24. August 2015

Konzept für das nationale Krisenmanagement bei Krisen mit Cyberausprägung
Auf der Grundlage der Massnahme 15 NCS

1. Ausgangslage

Im Handlungsfeld "Kontinuitäts- und Krisenmanagement" des Umsetzungsplans der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken NCS ist folgende Massnahme definiert (Massnahme 15):

Erarbeitung eines Konzeptes für Führungsabläufe und –prozesse zur zeitgerechten Problemlösung: *Das (allgemeine) Krisenmanagement muss angepasst werden und auch den Cyber-Aspekt beinhalten. Führungsabläufe und -prozesse des Bundes tragen innerhalb bestehender Prozesse der Cyber-Ausprägung Rechnung. Unter Federführung der BK soll ein Konzept für Führungsabläufe und -prozesse zur zeitgerechten Problemlösung erstellt werden, das auch den Cyber-Ausprägungen gerecht wird.*

Die Bundeskanzlei hat in Umsetzung dieser Massnahme ein Konzept auf Stufe Bund erarbeitet. Dieses ist vom Steuerungsausschuss NCS am 11. Februar 2014 verabschiedet worden. Davon abgeleitet, soll das vorliegende Konzept das Krisenmanagement Stufe Kantone miteinbeziehen und die entsprechenden Prozesse und Schnittstellen beschreiben. Die Bundeskanzlei und die Geschäftsstelle Sicherheitsverbund Schweiz haben das Konzept erarbeitet und bei Stellen des Bundes, der Kantone sowie bei Betreibern kritischer Infrastrukturen vernehmlasst. Es dient als Arbeitsgrundlage für Ausbildungssequenzen im staatlichen Krisenmanagement zu Szenarien, die eine Cyber-Ausprägung haben. Es wird als Folgearbeit zur Massnahme 15 dem Steuerungsausschuss NCS zur Kenntnis gebracht.

2. Krise mit Cyberausprägung

Ausgelöst durch einen Cyber-Angriff oder Systemfehler oder nicht böswilliges Handeln einer mitarbeitenden Person können die Integrität und Vertraulichkeit von Informationen verletzt oder kann die Verfügbarkeit eines IKT-Systems nicht mehr gewährleistet sein. Das Internet kann als Angriffsvektor missbraucht werden oder selber Ziel des Angriffs sein. Das Spektrum von Cyber-Angriffen reicht von Überlastungsangriffen (Distributed Denial of Service) durch Aktivisten und Erpresser über die Manipulation von Internet-Banking-Vorgängen durch Kriminelle bis hin zur Ausspähung und zu Cyber-Angriffen durch fremde staatliche oder nichtstaatliche Stellen – denkbar wären etwa Sabotage von kritischen Infrastrukturen oder Angriffe auf die Integrität des Finanzsystems, um das Funktionieren des Systems Schweiz zu beeinträchtigen. Führen diese Herausforderungen im Bereich der Cyber-Sicherheit einzeln oder in Kombination zu einer Eskalation der Lage und bleibt die Cyber-Sicherheit ein wesentlicher Bestandteil der Problembewältigung bei Bund und Kantonen, kann man von einer nationalen Krise mit Cyberausprägung sprechen. Dabei kann die Lage von der normalen über die besondere bis hin zu einer ausserordentlichen Lage eskalieren.[1] In jeder Krise herrscht zunächst Unsicherheit über Beschaffenheit der Gefahr oder Bedrohung sowie das Ausmass und die daraus resultierenden Konsequenzen. Bereits eine glaubwürdige Drohung, welche auf die Cyber-Sicherheit zielt, kann eine Lageverschärfung nach sich ziehen.

Die Beurteilung der Lage, insbesondere der Cyberkomponente, ob es sich um ein technisches Problem handelt oder ob politische Implikationen damit verbunden sind und wie gross deren Dimension ist, ist eine erste Herausforderung für die Führung. Gleichzeitig

[1] Vgl. Lagebegriffe normale Lage, besondere Lage, ausserordentliche Lage, in : Weisungen über organisatorische Massnahmen in der Bundesverwaltung zur Bewältigung besonderer und ausserordentlicher Lagen, vom 24. Oktober 2007, S.1.

stehen die Führungsverantwortlichen unter hohem Zeitdruck, um adäquate Entscheidungen im Rahmen der Krisenbewältigung zu fällen.
Sicherheitspolitisch relevante Krisenszenarien können eine starke Cyberkomponente beinhalten, indem der Missbrauch des Cyberraums wesentlich zur Lageverschärfung beiträgt und die Wiederherstellung der Cyber-Sicherheit zu einer Priorität der Krisenbewältigung werden kann.

3. Führungsverbund und Fachverbund

Notfall- und Krisenmanagement sind im Gegensatz zum Risikomanagement nicht szenario-, sondern prozessorientiert: Führungsorganisation und Entscheidungsprozesse müssen immer dieselben sein, unabhängig von der Beschaffenheit der Krise. Dies ist insbesondere wichtig, wenn die Reputation, die Handlungsfreiheit oder sogar die Existenz einer Organisation tangiert sind: Es gelten nach wie vor die eingespielten Geschäftsabläufe, und es sind dieselben Personen wie im Alltag, die auf höchster Ebene der Organisation Entscheidungen treffen müssen. Dieser Grundsatz gilt in der Bundesverwaltung, die vom Bundesrat geführt wird, wie in den Kantonsverwaltungen, die von den Kantonsregierungen geführt werden. Das allgemeine Krisenmanagement (Führungsabläufe und –prozesse) ist deshalb prinzipiell szenario-unabhängig. Die Führungsstrukturen von Bund und Kantonen bilden aber in einer nationalen Krisenbewältigung einen auf die Bewältigung der Krise zugeschnittenen Führungsverbund, der eine intensive Koordination zwischen beiden Entscheidungsabläufen erfordert. Die an diesem Verbund beteiligten Organe variieren je nach Art der Krise und der von der Exekutive mit der Krisenführung betrauten Instanz.
Prinzipiell szenario-abhängig sind jeweils diejenigen Organe bei Bund, Kantonen und Dritten (insbesondere kritischer Infrastrukturen), die sich mit bestimmten Risiken auseinandersetzen und diese im Alltag überwachen. Sie bilden den themenspezifischen Fachverbund. Wenn sich ein Risiko verschärft oder ein Ausmass annimmt, dessen Konsequenzen zu einer Krise führen könnten, dann sind es diese Fachstellen und Organe, die das "operative Krisenmanagement" in Gang setzen. Zudem werden sie die themenspezifische Lage aufbereiten, eine erste Problemerfassung durchführen, die Lage beurteilen und die fachliche Beratung der Entscheidungsträger wahrnehmen. Schlussendlich werden sie bei der Umsetzung der auf strategischer Ebene entschiedenen Bewältigungsmassnahmen mitwirken. Beim Bund ist dieses "risikospezifische Überwachungsorgan" im Cyber-Bereich die Melde- und Analysestelle Informationssicherung MELANI; bei den Kantonen sind es die Informatik- und Informationssicherheitsverantwortlichen, die teilweise in speziellen Fachgremien organisiert sind.

4. Krisenbewältigung im Verbund

4.1 Zusammenarbeit Bund-Kantone

Die Krisenbewältigung in einer stark vernetzten Gesellschaft erfordert erstens die enge Koordination der Krisenorgane und Entscheidungsträger auf allen Stufen und zweitens die Bündelung des staatlichen und privatwirtschaftlichen Fachwissens. Die Verantwortlichkeiten auf Stufe Bund wie Kantone sind gegeben. Das allgemeine Krisenmanagement (Führungsabläufe und –prozesse) muss auch in einer Krise, die eine Cyber-Komponente enthält, grundsätzlich drei Aufgaben erfüllen:

1. Vermittlung eines aktuellen, einheitlichen und umfassenden Lagebildes.
2. Schaffung der wesentlichen Grundlagen zur Entscheidungsvorbereitung des Bundesrates sowie der Kantonsregierung; insbesondere wird das Mitberichtsverfahren in abgekürzter Form durchgeführt.
3. Festlegung einer Kommunikationsstrategie und Definition der Kommunikationsmassnahmen.

Bei einer Krise mit Cyberausprägung müssen das fachliche Wissen und die fachspezifischen Kapazitäten von staatlichen und privatwirtschaftlichen Stellen genutzt und so organisiert werden, dass sie in der Krise ohne grossen Zeitverlust abgerufen werden können. Vorhandene staatlich-privatwirtschaftliche Partnerschaften sind zu nutzen, insbesondere sind die Informationen im Rahmen der rechtlichen Möglichkeiten auszutauschen. Ebenso müssen

die Fähigkeiten und Mittel der Armee, welche subsidiär zur Verfügung gestellt werden könnten, identifiziert und lagegerecht zur Unterstützung der zivilen Behörden verfügbar gemacht werden.

Ein Koordinationsbedarf zwischen Bund und Kantonen ergibt sich vor allem in folgenden Bereichen:

- Gemeinsames Lagebild und Beurteilung der Lage
- Abstimmung der Handlungsoptionen und Synchronisation der Entscheide
- Ressourcenüberblick und Ressourcenmanagement
- Abstimmung des Kontinuitätsmanagements
- Erarbeitung gemeinsamer Botschaften und deren Kommunikation.

4.2 Einbezug kritische Infrastrukturen

Eine besondere Herausforderung für das gesamtstaatliche Krisenmanagement bildet der Einbezug der kritischen Infrastrukturen. Diese spielen sowohl bei der Entstehung einer Krise einer Rolle (KI als strategische Ziele) als auch bei den Auswirkungen (Grundversorgung der Bevölkerung und der Wirtschaft).

- Es muss sichergestellt sein, dass die kritischen Infrastrukturen auch über entsprechende, bekannte, Krisenorganisationen sowie definierte Schnittstellen zu Bund und Kantonen sowohl auf politisch/strategischer wie auch auf operativer Ebene verfügen.
- Sind kritische Infrastrukturen betroffen, die ihre Dienstleistungen national sicherstellen, kann es notwendig sein, die Ereignisbewältigung auf nationaler Ebene zu koordinieren. Da ein Ausfall ihrer Infrastrukturen eine unmittelbare nationale und möglicherweise auch internationale Auswirkung haben kann, sind direkte Schnittstellen zum Bund auf politischer, strategischer und operativer Ebene notwendig.
- Die Koordination von kritischen Infrastrukturen muss hierbei in enger Zusammenarbeit mit Bund und Kantonen, unter der Verantwortung des Bundes, geschehen. Die Kompetenzen der Kantone bzw. Gemeinden im Rahmen des Bevölkerungsschutzes bzw. der inneren Sicherheit sind dabei zu berücksichtigen.

5. Gemeinsame Ausbildungssequenzen

5.1. Strategisches Seminar vom 11. Juni 2015

Ausbildungsmodule sollen dazu dienen, die Prozesse und Schnittstellen anhand eines Cyber-Szenarios mit nationaler Dimension zu verdeutlichen. Dies soll ermöglichen, die Strukturen und die Koordination im Hinblick auf einen Ereignisfall zu optimieren.
Als erstes Trainingsmodul schlug die Cyber-Landsgemeinde 2013 vor, ein strategisches Seminar mit Vertretern des Bundes, der Kantone und der Betreiber kritischer Infrastrukturen durchzuführen. Das Seminar, das am 11. Juni 2015 durchgeführt wird, hat zum Ziel, die Strukturen und Prozesse des Krisenmanagements im Cyber-Bereich der Kantone aufzuzeigen und die Schnittstellen mit dem Bund zu identifizieren.

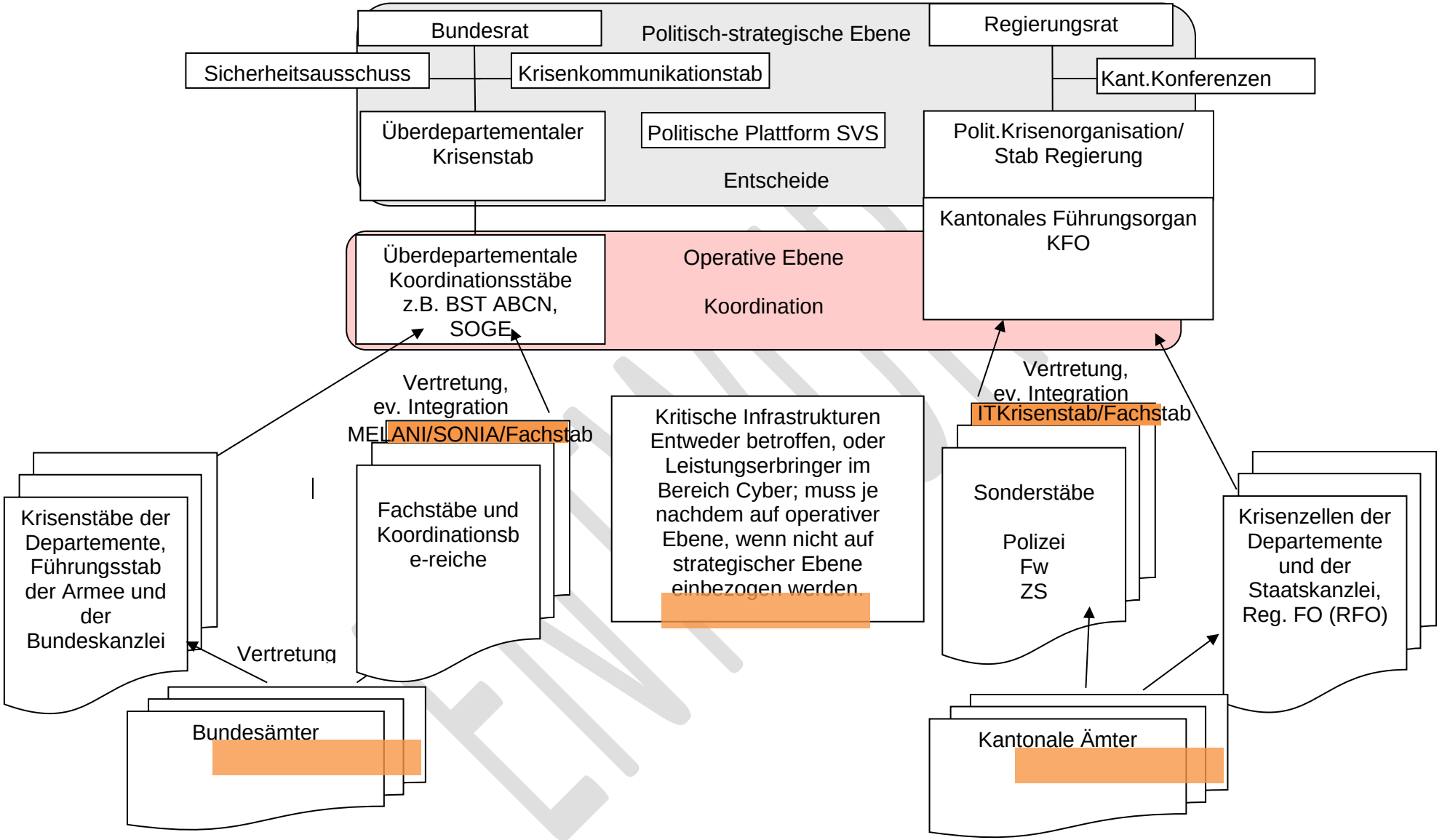
5.2. Weitere kantonale und nationale Übungen

Noch offen bleibt derzeit, in welcher Form zusätzlich weitere Ausbildungssequenzen durchgeführt werden können. So könnten etwa die Schlüsselfunktionen in der Krisenbewältigung auf den Stufen Bund, Kantone und Dritte im Rahmen eines Trainingsmoduls simuliert und so der Koordinationsbedarf noch deutlicher eruiert werden, um möglichen Friktionen vorzubeugen. Denkbar wäre auch, dass die Kantone mit ihren Kantonalen Führungsorganen entsprechende thematische Entschlussfassungsübungen durchführen. Als oberste Trainingsstufe zur Bewältigung einer nationalen Cyber-Krise wäre eine gemeinsame Stabsübung mit Bund, Kantonen und kritischen Infrastrukturen wünschenswert. Diese Stabsübung soll nach Möglichkeit in einer ohnehin geplanten Übung integriert werden (z.B. Sicherheitsverbundsübung SVU).

Beilage 1: Aspekte von Krisen mit Cyber-Ausprägung (nicht abschliessend)

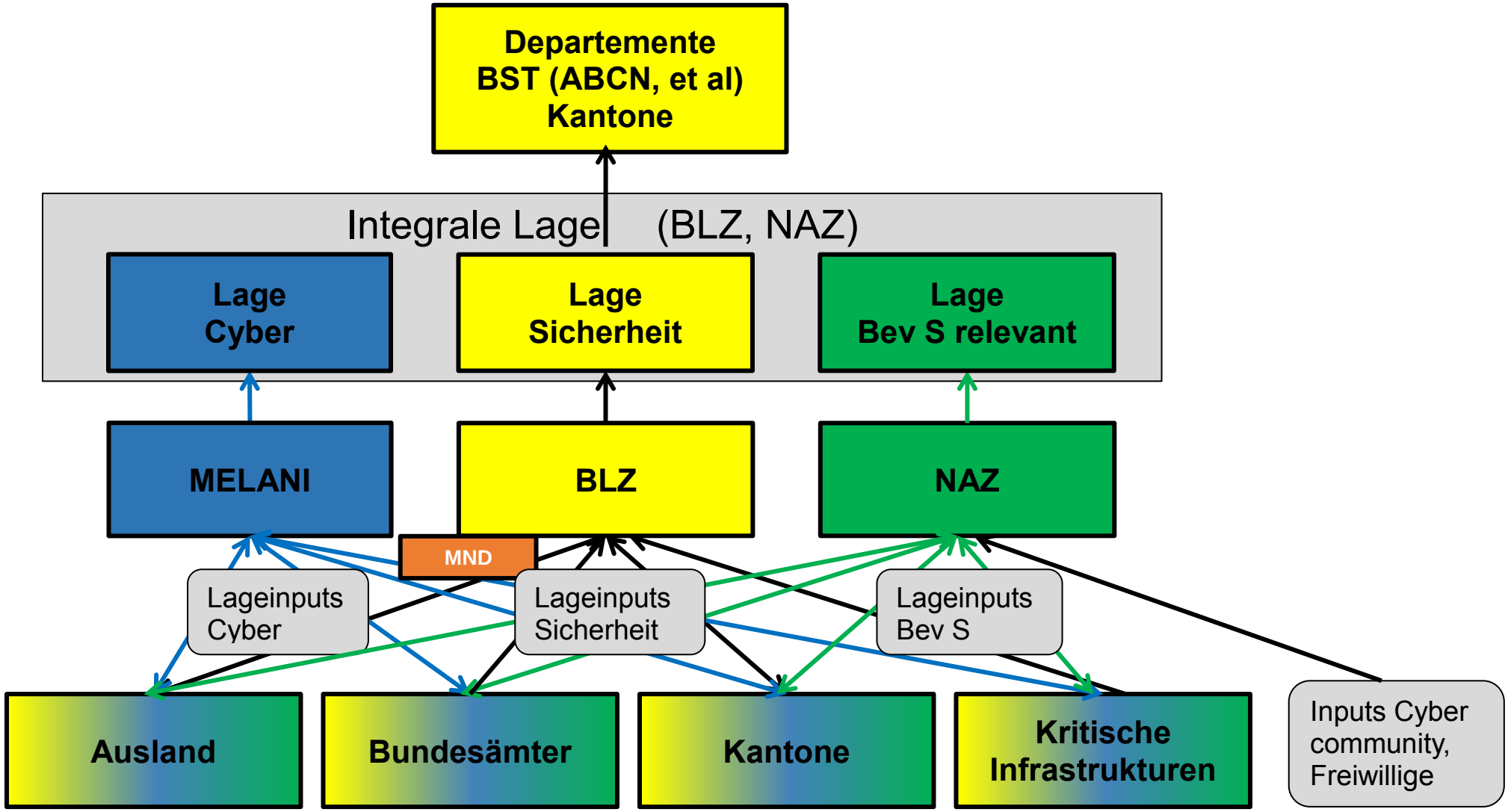
Hohes Potential für Eskalation der Lage
– Beeinträchtigungen Cyber-Sicherheit generell hohes Eskalationspotential – Schon unbeabsichtigter Ausfall IKT-Infrastruktur schwerwiegende Konsequenzen – Massive Beeinträchtigung des täglichen Lebens und der Wirtschaft – Bewältigung Schäden an Infrastrukturen – Hoher Druck, Ursache für den Ausfall der digitalen Netzwerke zu beheben
Technische Dimension
– IKT-Problem zunächst vor allem Herausforderung für Business-Continuity-Management – Betrifft zunächst in erster Linie IKT-Spezialisten, fachspezifische Fragen im Vordergrund – Meist Vorfälle in der normalen Lage – Erst wenn Lage eskaliert, wird technisches Problem Herausforderung für übergeordnetes Krisenmanagement: Kommunikation, rechtliche Abklärungen, Behebung Folgeschäden etc.
Informationssicherung (Integrität von Daten und Informationen)
– Integrität, Vertraulichkeit oder Verfügbarkeit von Daten im staatlichen Verantwortungsbereich bei Behörden und Kritischen Infrastrukturen verletzt – Daten entweder entwendet, manipuliert oder missbraucht, bspw. staatliche Zertifikate gefälscht oder Personendaten von Bürgern entwendet – Zunächst Verwaltungsstellen betroffen, die mit Informationssicherheit betraut, bei Eskalation sind politische Verantwortungsträger gefordert.
Erosion des Vertrauens in IKT, Systeme und Systembetreiber
– Vertrauen in Staat und IKT-Systembetreiber erodiert, wenn Sicherheitsprobleme nicht gelöst, Angreifer nicht identifiziert und unschädlich gemach – Öffentliche Empörung besonders gross, wenn persönliche Daten nicht mehr geschützt – Folgen: Gewisse Systeme und Systembetreiber nicht mehr genutzt und der elektronische Verkehr mit staatlichen Stellen gemieden – Beträchtliche wirtschaftliche Schäden und Funktionen Verwaltung beeinträchtigt.
Starker Druck auf politische Entscheidungsträger
– Funktionierende IKT-Infrastruktur für sämtliche Lebensbereiche zentral, inklusive für die Bewältigungsverantwortlichen Bund, Kantone, kritische Infrastrukturen – Grössere Ausfälle in Verwaltung haben politische Auswirkungen – Je nach Schadensausmass und Sensitivität der Informationen starker Druck auf politische Verantwortungsträger durch Öffentlichkeit und Medien – Forderung, Informationssicherheit wieder herzustellen, Datenabfluss zu stoppen, verursachte Schäden kompetent zu beheben oder zu mildern sowie Verursacher unschädlich zu machen und strafrechtlich zu verfolgen.
Dynamische Bedrohungskomponente
– Möglichkeiten und Bereitschaft, Cyberraum zu missbrauchen, zugenommen – Sich wandelnde Angriffspunkte und Methoden wie bspw. Einschleusen von Trojanern, digitale Hintertüren, Manipulation von Industriesteuerungsanlagen, Überwachung Kommunikation – Eindringen in IT-Netzwerke, die Manipulation von Mobiltelefonen der Zielpersonen als Abhöreinrichtung oder die legale und illegale Ausforschung per Internet – Schadprogramme können Daten unwiederbringlich zerstören oder schleichend verfälschen – Angriffe auf kritische Infrastrukturen können fatale Kettenreaktionen auslösen, etwa bei Manipulation von Steuerungsanlagen der Energieversorgung, der Telekommunikation und des Transports sowie von finanziellen Netzwerken – Entwendung von sensitiven Datensätzen können Personen und Behörden und den Staat an sich diskreditieren – Beeinflussung politischer Prozesse und Entscheide – Beeinträchtigung der wirtschaftlichen Entwicklung und Stabilität – Durch internationale Verknüpfung der IT-Netzwerke möglich, durch elektronische Angriffe auf Informationen zuzugreifen, ohne das Staatsgebiet des Zielobjekts je zu betreten – Selbst kleinere Staaten oder Organisationen können heute ihre wirtschaftlichen Konkurrenten oder politischen Gegner auf diesem Weg ausspionieren – Solche Angriffe können durch traditionellen Einsatz von Agenten flankiert sein.

Beilage 2 - Führungsstrukturen beim Bund und den Kantonen unter Einbezug der kritischen Infrastrukturen



Organe, die von Cyber-Ausprägung betroffen sind

Beilage 3 - Struktur für die Ermittlung des Lagebildes im Falle einer Krise mit Cyberausprägung



Erklärende Tabelle zu Grafik Beilage 2:

Bundesrat	• bestimmt federführendes Departement oder betraut Bundespräsident mit Krisenmanagement • entscheidet
Überdepartementaler Krisenstab	• wird von einem Mitglied des Bundesrates geführt • Einsitz von den Generalsekretären des federführenden Departementes • Schafft Grundlagen für Bundesratsbeschluss mit abgekürztem Mitberichtsverfahren • definiert Kommunikationsstrategie und Kommunikationsmassnahmen
Politische Plattform Sicherheitsverbund Schweiz (SVS)	• Konsultiert gemeinsame Bewältigungsstrategien Bund-Kantone • Koordiniert Entscheide Bundesrat und Entscheide Kantonsregierungen • Definiert Prioritäten in Versorgung, Verkehr und Ressourcen • Schlägt gemeinsame Botschaften der Krisenkommunikation vor
Überdepartementale Koordinationsstäbe Bund = BST ABCN/SOGE	• vermittelt den Krisenbewältigungsorganen ein umfassendes Lagebild auf strategischer Ebene • bereitet Entscheidungsgrundlagen zuhanden des Bundesrates (Ämterkonsultation) • Stab des federführenden Departements • Einsitz hochrangiger Vertreter aus betroffenen Departementen
Regierungsrat	• bestimmt federführendes Departement und betraut dessen Vorsteher mit Krisenführung • entscheidet
Stab Regierungsrat	• optional, einige Kt führen direkt mit KFO • wird von einem Regierungsrat geführt • Einsitz der Generalsekretäre der anderen Departemente • bearbeitet politisch-strategische Dimension der Krise und erarbeitet entsprechende Handlungsoptionen • definiert Kommunikationsstrategie und Kommunikationsmassnahmen
Kantonales Führungsorgan	• vermittelt umfassendes Lagebild auf strategischer Ebene (siehe Beilage 2) • bereitet Entscheidungsgrundlagen zuhanden der Kantonsregierung • definiert Kommunikationsstrategie und Kommunikationsmassnahmen
Fachstäbe wie SONIA und analoge Sonderstäbe bei den Kt Koordinationsbereiche (KSD, KOVE, Meteo CH, Telematik, ABC-Schutz, LAINAT)	• koordinieren auf operativer Ebene Entscheidungsgrundlagen zH. des Bundesrats bzw der Kt-Regierung oder Umsetzungsmassnahmen (im Sinne einer Ämterkonsultation) • entscheiden im eigenen Kompetenzbereich und ordnen operative Massnahmen an • führen Bundesratsbeschlüsse aus (operative Umsetzung).