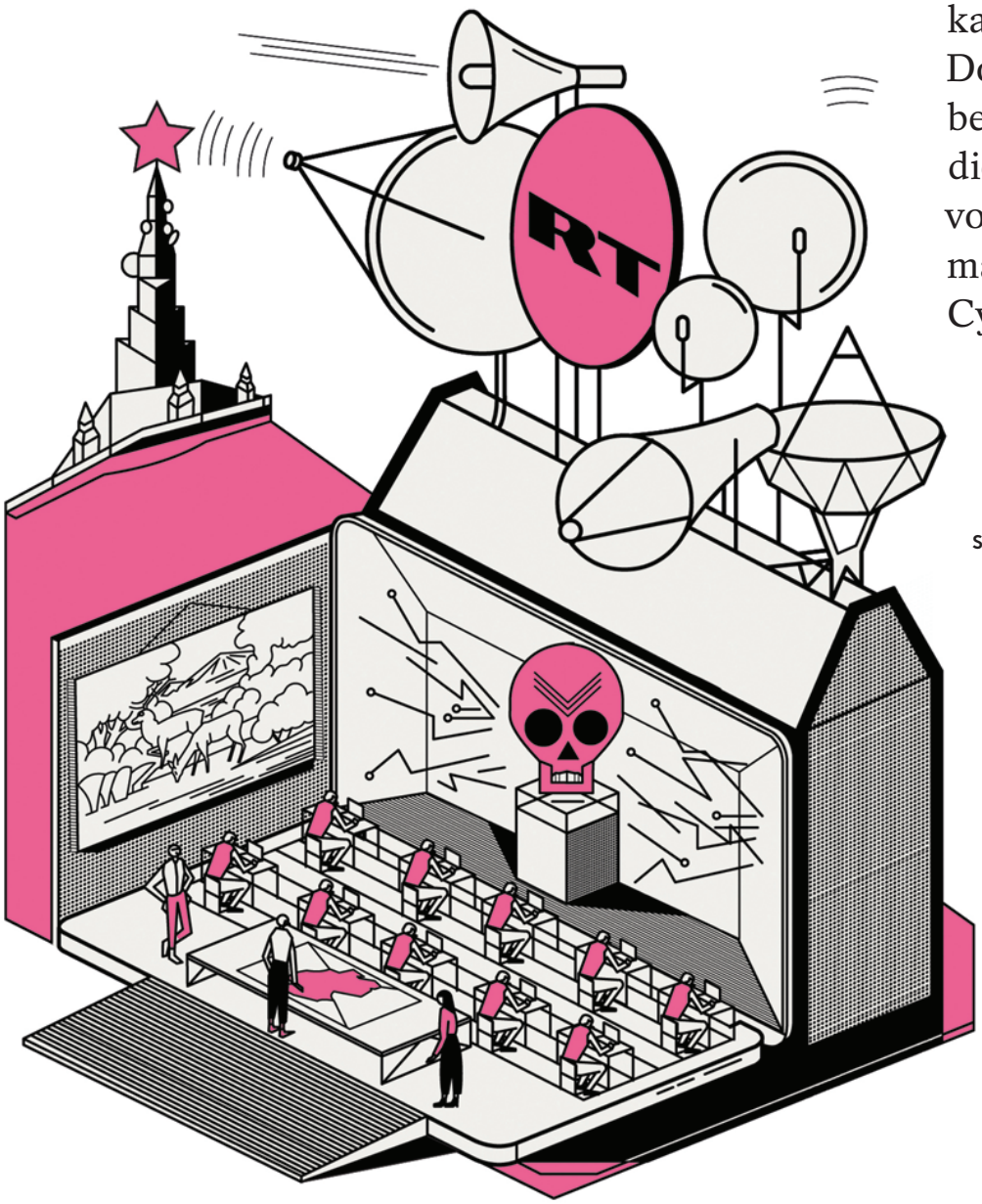
ANGRIFF AUS DEM IRGENDWO

Auch in Deutschland geht die Sorge um, Russland könnte Einfluss auf den Wahlkampf nehmen. Doch wie berechtigt sind die Ängste vor Desinformation und Cyberattacken?



Von
SIMONE BRUNNER

Illustration
EVA REVOLVER

Wenn es nach so manchem Beobachter geht, beginnt der Konflikt zwischen dem Westen und Russland nicht an der Front in der Ostukraine oder an der Nato-Ostflanke. Sondern an der Borowaja-Straße 3, in einem ehemaligen Industriegebiet. Hier, im Osten Moskaus, ist das Hauptquartier des russischen Fernsehsenders RT, vormals Russia Today. Das Logo des Senders, „Question more“ („Mehr infrage stellen“), ist allgegenwärtig: Es prangt auf den parkenden Kleinbussen und sogar an der Schranke zur Einfahrt. Man wolle Geschichten erzählen, „die von den Mainstreammedien verschwiegen werden“, mit einer „russischen Perspektive auf das Weltgeschehen“, heißt es auf der Homepage.

2005 als Russia Today gegründet, sendet RT heute auf Englisch, Arabisch und Spanisch. Webportale gibt es auch auf Deutsch und Französisch. Das Programm ist ein schillerndes Forum für Antiamerikanisten, Rechtspopulisten, Systemkritiker aller Couleur und Verschwörungstheoretiker. „Provokativ konträr“, wie es der *Guardian* beschrieb. Als „Agenturen der Einflussnahme und der verlogenen Propaganda“ hat es hingegen zuletzt der französische Präsident Emmanuel Macron bezeichnet. Der Fernsehsender hatte im französischen Wahlkampf für die Rechtspopulistin Marine Le Pen und gegen Macron Stimmung gemacht. Die russische Nachrichtenagentur Sputnik behauptete sogar, Macron sei schwul.

Wer sich vor Ort erkundigt, was diese „russische Perspektive“ sei, erntet vorerst Herablassung und Häme. „Wir bekommen Telefonanrufe direkt aus dem Kreml – wissen Sie das etwa nicht?“, spottet Alexei Kusnezow. Der untersetzte Anfangvierziger und gebürtige Moskauer ist stellvertretender Leiter der englischsprachigen Nachrichtenabteilung bei RT. Sein Englisch hat den rollenden Zungenschlag des Amerikanischen, hat er doch selbst für US-Medien in Moskau gearbeitet, bevor er 2010 zu RT kam. Die globale Medienwelt werde kontrolliert von „angelsächsischen Medien“, wie Associated Press und Thomson Reuters, sagt er. Doch dann kam RT. „Wenn Verbrechensbekämpfer Verbrechen bekämpfen und Feuerwehrmänner Feuer – was bekämpfen dann die Freiheitskämpfer?“ steht auf seinem Twitter-Account.

> „Mittlerweile lesen mehr Menschen über die russische Propaganda, als sie selbst zu konsumieren“

Auf alle Nachfragen, wie sich RT von anderen Fernsehsendern unterscheidet, reagiert er launisch. Ist RT ein Kreml-Sender? „Müssen wir denn die ganze Zeit Putin bashen, um ernst genommen zu werden?“ Was unterscheidet RT denn dann von westlichen Medien? „Seit meinem ersten Arbeitstag werde ich von Korrespondenten wie Ihnen gefragt: Fühlt ihr euch wie an der Frontlinie eines Informationskriegs?“ Fühlt sich RT also vom Westen missverstanden? „Würden Sie sich denn nicht missverstanden fühlen, wenn Sie die ganze Zeit als Propagandaorgan bezeichnet würden?“

SO IST ES aber gerade das Image von Macht und Einfluss, das RT ständig von sich selbst zeichnet. Wie eine Trophäe hängt in den Gängen der Moskauer Zentrale ein Zitat aus dem deutschen *Tagesspiegel*, auf Russisch übersetzt: „RT ist heute neben Gazprom und der Waffenindustrie das effizienteste Instrument der russischen Außenpolitik.“ RT wirbt mit kantigen Sprüchen, wie zuletzt auf dem Sankt Petersburger Wirtschaftsforum („RT ist mächtiger als Tausende Atomraketen“) oder auf dem Flughafen Sotschi („Finden Sie heraus, wen wir als Nächstes hacken werden“). „Unser Erfolg rührt daher, dass die Menschen wissen, dass die Ereignisse nicht so schwarz-weiß sind, wie es uns die Tausenden Mainstreammedien in ihren Echokammern immer glauben machen wollen“, kommentiert die RT-Chefredakteurin Margarita Simonjan per E-Mail.

Weltweit kommt RT derzeit auf 70 Millionen Zuschauer pro Woche, 36 Millionen davon in Europa, so die Medienforschung Ipsos. In den USA schafft es RT hingegen nicht einmal in das Ranking der 100 meistgesehenen Sender. In Großbritannien sehen RT überhaupt nur 0,04 Prozent der Zuschauer, so der Broadcasters’ Audience Research Board. Der deutsche Ableger von RT, der nur über Youtube läuft, kommt bei seinen Sendungen meist nicht über 10 000 bis 20 000 Klicks hinaus. Und an eine Expansion ist derzeit nicht zu denken: 2016 wurde das Budget von RT um 10 Prozent gekürzt. Mit dem Rubelverfall sind die Mittel des Senders in den vergangenen Jahren de facto auf die Hälfte zusammengeschmolzen. „Mittlerweile lesen mehr Menschen über die russische Propaganda, als sie selbst zu konsumieren“, sagt der russische Blogger Alexei Kowaljow.

1000 Kilometer weiter westlich, 200 Kilometer von der russischen Grenze entfernt, am Südrand der estnischen Hauptstadt Tallinn. Draußen reihen sich bunte Fahnenstangen aneinander, drinnen verschluckt der Teppichboden die Schritte. In dem zweistöckigen Kalksteinbau ist seit dem Nato-Beitritt Estlands der estnische Stützpunkt des westlichen Verteidigungsbündnisses

Illustration: Eva Revolver/Sepia

„Es geht darum, die Kräfte zu stärken, die das System infrage stellen, und das Selbstvertrauen demokratischer Staaten zu schwächen“

untergebracht. 2008 wurde hier das Kompetenzzentrum für Cyberabwehr der Nato eröffnet.

Das Verhältnis Estlands zu Moskau ist außerordentlich komplex. Als 2007 ein sowjetisches Kriegerdenkmal vom Zentrum Tallinns an den Stadtrand verlegt wurde, gingen russischstämmige Esten auf die Straße. Zugleich legte eine DDOS-Attacke, von 85 000 Computern gestartet, das Parlament, die Präsidialverwaltung, Banken und Medien im ganzen Land lahm. Estland („E-stonia“) gilt als Vorreiter der Digitalisierung, elektronische Krankenakten oder Wahlen über Mausklick gehören hier zum Alltag. Es war der erste groß angelegte Hackerangriff auf ein Land. Mutmaßlich stand Russland hinter den Angriffen.

Die Cyberabwehr ist eine Mischung aus Thinktank und Lehranstalt: Bis zu 100 Experten aus allen Nato- und Partnerländern arbeiten hier, zur Hälfte Militärs, zur Hälfte Zivile. In Trainings werden Beamte und Militärs aus den Mitgliedsländern dazu ausgebildet, digitale Sicherheitslücken zu schließen und im Ernstfall den Schaden zu begrenzen. Das Tallinn-Manual, ein internationaler Wegweiser zu Cyberkonflikten, wurde hier ausgetüftelt. Uniformierte und junge Nerds in Sneakers geben sich die Türklinken in die Hand.

Das estnische Know-how ist heute begehrt wie noch nie. Die Nachfrage nach Ausbildungskursen übersteigt das Angebot, heißt es. Kein Wunder, ist doch wenige Wochen vor der Bundestagswahl auch in Deutschland die Cyberbedrohung aus Russland ein großes Thema. Von einer gezielten „Angriffskampagne“ des russischen Geheimdiensts FSB und GRU mit „hohem Ressourceneinsatz und herausgehobenen technischen Fähigkeiten“ schrieb zuletzt die *Bild* („Russland führt Cyber-Krieg gegen Deutschland!“) und bezog sich dabei auf den Verfassungsschutz. Aber auch die *Zeit* schrieb zuletzt von einem „Krieg ohne Blut“.

„KEIN SYSTEM ist 100-prozentig sicher“, sagt Liisa Past. Die Estin mit dem blonden Bubikopf erinnert sich noch gut an die Cyberattacke vor zehn Jahren. Damals arbeitete sie als Redakteurin einer estnischen Zeitung. Nach einem Serverausfall mussten die Seiten vor Redaktionsschluss noch einmal neu verfasst und per USB-Stick in die Druckerei gebracht werden. „Das war unangenehm“, erinnert sich Past, die heute die Kommunikationsabteilung des Cyberzentrums leitet. „Aber bestimmt kein Krieg.“ Vielmehr sei die Cyberbedrohung „das neue Normal, auf das sich alle Staaten einstellen müssen“. Egal ob aus Ost oder West.

Eine These, die auch der Politologe Thomas Rid in seinem Buch „Mythos Cyberkrieg“ vertritt: So führe allein der Begriff „Cyberkrieg“ in die Irre. „Nicht ein einziger Mensch wurde jemals durch eine Cyberattacke getötet oder verletzt“, schreibt Rid. Genauso wichtig wie die technische sei daher auch die „psychologische Cybersecurity“, sagt Matthijs Veenendaal, Cyberexperte beim niederländischen Verteidigungsministerium. „Diese Attacken führen meist lediglich dazu, dass gewisse Onlinedienste für eine gewisse Zeit nicht verfügbar sind.“ Ein Staat müsse daher klarmachen: Ein Hackerangriff sei keine Kriegserklärung – sondern ein Problem, das mit technischer Expertise gelöst werden kann. Nicht mehr, aber auch nicht weniger. Wer mit Kriegsrhetorik auffährt, schürt Massenpanik und vernebelt den Blick.

Doch was, wenn ein Cyberangriff genutzt wird, um den Wahlkampf zu manipulieren? „Der russischen Führung geht es nicht darum, Donald Trump oder Marine Le Pen zum Sieg zu verhelfen oder Angela Merkels Wiederwahl zu verhindern; da schätzt der Kreml seine Möglichkeiten weit realistischer ein als westliche Kommentatoren“, schreibt der Osteuropaexperte Stefan Meister in einem Beitrag. „Vielmehr geht es darum, die Kräfte zu stärken, die das System infrage stellen, und darum, das Selbstvertrauen demokratischer Staaten zu schwächen.“ Es ist wohl kein Zufall, dass der russische Präsident Wladimir Putin zuletzt bewusst offenließ, ob der Kreml direkt hinter den russischen Hackerangriffen im US-Wahlkampf stand. Hacker seien „Freigeister“, so Putin. Wenn ihnen der Sinn danach stehe, würden sie hacken, um einen „gerechten Beitrag“ zu leisten für den „Kampf gegen jene, die schlecht über Russland sprechen“ – gerade so, wie Künstler Bilder malen.

Spätestens seit den US-Präsidentschaftswahlen werden die Fähigkeiten der russischen Politik in westlichen Medien daher überschätzt. „Von wesentlicher Bedeutung ist nicht das, was Russland mit Blick auf Cyberattacken, Desinformation und Propaganda wirklich kann, sondern das, was wir ihm zutrauen“, schreibt Meister. „Inzwischen haben alle angefangen, an die Allmacht der russischen Propaganda zu glauben“, sagt der Blogger Kowaljow. „Und das ist vermutlich ihr allergrößter Erfolg.“

SIMONE BRUNNER ist Journalistin in Wien und spezialisiert auf Themen aus Osteuropa

Foto: Alexander Gruber