**93. Sitzung des AK V am 11./12. Oktober 2017 in Wiesbaden**

**Bericht zu TOP xx**

# Strategische Krisenmanagementübung zum Schutz der nationalen Informationsinfrastrukturen und kritischen Infrastrukturen

## Auftrag:

Die IMK hat den AK V gem. Ziff 3. des Beschlusses zu TOP 50 der IMK vom 12. bis 14.06.2017 beauftragt, *„zu prüfen, wie eine strategische Krisenmanagementübung zum Schutz der nationalen Informationsinfrastrukturen und kritischen Infrastrukturen unter Beteiligung des Bundes, der Bundeswehr (Kommando CIR), der Länder (Fachministerien), der Kommunen und der Betreiber kritischer Infrastrukturen durchzuführen wäre und in Abstimmung mit den zuständigen Gremien der IMK zur nächsten Sitzung im Herbst 2017 Eckpunkte für ein Übungsszenario vorzustellen."*

## Eckpunkte:

Die vorgesehene strategische Krisenmanagementübung mit Cyberbezug und der Betroffenheit kritischer Infrastrukturen ist fachlich notwendig: Sie bedarf aufgrund der Verknüpfung thematischer Bezüge (Cyber / Kommunikationsstrukturen / KRITIS) und der großen Zahl zu beteiligender Akteure (Bund, Bundeswehr, Länder, Kommunen, Versorgungswirtschaft) einer besonders intensiven Vorbereitung. Deshalb wird auf das bewährte Format der LÜKEX-Übungen zurückgegriffen. Dies ermöglicht einen raschen Start der Arbeiten und führt zügig zu ersten Erkenntnissen.

In einem in der Regel zweijährigen Vorbereitungszeitraum werden im LÜKEX-Prozess das Szenario erstellt und durch eine umfassende thematisch/inhaltliche Befassung die Grundlagen für die eigentliche praktische Übungsdurchführung gelegt. Damit ist die Übungsvorbereitung ein wesentlicher Baustein der Übung. Das Format ist daher sehr gut für Vorbereitung und Durchführung einer breit angelegten, vielschichtigen und bundesweiten Übung unter Beteiligung einer Vielzahl von staatlichen und privatwirtschaftlichen Akteuren geeignet.

Die Thematik Schutz der nationalen Informationsinfrastrukturen und kritischen Infrastrukturen sowie die Verknüpfung beider Themen sollen in den Übungsfolgen 2018 bis 2020 in einem abgestuften Verfahren mit jeweils auch spezifischen Schwerpunkten beübt werden.

Zunächst soll hierzu die Übung LÜKEX 2018 um die Übungsziele der Kommunikationsfähigkeit bei Ausfall der Regelkommunikationswege unter erstmaliger Einbindung des BSI und der Bundeswehr (Kommando CIR) ergänzt werden.

Die Übung 2020 soll als Schwerpunktthema Cybersicherheit als fachlichen Inhalt haben. Das zu entwickelnde Szenario soll sich dabei an jenem orientieren, das derzeit im Prozess zur Umsetzung der neuen Konzeption Zivile Verteidigung erarbeitet wird. Demnach könnte ein Cyber-Vorfall die Stromversorgung betreffen und wäre insbesondere die Reaktions- und Handlungsfähigkeit von Regierung und Verwaltung zu betrachten.

Zur Übungsvorbereitung zu beiden Übungen gehören verschiedene Veranstaltungsformate, wie zum Beispiel Thementage, zur fachlichen Vorbereitung und Vertiefung einzelner Schwerpunkte.

**LÜKEX 2018**

Die für 2018 geplante LÜKEX-Übung hat eine Gasmangellage zum Inhalt und somit bereits einen KRITIS-Bezug. Die bisherige Übungsvorbereitung erfährt keine grundlegende Änderung in Bezug auf das Übungsszenario, sondern wird lediglich um nachfolgende Aspekte ergänzt:

a) Kommunikationsfähigkeit der Beteiligten auch bei Ausfall der Regelkommunikationswege (zum Beispiel durch einen zu vermutenden Cyberangriff) und

b) Einbindung des BSI und der Bundeswehr mit ihrem Kommando CIR und Beübung der Kommunikationswege unter Berücksichtigung ihrer Zuständigkeiten.

Neben den bereits vorgesehenen Übungsbeteiligten werden das BSI und das Kommando CIR zusätzlich eingebunden.

Durch die vorgeschlagene Ergänzung können bereits in der Übung 2018 auch für die Bewältigung eines Cyber-Angriffs wesentliche Elemente beübt werden.

**LÜKEX 2020**

Für den Übungszyklus LÜKEX 2020 wird als Szenario ein Cyberangriff auf die KRITIS der Stromversorgung zugrunde gelegt. Die Übung baut auf die Erkenntnisse der LÜKEX 2018 bei den Kommunikationswegen und bei der Zusammenarbeit mit dem BSI und der Bundeswehr (Kommando CIR) auf.

Basis des Szenarios bildet das Referenzszenario „Cyberangriff auf eine kritische Infrastruktur", das derzeit in der Umsetzung der Konzeption Zivile Verteidigung (KZV) erarbeitet wird. Auf diese Weise wird eine enge Verzahnung des KZV-Prozesses und der LÜKEX-Übung sichergestellt. Gewonnene Erkenntnisse können somit verlustfrei und wechselseitig in die jeweiligen Prozesse einfließen.

Aufgrund der Komplexität und der Vielzahl einzubindender Beteiligten wird der Zyklus „LÜKEX 2020" bereits im Januar 2018 begonnen. Dies eröffnet die Möglichkeit, sehr frühzeitig in die Übungsvorbereitung einzusteigen, erste Erkenntnisse zu generieren und ggf. bereits in die Übungsdurchführung der LÜKEX 2018 im November 2018 einfließen zu lassen.

**Beschlussvorschlag:**

1. Der AK V nimmt den Bericht zur strategischen Krisenmanagementübung mit Cyberbezug zur Kenntnis.

2. Der AK V bittet die IMK, wie folgt zu beschließen:

    1. Die IMK nimmt den Bericht des AK V zur Kenntnis.
    2. Die IMK beschließt folgende Eckpunkte einer strategischen Krisenmanagementübung zur Bewältigung einer Cyberlage:
        a) Zum Schutz der nationalen Informationsinfrastrukturen und kritischen Infrastrukturen wird eine Übungs- und Ausbildungsfolge unter Einbeziehung der Krisenmanagementübungen LÜKEX 2018 und 2020 durchgeführt.
        b) Die Übung LÜKEX 2018 (Gasmangellage) wird um die Themen Kommunikationsfähigkeit und Einbindung der Kommunikationswege mit dem BSI und der Bundeswehr erweitert.

c) Die Übung LÜKEX 2020 wird einen Cyberangriff auf die KRITIS mit einem Schwerpunkt Aufrechterhaltung der Staats- und Regierungsfunktionen zur Grundlage haben.

3. Die IMK stellt fest, dass mit der Cyber-Übung LÜKEX 2020 der wichtige Prozess der Neuen Konzeption Zivile Verteidigung aufgegriffen und kohärent mit behandelt wird, da dies einen wichtigen Baustein für die Sicherheit der deutschen Bevölkerung darstellt.

4. Die IMK bittet den Bund umgehend eine Projektgruppe LÜKEX 2020 einzurichten und mit der Übungsvorbereitung zum 1. Januar 2018 zu beginnen.