GLOBAL NETWORK & INTELLIGENCE

CII DEEP-DIVE

Hybride Bedrohungen Teil 3/3

Russische (Wegwerf-) Agenten und Spione

Anwerbung, Ziele und Vorgehensweisen

Dr. Christopher Nehring

CYBER|INTELLIGENCE
.Institute

Vorwort

Diese dreiteilige CII-Deep-Dive-Reihe bietet einen Überblick über aktuelle hybride Angriffsszenarien und -hintergründe sowie über Gegenmaßnahmen. Der erste Teil widmet sich den „Hybriden Bedrohungen“, der zweite Teil dem aktuellen Stand der „Drohnenabwehr“, während sich der dritte Teil den Methoden russischer Geheimdienste mit Fokus auf Agenten widmet.

Mit dieser Reihe möchte das CII zum besseren Verständnis der allgemeinen Ausgangslage aktueller hybrider Bedrohungen beitragen. Der Anspruch liegt nicht auf Vollständigkeit oder der Darstellung umfangreicher Quellennachweise, sondern der Orientierung und Förderung des Risikoverständnisses für Entscheider in Organisationen, um sich dieser Gefahrenlage und möglicher Handlungserfordernisse bewusst zu werden und in einen Dialog zu kommen.

Ich wünsche eine aufschlussreiche Lektüre.

Dr. Christopher Nehring
CII-Intelligence Director

Über den Autor

Dr. Christopher Nehring, Intelligence Director des cyberintelligence.institute in Frankfurt am Main. Er ist Forscher, Analyst und Experte für verschiedene Medien in Deutschland und Europa. Sein Themengebiet umfasst die Arbeit von Geheimdiensten, Desinformation, Hybride Kriegsführung und KI-Cyberrisken (insbesondere Deepfakes und Manipulationen). Er war Gastdozent und Experte für Desinformation des Medienprogramms der Konrad-Adenauer-Stiftung, wissenschaftlicher Leiter des Spionagemuseums Berlin sowie Senior Analyst des Institute for Global Analysis. Dr. Nehring ist regelmäßiger Gastautor und Experte für zahlreiche Medien (z.B. ARD, Tagesspiegel, Spiegel, NZZ, Welt etc.), als Speaker, Trainer, Kursleiter und Berater ist er für verschiedene Unternehmen, IHKs, Stiftungen und Medienorganisationen tätig.

Kontakt: christopher.nehring@cyberintelligence.institute

Hybride Bedrohungen.
Teil 3: Russische (Wegwerf-)Agenten und Spione

Das Wichtigste in Kürze:

- Trotz vielfältiger Cyberangriffe bleiben menschliche Agenten (HUMINT) ein zentrales Mittel russischer Geheimdienstarbeit und werden für Spionage und Sabotage eingesetzt.
- Russische Geheimdienste unterscheiden verschiedene Arten von Agenten; gerade „Wegwerf-Agenten“, die für einmalige Sabotageanschläge rekrutiert werden, sind eine zunehmende Bedrohung.
- Geld, Zwang und Druck, aber auch ideelle und persönliche Bindungen sind häufige Motive für russische Agenten. Aktuell rekrutieren russische Geheimdienste v.a. über Social Media und Messenger-Dienste (Telegram).
- Operative Geheimdienst-Psychologie spielt bei russischen Operationen eine wichtige Rolle: Viele Aktionen zielen auf psychologische Effekte (Einschüchterung, Angst, Verunsicherung und Lähmung), etwa durch offensichtliches Beschatten und Observation, offene Ansprachen oder Informationslecks über private Details.
- Durch Sicherheitskonzepte, Vorbereitung und Abschreckung können Organisationen gezielt psychologische und strukturelle Resilienz aufbauen.

Konkreter Mehrwert für KRITIS-Betreiber, CSOs, CISOs, Sicherheitsmitarbeiter und Dienstleister:

Dieses Deep-Dive-Paper …

- … bietet eine praxisnahe Ergänzung und übersetzt abstrakte Sicherheits- und Resilienzanforderungen in handlungsleitendes, maßnahmenzentriertes Wissen.
- … identifiziert typische Vorgehensweisen russischer Agenten und dient dadurch der Früherkennung und Musterschärfung in Risikoanalysen.
- … dient dem Taktikverständnis hinsichtlich feindlicher Akteure.
- … bietet die Grundlage für Frühwarnsysteme, Sicherheitsvorkehrungen, Schulungen, Sensibilisierungen und Resilienzbildungsmaßnahmen (§ 13 KRITIS-DachG).

Inhalt

Die Rolle von Agenten und Spionen für russische Geheimdienste 5

1. Warum sollten Grundlagen russischer Agentenarbeit bekannt sein? 5
2. Agenten: Arten und Ziele 5
   a) Geheimdienstoffiziere 5
   b) Diplomaten 6
   c) „Illegale“ 6

Fokus: Wegwerf-Agenten 7

1. Rekrutierung: Methoden, Ziele und Motive 8
   a) Ansprache über Social Media 8
   b) Botschaftsmitarbeiter 8
   c) Motivation: Geld & Ideologie 8
2. Vorgehensweise: Strategien & Umsetzung 9
   a) Arbeitsteilung 9
   b) Präsenz, Geduld und langfristige Planung 9
   c) Logistische Basis, Netzwerk, Ausrüstung 9
   d) Operative Psychologie 9
   e) Indirektes Vorgehen 10
   f) Kommunikation 10
   g) Versorgung 10
   h) Psychologische Einwirkung 10
3. Stärken und Schwächen 11
   Übersicht: Stärken und Schwächen der Agentenarbeit 11

Empfehlungen 12

Prävention und Kooperation 12

Weitere Maßnahmen 12

Impressum & Kontakt 13

Die Rolle von Agenten und Spionen für russische Geheimdienste

Spionage und Sabotage sind wesentliche Eckpfeiler russischer hybrider Angriffe in Europa und Deutschland.[1] Zwar rückt die digitale Dimension dieser Angriffe – von Cyberattacken bis zu digitaler Desinformation – immer mehr in den Vordergrund; nichtsdestoweniger sind menschliche Agenten und Spione nach wie vor ein wichtiges und von russischen Geheimdiensten geschätztes Werkzeug. Gerade unter der alten (und oftmals besonders „harten") Garde von Offizieren in FSB, GRU und SWR gelten menschliche Quellen und Agenten wegen ihrer Flexibilität, ihrer Fähigkeiten, schwer zugängliche Informationen zu liefern und direkt wirken zu können, trotz der Möglichkeiten technischer Spionage und Cyber-Aktionen als unverzichtbar.[2] Dies hat sich auch in Deutschland nach dem Beginn des Ukraine-Krieges 2022 gezeigt – sei es durch angeworbene Saboteure, mutmaßliche Drohnen-Steuerer, politische Einflussagenten oder klassische Spione.

1. Warum sollten Grundlagen russischer Agentenarbeit bekannt sein?

Russische Geheimdienste sind aktuell die wichtigsten Akteure hybrider Angriffe in Deutschland. Spionage, Sabotage und Agentenarbeit sind dabei gefährliche Faktoren und kein Nebenschauplatz. Grundlegende Erkenntnisse dienen daher als Basis für Sicherheitsbriefings, Awareness-Kampagnen und Sensibilisierungen sowie für die Überarbeitung von Sicherheitsrichtlinien. Sie ermöglichen einen Austausch und eine Kooperation mit Behörden und anderen Sicherheitsmanagern und schaffen die Grundlage für ganzheitliche Schutzkonzepte.

2. Agenten: Arten und Ziele

Geheimdienste haben für unterschiedliche Arten der offiziellen und inoffiziellen Mitarbeiter viele Kategorien. Der DDR-Geheimdienst („Stasi") unterschied zeitweise rund 20 verschiedene Arten.[3] Fachleute haben im Wesentlichen drei Gruppen menschlicher Spione und Agenten der russischen Geheimdienste identifiziert: Führungsoffiziere, Unterstützungspersonal und (angeworbene) Agenten.[4] Russische Geheimdienste unterscheiden Mitarbeiter zudem aufgrund ihrer Tarnung und Herkunft:

Bild: Aufnahme eines russischen Agenten in Den Haag beim Leeren eines toten Briefkastens, Quelle: niederländischer Geheimdienst AIVD.

a) Geheimdienstoffiziere

Es gibt die **Geheimdienstoffiziere**, also offiziell angestellte Beamte, die nicht nur in den russischen Geheimdienstfilialen sitzen, sondern auch an Botschaften im Ausland. Dort sind sie entweder als Verbindungsbeamte akkreditiert oder offiziell als normale Diplomaten im Gastland gemeldet, während sie eigentlich Geheimdienstaufgaben ausführen. Beide zusammen bilden die sog. „Residentur", die Geheimdienstzelle in einer russi-

1 Siehe das erste Paper der CII-Deep-Dive-Reihe „Hybride Bedrohungen: Überblick über Angriffsmethoden und Vorgehen" (https://cms.cyberintelligence.institute/api/media/file/ausgabe1_deepdiveangriffsartenimberblickpdf-1.ausgabe1_deepdiveangriffsartenimberblickpdf) sowie auch einleitend: https://www.bmvg.de/de/themen/sicherheitspolitik/hybride-bedrohungen; und: https://www.verfassungsschutz.de/SharedDocs/hintergruende/DE/spionage-und-proliferationsabwehr/gefaehrdung-russische-spionage-sabotage-desinformation.html.

2 Siehe dazu ausführlich: Kevin Riehle: Russian Intelligence: A Case-based Study of Russian Services and Missions Past and Present, London 2022, S. 217–235.

3 Siehe dazu ausführlich: Helmut Müller-Enbergs: Inoffizielle Mitarbeiter, Teil 3: Statistiken, hg.: BStU, Berlin 2008, S. 124–136.

4 Siehe: Riehle: Russian Intelligence, S. 217–235.

schen Botschaft. Auch sie hat eine festgelegte Struktur und ihre Arbeitsweise wird intern als Aufklärung aus legalen Positionen bzw. legaler Abdeckung bezeichnet, da diese Mitarbeiter offiziell akkreditiert sind.[5]

b) Diplomaten

Neben den offiziellen Geheimdienstlern werben die russischen Geheimdienste auch andere russische Beamte an, insbesondere **Diplomaten** und Mitarbeiter des Verteidigungsministeriums, aber auch z.B. offizielle Journalisten der Staatsmedien oder Mitarbeiter der russischen Kultureinrichtungen im Ausland. Dies sind dann nichtoffizielle Geheimdienstmitarbeiter, die eine spezielle Kategorie im Pool der Agenten, Spione und Quellen bilden. Dieser Agenten-Pool kennt dann weitere Unterkategorien, die oft den Zweck eines Agenten beschreiben (z.B. der sog. „Einflussagent", der politischen oder gesellschaftlichen Einfluss auf Entscheidungen nehmen soll).

c) „Illegale"

Eine andere und für russische Geheimdienste spezifische Art von Agenten sind sogenannte **Illegale**. Dies sind Personen aus Russland oder dem Ausland, die unter aufwendig konstruierten falschen Identitäten über einen längeren Zeitraum im Ausland leben.[6] Sie erhalten oft ein jahrelanges Sprach-, Kultur- und Spionagetraining, bevor sie über Drittländer in ihr eigentliches Zielland geschickt werden. Anders als oft angenommen, erfüllten die meisten erkannten Illegalen-Agenten hauptsächlich logistische und Verbindungsaufgaben, keine Sabotageaktionen. Diese Agenten sind hochprofessionell, gut getarnt und besonders schwer zu finden. Nach dem Ende des Kalten Krieges wurden Illegale-Agenten für ein Relikt gehalten, seitdem kam es jedoch immer wieder zu spektakulären Enttarnungen, die belegen, dass dieses Spionage-Programm nach wie vor sehr aktiv ist. In Deutschland wurde z.B. 2011 ein Ehepaar verhaftet, das seit 1988 unerkannt als Illegale-Agenten mit falscher Identität in Deutschland gelebt hatte und für den russischen Geheimdienst aktiv war.[7] In den letzten Jahren wurden weitere Illegale-Agenten z.B. in Slowenien, Italien, Schweden und Italien verhaftet. Auffällig oft hatten Illegale-Agenten in Europa Geburtsurkunden aus südamerikanischen Staaten.

> **Sie erhalten oft ein jahrelanges Sprach-, Kultur- und Spionagetraining, bevor sie über Drittländer in ihr eigentliches Zielland geschickt werden.**

5 Nach eEbd., S. 224 ff., ist eine Residentur hierarchisch und arbeitsteilig aufgebaut: Im Mittelpunkt steht der Reszident, der die gesamte Einheit leitet und die Verbindung zum Hauptquartier in Moskau hält. Ihm unterstellt ist der Stellvertretende Reszident, der die täglichen operativen Abläufe organisiert und als „Back-up" dient, wenn der Reszident politisch gut vernetzt, aber operativ schwächer ist. Die eigentlichen operativen Aufgaben führen die Führungsoffiziere aus, die innerhalb der Residentur in sogenannte thematische „Linien" gegliedert sind und zuin diesem Themen Informationen beschaffen, Berichte schreiben und Agenten anwerben. Hier gibt es folgende Bereiche: **Line PR**: Politische Aufklärung; **Line X**: Wissenschaftlich-technische Aufklärung; **Line N**: Unterstützung von Illegalen (z.B. Aufbau von Legenden, Geldtransfers); **Line KR**: Gegenspionage und Spionageabwehr; **Line SK**: Überwachung russischer Diplomaten; **Line EM**: Aufklärung von Emigrantenkreisen (vor allem während des Kalten Krieges). Zusätzlich gibt es Unterstützungspersonal, darunter: **Techniker** zur Verschlüsselung/Entschlüsselung von Nachrichten; **Sekretäre**, die Aktenführung betreiben und teils ebenfalls eine wichtige Rolle in der Aufklärung spielen können.

6 Siehe eEbd., S. 226–-230; ausführlich: Shaun Walker: The Illegals: Russia''s Most Audacious Spies and the Plot to Infiltrate the West, London, 2025; weiter: Christopher Andrew , Christopher/ Wassili Mitrochin, Wassili: Schwarzbuch des KGB, Bd. 1: Moskaus Kampf gegen den Westen, Berlin, 1999, S. 273–-282.

7 Siehe ausführlich: https://www.ardaudiothek.de/sendung/die-anschlags-russlands-spione-unter-uns-wdr-und-ndr/13420611/.

Fokus: Wegwerf-Agenten

Gerade in den vergangenen Jahren seit Beginn der russischen Invasion der Ukraine zeigen sich grundlegende Veränderungen bei der Arbeit russischer Geheimdienste mit Agenten: Statt auf langfristig aufgebaute, gut geschulte und an den Geheimdienst gebundene Agenten setzen vor allem FSB und GRU auf sog. Wegwerf-Agenten. Ähnlich wie Wegwerf-Handys sind dies Agenten, die kurzfristig, meist online und ohne direkten Kontakt rekrutiert wurden und für einzelne Aktionen benutzt werden.

Im Mai in der Ukraine verhafteter mutmaßlicher russischer Wegwerf-Agent, Quelle: ukrainischer Geheimdienst SBU.

Sie arbeiten ausschließlich für Geld, kennen ihre Hintermänner zumeist nicht und kommunizieren mit ihren Agentenführern über Messenger-Apps (v.a. Telegram).

Viele solcher Agenten wurden in Deutschland, aber auch in der Ukraine und anderen europäischen Ländern während oder nach ihren Aufträgen verhaftet. Solche Agenten werden nicht nur für kleinere Spionage- oder Beschattungsaufträge eingesetzt, sondern auch für Sprengstoffanschläge und andere Sabotageaktionen.

Sprengvorrichtung des mutmaßlichen Agenten, Quelle: ukrainischer Geheimdienst SBU.

Seitens der Geheimdienste sind diese Agentenbeziehungen nicht auf Dauer angelegt, sondern nur so lange, bis die Agenten enttarnt werden. Da sie jedoch fast ausschließlich digital kommunizieren und ihre Agentenführer nie persönlich getroffen haben, ist das Risiko für den Geheimdienst relativ gering.[8] Zudem ist diese Art der Agenten, obgleich sie wenig bis keine spezielle Agenten-Ausbildung haben, nicht weniger gefährlich (oft sogar im Gegenteil). Häufig werden hierzu speziell Personen mit krimineller Vergangenheit bzw. Neigung angesprochen, die brachial und skrupellos vorgehen. Weiterhin sind solche Agenten aufgrund des geringen direkten Kontakts mit Geheimdiensten nur sehr schwer zu entdecken. Russische Geheimdienste nutzen die Aktionen solcher „Wegwerf-Agenten“ geschickt aus, um psychologische Botschaften der Angst und Verwundbarkeit zu senden.

8 Siehe z.B.: https://www.tagesschau.de/investigativ/ndr-wdr/russland-sabotage-106.html; sowie: https://www.verfassungsschutz.de/SharedDocs/hintergruen-de/DE/spionage-und-proliferationsabwehr/gefaehrdung-russische-spionage-sabotage-desinformation.html.

Der Wechsel zu „Wegwerf-Agenten“ kam vor allem dadurch zustande, dass massenhaft offiziell an den Botschaften in Europa und den USA akkreditierte Geheimdienstmitarbeiter zu Beginn des Krieges ausgewiesen wurden und zudem Reisebewegungen von und nach Russland stark eingeschränkt wurden. Sogenannte „fliegende Illegale-Agenten“, also inoffizielle Agenten aus Russland mit aufwendig konstruierten Tarnidentitäten, die sporadisch zu Einsätzen im Ausland fliegen, ergänzen diese „Wegwerf-Agenten“.[9]

1. Rekrutierung: Methoden, Ziele und Motive

a) Ansprache über Social Media

Wie rekrutieren russische Geheimdienste Agenten, Quellen und Saboteure? Die Masse der „Wegwerf-Agenten“ wird – so zeigen auch zahlreiche Beispiele aus der Ukraine – zumeist auf Social Media gefunden, wo nach Personen mit pro-russischen Meinungen in Zielgebieten gesucht wird. Anschließend werden sie für einzelne Aktionen bezahlt. Geld ist hier also der Hauptanreiz, wobei zuvor der Personenkreis eingeengt wurde. Typisch für solche flachen und einfachen Beziehungen ist auch, dass die Kommunikation ausschließlich online über kommerzielle Apps erfolgt.

> **Die Masse der „Wegwerf-Agenten“ wird – so zeigen auch zahlreiche Beispiele aus der Ukraine – zumeist auf Social Media gefunden, wo nach Personen mit pro-russischen Meinungen in Zielgebieten gesucht wird.**

b) Botschaftsmitarbeiter

Außerhalb Europas, wo russische Dienste nach wie vor nach klassischer Art vorgehen können, sind vor allem die Geheimdienstmitarbeiter an den Botschaften vor Ort zuständig, um mögliche Agenten zu finden. Als Anhaltspunkt dienen oft öffentliche russlandfreundliche Äußerungen. Selten treten Geheimdienstmitarbeiter beim ersten Kontakt offen als solche in Erscheinung – entwickelt sich tatsächlich ein weiterer Kontakt, übernimmt ein anderer, speziell angereister Geheimdienstmitarbeiter die weitere Kontaktpflege.

Das Finden und Tippen, die Kontaktanbahnung und Kontaktpflege sowie die anschließende Anwerbung und Agentenführung werden also klassischerweise von verschiedenen Mitarbeitern durchgeführt. Dies dient dazu, die Zielperson nicht zu erschrecken und die operative Tarnung aufrechtzuerhalten.

c) Motivation: Geld & Ideologie

Es gibt eine kleine Reihe klassischer Motive, auf die russische Geheimdienste setzen:

- Das häufigste Motiv sind finanzielle Anreize, also Bezahlung für Agenten. Diese wird zuletzt auch gerne in Kryptowährungen angeboten und mit anderen positiven wie negativen Anreizen kombiniert.
- Häufig wird nach ideologischen Überschneidungen gesucht und versucht, eine Zielperson sowohl persönlich an ihre Verbindungsperson als auch ideell zu binden.
- Mit Zwang, also Erpressung (etwa durch kompromittierende Fotoaufnahmen nach sog. „Venusfallen“, dem „Kompromat“), arbeiten russische Geheimdienste zwar auch, aber selten ausschließlich. Zwang eignet sich meist nur für kurzfristige Aktionen, jedoch nicht, um einen Agenten auf Dauer zu binden. Das gezielte Inszenieren von Notsituationen oder das Überrumpeln einer Zielperson kann ebenfalls herbeigeführt werden. Dies können z.B. konstruierte Verhaftungen aus nichtigen Gründen, die Verwicklung in persönliche Notsituationen (Angriffe, Unfälle, Diebstahl o.Ä.) oder ein einfaches Überrumpeln der Zielperson durch eine offene Ansprache an einem unerwarteten Ort sein.
- Aufwendig und dementsprechend selten werben russische Geheimdienste „unter falscher Flagge“ an, spielen Zielpersonen dann also vor, sie würden für einen anderen Geheimdienst oder eine andere Organisation arbeiten.

Grundsätzlich arbeiten vor allem russische Geheimdienste mit einer Kombination verschiedener Motive. Vor allem die Bindung von Quellen und Agenten an ihren Führungsoffizier, der persönliche Umgang und die ständige ideologische und psychologische Bestätigung und Unterstützung sind dabei mindestens genauso

9 Siehe: Walker: The Illegals.

wichtig wie Geld.[10] Einladungen nach Russland und zu anderen Reisen, Gastfreundschaft, Geschenke und persönliche Aufmerksamkeiten, ein herzlicher und charmanter Umgang, der speziell auf ein eigens erarbeitetes Psycho-Profil der Agenten passt, sind Beispiele hierfür. Dies gilt auch in Geschäftsverbindungen und -beziehungen, wenn also z.B. Firmen im Ausland für Geschäfte (etwa Import oder Transport zur Umgehung von Sanktionen) genutzt werden sollen. Hier sind neben gutem persönlichem Umgang auch große Investitionen und wirtschaftlicher Nutzen wichtige Motive.

2. Vorgehensweise: Strategien & Umsetzung

Es gibt nicht die eine, große Strategie russischer Geheimdienste für die Arbeit mit Agenten in Deutschland und Europa. Stattdessen gibt es mehrere Ansätze, die nebeneinanderstehen und flexibel an die operative Lage angepasst werden:

a) Arbeitsteilung

Grundsätzlich gibt es eine Tendenz, Agenten entweder zur Informationsgewinnung oder zur Durchführung von Sabotage und Einfluss-Aktionen, aber nicht für beides gleichzeitig einzusetzen. Dies liegt vor allem daran, dass Agenten mit Zugang zu besonders wichtigen Informationen oft sehr lange aufgebaut werden müssen, sich durch risikoreiche Aktionen wie Anschläge oder öffentliche Einflussnahme aber verdächtig machen oder enttarnen würden.

b) Präsenz, Geduld und langfristige Planung

In vielen Operationen, v.a. zur Informationsgewinnung (also klassische Spionage), zeigen russische Geheimdienste einen sehr langen Atem, Ausdauer und Beharrlichkeit. „Illegale-Agenten“ z.B., ähnlich wie viele Cyber-Operationen, sind auf teils sehr lange Zeiträume angelegt, bei denen anfangs nicht immer klar ist, ob und wann überhaupt ein Ergebnis folgt. Warten, Präsenz zeigen und sich für spionagewillige Personen (sog. „Selbststeller“) als glaubwürdige Alternative, Ausweg und Fluchtmöglichkeit anbieten, gehört ebenfalls zu dieser Strategie. Russische Botschaften und andere offizielle (halb-)staatliche Einrichtungen dienen weltweit als Anlaufstellen für Agenten (und solche, die es sein wollen). Auf diese Art gewann der KGB z.B. seine wertvollsten Agenten in gegnerischen Geheimdiensten („Maulwürfe“) während des Kalten Krieges.[11] Wie bereits bei den „Wegwerf-Agenten“ gezeigt, ist dieser strategische Ansatz das Gegenteil von Brechstangen-Methoden, bei denen kurzfristig besonders brachiale Erfolge erzielt werden sollen, die dafür aber wenig strategisch und oft sehr risikoreich sind.

Viele (wahrscheinlich sogar die meisten) Agenten erfüllen weder direkte Spionage- noch Sabotageaufgaben; stattdessen unterhalten russische Geheimdienste ein sehr breites Netz an Agenten, die vor allem logistische Aufgaben haben.

c) Logistische Basis, Netzwerk, Ausrüstung

Viele (wahrscheinlich sogar die meisten) Agenten erfüllen weder direkte Spionage- noch Sabotageaufgaben; stattdessen unterhalten russische Geheimdienste ein sehr breites Netz an Agenten, die vor allem logistische Aufgaben haben (Kuriere, Briefkästen, Deckadressen, Hilfsaufgaben o.Ä.). Damit können und werden dann hochrangige Informationsquellen oder auch verdeckte Aktionen abgesichert und ermöglicht. Um dieses breite Netz und seine Infrastruktur zu erhalten, gehen russische Dienste akribisch vor.

d) Operative Psychologie

Psychologie spielt in der Agentenarbeit russischer Geheimdienste eine große Rolle. Umfängliche Psychogramme werden von interessanten Zielpersonen erstellt, jedes Wort, jeder Gesprächskontakt wird akribisch dokumentiert und charakterisiert, unverfängliches privates Geplauder wird zu Charakterisierungen verdichtet, um nach Überschneidungen, Druckmitteln, Anreizen, Motivation etc. zu suchen und entsprechend für die eigenen Ziele zu instrumentalisieren.[12]

10 Siehe zur Motivation von Agenten grundlegend: Bundesbürger im Dienst der DDR-Spionage. Eine analytische Studie, Göttingen 2007, S. 250–260; Klaus Wagner: Spionageprozesse. Spionagemethoden des MfS (HV A) und östlicher (u.a. KGB) sowie nahöstlicher Nachrichtendienste in den Jahren 1977–1990, Brühl bei Köln 2000; Rüdiger Henkel: Was treibt den Spion?, S. 448–478; Stand Taylor / Daniel Snow: Cold War Spies: Why They Spied and How They Got Caught, in: Intelligence and National Security 12 (1997) 2, S. 101–125; Ingrid Kerz-Rühling / Tomas Plänkers: Verräter oder Verführte. Eine psychoanalytische Untersuchung Inoffizieller Mitarbeiter der Stasi, Berlin 2004.

11 Zu solchen „Selbststellern“ („Walk-ins“) siehe z.B.: Ivan Serov: Work with Walk-ins, in: Studies in Intelligence, 05.07.2007 (https://web.archive.org/web/20080312083817/https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol8no1/html/v08i1a02p_0001.htm).

12 Siehe z.B.: Ursula M. Wilder: The Psychology of Espionage, in: Studies in Intelligence Vol. 61, No. 2 (Extracts, June 2017) (https://www.cia.gov/resources/csi/

e) Indirektes Vorgehen

Egal ob indirekte Reisen (also nicht von Moskau nach Berlin, sondern, wie z.B. der Tiergartenmörder V. Krasikov, von Moskau über Paris nach Warschau und von dort weiter nach Deutschland[13]), indirekte Ansprachen (ein Mitarbeiter sucht nach interessanten Zielpersonen, ein anderer spricht sie an und wieder ein anderer übernimmt die Führung) oder indirekte Agentenführung (z.B. über Geheimdienstmitarbeiter, die eigentlich im Nachbarland stationiert sind) – grundsätzlich bevorzugen es russische Geheimdienste, indirekt zu arbeiten. Dies dient der operativen Tarnung und Verwirrung. Ein indirekter Weg wird (zumindest in Friedenszeiten) oft auch beschritten, wenn es darum geht, ein Zielobjekt (z.B. ein bestimmtes Unternehmen oder Ministerium) zu infiltrieren. Ein Vorgehen dabei ist z.B., über Servicekräfte, Dienstleister oder Zulieferer erste Kontakte anzubahnen und Informationen aus dem Inneren zu beschaffen, um dann geeignete Kandidaten mit Zugang zu wichtigen Informationen zu finden. Eine ähnliche Vorgehensweise wird oft auch bei Cyber-Spionage-Operationen kopiert.[14]

f) Kommunikation

Für verschiedene Klassen und Arten von Agenten gibt es verschiedene Kanäle und Tools, über die sie mit Agentenführern und den Geheimdienstzentralen kommunizieren. Hochrangige und wichtige Agenten haben spezielle Tools (z.B. KI-Chatbots, speziell verschlüsselter Agentenfunk über Kurzwelle, Kommentarfunktionen in Online-Plattformen und Videospielen oder eigene Websites); Wegwerf-Agenten hingegen werden über kommerzielle Messenger-Apps (v.a. Telegram) kontaktiert.

g) Versorgung

Agenten und Quellen sollen ihr Risiko und ihre Arbeit schmackhaft gemacht werden, deshalb kümmert sich der russische Geheimdienst um seine Agenten. Um diese Botschaft zu kommunizieren und dieses Image aufrechtzuerhalten, betreiben die Dienste einiges an Aufwand: Zum einen initiieren sie Agentenaustausche groß und öffentlich, zum anderen versorgen sie Hinterbliebene, Verwandte und natürlich auch aktive Agenten mit Geld, Reisen, Geschenken, Auszeichnungen etc. Der groß inszenierte Austausch des russischen Tiergarten-Mörders im Jahr 2024 ist ein Beispiel hierfür: Er soll Nachahmern signalisieren, dass sie auch aus schwierigsten Situationen befreit werden und sich ihre Arbeit für den russischen Geheimdienst auszahlt.

Dieses Image, das oft mehr Schein als Sein ist, gehört fest zur Organisationskultur und Tradition russischer Geheimdienste.

h) Psychologische Einwirkung

Russische Geheimdienste sind Meister darin, ihren Operationen eine Komponente der psychologischen Kriegsführung zu geben. Egal, ob Operationen, Cyberattacken oder Anschläge erfolgreich waren oder nicht: Russische Geheimdienste und auch die russische Politik stellen sie immer als Zeichen von Stärke und Tatkraft dar. Das Ziel dahinter ist, Angst zu verbreiten, einzuschüchtern und Personen wie Organisationen zu lähmen.[15] Dazu werden z.B. Mordoperation gezielt ritualisiert, strategisch kommuniziert und mit versteckten Botschaften versehen. So senden auch „Wegwerf-Agenten“ eine psychologische Botschaft der Stärke, die z.B. in Deutschland Kriegs- oder Angriffsängste schüren soll. In anderen Fällen werden Entscheidungsträger und Führungspersonal, aber auch Kritiker in privaten Situationen offen, mit Namen und privaten Details von Geheimdienstmitarbeitern angesprochen, um ihnen zu zeigen, dass sie im Visier der Dienste stehen. Oder es wird auf offensichtliche Beschattung, Observation und Fotografieren zurückgegriffen, was die Opfer verunsichern soll.

static/psychology-of-espionage.pdf); auch: Nachrichtendienstpsychologie. Schriftenreihe der FH des Bundes, Fachbereich öffentliche Sicherheit (https://doi.org/10.23668/psycharchives.10357).

13 Siehe z.B.: https://www.spiegel.de/panorama/justiz/berlin-moabit-was-ueber-das-opfer-und-den-mutmasslichen-taeter-bekannt-ist-a-1283756.html.

14 Siehe:Kevin Riehle: Russian Intelligence, S. 235–-260; Andrew Bowen: Russian Cyber Units, in: Congressional Research Service,, 2021 (https://www.congress.gov/crs-product/IF11718).

15 Siehe z.B.: Adrian Hänni / Christopher Nehring: Lethal Signaling: Exploring the Communicative Dimension of State-sponsored Assassinations, in: Killing in the Name of the State, hg.: Kiril Avramov / Luca Trenta (erscheint 2025); Christopher Nehring: Geheimdienstmorde: Wenn Staaten töten – Hintergründe, Motive, Methoden, München 2022, S. 195–201.

3. Stärken und Schwächen

Forschung und Fallstudien ergeben ein recht klares Bild über die Stärken und Schwächen der Agentenarbeit russischer Geheimdienste.

Stärken und Schwächen der Agentenarbeit

Stärken	Schwächen
Politische Unterstützung & Ressourcen	Fixierung auf Hard power, Quantität & Aggressivität
Aggressivität, Skrupellosigkeit & Einfallsreichtum	Hierarchische (und toxische) Strukturen & Arbeitsweisen
Logistik, Infrastruktur & breites Agentennetz	Mängel in der Geheimhaltung & der Informationssicherheit im digitalen Zeitalter
Tarnung & bewährte Legenden von Agenten	Anfällig für digitale OSINT-Recherchen (Informationen aus öffentlich zugänglichen Quellen)
Operative Psychologie & psychologische Einflussnahme	Verschwörungsglaube & Misstrauen
Charme, routinierte Menschen- bzw. Agentenführung	Fehlende interkulturelle Fähigkeiten/ & Geschlechtersensibilität
Vorsorge, Versorgung & Nachsorge für Agenten	Korruption &und Politisierung
Umfängliche Informationsgewinnung	Indoktrinierte Informationsauswertung, Analyse & Umsetzung

Empfehlungen

Prävention und Kooperation

Aufgrund der allgemeinen Risikolage gilt für „interessante Zieleinrichtungen“ heute, dass das Risiko von Agententätigkeiten kaum mehr unter Einzelfälle, sondern als allgemeines Risiko im organisationellen Alltag zu betrachten ist. Dabei gilt auch hier: Einrichtungen mit starkem Bezug zu politischen und wirtschaftlichen sowie auch gesellschaftlichen Anliegen stehen im besonderen Fokus und sollten zusätzliche Strategien und Maßnahmen ergreifen.

Die folgenden Empfehlungen zur Abwehr von Risiken durch Agenten korrespondieren mit dem geplanten **KRITIS-Dachgesetz**[16] *und seinen Pflichten für KRITIS-Einrichtungen. Konkret:*

- **Durchführung einer Gefahrenanalyse:** Dieses Paper zeigt Ansatzpunkte, um menschliche Angriffsvektoren und Bedrohungen durch Agenten in konkrete Gefährdungs- und Risikoanalysen einfließen zu lassen.
- **Einführung organisatorischer und technischer Schutzmaßnahmen:** Einrichtung konkreter Analyse, Überprüfung und Ausgestaltung von Schutzmaßnahmen in Bezug auf hier beschriebene Agentenaktivitäten (z.B. Überprüfungen, Sensibilisierungen, Meldeketten, Reisesicherheit, Kommunikationssicherheit, Geheimnisschutz).
- **Sensibilisierung und Schulung von Personal:** Ausgestaltung von Schulungen mit konkretem Bezug zu den dokumentierten Angriffsvektoren anhand der hier beschriebenen Vorgehensweisen.
- **Weitergabe sicherheitsrelevanter Informationen an Behörden:** Einbeziehung möglicher Beobachtungen von Spionage- und Agententätigkeit in Austausch sowie Meldekette zwischen Unternehmen und Behörden.

Weitere Maßnahmen

Das cyberintelligence.institute fördert im Verbund mit seinen Partnern die Resilienz gegen hybride Bedrohungen. Dazu werden regelmäßig neue Studien und Erkenntnisse veröffentlicht sowie konkrete Hilfestellungen und Angebote auf den Weg gebracht.

Für weitere Informationen und Möglichkeiten der Unterstützung bei der Entwicklung wirksamer Strategien und Maßnahmen zur Steigerung der Resilienz gegen hybride Bedrohungen sowie für die Bereitstellung von Materialien, Schulungen und Trainings nehmen Sie gerne Kontakt mit uns auf.

Mehr unter: www.cyberintelligence.institute

16 Das Paper bezieht sich dabei auf den letzten Stand des Gesetzentwurfs der Bundesregierung: Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen vom 27.11.2024 (https://dip.bundestag.de/vorgang/gesetz-zur-umsetzung-der-richtlinie-eu-2022-2557-und-zur/317496).

Impressum & Kontakt

Autor
Dr. Christopher Nehring
Intelligence Director
christopher.nehring@cyberintelligence.institute

Herausgeberin
cyberintelligence.institute
Geschäftsführer: Clemens Kröger (V.i.S.d.P.)
MesseTurm I Friedrich-Ebert-Anlage 49
D-60308 Frankfurt am Main

www.cyberintelligence.institute
info@cyberintelligence.institute

+49 69 505034602

This paper is published under CreativeCommons License (CC BY-SA). This allows for copying, publishing, citing and translating the contents of the paper, as long as cyberintelligence.institute (CII) is named and all resulting publications are also published under the license “CC BY-SA”.

Please refer to https://creativecommons.org/licenses/by-sa/4.0/deed.de for further information on the license and its terms and conditions.

Über das CII

Neue Zeiten brauchen eine neue Form der Forschung: das cyberintelligence.institute (CII) – ein Ort, an dem sich Innovation, Technologie, Strategie und Resilienz treffen. An der Schnittstelle von Wirtschaft und Wissenschaft, NGO und Start-up entwickelt das CII in Frankfurt am Main neue Lösungen für eine sichere digitale Zukunft. Kerngedanken sind die Kooperation, der Dialog und der interdisziplinäre und globale Informations- und Wissensaustausch, um Staat, Wirtschaft und Gesellschaft resilienter zu machen. Gefragt sind dabei ganzheitliche Konzepte, die Cybersicherheit nicht nur als abstrakte technisch-organisatorische Gewährleistungsverantwortung, sondern als gesamtgesellschaftliche Aufgabe zum Schutz gemeinsamer europäischer Werte verstehen. Damit tritt das cyberintelligence.institute aktiv für mehr digitale Sicherheit in einem Zeitalter neuer digitaler Herausforderungen ein.

Weitere Informationen gibt es auf der Website des CII unter www.cyberintelligence.institute.