Bundesministerium
Landesverteidigung

bmlv.gv.at

Abteilung Fremdlegislative und internationales Recht

Mag. Sandra MAYER
Sachbearbeiterin

+ 43 502011021020
Roßauer Lände 1, 1090 WIEN

An das
Bundeskanzleramt
Ballhausplatz 2
A-1014 Wien
nis @bka.gv.at

Geschäftszahl: S91031/16-FLeg/2018 (1)

Entwurf eines Bundesgesetzes zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz - NISG);
Stellungnahme

Zu der vom Bundeskanzleramt/I.6 elektronisch übermittelten Note vom 19. September 2018, GZ BKA-180.310/0234-I/6/2018, betreffend den **Entwurf eines Bundesgesetzes zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsystemsicherheitsgesetz - NISG)** nimmt das Bundesministerium für Landesverteidigung wie folgt Stellung:

I. Grundsätzliche Vorbemerkung zur aktuellen Entwurffassung:

Die unionsrechtlichen Vorgaben der **Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen, zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union** (ABl. L 194 vom 19. 7. 2016, S 1) sollen in Österreich durch den do. der allgemeinen Begutachtung zugeleiteten Legislativvorschlag in jetziger Fassung umgesetzt werden. Auf Grund der Tatsache, dass hinsichtlich der **gesamtstaatlich** zu beurteilenden „**Cyber-Sicherheit**“ das **BMLV** einer der **vorrangigsten Akteure im Cyberbereich** ist, verwundert diese Fassung nun insofern, zumal der Erstentwurf eines solchen NISG im Zeitraum Mai 2016 bis Jänner 2018

in einer interministeriellen Arbeitsgruppe textiert worden ist, die sich aus Juristen/IKT-Fachleuten des BKA, BMI und BMLV zusammensetzte. Zwischen diesen drei Bundesministerien und dem BMEIA wurde gleichzeitig auch noch an der aktuell neu zu formulierenden **Cyber-Sicherheitsstrategie (ÖSCS 2.0)** gearbeitet. Der von dieser legistischen Arbeitsgruppe trilateral akkordierte Normvorschlag, welcher in seinen jeweiligen Fortschrittsstadien im Vorjahr regelmäßig in den zuständigen **CSS-Gremien** (behördenintern) und im Rahmen der **CSP** (im Rahmen einer PPP mit den führenden Branchen-/Sektorenunternehmen aus dem Bereich der kritischen Infrastruktur) vorgestellt worden war, wurde am 1. Februar 2018 von der Präsidialchefin des BKA entgegengenommen.

Die in § 6 Entwurf NISG (Stand 30. 1. 2018) aufgelisteten **Aufgaben des Bundesministers für Landesverteidigung als operative NIS-Behörde** wurden nun ersatz-/begründungslos gestrichen. Somit sind die **Cyberverteidigung durch das Bundesheer**, die **Sicherheitsbetreuung und Zertifizierung von Betreibern wesentlicher Dienste**, deren Dienste der Erfüllung von Aufgaben des Bundesheeres gemäß Art. 79 Abs. 1 B-VG dienen, und die **internationale militärische Zusammenarbeit** in Angelegenheiten der Netz- und Informationssystemsicherheit im vorliegenden Entwurf nicht mehr enthalten. Durch den Entfall dieser weitreichenden NISG-Normierungen, welche die militärische Landesverteidigung mit den einschlägigen MBG-Tatbeständen korrespondiert hätten, ergibt sich somit der Schluss, dass es sich beim vorliegenden Entwurf um ein **rein ziviles Regelungsmodell** handelt. Somit sind hinsichtlich eines Sicherheitsvorfalls im Cyberraum, die den **Verteidigungsmaßnahmen der Landesverteidigung gemäß Art. 79 B-VG** zuzurechnen sind, ausschließlich die einsatzrechtlichen Bestimmungen des **Militärbefugnisgesetzes (MBG**) anzuwenden.

Die **militärische „Cyberverteidigung**“ ist vom materiengesetzlichen Begriff der „Cyberkrise“ gemäß der §§ 3 Z 18 und 21 des Entwurfs strikt zu trennen, die ihrerseits ausschließlich zivilen Ursprungs/Inhalts ist. Diese im nunmehr zu beschließenden NISG **kompetenzbezogen vorgenommene Trennung** lässt sich unionsrechtlich aus der einschlägigen RL 2016/1148 ableiten, die keinen ausdrücklichen Militärbezug hat - die nach B-VG und BMG innerstaatlich differierenden Aufgabengebiete der Polizei und des Bundesheeres wurden jüngst auch in den Erläuterungen zum PStSG und der SPG-Novelle 2014 betont.

So wird etwa in den Erläuterungen zu **§ 8 PStSG** explizit zwischen den Regelungsbereichen des BMI und BMLV unterschieden, hier wörtlich „… *Aufgabe des Bundesamtes sowie der Landesämter soll es künftig sein, staatsschutzrelevante Bedro-*

hungslagen, also Gefährdungen verfassungsmäßiger Einrichtungen oder deren Handlungsfähigkeit, der Bevölkerung durch terroristische, weltanschauliche oder politisch motivierte Kriminalität, durch Spionage und nachrichtendienstliche Tätigkeit, durch Proliferation, illegalen Handel mit Kriegsmaterial sowie Waffen, Schieß- und Sprengmittel rechtzeitig zu erkennen und dahingehend zu beurteilen, ob sich daraus eine staatsschutzrelevante Bedrohung ergibt, worüber die in Abs. 2 und 3 genannten verfassungsmäßigen Einrichtungen zu informieren wären. … Hingegen ausdrücklich ***nicht erfasst ist der Vollziehungsbereich des Bundesministers für Landesverteidigung*** *~~(und Sport)~~,* ***insbesondere die Zuständigkeiten, die sich aus dem Militärbefugnisgesetz (MBG) ergeben****. So sind beispielsweise im Sinne des § 20 MBG sämtliche Informationen von sicherheitspolitischer Bedeutung aufklärungsfähig, wozu insbesondere die internationale Krisenbeobachtung oder die Beurteilung der militärstrategischen Lage zählen."*

Aus den Erläuterungen zu Z 5 **(§ 22 Abs. 1 Z 6) SPG-Novelle 2014** kann die Unterscheidung zwischen den Aufgabengebieten des BMLV und BMI ebenso herausgelesen werden, siehe hier etwa wörtlich: „*Die nach sonstigen Bundes- oder Landesgesetzen bestehenden Kompetenzen im Bereich des Schutzes kritischer Infrastrukturen bleiben von der sicherheitspolizeilichen Neuregelung unberührt. Dies betrifft insbesondere die* ***Zuständigkeit des Bundesheeres im Rahmen seiner gesetzlichen Aufgaben (Art. 79 B-VG und § 2 Abs. 1 WG 2001)*** *sowie die in die Kompetenz der Länder fallenden Aufgaben im Bereich des Katastrophenschutzes."*

Der durch § 3 Z 20 Entwurf NISG (Fassung vom 30. 1. 2018) ursprünglich normierte Begriff der „**Cyberverteidigung**" umfasst sämtliche vom Bundesheer im Rahmen der militärischen Landesverteidigung gemäß **Art. 79 Abs. 1 B-VG** zu setzenden Maßnahmen zur Bewältigung von Sicherheitsvorfällen, die einen Angriff auf die Souveränität der Republik Österreich darstellen. Dies schließt auch Maßnahmen zur Gewährleistung der IKT-Sicherheit im Rahmen der allgemeinen Einsatzvorbereitung des Bundesheeres nach § 2 Abs. 3 WG 2001 ein; davon unberührt bleibt jedoch die Befugnis militärischer Organe zum **Schutz militärischer Rechtsgüter** gemäß § 1 Abs. 8 MBG. Dem BMLV kommt daher innerhalb der ihm von der Bundesregierung erteilten Ermächtigung (**Art. 80 Abs. 2 B-VG**) die Entscheidung über das Vorliegen eines Anlassfalles der Cyberverteidigung zu.

Vor diesem Hintergrund nimmt das Bundesheer die **Cyberverteidigung als Teilbereich der militärischen Landesverteidigung** (Art. 79 Abs. 1 B-VG) operativ wahr. Die Durchführung der Cyberverteidigung erfolgt auf der Grundlage aller dafür ge-

eigneten einsatzrechtlichen Bestimmungen durch die dafür erforderliche Einsatzorganisationsstruktur (vgl. den Wortlaut von § 24 Entwurf NISG (30. 1. 2018)).
Die Ressortzuständigkeit des Bundesministers für Landesverteidigung ergibt sich aus der Subsumption der Cyberverteidigung unter die „militärischen Angelegenheiten" nach Teil 2 der Anlage zu § 2 BMG.

Die **militärische Sicherheitsbetreuung und Zertifizierung von Betreibern wesentlicher Dienste** iSd § 10 Abs. 1 und 3 Entwurf NISG (30. 1. 2018), deren Dienste der Erfüllung von Aufgaben des Bundesheeres gemäß Art. 79 Abs. 1 B-VG dienen, sind von grundlegender Bedeutung für die ständige Einsatzbereitschaft des Bundesheeres - auch die davon betroffenen Unternehmungen wären - dem Vernehmen nach wegen der dadurch erhöhten Reputation am internationalen Markt - daran interessiert gewesen, dass diesen Teil NISG-Vollzug das ho. Ressort wahrnimmt.

Abschließend wird darauf hingewiesen, dass die Beschlussfassung dieses NISG ho. zum Anlass genommen werden wird, um zu beurteilen, ob die entsprechenden **wehrrechtlichen Bestimmungen** allenfalls anzupassen sind.

II. Zu einzelnen Bestimmungen des Entwurfs:

1. Zu § 11 Abs. 1 und 4 („Gemeinsame Verarbeitung"):

Dem vorliegenden Entwurf zufolge wird der Bundesminister für Landesverteidigung in Zukunft nicht im Wege eines NIS-Büros (§ 3 Z 7 des Entwurfs) agieren. Neben dem Bundeskanzler als „strategischer" NIS-Behörde und dem Bundesminister für Inneres als „operativer" NIS-Behörde wird das **BMLV** - so wie seit jeher angestrebt - hingegen sowohl dem **IKDOK** (§ 7 Abs. 1 des Entwurfs) als auch dem **Koordinationsausschuss** (§ 22 Abs. 2 des Entwurfs) durch Experten **angehören**. Die Entscheidung über das Vorliegen einer (zivilen) „Cyberkrise" soll der Bundesminister für Inneres nach vorheriger Konsolidierung mit dem IKDOK und dem Koordinationsausschuss treffen. Das dafür benötigte Lagebild, auf Grund dessen operiert wird, entsteht unter der Federführung des BMI mit Beitragsleistungen durch den IKDOK.

Zur **Gewährleistung des gegenseitigen Informationsaustausches auf dem Gebiet der staatlichen Sicherheit** (so wie dies im **Regierungsprogramm 2017-2022** mit dem Titel „***Zusammen. Für unser Österreich***" mehrfach zum Ausdruck gebracht

wird) und zur **verfassungsgesetzlichen Auftragserfüllung durch das Bundesheer** wird § 11 Abs. 1 und 4 des Entwurfs daher begrüßt.

2. Zu § 19 Abs. 2 („Sicherheitsvorkehrungen und Meldepflicht für Einrichtungen des Bundes“):

Durch diese Bestimmung in jetziger Form würde auch das BMLV verpflichtet sein, einen internen Sicherheitsvorfall materiengesetzlichen Inhalts an das GovCERT zu melden.

Im Lichte der oben bereits erwähnten §§ 7, 11 Abs. 1 und 4 sowie 22 Abs. 2 des Entwurfs wird ersucht, neben dem BKA und dem BMI zusätzlich auch noch das **BMLV** von dieser Meldeverpflichtung **auszunehmen**.

Legistisch wäre daher im § 19 Abs. 2 jeweils nach dem Wort „*Inneres*“ die Wortfolge „***oder das Bundesministerium für Landesverteidigung***“ einzufügen.

3. Zu § 27 („Vollziehung“):

Der Entwurf sieht infolge § 11 Abs. 1 und 4 auch materiengesetzliche Zuständigkeiten das BMLV vor, weshalb die Vollziehungsvorschrift des § 27 angepasst werden müßte.

Legistisch wäre daher im § 27 nach dem Wort „*Bundeskanzler*“ das Wort „*und*“ durch einen Beistrich zu ersetzen und nach dem Wort „*Inneres*“ die Wortfolge „***und der Bundesminister für Landesverteidigung***“ einzufügen.

III. Mitteilung:

Unter Einem wird mitgeteilt, dass diese Stellungnahme ebenfalls per E-Mail dem Präsidium des Nationalrates übermittelt werden wird.

WIEN, am 31.10.2018
Für den Bundesminister:
MinR Mag. Christoph MOSER

Elektronisch gefertigt