

### Die nachrichtendienstlichen Schnittstellen der EU-Sicherheitspolitik: Optionen für einen Ausbau des Informationsflusses und der fachlichen Aufsicht

Bossong, Raphael

Veröffentlichungsversion / Published Version

Stellungnahme / comment

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:

Stiftung Wissenschaft und Politik (SWP)

#### Empfohlene Zitierung / Suggested Citation:

Bossong, R. (2018). *Die nachrichtendienstlichen Schnittstellen der EU-Sicherheitspolitik: Optionen für einen Ausbau des Informationsflusses und der fachlichen Aufsicht*. (SWP-Aktuell, 66/2018). Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit. <https://nbn-resolving.org/urn:nbn:de:0168-ssoar-60959-3>

#### Nutzungsbedingungen:

Dieser Text wird unter einer Deposit-Lizenz (Keine Weiterverbreitung - keine Bearbeitung) zur Verfügung gestellt. Gewährt wird ein nicht exklusives, nicht übertragbares, persönliches und beschränktes Recht auf Nutzung dieses Dokuments. Dieses Dokument ist ausschließlich für den persönlichen, nicht-kommerziellen Gebrauch bestimmt. Auf sämtlichen Kopien dieses Dokuments müssen alle Urheberrechtshinweise und sonstigen Hinweise auf gesetzlichen Schutz beibehalten werden. Sie dürfen dieses Dokument nicht in irgendeiner Weise abändern, noch dürfen Sie dieses Dokument für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, aufführen, vertreiben oder anderweitig nutzen.

Mit der Verwendung dieses Dokuments erkennen Sie die Nutzungsbedingungen an.

#### Terms of use:

This document is made available under Deposit Licence (No Redistribution - no modifications). We grant a non-exclusive, non-transferable, individual and limited right to using this document. This document is solely intended for your personal, non-commercial use. All of the copies of this documents must retain all copyright information and other information regarding legal protection. You are not allowed to alter this document in any way, to copy it for public or commercial purposes, to exhibit the document in public, to perform, distribute or otherwise use the document in public.

By using this particular document, you accept the above-stated conditions of use.

# SWP-Aktuell

NR. 66 NOVEMBER 2018

## Die nachrichtendienstlichen Schnittstellen der EU-Sicherheitspolitik

Optionen für einen Ausbau des Informationsflusses und der fachlichen Aufsicht

*Raphael Bossong*

Seit 2015 schreitet die sicherheitspolitische Kooperation zwischen EU-Mitgliedstaaten mit erhöhter Geschwindigkeit voran. Für die Außen-, Sicherheits- und Verteidigungspolitik der Union besteht die Aussicht, dass mit verstärkter Zusammenarbeit und vertiefter Rüstungskoopeation mehr internationale Handlungsfähigkeit geschaffen wird. Was die innere Sicherheit betrifft, spornt die anhaltende Bedrohung durch Terrorismus die Ausgestaltung einer »Europäischen Sicherheitsunion« an, die auf intensivem Informationsaustausch der Sicherheitsbehörden gründet. Im Schatten dieser Entwicklungen steht die Frage im Raum, inwiefern auch die europäische nachrichtendienstliche Kooperation vorangetrieben werden sollte. Zwar sind in diesem besonders sensiblen Bereich keine öffentlichkeitswirksamen Integrationsschritte zu erwarten. Dennoch sollten bestehende Ansätze zur nachrichtendienstlichen Unterstützung der EU-Sicherheitspolitik gezielt vertieft und besser kontrolliert werden.

Gemäß dem Vertrag von Lissabon fällt die nationale Sicherheit in die alleinige Verantwortung der Mitgliedstaaten (Art. 4(2) EUV). Schon deshalb bleibt die Idee eines gemeinsamen europäischen Geheimdienstes abwegig, die seit Mitte der 2000er Jahre wiederholt lanciert wurde. Klar ist auch, dass die EU keine direkte Rolle in besonders sensiblen Teilbereichen der nachrichtendienstlichen Arbeit spielen kann, etwa der großflächigen technischen Fernaufklärung, der Führung menschlicher Quellen oder der Ausführung verdeckter Operationen. Allerdings verfügt die EU-Sicherheitspolitik über indirekte Zugänge zu nachrichtendienstlichen Erkenntnissen. Vor allem bei der

Terrorismusbekämpfung wachsen die Schnittmengen zwischen Europol- oder EU-Datensystemen und Informationen der Inlandsnachrichtendienste. Für ihr außenpolitisches Handeln kann die EU derweil auf strategische Risiko- und Lageanalysen zurückgreifen, die der Europäische Auswärtige Dienst (EAD) aus Berichten unterschiedlicher nationaler Dienste zusammenstellt. Diese Verfahren sollten transparenter gestaltet und öffentlich diskutiert werden, um einen in den kommenden Jahren schrittweise erfolgenden, verhältnismäßigen Ausbau nachrichtendienstlicher Kapazitäten für die innere wie äußere Sicherheit der EU zu ermöglichen.



## Vertrauliche Analysen für die Außen- und Sicherheitspolitik

Im Jahr 2002 begann der Austausch nationaler nachrichtendienstlicher Informationen im sogenannten gemeinsamen Situationszentrum (SITCEN) des EU-Ratssekretariats. Vorrangig sollte er dazu dienen, EU-Auslandsmissionen zu unterstützen sowie zu einer gemeinsamen Einschätzung terroristischer Gefahren beizutragen. Die damals informell etablierten Arbeitsweisen gelten bis heute fort: Freiwillig übermitteln Mitgliedstaaten abgeschlossene nachrichtendienstliche Berichte (finished intelligence) an die EU. Aus der Gesamtschau werden gemeinsame Einschätzungen und Handlungsoptionen abgeleitet. Offen zugängliche Informationen, Berichte aus europäischen Delegationen und Erkenntnisse des EU-Satellitenzentrums ergänzen diese Arbeit der Analysten, die von ihren Nachrichtendiensten an die EU abgeordnet wurden.

Zudem konnte der aus der Westeuropäischen Union hervorgegangene EU-Militärstab seinen Zugang zum militärischen Nachrichtenwesen bewahren. Eine entsprechende interne Abteilung des Militärstabs (Intelligence Directorate) erstellt vertrauliche militärische Lageanalysen. Notwendig sind diese vor allem, um EU-Missionen in Risikoländern wie beispielsweise der Demokratischen Republik Kongo oder Somalia zu planen und durchzuführen. Die sachlich gebotene Zusammenarbeit zwischen dem Intelligence Directorate mit dem zivilen Lagezentrum wurde ab 2007 formalisiert und wird seither als Single Intelligence Analysis Capacity (SIAC) der EU geführt. 2011 wurde das Lagezentrum SITCEN in EU Intelligence Centre (INTCEN) umbenannt und in den damals neu eingerichteten EAD eingegliedert. Das INTCEN umfasst mittlerweile rund 100 Mitarbeiter, davon um die 60 in der nachrichtendienstlichen Auswertung. Zusammen mit dem militärischen Intelligence Directorate verfügt die EU-SIAC über etwa 80 bis 90 nachrichtendienstliche Verbindungsoffiziere und Analysten.

Die Auswertungen der EU-SIAC werden sowohl EU-Gremien als auch Entscheidungs-

trägern in nationalen Hauptstädten zur Verfügung gestellt. Sie ermöglichen ein umfassenderes sicherheitspolitisches Lagebild, als es die meisten EU-Mitgliedstaaten für sich allein entwickeln könnten. Allerdings ist davon auszugehen, dass die Mitgliedstaaten operativ relevante oder besonders wertvolle nachrichtendienstliche Informationen häufig für sich behalten. Daher liegt der Wert der EU-SIAC vor allem in der strategischen und längerfristigen Analyse. Im günstigen Fall kann jedoch auch in akuten Krisen eine gemeinsame Bewertung erstellt werden. Beispiele dafür wären die Besetzung der Krim oder der Nervengasanschlag im britischen Salisbury. Eine derartige europäische nachrichtendienstliche Aufklärung kann sich direkt auf außen- und sicherheitspolitische Reaktionen auswirken.

## Freiwillige Vertiefung der nachrichtendienstlichen Zulieferung

Die für die nachrichtendienstliche Arbeit bisher maßgeblichen Normen stehen einer Vertiefung dieser freiwilligen Zusammenarbeit eher entgegen. Bereits auf nationalstaatlicher Ebene etwa werden Informationen nur weitergegeben, wenn dies unbedingt notwendig ist (need to know), nicht schon, wenn sie grundsätzlich verfügbar sind (need to share). Doch die strukturellen Veränderungen der sicherheitspolitischen Lage Europas haben zur Folge, dass die Notwendigkeit des vertraulichen Informationsaustauschs neu bewertet werden muss. Zusätzlicher Reformdruck entsteht durch den Brexit, weil die Sachkompetenz der britischen Mitarbeiter in der EU-SIAC verloren gehen wird.

Konkret könnten einige EU-Mitgliedstaaten den Weg einer verstärkten Kooperation nach Artikel 329 AEUV für den Bereich der GASP einschlagen. Da das EU-SIAC bereits als Bestandteil der GASP und des EAD gilt, müsste eine Vertiefung dieser Strukturen nicht mit dem nationalen Souveränitätsvorbehalt in Fragen der nationalen Sicherheit (Art. 4 (2) EUV) in Konflikt

geraten. Die teilnehmenden Mitgliedstaaten könnten sich verpflichten, gemeinsam vereinbarte thematische und regionale Schwerpunkte arbeitsteilig mit den Mitteln ihrer nationalen Nachrichtendienste zu bearbeiten und daraus gewonnene Erkenntnisse verlässlich bei EU-SIAC einzuspeisen. Dies könnte zu einem europäischen Zirkel der nachrichtendienstlichen Analyse führen: Die Planung und Priorisierung nachrichtendienstlicher Ressourcen (erste Phase) würde dementsprechend stärker europäisch koordiniert werden. Auf nationalstaatlicher Ebene hingegen verblieben die Sammlung von Informationen (zweite Phase) und deren erste Verarbeitung (dritte Phase). Die abschließenden sekundären Auswertungen im EU-SIAC und die Weitergabe an Entscheidungsträger (vierte Phase) würden hochwertigere Ergebnisse liefern, die anschließend erneut in die künftige Prioritätensetzung einfließen sollten.

Flankierend könnten politische Gremien ausgebaut werden, um die Nutzung nachrichtendienstlicher Erkenntnisse zu verbessern. Auf Arbeitsebene hieße dies, dass die Rolle des Politischen und Sicherheitspolitischen Komitees (PSK) erweitert würde. Im Gespräch ist auch die Idee eines hochrangigen Europäischen Sicherheitsrats, wie ihn Bundeskanzlerin Merkel wiederholt vorgeschlagen hat. Ein solcher Sicherheitsrat böte besondere Vorteile, wenn es um nachrichtendienstliche Themen geht. Die Dienste der Mitgliedstaaten, bisher unterschiedlichen Ministerien zugeordnet, könnten auf Ebene der Staats- und Regierungschefs zusammengeführt werden. Zugleich könnte ein hoher Grad der Vertraulichkeit und Entscheidungsfähigkeit ermöglicht werden.

Allerdings gilt auf dieser Ebene wie in den meisten Fragen der GASP bisher das Prinzip der Einstimmigkeit, einschließlich der Autorisierung für eine vertiefte Zusammenarbeit. Als Alternative steht der Weg einer von der EU unabhängigen intergouvernementalen Kooperation offen. Das entspräche auch den Bestimmungen von Artikel 73 AEUV für die Kooperation im Bereich der nationalen Sicherheit. Hierbei

droht jedoch eine weitere Zersplitterung der europäischen Sicherheitsarchitektur. Ein Spannungsverhältnis zeigt sich bereits zwischen der Ständigen Strukturierten Zusammenarbeit (PESCO), an der sich 25 Mitgliedstaaten beteiligen wollen, und der neueren französischen Europäischen Interventionsinitiative (EI2), die zurzeit zehn europäische Staaten inklusive Großbritanniens umfassen soll. Mit Hilfe der EI2 soll die Einsatzfähigkeit europäischer militärischer Kräfte in der Nachbarschaft erhöht werden. Daraus leitet sich ein gemeinsames Interesse der EI2-Staaten an hochwertigen nachrichtendienstlichen Informationen aus Einsatzgebieten ab. Die exklusivere EI2 unterstützt dabei die notwendige Vertraulichkeit, während Großbritannien seine führenden Kapazitäten zur technischen Aufklärung und Anbindung an die USA zusätzlich in die Waagschale werfen kann. Um zu verhindern, dass die EI2 die PESCO spaltet, und um die Bedeutung der zivilen GASP nicht aus dem Blick zu verlieren, sollte die EU-SIAC deshalb durch eine möglichst breite Koalition von Mitgliedstaaten im Rahmen des EU-rechtlich vorgesehenen Verfahrens gestützt werden. Aus Perspektive der PESCO könnten mittelfristig zudem gemeinsame Projekte zur technischen Aufklärung und nachrichtendienstlichen Auswertung ins Auge gefasst werden.

## **Personenbezogene Daten für Terrorismusbekämpfung und innere Sicherheit**

Was den Bereich der inneren Sicherheit angeht, gaben die Terroranschläge vom 13. November 2015 in Paris den Anstoß für einen deutlich intensivierten Austausch nachrichtendienstlicher Informationen. Frankreich übermittelte sensible Fahndungshinweise an das Europäische Polizeiamt (Europol). Diese Daten sollten vor allem mit jenen des amerikanischen Programms zum Aufspüren der Finanzierung des Terrorismus (Terrorist Finance Tracking Program, TFTP) abgeglichen werden, für das Europol schon seit 2010 eine zentrale Scharnier-

funktion wahrnimmt. Weitere EU-Mitgliedstaaten, die zuvor nur zögerlich mit Europol zusammenarbeiteten, teilten daraufhin ihre Erkenntnisse zu sogenannten ausländischen Kämpfern. Im Zuge dieser Dynamik wurde Anfang 2016 das bei Europol angesiedelte Europäische Zentrum für Terrorismusbekämpfung (European Counter Terrorism Centre, ECTC) geschaffen, das zusammen mit einer Neufassung des rechtlichen Mandats von Europol neue Kooperationsmöglichkeiten eröffnete. Artikel 2 dieser reformierten Verordnung hält offen, welche für Bekämpfung und Verhütung schwerer Verbrechen national »zuständige Behörden« an Europol-Arbeitsprozessen beteiligt werden können. Zumindest einige Mitgliedstaaten beschränken den Weg einer weitergehenden Einbindung von Sicherheitsbehörden mit sowohl polizeilichen als auch nachrichtendienstlichen Aufgaben.

Richtet man den Blick auf die operative Dimension, so zeigt sich, dass im Informationssystem von Europol (EIS) die Zahl der Einträge zum islamistischen Terrorismus und zu ausländischen Kämpfern deutlich gewachsen ist. Zudem wurde im horizontalen Datennetzwerk SIENA (Secure Information Exchange Network Application) zwischen den Europol-Mitgliedstaaten eine geschlossene Benutzergruppe für nationale Antiterrorismusbehörden geschaffen, in der vertraulicher kommuniziert werden kann. Aufgrund der national unterschiedlich ausgeprägten Befugnisse der jeweiligen Antiterrorismusbehörden kann diese Gruppe auch zu einem verstärkten Austausch nachrichtendienstlicher Erkenntnisse beitragen. Auf deutsche Initiative wurde überdies eine Steuerungsgruppe nationaler Antiterrorismusbehörden im Rahmen des ECTC eingerichtet, welche die grenzüberschreitenden Ermittlungen und die Informationsverarbeitung verbessern soll.

Derweil bemüht sich Europol um Zugang zu besonders aussagekräftigen biometrischen Informationen, die amerikanische Dienste und Streitkräfte weltweit zu mutmaßlichen terroristischen Kämpfern sammeln. Solche Daten können vor allem bei Außengrenzkontrollen und in den so-

genannten EU-Hotspots für irreguläre Einwanderer abgeglichen werden. Im Sommer 2018 vereinbarte die EU zudem, dass Warnhinweise zu Terrorismusverdächtigen ins Schengener Informationssystem (SIS) eingestellt werden müssen. Das SIS dient bereits seit Mitte der 1990er als zentrales Informationsnetzwerk für Polizei- und Grenzschutzbehörden aller Schengen-Mitgliedstaaten und wurde schon früher informell mit nachrichtendienstlichen Informationen ergänzt. Künftig soll Europol bei der Auswertung von Fluggastdaten (Passenger Name Records) und einer gesamteuropäischen Warnliste mitwirken. Die Liste soll der Gefahrenabwehr dienen: Mit ihrer Hilfe soll verhindert werden, dass in die Schengenzone nicht visapflichtige Personen einreisen, die schwerer Verbrechen verdächtigt werden. Als Vorbild dafür dienen die Kontrollpraktiken der Vereinigten Staaten. Sie beruhen auf einer gemeinsamen Datenplattform zwischen polizeilichen und nachrichtendienstlichen Behörden. Derzeit wird mit den Maghreb-Staaten Ägypten, Tunesien, Algerien und Marokko sowie mit Jordanien und Israel über Europol-Abkommen zum Austausch personenbezogener Daten verhandelt. Es ist davon auszugehen, dass auch in diesen Staaten eine enge Verbindung zwischen nachrichtendienstlichen und polizeilichen Strukturen besteht.

Auf Seiten der europäischen Inlandsnachrichtendienste wurde 2016 eine Vertiefung der Counter Terrorism Group (CTG) vereinbart. Diese Gruppe umfasst alle EU-Mitgliedstaaten sowie Norwegen und die Schweiz. Sie war 2001 als Arbeitsgruppe des Berner Clubs entstanden, der seit den 1970er Jahren als informelle Plattform zur Bekämpfung des internationalen Terrorismus und zur Spionageabwehr dient. Trotz dieser langjährigen Beziehungen blieb es in der CTG zunächst bei einer einzelfallbasierten Zusammenarbeit sowie sporadischen Konsultationen mit der EU. Seit 2016 wurde für die CTG nun ein ständiges Hauptquartier in Den Haag entwickelt. Dort können Verbindungsbeamte der Dienste sowohl auf ihre jeweiligen nationalen Informationssysteme zugreifen als auch eine gemeinsa-

me Datenbank bearbeiten. Auf diese Weise soll ein umfassendes Bild terroristischer Netzwerke in Europa entstehen. Zusätzlich sollen die ständigen Verbindungsbeamten dabei helfen, grenzüberschreitende Ermittlungs- und Überwachungsmaßnahmen möglichst lückenlos durchzuführen.

## **Stärkung der Verbindung zwischen Polizeibehörden und Nachrichtendiensten**

Angesichts des parallelen Wachstums von Europol und CTG steht die Frage im Raum, ob über sporadische Kontakte hinaus eine gegenseitige Kooperation gestartet werden kann. Seit 2001 haben viele westliche Staaten Verfahren für einen Austausch zwischen Polizei und Nachrichtendiensten geschaffen. In Deutschland steht das Gemeinsame Terrorabwehrzentrum (GTAZ) exemplarisch für diese Entwicklung. Im Sommer 2018 schlug die CDU in einem Grundsatzpapier für die europäische Ebene eine mit dem GTAZ vergleichbare Datenplattform für die Bekämpfung des Terrorismus, des Organisierten Verbrechens und der illegalen Migration vor.

Abgesehen von der fehlenden EU-rechtlichen Kompetenz sprechen indes zahlreiche praktische Hindernisse gegen ein solches Konzept der europäischen Koordination. So kann Europol bisher keinen umfassenden Geheimschutz gewährleisten, ist aber seinerseits einem strengen Datenschutzregime unterworfen. Dies kollidiert mit der klassischen nachrichtendienstlichen Kooperation, bei der der übermittelnde Staat die Kontrolle über geteilte Informationen behält (Third Party Rule). In den Datenbanken von Europol könnten Daten zwar markiert werden, um ihre weitere Verwertung zu beschränken. Dieses technische System ersetzt jedoch nicht Vertraulichkeit und gegenseitige Abhängigkeiten in bilateralen nachrichtendienstlichen Beziehungen.

Zudem herrschen unter den dreißig Mitgliedstaaten der CTG unterschiedliche Vorstellungen über Rolle und Status der

CTG. Die deutsche Regierung zum Beispiel beantwortete parlamentarische Anfragen zu der Gruppe mit Verweis auf das Staatswohl zunächst nur äußerst zurückhaltend. Dagegen befassten sich die niederländischen Aufsichtsbehörden in öffentlich zugänglichen Berichten mit der Arbeitsweise der CTG. In anderen europäischen Staaten wird die internationale nachrichtendienstliche Zusammenarbeit vielfach ohne explizite rechtliche Grundlage betrieben. Aus operativer Sicht argumentieren zudem beteiligte Nachrichtendienste, dass das gegenseitige Vertrauen sich weiterhin im Aufbau befindet und der Grundsatz der Freiwilligkeit unbedingt gewahrt bleiben müsse. Insofern kann trotz wachsender Unterstützung für die CTG noch nicht von einer gefestigten Institution gesprochen werden.

Dennoch könnten die sporadisch vorhandenen Kontakte zur EU-Ebene vertieft werden, etwa indem Verbindungsbeamte der CTG im Zentrum für Terrorismusbekämpfung bei Europol platziert werden. Mitglieder nationaler Sicherheitsbehörden mit sowohl polizeilichen wie nachrichtendienstlichen Aufgaben, etwa aus Schweden oder Österreich, könnten hierbei eine Brückenfunktion erfüllen. Auf diese Weise könnten Informationen der CTG-Plattform regelmäßig in das Informationssystem von Europol (EIS) eingespeist werden und beispielsweise zur Sicherheitsüberprüfung irregulärer Einwanderer in EU-Hotspots beitragen. Dieselben Verbindungsbeamten könnten auf der anderen Seite sicherstellen, dass relevante Eintragungen aus EU-Datenbanken für die polizeiliche Zusammenarbeit oder Migrationskontrolle in die CTG zurückgespielt werden.

Bewährt sich ein solcher regelmäßiger Informationsaustausch durch vermehrte Treffermeldungen an EU-Außengrenzen oder in anderen Maßnahmen der Gefahrenabwehr, kann nach dem Vorbild des deutschen GTAZ eine weitergehende Kooperation erwogen werden. Diese würde direkte Fallbesprechungen zwischen Polizei und Nachrichtendiensten erlauben. Trotz einzelner Fehlschläge gelten derartige direkte Konsultationen als unverzichtbar für effek-

tive Terrorismusbekämpfung. Für die europäische Ebene hieße dies, dass Europol und CTG gemeinsame Diskussionen über einzelne Verdächtige führen und nationalen Sicherheitsbehörden konkrete Maßnahmen empfehlen. Wollen die Behörden den Empfehlungen nicht folgen, müssten sie dies begründen. Selbst ohne direkte Weisungsbefugnis der EU böte dieses Modell daher gute Chancen, dass die grenzüberschreitende Zusammenarbeit zunimmt.

Auch für andere Formen der schweren Kriminalität gibt es erste Beispiele für Datenplattformen. So betreibt Europol seit 2016 das Europäische Zentrum zur Bekämpfung des Migrantenschmuggels (European Migrant Smuggling Centre, EMSC). In Grundzügen ist es dem deutschen Gemeinsamen Analyse- und Strategiezentrum Illegale Migration (GASIM) vergleichbar und trägt zur vertraulichen Risikobewertung sowie zu Strafverfolgungsmaßnahmen bei. Das European Cybercrime Centre (EC3) bei Europol wiederum arbeitet in gemeinsamen Ermittlungsgruppen (Joint Cybercrime Action Taskforce, J-CAT) sowohl mit einer polizeilichen als auch einer nachrichtendienstlich tätigen Behörde der Vereinigten Staaten zusammen, nämlich dem FBI und dem Secret Service.

## Rechtsstaatliche und demokratische Aufsicht

Die politische Aufarbeitung des NSA-Spionageskandals verdeutlichte, dass sich die internationalen Aktivitäten der Nachrichtendienste vielfach dem Zugriff der Aufsichtsbehörden entziehen. Kontroverse politische Debatten sowie das Handeln europäischer Gerichte führten seither zu ersten Reformen. In Deutschland zum Beispiel wurden die Rechtsgrundlagen und Kontrollgremien des Bundesnachrichtendienstes neu geordnet. Der Europäische Gerichtshof mahnte Schweden und Großbritannien, die sogenannte Vorratsdatenspeicherung für Zwecke der Gefahrenabwehr restriktiver zu handhaben. Im September 2018 forderte der Europäische

Gerichtshof für Menschenrechte, die Befugnisse britischer Nachrichtendienste zur Erhebung und Auswertung von Massendaten präziser zu fassen. Grundsätzlich stehen alle europäischen Staaten vor großen Herausforderungen, unter den Bedingungen des technischen Fortschritts und der Globalisierung eine funktionierende Kontrolle über ihre Nachrichtendienste zu gewährleisten. Die Auseinandersetzung über die Rechtsstaatlichkeit in einigen EU-Mitgliedstaaten unterstreicht, wie dringlich es ist, liberale Grundrechte in Kernbereichen nationaler Sicherheit zu bewahren.

Die EU spielt zwar in der Massenüberwachung keine direkte Rolle. Ebenso wenig werden zumindest im EU-SIAC personenbezogene Daten verarbeitet. Dennoch stellen sich kritische Fragen zur Aufsicht und demokratischen Legitimierung. Fehlentscheidungen, die auf der Grundlage nachrichtendienstlicher Informationen getroffen werden könnten, gefährden die Legitimität der europäischen Außen- und Sicherheitspolitik. Es muss möglich bleiben, die Verantwortung für solche Fehlleistungen politischen Akteuren zuzuordnen. Das bedeutet beispielsweise, dass auch Vertreter anderer demokratischer Institutionen, etwa Abgeordnete des Europäischen Parlaments, die Befugnis erhalten müssen, vertrauliche Unterlagen im Rat (oder einem künftigen Europäischen Sicherheitsrat) einzusehen.

Für den Bereich der inneren Sicherheit stellen sich weitergehende Fragen zur Rechtmäßigkeit nachrichtendienstlicher Zusammenarbeit. Bei den Antworten darauf sind die EU-Grundrechtecharta, das neuere europäische Datenschutzrecht oder nationale verfassungsrechtliche Besonderheiten wie das deutsche Gebot der Trennung zwischen Polizei und Nachrichtendiensten zu berücksichtigen. Die Debatte über solche Fragen wird sich auch durch flexible oder niederschwellige Formen der Zusammenarbeit mit Nachrichtendiensten nicht vermeiden lassen. Vielmehr ist gerade bei informellen Verfahren, etwa dem Einsatz von Verbindungsbeamten, größtmögliche Transparenz gefragt. Nur so lässt sich problematischen Entwicklungen frühzeitig begegnen, statt

sie wie im Fall der NSA-Enthüllungen nachträglich skandalisieren zu müssen.

Gemäß Artikel 43(4) der Europol-Verordnung hat der Europäische Datenschutzbeauftragte grundsätzlich Zugang zu allen personenbezogenen Daten, inklusive der eingestuften Informationen. Das ist ein Grundpfeiler der rechtsstaatlichen Aufsicht über Europol. Auch die Nachrichtendienste sollten diese externe Kontrolle akzeptieren. Außerdem sollte sie zu einer weniger restriktiven Auslegung der sogenannten Third Party Rule führen. Darüber hinaus wurde 2017 ein Gemeinsamer Parlamentarischer Kontrollausschuss zu Europol eingerichtet. Die praktischen Erfahrungen mit diesem neuen, halbjährlich tagenden Gremium aus nationalen und europäischen Parlamentariern sind noch zu begrenzt, um aussagekräftige Schlüsse ziehen zu können. Aufgrund der gemischten Natur des Kontrollgremiums böte sich allerdings als möglicher künftiger Arbeitsschwerpunkt an, die nachrichtendienstlichen Schnittstellen bei Europol zu beobachten. Zudem können nationale Abgeordnete im Bereich der nationalen Sicherheit Auskunftsrechte geltend machen, die europäischen Vertretern wegen der kompetenzrechtlichen Beschränkungen der EU nach Artikel 4(2) EUV nicht zustehen. Daher könnte der Gemeinsame Parlamentarische Kontrollausschuss zu Europol als Baustein für eine weitergehende Aufsicht über die indirekten nachrichtendienstlichen Schnittstellen der EU fungieren.

Die niederländische Aufsichtsbehörde veröffentlichte im Februar 2018 einen ersten Bericht zur reformierten CTG. Darin betonte sie die Notwendigkeit, die Verhältnismäßigkeit der Datenverarbeitung stringent zu prüfen, sowie die kollektive Verantwortlichkeit der beteiligten Nachrichtendienste. Ein Folgeprojekt zur Vernetzung der Aufsichtsbehörden fünf europäischer Länder (Belgien, Norwegen, Dänemark, Niederlande, Schweiz) zeigte jedoch, dass die jeweilige nationale Gesetzgebung es weitgehend unmöglich macht, als geheim eingestufte Sachverhalte gemeinsam zu besprechen. Hinderlich sind auch die Unterschiede in den Befugnissen der Auf-

sichtsbehörden, sich direkt über Datenbestände, Arbeitsweisen, Techniken und internationalen Kooperationsbeziehungen der ihnen unterstellten nationalen Nachrichtendienste zu informieren.

Auch wenn die EU auf absehbare Zeit keine Kompetenz zur rechtlichen Harmonisierung in diesem Bereich erhalten wird, sollten die europäischen Mitgliedstaaten die genannten Divergenzen schrittweise abbauen. Als erster Schritt sollten die nationalen rechtlichen Grundlagen für die internationale Zusammenarbeit der Nachrichtendienste präzisiert und einer Aufsicht unterstellt werden. Zugleich sollten die EU-Staaten ein höheres Rechtsschutzniveau anstreben, wenn es sich nicht um allgemeine Auslandsaufklärung, sondern um nachrichtendienstliche Überwachung von EU-Bürgern handelt. Für den Umgang mit Personen, die schwerer Verbrechen oder des Terrorismus verdächtigt werden, stehen innerhalb der EU weitere Instrumente zur polizeilichen Zusammenarbeit, Informationsgewinnung oder Beweissicherung zur Verfügung, die an ein rechtsstaatliches Strafverfahren gekoppelt sind. Daher sollte nicht nur über den fortwährenden Ausbau nachrichtendienstlich unterstützter Polizeiarbeit (intelligence-led policing) nachgedacht werden, wenn es um die Schnittmenge der Arbeit von Inlandsnachrichtendiensten und Polizeibehörden geht. Stattdessen sollte auch die andere Richtung in den Blick genommen werden, nämlich eine möglichst weitgehende Rückverlagerung in den Bereich der rechtsstaatlichen Strafverfolgung.

## Schlussfolgerungen und Ausblick

Künftig muss die Rolle der Nachrichtendienste für die Weiterentwicklung der EU-Sicherheitspolitik stärker berücksichtigt werden. Dieser besonders sensible Aspekt nationaler Souveränität wird sich auf absehbare Zeit nicht direkt im EU-Institutionengefüge manifestieren können. Jenseits der EU bestehen zahlreiche multilaterale Foren und historisch gewachsene Beziehungen der Nachrichtendienste. Beispiele



© Stiftung Wissenschaft und Politik, 2018  
**Alle Rechte vorbehalten**

Das Aktuell gibt die Auffassung des Autors wieder.

In der Online-Version dieser Publikation sind Verweise auf SWP-Schriften und wichtige Quellen anklickbar.

SWP-Aktuelle werden intern einem Begutachtungsverfahren, einem Faktencheck und einem Lektorat unterzogen. Weitere Informationen zur Qualitätssicherung der SWP finden Sie auf der SWP-Website unter <https://www.swp-berlin.org/ueber-uns/qualitaetssicherung/>

**SWP**  
Stiftung Wissenschaft und Politik  
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3–4  
10719 Berlin  
Telefon +49 30 880 07-0  
Fax +49 30 880 07-100  
[www.swp-berlin.org](http://www.swp-berlin.org)  
[swp@swp-berlin.org](mailto:swp@swp-berlin.org)

ISSN 1611-6364

sind die europäischen Partner (SIGINT Seniors Europe) der transatlantischen Five-Eyes-Allianz zur Fernmeldeaufklärung, das militärische Nachrichtenwesen der Nato oder die ebenfalls jahrzehntealte Police Working Group on Terrorism für die europäische Terrorismusbekämpfung. Diese vielfältige Vernetzung europäischer Nachrichtendienste, die sich auf bilateraler Ebene weiter ausdifferenziert, wird aufgrund der komplexen transnationalen Gefahren weitgehend erhalten bleiben müssen.

Allerdings sollten die EU-Mitgliedstaaten nicht nur auf ausgetretenen Pfaden wandern, sondern eigene Vorstellungen darüber entwickeln, welche nachrichtendienstliche Unterstützung für eine effektive Sicherheitspolitik der EU vonnöten ist. Der anstehende Brexit und die zunehmend volatilen transatlantischen Beziehungen erhöhen den Reformdruck. Statt fruchtlose Grundsatzdebatten über einen gemeinsamen Nachrichtendienst zu führen, sollten die Mitgliedstaaten die Gewinnung von Informationen und deren Weitergabe an die EU deutlich verlässlicher machen und zugleich die Kohärenz der europäischen Sicherheitspolitik bewahren. Im Rahmen freiwilliger Koalitionen und der PESCO kann eine verstärkte Zusammenarbeit mittelfristig auch gemeinsame Forschungs- und Beschaffungsprojekte zur technischen Aufklärung einschließen.

Vor allem bei der Terrorismusbekämpfung innerhalb der EU hat sich die nachrichtendienstliche Zusammenarbeit weiter intensiviert. Gleichwohl bleibt es geboten, schrittweise vorzugehen. Erst wenn sich ein systematischer und rechtsstaatlich kontrollierter Einsatz von Verbindungsbeamten bewährt hat, ist eine gemeinsame Plattform für Polizei und Nachrichtendienste auf EU-Ebene denkbar.

In jedem Fall sollten die Mitgliedstaaten sowohl die Befugnisse als auch die grenzüberschreitende Vernetzung ihrer nationalen Aufsichtsbehörden vorantreiben. Zumindest die reformierte CTG und die sich

weiterentwickelnden Schnittstellen von Europol müssen möglichst lückenlos kontrolliert werden, und zwar durch administrative Aufsichts- oder Datenschutzbehörden sowie parlamentarische Gremien. Traditionelle Normen für die nachrichtendienstliche Arbeit wie die Third Party Rule oder strenge Auslegungen des Geheim-schutzes müssen hierfür auf den Prüfstand gestellt werden. Langfristig sollte an einer europäischen Konvergenz der Aufsichtsstrukturen gearbeitet werden, um eine belastbare Grundlage für jegliche Formen europäischer und internationaler nachrichtendienstlicher Zusammenarbeit zu schaffen.

*Dr. Raphael Bossong ist Wissenschaftler in der Forschungsgruppe EU/Europa.*