ESG
A HENSOLDT COMPANY

OSINT CHRONICLE

Vierteljährliche Paper-Reihe zur Einführung
in die Welt der offenen Quellen

OSINT CHRONICLE

Vierteljährliche Paper-Reihe zur Einführung in die Welt der offenen Quellen

Die vierteilige Paper-Reihe zu Open Source Intelligence (OSINT) gewährt jedes Quartal Einblicke in die tiefgründige Welt dieser Intelligence-Disziplin. Den Auftakt macht das erste Paper am 08.04.2024, danach erscheint am Montag jedes Quartals ein weiteres Paper. Die Paper sind dabei so konzipiert, dass sie verschiedene Facetten von OSINT beleuchten, um die Leserschaft fundiert in die Materie einzuführen. Die einzelnen Paper behandeln dabei unterschiedliche Schwerpunkte.

Das erste Paper widmet sich den Grundpfeilern von OSINT, angefangen bei der Historie, über die Definitionen bis hin zu den grundlegenden Konzepten.

Im zweiten Teil liegt der Fokus auf den notwendigen Fähigkeiten und Fertigkeiten sowie ganzheitlichen Schulungsansätzen, um in der Disziplin zu bestehen. Der dritte Teil deckt die rechtlichen Rahmenbedingungen und ethischen Fragestellungen der Thematik auf. Dabei wird ein einzigartiger Einblick in die Herausforderungen und Ungewissheiten dieser Disziplin gewährt. Das finale vierte Paper taucht in den gegenwärtigen technologischen Status quo von OSINT ein, präsentiert die neuesten Trends und analysiert die Diskrepanzen zwischen Theorie und Praxis.

Datum	Paper Thema
08.04.2024	Historische Herleitung und Definition von OSINT
01.07.2024	Ganzheitliche Schulung/Schulungsansätze
02.09.2024	Rechtliche und ethische Herausforderungen/Ungewissheiten
07.01.2025	Technologischer Status Quo

Verfolgen Sie die Serie für tiefgreifende Einblicke in die Intelligence-Disziplin OSINT.

Eine Kooperation der Unternehmen ESG Elektroniksystem- und Logistik-GmbH,
Munich Innovation Labs GmbH und PREVENCY GmbH

OSINT auf den Spuren

Die Evolution und Grundlagen von Open Source Intelligence

1 Abstract

Aktuell erfährt „Open Source Intelligence“ (OSINT) einen nie dagewesenen Diskurs. Grundlegende wissenschaftliche Publikationen, die die „Intelligence-Disziplin“ umfänglich durchdringen, fehlen jedoch bisher. Dieses Paper zielt darauf ab, diese Undurchsichtigkeit des Themas zu konterkarieren und liefert tiefgehende Einblicke in die Fundamente von OSINT. Das Paper erörtert dazu die Evolutionsstufen von OSINT, beleuchtet die Begriffe „Open Source Data“ (OSD) und „Open Source Information“ (OSINF), legt die Abgrenzung von OSINT zu den anderen Intelligence-Disziplinen offen und gibt die Phasen der Generierung von „Intelligence“ anhand des „Intelligence Cycle“ wieder.

2 Einleitung

OSINT ist ein derzeit so vielseitig diskutiertes Thema wie nie zuvor. Der Erkenntnisgewinn aus für die Öffentlichkeit verfügbaren Daten [1] spielt spätestens seit der russischen Invasion der Ukraine im Jahr 2022 eine unwiderlegbar große Bedeutung. Die Echtzeitanalyse insb. sozialer Medien brachte in diesem Zuge nachrichtendienstlich hochgradig relevante Erkenntnisse über Smartphone-Videos und -Posts zutage [3,4]. Aufgegriffen werden solche Informationen wiederum von anderen Staaten, um u. a. zur Meinungsbildung in der Weltöffentlichkeit beizutragen [3]. Auch dienen sie Recherchekollektiven wie Bellingcat [5] als Grundlage für investigativen Journalismus. Der Begriff OSINT ist jedoch über die ukrainisch-russischen Kriegsgeschehnisse hinaus allgegenwärtig. Anzutreffen ist er so beispielsweise ebenfalls in Bezug zu den sog. „Panama Papers“ [6,7], welche den größten „Informationsleak“ der Geschichte [8,9] verkörpern sollen. Datenjournalisten, die als OSINT-Experten für Verifizierungsarbeiten hinzugezogen werden, haben sich in diesem Zuge als unabdingbar etabliert [6].

OSINT ist allerdings kein neues Konzept, sondern geht weit vor die Entstehung und Nutzung des Internets zurück [10,11]. Sie zählt zu einer der ältesten nachrichtendienstlichen Disziplinen überhaupt [12]. Trotz zahlreicher Ansätze, OSINT zu definieren oder einheitliche Frameworks zu entwickeln [vgl. z.B.: 13–15], bleibt das Konzept der (intelligenten) Analyse allerdings bis heute in der einschlägigen Literatur umstritten [16,17,2]. Dies liegt nicht zuletzt daran, dass jede Definition von OSINT den Fortschritten der Computer- und Datenwissenschaften, die kontinuierlich Verbesserungen von (intelligenten) Erfassungs- und Analysemöglichkeiten hervorbringen, unterliegt [17,2]. Zudem gehen mit dem technologischen Fortschritt zahlreiche neue offene Kommunikationsmittel einher, die eine regelrechte „Informationsexplosion“ bewirkt haben [15,1,13]. Dies wiederum verlangt nach der fortlaufenden Generierung neuer Verifizierungs- und Zuordnungsmechanismen [18,1]. Damit einhergehend haben die Entwicklungen des 21. Jahrhunderts zahlreiche Debatten darüber angestoßen, ob und wie OSINT von den verwandten, eingestuften Intelligence-Disziplinen abzugrenzen ist [2,4]. Ursprünglich nur den Verteidigungs- und Nachrichtendiensten vorbehaltene Technologien sind heute, vorranging über das Internet, auch der breiten Öffentlichkeit zugänglich [13,2]. Das Verständnis von Intelligence hat sich in diesem Zuge gänzlich gewandelt [19]. Bisherige Definitionen von OSINT sind daher immer nur im jeweiligen historischen Kontext zu betrachten [2]. Die zunehmende Geschwindigkeit der Entwicklung macht es überdies nahezu unmöglich, Prognosen über die zukünftige Ausgestaltung von OSINT und deren Auswirkungen abzugeben [20]. Betroffen von diesen sind dabei nicht nur Individuen und Organisationen im Einzelnen, sondern auch die Gesellschaft als solche [17].

Bislang mangelt es allerdings an entscheidenden grundlegenden wissenschaftlichen Veröffentlichungen, um die Undurchsichtigkeit des Themenfelds zu durchdringen [21]. Um diesen Problemstellungen zu begegnen und eine solide Wissensgrundlage zu schaffen sowie das Forschungsgebiet von OSINT systematisch weiter zu durchdringen, erfolgt in diesem Paper zunächst eine umfassende Aufarbeitung der relevanten Definitionen im historischen Verlauf. Zudem werden

die mit der Definition von OSINT unmittelbar verbundenen Begriffe OSD und OSINF sowie Intelligence für ein vollumfängliches Verständnis eingehender erläutert [22]. Darüber hinaus wird die Abgrenzung von OSINT zu den anderen Intelligence-Disziplinen erörtert und die Phasen der Generierung von Intelligence werden anhand des „Intelligence Cycle" dargelegt.

3 Open Source Intelligence (OSINT)

OSINT kann vor dem historischen Hintergrund in drei „Generationen" unterteilt werden. Diese ziehen sich wellenartig (siehe Abb. 1), entsprechend der auf- und absteigenden Wichtigkeit der Thematik, durch die Historie [2].

3.1 Open Source Intelligence (OSINT) der ersten Generation

Die Terminologie OSINT ist zwar modern, dessen Techniken reichen jedoch weit vor das Internet zurück [4,22,23,10]. Das Sammeln von Informationen aus öffentlichen, nicht eingestuften, legal zugänglichen Quellen ist damit eine ebenso traditionelle nachrichtendienstliche Praktik [4] wie alle anderen [12,11]. Ihren Ursprung findet diese 1939 in Großbritannien (einige Quellen verweisen sogar auf eine Entstehung bis in das 16. Jahrhundert zurück, unabhängig beginnend in verschiedenen Ländern [24]). Die britische Regierung beauftragte die „British Broadcasting Corporation" (BBC) mit der Untersuchung und Zusammenfassung ausländischer Printmedien sowie des damalig immer wichtiger werdenden Rundfunks. Herausgegeben wurde diese in Form des Sammelbands „Digest of Foreign Broadcasts", heute bekannt als „BBC Monitoring" [25,11]. 1941, mit der Gründung des „Foreign Broadcast Monitoring Service" (FBMS), folgte in Amerika die erste offizielle OSINT-Einrichtung. Ihre Aufgabe war die Überwachung, Filterung, Transkription, Übersetzung und Archivierung von Nachrichten und Informationen aus (ausländischen) Medienquellen [10,26,11,2]. Nur ein Jahr später, 1942, mit dem Eintritt der USA in den zweiten Weltkrieg, wurde dann das „Office of Strategic Services" (OSS) gegründet [27,11]. Damit wurde der Grundstein der modernen nachrichtendienstlichen Forschung und Analyse sowie der späteren „Central Intelligence Agency" (CIA) gelegt [27]. In dieser Anfangsphase, auch bezeichnet als die „erste Generation" oder das „erste Level" von OSINT, lag

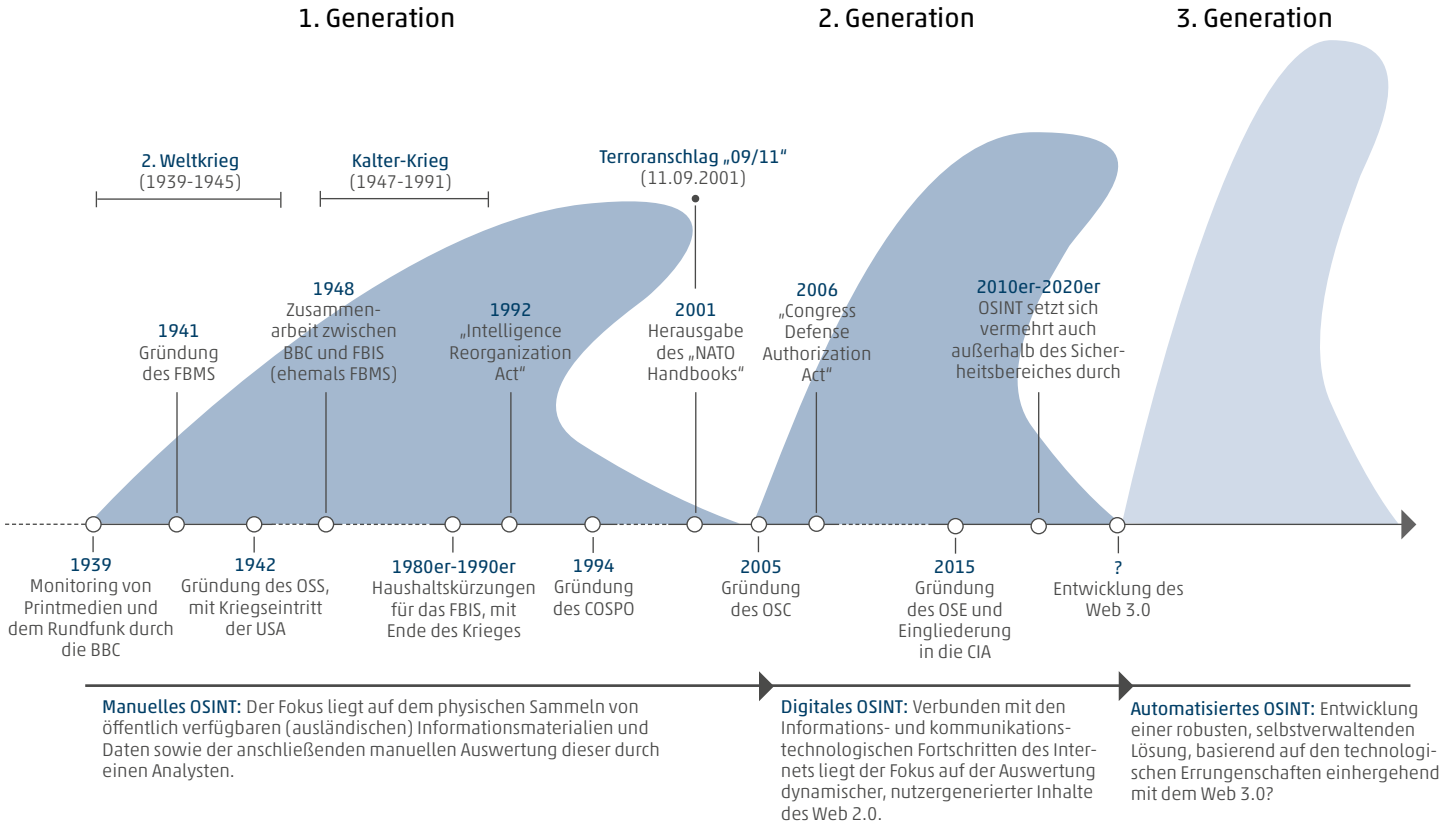

Abb.1: OSINT-Generationen sowie Einflüsse und Ereignisse im Zeitverlauf / Quelle: Eigene Darstellung, Design in Anlehnung an Williams und Blum [2]

der Fokus auf dem physischen Sammeln öffentlich verfügbarer Informationsmaterialien. Die anschließende Auswertung dieser erfolgte rein manuell [19,17,28,2]. Im Mittelpunkt der Tätigkeit stand somit die Fähigkeit eines Analysten, relevante Informationen zu finden, zu kodieren und auf transparente Weise zu einem sinnvollen Ganzen zusammenzusetzen [28,10]. Ihre Hochform fand diese Art der klassischen OSINT im Kalten Krieg. In dessen Verlauf setzte sie sich als etablierte nachrichtendienstliche Methode zur Informationsgewinnung durch [12,19,11]. 1948 folgte so eine offizielle Zusammenarbeit zwischen der BBC und dem „Foreign Broadcast Intelligence Service" (FBIS), dem ein Jahr zuvor umbenannten FBMS [26], mit dem Ziel der Vermeidung von Doppelarbeiten [11]. In den Folgejahren fand OSINT ebenfalls Verbreitung in weiteren Ländern auf beiden Seiten des Eisernen Vorhangs. Das „Ministerium für Staatssicherheit" (MfS) der DDR analysierte so beispielsweise monatlich rund 1.000 westliche Zeitschriften sowie 100 Bücher und fasste täglich mehr als 100 Zeitungen und 12 Stunden westdeutscher Radio- und Fernsehsendungen zusammen [11].

Trotz der Erfolge, die der FBIS verbuchte, wie z.B. die Erhebung erster Hinweise auf einen Abzug sowjetischer Raketen aus Kuba [12,2], folgten mit dem Ende des Kalten Krieges drastische Haushaltskürzungen für die Institution. Die OSINT-Bewegung der ersten Generation kam damit nach und nach zum Erliegen [2]. Die Voreingenommenheit der Nachrichtendienste gegenüber dem Informationsgehalt öffentlicher Quellen, einhergehend mit dem Fehler aus früheren Zeiten, ausschließlich Geheimnisse als Intelligence zu werten [29], überwog erneut [19,23,11,18,2].

Dies änderte sich erst wieder mit dem steigenden Informationsaufkommen der 1990er Jahre. Mit der Erfindung des Internets erfolgte schließlich eine grundlegende Informationsrevolution [17,22,30,11], die einen Wandel hin zur modernen Informationsgesellschaft nach sich zog. Begleitet wurde dies von einer steigenden Informationsflut und immer effizienter werdenden Technologien aus den Bereichen der Informatik, der Datenwissenschaft und der Statistik. Die Erfassung und die Analyse von Daten und Informationen vereinfachte sich in der Folge weitreichend [19,17,22]. Traditionelle Nachrichtenprinzipien wurden damit mit einem Schlag grundlegend revidiert. Mit der Einführung der modernen Informationssysteme wurde ein Großteil der Quellen und Techniken, die früher nur Geheimdiensten zur Verfügung standen, nun fortschreitend der breiten Öffentlichkeit zugänglich [23]. Dies führte schließlich auch bei der „United States Intelligence Community" (IC) zu der Erkenntnis, dass eine grundlegende strukturelle Reform notwendig ist, um den immer dynamischer werdenden Informationsanforderungen und -kanälen weiterhin gerecht zu werden [19,30,2]. Der Begriff OSINT hielt damit Einzug in die einschlägige Literatur [4]. Vorrangig geprägt wurde er zunächst von der US-Militäraufklärung, die 1992 im Rahmen des „Intelligence Reorganization Acts" erstmals auch öffentliche Quellen offiziell als Basis der Informationsbeschaffung aufführte [31,30]. 1994 folgte daraufhin die Errichtung des „Community Open Source Program Office" (COSPO) mit dem Ziel, die Nutzung öffentlicher Informationen gezielt durch die IC zu steuern. Dennoch konnte mit der rapiden Zunahme der verfügbaren Informationen und der wachsenden Bedeutung von OSINT nicht Schritt gehalten werden, wie schließlich die Anschläge vom 11. September 2001 zeigten [30]. „09/11" erwies sich als Wendepunkt für die Entwicklung von OSINT [11]. Die „North Atlantic Treaty Organization" (NATO) [22] veröffentlichte noch im selben Jahr ein Handbuch zu OSINT mit dem Versuch der Einführung eines einheitlichen Rahmenwerks. Sie publizierte damit eine der ersten und bis heute häufig referenzierten Definitionen [vgl. 1]:

> „Open Source Intelligence (OSINT) is information that has been deliberately discovered, discriminated, distilled, and disseminated to a select audience, generally the commander and their immediate staff, in order to address a specific question. OSINT, in other words, applies the proven process of intelligence to the broad diversity of open sources of information, and creates intelligence." [22]

Die NATO [22] unterteilte OSINT in diesem Zuge zudem erstmalig in die weiteren aufeinander aufbauenden Bestandteile OSD und OSIF (siehe Abb. 2).

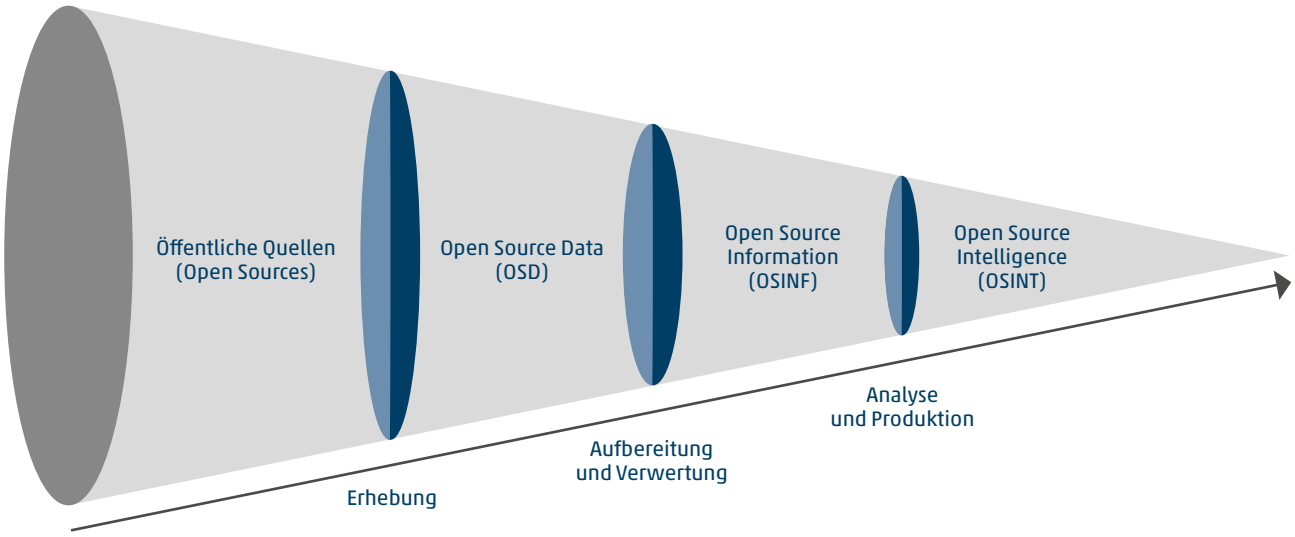

Abb.2: Open Source Intelligence Funnel
Quelle: Eigene Darstellung, Design in Anlehnung an die JCS [37]

3.2 Open Source Intelligence (OSINT) der zweiten Generation

Auf Anraten der „9/11 Commission" wurde im Jahre 2005 unter Eingliederung des FBIS das „Open Source Center" (OSC) errichtet [31,11,30]. Die Gründung des OSC als führende OSINT-Institution der US-Regierung markiert den Beginn der „zweiten Generation" von OSINT. Vorangetrieben durch die Weiterentwicklung des Internets zum Web 2.0 und die damit verbundenen informations- und kommunikationstechnologischen Fortschritte wird in diesem Zuge auch von „Digital OSINT" gesprochen [17,18,2]. Die damit einhergehenden dynamischen Webseiten und die Erzeugung dezentraler nutzergenerierter Inhalte, z.B. über die Entwicklung sozialer Netzwerke oder dem „Internet of Things" (IoT) haben OSINT zu einer immer komplexer werdenden Disziplin reifen lassen [32,20,33,2]. 2006 wurde mit der „Defense Strategy for Open-Source Intelligence'' in der Folge der weitere Ausbau von OSINT unter dem US-Verteidigungsministerium verabschiedet [11,30]. Zudem erfolgte unter dem „Congress Defense Authorization Act" eine neue Arbeitsdefinition für OSINT:

> „Open-source intelligence (OSINT) is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement." [30]

2011 wurde diese Definition vom Büro des Direktors der nationalen Nachrichtendienste der USA (DNI) übernommen und um den letzten Satz „OSINT draws from a wide variety of information and sources" erweitert [34]. Mit diesem unterstrich er die wachsende Informationsflut, häufig auch referenziert als „Big Data" [33,4,15]. Die steigende Datenflut führte überdies zu Ansätzen, die Definition von OSINT auf Basis der in einen Recherchevorgang überwiegend involvierten Quellen weiter zu unterteilen. Aus sozialen Medien abgeleitete Erkenntnisse werden so beispielsweise auch mit dem Akronym „Social Media Intelligence" (SOCMINT) betitelt [35–37].

Eine Definition, die starke Ähnlichkeit zu der vorangehenden aufweist, wurde schließlich auch von den „Joint Chiefs of Staff der U.S. Army" (JCS), die den U.S. Generalsstab repräsentieren, adaptiert:

> „Derived from the systematic collection, processing, and analysis of publicly available information in response to known or anticipated intelligence requirements. Also called OSINT." [38]

Ähnlich lautende Definitionen lassen sich ferner auch in Deutschland wiederfinden. Im Online-Glossar des Bundesamtes für Verfassungsschutz (BfV) heißt es so beispielsweise:

„Open Source Intelligence (OSINT) bezeichnet die Informationsgewinnung aus offenen Quellen. OSINT-Maßnahmen sind das Monitoring von Internetseiten, aber auch die gezielte Recherche nach sämtlichen öffentlich zugänglichen Informationen zu einer Zielperson. […]."[39]

3.3 Open Source Intelligence (OSINT) der dritten Generation

Die Definition von OSINT der zweiten Generation findet somit langsam Verstetigung in der Literatur und scheint sich als anerkannte nachrichtendienstliche Disziplin zu behaupten. 2015 wurde so beispielsweise das OSC in das „Open Source Enterprise" (OSE) umbenannt und unter dem neuen Direktorat für digitale Innovation direkt in die CIA eingegliedert [40]. Das Internet auf der anderen Seite erfährt bereits eine neue Transformation hin zum Web 3.0. Orientierend an der Historie könnte damit wiederum eine neue Generation von OSINT eingeläutet werden [2]. Unter dem Web 3.0 ist ein „semantisches" Web zu verstehen, das die direkte und indirekte maschinelle Verarbeitung von Daten bis hin zur künstlichen Intelligenz umfasst. OSINT zu einer robusten, selbstverwaltenden Lösung auszubauen und den Prozess vom Datensammeln bis hin zum Analysieren vollständig zu automatisieren, rückt somit in den Vordergrund [10,14]. Betrachtet wird dies jedoch längst nicht mehr nur als rein staatliche Angelegenheit. Auch private Forschungseinrichtungen und Organisationen außerhalb des Sicherheitsbereichs [41,29] treiben die Entwicklung solcher Systeme, z.B. für Wettbewerbsanalysen oder Marketingaktivitäten, massiv voran [32,19,17]. In der aktuellen Literatur lassen sich daher auch nicht speziell auf die Sicherheitsbehörden zugeschnittene Begriffsbestimmungen finden. Dokman und Ivanjko [19] verweisen in ihrer Definition so beispielsweise als Empfänger auf Zielgruppen und Begünstigte im Allgemeinen:

„Open Source Intelligence (OSINT) is an intelligence product which has been processed, analysed and obtained from the publicly available information. It should be actionable and disseminated in a timely manner to the appropriate audience. Open source intelligence transfers specific knowledge to beneficiaries for them to use it in their actions and the decision-making process."

4 Open Source Data (OSD)

Der Ausgangspunkt aller OSINT-Vorhaben liegt in Daten. Daten bilden die Grundlage der Analyse und der daraus abgeleiteten Rückschlüsse [36]. Unabdingbar gilt dabei, dass ein Entscheidungsunterstützungssystem immer nur so gut sein kann wie der verwendete Datensatz [42]. OSD referenziert in diesem Zusammenhang auf nicht prozessierte [1], allgemeine Rohdaten, die offen verfügbar [12] und auf legalem, ethisch vertretbarem Wege [11,22] zugänglich sind. Nicht ausgeschlossen werden in der Praxis Quellen, deren Zugang zusätzliche Anstrengungen erfordert [41] oder kommerziell erworben werden muss [2,22,38]. Gleichzeitig bedeutet der Zusatz „auf legalem und ethisch vertretbarem Wege" jedoch, dass nicht alle öffentlich zugänglichen Daten automatisch auch als OSD zu behandeln sind [31,11].

Eine große Schwierigkeit bei der Festlegung, welche Daten und Quellen dabei im Einzelnen unter OSD zusammenzufassen sind, besteht ebenfalls in den voranschreitenden technologischen Entwicklungen. Verbesserte Datenspeicher- und Übertragungstechnologien, wie 5G-Datennetze und Cloud-Technologien, sowie Suchmaschinen [28] ermöglichen es, historisch beispiellose Mengen an Daten zu produzieren, zu recherchieren, zu speichern und auszutauschen [18]. Zudem rufen sie eine sich rasch verändernde Natur der Quellen hervor [2]. Eine eindeutige Zuordnung ist daher bislang nicht abschließend geklärt [2]. Genauso ungeklärt sind die unmittelbar damit verbundenen rechtlichen und ethischen Fragestellungen [43,17,18]. Die Abgrenzung zwischen öffentlichen und verschlossenen/geheimen Quellen verläuft überaus schwimmend [23]. Zudem ist die Zugänglichkeit und Auswertung der Daten sowie die Nutzung der gewonnenen Informationen rechtlich bislang nicht klar umrissen [43,14].

5 Open Source Information (OSINF)

OSD sind für sich genommen noch von geringem Nutzen und werden erst in ihrer Zusammenführung von (nachrichtendienstlichem) Belang [2]. Die regelrechte Datenexplosion der letzten Jahre hat diese Aufgabe hinsichtlich der inbegriffenen „Junk"-Inhalte sowie irreführenden Informationen und Fehlinformationen zu einer wahren Herausforderung werden lassen [18,19]. Bevor aus ihnen Intelligence gewonnen werden kann,

sind die Daten daher zunächst einem Aufbereitungsprozess zu unterziehen, der eine gewisse Filterung, Validierung und Verdichtung umfasst [1,22]. Das Ergebnis dieser Organisation der Daten [11] wird als OSINF bezeichnet [22], auch bekannt unter der Abkürzung OSIF [22]. Sie bilden die Grundlage der darauf aufbauenden Wissensgenerierung [1,11]. In ihrem Handbuch verabschiedete die NATO dazu [22] folgende Definition:

> „OSIF is comprised of data that can be put together, generally by an editorial process that provides some filtering and validation as well as presentation management. OSIF is generic information that is usually widely disseminated. Newspapers, books, broadcast, and general daily reports are part of the OSIF world."

OSINF ist demnach klar von OSD zu unterscheiden [1,19,38], dennoch erfolgt die Verwendung der Begriffe in der Literatur nicht vollständig trennscharf [22,34,38]. Darüber hinaus stellt sich bei der Definition von OSINF die rechtliche Frage, ob auch öffentlich gewonnene Informationen ab einem gewissen Punkt als Verschlusssache einzustufen sind [23,38,18].

6 Intelligence und Intelligence-Disziplinen

Die aus den öffentlichen Daten gewonnenen Informationen [11] sind für sich genommen noch von beschränkter Aussagekraft. Sie beziehen sich auf die Vergangenheit und können die Gegenwart allenfalls porträtieren [44]. Erst durch ihre gezielte Analyse können aus ihnen fundierte Erkenntnisse über die Zukunft abgeleitet werden [45,46], die als Grundlage zur Entscheidungsfindung dienen [47,48]. Das in diesem Sinne extrahierte handlungsrelevante Wissen [19,34,49] wird als Intelligence bezeichnet [48,1]. Intelligence besteht somit immer aus Informationen, nicht alle Informationen repräsentieren aber Intelligence [50].

Neben OSINT wird in der einschlägigen Literatur in fünf weitere Disziplinen, die das Generieren von Intelligence aus Rohdaten zur Aufgabe haben, unterschieden [34]. Diese werden gemeinhin auch als "Intelligence gathering disziplines" (hier mit Intelligence-Disziplin umschrieben) bezeichnet [19,38]. Zu nennen ist hierunter zunächst **„Human Intelligence" (HUMINT)**. Sie beschreibt das Beziehen von Informationen durch Menschen von menschlichen Quellen in verbaler oder nonverbaler Form [18,38]. Als zweites aufzuführen ist die Disziplin **„Geospatial Intelligence" (GEOINT)**. GEOINT bezeichnet die statische oder zeitbezogene Analyse von Bildmaterialien und Geodaten [18,38]. Die dritte Disziplin entspricht **„Measurement and Signature Intelligence" (MASINT)**. Unter MASINT ist die quantitative und qualitative Analyse physischer Eigenschaften von Zielobjekten und Ereignissen/Phänomenen zu verstehen [38,34]. Als vierte Disziplin ist **„Signals Intelligence" (SIGINT)** zu nennen. Hierunter sind gewonnene Erkenntnisse aus der Auswertung (ausländischer) Kommunikationssysteme und nicht kommunikationsbezogener Sender zu verstehen [51,38]. Die fünfte Disziplin entspricht **„Technical Intelligence" (TECHINT)**. Unter TECHINT wird die Analyse ausländischen Materials/Equipments, wie z.B. Waffensystemen, und (damit verbundener) wissenschaftlicher Informationen sowie Forschungserkenntnissen, z.B. Ingenieurstechniken, verstanden [38,31].

Unterschieden werden die Disziplinen somit vorrangig nach den ihnen spezifisch zugrundeliegenden Datenquellen [23,4]. Viele dieser Quellen wurden neben den Nachrichtendiensten im Laufe des technologischen Fortschritts jedoch auch der Öffentlichkeit zugänglich [52,17,4,23]. Die daraus entstandenen zunehmenden Überschneidungen mit OSINT, die nur nach der Quellenzugänglichkeit definiert wird, haben zahlreiche Kontroversen ausgelöst. Zwei prägnante Grundstimmungen lassen sich dahingehend in der Literatur feststellen. Die erste betrachtet OSINT als inkohärentes Konzept, das über den und gegen die klar zu klassifizierenden „traditionellen" Intelligence-Disziplinen steht [4]. Die öffentlich verfügbaren Quellen seien demnach ebenfalls den angestammten Domizilen unterzuordnen [53,4]. Die zweite Sichtweise, zurückzuführen auf die NATO sowie die amerikanischen Geheimdienste und das Militär, erachtet OSINT als notwendiges Komplement der übrigen Disziplinen [30,23,22]. OSINT stellt damit kein Substitut dar, sondern ergänzt die anderen Disziplinen als Grundlage und ersten Ankerpunkt essenziell [52,31,22]. Sie liefert somit kosteneffizient [52,22] den notwendigen Kontext und schließt (erste) Wissenslücken, um die „aggressiveren" [18] eingestuften Sammeldisziplinen effektiver einzusetzen [31,22]. Bezogen wird sich damit

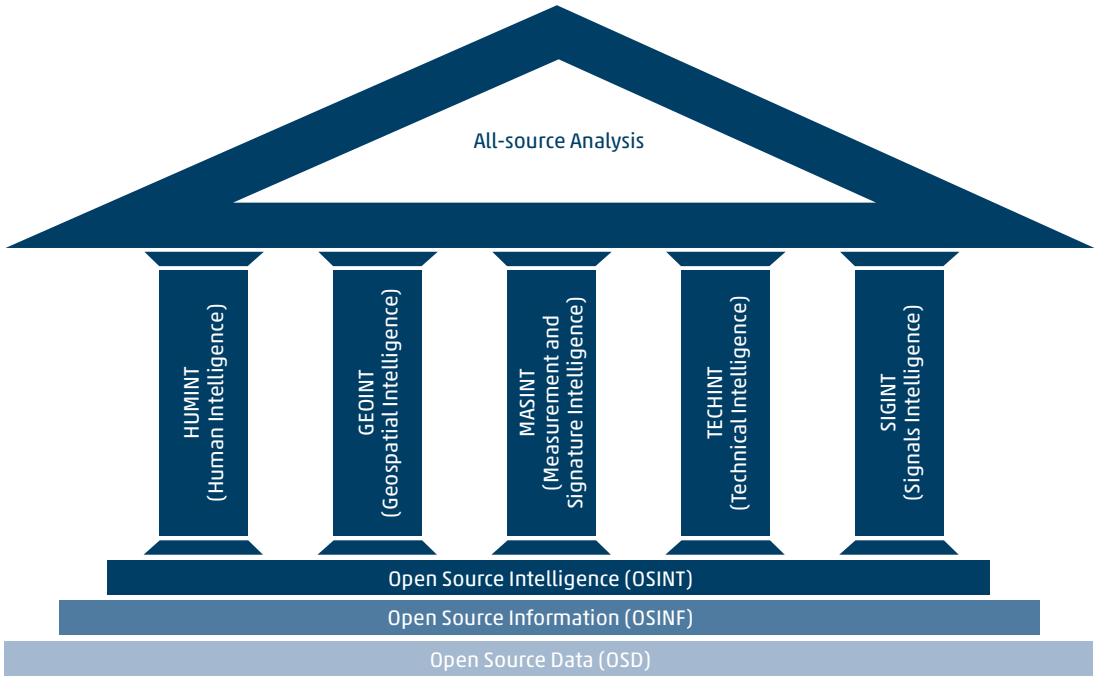

Abb.3: All-source Analysis-Tempel
Quelle: Eigene Darstellung, Design in Anlehnung an die NATO [22]

auf einen sog. „All-source Analysis"-Ansatz [38]. Demnach kann ein qualitativeres nachrichtendienstliches Produkt durch das Zusammenwirken und das gegenseitige Verifizieren [41,38] mehrerer Intelligence-Disziplinen erzeugt werden [34,22,38]. In diesem Kontext stellt die NATO [22] OSINT als das Fundament dar, auf dem die eingestuften Disziplinen ruhen, ähnlich den tragenden Säulen eines Tempels (siehe Abb.3).

7 Phasen von OSINT nach dem Intelligence Cycle

Der Generierungsprozess von Intelligence in Form zeitlich und inhaltlich relevanter Erkenntnisse zur Entscheidungsfindung [38] wird synonym auch als Intelligence Cycle bezeichnet [21,54]. Er stellt das zentrale Element einer jeden Intelligence-Disziplin, unabhängig von den zugrundeliegenden Quellen oder deren Zugänglichkeit, dar [46,19]. Die Darstellung des Prozesses als dynamischer, kontinuierlicher Zyklus [34] entspringt dem 1987 herausgegebenen „Factbook" der CIA [54]. Diese definiert den Prozess bis heute [55] als bestehend aus den fünf aufeinander aufbauenden Phasen: Planung und Direktion, Erhebung, Aufbereitung, Produktion und Analyse sowie Verbreitung [54]. Die unweigerliche Verbundenheit der einzelnen Phasen besteht darin, dass das Ergebnis der vorangehenden Phase der nachfolgenden als Input dient [38,56]. Zudem dient das Produkt eines Zyklus dem nächsten wiederum als Startpunkt zur Verfeinerung [19,36]. Auch innerhalb des Zyklus verlaufen die einzelnen Phasen dabei nicht linear, sondern werden aufgrund der Erfüllung früherer Anforderungen sowie neuer Erfordernisse laufend iteriert [38]. Die JCS ergänzten den Intelligence Cycle 2013 demgemäß um einen allen Phasen unterliegenden Evaluierungs- und Rückmeldungsvorgang [38] (siehe Abb. 4).

Heutzutage lassen sich zahlreiche weitere Abwandlungen in der Literatur antreffen [46,41]. Die Darstellung erstreckt sich dabei von der eindimensionalen linearen Form [vgl. bspw.: 50,57] bis hin zu komplexen Netzwerkansätzen [vgl. bspw.: 58,59]. Der Intelligence Cycle ist daher weniger als Leitfaden, sondern eher als informelles Koordinierungselement zu betrachten, das einer zum Teil sehr intuitiven [48] Auslegung folgt [13]. Es ist somit festzuhalten, dass es nicht den einen „richtigen" Intelligence Cycle gibt [46] und damit auch nicht den einen zertifizierten Weg zur Generierung von Intelligence [48]. Mit der Phase **der Planung und Direktion** wird der Grundstein für den Intelligence Cycle gelegt [34]. Sie vereint die Identifikation, Festlegung und Priorisierung der Anforderungen an den Zyklus. Zudem unterliegt ihr die Entwicklung der notwendigen Aktivitäten zur Errei-

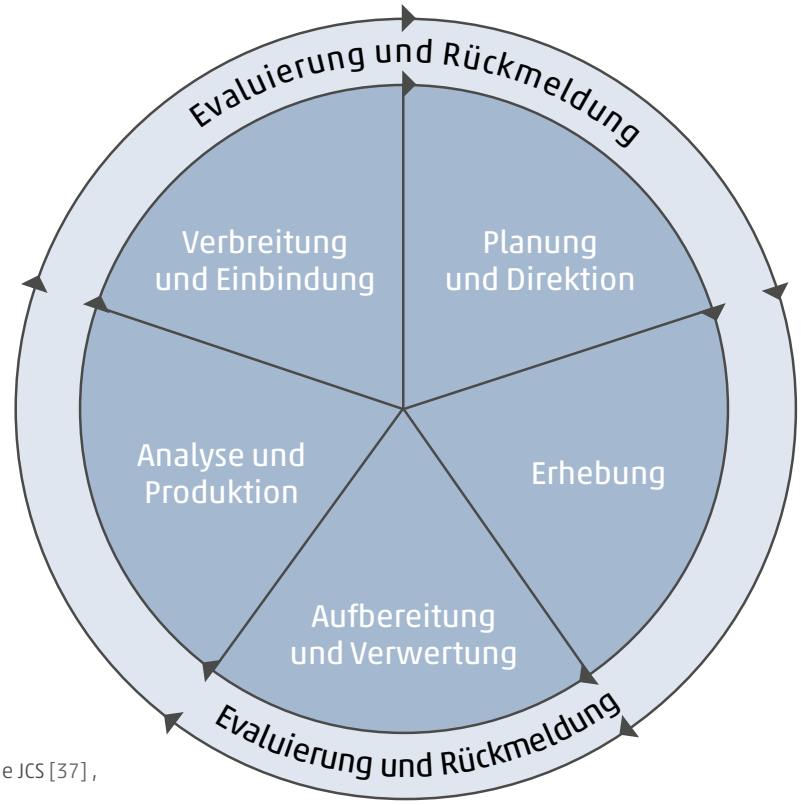

Abb.4: Intelligence Cycle
Quelle: In Anlehnung an die JCS [37] , eigene Übersetzung

chung dieser [31]. Der Phase kommt damit die Steuerung des gesamten Ablaufs zu [54]. Unter der Phase der **Erhebung** ist das Sammeln der Rohdaten zu verstehen [54]. In welchem Umfang die Datenerhebung jedoch erfolgen soll, ist nicht eindeutig zu beantworten und hängt nicht nur von den verfügbaren Ressourcen und Budgets ab, da nicht jedes Bit einen gleichwertigen Informationsgehalt aufweist [50]. Das Herzstück dieser Phase besteht somit in der iterativen Wiederholung von Recherchen [22], um die Suche mit jedem Durchlauf zu präzisieren [14]. Die erhobenen Rohdaten sind in der Regel noch von invalidierter, unstrukturierter Natur und enthalten oftmals Duplikate [46]. Die Phase der **Aufbereitung und Verwertung** befasst sich daher damit, diese Datenmengen für die weitere Prozessierung in werthaltige und handlungsrelevante Informationen zu verdichten [34,14,38] Unter der **Analyse und Produktion** wird die Synthese der gewonnenen Informationen zu einem nutzerorientierten, zeitgerechten und akkuraten „Intelligence-Produkt", in Form einer Erkenntnis [38], verstanden [31,34,13]. Der dahinterliegende Analysevorgang selbst kann sich je nach zugrundeliegender Art der Information bzw. des Datentyps sowie der Anforderungen wesentlich unterscheiden und Methodenmixe erfordern [51,45,2]. Die letzte Phase, **die Verbreitung und Einbindung**, besteht darin, das fertige Produkt in nutzbarer Form an den Kunden zu übergeben [54,2,31]. Der Ausgestaltung des Produkts sind dabei keine Grenzen gesetzt. Berücksichtigt werden sollte jedoch die Einhaltung der zeitlichen Vorgaben sowie die Reduktion der Übermittlung auf die relevanten Inhalte [31], bei gleichzeitiger Sicherstellung deren Vollständigkeit [50]. Die **Evaluierung und Rückmeldung** sind nicht als einzelne Phase innerhalb des Zyklus zu betrachten, sondern finden kontinuierlich über den gesamten Prozess statt. Ziel ist es, so eine fortschreitende Optimierung herbeizuführen [34,22,38]. Eine systematische Kommunikation innerhalb sowie über die einzelnen Schritte hinweg stellt dabei das wichtigste Instrument dar [50].

Einen vertiefenden Einblick in ganzheitliche Schulungsansätze und -methoden, um in dieser Disziplin erfolgreich zu agieren, bietet unser zweites Paper dieser Reihe. Erscheinungsdatum: 01.07.2024.

Ansprechpartner

Franz Kayser
Autor
Projektkoordinator Business Development
Franz.Kayser@esg.de

Stefan Vollmer
Divisionsleiter Abteilung Cyber- und Informationsraum
Stefan.Vollmer@esg.de

Timo Keim
Leiter Public Security Academy
Timo.Keim@esg.de

8 Quellen

[1] Dos Passos D. S.: Big Data, Data Science and Their Contributions to The Development of The Use of Open Source Intelligence. S&G, 11 (4) 2017, p. 392–396. doi:10.20985/1980-5160.2016.v11n4.1026.

[2] Williams H. J., Blum I.: Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. Santa Monica, Calif.: RAND Corporation, 2018.

[3] Smith-Boyle V.: How OSINT Has Shaped the War in Ukraine. Available at: https://www.americansecurityproject.org/osint-in-ukraine/#:%01:text=Open%2Dsource%20intelli-gence%2C%20or%20OSINT,synthesized%2C%20and%20analyzed%20into%20intelligence. Accessed July 24, 2023.

[4] Hatfield J. M.: There Is No Such Thing as Open Source Intelligence. International Journal of Intelligence and CounterIntelli-gence 2023, p. 1–22. doi:10.1080/08850607.2023.2172367.

[5] Bellingcat: Bellingcat auf Deutsch. Available at: https://de.bellingcat.com/. Accessed July 26, 2023.

[6] Wiegand R.: Investigative Recherche: Wie das Ressort bei der SZ entstand. Süddeutsche Zeitung 2022, 6 October 2022. Available at: https://www.sueddeutsche.de/kolumne/hans-leyendecker-investigative-recherche-panama-papers-pulitzer-preis-uiguren-1.5664676. Accessed July 24, 2023.

[7] Winiecki D. et al.: Validating Bad Entity Ranking in the Panama Papers via Open-source Intelligence. In: 2020 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM). IEEE, 2020, pp 752–759.

[8] Herrmann B. et al.: Mossack Fonseca: Datenleck offenbart letzte Geheimnisse. Süddeutsche Zeitung 2018, 20 June 2018. Available at: https://www.sueddeutsche.de/politik/mossack-fonseca-neues-datenleck-offenbart-die-letzten-geheimnisse-der-skandal-kanzlei-1.4025000. Accessed July 24, 2023.

[9] Obermayer B. et al.: Die Panama Papers - das bisher größte Datenleak. Available at: https://panamapapers.sueddeutsche.de/articles/56ff9a28a1bb8d3c3495ae13/. Ac-cessed July 24, 2023.
[10] Pastor-Galindo J. et al.: OSINT is the next Internet goldmine: Spain as an unexplored territory. Caceres, Spanien, 2019.
[11] Schaurer F., Störger J.: The Evolution of Open Source Intelligence. Zürich: ETH Zurich, 2010.
[12] Burke C.: Freeing knowledge, telling secrets: Open sourceintelligence and develop-ment. Research paper series: Centre for East-West Cultural & Economic Studies, (13) 2007.
[13] Hwang Y.-W. et al.: Current Status and Security Trend of OSINT. Wireless Communications and Mobile Computing, 2022 2022, p. 1–14. doi:10.1155/2022/1290129.
[14] Pastor-Galindo J. et al.: The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. IEEE Access, 8 2020, p. 10282–10304. doi:10.1109/ACCESS.2020.2965257.
[15] Yogish P. U., Krishna P. K.: Open Source Intelligence and its Applications in Next Generation Cyber Security - A Literature Review 2021. doi:10.5281/zenodo.5171580.
[16] Ish D. et al.: Evaluating the Effectiveness of Artificial Intelligence Systems in Intelligence Analysis. Santa Monica, Calif.: RAND Corporation, 2022.
[17] Ghioni R. et al.: Open source intelligence and AI: a systematic review of the GELSI liter-ature. AI & society 2023, p. 1–16. doi:10.1007/s00146-023-01628-x.
[18] Ünver H. A.: Digital Open Source Intelligence and International Security: A Primer. 2018.
[19] Dokman T., Ivanjko T.: Open Source Intelli-gence (OSINT): issues and trends. In: INFuture2019: Knowledge in the Digital Age. Faculty of Humanities and Social Sciences, University of Zagreb Depart-ment of Information and Communication Sciences, FF press, 2020.
[20] Benes L.: OSINT, New Technologies, Edu-cation: Expanding Opportunities and Threats. A New Paradigm. JSS, 6 (3Suppl) 2013, p. 22–37. doi:10.5038/1944-0472.6.3S.3.
[21] Herrera-Cubides J. F. et al.: Open-Source Intelligence Educational Resources: A Visual Perspective Analysis. Applied Sci-ences, 10 (21) 2020, p. 7617. doi:10.3390/app10217617.
[22] North Atlantic Treaty Organization: NATO Open Source Intelligence Handbook. 2001.
[23] North Atlantic Treaty Organization: NATO Open Source Intelligence Reader. 2002.
[24] Block L.: The long history of OSINT. Journal of Intelligence History 2023, p. 1–15. doi:10.1080/16161262.2023.2224091.
[25] British Broadcasting Corporation: BBC Monitoring – Essential Media Insight. Available at: https://monitoring.bbc.co.uk/. Accessed May 12, 2023.
[26] Roop J. E.: Foreign Broadcast Infomation Service: History Part 1: 1941 - 1947. 1969.
[27] Central Intelligence Agency: The Office of Strategic Services: America's First Intelligence Agency. Available at: https://www.cia.gov/legacy/museum/exhibit/the-office-of-strategic-services-n-americas-first-intelligence-agency/. Ac-cessed May 11, 2023.
[28] Glassman M., Kang M. J.: Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). Computers in Human Behavior, 28 (2) 2012, p. 673–682. doi:10.1016/j.chb.2011.11.014.
[29] Mercado S. C.: Reexamining the Distinction Between Open Information and Secrets. Studies in Intelligence, 49 (2) 2005.
[30] US Department of Defense: National Defense Authorization Act for Fiscal Year 2006: PUBLIC LAW 109–163—JAN. 6, 2006. 06.01.2006.
[31] Department of the Army: Open-Source Intelligence. Washington, DC, 2012.
[32] AlKilani H., Qusef A.: OSINT Techniques Integration with Risk Assessment ISO/IEC 27001. In: International Conference on Data Science, E-learning and Information Systems 2021 (Editors: J. A. Lara Torralbo et al.). New York, NY, USA: ACM, 2021, pp 82–86.
[33] Chen et al.: Business Intelligence and Analyt-ics: From Big Data to Big Impact. MIS Quarterly, 36 (4) 2012, p. 1165. doi:10.2307/41703503.
[34] Director of National Intelligence: U.S. National Intelligence: An Overview 2011. USA, 2011.
[35] Bundesnachrichtendienst: Was uns beson-ders macht: Nachrichtendienste dürfen, was anderen verboten ist: Spionieren. Available at: https://www.bnd.bund.de/DE/Die_Arbeit/Informationsgewinnung/informationsgewinnung_node.html. Accessed May 15, 2023.
[36] Gibson H.: Acquisition and Preparation of Data for OSINT Investigations. In: Open Source Intelligence Investigation (Editors: B. Akhgar et al.). Cham: Springer International Publishing, 2016, pp 69–93.
[37] Omand D. et al.: Introducing Social Media Intelligence (SOCMINT). Intelligence and National Security, 27 (6) 2012, p. 801–823. doi:10.1080/02684527.2012.716965.

[38] Joint Chiefs of Staff U.S. Army: Joint Intelligence. 2nd ed. USA, 2013.
[39] Bundesamtes für Verfassungsschutz: Glossar - Open Source Intelligence. Available at: https://www.verfassungsschutz.de/SharedDocs/glossaareintraege/DE/O/osint.html. Accessed May 15, 2023.
[40] Aftergood S.: Open Source Center (OSC) Becomes Open Source Enterprise (OSE). Available at: https://fas.org/publication/osc-ose/. Accessed May 16, 2023.
[41] Böhm I., Lolagar S.: Open source intelligence. International Cybersecurity Law Review, 2 (2) 2021, p. 317–337. doi:10.1365/s43439-021-00042-7.
[42] García Lozano M. et al.: Veracity assessment of online data. Decision Support Systems, 129 2020, p. 113132. doi:10.1016/j.dss.2019.113132.
[43] Wittmer S., Platzer F.: Zulässigkeit von Open Source-Ermittlungen zur Strafverfolgung im Darknet. Bonn: Gesellschaft für Informatik, Bonn, 2022.
[44] Kahaner L.: Competitive intelligence: How to gather, analyse, and use information to move your business to the top. 1st ed. New York, NY: Simon & Schuster, 1997.
[45] Theobald E.: Marketing Intelligence: Ein Lehrbuch für die Praxis. Stuttgart: Kohlhammer Verlag, 2018.
[46] Reuser A.: The RIS Open Source Intelligence Cycle. Journal of Mediterranean and Balkan Intelligence, 10 (2) 2017.
[47] Ackoff R. L.: From Data to Wisdom. Journal of applied Systems Analysis, 16 1989.
[48] Breakspear A.: A New Definition of Intelligence. Intelligence and National Security, 28 (5) 2013, p. 678–693. doi:10.1080/02684527.2012.699285.
[49] Kent S.: Strategic intelligence for American world policy. Princeton, NJ: Princeton University Press, 1966.
[50] Lowenthal M. M.: Intelligence: From secrets to policy. Thousand Oaks, Calif.: SAGE/CQ Press, 2020.
[51] Day T. et al.: Fusion of OSINT and Non-OSINT Data. In: Open Source Intelligence Investigation (Editors: B. Akhgar et al.). Cham: Springer International Publishing, 2016, pp 133–152.
[52] Mercado S. C.: A Venerable Source in a New Era: Sailing the Sea of OSINT in the In-formation Age. 2005.
[53] Lowenthal M. M.: OSINT: The State of the Art, the Artless State. Studies in Intelli-gence, 45 (3) 2001, p. 61–66.
[54] Central Intelligence Agency: Factbook on Intelligence. Washington, DC, 1987.
[55] Central Intelligence Agency: The Intelligence Cycle: Briefing. 2023.
[56] Pellissier R., Nenzhelele T. E.: Towards a universal competitive intelligence process model. S. Afr. j. inf. manag., 15 (2) 2013. doi:10.4102/sajim.v15i2.567.
[57] Dishman P. L., Calof J. L.: Competitive intelligence: a multiphasic precedent to market-ing strategy. European Journal of Market-ing, 42 (7/8) 2008, p. 766–785. doi:10.1108/03090560810877141.
[58] Oraee N. et al.: The competitive intelligence diamond model with the approach to standing on the shoulders of giants. Library & Information Science Research, 42 (2) 2020, p. 101004. doi:10.1016/j.lisr.2020.101004.
[59] Phythian M. (ed): Understanding the intelligence cycle. London: Routledge, 2013.