

CAPITAL-Kolumne 23/2001  
Ende der Anarchie

Haben Sie das auch gelesen? Da die Terroristen des 11. Septembers wussten, dass ihre Telefone abgehört würden, benutzten sie zur Vorbereitung ihres weltverändernden Verbrechens extensiv das Internet. Und zwar mit Steganographie. Das bedeutet, dass Informationen in allgemein zugänglichen bildlichen Darstellungen versteckt werden. Und wo tat man das, weil hier die meisten Menschen draufschauen und die Überwachung der Nutzung daher am schwersten fällt? Auf pornographischen Seiten. Stellen wir uns das bitte vor: In den Abbildungen von Brüsten sich räkelnder Mädchen sind Informationen über Terminpläne, Angriffsziele und -techniken versteckt, die sich Verbrecher in aller Welt durch Vergleich des Originalbildes mit einer leicht manipulierten Version erschließen können. Das Öffentlichste wird das Geheimste, die Perversion der Pornoindustrie gesteigert zur Perversion des Terrors als Kriegsform des dritten Jahrtausends.

Inzwischen denke ich am Bildschirm sitzend ständig darüber nach, was hinter seiner Oberfläche alles versteckt sein könnte. Wenn wir nicht aufpassen, kann das Internet zum optimalen Kommunikations- und Steuerungsmedium für global agierende Terrorgruppen werden. Welch perfide Ironie der Mediengeschichte! War das Netz der Netze doch entwickelt worden als friedliche Kommunikationsbasis für Wissenschaftler weltweit und für Krisenfälle militärischer Art, wenn Knotenpunkte im globalen Telefonnetz durch Kriegsakte zerstört würden. Und welche schöne und nützliche Perspektiven haben wir nicht seitdem am Internet kennen und schätzen gelernt! Wir können schnellstens und billig mit Partnern auf der ganzen Welt ohne Zeitverzögerung kommunizieren. Wir können mit neuesten Knowbots in der größten Datenbank der Welt innerhalb von Sekunden all die Informationen finden, die wir zur Beantwortung einer Frage oder zur Lösung eines Problems brauchen. Wir können Preise und Angebote auf der ganzen Welt vergleichen, Waren nach Hause bestellen, Geschäftsvorgänge aller Art beschleunigen und optimieren, personalisierte Nachrichten und aktuellste Kursverläufe auf den Bildschirm bekommen oder 24 Stunden am Tag lernen.

Kurzum: Das Internet verwirklicht viele menschliche Wunschträume. In ihm hat die globalisierte Informationsgesellschaft demokratischer Prägung ihr Medium gefunden.

Und nun wird es zum Handwerkszeug des Terrors. Kürzlich las ich, dass der Vatikan erwäge, einen Schutzheiligen für das Internet zu benennen. Den kann es jetzt brauchen. Schon vor bin Laden und seinen Todeskommandos hatte es dunkle Seiten: Aushebelung des Jugendschutzes, Nazi-propaganda, Urheberrechtsverletzung im großen Stil, global agierende Viren, Daten- und Kreditkartenmissbrauch, Hacker im Computer des Pentagons, Hassseiten, Mobbingfeldzüge etc. Aber dass seine globale Verfügbarkeit, seine schnelle Zugänglichkeit und seine chaotische Struktur es nun extrem geeignet für die Vorbereitung internationalen Verbrechens machen, ist unerträglich. Die besten Köpfe der Welt müssen ran, um hier Riegel vorzuschieben. Ich weiß, dass das Netz der Netze ein Stück seiner Stärke und Einzigartigkeit daraus zieht, dass es niemandem gehört und keinem unterworfen ist. Aber Freiheit ist nur dann sinnvoll, wenn sie sich mit Verantwortung paart. Das Argument, nur anarchisch und total unkontrolliert sei das Internet gut und produktiv, muss angesichts von

mehr als 6000 Toten und dem Schmerz ihrer Angehörigen und Kollegen ein wenig zurückstehen.

Die Herausforderung ist gigantisch, stehen wir doch auch vor ungeahnten Formen des asymmetrischen Cyberwars, bei denen ein paar Mausklicks Stromversorger, Telefonnetze, Fluggesellschaften, Börsen oder militärische Infrastrukturen lahmlegen oder desorientieren. Abhörsysteme wie „Carnivore“ (Fleischfresser), mit dem E-Mails und Chatrooms nach bestimmten Schlüsselbegriffen überprüft und dementsprechend aussortiert werden, oder „Omnivore“ (Allesfresser), mit dem das Suchen nach verdächtigen Stichwörtern aktenkundig wird, werden wir zu akzeptieren haben. Auch Verschlüsseltes muss der Staat im Verdachtsfall nach richterlichen Vorgaben mitlesen dürfen. Natürlich: Jede neue Technologie kreiert neue Umgehungsmöglichkeiten. Wir werden sehr viel Geld ausgeben müssen und uns trotzdem wie Sisyphos fühlen. Aber wir haben keine andere Wahl.

Schon das Wissen um die Bemühungen wird Unsicherheit bei potentiellen Tätern schaffen und viele abschrecken. Jeder Fahndungserfolg muss daher kommuniziert werden. Zufälle werden helfen, wenn Datenmengen zu gigantisch und kriminelle Energien zu groß sind. Den RAF-Terror im eigenen Lande haben wir trockenlegen können, ohne zum Big-Brother-Staat zu werden. Das sollte der Staatengemeinschaft beim globalisierten Cyberterror auch gelingen.