigkeit

2.2.1.1. Vorgaben der Bundesverfassung

Jedes staatliche Handeln hat sich an Art. 5 BV[29] auszurichten. Die Grundsätze der Rechtmässigkeit, der Verpflichtung auf das öffentliche Interesse und der Verhältnismässigkeit des Handelns gelten für alle staatlichen Organe und alle staatlichen Tätigkeitsbereiche[30]. Für das Handeln des Bundes kommt hinzu, dass er, anders als die Kantone, dafür eine spezifische (ausdrückliche oder inhärente) Kompetenzzuweisung auf Verfassungsebene benötigt[31]. Auf die vorliegende Situation bezogen heisst das, dass die Tätigkeit der Armee einer Rechtsgrundlage bedarf, im Rahmen der grundrechtlichen Vorgaben erfolgen muss, nicht gegen das Völkerrecht verstossen darf, einem öffentlichen Interesse entsprechen muss, verhältnismässig sein muss und sich im Rahmen einer Sachzuständigkeit des Bundes zu bewegen hat.
Da die Bundeszuständigkeit im vorliegenden Fall (Landesverteidigung und äussere Sicherheit) unbestritten ist[32], wird darauf in der Folge nicht näher eingegangen.

2.2.1.2 Räumlicher Geltungsbereich der verfassungsrechtlichen Vorgaben

Art. 5 BV ist vorliegend insoweit von Bedeutung, als er das Handeln schweizerischer staatlicher Organe generell erfasst. Dass sich ein Teil der CNO – insbesondere CNE und CNA – technisch gesehen ausserhalb des Hoheitsgebietes der Schweiz abspielt[33], hat auf die Verpflichtung der damit betrauten staatlichen Organe durch die Verfassungsgrundsätze keinen Einfluss[34]. Einerseits haben sie ihren Sitz auf schweizerischem Hoheitsgebiet, sind von hier aus tätig und unterstehen damit schweizerischem Recht. Andererseits sind sie als Organe der Eidgenossenschaft tätig und dabei durch die Verfassung verpflichtet, unabhängig davon, wo ihre Tätigkeit sich abspielt oder auswirkt.

2.2.1.3. Grundrechtliches

2.2.1.3.1. Allgemeines

Die Anwendungsbereiche von CNO (Eindringen in Computer-Netzwerke) betreffen in erster Linie zwei von der Verfassung garantierte Grundrechtsbereiche von Bedeu-

[29] Die Bestimmung lautet:

Art. 5 Grundsätze rechtsstaatlichen Handelns

[1] Grundlage und Schranke staatlichen Handelns ist das Recht.

[2] Staatliches Handeln muss im öffentlichen Interesse liegen und verhältnismässig sein.

[3] Staatliche Organe und Private handeln nach Treu und Glauben.

[4] Bund und Kantone beachten das Völkerrecht.

[30] Siehe etwa YVO HANGARTNER, in: St. Galler Kommentar (Fn. 10), Art. 5 RZ. 5 ff., 30 ff., 35 ff. und dortige Hinweise; GERHARD SCHMID/FELIX UHLMANN, Idee und Ausgestaltung des Rechtsstaates, in: Verfassungsrecht der Schweiz/Droit constitutionnel suisse, hgg. von Daniel Thürer/Jean-François Aubert/Jörg Paul Müller, Zürich 2001, S. 226 f.

[31] RAINER J. SCHWEIZER, in: St. Galler Kommentar (Fn. 10), Art. 3, Rz. 10 f. mit Hinweisen.

[32] Vgl. Art. 54 und 58 BV.

[33] Siehe hierzu grundlegend Bericht GPDel zum System Onyx (Fn. 19), S. 1526 ff.

[34] Vgl. dazu auch BVerfGE 100, 313 - Telekommunikationsüberwachung I: Das deutsche Bundesverfassungsgericht sprach sich darin für die extraterritoriale Geltung von Grundrechtsgarantien aus: Der räumliche Schutzumfang des Fernmeldegeheimnisses ist nicht auf das Inland beschränkt. Art. 10 GG kann vielmehr auch dann eingreifen, wenn eine im Ausland stattfindende Telekommunikation durch Erfassung und Auswertung im Inland hinreichend mit inländischem staatlichem Handeln verknüpft ist (Leitsatz 2).

tung. Art. 13 BV schützt die Privatsphäre[35]. Dieser Bestimmung entspricht inhaltlich der für die Schweiz ebenfalls unmittelbar verbindliche Art. 8 der Europäischen Menschenrechtskonvention (EMRK)[36]. Art. 16 BV[37] schützt die Meinungs- und Informationsfreiheit. Auch in diesem Fall findet sich eine entsprechende Garantie in der EMRK, welche in Art. 10 die Meinungsäusserungsfreiheit schützt[38]. Da die technische Entwicklung nicht stehen bleibt, kann nicht ausgeschlossen werden, dass weitere Grundrechte betroffen sein können.

Unter dem Titel des Schutzes der Privatsphäre wird in Art. 13 Abs. 1 BV ausdrücklich der Brief-, Post- und Fernmeldeverkehr der Privatpersonen gegen unbefugte Kontrolle und Einsichtnahme geschützt. Dies entspricht der Regelung von Art. 8 Ziff. 1 EMRK. Für die Ermittlung der Tragweite und Wirkungsweise dieses Grundrechtes sind daher entsprechende Entscheidungen des Europäischen Gerichtshofes für Menschenrechte[39] in gleicher Weise massgebend wie die Entscheidungen des Schweizerischen Bundesgerichtes[40].

Lehre und Praxis haben den Schutz des Fernmeldeverkehrs seit jeher unter dem Titel des Schutzes der Privatsphäre abgehandelt und nicht unter den Aspekten der Meinungs- und Informationsfreiheit[41]. Allfällige Berührungspunkte mit der Meinungsäusserungs- und Informationsfreiheit nach Art. 16 BV werden daher hier nicht näher behandelt.

---

[35] Die Bestimmung lautet:

Art. 13 Schutz der Privatsphäre

[1] Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs.

[2] Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.

[36] EMRK, SR 0.101; siehe dazu etwa MARK E. VILLIGER, Handbuch der Europäischen Menschenrechtskonvention, 2. Aufl., Zürich 1999, Rz. 554; ARTHUR HAEFLIGER/FRANK SCHÜRMANN, Die europäische Menschenrechtskonvention und die Schweiz, 2. Aufl., Bern 1999, S. 248 ff.

[37] Die Bestimmung lautet:

Art. 16 Meinungs- und Informationsfreiheit

[1] Die Meinungs- und Informationsfreiheit ist gewährleistet.

[2] Jede Person hat das Recht, ihre Meinung frei zu bilden und sie ungehindert zu äussern und zu verbreiten.

[3] Jede Person hat das Recht, Informationen frei zu empfangen, aus allgemein zugänglichen Quellen zu beschaffen und zu verbreiten.

[38] S. VILLIGER (Fn. 36), Rz. 603 ff.

[39] Vgl. Urteil des Europäischen Gerichtshofs für Menschenrechte (EGMR) in Sachen *Kruslin* gegen Frankreich vom 24. April 1990, wo festgehalten wird, dass Abhörungen und andere Formen der Erfassung von Telefongesprächen einen schweren Eingriff in die Achtung des Privatlebens und der Korrespondenz darstellen und deshalb auf einem besonders präzise abgefassten Gesetz fussen müssen, dass die Existenz von klaren und ausführlichen Regeln in diesem Bereich unabdingbar zu sein scheint, um so mehr, als sich die zum Einsatz gelangenden technischen Verfahren immer weiter entwickeln (§ 33). Vgl. auch die Urteile *Malone* gegen Vereinigtes Königreich vom 2. August 1984 (§ 67), *Huvig* gegen Frankreich vom 24. April 1990 (§ 29) und *Amann* gegen Schweiz vom 16. Februar 2000 (§ 58). Zum gegenwärtigen Zeitpunkt bezieht sich die Rechtsprechung des EGMR zwar auf gerichtliche oder administrative Telefonüberwachungen, die von den Behörden gegenüber den ihrer Gerichtsbarkeit unterstehenden Bürgern vorgenommen wurden. Der EGMR hat indes wiederholt, dass die Verantwortlichkeit der Vertragsstaaten nicht allein territorial begrenzt ist, sondern eben auch, „ […] que la notion de «juridiction» au sens de l'article 1 de la Convention ne se circonscrit pas nécessairement au seul territoire national des Hautes Parties contractantes […]. La Cour a admis que, dans des circonstances exceptionnelles, les actes des Etats contractants accomplis ou produisant des effets en dehors de leur territoire peuvent s'analyser en l'exercice par eux de leur juridiction au sens de l'article 1 de la Convention." (Urteil vom 8. Juli 2004 in Sachen *Ilascu et al.* gegen Moldawien und die Russische Föderation (§ 314); ferner das Urteil vom 23. März 1995 in Sachen *Loizidou gegen Türkei* (§ 62:). Massgebend ist mithin das faktische Kriterium der Ausübung einer "effektiven Kontrolle" über die betroffenen Personen (dazu : JUAN ANTONIO CARRILLO-SALCEDO, in Pettiti, Decaux, Imbert, La Convention européenne des droits de l'homme, Paris 1995, S. 136). Auch wenn der EGMR bis heute nicht spezifisch über Abhörungen hat befinden müssen, die von einem Vertragsstaat der EMRK auf dem Hoheitsgebiet eines anderen Staates vorgenommen wurden, ist von der Anwendbarkeit der Garantien der EMRK auszugehen.

[40] BGE 115 Ia 299; HAEFLIGER/SCHÜRMANN (Fn. 36), S. 44.

[41] Siehe etwa JÖRG PAUL MÜLLER, Grundrechte in der Schweiz, 3. Aufl., Bern 1999, S.42 ff. und 131 ff.

Der Schutz durch die Grundrechte gilt – mit Ausnahme ihres Kerngehaltes, der nicht an tastbar ist[42] – nicht absolut. Art. 36 BV[43] verlangt für Grundrechtseingriffe durch Behörden eine gesetzliche Grundlage, ein hinreichendes öffentliches Interesse und die Wahrung der Verhältnismässigkeit des Eingriffs. Es sind dies die Voraussetzungen für Eingriffe in die Freiheitsrechte[44]. Unter gesetzlicher Grundlage ist in diesem Zusammenhang eine generell abstrakte Regelung, also ein Rechtssatz zu verstehen[45]. Art. 164 Abs. 1 lit. b präzisiert ferner, dass alle wichtigen rechtsetzenden Bestimmungen – darunter fallen insbesondere die grundlegenden Bestimmungen über Einschränkungen verfassungsmässiger Rechte – in einem formellen Gesetz, d.h. einem dem Referendum unterstehenden Erlass vorgesehen sein müssen. Die Voraussetzungen der Bundesverfassung sind in diesem Punkt strenger, als die Voraussetzungen der EMRK, welche in diesem Zusammenhang ein materielles Gesetz als zulässig ansieht[46], zugleich aber bei schweren Eingriffen in besonderem Masse konkret sein, d.h. bestimmt und vorhersehbar, sein muss[47].

2.2.1.3.2. Schutz der Privatsphäre

Die Verpflichtung der Behörden, das Post- und Fernmeldegeheimnis zu wahren, gilt als besondere Ausprägung des grundrechtlichen Persönlichkeitsschutzes, welcher jedes ungerechtfertigte Eindringen in die Privatsphäre von Personen ausschliessen will[48]. Der Schutz hängt dabei weder vom jeweiligen Inhalt der Information noch vom Informationsträger ab, so dass sowohl persönliche als auch geschäftliche Korrespondenz sowie die Kommunikation etwa über E-mail oder SMS ebenfalls erfasst sind[49].
Das behördliche Eindringen in Informationen, deren Übermittlung von Art. 13 Abs. 1 BV geschützt ist, bedarf einer gesetzlichen Grundlage. Für die Überprüfung der Rechtmässigkeit eines Zugriffs auf elektronisch übermittelte Informationen Dritter stellt sich weiter die Frage, ob dieser Eingriff als schwerwiegende Einschränkung im Sinne von Art. 36 Abs. 1 BV zu qualifizieren ist und zumindest in seinen Grundzügen in einem formellen Gesetz vorgezeichnet sein muss. Ein behördlicher Zugriff auf die private Kommunikation bzw. eine behördliche Einsichtnahme in private Daten, die nie für eine wie auch immer geartete Verbreitung gedacht waren, ohne Mitteilung an die Betroffenen und ohne formelle Rechtsmittelweg stellt einen schweren Eingriff in den grundrechtlich geschützten Privatbereich dar, der einer formellgesetzlichen Grundlage bedarf[50].

---

[42] Siehe hierzu RAINER J. SCHWEIZER, in: St. Galler Kommentar (Fn. 10), Art. 36, Rz. 28 f. und dortige Hinweise.

[43] Die Bestimmung lautet:

> Art. 36 Einschränkungen von Grundrechten
>
> [1] Einschränkungen von Grundrechten bedürfen einer gesetzlichen Grundlage. Schwerwiegende Einschränkungen müssen im Gesetz selbst vorgesehen sein. Ausgenommen sind Fälle ernster, unmittelbarer und nicht anders abwendbarer Gefahr.
>
> [2] Einschränkungen von Grundrechten müssen durch ein öffentliches Interesse oder durch den Schutz von Grundrechten Dritter gerechtfertigt sein.
>
> [3] Einschränkungen von Grundrechten müssen verhältnismässig sein.
>
> [4] Der Kerngehalt der Grundrechte ist unantastbar.

[44] ULRICH HÄFELIN/WALTER HALLER/HELEN KELLER, Schweizerisches Bundesstaatsrecht, 7. Aufl., Zürich 2008, Rz. 302 f; RAINER J. SCHWEIZER, in: St. Galler Kommentar (Fn. 10), Art. 36, Rz. 7 und dortige Hinweise.

[45] HÄFELIN/HALLER/KELLER (Fn. 44), Rz. 308 ff.; SCHWEIZER (Fn. 44), Rz. 10 f.

[46] SCHWEIZER (Fn. 44), Rz. 13-15 und dortige Hinweise; vgl. auch JOCHEN ABR. FROWEIN/WOLFGANG PEUKERT, EMRK-Kommentar, 2. Aufl., Kehl/Strassburg/Arlington, 1996, Art. 5 Rz. 26.

[47] Jens MEYER-LADEWIG, EMRK-Handkommentar, 2. Aufl., Baden-Baden 2006, N 10 zu Art. 8.

[48] MÜLLER (Fn. 41), S. 132; VILLIGER (Fn. 36), Rz. 564.

[49] STEPHAN BREITENMOSER, in: St. Galler Kommentar (Fn. 10), Art. 13, Rz. 34 f.; CHRISTOPH GRABENWARTER, Europäische Menschenrechtskonvention, 3. Aufl., München/Basel/Wien 2007, § 22, Rz 24.

[50] BREITENMOSER (Fn. 49), Art. 13, Rz. 35; GIOVANNI BIAGGINI, BV-Kommentar, Zürich 2007, Art. 13, Rz. 10; vgl. BGE 126 I 50 zur Überwachung des E-Mail-Verkehrs.

2.2.2. Gesetzliche Grundlagen für CNE

Wie bereits oben gezeigt[51] besteht für CND eine ausreichende gesetzliche Grundlage.

Wie ebenfalls bereits ausgeführt[52], erübrigt sich die Schaffung einer gesetzlichen Grundlage für CNA in Friedenszeiten, da wir davon ausgehen, dass CNA nur im Falle eines Krieges – und zwar durch die Armee – zur Anwendung gelangen soll.

Für CNE besteht hingegen ausserhalb des Aktivdienstes keine gesetzliche Grundlage. Mit Art. 99 MG liegt nach den unter 2.2.1.3 aufgezeigten Bedingungen keine ausreichende formell-gesetzliche Grundlage für CNO vor[53]. Einerseits umschreibt Abs. 1 nur die Aufgaben des Nachrichtendienstes und andererseits setzt Abs. 2 den rechtmässigen Erwerb von Informationen voraus. Die Delegationen in Abs. 3 genügen der formellgesetzlichen Grundlage in Bezug auf CNO nicht. Wie gezeigt, bedürfen CNE jedoch einer formellgesetzlichen Grundlage. Mit der gleichen Begründung wird derzeit im übrigen eine formell-gesetzliche Grundlage für das die Funkaufklärung (System ONYX) geschaffen[54].

Will man für die Nachrichtenbeschaffungsorgane der Armee die Möglichkeit für CNE eröffnen, müsste eine entsprechende gesetzliche Grundlage geschaffen werden. Bei der Ausgestaltung dieser gesetzlichen Grundlage wäre insbesondere auf das ähnlich gelagerte geheime Durchsuchen eines Datenverarbeitungssystems durch den DAP[55] zu achten.

2.2.3. Öffentliches Interesse

Die Informationsbeschaffung durch die Armee (CNE) hat grundsätzlich im öffentlichen Interesse[56] zu geschehen. Die Wahrung der inneren und äusseren Sicherheit sowie die sicherheitsrelevanten Aspekte der Landesverteidigung gelten in Lehre und Rechtssprechung grundsätzlich als starke öffentliche Interessen[57]. Gleiches gilt für

---

[51] Siehe 2.1.

[52] Unter 1.3.

[53] Die Bestimmung lautet:

Art. 99 Nachrichtendienst

[1] Der Nachrichtendienst hat zur Aufgabe, sicherheitspolitisch bedeutsame Informationen über das Ausland zu beschaffen, auszuwerten und zu verbreiten.

[2] Er ist befugt, Personendaten, mit Einschluss von besonders schützenswerten Personendaten und von Persönlichkeitsprofilen, zu bearbeiten, gegebenenfalls ohne Wissen der betroffenen Personen, soweit und solange es seine Aufgaben erfordern. Er kann im Einzelfall Personendaten in Abweichung von den datenschutzrechtlichen Bestimmungen ins Ausland weitergeben.

[2bis] Er kann Informationen über Personen in der Schweiz, die bei Gelegenheit seiner Tätigkeit nach Absatz 1 anfallen und für die innere Sicherheit oder die Strafverfolgung von Bedeutung sein können, dem Dienst für Analyse und Prävention sowie dem Bundesamt für Polizei weiterleiten.

[3] Der Bundesrat regelt:

a. die Aufgaben des Nachrichtendienstes im Einzelnen, dessen Organisation sowie den Datenschutz;

b. die Tätigkeit des Nachrichtendienstes im Friedensförderungs-, Assistenz- und Aktivdienst;

c. die Zusammenarbeit des Nachrichtendienstes mit interessierten Stellen von Bund und Kantonen sowie mit ausländischen Diensten;

d. die Ausnahmen von den Vorschriften über die Registrierung von Datensammlungen, wenn diese die Informationsbeschaffung gefährden würde.

[4] Der Quellenschutz muss in jedem Fall gewährleistet werden.

[5] Der Nachrichtendienst untersteht unmittelbar dem Chef des Departements für Verteidigung, Bevölkerungsschutz und Sport.

[54] Siehe dazu 2.2.5.

[55] Siehe 2.2.5: Abgrenzung zu Art. 18 lit. m BWIS II.

[56] Zum Begriff s. etwa MARTIN PHILIPP WYSS, Öffentliches Interesse – Interessen der Öffentlichkeit? Das öffentliche Interesse im schweizerischen Staats- und Verwaltungsrecht, Bern 2001, Rz. 1 ff.; ULRICH HÄFELIN/GEORG MÜLLER/FELIX UHLMANN, Allgemeines Verwaltungsrecht, 5. Aufl., Zürich/St.Gallen 2006, Rz. 535 ff.

[57] WYSS, (Fn. 54), Rz. 199 ff.; HÄFELIN/MÜLLER/UHLMANN (Fn. 54), Rz. 544 ff. und dortige Hinweise.

die von Art. 13 BV bzw. Art. 8 EMRK geschützte Privatsphäre. Deshalb ist eine sorgfältige Abwägung der Sicherheitsinteressen gegenüber dem allenfalls entgegenstehenden – öffentlichen und privaten – Interesse einer unangetasteten Privatsphäre notwendig[58].

2.2.4. Verhältnismässigkeit

Wie weit die Informationsbeschaffung der Armee mittels CNE zugunsten des militärischen Nachrichtendienstes dem verfassungsmässigen Gebot der Verhältnismässigkeit entspricht, ist nach der herrschenden Lehre und Praxis an den drei Elementen dieses Grundsatzes zu messen: Eignung der Massnahme im Hinblick auf den angestrebten Zweck, Erforderlichkeit der Massnahmen, Verhältnismässigkeit von Eingriffszweck und Eingriffswirkung[59]. Gleichzeitig ist darauf hinzuweisen, dass sich das Bundesgericht im Rahmen der Verhältnismässigkeitsprüfung, welche an sich frei vorzunehmen ist, bei der Würdigung der Tatsachen und der Gewichtung der in Frage stehenden öffentlichen Interessen grosse Zurückhaltung auferlegt[60].

In Bezug auf die Eignung einer Informationsbeschaffung durch die FUB insbesondere über CNE kann auf Grund der Angaben der beteiligten Dienststellen festgestellt werden, dass das System es ermöglicht, aufgrund gezielter Verdachtsmomente und entsprechender Vorgaben sicherheitsrelevante Einzelinformationen aus Computernetzwerken bzw. einzelnen Computern herauszufiltern. Wohl müssen diese Einzelinformationen von den zuständigen Stellen auf ihren tatsächlichen Informationswert hin überprüft und im Rahmen eines bestimmten Kontextes beurteilt werden, doch stellt dies die grundsätzliche Eignung der Massnahmen nicht in Frage.

Der Grundsatz der Erforderlichkeit schliesst insbesondere das Gebot des geringstmöglichen Grundrechtseingriffes bzw. das Übermassverbot ein[61]. Dass der Bund die für seine Sicherheitsbedürfnisse notwendige Informationsbeschaffung über die Situation im Ausland auf auswertbare elektronische Quellen ausdehnt, entspricht im Hinblick auf die sich immer rascher ändernde internationale Entwicklung dem Gebot der Erforderlichkeit. Die Eignung der Abklärungsaufträge und das sogenannte Übermassverbot müssen vor allem bei der Auftragserteilung und bei einer noch zu erlassenden Regelung über die Auswahl, die Aufbereitung und Verwendung der aufgefangenen Informationen sichergestellt werden. Letzteres drängt sich in erster Linie deshalb auf, weil regelmässig auch höchstpersönliche Daten beispielsweise auf Festplatten zugänglich werden, d.h. solche, die nie für eine wie auch immer geartete Verbreitung gedacht waren.

Die Prüfung der Verhältnismässigkeit zwischen Eingriffszweck und Eingriffswirkung kann auf abstrakter Ebene nur sehr beschränkt erfolgen; sie hat eher bei der Ausgestaltung der einzelnen Informationsbeschaffungsaufträge und der Verwendung der Informationen zu geschehen. Die Beurteilung der Verhältnismässigkeit im Einzelfall hängt insbesondere davon ab, welcher Art die Gefahren sind, welche mittels der Nachrichtenbeschaffung abgewendet werden sollen, sowie davon, welche Auswirkungen für die betroffenen Telekommunikationsteilnehmer entstehen. Wie bei der Abwägung der öffentlichen Interessen fällt auch bei einer eher allgemeinen Verhältnismässigkeitsprüfung negativ ins Gewicht, dass die Betroffenen von der stattfindenden CNE im konkreten Fall in der Regel nichts erfahren (sollen) und dementsprechend dazu in keinem Ablaufstadium Stellung nehmen können. Dieser Mangel, der

[58] Siehe etwa HÄFELIN/MÜLLER/UHLMANN (Fn. 54), Rz. 562 ff.; WYSS (Fn. 54), Rz. 517 ff.

[59] Siehe dazu etwa HÄFELIN/MÜLLER/UHLMANN (Fn. 54) Rz. 581 ff.

[60] *In casu* wurde dies mit aussen- und sicherheitspolitischen Implikationen begründet; BGE 129 II 192, 208; bestätigt in BGE 132 I 229, 244.

[61] HÄFELIN/MÜLLER/UHLMANN (Fn. 54), Rz. 591 f.

zugleich ein systemimmanentes Ziel ist, ist durch institutionelle Kontroll- und Überprüfungsverfahren zu kompensieren.

Ob das Interesse an einem uneingeschränkten Schutz der in erster Linie privaten elektronischen Kommunikation gegenüber dem öffentlichen Interesse an einem staatlichen Zugriff im umschriebenen Rahmen vorgeht, kann aber vorliegend kaum in genereller Weise entschieden werden, sondern muss praktisch im Einzelfall bei der Auftragserteilung an die FUB und bei der weiteren Bearbeitung der ggf. gefundenen Einzelinformation entschieden werden[62].

Um Bedenken zu zerstreuen, dass im Wesentlichen die gleiche Behörde, welche den Abklärungsauftrag veranlasst, bei der Verwendung der gewonnenen Informationen die oben umschriebene Interessenabwägung vornimmt, ohne dass sich der Betroffene dazu äussern kann und ohne dass Rechtsmittelmöglichkeiten oder unabhängige Überprüfungen institutionalisiert sind, müsste *de lege ferenda* zumindest das heute übliche Verfahren im Rahmen der VEKF dienen. Es ist zwar nachvollziehbar, dass CNE häufig ohne Wissen und Mitwirkungsmöglichkeiten der Betroffenen geschehen muss. Ebenso unerlässlich sind aber kompensatorische Massnahmen zur Sicherstellung einer unvoreingenommenen Interessenabwägung durch eine unabhängige Kontrolle der Informationsbeschaffung und -verwertung[63]. Angesichts der Nähe der Nachrichtendienste zur Exekutive fordert der EGMR gestützt auf Art. 13 EMRK nunmehr zumindest im Normalfall in letzter Instanz eine gerichtliche Kontrolle[64].

2.2.5. Abgrenzung zu Art. 18 lit. m BWIS II

Das geltende Recht umschreibt heute die Mittel der Informationsbeschaffung für den DAP abschliessend in Art. 14 Abs. 2 BWIS; Elemente von CNO sind darin nicht enthalten[65]. Solches soll erst mit der BWIS II-Vorlage ermöglicht werden. Das geheime Durchsuchen eines Datenverarbeitungssystems nach Art. 18 lit. m BWIS II – der Sache nach CNE – soll so geregelt werden, dass Datenverarbeitungssysteme mutmasslicher Gefährder vom DAP durchsucht werden dürfen[66].

---

[62] Vgl. etwa HÄFELIN/MÜLLER/UHLMANN (Fn. 54), Rz. 564.

[63] EGMR, Urteil vom 6. Juni 2006 in Sachen *Segerstedt-Wiberg et al.* gegen Schweden (§ 103 [ständige Rechtsprechung]).

[64] EGMR, Urteil vom 4. Mai 2000 in Sachen *Rotaru* gegen Rumänien (§ 59): „ […] pour que les systèmes de surveillance secrète soient compatibles avec l'article 8 de la Convention, ils doivent contenir des garanties établies par la loi et qui sont applicables au contrôle des activités des services concernés. Les procédures de contrôle doivent respecter aussi fidèlement que possible les valeurs d'une société démocratique, en particulier la prééminence du droit, à laquelle se réfère expressément le préambule de la Convention. Elle implique, entre autres, qu'une ingérence de l'exécutif dans les droits de l'individu soit soumise à un contrôle efficace que doit normalement assurer, au moins en dernier ressort, le pouvoir judiciaire, car il offre les meilleures garanties d'indépendance, d'impartialité et de procédure régulière (arrêt Klass et autres précité, pp. 25-26, § 55)“ ; ebenso *Segerstedt-Wiberg* gegen Schweden (Fn. 96), § 121 f.

[65] Die Bestimmung lautet:

> Personendaten können beschafft werden durch:
>
> a. Auswerten öffentlich zugänglicher Quellen;
> b. Einholen von Auskünften;
> c. Einsicht in amtliche Akten;
> d. Entgegennahme und Auswerten von Meldungen;
> e. Nachforschen nach der Identität oder dem Aufenthalt von Personen;
> f. Beobachten von Vorgängen an öffentlichen und allgemein zugänglichen Orten, auch mittels Bild- und Tonaufzeichnungen;
> g. Feststellen der Bewegungen und der Kontakte von Personen.

[66] Der Wortlaut der Bestimmung:

> *Art. 18m (neu) Geheimes Durchsuchen eines Datenverarbeitungssystems*
>
> Lassen konkrete und aktuelle Tatsachen oder Vorkommnisse vermuten, dass ein mutmasslicher Gefährder oder eine mutmassliche Gefährderin ein ihm oder ihr zur Verfügung stehendes und gegen Zugriff besonders gesichertes Datenverarbeitungssystem benutzt, kann dieses vom Bundesamt durchsucht werden. Die Durchsuchung kann ohne Wissen des mutmasslichen Gefährders oder der mutmasslichen Gefährderin erfolgen.

Die vom Parlament im Rahmen des ZNDG beschlossene Änderung des Militärgesetzes[67] fasst Art. 99 MG neu[68]. Dabei sind die im Rahmen der Zusatzbotschaft BWIS II gemachten Änderungsvorschläge noch nicht berücksichtigt, welche in erster Linie die gesetzliche Verankerung der Funkaufklärung zum Gegenstand haben. Auch diese Fassung des Art. 99 MG genügt einer formell-gesetzlichen Grundlage für CNO nicht[69].

Berechtigt zum geheimen Durchsuchen eines Datenverarbeitungssystems wäre damit auch nach der Zusammenführung unter dem Dach des VBS allein der DAP, nicht etwa der SND oder der MND. Denn trotz der beschlossenen Zusammenführung des SND mit dem zivilen Dienst für Analyse und Prävention (DAP) unter dem Dach des VBS gilt es weiterhin deren unterschiedliche und gesetzlich definierte Aufträge zu betonen. Gemäss Art. 5 Abs. 2 der Verordnung über die Nachrichtendienste im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (Nachrichtendienstverordnung VBS, VND) vom 26. September 2003[70] vereinbaren die Nachrichtendienste des VBS eine Zusammenarbeitsregelung, welche durch den Chef VBS zu genehmigen ist.

Mit anderen Worten ändert die Entscheidung des Bundesrates, die nachrichtendienstlichen Teile des DAP dem Chef VBS zu unterstellen (Bundesratsbeschluss vom 21.5.2008) nichts an den grundlegend unterschiedlichen gesetzlichen Aufträgen der beiden Dienste. Eine engere Zusammenarbeit ist nur im Rahmen der bestehenden Gesetze zulässig.

CNO des Militärs zugunsten von zivilen Behörden stehen unter dem Vorbehalt von Art. 1 Abs. 3 MG, wonach dies nur zulässig ist, wenn die polizeilichen Mittel nicht mehr ausreichen, sei es bei der Abwehr von schwer wiegenden Bedrohungen der inneren Sicherheit (lit. a) oder sei es bei der Bewältigung von anderen ausserordentlichen Lagen, insbesondere im Falle von Katastrophen im In- und Ausland (lit. b). Gleichzeitig ist festzuhalten, dass nicht jeder Angriff auf ein Informationssystem – und sei es noch so wichtig – einen militärischen Angriff darstellt[71].

---

[67] Siehe Fn. 22.

[68] Die Bestimmung lautet:

> Art. 99 Abs. 1, 2bis, 3 Bst. c, 4 und 5
>
> [1] Der Nachrichtendienst der Armee (Nachrichtendienst) hat zur Aufgabe, für die Armee bedeutsame Informationen über das Ausland zu beschaffen und auszuwerten, insbesondere im Hinblick auf die Verteidigung des Landes, den Friedensförderungsdienst und den Assistenzdienst im Ausland.
>
> [2bis] Er kann Informationen über Personen in der Schweiz, die bei Gelegenheit seiner Tätigkeit nach Absatz 1 anfallen und die für die Strafverfolgung von Bedeutung sein können, den Strafverfolgungsbehörden des Bundes weiterleiten. Der Bundesrat regelt die Einzelheiten.
>
> [3] Der Bundesrat regelt:
>
> […]
>
> c. die Zusammenarbeit des Nachrichtendienstes mit interessierten Stellen von Bund und Kantonen sowie mit ausländischen Dienststellen; er genehmigt zwischenstaatliche Verwaltungsvereinbarungen des Nachrichtendienstes und sorgt dafür, dass solche Vereinbarungen erst nach erfolgter Genehmigung vollzogen werden dürfen;
>
> [4] Der Bundesrat regelt den Quellenschutz entsprechend den Schutzbedürfnissen der verschiedenen Quellen. Personen, die aufgrund ihrer Informationstätigkeit über das Ausland gefährdet sind, sind in jedem Fall zu schützen.
>
> [5] Der Bundesrat regelt die Unterstellung des Nachrichtendienstes. Er sorgt dafür, dass die Tätigkeit des Nachrichtendienstes auf Rechtmässigkeit, Zweckmässigkeit und Wirksamkeit überprüft wird. Das zuständige Departement erlässt jährlich einen Kontrollplan, der mit den parlamentarischen Kontrollen abgestimmt wird.

[69] Siehe 2.2.2.

[70] SR 510.291.

[71] Siehe dazu 3.2.2.1.

3. Völkerrechtliche Vorgaben für CNO

3.1. Einleitung und Übersicht

Die konkreten Fragen der Geschäftsprüfungsdelegation betreffen nicht direkt das Völkerrecht. Im Schreiben vom 20. Mai 2008 bat das VBS jedoch die Direktion für Völkerrecht, auch die völkerrechtlichen Fragen abzuklären.

Dieser zweite Teil des Rechtsgutachtens zeigt deshalb auf, welche völkerrechtliche Fragen Computernetzwerkoperationen aufwerfen. Auch wenn diese nicht abschliessend beantwortet werden können, bieten folgende Seiten aber eine Auslegeordnung und eine Diskussionsgrundlage. Vorbehalten bleibt, dass jeder Einzelfall gesondert zu untersuchen ist.

Für die völkerrechtliche Auslegeordnung massgebend sind die einzelnen Bereiche des Völkerrechts. Zunächst ist zwischen *ius ad bellum* und *ius in bello* zu unterscheiden.

Das *ius ad bellum* oder auch *ius contra bellum* verbietet grundsätzlich jegliche militärische Gewalt. Militärische Gewalt ist völkerrechtlich nur legitim, wenn sie als Selbstverteidigung oder im Rahmen der kollektiven Sicherheit angewandt wird. Für *Computer Network Operations* stellt sich also die Frage, ob und wann diese völkerrechtlich legitim durchgeführt werden können. Dabei ist ausserdem zu beachten, dass defensive militärische Gewaltanwendung nur dann legitim ist, wenn sie auf einen Angriff reagiert, der die Schwelle eines bewaffneten Angriffs gemäss Art. 51 UNO-Charta überschreitet [72]. Überschreitet ein Eingriff über Computernetzwerke diese Schwelle nicht, kann jedoch das Interventionsverbot verletzt sein. Dieses geht über das Gewaltverbot hinaus und verbietet Staaten grundsätzlich, die Souveränität anderer Staaten zu verletzen.

Das *ius in bello* indessen regelt die militärische Gewaltanwendung in bewaffneten Konflikten, ohne jedoch die Frage zu beantworten, ob die Teilnahme am bewaffneten Konflikt selbst völkerrechtlich legitim ist. Das *ius in bello* entspricht dem Regelwerk des Humanitären Völkerrechts. Hier stellt sich die Frage, wie dieses Regelwerk auf *Computer Network Operations* anzuwenden ist.

Für die Schweiz von besonderem Interesse ist ausserdem das Neutralitätsrecht. Es wirft die Frage auf, welche Rechte und Pflichten die Kriegsführung durch *Computer Network Operations* für einen dauernd neutralen Staat begründet.

Die völkerrechtliche Auslegeordnung bringt mit sich, dass im Völkerrechtsteil insbesondere der Graubereich zwischen *Computer Network Defense* (CND) und *Computer Network Attack* (CNA) nicht gleich behandelt werden kann wie in der Untersuchung über die nationalen Rechtsgrundlagen[73]. Gemäss Regeln des *ius ad bellum* können defensive Gegenattacken nicht mit offensivem CNA gleichgesetzt werden.

Die im Anhang abgedruckte Tabelle (Grafik 3) zeigt zusammenfassend die Auslegeordnung des Völkerrechts. Sie nimmt zwar an dieser Stelle Ergebnisse vorweg. Dabei gibt sie aber erstens einen Überblick über die Fragen des Völkerrechts und CNO. Zweitens zeigt sie auf, welche Fragestellungen wo im Völkerrechtsteil behandelt werden. Drittens sind zum besseren Verständnis auch die bisherigen Annahmen und Ergebnisse des Gutachtens in die Darstellung integriert.

---

[72] SR 0.120.

[73] Siehe Grafik 1 (CNO) im Anhang und Text unter 1.1. Vor Teil 3. sind im Gutachten die Graubereiche zur jeweils stärkeren Stufe gerechnet worden. So werden insbesondere defensive Gegenattacken als Reaktion auf gegnerisches CNA im Gutachtenteil über die nationalen Rechtsgrundlagen CNA zugeordnet.

3.2. CNO und *ius ad bellum* bzw. *ius contra bellum*

Heute gilt ein absolutes Gewaltverbot in den internationalen Beziehungen. Dieses Gewaltverbot stützt sich auf Art. 2 Abs. 4 UNO-Charta, gilt aber auch kraft Gewohnheitsrecht, und ist nach überwiegender Ansicht Teil des *ius cogens*. Ausgenommen vom Gewaltverbot sind gemäss UNO-Charta nur Massnahmen der kollektiven Sicherheit (Kapitel VII UNO-Charta) sowie die individuelle und kollektive Selbstverteidigung bei einem bewaffneten Angriff (Art. 51 UNO-Charta)[74].

3.2.1. Gewaltverbot

Zunächst stellt sich die Frage, ob ein Angriff auf ein Computernetzwerk unter das Gewaltverbot fällt. Das Gewaltverbot beschränkt sich gemäss herrschender Lehre und Praxis auf die militärische Gewalt zwischen Staaten. Um die Frage zu beantworten, ist also erstens festzustellen, ob ein Angriff auf ein Computernetzwerk unter den Begriff der militärischen Gewalt fällt. Falls ja, zweitens, ob ein solcher Angriff auch als zwischenstaatliche Gewalt bezeichnet werden kann.

3.2.1.1 Sind Angriffe über Computernetzwerke militärische Gewalt?

Kann ein Computer als Waffe bezeichnet werden, beziehungsweise der Angriff auf das Computernetzwerk in einem anderen Staat als militärische Gewalt?

Die Diskussion hierüber in der Völkerrechtslehre steht erst am Anfang[75]. Als erstes Ergebnis kann jedoch festgehalten werden, dass gemäss Lehre ein Computer zur Waffe werden kann und es vorstellbar ist, dass ein Angriff auf Computernetzwerke das Ausmass militärischer Gewalt annimmt.

Bei der Bestimmung des Begriffs der Waffe wird nicht auf das eingesetzte Mittel, sondern vielmehr auf die Absicht abgestellt, mit der ein Mittel eingesetzt wird, sowie auf die spezifischen Auswirkungen. Wird von einem Computer aus ein Angriff auf Computernetzwerke durchgeführt, um Sachwerte zu zerstören oder Leib und Leben zu verletzen, und die Auswirkungen sind dieselben wie bei physischer Waffengewalt, kann ein solcher Angriff mit militärischer Gewalt gleichgesetzt werden. Es handelt sich also um eine fallweise Beurteilung. Beispiele, die in der Lehre aufgeführt werden, sind Angriffe auf Kernkraftwerke, durch die Radioaktivität freigesetzt wird, Abschalten der Stromversorgung von Krankenhäusern ohne Notstromaggregate sowie Manipulation von Verkehrssicherheitssystemen, die zu Flugzeugabstürzen und Zugkollisionen führen. Solche Angriffsszenarien stehen nicht nur im Widerspruch zu den Prinzipien des Humanitären Völkerrechts[76], sondern fallen auch unter das Gewaltverbot.

Es sind jedoch nicht nur Angriffe auf Computernetzwerke denkbar, die physische Gewalt anwenden. Solche Angriffe können auch mit dem Ziel durchgeführt werden, wirtschaftlichen oder politischen Zwang auf einen anderen Staat auszuüben. Als Beispiele werden in der Literatur Angriffe auf das Zahlungs-, Banken- oder Börsensystem eines Landes genannt.

---

[74] Zum Gewaltverbot und Ausnahmen des Gewaltverbots vergleiche ANNE PETERS: *Völkerrecht*, Zürich 2008; MICHAEL BOTHE: Friedenssicherung und Kriegsrecht, in: WOLFGANG GRAF VITZHUM (Hrsg.), *Völkerrecht*, Berlin 2007; KNUT IPSEN: *Völkerrecht*, München 2004; WALTER KÄLIN et. al., *Völkerrecht*, Bern 2006.

[75] FALKO DITTMAR: Angriffe auf Computernetzwerke: *‚Ius ad bellum' und ‚ius in bello'*, Berlin 2005; MICHAEL N. SCHMITT, „Angriffe im Computernetz und das *ius ad bellum*" in: *Neue Zeitschrift für Wehrrecht*, S. 177 – 195; THOMAS C. WINGFIELD: „CNA and the Jus ad Bellum: An Introduction" in: *International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law*, Stockholm 2004; D.B. SILVER: Computer Network Attack as a Use of Force Under Article 2 (4) of the United Nations Charter, in: M.N. SCHMITT (Hrsg.), *Computer Network Attack and International Law,* 2002. Es handelt sich hier um eine Frage der Auslegung der UNO-Charta. Für diese ist Art. 31 Vertragsrechtskonvention (SR 0.111) einschlägig. Entscheidend in diesem Fall ist Sinn und Zweck der UNO-Charta.

[76] Siehe 3.4.

Politischer oder wirtschaftlicher Zwang fällt nicht unter das Gewaltverbot. Entsprechend verstossen solche Angriffe auch nicht gegen das Gewaltverbot.

Angriffe auf Computernetzwerke anderer Staaten, die unter der Schwelle des Gewaltverbots liegen, verletzen aber grundsätzlich das Interventionsverbot, das über das Gewaltverbot hinausgeht[77].

3.2.1.2. Sind Angriffe über Computernetzwerke zwischenstaatliche Gewalt?

Das Gewaltverbot gilt grundsätzlich nur für Gewalt zwischen Staaten. Ob ein Angriff auf ein Computernetzwerk als zwischenstaatliche Gewalt zu qualifizieren ist, kann bei solchen Angriffen weniger klar sein als bei herkömmlicher Waffengewalt. Die Zurückverfolgung kann mit grossen Schwierigkeiten verbunden sein, zumal ein Angreifer Vorkehrungen treffen kann, um die Zurückverfolgung zu erschweren.

Unter das Gewaltverbot fällt aber nicht nur direkte staatliche Gewaltanwendung, sondern auch indirekte staatliche Gewalt. Im Nicaragua-Fall hat der IGH geurteilt, dass die Unterstützung bewaffneter Banden und Rebellengruppen durch Waffenlieferungen, militärisches Training und logistische Unterstützung als Gewaltausübung i. S. des Gewaltverbots angesehen werden kann (s. a. Uganda-Kongo-Urteil)[78].

Eine solche indirekte Gewaltausübung ist auch im Rahmen von CNO denkbar, z.B. durch die Ausbildung und militärische Unterstützung von Hackern und im Fall, dass von diesen ein Angriff auf ein Computernetzwerk ausgeht, der die Intensität militärischer Gewalt erreicht. Gleichzeitig ist aber festzuhalten, dass gemäss Nicaragua-Urteil für die Qualifizierung als staatliche Gewalt der betreffende Staat in erheblichem Mass in die nicht-staatliche Gewalt involviert sein muss[79].

Umstritten ist, inwiefern das blosse Unterlassen bzw. Dulden seitens eines Staates als indirekte staatliche Gewaltanwendung qualifiziert werden kann[80]. Diese Frage stellt sich insbesondere für den Fall der Nicht-Verhinderung der Vorbereitung oder Durchführung terroristischer Akte gegen einen anderen Staat. Grundsätzlich kann ein solches Verhalten jedoch nicht ohne weiteres mit der Gewaltausübung des Staates gleichgesetzt werden[81].

Art 2. Abs. 4 UNO-Charta verbietet nicht nur die Anwendung von Gewalt, sondern auch deren Androhung. Ein Verstoss gegen Art. 2 Abs. 4 UNO-Charta liegt gemäss Rechtssprechung des IGH dann vor, wenn die Ausübung der angedrohten Gewalt rechtswidrig wäre (Nuklearwaffen-Gutachten)[82]. Sobald also ein Angriff über Computernetzwerke sich als Verstoss des Gewaltverbots qualifizieren lässt, ist auch die Androhung einer solchen Gewalt unrechtmässig.

Die Praxis der Abschreckung durch Verteidigungsbereitschaft gilt nicht als völkerrechtswidrig, da die darin angedrohte Gewaltausübung nur eine Drohung zulässiger Selbstverteidigung darstellt. Problematisch an dieser Folgerung ist, dass die Unterscheidung zwischen Rüstung zur Verteidigung und Rüstung zum Angriff nicht immer möglich ist.

---

[77] Siehe 3.3.

[78] ICJ, "Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. USA)", *ICJ Reports* 1986; ICJ, Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), *ICJ Reports* 2005; s. a. PETERS (Fn. 67), S. 285 ff.; IPSEN (Fn. 67), S. 1076 u. 1087; BOTHE (Fn. 67), S. 648 f.

[79] Siehe auch *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, adopted by the ILC, Drafting Committee on Second Reading, U.N. GAOR Int. Law Commission, 53d Sess., U.N. Doc.A/CN.4/L.602/Rev.1 (2001).

[80] Vgl. ebd.

[81] Dazu mehr unter 3.2.2.4.

[82] ICJ, "Legality of the Threat or Use of Nuclear Weapons", Advisory Opinion, *ICJ Reports* 1996. Siehe für weiterführende Diskussion STÜRCHLER Nikolas: *The Threat of Force in International Law*, Cambridge 2007.

Folgerung: *Angriffe über Computernetzwerke verletzen das Gewaltverbot, wenn sie gleiche Auswirkungen haben wie physische Waffengewalt. Dies gilt sowohl für direkte als auch für indirekte staatliche Gewalt. Indirekte staatliche Gewalt liegt dann vor, wenn ein Staat in erheblichen Masse in die nicht-staatliche Gewalt von Hackern involviert ist. Der Aufbau einer Verteidigungsbereitschaft verstösst nicht gegen das Gewaltverbot. Angriffe über Computernetzwerke, die nicht physischer Waffengewalt gleichkommen, wie z. Bsp. der Angriff auf die Computer des Bankensystems eines Landes, verletzen nicht das Gewaltverbot, aber das Interventionsverbot.*

3.2.2. Selbstverteidigungsrecht

Das individuelle wie kollektive Selbstverteidigungsrecht ist in Art. 51 UNO-Charta geregelt und gilt auch gewohnheitsrechtlich. Damit Gewaltanwendung zur Selbstverteidigung aber zulässig ist, müssen gewisse Voraussetzungen erfüllt sein. Diese Voraussetzungen gelten auch für die Reaktion auf militärische Gewalt durch Computernetzwerke.

3.2.2.1. Bewaffneter Angriff

Erste Voraussetzung für das Selbstverteidigungsrecht gemäss Art. 51 UNO-Charta ist das Vorliegen eines bewaffneten Angriffs. Gemäss Rechtssprechung IGH ist nicht jede Verletzung des Gewaltverbots ein bewaffneter Angriff[83]. Ein umfassendes Selbstverteidigungsrecht kann nur dann in Anspruch genommen werden, wenn militärische Gewalt eine gewisse Intensität erreicht hat. Erfolgt eine Verletzung des Gewaltverbots unterhalb der Schwelle des bewaffneten Angriffs, hat der Staat aber ein Recht auf sofortige und verhältnismässige nicht-militärische Abwehrmassnahmen.

3.2.2.2. Verhältnismässigkeitsprinzip

Die Verhältnismässigkeit der Abwehrmassnahmen ist ein Grundprinzip des Selbstverteidigungsrechts. Auch wenn ein bewaffneter Angriff vorliegt, sind nur diejenigen Aktionen zulässig, die verhältnismässig im Hinblick auf den vorausgegangenen Angriff sind. Das Prinzip der Verhältnismässigkeit ergibt sich auch aus dem Humanitären Völkerrecht[84]. Dabei spielt aber die Wahl der Waffenart keine Rolle, sondern deren Auswirkungen. Kommt ein Angriff über Computernetzwerke militärischer Gewalt im Ausmass eines bewaffneten Angriffs gleich, kann die Selbstverteidigung grundsätzlich auch über eine andere Waffengattung erfolgen. Die Intensität der Waffenwirkung muss aber dem Verhältnismässigkeitsprinzip entsprechen. Überschreitet die Selbstverteidigung diesen Rahmen, wird sie selbst zur verbotenen Gewalt.

3.2.2.3. Umstrittene präventive Selbstverteidigung

Eine wesentliche Frage ist der Zeitpunkt, wann die Anwendung von Gewalt zur Selbstverteidigung gerechtfertigt ist. Grundsätzlich ist die Selbstverteidigung nur erlaubt, wenn ein Angriff schon stattgefunden hat. Umstritten ist, ob Selbstverteidigung erlaubt ist, falls ein bewaffneter Angriff unmittelbar bevorsteht (Caroline Fall aus dem Jahr 1837, „*cases in which the necessity of self-defence is instant, overwhelming and leaving no choice of means, an no moment for deliberation*“). Die Problematik besteht hier in der Grauzone des Terms „unmittelbar“, deren Abgrenzung der individuellen, kaum nachprüfbaren Entscheidung des angreifenden Staates obliegt[85].

---

[83] ICJ, “Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. USA)”, *ICJ Reports* 1986, S. 104: “But the Court does not believe that the concept of ‘armed attack’ includes not only acts by armed bands where such acts occur on a significant scale but also assistance to rebels in the form of the provision of weapons or logistical or other support. Such assistance may be regarded as a threat or use of force, or amount to intervention in the internal or external affairs of other States.” In der Lehre umstritten, siehe IPSEN (Fn. 67), S. 1087

[84] Siehe 3.4.

[85] Vgl. zur „Grauzone“ IPSEN (Fn. 67), S. 1089.

Allerdings ist es einem Staat angesichts der modernen Waffen und Bedrohungen kaum zuzumuten, mit der Vornahme von Abwehrhandlungen zuzuwarten, bis ein Angriff effektiv stattgefunden hat. Für entsprechende militärische Massnahmen bedarf es aber einer schwerwiegenden, imminenten und klar nachweisbaren Gefahr; eine blosse erhöhte Bedrohungslage oder Vorhersehbarkeit eines Angriffs allein genügt nicht.

Die Vorverlagerung der präventiven Selbstverteidigung, wie sie die US-Doktrin seit 2002 mit *preemptive strikes* (vorbeugende Schläge) vorsieht, verstösst jedoch gegen die geltende Auffassung im Völkerrecht. Vor dem Angriff der USA auf den Irak im Jahr 2003 haben verschiedene Mitglieder des Sicherheitsrates ihre Ablehnung eines solchen ausgedehnten Rechts auf präventive Selbstverteidigung bekräftigt. Nach dem Irak-Krieg kann man heute davon ausgehen, dass die Mehrheit der Staatengemeinschaft dies ablehnt.

3.2.2.4. Staatlicher bewaffneter Angriff und indirekter staatlicher bewaffneter Angriff

Damit Selbstverteidigung legitim ist, muss der bewaffnete Angriff einem Staat zurechenbar sein. Im Fall von Angriffen über Computernetzwerke kann die Zuordnung, wie schon oben unter dem Gewaltverbot aufgeführt, besonders heikel sein. Es ist jedoch davon auszugehen, dass ein solcher Angriff Teil einer Gesamtoperation ist, die im gegebenen Fall genau zu analysieren ist.
Selbstverteidigung ist auch gegen indirekte Gewalt durch einen Staat zulässig, wenn sie die Schwelle des bewaffneten Angriffs erreicht. Im Nicaragua-Urteil hat der IGH die „Entsendung" bewaffneter Gruppen „durch oder im Auftrag eines Staates" als bewaffneten Angriff bezeichnet, wenn die mit Waffengewalt ausgeführten Handlungen durch ihren Umfang und ihre Auswirkungen über blosse Grenzvorfälle hinausgehen. Allein die zur Verfügungstellung von Waffen oder die logistische Unterstützung von Rebellen oder Banden stellen jedoch keinen bewaffneten Angriff, auch wenn sie das Gewaltverbot verletzen. Das bedeutet also, dass allein die Ausbildung von Hackern, die einen bewaffneten Angriff über Computernetzwerke durchführen, nicht zur umfassenden Selbstverteidigung gegen diesen Staat berechtigen würde. Die Hacker müssten auch im Auftrag dieses betreffenden Staates handeln.

Ein besonderes Problem ergibt sich in diesem Zusammenhang bei der Gewaltausübung von terroristischen Gruppen, wenn die Folgen der Gewaltausübung einem bewaffneten Angriff gleich kommen, die Terroristen jedoch nicht unter der Kontrolle des betreffenden Staates, von welchem der Angriff ausging, stehen. Im Fall des Angriffs vom 11. September 2001 hat der Sicherheitsrat in Resolution 1368 ein Recht der USA auf individuelle und kollektive Selbstverteidigung festgestellt. Al Quaida stand nicht unter der Kontrolle des Talibanregimes. Doch war im Falle Afghanistans die Unterstützung des Talibanregimes für die Terrorgruppe Al Quaida durch Resolutionen des Sicherheitsrates belegt[86]. Allein die Behauptung, ein anderer Staat beherberge Terroristen oder unterstütze sie ohne den Nachweis der Verbindung zu den verübten Gewaltakten, ist gemäss Staatenpraxis und Rechtssprechung des IGH nicht ausreichend zur Geltendmachung des Selbstverteidigungsrechts[87].

3.2.2.5. Keine militärische Repressalien

Das Selbstverteidigungsrecht setzt grundsätzlich nicht nur voraus, dass ein bewaffneter Angriff schon besteht oder unmittelbar bevorsteht, sondern dass er ausserdem

[86] RES SR 1214 (1998), RES SR 1257 (1999); siehe hierzu Diskussion in IPSEN (Fn. 67), PETERS (Fn. 67) und BOTHE (Fn. 67).

[87] Siehe auch IGH-Gutachten Sperrmauerfall: ICJ, "Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory", Advisory Opinion, *ICJ Reports* 2004 sowie *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (Fn. 72).

noch im Gang ist. Die bewaffnete Repressalie als Sanktion gegen einen früher erfolgten, aber nicht mehr bestehenden Angriff ist unzulässig.

Folgerung: *Für die legitime Selbstverteidigung beim Angriff auf die Computernetzwerke eines Staates müssen folgende Voraussetzungen kumulativ erfüllt sein*: *1) Der Angriff auf das Computernetzwerk muss dieselbe Wirkung wie physische Waffengewalt haben 2) er muss eine gewisse Intensität erreichen, 3) er muss einem Staat zurechenbar sei, d. h. die Hacker müssen im Auftrag des betreffenden Staates handeln; 4) ein Angriff muss erfolgt und noch im Gang sein oder unmittelbar und unausweichlich bevorstehen. Sind diese Voraussetzungen erfüllt, ist Selbstverteidigung mit jeglicher Waffenart legitim, solange sie das Prinzip der Verhältnismässigkeit einhält. Ist eine der Voraussetzungen nicht erfüllt, liegt kein umfassendes individuelles oder kollektives Selbstverteidigungsrecht gemäss UNO-Charta Art. 51 vor. Mögliche Optionen sind Massnahmen der kollektiven Sicherheit oder eine staatliche Reaktion auf die Verletzung des Interventionsverbots.*

3.2.3. UN-System der kollektiven Sicherheit

Das System der kollektiven Sicherheit der UNO gemäss Charta Kapitel VII ist das wesentliche Korrelat zum absoluten Gewaltverbot. Grundsätzlich sieht der Charta-Wortlaut vor, dass auch das Selbstverteidigungsrecht nur solange ausgeübt werden darf, bis der Sicherheitsrat eigene Massnahmen beschlossen hat. Dieser „Vorrang" von Massnahmen des Sicherheitsrates gegenüber dem Selbstverteidigungsrecht des angegriffenen Staates hat in der bisherigen Praxis jedoch kaum Bedeutung erlangt.

Im Fall, dass ein Angriff durch Computernetzwerke erfolgt ist, stellt sich die Frage, wie der Sicherheitsrat aktiv werden kann.

Gemäss Art. 39 UNO-Charta kann der Sicherheitsrat nicht-militärische und militärische Zwangsmassnahmen ergreifen, falls eine der drei Situationen vorliegen: Bedrohung des Friedens, Bruch des Friedens oder Angriffshandlung.

Angriffe durch Computernetzwerke, die mit militärischer Gewalt gleichzusetzen sind, können als ein Bruch des Friedens oder als eine Angriffshandlung gelten[88]. Dem Sicherheitsrat steht auch die Möglichkeit offen, Massnahmen gemäss Kapitel VII zu ergreifen, wenn er nur eine „Bedrohung des Friedens" feststellt. Dabei sieht Kapitel VII UNO-Charta eine stufenweise Folge von möglichen Massnahmen vor, die von nicht-militärischer bis zu militärischer Natur reichen. Welche Massnahmen der Sicherheitsrat im einzelnen Fall ergreift, ist in seinem Ermessen. Wenn es also zweifelhaft ist, ob ein Angriff durch ein Computernetzwerk mit militärischer Gewalt gleichgesetzt werden kann, wie z.B. ein Angriff auf das Zahlungs-, Banken- oder Börsensystem eines Landes, kann der Sicherheitsrat dennoch Massnahmen gemäss Kapitel VII anordnen. Die Kompetenzen des Sicherheitsrates gehen also weiter als das individuelle und kollektive Selbstverteidigungsrecht gemäss Art. 51 UNO-Charta.

Folgerung: *Das System der kollektiven Sicherheit erlaubt mehr Optionen für die Reaktion auf einen Angriff auf Computernetzwerke als das individuelle und kollektive Selbstverteidigungsrecht gemäss Art. 51 UNO-Charta.*

3.3. CNO und das Interventionsverbot

Unter Intervention wird die direkte oder indirekte Einmischung eines Staates mit Zwangsmitteln in die inneren und äusseren Angelegenheiten eines anderen Staates verstanden. Das Interventionsverbot gilt gewohnheitsrechtlich und folgt letztlich aus

[88] Der Begriff „Angriffshandlungen" ist nach überwiegender Meinung auch weiter als der Begriff des „bewaffneten Angriffs" im Sinne von Art. 51 UNO-Charta; siehe PETERS (Fn. 67), S. 324.

dem Prinzip der souveränen Gleichheit der Staaten, das auch in der UNO-Charta Art. 2 Abs. 1 verankert ist[89].

3.3.1. Inhalt des Interventionsverbots

Jeder Verstoss gegen das Gewaltverbot ist auch ein Verstoss gegen das Interventionsverbot. Das Interventionsverbot geht über das Gewaltverbot hinaus und kann auch wirtschaftlichen, politischen oder sonstigen Zwang beinhalten. Die Abgrenzung zwischen noch erlaubter Einwirkung und verbotenem Zwang ist jedoch im generellen nicht eindeutig vorzunehmen, sondern muss von Fall zu Fall beurteilt werden. Dies trifft insbesondere auch beim wirtschaftlichen Zwang zu. Es gibt keinen völkergewohnheitsrechtlichen Anspruch auf internationale Handelsbeziehungen oder Wirtschaftshilfe. Es kann aber z.B. davon ausgegangen werden, dass ein Angriff über Computernetzwerke, der das Bankennetzwerk eines Landes zerstört, eine unerlaubte Intervention ist. Schwierig ist auch die Abgrenzungsfrage bei der „subversiven Intervention" durch jegliche inhaltliche Manipulation, die über Computernetzwerke erfolgen kann.

Wie das Gewaltverbot kann auch das Interventionsverbot auf indirekte Weise verletzt werden. Es stellen sich ähnliche Zurechnungsfragen wie bei der indirekten Gewaltausübung und beim indirekten bewaffneten Angriff[90]. Der Staat muss grundsätzlich auch hier in erheblichem Mass an der nicht-staatlichen, verbotenen Intervention beteiligt sein. Subversive Propaganda gilt grundsätzlich nicht als Verstoss gegen das Interventionsverbot, wenn der Staat, von dessen Gebiet aus sie erfolgt, die Propaganda duldet, nicht jedoch kontrolliert[91].

3.3.2. Reaktion auf verbotene Intervention

CNA, die mit wirtschaftlichen Zwang verbunden sind, wie z.B. die Zerstörung von Bankennetzwerken, aber nicht die Schwelle des bewaffneten Angriffs überschreiten, erlauben nicht, das umfassende Recht der individuellen oder kollektiven Selbstverteidigung in Anspruch zu nehmen.

Als Reaktion auf solche Angriffe über Computernetzwerke eröffnen sich dem Staat gemäss Völkerrecht verschiedene Abwehrmassnahmen. Gemäss UNO-Charta Art. 2 Abs. 3 sind die Staaten verpflichtet, Streitigkeiten untereinander friedlich beizulegen. Hierzu gehören diplomatische Verfahren, die Einsetzung von Schiedsgerichten oder die Anrufung des Internationalen Gerichtshofs in Den Haag, IGH. Eine Möglichkeit ist auch, dass die internationale Staatengemeinschaft in einem solchen Fall tätig wird, und der Sicherheitsrat eine „Bedrohung des Friedens" feststellt und Zwangsmassnahmen gemäss Kapitel VII ergreift.

Schliesslich kennt das Völkerrecht als Gegenmassnahme auch unilaterale Sanktionen, bzw. die Retorsion und die Repressalie[92].

Eine Retorsion ist ein unfreundlicher Akt, der selbst aber nicht völkerrechtswidrig ist. Beispiele für eine Retorsion sind der Nichtabschluss eines für die Gegenseite interessanten Vertrags oder der Abbruch diplomatischer Beziehungen. Retorsionen müssen nach herkömmlicher Meinung nicht verhältnismässig sein, da sie an sich kein völkerrechtswidriges Handeln darstellen. Es beginnt sich jedoch auch hier die Meinung durchzusetzen, dass das Gebot der Verhältnismässigkeit einzuhalten ist.

[89] Zum Interventionsverbot siehe PETERS (Fn. 67); IPSEN (Fn. 67); KÄLIN (Fn. 67).

[90] Siehe unter 3.2.2.4.

[91] VPB 61 (1997), Nr. 129, S. 1030.

[92] Siehe hierzu PETERS (Fn. 67), IPSEN (Fn. 67).

Eine Repressalie ist ein an sich völkerrechtswidriger Akt, mit dem ein Staat auf ein völkerrechtswidriges Verhalten eines anderen Staates reagiert. Als Reaktion auf einen völkerrechtswidrigen Akt wird die Repressalie völkerrechtlich legitimiert. Damit eine solche Repressalie aber völkerrechtsmässig wird, sind gewisse Voraussetzungen zu beachten: So ist das Gebot der Verhältnismässigkeit einzuhalten und die Gegenseite muss vorgängig über die Repressalie informiert werden. Das Gebot der Verhältnismässigkeit verlangt, dass die Repressalie nicht als „Bestrafung" durchgeführt wird, sondern ausschliesslich zum Ziel hat, die völkerrechtsmässige Lage wieder herzustellen. Ausserdem dürfen Rechte dritter Staaten durch die Repressalie nicht beeinträchtigt werden. Es ist umstritten, ob ein Staat zunächst die vorhandenen Mittel zur friedlichen Streitbeilegung erschöpft haben muss, bevor er zum Mittel der Repressalie greifen darf. Die Schweiz kennt aber die Tradition, sich grundsätzlich für die friedliche Beilegung von Streitigkeiten einzusetzen.

Der Abbruch von Wirtschaftsbeziehungen oder die Diskriminierung in den Handelsbeziehungen ist grundsätzlich kein völkerrechtswidriges Handeln, wenn dabei nicht WTO-Regeln oder andere internationale Abkommen verletzt werden.

Folgerung: *Computerangriffe, die nicht physischer Waffengewalt entsprechen, wie z. Bsp. die Zerstörung des Computernetzes eines Bankensystems, verletzen nicht das Gewaltverbot, aber das Interventionsverbot, wenn ein solcher Angriff einem Staat zurechenbar ist. Ein Staat kann als Reaktion keine militärische Gewalt anwenden. Er kann sich gegen solche Angriffe über Massnahmen der kollektiven Sicherheit oder Mittel der friedlichen Streitbeilegung verteidigen. Auch Retorsion oder Repressalie sind nicht ausgeschlossen, vorausgesetzt der Computerangriff kann einem Staat zugerechnet werden.*

3.3.3. CNE und das Interventionsverbot

Schliesslich stellt sich noch die Frage, ob das blosse Eindringen in Computernetzwerke durch ein staatliches Organ oder im Auftrag eines Staates mit dem Ziel, Informationen zu beschaffen, völkerrechtswidrig ist.

Auch hier ist weder eine Staatenpraxis bekannt, noch besteht eine völkerrechtliche Vereinbarung.

Eine Analogie zur Spionage bietet sich hier an: Spionage wird in der Staatenpraxis kaum als völkerrechtswidriger Akt eingestuft. Staaten beantworten den Tatbestand der Spionage in der Regel nicht durch Repressalien, das heisst völkerrechtswidrige Handlungen, sondern stufen Spionage als „unfreundlichen Akt" ein.

Es ist in der Lehre jedoch umstritten, ob Spionage als Verletzung des völkerrechtlichen Interventionsverbots gilt[93]. Spionage verletzt meistens nationale Rechtsbestimmungen von Staaten, genauso wie auch das Eindringen in fremde Computernetzwerke von vielen Staaten strafrechtlich verfolgt wird.

Die Tatsache, dass Spionage im Völkerrecht grundsätzlich nicht verboten ist, bedeutet aber nicht, dass die Spione selbst sich in einem innerstaatlichen Verfahren auf das Völkerrecht als Rechtfertigungsgrund berufen können[94].

Eines der Probleme, das CNE aufwirft, ist, dass die Spionage über Computernetzwerke in keiner Weise den physischen Aufenthalt eines „Spions" im Territorium und damit im Rechtsraum des Staates bedingt, der ausspioniert wird. Es besteht keine völkerrechtliche Pflicht zur Auslieferung von Spionen.

[93] JOHN A. RADSAN: "The unresolved equation of espionage and international law", in *Michigan Journal of International Law*, S. 595-634.

[94] GRAF VITZHUM (Fn. 67), S. 143 f.

Folgerung: *Das Völkerrecht verbietet CNE nicht. In Analogie zur Spionage kann CNE als „unfreundlicher Akt" eingestuft werden. Dies gilt grundsätzlich für jegliches verdecktes Eindringen in Computernetzwerke zur Informationsbeschaffung, auch wenn dies zum Zweck hat, CND-basiertes Wissen über gegnerische Fähigkeiten zu sammeln*.

3.4. CNO und *ius in bello*

Das humanitäre Völkerrecht kommt nur in bewaffneten Konflikten zur Anwendung und erfüllt zwei Aufgaben: Es regelt die Führung der Kampfhandlungen und schützt alle Personen, die nicht oder nicht mehr an den Kampfhandlungen teilnehmen. Die Frage nach der Rechtmässigkeit eines Kriegs (*ius ad bellum*), die oben ausgeführt worden ist, beantwortet es jedoch nicht. Das humanitäre Völkerrecht gilt in jedem bewaffneten Konflikt, unabhängig davon, ob die Teilnahme "rechtmässig" ist oder nicht. Es gilt für alle Konfliktparteien.

Es ist unbestritten, dass das humanitäre Völkerrecht mit all seinen Prinzipien und Regeln auch auf Angriffshandlungen über Computernetzwerke anwendbar ist, die im Rahmen eines bewaffneten Konfliktes durchgeführt werden[95]. Da sich diese aber von den traditionellen Kriegsmethoden unterscheiden, ist die konkrete Umsetzung mit einer Reihe von Fragen behaftet.

3.4.1. "Angriffe" im humanitären Völkerrecht und CNO

„Angriffe" im humanitären Völkerrecht umfassen sowohl Angriffshandlungen als auch Verteidigungsmassnahmen. Die Definition von "Angriff" im humanitären Völkerrecht ist vom „bewaffneten Angriff" im *ius ad bellum* zu unterscheiden[96]. Gemäss Art. 49 Abs. 1 Zusatzprotokoll I[97] bezeichnet der Begriff „Angriffe" „*sowohl eine offensive als auch eine defensive Gewaltanwendung gegen den Gegner*". Wenn im Folgenden von „Angriffen" gesprochen wird, gilt dies deshalb sowohl für Angriffshandlungen über Computernetzwerke wie auch für Verteidigungsmassnahmen.

Bei der Definition des Angriffs im Sinne des humanitären Völkerrechts kommt es nicht auf die Handlung selbst und die eingesetzten Mittel, sondern vielmehr auf die Auswirkungen an. Ein Angriff liegt vor, wenn er bestimmte Auswirkungen wie Verletzungen oder den Tod von Menschen, die Zufügung von Schaden oder die Zerstörung von Sachwerten verursacht[98]. „Angriffe" über Computernetzwerke sind nur als Angriffe im Sinne des humanitären Völkerrechts einzustufen, wenn sie Verletzungen, Tod, Schaden oder Zerstörungen zufügen. CNA, das keine von den zitierten Folgen verursacht, ist nach dem humanitären Völkerrecht in der Regel erlaubt.

3.4.2. Grundlegende Prinzipien des humanitären Völkerrechts

Es sind sowohl das gesamte kodifizierte humanitäre Völkerrecht über die Kriegsführung (die vier Genfer Konventionen von 1949 und die zwei Zusatzprotokolle von 1977) als auch das humanitäre Völkergewohnheitsrecht auf „Angriffe" über Computernetzwerk anwendbar. Anschliessend werden jedoch nur die grundlegenden Prinzipien des humanitären Völkerrechts kurz beschrieben. Die Verletzung eines dieser Prinzipien führt direkt zu einer Verletzung des humanitären Völkerrechts.

---

[95] International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law: Chairman's Conclusions, Stockholm, 17-19 November 2004; FALKO DITTMAR, Angriffe auf Computernetzwerke, Ius ad bellum und ius in bello, Berlin 2005; Michael N. Schmitt, CNA and The Jus in Bello : An Introduction (CNA), in Byström Karin, Proceedings of the International Expert Conference on Computer Attacks and the Applicability of International Humanitarian Law, Stockholm, Swedish National Defense College, 2004.

[96] Siehe unter 3.2.2.1.

[97] SR 0.518.521.

[98] Vgl. SCHMITT (Fn. 68), S. 112-113 ff.

3.4.2.1. Unterscheidungsprinzip

Das Unterscheidungsprinzip verpflichtet eine Konfliktpartei, jederzeit zwischen Zivilpersonen und zivilen Objekte und militärischen Zielen (Kombattanten und militärische Objekte) zu unterscheiden und erlaubt nur, die letzteren anzugreifen. Dieses Prinzip ist in Art. 48 und 51 Zusatzprotokoll I geregelt und stellt eines der wichtigsten Prinzipien des Rechts der bewaffneten Konflikte dar. Es enthält drei Arten von Verpflichtungen: das Verbot, Zivilisten anzugreifen[99]; das Verbot, „Angriffe" gegen zivile Objekte zu richten; und das Verbot unterschiedloser „Angriffe", die Zivilisten oder zivilen Objekte übermässige kollaterale Schaden zufügen[100].

3.4.2.2. Vorsichtsprinzip

Das Vorsichtsprinzip ist in Art. 57 Zusatzprotokoll I geregelt (Vorsichtsmassnahmen beim Angriff). Aus dieser Norm entstehen für die Kriegsparteien verschiedene Pflichten. Sie müssen stets darauf achten, dass Zivilpersonen und zivile Objekte verschont bleiben und dass sie die „Angriffe" gezielt vorbereiten, um den geplanten Ablauf der Kriegshandlungen sicherzustellen. Die Kriegsparteien sind insbesondere verpflichtet, „Angriffe" endgültig oder vorläufig einzustellen, wenn sich erweist, dass ihr Ziel nicht militärischer Art ist, oder wenn sie das Verhältnismässigkeitsprinzip verletzen.

3.4.2.3. Prinzip der Verhältnismässigkeit

Das Ziel des Krieges ist, die gegnerische Seite durch Gewaltanwendung zu kontrollieren und sie zur Aufgabe zu zwingen und dabei den geringsten möglichen Schaden an Zivilpersonen und zivilen Objekte zu verursachen[101]. Das Verhältnismässigkeitsprinzip trägt der Tatsache Rechnung, dass „Angriffe" auf militärische Ziele auch zu Schäden unter der Zivilbevölkerung oder an zivilen Objekten führen können (Kollateralschäden)[102]. Das Verhältnismässigkeitsprinzip verpflichtet den Angreifer, „*von jedem Angriff Abstand zu nehmen, bei dem damit zu rechnen ist, dass er auch Verluste unter der Zivilbevölkerung, die Verwundung von Zivilpersonen, die Beschädigung ziviler Objekte oder mehrere derartige Folgen zusammen verursacht, die in keinem Verhältnis zum erwarteten konkreten und unmittelbaren militärischen Vorteil stehen*"[103]. Die Kriegsparteien sind also verpflichtet, jene Mittel und Methoden zu wählen die mit Blick auf den zu erwartenden militärischen Vorteil verhältnismässig sind. Damit ein Angriff" verhältnismässig ist, muss er mit Blick auf das angestrebte Ziel geeignet, notwendig und zumutbar sein. Der „Angriff" ist geeignet, wenn er ermöglicht, das Ziel zu erreichen; er ist notwendig, wenn keine andere, ebenfalls geeignete aber mildere Massnahme das anvisierte Ziel ebenso erreicht; und er ist zumutbar, wenn ein vernünftiges Verhältnis zwischen Ziel und „Angriff" besteht.

3.4.3. Ausgewählte Fragen bezüglich CNO

Da „Angriffe" über Computernetzwerke eine neue, von den traditionellen Methoden unterschiedliche Kriegsmethode darstellen, sind viele Fragen, wie das humanitäre Völkerrecht bei solchen „Angriffen" umzusetzen ist, noch nicht klar beantwortet. Erst seit kurzem wird von Expertengruppen, zusammengesetzt aus Juristen und Informa-

[99] Diese Regel gilt aber nicht wenn Zivilpersonen direkt an Feindseligkeiten teilnehmen und wenn zivile Objekte für militärische Zwecke verwendet werden.

[100] Vgl. ROBERT KOLB, Ius in bello, Le droit international des conflits armés: Précis, Basel, 2003, S. 115.

[101] Vgl. KOLB (Fn. 94), S. 58.

[102] Vgl. DITTMAR (Fn. 68), S. 247 f.

[103] Art. 57 Abs. 2 lit. a Zusatzprotokoll I.

tikern, versucht, eine Antwort auf diese Fragen zu finden[104]. Es existiert bis anhin auch keine gefestigte Staatenpraxis.

Die nächsten Paragraphen werden einen kurzen Einblick in die verschiedenen Fragen erlauben, die sich spezifisch bei „Angriffen" über Computernetzwerke stellen. Diese Illustration ist aber nicht umfassend, sondern wirft nur die ersten offensichtlichen Fragen auf, die sich im Hinblick auf die drei grundlegenden Prinzipien des humanitären Völkerrechts ergeben.

Ein erstes Problem ist, dass CNO durch selbstfortpflanzende Codes, Viren, Würmer, logische Bomben usw. charakterisiert ist. Diese Viren können sich über Computernetzwerke ohne Unterscheidung zwischen militärischen Zielen und Zivilpersonen oder zivilen Objekten verbreiten, ohne dass sie vom Angreifer kontrolliert werden können. Es besteht also die Gefahr, dass „Angriffe" über Computernetzwerke das Unterscheidungsprinzip verletzen[105].

Dieses Prinzip wird auch verletzt, wenn bei „Angriffen" nicht klar zwischen militärischen und zivilen Systemen unterschieden werden kann. Oft bestehen Interdependenzen: das Militär und die Armee sind in zunehmendem Masse von den zivilen Systemen abhängig, beispielsweise für die Telekommunikation[106].

Eine weitere Charakteristik von solchen „Angriffen" über Computernetzwerke ist, dass sie aus geographischer Distanz geführt werden. Dieser Aspekt bringt zwei wichtige Probleme mit sich, die insbesondere das Vorsichtsprinzip verletzen können. Erstens besteht aufgrund der Distanz zum angezielten Objekt die Gefahr, ein Objekt irrtümlicherweise als militärisches Ziel zu bestimmen. Zweitens ist es äusserst schwierig, einen Erstschlag zurückzuverfolgen, weshalb die Gefahr besteht, dass die Gegenpartei den Gegenschlag auf das falsche Ziel richtet.

Die Tatsache, dass bei „Angriffen" über Computernetzwerke die Einhaltung sowohl des Unterscheidungsprinzips als auch des Vorsichtsprinzips mit Schwierigkeiten behaftet ist, hat zur Folge dass auch das Verhältnismässigkeitsprinzip problematisch ist. „Angriffe" über Computernetzwerke können eine Kaskade von Wirkungen verursachen, die sowohl militärische als auch zivile Objekte treffen und deren Ausmass schwer voraussehbar sein kann.

In Zusammenhang mit „Angriffen" über Computernetzwerke stellt sich also die Frage, ob der Angreifer die konkreten technischen Möglichkeit hat, die militärischen Netzwerke von den zivilen zu trennen, die Herkunft und das Ziel des „Angriffs" präzis zu identifizieren und Kaskadenwirkungen zu vermeiden, um zunächst die drei grundlegenden Prinzipien des humanitären Völkerrechts zu respektieren.

Ein besonderes Problem stellt auch die Frage des Status von an Kampfhandlungen beteiligten Personen dar. Konkret geht es dabei etwa um die Frage, ob eine durch eine Zivilperson ausgeführte Handlung als direkte Teilnahme an Feindseligkeiten zu qualifizieren ist. Wie erwähnt können Angriffe über Computernetzwerke aus grosser geographischer Distanz geführt werden. Die Person, die den Angriff ausführt, ist eventuell nicht ein Angehöriger der Streitkräfte, sondern ein ziviler Computerspezialist. Und diese Person könnte sich sogar in einem Land befinden, welches nicht Kon-

[104] Vom 17. bis zum 19. November 2004 wurde in Stockholm eine Expertenkonferenz durchgeführt, mit dem Ziel, die Diskussion über CNA und CND zu beginnen. Während dieser Konferenz wurde festgestellt, dass das humanitäre Völkerrecht auch für „Angriffe" auf Computernetzwerke zur Anwendung kommt. Es wurden auch verschiedene Probleme, die mit dieser neuen Kriegsmethode verbunden sind, identifiziert. Mehr hierzu unter 4.2.

[105] Vgl. DAVIS BROWN, A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict, Harvard International Law Journal, Vol. 47, n°1, 2006, S. 22.

[106] Vgl. DITTMAR (Fn. 68), S. 242.

fliktpartei ist. Die Ausführung eines Angriffs stellt eine direkte Teilnahme an Feindseligkeiten dar. Wie ist aber der Unterhalt des Systems zu beurteilen, über welches Angriffe ausgeführt werden, oder die Verteidigung eines solchen Systems durch Sicherheitsmassnahmen gegen Angriffe? Und wie kann gegen eine Zivilperson vorgegangen werden, die aufgrund ihrer Teilnahme an Feindseligkeiten den Schutz vor direkten Angriffen verloren hat, insbesondere wen sie sich in einem Drittland befindet?

Diese kurze Illustration zeigt auf, dass für die rechtliche Analyse, wie die Prinzipien und Regeln des humanitären Völkerrechts durch CNO einzuhalten sind, eine umfassende Analyse der technischen und praktischen Fragen Voraussetzung ist.

Folgerung: *Das humanitäre Völkerrecht ist grundsätzlich auch auf Kampfhandlungen anwendbar, die durch Computernetzwerke durchgeführt werden. Viele einzelne Rechtsfragen sind jedoch noch offen. Deren Beantwortung setzt eine umfassende technische und praktische Analyse voraus*.

3.5. CNO und Neutralitätsrecht

Für die Schweiz von besonderem Interesse ist, welche neutralitätsrechtlichen Fragen durch CNO aufgeworfen werden.

Das Neutralitätsrecht kommt zur Anwendung, wenn ein zwischenstaatlicher bewaffneter Konflikt besteht. Im Fall von militärischen Massnahmen, die durch den Sicherheitsrat beschlossen worden sind, kommt das Neutralitätsrecht, das seine Grundlagen noch im klassischen Kriegsrecht hat, nicht zur Anwendung.

Vorausgeschickt wird die grundsätzliche Pflicht des Neutralen, nicht gegen das Gewaltverbot zu verstossen[107].

3.5.1. Territorium des Neutralen

Besteht ein zwischenstaatlicher bewaffneter Konflikt, hat ein neutraler Staat die Pflicht, sein Territorium den Kriegsparteien nicht zur Verfügung zu stellen. Damit hat er auch die Pflicht, dieses Territorium zu verteidigen. Umgekehrt haben die Kriegsparteien die territoriale Unversehrtheit des Neutralen zu respektieren.

Diese auf das Territorium bezogenen Pflichten und Rechte des Neutralen werfen im Fall von CNO einige Fragen auf. Würde der *Cyber Space* als eigener Raum, wie z.B. der Luftraum aufgefasst werden, hätte dies zur Folge, dass der Neutrale sein Datennetz für die Kriegsparteien sperren müsste und umgekehrt, die Kriegsparteien darauf verzichten müssten, dieses Datennetz zu missbrauchen.

Doch anders als Flugzeuge, werden Daten auf ihrem Weg zum Ziel nicht gesteuert. Oft ist nicht einmal absehbar, welchen Weg Daten im internationalen Verkehr nehmen. Während ein Luftraum für spezifische Flugobjekte gesperrt werden kann, ist dies bei Daten viel weniger offensichtlich. Ausserdem werden Daten auch über Satelliten übertragen, die sich im Weltraum und damit ausserhalb des Anwendungsbereichs des Neutralitätsrechts befinden.

Generell wird deshalb angenommen, dass der virtuelle Raum des *Cyber Space* nicht vom Grundsatz erfasst wird, dass der Neutrale sein Territorium für Kriegsparteien zu sperren hat. Umgekehrt verletzen Kriegsparteien nicht das Neutralitätsrecht, wenn bei Kampfhandlungen über Computernetzwerke Daten über neutrale Datennetze fliessen[108].

[107] Siehe oben unter 3.2.1.

[108] Vgl. auch DITTMAR (Fn. 68), S. 263 ff.

Die Folgerung, dass der Neutrale im Kriegsfall die Datennetze nicht für die Kriegsparteien zu sperren hat, ergibt sich in übertragender Anwendung auch aus Art. 8 Haager Konvention, wonach eine neutrale Macht nicht verpflichtet ist, „für Kriegführende die Benutzung von Telegraphen- oder Fernsprechleitungen sowie Anlagen für drahtlose Telegrafie, gleichviel, ob sie ihr selbst oder Gesellschaften oder Privatpersonen gehören, zu untersagen oder zu beschränken“[109].

Das Neutralitätsrecht bedeutet aber eine Schranke für den Einsatz von Waffen, die weiträumige Schäden verursachen[110]. Das neutrale Staatsgebiet muss von etwaigen Nebenwirkungen der Kampfhandlungen verschont bleiben. Es ist den Kriegsparteien deshalb grundsätzlich nicht erlaubt, durch ihre über Computernetze durchgeführten Kampfhandlungen die Datennetze von Neutralen zu schädigen.

3.5.2. Keine staatliche Unterstützung der Kriegsparteien

Ein neutraler Staat darf Kriegsparteien weder durch Truppen noch durch eigene Waffen unterstützen. Übertragen auf militärische CNO im Rahmen von bewaffneten Konflikten bedeutet dies, dass ein neutraler Staat den Konfliktparteien die Nutzung seiner militärischen Netzwerke nicht gestatten darf. Militärische Netzwerke sind grundsätzlich abgeschirmt und nicht allgemein zugänglich.

Folgerung: *Der Neutrale muss im Fall eines zwischenstaatlichen Konflikts nicht die allgemein zugänglichen Datennetze sperren, um zu verhindern, dass Konfliktparteien diese für einen Angriff über Computernetzwerke missbrauchen könnten. Militärische Netzwerke dürfen Konfliktparteien aber nicht zur Verfügung gestellt werden und müssen deshalb abgeschirmt werden können.*

4. Internationale Bestrebungen

4.1. Europaratskonvention über die Cyber-Kriminalität

Ausgehend vom materiellen Geltungsbereich der Konvention werden Kampfhandlungen nicht ausgeschlossen. In diesem Sinne werden sich zukünftig CNO grundsätzlich auch an der Europarats-Konvention über die Cyber-Kriminalität von 2001 messen lassen müssen.

Die am 1. Juli 2004 in Kraft getretene Europaratskonvention über die Cyberkriminalität vom 23. November 2001 ist das erste und bisher einzige internationale Übereinkommen, das sich mit Computer- und Netzwerkkriminalität befasst. Sie verpflichtet die Vertragsstaaten, ihr Straf- und Strafprozessrecht sowie die Bestimmungen über die internationale Zusammenarbeit in Strafsachen der fortgeschrittenen Informationstechnologie anzupassen. Es geht nicht um eine Konvention, in welcher CNO grundsätzlich in Frage gestellt würden, sondern darum, Rahmenbedingungen für das nationale Strafrecht zu setzen.

In einem ersten Teil enthält die Konvention materielle Strafbestimmungen. Ziel ist eine Harmonisierung des Strafrechts unter den Staaten. Im Hinblick auf CNO von Bedeutung sind insbesondere die Artikel 2 bis 6 der Konvention (rechtswidriger Zugang, rechtswidriges Abfangen, Dateneingriff und Systemeingriff, Missbrauch von Vorrichtungen). Im vorliegenden Zusammenhang dürfte v.a. Art. 2 (Rechtswidriger Zugang) relevant sein. Bei einer entsprechenden Umsetzung würde vermutlich Art. 143bis StGB ergänzt[111]. In einem zweiten Teil der Konvention werden Regelungen für

[109] SR 0.515.21.

[110] Vgl. auch BOTHE (Fn. 67), S. 714.

[111] Die Bestimmung lautet:

das Strafverfahren getroffen. Es geht um Fragen der Beweiserhebung und Beweissicherung von elektronischen Daten in der Strafuntersuchung. Schliesslich behandelt das Übereinkommen die internationale Zusammenarbeit in Strafsachen zwischen den Staaten. Das Zusammenwirken zwischen den verschiedenen Vertragsparteien soll in seinem Ablauf schnell und effizient gestaltet werden.

Die Schweiz hat das Übereinkommen am 23. November 2001 unterzeichnet. Es ist vorgesehen, die Vernehmlassung zur Umsetzung und Ratifikation der Europaratskonvention in den ersten Monaten des Jahres 2009 zu eröffnen.

4.2. Verletzung des Humanitären Völkerrechts durch CNO

Die Schweiz, Schweden und Finnland haben anlässlich der 28. Internationalen Konferenz des Roten Kreuzes und des Roten Halbmonds das Versprechen abgegeben, auf internationaler Ebene einen Prozess zu lancieren, um die Frage der Anwendbarkeit des humanitären Völkerrechts auf Computernetzwerkgestützte Angriffe zu klären[112]. Ein erstes, von Schweden organisiertes internationales Expertentreffen fand im Dezember 2004 statt. Die Experten kamen zum Schluss, dass CNO als solche nicht dem humanitären Völkerrecht zuwiderlaufen, dass gewisse von ihnen aber eine Verletzung des humanitären Völkerrechts darstellen können[113]. Zur weiteren Klärung und Diskussion offener Fragen hat sich die Schweiz bereit erklärt, ein weiteres Expertentreffen zu veranstalten[114].

5. Antworten auf die Fragen der GPDel vom 17. Oktober 2007

Frage 1: Genügen die heutigen Rechtsgrundlagen für CND? – Nach unserer Definition von nicht-aggressivem CND genügen die heutigen Rechtsgrundlagen.

Frage 2: Welche Rechtsgrundlagen erlauben CNE und CNA durch Dienststellen des VBS? Im Rahmen welcher Einsatzarten der Armee sind heute CNE und CNA möglich? – CNE und CNA sind heute nur im Aktivdienst möglich. Für die anderen Einsatzarten bestehen keine gesetzlichen Grundlagen. Wir gehen davon aus, dass CNA nur im Aktivdienst durchgeführt werden soll; deshalb ist keine formellgesetzliche Grundlage notwendig. Will man CNE betreiben, bedingt dies eine formellgesetzliche Grundlage.

Frage 3: Wie verhalten sich die bestehenden Rechtsgrundlagen für den Nachrichtendienst (Art. 99 MG) zu allfälligen Rechtsgrundlagen für InfoOps der Armee, insbesondere die Informationsbeschaffung mittels CNE? – Die bestehende Rechtsgrundlage für den Nachrichtendienst (Art. 99 MG) erlaubt keine Informationsbeschaffung mittels CNE.

Frage 4: Welche Konsequenzen hätte die Annahme des neuen Art. 18m BWIS (Geheimes Durchsuchen eines Datenverarbeitungssystems) auf die Arbeiten im Bereich CNE und CNA im VBS? – Die Annahme des neuen Art. 18m BWIS (Geheimes

---

Art. 143[bis] Unbefugtes Eindringen in ein Datenverarbeitungssystem

Wer ohne Bereicherungsabsicht auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

[112] Vgl. auch THOMAS C. WINGFIELD, When is a Cyber Attack an "Armed Attack?" Legal Thresholds for Distinguishing Military Activities in Cyberspace, The Potomac Institute for Policy Studies, 2006.

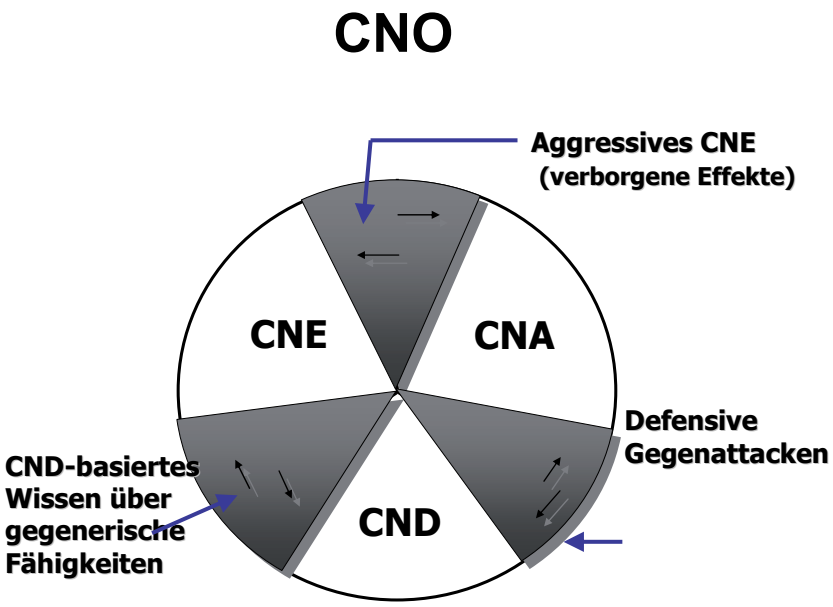
[113] Siehe dazu 3.4.

[114] Aussenpolitischer Bericht vom 15. Juni 2007, BBl 5531, 5587 f.

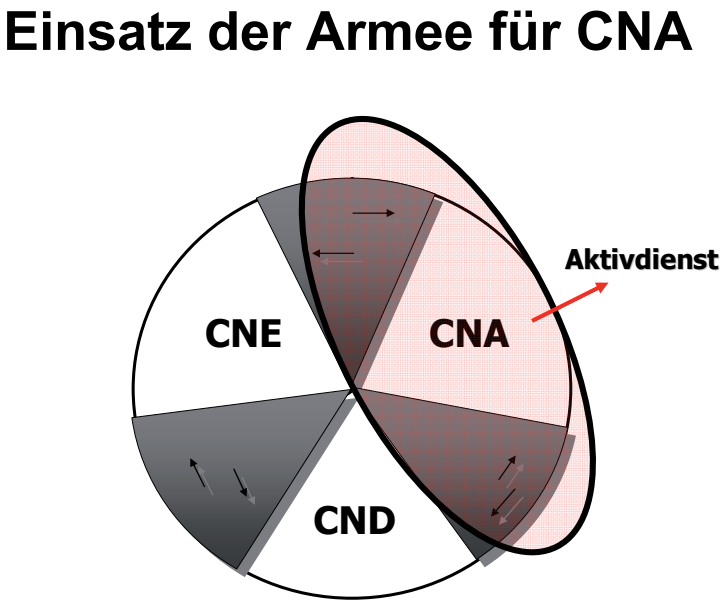
Durchsuchen eines Datenverarbeitungssystems) hätte auf die Arbeiten im Bereich CNE und CNA im VBS keine Auswirkungen, da davon nur der zuständige Nachrichtendienst betroffen ist.

Anhang

Grafik 1

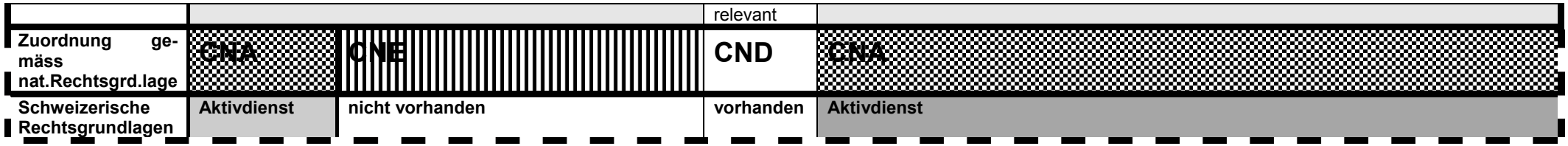


Grafik 2



Grafik 3

	CNE + (offens. CNE) **Anbringen von verborgenen Effekten als Vorbereitung für einen möglichen Angriff**	**CNE i. e. S.** **Eindringen in Datenverarbeitungsanlagen oder Entwendung von Informationen durch verborgene Effekte**	**CND +** (explorat. CND) **CND-basiertes Wissen über gegnerische Fähigkeiten durch Eindringen in Computernetzwerke**	**CND i. e. S.** **Informatiksicherheit**	**CND +** (offens. CND) **Defensive Gegenattacken als Reaktion auf gegnerisches CNA < Schwelle bewaffneter Angriff Art. 51 UNO-Charta**	**CND +** (offensives CND) **Defensive Gegenattacken als Reaktion auf gegnerisches CNA > Schwelle bewaffneter Angriff Art. 51 UNO-Charta**	**CNA i. e. S.** **Angriff über Computer, der nicht militärischer Gewalt gleichkommt.**	**CNA i. e. S.** **Angriff über Computer, der militärischer Gewalt gleichkommt**
Ius ad bellum (***ius contra bellum***) **und allgemeines Völkerrecht** *behandelt unter 3.2. und 3.3.*	verboten Verstoss gegen das Gewaltverbot *behandelt unter 3.2*	nicht verboten Verstoss gegen das Interventionsverbot? *behandelt unter 3.3.3*	nicht verboten Verstoss gegen das Interventionsverbot? *behandelt unter 3.3.3*	erlaubt	erlaubt, aber keine militärische Gewalt erlaubt Gilt für Reaktion auf direkten wie indirekten Verstoss gegen staatliches Interventionsverbot, gemäss Regeln der Staatenverantwortlichkeit Präventive Reaktion auf imminent anstehende Gefahr? *behandelt unter 3.3.*	erlaubt militärische Gewalt erlaubt Gilt für Reaktion auf direkte wie indirekte staatliche Gewalt, gemäss Regeln der Staatenverantwortlichkeit Präventive Reaktion auf imminent anstehende Gefahr? *behandelt unter 3.2*	nicht erlaubt kein Verstoss gegen das Gewaltverbot, aber gegen das Interventions-verbot Gilt für direkte wie indirekte Intervention gemäss Regeln der Staatenverantwortlichkeit. *behandelt unter 3.3.*	verboten Verstoss gegen das Gewaltverbot. Gilt für direkte wie indirekte Gewalt gemäss Regeln der Staatenverantworltichkeit *behandelt unter 3.2.*
Ius in bello **(humanitäres Völkerrecht)** *behandelt unter 3.4*	*kommt zur Anwendung, falls im Rahmen von international bewaffneten oder internen bewaffneten Konflikten gemäss Genfer Konventionen*			nicht relevant	*kommt zur Anwendung, falls im Rahmen von international bewaffneten oder internen bewaffneten Konflikten gemäss Genfer Konventionen*			
Neutralitätsrecht *behandelt unter 3.5*	*kommt zur Anwendung im Fall von zwischenstaatlichen Konflikten*			nicht neutralitäts-	*kommt zur Anwendung im Fall von zwischenstaatlichen Konflikten*			


relevant
Zuordnung gemäss nat.Rechtsgrd.lage
CNA
CNE
CND
CNA
Schweizerische Rechtsgrundlagen
Aktivdienst
nicht vorhanden
vorhanden
Aktivdienst