Das virtuelle Terrornetz

Der IS und die Kaida nutzen das Internet raffiniert für Propaganda, Rekrutierung und Koordination

Ob zur Anschlagsplanung oder Eigenwerbung, im Netz scheinen Terroristen den Regierungen und Firmen stets einen Schritt voraus zu sein. Wie lässt sich das ändern?

DANIEL STAUFFACHER, REGINA SURBER

Eigentlich hätten wir es wissen müssen. Bereits 1990 prognostizierten Experten der Vereinten Nationen, dass der technische Fortschritt, den wir ungehemmt fördern, Phänomene unterstützen könnte, die wir bekämpfen möchten: Terrorismus, innerstaatliche Gewalt, ethnische und religiöse Intoleranz. 25 Jahre später ist allen klar, dass sich diese Warnungen bewahrheitet haben: Viele der jüngst aufgetauchten Terrororganisationen haben sich zu versierten Nutzern des Internets gemausert, insbesondere von Social-Media-Plattformen.

Die Liaison von IT und IS

Die Fachkenntnis und das Raffinement, mit welchen diese Gruppierungen die Informationstechnologien nutzen, haben viele überrascht. Beispiele gibt es genügend: Die Terrormiliz Islamischer Staat (IS) verteilt Anleitungen an ihre Mitglieder, in denen sie bestimmte Online-Plattformen empfiehlt und erklärt, wie man das Risiko minimiert, abgehört zu werden. Ferner benutzt der IS das Internet unmittelbar nach seinen Anschlägen, wenn das Potenzial, Neumitglieder zu rekrutieren, besonders gross ist. Al-Kaida verteilte über ihr Online-Magazin «Inspire» Anleitungen zum Bombenbau, was als eine der Inspirationsquellen für den Anschlag am Boston-Marathon 2013 gilt. Die der IS-Ideologie verwandte Gruppierung «Wafa Media Foundation» kündigte im Juni Anschläge in Spanien an und ermutigte private Einzelkämpfer, Spanier zu entführen. Auch pflegen unzählige radikalisierte Personen gekonnt Social-Media-Konten.

Das Internet ist für Terrororganisationen also Kapital. Es vereinfacht die Kommunikation, die Propaganda, die Aufforderung zu Gewalt, die Rekrutierung von Mitgliedern, den Wissenstransfer sowie die finanzielle Abwicklung von Anschlägen. Kombiniert, verstärken diese Funktionen die Wirkungsmacht von Terrorgruppen enorm. Wenn Rekrutierung und Kommunikation nicht mehr nur physisch, sondern auch im Netz stattfinden, nützen klassische militärische Ansätze wenig. Das bekräftigt auch der Uno-Generalsekretär in seinem jüngsten Bericht: Die gegenwärtigen militärischen und wirtschaftlichen Massnahmen gegen den IS haben nicht geholfen, seine Nutzung des Cyberspace zu reduzieren.

Was entgegnet man dieser neuen Form der Terrororganisation – insbesondere angesichts des exponentiell wachsenden technischen Fortschritts? Wie können Regierungen, die im heutigen internationalen System das Gewalt- und Sicherheitsmonopol besitzen, wirkungsvoll gegen einen Gegner vorgehen, der sich Dienstleistungen bedient, die hauptsächlich von privatwirtschaftlichen Akteuren angeboten werden?

Ideen aus dem Kalten Krieg

Auf nationaler Ebene fokussieren sich die Reaktionen erstens auf die Deradikalisierung und die Entkräftung von ideologischen Botschaften im Internet. Verwendet werden oft Propagandastrategien, welche aus den Zeiten des Kalten Krieges stammen. Beispiele sind die sogenannte Counter-Initiative des Vereinigten Königreichs oder das «Madison Valley Wood»-Projekt in den USA.

Zweitens verpflichten Staaten Internetfirmen dazu, bedrohliche Inhalte entweder von vorneherein zu blockieren oder vor der Veröffentlichung herauszufiltern. Diese Regulierungsmassnahmen basieren allgemein auf rechtlichen Grundlagen. Allerdings stützen einige Länder diese Weisungen nicht auf offizielle Rechtstexte, sondern auf die Nutzungsbedingungen der IT-Unternehmen ab. Die Regulierungsmassnahmen sind in diesem Falle aussergesetzlich. Ein Beispiel hierfür ist die United Kingdom Counter-Terrorism Internet Referral Unit (CTIRU), durch deren Aufforderung seit 2010 mehr als 163 000 Online-Inhalte auf diversen Websites gelöscht worden sind.

Auf der inter- und supranationalen Ebene konzentrieren sich die Reaktionen ebenfalls auf die Verbreitung von Gegennarrativen sowie die Filterung und Überwachung von Inhalten. Das Counter-Terrorism Executive Directorate erarbeitet zurzeit einen Vorschlag für eine Rahmenvereinbarung, um den von IS und al-Kaida verwendeten Narrativen entgegenzuwirken. Die Internet Referral Unit der EU ist eine der CTIRU ähnliche Institution, welche terroristisch motivierte Inhalte im Netz identifiziert und den EU-Mitgliedstaaten meldet.

Bei staatlichen Regulierungsmassnahmen ist das Einbeziehen der Privatwirtschaft – vor allem im Bereich der Informationstechnologie – essenziell. Leistungsträger wie Twitter, Facebook und Microsoft besitzen eine enorme Macht im Cyberspace. Viele dieser Unternehmen, besonders aus dem Bereich der Social Media, sahen sich bisher jedoch gezwungen, selbständig Massnahmen gegen die terroristische Nutzung ihrer Produkte zu ergreifen. Sie löschen deshalb vermehrt eigenhändig Inhalte von ihren Websites. Twitter etwa hat innert sieben Monaten 125 000 Benutzerkonten mit Verbindungen zu Terroristen von seiner Plattform entfernt. Viele Firmen ändern auch die Nutzungsbedingungen und verbieten die Veröffentlichung von «terroristischen Inhalten» auf ihren Websites. Das Problem ist, dass der Terminus nicht einheitlich definiert ist. Microsoft stützt sich deshalb auf eine Liste des Uno-Sicherheitsrates: Jegliches Material, welches mit den darauf aufgeführten Organisationen in Verbindung steht, stuft Microsoft als «terroristisch» ein und entfernt es.

Unsicherheit bleibt

Terroristische Inhalte im Netz können also gelöscht werden – aber an anderen Orten im Internet genauso rasch wieder auftauchen. Um dies zu verhindern, investieren Firmen neuerdings in Technologien, die Inhalte erkennen und entfernen, auch nachdem sie schon von einer Website gelöscht worden sind. Dies entlastet vor allem kleinere Firmen, die keine Ressourcen für derartige Kontrollmechanismen aufbringen können.

Die entscheidende Frage lautet allerdings: Sind diese Massnahmen effektiv? Es ist schlicht zu früh, um das zu beantworten. Auch ist ungewiss, wie Regierungen und Firmen den Erfolg dieser Ansätze messen können. Ferner ist offen, wie sich Staaten an die Herausforderungen, die mit der technischen Entwicklung einhergehen, anpassen können.

Eine wiederkehrende Frage ist auch, ob man gar die terroristische Nutzung des Internets unterstützen statt unterdrücken soll. Wenn gelöschte terroristische Inhalte an anderen Orten im Netz sofort wieder auftauchen, ist das Filtern nur eine kurzfristige Lösung, die enor-

me Ressourcen verschlingt. Erlaubt man hingegen terroristische Inhalte, können Strafverfolgungsbehörden die Urheber einfacher überwachen und allenfalls Anschläge verhindern.

Des Weiteren werfen diese Entwicklungen komplexe normative Fragen auf: Kann man die staatliche Sicherheitsverantwortung mit den Anforderungen des Rechts auf Meinungs- und Informationsfreiheit in Einklang bringen? Welche Verantwortung tragen private Akteure in der Bekämpfung der terroristischen Nutzung von Informationstechnologien, und worauf basiert diese Verantwortung (Menschenrechte, Nutzungsbedingungen, Vertragsvereinbarungen)? Dürfen Regierungen die Durchsetzung ihrer Regulierungsmassnahmen vollständig an private Firmen auslagern?

Wenn sich Regierungen immer stärker auf technisch ausgerichtete Lösungen verlassen, ignorieren sie strukturelle Faktoren, die für das Entstehen des Terrorismus ursprünglich verantwortlich waren. Hart erarbeitete Prinzipien wie Mitsprache, Transparenz und Verantwortlichkeit in der Entscheidungsfindung werden so auf den zweiten Platz verwiesen. Es liegt auf der Hand, dass so viele verschiedene Akteure wie möglich in die Diskussionen über Herausforderungen, Lösungen, die Beurteilung der Effektivität und der sozialen Auswirkungen der Gegenmassnahmen involviert werden müssen. Internationale Initiativen wie der ICT Sector Guide on Implementing the Business and Human Rights Principles der EU, die Principles on Freedom and Privacy der Global-Network-Initiative, sowie die ICT4Peace-UNCTED-Initiative bieten Diskussionsplattformen und integrieren Akteure aus Politik und Privatwirtschaft.

Gleichzeitig müssen wir mit der rasanten technologischen Entwicklung Schritt halten. Künftige Technologien werden sicherlich unser heutiges Vorstellungsvermögen sprengen, deswegen müssen wir über bisherige Grenzen hinausdenken. Überwachung, Filterung und Gegennarrative mögen helfen, aber genügen wahrscheinlich kaum. Innovationen, gepaart mit Pragmatismus und extremer Schnelligkeit, sind unerlässlich.

Dr. Daniel Stauffacher ist ehemaliger Schweizer Botschafter und Gründer der ICT4Peace-Foundation. **Regina Surber** ist Mitarbeiterin bei ICT4Peace.