«Abhängigkeit vom Internet macht verwundbar»

VON JAN STROBEL

Myriam Dunn Cavelty ist Leiterin des Forschungsteams «Neue Risiken» an der ETH. Mit ihren 34 Jahren berät die Wissenschaftlerin Regierungen und Unternehmen. Dabei steht für sie eine Gefahr besonders im Mittelpunkt: die Kriminalität im Netz.

Tagblatt der Stadt Zürich: Myriam Dunn Cavelty, wir sind tagtäglich Risiken ausgesetzt, ob ich auf dem Velo unterwegs bin oder in der Küche hantiere.

Myriam Dunn Cavelty: *Das Individuum ist tatsächlich einer Menge von verschiedensten Risiken ausgesetzt, wie zum Beispiel demjenigen, auf dem Fussgängerstreifen angefahren zu werden. Wir beschäftigen uns aber nicht mit solchen Risiken, sondern ausschliesslich mit denjenigen, die das Kollektiv etwas angehen, also den Staat und die Gesellschaft – und dies insbesondere im Bereich der Sicherheitspolitik. In diesem Bereich sind letztes Jahr vor allem sogenannte Cyber-Risiken ins Bewusstsein der breiteren Öffentlichkeit getreten.*

Stichwort Cyber-Risiken: Das Internet bietet uns Freiheiten, wie wir sie zuvor wohl nie gehabt haben. Wo lauern hier die grössten Gefahren?

Dunn Cavelty: *Das Internet ist eine grundsätzlich unsichere Technologie – es wurde nicht für den heutigen Nutzen gebaut, es hat viele Schwachstellen, und es ermöglicht weitgehend anonyme Übeltaten. Für Individuen lauern die grössten Gefahren in allerlei kriminellen Machenschaften, die mithilfe des Internets durchgeführt werden und die unter Umständen teuer werden können. Für Firmen ist neben der Cyberkriminalität vor allem die Cyberspionage ein Problem, für Regierungen wiederum vor allem der Datenklau. Darüber hinaus haben Regierungen für die Sicherheit der Bevölkerung zu sorgen und ihr Bestmöglichstes dafür zu tun, dass sogenannte «kritische Infrastrukturen», also zum Beispiel Energie oder Informationstechnik, zur Verfügung stehen.*

Sollten unsere Freiheiten zugunsten der Sicherheit beschnitten werden?

Dunn Cavelty: *Sobald sich Menschen in Gruppen zusammengefunden und sich auf Regeln des Zusammenlebens geeinigt haben, haben sie ein gewisses Mass an Freiheit für Sicherheit aufgegeben. Heute ist es nicht anders – jede Gesellschaft in demokratischen Staaten nimmt gewisse Einschränkungen der persönlichen Freiheit für die Garantie von Sicherheit in Kauf. Das Mass dieser Einschränkung ist keinesfalls fix, sondern kann und wird auch immer wieder verhandelt werden. Häufig hängt eine weitere Beschneidung von Freiheiten mit Grossereignissen zusammen. Im Bereich von Cyber-Risiken gibt es bisher keinen drängenden Grund, etwas an der Balance zu ändern. Je nachdem, wie sich die Situation entwickelt, kann es aber durchaus sein, dass sich das in Zukunft ändert.*

Macht das Internet unsere Gesellschaft aber nicht verwundbarer?

Dunn Cavelty: *Nicht das Internet per se – aber die Abhängigkeiten, die wir selber davon geschaffen haben.*

In den Medien geistert immer wieder der Begriff Cyberwar herum. Was genau ist darunter zu verstehen?

Dunn Cavelty: *In den Medien wird Cyberwar häufig für so ziemlich alle Phänomene verwendet, bei denen das Internet für aggressive Zwecke eingesetzt wird. Eine so breite Verwendung des Begriffs ergibt meiner Meinung nach jedoch wenig Sinn. Der Cyberkrieg ist eine in den Köpfen von Militärstrategen existierende Form des Krieges, bei der Krieg im Cyberspace geführt wird. Zum Beispiel sollen dabei kritische Infrastrukturen wie der Strom oder die Wasserversorgung mittels Hackerangriff lahmgelegt und somit der Krieg innert Sekunden entschieden werden.*

Das Interview: Myriam Dunn Cavelty

Ist ein solches Szenario glaubwürdig oder völlig realitätsfern?

Dunn Cavelty: *Der reine Cyberkrieg gilt unter Experten als sehr unwahrscheinlich. Schon heute aber haben Konflikte eine Cyber-Dimension; das wird sich in Zukunft einfach weiter verstärken.*

Welche Quellen benutzen Sie für Ihre Forschung?

Dunn Cavelty: *Wir benutzen nur offene Quellen – alles andere, also zum Beispiel Informationen von Geheimdiensten, kann man in der Forschung nicht verwenden, weil man sie nicht wissenschaftlich belegen kann.*

Sie beraten unter anderem auch Regierungen und Unternehmen. Welche Massnahmen können sie ergreifen, um sich vor Cyberkriminalität zu schützen?

Myriam Dunn Cavelty untersucht die Gefahren aus dem Internet. Bild: PD

Dunn Cavelty: *Erstens muss man das Problem einmal ernst nehmen – allzu viele tun dies noch nicht, häufig aus Kostengründen. Zweitens gilt es Massnahmen zu ergreifen, die unter dem Sammelbegriff Informationssicherheit bekannt sind. Informationssicherheit ist grundsätzlich eine Aufgabe der Leitung einer Organisation oder eines Unternehmens. Die operativen Massnahmen, die ergriffen werden müssen, variieren dann stark, je nach Art der Daten, die jemand schützen muss. Drittens müssen Angestellte sensibilisiert und befähigt werden. Viertens müssen sowohl Firmen untereinander wie auch Regierungen mit Firmen Informationen austauschen.*

Was kann der Einzelne tun?

Dunn Cavelty: *Auch für den Einzelnen gilt, wenn auch meistens im kleineren Stil, Informationssicherheit zu gewährleisten. Darunter fällt das Verwenden von Antiviren-Software, Firewalls, dem Updaten von Software, Verschlüsseln von sensiblen Daten. Aber wir müssen uns auch an Sicherheitsregeln halten, wenn wir im Internet surfen – genau so, wie wir im Strassenverkehr darauf bedacht sind, sicher zu fahren.*

Kann man sagen: Je offener die Gesellschaft, umso grösseren Gefahren ist sie ausgesetzt?

Dunn Cavelty: *Nein, so würde ich das nicht sagen. Es stimmt aber, dass offene Gesellschaften gewissen Gefahren mehr ausgesetzt sind als geschlossene. Dafür aber bieten offene Gesellschaften einen so grossen Mehrwert, dass wir viele Risiken gerne in Kauf nehmen.* ■

CURRICULUMVITAE

Geboren
1976 in Zürich.

Ausbildung
Studium der Geschichte und Politologie an der Uni Zürich.

Karriere
2005 Doktorat (summa cum laude) an der Uni Zürich, Leiterin des Teams «Neue Risiken» am Center for Security Studies an der ETH, seit 2010 forscht Dunn Cavelty auch in der Stiftung neue Verantwortung in Berlin.