1 | Dokument aus den »Vulkan Files« **2 |** Russischer Präsident Putin **3 |** Vulkan-Gründer Markow **4 |** Vulkan-Gründer Irschwaskij

[M] Lea Rossa / DER SPIEGEL; Fotos: Vulkan Files (4); Gavriil Grigorov / dpa; Bobylev Sergei / Itar-Tass / action press; Wikimedia Commons; Sebastien Bozon / AFP; Denis Charlet / AFP

Sandwurm und Schlange

SPIONAGE Wladimir Putins Geheimdienste bereiten sich auf einen Cyberkrieg vor. Es geht darum, Flughäfen, Kraftwerke und das Internet lahmlegen zu können. Geheime Daten aus Moskau geben nun erstmals Einblick in das Waffenarsenal der russischen Hacker.

Moskau ist düster im feinen Spätwinterniesel, noch immer häufen sich schmutzige Schneereste vor dem grauen Bürogebäude im östlichen Sokolinaja-Gora-Bezirk. Es ist ein unauffälliges Haus in einer unauffälligen Gegend, unweit des Preobraschenskoje-Friedhofs, wo eine ewige Flamme zum Gedenken an die Toten des Zweiten Weltkriegs brennt. Draußen, vor dem Haupteingang, schrecken keine Stacheldrahtzäune ab, keine finsteren Wachleute.

Alles ganz normal. Alles Tarnung.

Die Firma, die hier an der Uliza Ibragimowa 31 residiert, nennt sich NTC Vulkan und gibt sich als normales Unternehmen für IT-Beratung aus, als kleiner Mittelständler mit Softwareexpertise. IBM sei ein enger Partner, die Toyota Bank eine gute Kundin, wirbt das Unternehmen im Internet, ein Spezialgebiet: »Management der Informationssicherheit«. Es ist eine sorgfältig gebaute Fassade, die auf den ersten Blick standhält. Auch auf den zweiten. Aber es ist nicht die ganze Wahrheit.

Wer hineinwill in die oft verdunkelten Büros, voll mit Computern, Servern, Hightechelektronik, muss vorbei an Sicherheitstüren und Kameras. Denn dahinter arbeiten Programmierer und Hacker mit gefährlichen Absichten: Chaos säen. Zerstören.

So etwa: Die Computer eines Flughafens lahmlegen, über die der Tower mit Flugzeugen kommuniziert. Züge entgleisen lassen durch eine Software, die Sicherheitskontrollen ausschaltet. Die Stromversorgung kappen.

Cyberkriegsführung nennt sich das. Eine Spezialität russischer Agenten. Vulkan arbeitet für sie: für den Militärgeheimdienst GRU, den im Inland tätigen FSB, den für Auslands- und Wirtschaftsspionage zuständigen SWR. »Als ich angefangen habe, für die Firma Vulkan zu arbeiten, war mir nicht klar, woran ich arbeiten werde«, sagt ein ehemaliger Angestellter, der sich inzwischen abgesetzt hat. »Später habe ich verstanden, dass wir nicht einfach nur Daten sammeln. Sondern dass wir sie für die russischen Geheimdienste nutzen.«

Die von Vulkan entwickelten Systeme tragen nichtssagende Codenamen, »Scan-V«, »Crystal-2V«, »Amezit«, aber ihre Funktionen sind alles andere als ordinär. Sie sollen dem russischen Militär etwa helfen, digitale Schwachstellen seiner Gegner aufzuspüren, und damit Cyberangriffe deutlich leichter machen. Feindliche Kommunikationssysteme überrumpeln und übernehmen. Desinformation verbreiten.

All das lässt sich herauslesen aus mehr als 1000 geheimen Dokumenten: 5299 Seiten mit Projektplänen, Anleitungen und internen E-Mails von Vulkan aus den Jahren 2016 bis 2021. Sie sind auf Russisch und oft extrem technisch, aber wer beginnt, sie zu verstehen, bekommt einen einmaligen Einblick in die Abgründe der russischen Cyberkriegspläne. In einen Militärstaat, der den Westen nicht nur mit Kampfflugzeugen, Panzern und Geschützen bedroht, sondern der mit Hackern und Angriffssoftware aufrüstet.

Zu beobachten ist diese Strategie insbesondere in der Ukraine, die seit dem russischen Einmarsch so unerbittlich und pausenlos von russischen Hackern attackiert wird, dass Experten vom »ersten vollumfassenden Cyberkrieg der Welt« sprechen. Die Russen greifen wichtige Behörden und Firmen an, schalten das Internet aus, legen einen Kommunikationssatelliten lahm.

Aber längst werden die Cyberangriffe auch in anderen Teilen der Welt immer dreister, immer gefährlicher. Russische Saboteure drangen in die IT-Systeme des Deutschen Bundestags und dort bis in den Rechner von Angela Merkel vor. Sie attackierten das Team des französischen Präsidenten Emmanuel Macron und veröffentlichten vertrauliche Dokumente. Während der Olympischen Spiele in Südkorea schnitten sie zeitweise die Verbindungen ins Internet ab.

Verantwortlich zumindest für die beiden letzteren Attacken war die Einheit 74 455 des russischen Militärgeheimdienstes GRU, Codename: »Sandworm«. Die gefährlichste Hackergruppe der Welt. Vulkan, das legen die Dokumente nahe, versorgt auch sie mit Angriffswerkzeugen.

Bislang konnten Ermittler nur rückwirkend die Spuren solcher Cyberattacken analysieren. Dank der »Vulkan Files« lässt sich nun erstmals detailliert erkennen, wie solche Angriffe vorbereitet und organisiert werden, wie ruchlos Wladimir Putin mithilfe privater Firmen weltweite Hacking-Operationen planen und durchführen lässt. In den Dokumenten lässt sich Schritt für Schritt verfolgen, wie solche Angriffe ablaufen sollen.

Ein Großteil der Unterlagen stammt von einer anonymen Quelle. Sie hat die Daten wenige Tage nach Beginn des russischen Einmarschs in die Ukraine der »Süddeutschen Zeitung« zugespielt und später ebenfalls mit dem SPIEGEL geteilt. »Wegen der Vorgänge in der Ukraine habe ich mich entschieden, diese Information öffentlich zu machen«, so die Quelle, die sich nie zu erkennen gab und seither abgetaucht ist. »Die GRU und der FSB versteckten sich hinter dieser Firma. Die Menschen sollten wissen, welche Gefahren das birgt.«

Der SPIEGEL hat die Unterlagen zusammen mit zehn Medienpartnern aus acht Ländern verifiziert und ausgewertet. Darunter waren das ZDF, der »Guardian«, die »Washington Post«, der österreichische »Standard«, »Le Monde« aus Frankreich, die Schweizer Tamedia-Gruppe und das russische Investigativportal »IStories«. Eine monatelange Spurensuche förderte weitere interne Dokumente der Firma und Überweisungsdaten zutage. Zusätzlich wurde Vulkan und dem Kreml Gelegenheit zur Stellungnahme gegeben, mehrfach. Antworten gab es nicht. Offenbar besteht kein Grund, an den Schlüssen des Rechercheteams zu zweifeln.

Fünf westliche Geheimdienste bestätigten zudem, dass die Dokumente authentisch sind. Die meisten von ihnen beobachten Vulkan wegen der Arbeit für russische Spionageorganisationen schon länger. Dabei erscheint die Firma als Teil eines undurchsichtigen militärisch-industriellen Komplexes, in dem russische Geheimdienste und mehr als 40 private IT-Unternehmen eng miteinander verwoben sind. Eines ihrer Ziele besteht darin, Cyberwaffen zu entwickeln, um sie auf alle zu richten, die Moskaus Machthaber zu Feinden erklärt haben. Insbesondere natürlich im Westen.

»Russland ist in unseren Netzen«, warnt Wolfgang Wien, Vizechef des Bundesnachrichtendienstes. Staaten hätten ihre Hacker schon lange vor einer Krise in Stellung gebracht, damit sie schnell zuschlagen könnten, sobald sie einen Befehl erhielten.

Das klingt beängstigend, wie so vieles, wenn man sich erst einmal hineinbegibt in diese finstere Halbwelt von Hackern und Agenten, Saboteuren und Kriegstreibern. Dazu zählt auch diese Erkenntnis: Die russischen Cybersoldaten bleiben nicht nur in ihren geheimen Bunkern und versteckten Hauptquartieren irgendwo in Moskau. Man-

che haben sich anwerben lassen von internationalen Konzernen, auch von deutschen Firmen: Der SPIEGEL hat ehemalige Vulkan-Mitarbeiter entdeckt bei Siemens und einem BASF-Dienstleister, bei Trivago und Booking.com. Die bedenklichste Spur führt nach Dublin, Irland, mitten hinein in eines der europäischen Zentren der Techindustrie.

Ranelagh ist ein wohlhabender Vorort im Süden Dublins, mit hübschen Pubs und szenigen Restaurants, die »Butcher Grill« oder »Firebyrd« heißen. Ausländische Botschaften haben sich in viktorianischen Villen angesiedelt. In dem Viertel mit seinen kleinen Backsteinhäusern mit weißen Fensterrahmen wohnen oft Angestellte von Google, IBM, Meta. Ihre Niederlassungen sind nur wenige Minuten entfernt.

In einem dieser Häuser lebt Sergej N., 35 Jahre alt, doch er wirkt jünger, als er die Tür öffnet. Auch N. hat es nicht weit zur Arbeit, weniger als eine halbe Stunde ist es mit dem Auto bis zu Amazon Web Services (AWS), einem Tochterunternehmen von Amazon, 80 Milliarden Dollar Jahresumsatz und weltgrößter Anbieter von Cloud Computing. Hier lagern unzählige der größten Unternehmen der Welt ihre Informationen oder gleich große Teile ihrer IT. Darunter Netflix, Vodafone, die Nasa, die US-Marine und die meisten Dax-Konzerne von Allianz bis Volkswagen. Auf den AWS-Servern laufen große Teile des globalen Internets. Und ukrainische Regierungsdaten.

Der Russe Sergej N. firmiert jetzt als »Senior Software Development Engineer«, er muss zahlreiche Auswahlrunden überstanden haben, um diesen Job zu bekommen. Amazon kann sich die weltbesten Programmierer aussuchen, und N. ist erfahren. Er hatte auch vorher schon einen Führungsposten. Als Chefentwickler von Vulkan.

AWS hat ihn wohl 2018 eingestellt, vor der Invasion. Als es noch unproblematischer schien, Experten von russischen IT-Unternehmen zu übernehmen. Vor allem von so unscheinbaren wie Vulkan. Ein Imagefilm der Firma verspricht, man könne bei Vulkan die »Welt zum Besseren verändern«. Etwa 135 Menschen sind derzeit dort angestellt.

Allerdings hat N. fast sieben Jahre lang bei Vulkan an wenig friedlichen Dingen gearbeitet. Zum Beispiel am System »Scan-V«, einer Software, die IT-Sicherheitsexperten und mehrere westliche Geheimdienste als »offensiv« einschätzen. Also auch geeignet, andere Nationen über das Internet zu attackieren.

Darüber gilt es, mit N. zu reden, als er die Tür öffnet: »Wir arbeiten für den SPIEGEL und recherchieren zu einer Firma namens Vulkan. Sie haben für die Firma gearbeitet. Dürfen wir Ihnen ein paar Fragen stellen?«

N. wirkt irritiert, in seinem Gesicht steht eine Mischung aus Angst und Verwirrung. Er will keine Fragen beantworten. »Kennen Sie das System Scan-V?« N. reißt die Augen auf, er wirkt erschrocken. »Nein, sorry.« Dann schlägt er die Tür zu.

Ähnlich erging es Reportern zeitgleich an vielen anderen Orten in Europa, an denen ehemalige Vulkan-Mitarbeiter leben. Über ihre frühere Arbeit wollten die meisten nicht sprechen. Ob aus Furcht vor Vergeltung oder weil ihre Tarnung aufzufliegen drohte, bleibt unklar.

Allein das Beispiel Sergej N. wirft beunruhigende Fragen auf: Was macht ein russischer Cyberkriegsspezialist in einem Unternehmen, das weite Teile der IT Hunderter Weltkonzerne beherbergt, dessen Infrastruktur eine tragende Säule des globalen Internets bildet? Konnte oder wollte AWS nicht wissen, was N. früher gemacht hat? Noch im Juni 2019 finden sich in einem geleakten Dokument Kommentare, die mit seinem Namen signiert sind. Zu diesem Zeitpunkt arbeitete er nach eigenen Angaben schon für AWS. Auf Anfrage teilte der US-Konzern lediglich mit, die Sicherheit seiner Kundendaten genieße höchste Priorität.

Ebenso unverbindlich antwortete Siemens, auch dort hat der SPIEGEL eine ehemalige Vulkan-Mitarbeiterin entdeckt: Man nehme das Thema ernst, könne aber aus Datenschutzgründen nichts zu einzelnen Angestellten sagen. Die Integrität von Bewerberinnen und Bewerbern werde im Rahmen der rechtlichen Möglichkeiten geprüft. IBM teilte mit, dass die Geschäftsbeziehung zu Vulkan seit 2020 beendet sei.

Offenbar scheinen Konzerne im harten Wettbewerb um gut ausgebildete IT-Fachkräfte erstaunlich leichtsinnig zu sein. Viele Vulkan-Mitarbeiter sind Absolventen der Moskauer Bauman-Universität, einer Kaderschmiede. Die Universität unterhält enge Drähte zum russischen Sicherheitsapparat, führt »Spezialstudien« für das russische Verteidigungsministerium und den Geheimdienst FSB durch.

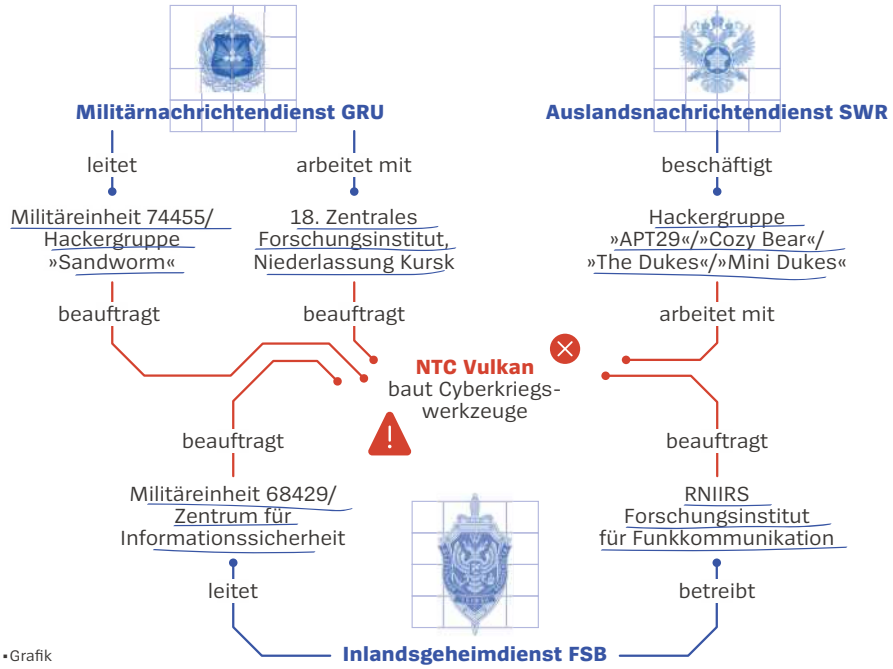
Solche Drähte hat auch zumindest einer der Vulkan-Gründer, Alexander Alexandrowitsch Irschawskij. Er ist regelmäßiger Gast auf Konferenzen des Verteidigungsministeriums. Als Beamte einen Verkehrsverstoß ahndeten, gab er als seine Adresse die eines Instituts an, das eng mit dem Militärgeheimdienst GRU verbunden ist. 2010 gründete Irschawskij gemeinsam mit Anton Wladimirowitsch Markow die Firma Vulkan. Beide Männer sind mittleren Alters – und unscheinbar.

Herausfinden lässt sich indes, woran sie und ihre Firma im vergangenen Jahrzehnt gearbeitet haben. Zum Beispiel an einem System mit dem Codenamen »Amezit«. Das Ziel: Informationskontrolle über bestimmte Gebiete. So steht es unter anderem in einem Dokument unter der Überschrift »Zweck der Software«. In vielen weiteren Dokumenten und Hunderten Seiten Bauplänen, Schaubildern und Tabellen wird eine Plattform beschrieben, die praktisch alle Aspekte der modernen Cyberkriegsführung abdecken würde. Sie reicht von Zensur und der Manipulation von Social-Media-Inhalten bis zu Angriffen auf Einrichtungen der kritischen Infrastruktur. Im Material enthaltene Spuren führen etwa zu Serverstandorten in den USA oder einem Atomkraftwerk in der Schweiz.

»Diese Dokumente deuten darauf hin, dass Russland Angriffe auf zivile kritische Infrastrukturen und die Manipulation sozialer Medien als ein und dieselbe Mission ansieht, die

Hackergrüße aus Moskau

Drei **russische Geheimdienste** verlassen sich auf die Produkte und Hackerwerkzeuge der Moskauer Firma **NTC Vulkan.**



Wikimedia Commons

S • Grafik

im Wesentlichen ein Angriff auf den Kampfeswillen des Feindes ist«, sagt John Hultquist von der IT-Sicherheitsfirma Mandiant, ein führender Experte für russische Cyberkriegsführung.

Diverse Funktionen des Programms legen nahe, dass »Amezit« bei der Übernahme besetzter Gebiete eine Rolle spielen könnte, wenn schnell die kommunikative Kontrolle gewonnen werden soll – wie auf der Krim oder im Donbass. Der Zeitraum seiner Entwicklung fällt zudem mit Bestrebungen des Kreml zusammen, ein abgeschottetes nationales Internet aufzubauen.

Ob und für wen genau ein solches System gebaut wurde, lässt sich nicht mit Sicherheit sagen, aber es gibt deutliche Hinweise. Wie eine E-Mail des Projektleiters Maxim Andrejewitsch D. an mehrere Vulkan-Mitarbeiter, datiert auf den 22. Juni 2018, mit der Betreffzeile: »Dienstreise nach Rostow«. Genauer: zum Forschungsinstitut für Funkkommunikation des FSB, des vielleicht mächtigsten russischen Geheimdienstes mit geschätzt 350 000 Mitarbeitern.

Putin selbst leitete den FSB Ende der Neunzigerjahre. Heute ist er sein wichtigstes Werkzeug zur Unterdrückung der Opposition im Inland. Es war ein FSB-Kommando, wie der SPIEGEL und die Investigativplattform Bellingcat enthüllten, das im Sommer 2020 mutmaßlich versuchte, den Oppositionellen Alexej Nawalny in Sibirien zu ermorden: Agenten trugen heimlich den Nervenkampfstoff Nowitschok auf seine Unterhose auf.

Auch die Cyberfähigkeiten des FSB sind beträchtlich. Vor Jahren drangen Hacker des Dienstes in die Computer des Auswärtigen Amts in Berlin ein. Langsam tasteten sie sich vor bis zu den Rechnern des für Russland und Osteuropa zuständigen Referats, ihr offenkundiges Ziel. »Snake«, die Schlange, tauften westliche Sicherheitsexperten die Angriffskampagne.

Eine andere Hackereinheit des FSB, unter Experten als »Berserk Bear« bekannt, schleuste über Jahre unentdeckt Schadcode in die Computersysteme von Kernkraftwerken, Öl- und Gasfirmen und anderen Energieunternehmen in 135 Ländern ein, darunter in den USA und Deutschland.

Dass Geheimdienste trotz solcher eigenen Spezialabteilungen mit Privatfirmen arbeiten, ist nicht ungewöhnlich. Auch der Whistleblower Edward Snowden war nicht direkt für den US-Geheimdienst NSA tätig, sondern für eine private Partnerfirma namens Booz Allen Hamilton. Ähnliche Beispiele sind aus China und Indien bekannt. Manchmal ist es, ähnlich wie auch bei Unternehmen, einfacher und schneller, Aufträge an spezialisierte Zulieferer outzusourcen. An Firmen wie Vulkan.

Vulkan-Zentrale in Moskau: Auf Firmenausflügen wird mit Panzern über einen Übungsplatz gejagt

135

Angestellte hat Vulkan. Die Firma arbeitet seit Jahren für russische Geheimdienste.

So ist auch die Dienstreise des Vulkan-Teams zum FSB-Ableger in Rostow am Don Teil einer typischen Geschäftsbeziehung. In seiner E-Mail beauftragt Vulkan-Manager D. sein Team, umgehend eine Präsentation »unserer Softwareplattform für den Militärvertreter in Rostow« vorzubereiten. Über mehrere Tage solle »Amezit« mit mehreren Subsystemen demonstriert werden. Mitfahren sollte laut den E-Mails auch der heutige Amazon-Informatiker Sergej N. – um vier Teilsysteme des »Amezit«-Angriffssystems vorzustellen. Dazu gelte es, heißt es weiter, nun möglichst schnell das nötige Equipment (»drei Server, fünf Armaturen, Switchboard«) an das FSB-Institut zu schicken.

Ob die Dienstreise nach Rostow erfolgreich war und ob der FSB »Amezit« derzeit einsetzt, lässt sich aus den geleakten Dokumenten nicht ersehen. Aber für die Vulkan-Ingenieure gibt es reichlich weitere Gelegenheiten, ihre Cyberwaffen zu präsentieren. Regelmäßig müssen Entwicklungsteams direkt beim FSB am Moskauer Lubjanka-Platz zum Rapport antreten: Mit der U-Bahn, blaue Linie, sind es nur vier Stationen vom Firmensitz bis ins Zentrum Moskaus. Am Rande des Platzes thront ein Koloss, ein gefürchteter Ort, hier ließen Stalins Geheimdienstchefs einst foltern und ermorden. Zum Kreml sind es nur wenige Hundert Meter.

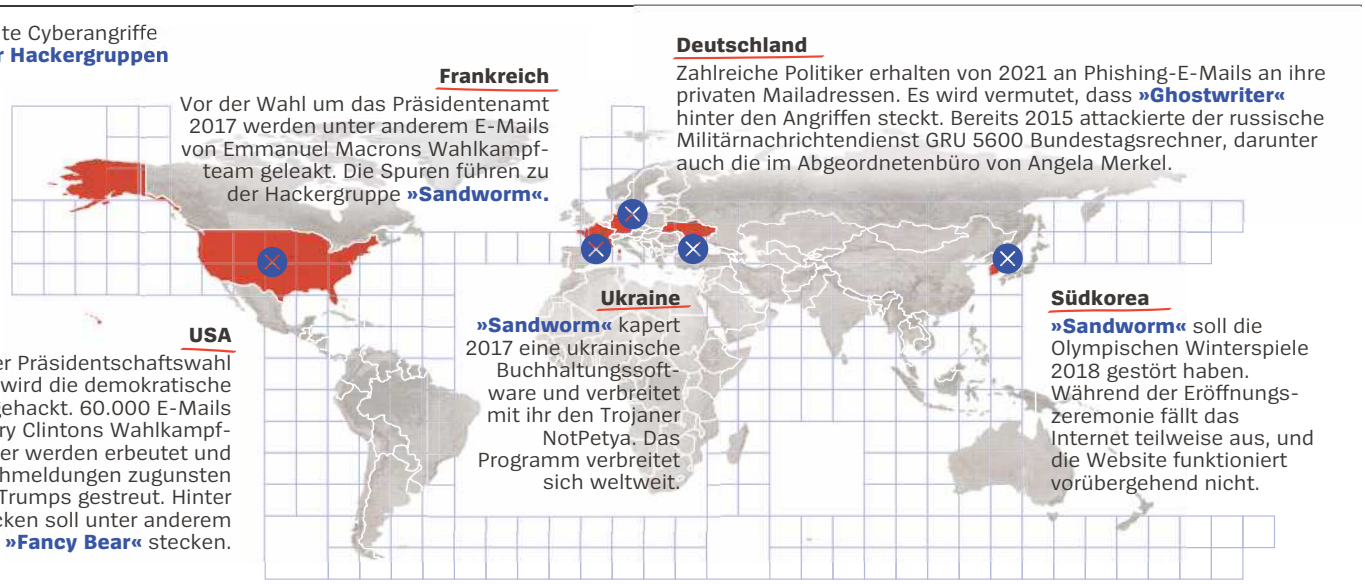
Die Vulkan-Mitarbeiter betreten das Reich des FSB in der Regel durch ein unauffälligeres Nebengebäude, so schildert es ein Teilnehmer der Treffen. Dort befinden sich die Büros des Zentrums für Informationssicherheit des FSB. Es ist eine der wichtigsten Hackerabteilungen des russischen Geheimdienstes. Die Vulkan-Leute tragen ihre Laptops durch eine lange Zugangsschleuse, mehrmals schließen und öffnen sich Sicherheitstüren, bevor ihre Papiere kontrolliert werden. Dann werden sie von FSB-Agenten abgeholt. Gemeinsam fährt man in die oberen Stockwerke. Dort führen die Vulkan-Leute stundenlang ihre Produkte vor, beantworten Fragen. Unterbrochen nur von einer Mittagspause mit ihren Auftraggebern in der Kantine des Lubjanka-Komplexes.

Beliebt waren die Besuche nicht bei allen Vulkan-Leuten, denn oft verlassen sie das Gebäude mit technisch unrealistischen Wünschen der Agenten.

Die Cyberpläne des Kreml sehen vor, nicht nur schnellstens immer mehr digitale Offensivwaffen zu entwickeln, sondern auch russische IT-Experten in deren Nutzung auszubilden. Darin ist auch Vulkan offenbar tief verstrickt: Die Firma entwickelte eigens ein Trainingsprogramm für die Staatshacker

Putins Schattenarmee

Ausgewählte Cyberangriffe
russischer Hackergruppen



Frankreich
Vor der Wahl um das Präsidentenamt 2017 werden unter anderem E-Mails von Emmanuel Macrons Wahlkampfteam geleakt. Die Spuren führen zu der Hackergruppe **»Sandworm«.**

Deutschland
Zahlreiche Politiker erhalten von 2021 an Phishing-E-Mails an ihre privaten Mailadressen. Es wird vermutet, dass **»Ghostwriter«** hinter den Angriffen steckt. Bereits 2015 attackierte der russische Militärnachrichtendienst GRU 5600 Bundestagsrechner, darunter auch die im Abgeordnetenbüro von Angela Merkel.

USA
Vor der Präsidentschaftswahl 2016 wird die demokratische Partei gehackt. 60.000 E-Mails von Hillary Clintons Wahlkampfleiter werden erbeutet und Falschmeldungen zugunsten Donald Trumps gestreut. Hinter den Attacken soll unter anderem **»Fancy Bear«** stecken.

Ukraine
»Sandworm« kapert 2017 eine ukrainische Buchhaltungssoftware und verbreitet mit ihr den Trojaner NotPetya. Das Programm verbreitet sich weltweit.

Südkorea
»Sandworm« soll die Olympischen Winterspiele 2018 gestört haben. Während der Eröffnungszeremonie fällt das Internet teilweise aus, und die Website funktioniert vorübergehend nicht.

S • Grafik

von morgen. In einem geleakten Dokument zu dem Geheimprojekt mit dem Codenamen »Crystal-2V« heißt es unverblümt, es gehe um ein »umfassendes Training von Spezialisten« im Bereich der »Informationskonfrontation«. So nennen die russischen Dienste ihren Cyberkrieg.

Bis zu 30 Nachwuchshacker sollen demnach mit »Crystal-2V« Angriffe auf kritische Infrastrukturen erlernen. Es gehe darum, »die Kontrollsysteme von Eisenbahn-, Luft- und Schiffstransport lahmzulegen« sowie die anderer »lebenswichtiger« Bereiche wie der Strom- und Wasserversorgung. Zudem sollen sie üben, die Zugänge zum globalen öffentlichen Informationssystem zu blockieren – gemeint ist offenbar das Internet. Derlei Angriffe auf Versorgungs- und Verkehrsadern und industrielle Kontrollsysteme gehören seit Jahren zu den Schreckensszenarien westlicher Geheimdienste.

Das ist längst mehr als Theorie: 2017 flog ein Angriff auf eine saudi-arabische Ölraffinerie auf. Russische Angreifer wollten die Sicherheitsmechanismen der Anlage mit einer Schadsoftware manipulieren. Vor einem Jahr machte die US-Justiz den GRU-Agenten Jewgenij Gladkich dafür verantwortlich und klagte ihn an. Offiziell arbeitete der mutmaßliche Hacker für ein Forschungsinstitut, das wiederum Vulkan mitfinanzierte.

Im Vulkan-Trainingsprogramm werden solche Angriffe genau beschrieben. Es geht um den »nicht autorisierten Zugang« zu kritischen Netzen, ums »Aufspüren von Schwachstellen« von Opfern. Ein weiteres Unterrichtsmodul lehrt Denial-of-Service-Attacken, um den Zugang zu Internetangeboten zu blockieren. Das alles sollen die Rekruten anhand von theoretischen Lehrgängen, aber auch in Laborsimulationen erlernen.

Vulkan trainiert nicht nur die nächste Generation der Cyberkrieger, sondern will ihnen auch neue Waffen in die Hand geben. Dazu haben die Vulkan-Programmierer »Scan-V« entwickelt. Mit dem System sollen Cyberangriffe deutlich leichter zu planen sein. Denn oft dauert es Wochen oder Monate, eine Attacke vorzubereiten. Die Ziele müssen erst umfassend ausgeforscht werden: Wie ist das IT-Netzwerk aufgebaut? Welche Betriebssysteme sind installiert, und wo sind diese anfällig?

»Scan-V« soll laut den geleakten Dokumenten diese Schritte automatisieren. Anschließend werden die Informationen ausgewertet und Vorschläge gemacht, wie Angriffe aussehen könnten.

Das erinnere sie an »alte Militärfilme«, sagt Gabby Roncone von der IT-Sicherheitsfirma Mandiant. Da stünden Militärs um eine Landkarte herum und verschöben Truppen auf dem Tisch. Sie versuchten, sich klarzumachen, »wo sie zuerst zuschlagen müssten, um die feindlichen Linien zu durchbrechen«. »Scan-V« wird demnach von Experten als offensiv eingestuft. Gemacht vor allem für Hackereinheiten, die oft und in großem Stil attackieren. Und dabei noch schlagkräftiger werden wollen. Im Mai 2020 plant ein Vulkan-Team den Besuch bei einem der wichtigsten Kunden.

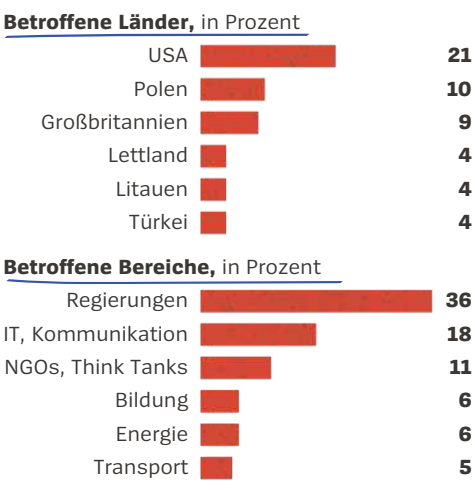
Die Reise geht nach Chimki, eine Industriestadt vor den Toren Moskaus. »Teilt bitte vorher eure Passdaten mit«, schreibt Scan-Projektleiter Oleg N. am 27. Mai in einer E-Mail an seine Leute. Das Gelände sei besonders gesichert, die Zugangskontrolle strikt. Das Meeting findet wohl statt in einem 20-stöckigen, Hochhaus am Ufer der Moskwa. Westliche Sicherheitsbehörden kennen es gut.

Es taucht sogar in einer Anklageschrift aus dem Jahr 2018 auf, die weltweit Furore machte. Sie beruht auf den Untersuchungen des Sonderermittlers Robert Mueller über die russische Einflussnahme auf den US-Wahlkampf 2016. In dem Dokument wird das Hochhaus in Chimki »The Tower« genannt, der Turm. Die Einheit des Militärgeheimdienstes GRU, die hier ihren Sitz hat, soll daran beteiligt gewesen sein, das Wahlkampfteam von Hillary Clinton auszuspionieren, und Donald Trump zum Sieg verholfen haben. Offiziell sind die Militär-Hacker nach ihrer Feldpostnummer benannt: Einheit 74 455. Besser bekannt sind sie unter ihrem Codenamen: »Sandworm«. Die berüchtigtsten Cybersoldaten der Welt.

Viele der spektakulärsten Hacks und Cyberangriffe des vergangenen Jahrzehnts werden den Hackern hinter den verspiegelten Glasfronten des Towers zugeschrieben. Ihr neuer mutmaßlicher Chef, Jewgenij Serebriakow, wirkt auf seinem Passfoto eher milchgesichtig. Vor ein paar Jahren flog er in Den Haag auf, als er mit drei Kollegen versuchte, die Chemiewaffen-Kontrollorganisation

Attacken überall

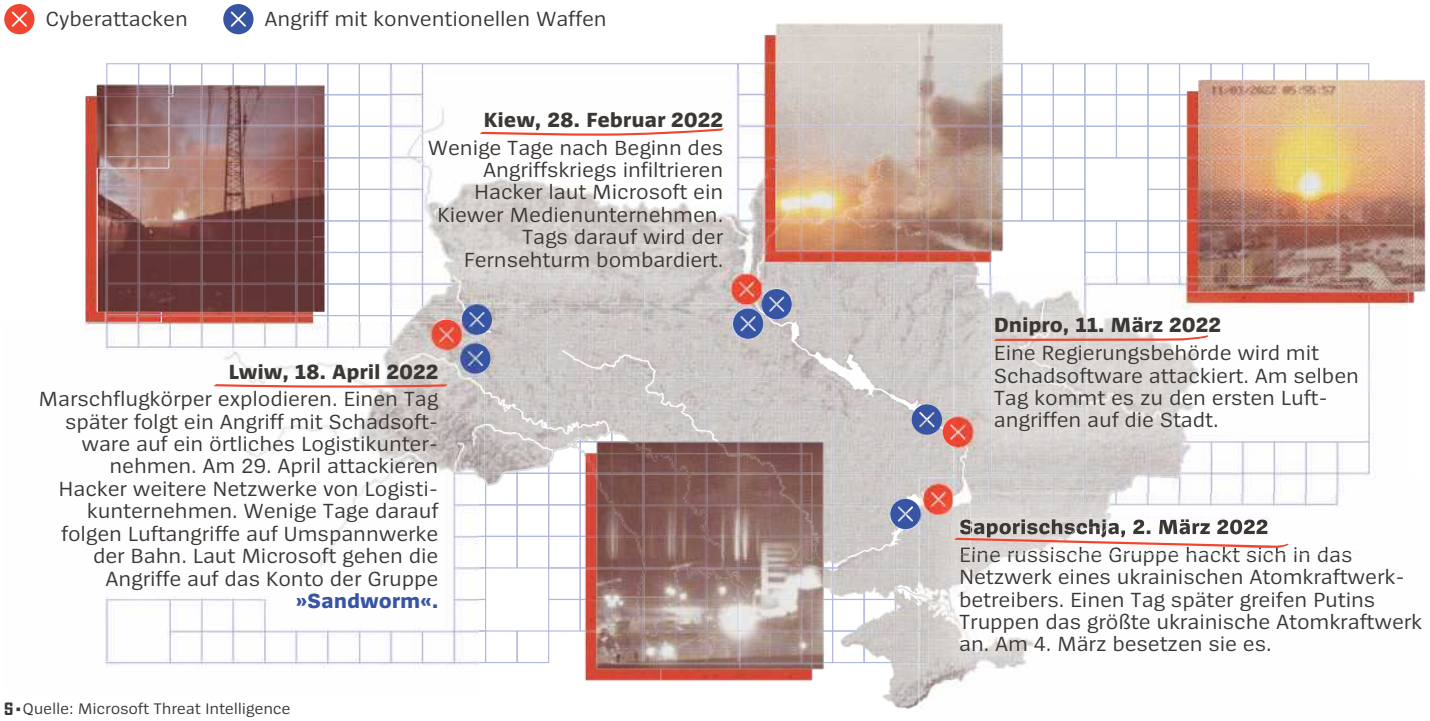
Microsoft hat seit dem 23. Februar 2022 **279 mutmaßlich russische Hackerangriffe** außerhalb der Ukraine dokumentiert.



S • Quelle: Microsoft Threat Intelligence, Stand: 7. Feb. 2023, an 100 fehlende Prozent: andere Länder und Bereiche

Digitaler Beschuss

Ausgewählte russische Cyberattacken in Kombination mit konventionellen Waffen in der Ukraine 2022



5 • Quelle: Microsoft Threat Intelligence

OPCW zu attackieren. Die Niederländer ertappten die vier Spione auf frischer Tat, stellten ihre Laptops und Mobiltelefone sicher und verwiesen sie des Landes.

Der weiteren Karriere von Serebriakow war der peinliche Zwischenfall nicht abträglich. Hochrangige Beamte, die sich schon lange mit russischen Geheimdiensten beschäftigen, überrascht das nicht. Die Demonstration von Stärke und Entschlossenheit nach außen ist in Moskau mitunter wichtiger als der Erfolg einer Operation. Russland überschreite bewusst Grenzen, um Gegner zu verängstigen, so ein Nachrichtendienstler. Oft seien russische Hacker nicht sehr vorsichtig, wenn sie angriffen. »Vielleicht war die Attacke gar nicht so ausgefeilt und führte nicht zum Ziel. Aber das ist fast schon egal. Die Botschaft ist: Wir drohen nicht nur, wir machen auch.« Breitbeinigkeit zur Abschreckung.

Das gilt insbesondere für die GRU, den brachialsten der russischen Geheimdienste. Etwa 37 000 Leute arbeiten dort, darunter 25 000 Speznaz-Elitesoldaten. Und nach Einschätzung westlicher Sicherheitsbehörden mehrere Tausend Hacker. »Wirkung vor Deckung«, so könne man die Strategie der GRU beschreiben, sagt ein Spionageexperte. Nicht aufzufliegen sei im Zweifel zweitrangig. Das GRU-Arsenal der »aktiven Maßnahmen« reicht von Sabotage über Subversion und Desinformation bis zu Attentaten. Ihr Ziel: Chaos stiften und die Demokratien des Westens zersetzen.

Spektakulär und unerbittlich sind insbesondere die Angriffe der GRU-Einheit »Sandworm« auf ukrainische Ziele, die seit rund zehn Jahren andauern. So gelangen den russischen Hackern jeweils kurz vor Weihnachten in den Jahren 2015 und 2016 Angriffe auf die Stromversorgung. Es waren weltweit die ersten durch Cyberangriffe herbeigeführten Blackouts. Eine Machtdemonstration.

Wenige Monate später startete Moskau einen Angriff, der als folgenreichster Hack aller Zeiten gilt. Die Angreifer missbrauchten eine populäre ukrainische Steuersoftware, um ein Schadprogramm namens »NotPetya« in die Welt zu setzen. Das breitete sich rapide aus, verschlüsselte befallene Rechner und machte sie unbrauchbar. Weil multinationale Firmen betroffen waren, wirkte es schnell über die Landesgrenzen der Ukraine hinaus – und bald weltweit. Konzerne wie der Logistikgigant Maersk oder der Kosmetikriese Beiersdorf mussten ihre IT erneuern. Global wird der Schaden auf mindestens zehn Milliarden Dollar geschätzt.

Derzeit attackieren die Russen ukrainische Firmen und Behörden mit »Wiper«-Angriffen: destruktiven Schadprogrammen, die darauf abzielen, die infizierten Rechner unbrauchbar zu machen. Bei einer im Januar aufgeflogenen Operation gegen die nationale Nachrichtenagentur Ukrinform schleuste »Sandworm« gleich fünf dieser Programme ein.

Nach Einschätzung mehrerer IT-Sicherheitsexperten und westlicher Nachrichtendienstler, die der SPIEGEL befragen konnte, wäre »Scan-V« ein geeignetes Aufklärungswerkzeug, das zur Vorbereitung solcher Angriffe eingesetzt werden könnte. Ob die GRU tatsächlich »Scan-V« nutzt oder eingekauft hat, lässt sich nicht mit Sicherheit belegen. Die GRU-Hacker haben aber offenbar die Entwicklung dieses Cyberwerkzeugs begleitet. Ein klares Indiz dafür findet sich in einem elf Seiten langen Dokument voller Fachsimpeleien zu Prozess-Systemen und Datenverarbeitung. Es ist offenbar ein Protokoll zu »Scan-V«, so steht es auf dem Deckblatt. Es geht um den »Datenaustausch zwischen den Subsystemen PU-L, PSAP, Scan-AS«. Links oben prangt eine Notiz: »Genehmigt Vertreter Militäreinheit 74455«. Die »Sandworm«-Truppe.

Dazu passt, dass die Werkzeuge von Vulkan über Jahre verfeinert wurden – und einer ihrer Mitarbeiter schon vor zehn Jahren an einem globalen Angriff einer der besten russischen Hackergruppen beteiligt war. Das zeigt eine Analyse von Google, die der SPIEGEL nun erstmals öffentlich macht.

»MiniDuke« tauften Forscher die damalige Kampagne, in deren Verlauf staatliche Rechner in Ländern wie Deutschland, den USA und der Ukraine angegriffen wurden. Das Ziel der Hacker: geheime Informationen aus Behördennetzen stehlen. Mindestens drei westliche Regierungsvertreter wurden erfolgreich gehackt, weit mehr als 100 Server weltweit infiziert, so IT-Sicherheitsexperten. Hinter den Angriffen steckte die Gruppe »The Dukes«, auch bekannt als »Cozy Bear« – zuzuordnen Moskaus Auslandsgeheimdienst SWR. Später hackten die Agenten das Pentagon.

Ende 2012 identifizierte Google eine E-Mail-Adresse, die man später »MiniDuke« zuschreiben konnte. »Wir beobachteten, dass diese Mail-Adresse eine Testnachricht an eine

E-Mail-Adresse von NTC-Vulkan.ru sendete«, so ein Firmensprecher. Mit solchen Testnachrichten prüfen Angreifer üblicherweise, ob die Spamfilter von Google ihre Viren oder Hacking-Werkzeuge erkennen. Die Tests waren erfolgreich, denn später verschickten die Angreifer von derselben Adresse aus tatsächlich jene Schadsoftware, die als »MiniDuke« um die Welt ging. Diplomaten, Beamte oder Militärangehörige zahlreicher westlicher Länder bekamen maßgeschneiderte E-Mails aus Moskau. Wer die Dateien öffnete, infizierte seinen Rechner.

Dass Google überhaupt eine Spur von »MiniDuke« zu Vulkan ziehen konnte, liegt an einem Fehler der Hacker: Sie nutzten dieselbe IP-Adresse, um einen Kontrollserver anzumieten, mit der sie auch den Google-Account zum Verschicken der Schadsoftware registriert hatten. »Das war nicht besonders schlau, definitiv ein Ausrutscher«, sagt ein IT-Sicherheitsexperte von Google dazu. Der Konzern sperrte die E-Mail-Adresse. Die globale Hacking-Kampagne jedoch ließ sich nicht mehr stoppen.

Solche frühen Erfolge dürften dazu beigetragen haben, dass Vulkan offenbar über Jahre finanziert wurde, seine Fähigkeiten weiterzuentwickeln. Immer wieder erhielt die Firma Ratenzahlungen, insgesamt mehrere Millionen Euro, von Instituten, die den russischen Geheimdiensten und dem Militär nahestehen. In mehr als 17 000 Überweisungsvorgängen der Firma Vulkan, die dem internationalen Rechercheteam vorliegen, werden die Systemnamen »Scan-V«, »Amezit« und »Crystal-2V« regelmäßig als Zahlungsgrund genannt.

Es liegt zudem nahe, dass die russischen Hacker dringend nach Möglichkeiten suchen, ihre massiven Cyberattacken noch effizienter zu machen. Die Ukraine treffen Angriffe schon jetzt fast täglich. Oft sehen sie aus wie am 28. März 2022.

An diesem Morgen seines 40. Geburtstags wird Kyrylo Hontscharuk vom Klingeln seines Handys geweckt. Es ist kein Gratulant, sondern ein aufgeregter Mitarbeiter seiner Firma. Hontscharuk ist Chief Information Officer (CIO) des ukrainischen Internetanbieters Ukrtelecom. Seit Kriegsbeginn hat er mit einer Hackerattacke gerechnet, nun ist es so weit. Die Angreifer haben es geschafft, das Konto eines Mitarbeiters zu infiltrieren. Sie dringen in das interne System der Firma ein, verschaffen sich Administratorenrechte, haben damit die Möglichkeit, Programmiercodes zu ändern.

74 455

lautet die Feldpostnummer der gefährlichsten Hackertruppe der Welt: »Sandworm«.

Hören Sie hier
▸»Putins Krieg im Netz«, einen SPIEGEL-Original-Podcast

Hontscharuk weiß: Wenn die Hacker weiter vorrücken, können sie auch die Rechner der ukrainischen Behörden und der Armee erreichen.

Hontscharuk sieht nur eine Chance. Er muss Server vom Netz nehmen, um bleibenden Schaden zu verhindern. Aber er muss Hunderttausenden Ukrainerinnen und Ukrainern die Verbindung kappen. Viele sitzen in Bunkern, erfahren nur über das Internet, wo und wie die russische Armee vorrückt, was mit ihren Angehörigen geschieht.

Bis zum nächsten Tag arbeitet Hontscharuks Team daran, die Saboteure auszusperren. »Noch mal sollte ein solcher Angriff jetzt nicht mehr möglich sein«, sagt Hontscharuk. »Einen hundertprozentigen Schutz gibt es aber nicht.«

Die russischen Cybersoldaten zielen nicht nur auf vermeintliche Feinde im Ausland. Zunehmend richten sie ihre Waffen auch nach innen. Putins Russland ist längst zu einem Geheimdienststaat geworden. Unter dem Ex-KGB-Offizier stiegen die »Silowiki«, seine Vertrauten aus der zwielichtigen Agentenwelt, zum neuen Adel auf. Die Bedeutung dieser Blase für Putin, so erzählen es hochrangige westliche Sicherheitsexperten, sei kaum zu überschätzen.

Die alten Seilschaften sollen seine Macht sichern. Dem Westen traue Putin nicht, sagt ein Geheimdienstler, dem eigenen Volk aber vielleicht noch weniger. Deshalb sollen Putins Dienste heute möglichst alles wissen, sammeln, speichern, egal ob die Information gerade gebraucht wird oder nicht.

Auch dabei hilft Vulkan. Im Auftrag des FSB entwickelten die Software-Ingenieure eine Spionagesoftware, um die russische Bevölkerung zu kontrollieren. Codename: »Fraction«. Das Ziel: automatisierte Überwachung von Online-Aktivitäten. »Ein System«, so steht es in den Dokumenten, »um Aktionen in sozialen Netzwerken zu monitoren und zu identifizieren«. Ein »Big Brother« im Netz, der Social-Media-Posts auf verdächtige Inhalte scannt und diese sichert. So lässt sich filtern, wer kritisch über Putin schreibt.

Unterdrückungsinstrumente gegen die eigenen Landsleute zu bauen behagt nicht allen Vulkan-Mitarbeitern. Für manche ist damit eine Grenze überschritten. Als er von der Zusammenarbeit mit den Geheimdiensten in diesem Bereich erfahren habe, sei für ihn klar geworden, »dass ich dieses Regime nicht unterstützen möchte«, sagt Jewgenij. Es ist nicht sein richtiger Name. Mehrere Jahre hat er für Vulkan gearbeitet, inzwischen lebt er im Westen. Wo genau, muss zu seinem Schutz geheim bleiben, auch woran er gearbeitet hat, darf nicht verraten werden.

Jewgenij ist einer der mehr als 90 aktuellen und ehemaligen Vulkan-Mitarbeiter, die im Laufe der »Vulkan Files«-Recherche kontaktiert wurden. Ein stiller IT-Nerd und das Gegenteil der militärischen Machos, als die er die beiden Firmengründer beschreibt: »Vor denen hatte ich immer ein bisschen Angst.« Die Arbeit aber habe »Spaß« gemacht. Der Alltag sei wie bei einem Start-up gewesen, die Bezahlung überdurchschnittlich.

Die Vulkan-Großraumbüros verströmen zwar den biederen Charme einer Versicherungsagentur, brauner Teppich auf dem Boden, gelbe Wände. Doch die Stimmung sei locker gewesen, sagt Jewgenij, der Umgang freundschaftlich. Nach einer Feier hätten Kollegen etwa die offenen Schnapsflaschen mitgenommen, um gemeinsam weiterzutrinken. Auf Firmenausflügen wird gemeinsam geangelt. Oder mit Panzern über einen Übungsplatz gejagt. Putin wird schon mal als »Großvater aus dem Bunker« verspottet. Sogar über den Einmarsch auf der Krim diskutieren sie bei Vulkan, manche Mitarbeiter sind dagegen.

Erst nach und nach wird Jewgenij klar, woran die Firma auch arbeitet. Die immer rabiateren Methoden des russischen Regimes ließen Jewgenij schließlich zum Kremlgegner werden, zum Nawalny-Anhänger. »Totale Überwachung von Aktivisten darf es in einem modernen Land nicht geben«, sagt er. Inzwischen hat er sich ein Leben im Westen aufgebaut. In seine Heimat möchte Jewgenij nicht mehr zurückkehren: »Dieses Regime ist ein Polizeistaat, und eine der Säulen dieses Staats sind Unternehmen wie Vulkan.«

Seine ehemaligen Kollegen machen weiter. Die russische Cyberkriegsmaschine verlangt nach immer mehr Soldaten, nach immer mehr Waffen. Für »Sandworm« und »Cozy Bear«, für Vulkan und all die anderen Cybersöldner scheinen goldene Zeiten angebrochen.

Denn für Putin und sein Militär ist das Internet nicht das Schlachtfeld der Zukunft, sondern das der Gegenwart.

Nikolai Antoniadis, Sophia Baumann, Christo Buschek, Maria Christoph, Jörg Diehl, Christo Grozev, Roman Höfner, Max Hoppenstedt, Carina Huppertz, Dajana Kollig, Roman Lehberger, Hannes Munzinger, Frederik Obermaier, Bastian Obermayer, Fedir Petrov, Alexandra Rojkov, Marcel Rosenbach, Thomas Schulz, Hakan Tanriverdi, Wolf Wiedmann-Schmidt ■