

## **Untersuchungskomitee (Sledstwennyj komitet, SK)**

Nachdem das Untersuchungskomitee 2011 als eigenständige Institution aus dem Büro des Generalstaatsanwalts hervorging, ist es die wichtigste föderale Ermittlungsbehörde Russlands. Es untersteht direkt dem russischen Präsidenten und ist zuständig für die Überwachung von Polizeikräften, der Bekämpfung von Korruption und Machtmissbrauch innerhalb der Polizei sowie der Überprüfung von lokalen Behörden und föderalen Regierungsinstitutionen. Auch wenn es dem Untersuchungskomitee in der Praxis an der nötigen Durchsetzungskraft fehlt, hat es die theoretische Befugnis, Weisungen an die Geheimdienste zu erteilen. Die Leitung untersteht seit dem 14. Januar 2011 Alexander Bastrykin.

## **Sicherheitsrat (Sowet besopasnosti)**

Der Sicherheitsrat wird direkt vom Präsidenten einberufen und von diesem geleitet. Der Sicherheitsrat der Russischen Föderation gilt als Beratungsinstitution für den Präsidenten. Da Vertreter aller wichtigen Machtministerien im Sicherheitsrat zusammenkommen, dient dieser auch als Koordinationszentrum für die Machtministerien. Um deren Zusammenarbeit zu vertiefen, werden dienstübergreifende Kommissionen gegründet. Die Leitung untersteht zwar dem Präsidenten, der Sicherheitsrat wird aber von seinem Sekretär überwacht. Sekretär ist seit dem 12. Mai 2008 Nikolaj Patruschew.

*Zusammengestellt von: Franz Springer*

### *Quellen:*

- Galeotti, Mark: Putin's Hydra: Inside Russia's Intelligence Services, European Council on Foreign Relations, London 2016.
- Soldatov, Andrei; Rochlitz, Michael: The Silvoki in Russian Politics; in: Treisman, Daniel (Hrsg.): The New Autocracy. Information, Politics and Policy in Putin's Russia, Brookings Institution Press: Washington, D.C. 2018, S. 83–108.
- Taylor, Brian D.: State Building in Putin's Russia. Policing and Coercion after Communism, Cambridge University Press 2011.
- Offizielle Website des Präsidenten der Russischen Föderation, <http://en.kremlin.ru/>
- Offizielle Website der Regierung der Russischen Föderation, <http://government.ru/en/structure/>

DEKODER

## **100 Jahre GRU: Werdegang und Professionalität eines russischen Geheimdienstes**

Christopher Nehring (Deutsches Spionagemuseum, Berlin)

Der folgende Beitrag von Christopher Nehring wurde am 26. Oktober von dekoder.org veröffentlicht.

### **Einleitung von dekoder**

Am 5. November 2018 feierte die Glawnoje raswedyvatelnoje uprawlenije GRU (dt. »Hauptverwaltung für Aufklärung«) 100-jähriges Jubiläum. Pünktlich zu seinem Ehrenjahr steht der Militärgeheimdienst Russlands so sehr im Fokus der Weltöffentlichkeit wie nie zuvor. Der Giftanschlag in England und Cyberangriffe auf internationale Einrichtungen sind nur die Spitze eines Eisberges an Operationen, mit denen die GRU 2018 öffentlich in Verbindung gebracht wird. Das klingt zunächst einmal nach einem außerordentlich potenzen Geheimdienst mit wenig Skrupel, viel Know-how und einem breiten Spektrum an Tätigkeiten.

### **GRU – russischer Militärgeheimdienst**

Von den schweren Vergiftungen in England war nur einer der Giftanschläge auch tatsächlich so geplant: der auf den ehemaligen GRU-Offizier Sergej Skripal. Der Doppelagent überlebte, seine Tochter, das zweite und

unerwartete Giftopfer, ebenfalls. Die beiden anderen Opfer, von denen eines der Vergiftung mit Nowitschok erlag, waren »Kollateralschäden«: Sie fanden zufällig das Behältnis, in dem das Gift transportiert worden war. Alles in allem war es eine ziemliche Blamage für

die GRU, vor allem weil sich der Fall unter ständiger Beobachtung der Medien abspielte.

Und dann wurden auch noch die beiden Tatverdächtigen präsentiert und von britischen und russischen Investigativjournalisten eindeutig mit der GRU in Verbindung gebracht. Dabei kam sogar heraus, dass die GRU 305 Fahrzeuge mehr oder weniger offiziell auf ihre Mitarbeiter registriert und sie damit praktisch selbst enttarnt hatte [<https://www.bellingcat.com/news/2018/10/04/305-car-registrations-may-point-massive-gru-security-breach/>]. Für alle ersichtlich.

Mitnichten weniger peinlich war es, als im April 2018 niederländische und britische Ermittler der Spionageabwehr eine Gruppe von vier GRU-Computerspezialisten in ihrem Auto während eines Cyberangriffs verhafteten. Das komplette Equipment im Kofferraum, dazu gefälschte Pässe mit fortlaufender Nummerierung, wie schon bei Alexander Petrow und Ruslan Boschirow [den Verdächtigen im Fall Skripal – Anm. d. Red.]. Das Ziel des Angriffs war die Organisation für das Verbot chemischer Waffen (OPCW), die zu dieser Zeit die Giftproben des Anschlags aus Salisbury untersuchte [siehe dazu auch den Beitrag von Una Becker-Jakob in den Russland-Analysen Nr. 356, S. 21: <http://www.laender-analysen.de/russland/pdf/RusslandAnalysen356.pdf> – Anm. d. Red.]. Geparkt hatten die vier Hacker in einem blauen Citroën direkt gegenüber der OPCW in Den Haag.

Was an Dreistigkeit wohl kaum zu überbieten ist, gehört allerdings nicht in die Kategorie professionalen Arbeitens, wie es sich die geheimdienstliche Elite-truppe auf die eigenen Fahnen schreibt. Wo also steht die gefürchtete und nun verspottete russische Militäraufklärung 100 Jahre nach ihrer Gründung?

## Die GRU im System

Wie der gesamte Sicherheitsapparat der Russischen Föderation hat die GRU ihre Wurzeln tief im kommunistischen Staat der Bolschewiki nach der Oktoberrevolution 1917. Eine Besonderheit war es, dass die GRU trotz aller Wirren der Zeit nicht mit anderen Geheimdiensten vereint wurde. Wo der mächtige KGB jahrzehntelang In- und Auslandsgeheimdienst, Personenschutz, Grenztruppen und technische Abteilungen mit mehreren hunderttausend Mann vereinte, war und ist die GRU der Armee und dem Verteidigungsministerium unterstellt. Im Vergleich zum KGB und seinen Nachfolgern FSB und SWR nahm und nimmt die GRU damit eine Sonderstellung ein, denn diese sind direkt dem Präsidenten unterstellt. Einerseits bedeutet das für die GRU eine größere Unabhängigkeit vom Gravitationszentrum staatlicher Macht in der russischen Präsidialadministration. Andererseits ist die Entfernung zum Präsidenten ein Nachteil im ständigen Ringen der Sicherheitsdienste um Präsidentengunst und knappe Ressourcen.

Wie wechselhaft sich diese Stellung im politischen System auswirken kann, hat die GRU in den vergangenen 20 Jahren mehrfach erfahren. Im Zuge der Armeereformen der postsowjetischen Zeit wurde die stolze Truppe erst einmal herabgestuft: Spezialeinheiten wurden den regulären Truppen unterstellt, Mittel gekürzt, aus GRU wurde »GU«, also einfach nur Hauptverwaltung. Die stille, aber alles hörende Fledermaus im Wappen wurde durch eine Nelke ersetzt – Symbol für Standfestigkeit und Entschiedenheit.

Als 2012 Sergej Schoigu Verteidigungsminister wurde, machte er sich daran, die GRU nicht nur symbolisch wieder aufzuwerten. Personell soll die GRU mit rund 12.000 Mitarbeitern ungefähr dasselbe Niveau wie der Auslandsgeheimdienst SWR erreichen. Nach Angaben des GRU-Überläufers Stanislaw Lunew aus dem Jahr 1997 führte der Militärgeheimdienst damals allerdings sechsmal so viele Auslandsagenten wie sein ziviles Pendant. Mark Galeotti zufolge, solle darüber hinaus die Anzahl der Spezialkämpfer, die der GRU unterstellt waren, deutlich über 20.000 Mann betragen haben.

## Aufträge und Einsätze

Auch in ihrem Arbeitsauftrag sticht die Sonderrolle der GRU durch. 1918 oder 1941 ging es vor allem um traditionelle militärstrategische Aufklärung auf allen Schlachtfeldern der Roten Armee, von Polen bis zum Pazifik. Im Kalten Krieg kam dann schon Rüstungs- und Wirtschaftsspionage hinzu. Eine weitere Besonderheit der GRU war und ist, dass sie nicht nur im Ausland aufklärt, sondern auch die Spionageabwehr der Armee in sich vereint. Was der FSB im zivilen Sektor ist oder in Deutschland der Militärische Abschirmdienst MAD für die Bundeswehr, ist die GRU für die russische Armee.

Ebenso waren die berühmt-berüchtigten Speznas-Elite-Kampftruppen der GRU ein Kind der Stellvertreterkriege während des weltweiten Systemkonflikts. Wo reguläre sowjetische Truppen zu auffällig gewesen wären oder wo inoffizielle Waffenlieferungen in Krisengebiete besonderer Tarnung bedurften, dort waren die Speznas zu finden. Das gilt auch für sogenannte Kommandoeinsätze wie Sabotage, Geiselbefreiungen, Entführungen und gezielte Tötungen im Ausland.

Dabei ist die GRU global orientiert: USA, NATO, Westeuropa, aber eben auch der Nahe und Mittlere Osten, Afrika, China und der Pazifikraum sind Aufklärungsziele und Einsatzgebiete.

## Agenten und Operationen

Lange Jahre schwamm die GRU eher leise im Kielwasser der wesentlich bekannteren NKWD, KGB und schließlich SWR. Öffentliche Nennungen hielten sich in Grenzen, Experten und Forscher konzentrierten sich ebenfalls lieber auf die zivilen Brüder. Bis auf den heu-

tigen Tag existiert keine Gesamtgeschichte der GRU, wo es selbst die offizielle Geschichtsschreibung der russisch-sowjetischen Auslandsaufklärung auf ganze sechs Bände bringt. Ganz so eben, wie man es von einem klassischen Geheimdienst erwartet: Im Großen und Ganzen ein Mysterium, presseabstinent, unter Kennern aber als absolute Profis ihres Metiers bekannt.

Dass dem tatsächlich so ist, zeigt ein Parforceritt durch die Spionagegeschichte. Wie die gesamte Sowjet-Spionage, war die GRU in der Zeit zwischen den Weltkriegen außerordentlich erfolgreich: Gleich zwei der bekanntesten Spione aller Zeiten arbeiteten für die GRU – und waren Deutsche. Der als Journalist getarnte Richard Sorge meldete 1941 aus Japan den bevorstehenden Angriff der Wehrmacht auf die Sowjetunion (und wurde von Stalin deswegen geopfert). Der Physiker Klaus Fuchs, einer der Väter der amerikanischen Atom bombe, war ebenfalls ein GRU-Agent und sorgte dafür, dass auch die Sowjets zur Nuklearmacht werden konnten. Diese Taktik, sogenannte »illegale« Agenten unter falscher Identität in westlichen Ländern zu führen, praktizierte die GRU über die gesamte Zeit des Kalten Krieges.

Schon zu Sowjetzeiten zählten militärische Kommandoaktionen zur Aufgabe der GRU und ihrer Spez nas. Diese Aufgabe hat die GRU auch heute nicht eingebüßt. Während der Tschetschenenkriege übernahm die GRU »Spezialaufgaben«, in Dubai soll der Spezna s 2009 den Anführer tschetschenischer Rebellen, Sulim Jamadajew, in einer Kommandoaktion getötet haben.

Auch die Bilder der Krim-Annexion sind immer noch einprägsam: »Grüne Männchen« ohne Abzeichen, die später als GRU-Truppen identifiziert wurden, bereiteten damals den Weg für die Angliederung. Ein ähnliches Schicksal hatte die GRU offenbar dem kleinen Montenegro zugesetzt: 2016 sollten pro-serbische Teile der Armee unter Anleitung von GRU-Offizieren just in der Wahlnacht einen Putsch in dem Land auf dem Westbalkan unternehmen. Als einzige der in jüngster Zeit bekannt gewordenen Kommandounternehmen der GRU scheiterte dieser Versuch allerdings kläglich.

## Cyberangriffe

Eine gänzlich neue Aufgabe, die die GRU in den letzten Jahren ebenfalls ausführt, sind geheimdienstliche Cyberangriffe wie jener in Den Haag. Geheimdienste und Regierungen von den USA bis nach Australien rechnen Hackergruppen wie ATP 28, Fancy Bear oder Pawn Storm der GRU zu. Das besondere an ihren bekannten Attacken war dabei, dass sie keineswegs nur militärische Ziele verfolgten, sondern Aufgaben ausführten, die eigentlich den zivilen russischen Diensten obliegen. So haben die Wahlkampfunterlagen der US-Demokraten, die ATP 28 im Vorfeld der Präsidentschaftswahl

2016 mittels eines versteckten Trojaners erbeuteten, mit Militäraufklärung ebenso wenig zu tun wie Aktionen von Fancy Bear. Diese Gruppe drang offenbar besonders gerne in westliche oder internationale Sportverbände ein. Aus Sicht der US-Geheimdienste waren die Angriffe im Bereich von Doping und Sport eine gezielte Vergeltungsaktion gegen die Doping-Vorwürfe und Sanktionen gegen russische Mannschaften. Dass der Inlandsgeheimdienst FSB in das russische Staatsdoping involviert war, war schon länger bekannt [siehe dazu den sog. McLaren-Report aus dem Jahr 2016: <https://www.wada-ama.org/en/resources/doping-control-process/mclaren-independent-investigation-report-part-ii>]. Dass die GRU die propagandistischen Gegenmaßnahmen offenbar maßgeblich organisierte, war hingegen neu.

Für die »neuen« Aufgaben der GRU im Cyberbereich gibt es drei Interpretationen: Einmal steht das pure Potential, das heißt die GRU unternimmt Cyberangriffe im zivilen Bereich, weil sie es schlicht kann. Das enorme Reservoir an IT-Spezialisten in Russland und die Mittel, die den Spezialbereichen des Militärs zur Verfügung stehen, machen die GRU zu einer Weltspitze der Cyberspionage.

Zweitens geht es um die Konkurrenz der Weltmächte: US-Militär und die Defense Intelligence Agency DIA sind auf diesem Gebiet genauso aktiv wie zum Beispiel auch die Cybereinheit 61398 des chinesischen Militärs. Präsenz durch aufsehenerregende Hacking-Operatio nen zu zeigen, ist da nur logisch.

Drittens spielt auch der Druck eine Rolle, sich gegenüber FSB und SWR beweisen zu müssen. Dass beide ebenfalls Cyberangriffe durchführen, ist bekannt. Die Ausflüge der GRU in die zivile Cyberwelt können also auch als interne *show of force* und Fingerzeig im russischen Sicherheitsapparat gedeutet werden. Wie fluide hier Zuständigkeiten wechseln, ausgebaut oder gestrichen werden und wie wichtig die Gunst des innersten Machtzirkels ist, das hat die Vergangenheit immer wieder gezeigt.

## Korruption und Schlamperei

Doch auch in der geheimnisumwitterten GRU scheint so manches in Bewegung gekommen zu sein. Gerade die jüngsten Schlagzeilen passen nicht zum Image eines hochprofessionellen Geheimdienstes: Warum der Anschlag auf den ausgetauschten Ex-Agenten Skripal? Warum die schlampige Ausführung? Wie kam die GRU auf die Idee, zwei Offiziere könnten erfolgreich einen Putsch in Montenegro betreuen? Und wie kommt ein Geheimdienst auf die Idee, über 300 PKW auf seine offizielle Adresse zu registrieren und damit möglicherweise eigene Agenten zu enttarnen?

Neben der professionellen GRU existiert anscheinend auch eine normale russische Behörde, in der Schlamperei, Realitätsverweigerung und Korruption zum Alltag gehören. Die vielen bürokratischen Details erfolgreicher geheim-

dienstlicher Arbeit gingen offenbar immer wieder bei der Operationsplanung ab. Dafür haben die jahrelang erfolgreichen Hackingangriffe und die getarnten Kommandoaktionen wohl ein Gefühl der Unverwundbarkeit wachsen lassen. Wer aber so oft durchkommt, der wird nachlässig.

Gleichfalls hat der lasche Umgang westlicher Behörden mit den russischen Agenten offenbar zu immer dreisterem Vorgehen ermuntert: Obwohl westlichen Geheimdiensten offensichtlich schon bekannt war, dass die GRU-Agenten Jewgenij Serebrjakow und Alexej Morenez im Herbst 2016 den Computer eines Vertreters des kanadischen Antidopingzentrums CCES gehackt hatten [<https://www.nzz.ch/international/die-jagd-nach-putins-agenten-wie-ein-spyionagefall-in-lausanne-zu-einem-fiasko-des-russischen-geheimdiensts-fuehrte-ld.1429047>], sahen diese Agenten im April 2018 offenbar überhaupt kein Risiko und parkten fast schon demonstrativ direkt vor dem Zielobjekt in Den Haag.

Darüber hinaus gibt es auch Korruptionsgerüchte um die GRU. Wo schmale Gehälter des öffentlichen Dienstes auf Milliarden Rubel für Aufträge ans Militär aufeinandertreffen, lockt das große Geld. Auch die GRU-Leitung soll in der Vergangenheit auf diese Art zu Reichtum gekommen sein. Auf die Arbeitsmoral des Dienstes wirkte sich das offenbar nur dahingehend positiv aus, dass in immer waghalsigeren Aktionen ein schneller Aufstieg gesucht wurde, um ebenfalls an die »Fleischköpfe« zu kommen.

#### *Über den Autor*

Christopher Nehring ist Leiter *Forschung* im Deutschen Spionagemuseum in Berlin. Er hat Osteuropäische und Neuere Geschichte in Heidelberg und St. Petersburg studiert und 2016 zum Thema der Geheimdienstgeschichte promoviert.

#### *Lesetipps*

- Lunew, Stanislaw: Through the Eyes of the Enemy: The Autobiography of Stanislav Lunev, Washington 1998.
- Galeotti, Mark: Putin's Hydra: Inside Russia's intelligence Services, European Council on Foreign Relations 2016.
- Bajrovic, Reuf; Garcevic, Vesko; Kramer, Richard: Russia's Strategy of Destabilization in Montenegro, Foreign Policy Institute 2018.
- Dekoder: Debattenschau Nr. 63: Anschlag auf Ex-Doppelagent Skripal, <https://www.dekoder.org/de/article/debattenschau-skripal-nervengift-spion>
- Dekoder: »Als Kind war ich Fan von Detektivgeschichten« über Roman Dobrohotows gemeinsame Recherche mit Bellincat zu den Tatverdächtigen im Fall Skripal, <https://www.dekoder.org/de/article/bellingcat-skripal-gru-recherche>
- Dekoder: Bystro #4: 6 Fragen an die Verdächtigen im Fall Skripal über die offenen Fragen nach dem Interview mit den Tatverdächtigen auf RT, <https://www.dekoder.org/de/article/bystro-skripal-verdaechtige-interview-boschirow-petrov>

Das Original dieses Beitrags ist online verfügbar unter: <https://www.dekoder.org/de/gnose/gru-militaergeheimdienst-hacker-skripal>.

Die Redaktion der Russland-Analysen freut sich, dekoder.org als langfristigen Partner gewonnen zu haben. Wir danken unserem Partner dekoder und Christopher Nehring für die Erlaubnis zum Nachdruck.

*Die Redaktion der Russland-Analysen*