Der Teufel steckt in der Anwendung

Der Teufel steckt in der Anwendung

Ist Verschlüsselung ein Menschenrecht oder eine Waffe von Kriminellen? Technische Lösungen sind ambivalent und können guten wie auch schlechten Zwecken dienen. Deshalb ist ihre Regulierung hochpolitisch – und für alle relevant.

von Myriam Dunn Cavelty

Bei der Konzipierung des Internets als Kommunikationsmittel in den späten 1960er-Jahren stand die Funktionalität im Zentrum. Die Sicherheit spielte hingegen kaum eine Rolle – der Kreis der Nutzer war klein, man kannte und vertraute sich. Niemand konnte sich vorstellen, dass dieselbe Netzwerktechnologie später einmal Milliarden von teilweise hoch sicherheitsrelevanten Geräten verbinden und Zettabytes von Daten generieren würde. Damals, vor rund 50 Jahren, wurde die Grundlage für ein ausfallsicheres Netzwerk geschaffen, in welchem Informationen jedoch standardmässig unverschlüsselt ausgetauscht werden.

Eines haben die Entwickler des Internets nicht berücksichtigt: Unverschlüsselte Daten sind leider unsichere Daten. Kryptografie ist als einer der wichtigsten Bausteine der IT-Sicherheit zu verstehen: Verschlüsselung ist zwingend nötig, um die Vertraulichkeit, Integrität und Authentizität von Daten sicherzustellen – und zwar bei deren Speicherung, Übertragung und Verarbeitung. Aus technischer Sicht gilt: Ohne Kryptografie kann es keine Cybersicherheit geben.

Unvorhergesehene Gefahren

Nur: Die technische Sicht reicht meistens nicht aus, um die Auswirkungen komplexer Interaktionen zwischen Technik, Gesellschaft und Politik zu verstehen. Im Gegenteil: Der teilweise missionarische Glaube an technische Lösungen, die alle gegenwärtigen Probleme der Menschheit zu lösen vermögen, führt bei technischen Experten und Entscheidungsträgern regelmässig zu Erstaunen oder gar Frust – die Technologien erzielen nicht immer die intendierten, «guten» Effekte, sondern können in unvorhergesehener Weise zu gesellschaftlichen Unsicherheiten beitragen. Um nachzuvollziehen, warum scheinbar «gute» Technologien negative oder zumindest sehr ambivalente Wirkungen entfalten, müssen wir Technologie im Sinne von Wissenschafts- und Technikforschung (auf Englisch: Science Technology Studies, STS) als ein soziales Konstrukt verstehen. Technologien sind nicht bloss starre Objekte, die Einfluss auf die soziale Welt ausüben, ohne auch durch sie geformt zu werden.

Bereits in ihrer Entstehungsphase werden Technologien unterschiedlich interpretiert und erhalten ihre Form und ihre Bedeutung erst in einem kontroversen Zusammenspiel relevanter sozialer Gruppen mit unterschiedlichen Interessen und unterschiedlichen Wertvorstellungen. Diese interpretative Flexibilität und Nutzung führen zu technologischer Ambivalenz, also einem unweigerlichen Widerspruch der Möglichkeiten, die Technologien uns bieten: Allesamt können sie die Menschheit voranbringen, genauso gut aber auch von ihr missbraucht werden. Bei der Verschlüsselungstechnologie zeigt sich diese Ambivalenz sehr anschaulich: Journalisten und Aktivisten in autoritären Systemen sind auf verschlüsselte Kommunikation angewiesen, um sicher zu kommunizieren – die organisierte Kriminalität benutzt jedoch die gleiche Technologie, um Drogen, Waffen und andere illegale Güter anzubieten und zu verkaufen. Die Wirtschaft schützt ihre Daten mittels Kryptografie vor den Ausspähungen durch Konkurrenten – Kriminelle verwenden Verschlüsselung bei Ransomware-Attacken, um befallene Firmen zu erpressen. Der weltweite Schaden dieser Art von Cyberattacken wird auf rund 20 Milliarden US-Dollar im Jahr 2021 geschätzt – Tendenz steigend.

Kryptografie ist eine Grundvoraussetzung für sichere digitale Kommunikation – und wird gleichzeitig für schädliche Dinge verwendet. Diese Ambivalenz von Kryptografie ist ein seit Jahrzehnten diskutiertes, ungelöstes, sogar *unlösbares* Problem: Die «negative» Nutzung lässt sich nicht unterbinden, ohne dass die «positive» ebenfalls darunter leidet. Das lässt sich exemplarisch an den über die Jahre regelmässig wiederkehrenden «Crypto Wars» aufzeigen: Darunter versteht man Bestrebungen von Sicherheitsbehörden in demokratischen Ländern, die private Verschlüsselung von Daten einzuschränken oder den Export von starken Verschlüsselungstechnologien zu unterbinden. Diese Bestrebungen werden wiederum durch Bürgerbewegungen, Fachexperten und Unternehmen bekämpft. Die unterschiedlichen Interpretationen der gleichen Technologie kommen durch die Priorisierung von unterschiedlichen Interessen und Werten zu-

«Journalisten und Aktivisten in autoritären Systemen sind auf verschlüsselte Kommunikation angewiesen – die organisierte Kriminalität benutzt jedoch die gleiche Technologie, um Drogen oder Waffen zu verkaufen.»

Myriam Dunn Cavelty

Myriam Dunn Cavelty, zvg.

stande, die auch andersgeartete Gefahrenperzeptionen und Lösungsansätze abbilden.

Bei der Debatte um Kryptografie stehen auf der einen Seite die Nachrichtendienste mit ihrem «Going Dark»-Argument: Sie glauben, dass durch den grossflächigen Einsatz von verschlüsselter Kommunikation das effiziente Abhören und Überwachen von Datenströmen verhindert werde – die Gefahr sei somit, dass Nachrichtendienste bald «im Dunkeln» sitzen und nicht mehr gegen Terroristen vorgehen könnten (was erwiesenermassen nicht stimmt). In einer Abwandlung dieses Arguments führen Strafverfolgungsbehörden an, dass die Nutzung kryptografischer Verfahren so zu regulieren sei, dass der Klartext der übertragenen Daten bei Bedarf eingesehen werden könne. Dies soll durch mandatierte Hintertüren oder das Hinterlegen geheimer Schlüssel bei einer Behörde ermöglicht werden. Bei dieser Sichtweise legitimiert der Kampf gegen den Terrorismus oder die organisierte Kriminalität die Einschränkung von Bürgerrechten, insbesondere des Grundrechts auf informationelle Selbstbestimmung oder der Anonymität im Netz. Erst im Dezember 2020 hat der EU-Ministerrat eine umstrittene Resolution angenommen, in der für WhatsApp, Telegram und andere Messenger, die Ende-zu-Ende-Verschlüsselung einsetzen, ein Zugang für Behörden gefordert wird.

«Anstatt technologische Entscheide bequem an Experten zu delegieren, können und müssen wir alle unsere technische Zukunft aktiver gestalten.»

Myriam Dunn Cavelty

Wir können mitbestimmen

Demgegenüber stehen Plädoyers wie etwa ein solches für ein Menschenrecht auf Verschlüsselung, wie es 2015 vom Sonderbeauftragten der Vereinten Nationen für Meinungsfreiheit vorgebracht wurde. Dieser Sichtweise liegt ein anderer Sicherheitsbegriff zugrunde, der sich viel stärker am Individuum und dessen Rechten orientiert: Die Verschlüsselung wird als Mittel zur Selbstverteidigung gegenüber dem Schnüffelstaat oder der Internetkriminalität präsentiert. Zudem argumentieren die Aktivisten, dass ein sicheres System per se keine Hintertüren haben könne: Mandatierte Hintertüren oder hinterlegte Schlüssel stehen nämlich nicht nur den Strafverfolgungsbehörden offen, sondern potentiell auch kriminellen Hackern und Nachrichtendiensten anderer Staaten. Kryptoregulierungen würden also den nötigen Schutz für die Wirtschaft und die Gesellschaft schwächen und somit das allgemeine Gefahrenpotenzial auch aus Sicht der kollektiven Sicherheit erhöhen.

Welche dieser Sichtweisen bewerten wir nun als die richtige? Ob Effekte von Technologien positiv oder negativ gesehen werden, lässt sich nie pauschal beantworten – die Anwendungsambivalenz ist inhärent und lässt sich nicht ausmerzen. Unser Umgang mit ambivalenten Technologien muss somit unweigerlich mit einer Abwägung von Chancen und Risiken verbunden sein. Wenn wir den Erkenntnissen von Science Technology Studies folgen, ist der Pfad technischer Innovation nicht vorgezeichnet: Technologien werden von Menschen entwickelt, deren Entscheidungen von politischen, sozialen, wirtschaftlichen und kulturellen Faktoren abhängen. Wir, die Gesellschaft, können mitbestimmen, ob und wie wir Technologien einsetzen, und wir, die User, entscheiden über die Nutzen der Technologie.

Diese Sichtweise gibt uns mehr Handlungsmacht, nimmt uns aber auch in die Pflicht. Anstatt technologische Entscheide bequem an Experten zu delegieren, können und müssen wir alle unsere technische Zukunft aktiver gestalten. Digitale Technologien stechen dadurch hervor, dass sie unvorhergesehenes menschliches Verhalten hervorrufen. Bevor sie ihre Wirkungen entfalten, können sie nicht sinnvoll reguliert werden, denn erst durch die Nutzung entstehen neue Effekte. Das macht Technologien wie die Kryptografie in ihrem Kern durch und durch politisch: Sie müssen Gegenstand einer permanenten Beobachtung, Diskussion und Bewertung bleiben. ‹

Myriam Dunn Cavelty
ist Dozentin und stellvertretende Leiterin des Center for Security Studies (CSS) der ETH Zürich.

Illustration von Stephan Schmitz.