SVU 19 : Lageberichte zur vertieften Analyse einer Terrorlage

Autor(en): **Wigger, Bernhard**

Objekttyp: **Article**

Zeitschrift: **ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift**

Band (Jahr): **184 (2018)**

Heft 10

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-813232

SVU 19 – Lageberichte zur vertieften Analyse einer Terrorlage

Vor der Sicherheitsverbundsübung (SVU 19) im November 2019 werden den Übungsteilnehmenden vier fiktive Lageberichte abgegeben. Diese sollen sie dabei unterstützen, sich mit zentralen Aspekten einer anhaltenden Terrorbedrohung auseinanderzusetzten. Bisher sind zwei Lageberichte erschienen.

Bernhard Wigger, Christian Hirschi

Übungsthemen und damit auch Szenarien werden durch momentane Bedrohungstrends beeinflusst. Standen in der SVU 14 eine Strommangellage und eine Pandemie im Zentrum, werden dies in der SVU 19 Terrorismus und Cyber-Bedrohung sein.

Das Szenario – die Übungsumwelt

Ein Szenario muss eine möglichst echte Übungsumwelt beschreiben und damit eine ungewohnte, aber dennoch realistische Krisensituation für die Übenden schaffen. Dies setzt einen Spannungsbogen aus verschiedenen Herausforderungen und Dilemmas voraus. Das ist immer eine Gratwanderung zwischen Realität, Fiktion und Methodologie.

Um dieses Ziel zu erreichen, agiert in der SVU 19 die fiktive Global Liberation Front (GLF), eine «religiöse Sekte mit globaler Agenda» aus dem ebenfalls fiktiven Staat Agrarien (siehe ASMZ 03 und 05/2018). Dieser Gegner betreibt massive Propaganda und politische Erpressung, sabotiert kritische Infrastrukturen und schreckt auch nicht vor blutigen Terroranschlägen zurück.

Struktur der Lageberichte

Die vier Lageberichte im Vorfeld der SVU 19 gliedern sich in fünf Kapitel. Die Einleitung weist auf die Besonderheit der jeweiligen Ausgabe hin. Darauf folgt die allgemeine Lage mit Hinweisen zur Krisenbewältigung auf Stufe Bund, einem allgemeinen Stimmungsbild Schweiz und einem aktualisierten Lagebericht des Nachrichtendienstes des Bundes (NDB). Die besondere Lage beschreibt die Aktivitäten der Organe der inneren Sicherheit, des Bevölkerungsschutzes sowie der Armee zum Zeitpunkt des Erscheinens des jeweiligen Lageberichts. Aus methodisch-didaktischer Sicht liegt der Schwerpunkt der Lageberichte auf dem Kapitel Analyse, Beurteilung und Herausforderungen. Das letzte Kapitel gibt einen Ausblick auf die kommenden 6, 12 und 18 Monate. Dieser letzte Teil soll die Übenden im antizipativen Denken unterstützen und Eventual- beziehungsweise Vorsorgeplanungen auslösen.

Berichterstattung zur SVU 19

Die ASMZ wird regelmässig über die SVU 19 berichten. In der Ausgabe vom März 2018 wurde das Detailkonzept der Übung vorgestellt. Die Ausgabe von Mai 2018 hat die Themen des Szenarios behandelt.

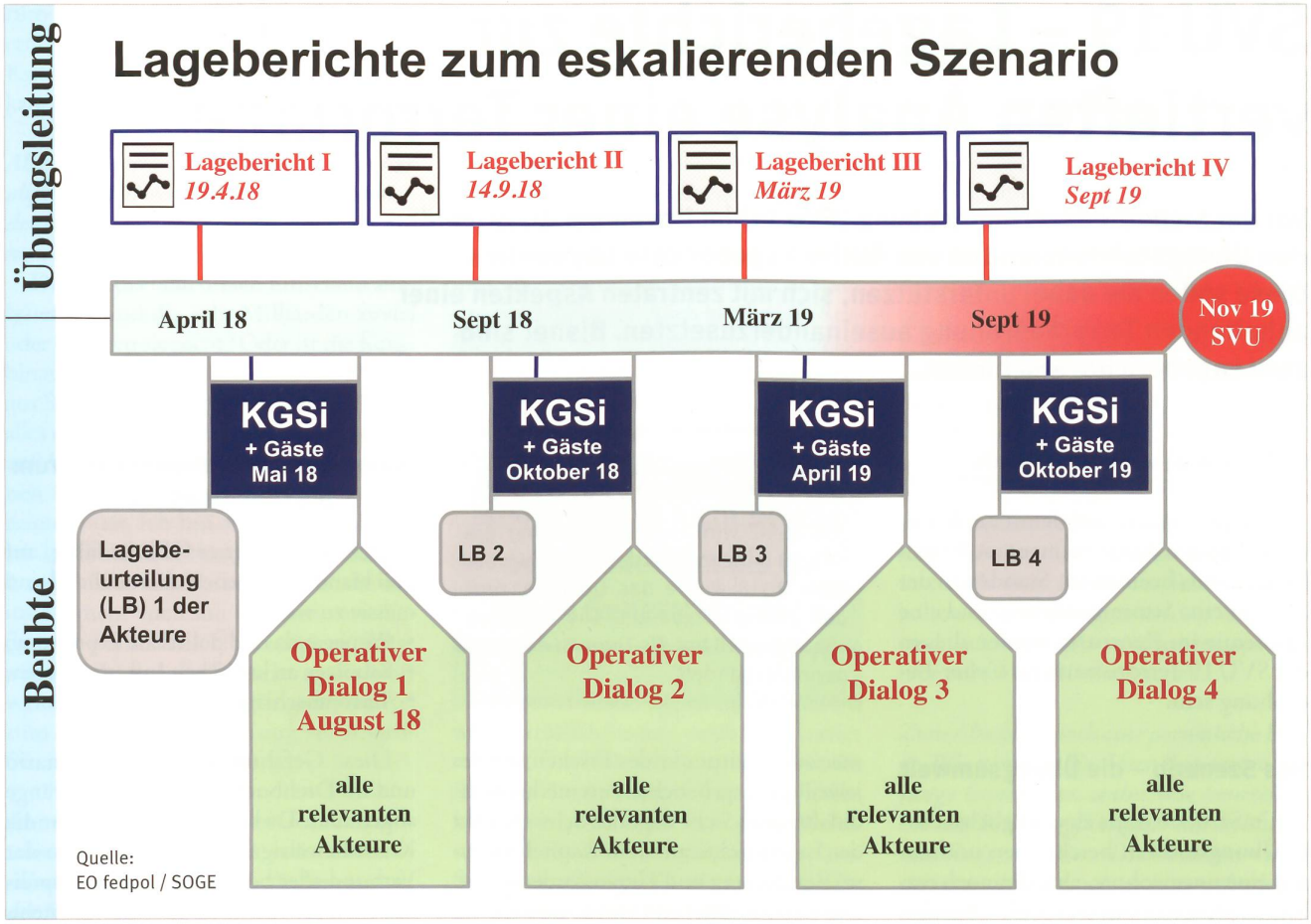
Komplexes Bedrohungsspektrum als Übungsannahme

Der Modellgegner GLF ist fähig, auf drei Handlungsebenen überraschend und massiv zu wirken:

- Propaganda und politische Erpressung;
- Sabotage an kritischen Infrastrukturen;
- Terroranschläge.

Diese Gefahren werden im Szenario und im Drehbuch als Handlungsstränge abgebildet. Da bei der SVU 19 nicht die Krisenbewältigung an sich, sondern der Verbund aller beteiligten sicherheitspolitischen Instrumente im Vordergrund steht, reicht oft nur schon eine konkrete Bedro-

Der Schutz von Personen des öffentlichen Lebens ist ein Thema im Lagebericht 2 der SVU 19. Bild: KAPO Bern



hung, um den gewünschten Übungseffekt zu erzielen.

Propaganda und politische Erpressung

Entlang dieses Handlungsstranges versucht die GLF Behörden, Medien und die öffentliche Meinung zu manipulieren, Institutionen oder Personen zu deskreditieren, um dadurch die politischen Entscheide zu beeinflussen und das Vertrauen der Bevölkerung in die Behörden zu unterminieren.

Angriffe erfolgen in dieser Phase in erster Linie über den Cyber-Raum: IT-Netzwerke werden infiltriert und Speichersysteme gezielt angegriffen, um vertrauliche Informationen zu beschaffen, zu verfälschen und Desinformation zu betreiben.

Durch den Propagandafeldzug kann die GLF ihre Anhänger im Informationsraum mobilisieren und so aus sicherer Entfernung den Druck auf die Schweiz erhöhen. Durch eine Reihe von öffentlichkeitswirksamen Aktionen im Cyber-Raum kann die GLF über einen längeren Zeitraum immer wieder auf sich aufmerksam machen. Die Aktionen werden im Vorfeld in den sozialen Medien angekündigt oder nachher die Urheberschaft beansprucht.

Dieser Missbrauch des Cyber-Raums trägt zur Lageverschärfung bei: Angriffe müssen rechtzeitig erkannt, forensische Massnahmen eingeleitet und Abwehrmassnahmen getroffen werden. Falschmeldungen müssen berichtigt und Propaganda entkräftet werden. Desinformation und Verunsicherung in der Bevölkerung müssen mit sachlicher und überzeugender Kriseninformation auf Seiten der Behörden entgegnet werden.

Sabotage an kritischen Infrastrukturen

Zur Sabotage von kritischen Infrastrukturen sind für einen Gegner Cyber-Angriffe attraktiv, weil er unter geringen eigenen Risiken von irgendwoher beträchtliche Schäden verursachen kann. Digitalisierung, Vernetzung und Automatisation führen zu wachsenden Verletzlichkeiten für kritische Infrastrukturen und lösen Kettenreaktionen wie Versorgungsstörungen aus. So kann sich eine Gegenseite digitalen Zugang zu elektronischen Steuerungsanlagen verschaffen, um kritische Systeme zu sabotieren. Solche Angriffe können durch den Einsatz von Insidern flankiert sein. Bei schweren Angriffen kann das Funktionieren der staatlichen Führung, von wirtschaftlichen Abläufen und des gesellschaftlichen Lebens beeinträchtigt werden.

«Terrorismus gehört zu den realsten und akutesten Bedrohungen, auch für die Schweiz.»

Sicherheitspolitischer Bericht 2016

Für die GLF bieten spektakuläre Anschläge gegen öffentliche Gebäude sowie Objekte und Einrichtungen, denen eine Schlüsselfunktion für das Funktionieren des Landes zukommt, die Möglichkeit, den propagandistischen und effektiven Druck auf die Schweiz stufenweise zu erhöhen und über einen langen Zeitraum auf einem hohen Niveau zu halten. Ausserdem können Gefährdungen von kriti-

schen Objekten der Energieversorgung, des Transportnetzes, der Kommunikation oder des Finanzsystems im Sinne taktischer Ablenkungsmanöver geschehen, um Sicherheitskräfte punktuell zu binden und die Aufmerksamkeit im Sinne des Angreifers zu lenken. Schliesslich beinhaltet die GLF-Ideologie den Willen, die industrialisierte, westliche Welt durch Terror und Gewalt in ihren Grundfesten zu erschüttern.

Von einer erhöhten Gefährdung kritischer Infrastrukturen sind alle Sicherheitsbereiche von Bund und Kantonen wie auch die Privatwirtschaft betroffen. Die Akteure des Bevölkerungsschutzes sind gefordert, um die Resilienz zu gewährleisten und die Konsequenzen von Ereignissen zu bewältigen. Die Polizei muss Wechsel- und Folgewirkungen für die öffentliche Sicherheit beachten und die Armee ist neben dem Schutz für die eigenen Einrichtungen und Systeme mit Gesuchen für subsidiäre Unterstützung konfrontiert.

Terroranschläge – Eskalation der Sicherheitslage

Angriffe gegen Menschen mit Waffen, Fahr- oder Flugzeugen, Sprengstoff, eventuell auch mit radiologischen, biologischen oder chemischen Substanzen, sind die emotionalste und tödlichste terroristische Bedrohung. Im Szenario der SVU 19 eskaliert die Situation über eine längere Zeit. Die fiktiven Anschläge von Genf im November 2017 erschütterten das schweizerische Selbstverständnis als eines der sichersten Länder der Welt. Seither sind Privatwirtschaft und Behörden gefordert, in physische Schutzmassnahmen und elektronische Überwachungsmittel zu investieren. Die Polizeipräsenz im öffentlichen Raum muss über einen längeren Zeitraum sichtbar erhöht werden, um dem gestiegenen und anhaltenden Sicherheitsbedürfnis gerecht zu werden. Die Dauerbelastung stellt die Durchhaltefähigkeit der Sicherheitskräfte auf die Probe. Zahlreiche Kantone müssen mangels eigener Mittel subsidiäre Unterstützung durch die Armee anfordern.

Auch wenn sich danach die Sicherheitslage durch die ergriffenen Massnahmen und das Ausbleiben von konkreten Hinweisen auf Angriffe bis Mitte 2018 etwas entspannt, bleibt eine Grundlast sowohl wegen den Fähigkeiten der GLF als auch ihrem Motiv gegen die Schweiz bestehen. Bedrohung und Eskalation nehmen dann sukzessive wieder zu und führen zu einer erhöhten Gefährdung für Leib und Leben. Mit Aufrufen zu Anschlägen auf die Finanzwelt rückt die Schweiz noch konkreter ins Visier der GLF. Es muss jederzeit damit gerechnet werden, dass GLF-Zellen physische Anschläge gegen Einrichtungen in der Schweiz oder schweizerische Einrichtungen im Ausland verüben. Am wahrscheinlichsten sind mit wenig logistischem Aufwand vorbereitete Angriffe von Kleingruppen oder Einzeltätern mit Schusswaffen und improvisierten Sprengmitteln. Ausserdem muss jederzeit mit einem breiten Spektrum von Cyber-Angriffen gegen behördliche und privatwirtschaftliche Ziele gerechnet werden.

Alle sechs Monate ein Lagebericht

Verschiedene Partner im Sicherheitsverbund haben sich bereits mit der Thematik einer anhaltenden Terrorbedrohung intensiv auseinandergesetzt. In diversen Kantonen und Verwaltungen konnten unter anderem Konsequenzen abgeleitet und mögliche Massnahmen getroffen werden. Zudem wird auf Stufe Bund unter der Leitung von fedpol und dem Führungsstab Polizei im Nachgang zu jedem Lagebericht ein operativer Dialog zu den jeweiligen Lagebeurteilungen geführt. Auch im Sicherheitsverbund Schweiz und in der Kerngruppe Sicherheit wird die fiktive Terrorbedrohung intensiv behandelt.

Im kommenden Jahr werden zwei weitere Lageberichte die fiktive Terrorbedrohung fortführen. Die Ereignisse dieser beiden Übungsdokumente werden sich vor allem mit den Themen der Sabotage kritischer Infrastrukturen und der Eskalation der Sicherheitslage befassen. Die Ausgangslage und das Drehbuch der Stabsrahmenübung setzen die Ereignisse der Lageberichte fort. ■

Major a D
Bernhard Wigger
Dr. phil., Historiker
Nachrichtenoffizier,
Projektleiter SVU 19
3303 Jegenstorf

Oberst i Gst
Christian Hirschi
Wissenschaftlicher
Mitarbeiter SVU 19
Generalsekretariat VBS
3232 Ins

Cyber Observer

Biometrie. Alle Jahre wieder als Allheilmittel angepriesen. Man müsse sich nicht mehr mit leidigen Passwörtern auseinandersetzen. Passwörter, die man vergessen kann oder die gestohlen werden. Alles wird also besser mit Biometrie!

Alles? Nicht ganz. Zwar spricht man gerne von «biometrischer Authentisierung». Das eigene biometrische Merkmal wird ja genutzt, um den entsprechenden Zugang zu erhalten. Fingerabdruck bei Smartphones gibt es seit Jahren. Gesichtserkennung wird alternativ oder zusätzlich eingesetzt.

Wenn solche Mechanismen gut umgesetzt sind, dann finden sie bei den Nutzern eine hohe Akzeptanz. Unkompliziert und zuverlässig müssen sie aber sein.

Doch damit ist eigentlich der Hauptvorteil biometrischer Verfahren schon zusammengefasst. Mit ihnen gehen jedoch eine Reihe von Nachteilen einher. Zum Beispiel, dass sich so manches biometrische Merkmal durchaus nachbilden lässt. Die Rillen, die einen Fingerabdruck ausmachen, können mit Weissleim abgebildet werden. Und eine Gesichtserkennung der ersten Generation lässt sich mit einem Foto überlisten.

Doch damit nicht genug. Sah sich jemand nämlich in der Lage, den Fingerabdruck «zu stehlen», kann dieser fortan missbraucht werden. Im Gegensatz zu einem Passwort lässt sich der Fingerabdruck nämlich nicht ohne weiteres ändern.

Es ist deshalb wichtig zu verstehen, dass Biometrie in erster Linie ein «Erkennungsmerkmal» und kein echtes «Authentisierungsmerkmal» ist. Jedenfalls keines, das den modernen Anforderungen genügen würde. Biometrie sollte die Eingabe des Benutzernamens ersetzen. Und in unkritischen Fällen die Eingabe des Passworts. Wo Sicherheit aber wichtig ist, darf Biometrie alleine nicht das Mass der Dinge sein ... Denn nicht alles wird besser mit Biometrie.

Marc Ruef
Head of Research, scip AG