53. Sicherheitspolitische Informationstagung der Clausewitz-Gesellschaft e.V.

Stärkung von Resilienz und nationaler Führungsfähigkeit
im Rahmen der Landes- und Bündnisverteidigung“

Panel 1

Droht uns der totale >>Black- and Service Out<<? - Resilienz kritischer Infrastrukturen: Aktueller Stand, künftige Herausforderungen und Entwicklungsperspektiven"

Dr. Monika John-Koch, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

1. Schutz Kritische Infrastrukturen - Verantwortlichkeit im vernetzten Sicherheitsansatz

Im Rahmen der gesamtgesellschaftlichen Sicherheitsvorsorge gilt es, *„die Zusammenarbeit zwischen staatlichen Organen, Bürgerinnen und Bürgern sowie privaten Betreibern kritischer Infrastruktur … zu intensivieren. Das Miteinander aller in der gemeinsamen Sicherheitsvorsorge muss selbstverständlich sein“*. Was im Weißbuch 2016 als Selbstverständlichkeit eingefordert wird, fordert in der Praxis zuweilen schon Bund und Länder heraus; im Verhältnis Staat und Wirtschaft stößt diese Aussage aber häufig an Grenzen. Dies ergibt sich schon aus der Charakterisierung Kritischer Infrastrukturen, mit der Organisationen und Einrichtungen erfasst werden, bei deren Störungen oder Ausfällen gravierende Auswirkungen auf die Versorgung der Bevölkerung eintreten.

Während staatliche Vorsorgeplanungen in erster Linie die Aufrechterhaltung der Versorgung der Bevölkerung im Blick haben und unternehmerische Prozesse somit ein Mittel zum Zweck sind, orientieren sich unternehmerische Vorsorgeplanungen an der Aufrechterhaltung ihrer Betriebsfähigkeit, aus der dann die Bereitstellung (auch) kritischer Versorgungsdienstleistungen erfolgen kann. Zwei unterschiedliche Herangehensweisen, die zwar jeweils ihre Berechtigung haben, aber auch verschiedenen Handlungslogiken unterliegen und tendenziell divergierende Erwartungen an den Umfang von Notfallplanungen widerspiegeln. Hier gilt es, Möglichkeiten und Grenzen staatlicher und unternehmerischer Planungen zu kommunizieren und Anforderungen in einem Aushandlungsprozess festzulegen.

2. Vorsorgeplanungen - nicht ohne meine Betreiber

Gesamtgesellschaftliche Sicherheitsvorsorge bedeutet die Übernahme von Verantwortung durch alle Beteiligten: seitens des Staates für die Sicherheit und die Versorgung der Bevölkerung, seitens der Wirtschaft und insbesondere der Betreiber Kritischer Infrastrukturen für den sicheren Betrieb ihrer Anlagen und die Bereitstellung ihrer Dienstleistungen. So sind KRITIS-Betreiber gefordert, gesetzliche, untergesetzliche, brancheninterne oder auch freiwillige präventive Anforderungen an den Schutz ihrer Infrastrukturen zu prüfen und umzusetzen, um Ausfälle ihrer Dienstleistungen zu verhindern oder deren Ausmaß zu reduzieren.

Da die Summe von Einzelmaßnahmen aber nicht zwingend zur Sicherheit vernetzter Infrastruktursysteme führt, bedeutet gesamtgesellschaftliche Sicherheitsvorsorge, den Blick nicht nur auf das eigene Unternehmen, die eigene Organisation zu zentrieren, sondern auch über den Tellerrand hinaus zu sehen.

Hier ist der staatliche Akteur angesprochen, trotz oder gerade wegen verschiedener Zielsetzungen von Staat und Wirtschaft, Vorsorgeplanungen im gegenseitigen Austausch und branchenübergreifend zu erarbeiten und miteinander zu verknüpfen sowie Risiko- und Krisenmanagementstrukturen aufeinander abzustimmen. Dies setzt aber voraus, dass Erwartungen qualitativ und quantitativ formuliert und der Leistungsfähigkeit im Gegenstromverfahren gegenüber zu stellen sind, um Versorgungslücken erkennen und bestenfalls im Zuge von Aushandlungsprozessen schließen zu können, zumindest aber zu reduzieren.

Ohne Engagement und gegenseitiges Vertrauen, ohne den Austausch von Informationen und ohne Kenntnis der jeweiligen Möglichkeiten, aber auch der Grenzen, droht das Prinzip der gesamtgesellschaftlicher Sicherheitsvorsorge aber auf tönernen Füßen zu stehen.

3. Ja mach nur einen Plan … Planungen sind gut, Fähigkeiten sind notwendig

Organisationen bereiten sich in der Regel anhand von Szenarien auf bestimmte Ereignisse, Ausfälle und Störungen vor. Szenarien unterstützen die menschliche Vorstellungskraft und eröffnen konkrete Handlungsoptionen. Die Bewältigung eines Szenarios durch szenarioangepasste Notfallplanungen und Krisenmanagementkonzepte scheint Sicherheit zu geben. Was aber, wenn das Szenario nicht wie geplant eintritt? Wenn sich Kaskadeneffekte entwickeln, die nicht Gegenstand des Szenarios sind? Wenn ein weiteres Ereignis hinzukommt, dass sich krisenverschärfend auswirkt? Dann können szenariobasierte Planungen ggf. nur in der ersten Phase, z.B. beim Aufbau von Krisenmanagementstrukturen und der Einleitung erster Maßnahmen, einen maßgeblichen Beitrag zur Krisenbewältigung leisten.

Sicherheitspolitische Analysen beruhen auf der Erkenntnis, dass es keine 100% Sicherheit gibt, dass Unsicherheit eine Konstante ist, in und mit der Gesellschaften leben müssen. Dies gilt letztlich auch für den Umgang mit Szenarien: Indem sich krisenhafte Situationen dynamisch verändern können, bleiben auch szenariobasierte Planungen unsicher, unvollständig und im schlimmsten Fall unwirksam. Kernkomponenten der Krisenbewältigung in fragilen Zeiten sind Erfahrungswissen und Entscheidungskompetenz, Gestaltungsfähigkeit und Flexibilität - oder einfach: resiliente Strukturen.

4. Anpassungsbedarf – back to the roots?!

Gefahren für die Gesellschaften und damit für den Bevölkerungsschutz haben sich deutlich gewandelt. Dabei stehen nicht nur militärische oder quasi-militärische Herausforderungen im Zentrum, auf die sich die Diskussion um hybride Bedrohungen oftmals konzentiert. Neue Lebens- und Arbeitsformen, digitale Vernetzung und industrielle just-in-time-Produktion führen zwar zu effizienten Strukturen, gleichzeitig wächst aber die Gefahr neuer Schwachstellen, steigt die Verletzlichkeit und damit auch die Komplexität von Schadenslagen. Auch klimatische Veränderungen oder Auswirkungen der zunehmenden Technisierung ziehen Entwicklungen nach sich, die sich auf die Funktionsfähigkeit von Staat, Wirtschaft und Gesellschaft krisenhaft auswirken können. Klassische Hochwasser werden von plötzlich auftretendem Starkregen und Orkan begleitet, für Stromausfälle ist nicht mehr der Vor-Ort-Bagger, sondern der Hacker im Ausland verantwortlich, „soft targets“ stehen im Zentrum von terroristischen Angriffe mit „Alltagsgegenständen“.

Eine der größten Herausforderung ist die Sicherstellung der Kommunikation bei einem „Black- and Service Out“. Wie funktioniert Krisenbewältigung, wenn der Austausch von Lagebildern, die Anforderung von Unterstützungsleistungen oder die Abstimmung staatlicher Maßnahmen und zwischen Staat und Wirtschaft nicht möglich sind? Der Ausfall von Kommunikation, bislang lediglich „Begleiterscheinung“ eines Stromausfallszenarios, entwickelt sich mehr und mehr zur Achillesferse gesamtgesellschaftlicher Sicherheitsvorsorge.

Diese Fragen stellen auch die Vorbereitung auf und die Bewältigung von Ereignissen vor Herausforderungen, da ein geeignetes Instrumentarium zur Stärkung „hybrider Sicherheit“ auf den ersten Blick anachronistisch wirken: In Zeiten von Stromausfallszenarien und Cyberbedrohungen, dem elektrischen und elektronischem Black-out, können ausgerechnet „old-school“-Maßnahmen wie manuelle Steuerungsmöglichkeiten von Anlagen, Papierdokumente und nicht zuletzt die mechanische Schreibmaschine dazu beitragen, die Handlungsfähigkeit privater und staatlicher Akteure aufrechtzuerhalten.

Vielleicht ist dies der größte Anpassungsbedarf, die Erkenntnis und Akzeptanz, dass resiliente Krisenbewältigung in einer digitalen, vernetzten, „smarten“ und damit bequemen Welt analog, nicht vernetzt, aber anschlussfähig und unbequem, dafür aber stabil sein sollten.