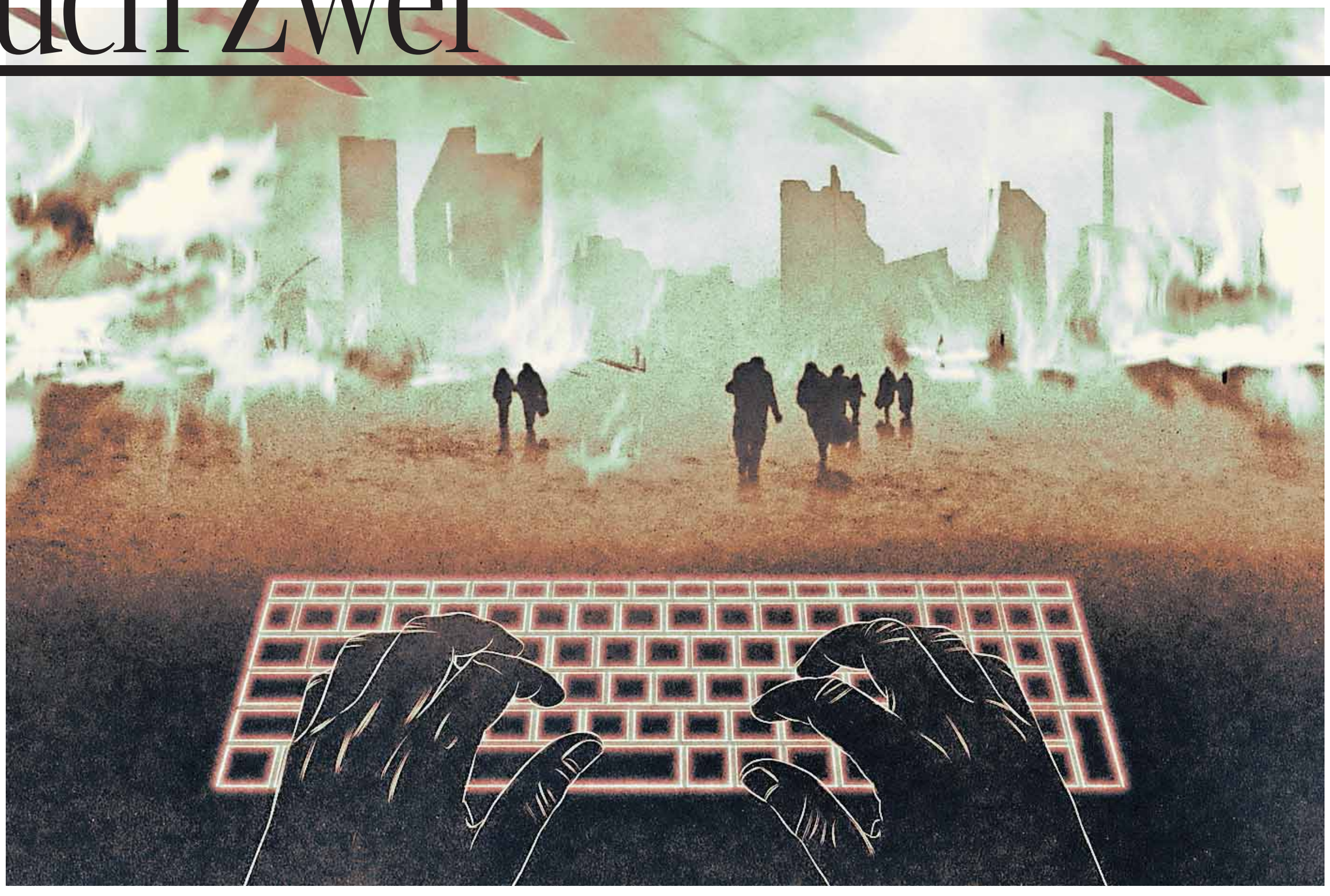
Buch Zwei



Im Netz der Krieger

Russland verschiebt die Grenzen in Europa mit Panzern und Granatendonner. In der digitalen Welt aber greift der Kreml leise und unsichtbar die Freiheit an. Einblicke in die Waffenkammer von Putins Cyberarmee – die Vulkan Files

Text von Christoph Cadenbach, Ben Heubl, Lena Kampf, Georg Mascolo, Mauritius Much, Max Muth, Natalie Sablowski, Lea Weinmann und Ralf Wiegand; Illustrationen von Isabel Seliger/sepia

Die Panzer sind vor wenigen Tagen über die Grenze gerollt, russische Truppen stehen schon kurz vor Kiew, als eine verschlüsselte Nachricht das Investigativteam der Süddeutschen Zeitung erreicht. Sie sei wütend über die Invasion in der Ukraine „und auch über die schrecklichen Dinge, die dort geschehen“, schreibt eine Person, die nichts über ihre Identität verrät. Deshalb habe sie sich dazu entschieden, „Informationen öffentlich zu machen“. So kündigen Whistleblower ein Leak an, in diesem Fall: ein Datenleck aus der Rüstungsindustrie für den Cyberkrieg.

Die Dokumente, die die Person dann über Wochen hinweg der SZ übermittelt, berühren russische Staatsgeheimnisse. Es sind interne Unterlagen einer IT-Firma, die – den Dokumenten zufolge – drei russische Geheimdienste mit Software belieferte, mit Waffen für einen Krieg, in dem Kraftwerke nicht bombardiert, sondern gehackt werden. Die Menschen von Energie- und Kommunikationsnetzen abzuschneiden, heißt, sie vom Leben abzuschneiden. Sie sollen frieren, verstummen, verzweifeln.

„Die Firma tut falsche Dinge“, schreibt die Quelle. „Die Menschen sollten wissen, welche Gefahren das birgt.“

Die Firma: Das ist das russische IT-Unternehmen NTC Vulkan. Von außen betrachtet wirkt Vulkan wie ein gewöhnliches, junges Tech-Unternehmen, Sitz im Nordosten von Moskau, 135 Mitarbeiter, 13,6 Millionen Euro Umsatz im Jahr 2021. Auf seiner Internetseite wirbt Vulkan damit, für bedeutende Kunden gearbeitet zu haben, auch für westliche Konzerne. Autoindustrie, Hightech-Branche, Banken, alles dabei. Vulkan bietet nach eigenen Angaben vor allem Lösungen für die Cybersicherheit an, zum Beispiel den Schutz von Firmennetzwerken vor Angriffen von außen, Firewalls, die sensible Daten schützen sollen wie eine Rüstung.

Aber Vulkan spielt ein doppeltes Spiel. Denn gleichzeitig entwickelt die Firma Werkzeuge, die Schwachstellen in solchen Rüstungen aufspüren sollen – damit Hacker im staatlichen Auftrag ihre Gegner attackieren können. Der Cyberkrieg spielt sich meistens hinter einer Mauer aus Konjunktiven ab, was könnte da nicht alles passieren, wenn jemand die Lebensadern der Gesellschaften von heute angriffe. Aber was passiert wirklich? In wessen Auftrag? Mit welchem Ziel?

Das Vulkan-Leak bohrt zumindest ein kleines Loch in diese Mauer. Und durch das kann man sehen, was verborgen bleiben sollte: wie Russland um Waffenhoheit im weltweiten Informationskrieg ringt.

„Ein Leak, das so eng an den Diensten ist und Rückschlüsse auf ihre Fähigkeiten erlaubt, ist neu.“

Kein Land hat zuletzt so viele verheerende Angriffe auf dem digitalen Schlachtfeld ausführen lassen wie Russland. Kein Land war so oft Ziel dieser Angriffe wie die Ukraine.

Hacker attackierten das ukrainische Finanzministerium, die staatliche Eisenbahngesellschaft und Energieversorger. Bereits 2015, im Jahr nach der Annexion der Krim, provozierten sie mit einem Schadprogramm namens Black Energy einen Stromausfall, von dem rund 700 000 Menschen in der Ukraine betroffen waren, stundenlang. 2017 wurde eine ukrainische Buchhaltungssoftware mit dem Trojaner NotPetya attackiert, der wenig später Computersysteme auf der ganzen Welt infizierte. Geldautomaten in der Ukraine funktionierten nicht mehr, und Containerschiffe der dänischen Reederei Maersk standen still, weil die digitalen Systeme versagten. Der wirtschaftliche Schaden allein dieses Angriffs wird auf rund neun Milliarden Euro weltweit geschätzt. Er gilt als der verheerendste in der Geschichte. Und er hat sehr deutlich gemacht, was ein digitaler Krieg anrichten kann – ohne dass eine einzige Rakete explodiert.

Auch hinter Angriffen auf den Deutschen Bundestag 2015 und auf die US-Präsidentschaftswahl 2016 soll Russland gestanden haben. Westliche Geheimdienste sind sich da einig, auch wenn die Spuren oft verschwommen sind und der Cyberkrieg leise und unsichtbar ist.

Wer hinter solchen Angriffen steht, lässt sich, wenn überhaupt, oft nur durch aufwendige forensische Spurensuche nachvollziehen oder durch Fehler der Angreifer. Die Unterlagen aus dem Inneren des Moskauer Tech-Betriebs sind auch deshalb außergewöhnlich, weil sie erstmals einen präzisen Eindruck vermitteln, wie Russland Cyberangriffe plant und vorbereitet. „Ein Leak, das so eng an den Diensten ist und Rückschlüsse auf ihre Fähigkeiten erlaubt, ist neu“, lässt sich ein westlicher Geheimdienst zitieren.

Die Dokumente, sie stammen aus den Jahren 2016 bis 2021, sind zunächst der SZ und später auch dem Investigativ-Startup Paper Trail Media zugespielt worden, das die Zusammenarbeit eines internationalen Rechercheteams koordiniert hat. Medien wie der *Spiegel*, die *Washington Post* und der *Guardian* veröffentlichen die Ergebnisse unter dem Titel Vulkan Files.

Die Moskauer IT-Firma ist nur eine von vielen in Russland. Mehr als ein Dutzend davon halten die USA für so relevant, dass sie sie mit Sanktionen belegt haben, die internationale Geschäfte zumindest erschweren sollen. Vulkan gehört bisher nicht dazu. Und Cyberattacken sind auch keine Erfindung Russlands. Im Juni 2013 hatte der Whistleblower Edward Snowden enthüllt, wie Hacker des größten US-Auslandsgeheimdienstes NSA auf der ganzen Welt Netze infiltrieren und amerikanische sowie britische Behörden digitale Kommunikation systematisch filtern und überwachen. Auch das Handy der damaligen deutschen Kanzlerin Angela Merkel war ein Ziel: Spionage unter Freunden ging gar nicht.

Längst wird auf höchster Ebene über einen digitalen Nichtangriffspakt diskutiert. Als im Sommer 2021 US-Präsident Joe Biden und der russische Präsident Wladimir Putin zum bisher einzigen Gipfel in Genf zusammenkamen, beklagte Putin „Attacken aus dem Cyberraum der USA“, etwa auf das Gesundheitssystem seines Landes. Biden seinerseits warf dem Kreml vor, hinter Angriffen auf Behörden und die Energieversorgung in den USA zu stecken und Cyberkriminelle, die Unternehmen mittels sogenannter Ransomware-Software erpressten, zu schützen. Der Amerikaner wünschte sich, Ziele zu definieren, die für solche Attacken tabu seien; der Russe verwahrte sich gegen Unterstellungen und empfahl, man solle sich auf Expertenebene „hinsetzen und im Interesse der USA und Russlands zu arbeiten beginnen“.

Graue Fassade, mächtige Freunde: Vulkan in Moskau. FOTO: GOOGLE MAPS

Im Sommer 2021 reden Biden und Putin über digitale Waffen. Genug davon haben beide

Aber die digitale Rüstungsspirale drehte sich weiter wie eh und je. Auch davon erzählen die Vulkan Files: Sie zeigen, wie der russische Staat die Fähigkeiten privater Entwickler für seine Zwecke nutzt.

Hinter Vulkan, schreibt die Quelle, „verstecken sich der GRU und der FSB“ – Russlands Militär- und Inlandsgeheimdienst. Es sind mächtige und skrupellose Organisationen, die Staatsfeinde nicht nur aufspüren, sondern auch beseitigen, wenn sie es für nötig halten. Der GRU soll den in den Westen übergelaufenen Ex-GRU-Oberst Sergej Skripal lebensgefährlich vergiftet haben. Und der FSB gilt als Drahtzieher des sogenannten Tiergartenmordes, der Erschießung eines tschetschenischen Separatistenkämpfers im August 2019 mitten in Berlin. Als Täter hat das Kammergericht Berlin Ende 2021 den mutmaßlichen FSB-Agenten Wadim N. Krassikow zu lebenslanger Haft verurteilt. In den geleakten Unterlagen finden sich außerdem Hinweise auf geschäftliche Beziehungen Vulkans zur Militäreinheit 33949, die dem Auslandsgeheimdienst SWR zugerechnet wird.

Vulkan ist eine Firma mit mächtigen Freunden, und die Quelle ist sich der Gefahr bewusst. Sie habe ihr bisheriges Leben zurückgelassen, schreibt sie, und lebe nun „wie ein Geist“.

Zu den Dokumenten, die dieser Geist geteilt hat, gehören interne E-Mails, Verträge, Handbücher und Skizzen, mehr als 5000 Seiten insgesamt. Fünf westliche Geheimdienste, denen Auszüge daraus gezeigt wurden, halten sie für authentisch, ebenso wie zahlreiche Expertinnen und Experten von Cybersicherheitsfirmen. Die Softwaresysteme, die darin beschrieben werden, können als Überwachungs- und Spionagemaschinen eingesetzt werden. Als Waffen gegen Regime-Kritiker zum Beispiel. Mit anderen ließen sich Cyberangriffe systematisch vorbereiten.

Einige Dokumente beschreiben ein Trainingsseminar, bei dem Hacker lernen sollen, wie sie kritische Infrastruktur attackieren, Eisenbahnnetze oder Kraftwerke zum Beispiel. Etliche Dokumente zeigen Pläne für ein System, das gesamte Regionen vom freien Internet abschneiden und mit Propaganda fluten könnte. Es wäre eine neue Stufe der Eskalation im russischen Informationskrieg.

Dessen Wert hat die russische Regierung längst erkannt. Schon 2015 sagte Verteidigungsminister Sergej Schojgu: „Ein Wort, eine Kamera, ein Foto, das Internet und Informationen im Allgemeinen sind nur eine andere Art von Waffe. Ein weiterer Teil der Streitkräfte.“ Dass die von Vulkan entwickelten Cyberwaffen auf dem digitalen Schlachtfeld tatsächlich eingesetzt werden, beweisen die Dokumente nicht. Aber sie belegen, dass Programme zumindest getestet wurden. Eine deutliche Spur führt dabei von Vulkan auch zu einer russischen Hackergruppe, deren Name fast immer fällt, wenn besonders verheerende Cyberangriffe geschehen: Sandworm.

Das US-Justizministerium hält sie für die weltweit „zerstörerischste“ staatliche Hackergruppe, bis zu zehn Millionen Dollar Belohnung zahlt die US-Ragierung für Informationen über Sandworm.

Private IT-Firmen spielen bei der digitalen Aufrüstung der russischen Streitkräfte nach Ansicht von Wiktor Schora, dem Leiter der staatlichen Cyberabwehr in der Ukraine, eine wichtige Rolle. Er spricht

▸ *Fortsetzung auf der nächsten Seite*

› *Fortsetzung von Seite 11*

von einem „Ökosystem“, das von der Regierung und dem Militär, von Cyberkriminellen und kommerziellen Unternehmen gefüttert werde. Auch Vulkan hat von den staatlichen Aufträgen offenbar gut gelebt. Finanzdaten zeigen, dass allein der Auslandsgeheimdienst von 2019 bis 2022 umgerechnet etwa 2,5 Millionen Euro an Vulkan überwies.

Wiktor Schora möchte über NTC Vulkan öffentlich nicht sprechen. Ebenso wenig wie der ukrainische Inlandsgeheimdienst SBU, der allerdings bestätigt, das Unternehmen zu kennen. Auch fünf westliche Geheimdienste, die nicht namentlich genannt werden wollen, tun das. Es seien „Firmen wie Vulkan“, sagt einer, „die dem GRU helfen, ihre Cyberangriffe auszuführen“.

Vulkan hat auf mehrere schriftliche Anfragen der an der Recherche beteiligten Medien nicht reagiert. Eine Mitarbeiterin bestätigte jedoch am Telefon, dass die Firma die Fragen per Mail erhalten habe. Sie habe sie an die Chefs weitergeleitet. Die würden sich melden, „wenn die E-Mail für sie von Interesse ist“. Dies geschah bis Redaktionsschluss nicht. Auch der Kreml antwortete nicht.

Vulkans Firmensitz liegt in einem Gewerbegebiet im Nordosten von Moskau. Auf Google Street View sieht man ein schmuckloses, mehrstöckiges Bürogebäude gegenüber einer Schwimmhalle. Zur Nachbarschaft gehören ein Sicherheitsdienst, ein Tonstudio und ein Süßwarengeschäft namens „Mon Bon“.

Ein Video, das Vulkan im Februar auf Youtube veröffentlichte, soll die Büros von innen zeigen. Helle Wände, sanftes Deckenlicht. Auf den Schreibtischen stehen riesige Flachbildschirme, davor sitzen Menschen auf rückenschonenden Bürostühlen.

Es sind vor allem Männer, kaum einer wirkt älter als 40, alle lächeln. Der Film soll neue Mitarbeitende anwerben und könnte so auch von einer IT-Firma in München inszeniert worden sein. Eine modern eingerichtete Küche ist zu sehen, ein Fitnessraum mit Laufband, eine Tischtennisplatte und ein Labor.

Was NTC Vulkan zu sein vorgibt: eine Firma, die dazu da ist, „die Welt zum Besseren zu verändern“

Dort beugt sich eine junge Frau über ein Mikroskop, um an einer Platine zu löten. Im Hintergrund läuft mitreißende Piano- und Geigenmusik wie in einer Hollywoodromanze. Eine Männerstimme aus dem Off fragt: „Warum gerade Vulkan?“ – und gibt die Antwort dann selbst: wegen des Teams und des komfortablen Arbeitsumfelds. „Und, am allerwichtigsten“, sagt die Stimme, um „die Welt zum Besseren zu verändern“.

Wie es in dem Unternehmen tatsächlich aussah, haben ehemalige Mitarbeitende beschrieben. „Die Arbeit hat Spaß gemacht“, sagt einer, weil sie bei Vulkan mit der neuesten Technologie gearbeitet und auch öfters gemeinsam gefeiert hätten. Bei einem Neujahrsessen lud die Chefetage ihre Belegschaft in ein teures Restaurant ein, dort gab es Pancakes, Blini und gebratenen Lachs. Bei einem Firmenausflug wurde geangelt, bei einem anderen durften die Mitarbeiter Panzer fahren und mit Maschinengewehren schießen.

Von mehr als 90 Personen, die Reporterinnen und Reporter anschrieben, anriefen oder zu Hause besuchten, ist dieser Mitarbeiter einer der wenigen, die reden wollten. Viele legten auf, sobald der Name der Firma fiel. Andere verlangten Geld, bevor sie sprechen würden. Auch diese Gespräche endeten dann schnell.

Vulkan sei eine „normale IT-Firma“, behaupteten manche. Ein Ex-Mitarbeiter sagte hingegen: „Vulkan ist eine Organisation mit doppeltem Boden. Dort gibt es einen Bereich für die Vitrine, für die Leute zum Gucken – und das, was sich im Inneren tatsächlich abspielt. Darüber wissen nur Einzelne Bescheid.“

Zu diesen Insidern innerhalb der Firma gehören fünf Mitarbeiter, die am 27. Mai 2020 eine E-Mail von ihrem Projektmanager erhalten. Sie findet sich in den geleakten Unterlagen – und sie lässt hinter die Fassade von Vulkan blicken. „Chimki ist Sperrgebiet, die Regeln sind streng“, schreibt der Projektmanager und fordert seine Mitarbeiter in einer weiteren Mail auf, ihm ihre Geburtsdaten und aktuellen Adressen zu schicken. Offenbar für einen Sicherheitscheck vor einem Besuch in Chimki, einem Vorort von Moskau. Dort residiert die Einheit 74455 des Militärgeheimdiensts GRU in einem modernen Hochhaus aus Glas und Stahl am Ufer des Moskau-Wolga-Kanals, das nur „der Turm“ genannt wird. Im Westen ist diese Einheit 74455 besser bekannt als Sandworm.

Die fünf Vulkan-Mitarbeiter sollen also offenkundig die berüchtigtste russische Hackergruppe besuchen, weil es, den E-Mails zufolge, dort für ein von Vulkan entwickeltes Softwaresystem namens Skan einen Testlauf geben soll. Dass es sich bei dem Kunden wirklich um Sandworm handelt, legt auch ein anderes Dokument nahe, auf dem eine Komponente von Skan genehmigt wird durch „Militäreinheit 74455“.

Bisher war nicht bekannt, dass Sandworm für seine Angriffe auch auf Werkzeuge von privaten IT-Firmen zurückgreift. Aus den Dokumenten geht hervor, dass Skan systematisch und kontinuierlich Sicherheitslücken in Computernetzwerken aufspüren und diese dann in einer „streng geheimen“ Datenbank speichern kann. Wie eine Drohne, die ständig über den Köpfen der Gegner kreist, um zu dokumentieren, wo sie verwundbar sind.

Mehrere Expertinnen und Experten, denen Dokumente aus den Vulkan Files vorgelegt wurden, sind sich einig, dass diese Software offensive Einsätze ermöglichen könnte – das heißt, Hacker könnten damit gegnerische Systeme weltweit angreifen „Skan könnte für jede Art von Geheimdienst, der Cyberoperationen durchführt, sehr hilfreich sein“, sagt Gabriella Roncone, die für Mandiant, eines der führenden IT-Sicherheitsunternehmen in den USA, arbeitet. Skan erinnere sie an Szenen aus der Serie „Game of Thrones“, wo Kriegsstrategen sich über Landkarten beugten und über Truppenbewegungen berieten, sagt sie. Roncone hat zahlreiche russische Cyberangriffe analysiert, auch in den vergangenen Kriegsmonaten. „Solche schnellen Operationen, wie wir sie in der Ukraine sehen, wären nicht möglich ohne eine große Datenbank, auf die sie zugreifen können.“

Kommunikation in der Ukraine und Windräder in Deutschland: Alles hängt mit allem zusammen

Seit dem 24. Februar 2022 werden die Menschen in der Ukraine nicht nur mit Granaten beschossen. Der Feind traktiert sie auch so intensiv wie nie mit Viren oder Falschinformationen auf sämtlichen digitalen Kanälen. Die Anzahl der Cyberangriffe auf sein Land habe sich seit Kriegsbeginn verdreifacht, sagt Wiktor Schora von der ukrainischen Cyberabwehr.

Manche dieser Attacken haben Auswirkungen bis weit über die Grenzen der Ukraine hinaus. Nachdem zu Kriegsbeginn der Satelliten-Internetanbieter Viasat gezielt von russischen Hackern attackiert worden war, um die Kommunikation der ukrainischen Streitkräfte zu stören, konnten in Deutschland mindestens 3000 Windräder nicht mehr gewartet werden, weil dies normalerweise über das Viasat-Netz geschieht. Die Bundesregierung bewertete den Fall als „Cyber-Kollateralschaden“. Im Februar warnte Bundesinnenministerin Nancy Faeser (SPD) in einem Interview mit der Funke Mediengruppe vor der großen Gefahr durch russische Sabotage, Spionage und Desinformation: „Die Cyber-Sicherheitslage hat sich durch den Krieg weiter verschärft.“

Der Cyberkrieg sei eine weitere Methode Russlands, „die Sowjetunion wiederherzustellen und die globale Ordnung zu verschieben“, sagte Wiktor Schora vor Kurzem in einem Interview mit der Tech-Zeitschrift Wired. „Sie haben die Absicht, eine ganze Nation auszulöschen.“ Die staatlichen Hacker zielen dabei vor allem auf die Infrastruktur, von der die Menschen besonders abhängig sind: die Stromversorgung, die Kommunikation. Die Menschen in der Ukraine erleben das gerade.

Diese Recherche führt deshalb im Februar 2023 auch nach Kiew zu Kyrylo Gontscharuk, dem IT-Chef eines der größten Internet- und Telefonanbieter des Landes, Ukrtelecom.

Gontscharuk ist 41 Jahre alt und trägt an diesem Februartag eine dunkelblaue Strickjacke zur Jeans. In dem kleinen Café im Stadtzentrum von Kiew, das er für das Treffen vorgeschlagen hatte, bestellt er schwarzen Tee, um seinen kratzenden Hals zu beruhigen. Vor wenigen Tagen erst ist er aus Davos zurückgekommen, wo er auf einer Veranstaltung am Rande des Weltwirtschaftsforums über Cybersicherheit mitdiskutierte.

„Seit 2014 werden wir ständig angegriffen“, sagt er, seit Russland die Krim besetzt also. So schlimm wie im vergangenen Jahr sei es aber nie gewesen. Mehr als eine Million Angriffe hätte sein Unternehmen seit Kriegsbeginn registriert. Die allermeisten davon hätten sie automatisch abwehren können, einige wenige aber nicht – wie den vom 28. März 2022.

An diesem Tag verlieren rund eine Million Kundinnen und Kunden von Ukrtelecom ihre Verbindung ins Internet. So erzählt es Gontscharuk, der sich sehr gut daran erinnern kann: Es war sein Geburtstag. Gemeinsam mit Experten der staatlichen Cyberabwehr hat er den Angriff rekonstruiert, der demnach in zwei Phasen verlief: Zuerst spionierten Hacker die digitale Infrastruktur von Ukrtelecom nach Schwachstellen aus.

Den Zugang verschafften sie sich über das Benutzerkonto eines Mitarbeiters von Ukrtelecom, der in einem der Gebiete arbeitete, die zeitweise von russischen Truppen besetzt waren. In einem zweiten Schritt versuchten sie dann, die Kontrolle über die Server und das gesamte Netzwerk zu übernehmen. Das gelang ihnen laut Gontscharuk zwar nicht, aber er habe sich gezwungen gesehen, aufgrund der Störungen die Dienste für Privatkunden zu kappen, damit zum Beispiel das Militär weiterversorgt werden konnte.

„Wir sind das erste Land in der Geschichte, das sich in einem hybriden Krieg befindet“, sagt Gontscharuk. Damit meint er die Gleichzeitigkeit von physischen und digitalen Angriffen, die womöglich sogar aufeinander abgestimmt sind. In der Stadt Dnipro wurde im Oktober ein Gebäude von Ukrtelecom durch Raketen beschädigt. Die Unternehmenszentrale in Kiew, ein lang gezogener Altbau gegenüber der Universität, wurde beinahe von Raketen getroffen. Gontscharuk zeigt auf seinem Smartphone ein Video von den brennenden Überresten einer dieser Raketen, die auf der Straße vor der Zentrale explodierten. Spuren dieses Angriffs sind heute nicht mehr zu sehen.

Kiew wirkt in diesen Februartagen 2023 auf den ersten Blick wie in den Jahren vor dem Krieg. Auf den breiten Bürgersteigen im Stadtzentrum eilen Menschen in ihre Büros oder zum Shopping. Abends stauen sich die Autos auf den Verkehrsadern und die Menschen vor den Restaurants, von denen einige ab 17 Uhr so voll sind, dass sich Warteschlangen davor bilden. Falsch parkende Autos werden abgeschleppt, die Müllabfuhr ist unterwegs. Die Stadt, sie funktioniert offenkundig.

Der Krieg mag momentan vor allem im Osten des Landes, in den Schützengräben von Bachmut, wüten, hier im ruhigeren Kiew hängt er dennoch wie ein grauer Schleier über der Stadt. Spätestens um 23 Uhr, zur Sperrstunde, wird sie totenstill. Wer dann noch mit seinen Verwandten oder Freunden sprechen will, klappt den Laptop auf oder nimmt sein Smartphone in die Hand. Kommunikationsmedien werden in Krisenzeiten besonders wichtig. Manchmal: überlebenswichtig. Der Blackout bei Ukrtelecom habe glücklicherweise nur wenige Stunden angedauert, sagt Gontscharuk.

Ob Cyberwaffen von Vulkan wie zum Beispiel Skan tatsächlich von russischen Hackern für Angriffe in der Ukraine genutzt wurden oder immer noch werden, geht aus den geleakten Dokumenten nicht hervor. Auch die ehemaligen Mitarbeitenden, die reden wollten, wissen es angeblich nicht. Sie wollen, zumindest zu Beginn ihrer Jobs, nur die gewöhnliche, kommerzielle Seite ihres Arbeitgebers gekannt haben. „Als ich angefangen habe, war mir nicht klar, woran ich arbeiten werde oder was mit meiner Arbeit passieren wird“, sagt einer, der mittlerweile nicht mehr in Russland lebt, weil er die Putin-Regierung und auch seine Arbeit bei Vulkan mit der Zeit immer kritischer sah. Er soll hier Jewgenij heißen. Dass er bei Vulkan einige Jahre beschäftigt war, belegt er mit seinem Arbeitsbuch, das in Russland zur Dokumentation einer Anstellung verwendet wird.

Jewgenij nimmt sich viele Stunden Zeit, die Dokumente aus den Vulkan Files, die ihm gezeigt werden, zu lesen und zu durchdringen. Etliche Stellen markiert er mit bunten Zetteln und macht sich Notizen. In einer steht: „what the fuck“. Immer wieder hält er beim Lesen inne, schüttelt den Kopf. „Das habe ich nicht gewusst“, sagt er dann.

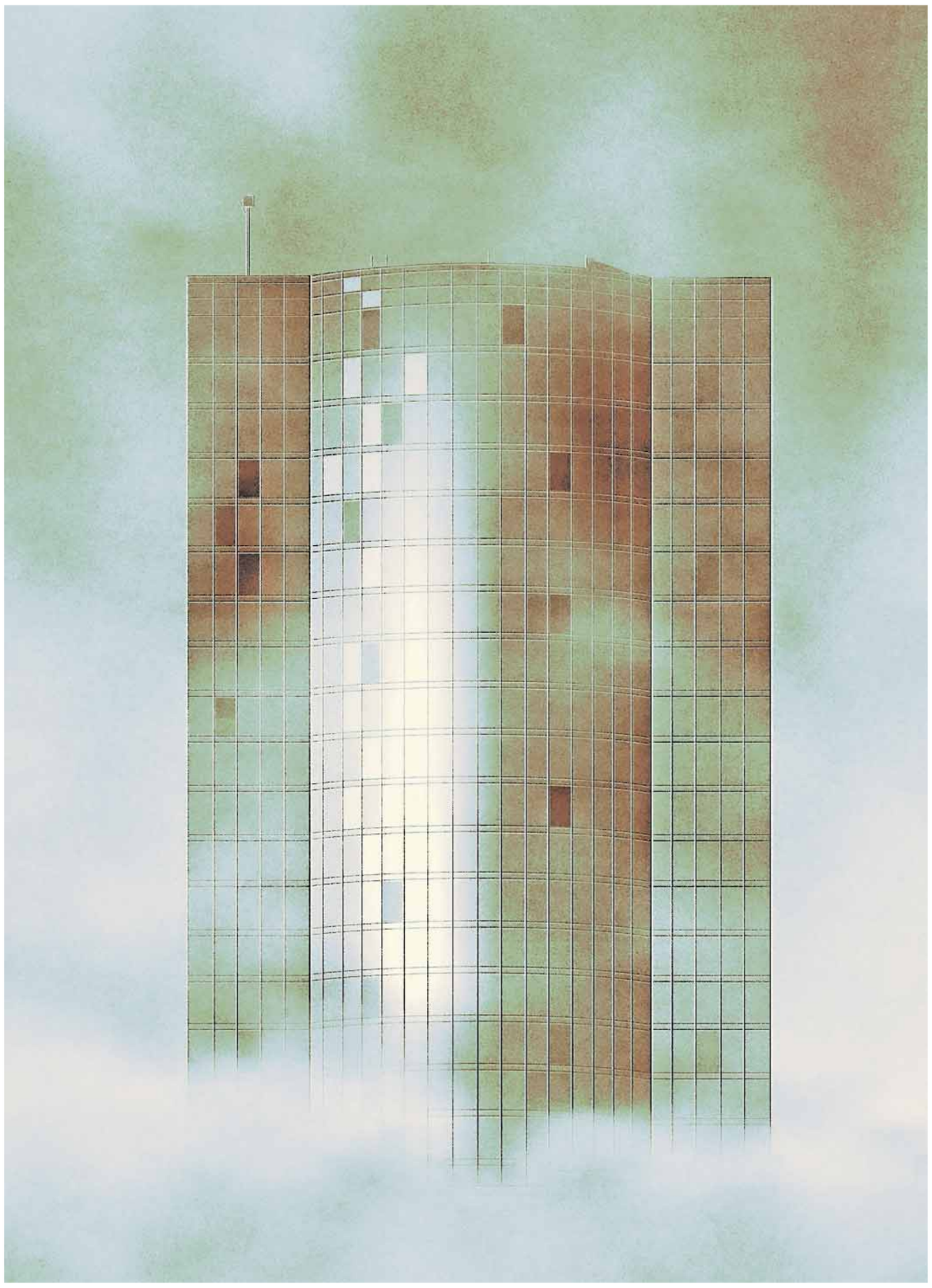
Zu Beginn sei der Job spannend für ihn gewesen, erzählt Jewgenij. Er habe sich lediglich darüber gewundert, dass er nicht einmal mit den Kollegen im Nebenzimmer über Projekte habe reden dürfen. Man habe ihm Aufgaben gegeben, und er habe sie erledigt.

Vulkan scannte das Netz nach Regimekritikern. „What the fuck“, sagt ein Ex-Mitarbeiter

Seine Entfremdung vom russischen Regime hat ausgerechnet bei Vulkan begonnen. So erzählt es Jewgenij heute. Er sei an Politik nicht interessiert gewesen, aber im Gespräch mit einigen seiner Kolleginnen und Kollegen habe sich das langsam geändert. „Sie haben über aktuelle Proteste diskutiert, darüber, wer von den Oppositionspolitikern etwas ändern will – und ich fand das interessant.“ Es war die Zeit, als der berühmteste Oppositionelle des Landes, Alexej Nawalny, noch nicht in Haft saß und seine Anhänger auf den Straßen Moskaus demonstrierten. Auch über Putin habe man bei Vulkan Witze gemacht, ihm verschiedene Spitznamen gegeben, sagt Jewgenij, „Großvater aus dem Bunker“ zum Beispiel.

Im Laufe der Zeit sei er Anhänger von Nawalny geworden und habe „versucht, ihn im Rahmen meiner Möglichkeiten zu unterstützen“. Zum ersten Mal will er hingeschaut haben, was im Land eigentlich passierte: „Ich habe verstanden, dass der russischen Regierung ihre Bürger völlig egal sind.“ Er sah, dass Sicherheitskräfte bei Demonstrationen Frauen verprügelten, dass sie Menschen in Gefangenenbusse sperrten. Dieses Regime, sagt er, habe er nicht mehr unterstützen wollen.

Sein Arbeitgeber Vulkan trieb – den Dokumenten zufolge – auch ein Softwareprojekt namens Fraction voran, dass gezielt solche Regimekritiker ins Visier nimmt, zum Beispiel die Anhänger von Nawalny. Fraction kann demnach soziale Netzwerke



The Tower, der Turm (oben), ist Sitz der berüchtigten Hacker von Sandworm, der Einheit 74455. Ein Dokument aus den Vulkan Files (Mitte) stellt die Verbindung zwischen den Cyberkriegern, der Firma und deren Gründer Anton Markow (rechts) her.

FOTOS: SCREENSHOTS

und Internetseiten automatisiert nach definierten Schlagworten durchsuchen und analysieren. Schreibt eine Person zum Beispiel auf Twitter etwas über Putin, könnte Fraction diesen Tweet nicht nur aus der Masse der Beiträge herausfiltern und ihn in einer Datenbank speichern, sondern sogar die Tonalität des Textes prüfen: Ist er für oder gegen den Präsidenten?

Erst mit der Zeit, sagt Jewgenij heute, habe er gemerkt, dass etwas nicht zusammenpasste in seinem Betrieb. „Dass wir nicht einfach nur Daten sammeln. Sondern dass wir sie für die russischen Geheimdienste nutzen." Heute ist er sich sicher, dass der FSB einer der „Hauptauftraggeber" von Vulkan war. Jener FSB, dem später ein Anschlag ausgerechnet auf Alexej Nawalny zugeschrieben wird. Nawalny wurde am 20. August 2020 auf einem Flug von Tomsk nach Moskau vergiftet, überlebte – und sitzt nach einem rechtsstaatlich fragwürdigen Prozess wegen angeblicher Veruntreuung heute im Straflager Nr. 2 in Pokrow eine mehrjährige Haftstrafe ab.

Firmengründer Markow ist patriotisch wie Putin. Im Netz ist er ein Phantom

Angst vor Gefängnis habe er auch gehabt, erzählt Jewgenij, deswegen habe er seine Heimat Russland verlassen. In Erinnerung geblieben sind ihm bis heute aber die beiden unnahbaren Vulkan-Chefs: „Auf mich haben sie wie Militärleute gewirkt, also vom Gefühl her: Wie sie sich bewegt haben, wie sie geredet haben. Immer nur das Notwendigste."

Dass Vulkan sich offenbar bereitwillig in den Dienst fürs Vaterland stellte, könnte auch etwas mit der Persönlichkeit eines der beiden zu tun haben. Anton Markow hat das Unternehmen seit 2010 zusammen mit Alexander Irschawskij aufgebaut. Heute scheint Markow als alleiniger Geschäftsführer die zentrale Figur zu sein. Auf den wenigen Fotos, die man von ihm findet, trägt er Anzug und Krawatte. Seine Haare sind kurz, sein Gesicht ist glattrasiert. Er wirkt durchtrainiert.

Das Auffälligste an ihm ist aber, wie wenig Informationen über ihn öffentlich sind. Wie alt er ist? Ob er Familie hat? Wo und wie er ausgebildet wurde? Das alles ist öffentlich nicht bekannt. Man findet keine Social-Media-Profile unter seinem Namen, er ist nicht auf Businessportalen präsent, nirgendwo eine Biografie. Einer seiner Ex-Mitarbeiter sagt, Markow sei an der Moschajsskij-Militär-Weltraum-Akademie in Sankt Petersburg ausgebildet worden und etwa 50 Jahre alt.

Markow, das Phantom, hinterlässt entweder keine digitalen Spuren oder hat sie löschen lassen. Nur E-Mails aus den Vulkan Files verraten etwas mehr über ihn: Er ist offenbar ein glühender Patriot. Er verschickt Glückwünsche zum Großen Tag des Sieges, dem 9. Mai, an sämtliche seiner Mitarbeitenden. Für ihn sei das „einer der wichtigsten Feiertage unseres Landes", schreibt er. An diesem Tag feiert Russland jedes Jahr den Sieg über Nazideutschland.

„Ich bin mit Kriegsfilmen aufgewachsen", schreibt Markow außerdem. „Und ich hatte das Glück, mit Veteranen sprechen zu können. Diese Menschen sind für uns gestorben, für die, die jetzt in Russland leben." Ähnlich wie der Präsident Wladimir Putin sieht auch Anton Markow anscheinend das Erbe seiner Heimat in Gefahr: Die Versuche, die Geschichte neu zu schreiben, dürften niemals erfolgreich sein, mahnt Markow seine Mitarbeitenden.

Der Vulkan-Gründer nimmt damit eine Erzählung auf, die im russischen Machtapparat weitverbreitet ist. Demnach werde Russland durch den Einfluss des Westens und dessen Kultur destabilisiert und drohe am Ende unterzugehen. „Diese Angst entstammt einer alten, sowjetischen Überzeugung, dass Menschen und Gesellschaften allein anhand von Propaganda geformt und geführt werden können", sagt der Russlandexperte Gavin Wilde von der Carnegie-Stiftung für Internationalen Frieden in Washington. Russland sehe sich in einem Krieg um Informationsdominanz. Ob Fake News oder Blackout: Es gehe Russland darum, Chaos und Verwirrung zu stiften.

Bereits 2013 hielt der damalige Generalstabschef der russischen Streitkräfte, Walerij Gerassimow, eine Rede über moderne Kriegsführung. Russland, sagte er, könne seine Feinde durch asymmetrische, verdeckte Attacken auf die Säulen ihres sozialen Zusammenhalts schwächen. Explizit erwähnte der General die „Konfrontation mit Information". Gerassimow ist seit Januar 2023 Oberbefehlshaber über die russischen Truppen in der Ukraine.

„Für Russland gehören Desinformation in den sozialen Medien und die Zerstörung kritischer Infrastruktur zu ein und derselben Mission", sagt John Hultquist, verantwortlich für Geheimdienstanalysen bei der Cybersicherheitsfirma Mandiant. „Es geht nicht nur darum, das Licht irgendwo auszuknipsen. Es geht darum, den Feind zu beeinflussen."

Liegt es da fern, ein Programm entwickeln zu lassen, das alles kann?

Auf Hunderten Seiten wird in den Vulkan Files genau so eine digitale Allzweckwaffe beschrieben: das Projekt Amezit, benannt nach dem seltenen, violett schimmernden Mineral Amesit. An dem Programm, erinnert sich Ex-Mitarbeiter Jewgenij, „haben wirklich viele Leute gearbeitet". Viel Geld, Zeit und Kraft seien in das Projekt investiert worden.

Auf einer Trainingslandkarte für Hacker ist ein Kernkraftwerk in der Schweiz zu sehen

Womöglich ist Amezit sogar so etwas wie das Kronjuwel der Firma, eine Art Schweizer Taschenmesser für Cybersoldaten: Überwachungstool, Propagandamaschine und Spionagewerkzeug in einem.

Amezit, das legt eine Art Gebrauchsanweisung in den Vulkan Files nahe, scheint dafür geeignet zu sein, ganze Regionen vom offenen, weltweiten Internet abzuschneiden und dafür ein lokal begrenztes Netz einzurichten. Wer auch immer Amezit steuert, hätte dann die totale Kontrolle, könnte sämtliche Daten abfangen, auswerten, blockieren und verändern. Wahrscheinlich ist, dass Amezit die militärische Übernahme von Gebieten flankieren soll, um dort schnell die Informationshoheit zu gewinnen. So ähnlich, wie es die russischen Besatzer schon auf der Krim versucht hatten, indem sie die Bevölkerung vom freien ukrainischen Netz abgeschnitten und ans regulierte russische Netz angeschlossen haben.

Das alles könnte einem großen Drehbuch folgen. In den Dokumenten zu Amezit wird angedeutet, in welchen Regionen das Werkzeug eingesetzt werden könnte: in Ländern der ehemaligen Sowjetunion, die das heutige russische Regime zu seiner Einflusssphäre zählt – wie zum Beispiel der Republik Moldau oder Belarus. Für diese beiden Länder plant der Kreml offenbar ohnehin Szenarien aus dem Drehbuch fürs Lügen, Täuschen und Angstverbreiten. So existiert in Moskau Recherchen der SZ zufolge angeblich der Plan, in den kommenden Jahren „die Kontrolle über den Informationsraum der Republik Belarus" zu gewinnen. In der Republik Moldau wollen Putins Strategen verhindern, dass „russische und prorussische Medien eingeschränkt " werden. Im digitalen Informationszeitalter eine Strategie wie gemalt für hybride Cyberkrieger – und für die Anwendung von Programmen wie Amezit.

„Ein System für die Koordination des absoluten Informationskriegs" nennt es John Hultquist. Ein Experte eines westlichen Geheimdienstes geht davon aus, dass Amezit die Voraussetzungen dafür schafft, um dann mit anderen Waffen anzugreifen – etwa mit Schadprogrammen, die Rechner verseuchen, wie Computerwürmer und Viren. Tatsächlich sollen Hacker anhand von Amezit genau solche Einsätze lernen: Vulkan hat ein Trainingsseminar entwickelt, in dem 30 „IT-Spezialisten" gleichzeitig Angriffe auf „lebenswichtige Infrastruktur" simulieren können. Die Hacker sollen zum Beispiel die „Geschwindigkeit von Zügen" verändern oder „Pumpen überhitzen". Im Ernstfall wären schon das Eingriffe mit womöglich katastrophalen Folgen.

Aber es ginge noch schlimmer. In den Dokumenten findet sich die Abbildung einer Amezit-Benutzeroberfläche, die offenbar potenzielle Ziele auf einer Landkarte visualisiert. Zu erkennen sind darauf die Region rund um die Stadt Bern in der Schweiz und das Kernkraftwerk Mühleberg. Allerdings stimmen viele Daten auf diesem Entwurf nicht. Beispielsweise führen die GPS-Koordinaten, die neben dem Kernkraftwerk verzeichnet sind, nicht in die Schweiz, sondern nach Afghanistan.

Die Allzweckwaffe Amezit soll – ganz im Sinne der russischen Cyberdoktrin, wonach Zerstörung und Desinformation Hand in Hand gehen – aber noch mehr können und die öffentliche Meinung kontrollieren und manipulieren. Die Entwickler von Vulkan schreiben in diesem Zusammenhang von „speziellem Material", gemeint ist offenkundig Propaganda, das vor allem in sozialen Medien seine Wirkung

Automatisierte Propaganda soll in den alten Sowjetrepubliken die Stimmung für Russland drehen

entfalten soll. Denn dort würden diese „Informationen nicht vormoderiert und von der großen Mehrheit der Nutzer ohne kritische Beurteilung aufgenommen", heißt es. Offenbar soll das Programm etwa auf Twitter oder Facebook falsche Profile anlegen, perfekt ausgerichtet auf die jeweilige Zielgruppe. „Social Engineering" nennen Fachleute diese Taktik. In einem Dokument kommentiert ein Mitarbeiter: „Nur ein sehr simples Szenario: Für Jungs registrieren wir süße Mädchen, etwa selbes Alter, selbe Herkunft, Interessen, etc. wie die Zielpersonen."

Auch Texte, Fotos oder Videos soll Amezit erstellen, die von diesen Fake-Profilen dann weitgehend automatisiert und großflächig geteilt werden. Amezit wäre demnach als eine Art Super-Bot effizienter als herkömmliche Bot-Fabriken, die das Netz bisher schon mit gefälschten Profilen und Informationen unterwandern.

„Ich hoffe, dass Sie diese Informationen nutzen können, um zu zeigen, was hinter verschlossenen Türen geschieht", schrieb die Quelle, die all das Material übermittelt hatte, um die Tür einen Spalt zu öffnen. Man solle sich keine Sorgen um sie machen. Seitdem ist die Person, die sich als Geist beschreibt, nicht mehr zu erreichen. Was sie hinterlassen hat: den bislang intensivsten Einblick in das Netzwerk der russischen Cyberkriegsführung.