

Kritische Infrastruktur – gut genug gesichert?

von Arne Heise¹

Hacker dringen in die Computersysteme von Unternehmen oder Behörden ein und bringen damit die Energieversorgung ganzer Städte und Regionen zum Zusammenbruch oder den Personennah- und -fernverkehr zum Erliegen. Solche oder ähnliche Nachrichten sind bereits Realität oder werden zumindest verstärkt als Szenarien für Planspiele verwendet, um mögliche Auswirkungen solcher Ereignisse auf die Lebensbedingungen der Bürger einschätzen zu lernen. Damit tritt etwas in den Blickpunkt, was bisher eher Sicherheitsexperten interessiert hat: die Kritische Infrastruktur (KRITIS) moderner Gesellschaften.

Natürlich hat es immer Gefahren gegeben, die das friedliche Zusammenleben der Menschen unterminierten: Kriege, Naturkatastrophen oder Sabotageakte beispielsweise. Und doch sind die Gefährdungspotentiale moderner Gesellschaften aufgrund des zunehmenden Grades an Vernetzungen und Interdependenzen sehr viel größer als früher und der mögliche Schaden ungleich höher: Fehlerhafte Risikoeinschätzungen können die Finanzsysteme kollabieren lassen, mangelnde oder technisch überforderte Warnsysteme können die Auswirkungen von Naturkatastrophen erheblich vergrößern und Hackerangriffe mögen künftig den Ausgang von demokratischen Wahlen im Zeitalter des E-Governance beeinflussen.

Der notwendige Schutz kritischer Infrastruktur wird seit Mitte der 1990er Jahre in der Bundesrepublik verstärkt diskutiert, 1997 wurde auf Initiative des Bundesinnenministeriums die ressortübergreifende Arbeitsgemeinschaft „Kritische Infrastruktur“ (AG KRITIS) geschaffen, was 2004 in die Gründung des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK) mündete. Dort wurde zunächst festgelegt, was unter KRITIS zu verstehen ist und welche Bereiche der KRITIS zuzuordnen sind. Das BBK hat KRITIS dabei „als Organisationen und Einrichtungen mit (lebens-)wichtiger Bedeutung für das staatliche Gemeinwesen definiert, bei deren Ausfall oder Störungen für größere Bevölkerungsgruppen nachhaltig wirkende Versorgungsengpässe oder andere dramatische Folgen eintreten“². Die Aufgabe dieser Organisationen und Einrichtungen ist die Bereitstellung „Kritischer Dienstleistungen“, deren Ausfall zu den genannten, weitreichenden – das System „Gemeinwesen“ gefährdenden – Auswirkungen führen könnte. Hierfür werden folgende 10 Bereiche identifiziert (vgl. Abb. 1): Energie, Ernährung, Finanz- und Versicherungswesen, Gesundheit, Informations- und Telekommunikationstechnik, Medien und Kultur, Siedlungsabfallentsorgung, Staat und Verwaltung, Transport und Verkehr, Wasser. Einerseits erscheint die Auswahl so umfassend, dass kaum ein Bereich ausgespart ist und die

¹ Dr. Arne Heise ist Professor für Volkswirtschaftslehre an der Universität Hamburg.

² BBK; 10 Jahre „KRITIS-Strategie“. Einblicke in die Umsetzung der Nationalen Strategie zum Schutz Kritischer Infrastrukturen. Praxis im Bevölkerungsschutz Bd. 21, Bonn 2020.

priorisierende Bedeutung des „kritisch“ (im Sinne von systemrelevant) unersichtlich bleibt, andererseits kann sicher kritisiert werden, dass z. B. die Bereiche „Wohnen“ und „Bildung“ unerwähnt bleiben. Und die Bereitstellung kritischer Dienstleistungen erfolgt auch – aufgrund der sehr weiten Fassung – in sehr unterschiedlicher Form: es sind gleichermaßen öffentliche Organisationen und Einrichtungen darunter subsummiert wie etwa im Bereich der Energie- oder Wasserversorgung, wie aber auch private Unternehmen etwa im Bereich des Finanz- und Versicherungswesens und natürlich auch Mischformen wie im Bereich der Gesundheit oder der Informations- und Telekommunikationstechnologien.

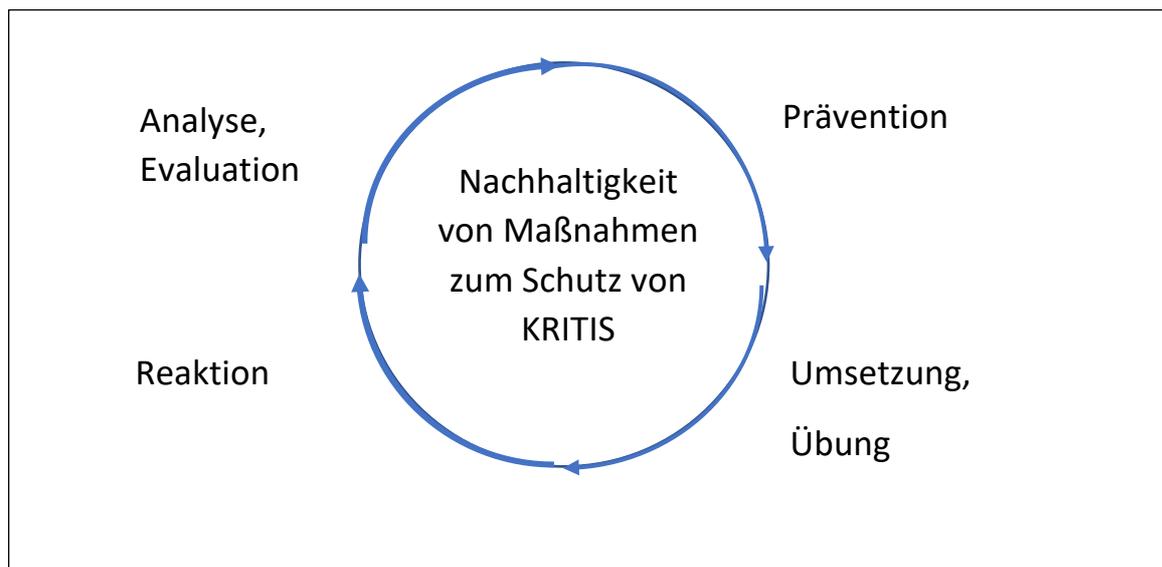
Abbildung 1: Bereiche der KRITIS



Quelle: BBK (2020)

Die Identifikation der KRITIS ist aber natürlich nur ein erster Schritt, es geht in erster Linie darum, die Kritische Infrastruktur zu schützen. Dem Schutz vorgelagert ist die Bereitstellung, d. h. bevor etwas zu schützen ist, muss es – in ausreichendem Maße – vorhanden sein. Hier könnte die Diskussion um den Mangel an öffentlichen Investitionen z. B. im Verkehrsbereich (aber eben auch im Bereich Wohnen und im Bildungsbereich) und die Sicherstellung lokaler Produktion privater Güter z. B. im Bereich der Energieproduktion, von Arzneimitteln und Impfstoffen, aber auch von Chips ansetzen – für diesen Artikel aber auch zu weit führen.

Abbildung 2: Schutzkonzept der KRITIS



Quelle: BBK (2020)

Das Schutzkonzept des BBK (vgl. Abb. 2) sieht zunächst präventive Maßnahmen vor, die je nach Bereich rein physischer (z. B. polizeilicher oder militärischer Schutz), technologischer (z. B. IT-Schutzlösungen) oder regulativer Art (z. B. Eigenkapitalbestimmungen im Finanzbereich) sein können, deren Umsetzung im zweiten Schritt erfolgen und ggf. auch ständig überprüft werden muss. Im Störfall muss es dann zu einer Reaktion kommen, die ebenfalls je nach Bereich sehr unterschiedlich ausfallen muss: Im Falle einer Naturkatastrophe müssen technische Warn- und Notfalldienste greifen und ggf. vorhandene Redundanzen (z. B. Doppelstrukturen für die Energie- oder Mobilitätsversorgung) eingesetzt werden – es geht letztlich darum, die Resilienz der systemrelevanten Strukturen zu stärken. Schließlich muss im Nachgang der gesamte Ablauf überprüft und ggf. weiterentwickelt werden.

Die Bundesregierung hat Ende des letzten Jahres ein neues „KRITIS-Dachgesetz“ angekündigt. Damit soll einerseits einer erwarteten EU-Richtlinie Rechnung getragen werden, aber auch identifizierten Mängeln beim bisherigen Schutz des KRITIS begegnet werden. Diese Mängel werden in einer klaren Definition der KRITIS, mangelnder Risikoanalyse und mangelhaftem Schutzniveau im Bereich von Prävention und Umsetzung, aber auch im Risikomanagement und dem allgemeinen institutionellen Rahmen gesehen³. Angesichts der Geschichte der Bemühungen um den Schutz Kritischer Infrastruktur in Deutschland und der konzeptionellen Möglichkeiten und Vorleistungen des BBK erscheint diese Einschätzung erstaunlich. Angesichts der sektoralen Breite der KRITIS müssen sicher Priorisierungsrichtlinien entwickelt werden, die den unterschiedlichen „Kaskadenpotentialen“, also der gesellschaftlichen Wirkungstiefe eines betroffenen Sektors,

³ Vgl. BMI; Eckpunkte für das KRITIS-Dachgesetz; einsehbar unter: [Eckpunkte für das KRITIS-Dachgesetz \(bund.de\)](https://www.bund.de).

Rechnung tragen könnten. So zeigt sich, dass das Kaskadenpotential des Teilssektors „Elektrizität“ etwa 80 Mal so hoch ist wie des Teilssektors „Binnenschifffahrt“⁴.

Klar muss allerdings sein, dass der KRITIS-Schutz einer Versicherungsleistung vergleichbar ist: Es geht nicht nur darum, die Frage nach den Schutzbemühungen mit ja oder nein zu beantworten, sondern auch das gewünschte Schutzniveau zu bestimmen. Denn es ist ja klar, dass jede Schutzmaßnahme – egal ob physischer, technischer oder regulativer Art – mit Kosten verbunden ist, die entweder von den Gewährleistern (Staat), Anbietern (Staat und/oder Unternehmen) oder Nutzern (private Haushalte und Unternehmen) zu tragen sind – über Höhe und Verteilung der Kosten scheint es bisher noch keinerlei konkrete Vorstellungen zu geben. Und die Kosten-Nutzen-Analysen dürften innerhalb des Gemeinwesens recht unterschiedlich ausfallen und können deshalb keine rein technokratischen Entscheide bleiben, sondern müssen verstärkt Teil der demokratischen Beschlussfassung werden.

⁴ Vgl. Schmitt, H.C.; Systemisches Kaskadenpotential von KRITIS-Teilssektoren; in: Informationen zur Raumentwicklung, H. 4, 2019, S. 48–61.