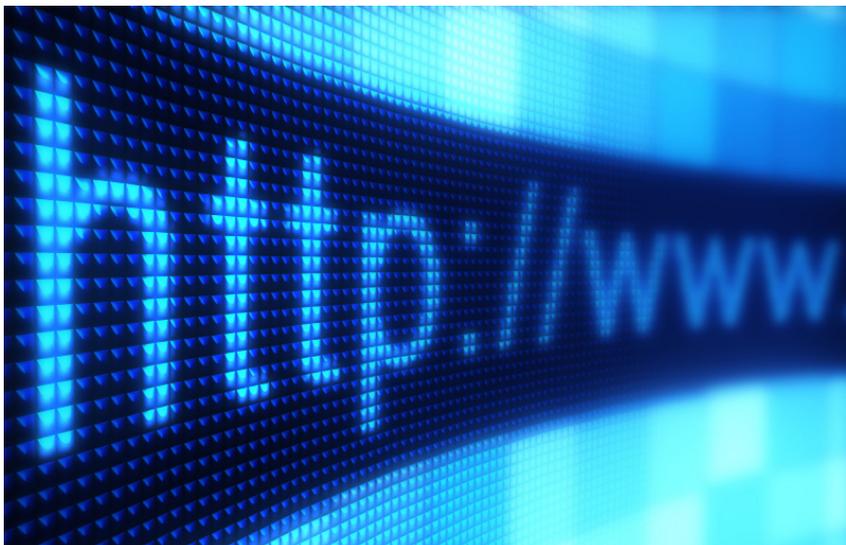


OPEN SOURCE INTELLIGENCE: NEUES NACHRICHTENDIENSTLICHES PARADIGMA?

Die nachrichtendienstliche Bedeutung von offen zugänglichen Informationen hat in den letzten Jahren zugenommen. Für die klassischen Nachrichtendienste wird *Open Source Intelligence* (OSINT) nur eine von mehreren Beschaffungsarten bleiben. Für viele andere Regierungsstellen ist OSINT jedoch häufig die einzige Möglichkeit der Informationsgewinnung und damit eine strategische Entscheidungsgrundlage. Die Ausarbeitung einer nationalen OSINT-Strategie und die Einrichtung eines OSINT-Zentrums sind prüfenswerte Massnahmen, um offen zugängliche Informationen systematischer nutzen zu können.



www.istockphoto.com

Das Konzept der *Open Source Intelligence* hat in den letzten Jahren an Bedeutung gewonnen. Früher beschäftigten sich die Nachrichtendienste hauptsächlich mit der Beschaffung und Auswertung von klassifizierten Informationen. Die massgeblichen Quellen für die Informationsgewinnung umfassten menschliche Quellen (*human intelligence*, HUMINT), die Fernmeldeaufklärung (*signals intelligence*, SIGINT) sowie die Satellitenaufklärung (*image-ry intelligence*, IMINT). Obwohl oft auch offene Quellen verwendet wurden, stellten diese nur ein ergänzendes Mittel dar. Die systematische Sammlung nicht geheimer Informationen war für die Nachrichtendienste nicht vorrangig, was unter anderem mit der überwiegend militärischen Natur der aufzuklärenden Bereiche zu tun hatte.

Heute wird OSINT von weiten Kreisen als unerlässliche Informationsquelle anerkannt. Dieser Wandel äussert sich darin, dass bei vielen Regierungsstellen und Nachrichtendiensten eine Diskussion über die bessere Nutzung von OSINT in Gang gekommen ist. Die genaue Rolle und das Potenzial von OSINT bleiben jedoch umstritten. Die einen schreiben OSINT eine Schlüsselrolle zu und fordern einen nachrichtendienstlichen Paradigmenwechsel mit einem neuen Schwerpunkt auf öffentlich zugänglichen Informationen und einer sektorübergreifenden Zusammenarbeit mit einem grossen Netzwerk von Fachleuten und privaten Unternehmen. Andere plädieren lediglich für eine Anpassung des traditionellen Paradigmas im Sinne einer stärkeren Gewichtung von OSINT innerhalb des multidimensionalen Ansatzes der Informationsbeschaffung.

Wachsende Bedeutung von OSINT

Unter OSINT versteht man die Beschaffung von allgemein zugänglichen Informationen und deren Aufbereitung zu einem Produkt mit nachrichtendienstlichem Mehrwert. Der Zugriff auf die verwendeten Quellen kann gratis oder kostenpflichtig sein. Die Informationen können aus den Medien, von öffentlichen Stellen, Think Tanks, Universitäten, Nichtregierungsorganisationen (NGOs) oder dem Privatsektor stammen.

Drei Hauptfaktoren haben dazu beigetragen, dass OSINT in letzter Zeit zunehmende Beachtung findet. Der erste Faktor bezieht sich auf die erhebliche Ausweitung des sicherheitspolitischen Bedrohungsspektrums in den letzten beiden Jahrzehnten. Zur Zeit des Kalten Kriegs beschäftigten sich die Nachrichtendienste mit einer beschränkten Zahl vorwiegend staatenbezogener Herausforderungen. Kernaufgabe war die Aufdeckung der Absichten und Fähigkeiten der Sowjetunion und des Warschauer Paktes. Seit dem Fall der Berliner Mauer hat sich der Themenbereich, mit dem sich die Nachrichtendienste befassen, jedoch dramatisch erweitert. Er schliesst heute Terrorismus, die Verbreitung von Massenvernichtungswaffen, die organisierte Kriminalität, innerstaatliche Konflikte, regionale Krisen, illegale Migration und Energiesicherheit mit ein. Da Themen wie Transport, Nahrungsmittelversorgung, Wasser und Klima ebenfalls zunehmend unter sicherheitspolitischen Gesichtspunkten betrachtet werden, steigt die Zahl der Regierungsstellen mit nachrichtendienstlichem Bedarf rasch an. Mit der steigenden Nachfrage nach Informationen in einem breiten Themenfeld hat

auch die Wertschätzung von OSINT zugenommen.

Der zweite Faktor betrifft die Technologie. Die Informationsrevolution hat das nachrichtendienstliche Umfeld stark verändert. Sie hat dazu geführt, dass heute eine Fülle von Informationen und ein breites Spektrum von Quellen nachrichtendienstlich verfügbar sind und die Welt insofern transparenter geworden ist. Gleichzeitig hat sie jedoch auch bewirkt, dass die klassischen Nachrichtendienste ihr Monopol bezüglich der Fähigkeiten und Informationen, die zum Verständnis und zur Bewältigung sicherheitspolitischer Bedrohungen nötig sind, verloren haben. Google Earth liefert heute mehr raumbezogene Aufklärungsdaten, als den meisten Regierungen noch vor wenigen Jahren zur Verfügung standen. Andere Internetdienste wie Wikipedia werden zunehmend auch als nachrichtendienstlich relevante Quellen verwendet. Daneben gibt es einen wachsenden kommerziellen Informations- und *Intelligence*-Markt mit Diensten, die lange Zeit dem öffentlichen Sektor vorbehalten waren.

Der dritte Faktor, der den Aufstieg von OSINT begünstigt hat, waren die nachrichtendienstlichen Fehlleistungen im Umfeld der Terroranschläge von 9/11 und des Irakkriegs. Vor allem in den USA war das Versagen der Nachrichtendienste Anlass für eine gründliche Überprüfung, wie Informationen gesammelt, analysiert und im politischen Entscheidungsfindungsprozess verwendet werden. Aufgrund der Forderung mehrerer Kommissionen, künftig OSINT systematischer zu verwenden, wurde schliesslich vom *US Director of National Intelligence* im November 2005 ein *Open Source Center* eröffnet. Seither hat die Anzahl von OSINT-Einheiten in US-Regierungsstellen zugenommen. Parallel dazu hat sich die OSINT-Debatte auch in anderen Ländern, vor allem in Europa, intensiviert.

Stärken von OSINT

Ein wichtiger Vorteil von OSINT ist, dass die Beschaffung weniger kostspielig als bei herkömmlichen Verfahren ist. Zudem können öffentlich zugängliche Informationen von einem viel grösseren Kreis potenzieller Analysten und Anwender gesammelt werden, da es sich nicht um eine Tätigkeit handelt, für die besondere gesetzliche Voraussetzungen geschaffen werden müssen. Offene Informationen sind rund um die Uhr zugänglich und verwertbar. Hinzu kommt, dass ihre Weitergabe weniger

OSINT: Nützliche Websites

Die folgenden Websites bieten aussen- und sicherheitspolitisch Interessierten eine Fülle offener Informationen.

- International Relations and Security Network** (www.isn.ethz.ch)
 Das ISN des Center for Security Studies (ETH Zürich) sammelt und verwaltet in seiner digitalen Datenbank Informationen von zahlreichen Think Tanks, Forschungsinstituten, internationalen Organisationen und Regierungsstellen. Es bietet einen tägliche Nachrichtenservice (Security Watch) an und indexiert den Inhalt sicherheitspolitisch relevanter Websites.
- Oxford Analytica** (www.oxan.com)
 Ein erstklassiger strategischer Analyse- und Beratungsdienst, der mit einem Netzwerk von Forschern und Fakultätsmitgliedern in Oxford und anderen grossen Universitäten weltweit zusammenarbeitet.
- Silobreaker** (www.silobreaker.com)
 Ein innovativer Nachrichten-Sammeldienst, der seine Informationen von mehr als 10'000 verschiedenen Quellen, einschliesslich Blogs sowie Forschungs- und Multimedia-Websites, bezieht. Silobreaker bietet auch soziale Netzwerkanalysen und Hintergründe zu Akteuren aus Politik, Wirtschaft und anderen Kreisen an.

kompliziert ist, als dies bei klassifizierten Informationen der Fall ist.

Aus der Perspektive der klassischen Nachrichtendienste erleichtert OSINT die Weitergabe und Veröffentlichung von Erkenntnissen, deren Relevanzüberprüfung de facto vorwiegend auf klassifizierten Informationen beruht. Aus der Perspektive eines sehr viel weiteren Nutzerkreises liegt die Hauptstärke von OSINT jedoch eher bei der Vermittlung des Kontexts, der für das Verständnis der heutigen Sicherheitsfragen unabdingbar ist. Angesichts der zunehmenden Komplexität und globalen Interdependenzen wird die Fähigkeit zur Identifizierung der sich abzeichnenden Problemlagen und längerfristigen Trends weiter an Bedeutung gewinnen. Die für eine strategische Früherkennung erforderlichen Quellen werden in aller Regel nicht klassifiziert sein.

Grenzen von OSINT

OSINT-Befürworter argumentieren, dass offen zugängliche Informationen 80 bis 95 Prozent des heutigen nachrichtendienstlichen Informationsbedarfs abdecken können. Die Nutzung von offenen Informationen für nachrichtendienstliche Zwecke hat jedoch auch ihre Grenzen. Es ist schwierig und zeitraubend, aus der Informationsfülle diejenigen Nachrichten herauszufiltern, die für die Aufklärung tatsächlich relevant sind. Oft können solche Informationen nur mit traditionellen nachrichtendienstlichen Mitteln überprüft und hinterfragt werden. Die Tatsache, dass die gleiche Information in verschiedenen Medien wiedergegeben wird, erhöht weder ihre Sachlichkeit noch ihren Wahrheitsgehalt. Was die insbesondere von privaten Akteuren angebotenen Informationsmanagement-Systeme betrifft, so können diese den gros-

sen analytischen Aufwand, der für die Einordnung und Bewertung von offenen Informationen erforderlich ist, nicht verkleinern.

Neben der Qualitätskontrolle besteht eine zweite Schwäche von offenen Informationen darin, dass OSINT nur beschränkt Daten liefert, die auf der operativen Ebene umsetzbar sind. OSINT kann viel zu einem besseren Verständnis der Motive des Terrornetzwerks al-Kaida beitragen, wird aber deshalb noch nicht den genauen Aufenthaltsort von Osama bin Laden liefern. Terroristische Organisationen und das organisierte Verbrechen sind sich ihres verräterischen «digitalen Fussabdrucks» zunehmend bewusst und sehen sich gezwungen, offline zu gehen und unterhalb des Radarhorizonts zu operieren. Ebensowenig lassen sich durch OSINT alle relevanten Informationen über das iranische Atomprogramm oder die nuklearen Absichten Nordkoreas erfassen. Dasselbe gilt für operative Aspekte der Geldwäscherei oder des Drogenhandels, um zwei weitere Beispiele zu nennen.

Unterschiedliche Bedürfnisse

Aus der obigen Analyse lassen sich zwei zentrale Schlussfolgerungen ziehen. Erstens erscheint eine verstärkte strategische Nutzung von OSINT notwendig, machbar und vielversprechend. Zweitens kommt diesem Befund je nach Benutzerkreis unterschiedliche Bedeutung zu. Ob OSINT ein neues nachrichtendienstliches Paradigma darstellt oder lediglich eine Modifikation des traditionellen Paradigmas erfordert, hängt wesentlich vom Standpunkt des Betrachters ab. Für die klassischen nachrichtendienstliche Kreise wird OSINT nach wie vor eine von mehreren Beschaffungsmethoden bleiben, die HUMINT, SIGINT und IMINT ergänzt und diese Ansätze in Zukunft noch vermehrt durchdringen

dürfte. Für viele andere Regierungsstellen ist OSINT jedoch die einzige «INT», zu der sie einen umfassenden Zugang haben. Für sie kann OSINT deshalb eine zentrale strategische Entscheidungshilfe darstellen.

Entsprechend sind auch die Herausforderungen, die sich im Hinblick auf eine systematischere Nutzung von OSINT ergeben, je nach Regierungsstelle teilweise unterschiedlich. Innerhalb der traditionellen Nachrichtendienste ist vor allem ein Mentalitätswandel erforderlich. Viele Analysten haben immer noch Vorurteile gegenüber offenen Quellen. Das kann so weit gehen, dass aus öffentlichen Quellen stammende Informationen routinemässig mit dem Stempel «geheim» versehen und unter Verschluss gehalten werden, was ihren Nutzen reduziert. Es gibt westliche Nachrichtendienste, die ihren Mitarbeitenden aus Sicherheitsgründen den Zugang zum Internet untersagen. Neben einem Mentalitätswandel werden in Zukunft auch mehr finanzielle Ressourcen erforderlich sein. Eine Stärkung der OSINT-Kapazitäten verlangt Investitionen sowohl in die Ausbildung der Analysten als auch in den IT-Bereich.

Für die Regierungsstellen ausserhalb des nachrichtendienstlichen Sektors besteht die zentrale Herausforderung darin, ämter- oder departementsspezifische Lösungen zu vermeiden, die zu Doppelspurigkeiten und einem unkoordinierten System von Partnerschafts-Vereinbarungen und Outsourcing-Verträgen führen. In diesem Zusammenhang kann die Erarbeitung einer nationalen OSINT-Strategie nützlich sein. Eine solche Strategie sollte die folgenden grundlegenden Fragen thematisieren: Welche institutionelle Lösung trägt den OSINT-Bedürfnissen der verschiedenen Regierungsstellen am besten Rechnung? Wie können der Informationsfluss und die Zusammenarbeit zwischen den Regierungsstellen verbessert werden? Wo findet man Personal, das in der Lage ist, interdisziplinär zu denken und zu arbeiten? Wie ist mit der rasanten technologischen Entwicklung umzugehen?

Vorteile eines OSINT-Zentrums

Auf diese Fragen muss jede Regierung ihre spezifischen Antworten finden. Eine sinnvolle Massnahme könnte die Einrichtung eines OSINT-Zentrums als Kompetenzzentrum für offene Informationen sein. Eine solche Einheit könnte entweder im Rahmen bestehender nationaler Sicherheitsstrukturen oder als separate Organisation errichtet werden. In beiden Fällen sollte sie

Die Institutionalisierung von OSINT: Das US-Modell

Assistant Deputy Director of National Intelligence for Open Source

- Entwickelt und beaufsichtigt das nationale OSINT-Konzept
- Stellt die Entwicklung einer einheitlichen OSINT-Architektur sicher
- Berät nicht-nachrichtendienstliche Regierungsstellen hinsichtlich der Beschaffung von offenen Informationen

National Open Source Committee

- Lenkungsgruppe für alle OSINT-Belange
- Mitglieder sind hochrangige Beamte des Open Source Center, des Office of the Under Secretary of Defense for Intelligence, des Department of Homeland Security, des CIA, der National Security Agency, der National Geospatial-Intelligence Agency, des Department of State's Bureau of Intelligence and Research, der Defense Intelligence Agency, des Federal Bureau of Investigation, u.a.

Open Source Center

- Gegründet 2005 vom Director of National Intelligence; CIA dient als Exekutivorgan
- Mehrere hundert Vollzeitbeschäftigte
- Unterstützt die Nachrichtendienste in der Nutzung von OSINT und der Entwicklung von kleinen OSINT-Zentren in den jeweiligen Ämtern
- Fördert die Beschaffung, Analyse und Verbreitung von OSINT in allen Regierungsstellen
- Stellt Regierungsbeamten Berichte, Übersetzungen und analytische Produkte auf einer passwortgeschützten Website online zur Verfügung (www.opensource.gov)

Quellen: Intelligence Community Directive No. 301; CRS Report for Congress, 5 December 2007.

jedoch dem direkten Einfluss eines einzelnen Departements entzogen sein.

Ein OSINT-Zentrum könnte mit folgenden Hauptaufgaben befasst sein: Unterstützung sowohl der traditionellen Nachrichtendienste als auch anderer Regierungsstellen mit OSINT-Recherchen; Koordinierung regierungswweiter OSINT-Bedürfnisse; Definition der geeigneten OSINT-Instrumente und -Technologien; Kooperation mit regierungsexternen Akteuren; Kommunikation von *Best Practices* für die Sammlung, das Management, die Auswertung und die Verbreitung von Informationen; Training und Ausbildung; Frühwarnung und langfristige Prognosen.

Ein OSINT-Zentrum sollte sowohl über einen ständigen Mitarbeiterstab als auch über wechselnde Mitarbeiter von verschiedenen Regierungsstellen verfügen. Unerlässlich dürfte zudem der Austausch und die Zusammenarbeit mit Partnern aus dem Privatsektor und der Wissenschaft sein. Zwar werden die Einrichtung und der Unterhalt einer derartigen Behörde mit einem Kostenaufwand verbunden sein. Durch den koordinierten Zugang zu erstklassigen Informationsdiensten und durch Synergien im IT-Bereich werden im Vergleich zu ämter-spezifischen Lösungen aber erhebliche Kosten eingespart werden können.

OSINT in der Schweiz

Eine Reihe von Initiativen und Massnahmen deutet daraufhin, dass OSINT auch in

der Schweiz zum Thema geworden ist. So existiert eine interdepartementale OSINT-Arbeitsgruppe, die Synergienmöglichkeiten zwischen den betroffenen Ämtern ausleuchtet. Eine zweite Arbeitsgruppe befasst sich mit OSINT auf Stufe VBS. Im Strategischen Nachrichtendienst und im Militärischen Nachrichtendienst ist OSINT ebenso institutionalisiert worden wie im Inlandnachrichtendienst im Bundesamt für Polizei, wo 2001 eine kleine OSINT-Sektion gegründet wurde. Ferner haben einzelne Departemente ihre ersten – zwispältigen – Erfahrungen mit IT-basierten Wissensmanagement-Systemen gemacht.

Ausstehend ist die Formulierung einer OSINT-Strategie, die diese Aktivitäten auf politischer Ebene koordiniert, Rollen und Verantwortlichkeiten definiert und allenfalls die Schaffung einer zentralisierten OSINT-Infrastruktur für alle interessierten Ämter veranlasst. Die gegenwärtigen Diskussionen bezüglich einer Revision der zivilen Nachrichtendienste und der Schaffung eines Sicherheitsdepartments sollten als Chance genutzt werden, um auch die Frage der künftigen Rolle und institutionellen Verankerung von OSINT in der Schweiz gründlich zu untersuchen und zu klären.

■ Verantwortlicher Editor: Daniel Möckli analysen@sipo.gess.ethz.ch

■ Bezug und kostenloses Abonnement: www.ssn.ethz.ch