

Wie krisenfest ist die Schweiz wirklich?

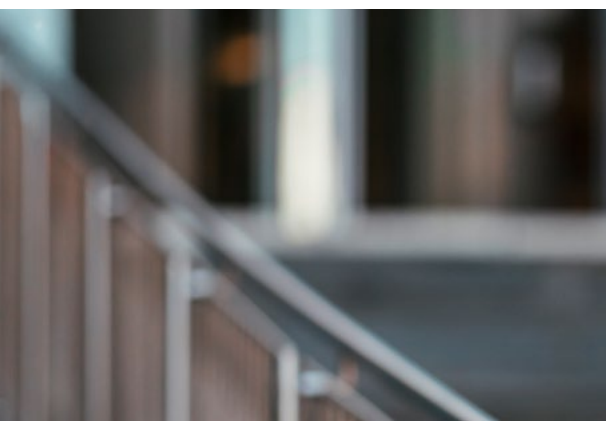
Interview mit Dr. Myriam Dunn Cavelty
Stv. Leiterin des Think Tanks ("Deputy Director")
am Center for Security Studies (CSS) der ETH Zürich

Cyberangriffe, Strommangellagen, geopolitische Abhängigkeiten und KI zeigen, wie eng technische, gesellschaftliche und wirtschaftliche Risiken heute miteinander verflochten sind. Im Gespräch mit den KPMG-Experten Prof. Dr. Reto Eberle und Dr. Matthias Bossardt erklärt Dr. Myriam Dunn Cavelty, weshalb Resilienz weniger in der Vermeidung einzelner Krisen als in der Vorbereitung, Urteilkraft und dem Verständnis von Abhängigkeiten liegt.

Prof. Dr. Reto Eberle (RE): *Das Center for Security Studies (CSS) der ETH Zürich untersucht sicherheitspolitische und soziotechnische Risiken. Was macht das CSS genau, und welche Rolle nehmen Sie dort ein?*

Dr. Myriam Dunn Cavelty (MDC): Das CSS ist mehr als ein Think Tank. Wir sind ein Kompetenzzentrum für internationale und schweizerische Sicherheitspolitik und nehmen seit 2022 im Auftrag des Bundes eine nationale Aufgabe wahr. Unser Auftrag beruht auf vier Pfeilern: Lehre und Weiterbildung, Forschung, Nachwuchsförderung und Politikberatung. Ich selbst arbeite über alle vier Bereiche hinweg. In der Forschung beschäftige ich mich vor allem mit digitalen Technologien an der Schnitt-

stelle zur Sicherheitspolitik, also mit Cybersicherheit, internationaler Politik und der Frage, wie Technologien Politik und Gesellschaft verändern. In der Lehre unterrichte ich unter anderem Cybersicherheitspolitik und bin im Masterstudiengang Politikwissenschaft tätig. Hinzu kommen Weiterbildungsformate sowie Coaching und Mentoring für jüngere Forschende. In der Politikberatung arbeite ich seit vielen Jahren mit der Bundesverwaltung zusammen, heute etwa zu Cybersicherheit, digitaler Souveränität und der Einbindung von Wissenschaft in das Krisenmanagement. Das Besondere am CSS ist genau diese Verbindung. Forschung, Lehre, Nachwuchsförderung und Beratung nähren sich gegenseitig.





Matthias Bossardt (MB): *Wie gelangen wissenschaftliche Erkenntnisse konkret zu Entscheidungsträgern in Politik und Wirtschaft?*

MDC: Unser Beratungsmodell ist dialogisch. Wir veröffentlichen nicht einfach Berichte, sondern arbeiten mit Bundesstellen und teilweise mit Kantonen, schaffen Dialogplattformen, führen Workshops durch und bringen Akteure über institutionelle Silos hinweg an einen Tisch. Besonders wichtig ist Antizipation: Wir versuchen Expertise aufzubauen, bevor ein Thema akut wird. Gleichzeitig halten wir Abstand, sobald ein Prozess in die eigentliche parteipolitische Auseinandersetzung übergeht. Wirkung messen wir deshalb weniger über Downloads als über qualitative Indikatoren. Werden Analysen in Entscheidungsprozesse aufgenommen, in parlamentarischen Vorstössen genutzt oder international referenziert? Entscheidend ist das über Jahre gewachsene Vertrauensverhältnis, bei gleichzeitig verteidigter akademischer Freiheit.

RE: *Welche Risiken fordern die Resilienz der Schweiz heute am stärksten heraus?*

MDC: Einzelrisiken wie Pandemie, Strommangellage oder bewaffnete Konflikte werden grundsätzlich recht gut analysiert. Die grössere Herausforderung liegt aber in ihrer Kombination. In der internationalen Politik sprechen wir von Polykrisen oder Polyrisiken: Risiken, die gleichzeitig auftreten, sich gegenseitig verstärken oder Kaskaden auslösen. Unsere starke Vernetzung ist dabei zugleich Stärke und Verwundbarkeit. Digitale Systeme, Lieferketten, Energieversorgung, Finanzsysteme und gesellschaftliche Reaktionen hängen eng zusammen. Genau solche Wechselwirkungen aber sind in klassischen Einzelrisikoplanalysen schwer abzubilden.

RE: *Das weckt Erinnerungen an die Finanzkrise. Viele Einzelrisiken waren bekannt, aber ihre Vernetzung wurde unterschätzt. Was folgt daraus für die Vorbereitung?*

MDC: Man muss komplexe Szenarien üben. Gerade bei soziotechnischen Risiken entscheidet nicht nur das Ereignis, sondern auch, wie Gesellschaft, Organisationen und Politik darauf reagieren. Übungen helfen, solche Dynamiken sichtbar zu machen. Sie erfordern allerdings Zeit und Ressourcen und führen manchmal auch zu unangenehmen Erkenntnissen. Deshalb ist es nicht genug, zu üben; man muss die gewonnenen Erkenntnisse auch konsequent umsetzen. Genau das fällt Institutionen schwer, weil präventive Investitionen heute Kosten verursachen, während ihr Nutzen erst im Ernstfall sichtbar wird.





«Cyber ist vom Ausnahmeereignis zum permanenten Hintergrundrauschen geworden.»

MB: Welche Rollen spielen dabei sogenannte kritische Infrastrukturen und wie werden diese definiert?

MDC: Kritische Infrastrukturen sind Systeme, Dienstleistungen oder Objekte, deren Ausfall gravierende Folgen für Bevölkerung, Staat, Gesellschaft oder Wirtschaft hätte. Entscheidend ist aber nicht nur, was wichtig ist, sondern was tatsächlich kritisch wird. Welche Auswirkungen hätte ein Ausfall? Welche Abhängigkeiten und Kaskadeneffekte entstehen? Gibt es Ersatz? Ein grosser Teil kritischer Infrastruktur liegt zudem nicht in staatlicher Hand. Deshalb braucht es Zusammenarbeit zwischen Staat und Privatwirtschaft. Besonders relevant sind Querschnittsinfrastrukturen wie Strom und digitale Netze, weil von ihnen viele andere Funktionen abhängen. Die Schwierigkeit ist, dass Unternehmen sich ihrer eigenen Rolle im Gesamtsystem und ihrer Abhängigkeiten nicht immer ausreichend bewusst sind.

RE: Strom ist eine solche Querschnittsinfrastruktur. Wie gut ist die Schweiz gegen Blackouts oder Strommangellagen geschützt?

MDC: Eine eindeutige Antwort ist kaum möglich, weil schon «ausreichend geschützt» schwer zu definieren ist und Resilienz sich oft erst im Ereignis zeigt. Wichtig ist die Unterscheidung zwischen Blackout, lokalem Stromausfall und Strommangellage. Seit 2022 wurde die Vorsorge für Mangellagen verstärkt, etwa durch Reserven, Notfallplanung und stärkere Sensibilisierung der Bevölkerung. Gleichzeitig üben einzelne Unternehmen sehr konkret, was bei einem länger dauernden Ausfall geschehen würde: Welche Standorte bleiben offen, wie werden Güter verteilt, was passiert bei Ausfall der Zahlungssysteme, wie koordiniert man sich mit Behörden? Solche Übungen machen Resilienz praktisch greifbar. Vorbereitung ist also keineswegs nur eine staatliche Aufgabe.

MB: Cyberangriffe treffen heute Unternehmen und Staaten gleichermassen. Wo liegen für die Schweiz die grössten Herausforderungen?

MDC: Cyber ist vom Ausnahmeereignis zum permanenten Hintergrundrauschen geworden. Im kriminellen Bereich verursachen etwa Ransomware-Angriffe weiterhin erhebliche Schäden. Besonders kleinere und mittlere Unternehmen haben Mühe, mit der Professionalisierung der Angreifer Schritt zu halten. Im hybriden Konflikt eignet sich der Cyberraum zudem sehr gut für Störungen und Verunsicherung. Attribution ist möglich, aber sie braucht Zeit und Ressourcen. Das macht den Cyberraum zu einem wirkungsvollen Feld, um Unsicherheit zu erzeugen und Vertrauen zu schwächen.

MB: Wie resilient sind die kritischen Infrastrukturen der Schweiz dagegen?

MDC: Sehr unterschiedlich. Grosse Akteure mit grossen Ressourcen verfügen teilweise über ausgezeichnete Fähigkeiten, kleinere Unternehmen deutlich weniger. Die Schweiz verfügt zwar über gute Fachkräfte, Ausbildungsinstitutionen, Unternehmen und finanzielle Möglichkeiten. Trotzdem würde ich nicht sagen, dass wir insgesamt ausreichend resilient sind. Denn es geht nicht nur um den einzelnen Hackerangriff. Technische Risiken lassen sich mit gutem Risikomanagement und Business Continuity Management teilweise beherrschen. Schwieriger sind Abhängigkeiten und die psychologische Dimension. Menschen müssen darauf vertrauen können, dass Systeme grundsätzlich funktionieren. Wenn dieses Vertrauen schwindet, wird auch die Gesellschaft verletzlicher.

RE: Ist diese Verunsicherung vor allem gezielte Einflussnahme oder entsteht sie aus der Gesellschaft selbst?

MDC: Beides. Es gibt Akteure, die Unsicherheiten ausnutzen oder verstärken. Gleichzeitig erleben wir einen breiteren Vertrauensverlust und eine pessimistischere Sicht auf die Zukunft. Besonders schwierig sind diffuse Ängste. Bei einer konkreten Sorge kann man mit Information reagieren. Wenn Menschen aber grundsätzlich nicht mehr wissen, wem oder was sie glauben sollen, reicht der Hinweis «Das stimmt nicht» nicht mehr. Das merkt man selbst bei Bildern. Früher nahm man zunächst an, sie seien echt; heute entsteht oft zuerst der Verdacht einer Manipulation. Diese Erosion der Verifikations- und Vertrauensfähigkeit ist eine zentrale Herausforderung.

RE: Was bedeutet digitale Souveränität für die Schweiz konkret?

MDC: Digitale Souveränität bedeutet nicht vollständige Unabhängigkeit, die gibt es nicht. Abhängigkeiten sind auch nicht grundsätzlich schlecht, weil sie Effizienz, Kooperation und Spezialisierung ermöglichen. Entscheidend ist, sie zu verstehen und zu bewerten. Eine Organisation muss wissen, welche Aufgaben kritisch sind und von welchen Ressourcen sie abhängen: Software, Hardware, Daten, Cloud-Dienste, Know-how oder Betriebskompetenzen. Danach stellt sich die Frage, was passiert, wenn ein Anbieter ausfällt, insolvent wird oder die Preise massiv erhöht; oder wenn beispielsweise durch geopolitische Entwicklungen ein zusätzliches Risiko entsteht. Technisches Mapping allein reicht deshalb nicht.

«Man muss Krisen nicht nur üben, sondern auch die gewonnenen Erkenntnisse konsequent umsetzen.»

MB: Was braucht es denn darüber hinaus?

MDC: Ein gutes Risikomanagement. Welches Risiko kann und will man tragen, wo ist Redundanz sinnvoll, wo wäre eine Alternative unverhältnismässig teuer? Solche Fragen gehören in interdisziplinäre Teams, nicht allein zur IT. Aber wir haben nach wie vor zu wenige Fachleute, die mehrere dieser Perspektiven zusammenbringen. Vieles wird erst in der Praxis gelernt. Auch die Ausbildung ist noch nicht konsequent auf solche interdisziplinären Fragestellungen ausgerichtet.

MB: Welche gesellschaftlichen Werte geraten durch digitale Technologien und insbesondere KI unter Druck?

MDC: Vertrauen steht stark unter Druck, ebenso Privatsphäre, Datensouveränität und Autonomie. Hinzu kommen Fragen der Gleichbehandlung und des Zugangs. Wer bessere KI-Werkzeuge nutzen kann, kann sich Bildungs- und Wettbewerbsvorteile verschaffen. Gleichzeitig gewinnen Werte wie Nachvollziehbarkeit, Verantwortlichkeit und Anfechtbarkeit an Bedeutung. Wenn ein KI-System eine Empfehlung liefert, muss ein Mensch verstehen oder zumindest nachvollziehen können, warum. Besonders kritisch ist der Automation Bias. Automatisierte Ergebnisse sind bequem, und genau deshalb besteht die Gefahr, dass der Mensch formal entscheidet, praktisch aber nur noch bestätigt, was die Maschine vorbereitet. Organisationen brauchen deshalb bewusst eingebaute Stoppunkte, an denen Menschen prüfen und widersprechen können.

RE: Das sehen wir auch in der Ausbildung. KI kann hervorragend vorbereiten, aber die Versuchung ist gross, die Vorbereitung gleich als Ergebnis zu übernehmen. Wie trainieren wir weiterhin Urteilskraft?

MDC: Dafür braucht es Grundlagenwissen und bewusstes Training des kritischen Denkens. Wer die Grundlagen nicht beherrscht, kann den Output eines Systems gar nicht mehr beurteilen. Schulen, Hochschulen und Unternehmen müssen deshalb Lern- und Prüfungsformen anpassen. KI wird nicht verschwinden. Die Frage lautet, wie wir Menschen befähigen, sie sinnvoll zu nutzen und gleichzeitig kritisch zu prüfen. Das ist auch eine Frage der Chancengleichheit. Zugang, Unterstützung und Kompetenzen dürfen nicht zu einer neuen sozialen Trennlinie werden.





MB: *Kritisches Denken erfordert Energie und Zeit. Inwiefern spielt dabei Langsamkeit (z.B. mancher politischer Entscheidungsprozesse in der Schweiz) eine Rolle?*

MDC: Für Demokratien kann Langsamkeit ein positiver Wert sein. Das Abwägen und Anhören unterschiedlicher Positionen sowie die bewusst eingebaute Reibung und bewusst eingebaute Reibung brauchen Zeit. In einer Welt, in der alles schneller wird, sollten bestimmte Entscheidungen gerade deshalb nicht beliebig beschleunigt werden. Das lässt sich übrigens auch technisch gestalten. Systeme können so gebaut werden, dass nicht jeder Entscheid sofort möglich ist. Manchmal ist Reibung eine Sicherheitsfunktion.

RE: *In der Wirtschaftsprüferausbildung experimentieren wir deshalb bewusst mit analogen Formaten wie Papier, Szenarien oder Diskussion. Nicht als Gegenmassnahme gegen die Technologie, sondern um das eigene Denken zu trainieren.*

MDC: Genau. Kritisches Denken wird im KI-Zeitalter nicht weniger wichtig, sondern mehr.

RE: *Wo liegt bei KI der dringendste Handlungsbedarf? Bei der Regulierung, der institutionellen Resilienz oder beim gesellschaftlichen Bewusstsein?*

MDC: Bei allen drei Ebenen gleichermassen. Regulierung und Selbstregulierung sind wichtig, werden aber nicht reichen. Entscheidend ist die institutionelle Einbettung. Wie verändert KI Abläufe und Berufsbilder, wer trägt Verantwortung, was passiert, wenn Systeme plötzlich nicht mehr verfügbar sind? Je stärker KI in industrielle

Prozesse, Energieversorgung oder andere kritische Bereiche eingebettet wird, desto wichtiger werden Ausfallfähigkeit und Alternativen. Gleichzeitig braucht es eine breite gesellschaftliche Diskussion über Arbeitswelt, Bildung, Verantwortung und Governance. Ich bin dabei keine Schwarzmalerin. Menschen und Institutionen haben sich auch an frühere technologische Umbrüche angepasst. Wir können KI produktiv nutzen, aber Zugang und Kompetenz dürfen nicht zusätzliche Ungleichheiten erzeugen.

MB: *Bei Wahlen und Abstimmungen wird zudem immer wieder über Desinformation und ausländische Einflussnahme diskutiert. Was wissen wir über deren Wirkung?*

MDC: Desinformationsversuche und zuordenbare Kampagnen gibt es, auch in der Schweiz. Sie stammen nicht nur von ausländischen Akteuren, auch interne Kräfte können Informationen verzerren. Viel schwieriger ist die Frage nach dem Effekt. Wissenschaftlich lässt sich kaum sauber messen, wie stark eine konkrete Kampagne Verhalten verändert. Menschen suchen häufig Informationen, die zu ihren bestehenden Ansichten passen. Dadurch werden Überzeugungen eher verstärkt als vollständig umgekehrt. Ein wichtiger Effekt kann aber schon die Verunsicherung selbst sein. Wenn Menschen ständig hören, dass sie manipuliert werden und nichts mehr verlässlich sei, entsteht Vertrauensverlust. Deshalb sollten wir nicht jede Störung spektakulär inszenieren, sondern vor allem Medienkompetenz und gesellschaftliche Resilienz stärken, also die Fähigkeit, Informationen einzuordnen, Quellen zu prüfen und Unsicherheit auszuhalten.





RE: Wenn wir die Themen zusammenführen, wo liegt der dringendste Handlungsbedarf für die Schweiz?

MDC: Erstens müssen wir präziser vermitteln, was Resilienz überhaupt bedeutet. Sie ist nicht nur eine Eigenschaft einzelner Organisationen oder Personen, sondern eine gesamtgesellschaftliche Aufgabe. Dann geht es um Vorbereitung. Menschen müssen wissen, was in einer Krise zu tun ist, dazu gehören Information, Notfallvorsorge und konkrete Übungen. Zweitens müssen wir Silos überwinden: Energie, Cyber, Versorgung und Verwaltung dürfen nicht getrennt gedacht werden. Vorbereitung muss sektorübergreifend zwischen Bund, Kantonen, Gemeinden und Privatwirtschaft stattfinden. Drittens braucht es mehr Antizipation. Nicht als exakte Vorhersage, sondern als kontinuierliches Horizon-Scanning und als Beobachtung von Abhängigkeiten und Risikokombinationen. Wenn wir resilient sein wollen, müssen wir uns als Gesamtsystem verstehen. Das eigentliche Problem ist oft nicht mangelndes Wissen, sondern mangelndes Handeln.

MB: Wen meinen Sie genau, wenn Sie von «wir müssen» sprechen?

MDC: Wir als Gesellschaft. Und genau das macht es schwierig. Verantwortung lässt sich leicht auf andere abschieben, während Menschen ihr Verhalten ungern ändern, solange der Handlungsdruck abstrakt bleibt.

RE: Vielleicht ist deshalb eine dezentrale Struktur mit Einbezug der lokalen Ebene besonders wichtig. Wenn Risiken konkret werden und man versteht, wo Widerstände entstehen, wird aus einem abstrakten Thema etwas Greifbares.

MDC: Ja. Lokale Initiativen, Veranstaltungen, Übungen und konkrete Szenarien können sehr wirksam sein. Anreize funktionieren oft besser als Zwang. Entscheidend ist, Menschen so zu sensibilisieren, dass sie selbst verstehen, warum Vorbereitung sinnvoll ist. Eine unserer Studien zur Notfallvorsorge hat gezeigt, dass ein erheblicher Teil der Bevölkerung schon bei grundlegenden Fragen unsicher ist, etwa, was bei einer Sirenenwarnung zu tun wäre. Resilienz beginnt deshalb nicht erst im Krisenstab. Sie beginnt lange vorher im Alltag.

RE: Vielen Dank für das Gespräch.

Prof. Dr. Reto Eberle

Partner, Mitglied des Department of Professional Practice
KPMG Schweiz

Dr. Matthias Bossardt

Partner, Leiter Risk Consulting Services
KPMG Schweiz

Dieser Artikel ist Bestandteil der KPMG Board Leadership News, unser Newsletter für Verwaltungsrätinnen und Verwaltungsräte. Er erscheint dreimal pro Jahr.

Über das KPMG Board Leadership Center

Das KPMG Board Leadership Center ist unser Kompetenzzentrum für Verwaltungsrätinnen und Verwaltungsräte. Mit vertieftem Fachwissen und neusten globalen Kenntnissen unterstützen wir Sie in Ihren aktuellen Herausforderungen, damit Sie Ihre Rolle höchst effektiv erfüllen können. Zusätzlich bieten wir Ihnen die Möglichkeit, mit Gleichgesinnten in Kontakt zu treten und sich auszutauschen.

Erfahren Sie mehr unter kpmg.ch/blc.

Registrieren Sie sich zum Board Leadership Newsletter: [Hier registrieren](#)

Die hierin enthaltenen Informationen sind allgemeiner Natur und beziehen sich daher nicht auf die Umstände einzelner Personen oder Rechtsträger. Obwohl wir uns bemühen, genaue und aktuelle Informationen zu liefern, besteht keine Gewähr dafür, dass diese die Situation zum Zeitpunkt der Herausgabe oder eine künftige Situation akkurat widerspiegeln. Die genannten Informationen sollten nicht ohne eingehende Abklärungen und professionelle Beratung als Entscheidungs- oder Handlungsgrundlage dienen. Bei Prüfkunden bestimmen regulatorische Vorgaben zur Unabhängigkeit des Prüfers den Umfang einer Zusammenarbeit. Sollten Sie mehr darüber erfahren wollen, wie KPMG AG personenbezogene Daten bearbeitet, lesen Sie bitte unsere Datenschutzerklärung, welche Sie auf unserer Homepage www.kpmg.ch finden.

© 2026 KPMG AG, eine Schweizer Aktiengesellschaft, ist eine Gruppengesellschaft der KPMG Holding LLP, die Mitglied der globalen KPMG-Organisation unabhängiger Firmen ist, die mit KPMG International Limited, einer Gesellschaft mit beschränkter Haftung englischen Rechts, verbunden sind. Alle Rechte vorbehalten.