sandfire

Analysen Beratung Technologie Training

Analyse

# CHANCEN UND RISKEN EINES EUROPÄISCHEN NACHRICHTENDIENSTES

Günther K. Weisse und Felix Juhl

## Über die Autoren

**Günther K. Weiße** ist Senior Associate der Sandfire AG und arbeitet seit mehr als 35 Jahren in Führungs- und Sicherheitsrelevanten Positionen in der Bundeswehr und der Privatwirtschaft. Nach längerer Tätigkeit für die Deutsche Bundespost erfolgte im Jahr 1964 der Eintritt in die Bundeswehr, in die fernmelde- und elektronische Aufklärung der Luftwaffe. Es folgten Fachverwendungen in Mons/Belgien in den Bereichen Intelligence and Security beim Supreme Headquarters Allied Powers Europe (SHAPE), dem Luftwaffenkommando Süd in Messstetten sowie beim NATO Reaction Force Air Staff folgte. Bis zum Dienstende war er beim Luftwaffenkommando Süd eingesetzt. Im Rahmen der Reservedienstverhältnisse folgten Einsätze beim damaligen Amt für Nachrichtenwesen der Bundeswehr in Ahrweiler, dem Militärattachéstab an der Botschaft der Bundesrepublik Deutschland in Wien, dem Zentrum für Nachrichtenwesen sowie in der Stabsabteilung II beim Bundesministerium für Verteidigung.

**Felix Juhl** ist Senior Partner der Sandfire AG und arbeitet seit 15 Jahren in Führungspositionen in der Privatwirtschaft. Nach mehrjähriger Tätigkeit für eine Sondereinheit der deutschen Bundeswehr war Felix Juhl in leitender Führungsfunktion für verschiedene internationale Technologie- und Beratungsunternehmen tätig. Vor seinem Wechsel zur Sandfire AG verantwortete er als Head Outreach and External Affairs im International Relations and Security Network bei der Forschungsstelle für Sicherheitspolitik der ETH Zürich u.a. den Arbeitsbereich Open Source Intelligence und betreute Kooperationsprojekte mit nationalen und internationalen Partnern.

Sandfire AG Bruchmattstrasse 12 CH-6003 Lucerne
Phone +41 41 312 07 40 Fax +41 41 312 07 44 www.sandfire.ch info@sandfire.ch

sandfire

Übersicht

Die nationale Nachrichtengewinnung und Aufklärung als Aufgabe eines Staatswesens ..... 6

Die Fähigkeiten der Europäischen Union zur Nachrichtengewinnung und Aufklärung ..... 6

Die strategischen Ziele der Neuordnung des NATO-Nachrichtenwesens ..... 9

Reorganisation der US-Nachrichten- und Sicherheitsdiensten und mögliche Konsequenzen für NATO und EU ..... 11

Ausblick ..... 13

# Chancen und Risiken eines Nachrichtendienstes der Europäischen Union

Günther K. Weiße und Felix Juhl

***Zusammenfassung***

*Die Beschaffung von Informationen mit Hilfe nachrichtendienstlicher Mittel gehört neben der Verpflichtung, eigene, schutzwürdige Belange gegen Aufklärung durch fremde Mächte zu schützen, zu den originären Aufgaben der Nachrichtendienste eines Staates. Die Aufgaben werden zumeist im Rahmen nationaler Strukturen und Verfahren wahrgenommen. Aus Gründen der Opportunität pflegen nationale Dienste die Zusammenarbeit mit befreundeten Nachrichtendiensten und Partnern, meist auf bilateraler Basis. Gegenwärtig verfügt die Europäische Union noch nicht über einen eigenen, originären Nachrichtendienst. Der Wunsch der Politik nach einem gemeinsamen Europäischen Nachrichtendienst wird immer erkennbarer und bereits durch Forschungsvorhaben vorbereitet. Wenngleich die „Europäischen Nationen" auf dem Gebiet der Terrorabwehr bereits einen sehr hohen Vernetzungsgrad beim Austausch von relevanten Informationen erreicht haben, bleiben nationale Vorbehalte bei der Weitergabe von Informationen bestehen.*

*Diese Analyse befasst sich mit den Chancen und Risiken eines gemeinsamen Europäischen Nachrichtendienstes sowie der Zusammenarbeit der Nachrichtendienste der EU -Staaten insbesondere im Hinblick auf reelle Möglichkeiten des umfassenden Austauschs (Teilhabe) an nationalen nachrichtendienstlichen Informationen innerhalb der EU und deren Mitgliedsnationen.*

## Die nationale Nachrichtengewinnung und Aufklärung als Aufgabe eines Staatswesens

Die Beschaffung von Informationen mit Hilfe nachrichtendienstlicher Mittel und Methoden, die Gewinnung von Informationen aus offenen Quellen und durch die Erfassung von elektromagnetischen Ausstrahlungen aller Art gehören zu den originären Aufgaben eines Staates. Daneben hat der Staat die Verpflichtung, eigene, schutzwürdige Belange gegen Aufklärung und Nachrichtengewinnung durch fremde Mächte zu schützen. Er erfüllt damit eine wichtige Abwehr- und Schutzfunktion. Die unaufhaltsame Entwicklung der Informationstechnik und deren Vernetzung, sowohl im staatlichen Bereich als auch in der Wirtschaft, erfordern ebenfalls umfangreiche Schutzmaßnahmen auf organisatorischem als auch auf technischem Gebiet um die Kritischen Informationsinfrastrukturen vor Ausspähung und Manipulationen aller Art zu schützen, da ein partieller oder vollständiger Ausfall der Kritischen Informationsinfrastrukturen für das gesamte Gemeinwesen absolut existenzbedrohend sein kann.

Die Aufgaben der Nachrichten- und Sicherheitsdienste werden zumeist im Rahmen nationaler Strukturen und Verfahren wahrgenommen. Aus Gründen der Opportunität pflegen nationale Dienste die Zusammenarbeit mit befreundeten Nachrichtendiensten und Partnern, meist auf bilateraler Basis. Auch hier gelten bei der Weitergabe von Informationen meist Grundsätze der Ausgewogenheit im gegenseitigen Informationsaustausch. Eine Sonderstellung hierbei nimmt der Austausch von Informationen ein, die mit technischen Mitteln (Fernmelde- und Elektronische Aufklärung, Signals Intelligence SIGINT) im nationalen Rahmen gewonnen werden. Hier gilt vor allem der Quellenschutz, um die eigenen Fähigkeiten, Mittel und Methoden auch gegenüber Partnern nicht gänzlich offen zu legen. Ähnliche Prinzipien können auch für Erkenntnisse gelten, die mit Hilfe eigener, hochwertiger menschlicher Quellen (Human Intelligence, HUMINT) gewonnen werden,. Diese Erkenntnisse werden aus Gründen des nationalen Quellenschutzes meist „quellenbereinigt" nur an besonders ausgewählte Partner weitergegeben. Auch Erkenntnisse aus der raumgestützten abbildenden Aufklärung werden häufig nur ausgewählten Partnern zur Verfügung gestellt.

Die gewachsene asymmetrische Bedrohung der gesamten Informations- und Kommunikations-Struktur eines Staates durch Terroristen, die transnationale organisierte Kriminalität, andere Staaten und regierungsnahe fremde Gruppierungen erfordern die systematische Entwicklung von entsprechenden Abwehrmechanismen im Cyber-Raum und Instrumenten zur Führung von vernetzten Operationen gegen mögliche Angreifer-Systeme. Gegenwärtig verfügen etwa 150 Staaten weltweit über Fähigkeiten zur Führung von Informationsoperationen im Sinne der US DOD JP 3-13 Informations Operations. Damit gewinnt die Aufklärungs- und Abwehrfähigkeiten eines Staates im Cyber-Raum kardinale Bedeutung. Nicht zuletzt die Fähigkeiten eines Nachrichten- und Sicherheitsdienstes zur zeitgerechten Analyse und Auswertung der eingehenden Informationen sind hier von besonderem Gewicht. Auch die Rezeption derartiger Erkenntnisse innerhalb der politischen und militärischen Führung eines Staates ist dabei von ausschlaggebender Bedeutung, wie historische Beispiele eindrücklich zeigen.[i]

## Die Fähigkeiten der Europäischen Union zur Nachrichtengewinnung und Aufklärung[ii]

Gegenwärtig verfügt die Europäische Union noch nicht über einen eigenen, originären Nachrichtendienst. Die EU verfügt zwar aktuell auf die Fähigkeiten zur Auswertung der

abbildenden Aufklärung aus dem Weltraum (Satellite –Centre ), aber zum heutigen Zeitpunkt noch nicht über eigenständige Fähigkeiten zur Nachrichtengewinnung und Aufklärung (NG&A). Im nachrichtendienstlichen Sinne handelt es sich bei den durch FRONTEX oder andere Organisationen der EU gewonnene Informationen nicht um "Intelligence"im traditionellen Begriff. Hierbei handelt es sich vielmehr um Informationen aus dem Bereich der Strafverfolgung, die im Rahmen bestehender Vereinbarungen durch die EU-Staaten bereitgestellt werden oder durch "Lawful Interception" von Fernmeldeverkehren aller Art gewonnen werden. EUROPOL kann in diesem Zusammenhang nicht als "nachrichtengewinnende" Institution verstanden werden. Gegenwärtig verfügt die EU weiterhin nicht über eigenständige HUMINT- Fähigkeiten. Die EU verfügt gegenwärtig auch nicht über eigenständige Fähigkeiten in der "Technischen Aufklärung –SIGINT". Ob hier künftig die ENISA eine Rolle wird spielen können, bleibt zweifelhaft. Die Gewinnung von Informationen über Strahlungsquellen aller Art (Emitter-Data-Base) ist ein kosten – und personalintensiver Prozess, der auch beträchtlichen technischen Aufwand bei der Erfassung und Auswertung erfordert. Zudem würde eine Weitergabe der gewonnenen Erkenntnisse an "Third Parties" die Fähigkeiten eines Staates auf diesem Gebiet offen legen. Dies kann ebenfalls für die Fähigkeiten eines Staates zur Durchführung von Informationsoperationen gelten. Auch die Weitergabe selbst "quellenbereinigter" HUMINT -Erkenntnisse würden einer "Third Party" Rückschlüsse auf die HUMIT- Fähigkeiten eines nationalen Nachrichten- und/oder Sicherheits-dienstes erlauben. Ob der in Aufstellung begriffene Europäische Auswärtige Dienst (EAD) später eine derartige Funktion neben seiner eigentlichen Aufgabe, der diplomatischen Vertretung der EU in den Gastländern übernehmen kann, steht dahin.[iii]

Ob das EU-SITCEN in Brüssel, das derzeit den Nukleus einer nachrichtendienstlichen Auswerteorganisation darstellt, später einmal die Führung eines noch zu gründenden „Europäischen Nachrichtendienstes" übernehmen könnte, muss allerdings bezweifelt werden. Gegenwärtig stellen die Dienste der EU-Mitgliedstaaten dem EU-SITCEN und der Intelligence Division des Europäischen Militärstabes (EUMS)[iv] in der Regel nur quellenbereinigte nachrichtendienstliche Informationen zur Verfügung. Dem SITCEN und dem EUMS können diese Informationen lediglich evaluieren und in das Lagebild der EU einfügen. Wenngleich die EU-Mitgliedstaaten auf dem Gebiet der Terrorabwehr bereits einen sehr hohen Vernetzungsgrad beim Austausch von relevanten Informationen erreicht haben, bleiben auch hier nationale Vorbehalte bei der Weitergabe von Informationen[v] bestehen.

Wenn die EU dereinst ihr geplantes, umfassendes Datenbanksystem, in dem alle bereits vorhandenen Datensammlungen der EU (SIS, EURODAC, FRONTEX, VISA, SWIFT, TISPAN, nationale Melderegister, VIS, EUROSUR u.ä.) zusammengefasst werden, implementiert haben wird, könnte ein umfassendes und unkontrolliertes Zugriffsrecht der beteiligten Nationen zu Irritationen führen, da die im System enthaltenen sensitiven personenbezogenen Daten durch die Behörden der Teilnehmerstaaten nach eigenem Gutdünken verwendet werden. Auch hier kann nicht ausgeschlossen werden, dass Staaten die ihnen zugänglich gemachten Daten für andere, als für den vorgesehenen Zweck nutzen werden.

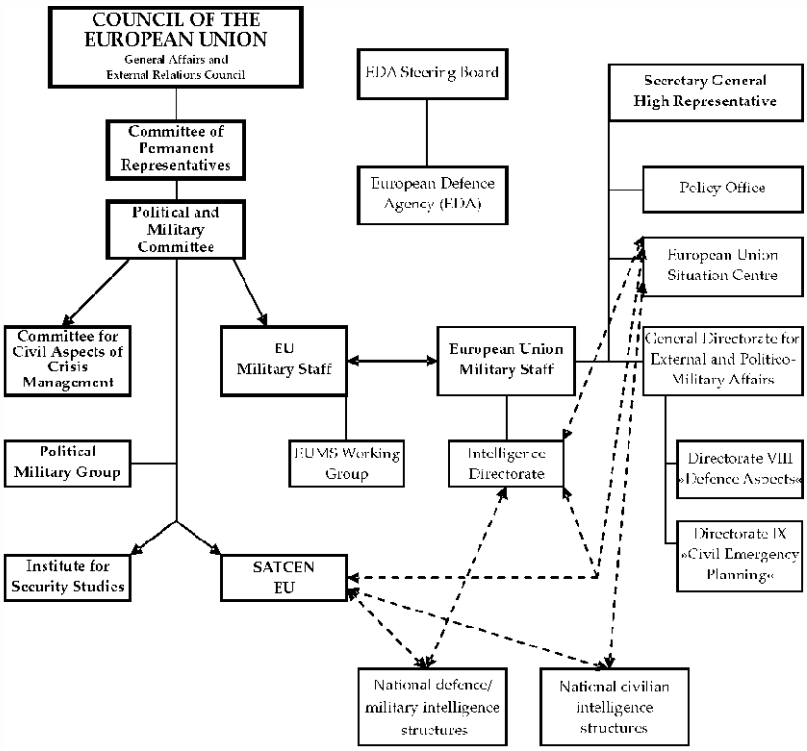


Abbildung 1: Nachrichtendienste in zivilen und militärischen Strukturen in der Europäischen Union[vi]

Für den Bereich der Telekommunikationsüberwachung (Lawful Interception) wurden in der EU bereits entsprechende Instrumente und Standards eingeführt, die sich offenbar bewährt haben[vii]. Auch hier findet eine evolutionäre Entwicklung, im Sinne einer fortschreitenden Entwicklung von Kontroll- und Überwachungsmechanismen innerhalb der EU und deren Einführung ohne nennenswerte parlamentarische Kontrolle durch Gremien der EU statt, deren letzte Konsequenzen noch nicht abzusehen sind. Dies kann jedoch nicht für den Bereich der, mit Hilfe von SIGINTdurch die Nationen gewonnenen Informationen gelten, die gegenwärtig nur im Rahmen von bilateralen Vereinbarungen eingeschränkt zwischen beteiligten Partner ausgetauscht werden. Gleiches kann für den Austausch von Informationen aus der raumgestützten, abbildenden Aufklärung gelten. Dies gilt umso mehr für den Bereich der Abwehr von „digitalen Angriffen" aus dem Cyber- Raum, wenn auch die NATO nun eine eigene Strategie und ein entsprechendes Instrumentarium implementiert hat.

Auch die Europäische Union verstärkt ihre Bemühungen, eine eigenständige Strategie zur Abwehr von Angriffen aller Art aus dem "Digitalen Raum" zu schaffen zum Schutz der Informations- und Kommunikationssysteme. Die ungestörte Funktion "KritischeR Infrastrukturen" aller Art ist für einen Staat/eine Staatengruppe von existenzieller Bedeutung. Daher sollte hier nicht ausschließlich auf die Funktion der Informations-gesellschaft Bezug genommen werden.Insbesondere bei asymetrischen Angriffen gegen einen Staat/eine Staatengruppe ist die Zielsetzung des Angreifers von besonderer Bedeutung.

Ob künftig jedoch eine umfassende Zusammenarbeit innerhalb der EU auf diesem Gebiet zu Stande kommen wird, muss wegen möglicher nationaler Vorbehalte hinsichtlich der Offenlegung eigener Fähigkeiten in Computer Network Operations bezweifelt werden. Auch im Bereich der Nachrichtengewinnung zur „Inneren Sicherheit Europas" sind die

Bemühungen der EU bereits sehr weit fortgeschritten. Die später zu erwartende Implementierung des „INDECT- Programms“ *(Intelligent Information System Supporting Observation,Searching and Detection for Citizens in Urban Areas*), ein im Rahmen des Stockholm-Beschlusses durch die EU angestossenes Projekt zur Ausweitung der Kontrolle von Informationsbeziehungen aller Art um Anzeichen für “unsoziales Verhalten” ode “Aufruhr” zu erkennen sowie anderer Vorhaben innerhalb der EU werden die Überwachungsmöglichkeiten der nationalen Sicherheits- und Strafverfolgungsbehörden erheblich ausweiten. Die mit Hilfe ausgeklügelter Überwachungs- und Kontrollsysteme gewonnenen Informationen werden, so die Planungen, in einem zentralen Datensystem der EU erfasst und stehen damit allen EU-Mitgliedsstaaten zur Verfügung. Auch hier sind erhebliche Vorbehalte angebracht, da die an diesem Programm beteiligten Nationen Souveränitätsrechte an ein nicht kontrollierbares supranationales Gremium abgeben. *Soweit den Autoren heute bekannt,liegen noch keine konkreten Rahmenbedingungen für das geplante zentrale Datensystem der EU vor. Daher ist davon auszugehen, dass die Bedingungen zu denen das System betrieben werden soll , ohne Mitwirkung des EU-Parlaments festgelegt und durch die Kommission oder eine nachgeschaltete Behörde der EU verwaltet wird.*

## Die strategischen Ziele der Neuordnung des NATO-Nachrichtenwesens

Ein verändertes sicherheitspolitisches Umfeld, die Erweiterung der NATO und der Europäischen Union, die Bedrohung der Staaten durch internationalen Terrorismus und die mögliche Verfügbarkeit von Massenvernichtungswaffen bei Schwellenländern und sonstigen Gruppierungen erfordern innerhalb des Bündnisses eine verstärkte internationale Zusammenarbeit auf nachrichtendienstlichem Gebiet und damit auch eine Neuorientierung der Nachrichtengewinnung, der Weitergabe der Informationen innerhalb dieser Organisationen[viii] und deren Verwendung, sowohl im multinationalen als auch im nationalen Rahmen. Die Transformation und die künftigen zu erwartenden Aufgaben der NATO erfordern eine völlige Neuorientierung des Nachrichtenwesens. Nach den Beschlüssen des NATO-Gipfels 1999 in Washington und der NATO-Gipfelgespräche im November 2002 in Prag veränderten sich die Ziele des NATO-Nachrichtenwesen vom reinen Verteidigungsbündnis hin zu einer umfassenderen, neuartige Bedrohungen und globale Risiken berücksichtigender Organisation, die fähig sein muss, in einem geografisch weitgespannten Umfeld zu agieren. Die Bewertung der nachrichtendienstlichen Fähigkeiten der NATO durch deren Verteidigungsminister und Chefs der Stäbe 2003 in Colorado Springs und die Ergebnisse der Übung ALLIED REACH 04 machten allen Beteiligten deutlich, das entsprechende korrektive Maßnahmen auf politischer und militärischer Ebene erforderlich sein werden, damit die Neuordnung des Nachrichtenwesens der NATO als „ Treibende Kraft“ für den Transformationsprozess der gesamten Organisation wirksam werden kann. Dies wird auch in der neuen NATO-Strategie vom Herbst 2010 deutlich:

- Eines der Ziele ist die umfassende Berücksichtigung der Informationserfordernisse auf der Ebene der NATO-Befehlshaber und Kommandobehörden aller Ebenen unter Beachtung politischer und strategischer Planungserfordernisse. Die Nationen einschließlich möglicher Koalitionspartner werden verpflichtet, nachrichtendienstliche Erkenntnisse (Daten, Bewertungen unter Einschluss möglicher Ziele), entsprechend ausgebildetes Personal und die erforderliche Hilfsmittel uneingeschränkt an jedem erforderlichen Ort bereitzustellen.

- Die NATO-Führungsorganisation ist verantwortlich für die Bereitstellung entsprechender Führungsmechanismen (Doktrin, organisatorischer Rahmen, Ausbildung, Führungspersonal Einrichtungen und standardisierter Verfahren), die eine Integration und Präsentation der nachrichtendienstlichen Erkenntnisse unter Beachtung der Prinzipien des Schutzes sensitiver Informationen auf allen politischen und militärischen Führungsebenen der NATO und ihrer Koalitionspartner erlauben.

- Die beteiligten Nationen werden die Hauptlast der Nachrichtengewinnung innerhalb der NATO zu tragen haben. Nur in außergewöhnlichen Fällen werden Nationen berechtigt sein, wichtige nachrichtendienstliche Informationen nicht an die NATO weiter zu geben. Bei der Übermittlung von Informationen durch die Nationen an die NATO.

- Militärische nachrichtendienstliche Informationen müssen mit anderen verfügbaren Informationen aus dem militärischen und zivilen Bereich verglichen werden um als Teil des gemeinsamen Lagebildes den NATO-Befehlshabern, strategischen Planern und politischen Entscheidungsträgern präsentiert zu werden. Hierzu werden die Nationen aufgefordert, entsprechend ausgebildetes Personal im erforderlichen Umfang bereitzustellen und die NATO-Führung durch Vorlage zeitrelevanter Informationen und Bewertungen, der Mitarbeit im nachrichtendienstlichen Bewertungsprozess, Beistellung entsprechender Auswertehilfsmittel (Programme u.ä.) sowie Nachrichtengewinnungsplattformen aller Art und dazugehöriges Personal zu unterstützen, um laufende Operationen lagegerecht führen zu können. Dazu zählt auch die gegenseitige Unterstützung durch bi- und multilaterale Kooperationsvereinbarungen bei der Entwicklung von Fähigkeiten zur Nachrichtengewinnung und der Ausbildung.

- Wichtig ist auch die Verpflichtung der Nationen, entsprechende Instrumente für den Quellenschutz bei sensitiven Informationen zu entwickeln und deren verzugslose Übermittlung an die entsprechenden NATO-Stellen zu gewährleisten. Die NATO-Organisation ist durch die beteiligten Nationen bei der Entwicklung von Verfahren zur raschen Weitergabe von Informationen an Nicht-NATO-Staaten und ziviler Stellen in einem Koalitionsumfeld zu unterstützten.

- Die NATO-Organisation wird ihrerseits den erforderlichen Umfang der Nachrichtengewinnung festlegen und auftretende Probleme auf allen Ebenen lösen, eine NATO-weite interoperable nachrichtendienstliche Architektur entwickeln und eine vernetzte Verteilungsorganisation für Gewinnung, Vergleich und Verteilung nachrichtendienstlicher Informationen schaffen. Dabei werden auch planerische Aspekte hinsichtlich des erforderlichen Personalumfangs in nachrichtendienstlichen Positionen der NATO berücksichtigt. Zu den Aufgaben der NATOOrganisation wird auch die Entwicklung von Richtlinien zur Erstellung gemeinsamer Datenbanken für die Unterstützung strategischer und operationeller Planungen als auch die kontinuierliche Anpassung aller Prozesse gehören, um die Interoperabilität auf dem Gebiet des Nachrichtenwesens sicherzustellen. Schließlich wird die NATO gemeinsame Standards und Mechanismen für die Gewinnung, Auswertung und Verteilung von geospatialen Informationen aufstellen, um auch auf diesem Gebiet die reibungslose Zusammenarbeit aller beteiligten Nationen sicherzustellen.

Die geschilderte strategische Zielsetzung der NATO wird damit auch unmittelbaren Einfluss auf die Gewinnung von Nachrichten im nationalen Rahmen haben, da die Nationen

verpflichtet werden, sich künftig umfassender an der Gewinnung von Nachrichten und deren Verteilung innerhalb der NATO zu beteiligen. Insbesondere im Hinblick auf mögliche Einsätze von EU–geführten multinationalen Truppenkontingenten, auch unter deutscher Beteiligung, gewinnt damit die neue NATO–Strategie an Bedeutung. Da die EU selbst nicht über nachrichtendienstliche Strukturen verfügt, wird sie sich bei von ihr geführten multilateralen, friedensstiftenden und friedenserhaltenden Missionen auf die nachrichtendienstlichen Erkenntnisse der NATO und anderer möglicher Partner abstützen müssen. Auch hier kann künftig nicht ausgeschlossen werden, das sensitive „nationale", unter Umständen auch personenbezogene Datenbestände in unkontrollierbarer Weise an multilaterale Organisationen gelangen.

Die Gewinnung von Nachrichten wird sich künftig nicht ausschließlich auf militärische Ziele und Bereiche von Bedeutung beschränken. Da zunehmend auch Informationen aus dem gesamten zivilen Umfeld an Bedeutung gewinnen, kann nicht ausgeschlossen werden, das Informationen aus bisher „national" verwalteten Datenbeständen der deutschen Sicherheitsbehörden (BKA, LKA und sonstiger Behörden) mit in derartige Sammlungen einfließen werden, die damit weiterer nationaler Kontrolle hinsichtlich Nutzung, Verknüpfung mit anderen „nationalen" Dateien von NATO-, EU – oder –anderen internationalen Koalitionspartnern entzogen und möglicherweise damit dann in andere internationale und nationale Datenbestände integriert werden könnten.

Da künftig die Gewinnung von Informationen mit technischen Mitteln (Fernmelde – und elektronische Aufklärung, Überwachung von Fernmeldebeziehungen (Art 10 GG[ix]) sowohl bei Telefon, Mobiltelefon, Fax und sonstigen Internet- Anwendungen vermehrt an Bedeutung gewinnen wird, können hier Konflikte bei der Weitergabe von Erkenntnissen nationaler Stellen im Rahmen von NATO- und EU-Übereinkünften auftreten, deren teilweise drastische Konsequenzen bereits jetzt im Zusammenhang mit den Aktivitäten in der Informationsgewinnung[x] der Vereinigten Staaten für Bürger der Europäischen Union erkennbar werden.

## Reorganisation der US-Nachrichten- und Sicherheitsdiensten und mögliche Konsequenzen für NATO und EU

Ziele der, auf den Zeitraum bis 2015 angelegten grundlegenden Reformen in den US-Nachrichten – und Sicherheitsdienste sind: [xi]

- Entwicklung integraler Fähigkeiten zur Erkennung und Bewertung plötzlich erkennbar werdender Herausforderungen im Cyber-Raum und im Weltall,
- Erhaltung der Sicherheit der Energieversorgung,
- Fortentwicklung der Fähigkeiten zur Früherkennung von strategischen Risiken und der Bereitschaft zur globalen Risikoüberwachung,
- Ressortübergreifende Bündelung aller nachrichtendienstlichen Fähigkeiten um in Echtzeit weltweit auf kritische Entwicklungen aller Art reagieren zu können,
- Entwicklung einer vernetzten Fähigkeit zur Feststellung von Risiken, der Verarbeitung der erhaltenen Informationen in einem bedrohungsgerechten und bedarfsangepassten System,
- Abbau der ressortbezogenen Beschränkungen hinsichtlich des Zugriffs auf Informationen und Ressourcen mit dem Ziel, die auf strategischer Ebene handelnden Verantwortlichen zu unterstützen.

- Intensivierung der Personalgewinnung, Aus – und Weiterbildung, Fortentwicklung und Anwendung von in der Wirtschaft bereits bewährten Führungsmodellen für Zwecke des Nachrichtendienstes sowie Beschaffung geeigneter Systeme,
- Intensivierung der Forschung im Bereich der Grundlagen und fachbezogener Technologien als auch der Beschaffung geeigneter Systeme in der Zukunft.

Die erkennbar werdende Verwischung der Grenzen zwischen der Auslandsaufklärung und der internen Gefahrenabwehr bedingt eine steigende Bedeutung des Heimatschutzes besonders im Hinblick auf das von den Vereinigten Staaten propagierte "Information Sharing". Sowohl innerhalb der US-Intelligence Community als auch mit Partnern und "bevorrechtigten Third Parties" wird durch eine solche Vorgehensweise die Trennungslinie zwischen Nachrichten-gewinnung/Beschaffung durch die Nachrichtendienste und durch Strafverfoldungs-behörden, sowohl in den USA als auch in der Zusammenarbeit mit Partnern, aufgehoben. Dies wird besonders durch die Rolle der über 72 Intelligence/Information Fusuion Centers in den USA deutlich.Dort sollen künftig Informationen aller Art, insbesondere zu kriminellen und terroristischen Bedrohunge gesammelt, ausgewertet und verfügbar gehalten werden. Dabei soll nach dem Willen der Planer der „Vision 2015" die bürgerlichen Freiheiten in den USA den Schutz behalten, der ihnen nach der Verfassung garantiert ist. Nachrichtendienstliche Erkenntnisse aus dem In- und Ausland sowie Informationen der Sicherheitsbehörden aus der Zusammenarbeit mit in- und ausländischen Partnern[xii] werden in die politische Lagebewertung und Entschlussfassung der US-Administration verstärkt einfließen. Besondere Bedeutung erlangt künftig der Schutz Kritischer Infrastrukturen, besonders im Bereich der Versorgung und der Kommunikations- und Informationssysteme. Nachrichtendienstliche Operationen im In- und Ausland werden künftig durch ein „integriertes Mission Management „ geführt, das „auftragsfokussiert" Unterstützungs-aufgaben im In- und Ausland durchführen wird. Dies bedingt auch die Einführung von multiplen, integrierten Sensorsystemen zur Gewinnung von Informationen. Diese Informationen werden in einer voll integrierten bearbeitungs- und nachrichten-gewinnungsorientierten Systemarchitektur verarbeitet und ohne Zeitverzug ressortübergreifend an die Bedarfsträger verteilt.

Für spezifische nachrichtendienstliche Missionen werden dezidierte Netzwerke eingerichtet, um das Risiko der Informationsüberflutung zu minimieren. Die Nachrichtendienst der USA werden zur Erreichung ihrer Ziele strategische Partnerschaften eingehen. Diese dienen dazu, die weltweite Abdeckung der Informationsgewinnung auszubauen sowie örtliche verfügbare nachrichtendienstliche Expertise umfassender und gezielter in die eigenen Auswertungen einfließen zu lassen. Besonderes Augenmerk wird künftig auf die eigenen nachrichtendienstlichen Fähigkeiten im Bereich der Bewertung kultureller und ethnischer Rahmenbedingungen einschließlich der Kenntnis von Fremdsprachen gelegt werden. Der Schwerpunkt künftiger Aktivitäten der US-Nachrichtendienste wird sich von der ressortabgrenzenden Informationsteilhabe zur umfassenden Wissens-Teilhabe wandeln. Damit einhergehend sollen langfristige Planungen, die die bisherigen, unter Zeitdruck gefassten Entscheidungen ablösen.

Von besonderer Bedeutung ist in diesem Zusammenhang die Neubewertung der Rolle menschlicher Quellen bei der Informationsgewinnung. Mit einer Entscheidung vom 22. Juli 2008 wurden die Fähigkeiten des US-Verteidigungsministeriums auf dem Gebiet der Spionageabwehr (Counterintelligence Field Activity, CIFA) auf den Director of Intelligence der Defense Intelligence Agency (DIA) übertragen. Hierzu wird künftig das Defense

Counterintelligence and Human Intelligence Center (DCHC) unter Führung des DIA-Direktors verantwortlich sein.

Der Auftrag des DCHC umfasst die Durchführung von Aktivitäten auf dem Gebiet der Spionageabwehr, Gegenspionage und des Einsatzes menschlicher Quellen durch das DCHC weltweit. Das DCHC wird auch weltweit einsetzbare Systeme für die Gegenspionage und zur Gewinnung von HUMINT entwickeln. Es ist zudem verantwortlich für die Sicherheits-überprüfungen des Personals im nationalen Rahmen und wird aktive Gegenspionage-operationen im In- und Ausland führen. Allerdings erhält das DCHC keine Exekutivbefugnisse innerhalb der Vereinigten Staaten. Ob und welche Befugnisse das DCHC außerhalb der Vereinigten Staaten erhalten wird, hängt nicht zuletzt von den bilateralen Abkommen der Vereinigten Staaten mit möglichen Gaststaaten ab, in denen Kräfte des DCHC bereits aktiv sind oder künftig noch werden. Hier können insbesondere die Status of Forces Agreements (SOFA), Letters of Agreement (LOA) oder ähnliche Rechtskonstrukte von Bedeutung sein. Ob das in Deutschland im Bezug auf die hier stationierten US-Truppen geltende Streitkräfteaufenthaltsgesetz diesbezügliche Regelungen enthält, ist noch zu untersuchen. In der Folge kann auch mit der Ausweitung weltweiter Operationen der US-Special Operations Forces[xiii] gerechnet werden.

Zusammenfassend ist davon auszugehen, dass die zu erwartenden Reorganisations-maßnahmen der US-Nachrichtendienste sowohl die künftige Politik der Vereinigten Staaten im Hinblick auf den Schutz der Heimat (Defense of the Homeland) als auch die Beziehungen zu befreundeten Staaten nachhaltig beeinflussen. Mit verstärkten Aktivitäten der US-Nachrichtendienste, insbesondere beim weltweiten Einsatz menschlicher Quellen zur Nachrichtenbeschaffung in allen Bereichen, die für die künftige Sicherheit der Vereinigten Staaten von Relevanz sind, kann daher gerechnet werden. Nicht zuletzt die Penetrierung der Führungsstrukturen terroristischer Organisationen in aller Welt durch eigene Quellen der US-Nachrichtendienste und deren Partner wird künftig noch an Bedeutung zunehmen.

## Ausblick

Eine Zusammenarbeit der Nachrichtendienste der EU-Staaten und der umfassende Austausch (Teilhabe) an nationalen nachrichtendienstlichen Informationen innerhalb der EU wird auch langfristig nur sehr schwer wegen sachlich begründeter nationaler Vorbehalte, insbesondere in den Diensten, zu realisieren sein. Dies gilt auch für nationale Erkenntnisse aus den Bereichen SIGINT und raumgestützte Aufklärung. Im Bereich der Strafverfolgung, insbesondere auch im Bereich der zulässigen Telekommunikationsüberwachung sind in der EU schon beachtliche Fortschritte erreicht worden, die gegenwärtig noch nationale Vorbehalte berücksichtigen. Berechtigte Zweifel sind angebracht, ob sich eine Zusammenarbeit auf dem Gebiet der Nachrichtendienste (Nachrichtenbeschaffung mit klandestinen Mitteln,der "Technischen Aufklärung" und im Bereich der "Geospatialen abbildenden Aufklärung" ) möglich sein wird.Auch bei der Planung und Durchführung von Informationsoperationen werden der Kooperation wie bereits vorher angeführt ,enge Grenzen gesetzt sein.

Ob diese auch künftig noch gelten können, bleibt abzuwarten. Im Bereich der Cyber-Abwehr können auch langfristig nur Fortschritte im Bereich der Abwehr erwartet werden, wenn sich die Nationen der EU und ihre Partner zu einem umfassenden Austausch von Informationen und der Vernetzung ihrer Fähigkeiten bereit erklären. Für den Bereich der offensiven Computer Network Operations[xiv] im Falle von Angriffen gegen nationale Systeme

muss nach wie vor mit der nationalen Zurückhaltung der Offenlegung eigener Fähigkeiten gerechnet werden, so das auf diesem Gebiet auch in nächster Zukunft kein Durchbruch erwartet werden kann. Dies kann auch für die HUMINT- Operationen der nationalen Nachrichten- und Sicherheitsdienste gelten. Daher sollte die EU auf die Bündelung der bereitgestellten Informationen zu europäischen Lagebildern fokussieren und gezielt durch Aspekte aus Politikfeldern vervollständigen, in denen sie Vorteile gegenüber der NATO aufweist (z.B. Financial Intelligence). Daneben sollten die entsprechenden EU-Organisationseinheiten die Zusammenarbeit mit den nachrichtendienstlichen Stellen der NATO intensivieren, da hier bereits erprobte Verfahren mit Erfolg angewandt werden.

Auch verfügt die NATO über ein umfassendes Informations- und Kommunikationssystem, auf das sich die EU bei Planung und Durchführung von Operationen, abstützen könnte. Das Aufrechterhalten nachrichtlicher Doppelstrukturen z.B. im Bereich der EU-Battlegroups ist in diesem Kontext kritisch zu betrachten. Symbolisch kann damit zwar eine gewisse Unabhängigkeit zum Ausdruck gebracht werden, doch in der Substanz ist der eigenständige Beitrag dieser Einheiten nach wie vor bescheiden. Es ist daher im Sinne der kürzlich neu entfachten Diskussion über die Möglichkeiten der Rollenspezialisierung und der Ressourcenzusammenlegung zu überlegen, ob und in welcher Form diese Überlegungen auch auf nachrichtendienstliche Fähigkeiten und die nachrichtendienstliche Zusammenarbeit zwischen EU und NATO angewendet werden könnten.

Für den Schutz Kritischer Infrastrukturen in der EU erscheint dagegen die Schaffung einer zentralen Stelle wünschenswert, da diese die Koordination aller Maßnahmen übernehmen könnte. Die bereits bestehende ENISA[xv] verfügt sicherlich über ausreichende fachliche Kompetenz auf diesem Gebiet. Problematisch erscheint allerdings der Schutz der Netze. die sich zum großen Teil im Besitz privatwirtschaftlicher Unternehmen befinden, auf staatliche Stellen nur in außergewöhnlichen Fällen Zugriff[xvi] auf diese haben. Hier scheint die Schaffung einer Richtlinie, ähnlich wie bei EPKI, zum Schutz kritischer Informations-infrastrukturen „ angebracht.

Die NATO hingegen wird sich auf den Schutz ihrer Netze gegen Angriffe aus dem Cyber-Raum konzentrieren, wie dies aus Veröffentlichungen des NATO-Centers of Excellence in Talinn ersichtlich wird. Diese Betrachtung gewinnt auch für die EU an Bedeutung. Angriffe aus dem Cyberraum gegen die unterschiedlichen sensitiven Datenbestände, die verschiedene EU-Einrichtungen in den Bereichen der inneren und äußeren Sicherheit. Sollten derartige Angriffe erfolgreich sein, können die Folgen nur sehr schwer abgeschätzt werden. Daher sollten sensitive, personenbezogene Daten ausschließlich in nationalen, besonders zu schützenden Datensammlungen verbleiben und nur im Rahmen eines kodifizierten Verfahrens anlassbezogen an Partner in der EU weitergegeben werden. Von besonderer Bedeutung hierbei ist auch die Möglichkeit für den Betroffenen, unrichtige Daten löschen oder berichtigen zu lassen.

Nach Auffassung maßgeblicher Stellen in den Vereinigten Staaten können Art und Umfang künftig zu erwartender Angriffe aus dem Cyberraum gegen die Kritischen Informationsinfrastruktur nur sehr schwer abgeschätzt werden, da eine Reihe von Staaten bereits über ernstzunehmende Fähigkeiten zur Kriegsführung im digitalen Raum verfügen. Daher gewinnt der künftige Schutz der Kritischen Infrastruktur in allen entwickelten Staaten einen hohen Stellenwert. Daher muss es das oberste Ziel der EU bei der zu erwartenden Entwicklung sein, ausreichend auf Angriffe aus dem Cyberraum und deren Abwehr vorbereitet zu sein. Gemeinsame Anstrengungen zur Verbesserung des Verständnisses der

Bedrohungen aus dem Cyberraum und der möglichen gemeinsamen Präventions-, Abwehr- und Gegenmaßnahmen sollten daher mit Nachdruck vorangebracht werden. Nachrichtendienstliche Fähigkeiten spielen dabei eine wichtige Rolle. Aus europäischer Sicht wäre es ratsam, die hierfür vorhandenen nationalen und europäischen Fähigkeiten in einer Gesamtschau zu erfassen, um dadurch mögliche Handlungsfelder für verstärkte gemeinsame Anstrengungen zu identifizieren.

[i] Der Angriff auf die Sowjetunion im Jahre 1941 wurde sowohl von Richard Sorge als auch anderen Quellen (Rote Kapelle) gemeldet, aber von J.W. Stalin wohl wegen möglicher Voreingenommenheit, nicht beachtet. Siehe hierzu: Gilles Perrault, Auf den Spuren der Roten Kapelle (Wien und München: Fischer Verlag, 1990). Gleiches gilt für die Mitteilung des Obersten Oster vom Amt Ausland-Abwehr des OKW an den

niederländischen Militärattaché Oberst Sas in Berlin über den Angriffstermin auf Belgien und die Niederlande. im Jahre 1940. Hierzu: Karl Bartz, Die Tragödie der Abwehr (Preußisch-Oldendorf: Pilgram, 1972), S. 63 f. Dies kann auch für die Angriffsindikationen auf die israelische Bar-Lev Linie am Ostufer des Suez-Kanals bei Beginn des Yom- Kippur- Krieges 1973 gelten. Mindestens 400 Informationen zur ägyptischen Operation „BADR" lagen dem israelischen Nachrichtenddienst vor. Diese wurden aber nicht beachtet, will man Follath glauben. Siehe Erich Follath, Das Auge Davids (Hamburg: Goldmann Wilhelm GmbH,1980), S. 207 f. Ein besonders signifikantes Beispiel für die Nichtbeachtung von Angriffsindikationen stellt der japanische Angriff auf Pearl Harbour im Dezember 1941 dar. Auch hier war die politische Seite offenbar gewarnt, hat aber möglicherweise aus politischen Gründen nicht auf die Warnungen des eigenen Dienstes reagiert. Siehe: James Bamford, NSA: Die Anatomie des mächtigsten Geheimdienstes der Welt (München: Goldmann, 2002), S. 33, 40, 82, 130, 319, 319, 375, 696, 738; James Bamford, Puzzle Palace, (Boston: xxx, 1982). Zur Rezeption nachrichtendienstlicher Erkenntnisse in der deutschen Politik, siehe Wolbert Smid, „Nachrichtendienst-Kultur in der Demokratie: Defizite, Fragen, Forderungen", in Melanie Morisse-Schildbach und Anke Peine (Hrsg.), Demokratische Außenpolitik und Geheimdienste (Berlin: LIT, 2008), S. 143-173. Ähnliches hat sich beim Beginn des ersten Golfkrieges 1991 zugetragen. Auch hier wurden die Indikationen, die auf einen irakischen Angriff auf Kuwait deuteten, von der politischen Führung in den USA nicht wahrgenommen oder bewusst missachtet. Siehe: Hopple, G. W. „Indications and Warning and Intelligence Lessons", in Bruce W. Watson, Bruce George, Peter Tsouras, B. L. Cyr, Military Lessons of the Gulf War (London: BCA, 1991), S. 146 f.

[ii] Siehe hierzu auch: Björn Müller-Wille: „For your eyes only? Shaping an intelligence community within the EU", Occasional Papers No 50 (Paris: EU Institute for Securit Studies, 2004). Die in dieser Publikation enthaltene Analyse hat auch bis heute nichts von ihrer Aktualität eingebüßt. Vergleiche auch Einzelbeiträge zu diesem Thema in: <www.sicherheitsmelder.de/>

[iii] Charles Baker, The search for a European intelligence policy (http://www.fas.org/irp/eprint/baker.html, 1999). Baker beschreibt die grundsätzlichen Probleme der Nachrichtenbearbeitung in einer Koalition. Daher sind seine Ausführungen auch heute noch von besonderer Bedeutung. Der Anhang seiner Ausarbeitung enthält eine Vielzahl von Quellen zu diesem speziellen Komplex bis zum Jahre 1999.

[iv] Maj. Gen. João Nuno Jorge Vaz Antunes, The European Union; Developing an Intelligence Capability (http://www.opensourcesinfo.org/journal/2006/8/11/the-european-union-developing-an-intelligence-capability.html, August, 2006). Der Autor beschreibt als kenntnisreicher "Insider" die Probleme der Nachrichtenbearbeitung innerhalb des European Union Military Staff – EUMS in Brüssel.

[v] „Forget Lisbon-EU Intelligence Plan is Really Dangerous", <http://www.wordpress.com>, 7. August 2008; Bruno Waterfield and Duncan Gardham, „New European spying proposals „threaten British security", The Telegraph, 8. August 2008.

[vi] A New Intelligence Paradigm and the European Union, Damir C□rnc□ec ( former director general of the Intelligence and Security Service of the MoD of Slovenia, University of Maribor, Faculty of Criminal Justice and Security, 2009)

[vii] Sowohl Russland als auch die VR China sind in den entsprechenden ETSI -Gremien vertreten und wenden soweit bekannt, bereits Standards der EU zur Telekommunikationsüberwachung an.

[viii] Die NATO hat bereits mit der Errichtung des Intelligence Fusion Centre im britischen Molesworth die Konsequenzen gezogen. Die Aufgabe des Fusion Centre besteht in der Bewertung verfügbarer nachrichtendienstlicher Informationen und deren Verteilung innerhalb der NATO.

[ix] (1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich. (2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, dass sie dem Betroffenen nicht mitgeteilt wird und dass an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.

[x] Zugriff auf Banktransferdaten im Rahmen des SWIFT- Abkommens und der Weitergabe von Passagierdaten im Rahmen des Passenger Name Record-Abkommens. Auch ist wohl langfristig der Zugriff der US-Behörden auf Gesundheitsdaten von EU-Bürgern im Rahmen eines Forschungsprogramms geplant.

[xi] Vision 2015 (Washington, D.C.: Director of National Intelligence, 2008); Pamela Hess, „DIA´s new mission adds to intel arsenal", The Associated Press, 5. August 2008; Deputy Secretary of Defense, „Subject: Directive Type Memorandum (DTM) 08-032, Establishment of the Defense Counerintelligence and Human Intelligence Center (DCHC)", Washington, D.C., 22. Juli 2008; Verfassungsschutzbericht 2007 (Stuttgart: Innenministerium Baden-Württemberg, 2008), Abschnitt G, S. 250; „CIA hatte Organisation der Sauerlandgruppe unterwandert", Tagesspiegel, 7. September 2008.

[xii] Im Rahmen der US Information Sharing Strategy sind auch vermehrte Forderungen der US-Seite auf „Teilhabe" an nachrichtendienstlichen Informationen der Partner der USA in Europa zu erwarten.

[xiii] Vergleiche hierzu auch: Counterinsurgency Operations, JP 3-24 (Washington, D.C.: Joint Chiefs of Staff, 2009); Multinational Operations, JP3-16 (Washington, D.C.: Joint Chiefs of Staff, 2007); Joint Special Operations

Task Force, JP 3-05.1 (Washington, D.C.: Joint Chiefs of Staff, 2007); Joint Forcible Entry Operations, JP3-18 (Washington, D.C.: Joint Chiefs of Staff, 2001); Joint Urban Operations, JP 3-06 (Washington, D.C.: Joint Chiefs of Staff, 2002).

[xiv] Auch sind die rechtlichen Rahmenbedingungen für aktive Computer Network Operations noch nicht, auch nicht ansatzweise, international kodifiziert. Gleichwohl haben die die Vereinigten Staaten erkennen lassen, das diese im Anlassfalle (Cyber-Angriff), sogenannte „preemtive strikes" gegen den Verursacher nicht ausschließen werden.

[xv] European Nertwork and Information Security Agency (http://www.enisa.europa.eu/about-enisa)

[xvi] Diese Befürchtung hegt auch der derzeitige Director of National Intelligence (DNI) und Kommandeur des US-Cyber Command, General Keith B. Alexander, in einem Interview. Siehe: Robert K. Ackermann, „Cyber Command Confronts Evolving Environment", AFCEA-Signal (February 2011), S. 18.