Die neuen Armeen

Invasion der Meinungs-Roboter: Wie gefährdet ist der deutsche Wahlkampf durch Bots und Fake News? Nehmen ausländische Geheimdienste Einfluss? Ist die Auszählung der Stimmen sicher? Fest steht: Im digitalen Raum gibt es selten Gewissheit

VON ANNE LENA MÖSKEN UND KAI SCHLIETER

2017 Bundestagswahl

BERLIN. Unsichtbar und lautlos schlichen sich die Hacker an. Ihre Spur führte nach Russland, heißt es. Ein „Advanced Persistent Threat" – eine ausgefuchste Bedrohung durch Hacker, mutmaßlich von einer Regierung gesteuert. 16 Abgeordnetenbüros des Bundestages nahm dieser „APT28" im Mai 2015 ins Visier, 16 Gigabyte Daten flossen ab. Nach dieser Cyberattacke folgte eine weitere Angriffswelle im August 2016. „Mit Blick auf die bevorstehende Bundestagswahl 2017 könnten auch deutsche Parteien oder Politiker das Ziel russischer Einflussnahme werden", heißt es dazu im Bericht der Verfassungsschützer.

Seit Wochen warnen Vertreter von Sicherheitsbehörden vor digitalen Beeinflussungskampagnen, die mit erbeuteten Informationen angeheizt werden könnten. Flankiert von Fake News und Armeen von Software-Robotern, die bei Twitter und Facebook automatisiert Propaganda erzeugen. „Hybride Bedrohung" nennt sich das. Doch drohen tatsächlich „erhebliche Auswirkungen auf die innenpolitischen Verhältnisse" durch den russischen Geheimdienst, wie deutsche Agenten nahelegen?

Wer Antworten sucht, kann in einem herrschaftlichen Altbau in Berlin-Charlottenburg damit beginnen. Im Innern des sandsteinfarbenen Gebäudes gelten erhöhte Schutzvorkehrungen. Durch eine Glastür die Treppe hinauf, einen Gang mit Sicherheitsschleusen entlang – hier befindet sich das Büro von Marcel Dickow, Chef für Sicherheitspolitik der Stiftung Wissenschaft und Politik. Auf einem Sofa ihm gegenüber sitzt Matthias Schulze, ein Kollege, der den Bereich Cyber-Sicherheit aufbaut. Die Stiftung, die zu einem großen Teil aus dem Etat des Kanzleramtes finanziert wird, berät Regierungsmitglieder, Abgeordnete des Bundestages oder auch Militärs der Nato in außenpolitischen Fragen.

Marcel Dickow ist ein schlanker Physiker mit Kinnbärtchen, der sich mit autonomen Militärrobotern, Raumfahrt und Geheimdiensten befasst. Er ist der Technikexperte des Think Tanks, Anfang vierzig. Er meint, es müsse zunächst „nach dem Motiv gefragt werden", das die Regierung in Moskau verfolgen könnte. „Selbst wenn alles auf den russischen Geheimdienst hindeuten würde, können wir immer noch nicht beweisen, dass es die Russen waren", sagt Dickow.

Hackerangriffe lassen sich fast nie eindeutig zuordnen. Meist überprüfen spezialisierte Softwarefirmen den Schadcode und suchen nach Spuren und Mustern. Matthias Schulze weist darauf hin, dass es „Werkzeuge gibt, die automatisiert die Syntax von anderen Sprachen imitieren. Hacker können solche Tools nutzen, um bestimmten Nationalitäten vorzutäuschen."

Im digitalen Raum existieren keine Gewissheiten. Die Amerikaner geben deswegen für Täter nur Grade an Wahrscheinlichkeiten an. Dickow ist nicht einmal davon überzeugt, dass die identifizierte Gruppe „APT28" mit Sicherheit dem russischen Geheimdienst zuzuordnen ist.

Er lehnt sich in seinem Stuhl zurück und sagt: „SPD und CDU liegen in den wichtigen außenpolitischen Fragen nicht allzu weit auseinander. Auch die SPD stimmt für die Sanktionen gegen Moskau, und die Positionen im Syrienkonflikt sind identisch." Er meint, eine Beeinflussung von Wählern in die eine oder andere Richtung ändert kaum das Gefüge der Bundesrepublik. Auch ist weder die deutsche Gesellschaft so polarisiert wie die USA, noch handelt es sich um eine Präsidentschaftswahl, bei der zwei Spitzenkandidaten mit ander antreten. Auch mache das deutsche Verhältniswahlrecht eine Manipulation schwerer. „Die Mediennutzung ist in Deutschland viel weniger polarisiert als in den USA und mittlerweile kennen westliche Gesellschaften das Vorgehen, was die Wirkungsweise von Desinformationskampagnen mindert", sagt Schulze.

Nach dem Hackerangriff auf das Netz des Bundestages setzte das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Serverstruktur des Bundestages neu auf. Experten berieten die Abgeordneten. Techniker der Behörde schotteten die Netze der Verwaltung, der Fraktionen und der Wahlkreisbüros der Parteien stärker voneinander ab. Doch effektiver Schutz ist schwer möglich bei Tausenden von Rechnern, WLAN und oft unverschlüsselter Kommunikation.

Einer, der zu den Warnern zählt, ist Arne Schönbohm, Präsident des BSI. Er reist viel. Auf einer Autofahrt zwischen zwei Terminen ist er auf dem Handy erreichbar. „Eine Gefährdungslage der IT-Systeme im Zusammenhang mit der Bundestagswahl ist vorhanden, es besteht die Möglichkeit, dass versucht wird, durch Cyber-Angriffe die Bundestagswahl zu beeinflussen", sagt Arne Schönbohm. „Wir verzeichnen eine Menge Aktivitäten." Als Präsident des BSI ist er Sprecher des Nationalen Cyber-Abwehrzentrums, das verschiedene Behörden und Akteure an einem Tisch versammelt: das Bundesamt für Verfassungsschutz, das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, das Bundeskriminalamt, die Bundespolizei, das Zollkriminalamt, der Bundesnachrichtendienst, die Bundeswehr. Das Cyber-Abwehrzentrum fungiert als Koordinierungsstelle. Seit Anfang Juli hat das BSI dem Bundeswahlleiter einen Mitarbeiter an die Seite gestellt. Da in Deutschland zwar noch immer auf Papier abgestimmt und per Hand ausgezählt wird, sind die Stimmabgabe und -auszählung selbst nicht gefährdet. Wohl aber die Übermittlung der Daten, sagt Schönbohm. „Hier sensibilisieren wir den Bundeswahlleiter und beraten ihn, wie die Übertragung der Ergebnisse gesichert werden kann." Mit Blick auf die USA und Frankreich, wo vor den Wahlen geleakte E-Mails der Kandidaten auftauchten, betont er: „Aus diesen Vorfällen haben wir unsere Lehren gezogen und gemeinsam mit dem Bundeswahlleiter entsprechende präventive Maßnahmen ergriffen."

Gerade im digitalen Raum ist es schwer zu erkennen, welche Informationen einem bestimmten Interesse dienen. Deutsche Sicherheitskräfte weiten beispielsweise derzeit ihr Arsenal an Cyberwaffen mit Staatstrojanern aus. Bundesinnenminister Thomas de Maizière rief eine Behörde für staatliches Hacken ins Leben, die jene Sicherheitslücken nutzen will, die das BSI bekämpft. Eine Gemengelage, in der Bedrohungsszenarien nützlich sind.

Unter falscher Flagge

Bernd Fix, Hacker der ersten Stunde, ist deshalb besonders vorsichtig. Sein Hobby: Quantencomputer und Kryptografie. Fix entwickelte einen der ersten Viren und das weltweit erste Antiviren-Programm. Er kommuniziert nur verschlüsselt. Zum APT-Angriff durch Russland, schreibt er: „Ausschließlich Indizien basierte Schlussfolgerungen". Es müssten „False-flag-Operationen in Betracht gezogen werden". Also geheimdienstliche Desinformationskampagnen von Gegner Russlands. „Alle Spieler kennen die Kriterien, auf deren Basis Firmen wie Symantec, Kaspersky und Co die Zuschreibungen vornehmen, von wem ein Angriff stammt. Es ist ein Leichtes, ähnlich erscheinende Cyber-Attacken zu inszenieren", sagt der Computerexperte.

Im Netz wimmelt es von staatlichen Akteuren, die automatisiert die Öffentlichkeit beeinflussen. Nicht nur Putin setzt „Trolle", also menschlichen Manipulateure, ein, die von Sankt Petersburg aus Kommentare im Internet manipulieren. Die „Hasbara-Brigaden" sind eine Cyber-Einheit des israelischen Außenministeriums, die Meinungsmache auf Nachrichtenportalen orchestriert. Zuständig bei den britischen Kollegen des Geheimdienstes GCHQ ist die Einheit „Joint Threat Research Intelligence Group". Eine ihrer Spezialitäten, wie aus den Dokumenten von Edward Snowden hervorgeht: „systematische Verbreitung und Diskreditierung von Gegnern auf sämtlichen Kanälen im Internet". Die DARPA, die militärische Forschungsbehörde des Pentagon, steckt mehr als 40 Millionen Dollar in das Programm „Social Media in Strategic Communication", das in Sozialen Medien automatisiert Propaganda erkennt und Gegenpropaganda erzeugen kann. Und ganz klassisch: Das Pentagon beschäftigte 2009 etwa 27 000 Fachleute allein für Public Relations, wie Wired berichtete.

Die Szenarien sind so vielfältig wie die Instrumente: Armeen von Bots beeinflussen die öffentliche Diskussion. Es ließe sich ein Krieg der „Memes" entfesseln – im Militärjargon „memetic warfare": Internet-Inhalte, Bilder oder gezielte Narrative, die sich im Netz viral wie Krankheiten ausbreiten, digitale Propaganda, mit der sich auch die Nato beschäftigt. Erst im Juni fand in Estland dazu eine Tagung statt. Und eines der Pentagon-Programme zum „memetic warfare" nennt sich „Narrative Networks". Es erforscht, wie sich im Internet Narrative, also gezielte Deutungen, erzeugen lassen und untersucht „ihren Effekt für die menschliche Psyche.

Eine neue Studie der Indiana University dokumentiert, wie sich die Werkzeuge ergänzen. Demnach spielen Social Bots für die Verbreitung von Fake News eine wichtige Rolle. Die Software reagiert dabei bei Erscheinen von Fehlinformationen und versucht, sie gezielt an reale Menschen zu verbreiten, die besonders viele Follower bei Twitter haben. Zuvor hatten Forscher der Universität „schädlich designte Bots mit dem Ziel der Beeinflussung" bei den US-Wahlen 2010 und zwei Jahre später in Mexiko beobachtet.

In Deutschland gibt es noch nicht viele Experten, die sich mit Bots auskennen. Mitte Juli sitzt einer von ihnen im Europasaal des Paul-Löbe-Hauses und unterrichtet Abgeordnete. Simon Hegelich trägt sein Jeanshemd offen, ein T-Shirt darunter, er hält seinen Vortrag im Plauderton, das Wort „vermutlich" kommt häufig vor. Seit März 2016 hat er die erste deutsche Professur für Political Data Science an der Technischen Universität München inne. Der Politikwissenschaftler und Datenanalytiker leitet das Projekt Social Media Forensics. Er zeigt Fieberkurven: Wie oft wurde der Hashtag #Merkel, wie oft #Schulz in den vergangenen Monaten von Bots verwendet? Zehn Prozent, sagt Hegelich, schätzungsweise. Er glaubt: Bots verfälschen Trends durch die pure Masse ihrer Posts. Das größte Botnetz, das bisher auf Twitter gefunden wurde, umfasst 350 000 Accounts – die posteten vor allem Zitate aus „Star Wars". Was aber wäre, wenn in einer Krisensituation auf einmal eine derart große Zahl an Accounts eine bestimmte Nachricht verbreiten? Hegelich macht eine kunstvolle Pause. „Könnte heikel werden."

In Deutschland, sagt er, findet man seit Mai vermehr Bots, die auf ein Netzwerk verlinken, das der Alt-Right-Bewegung in den USA zuzuordnen ist. „Hier werden Strategien angewandt, die eigentlich aus dem militärischen Kontext kommen", sagt Hegelich. Und Bots sind billig: Zwischen 45 bis 150 Dollar kosten 1 000 Fake-Konten. Bei Twitter sollen rund 50 Millionen davon herumschwirren. Hegelich sieht eine „Invasion der Meinungs-Roboter".

Das bewerten Kollegen der Universität Oxford ähnlich: „Von Computern erzeugte Propaganda ist heute eines der wohl mächtigsten Werkzeuge, das gegen unsere Demokratie eingesetzt wird", schreiben sie in ihrer Studie. Zwölf Forscher untersuchten dort die Aktivitäten in neun Ländern. Sie fanden heraus, dass Donald Trump und Hillary Clinton Bots einsetzten. Beim Brexit spielten die künstlichen Fieslinge eine „strategische Rolle".

Lisa-Maria Neudert erforscht in Oxford den Einsatz in Deutschland. Per Skype erklärt sie, wie Software-Roboter wirken: „Sie beeinflussen die Algorithmen des Newsfeeds durch Likes, Retweets und Kommentare. So werden bestimmte Themen nach oben gepusht und trenden." Auf diese Weise erhöhten Parteien ihre Sichtbarkeit. „So machen Politiker seit jeher ihren Wahlkampf: Sie platzieren ihre Inhalte so, dass ihre Wähler sie sehen. Nichts anderes machen Social Bots." Für Deutschland kann sie bisher Entwarnung geben. Sie hat die Wahlen im Saarland und in Nordrhein-Westfalen und die Wahl des Bundespräsidenten untersucht. „Es gibt wenig empirisch dokumentierte Befunde für den Einfluss von computerisierter Propaganda in Deutschland." Auffällig ist allerdings die starke Verbreitung von Fake News. Und noch etwas fiel auf: Der Einsatz von Software-Robotern ist besonders in Russ-

„Es besteht die Möglichkeit, dass versucht wird, durch Cyber-Angriffe die Bundestagswahl zu beeinflussen."

Arne Schönbohm, Chef des Bundesamtes für Sicherheit in der Informationstechnik

„Selbst wenn alles auf den russischen Geheimdienst hindeuten würde, können wir immer noch nicht beweisen, dass es die Russen waren."

Marcel Dickow, Chef für Sicherheitspolitik der Stiftung Wissenschaft und Politik