AUSSENANSICHT

Alles unter Kontrolle

Kameras, Computer und militärische Hightech-Strategien sollen Verbrechen verhindern. Doch technikfixierte Sicherheitspolitik mündet in totale Überwachung. *Von Jutta Weber*

Zielen, identifizieren und verfolgen – so lässt sich die Logik moderner, netzwerkzentrierter High-Tech-Kriegsführung charakterisieren. Auf der Basis eines komplexen Netzwerks digitaler Rechner und Sensoren soll ein umfassender Überblick über den Kampfraum in Echtzeit hergestellt werden. Dieser Idee liegt die Vorstellung zugrunde, dass sich militärischer Erfolg durch Informationshoheit, technische Überlegenheit und enge Verzahnung von Aufklärung, Kommandozentralen und Waffentechnologie herstellen lässt.

Erstaunlicherweise dominiert diese militärstrategische Logik auch zivile, demokratisch legitimierte Sicherheitspolitik. Ein Beispiel hierfür ist DAS – das neue *Domain Awareness System* der New Yorker Polizei, das in Kooperation mit Microsoft entwickelt und vor kurzem vorgestellt wurde. Bei der Einweihung pries der New Yorker Bürgermeister Michael Bloomberg das System als Anti-Terror-Wunderwaffe. Das *Domain Awareness System* führt in Echtzeit Daten von 3000 Überwachungskameras, 1600 Strahlungssensoren sowie mehr als 100 stationären und mobilen Nummernschild-Scannern zusammen, speist Polizeifunk und Notrufe in sein Netz ein und gleicht die Daten von Verdächtigen in riesigen Datenbanken ab. Es erlaubt, Bewegungen von Personen oder Fahrzeugen über weite Strecken in Echtzeit zu verfolgen oder über Wochen nachzuvollziehen. Ein eng gestricktes Sensorensystem soll dafür sicherstellen, dass nichts im öffentlichen Raum unbeobachtet bleibt. Die Planung eines Terrorakts oder auch nur ein ungewöhnliches Vorkommnis soll in Echtzeit verfolgt und Verbrechen präventiv erkannt werden.

Nun könnte man argumentieren, dass wir es in New York mit den Spätfolgen des amerikanischen 9/11-Traumas zu tun haben und eine ähnliche Situation schon aufgrund des Datenschutzes in Europa undenkbar wäre. Doch die militärische Logik durchzieht auch europäische Sicherheitsarchitekturen. Augenfälligstes Beispiel für militärische High-Tech-Aufrüstung waren die Olympischen Spiele in London, bei der mehr als 13 000 britische Soldaten sowie Flugzeugträger, Boden-Luft-Raketen und unbemannte Drohnen im Einsatz oder wenigstens einsatzbereit waren. Zeitweise wurden Datenschutz und Grundrechte außer Kraft gesetzt. So wurden friedliche Demonstranten kurzzeitig verhaftet und ihnen das Betreten der olympischen Zone für die Dauer der Spiele verboten. Was man bisher nur von G-8-Gipfeln kannte, wird zur Normalität bei Groß-Events.

Der Blick auf die Sicherheitspolitik der EU zeigt, dass es eine recht einseitige Fokussierung auf Sicherheitstechnologien gibt und traditionelle Aufklärungsarbeit in den Hintergrund gedrängt wird. So fordert die aktuelle EU-Sicherheitsstrategie des Stockholmer Programms mehr technische Werkzeuge und eine umfassende Informationsmanagement-Strategie. Der Bericht der EU-Kommission zu den Sicherheitsprojekten im letzten Forschungsrahmenprogramm hält fest, dass es einer technologisch gestützten Wachsamkeit bedürfe, um die Freiheit gegen potenzielle Gefahren zu schützen. Obwohl sich in Deutschland schon länger zivilgesellschaftlicher Widerstand gegen eine zunehmend drakonische Sicherheitspolitik regt, lancierte das Wissenschaftsministerium ein 100 Millionen Euro schweres Forschungsprogramm für zivile Sicherheitsforschung, das in der gleichen Logik mit neuen Bedrohungen und der Verwundbarkeit kritischer Infrastrukturen argumentiert. Aus der Sicht von Wissenschaftsministerin Annette Schavan hängt Sicherheit „vom Vorsprung in Wissenschaft und Forschung ab und der Umsetzung in Organisation und Technologie“.

Statt Präventionsparanoia brauchen wir eine nüchterne, sozial verträgliche Politik

Nicht hinterfragt wird in diesem digitalen Traum von der perfekten Bewegungs-, Zugangs- und Raumkontrolle, ob diese High-Tech-Ideen für die Lösung eines gesellschaftlichen Problems geeignet sind – und welche Art von Sicherheit sie produzieren. Im Konzept der netzwerkzentrierten Kriegsführung und der verteilten Sicherheit gelten Kommunikationsstrukturen als das zu verteidigende Herzstück der Gesellschaft und gleichzeitig als wichtigste Waffe im Krieg gegen Terror oder Kriminalität. Da fast alle Infrastrukturen – vom Verkehr bis zur Energieversorgung – auf Informationsnetze angewiesen sind, sind sie anfälliger für Cyberbedrohungen geworden. Diese „kritischen“ Infrastrukturen durchziehen alle Lebensbereiche und sind ein wesentlicher Grund dafür, warum die Grenzen zwischen militärischer und ziviler Sicherheit, von Krieg, Strafverfolgung und Alltag zunehmend verschwinden. Durch 9/11 und seine mediale Inszenierung haben sie an kultureller, identitätsstiftender Bedeutung gewonnen, derer sich die Politik durchaus bewusst ist.

Den Ausbau exzessiver Sicherheitsarchitekturen verdanken wir vor allem einer technowissenschaftlichen Rationalität, die mit Hilfe von Komplexitätstheorie, Computersimulation und Systemanalyse unvorhersehbare Gefahren modellieren will, anstatt konkrete Gefahren zu bekämpfen. Der Fokus dieser Logik ist das Unvorhersehbare, das man nun einkreisen und abwehren will. Eine Logik, die sich der Bekämpfung des Nichtkalkulierbaren verschreibt, ist aber problematisch, weil sie permanent neue Anforderungen produziert. In der Praxis führt diese Techno-Security zu einer recht konventionellen Gefahrenbekämpfung, die Wahrscheinlichkeiten durchexerziert. So stufen „smarte“ Kameras schon den kurzfristig abgestellten Koffer oder hektische Bewegungen von Passanten als potenzielle Bedrohung ein. Wenn Computerzeitschriften ihren Lesern empfehlen, „problematische“ Stichwörter in E-Mail oder SMS zu vermeiden oder ihre Handys in der Nähe von Demonstrationen auszuschalten, dann hat diese Art der Überwachung unseren Alltag und unsere Verhaltensweisen bereits grundlegend verändert.

Darum reicht es auch nicht, Datenschutz und das Recht auf Privatheit einzufordern. Es gilt vielmehr, das Verständnis von Sicherheit als vermeintlichem All-Gefahren-Schutz als das eigentliche Problem zu erkennen – und mit ihr eine militär- wie sicherheitsstrategische Logik, die *Worst-Case*-Szenarien vorhersehen und beherrschen will und dabei in totaler Raum-, Bewegungs- und Zugangskontrolle mündet. Bei ein wenig kritischer Distanz wirkt der „Lösungsansatz“ dieser Sicherheitslogik eher wie Präventionsparanoia. Wir brauchen eine nüchterne und zugleich sozial verträgliche Sicherheitspolitik, die sich weniger populistischer und technokratischer Mittel bedient als gesamtgesellschaftliche Fragen im Auge behält und der Logik der Angst eine deutliche Absage erteilt.

Jutta Weber, 49, ist Technikphilosophin und Professorin für Medienwissenschaften an der Universität Paderborn. Zu ihren Arbeitsschwerpunkten gehört die Technikforschung in Informatik, Robotik und künstlicher Intelligenz. FOTO: CZOGALLA