Wochenkommentar 41/2024 von Matthias Zehnder

Informationelle Landesverteidigung – wie könnte das gehen?

Bild: KEYSTONE/Georgios Kefalas

Die Patrouille Suisse an einer Show in Dittingen im August 2009.

Was ist die grösste Bedrohung der Schweiz? Stellen Sie sich vor, Sie wären ein autokratischer Herrscher in einem fernen Land und möchten dem Westen, insbesondere der Schweiz schaden. Würden Sie eine Bombe auf unser Land werfen, ein paar Raketen abfeuern oder gar Panzer schicken? Das wäre höchst ineffizient. Und zwar nicht nur, weil der Schaden nicht allzu gross wäre, sondern weil dem ganzen Land sofort klar wäre: Wir werden angegriffen. Die Reaktion wäre ein grosses Zusammenrücken. Nein, viel effizienter als Bomben und Raketen ist es, ein Land im Informationsraum anzugreifen. Und zwar indirekt, indem unser Autokrat für Unsicherheit sorgt, das Vertrauen der Bevölkerung in Regierung, Staat und Institutionen untergräbt und schwelende Konflikte schürt. Unser Autokrat muss dafür gar nicht viel tun. Die Medien sind ökonomisch längst auf pure Reichweite gepolt und deshalb äusserst empfänglich für Sensationen, Konflikte und emotionalisierende Inhalte. Ganz besonders gilt das für die sozialen Medien, wo Fake News sich sieben mal so schnell verbreiten wie reale Nachrichten – weil Falschnachrichten meistens sensationeller sind und mehr Emotionen wecken. Unser Autokrat reibt sich also die Hände, er sorgt mit einem kleinen Team gezielt für etwas Desinformation im Land und schon krachts. So weit, so klar. Die spannende Frage ist: Wie kann sich eine westliche Demokratie, wie kann sich die Schweiz davor schützen? Unser Autokrat verweist grinsend auf die Medien- und Meinungsfreiheit – sind dem Staat also die Hände gebunden? Ist die Schweiz feindlicher Desinformation schutzlos ausgeliefert?

Denken wir gemeinsam darüber nach: Wie könnte heute eine informationelle Landesverteidigung aussehen?

Die Schweiz wird angegriffen. Jetzt, heute, in diesem Moment. Nicht mit Bomben und Raketen, sondern im Internet. «Hacker», denken Sie jetzt wohl. Und haben damit zur Hälfte recht. «Hybride Kriegsführung» nennen das die Militärs. Der russischen Invasion in die Ukraine im Februar 2022 zum Beispiel gingen massive Cyberangriffe auf staatliche Stellen und kritische Infrastrukturen in der Ukraine voraus. Der Cyberraum muss heute so selbstverständlich verteidigt werden wie das physische Land. Bei den Angreifern handelt es sich um Kriminelle, um Hacktivisten, um klassische Hacker, aber auch um staatliche und parastaatliche Hackergruppen. Sie versuchen, in kritische Infrastrukturen einzudringen und Schadsoftware zu platzieren. Kriminelle klauen Daten oder versuchen, Institutionen und Unternehmen zu erpressen.

Der Schutz und die Verteidigung vor Hackerangriffen ist als Cyberdefence heute unbestrittener Teil der Landesverteidigung. In der Schweiz ist das Bundesamt für Cybersicherheit dafür zuständig: Das BACS ist als nationales Kompetenzzentrum des Bundes für Cybersicherheit eine Anlaufstelle für Wirtschaft, Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen. Die Aufgabe des BACS ist es, die Schweiz im Cyberraum sicherer zu machen. Es warnt vor Cyberbedrohungen und Cyberangriffen, unterstützt Betreiber von kritischen Infrastrukturen bei Angriffen, analysiert Cybervorfälle technisch und ist mit den Strafverfolgungsbehörden vernetzt. Man könnte also sagen, dass das BACS für die Verteidigung des Landes im Internet sorgt. Es ist gehört deshalb zum VBS und ist quasi eine Schwester der Armee, des Staatssekretariats für Sicherheitspolitik, des Bundesamts für Bevölkerungsschutz, des Nachrichtendiensts des Bundes und von Armasuisse.

Die andere Hälfte: Desinformation

Alles gut also? Nur zu Hälfte. Denn das Bundesamt für Cybersicherheit ist nur um die technische Sicherheit des Landes besorgt. Das BACS schützt vor Viren, Schadprogrammen und Angriffen auf die technische Infrastruktur. Es schützt aber nicht vor Angriffen auf die Köpfe der Menschen: also vor Desinformation, Propaganda und Fake News. Das ist ungleich schwieriger zu bewerkstelligen. Jetzt sagen Sie vielleicht: «Das ist doch nicht Aufgabe des Staates, wir haben doch die Medien!» Das ist genau die Schwierigkeit.

Zwar nutzen die Menschen so viele mediale Inhalte wie noch nie, bloss sind es immer seltener journalistische Medien. Und auf Social Media verbreiten sich gerade gefälschte Nachrichten etwa siebenmal schneller als reale Nachrichten. Dazu kommt, dass sich auch Qualitätsmedien immer stärker wie Facebook und Twitter verhalten, weil die meisten Medienangebote in der Schweiz heute ökonomisch auf Reichweitenmodelle setzen. Was dann passiert, habe ich schon 2017 in meinem Buch «Die Aufmerksamkeitsfalle» beschrieben. Der Untertitel fasst das Buch zusammen: «Wie die Medien zu Populismus führen». Die Folgen davon können Sie heute in Deutschland, Österreich, Frankreich und den USA besichtigen.

Der Westen demontiert sich selbst

Unser Despot lächelt. Der Westen demontiert sich selbst, indem er seine

Medien den Bach runter gehen lässt. Gleichzeitig bietet die Künstliche Intelligenz fantastische Möglichkeiten für das Fälschen von Bildern und Videos und das massgeschneiderte Kreieren von Texten. Unser Despot kann sich zurücklehnen und händereibend abwarten.

Aber gäbe es nicht doch Möglichkeiten, wie unser Land sich informationell besser verteidigen kann gegen Falschnachrichten, Desinformation und Propaganda? Was könnte das Ziel einer solchen Verteidigung sein und welche Mittel könnte der Staat dafür einsetzen? Denken wir mal gemeinsam darüber nach. Ich versuche dabei, mir alle Hinweise darauf zu verkneifen, wie kontraproduktiv es ist, die SRG zu verkleinern und die Medienförderung einzudampfen. Es geht also ganz konkret um die Frage, ob und wie der Bund, also das Verteidigungsdepartement oder die Armee, die Schweiz informationell besser verteidigen könnte.

Wir stossen dabei sofort auf drei Probleme:

1. Problem: Der Staat darf nicht in die Medienfreiheit und schon gar nicht in die Meinungsfreiheit eingreifen. Wenn also Herr Meier oder Frau Müller der Meinung sind, die Erde sei flach und Zucker mache schlank, dann ist das zwar falsch, aber eine Meinung, die sie haben dürfen. Natürlich dürfen Herr Meier oder Frau Müller auch der Meinung sein, dass die Ukraine ein Feind des Westens sei. Sie dürfen diese Meinung auch im Internet vertreten, auch dann, wenn sie auf YouTube oder X Millionen von Follower haben.

Genau das haben die amerikanischen Polit-Influencer Benny Johnson, Dave Rubin und Tim Pool gemacht. Nur hat sich jetzt herausgestellt, dass sie dafür verdeckt Zahlungen aus Russland erhalten haben. Das US-Justizministerium wirft zwei Russen vor, dass sie über eine amerikanische Produktionsfirma Einfluss auf die Blogger und YouTuber genommen haben. Die Russen sollen fast zehn Millionen Dollar an ein Unternehmen überwiesen haben, das Videos und Podcasts über zahlreiche Plattformen wie etwa TikTok, Instagram und YouTube veröffentlicht. Das Geld macht die Sache in den USA strafbar – die Meinungen der YouTuber sind es nicht. Unser fiktiver Despot reibt sich weiter die Hände.

2. Problem: Der Staat darf kein «Wahrheitsministerium» gründen. In einer liberalen Demokratie muss die Wahrheit immer verhandelbar sein. Das gilt auch und gerade für wissenschaftliche Erkenntnisse. Ganz abgesehen davon, dass auch in den Naturwissenschaften Fakten und Meinungen schwieriger zu trennen sind als man meint. Natürlich gibt es trotzdem so etwas wie einen wissenschaftlichen Konsens und jede Gesellschaft hat Eckwerte, die sie nicht in Frage stellt. In der Schweiz ist das die Bundesverfassung, übrigens ein wirklich kluger Text. Aber die Bundesverfassung gibt zu aktuellen politischen Fragen natürlich keine Auskunft.

Im Idealfall führt die offene Auseinandersetzung zwischen Wissenschaftlern, Politikern oder Künstlern dazu, dass sich die Gesellschaft auf eine Sicht, einen *common Sense* einigt. Wir sind aber heute von diesem Idealfall weit entfernt. Zum einen greift zum Beispiel Russland sehr konkret und teils massiv in den Diskurs ein und verbreitet Desinformation, unter anderem über gefälschte Websites westlicher Medien. Zum anderen sorgen die Algorithmen der digitalen Medien im Internet dafür, das es nicht zum sachlichen Aushandeln der Wahrheit kommt. Ziel der Algorithmen ist es, die Nutzerinnen und Nutzer möglichst lang auf einer Plattform zu halten. Sie fördern deshalb nicht das beste Argument, sondern Streit,

Emotionen, Skandale und extreme Inhalte. Unser Despot reibt sich weiter grinsend die Hände.

3. Problem: Der Staat darf keine Medien betreiben. Der Bund kann auf seinen Plattformen zwar über Statistiken, Vorlagen, Studien und seine Aktivitäten informieren, mehr aber auch nicht. Das ist auch richtig so. Die Medien haben in einer Demokratie als vierte Gewalt eine Watchdog-Funktion. In strenger Lesart heisst das auch: Der Staat darf die Medien nicht unterstützen, weil er sei nicht beeinflussen darf. Das ist nachvollziehbar, hat aber verheerende Folgen: Das Internet hat die Geschäftsgrundlage der Medien zerstört, ohne Unterstützung wird die Medienlandschaft in der Schweiz weiter ausgedünnt. Journalistische Medien haben bald keine Chance mehr gegen Desinformation und Propaganda. Unser Despot klatscht vor Freude in die Hände. Der Westen macht es ihm wirklich leicht.

Können wir der Desinformation und der Propaganda wirklich nichts entgegensetzen? Gibt es keine Möglichkeiten, so etwas wie eine informationelle Landesverteidigung aufzuziehen? Was könnten die konkreten Messgrössen für eine solche Verteidigung unseres Informationsraums sein?

Gehen wir einmal davon aus, dass irgendwo auf der Welt ein Despot oder ein Regime der Schweiz durch Desinformation schaden will. Welche Messgrössen müsste eine informationelle Landesverteidigung erfüllen? Ich sehe drei konkrete Punkte:

1) Reaktionsgeschwindigkeit: Wie schnell können Regierung und Bundesverwaltung oder allenfalls Armee und Nachrichtendienst eine Desinformationskampagne erkennen?

2) Gegenmassnahmen: Mit welchen Mitteln kann der Bund auf eine Desinformationskampagne reagieren, wie kann es gelingen, die Öffentlichkeit zu erreichen und die Wahrheit zu verbreiten, insbesondere auf Plattformen, auf denen Fake News kursieren?

3) Wirksamkeit und öffentliches Vertrauen: Wie stark wird das Vertrauen der Öffentlichkeit durch eine Desinformationskampagne beeinträchtigt, und wie kann es wiederhergestellt werden?

Wie lassen sich diese Ziele erreichen? Einfach ist das nicht. Es ist wesentlich einfacher, ein feindliches Flugzeug abzuschiessen, als feindliche Fake News. Das heisst aber nicht, dass ein Land wie die Schweiz nichts tun könnte. Als Verteidigungsministerin würde ich von der Landesverteidigung drei Punkte einfordern. Ich würde also der Armee, dem Bundesnachrichtendienst oder der Cyber-Truppe drei Aufgaben geben.

1. Aufgabe: Überwachung von Fake News.

Der erste Schritt ist immer die Aufklärung. Das bedeutet: Bund, Armee, Regierung und Landesverteidigung müssen die aktuelle Lage in Sachen Fake News kennen. Welche Falschnachrichten kursieren gerade? Sind sie gefährlich? Welche Narrative verbreiten sie? Welche Ziele haben sie? Was oder wer könnte durch die Falschnachrichten destabilisiert werden? Wer bringt sie in Umlauf? Können wir juristisch oder technisch gegen

die Fake News vorgehen? Ein Land sollte heute die Nachrichtenlage in Bezug auf Falschnachrichten und Desinformation ähnlich präzise überwachen wie seinen Luftraum – und diese Informationen auch zugänglich machen.

2. Aufgabe: Handlungsbereitschaft herstellen.

Aufklärung alleine reicht nicht. Wenn eine Bedrohung durch Fake News auftaucht, stellt sich die Frage, was wir dagegen tun können. Anders als bei Flugzeugen und Panzern ist die Zahl der möglichen Bedrohungen und ihrer Erscheinungsformen unendlich gross. Als Armee würde ich deshalb eine Art ständigen Think Tank einrichten. Ein kreatives Beratergremium, das regelmässig zusammentritt und sich inhaltlich mit den Narrativen der Fake News und möglichen Gegenmassnahmen auseinandersetzt. Eine Art Anti-Desinformations-Writer-Room, jederzeit bereit, feindlichen Narrativen mit guten Ideen den Garaus zu machen.

3. Aufgabe: Sensibilisieren der Bevölkerung.

Der beste Schutz vor Angriffen aus dem Informationsraum wäre eine resiliente Bevölkerung. Wie liesse sich das erreichen? Eine Kampagne à la «Stop Aids»-Kampagne reicht nicht aus, weil es gegen Desinformation kein einfaches Gegenmittel gibt. Das (langfristig) wirkungsvollste Mittel sind die Schulen: Kinder und Jugendliche müssen den Umgang mit Desinformation und KI an den Schulen lernen. Nein, dafür braucht es kein neues Fach. Der erste Schritt wären Weiterbildungen für Lehrpersonen. Ich halte immer wieder Vorträge über Künstliche Intelligenz an Schulen und habe dabei festgestellt, dass die meisten Lehrpersonen durchaus intelligent sind. Ich bin überzeugt, dass sie, mit etwas Unterstützung, ihre Schüler und Studenten gut sensibilisieren und auf die Gefahren vorbereiten können.

Überwachen von Fake News, Handlungsbereitschaft herstellen mit einem kreativen Think Tank für Narrative, Sensibilisieren von Lehrpersonen – das sind drei Massnahmen, die problemlos umsetzbar sind. Ja, das kostet, aber es ist ganz bestimmt günstiger als ein neuer Panzer oder ein neues Flugabwehrsystem. Ganz zu schweigen von den Schäden, vor denen uns die kleine Investition in die informationelle Landesverteidigung bewahren könnte. Das Ziel muss sein, dass unserem vorgestellten Despoten das Lächeln vergeht. Das schaffen wir. Oder?

Basel 11. Oktober 2024, Matthias Zehnder **mz@matthiaszehnder.ch**

Quellen

Zehnder, Matthias (2017): *Die Aufmerksamkeitsfalle. Wie die Medien zu Populismus führen.* Basel: Zytglogge-Verlag

Zehnder, Matthias (2019): *Die digitale Kränkung. Über die Ersetzbarkeit des Menschen*. Zürich: NZZ Libro.

Einfach mit dem Handy diesen QR-Code scannen – und schon können Sie den Wochenkommentar unterstützen.

Werden Sie jetzt **Unterstützerin, Unterstützer** des Wochenkommentars!

Hier können Sie mit allen digitalen Zahlungsmitteln spenden oder sich bequem zu Hause einen Einzahlungsschein ausdrucken:

https://www.matthiaszehnder.ch/unterstuetzen/