Anhang 3 – Klärungsbedarf zu Gesetz VIII und IX

· 14. Oktober 2025

> Dieses Dokument fasst die offenen und klärungsbedürftigen Punkte für die Ausschussarbeit zusammen und präzisiert Zuständigkeiten, Abläufe und Schutzmechanismen für Krisenlagen.

1. Zuständigkeitsabgrenzung (BKIE ↔ BSEE ↔ BSI ↔ Bundeswehr)

Im Fall eines Sicherheitsvorfalls ist die Reihenfolge der Maßnahmen wie folgt zu verstehen:

- **Erstmeldung** durch die **zivile Behörde**, die das betroffene System beaufsichtigt oder genehmigt hat (z. B. BKIE oder BSI).
- **Weiterleitung** an das **BSEE**, das die Koordination zwischen zivilen, militärischen und internationalen Stellen übernimmt.
- **Übergabe der Einsatzleitung** an die **militärische Seite**, sobald bestätigt ist, dass der Vorfall sicherheitsrelevant oder strategisch gefährdend ist.
- **Technische Abschaltung und Schadensbegrenzung** durch die zuständigen militärischen IT- und Cyber-Einheiten in Abstimmung mit dem BSEE.
- **Dokumentation und Ursachenanalyse** verbleiben vollständig in ziviler Hand (BKIE).

2. Definition „Krisenlage / außergewöhnliche Gefährdung“

Eine Krisenlage im Sinne dieses Gesetzes liegt vor, wenn mindestens eine der folgenden Bedingungen erfüllt ist:

- Ausfall oder Manipulation kritischer Infrastruktur (Energie, Kommunikation, Verkehr, Gesundheit, Verteidigung).
- Massiver Datenverlust oder Informationsverfälschung durch KI-Systeme.
- Fehlverhalten autonomer Systeme mit unmittelbarer Gefahr für Leib, Leben oder Staatssicherheit.
- Zivile oder militärische Systeme sind nicht mehr steuerbar oder kommunikationsfähig.
- Internationale Eskalationsgefahr durch digitale Fehlsteuerungen.

3. Eingriffsrecht und Reaktionszeit

- In der **ersten Stunde** nach Eintritt einer Gefährdung entscheidet die **Fachinstanz mit der höchsten technischen und operativen Kompetenz**, unabhängig vom Verwaltungsrang.
- Diese Instanz wird im **BSEE-Leitungsgremium** institutionalisiert, mit Zugriff auf alle relevanten zivilen und militärischen Kommunikationskanäle.

- Das BSEE ist befugt, **sofortige Schutzmaßnahmen** einzuleiten, bevor eine parlamentarische Genehmigung vorliegt, sofern Gefahr im Verzug ist.
- Die Entscheidung ist anschließend binnen **48 Stunden** zu legitimieren und vollständig zu dokumentieren (`EvoLog`).

4. Rolle der KI in Krisenzeiten

- KI-Systeme werden **ausschließlich beratend** eingesetzt (Analyse, Prognose, Muster- und Risikoerkennung).
- Entscheidungen über Einsatz, Abschaltung, Ressourcenzuteilung oder Kommunikation erfolgen **nur im Zusammenspiel zwischen Mensch und Maschine** (Vier-Augen-Prinzip).
- Das Vier-Augen-Prinzip: eine menschliche Verantwortungsperson + ein autorisiertes KI-System im BSEE-Register.
- Fehlerhafte Analysen/Fehlfunktionen der KI führen zur **temporären Deaktivierung** bis zur menschlichen Überprüfung.

5. Internationale Meldekette und Koordination

- Meldeweg: **Nationale Institution → Bundesregierung/Krisenstab → EU-Krisenkoordination → NATO-KI-Gremium**.
- Ziel: schnellstmögliche internationale Informationsweitergabe zur Abwehr grenzüberschreitender digitaler Bedrohungen.
- Erstmeldung an das BSEE innerhalb von **60 Minuten** nach Feststellung; internationale Benachrichtigung innerhalb von **3 Stunden**.

6. Kommunikation gegenüber der Öffentlichkeit

- Die Bevölkerung wird bei aktivierten Krisenmaßnahmen grundsätzlich informiert.
- Veröffentlichung ausschließlich über eine **zentrale, neutrale Stelle** unter Aufsicht des BSEE.
- **Gestuftes Informationssystem** (öffentlich / intern / geheim) analog zu erprobten Presseordnungen.
- Prinzip: *Transparenz ohne Gefährdung der Sicherheit*.

7. Finanzierung und Ressourcenstruktur

- Primär: **Bundesmittel** (Digital- und Verteidigungshaushalt).
- Ergänzend: **Lizenzen, Zertifizierungsentgelte, Förderprogramme**, Forschungskooperationen (ethik-konform).
- Möglichkeit einmaliger **Systemlizenzierungen** für staatliche Dauer-Nutzung.
- **Sonderfonds** für besonders sicherheitsrelevante Bereiche.

8. Langzeitarchivierung und Rückführbarkeit von Krisendaten

- Archivierung in einer **nationalen, gesicherten Datenbank** mit Geheimschutzstufen.
- Zugriff nur für autorisierte Prüfinstanzen/Forschung mit Sicherheitsfreigabe.
- Aufbewahrung: mindestens **30 Jahre**, sicherheitsrelevante Fälle bis **50 Jahre**.
- Nutzung zu Forschungszwecken zulässig, sofern **anonymisiert** und BSEE-genehmigt.

Hinweis: Dieses Dokument dient als Arbeits- und Diskussionsgrundlage für den Fachausschuss. Es konkretisiert offene Punkte, ohne bestehende Kompetenzen anderer Behörden zu ersetzen.